2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC) | 978-1-6654-3161-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/CCNC49033.2022.9700731

An End-to-End System for Monitoring IoT Devices in Smart Homes

Keith Erkert, Andrew Lamontagne, Jereming Chen, John Cummings, Mitchell Hoikka, Kuai Xu, and Feng Wang

School of Mathematical and Natural Sciences
New College of Interdisciplinary Arts and Sciences
Arizona State University

***Abstract*—The technology advance and convergence of cyber physical systems, smart sensors, short-range wireless communications, cloud computing, and smartphone apps have driven the proliferation of Internet of things (IoT) devices in smart homes and smart industry. In light of the high heterogeneity of IoT system, the prevalence of system vulnerabilities in IoT devices and applications, and the broad attack surface across the entire IoT protocol stack, a fundamental and urgent research problem of IoT security is how to effectively collect, analyze, extract, model, and visualize the massive network traffic of IoT devices for understanding what is happening to IoT devices. Towards this end, this paper develops and demonstrates an end-to-end system with three key components, i.e., the IoT network traffic monitoring system via programmable home routers, the backend IoT traffic behavior analysis system in the cloud, and the frontend IoT visualization system via smartphone apps, for monitoring, analyzing and virtualizing network traffic behavior of heterogeneous IoT devices in smart homes. The main contributions of this demonstration paper is to present a novel system with an end-to-end process of collecting, analyzing and visualizing IoT network traffic in smart homes.**

I. Introduction

The last two decades have witnessed the rapid adoption and deployment of IoT devices such as smart lights, smart locks, IP cameras, smart motion sensors, and smart thermostats in homes, cities, and factories for a broad range of innovative services and applications [1]. However, the recent spate of cyberattacks exploiting system vulnerabilities and insufficient security management of IoT devices have created challenges for securing IoT devices, data, and services [2], [3], [4].

In light of the high heterogeneity of IoT devices, the prevalence of system vulnerabilities in IoT devices, and the broad attack surface across the entire IoT protocol stack, a fundamental and urgent research problem of IoT security and monitoring is how to effectively collect, analyze, extract, model, and visualize the massive network traffic of IoT devices for understanding the activities, behaviors, and statuses of heterogeneous IoT devices [5]. Towards this end, this paper develops and demonstrates an end-to-end system for monitoring, analyzing and virtualizing network traffic behavior of heterogeneous IoT devices in smart homes.

II. IoT Monitoring and Visualization Systems

Figure 1 illustrates an overall system of our developed end-to-end system for monitoring and visualizing network traffic behaviors of IoT devices in smart homes. The system includes three key components: i) the IoT network traffic monitoring system via programmable home routers, ii) the backend IoT traffic behavior analysis system - Prometheus, and iii) the frontend IoT visualization system via smartphone apps - Epimetheus. The system continuously monitors, collects, and characterizes network traffic behavior of heterogeneous IoT devices in smart homes, and provides companion smartphone apps to visualize traffic summaries and behavioral patterns of these IoT devices.

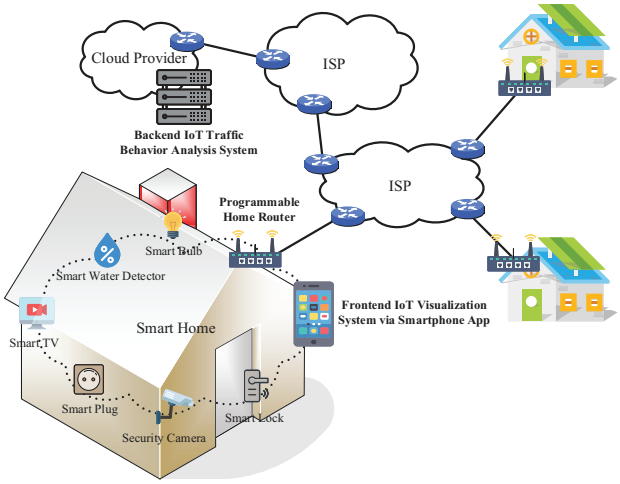


Fig. 1: The system architecture of the developed end-to-end system for monitoring and visualizing traffic behaviors of IoT devices in smart homes.

A. IoT Network Traffic Monitoring via Programmable Routers

In this project, we explore programmable home routers to capture and collect IoT network traffic in smart homes. Specifically, we use the small and affordable computers, i.e., Raspberry Pi, as the routers and wireless access points of the smart homes. Thanks to Debian-based operating system, i.e., Raspberry Pi OS, we install and configure *softflowd* and *nfdump* tools to continuously capture network traffic of all IoT device in smart homes, and export network flow records

every 5 minutes or any other configurable export frequency to Prometheus, our backend IoT traffic behavior analysis system.

B. Backend IoT Traffic Behavior Analysis System

The backend IoT traffic behavior analysis system, namely Prometheus, runs on the cloud, so the smartphone apps could connect the system anytime and anywhere to retrieve network traffic statistics and summaries over the Internet. Prometheus builds a user authentication and authorization module for creating user accounts and passwords, associating Raspberry Pis with user accounts for protecting user privacy, and supporting the standard OAuth 2.0 authorization protocol.

Based on the raw network traffic data from Raspberry Pi, Prometheus analyzes the traffic on the fly to generate the top applications and remote Internet systems for each IoT device in smart homes, as well as to send the traffic summaries and statistics with timestamps into a MySQL database on the backend system using encrypted connections.

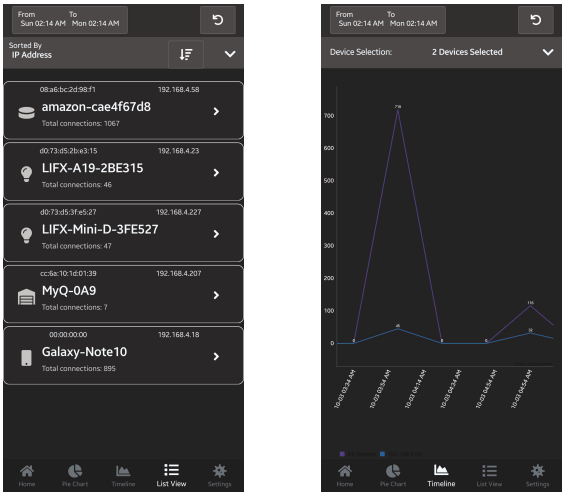
In addition to the traffic volume analysis and the top applications and remote Internet systems, Prometheus also uses *entropy* to calculate the probability distributions on traffic features from IoT network traffic [6]. The *entropy* measure quantifies the probability distributions of a given variable, reflecting the underlying randomness or certainty in the observations. For example, given the m unique values of the variable x, i.e., $x_1, x_2, \ldots, x_m$, we can calculate the entropy as $H(x) = -\sum_{i=1}^{m} p(x_i) log_2 p(x_i)$, where $p(x_i)$ denotes the probability of the value x_i observed in the data-set. If there is one and only one value in the observations, $H(x)$ becomes the minimum entropy, i.e., 0. On the other hand, if each observed value has the equal probability of $1/m$, $H(x)$ becomes the maximum entropy, i.e., $log_2 m$. To compare the entropy values for different IoT devices, we use the standardized or normalized entropy $H_s(x) = H(x)/log_2 m$. The value of $H_s(x)$ follows in the range of [0, 1], where $H_s(x)$ of 1 indicates the random distribution of the variable and $H_s(x)$ of 0 indicates the deterministic distribution. In other words, the standardized entropy measures provide critical insights on traffic behavioral features of smart home IoT devices.

C. Frontend IoT Visualization System via Smartphone App

The smartphone app we developed for visualization IoT network traffic patterns, namely Epimetheus, provides *authorized* and *authenticated* home users a simple interface on iOS or Android phones to view a variety of traffic summaries and statistics including the active list of IoT devices in smart homes, the application breakdown for each IoT device, and the time series traffic graphs for each IoT device. Figures 2(a)b) show two smartphone app screenshots illustrating the list of active IoT devices in the smart home and sample time series traffic graphs for two selected IoT devices.

III. Demonstrations

IoT Network Traffic Capture via Raspberry Pi: We will demonstrate the feasibility of Raspberry Pi to capture network traffic flows in smart home network with heterogeneous IoT devices. To illustrate Raspberry Pi's capability in network traffic capture and collection, we will show how to run *softflowd* and *nfdump* on Raspberry Pi OS to capture IoT network network and extract the records of network flows in smart homes.



(a) List of active IoT devices (b) Time series traffic graph

Fig. 2: Two screenshots from the Epimetheus iOS app.

IoT Network Traffic Analysis: We will show how Prometheus, the backend IoT monitoring system, explores and analyzes IoT network traffic flows collected on Raspberry Pi and generates important traffic characteristics of each IoT device in the smart home. For each IoT device, the traffic characteristics will include the top applications and the top Internet hosts baed on the traffic volume exchange between the device and the remote Internet systems, as well as include the traffic distributions with entropy measures on the applications and the Internet hosts.

IoT Traffic Behavioral Virtualization: We will also demonstrate Epimetheus, the frontend IoT visualization app on both iOS and Android smartphones. The Epimetheus smartphone app will support a variety of features such as user login, IoT device summary, probability distribution charts, and time series traffic graphs.

References

[1] R. Want, B. Schilit, and S. Jenson, "Enabling the Internet of Things," *Computer*, vol. 48, no. 1, pp. 28 – 35, February 2015.

[2] D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta, and Z. Durumeric, "All Things Considered: An Analysis of IoT Devices on Home Networks," in *Proc. of USENIX Security*, 2019.

[3] L. Yu, B. Luo, J. Ma, Z. Zhou, and Q. Liu, "You Are What You Broadcast: Identification of Mobile and IoT Devices from (Public) WiFi," in *Proc. of USENIX Security*, August 2020.

[4] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security Evaluation of Home-Based IoT Deployments," in *Proc. of IEEE Symposium on Security and Privacy (S&P)*, May 2019.

[5] Y. Wan, K. Xu, F. Wang, and G. Xue, "Characterizing and Mining Traffic Patterns of IoT Devices in Edge Networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, January 2021.

[6] K. Xu, Z.-L. Zhang, and S. Bhattacharyya, "Internet traffic behavior profiling for network security monitoring," *IEEE/ACM Transactions on Networking*, vol. 16, pp. 1241–1252, December 2008.