Jul 30th, 11:30 AM - 1:15 PM

On the Vulnerability of OpenThread to Agile Denial of Service Attacks

Casey Cronin
University of Northern Iowa

Sarah Diesburg Ph.D.
University of Northern Iowa

See next page for additional authors

Author

Casey Cronin, Sarah Diesburg Ph.D., and Dheryta Jaisinghani Ph.D.

On the Vulnerability of OpenThread to Agile Denial of Service Attacks

Casey Cronin• Brandon Purvis • Dr. Sarah Diesburg • Dr. Dheryta Jaisinghani

cronicab@uni.edu • purvisb@uni.edu • sarah.diesburg@uni.edu • dheryta.jaisinghani@uni.edu

Abstract

The Internet of Things (IoT) includes physical devices such as sensors, connected home appliances, video monitoring systems, and smart classroom or smart warehouse applications. These devices can capture large amounts of data while using low amount of power to do it, as well as keep track of things going on around it and turn it into usable data for the user depending on what task it is performing.

IoT devices are not immune from security concerns, such as Denial of Service (DoS) attacks. These attacks are important to investigate because they can play a dangerous role in shutting down applications, shutting down entire networks, and can potentially interfere with data in systems that are found in organizations like stores and commerce, banks, government facilities and many other places. Understanding how DoS attacks affect IoT nodes can lead to more robust security in the future.

Background

OpenThread[1], which is an open-source networking technology released by Google, gives access to developers to create and develop products that connect devices together in places like commercial buildings, school classrooms and homes. These devices incorporate end to end encryption and a persistent connection to one another which allows data to be encrypted as it travels through the Thread network until it reaches either an end device or uploaded to a cloud server for transfer to other servers and systems.

OpenThread networks can maintain many devices at a time, and the project is being actively developed. Google uses these OpenThread networks mainly in their line of Nest products (e.g., Nest Thermostat, Nest Cameras, Nest Doorbell). The technology is also seeing development from big companies like Amazon, Apple, Samsung, and many others. Figure 1 shows one of the development boards we used to create our OpenThread research network.

A DoS attack is one type of attack that can be performed on a network. The attack results in the flooding and crashing of system services by sending large amounts of traffic to a target.

OPENTHREAD
released by Google

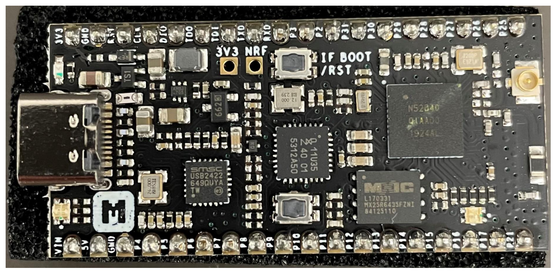


Figure 1: nRF52840 OpenThread Node

Methodology

By using OpenThread development boards[2], we constructed a test network (figure 2) of 5 nodes consisting of 1 *leader node* and 2 *routers* with a 4th node acting as a *sniffer* (figure 3). Finally, we added an *attacker* node which could be dropped into the network by an attacker to cause a possible DoS attack.

Below we explain our experimental setup in more detail.

Leader Node:
- Manages set of routers
- Self-elected when network is created
- Distributes network wide information

Router Node:
- Constantly transmits and receives communications with the leader node
- Forwards packets along the network
- In charge of the secure joining of other devices to the network

Sniffer Node:
- Passively captures network traffic for research purposes
- Does not forward packets to other nodes
- Allows researchers to visualize effects of actions with the network

Attacker Node:
- Has capabilities of the sniffer, but not joined with the network
- Attempts to overwhelm one or more nodes to keep the network from functioning normally

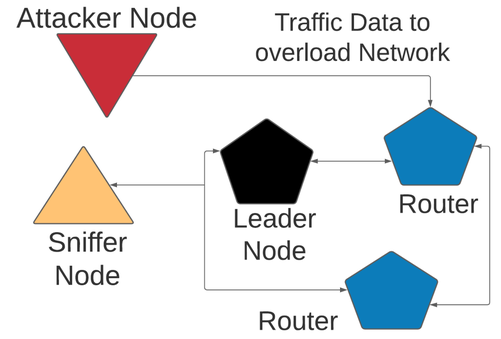
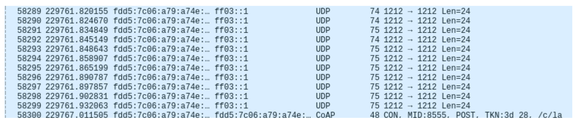


Figure 2: Experimental Setup



```
58289 229761.820155 fdd5:7c06:a79:a74e:… ff03::1          UDP      74 1212 → 1212 Len=24
58290 229761.824670 fdd5:7c06:a79:a74e:… ff03::1          UDP      74 1212 → 1212 Len=24
58291 229761.834849 fdd5:7c06:a79:a74e:… ff03::1          UDP      75 1212 → 1212 Len=24
58292 229761.845149 fdd5:7c06:a79:a74e:… ff03::1          UDP      74 1212 → 1212 Len=24
58293 229761.848643 fdd5:7c06:a79:a74e:… ff03::1          UDP      75 1212 → 1212 Len=24
58294 229761.858907 fdd5:7c06:a79:a74e:… ff03::1          UDP      75 1212 → 1212 Len=24
58295 229761.865199 fdd5:7c06:a79:a74e:… ff03::1          UDP      75 1212 → 1212 Len=24
58296 229761.890787 fdd5:7c06:a79:a74e:… ff03::1          UDP      75 1212 → 1212 Len=24
58297 229761.897857 fdd5:7c06:a79:a74e:… ff03::1          UDP      75 1212 → 1212 Len=24
58298 229761.902831 fdd5:7c06:a79:a74e:… ff03::1          UDP      75 1212 → 1212 Len=24
58299 229761.932063 fdd5:7c06:a79:a74e:… ff03::1          UDP      75 1212 → 1212 Len=24
58300 229767.011505 fdd5:7c06:a79:a74e:… fdd5:7c06:a79:a74e:… CoAP 48 CON. MID:8555. POST. TKN:3d 28. /c/la
```

Figure 3: Sniffer Network Traffic

Future Work

Much of the work this semester was spent getting the research experimental setup working. The next stage of the research is performing various types of DoS attacks using an attacker node. One promising direction of DoS is to broadcast fake network scanning, discovery, and/or joining packets based on the OpenThread protocol. Another type of DoS attack could possibly be performed on the physical layer of the OpenThread network (IEEE 802.15.4) by sending jamming packets to attempt to corrupt the transfer of messages throughout the network[3].

Acknowledgements

We would like to thank Dr. Andrew Berns and Habib Ullah for their help and expertise. We would also like to thank the UNI Student Undergraduate Research Program for the necessary support for this research.

References

[1] OpenThread: https://openthread.io/. Accessed: 2021-07-25.

[2] nRF52840 - Nordic Semiconductor: https://www.nordicsemi.com/Products/nRF52840. Accessed: 2021-07-25.

[3] O'Flynn, C.P. 2011. Message denial and alteration on IEEE 802.15. 4 low-power radio networks. *2011 4th IFIP International Conference on New Technologies, Mobility and Security* (2011), 1–5.