A Study for IoT Device Fingerprinting using Zero-Shot Learning

Abstract

The Internet of Things technology facilitates a wide range of applications and services for a better quality of life. This can be witnessed across emerging household appliances, medical devices, smart assistants, smart vehicles, and almost every cyber-physical system. However, the heterogeneity of IoT in terms of device types and vendors poses unknown challenges for an efficient device or network management, QoS-aware provisioning, end-to-end security and privacy assurance. Thus, automated and accurate IoT device fingerprinting becomes a requisite step to deal with unknown challenges.

Keywords:

1. Introduction

In recent years, the Internet of Things (IoT) technology has been embraced by many cyber-physical systems (CPS) to minimize human errors and to improve our day-to-day lives that results in the astronomical growth of interconnected devices. According to a report by Statista [1], there will be twenty-nine billion IoT devices worldwide by 2030 constituting diversified CPS like smart homes, smart buildings, smart cities, and smart industries. Unlike traditional CPS, which involves general-purpose computers and electro-mechanical machines with limited network connectivity, IoT technologies rely on the nexus of highly dedicated interconnected devices designed for environment sensing, data processing, and information-extracting activities. Consequently, the heterogeneous IoT devices and their diversity can augment many new challenges related to IoT device management, location tracking, anomaly detection, faulty device identification, security rules enforcement, authentication, and cyber-attack detection [2]. Thus, IoT device fingerprinting can be a promising strategy to mitigate these challenges.

Studies have shown that fingerprinting can be typically divided into device and device-type fingerprinting [3]. *Device fingerprinting* can be specified as the determination of features or traits unique for a particular device instance and *device-type fingerprinting* can be specified as the determination of features or traits common for the type or class of all the instances of a given device. However, properties, such as *universality*, *uniqueness*, *permanence*, *collectability*, *performance*, *acceptability*, and *circumvention* that play a vital role in the choice of a biometric trait for a particular application can also be useful for the selection of features or traits for device fingerprinting [4]. Table 1 explains the importance of these seven properties concerning feature selection for device fingerprinting.

Table 1: A description of properties essential for feature selection process

Properties	**Description**
Universality	Is a specific feature present in the devices?
Uniqueness	How efficiently the features can be useful to differentiate one device from another?
Permanence	Are the features sufficiently invariant (concerning the matching criterion) over a period of time?
Collectability	How can the features be collected from a device without requiring any special permission or adding computation load?
Performance	How accurate and robust are the features for device fingerprinting.
Acceptability	How can it be ensured that the acquired features do not include sensitive data or adhere to the privacy policies?
Circumvention	How can be the tempering of the features avoided or prevented during the acquisition process?

1.1. Contributions

Our study can facilitate an insight into device fingerprinting taking the complex and heterogeneous nature of IoT devices into account.

1.2. Paper Structure

2. Background

2.1. IoT Device Fingerprinting

Device fingerprinting can be described as a technique for gathering device information to generate a robust, verifiable and unique device-specific signatures that can be exploited for the device's identification or classification [5]. Table 2 summarizes some of the physical layer (PHY) features, medium access control (MAC) layer features, and upper layer features that can be useful for a device fingerprint. However, it is recommended that the features selected for a device fingerprinting must be agnostic to environmental changes and node mobility as well as resilient against forgery or spoofing.

Table 2: Layer-wise features [5]

Layer	**Feature/Signature**	**Remarks**
PHY Layer	Radio signal strength (RSS)	Location-Dependent
PHY Layer	Channel state information at the receiver (CSIR)	Location-Dependent
PHY Layer	Turn-on transient portion of signals (phase angle and frequency using Discrete Wavelet Transform (DWT))	Location-Independent
PHY Layer	Power amplifier imperfections (I/O characteristic)	Location-Independent
PHY Layer	I/Q origin offset, magnitude and phase errors	Location-Independent
PHY Layer	Clock offset, Carrier frequency difference (CFD) and phase shift difference (PSD)	Location-Independent

Layer	Feature/Signature	Remarks
MAC Layer	Transmission rate, frame size, medium access time, medium access time (e.g., backoff mechanism), transmission time, and frame inter-arrival time	802.11 devices
MAC Layer	Inter-burst latency, bin frequency of arrival time between probe request frames	Active scanning
MAC Layer	Duration field values in 802.11 data and management frames	Passive method
MAC Layer	Responses of wireless interfaces to non-standard events	Active probe
Network and Upper Layer	TCP or UDP packet inter-arrival time (ITA) from Access Points (AP)	AP types distinction
Network and Upper Layer	Version and configuration of applications installed on the devices or services	Useful for homogeneous composition
Network and Upper Layer	IP addresses, MAC addresses, electronic serial number (ESN), international mobile station equipment identity (IMEI) number, or mobile identification number (MIN)	Explicit identifiers

2.2. Zero-Shot Learning

Zero-shot learning (ZSL) is a type of cross-modal retrieval learning that aims at the recognition of new classes using unlabeled data [6]. The basic concept exploited for the ZSL is to transfer knowledge from seen classes to unseen classes by sharing attributes akin to how humans quickly recognize new or unknown objects using their accrued knowledge and past experiences. The object of ZSL is to eliminate the constraint of labeled data on artificial intelligence systems. ZSL can be divided into transductive type, i.e., during the training phase unlabeled data are also available, and inductive type, i.e., during the training phase only the training sets are available. Eventually, knowledge about the attributes is captured in the training stage and this collected knowledge is used to categorize instances among a new set of classes in the inference stage [7].

3. Literature Review

3.1. Device Fingerprinting

Choudary et al. [2] described that both implicit identifiers, i.e., network traffic and radio signal features, and explicit identifiers, i.e., internet protocol/media access control addresses, can be used for device fingerprinting. However, implicit identifiers can be more reliable, robust, and secure for device fingerprinting than explicit identifiers. As explicit or user-defined identifiers can be easily manipulated using malicious software, such as MAC address changer and IP spoofing resulting in attacks like spoofing, DoS, and MAC address randomization. Open source tools, such as *macchanger* for IEEE 802.11 and *zbassocflood* for IEEE 802.15.4 are readily available for MAC address spoofing [8].

Commonly, physical device fingerprinting techniques can be classified as active and passive based on the data collection process [9]. *Active device fingerprinting* involves a signal injection or message probing to elicit responses from devices for obtaining useful features. Whereas, *passive device fingerprinting* characterizes a target device by observing its only inbound and outbound communication traffic traces. However, passive fingerprinting techniques in contrast to active fingerprinting techniques can be completely undetectable to the fingerprinted device. Sanchez et al. [10] mentioned that existing device fingerprinting techniques can also be grouped into rule-based, statistical, knowledge-based, Machine Learning and Deep Learning, and time series approaches according to the underlying principle.

Sun et al. [11] investigated telemetry information about IoT device communications at the network edge that can be useful to extract a wide range of data features for characterizing the network flows generated by both IoT and conventional non-IoT devices. The feature set combines traditional flow features, device-specific behavioral features, and TLS-related features by analyzing the unencrypted TLS handshake data. The authors classified these feature sets into aggregate and intraflow features. Aggregate features include flow statistics and device activities spanning multiple flows. Whereas, Intraflow features include flow metadata (from packet header), time-series features (e.g., packet lengths and inter-arrival times), and TLS-related features (for SSL/TLS encrypted traffic).

Radhakrishnan et al. [12] proposed a method that can be operated actively or passively to fingerprint wireless devices and their types based on information that are leaked as a result of heterogeneity in devices. The author described devices' heterogeneity as a function of different device hardware compositions, e.g., processor, DMA controller, memory and variations in devices' clock skew. The method relies on statistical techniques to capture time-variant behavior of network traffic irrespective of protocol (e.g., TCP, UDP, and ICMP) used and create unique, reproducible device and device type signatures.

Wu et al. [13] investigated implicit identifiers deriving the features of physical layer, application layer, and user layer in Android system that can be acquired without a user permission for fingerprinting. The authors utilized the concept of surprisal and entropy in information theory for evaluating the goodness of features. Jose et al. [14] integrated device fingerprinting into Smart Home for improving home automation security. The author utilized JavaScript exploiting *navigator.userAgent*, *navigator.javascript Enabled*, *navigator.flashEnabled*, *navigator.mime Types* and *navigator.plugins* to obtain browser specific parameters and *navigator.userAgent* to obtain OS name, OS Bits, Browser Name and Version. Table 3 presents the categories and features exploited for IoT device fingerprinting.

Table 3: IoT device fingerprinting

Category	**Features**	**Reference**
Telemetry Data	Flow statistics and device activities spanning multiple flows, flow metadata (from packet header), time-series features (e.g., packet lengths and inter-arrival times), and TLS-related features (for SSL/TLS encrypted traffic).	[11]
Network Traffic	Time-variant behavior of network traffic.	[12]
Implicit identifiers spanning physical-, application-, and user layers	Device model and brand, equipment manufacturer, screen information, internal and external storage capacity, kernal information, os version, user agent string in HTTP, structure of system storage and root directory, timezone, hour and date format, automatic time synchronization, automatic selection of timezone, screen locking time, notification of wifi availability, wifi sleep policy, location information, local pattern, system language, font-size, type face, user and system packages, ringtone, alarm alert, notifications, sound effects, screen brightness mode, screen rotation, wallpaper in use, CPU info/core/clock.	[13, 15]
Applications specific	Browser name and version, Javascript/Flash/Cookie/local storage enabled, Mime length and type, Suffix and plugin for each mime type, Plugin name, length, and version, OS name and bits, screen maximum height and width, screen current height and width, screen color and pixel depth, taskbar size and position, time zone, country name, current time, geographical location (latitude and longitude)	[14]
Hardware specific	Sum, mean and median of timestamp values, largest and smallest increment between two consecutive timestamp values, timestamp overflow occurred, smallest, largest, and last timestamp in a scan period	[16]

3.2. Zero-Shot Learning

Hu et al. [17] proposed ZSL framework based on attribute semantic space for encrypted traffic classification. The framework consists of a feature-attribute embedding (FAE) model to learn the mapping between flow features and attributes from seen classes and a Generative Adversarial Networks (GAN) based feature generation model (FAE-G) that leverages the trained FAE model to improve the generalization of the classifier for unseen classes.

Table 4: Zero-shot learning

Category	Features	Reference

https://www.sciencedirect.com/science/article/abs/pii/S003132032200749X

4. Methodology

Draw a reference architecture HU [17]
Attack Model

4.1. Identifying Relevant Features

4.2. Extracting and Modeling Features

4.3. Device Identification

5. WHY ZSL

Most classification methods are supervised learning requiring large amount of labeled samples, while data labeling is a tough task for network traffic analysis [17].

6. Conclusions

Device fingerprinting aims to generate a distinctive traits or features that uniquely identifies individual computing devices.

7. Unused

–Thus, the device fingerprint guarantees to be unique for a particular device instance, whereas the device-type fingerprint can be common for all the instances of that device.

The first category of fingerprinting is host or physical device fingerprinting.

Another body of work that is relevant to our work is device type fingerprinting. The main objective of the techniques in this category is to be able to remotely identify a specific device type.

References

[1] Statista, "Number of internet of things (iot) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030," https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, *(Accessed on 10-01-2023)*, online web resource.

[2] R. R. Chowdhury and P. E. Abas, "A survey on device fingerprinting approach for resource-constraint iot devices: Comparative study and research challenges," *Internet of Things*, p. 100632, 2022.

[3] B. Bezawada, I. Ray, and I. Ray, "Behavioral fingerprinting of internet-of-things devices," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 11, no. 1, p. e1337, 2021.

[4] S. Gupta, "Next-generation user authentication schemes for iot applications," Ph.D. dissertation, Ph.D. dissertation, University of Trento, Italy, 2020.

[5] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 94–104, 2015.

[6] X. Sun, J. Gu, and H. Sun, "Research progress of zero-shot learning," *Applied Intelligence*, vol. 51, no. 6, pp. 3600–3614, 2021.

[7] B. Romera-Paredes and P. Torr, "An embarrassingly simple approach to zero-shot learning," in *Proceedings of the International conference on machine learning*. PMLR, 2015, pp. 2152–2161.

[8] B. W. Ramsey, B. E. Mullins, M. A. Temple, and M. R. Grimaila, "Wireless intrusion detection and device fingerprinting through preamble manipulation," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 585–596, 2014.

[9] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 2, pp. 93–108, 2005.

[10] P. M. S. Sánchez, J. M. J. Valero, A. H. Celdrán, G. Bovet, M. G. Pérez, and G. M. Pérez, "A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1048–1077, 2021.

[11] J. Sun, K. Sun, and C. Shenefiel, "Automated iot device fingerprinting through encrypted stream classification," in *Proceedings of the International Conference on Security and Privacy in Communication Systems*. Springer, 2019, pp. 147–167.

[12] S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah, "Gtid: A technique for physical device and device type fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 519–532, 2014.

[13] W. Wu, J. Wu, Y. Wang, Z. Ling, and M. Yang, "Efficient fingerprinting-based android device identification with zero-permission identifiers," *IEEE Access*, vol. 4, pp. 8073–8083, 2016.

[14] A. C. Jose, R. Malekian, and N. Ye, "Improving home automation security; integrating device fingerprinting into smart home," *IEEE Access*, vol. 4, pp. 5776–5787, 2016.

[15] Z. Ding, W. Zhou, and Z. Zhou, "Configuration-based fingerprinting of mobile device using incremental clustering," *IEEE Access*, vol. 6, pp. 72 402–72 414, 2018.

[16] P. Oser, F. Kargl, and S. Lüders, "Identifying devices of the internet of things using machine learning on clock characteristics," in *Proceedings of the International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 2018, pp. 417–427.

[17] Y. Hu, G. Cheng, W. Chen, and B. Jiang, "Attribute-based zero-shot learning for encrypted traffic classification," *IEEE Transactions on Network and Service Management*, 2022.