IoT-Sphere: A Framework To Secure IoT Devices From Becoming Attack Target And Attack Source

Syed Ghazanfar Abbas (ghazanfar.abbas@kics.edu.pk)
KICS, UET Lahore
Muhammad Husnain
KICS, UET Lahore
Ubaid Ullah Fayyaz
KICS, UET Lahore
Farrukh Shahzad
KICS, UET Lahore
Ghalib A. Shah
KICS, UET Lahore
Kashif Zafar
KICS, UET Lahore

Research Article

Keywords: IoT, IoT devices security, Difference Between IoT and Non-IoT, IoT attacks, IoT communication

Posted Date: January 29th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-170019/v1

IoT-Sphere: A Framework To Secure IoT Devices From Becoming Attack Target And Attack Source

Syed Ghazanfar Abbas
Al-Khawarizmi Institute of Computer Science (KICS)
University of Engineering and Technology, Lahore, Pakistan
ghazanfar.abbas@kics.edu.pk

Muhammad Husnain
Al-Khawarizmi Institute of Computer Science (KICS)
University of Engineering and Technology, Lahore, Pakistan
muhammad.husnain@kics.edu.pk

Ubaid Ullah Fayyaz
Al-Khawarizmi Institute of Computer Science (KICS)
University of Engineering and Technology, Lahore, Pakistan
ubaid@uet.edu.pk

Farrukh Shahzad
Al-Khawarizmi Institute of Computer Science (KICS)
University of Engineering and Technology, Lahore, Pakistan
farrukh.shahzad@kics.edu.pk

Ghalib A. Shah
Al-Khawarizmi Institute of Computer Science (KICS)
University of Engineering and Technology, Lahore, Pakistan
ghalib@kics.edu.pk

Kashif Zafar
National University of Computer and Emerging Sciences, Lahore, Pakistan
kashif.zafar@nu.edu.pk

***Abstract*—In this research we propose a framework that will strengthen the IoT devices security from dual perspectives; avoid devices to become attack target as well as a source of an attack. Unlike traditional devices, IoT devices are equipped with insufficient host-based defense system and a continuous internet connection. All time internet enabled devices with insufficient security allures the attackers to use such devices and carry out their attacks on rest of internet. When plethora of vulnerable devices become source of an attack, intensity of such attacks increases exponentially. Mirai was one of the first well-known attack that exploited large number of vulnerable IoT devices, that bring down a large part of Internet. To strengthen the IoT devices from dual security perspective, we propose a two step framework. Firstly, confine the communication boundary of IoT devices; IoT-Sphere. A sphere of IPs that are allowed to communicate with a device. Any communication that violates the sphere will be blocked at the gateway level. Secondly, only allowed communication will be evaluated for potential attacks and anomalies using advance detection engines. To show the effectiveness of our proposed framework, we perform couple of attacks on IoT devices; camera and google home and show the feasibility of IoT-Sphere.**

***Index Terms*—IoT, IoT devices security, Difference Between IoT and Non-IoT, IoT attacks, IoT communication**

1. Introduction

Internet of Things (IoT) is mainly about connected objects, spanning from home automation, transportation, logistics, environmental monitoring and smart cities [1]. In a recent Paloalto report, more than 30% of all network-connected endpoints are IoT devices (excluding mobile devices) at the average enterprise [2]. According to Gartner survey, there will be an estimated 8.4 billion connected objects in 2020. And by 2022 this number will reach up-to 20.4 billion [3]. Also the machine to machine connections are expected to raise from 5.6 billion (2016) to 27 billion (2024). In terms of revenue IoT industry is also believed to grow from $892 billion (2018) to $4 trillion (2025) [4]. These statistics affirm the significance and the fast pace growth of IoT in the near future.

The undeniable perks of IoT are amalgamated with serious security pitfalls, mainly due to constrained devices, manufacturers primary priority is not security and lack of legislation [5]. Poorly designed IoT devices allow attackers to carry out their nefarious actions; attacks on medical implantable devices [6], smart cars [7], smart toys [8], unauthorized access of voice recordings [11], smart meters attacks [10] etc. The insecurity of these connected devices not only a potential threat for IoT but also for the whole internet. Attackers can easily convert these exploit these constrained devices and carry out their nefarious actions. For instance, mirai was one of the first well-known IoT botnet exploited large number of vulnerable IoT devices. In the history of internet, it performed some of the most devastating DDoS attacks; in October 2016, it took down Twitter, Github, Netflix, CNN and many others in US and

the Europe [9].

Motivated by an increasing number of attacks on/from IoT devices, in this research we propose a defense system with two level of security. Confine the communication boundary of IoT devices and only evaluate the allowed communication using attack detection engine. Proposed framework is called IoT-Sphere. A sphere of trusted IPs that are only allowed to communicate with a respective device. Any communication other than the sphere IPs will be blocked at the gateway level and will not reach the device and vice versa. But still there is a possibility of malicious communication between a device and allowed IPs. Propose framework will continually monitor the trusted communication using advance attack detection engines; rules and/or machine learning based and block anomalies. Other than security, proposed framework will provide couple of other advantages; IoT-Sphere will reduce the work load on attack detection engines, because only allowed communication will reach them. Blocking unnecessary communication at the gateway will also save constrained devices resources; battery, computation and bandwidth. Key contributions of proposed research are:

- An easily manageable framework, that with best efforts secure IoT devices from cyber attacks and secure rest of the internet from potential attacks carried out by IoT devices.
- Presents a comparison of 50 devices; IoT and Non-IoT, based on IPs used in their communication.
- Implement couple of real time attacks on IoT devices; google home and wireless camera and show effectiveness of IoT-Sphere.

The most relevant existing research is [21], where authors secure IoT devices from botnet attacks using device profiling at gateway level. For each monitored device a profile was created on the gateway, consist of IPs that can communicate with the respective device. But our proposed framework has certain distinctions. Firstly, [21] proposed one level of security, create a profile of white listed IPs and only allow them to communicate with the respective device. Such defense mechanism has certain flaws; malicious IP can be part of white-list and malicious communication can be carried out by a trusted IP. To mitigate this, we propose another security level; continually evaluate the white listed IPs communication with attack detection engines. In this way any malicious communication from even allowed IPs will be identified and blocked. Secondly [21] proposed only for botnet attacks defense, but our proposed framework will cover larger attack vector; scanning attack, protocol vulnerabilities exploitation etc. Finally, we propose an easy way of creating and managing device sphere. Explicitly specify the possible benign communication duration and framework will create a complete device sphere.

In the rest of this paper, we will provide the literature review in Section II, difference between IoT & Non-IoT devices communication in Section III, and then describe the proposed framework in Section IV. Section V evaluates the effectiveness of proposed framework against attacks carried out on IoT devices, while Section V concludes the paper.

2. Literature Review

Numerous researchers have discussed the use of network-based security solutions for IoT due to constrained nature of devices. Mostly security solutions are equipped with anomalies detection engines that audit outside communication before it reaches target device. Some researchers also discussed solutions for securing attacks carried out by IoT devices, for instance botnets. To the best of our knowledge we are the first one to present a framework that with best efforts secure IoT devices from becoming attack target as well as attack source.

Researchers in [12] propose a gateway level security manager that is equipped with the latest reported devices vulnerabilities and their available patches. It intercepts the devices traffic and alert the user about potential vulnerabilities and their available patches. Authors in [13] negate external entities direct communication with IoT devices due to lack of proper authentication support on constrained devices. They suggest to use a better authentication supported device to communication between the external entities and IoT devices. Researchers in [14] propose gateway equipped with rules for identifying issues in IoT services. Authors in [15] use artificial neural network for detection of anomalies in IoT communication passes through the gateway. In [16], authors have developed network based security system for IoT devices to detect IoT botnet attacks using deep auto-encoders. The developed system, captures snapshots of the network and utilized deep auto-encoders to detect maliciousness of network traffic from the IoT devices. For testing and validation of the system IoT botnets used are: Mirai and BASHLITE. According to the authors, the developed system was able to accurately detect attacks generated from IoT botnets. In [17], authors developed an anomaly based Intrusion Detection System for IoT edge devices, named as Passban. The system was able to detect a variety of network based attacks such as port scanning, brute force, and SYN flood with minimum false positive rate. For testing and validation of the system, they have tested their system on a testbed of smart home environment. The developed system was deployed on IoT gateway, so that it can protect all the devices connected via IoT gateway. The proposed system was able to train itself automatically via legitimate traffic flow with the help of one class classification ML algorithm. Any traffic deviating from the legitimate traffic flow is detected and identified as an anomaly.

3. Difference Between IoT & Non-IoT Devices Communication

Proposed framework is based on our conclusion drawn from analysis of network communication of 50 devices [18] shown in Table. 1; IoT and Non-IoT. Network communication span over multiple days are publicly available in the

TABLE 1. IPs COUNT IN 50 DEVICES COMMUNICATION

Device	Type	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Day 8	Day 9	Day 10
Aria	IoT	4	4	4	4	4	4	4	4	4	4
D-LinkCam	IoT	13	12	13	11	12	12	11	12	12	12
D-LinkDayCam	IoT	4	4	4	4	4	4	4	4	4	4
D-D-LinkDoorSensor	IoT	3	4	5	3	3	4	3	3	4	6
D-LinkHomeHub	IoT	16	16	16	16	16	15	16	16	18	17
D-LinkSensor	IoT	14	12	13	13	13	13	14	13	14	14
D-LinkSiren	IoT	14	13	13	14	13	13	14	13	14	14
D-LinkSwitch	IoT	14	15	14	14	13	14	14	13	14	14
D-LinkWaterSensor	IoT	14	13	14	14	13	12	14	13	13	13
EdimaxCam1	IoT	4	4	4	4	4	4	4	4	4	4
EdimaxCam2	IoT	4	4	4	4	4	4	4	4	-	-
EdimaxPlug1101W	IoT	9	9	8	9	9	8	9	8	8	8
EdimaxPlug2101W	IoT	9	9	8	8	8	7	8	8	8	8
EdnetCam1	IoT	3	3	3	3	3	3	3	3	3	3
EdnetCam2	IoT	3	3	3	3	3	3	3	3	3	-
EdnetGateway	IoT	8	8	8	8	8	8	8	8	8	8
HomeMaticPlug	IoT	2	2	2	2	2	2	2	2	2	2
HueBridge	IoT	15	15	15	15	15	15	15	15	15	15
HueSwitch	IoT	8	7	8	8	8	7	8	7	7	7
iKettle2	IoT	3	3	3	3	3	3	3	3	3	3
Lightify	IoT	7	7	7	7	7	7	7	7	7	7
MAXGateway	IoT	6	6	6	6	6	7	7	6	7	7
SmarterCoffee	IoT	3	3	3	3	3	3	3	3	3	3
TP-LinkPlugHS100	IoT	5	6	5	6	6	6	7	6	5	8
WeMoInsightSwitch2	IoT	15	17	16	16	16	16	-	-	-	-
WeMoSwitch	IoT	11	12	10	12	10	11	12	11	10	12
WeMoSwitch2	IoT	15	18	17	16	16	-	-	-	-	-
Withings	IoT	5	5	5	4	5	4	4	5	4	4
Triby speaker	IoT	4	7	4	4	4	6	4	4	4	4
Withings smart baby monitor	IoT	13	13	13	13	12	15	12	14	14	13
Withings smart scale	IoT	5	5	5	5	5	5	5	5	5	5
Withings smart sleep sensor	IoT	11	4	5	4	5	4	7	4	7	6
TP-Link day night cloud camera	IoT	34	26	18	20	15	21	18	18	18	24
Smart Things	IoT	76	64	71	67	76	79	74	74	61	65
PIX-STARPhoto-frame	IoT	6	7	6	6	6	8	7	7	7	6
Netatmo Welcome	IoT	23	25	23	23	25	24	24	14	14	23
Netatmoweatherstation	IoT	17	17	17	17	17	17	17	17	17	17
NESTProtectsmokealarm	IoT	8	8	8	8	8	8	8	9	8	8
LightBulbsLiFXSmartBulb	IoT	152	152	158	142	142	152	151	141	147	153
InsteonCamerawired	IoT	31	30	31	33	29	29	29	32	32	30
Dropcam	IoT	3	9	3	7	3	9	3	3	3	3
iHome	IoT	9	6	6	6	8	6	6	15	11	-
BlipcareBloodPressuremeter	IoT	4	4	4	-	-	-	-	-	-	-
BelkinWemoswitch	IoT	7	8	7	11	4	10	7	6	7	10
Belkinwemomotionsensor	IoT	8	8	7	7	6	12	8	7	8	9
AmazonEcho	IoT	35	38	34	36	35	38	35	36	38	35
Samsung Galaxy Tab	-	140	111	84	101	108	0	140	52	143	121
Laptop	-	277	1010	807	-	-	-	-	-	-	-
MacBook	-	496	92	155	105	141	94	-	-	-	-
AndroidPhone	-	58	60	85	169	132	-	-	-	-	-

form of raw pcap files. Some files contain multiple devices communication. Firstly we separate each device communication and acquire unique IPs in their communication using tshark tool. Results are shown in Table 1. Traditional devices; laptops, mobile phones and tablets are considered Non-IoT devices. Researchers in [18] have already classified the devices in the data sets.

IoT devices communicate with limited number of destinations and most of them repeat in daily communication. On the contrary, Non-IoT devices communicate with large number of destinations, that randomly varies on daily basis. Therefore, confining the communication boundary of IoT devices is quite practical than traditional devices. Along with practical justification, our conclusion has empirical logic too. IoT devices are mostly developed for some specific tasks and work with minimal human intervention [20], therefore their communication boundary must be quite limited when compared with Non-IoT devices.

4. Proposed Method

In this research we propose a method that will strengthen the IoT devices security from dual perspectives; avoid devices to become attack target as well as a source of an attack. Architecture diagram of proposed framework is shown in Fig. 1. To achieve this dual security objective, we propose to confine the communication boundary of constrained devices; create a trusted communication environment, called IoT-Sphere. Each device sphere will consist of IPs, that are allowed to communicate with a respective device and vice versa. Any communication other than the allowed IPs will be blocked at gateway level and will not reach the target device. User will be notified once a non allowed IP tries to communicate with the sphered device. Proposed framework also considers the possibility of attacks carried out by the trusted IPs, for instance if a malicious IP added into white-list or a trusted IP later performs malicious communication. Therefore, we propose a continuous monitoring of white listed IPs communication using advance methods; rule-based and machine learning models. If any anomaly found, an alert will be generated for possible sphere update. Confining the communication boundary of an IoT device and continually monitor the trusted communication will surely reduce the potential of attacks carried by/on the device.

Another key distinction of proposed method is the quick and easy way of sphere management; sphere creation, modification, activation and deactivation. With one click a device communication sphere is created and easily modifiable. Now we will explain the modules of proposed method.

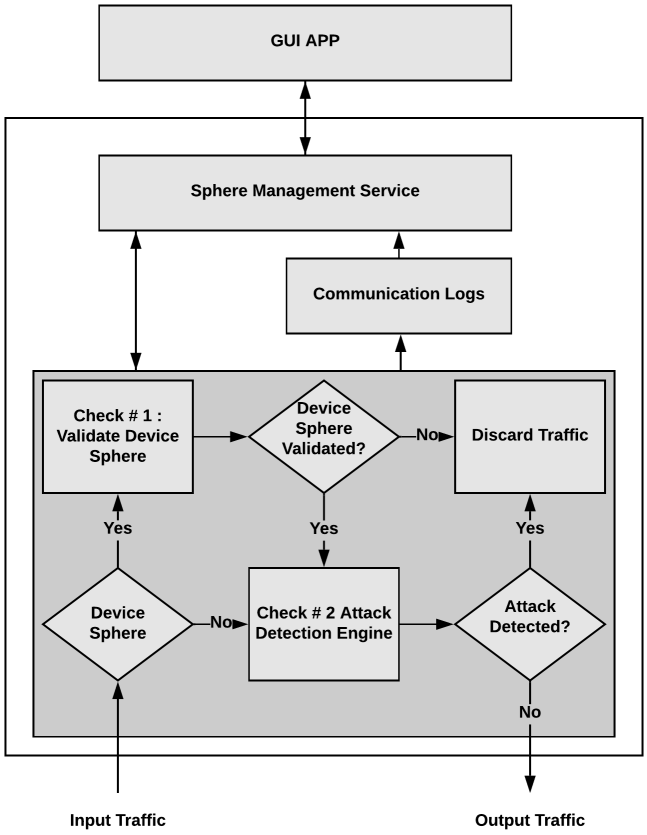

Figure 1. Architecture of Proposed Method

4.1. Communication Logs

A quick and an efficient method of defining and managing devices communication sphere is one of the key characteristic of our proposed method. Instead of manually define the IPs that can communicate with the device and vice versa. Propose framework will automatically display the actual IPs communicated with a device. Therefore devices communication log is an essential requirement. Many network based log gathering methods are available; routers port mirror, firewalls etc. Firewall will be an integral part of our proposed method, therefore we also consider it for acquiring communication logs.

Several open source IDS (Intrusion Detection Systems) are available; suricata [23], snort [24] etc. We have chosen suriata because of its distinctive features; multi-threading support, custom logging and live firewall policies update. Multi threading feature will increase propose system efficiency when it needs to deal with a large number of devices, custom logging will allow us to acquire the logs in require format and live firewall polices update will enable real time utilization of proposed method. Suricata deployed on a network gateway will be a central point of communication between devices inside and outside of a network. It will log all devices communication on the gateway. Whenever a connection is initiated by a device or towards a device, suricata log the source and destination IPs along with the time stamp. These logs will be utilized in further steps.

4.2. Sphere Creation

Once a device communication records are available on a gateway, it is a potential candidate for a trusted communication boundary. Sphere creation process will be initiated from a GUI application, that takes commands from users and communicate with the sphere management service. User will select a device from a list of available devices, shown in Fig. 2. Along with a device selection, user will also select the communication duration. Idea is to create sphere of a time span, that is attack free, according to end-user. For instance, initial communication span of a newly purchased device is more appropriate for a device sphere. Unique IPs that communicate with the device will be listed, shown in Fig. 3. Along with IPs, Urls if available in logs will also appear. GUI app gives the freedom to add IPs that are not available in list or remove existing ones. Finally, with a single click, device sphere is created on the gateway.

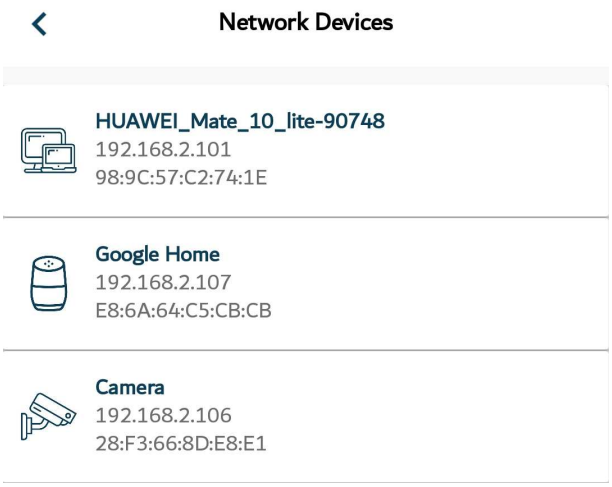

Figure 2. List of Available Devices Found in Communication Logs

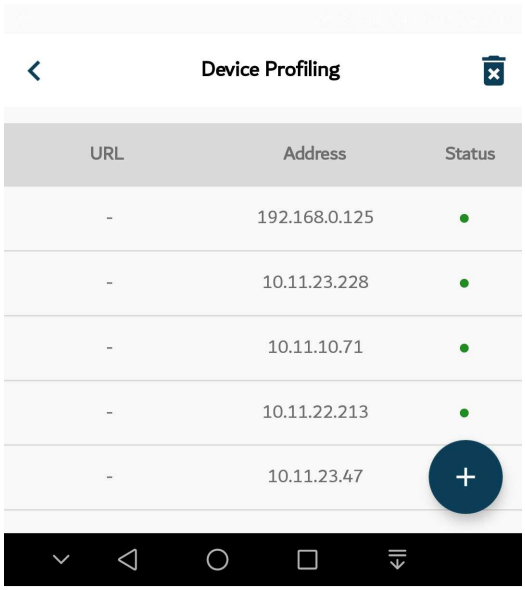

Figure 3. Unique IPs Communicated With a Respective Device

4.3. Sphere Implementation

Once a sphere is created, sphere management service is responsible to automatically implement the sphere. Sphere implementation is a process of converting the user defined sphere into firewall security rules. Sphere management service convert IPs defined in a sphere into a firewall rules. Rules are building blocks of security systems; firewall. It matches rules against the communication passes through it and perform the specified action on them; block, allow etc. Suricata rule for a sphere camera is shown in Fig. 4. It states that only IPs defined in the rule are allowed to communicate with the camera. Whenever, any non allowed IP try to communication with camera, it will be blocked at the gateway level.

Sphere implementation is the heart of the proposed system. It is an actual point when the communication boundary of a device is confined. Trusted communication that pass the sphere check will be further evaluated in attack detection engine. Attack detection engine will be equipped with security rules and/or machine learning model. In this research we consider the rules based attack detection. Many open source rules repositories are available, for instance emerging threats [24]. These rules are easily integrated in suricata and provide a strong line of defense against emerging cyber attacks; exploits, malwares, botnet, telnet attacks, phishing, scanning attacks, dos attacks etc. Once trusted communication is evaluated against these rules, it will further strengthen the devices security. Moreover when minimal communication is evaluated by the rules based engine its efficiency will be improved.

```
drop ip 192.168.2.106 any <> ![192.168.0.125, 10.11.23.228, 10.11.10.71,
10.11.22.213, 42.96.193.232, 10.11.23.59, 10.11.34.22, 10.11.20.108, 120.24.36.178,
10.11.23.110, 10.11.20.83, 10.11.23.47, 10.11.18.232, 196.168.0.196, 10.11.10.58,
47.74.152.38, 10.11.10.59, 10.11.19.237, 192.168.2.102, 10.11.22.175,
10.11.10.100, 10.11.10.52, 10.11.23.205, 10.11.14.42, 10.11.19.233, 10.11.14.92,
10.11.22.146,10.11.38.98, 192.168.2.1] any (msg:"Camera profile";sid:1000211;)
```

Figure 4. Selected Device Unique IPs

4.4. Sphere Enhancement

Sphere enhancement is a process of adding or removing IPs in an active device sphere. Possible sphere enhancement cases are.

- When a non allowed IP tries to communication with a sphere device or vice versa.
- When anomalies found in trusted IPs communication.

When a new IP, previously not part of trusted sphere, communicate with the device and vice versa. In this case, as soon as the request reaches the gateway, sphere enhancement notification appear on GUI application. Another scenario where sphere enhancement notification appear when attack detection engine detect anomalies in trusted communication. In both cases end users can either extend or reduce the IPs in a respective sphere.

5. Experimental Setup & Results

To demonstrate the effectiveness of our proposed framework, we have experimented couple of attacks on IoT devices; camera and google home, shown in Fig. 5 . Our experimental setup comprise of a gateway, IoT devices, a penetration testing system and monitoring/management system. Raspberry pi device is converted into a network gateway, sufficient guidelines are provided by researchers [25]. Suricata hosted on the gateway intercepts all network traffic and allow it according to its security policies. Gateway is also amalgamated with sphere management service, implemented in python. It is responsible to communicate with the GUI application for sphere management. Penetration testing system will perform attacks on the IoT devices;

DoS attack on wireless camera and scanning attack on the google home. And monitoring/management systems will assist in attack monitoring and managing devices spheres.

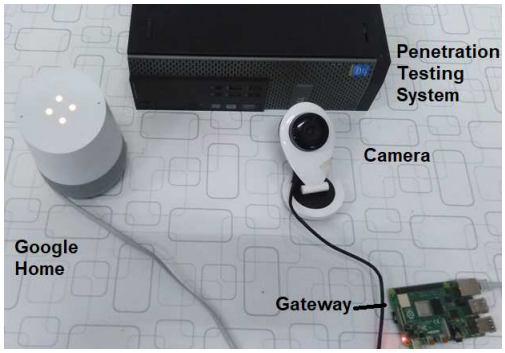

Figure 5. Devices Used in The Experimental Setup

5.1. DoS Attack on a Wireless Camera From A Non-Trusted IP

Denial of Service (DoS) attacks that have been targeting the traditional networks for years, are also a big concern for insecure IoT devices. This attack has devastating effects on the constrained devices; drain out their battery, hinder their normal operation etc. Propose method will automatically secure devices from DoS attacks, specially from sources that are not required to communicate with the respective device. To see the feasibility of propose method against DoS attacks, we have performed a DoS attack on a sphered wireless camera. A Camera, video monitoring PC and a penetration testing system connects in a same network. Camera is designed to provide a real time video stream on its open port 554 using Real Time Streaming Protocol (RTSP) [26]. In this experiment VLC software running on a monitoring PC will receive the camera stream. Wireshark I/O graph is also running on the same system to analyze the camera transmission performance during DoS attack. Because RTSP is TCP based protocol, therefore, we have planned to perform TCP flood on camera port 554 and try to hinder its communication with video receiver. Freely available DoS attacking tool, Low Orbit Ion Cannon (LOIC) [28] is installed on the penetration testing system.

After testbed ready, we implement a camera sphere using GUI app. The Initial sphere does not contain the penetration system and video monitoring system IPs. VLC player when try to connects with the camera, connection is unsuccessful. Because propose system does not allow any communication that violates the device sphere. A notification appears on GUI app, a new IP trying to connect the camera. We update the sphere and then VLC player starts receiving the live camera stream. Wireshark also running on the monitoring system, parallel to VLC player. Wireshark I/O graph shown in Fig. 6 will show the effect on camera stream during this experiment. Before a DoS attack, I/O graph is normal with a smooth camera stream. But when DoS attack starts, we see variations in camera transmission. But still camera stream is receiving at the monitoring system. Because camera sphere is active at the gateway and DoS attack stop at the gateway level. Camera is safe from any DoS traffic. Difference between the normal transmission and the stream transmission during DoS attack, is due to the extensive processing at gateway. A better gateway hardware will further minimize this difference. After some time we remove the camera sphere at gateway using the GUI app. As soon as sphere remove, DoS traffic reaches camera and it stop sending its stream to the VLC player. Section of I/O graph label with sphere inactive shows lack of stream on video monitoring system. After some time, once again we activate the camera sphere and video appears on VLC player. Propose method effectively secure camera from DoS attack carried out by an IP that never requires to communicate with the camera.

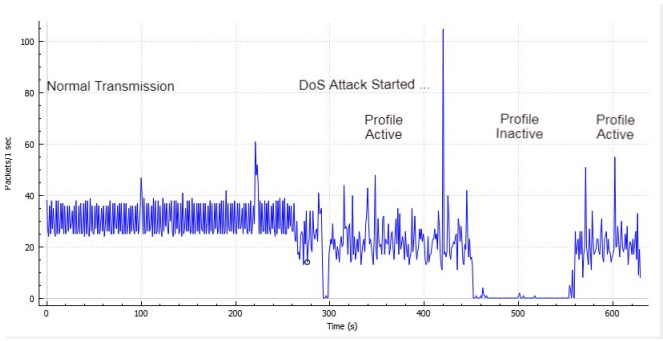

Figure 6. I/O Graph During DoS Attack, With Active/Inactive Device Sphere

5.2. Scanning Attack on Google Home From A Trusted IP

In the previous experiment we show that if IoT devices only communicate with the allowed IPs, it will reduce the potential attackers. In this experiment we will evaluate the propose method against attacks carried out by a trusted IP, that is also a part of a device sphere. Idea erupted from the fact, that an IoT device may be vulnerable from the beginning or before profiling, for instance it is part of a botnet. Therefore blindly allow the trusted IPs communication will not secure the IoT devices. Devices included in this experiment are google home and penetration testing system. Penetration system will perform the scanning attacks on the google home. Such attacks assist attackers to gain initial access of devices. We create a trusted communication sphere for the google home. This sphere will also include the penetration testing system IP, therefore scanning attacks traffic will pass the first check point of propose method; device sphere. Once a communication pass through the device sphere check, suricata evaluate the communication against emerging threats security policies. Ruleset is enrich with number of scanning detection rules. Therefore scanning traffic stop at the gateway level and penetration system does not get google home scan results. To show the effectiveness

of proposed framework, we inactive the google home sphere and then again perform scan attack on it. This time, scan results include critical information about the google home; open ports, services running etc. This shows propose system provides a strong second line of defense against attacks even if they pass first check point.

5.3. Secure Internet From Attacks Carried Out by IoT Devices

One of the most devastating attack that effect the whole internet is the botnet activity carried out by IoT devices. Constrained devices are widely exploited by botnet attackers due to their continuous internet connection, insufficient host based security and deployment of IoT devices along with traditional network devices. Mirai and other botnet attacks revealed that IoT devices sphere fertile ground to carry out large scale attacks.

We have analyzed the publically available code of couple of qbot variants (Cayo, Galaxy) [27] with the aim to understand the threat that need to counter. Two major bot activities; scanning activity and other network attacks, when carried out by the IoT devices, make them a real threat. During scanning activity, bots randomly scan new potential victims and at times convert them into new bots or report their details to the server. And in network attacks, bot take target IPs from its C&C server and perform respective attacks. Researchers in [21] discussed that profiled IPs mechanism will secure internet targets from bots malicious activities. But if C&C server is one of the trusted IPs and bot carries out attacks on other trusted IPs included in its profile. In this case our proposed second level security; validate the trusted IPs communication using attack detection engine, and block any malicious bot activity.

6. Conclusion

Security and convenience are two main elements that will ensure the success of IoT. This paper proposes a method that will strengthen IoT devices security and is easy to use. Key distinction of proposed framework is its effectiveness in securing IoT devices from becoming source as well as target of attacks. Due to the effectiveness of proposed framework, a wireless camera is easily secured from a DoS attack carried out by an IP that actually never needs to communicate with camera. Moreover, a google home is secured from scanning attack carried out by a trusted source from where an attack is never expected. Also it is discussed how IoT-Sphere will avoid attacks carried out by IoT devices towards rest of internet. Along with strengthening the dual aspect of security, propose system will also reduce the work load on threat detection engines that will increase overall system performance. When only limited required communication will reach IoT devices, it will save devices constrained resources.

7. Declaration

The authors declare no conflict of interest.

References

[1] Gokhale, Pradyumna, Omkar Bhat, and Sagar Bhat. "Introduction to IOT" International Advanced Research Journal in Science, Engineering and Technology (IARJ SET) 5.1 (2018).

[2] "What Is Iot Security," Paloaltonetworks, [Online]. Available https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

[3] Bang Nguyen amp; Lyndon Simkin (2017) The Internet of Things (IoT) and marketing: the state of play, future trends and the implications for marketing, Journal of Marketing Management, 33:1-2, 1-6, DOI: 10.1080/0267257X.2016.1257542.

[4] "The Global Iot Market Opportunity Will Reach USD4 Trillion By 2025," Iot Business News, [Online]. Available https://iotbusinessnews.com/2016/05/03/10333-global-iot-market-opportunity-will- reach-usd4-trillion-2025

[5] "The Challenges Of Ensuring Iot Security," Netsparker, [Online]. Available https://www.netsparker.com/blog/web-security/the-challenges-of-ensuring-iot-security/

[6] Beavers J., Pournouri S. (2019) Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions. In: Jahankhani H., Kendzierskyj S., Jamal A.,
Epiphaniou G., Al-Khateeb H. (eds) Blockchain and Clinical Trial. Advanced Sciences and Technologies for Security Applications. Springer, Cham

[7] Okul Ş., Aydin M.A., Keleş F. (2019) Security Problems and Attacks on Smart Cars. In: Boyaci A., Ekti A., Aydin M., Yarkan S. (eds) International Telecommunications Conference. Lecture Notes in Electrical Engineering, vol 504. Springer, Singapore

[8] D. Rivera, A. García, M. L. Martín-Ruiz, B. Alarcos, J. R. Velasco and A. Gómez Oliva, quot;Secure Communications and Protected Data for a Internet of Things Smart Toy Platform,quot; in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3785-3795, April 2019, doi: 10.1109/JIOT.2019.2891103.

[9] "The 5 Worst Examples Of Iot Hacking And Vulnerabilities In Recorded History," iotforall, [Online]. Available https://www.iotforall.com/5-worst-iot-hacking- vulnerabilities/

[10] Liu, Yang, et al. "Hidden Electricity Theft by Exploiting Multiple-Pricing Scheme in Smart Grids." IEEE Transactions on Information Forensics and Security 15 (2020): 2453-2468.

[11] Caron, Xavier, et al. "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective." Computer Law Security Review 32.1 (2016): 4-15.

[12] Simpson, Anna Kornfeld, Franziska Roesner, and Tadayoshi Kohno. "Securing vulnerable home IoT devices with an in-hub security manager." 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2017.

[13] Santoso, Freddy K., and Nicholas CH Vun. "Securing IoT for smart home system." 2015 International Symposium on Consumer Electronics (ISCE). IEEE, 2015.

[14] Lee, Yann-Hang, and Shankar Nair. "A smart gateway framework for iot services." 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2016.

[15] Canedo, Janice, and Anthony Skjellum. "Using machine learning to secure IoT systems." 2016 14th annual conference on privacy, security and trust (PST). IEEE, 2016.

[16] Meidan, Yair, et al. "N-baiot—network-based detection of iot botnet attacks using deep autoencoders." IEEE Pervasive Computing 17.3 (2018): 12-22.

[17] Eskandari, Mojtaba, et al. ”Passban IDS: An intelligent anomaly based intrusion detection system for IoT edge devices.” IEEE Internet of Things Journal (2020).

[18] Sivanathan, Arunan, et al. ”Classifying IoT devices in smart environments using network traffic characteristics.” IEEE Transactions on Mobile Computing 18.8 (2018): 1745-1759.

[19] SDange, Smita, and Madhumita Chatterjee. ”IoT Botnet: The Largest Threat to the IoT Network.” Data Communication and Networks. Springer, Singapore, 2020. 137-157.

[20] Ding, Jie, et al. ”IoT connectivity technologies and applications: A survey.” arXiv preprint arXiv:2002.12646 (2020).

[21] Habibi, Javid, et al. ”Heimdall: Mitigating the internet of insecure things.” IEEE Internet of Things Journal 4.4 (2017): 968-978.

[22] Wu, Chun-Jung, et al. ”Iotprotect: Highly deployable whitelist-based protection for low-cost internet-of-things devices.” Journal of Information Processing 26 (2018): 662-672.

[23] “Snort,” Sourcefire, [Online]. Available https://www.Snort.org/

[24] “Suricata,” OISF, [Online]. Available https://suricata-ids.org/

[25] “Rules,” Emerging Threat, [Online]. Available https://rules.emergingthreats.net/

[26] “Real Time Streaming Protocol,” wikipedia, [Online]. Available https://en.wikipedia.org/

[27] “Tl-bots,” GitHub, [Online]. Available https://github.com/threatland/TL-BOTS, 2019.

[28] ”Low Orbit Ion Cannon (LOIC)”, SOURCEFORGE, [Online]. Available https://sourceforge.net/projects/loic/

Figures

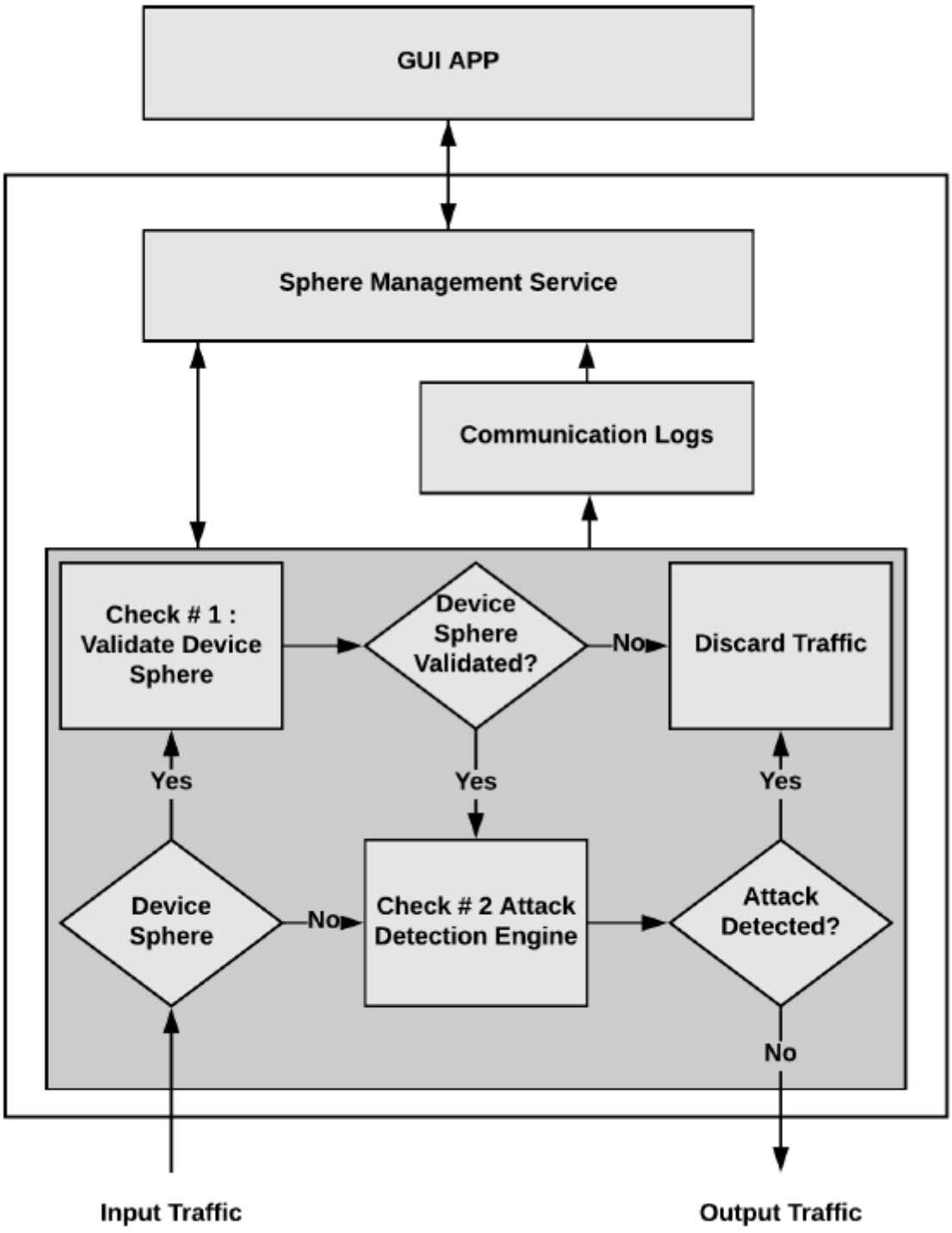

Figure 1

Architecture of Proposed Method

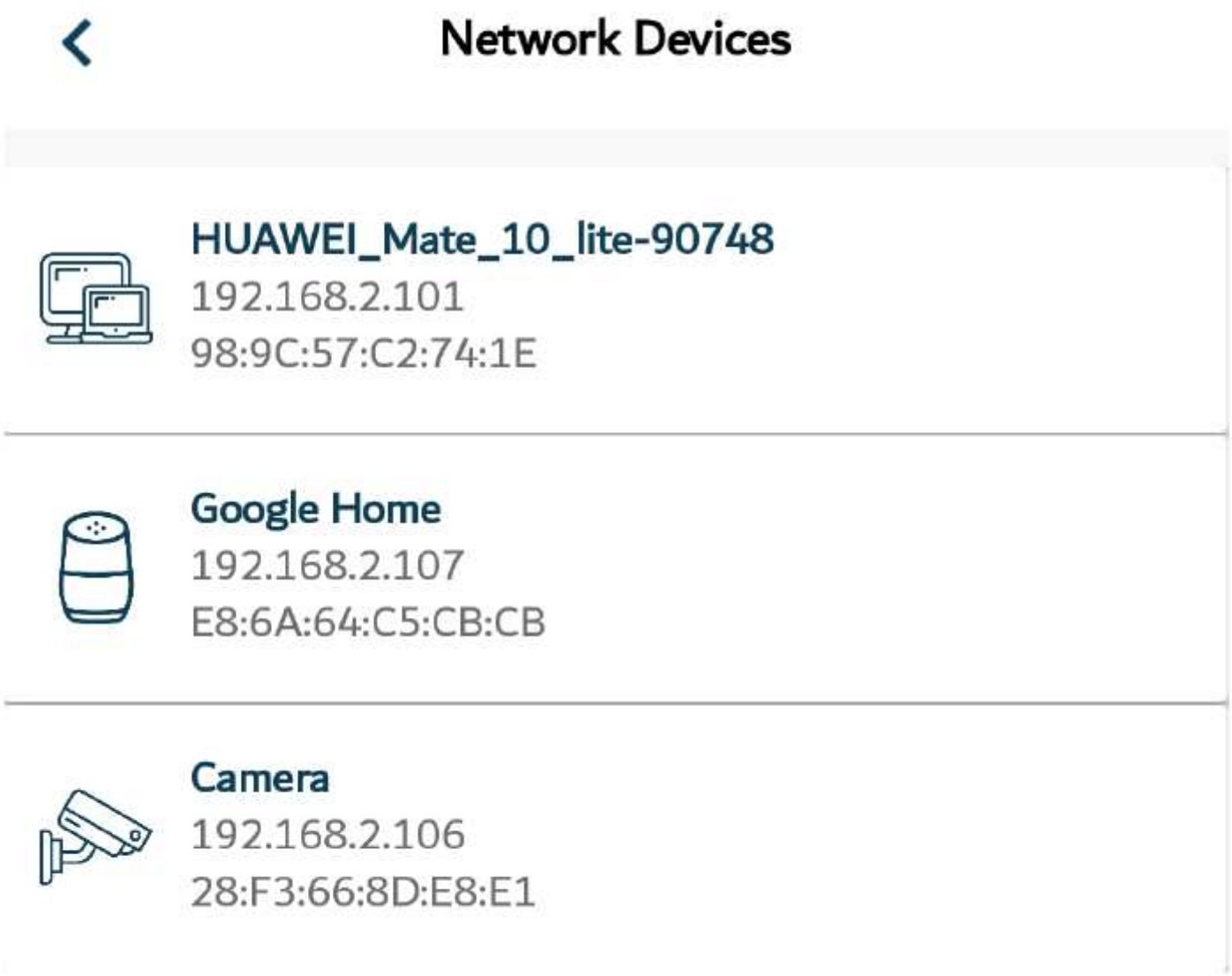

Figure 2

List of Available Devices Found in Communication Logs

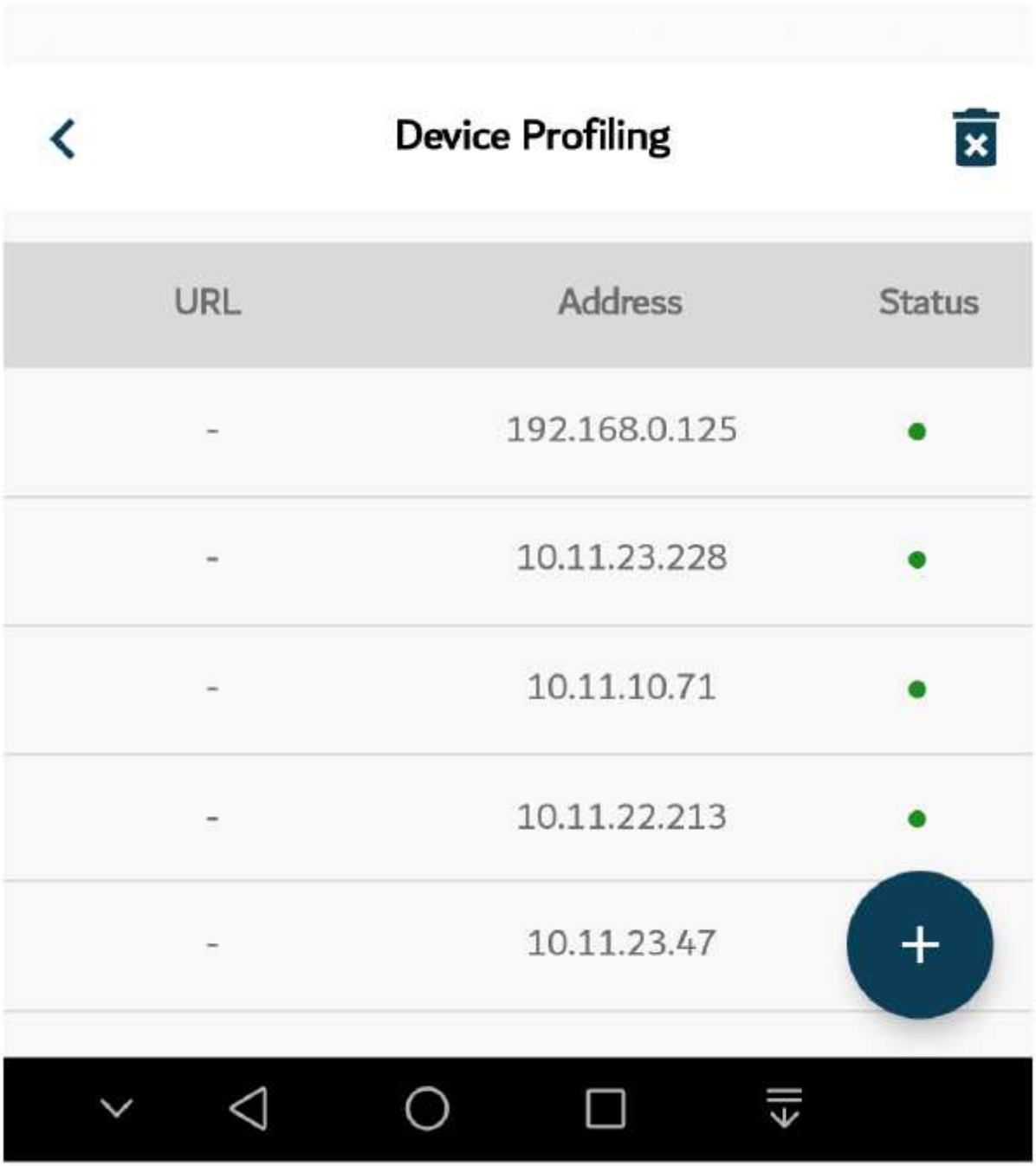

Figure 3

Unique IPs Communicated With a Respective Device

```
drop ip 192.168.2.106 any <> ![192.168.0.125, 10.11.23.228, 10.11.10.71,
10.11.22.213, 42.96.193.232, 10.11.23.59, 10.11.34.22, 10.11.20.108, 120.24.36.178,
10.11.23.110, 10.11.20.83, 10.11.23.47, 10.11.18.232, 196.168.0.196, 10.11.10.58,
47.74.152.38, 10.11.10.59, 10.11.19.237, 192.168.2.102, 10.11.22.175,
10.11.10.100, 10.11.10.52, 10.11.23.205, 10.11.14.42, 10.11.19.233, 10.11.14.92,
10.11.22.146,10.11.38.98, 192.168.2.1] any (msg:"Camera profile";sid:1000211;)
```

Figure 4

Selected Device Unique IPs

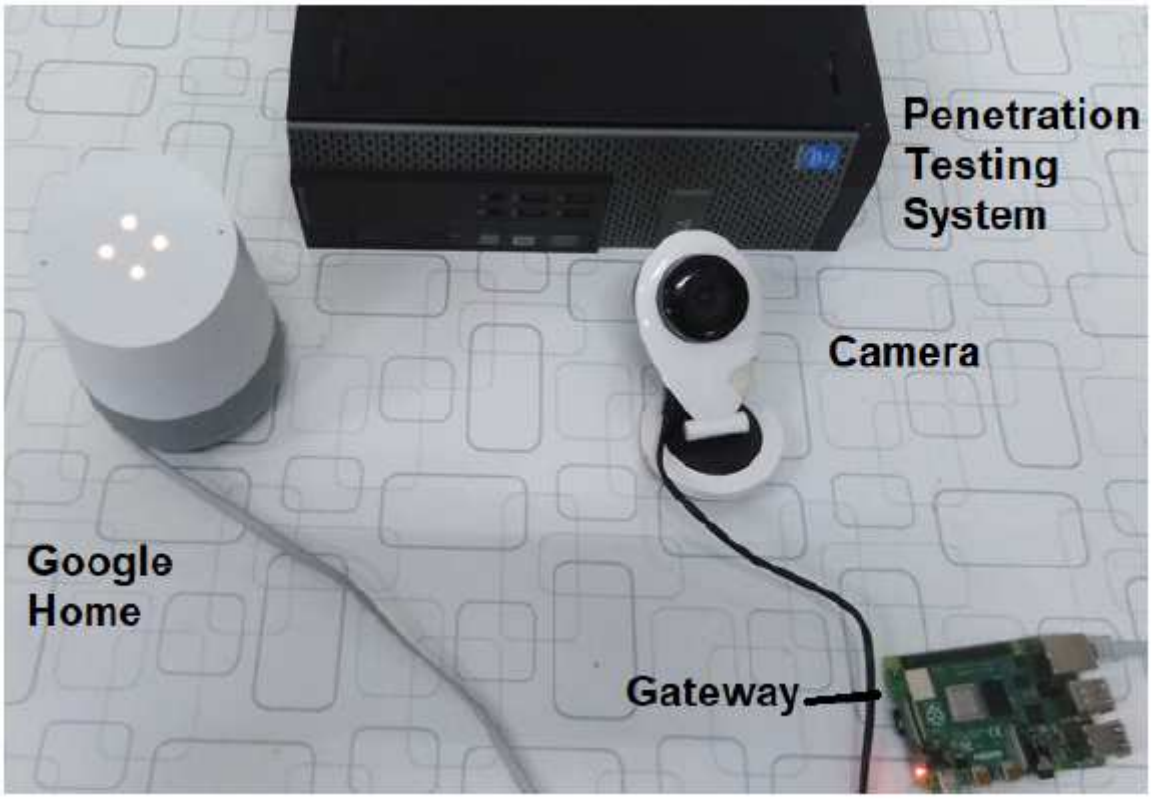

Figure 5

Devices Used in The Experimental Setup

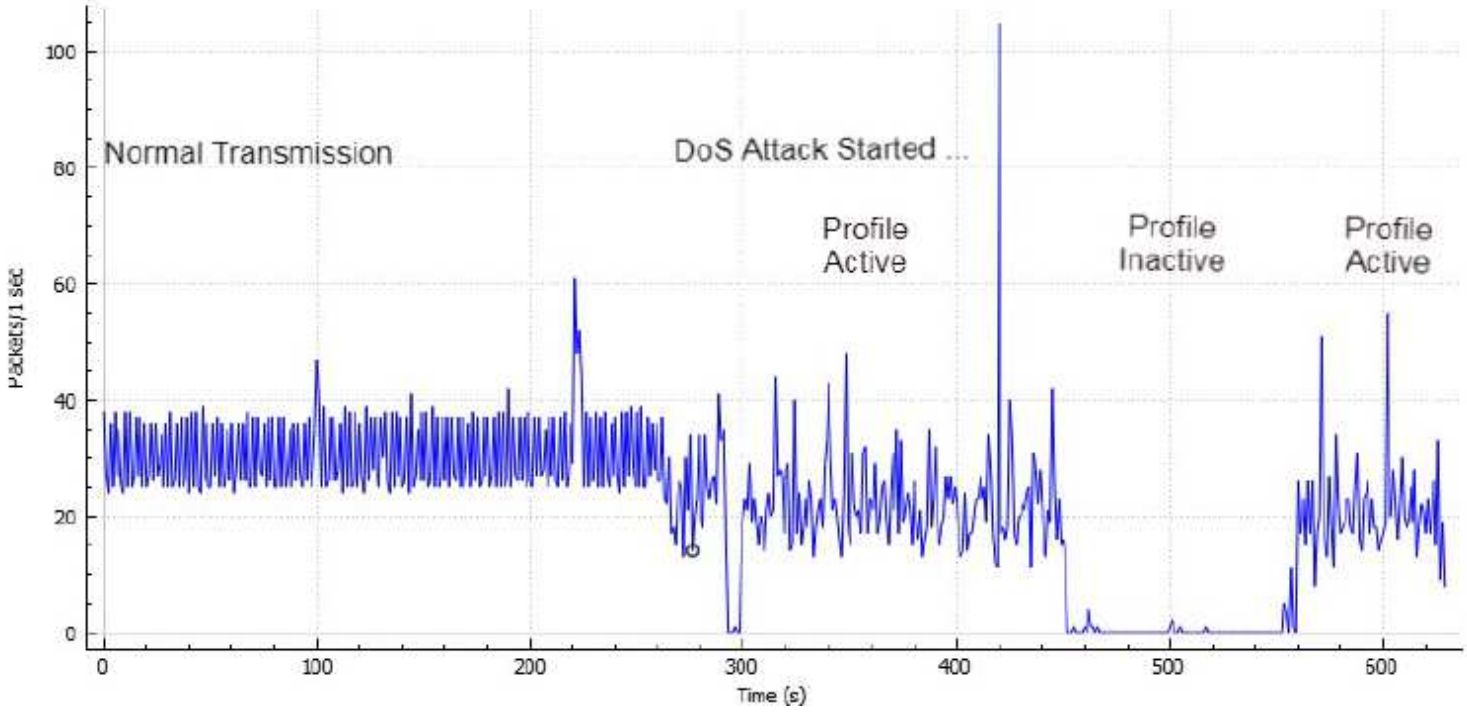

Figure 6

I/O Graph During DoS Attack, With Active/Inactive Device Sphere