# An Exploratory Data Analysis of the Network Behavior of Hive Home Devices

Asmau Wali [1], Oluwasegun Apejoye [2], Jun He [3], Xiaoqi Ma [4]

*Department of Computer Science*

*Nottingham Trent University*

Nottingham, UK

asmau.kazaure2018@my.ntu.ac.uk [1]

oluwasegun.apejoye2020@my.ntu.ac.uk [2]

ORCID 0000-0002-5616-4691 [3]

ORCID 0000-0003-0074-4192 [4]

***Abstract*— Smart homes are gaining more popularity by the day due to the ease they provide in terms of running our homes. However, the energy and resource constrained nature of the smart home devices make security integration challenging, thus making them prone to cyber-attacks. This calls for a need to carry out extensive research on the behavior of these devices in order to design and incorporate better security tailored to their behavior. This paper collects traffic from the Hive home network and carries out an Exploratory Data Analysis (EDA) in terms of their behavior due to the lack of attention they face from the research community despite being one of the largest smart home service providers in the UK. The areas covered are device identification, traffic classification, device mode of control identification, flow volume, flow duration and protocols utilized by these devices both in active and idle states. Some of the covered areas involve components, which are exploited and used maliciously in DDoS flooding attacks, thus this paper compares the normal behavior of these components, to when they are exploited during attacks and in turn giving the end user what to watch out for in the case of an attack.**

***Keywords— exploratory data analysis, Hive home devices, device behavior, network characteristics, device mode of control, traffic analysis, device identification, DDoS***

## I. INTRODUCTION

IoT devices are becoming more popular in our daily lives due to the advantageous services they render to users. These devices cover a broad surface in terms of connectivity ranging from but not limited to, healthcare, home automation, weather forecast, transport, agriculture, security and a variety of other dimensions. IoT further gives us the ability to have more control over IoT ecosystem. By tailoring these devices to run exactly when we need them, this improves our energy conservation plans. We also get to monitor devices' usage in real time, which paves way for accountability when the need arises. It is estimated that 150,000 IoT devices join the global network every minute [1].

However, the energy and resource constrained nature of these devices make them prone to cyber-attacks [2] [3] [4] [5] [6]. This, in addition to their heterogeneous nature, makes security implementation challenging [7] [8]. The device vendors are not helping matters too as their focus is more aligned to device functionality and features rather than security [9]. This poses risks in terms of privacy and security as the lives of individuals are directly affected [10]. Several IoT attacks have been propagated [11] [12] [13]. Furthermore, these attacks are moving at a much faster pace than security countermeasures.

This brings the need for proper research and security integration into these devices and the networks they form in order to protect the devices and privacy of users. However, this cannot be achieved without an in depth study and analysis of device and user behavior within a network as these observations and analyses will be used to tailor security protocols that will suit the IoT ecosystem in question.

Smart home, being one of the most popular and relatable IoT to users, has gained a lot of attention in the research community. This has led to growth in research relating to smart home behavior and security. Several works have addressed smart home device identification or fingerprinting [1] [10] [14] [15] [16] [17] [18] [19] [20] [21] [22]. Privacy attacks from the adversary angle have also gained much attention within the research community, thereby being able to profile a smart home users' behavior [23] [24] [25] [26] [27] [28] [29] from unencrypted logs.

However, with all the tremendous developments mentioned above, it was observed that Hive home devices face a lack of interest or attention with regards to behavioral identification or fingerprinting from the research community. Going through literature, it was observed that there is hardly any mention of Hive devices being analyzed. Existing works mostly focus on Google home, Amazon Alexa, DLink, TPLink, PhiliphsHue and the like. It is found that a paper can analyze ranging from 30 to 200 IoT devices but with no single Hive device. This includes recent and state of the art papers [14] [15] [16] [17] [18] [19]. Despite the absence of Hive devices being a point of interest in research, it was discovered that [30]:

- Hive is one of the largest connected smart home providers in the UK, as at 2018 it had over one million customers.
- It is owned by British Gas, thus the reason why British Gas promotes the use of Hive active heating (A smart thermostat allowing customers to control water and heating remotely via the app or their website).
- Hive home app is one of the highest rated smart

RESEARCH FUNDED BY PTDF NIGERIA

home apps in the UK with over 68,000 customer reviews.

Furthermore, reviewed literature focuses on device fingerprinting and classification will less emphasis on the behavioral patterns to watch out for during an attack. This is a very important aspect in securing our smart homes, as we will have an early detection plan in case of an attack.

This brings about the motivational need to analyze Hive home devices. This work carries out an EDA on Hive home devices, which is a method, used to analyze datasets summarizing their main characteristics using data visualization techniques. The unencrypted network logs collected from the Hive network can be used to identify Hive devices from a pool of other IoT devices, which will be useful in device identification and management to detect rogue or unauthorized devices on a network [15]. The behavior of Hive devices can also be compared to other similar devices from other vendors using this data as a reference point. Several behavioral components of the Hive devices are analyzed in comparison to when they are maliciously used in DDoS attacks. This will aid in tailoring the security details against such attacks. Device mode of operation of these devices is also studied, as this has never been addressed from past literature, thus this work also being a pioneer in this field. Five modes of operation will be looked at in this paper which are, controlling the devices using the proprietary Hive home app, using Google home app and home kit app which are compatible with Hive devices, automated control by scheduling times on the Hive app and finally manually operating the devices.

The contribution of this paper is 2 folds:

- First, it collects network data from the Hive home network over a period of one week due to unavailability of Hive dataset in existing works.
- Secondly, it performs EDA on the collected logs visualizing the behavior of these devices covering the following aspects: flow volume, flow duration, protocols, traffic categorization, device identification, and varying flow volumes and duration based on device mode of control (manual, automated, Hive app, home kit app, Google home app) and compares their normal behavior to when they are used maliciously as bait in DDoS attacks.

This paper is organized as follows: Section 1 introduces the paper. Section 2 talks about the tools used and data collection process. Section 3 delves into Hive home devices EDA and relates it to DDoS propagation while section 4 concludes the paper.

## II. Tools and Data Collection

Hive home smart devices were used for this study. The devices include a smart hub (to integrate the smart devices), a motion sensor, a smart plug and a smart bulb. The network communication that takes place when these devices are both idle and active is the main point of interest, thus a setup to collect this network data for further analysis was carried out.

Hardware and software tools used are listed as follows:

- Netgear GS308E – 100NAS switch
- Samsung A12 smart phone
- Mac book air OS X El Capitan 10.11.6
- Jupyter Notebook
- TL-WR940N Router
- IPhone SE
- IPad
- LAN cable
- Wireshark 2.6.0
- Hive starter pack (motion sensor, plug, Bulb, hub)
- Hive home app v.10.44.0 (6)
- Google home app v.2.42.120
- Home kit app 14.4.2

Traffic generated from/to each of the mentioned devices was captured separately in order to know the type of network traffic that relates to a particular device. In order to get very detailed network traffic, the capture setup was made to collect traffic at layer 2 (datalink). This was done by connecting the hub to port 1 of the switch. Port 8 of the switch was then connected to the router (for internet connection). In order to capture all that flowed in and out of the hub and all devices paired to it, port 1 was mirrored on port 4. Port 4 was connected to the laptop using a Local Area Network (LAN) cable and Wireshark was used to capture this traffic over a period of one week. This capture setup is depicted in Fig. 1. Data was captured in trenches like during boot/pairing, event triggers and idle moments. The event trigger test cases used to arrive at the results in this research are:

- Switching plug ON & OFF via the five modes listed
- Switching bulb ON & OFF via the five modes listed
- Setting motion sensor to trigger bulb ON for five minutes and plug ON for 10 minutes if motion is detected. The plug and bulb go OFF after 5 and 10 minutes respectively if no motion is detected.

## III. Exploratory Data Analysis and DDoS Patterns

This section delves into the EDA of the unencrypted collected logs and further relates it to how some of the network components are exploited and used maliciously in DDoS attacks. EDA is a statistical method of analyzing data so as to summarize the main characteristics of the dataset by using data visualization tools and techniques to represent the results derived for ease of understanding. Jupyter notebook is the tool used for this purpose. The areas covered were chosen for specific reasons. Traffic categorization was covered in order to have a holistic view of the kind of traffic Hive devices exchange. This will help in addressing strange and malicious traffic. Device identification was carried out in order to know the fingerprint of each device so as to be able to identify Hive devices in a pool of other IoT. Protocols and flow volume and duration were studied as these aspects are used in propagating DDoS attacks. Studying them will help in knowing the normal Hive traffic pattern when it comes to protocol sequence, flow volume and duration in comparison to malicious use of them in flooding attacks. This section is further divided into

subsections addressing traffic categorization, device identification, protocols in both Idle and active states, flow volume (total number of incoming and outgoing bytes in one cycle) and flow duration (time it takes from the beginning of a flow to the end).

### A. *Traffic Categorization*

Traffic collected from this network was broadly categorized into 3 after analysis. These categories are:

- Periodic queries: These queries were found to take place automatically regardless of an event trigger ranging from every few minutes to some hours depending on the protocol or device. The hub was studied without pairing any device to it so as to capture the network activity that takes place in its lone state. This was repeated with devices (plug, lamp, motion sensor) paired to the hub in order to identify what happens differently in this scenario. Fig. 3 shows this periodic activity originating from the hub without any device paired to it compared to when a device is paired to the hub over a period of 2 hours. As seen from Fig. 3 there is more frequent DNS, TCP and TLS activity happening when a device is paired to the hub as opposed to when the hub is on its own.
- Event trigger: This kind of traffic gets generated whenever an event is triggered. For instance, when the plug or lamp goes ON or OFF or the motion sensor detects movement. This results in generation of DNS, TCP AND TLS packets. In some cases, MDNS traffic is also generated depending on the mode of operation used to trigger the event.
- Boot, pairing and firmware updates: This traffic is generated whenever the hub is in boot mode, when paring with the devices or a firmware update takes place. A fixed number of DNS servers are communicated with when these take place.

### B. *Device Identification*

Each device was paired with the hub individually so as to get a unique fingerprint of the device. This method will help in identifying each device from the type of traffic it generates when all devices are paired to the hub. However, it was discovered that all 3 devices have a similar pattern. All devices utilized the same source MAC and IP Address, which is that of the hub. They also utilized the same protocols and server-side port numbers. Furthermore, when an event is triggered, all devices have the same traffic pattern of contacting the same DNS servers, having the same flow volume and duration as will be seen in subsequent sections of this paper. However, one slightly different behavior was observed which differentiated the motion sensor from the plug and lamp. When it detects motion, a DNS query and response is established as mentioned earlier which is the same with the plug and lamp. However, the motion sensor always establishes another DNS query 5 minutes later, which is not the case for the plug and lamp. Fig. 2 shows event triggered DNS activity from these devices, independently. The lamp and bulb have a single peak when an event is triggered while the motion sensor has a distinct pattern of having 2 peaks for every event trigger. In Fig. 2 the lamp was triggered at 12:00, 1:00, 2:30 and at 3:30, all having a single peak. The plug was triggered at 2:30, 3:30 and 4:30 with single peaks as well for each trigger. The motion sensor detected motion 3 times between 8:30 and 12:00 each time having double peaks when motion was detected. As observed from the section above in periodic queries, the hub has a unique pattern of generating periodic traffic like TCP Keep Alive, DNS, ARP, and DHCP. This unique traffic makes it easier to identify the hub in a pool of other IoT devices.

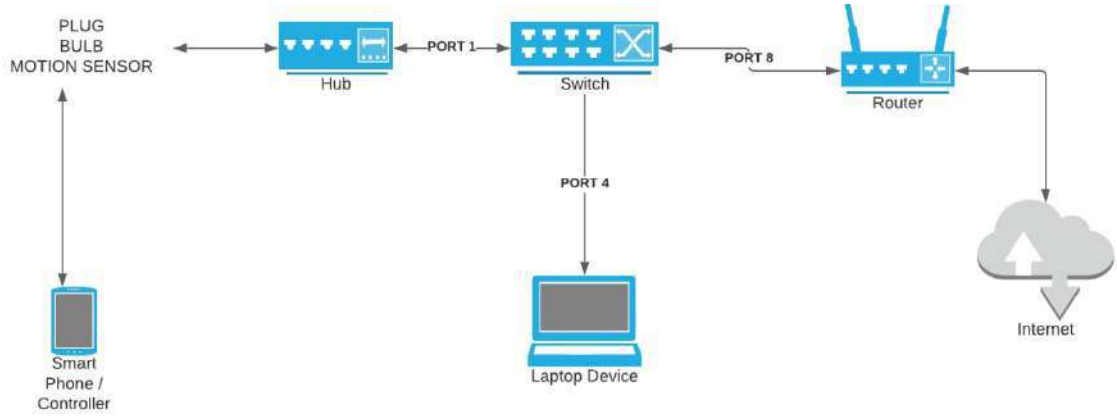


**Figure 1 Data collection connectivity**

### C. *Protocols (idle and active states)*

These devices both in idle and active state utilize several protocols. The hub sends TCP Keep Alive messages every 14 and then every 19 seconds. This message tends to keep the hub awake to prevent the connection between the client (hub) and the server from breaking, which is why this takes place frequently. Another protocol is NTP (Network Time Protocol) taking place every 34 minutes. NTP is a protocol utilized by IoT devices, as very accurate timings are highly important in IoT communication. This happens periodically to synchronize their time with publicly available NTP servers. DNS requests are also made to four particular addresses every 3 to 4 hours. Other protocols observed were TLS, ARP, ICMPv6, DHCP and MDNS. This shows that the hub regardless of a device paired to it, or an event being triggered generates this traffic intermittently. By pairing a device to the hub and triggering events, the frequency of some of these protocols increase. The ratios of these protocols are compared over 2 hours when the hub is not paired with any device, when the hub is paired with devices but are in idle state and when there is activity (event triggers). This is shown in Fig. 3. It is observed that the volume or count of some of these protocols like DNS (52), TCP (3143) AND TLS (1423) drastically increase due to the

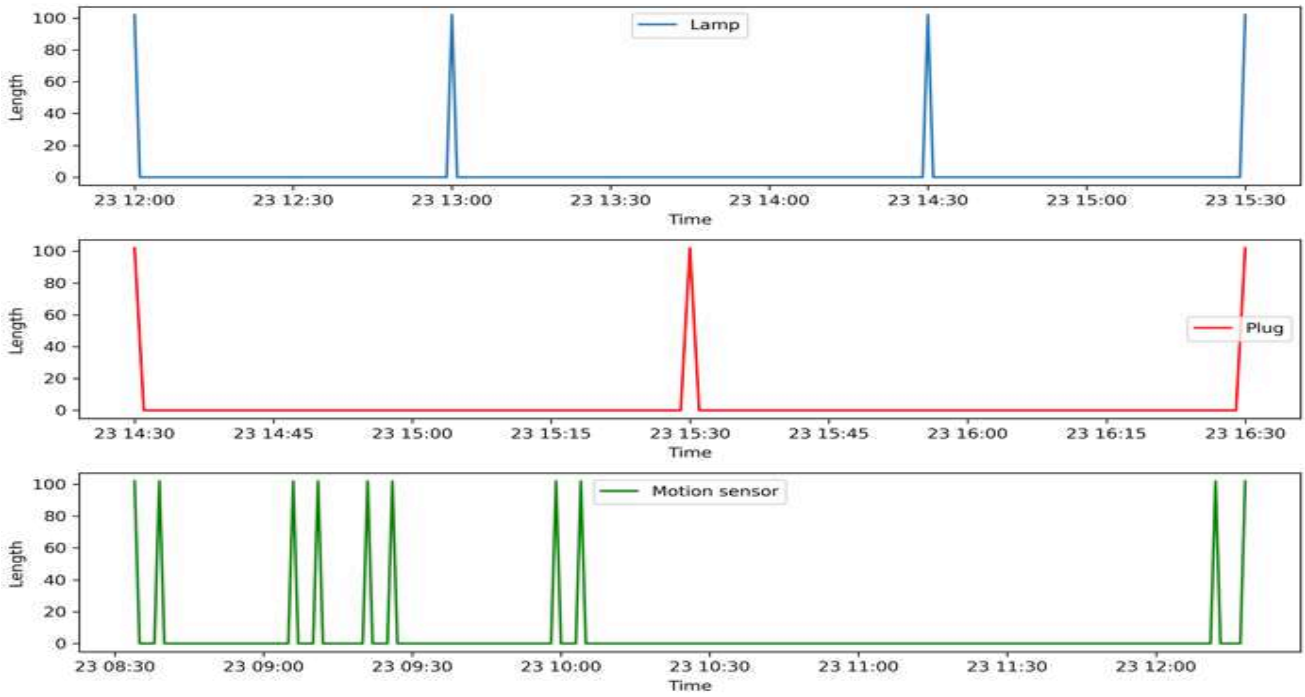


Figure 2 Device identification by activity pattern

presence of activity while NTP (8) and DHCP (4) remain fairly the same. The hub without devices paired has the least count of these protocols DNS (10), TCP (2239) TLS (900), NTP (8) and DHCP (4) followed by when devices are idle which shows a slight increase in DNS (22), TCP (2401) and TLS (1003) while NTP (8) and DHCP (4) remain the same.

This protocol data gives us an idea on the frequency or count of the several protocols utilized by these devices over time. We can see that there is a limit or cap to how frequent these get generated as opposed to when a flooding attack takes place violating this limit. For instance, an ICMP, ARP or TCP flooding attack does not have a limit as to the number of packets transferred neither does it have an interval in between flows. By applying this normal behavioral limit not to be exceeded over a certain period of time, this can help reduce the severity of the attack.

*D. Flow volume and Duration*

Whenever an event is triggered, or boot and pairing modes are taking place or some particular periodic updates take place, a DNS query and response happens. A TCP connection is then established which follows a TCP sequence routine of SYN, ACK, FIN+ACK, and ACK. This also involves a client and server handshake and a change of cipher spec between the smart devices and the DNS servers. This entire process is referred to as a flow. The total number of bytes exchanged in this entire flow is known as the flow volume while the total time it takes for one complete flow is the flow duration. This was computed by getting the time difference between the first and last packet in that flow. Packets in a flow come in pairs consisting of a request and reply packet. Each packet also has a fixed length. Furthermore, a single flow comprises of several combination of protocols as we have seen. This can include DNS, TCP, TLS and MDNS. The flow volume and flow duration differ for each mode of operation and also when an event is triggered by one device compared to when multiple devices are triggered like a motion sensor detecting movement and triggering the light bulb to go ON. The Hive devices were tested in 5 different operation modes. This was carried out using several control devices, which are Samsung A12 phone, iPhone SE and an iPad. This was done to make sure these discovered distinct patterns for each mode are uniform across a variety of control devices. The operation modes tested were:

- Using the Hive proprietary app: The Hive app was used to control these devices after downloading it on the above-mentioned devices.
- Using Google home app: The Google home app was used to control these devices after downloading it on the above-mentioned devices.
- Using home kit: This app comes preloaded on apple devices (iPhone, iPad). This app is compatible with Hive devices just like the Google home app.
- Manually: The devices (plug and smart bulb) were controlled by physical means by turning their switch ON and OFF.
- Scheduled: Using the Hive app, times when the devices should automatically go ON and OFF were set without any manual intervention either physically or via the apps.

Traffic was captured from all the above-mentioned control modes so as to identify a pattern for each mode and mode and also the flow volume and duration. The trigger trigger times for each mode of operation was noted so as to use these for cross referencing during analysis. Several unencrypted parameters were captured including source, destination, time, packet length, protocol and info (a column that gives extra details like packet sequence and labels). Fig. 4 shows the varying flow volumes and duration for the different modes of operation. It is observed that when we use any of the smart phone apps (Hive, home kit, Google home) to control the devices, the flow volumes and duration tend to be higher compared to when we operate the devices manually or the scheduled way, which have the same

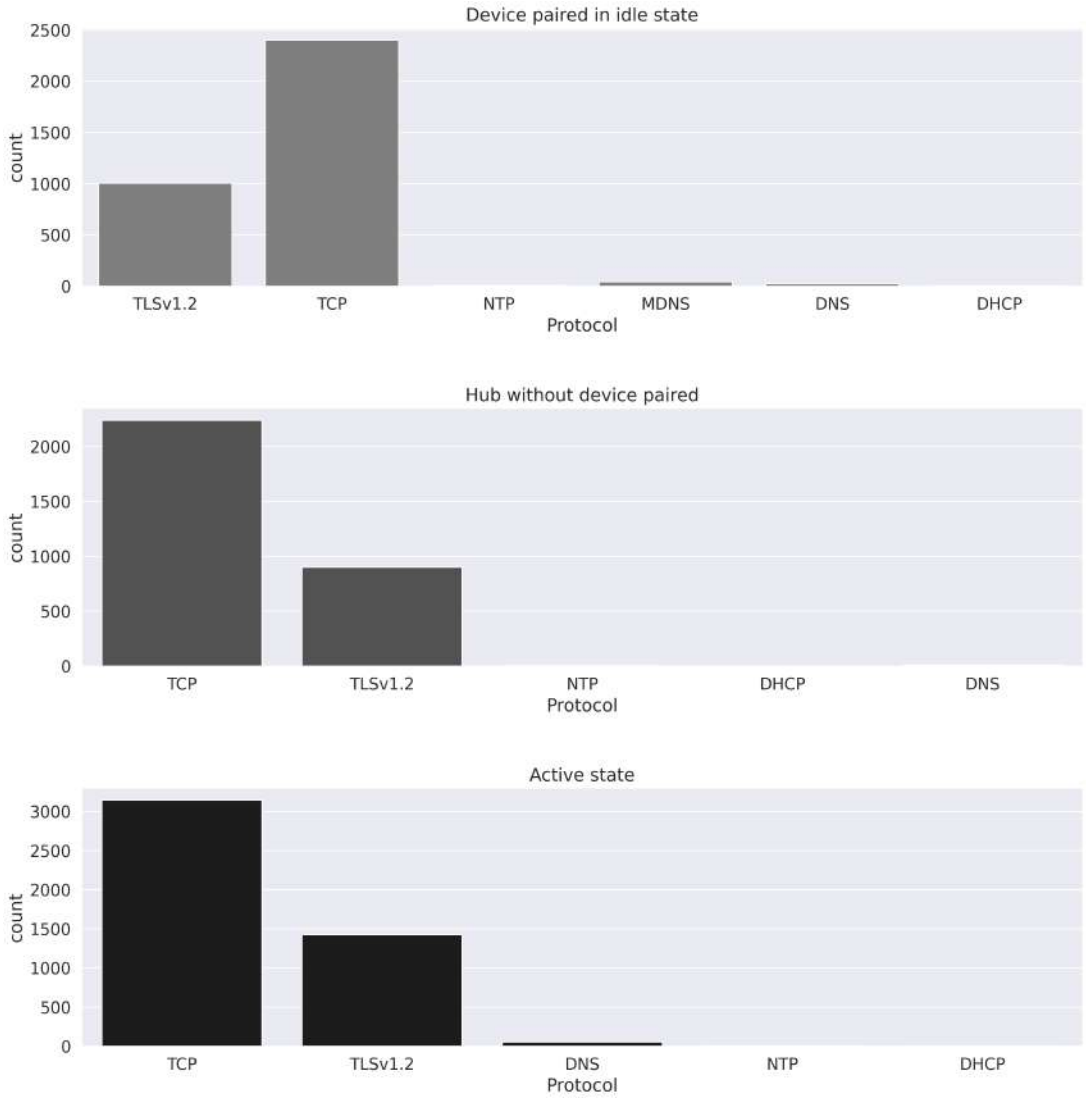


**Figure 3 Protocol count compared by device state**

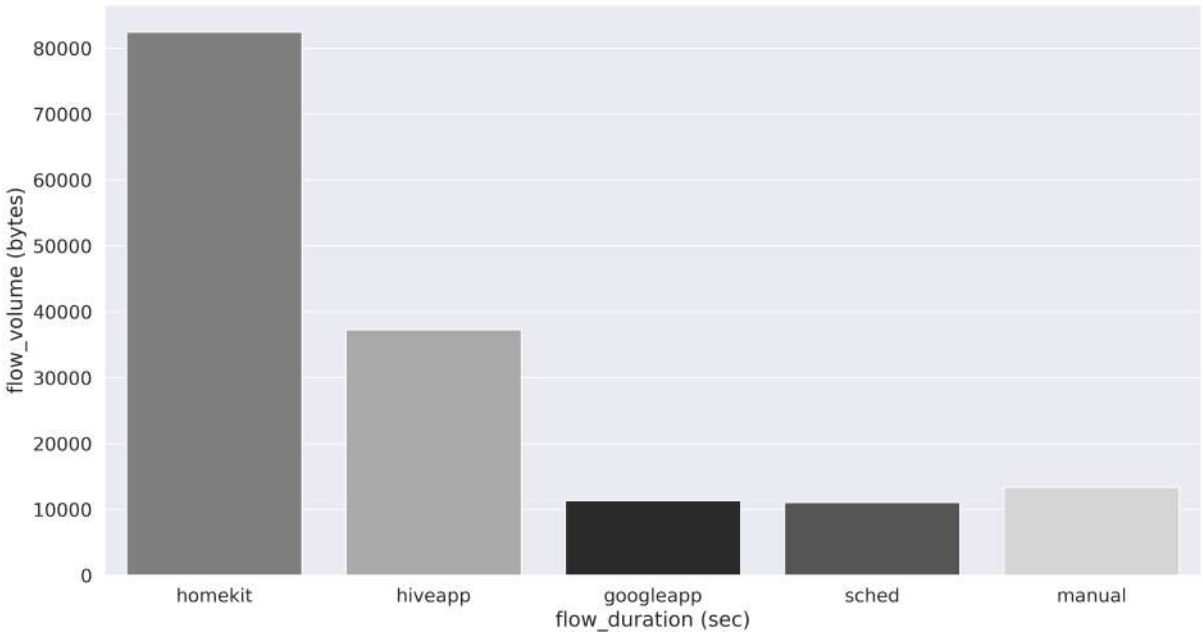


**Figure 4 Device mode of operation by flow volume and duration**

flow volume and duration. This increase in volume is due to the extra traffic generated as a result of using an application to control the devices. Mere opening any of the apps generates bytes of traffic without triggering an event. The duration is also longer as a result of extra time taken by the user to launch the app and further trigger an event as opposed to the scheduled and manual modes that has no delay involved during the flow, as there is less human intervention. Fig. 5 also shows the varying flow volumes and duration of a triggered event originating from one device compared to when the motion sensor triggers the plug and bulb to go ON (integrated form).

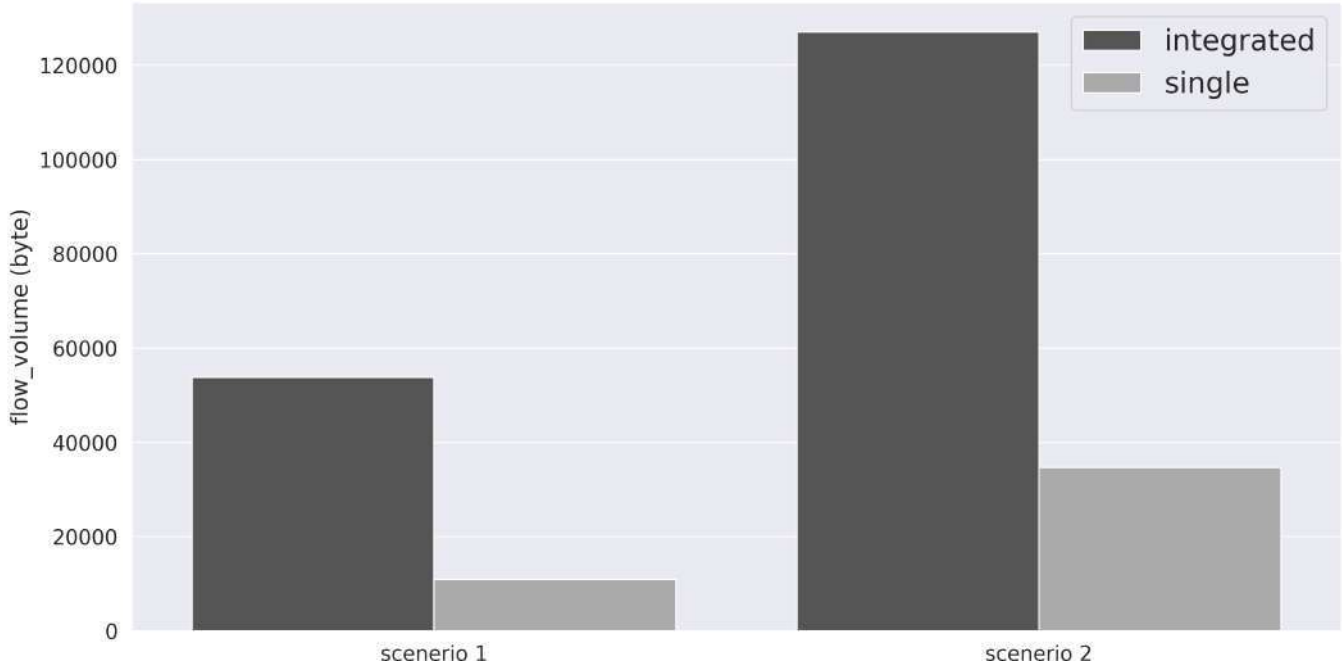


Figure 5 Single vs. integrated device traffic

Both the flow volume and duration of the traffic that originated as a result of multiple devices being active at the same time is higher. Fig. 6 shows idle and active periods (triggered event) of the devices using a scatter plot. DNS protocols are used in the scatter plot. It shows the periodic DNS protocols that take place every 19 minutes

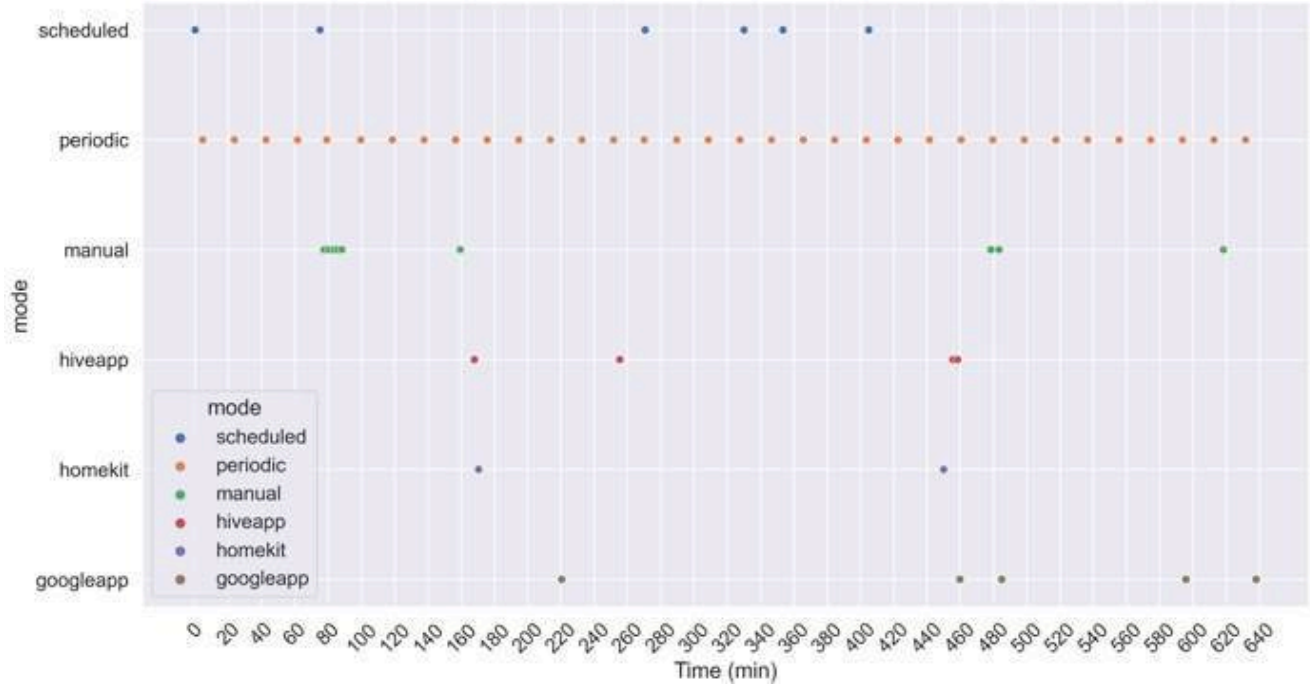


Figure 6 Triggered events with mode of operation identified

while showing other times an event was triggered specifying the particular mode of operation used.

From this section we can see that a normal Hive TCP flow follows SYN, ACK, FIN+ACK, and ACK routine as opposed to a DDoS flooding attack that has a single routine label attributed to it. For instance, a TCP SYN flood attack has only the SYN label all through rather than the normal combination listed. Furthermore, packets flow in opposite directions as a reply packet is paired to each request packet

in the normal flow pattern. However, in a flooding attack like the TCP SYN, ICMP or UDP flooding attacks, the packet flow direction is one way. Packets keep coming in without any prior request for each packet. This makes the flow a one-way type as opposed to the normal two-way flow. A flow also consists of a combination of varying packet lengths as opposed to the lengths from a flooding source, which carries the same length for a vast number of packets. Lack of varied lengths in a flow should be flagged as a threat in this case. The flow volume and duration also matter in identifying a flooding attack. From this research it is observed that these devices have a certain flow volume over time. Each mode of operation has a unique figure when it comes to this. Furthermore, the flow volume and duration from a single device compared to multiple devices vary. These figures can be applied as a limit that should not be exceeded in certain conditions. If this normal limit gets exceeded, it could be that a flooding attack is in the way and an appropriate action should be put in place to curb the attack. Lastly, a normal flow process comprises of several protocols like DNS, MDNS, TCP and TLS. However, a flooding attack does not follow this combination as it carries a single protocol all through. Lack of varying protocols in a flow should raise a flag.

## IV. CONCLUSION

This paper has analyzed several behavioral aspects of Hive home devices. An EDA was performed on the unencrypted features from the captured logs addressing traffic categorization, device identification, protocols in both Idle and active states, flow volume (total number of incoming and outgoing bytes in one cycle) and flow duration (time it takes from the beginning of a flow to the end).

Based on these logs it conforms to [31] about generally categorizing M2M generated traffic into 3, which are periodic update, event driven and payload exchange. Furthermore, this research also agrees with [32] where it states that IoT communicates with a number of fixed DNS servers. Several protocols were found to be utilized by these devices, which vary in volume and duration depending on the device state (active or idle). The flow volume and duration were studied based on 2 factors, being device mode of control and single vs. multiple device activity. Interestingly we have seen that each mode of control has a varying flow volume and duration. The flow volume and duration from event-triggered activity generated by a single device is much less when compared to multiple devices triggered at the same time. On the aspect of device identification, the motion sensor and the hub have their unique patterns, but this was not the case with the plug and bulb as they had an identical pattern. This could be due to their similar basic functionalities of ON and OFF. Other similarities shared by all the devices are communication with the same DNS servers, server-side port numbers and protocols among others. This conforms to the findings in [15] that devices from the same vendor behave in a very similar manner. The idle and active moments of these devices can also be identified based on the drastic increase in the volume or count of certain protocols when active as we have seen in this study.

This work has also identified some key network components that get exploited and used maliciously to propagate DDoS flooding attacks. It has presented the normal behavioral pattern of these components and compared them to their malicious counterparts. On the normal pattern side, we see that Hive devices make use of several protocols with varying packet lengths during a flow while a flooding attack utilizes one protocol with the same packet length. A normal flow has a two-way communication pattern while a flooding attack is a one-way direction. The TCP packet sequence follows a normal pattern of SYN, ACK, FIN+ACK, and ACK while a flooding attack has just one sequence label like the SYN label in a TCP SYN flood attack. Lastly, these devices have a limit when it comes to flow volume and duration as opposed to a flooding attack, which has no limit. Taking these listed aspects into consideration during security design and integration will provide a more robust detection engine when it comes to DDoS flooding attacks.

Future work is aimed at exploring the device mode of control aspect on how it can be applied in security design and integration for these devices and other similar IoT in general. As each operation mode has a unique pattern, these patterns could be whitelisted on the smart home network in order to detect certain attacks relating to unauthorized control of device by rogue devices which might have a deviating pattern from the whitelisted ones. Another potential angle to work on is the use of machine learning in DDoS detection using the listed network features or components in this paper.


## ACKKNOWLEDGMENT

This research was funded by Petroleum Technology Development Fund (PTDF) Nigeria, with maximum support and expertise guidance by Nottingham Trent University (NTU).


## REFERENCES


[1] K. Kostas, M. Just and M. A. Lones, "IoTDevID: A Behaviour-Based Fingerprinting Method for Device Identification in the IoT," arXiv Preprint arXiv: 2102.08866, 2021.

[2] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in 2014 IEEE Conference on Communications and Network Security, 2014, pp. 79-84.

[3] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," in Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, 2017, pp. 1-6.

[4] L. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 180-187.

[5] K. Moskvitch, "Securing IoT: In your smart home and your connected enterprise," Engineering & Technology, vol. 12, (3), pp. 40-42, 2017.

[6] N. Dhanjani, "Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts. " O'Reilly Media, Inc.", 2015.

[7] J. Fernandes and A. Prakash, "Security analysis of emerging smart home applications," in 2016 IEEE Symposium on Security and Privacy (SP), 2016, pp. 636-654.

[8] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," IEEE Communications Surveys & Tutorials, vol. 21, (3), pp. 2671-2701, 2019.

[9] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," IEEE Communications Surveys & Tutorials, vol. 22, (3), pp. 1686-1721, 2020.

[10] B. Bezawada, M. Bachani, J. Peterson, H. Shirazi, I. Ray and I. Ray, "Behavioral fingerprinting of iot devices," in Proceedings of the 2018

Workshop on Attacks and Solutions in Hardware Security, 2018, pp. 41-50.

[11] D. Wood, N. Apthorpe and N. Feamster, "Cleartext data transmissions in consumer iot medical devices," in Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, 2017, pp. 7-12.

[12] J. Naughton, "Why the internet of things is the new magic ingredient for cyber criminals," The Guardian, 2016 [Online]. Available: https://www.theguardian.com/commentisfree/2016/oct/02/brian-krebs-ddos-attack-google-protection-cybercrime. [Accessed: 01- Sep- 2021].

[13] K. Brian, " Mirai IoT Botnet Co-Authors Plead Guilty"-Krebs on Security, 2017. [Online]. Available: https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/. [Accessed: 01- Sep- 2021].

[14] S. Marchal, M. Miettinen, T. D. Nguyen, A. Sadeghi and N. Asokan, "Audi "Toward autonomous iot device-type identification using periodic communication," IEEE J. Select. Areas Commun. , vol. 37, (6), pp. 1402-1412, 2019.

[15] A. Sivanathan, H. H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath and V. Sivaraman, "Classifying IoT devices in smart environments using network traffic characteristics," IEEE Transactions on Mobile Computing, vol. 18, (8), pp. 1745-1759, 2018.

[16] M. Mazhar and Z. Shafiq, "Characterizing smart home iot traffic in the wild," in 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI), 2020, pp. 203-215.

[17] Y. Amar, H. Haddadi, R. Mortier, A. Brown, J. Colley and A. Crabtree, "An analysis of home IoT network traffic and behaviour," arXiv Preprint arXiv: 1803.05368, 2018.

[18] K. Xu, Y. Wan, G. Xue and F. Wang, "Multidimensional behavioral profiling of internet-of-things in edge networks," in 2019 IEEE/ACM 27th International Symposium on Quality of Service (IWQoS), 2019, pp. 1-10.

[19] S. Dong, Z. Li, D. Tang, J. Chen, M. Sun and K. Zhang, "Your smart home can't keep a secret: Towards automated fingerprinting of iot traffic," in Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, 2020, pp. 47-59.

[20] Y. Meidan, M. Bohadana, A. Shabtai, J. D. Guarnizo, M. Ochoa, N. O. Tippenhauer and Y. Elovici, "ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis," in Proceedings of the Symposium on Applied Computing, 2017, pp. 506-509.

[21] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas and J. Lloret, "Network traffic classifier with convolutional and recurrent neural networks for Internet of Things," IEEE Access, vol. 5, pp. 18042-18050, 2017.

[22] A. Sivanathan, D. Sherratt, H. H. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath and V. Sivaraman, "Characterizing and classifying IoT traffic in smart cities and campuses," in 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2017, pp. 559-564.

[23] B. Copos, K. Levitt, M. Bishop and J. Rowe, "Is anybody home? Inferring activity from smart home network traffic," in 2016 IEEE Security and Privacy Workshops (SPW), 2016, pp. 245-251.

[24] R. Trimananda, J. Varmarken, A. Markopoulou and B. Demsky, "PingPong: Packet-level signatures for smart home device events," arXiv Preprint arXiv: 1907.11797, 2019.

[25] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A. Sadeghi and S. Uluagac, "Peek-a-boo: I see your smart home activities, even encrypted!" in Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2020, pp. 207-218.

[26] N. Apthorpe, D. Reisman and N. Feamster, "A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic," arXiv Preprint arXiv: 1705.06805, 2017.

[27] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan and N. Feamster, "Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic," arXiv Preprint arXiv: 1708.05044, 2017.

[28] T. OConnor, R. Mohamed, M. Miettinen, W. Enck, B. Reaves and A. Sadeghi, "HomeSnitch: Behavior transparency and control for smart home IoT devices," in Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, 2019, pp. 128-138.

[29] W. Zhang, Y. Meng, Y. Liu, X. Zhang, Y. Zhang and H. Zhu, "Homonit: Monitoring smart home apps from encrypted traffic," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 1074-1088.

[30] "Build your home with smart home technology | Hive Home", Hivehome.com, 2021. [Online]. Available: https://www.hivehome.com/. [Accessed: 29-Oct-2021].

[31] M. Laner, N. Nikaein, P. Svoboda, M. Popovic, D. Drajic and S. Krco, "Traffic models for machine-to-machine (M2M) communications: Types and applications," in Machine-to-Machine (M2M) Communications Anonymous Elsevier, 2015, pp. 133-154.

[32] K. Xu, F. Wang, S. Jimenez, A. Lamontagne, J. Cummings and M. Hoikka, "Characterizing DNS Behaviors of Internet of Things in Edge Networks," IEEE Internet of Things Journal, vol. 7, (9), pp. 7991-7998, 2020.