Designing and Evaluating a Testbed for the Matter Protocol: Insights into User Experience

Ravindra Mangar*[1], Jingyu Qian†[1], Wondimu Zegeye‡,
Abdulrahman AlRabah†, Ben Civjan†, Shalni Sundram†, Sam Yuan†,
Carl A. Gunter†, Mounib Khanafer§, Kevin Kornegay‡, Timothy J. Pierson*, David Kotz*
*{ravi.gr, timothy.j.pierson, david.f.kotz}@dartmouth.edu, Dartmouth College, Hanover, NH
†{jingyuq2, alrabah2, bcivjan2, shalnis2, jintaoy3, cgunter}@illinois.edu, University of Illinois, Urbana-Champaign, IL
‡{wozeg1, kevin.kornegay}@morgan.edu, Morgan State University, Baltimore, MD
§mkhanafer@auk.edu.kw, American University of Kuwait

***Abstract*—As the integration of smart devices into our daily environment accelerates, the vision of a fully integrated smart home is becoming more achievable through standards such as the Matter protocol. In response, this research paper explores the use of Matter in addressing the heterogeneity and interoperability problems of smart homes. We built a testbed and introduce a network utility device, designed to sniff network traffic and provide a wireless access point within IoT networks. This paper also presents the experience of students using the testbed in an academic scenario.**

Keywords—Matter Protocol, Smart Home, IoT, Access Control.

I. Introduction

The rise in popularity of smart home technologies has led to an expanding landscape consisting of diverse devices, manufacturers, and protocols, which pose challenges in achieving interoperability and homogeneity in the consumer IoT environment. These complexities led the community to develop the Matter protocol, an emerging standard designed to address interoperability within this domain [6]. The Matter protocol, developed by the Connectivity Standards Alliance (formerly the Zigbee Alliance), represents a unifying leap in smart homes and has contributors from Apple, Amazon, and Google, among others. As Matter is set to position itself as the cornerstone in the consumer IoT landscape, there is a need to comprehensively evaluate and understand the capabilities and shortcomings of the protocol. This paper introduces our initiative to develop a testbed specifically tailored to investigate the nuances of the Matter protocol.

Prior research has highlighted the importance of developing a testbed to assess the security vulnerabilities associated with wireless protocols [20], [24]. While other literature discusses the characteristics and functionality of Matter [11], [25], very few create a tangible testbed to evaluate the protocol. Zegeye et al. introduced a testbed comprising several development kits [31]. Their testbed, however, lacks a variety of Matter devices and does not closely replicate a consumer setting. In light of this, our contributions are:

1) **Construction of a Comprehensive Matter Testbed:** We built a testbed specifically designed to evaluate the Matter protocol in a smart home environment. This testbed is unique in its ability to capture traffic through all stages of an IoT device's life cycle, including the commissioning phase. Given the recency of Matter, there is little published research on its practical applications. Our testbed offers an extensible platform that uses open-source tools, add-ons, and APIs.
2) **Educational Implementation and Real-World Application:** To demonstrate the usability of our testbed, we describe its application in an educational setting. The testbed served as a research platform for graduate students undertaking a course project focused on security and privacy in IoT devices.

The rest of the paper is organized as follows. Section II provides a comprehensive overview of the setup and tools used for the testbed. In Section III we discuss the user experience for students who used the testbed. We conclude with a discussion on future directions.

II. Testbed Setup

This section details the specific components, configurations, and methods used in our setup. We sought to create a realistic smart home environment that integrates the Matter protocol but also supports extensive data collection and can be adapted for various research applications. Section II-A outlines the hardware components of our testbed and discusses the rationale for choosing such devices. Section II-B introduces a device known as The Hub – a conceptual home device functioning primarily as a traffic-capturing network router within our testbed. Designed to be the central hub for IoT networks, the Hub has the flexibility to accommodate additional hardware and software routines. Our testbed is designed to collect comprehensive network data, encompassing Thread [18], [27], Wi-Fi, and Bluetooth Low Energy (BLE) [12] networks. Section II-C discusses the tools and methods used for data collection.

[1]These authors contributed equally to this work.

Workshop on Security and Privacy in Standardized IoT (SDIoTSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-6-9
https://dx.doi.org/10.14722/sdiotsec.2024.23012
www.ndss-symposium.org

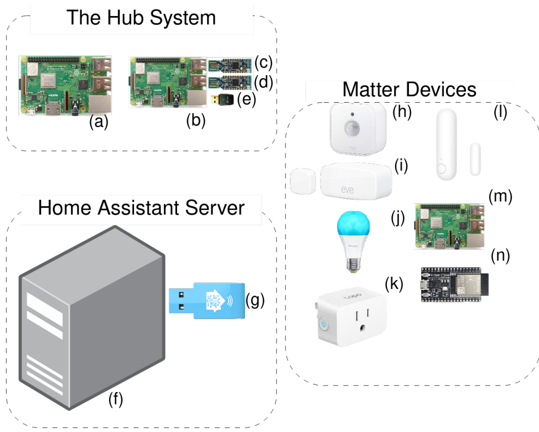

Fig. 1. Components of the testbed. Details on individual components can be found in Table II. Image Credits: [10], [13]–[15], [17], [21]–[23], [28]

A. Hardware Components

To replicate a household IoT network, we used five off-the-shelf Matter-certified devices; they operate via Matter over Wi-Fi as well as Matter over Thread. In our testbed, the central smart home hub is a desktop computer equipped with Home Assistant supervised [2], installed on Debian Bookworm serving as the host operating system [Figure 1(f)]. Home Assistant is an open-source home automation platform that supports multiple smart devices from various manufacturers and allows users to control devices from a single interface. Additionally, this Home Assistant server functions as the Matter Controller, using specific add-ons designed for Home Assistant platforms to enable this capability. For network infrastructure, we use a Raspberry Pi [Figure 1(a)] running HostAPD [19], which allows it to serve as the main access point for our setup. The default maximum number of clients in this setup is thirty-two.

Since Matter devices can operate over both Wi-Fi and Thread, an OpenThread Border Router (OTBR) is needed. For this, we use a Home Assistant SkyConnect dongle [4] [Figure 1(g)], which uses a Silicon Labs Multi-protocol EFR32MG21 chipset. The SkyConnect dongle creates a Thread network to which Thread-enabled Matter devices can join. For capturing wireless traffic, we use a TP-Link Archer AC600 T2U [Figure 1(e)] for Wi-Fi traffic and two Nordic Semiconductor nRF52840 USB dongle [Figure 1(c)(d)]. One dongle is used to capture Thread traffic, while the second captures BLE traffic. Most Matter devices use BLE during the commissioning phase. Consequently, the testbed is equipped to capture traffic throughout the entire life cycle of the device, starting from the commissioning phase.

B. The Hub

A Raspberry Pi serves as the only Wi-Fi access point for the network. This Raspberry Pi lays the basis for a device we dub The Hub. In its current setup The Hub serves primarily as an access point with the ability to capture traffic, while the Home Assistant server operates as the Matter controller. We envision The Hub to provide both researchers and smart home residents with a unified interface for monitoring and controlling smart devices. In addition to housing the hardware and software required to broadcast a Wi-Fi SSID and capture network traffic, The Hub also houses the routines for collecting and parsing the data as well as the databases used to store such data. Furthermore, The Hub system supports a Google Remote Procedure Call (gRPC) API [1]. This feature allows users to query the data collected from the traffic capture. Through such queries, researchers can obtain a comprehensive inventory of observed devices, track IP/MAC addresses devices communicate with, and gain other insights into network interactions. By offering these capabilities, the Hub serves as a versatile platform that can function as a research tool as well as a consumer device for enhancing smart home networks.

To augment the capabilities of The Hub, we introduce additional satellite components [Figure 1(b)], that complement the main Hub unit and are distributed around the home. Each satellite unit contains the necessary hardware and software to capture Wi-Fi, Thread, and BLE network traffic and to relay this data to The Hub. This modular approach allows us to extend the coverage and effectiveness of our traffic analysis, enabling the system to monitor a larger area than a single device alone can provide.

C. Data Collection

To support the collection of Wi-Fi traffic, we add an external Wi-Fi dongle to the Hub, running in monitor mode. Once the necessary drivers are installed and the dongle is in monitor mode, we use the libpcap API [26] to capture and decode Wi-Fi packets. Once decoded and parsed, the data is systematically stored in a database. Our testbed is continuously set to capture and store traffic. To extend the capture to Thread and BLE, we leverage Wireshark [30] and TShark [29] to capture and parse the data. We integrated Wireshark add-ons (from Nordic Semiconductors) enabling it to process Thread and BLE data [7], [8]. Additionally, to effectively capture Thread and BLE traffic, we flash the respective dongles with specialized firmware [7], [8] that enables them to detect and capture this specific traffic. Similar to placing the Wi-Fi in monitor mode, we set the Thread adapter responsible for traffic capture to the channel on which the Thread network is operating on. To enable the continuous capturing of data, we use TShark, which is a command-line utility that can use Wireshark add-ons. This approach allows us to create scripts that facilitate the ongoing and automated collection of network data.

In addition to these methods, we leverage the logging capabilities of the Python Matter Server add-on within Home Assistant. This add-on enhances our data collection framework by enabling queries to Matter nodes, which provide insight such as access control lists, information on subscribed nodes, and other endpoint data from Matter devices.

III. User Experience

In this section, we introduce a student course project that utilized our Matter testbed. The student group includes four graduate students in the Computer Science major who accessed the testbed remotely. The total time for students to finish the project is around two months. We use their project to demonstrate how novice researchers with little background knowledge of the Matter protocol can conduct Matter-related research with the testbed. We discuss challenges during the students' experience and the potential of our testbed.

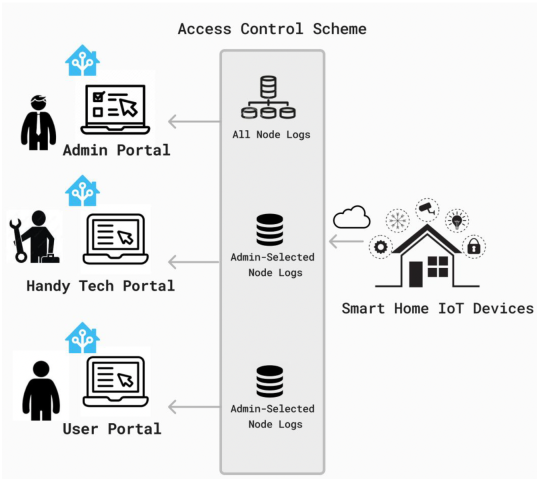

Fig. 2. Role-based access control on Matter device attributes. The student project supports three roles: "Admin", "Handy Tech", and "User".

A. Student Project Preparation

The students were introduced to the Matter protocol through a presentation on basic information, including its goal, typical network topology, data model basics, and some examples of Matter endpoints and clusters. The presentation materials were based on the articles by Espressif [5]. We then introduced them to our Matter testbed, including the desktop computer as the Secure Shell (i.e., SSH) server and the Matter controller, the sniffing hardware for Wi-Fi, Thread, and Bluetooth, the Home Assistant SkyConnect [4] as the OpenThread border router, and the full list of Matter devices in the testbed. We also briefly introduced Home Assistant [2] to the students, which can be utilized for potential projects related to user-friendly management of IoT devices.

The students were provided with some high-level project ideas listed as follows.

- Building role-based access control on device metadata or logs.
- Studying how to reason about access to Matter devices and how to delegate access easily.
- Exploring how to trigger Matter device debug test cases and studying how Acess Control List(ACL) should be updated throughout the process.

The students were also encouraged to think of other project ideas. In the end, the students elected to build a prototype for role-based access control on Matter device logs, focusing specifically on Matter device cluster attributes (i.e., device attributes). To access the testbed host, the students were given temporary accounts to remotely access the devices in the testbed and the Matter controller.

B. Design and Implementation

The student project aims to build a prototype that enforces role-based access control over device attributes (Figure 2). The prototype supports three roles (i.e., Admin, Handy Tech, and User). "Admin" plays the main role as the administrator of all the devices in the Matter network. They need to perform access control by granting or revoking access to device attributes on a Matter cluster of a specific Matter node for the other two roles. "Handy Tech" (same as HandyTech in [9]) is a tech support role that provides services, such as fixing malfunctioning devices or regularly inspecting the devices for vulnerabilities. "User" role is considered as the daily users of the IoT devices in their environment. However, their management and control over certain devices may be restricted by the administrator. For example, the property landlord may disallow the resident to inspect or tamper with the smart water leak detector, on which the landlord relies to monitor the property states. However, the resident may be given full control of the smart light bulb in their bedrooms and allowed to inspect its status (e.g., on/off state).

TABLE I. CLUSTER ACCESS DEPENDING ON THE ROLE.

	Admin	Handy Tech	User
Access control cluster	✔		
Node operational credentials cluster	✔		
Administrator commissioning cluster	✔		
Diagnostic clusters		✔	
Basic information cluster	✔	✔	✔
Other utility clusters	✔	✔	
Application clusters	✔	✔	✔

The prototype supports two levels of granularity for access control (i.e., node-based and cluster-based). Each role can be granted access to a whole node, which includes all the device clusters and, in turn, all the device attributes on that node. On the other hand, each role can also be granted access to specific clusters on a specific Matter node. By design, "admin" can see the most information for each node, while "user" and "handy tech" can see clusters on selected nodes depending on the visibility setting created by "admin." The detailed clusters one can access based on the role are listed in Table I.

The implementation of the prototype relies on Home Assistant [2]. The students implemented a Home Assistant add-on with the front end to sign up for different roles in the access control scheme. By default, "user" and "handy tech" can not access device attributes on any node. The administrator manages access of other roles through this add-on by granting selected nodes' access to different users. The administrator can revoke access at any time. If access to a node is granted, one can use the add-on to query the device attributes on that node depending on the allowed clusters in Table I through the Python Matter server of Home Assistant [3]. The snapshot of Matter device attributes can be regularly captured in the background and logged in a MongoDB database, structured hierarchically by node, endpoint, cluster, and attribute to reduce query time further.

C. Challenges and Potential from Student Experience

To evaluate the user experience of our testbed and understand how to improve it, we asked the students to provide any impediments during their project. We recorded every incident and carefully examined the cause. When the students presented their course project, they also included a section to highlight the issues they had encountered.

Overall, the students' experience of conducting the project with our testbed was smooth, and their project was well-suited as a course project, where they clearly revealed what they had learned about Matter and how they succeeded in conducting related research. They found our testbed easy to set up and use. The official Matter protocol documents [6] gave them a quick start toward their project design and implementation. Though they cannot physically access the testbed, the remote VPN works fine throughout their experience, with only a few impediments that required someone with physical access to the testbed to help or fix. Here, we list the challenges encountered during the experience.

- The students needed to build features into the docker image for the home assistant add-on. Compiling the docker image took a long time, which slowed the process of validating the design. This issue had not been raised during the students' project, but was revealed through the students' final project presentation. This is not an issue with the university VPN or the desktop machine in the testbed. We conjecture that the removal of unused dependencies can improve the build time.
- The Home Assistant add-on container requires the configuration of the shared port on the host desktop machine, which requires updating firewall rules for the network. This was easily solved as we had colleagues who could physically access the testbed and configure the host desktop machine.
- We needed to restart the Home Assistant once as it became unresponsive. One student pointed our this remote access issue when attempting to test their Home Assistant add-on. We found that the reason was that its updates were not applied promptly. If the Home Assistant core version is not up to date, the Home Assistant supervisor does not run in a privilege mode.
- System stability was affected by update issues in other ways. Our installation of Home Assistant has two components: the Home Assistant core and the Matter add-on for Home Assistant. Sometimes, an update is released for one component, which renders the other component non-functional, so we have to make sure different components have compatible versions. Matter is a relatively new protocol and is still evolving, and we expect these issues to abate in the future, though extra care is required at the current stage of developing such testbeds.

Due to the time limit and scope of the course project, the students did not take advantage of all the features in our testbed, such as traffic sniffing, node-level log analysis, and virtual device development [16]. The students also provided their insights of some potential research directions in their presentation, including monitoring other device data besides device attributes and more fine-grained access control on the endpoint or cluster level. We expect that our Matter testbed can promote more Matter-related research. As an open-source and unified connectivity protocol, Matter allows the construction of similar testbeds as ours to be scalable in the face of more Matter devices by different manufacturers, creating an easy channel for future researchers to study the Matter protocol directly without understanding all the current diverse connectivity protocols used in the IoT ecosystem.

IV. Future Directions

The future direction of this research involves the expansion of the testbed by incorporating additional smart home devices to create a more realistic environment. We also plan to enhance the capabilities of the Hub by having it serve as the main hub in the home and act as the Matter controller. These enhancements will streamline the testbed's architecture and reduce its physical footprint - achieving a more efficient network infrastructure with fewer devices.

Furthermore, the study intends to implement sophisticated log analysis techniques to scrutinize the captured traffic, focusing on enhancing cyber security and privacy measures within the smart home ecosystem. In addition to these security aspects, we also plan to delve into investigating usability challenges associated with the Matter protocol, particularly in the realms of device commissioning and discovery. This exploration will aim to address key questions such as how users can efficiently commission new Matter devices into their home and how they can become aware of the presence and functionality of pre-existing devices. We also intend to explore the usage of large language models in building smart and usable access control frameworks.

V. Conclusion

In this paper, we have presented a comprehensive testbed tailored for the exploration and analysis of the Matter protocol. Our testbed stands out due to its ability to capture and analyze traffic throughout the complete lifecycle of IoT devices, all while effectively simulating the environment of a typical smart home network. Through the development of The Hub, we have established a device which can serve as the central controller for a consumer smart home. The modular design of The Hub, augmented with the satellite units, enables extensive coverage and effective analysis of network traffic. Our work also incorporates the real world practical application of the testbed by discussing its successful utilization in a graduate student project.

In conclusion our testbed serves as a extensible platform for future research and provides a means of understanding and improving the Matter protocol. Since the setup utilizes readily available software and hardware components, we hope it could be used by other researchers.

VI. Acknowledgements

This research is supported by the National Science Foundation under award numbers CNS-1955805, CNS-1955228, CNS-1955231, the VeChain Foundation, and the Dartmouth College and American University of Kuwait (Dartmouth-AUK) fellowship program. The views and conclusions contained herein are those of the authors alone.

References

[1] Google Remote Procedure Call - gRPC. [Online]. Available: https://grpc.io

[2] Home Assistant. [Online]. Available: https://www.home-assistant.io

[3] Home Assistant Python Matter Server. [Online]. Available: https://github.com/home-assistant-libs/python-matter-server

[4] Home Assistant SkyConnect. [Online]. Available: https://www.home-assistant.io/skyconnect/

[5] Matter Articles by Expressif. [Online]. Available: https://blog.espressif.com/matter-38ccf1d60bcd

[6] Matter Specifications. [Online]. Available: https://csa-iot.org/developer-resource/specifications-download-request/

[7] nRF Sniffer for Bluetooth LE. [Online]. Available: https://www.nordicsemi.com/Products/Development-tools/nrf-sniffer-for-bluetooth-le/

[8] Thread Sniffer based on nRF52840 with Wireshark. [Online]. Available: http://tinyurl.com/596pnz6c

[9] D. Anthony, C. A. Gunter, W. He, M. Khanafer, S. Landau, R. Mangar, and N. Reitinger, "The handytech's coming between 1 and 4: Privacy opportunities and challenges for the iot handyperson," in *Proceedings of the 22nd Workshop on Privacy in the Electronic Society*, 2023, pp. 129–134.

[10] Aqara. Door and window sensor. [Online]. Available: https://www.aqara.com/us/product/door-and-window-sensor/

[11] D. Belli, P. Barsocchi, and F. Palumbo, "Connectivity standards alliance matter: State of the art and opportunities," *Internet of Things*, p. 101005, 2023.

[12] Bluetooth Special Interest Group, *Bluetooth Core Specification: Low Energy Technology*, Bluetooth SIG Document, Bluetooth Special Interest Group, 2020. [Online]. Available: https://www.bluetooth.com/specifications/bluetooth-core-specification/

[13] Espressif. Esp32. [Online]. Available: https://www.espressif.com/en/products/socs/esp32

[14] Eve. Door and window contact sensor. [Online]. Available: https://www.evehome.com/en-us/eve-door-window

[15] ——. Motion detector. [Online]. Available: https://www.evehome.com/en-us/eve-motion

[16] Google. Build a matter virtual device. [Online]. Available: https://developers.home.google.com/codelabs/matter-device-virtual#1

[17] Home Assistant. Sky connect. [Online]. Available: https://www.home-assistant.io/skyconnect/

[18] Institute of Electrical and Electronics Engineers, "Ieee standard for low-rate wireless networks," Institute of Electrical and Electronics Engineers, IEEE Std 802.15.4-2020, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9144691

[19] Jouni Malinen, "hostapd: Host access point daemon," Software package, 2023. [Online]. Available: https://w1.fi/hostapd/

[20] V. Kampourakis, V. Gkioulos, and S. Katsikas, "A systematic literature review on wireless security testbeds in the cyber-physical realm," *Computers & Security*, p. 103383, 2023.

[21] Lucasbosch. Raspberry pi b+ top. [Online]. Available: https://en.m.wikipedia.org/wiki/File:Raspberry_Pi_B%2B_top.jpg

[22] Nanoleaf. A19 smart bulb. [Online]. Available: https://nanoleaf.me/en-US/products/essentials/bulbs/?category=A19-E26&standard=matter&size=each

[23] Nordic Semiconductor. nrf52840. [Online]. Available: https://www.nordicsemi.com/Products/Development-hardware/nrf52840-dongle

[24] S. Rizvi, R. Pipetti, N. McIntyre, J. Todd, and I. Williams, "Threat model for securing internet of things (iot) network at device-level," *Internet of Things*, vol. 11, p. 100240, 2020.

[25] S. Singh, "Intercompatibility of iot devices using matter: Next-generation iot connectivity protocol," in *International Conference on Advances in IoT and Security with AI*. Springer, 2023, pp. 49–58.

[26] The Tcpdump Group, "libpcap: An independent packet capture library," Software library, 2023. [Online]. Available: https://www.tcpdump.org/

[27] Thread Group, "Thread wireless networking protocol." [Online]. Available: https://www.threadgroup.org/What-is-Thread

[28] TP Link. Archer t2u. [Online]. Available: https://www.tp-link.com/us/home-networking/usb-adapter/archer-t2u/

[29] Wireshark Foundation, "Tshark: Terminal network protocol analyzer," Software package, 2023. [Online]. Available: https://www.wireshark.org/docs/man-pages/tshark.html

[30] ——, "Wireshark: A network protocol analyzer," Software package, 2023. [Online]. Available: https://www.wireshark.org/

[31] W. Zegeye, A. Jemal, and K. Kornegay, "Connected smart home over matter protocol," in *2023 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2023, pp. 1–7.

APPENDIX

TABLE II. TESTBED COMPONENTS.

Device	Component in Figure 1	Note
Raspberry Pi 4 (4GB RAM)	(a)	Main unit.
Raspberry Pi 4 (4GB RAM)	(b)	Satellite unit which houses hardware to capture wireless traffic.
Nordic Semiconductor nRF52840 USB Dongle	(c)	Used to sniff traffic from Thread networks.
Nordic Semiconductor nRF52840 USB Dongle	(d)	Used to sniff traffic from BLE networks.
TP-Link Archer AC600 T2U USB Dongle	(e)	Used to sniff traffic from Wi-Fi networks.
Desktop Computer	(f)	Home Assistant Server and Matter Controller.
Home Assistant SkyConnect USB Dongle	(g)	Used to create thread network and act as OpenThread Border Router.
Eve Smart Motion Sensor with Light Sensor	(h)	Matter device using Thread.
Eve Matter Door and Window Sensor	(i)	Matter device using Thread.
Nanoleaf A19 Smart Bulb	(j)	Matter device using Thread.
TP-Link P125M Smart Plug	(k)	Matter device using Wi-Fi.
Aqara Door and Window Sensor P2	(l)	Matter device using Wi-Fi.
Raspberry Pi 4 (4GB RAM)	(m)	Development device using Wi-Fi.
ESP32-H2	(n)	Development device using Thread.