Poster: IoT Location Impact on Network Behavior and MUD

Anat Bremler-Barr
Reichman University, Israel

Bar Meyuhas
Reichman University, Israel

Ran Shister
Reichman University, Israel

ACM Reference Format:
Anat Bremler-Barr, Bar Meyuhas, and Ran Shister. 2021. Poster: IoT Location Impact on Network Behavior and MUD. In *Internet Measurement Conference (IMC '21), November 2–4, 2021, Virtual Event*. ACM, New York, NY, USA, 2 pages. https://doi.org/TBA

1 INTRODUCTION

The field of IoT is very diverse; it has many vendors but no leading paradigm of how devices should be designed and secured. This work examines the influence of a device's location on its network behavior. We found that *the same IoT device with the same firmware behaves differently and communicates with different domains, protocols, and ports, depending on its location.* To the extent of our knowledge, this is the first work that defines device location as a factor impacting device behavior. The only related work we are aware of focuses on the impact of privacy regulations such as GPDR and FTC on the network behavior of IoT devices; this work [5] covered only the United Kingdom and the United States. In comparison, our work investigates the impact of location in many different countries and shows that there are additional factors that influence the differences, including cloud regions, country encryption policies, and so on.

Our dataset contains measurements for devices in our lab that were virtually connected to different locations using VPN, along with information from [5] capturing devices that were physically positioned in different locations. We leveraged the varied locations to examine their impact on network behavior.

We discuss the impact of these observations on the IoT white-list security, such as the Manufacturer Usage Description (MUD). MUD is an IETF standard [2] that enables us to formalize the legitimate network behavior of IoT devices in a file. In this way, a network firewall can verify that the device is not compromised. The MUD file is fetched by the IoT using DHCP or LLDP, and there is commonly a single MUD file for each firmware version. Nevertheless, our work shows that in many cases, the same device with the same firmware demonstrates different network behavior in different locations. This observation has a significant effect on the MUD learning process. The MUD can be learned based on information captured from device network traffic. To be comprehensive, the capture should consist of all potential network behaviors. NIST defined a list of environmental variables that can influence the network behavior of an IoT device [4] (i.e., internet connection, DNS blocking, human interaction) but they did not address device location as a factor. We argue that location is another important environmental variable.

We suggest a **similarity measure** between two MUD files, and show that this measure is higher when we compare the MUD files captured from the same device at different locations, provided these two locations are closer to each other geographically and culturally. As part of our future work, we are studying generalization techniques that will be able to learn a comprehensive MUD file from just a few captures in different locations. These techniques will automatically expand the MUD file rules so the resulting MUD provide accurate information for all available locations.

2 MEASUREMENT

Our dataset consists of network traffic data (pcap files) captured from the router in our lab, and log files from Jingjing et al. [5]. Our captures comprise 31 IoT devices (plugs, cameras, bulbs) that are located in up to 14 countries and use all of their device functionalities. In our lab, we connected the IoT devices by VPN to simulate different locations. However, we found that the network behavior in most cases is not based on the IP of the device (as seen in the VPN) but rather on the country chosen in the device registration process. We generated MUD files from the pcap using MUDGEE [1]. The resulting MUD files (per country) are available at [3].

For simplicity, we formalize MUD, which is basically an Access Control List (ACL), as a set of Access Control Entries (ACEs)[2]. The ACE is defined as 5-tuple: ACE = (legitimate endpoint,protocol,source port, destination port, direction). The legitimate endpoint is the endpoint with which the IoT connects; this endpoint is commonly defined by domain name, sometimes by IP or MAC (the later for intra-LAN scenarios). The corresponding action of the ACE is typically

IMC '21, November 2–4, 2021, Virtual Event

ACM ISBN TBA…$TBA
https://doi.org/TBA

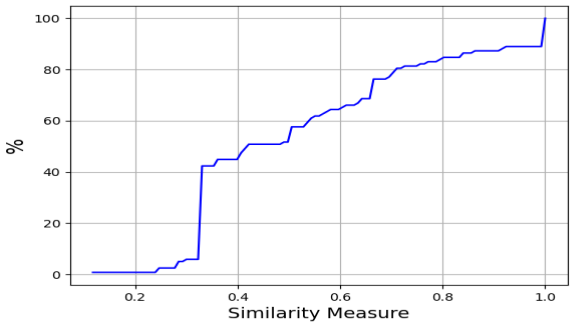

Figure 1: CDF of MUD similarity measure values.

to either "accept" or "drop". Since the MUD file specifies a white-list, the default rule is to drop traffic that does not correspond to any ACE. To compare and find the similarities between two MUDs, we define **MUD similarity** as the Jaccard similarity coefficient of the two MUDs, and divide the number of equal ACEs in two MUDs by the total number of ACEs in both MUDs. Let MUD_i^d be the MUD of device d at location i. The **similarity measure** of MUDs for the same device d, at location i and location j is defined formally as:

$$Similarity_d(MUD_i^d, MUD_j^d) = \frac{|MUD_i^d \cap MUD_j^d|}{|MUD_i^d \cup MUD_j^d|} \quad (1)$$

In Figure 1 we show the cumulative distribution function (CDF) of MUD similarity values of 31 devices, comparing their resulted MUD in different locations (up to 14 countries). It is clear that device location has a significant impact on the MUD, since 80% of the MUD comparisons show similarity measure lowers than ~ 0.7 .

In Figure 2 we show the MUD similarity of the Xiaomi light bulb (Mi Smart LED Bulb Warm White) as measured between countries. We ordered the countries according to region to highlight that places further away from each other (cross-regions) have lower MUD similarity values. Looking at the data, we observe that many of the differences are due to domains, which correlate to regions. For example, the device uses the domain *ru.ot.io.mi.com* in Russia and *de.ot.io.mi.com* in the UK. We speculate that this correlates to each region's location of cloud services, which are commonly used in the IoT field. We encountered another interesting example of the effect of device location when we compared the MUD similarities of the Xiaomi camera (IMILAB Home Security Basic) in China and Israel. Table 1 summarizes the results showing that the location also affects the protocols and ports. In China, the camera uses a plaintext protocol (HTTP), while in Israel, it uses an encrypted protocol (HTTPS).

3 CONCLUSION AND FUTURE WORK

We demonstrated that device location has an impact on the network behavior of IoT devices and their corresponding

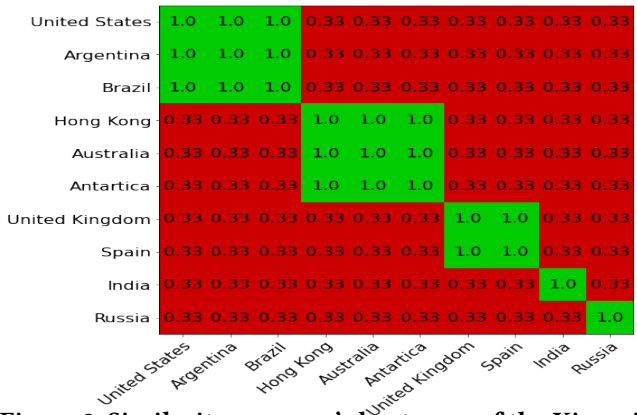

Figure 2: Similarity measure's heat-map of the Xiaomi light bulb and in ten different countries. The countries are ordered according to geographical regions. The heat-map highlights that places further away from each other (cross-regions) have lower MUD in the common case.

	China	Israel
Domain Names	Fixed IP	sg.ots.io.mi.com
Port	HTTP (80)	HTTPS (443)
IP Resolution	HTTP Request	DNS
Encryption	Self-signature	Standard TLS

Table 1: Comparison of Xiaomi Camera network behavior (domains, ports and protocols)

MUD values. In our ongoing work, we designed and built a tool to easily compare MUD files and generalize them if possible. These generalization techniques will automatically expand the MUD file rules so the resulting MUD provide accurate information for all available locations. For example, the Xiaomi light bulb in our evaluation above uses *ru.ot.io.mi.com* in Russia and *de.ot.io.mi.com* in UK, and we were able to generalize the ACE to $*.ot.io.mi.com$.

Acknowledgement: This research was supported in part by a Cisco grant.

REFERENCES

[1] Ayyoob Hamza, Dinesha Ranathunga, Habibi Gharakheili, Matthew Roughan, and Vijay Sivaraman. 2018. Clear as MUD: Generating, validating and applying IoT behavioral profiles. In *Workshop on IoT Security and Privacy*. Association for Computing, USA, 8–14.

[2] Eliot Lear, Ralph Droms, and Dan Romascanu. 2019. Manufacturer Usage Description Specification. RFC 8520. (March 2019). https://doi.org/10.17487/RFC8520

[3] Bremler Meyuhas, Shister. 2021. MUD files dataset in different locations. (2021). https://github.com/barmey/IoT_mud_files_locations

[4] NIST. 2020. Methodology for Characterizing Network Behavior of Internet of Things Devices. (Apr 2020). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04012020-draft.pdf

[5] Jingjing Ren, Daniel J Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. 2019. Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. In *IMC Conference*. ACM, New York, NY, USA, 267–279.