Your smart home exchanged 3M messages: defining and analyzing smart device passive mode

Christian Badolato, Kaur Kullman, Nikolaos Papadakis, Manav Bhatt, Georgios Bouloukakis, Don Engel, Roberto Yus

Your Smart Home Exchanged 3M Messages: Defining and Analyzing Smart Device Passive Mode

Christian Badolato[†], **Kaur Kullman**[†], **Nikolaos Papadakis**[*], **Manav Bhatt**[†],
Georgios Bouloukakis[*], **Don Engel**[†], **Roberto Yus**[†]
{cbad1, kak, manavb1, donengel, ryus}@umbc.edu, {nikolaos.papadakis, georgios.bouloukakis}@telecom-sudparis.eu
[†]Dept. of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, USA
[*]Télécom SudParis, Institut Polytechnique de Paris, France

***Abstract*—The constant connectedness of smart home devices and their sensing capabilities pose a unique threat to individuals' privacy. While users may expect devices to exhibit minimal activity while they are not performing their intended functions, this is not necessarily the case, and traditional idle mode designations are insufficient to address the current landscape of smart home devices. To address this we propose a *passive mode* designation based on a comprehensive categorization of smart home devices. We then measure the network traffic of thirty-two devices in their respective passive modes. We find that 97% of the devices exhibit near-constant network activity in these modes (exchanging over 3M messages in 24 hours), with many of the devices initiating and responding to LAN communications with other devices, which potentially exposes users to privacy leakages.**

***Index Terms*—Smart Devices, Internet of Things, Smart Homes, Traffic Analysis, Privacy**

I. Introduction

The number of households equipped with Internet-of-Things (IoT) devices increased by 88% between 2019 and 2023, and is projected to increase another 86% by 2027 [1]. These devices provide convenience and comfort to their users by offering remote control, monitoring, and automation of household spaces [2]. However, this rapid growth goes hand-in-hand with ever increasing privacy concerns [3]–[5]. Smart home devices are often designed to remain network-connected and ready to accept commands for long periods of time without powering off; furthermore, they possess sensors, cameras, or microphones capable of collecting sensitive information which may be revealed to device manufacturers and third parties in at least some capacity. Even fully encrypted network traffic from much less invasive sensors can reveal sensitive information about users' behaviors and schedules to anyone with access to the devices' network traffic metadata [6], [7].

A large amount of research has focused on the privacy of smart home devices, including analysis of automation rules [8], [9], exploration of user perceptions and preferences [10], [11], and creation of privacy-enhancing techniques [12]. One mechanism used in the literature to understand the privacy implications of these devices is Network Traffic Analysis (NTA) [6], [7], [13], [14]. However, existing smart device NTA focuses either on the behavior of these devices during active use, or during "idle" periods in which they are not performing operations, but are ready to process commands and events.

Many smart home devices are capable of existing in states of limited functionality, either because the functionality is unneeded or because it has been intentionally disabled for privacy reasons. A smart speaker may have its microphone muted to prevent it from receiving voice commands, or a smart light bulb may still be able to receive commands and firmware updates [15] while not illuminating a space. These reduced-functionality, "passive" states deserve specialized attention, as an individual wrongly assuming a device is completely off may impact the way they interact with a space or the people within it. Furthermore, if no formal definition or standards exist for these states, manufacturers must either create their own or ignore this mode entirely. Hence, there is a critical need to formalize these states and investigate device behaviors. However, up to the authors' knowledge, no previous NTA work has focused on analyzing devices in passive states.

We present, to the best of our knowledge, the first formalization of smart home device passive modes and NTA of device behavior in such states. We establish a comprehensive categorization of smart home devices based on device behaviors, which enables straightforward construction of device-specific passive mode definitions. We then study the passive mode network behavior of a varied selection of 32 representative smart home devices across three test benches located in the US and France. To focus our analysis, we define and address the following research questions:

- **RQ1:** *Do smart home IoT devices communicate through the network while in passive mode and to what degree?*
- **RQ2:** *What type of communications take place in passive modes and what are the implications?*
- **RQ3:** *With whom do the devices communicate in passive modes and to what degree?*
- **RQ4:** *Are there differences in passive mode communication behavior between US and EU-located devices?*

Our analysis shows more than 3M packets transceived daily among the 32 devices in passive mode[1]. We also discover an abundance of Local Area Network (LAN) traffic, including discovery protocols, through which devices advertise their presence without explicit permission and share sensitive attributes (e.g., location) to other manufacturers' devices.

[1]Code at https://github.com/DAMSlabUMBC/Passive-Mode-Study

II. Background and Related Work

Network traffic analysis (NTA) is a popular approach within IoT for characterizing traffic patterns [16], performing automatic fingerprinting and device classification [17], and identifying non-essential communications [18]. NTA is also used to explore privacy considerations. Kayode and Tosun [19] decrypted and analyzed HTTPS traffic, discovering that many IoT devices rely solely on TLS to protect sensitive information. Hong et al. [20] used NTA to argue that IoT network communication should be disabled by default in order to preserve user privacy. Additionally, Apthorpe et al. [21] and Trimananda et al. [22] were able to infer user behaviors solely through the network metadata of IoT devices during normal operation. IoT traffic datasets have also been created to facilitate analysis of smart home devices. The GHOST project provides 10 days of smart home network traffic across several protocols [23], and Huang et al. compiled a massive collection of crowdsourced data from over 50,000 devices [24].

The majority of IoT NTA focuses on traffic generated by devices during active use. However, smart home devices almost universally support states in which they are not actively processing commands or performing functions for users. The term "idle" is typically used to describe states in which a smart device remains ready to respond to triggers. However, this term lacks the granularity required to fully describe the behaviors of non-active IoT devices. For example, there is a notable difference between a smart speaker having its microphone muted and it idly listening for a voice command. This is demonstrated by manufacturers' inclusions of "privacy modes" in smart devices such as cameras [25]. The ambiguity surrounding the expected behavior of device idle states implies the existence of a logical "passive" state which describes the expected behavior of the devices themselves. Despite this, no accepted standards exist to define such a state. This hinders researchers' abilities to compare devices' non-active behaviors, requires manufacturers spend resources to define their own passive states, reduces transparency in data privacy practices by encouraging the creation of proprietary mode definitions, and places a significant burden on users to understand the individual privacy implications of each device.

A few existing works perform NTA on idle states. Ren et al. [26] analyzed 112 hours of idle device traffic as part of a study on information leakage in consumer smart home devices. Girish et al. [27] analyzed the threat profile of IoT LAN traffic using a dataset including five days of idle traffic. Wan et al. [28] noted a significant amount of background traffic present outside of periods of active device use. However, neither these studies, nor the previously mentioned works and datasets, reflect the consideration for a "passive" mode for IoT. Indeed, the exploration and formalization of smart home device "passive" modes is notably absent from the literature.

III. Defining IoT Device Passive Mode

We propose a formal passive mode definition for smart home devices based on a novel categorization.

Device Categorization for Passive Behavior Analysis. Existing categorizations of smart home devices [17], [29]–[33] are tailored towards specific research tasks (e.g., device fingerprinting). Two multi-layered smart home taxonomies have been proposed: [34], which is based on communication methods and coarsely defined objectives, characteristics, and technologies; and [35], which groups devices based on high-level outcomes containing certain characteristics. The most robust IoT categorization to date defines 15 categories by functionality [36]. However, these taxonomies do not allow for privacy generalizations since: 1) Devices belonging to the same category might not perform similar operations (such as a smart dishwasher and a vacuum robot within the *Cleaning Systems* category), and 2) The coarseness of the categories results in grouped devices collecting (and thus, potentially exposing) different information (e.g., a vacuum robot may map a room, which is not required for the dishwasher).

To address these shortcomings, we propose a two-tiered categorization (see Table I) based on a synthesis of the categorization in [36] and the analysis of multiple smart home device directories [37]–[39]. Under this categorization, devices are assigned to a category by purpose and a subcategory by functionality; devices may belong to multiple categorizations (e.g., *Hubs and Assistants - Voice Assistants* and *Security and Monitoring - Indoor Cameras* for a voice assistant-enabled camera). Grouping devices by functionality ensures device comparability within the same subcategory w.r.t privacy.

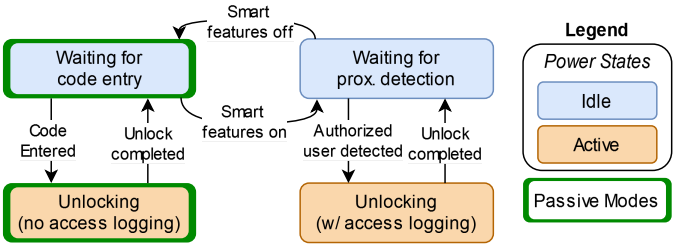

Fig. 1. Example states of a smart lock.

Formalizing IoT Passive Modes. We define a device to be in *passive mode* if either (1) the device is not actively performing its primary function, or (2) all data collection and reporting features of the device are disabled. For example, a voice-assistant enabled smart speaker with the primary function of "listen for and process voice commands" would be considered passive under condition (1) if its microphone were muted while no voice command was being processed. A smart space heater would be considered passive under condition (2) if its network features were disabled while heating an area. We construct this definition to be intuitive for privacy-conscious end users and to allow for similar devices to have equivalent passive mode definitions. The categorization in Table I facilitates expressing these modes per-subcategory instead of per-device.

For each subcategory, we satisfy condition (1) by determining the primary functions of devices within the subcategory (e.g., "Provide heating") and expressing device conditions which would disable these functions as a boolean expression

TABLE I
TWO TIER CATEGORIZATION OF SMART HOME IOT DEVICES.

Category	Subcategory	Passive Mode Def.
Entertainment and Media	Smart TVs	A/V Presentation off
	Speakers and Audio	
	VR Devices	
	Streaming Devices	Media streaming not active
Ambient Sensors	Environmental	Environment sensing disabled
	Occupancy	
Security and Monitoring	Outdoor Cameras	Camera off AND Microphone off AND Motion sensor off
	Indoor Cameras	
	Doorbells	
	Locks and Keypads	(Prox. sensing disabled AND No command processing) OR Data monitoring disabled
	Alarms and Notifiers	No notifications active
	Hazard Sensors	Environment sensing disabled
	Contact Sensors	
	Security Hub	Data monitoring disabled AND No command processing
Lighting	Outdoor Lighting	Actuator off OR Data monitoring disabled
	Indoor Lighting	
	Lighting Control	No command processing
	Lighting Hub	Data monitoring disabled AND No command processing
Wardrobe and Hygiene	Hygiene Tools	Data monitoring disabled AND Main device purpose not active
	Clothing Storage	
	Bathing	
	Toilets	User not detected OR Data monitoring disabled
	Mirrors	A/V Presentation off
Wearables	Accessories	(Environment sensing disabled AND Health sensing disabled AND Smartphone connection not active) OR Device not worn
	Clothing	(Environment sensing disabled AND Health sensing disabled) OR Device not worn
	Glasses	A/V Presentation off OR Device not worn
Fitness	*N/A*	Main device purpose not active
Power and Energy	Switches	No command processing
	Plugs and Outlets	Actuator off OR Data monitoring disabled
	Energy Meters	Data monitoring disabled
Cleaning and Sanitation	Vacuum/Mop Robots	Main device purpose not active
	Trash Disposal	No command processing
	Laundry	Main device purpose not active OR Data monitoring disabled
Meal and Food	Ranges	Main device purpose not active OR Data monitoring disabled
	Dishwashers	
	Small Appliances	
	Refrigerators	A/V Presentation off OR Data monitoring disabled
Sleep	Sleep Trackers	Health sensing disabled OR User not detected
	Beds and Bedding	
	Alarm Clocks	No notifications active AND A/V Presentation off
Simple Actuators	*N/A*	Main device purpose not active AND No command processing
Gardening and Property Maintenance	Lawn Care Robots	Main device purpose not active
	Irrigation	Main device purpose not active OR Data monitoring disabled
	Weather Sensor	Environment sensing disabled
	Planters	Data monitoring disabled
HVAC and Water	Thermostats	No command processing AND Data monitoring disabled
	Water Meters	Data monitoring disabled
	Standalone Heating	Main device purpose not active OR Data monitoring disabled
	Standalone Cooling	
Hubs and Assistants	Voice Assistants	Microphone off AND Data processing not active
	IoT Protocol Hubs	No command processing AND Data monitoring disabled
	Status Displays	A/V Presentation off
Pet	Food/Water Bowls	Data monitoring disabled AND Main device purpose not active
	Waste management	Data monitoring disabled OR User not detected

(e.g., "`Heating function not active`"). We satisfy condition (2) by expressing conditions which enable device functionality without data monitoring or collection (e.g., "`Monitoring functions off`"). As only one condition needs to be satisfied, we express the complete definition as the logical OR of these expressions. We generalize the definitions by abstracting subcategory-specific conditions into generalized conditions (e.g., "`Heating function not active`" to "`Main device purpose not active`"). Finally, we simplify the resulting boolean expressions to produce the final passive mode definitions shown in Table I. The boolean format of the subcategory definitions allows one to easily determine the complete definition for a device as the logical AND of each of its subcategories' definitions. For example, the passive mode for the previously mentioned voice assistant-enabled camera would be defined as *`Camera off AND Microphone off AND Motion sensor off AND Data processing not active`*.

We emphasize that these passive modes are distinct from the "idle" states discussed in Section II as shown by the mode breakdown for an example smart lock given in Figure 1. We also note that these definitions provide a framework for expressing behavior w.r.t. privacy but do not confer privacy guarantees. For example, a Smart TV is considered to be in passive mode when its display is off; however, an embedded microphone could still be capturing ambient audio.

IV. METHODOLOGY

A. Device Selection

Thirty-two smart home devices were selected for analysis across three physical test benches (two in the US and one in France, hereafter referred to as US1, US2, and FR). Devices in FR and US2 were part of existing IoT testbeds. The US1 devices were chosen to provide overlap with subcategories from the other test benches (including six devices shared with FR— five identical, and one differing only by generation), and to introduce the *Small Appliance* subcategory, which is projected to be present in 34.8% of households by 2029 [40]. To select these new devices, we conducted a search on Amazon and chose devices on the first page of results with over 1,000

TABLE II
DEVICES PER CATEGORY TESTED FOR PASSIVE MODE TRAFFIC.

Device Name	Bench	Subcategory
DreamGlass Air	US1	Glasses
HoloLens 2	US2	Glasses
Magic Leap 1	US2	Glasses
D-Link Wi-Fi Camera	FR	Indoor Cameras
Nest Camera 1st Gen	FR	Indoor Cameras
Litokam Security Camera	US1	Indoor Cameras
Netvue Orb Mini	US1	Indoor Cameras
Hue Go Accent Light	FR	Indoor Lighting
TP-Link Smart Bulb	FR	Indoor Lighting
Hue Smart Bulb	US1/FR	Indoor Lighting
Amazon Basics Light Bulb	US1	Indoor Lighting
Hue Bridge	US1/FR	Lighting Hub
Maxcio Smart Power Strip	FR	Plugs and Outlets
Hue Smart Plug	US1/FR	Plugs and Outlets
TP-Link Wi-Fi Plug	US1/FR	Plugs and Outlets
GoveeLife Electric Kettle	US1	Small Appliance
Sony Smart TV	FR	Smart TVs
Nest Learning Thermostat	FR	Thermostats
Roborock S7	US2	Vacuum/Mop Robots
Echo Show 5th Gen	FR	Voice Assistants
Google Home Speaker	FR	Voice Assistants
Nest Mini	US1/FR	Voice Assistants
Echo Dot	US1/FR‡	Voice Assistants
Metaquest Pro	US1	VR Devices
Metaquest 1	US2	VR Devices
Metaquest 2	US2	VR Devices

‡Device differs in generation number between US1 and FR.

reviews, focusing on manufacturers not already present in the other test benches. Across all test benches, the devices belonged to eleven different subcategories and fifteen unique manufacturers as summarized in Table II.

B. Network Capture Methodology

Test Bench Configurations. Figure 2 provides an overview of the test bench setup. All devices utilize wireless IP communication except the Hue light bulbs and smart plugs which communicate to the Hue Bridge via the Zigbee protocol [41]. The Hue Bridge then performs both LAN and Wide Area Network (WAN) communication through Ethernet. To ensure comparability between all devices, we limit our analysis to IP communication and aggregate Hue device results under their respective bridges. No user-initiated pairing was performed between any US1 devices with the exception of the Amazon Echo Dot with the Amazon Light, and the Hue devices with their bridges, both of which were required for device control.

Each test bench communicates through its own router running OpenWrt 23.05 [42] set to UTC+0 to avoid time-zone confusion between test benches. US1/2 used a Netgear WAX206 and FR used a Netgear WAX220 (both models are officially supported by OpenWrt 23.05, which ensures consistent results). Each router was configured to allow wireless connections to all Wi-Fi devices, while the Hue Bridges were connected to their routers' LAN port. This LAN port was bridged with the router's wireless interfaces to ensure all traffic passed through the same logical interface. US1 and US2 devices were allowed to request and communicate freely through IPv6 addresses. Due to network restrictions, only LAN-based IPv6 traffic was allowed for FR devices, however, the findings detailed in Section V-B indicate it is unlikely these devices would have attempted IPv6 WAN communication.

Passive Mode Conditions. Some devices provide manufacturer-defined "sleep" or "privacy" modes which are intended to allow a user to express their desire to have some degree of control over their privacy. In several cases, these modes preclude the ability to place the devices into a truly passive mode. We attempt to align the devices' functionality with the definitions provided in Table I, falling back to these manufacturer-defined modes when required. In this way, we closely emulate the experience of a typical user configuring their device through vendor-provided interfaces.

Traffic Captures. Network captures were collected in PCAP format via the `tcpdump` utility filtered on the bridged interfaces of the routers. Prior to each capture, the devices were rebooted to clear all existing session data. Each device was placed into their passive modes and left in this state for the duration of the capture. Furthermore, no user-triggered interactions were initiated with the devices during this period, nor were any device companion apps opened.

Multiple captures were performed across the test benches to account for device-level network failures and device availability. The combined captures resulted in between 71 and 168 hours of passive mode data per device. Each capture contained purely steady-state passive mode traffic with no user-initiated interactions, mode transitions, or power cycles. Device traffic was identified and isolated by MAC addresses, and non-IP traffic, TCP re-transmissions, TCP lost segment notifications, and duplicate TCP acknowledgements were filtered out. We also removed DHCP, IGMP, and ICMP traffic, as their primary purpose is network administration and error reporting. DNS records were kept to assist with the identification of endpoints but DNS traffic was not included in communication metrics.

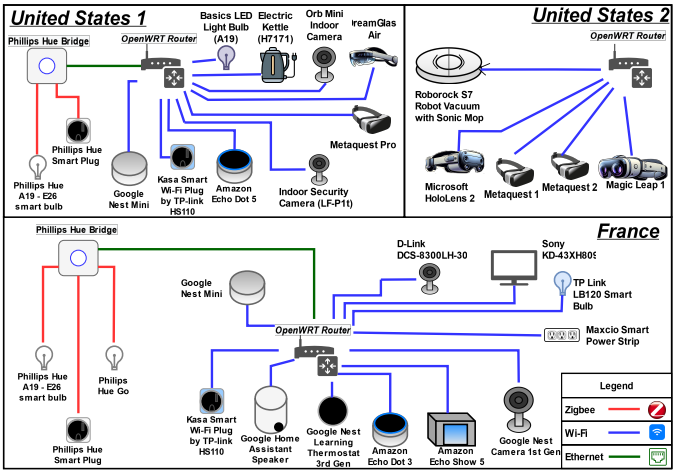

Fig. 2. The physical setup of each test bench.

C. Analysis Methodology

1) Parties of Concern: To identify potential privacy implications within our dataset, we first define the network entities of concern. We adopt a modification of the categorization by Ren et. al [26] intended to capture concerns specific to networks with multiple LAN-communicating devices:

Remote First Parties. The manufacturer of the device, their parent company, or their subsidiaries. We assume these entities may know device identifications and configurations, identifying information about a user (e.g., a user's email), the layout of a user's space (e.g., rooms configured within a smart hub), and pairings with other smart devices. However, there may be information a user may not wish to share with these parties such as their schedule or the existence of unpaired devices within the space. Furthermore, we do not assume these parties know the same identifying information about a user (e.g., one may know a user's surname, while another may not).

Remote Support Parties. Entities used by the device manufacturer to provide services and/or resources in support of a device's primary functions. This may include content delivery networks (CDNs) [43], IoT platforms (such as Tuya [44]), and cloud computing entities. We assume these entities have the same knowledge of device and user attributes as first parties with the exception of user-identifying information.

Remote Third Parties. All other WAN entities. These parties are not required for the device to perform its primary functions and may provide advertising or analytics services. We consider any data sent to these parties to be a potential concern.

Network Infrastructure Parties. Entities which manage the networking routing infrastructure, which includes a user's internet service provider (ISP) or proxy servers. As WAN traffic must pass through these parties, we assume these entities may record traffic metadata and observe plaintext communication, but will not attempt to decrypt encrypted data.

Local Smart Devices. Other IoT devices which are connected to the LAN network. Even information shared across LAN networks can pose privacy concerns [27]; this includes devices created by the same manufacturer should they transmit LAN-collected data to remote servers without prior user consent.

2) Traffic Analysis Approach: To the best of our knowledge, no other NTAs of smart home devices' passive behaviors have been performed. Hence, we perform a manual characterization to avoid issues which could arise from automated or machine learning-based classifications. We leverage the `tshark` utility provided by Wireshark [45], with some manual analysis being performed using the open-source packet capture, indexing, and search tool Arkime [46]. To address the research questions presented in Section I, we targeted the following attributes.

Overall Communication Statistics. We quantify the degree to which the devices communicate using the aggregated average and coefficient of variation (CoV) over periodic intervals as in [47]. This metric allows comparison of traffic variation between devices with statistics that differ by multiple orders of magnitude. A low CoV correlates to more consistent traffic patterns over the course of the experiment (relative to its mean and standard deviation), whereas device traffic with higher CoVs exhibit more inconsistent behaviors while passive. We select 1-hour intervals to provide sufficient data points to construct an accurate average over the varying length captures.

Protocols. We analyze the distribution and implications of utilized protocols, focusing on application-layer protocols encapsulated within UDP and TCP. We leverage Wireshark's native dissectors to identify each packet's protocol. If no application protocol is detected, we resolve the protocol using well-known port associations. If no association is found, we record the port and its transport protocol. We also analyze the proportion of traffic which uses protocol-level TLS encryption.

Endpoints. We analyze contacted endpoints by first attempting to resolve an IP address to an associated domain name. For TLS communication, we prioritize the SNI attributes in Client Hello messages to precisely identify domain names and owning parties [48]. If no SNI is provided, we extract the subject name from the certificates as the host identity. For non-TLS WAN traffic, we resolve domain names via captured DNS queries. If a domain name still cannot be determined, endpoint owners are identified through public DNS registrations if available, otherwise we fall back to the owners defined within the WHOIS and ASN [49] databases. LAN devices are resolved via MAC address. We classify the owners and IP addresses as described in Section IV-C1.

Geolocating IP addresses is a difficult task due to anycast routing prevalent among CDNs [50], and standalone databases have been shown to be ineffective at reliably determining the location of endpoints [26]. Overcoming this limitation is an active field of research. While preliminary tools for accurate IP geolocation exist [51], [52], they require custom environments or curated datasets. Hence, we consider accurate passive mode endpoint geolocation to be a subject of future interest.

V. Experimental Results

A. RQ 1: Traffic Volume and Variation

Overall Volume. We explore the degree to which passive smart home IoT devices communicate to gain an initial understanding of the importance of analyzing passive traffic. Our findings are shown in Table III. Both the packet and byte-wise volume of the traffic differs significantly, from less than 100 packets and 0.5KB per hour to as much as nearly 40,000 packets and 55.8MB worth of data. The overall volume of traffic is strikingly high. When accounting for all devices, roughly 142,000 packets and 77.4MB of traffic was transceived per hour (3.4 million packets and 1.86GB a day) with *Voice Assistants* responsible for the majority of the traffic.

Differing devices also show large differences in the variation of their traffic. Devices such as the Metaquest 1 and D-Link Camera exhibited inconsistent behavior while passive. This is indicative of non-periodic operations still being performed by the devices without explicit user interaction, which could leak user data to both local and remote parties [26]. Furthermore, using packet header information for device fingerprinting has

TABLE III
HOURLY AVERAGE VOLUME AND VARIANCE OF TRAFFIC.

Device Name	Packet		Byte	
	Average	CoV	Average	CoV
Metaquest 1 (US2)	39,364	9.45	55838.9KB	10.75
Echo Show 5 (FR)	19,781	0.05	3159.5KB	0.33
Echo Dot 3 (FR)	19,324	0.02	2323.7KB	0.13
Google Speaker (FR)	17,559	0.28	2398.5KB	0.50
Nest Mini (FR)	15,860	0.25	2475.8KB	0.57
Metaquest Pro (US1)	5112	0.53	3370.3KB	2.01
Hue Bridge (FR)	3581	0.15	947.0KB	0.21
Hue Bridge (US1)	3065	0.62	677.5KB	1.12
Nest Mini (US1)	2554	0.22	600.4KB	0.79
Echo Dot 5 (US1)	2359	0.70	1139.4KB	4.34
Netvue Camera (US1)	2078	0.92	425.4KB	0.95
Sony TV (FR)	2074	0.23	752.1KB	0.68
Litokam Camera (US1)	1309	0.02	246.6KB	0.02
Metaquest 2 (US2)	1126	1.02	662.1KB	1.42
Roborock S7 (US2)	1120	0.09	133.4KB	0.22
Nest Thermostat (FR)	1057	1.00	428.1KB	1.06
Nest Camera (FR)	929	0.09	98.5KB	0.14
D-Link Camera (FR)	870	4.60	746.2KB	5.54
Maxcio Power Strip (FR)	665	0.23	96.0KB	0.31
DreamGlass Air (US1)	614	4.56	268.4KB	5.10
TP-Link Light (FR)	573	0.32	239.8KB	0.34
TP-Link Plug (FR)	472	0.14	156.7KB	0.28
HoloLens 2 (US2)	358	1.47	130.9KB	3.17
Govee Kettle (US1)	187	0.42	20.9KB	2.38
Amazon Light (US1)	94	0.15	15.2KB	0.29
TP-Link Plug (US1)	50	0.20	5.9KB	0.57
MagicLeap (US2)	22	6.97	8.4KB	7.62
TOTAL	142,157	N/A	77365.6KB	N/A

been shown to be able to identify the company, make, model, and other attributes of individual devices with a high degree of accuracy [17]. The degree and variability of the traffic observed in our test benches indicates that network infrastructure parties with access to traffic metadata could reasonably infer these attributes, even when the devices are in passive modes. High CoVs may also imply short bursts of significant activity, for example, a system update by the Echo Dot 5 resulted in a drastic increase in transceived data for a small time-frame. Overall, we observe being in passive mode does not preclude devices from performing unexpected operations.

B. RQ 2: Type of Communication

LAN Traffic. LAN traffic accounts for a significant degree of passive mode network activity. LAN communication accounted for 50.4% of the total packet counts and was observed in 19 of the 27 non-Zigbee devices, including more than 75% of the packets captured for 9 of them. Figure 3 provides the distribution of LAN versus WAN packets transceived.

We see varied behaviors with regards to LAN communication, even within subcategories. For example, within *Indoor Lighting*, the TP-Link Light showed a notable preference for LAN communication while the Amazon Basics light did not communicate over the LAN in any capacity. Furthermore, shared devices and subcategories between the FR and US1 test benches exhibited different patterns. The FR *Voice Assistants* all exhibited greater than 75% LAN traffic by packet volume, however, neither US *Voice Assistant* surpassed 25% LAN traffic. *Indoor Cameras* showed the reverse trend, with both US cameras choosing to communicate over LAN more than 50% of the time, while the FR cameras never used LAN traffic in excess of 2% of their total packet counts. Some of this variation can be explained as traffic meant to discover and communicate with other local devices (examined later in this section). However, this also indicates a potential lack of commonality among the current passive mode behaviors of similar devices, which can contribute to users' uncertainty over privacy expectations in smart home environments. Additionally, while this overall volume of LAN traffic may be expected during active periods (when devices are actively streaming information for local control and monitoring), this is a large amount of local communication for passive devices. Despite being constrained to the local network, this type of traffic has been shown to be a significant vector of privacy leakage in networks containing other local smart devices [27].

IPv6 Traffic. IPv6 communication was present among all *Voice Assistants* and *VR Devices*, as well as the Sony TV, Hue Bridge, HoloLens 2, and DreamGlass Air. However, most devices only used LAN-based IPv6 for network discovery— only the *VR Devices* and two *Glasses* contacted remote endpoints over IPv6, with the Meta Quest 1 accounting for over 95% of the total IPv6 traffic. We also observe the DreamGlass Air assigned itself several externally-facing IPv6 addresses despite IPv6 accounting less than 0.5% of its total traffic. These assignments may be automatically allocated by the underlying operating system and may not be intentionally requested.

Overall, due to the lack of unique privacy implications with the use of IPv6 over IPv4, and due to the minimal quantity of IPv6 traffic outside of the Meta Quest 1. We do not consider IPv6 traffic separately from IPv4 for the rest of this paper.

Application Protocols. We classify the observed application layer protocols into four categories: *management*, responsible for ensuring device synchronization and network traversability; *discovery*, responsible for detecting other IoT devices on the LAN; and both *encrypted* and *unencrypted application-specific protocols*, responsible for performing device functions and allowing user control. Table IV summarizes the protocols used by the devices. We denote protocols that are not well-known by their port and transport protocol (e.g., udp/1982).

Management protocols (4 in total) including the well-known Network Time Protocol (NTP) and Session Traversal Utilities for NAT (STUN). Classic STUN, a deprecated version of STUN, was detected between the Google *Voice Assistants*, however, this may indicate a Google-specific protocol masquerading as classic STUN since the protocol was used over LAN and never successfully executed. Additionally, we observe an Echo-specific protocol on udp/55444 which is used to synchronize time and audio services across Amazon Alexa-enabled devices on the same LAN [53], [54]. We note that the Echo Dot 5 did not generate any such traffic due to no other Alexa-enabled devices being present on the US1 LAN.

Discovery protocols (7) including the well-known Link-Local Multicast Name Resolution (LLMNR), Simple Service

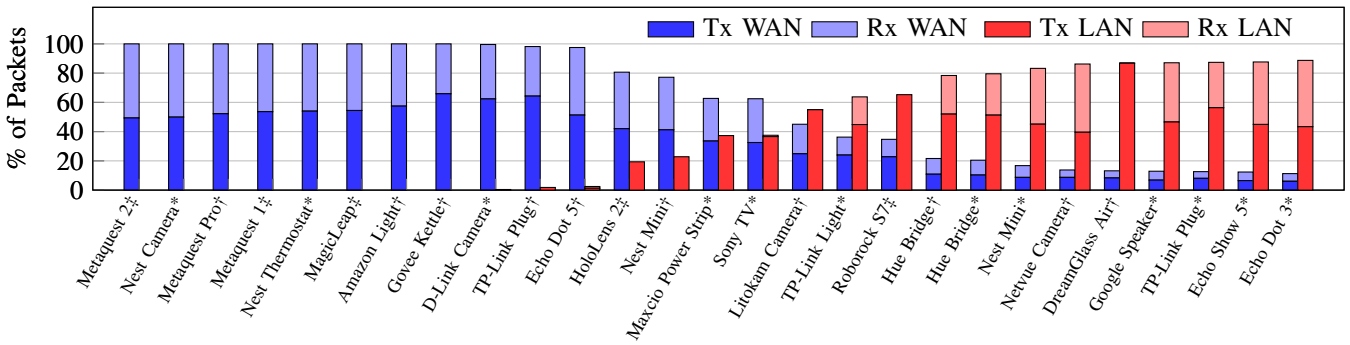

Fig. 3. Packet-wise WAN vs. LAN distribution for each device ordered by % of LAN packets (*FR - †US1 - ‡US2).

Discovery Protocol (SSDP), and multicast DNS (mDNS). These provide similar services by allowing local name resolution and LAN service discovery. Devices sometimes implement all three protocols to support maximal discovery functionality. We also observe four vendor-specific discovery protocols. The Tuya smart-home platform protocol detected on udp/6667 allows discovery of Tuya-integrated applications through AES-encrypted polling. The TP-Link discovery protocol, recognized as TPLINK-SMARTHOME ("smarthome" in Table IV) on tcp/9999 and udp/9999 supports devices querying the network for TP-Link devices via a request-reply paradigm. Finally, two protocols (udp/50000 and udp/1982) present on Echo devices were identical to SSDP traffic, indicating a custom implementation using non-standard ports.

Encrypted application-specific protocols (12) including HTTPS and secure-MQTT (a popular messaging protocol for IoT deployments [55]). We observe 10 vendor-specific encrypted protocols. Tuya provides their own implementation of secure-MQTT on tcp/8886. There is also an Echo-only protocol on tcp/55443 used to coordinate Alexa commands similar to the udp/55444 management protocol [54]. The Nest Thermostat communicates with *.transport.home.nest.com over tcp/9543, which is presumably used to perform cloud-based commands and queries. TP-Link devices also communicate with cloud servers via their own port of tcp/50443. Finally Google *Voice Assistants* used six different non-standard protocols: two WAN protocols, tcp/5228 (Google Talk as validated by the TLS certificates used for this connection) and udp/443 (QUIC, Google's open protocol for establishing stateful UDP connections [56]), and four LAN protocols tcp/8012, tcp/9000 (shared by the Sony TV), tcp/10005, and tcp/10101. The purpose of the LAN protocols is unknown, however, this traffic is only used between Google devices and is signed by certificates linked to Chromecast capabilities.

Unencrypted application-specific protocols (8) with the only well-known protocol being HTTP. The rest include udp/58866, which enables command and control of the Roborock S7 from connected smart home platforms; udp/56700 on all Echo devices, which allows Alexa-enabled devices to communicate with LIFX compatible light bulbs [57]; and five protocols of unknown purpose: two WAN protocols (8555/udp and 9700/udp) for Netvue cameras, as well as three on the LAN (udp/9478, udp/1111, and udp/10101) from Google sources.

TABLE IV
PROTOCOLS PRESENT WITHIN DEVICE TRAFFIC.

Device Name	Discovery	Manage.	Encrypt.	Unencrypt.
Amazon Echos	mdns†, ssdp†, smarthome†, udp/1982†, udp/50000†	ntp*, udp/55444†	https*, tcp/55443†	http*†, udp/56700†
Amazon Light	-	ntp*	https*, secure-mqtt*	-
D-Link Camera	mdns†	stun*	https*	http*
DreamGlass Air	mdns†, ssdp†, udp/50000†	ntp*	https*	http*†
Google Speaker & Nest Mini	mdns†, smarthome†	ntp*, classic-stun†	https*, quic*, tcp/5228*, tcp/8012†, tcp/9000†, tcp/10005†, tcp/10101†	http*†, udp/1111†, udp/9478†, udp/10101†
Govee Kettle	-	ntp*	secure-mqtt*	http*
HoloLens 2	mdns†, llmnr†	ntp*	https*	http*
Hue Bridge	mdns†, ssdp†	ntp*	https*	http*†, udp/1111†
Litokam Camera	udp/6667†	-	https*, secure-mqtt*	-
Maxcio Power Strip	udp/6667†	-	https*, tcp/8886*	-
Nest Camera	-	ntp*	https*	-
Nest Thermostat	-	ntp*	https*, tcp/9543*	http*
Netvue Orb Mini	ssdp†	-	https*, secure-mqtt*	http*†, udp/8555*, udp/9700*
Quests & MagicLeap	-	ntp*	https*	http*
TP-Link Devices	smarthome†	ntp*	https*, tcp/50443*	udp/1111†
Roborock S7	-	-	https*, secure-mqtt*	udp/58866†
Sony TV	mdns†, ssdp†, smarthome†, udp/50000†	ntp*	https*, quic*, tcp/5228*, tcp/9000†	http*†

*Observed on WAN traffic. †Observed on LAN traffic.

Protocol Distribution. To avoid skewing the results towards the devices that transceived the most data, we calculate the distribution per device then average these values. Across the four classes, encrypted traffic is most prevalent at 59.9%, while discovery encompasses 22.1% of the packets (see Figure 4).

While the large majority of the observed WAN traffic is encrypted, LAN traffic is rarely secured. Unencrypted LAN traffic has been identified as a source of potential privacy issues [58]. Discovery protocols are a particular concern as

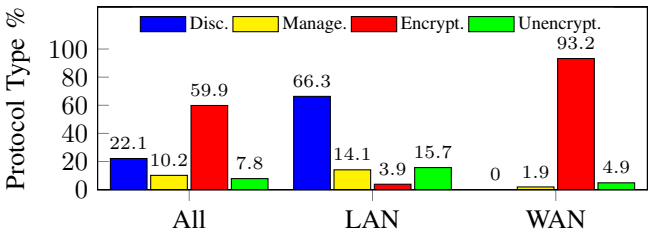

Fig. 4. Distribution of packet-wise application protocol types.

a potential vector for privacy leakage, as local smart devices devices may share identifying information among each other without explicit authorization, which can then be forwarded to the cloud [27]. We observed this in a particularly notable example: the US1 TP-Link Plug's discovery data is freely offered to any device which requests it, even if the devices have not been explicitly paired. This data contains the device's latitude and longitude coordinates up to the sixth decimal place —a precision capable of identifying the exact desk on which our test bench was located. This disclosure is not unique to our device and was also observed by the authors of [27]. We observe a geographical behavioral difference with the FR TP-Link Plug: while still disclosing latitude and longitude, the precision was limited to four decimal places (which "only" identifies the building in which the test bench is located).

C. RQ 3: Endpoints

While the number of endpoints contacted by each device varied significantly (e.g. the Litokam camera contacted only 2 unique endpoints while the Echo devices all contacted over 300), the main metric we examine is the distribution of the party types to which each device communicates. Each device's WAN communication primarily favored either first or support parties, with 18 devices (All *Voice Assistants*, *VR Devices*, Google Devices, Hue bridges, as well as the TP-Link Light, Roborock, HoloLens, MagicLeap. and D-Link) having more than 80% first party communication, 7 devices (both FR *Plugs and Outlets*, both US1 *Indoor Cameras*, the DreamGlass Air, Sony TV, and Govee Kettle) having more than 80% support party communication, and only 2 devices (the US1 TP-Link *Plugs and Outlets* device and the Amazon Light) having less than a 20% difference between first and support parties. The only devices which exhibited more than 1% third party communication were the Nest Minis (12.2% FR, 1.9% US1), Google Speaker (11.2%), Sony TV (10.9%) and Roborock S7 (1.9%). As, from a privacy standpoint, outgoing traffic is particularly relevant, Figure 5 illustrates the proportion of outgoing WAN traffic transmitted to different remote parties.

Figure 6 shows the distribution of protocol types transmitted over WAN. A large majority of unencrypted and encrypted application traffic is sent to first parties (88.5% and 91.9%, respectively), whereas management protocols preferred support parties at a rate of 92.4%. This overwhelming preference for support parties is partially due to NTP encompassing a majority of management traffic, since NTP servers often belong to pools which load-balance traffic between them. However, CDNs also contribute heavily to the presence of support party

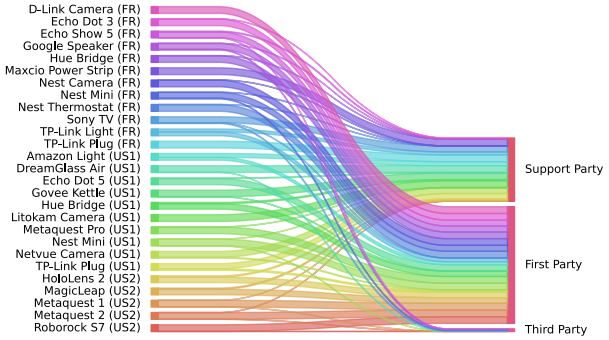

Fig. 5. Target entities for outgoing (Tx) device traffic.

traffic. The nature of these CDNs may cause potential privacy leakages either through intentional profiling or as a by-product of intrusion detection [59]. This is especially relevant to the IoT domain, where even encrypted traffic from normal device functions can reveal lifestyle information [7]. While these threats are currently unavoidable during active device use, the pervasiveness of these considerations extending to passive mode behaviors is important to consider.

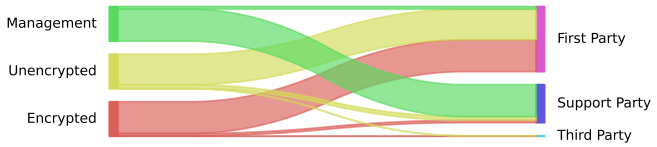

Fig. 6. Target entities for outgoing (Tx) traffic types.

Third-party traffic accounted for 1.3% of encrypted traffic and only 0.7% of unencrypted traffic, which indicates smart home devices may generally avoid third party communications when passive. Notably, however, the Google Speaker did communicate with YouTube addresses using unencrypted communications while passive, which could potentially leak private information to infrastructure parties.

LAN Endpoints. We observe LAN communication among 19 of the devices as shown in Figure 7. In particular, LAN communication accounted for greater than 80% of each of the FR *Voice Assistants*' total traffic. Many devices participate in LAN discovery even when unpaired. Amazon and Google devices across both FR and US1 both advertised their presence to TP-Link devices, and the Litokam camera sent Tuya discovery messages via broadcast every five seconds. Similarly, the Netvue camera requested SSDP information every minute over multicast, which initiated information exchange and service discovery with the Hue Bridge. The HoloLens 2 also issued many requests over multicast, and the S7 frequently advertised its presence via local broadcast. While not all LAN traffic is indicative of privacy concerns (traffic between *Voice Assistants* of the same vendor can coordinate time synchronization and command processing [54]), the existence of this traffic among passive devices is worth investigating further.

D. RQ 4: EU vs. US

Throughout our investigation, the FR and US devices behaved similarly. Differences in LAN traffic were more closely related to the number and manufacturer of devices present

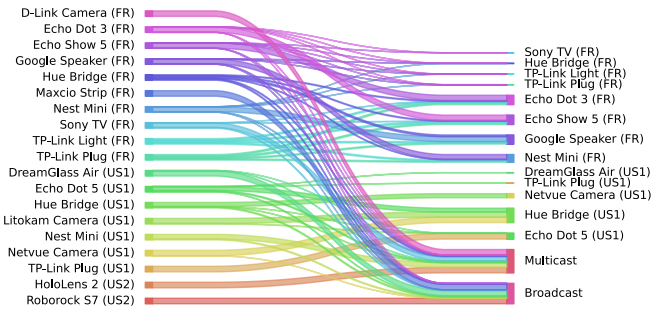

Fig. 7. Summary of LAN Traffic.

on the local network, and FR devices were equally eager as US devices to share their discovery information —the reduced precision of location information present within the TP-Link devices was the largest observed difference in discovery. However, similarities are partially to be expected as it would be costly for manufacturers to maintain multiple hardware models and software versions based on location. At the same time, we do not notice any special considerations to account for compliance to regulations such as the General Data Protection Regulation (GDPR) [60]. While not a privacy concern by itself, it is an aspect worth investigating further.

VI. Discussion

Here we note several key observations from our study.

Current "passive" modes are insufficient. The lack of standardization among smart device operational modes allows for significant variation between the behaviors and privacy capabilities of different device categories. Only *Indoor Cameras* possessed an explicit "Privacy" or "Sleep" mode. This both burdens the users by requiring them to evaluate the capabilities and privacy of every device, and hurts the interoperability and comparability of devices. Furthermore, privacy policies do not remedy this situation. While it is clear that websites and other non-pervasive technologies can only capture data during active use, this cannot be assumed in the IoT domain. However, no policy for any tested device contained information regarding periods during which devices captured data. The only assumption privacy-focused users can make is that these devices always collect data, even while passive. A standardized set of requirements for device passive modes must be adopted to provide clear understanding of devices' privacy implications.

Idle does not imply "passive." We observed roughly 3 million packets being transceived while the devices were not performing any active functions, with *Voice Assistants* accounting for 54%. This is concerning since these assistants contain microphones and other invasive sensors capable of capturing significant amounts of private information [61]. Additionally, there is a lack of transparency as to the passive-mode behavior of the devices; we were unable to determine the purpose of 11 observed protocols, which prevents us from assuming the devices are truly passive. Furthermore, the degree of LAN activity was heavily related to the amount and types of other local devices. The FR bench exhibited over 4 times the average amount of LAN traffic than the US1 bench (despite only having 3 more devices) due to excessive traffic between *Voice Assistants*. We also observed no mechanism for users to disable network traffic while retaining more limited features. The pervasiveness of traffic during periods of device "idleness" injects ambiguity into a user's expectations of privacy, especially when these devices contain invasive sensors. This forces privacy-focused users to completely shutdown their devices when not in use, which may require physical de-powering.

Passive devices often probe the LAN. We observed 19 devices participating in LAN communication while passive, including 6 US1 devices which had never been paired with each other. While the purpose of this traffic is primarily discovery services meant to improve the user's experience or allow coordination between devices of the same manufacturer, this still requires users to accept all privacy risks posed by this communication. The inability to disable or easily prevent LAN traffic exposes users to tracking and device fingerprinting attacks even within the confines of their own home network.

Outgoing traffic is encrypted, internal not so much. 90% of WAN traffic was encrypted with protocol-level encryption, which drastically reduces the threat surface for passive network observers to discover private information. However, this number drops to only 3.9% over the LAN. While discovery traffic needs to be unencrypted to facilitate device discovery without pre-shared keys or trusted third parties, we observed at least one instance of personal location data being leaked in cleartext to other local devices. With the increasing shift towards more devices being co-located on the same LAN, it is critical for manufacturers and developers to consider the growing need to preserve user privacy through local traffic encryption, especially during periods of device passivity.

VII. Conclusion and Future Work

We presented a formal definition for characterizing smart home IoT passive modes by establishing and leveraging a two-tiered device categorization. With this definition, we provided a method for defining the passive mode of emerging IoT devices in a generalized manner. We found that current implementations of IoT idle states is insufficient to properly address privacy concerns. We then performed NTA on 32 smart home devices in modes in which a user could assume device passivity. Devices in these states freely communicate amongst themselves and the Internet regardless of whether their functions are in active use. In the future, we plan to further explore the issue by analyzing a larger range of devices focusing on the transitions between passive and active modes, and to include geolocation within our metrics. Also, we will conduct an in-depth user study to understand how to fully capture users' privacy concerns in passive mode implementations.

Acknowledgment

This work is partially supported by the Horizon Europe projects DI-Hydro (grant agreement No. 101122311) and MEDIATE (grant agreement No. 101168465). We also thank Krish Chatterjie, Hannah Stasik, and Ben Hawkins for their help running experiments.

REFERENCES

[1] Statista, "Number of users of smart homes worldwide from 2019 to 2028," 2023. [Online]. Available: https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the-world

[2] R. Yus *et al.*, "The SemIoTic ecosystem: A semantic bridge between IoT Devices and smart spaces," *ACM Trans. Internet Techn.*, vol. 22, 2022.

[3] P. Pappachan *et al.*, "Towards privacy-aware smart buildings: Capturing, communicating, and enforcing privacy policies and preferences," in *37th IEEE Int. Conf. on Distributed Computing Systems, ICDCS*, 2017.

[4] S. Zheng *et al.*, "User perceptions of smart home iot privacy," *Human-Computer Interaction*, vol. 2, 2018.

[5] D. Geneiatakis *et al.*, "Security and privacy issues for an IoT based smart home," in *40th Int. Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2017.

[6] Y. Wan *et al.*, "IoTMosaic: Inferring User Activities from IoT Network Traffic in Smart Homes," in *IEEE Conference on Computer Communications (INFOCOM)*, 2022.

[7] B. Copos *et al.*, "Is Anybody Home? Inferring Activity From Smart Home Network Traffic," in *IEEE Security and Privacy Workshops (SPW)*, 2016.

[8] B. Breve *et al.*, "Identifying Security and Privacy Violation Rules in Trigger-Action IoT Platforms With NLP Models," *IEEE Internet of Things Journal*, vol. 10, 2023.

[9] M. Surbatovich *et al.*, "Some Recipes Can Do More Than Spoil Your Appetite: Analyzing the Security and Privacy Risks of IFTTT Recipes," in *26th Int. Conference on World Wide Web (WWW)*, 2017.

[10] A. Alshehri *et al.*, "Exploring the Privacy Concerns of Bystanders in Smart Homes from the Perspectives of Both Owners and Bystanders," *Proceedings on Privacy Enhancing Technologies*, vol. 2022, 2022.

[11] N. M. Barbosa *et al.*, ""What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, 2019.

[12] I. Zavalyshyn *et al.*, "SoK: Privacy-enhancing Smart Home Hubs," *Proceedings on Privacy Enhancing Technologies*, vol. 2022, 2022.

[13] Y. Luo *et al.*, "Context-Rich Privacy Leakage Analysis Through Inferring Apps in Smart Home IoT," *IEEE Internet of Things Journal*, vol. 8, 2021.

[14] I. Sanchez *et al.*, "Privacy leakages in Smart Home wireless technologies," in *Int. Carnahan Conference on Security Technology (ICCST)*, 2014.

[15] J. P. Tuohy, "Philips hue will soon require an account to use its app," 2023. [Online]. Available: https://www.theverge.com/2023/9/28/23892761

[16] M. H. Mazhar and Z. Shafiq, "Characterizing Smart Home IoT Traffic in the Wild," in *IEEE/ACM 5th Int. Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2020.

[17] D. Ahmed *et al.*, "Analyzing the Feasibility and Generalizability of Fingerprinting Internet of Things Devices," *Proceedings on Privacy Enhancing Technologies*, vol. 2022, 2022.

[18] A. M. Mandalari *et al.*, "Blocking Without Breaking: Identification and Mitigation of Non-Essential IoT Traffic," *Proceedings on Privacy Enhancing Technologies*, vol. 2021, 2021.

[19] O. Kayode and A. S. Tosun, "Analysis of IoT Traffic using HTTP Proxy," in *IEEE Int. Conference on Communications (ICC)*, 2019.

[20] J. Hong *et al.*, "Don't Talk Unless I Say So! Securing the Internet of Things with Default-Off Networking," in *IEEE/ACM Third Int. Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018.

[21] N. Apthorpe *et al.*, "Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic," 2017. [Online]. Available: http://arxiv.org/abs/1708.05044

[22] R. Trimananda *et al.*, "Packet-level signatures for smart home devices," *Network and Distributed Systems Security Symposium (NDSS)*, 2020.

[23] M. Anagnostopoulos *et al.*, "Tracing your smart-home devices conversations: A real world iot traffic data-set," *Sensors*, vol. 20, 2020.

[24] D. Y. Huang *et al.*, "Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale," *Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, vol. 4, Jun. 2020.

[25] John Velasco, "Security Camera Scorecard: Which Takes Privacy Seriously?" 2021. [Online]. Available: https://www.digitaltrends.com/home/security-camera-scorecard-feature-comparison/

[26] J. Ren *et al.*, "Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach," in *Internet Measurement Conference (IMC)*, 2019.

[27] A. Girish *et al.*, "In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes," in *Internet Measurement Conference (IMC)*, 2023.

[28] Y. Wan *et al.*, "IoTAthena: Unveiling IoT Device Activities From Network Traffic," *IEEE Transactions on Wireless Communications*, vol. 21, 2022.

[29] P. R. J. Pêgo and L. Nunes, "Automatic discovery and classifications of IoT devices," in *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, 2017.

[30] A. Hsu *et al.*, "Automatic IoT Device Classification using Traffic Behavioral Characteristics," in *SoutheastCon*, 2019.

[31] B. D. Davis *et al.*, "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," *IEEE Internet of Things Journal*, vol. 7, 2020.

[32] M. Fagan *et al.*, "Security Review of Consumer Home Internet of Things (IoT) Products," National Institute of Standards and Technology, Tech. Rep. NIST Internal or Interagency Report (NISTIR) 8267 (Draft), 2019.

[33] D. Kumar *et al.*, "All Things Considered: An Analysis of {IoT} Devices on Home Networks," in *28th USENIX Conference on Security Symposium (SEC)*, 2019.

[34] E. Ahmed *et al.*, "Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges," *IEEE Wireless Communications*, vol. 23, 2016.

[35] L. Andraschko *et al.*, "Towards a Taxonomy of Smart Home Technology: A Preliminary Understanding," in *International Conference on Information Systems (ICIS)*, 2021.

[36] M. Schiefer, "Smart Home Definition and Security Threats," in *9th Int. Conference on IT Security Incident Management & IT Forensics (IMF)*, 2015.

[37] Amazon.com, Inc., "Get Started with Device Templates — Alexa Skills Kit," 2023. [Online]. Available: https://developer.amazon.com/en-US/docs/alexa/smarthome/get-started-with-device-templates.html

[38] SmartThings, "Production Capabilities," 2023. [Online]. Available: https://developer.smartthings.com/docs/devices/capabilities/capabilities-reference

[39] G. Zunic, "Smarthome Database," 2018. [Online]. Available: https://www.smarthome-database.eu/en

[40] Statista Research Department, "Smart Appliances - United States," 2024. [Online]. Available: https://www.statista.com/outlook/cmo/smart-home/smart-appliances/united-states

[41] Zigbee Alliance, "ZigBee Specification," 2017.

[42] R. Brown, "Welcome to the OpenWrt Project," 2016. [Online]. Available: https://openwrt.org/start

[43] A. Vakali and G. Pallis, "Content delivery networks: Status and trends," *IEEE Internet Computing*, vol. 7, 2003.

[44] Tuya Smart, "Tuya Smart," Tuya Smart, 2024. [Online]. Available: https://www.tuya.com/

[45] Wireshark Foundation, "Wireshark," Wireshark Foundation, 2024.

[46] Arkime, "Arkime," Arkime, 2023. [Online]. Available: http://arkime.com

[47] J. Lee and P. Seeling, "An overview of mobile device network traffic and network interface usage patterns," in *IEEE Int. Conference on Electro-Information Technology (EIT)*, 2013.

[48] S. Blake-Wilson *et al.*, "Transport Layer Security (TLS) Extensions," IETF, Request for Comments RFC3546, 2003.

[49] L. Daigle, "WHOIS Protocol Specification," Internet Engineering Task Force, Request for Comments RFC 3912, 2004.

[50] T. Mendez *et al.*, "Host Anycasting Service," Internet Engineering Task Force, Request for Comments RFC 1546, 1993.

[51] O. Darwich *et al.*, "Replication: Towards a Publicly Available Internet Scale IP Geolocation Dataset," in *Internet Measurement Conference (IMC)*, 2023.

[52] M. A. Rehman *et al.*, "Passport: Enabling Accurate Country-Level Router Geolocation using Inaccurate Sources," in *arXiv*, vol. abs/1905.04651, no. arXiv:1905.04651, 2019.

[53] Ryan (Amazon Staff), "Pairing Echoes," 2023. [Online]. Available: https://www.amazonforum.com/s/question/0D56Q0000BwWIPeSQO/pairing-echoes

[54] W. Huiyu and Q. Wenxiang, "Breaking Smart Speakers: We are Listening to You," in *DEFCON*, 2018, Conference Talk.

[55] MQTT.org, "MQTT Specification," 2022.

[56] J. Iyengar and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport," Internet Engineering Task Force, Request for Comments RFC 9000, 2021.

[57] daniel_hall, "Developing with LIFX," 2015. [Online]. Available: https://community.lifx.com/t/discovering-lifx-bulbs/265

[58] A. Cooper *et al.*, "Privacy Considerations for Internet Protocols," Internet Engineering Task Force, Request for Comments RFC 6973, 2013.

[59] M. Ghaznavi *et al.*, "Content Delivery Network Security: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, 2021.

[60] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," 2016.

[61] D. Smith, "Microphonegate: The world's biggest tech companies were caught sending sensitive audio from customers to human contractors." 2019. [Online]. Available: https://www.businessinsider.com/amazon-apple-google-microsoft-assistants-sent-audio-contractors-2019-8