UDP-Based Active Scan for IoT Security (UAIS)

Hyun-Chul Jung[1], Hyun-geun Jo[2], and Heejo Lee[1]*
[1] Department of Computer Science and Engineering, Korea University
Seoul, 02841, Republic of Korea
[e-mail: {change, heejo}@korea.ac.kr]
[2] Norma, Inc.
Seoul, Republic of Korea
[e-mail: gusrmsdlrh@gmail.com]
*Corresponding author: Heejo Lee

Received September 8, 2020; revised November 16, 2020; accepted January 6, 2021; published January 31, 2021

Abstract

Today, IoT devices are flooding, and traffic is increasing rapidly. The Internet of Things creates a variety of added value through connections between devices, while many devices are easily targeted by attackers due to security vulnerabilities. In the IoT environment, security diagnosis has problems such as having to provide different solutions for different types of devices in network situations where various types of devices are interlocked, personal leakage of security solutions themselves, and high cost, etc. To avoid such problems, a TCP-based active scan was presented. However, the TCP-based active scan has limitations that it is difficult to be applied to real-time systems due to long detection times. To complement this, this study uses UDP-based approaches. Specifically, a lightweight active scan algorithm that effectively identifies devices using UPnP protocols (SSDP, MDNS, and MBNS) that are most commonly used by manufacturers is proposed. The experimental results of this study have shown that devices can be distinguished by more than twice the true positive and recall at an average time of 1524 times faster than Nmap, which has a firm position in the field.

Keywords: IoT Device Identification, Active Scan, UPnP Protocols, UDP Based Scan

This work is supported in part by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2019-0-01343 Regional strategic industry convergence security core talent training business, No.2019-0-01697 Development of Automated Vulnerability Discovery Technologies for Blockchain Platform Security, and No.2020-0-01819 ICT Creative Consilience program).

http://doi.org/10.3837/tiis.2021.01.002 **ISSN : 1976-7277**

1. Introduction

The introduction of IoT devices is accelerating rapidly due to the recent activation of smart city businesses. Among them, there is a growing number of devices in SOHO stores such as POS payment terminals that accept orders and CCTVs that monitor stores on behalf of people. [1] Such increasing trend of these devices helps us to process our requirements faster and more efficiently, but on the other hand, there are often situations in which information about our requirements is abused or maliciously edited to harm users [2]. In 2018, there was a Pin 7 incident that leaked important information such as credit card numbers and security codes by planting malicious codes in POSs of hotels and casinos.

Because IoT devices come in a wide variety of types, device classification is essential for security checks and responses [3]. Since the items to be checked and the attack scenario are different depending on the type of device the efficiency of vulnerability inspection is significantly reduced if the type of device is not accurately classified. For example, targeting CCTV, an attack to the C&C server occurs by exploiting a video transmission service. On the other hand, routers are mainly attacked by stealing the information of the visitor through the administrator service (web). Therefore, the security official should check the video transmission protocol of CCTV and the web service of the router. For this reason, Bitdefender [4] and Fingbox [5] solutions basically provide the function of classifying IoT devices.

Passive scan method has traditionally been used to distinguish types of IoT devices on the network. Passive scan, like the traditional IDS/IPS method, maintains the listing status on network traffic to check security issues such as malware infection and intermediary attacks. However, the Passive scan method has private issues such as cases where collected personal information is leaked [6], as well as cost issues to overcome performance degradation caused by maintaining the listing state [7] and a vulnerability to attacks in the internal network. To overcome this, a recent study suggested a technique for preemptively identifying security issues caused by the device by identifying the device through an active scan method within the network traffic [8]. In addition, Nmap [9] is also most widely used for detecting and distinguishing IoT devices using active scan techniques.

The current active scan approach has shown excellent device type identification function, primarily by using a TCP-based approach to send requests to the device and handle the device's responses. The reason why most IoT devices prefer TCP-based approaches in previous active scan methods is because they are prone to provide TCP-oriented services. However, current TCP-based active scan two limitations: the latency and the accuracy. In terms of the latency, redundant overhead occurs due to its user service-oriented nature. For example, in the case of the Nmap, it checks all possible TCP protocols available to the user when scanning a target device. Each check proceeds not only to the TCP network area itself, but also to the application area used by TCP. In addition, in the case of the accuracy, the device signature for classifying cannot be properly refined because identification is performed in an environment where the appropriate classification criteria for IoT devices are not provided.

As a remedy, this study proposes a device classification technique that overcomes two shortcomings of the TCP-based approach. We have confirmed that real-time availability and efficiency can be achieved through active scan using UDP port based on the fact that IoT devices basically exchange information based on UDP for the configuration between devices. UDP has the advantage of having a simple structure compared to TCP in nature and is very fast for a device or application on the network to process it. However, due to the simplicity of the information contained in the structure, there is also a disadvantage that it is difficult to transmit complete information of the device. Nevertheless, we improved the latency and the

accuracy compared to Nmap through an algorithm called UDP-based Active Scan for IoT Security (UAIS) that refines packets according to known IoT device classification so that devices can be classified in a short time using the properties of the UDP UPnP protocol.

Specifically, the minimal scan method using SSDP, MDNS, and NBNS among the protocols used in UPnP designed to efficiently transmit device information, rather than performing scanning in brute-force method using all protocols of UDP. Use. This minimizes the overhead of a full scan that uses all ports of TCP and the overhead that occurs in the application area. In addition, since there is no publicly defined criteria for classifying IoT devices so far, open scanning tools such as Nmap have not been able to properly refine device information in the classification process. We have established the classification criteria for IoT devices in reverse based on the latest classification results from studies known to date, so that UAIS can effectively refine information. These two points are the main contributions of this study when compared to related studies.

To evaluate the efficiency and accuracy performance of the proposed approach, we compared it with the most widely used Nmap for detecting and distinguishing devices as the byword for network scanners in the existing IoT environment. The results of the experiment showed that UAIS can distinguish with more than twice the true positives and recall in time when UAIS is 1524 times faster than Nmap on average for 50 kinds of commercial off-the-shelf products.

2. Problem Definition

With the emergence of various types of IoT devices today, the types of devices connected to the network has increased simultaneously. As the types of devices become more diverse, proper security vulnerability checks are needed for each type. At this time, efficient device-identification performance has a significant impact on security vulnerability checking performance.

The Passive scan method of monitoring and maintaining the listening status for traffic on the network has the aforementioned privacy issues [10]. In addition, in the case of Passive scan, if a sub-device does not go outside and only communicates internally and plants a malicious code, a problem occurs without any means to detect it. It is also problematic that the cost of ensuring effective network performance is high. Active scan methodology has three advantages. First, because traffic is not checked, analyzed and stored in IoT network for device identification, time is shortened and resources are consumed less. It also reduces security points for IoT networks, which have many transmissions of sensitive information such as personal information. Secondly, the scanning can be performed at the desired point in time. For example, a device scan can proceed when a new device appears on the network or when an attack occurs. Finally, only the desired network segment can scan the device. If the network one wants to monitor is large, the person can send scanning packets only to the target network segment for quick identification.

However, traditional active scan methods have limitations that they are slow to discern using TCP-based protocols. Therefore, in this study, lightweight active scan algorithm that identifies IoT devices at an efficient time compared to TCP-based active scan by using UDP-based UPnP protocol (SSDP, MDNS, MBNS), which are free from the Passive scan security and practicality issues and most commonly used by manufacturers is proposed. IoT devices often implement protocols based on UDP for linking their products. **Fig. 1** shows the percentage of devices that support SSDP, MDNS, MBNS protocols among the 50 devices collected for this study. Based on this fact, a technique that identifies the majority of IoT

devices directly within an efficient time based on UDP in various types of IoT devices has been devised.

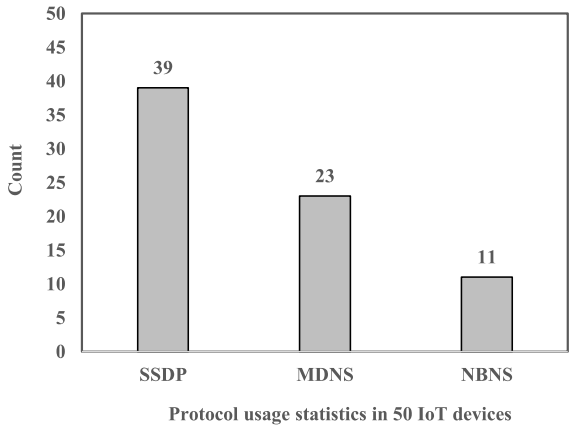

Fig. 1. Popular UPnP Protocols used by 50 IoT devices. The collection standard of target devices is explained in Section 4.1

3. Overall Description

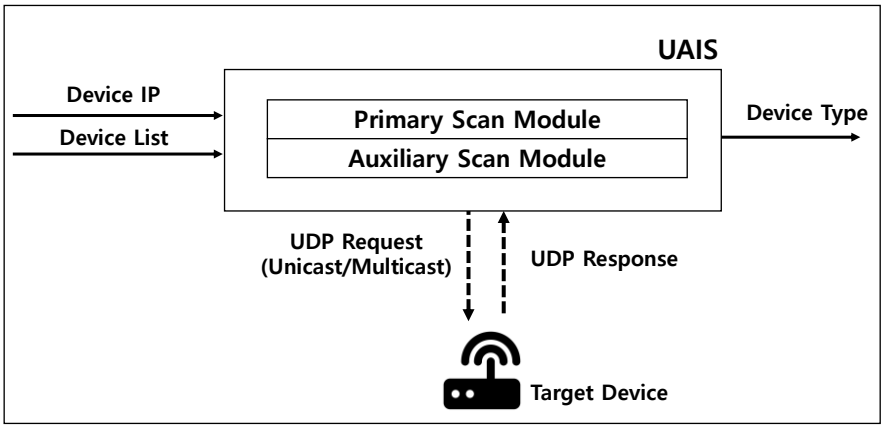

Fig. 2. Overview of UAIS

Fig. 2 shows an overview of UAIS. UAIS uses as inputs device IP and device list containing the known IoT device types. It is difficult to have objectivity to select the known IoT device types when configuring device list because device types are subjectively divided by device manufacturers. The types of IoT devices to be classified in this study were combined with those mentioned in the published papers and ArXiv document [4, 5, 8, 11, 12] within the last four years. The details are described in Chapter 3.1. UAIS performs a Primary Scan on the relative device with the given input device IP, and Auxiliary Scan on the device that is not identified in the Primary Scan. Both Scan methods have something in common in that they distinguish target devices using UDP-based protocols. On the other hand, Primary Scan uses SSDP and Auxiliary Scan uses a combination of MDNS and NBNS. Specifically, for the convenient connection between IoT devices, a primary classification is done in the Primary Scan using SSDP, the representative protocol used in the open project, UPnP. Some devices

do not support SSDP or have incomplete functions due to abusing cases (such as DDoS attacks) via SSDP. Hence, when a response is not received or device identification is unsuccessful, a scan method using the MDNS, NBNS protocols borrowed from a number of devices is used as alternative classification methods.

Table 1. IoT device classification list

No.	Categories
1	(IP / Network / Sec.) camera [8, 10, 11, 13, 14]
2	(IP) television / TV [8, 13, 14]
3	Router / Switch / Hub / Gateway / Modem / (Wireless) Access point / WAP [10, 11, 13]
4	(Baby) Monitor [8, 14]
5	(Motion) Sensor / Thermostat / Smoke detector [11, 14]
6	Printer [8, 10, 13]
7	Refrigerator [8, 14]
8	(Smart) watch [8, 14]
9	Socket [8, 14]
10	Consumer game [10]
11	(Digital) video [13]
12	Digital media receiver [10]
13	Electronics [11]
14	Firewall [13]
15	Healthcare (device) [11]
16	Light bulbs [11]
17	NAS [10]
18	Programmable / (Logic) controller [13]
19	Recorder [13]
20	Trigger [11]

3.1 IoT Device Classification

Recently, a variety of studies have been conducted to identify IoT devices connected within the network. In each study, the distinguishment category of the devices that were intended to be distinguished was randomly selected. In this study, to establish objective classification criteria, each study was composed of one set, and the IoT device distinguishment categories presented in each study were based on the elements of each set, and one IoT device classification list was formed by union-ing each set. The list is listed in **Table 1**, with a total of 20 categories. The list was arranged in descending order in the order of the number of mentioning each category. Devices with similar personalities were identified by a random cluster. Keywords in parentheses mean keywords that are optionally written for a particular function, even though they are in the same category. For example, '(Wireless) access point' is marked as 'wireless access point' or 'access point', but all are considered to be of the same type.

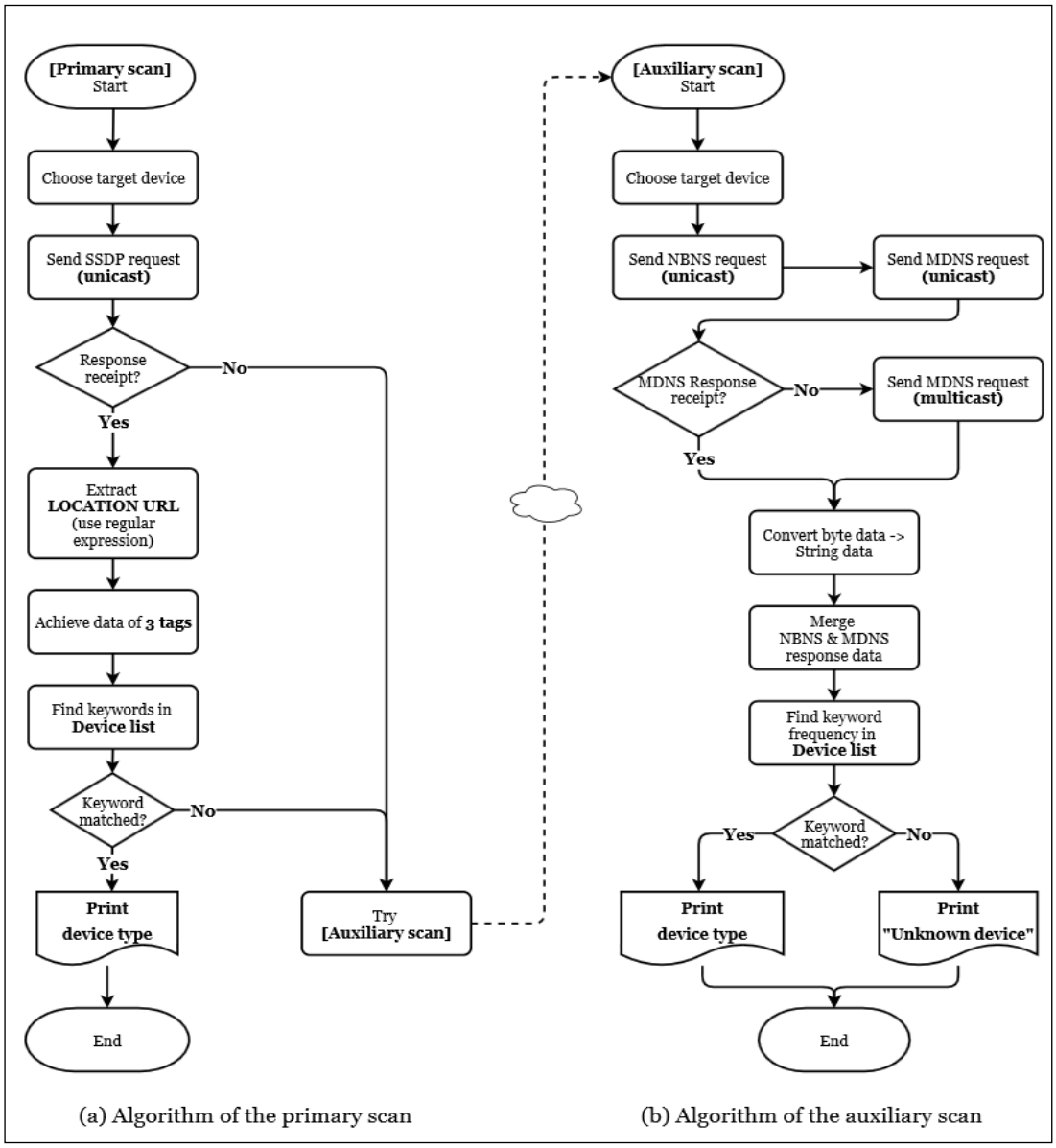

Fig. 3. Detailed algorithm of the Primary Scan and the Auxiliary Scan

3.2 Algorithm of UDP based Scan

This chapter describes Primary Scan and Auxiliary Scan. **Fig. 3** shows the Detailed Algorithm of the Primary Scan and the Auxiliary Scan used by UAIS to identify the device. (a) Primary Scan requests information about the device through the Unicast directly to the target device using the SSDP protocol. If there is a response, it parses the response data. Response data is received in XML format, as shown in **Table 2**. The device type is printed when the keywords in the <deviceType>, <friendlyName>, and <ModelDescription> tags of the entire response data are extracted, and it compares with the keywords in the given device list, and if there is a keyword that is most frequently matched within the list, that device type is printed out.

Table 2. Example of SSDP active scan response from a home IoT device

…
<deviceType>**urn:schemas-upnp-org:device:InternetGatewayDevice:1**</deviceType>
<friendlyName>**HG532e**</friendlyName>
…
<modelDescription>**Huawei Home Gateway**</modelDescription>
…

If there is no response to the Primary Scan, it performs (b) Auxiliary Scan. Auxiliary Scan uses the NBNS and MDNS protocols to request information about the device via Unicast on both protocols. Note that, in particular, for certain devices (e,g, Xiaomi IP Camera), not handling the responses to MDNS Unicast requests is set by default, so in the case of MDNS, if it does not receive a response, it will request again via Multicast. Responses to requests using both protocols will receive byte string data, unlike the Primary Scan method. It then converts this to parseable string format and merge the data on the responses of the two protocols into a sequence of character string. Similar to the Primary Scan method in this sequence, keywords are extracted and the device type is printed when the most frequently matched keyword is present in the list when compared with the keywords in the given device list.

4. Evaluation

In order to evaluate performance of UAIS, a number of IoT devices by various manufacturers were secured and device identification speed and accuracy were compared with Nmap, the most commonly used TCP-based active scan tool.

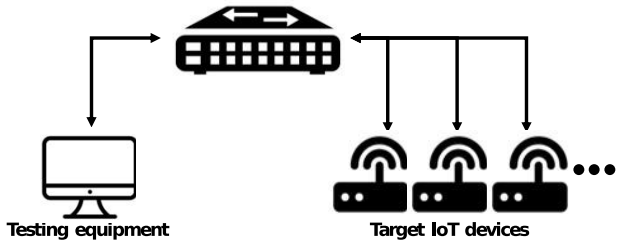

Fig. 4. Network setup for the experiment testbed

4.1 Experiment Setup

The experimental equipment used was Intel(R) Core (TM) i5-8400 CPU @ 2.80GHz, RAN 16G, storage 256G. For the communication environment, a real internal network at the 100Mbps speed in the internal network, such as **Fig. 4** was established, and the testing equipment was connected the target device. However, in the case of AP, it was regarded that the AP was accessed and proceeded from an external network. A total of 50 devices from various manufacturers were prepared and tested, including those with high market share in Asia, such as **Table 3**. Because it was practically difficult to obtain a wide variety of devices,

the experiment was limited to three types of devices: AP, IP Camera, and NAS (Network Attached Storage).

Table 3. List of target devices (50 in total)

Device type	No.	Manufacturer	Device name
Access Point	1	IPTIME	A2003NS-MU
	2	IPTIME	A3008-MU
	3	IPTIME	A5004NS-M
	4	IPTIME	A8004T
	5	IPTIME	N3-i
	6	IPTIME	N702R
	7	IPTIME	N704BCM
	8	IPTIME	N804R
	9	TP-LINK	C2
	10	TP-LINK	TL-WR840N
	11	CISCO	RV110W
	12	CISCO	RV215W
	13	H3C	ERG-21350W
	14	HUAWEI	HG532e
	15	HUMAX	T3AV2
	16	SYNOLOGY	RT2600AC
	17	ASUS	RT-AX88U
	18	ASUS	RT-N10+
	19	D-LINK	DIR-601
	20	D-LINK	DIR-882
IP Camera	1	WISENET	SNH-C6417BNC
	2	WISENET	SNH-P6410BN
	3	WISENET	SNH-V6410PN
	4	WISENET	SNH-V6414BN
	5	VSTARCAM	VSTARCAM-130E
	6	VSTARCAM	VSTARCAM-200T
	7	DAUHA	IPC-HDW-1220SN
	8	DAUHA	IPC-HDW-1320SN
	9	FOSCAM	C1
	10	FOSCAM	C2
	11	HANWHA	QND-6022R
	12	HANWHA	QNO-6010R
	13	HANWHA	QNO-6030R
	14	D-LINK	DCS-5222LB
	15	D-LINK	DCS-5020L
	16	TP-Link	Tapo C200
	17	JWC	JWC-O1500IB
	18	IPTIME	C200
	19	XIAOMI	MJSXJ02HL
	20	XIAOMI	MJSXJ02CM
NAS	1	ASUSTOR	AS6302T
	2	IPTIME	NAS1dual
	3	IPTIME	NAS2dual
	4	QNAP	TS-230
	5	QNAP	TS-228A
	6	SYNOLOGY	DS120j
	7	SYNOLOGY	DS218
	8	SYNOLOGY	DS218j
	9	SYNOLOGY	DS220j
	10	TERRA-MASTER	F2-210

4.2 Experimental Result

This chapter describes the comparative evaluation between UAIS and Nmap. In this study, performance was compared in two aspects: distinguishment speed and accuracy. The experiment has shown that UAIS has succeeded in distinguishing at an average speed of 1524 times faster than Nmap in terms of speed. In addition, in terms of accuracy, UAIS has shown that distinguishment is possible with more than twice the true positives and recall compared to Nmap.

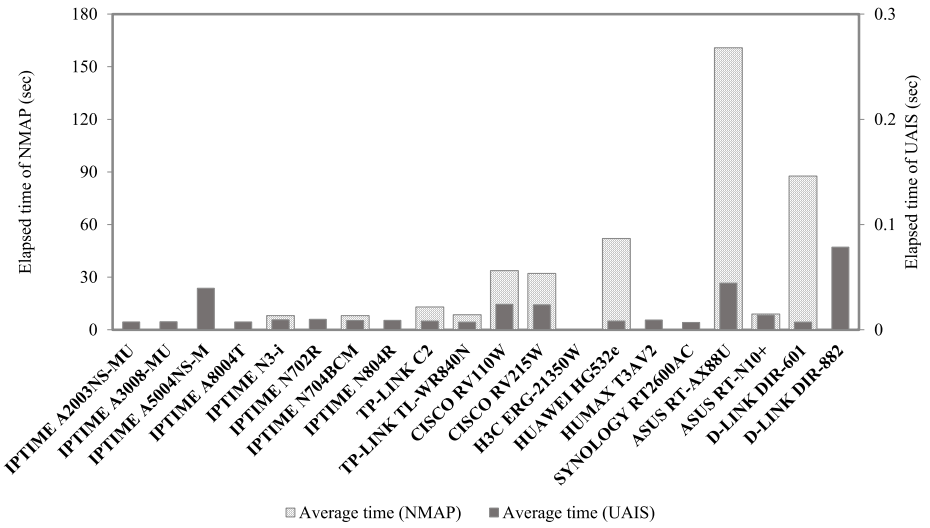

Fig. 5. Comparison of time to distinguish AP devices between Nmap and UAIS. The average time required for each of Nmap and UAIS is 41.31 and 0.02 seconds

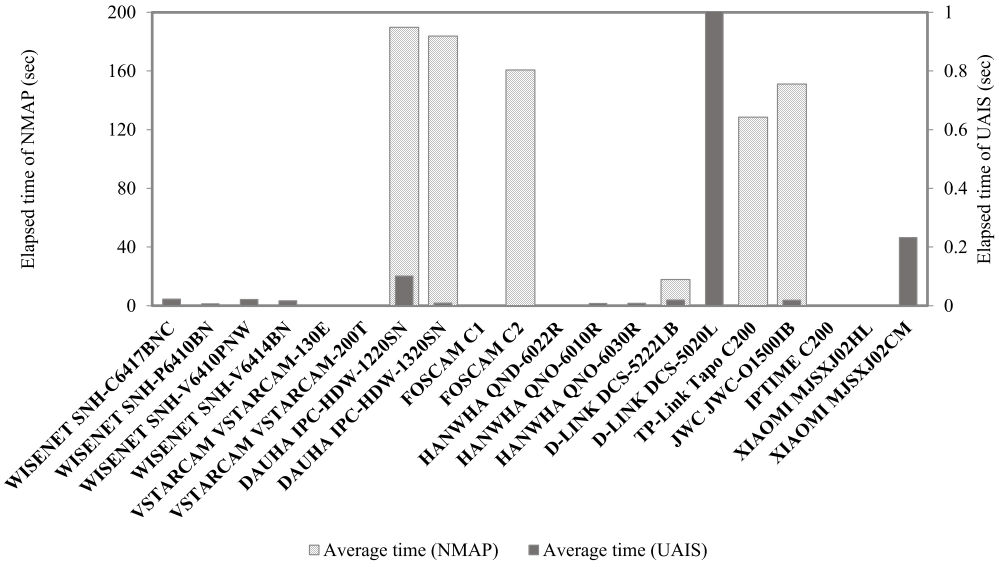

Fig. 6. Comparison of time to distinguish IP Camera devices between Nmap and UAIS. The average time required for each of Nmap and UAIS is 138.64 and 0.12 seconds

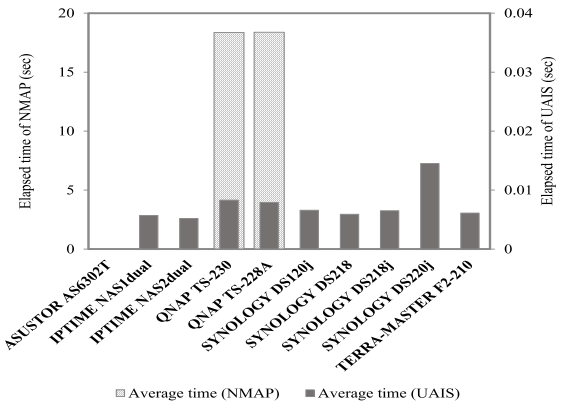

Fig. 7. Comparison of time to distinguish NAS devices between Nmap and UAIS. The average time required for each of Nmap and UAIS is 18.37 and 0.01 seconds

4.2.1 Speed of Distinguishment

To compare the distinguishment speed between UAIS and Nmap, we recorded the time from the start of the distinguishment test to the point where the results were obtained for each test device. All devices were tested 10 times each. Specifically, Nmap performed a device scan on the pre-opened TCP ports and based on the time value at the end of the output. In case of UAIS, the time required was measured using the Python *Time Module*. **Fig. 4-7** shows the time required for each cluster of device type: Access point (AP), IP Camera, and NAS IoT device. For all graphs, Nmap is a gray diagonal stripe pattern, and UAIS is a dark gray bar to indicate elapsed time. Since the difference between the two required times is remarkable, the time required for Nmap on the left Y main axis and the range of time required for UAIS on the right Y auxiliary axis are shown. If the test fails to distinguish, bars are omitted from the graph.

For every group, UAIS succeeded in distinguish, against Nmap, by a significant speed difference. In the AP cluster, distinguishment was achieved in the speed faster by the average of 2371 times. In the IP Camera cluster, the distinguishment was successful at an average rate of 1130 times. In NAS clusters, the average speed was 2477 times faster, the biggest difference of the three device clusters. The average distinguishment speed of the entire device was found to be that UAIS was approximately 1524 times faster than Nmap. The speed differences were compared only with the time required of the successful device for each methodology.

4.2.2 Accuracy of Distinguishment

We use precision and recall to evaluate the each methodology and compare the distinguishment accuracy between Nmap and UAIS. We choose precision and recall indicators because they are the popular indicators used to evaluate the performance of classification studies in the information retrieval academic field [12] Precision and recall are calculated by the following formulas.

$$Precision = \frac{True\ Positive\ (TP)}{True\ Positive\ (TP) + False\ Positive\ (FP)}$$

$$Recall = \frac{True\ Positive\ (TP)}{True\ Positive\ (TP) + False\ Negative\ (FN)}$$

Table 4 shows the results of Nmap and UAIS distinguishment. For Nmap, it is marked as N/A when the response was 'general purpose' or there were no responses. For UAIS, the device distinguishment results were presented based on the response data received from either the Primary Scan or the Auxiliary Scan. If neither method received a response or there was no matching keyword in the device list, it is marked as “N/A”. The result showed that in case of UAIS, true positive was more than twice than Nmap if the distinguishment was carried out normally. Also, for recall, since the number of UAIS true positive was significantly higher than that of Nmap the result was more than twice as high as that of Nmap.

Table 4. Classification result of Nmap and UAIS. In the column of UAIS, parentheses after each device type describe the successful method, either the Primary Scan or the Auxiliary Scan

Device type	Manufacturer	Device name	Classified type	
			Nmap	UAIS (Primary/Auxiliary)
Access Point	IPTIME	A2003NS-MU	N/A	Gateway (Primary)
	IPTIME	A3008-MU	N/A	Gateway (Primary)
	IPTIME	A5004NS-M	N/A	Gateway (Primary)
	IPTIME	A8004T	N/A	Gateway (Primary)
	IPTIME	N3-i	Router	Gateway (Primary)
	IPTIME	N702R	N/A	Gateway (Primary)
	IPTIME	N704BCM	Router	Gateway (Primary)
	IPTIME	N804R	N/A	Gateway (Primary)
	TP-LINK	C2	WAP	Gateway (Primary)
	TP-LINK	TL-WR840N	WAP	Gateway (Primary)
	CISCO	RV110W	WAP	Router (Auxiliary)
	CISCO	RV215W	WAP	Router (Auxiliary)
	H3C	ERG-21350W	N/A	N/A
	HUAWEI	HG532e	Router	Gateway (Primary)
	HUMAX	T3AV2	N/A	Gateway (Primary)
	SYNOLOGY	RT2600AC	N/A	Router (Primary)
	ASUS	RT-AX88U	WAP	Router (Primary)
	ASUS	RT-N10+	Router	Gateway (Primary)
	D-LINK	DIR-601	Router	Gateway (Primary)
	D-LINK	DIR-882	N/A	Gateway (Primary)
IP Camera	WISENET	SNH-C6417BNC	N/A	Camera (Primary)
	WISENET	SNH-P6410BN	N/A	Camera (Primary)
	WISENET	SNH-V6410PN	N/A	Camera (Primary)
	WISENET	SNH-V6414BN	N/A	Camera (Primary)
	VSTARCAM	VSTARCAM-130E	N/A	N/A
	VSTARCAM	VSTARCAM-200T	N/A	N/A
	DAUHA	IPC-HDW-1220SN	Webcam	N/A
	DAUHA	IPC-HDW-1320SN	Webcam	N/A
	FOSCAM	C1	N/A	N/A
	FOSCAM	C2	Webcam	N/A
	HANWHA	QND-6022R	N/A	N/A
	HANWHA	QNO-6010R	N/A	Camera (Primary)
	HANWHA	QNO-6030R	N/A	Camera (Primary)
	D-LINK	DCS-5222LB	Webcam	Camera (Primary)
	D-LINK	DCS-5020L	N/A	Camera (Primary)
	TP-Link	Tapo C200	Webcam	N/A
	JWC	JWC-O1500IB	Webcam	N/A

	IPTIME	C200	N/A	N/A
	XIAOMI	MJSXJ02HL	N/A	N/A
	XIAOMI	MJSXJ02CM	N/A	Camera (Auxiliary)
NAS	ASUSTOR	AS6302T	N/A	N/A
	IPTIME	NAS1dual	N/A	NAS (Primary)
	IPTIME	NAS2dual	N/A	NAS (Primary)
	QNAP	TS-230	Storage (NAS)	NAS (Primary)
	QNAP	TS-228A	Storage (NAS)	NAS (Primary)
	SYNOLOGY	DS120j	N/A	NAS (Primary)
	SYNOLOGY	DS218	N/A	NAS (Primary)
	SYNOLOGY	DS218j	N/A	NAS (Primary)
	SYNOLOGY	DS220j	N/A	NAS (Primary)
	TERRA-MASTER	F2-210	N/A	NAS (Primary)
True positive (TP)			18	**37**
False positive (FP)			0	**0**
False negative (FN)			32	**13**
Precision			18/18 (100%)	**37/37 (100%)**
Recall			18/50 (36%)	**37/50 (74%)**

5. Related Work

Ways to distinguish devices has been carried out diversely due to the necessity of the security diagnosis in IoT environment. PropilIoT [8] introduced the method of analyzing network traffic through machine learning and distinguishing it into nine devices. In IoT Sentinel [3], it also automatically identified device types using features classified according to network traffic and conducted research on security perspective by using them. In IoT Sense [15], it dealt with how to deduce the type of device using the packet's header, payload, and behavior patterns, etc. Various views were also presented on how to distinguish devices. There are also fields in the methodology of distinguishing devices according to their service functions or applications. A paper [11] presented a classification plan according to the characteristics of IoT devices found in the city/campus and selected an attribute considering security vulnerabilities. There is also a study of functional classification of devices according to their own classification criteria based on the devices' characteristics [16].

Traditionally, the Passive Scan method has been used to distinguish the types of IoT devices [17-19]. However, such Passive scan is disadvantageous due to the fact that it has to monitor the traffic, which requires a lot of resource and time. Numerous researches using TCP-based approaches have been conducted as well. Scanning methods using TCP protocol have been widely used, and they were researched in fields that were strong in security [20, 21]. However, they were also time-consuming and less accurate. For Nmap full scan, one of the most well-known methods, it takes more than 5 minutes, and this, in some cases, was enough time for the attempted attacks to be successfully infiltrate to devices [22, 23]. There are also attempts to search and identify devices using DNS. They have methods distinguishing device categories according to DNS [24], and they also suggest a framework for the overall IoT environment and perform the module management for this [25]. Studies using UDP-based approaches have also been conducted. Based on the increase in UDP traffic, KISS attempted Fingerprint classification using UDP [26].

In this study, we proposed a lightweight active scan algorithm that effectively identifies devices using UPnP protocols (SSDP, MDNS, MBNS), which are most commonly used

methods by manufacturers, although we used the same UDP approach, we proved that this methodology was effective by the experiment.

6. Conclusion

Although the introduction of IoT devices is accelerating recently, IoT hacking cases such as POS(Point Of Sale) machine malware continue to occur. To prevent these security issues, it is important to deploy a security solution suitable for IoT devices on the network. In addition, different types of devices lead to different attack scenarios. Therefore, the effectiveness of security algorithm is reduced if the types of devices are not identified.

Passive scan method has traditionally been used to distinguish types of IoT devices on the network. However, the Passive Scan method has several issues related to personal data of clients. To overcome this, a recent study suggested a technique for preemptively identifying security issues caused by the device by identifying the device through an active scan method used by Nmap using TCP based scanning method.

However, TCP based active scan method is time-consuming. To overcome this, we proposed a technique called UAIS that can distinguish devices in a short period of time to ensure real-time availability. We have confirmed that real-time availability and efficiency can be achieved through active scan using UDP port based on the empirical study that the packet processing speed is remarkably fast.

To evaluate the efficiency and accuracy performance of the proposed approach, we compared it with the most widely used Nmap for detecting and distinguishing devices as the byword for network scanners in the existing IoT environment. The results of the experiment showed that UAIS can distinguish with more than twice the true positives and recall in time when UAIS is 1524 times faster than Nmap on average for 50 kinds of commercial off-the-shelf products.

For the future work, we hope to study the method of testing vulnerabilities (testing proof-of-concept (PoC) code devices to determine if they are vulnerable) according to the distinguished device types.

References

[1] A. Raza, A. Ikram, A. Amin, and A. J. Ikram, “A review of low cost and power efficient development boards for IoT applications,” in *Proc. of 2016 Future Technologies Conference*, pp. 786-790, 2016. Article (CrossRef Link)

[2] M. A. Khan and K. Salah, “Iot security: Review, blockchain solutions, and open challenges,” *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018. Article (CrossRef Link)

[3] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. R. Sadeghi, and S. Tarkoma, “IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT,” in *Proc. of* 2017 *IEEE 37th International Conference on Distributed Computing systems,* pp. 2177-2184, 2017. Article (CrossRef Link)

[4] Bitdefender. Bitdefender Advanced Business Security, Data Sheet. [Online]. Available: https://www.bitdefender.com/box

[5] Fing ltd. Device Recognition. [Online]. Available: https://www.fing.com/products/fingbox

[6] B. V. Solms and R. V. Solms, “The 10 deadly sins of information security management,” *Computers & security*, vol. 23, no. 5, pp. 371-376, July 2004. Article (CrossRef Link)

[7] S. S. Hasan and M. A. Qadeer, “Security concerns in WiMAX,” in *Proc. of First Asian Himalayas International Conference on Internet*, pp. 1-5, 2009. Article (CrossRef Link)

[8] 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 *Proc. of SAC 2017: Symposium on Applied Computing*, pp. 506-509, Apr. 1017. Article (CorssRef Link)
[9] G. F. Lyon, Nmap network scanning: The official Nmap project guide to network discovery and security scanning, Sunnyvale, CA, USA: Insecure, 2009.
[10] H. Kawai, S. Ata, N. Nakamura, and I. Oka, "Identification of communication devices from analysis of traffic patterns," in *Proc. of the 13th International Conference on Network and Service Management*, pp. 1-5, 2017. Article (CrossRef Link)
[11] 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 *Proc. of 2017 IEEE Conference on Computer Communications Workshops*, pp. 559-564, 2017. Article (CrossRef Link)
[12] M. Arora, U. Kanjilal, and D. Varshney, "Evaluation of information retrieval: precision and recall," *International Journal of Indian Culture and Business Management*, vol. 12, no. 2, Jan. 2016. Article (CrossRef Link)
[13] K. Yang, Q. Li, and L. Sun, "Towards automatic fingerprinting of IoT devices in the cyberspace," *Computer Networks*, vol. 148, pp. 318-327, Jan. 2019. Article (CrossRef Link)
[14] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. D.Guarnizo, and Y. Elovici, "Detection of unauthorized IoT devices using machine learning techniques," *arXiv: Cryptography and Security*, Sep. 2017. Article (CrossRef Link)
[15] B. Bezawada, M. Bachani, J. Peterson, H. Shirazi, I. Ray, and I. Ray, "Iotsense: Behavioral fingerprinting of IoT devices," in *Proc. of 2018 Workshop on Attacks and Solutions in Hardware Security*, pp. 41-50, 2018. Article (CrossRef Link)
[16] V. Jincy and S. Sundararajan, "Classification mechanism for IoT devices towards creating a security framework," *Intelligent Distributed Computing,* vol. 321. pp. 265-277, 2015. Article (CrossRef Link)
[17] J. Gonzalez and M. Papa, "Passive scanning in Modbus networks," in *Proc. of International Conference on Critical Infrastructure Protection*, vol. 253, pp. 175-187, 2007. Article (CrossRef Link)
[18] Adaptive passive scanning and/or active probing techniques for mobile device positioning, by V. Sridhara, S. M. Das, A. F. Naguib, and R. Palanki. (2013, Dec. 19). Patent Published No. US20130337847A1. Article (CrossRef Link)
[19] K. Gao, C. Corbett, and R. Beyah, "A passive approach to wireless device fingerprinting," in *Proc. of IFIP International Conference Dependable Systems & Networks*, pp. 383-392, 2010. Article (CrossRef Link)
[20] J. P. S. Medeiros, A. M. Brito, and P. S. M. Pires, "An effective TCP/IP fingerprinting technique based on strange attractors classification," in *Proc. of the 4th international workshop, and Second international conference on Data Privacy Management and Autonomous Spontaneous Security*, pp. 68-75, 2019. Article (CrossRef Link)
[21] A. Osanaiye and M. Dlodlo, "TCP/IP header classification for detecting spoofed DDoS attack in cloud environment," in *Proc. of 2015 International Conference on Computer as a Tool*, pp. 1-6, 2015. Article (CrossRef Link)
[22] N. Provos and P. Honeyman, "ScanSSH: Scanning the Internet for SSHServers," in *Proc. of the 15th UNENIX Systems Administration Conference*, pp. 25-30, 2001. Article (CrossRef Link)
[23] S. Balram and M. Wiscy, "Detection of TCP SYN scanning using packet counts and neural network," in *Proc. of IEEE International Conference on Signal Image Technology and Internet Based Systems*, pp. 646-649, 2008. Article (CrossRef Link)
[24] S. Lee, J. Jeong, and J. Park, "DNS name autoconfiguration for IoThome devices," in *Proc. of IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, pp. 131-134, 2015. Article (CrossRef Link)

[25] J. Jara, P. Lopez, D. Fernandez, J. F. Castillo, M. A. Zamora, and A. F. Skarmeta, "Mobile digcovery: A global service discovery for the Internet of Things," in *Proc. of 27th IEEE International Conference on Advanced Information Networking and Applications Workshops*, pp. 1325-1330. Article (CrossRef Link)
[26] A. Finamore, M. Mellia, M. Meo, and D. Rossi, "Kiss: Stochastic packet inspection classifier for udp traffic," *IEEE/ACM Transactions on Networking*, vol. 18, no. 5, pp. 1505-1515, Oct. 2010. Article (CrossRef Link)

Hyun-Chul Jung is PhD candidate in Computer Science and Engineering, Korea University, Seoul, Korea. He has served as the CEO of Norma Inc.(Wireless and IoT security solution company) since 2014. Before Norma, he was executive of wireless business department of Future System Inc. from 2012 to 2013. He was head of wireless business department of Konic Glory Inc. from 2011 to 2012. In addition to wireless intrusion prevention system and methods, he owns 7 registration patents and 25 application patents as inventor.

Hyun-geun Jo is researcher working at Norma Inc, he is in charge of checking and security certification for IoT vulnerabilities. He obtains Network Security Certification (CCNA, CCNP), has expertise in checking IoT vulnerabilities (Zero Day, One Day) and IoT Security Certification (KISA Project).

Heejo Lee is a professor at the Department of Computer Science and Engineering, Korea University, Seoul, Korea. Before joining Korea University, he was at AhnLab, Inc. as CTO from 2001 to 2003. From 2000 to 2001, he was a postdoctorate at the Department of Computer Sciences and security center CERIAS, Purdue University. He received his B.S., M.S., and Ph.D. degrees in Computer Science and Engineering from POSTECH, Pohang, Korea. He serves as an editor of both the Journal of Communications and Networks and the International Journal of Network Management.