# PhD school: An Investigation of Matter Smart Home Mechanisms to Mitigate Denial-of-Service (DoS) Attacks

Andrew Losty
andrew.losty.23@ucl.ac.uk
University College London

Anna Maria Mandalari
a.mandalari@ucl.ac.uk
University College London

## Abstract

The rapid expansion in the use of Internet-of-Things (IoT) devices in smart homes has introduced numerous security challenges, primarily due to their diverse architectures, lack of standardized protocols, and differing security implementations. These challenges make IoT devices particularly vulnerable to security and privacy attacks. The introduction of the Matter IoT standard represents a significant shift in the architecture of the smart home ecosystem, prompting important security questions to be raised regarding the adoption of a unified multi-vendor protocol. While adopting a single protocol can reduce the attack surface and enhance scrutiny across devices, it also raises the risk of widespread security breaches if a single vulnerability is exploited. This research identifies a potential threat to home security by demonstrating viable security attacks on Matter smart home devices. Specifically, the research explores how DoS flooding attacks are capable of selectively incapacitating Matter devices, such as security cameras, door locks, and sensors.

## CCS Concepts

• **Networks** → **Network protocol design**; • **Security and privacy** → **Denial-of-service attacks**;

## Keywords

Security, Privacy, Matter, Internet of Things, Denial of Service

## 1 Introduction

The growing adoption of Smart Home IoT devices, their proliferation in critical applications and an increasingly sophisticated security threat model has led to increased concerns regarding the threat from Denial-of-Service attacks [1]. This was highlighted by Chen et all., who observed that "DoS is one of the most catastrophic attacks against IoT devices" [2]. Matter is a new Smart Home IoT specification that aims to build a common highly secure communication framework that can be adopted by a large range of manufacturers[3]. The adoption of a single ubiquitous protocol may however potentially increase risk as any vulnerability may be exhibited by a far larger and more diverse range of devices. Our research focuses on evaluating the security mechanisms of Matter devices, specifically their ability to withstand DoS attacks.

By conducting laboratory experiments and reviewing existing literature, we aim to provide a deeper understanding as to the level of resilience that Matter devices exhibit under such conditions. The research acknowledges that the limited CPU and storage resources of smart appliances may impact their resilience to DoS attacks. Matter devices have a suggested minimum of 1MB of flash memory / 256kB of RAM. [4].

We aim to answer the following three research questions:
**RQ1:** How effective are Matter Smart-Home DoS mitigation techniques when evaluated in a controlled laboratory environment?
**RQ2:** What research or commercial information is available that defines Matter DoS defence mechanisms?
**RQ3:** How can an effective methodology be developed to evaluate Denial-of-Service (DoS) exploits against Matter Thread 802.15.4 connections?

We conduct lab experiments with multiple Matter ecosystems and devices from three vendors. A reconnaissance of Matter devices is performed over IPv4 and IPv6 to identify open ports and services. Wireless Matter devices were then subjected to DoS attacks, showing that 802.11-connected devices are vulnerable and rendered inoperable during attacks. These DoS attacks could potentially exploit compromised consumer routers to target local Matter devices. We establish laboratory experiments with multiple Matter ecosystems, and Matter devices from three vendors.

Furthermore we plan to perform DoS testing on Thread IEEE 802.15.4 devices [5], in order to reveal if additional vulnerabilities are present.

## 2 Background

The goals of the Matter Smart Home protocol are hugely ambitious. Matter is an open-source, unified IPv6 based Smart Home protocol that provides increased levels of connectivity and security [6]. Matter supports local operation without the need for an Internet connection, however cloud connectivity is required for device commissioning.

The Matter protocol aims to provide inter-connectivity of Smart Home IoT, allowing devices to be shared between ecosystems, with the formation of a single ecosystem that supports devices from over 270 manufacturers [7]. Prior to the release of Matter, Smart Home environments were formed from multiple separate isolated proprietary ecosystems each with their own applications, communications framework, and security mechanisms. Matter is an open-source, royalty-free framework that “enables developers and device manufacturers to build reliable, secure ecosystems and increase compatibility” [8].

In December 2019 a working group founded by Amazon, Apple, Google and the Zigbee Alliance, collaborated to develop a new open-source Smart Home IoT environment that supported a range of devices with a single management protocol [9]. The development group was formalised as the ‘Connectivity Standards Alliance’ (CSA) and went on to release the initial specification of Matter 1.0 in October 2022. There have since been three revisions of the Protocol: 1.1, 1.2 and 1.3. A maintained list of supported Matter devices is published online by ‘Matter-SmartHome’ [10].

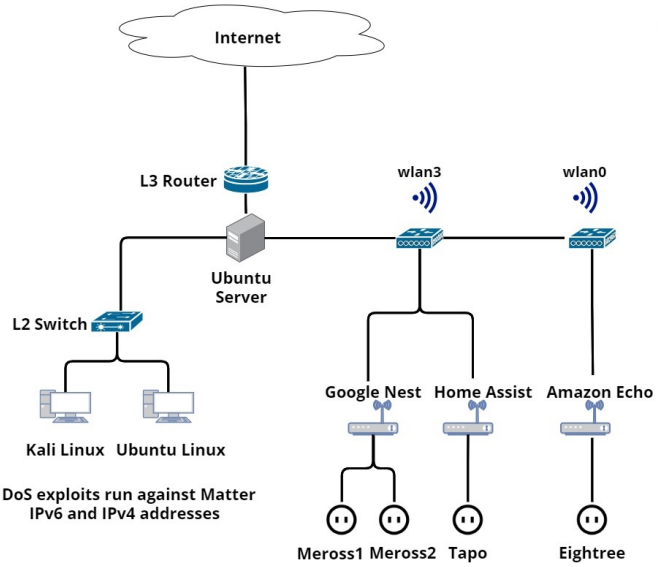


**Figure 1: Matter DoS Test Environment.**

The CSA white paper 'Matter Security and Privacy Fundamentals' is a 9-page document that defines the need to protect Matter devices from Distributed-Denial-of-Service (DDoS) attacks [11].

The paper states that "Several mechanisms have been built in the Matter definition to prevent the most common DoS attacks" and describes a sophisticated message counter mechanism to offer this resilience. It details the use of 32-bit message counters in order to protect Matter communications by providing both Duplicate Message Detection and Replay Prevention. While the CSA outlines a mechanism to prevent DoS outages, it does not however define the methods of attacks.

## 3 Experimentation Environment

We establish a Matter test environment that includes three ecosystems and a range of Matter devices. The chosen ecosystems are Google Nest, Amazon Echo and Home Assist. The devices from three manufacturers Meross, Eightree and Tapo, are all smart plugs and all connect via 802.11 Wireless connections. Having Matter devices with the same functionality allows for a direct comparison of results. We perform DoS testing from an Ubuntu 22.04.4 LTS server, running a Xeon(R) 4114 CPU 2.20GHz and with Wireless AR9462 2.4GHz 300Mbps adapters.

The attacks described in this research focus on DoS exploits where an attack is launched from a specific possibly compromised host to selected Matter devices.

There are a wide range of publicly available tools that are either specifically designed to perform DoS attacks or that can be utilized for this purpose. [12].

Following a network reconnaissance using NMAP(7.8), Nessus Expert(10.7.4) and ZenMAP (7.94) the Matter devices were identified, and their MAC, IPv4/IPv6 addresses determined.

| Device | Type |
|---|---|
| Google Nest Hub (2nd Gen) | Smart Hub |
| Amazon Echo (DOT 5) | Smart Hub |
| Home Assistant | Smart Hub |

**Table 1: Matter Controllers**

| Device | Type |
|---|---|
| Meross Smart Plug (1) (MSS315) | Smart Plug |
| Meross Smart Plug (2) (MSS315) | Smart Plug |
| Eightree Smart Plug (ET36) | Smart Plug |
| Tapo Smart Plug (P110M) | Smart Plug |

**Table 2: Matter Test Devices**

## 4 Denial of Service (DoS) Exploits

Matter control and data communications are limited to IPv6 using UDP port 5540 [13] and TCP/UDP port 5353 for multicast network/neighbour discovery [14]. While not required for core operations, Matter devices obtain an IPv4 address and actively have ports open for both DNS(53), and NTP(123).

We select three utilities to allow custom packets generation and flooding to specific clients. This allows options such as the source MAC address or data payload size to be manipulated. The three utilities are (i) Hping3 (3.0.0) [15], Metasploit (6.3.55) [16] and Scapy (2.5.0) [17].

We perform DoS Syn-flooding using Scapy on the IPv6 address of the target devices, resulting in the Meross and Eightree devices losing connectivity or causing the application to halt communication. While the Tapo device does not fully lose connectivity, it suffers significant intermittent loss and delays operation. We note that a key requirement for executing a successful DoS attack is to craft the packets in such a way that they seem to originate from the correct Matter controller.

We perform a wider range of exploits using IPv4 utilities against the target devices. This includes Syn-Flood [18], UDP-Flood [19], ACK-Flood [20], IP-Fragment [21], and LAND attacks [22]. The DoS Syn-Flood, UDP-Flood, ACK-Flood, IP-Fragment, and LAND attack tests are successful in incapacitating the selected Matter devices within the 10-minute time window. The Tapo device appears more resilient, with only the IP-Fragment attack being successful. DoS attacks targeting the host's capacity to handle large Maximum Transmission Unit (MTU) payloads do not cause disruption. Matter devices limit responses to IPv6 "Ping of Death" exploits, capping packet sizes at 7k or 14k, well below the 65k maximum [23].

## 5 Literature Review

The literature review is constrained by the recent release of the Matter 1.0 specification by the CSA in October 2022. Four databases—Web of Science, Scopus, ProQuest, and IEEE Explore—were selected to identify academic research on mechanisms to mitigate DoS attacks on Matter devices. However, significant gaps in the literature were found, confirming the need for further research, as highlighted in the study's research questions. Several relevant papers were identified. The first, "Connectivity Standards Alliance Matter: State of the Art and Opportunities" [24], provides an overview of the Matter

protocol, noting its early development stage but does not focus on DoS vulnerabilities. The paper "Fuzzing Matter(s)" [25] explores security testing through fuzzing, leveraging similarities between Matter and Zigbee protocols, though it does not address DoS issues. A further identified paper, "Matter: IoT Interoperability for Smart Homes" [26] offers a detailed breakdown of the protocol's operation across OSI layers, focusing on Wi-Fi and Thread communications, but lacks analysis of DoS defences.

The paper "One Standard to Rule Them All" [27] investigates the susceptibility of Matter Thread networks to radio-frequency jamming attacks, and observes that jamming is successful in 91 percent of all cases. A final 2024 paper, "Smart Homes App Vulnerabilities, Threats, and Solutions," analyses vulnerabilities in smart home apps but does not examine Matter's DoS defence mechanisms.

None of the papers reviewed specifically focus on Matter's DoS vulnerabilities or the methods to mitigate these attacks. This underscores the necessity for independent research into the effectiveness of its defence mechanisms, making it a crucial and timely area for future investigation.

## 6 Conclusion

Our research identifies a significant vulnerability in Matter Smart Home devices, highlighting the potential for DoS attacks that compromise security. During controlled testing in a lab environment, devices from Meross [28], Eightree [29], and Tapo [30] were successfully incapacitated using DoS flooding attacks, rendering them inoperable during the attack. The research suggests that security devices such as cameras [31] door locks [32] and security sensors [33] may be targeted in real-world scenarios. A possible attack vector could include the hijacking of consumer internet routers from which targeted DoS attacks are launched.

Further research is proposed to enhance understanding of the identified vulnerabilities by expanding testing to a broader range of Matter devices, including those that connect via Thread (IEEE 802.15.4). This research will reveal whether low power mesh Thread-connected devices, are similarly vulnerable to DoS attacks.

We plan to refine the testing framework to incorporate automated tools to identify Matter devices for more targeted attack mechanisms. This research area is original, with no existing literature found regarding DoS vulnerabilities in Matter devices. This suggests it offers new insights into the security of the Matter protocol.

## References


[1] O. Toutsop, S. Das, and K. Kornegay, "Exploring The Security Issues in Home-Based IoT Devices Through Denial of Service Attacks," in *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, Oct. 2021, pp. 407–415. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9604385

[2] Q. Chen, H. Chen, Y. Cai, Y. Zhang, and X. Huang, "Denial of Service Attack on IoT System," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, Oct. 2018, pp. 755–758, iSSN: 2474-3828. [Online]. Available: https://ieeexplore.ieee.org/document/8589403

[3] "What is Matter?" [Online]. Available: https://developers.home.google.com/matter/overview

[4] "Qorvo's QPG6105DK Matter and Bluetooth Development Kit, Now Available at Mouser, Simplifies IoT Device Development." [Online]. Available: https://www.mouser.co.uk/newsroom/publicrelations-qorvo-qpg6105dk-kit-2024final/?_gl=1*u0xmj0*_gcl_au*MTU5MzQ4NzYwOC4xNzE5ODQwMDky*_ga*MTA3OTQ1MDUyMC4xNzE5ODQwMDk2*_ga_15W4STQT4T*MTcxOTg0MDA5NS4xLjAuMTcxOTg0MDA5Ni41OS4wLjA.

[5] I. Unwala, Z. Taqvi, and J. Lu, "Thread: An IoT Protocol," in *2018 IEEE Green Technologies Conference (GreenTech)*, Apr. 2018, pp. 161–167, iSSN: 2166-5478. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8373620

[6] "The Alliance Specifications Download Request Form," Jan. 2022. [Online]. Available: https://csa-iot.org/developer-resource/specifications-download-request/

[7] "Our Members | Promoters | Participants | Adopters." [Online]. Available: https://csa-iot.org/members/

[8] "Apple, Google, and Amazon have teamed up to fix the smart home with a new standard called Matter - The Verge." [Online]. Available: https://www.theverge.com/22787729/matter-smart-home-standard-apple-amazon-google

[9] "Timeline." [Online]. Available: https://matter-smarthome.de/en/timeline/

[10] "Matter Arrives Bringing A More Interoperable, Simple And Secure Internet Of Things to Life," Oct. 2022. [Online]. Available: https://csa-iot.org/newsroom/matter-arrives/

[11] F. Lau, S. Rubin, M. Smith, and L. Trajkovic, "Distributed denial of service attacks," in *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics. 'cybernetics evolving to systems, humans, organizations, and their complex interactions' (cat. no.0*, vol. 3, Oct. 2000, pp. 2275–2280 vol.3, iSSN: 1062-922X. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/886455

[12] "Top 125+ Network Security Tools in 2020." [Online]. Available: https://ehackacademy.com/blog/top-125-network-security

[13] "Service Name and Transport Protocol Port Number Registry." [Online]. Available: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=554

[14] "Service Name and Transport Protocol Port Number Registry." [Online]. Available: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=92

[15] "hping3 | Kali Linux Tools." [Online]. Available: https://www.kali.org/tools/hping3/

[16] "Metasploit | Penetration Testing Software, Pen Testing Security." [Online]. Available: https://www.metasploit.com/

[17] "Scapy." [Online]. Available: https://scapy.net/

[18] W. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," Internet Engineering Task Force, Request for Comments RFC 4987, Aug. 2007, num Pages: 19. [Online]. Available: https://datatracker.ietf.org/doc/rfc4987

[19] "UDP flood," Jun. 2022. [Online]. Available: https://www.ionos.co.uk/digitalguide/server/security/udp-flood/

[20] "What is an ACK flood DDoS attack? | Types of DDoS attacks." [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-an-ack-flood/

[21] "Standard for the transmission of IP datagrams over IEEE 802 networks," Internet Engineering Task Force, Request for Comments RFC 1042, Feb. 1988, num Pages: 15. [Online]. Available: https://datatracker.ietf.org/doc/rfc1042

[22] "Service Name and Transport Protocol Port Number Registry." [Online]. Available: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=554

[23] K. M. Elleithy, D. Blagovic, W. K. Cheng, and P. Sideleau, "Denial of Service Attack Techniques: Analysis, Implementation and Comparison," vol. 3, no. 1.

[24] "Connectivity Standards Alliance Matter: State of the art and opportunities - ScienceDirect." [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660523003281

[25] M. Maugeri, "Fuzzing Matter(s): A White Paper for Fuzzing the Matter Protocol:," in *Proceedings of the 10th International Conference on Information Systems Security and Privacy*. Rome, Italy: SCITEPRESS - Science and Technology Publications, 2024, pp. 446–451. [Online]. Available: https://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0012469200003648

[26] S. Madadi-Barough, P. Ruiz-Blanco, J. Lin, R. Vidal, and C. Gomez, "Matter: IoT Interoperability for Smart Homes," May 2024, arXiv:2405.01618 [cs]. [Online]. Available: http://arxiv.org/abs/2405.01618

[27] "One Standard to Rule Them All? Assessing the Disruptive Potential of Jamming Attacks on Matter Networks | IEEE Conference Publication | IEEE Xplore." [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10374874

[28] "Meross Matter Smart Wi-Fi Plug with Energy Monitor, MSS315 (UK Version), 2 Pack." [Online]. Available: https://shop.meross.com/products/meross-matter-plug-with-energy-monitor-mss315-uk

[29] "UK Products." [Online]. Available: https://eightreesmart.com/collections/uk

[30] "Tapo P110M | Mini Smart Wi-Fi Plug, Energy Monitoring | Tapo." [Online]. Available: https://www.tapo.com/uk/product/smart-plug/tapo-p110m/

[31] "Matter Alpha - 5 Best Matter-Compatible Security Cameras: Enhance Your Smart Home Security." [Online]. Available: https://www.matteralpha.com/explainer/5-best-matter-compatible-security-cameras

[32] "Top 5 Matter-Enabled Smart Locks of 2024 - SwitchBot – SwitchBot UK." [Online]. Available: https://uk.switch-bot.com/blogs/news/top-5-matter-enabled-smart-locks-of-2024

[33] "Matter Alpha - The Best Matter-Compatible Motion Sensors." [Online]. Available: https://www.matteralpha.com/explainer/best-matter-compatible-motion-sensors