A Quantitative Study of DDoS and E-DDoS Attacks on WiFi Smart Home Devices

Bhagyashri Tushir Yogesh Dalal Behnam Dezfouli Yuhong Liu

Internet of Things Research Lab, Department of Computer Science and Engineering, Santa Clara University, USA

Introduction

- IoT facilitates device connectivity via the Internet using sensory devices for data sensing, monitoring, and analysis
- IoT adoption in smart homes has increased due to WiFi advancements and cost-effectiveness
- However, IoT devices are vulnerable to attacks
- This research focuses on DDoS and E-DDoS attacks that overload IoT device resources with malicious traffic and maximize energy consumption
- Despite prior studies on data centers, the impact of these attacks on smart homes IoT devices still needs to be explored
- The study reveals that E-DDoS attacks on IoT devices for a month can lead to an estimated $253.7 million increase in electricity bills
- And DDoS attacks on IoT devices can disrupt device services by disconnecting them from the AP, affecting the IoT market and public confidence

Contribution

The key contributions of this research are as follows

- Designed a smart home testbed to capture real-time network traffic and measure the power consumption of victim IoT devices
- Quantified the impact of DDoS attacks on victim devices' service disruptions by identifying minimum attack rates and durations
- Identified the vulnerability of the WPA group temporal key updating process, facilitating DDoS attacks that disconnect victim IoT devices from their associated AP
- Identified critical factors (communication protocol, attack rate, payload size, victim devices' port state) and assessed their influence on energy consumption in victim devices

Automated data collection setup

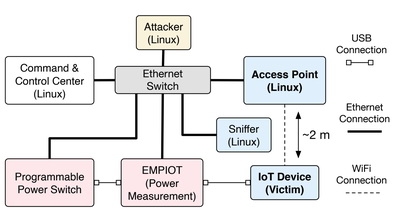

Figure 1. Interconnections of the testbed components to automate attack generation and data collection.

Data processing

Linear regression is utilized to examine the correlation between the attack rate and the energy consumption of the victim IoT device. The formula for this analysis is provided in Equation 1

$$\Delta p = \alpha_0 + \alpha_1 \times v \tag{1}$$

where Δp is an IoT device's energy increase, v is E-DDoS attack rate, and α_1 is the slope of variable v

The values of α_1 and α_0 are calculated by Equation (2) and Equation (3), respectively:

$$\alpha_0 = \frac{(\sum \Delta p)(\sum v^2) - (\sum v)(\sum \Delta p * v)}{n(\sum v^2) - (\sum v)^2} \tag{2}$$

$$\alpha_1 = \frac{n(\sum \Delta p * v) - (\sum v)(\sum \Delta p)}{n(\sum v^2) - (\sum v)^2} \tag{3}$$

where n is the number of samples

Findings on DDoS attacks

- To explore the internal status of victim IoT devices and identify the cause of service interruption, a DevBoard (CYW43907) is employed, revealing buffer overflow as a contributing factor
- DDoS attacks lead to significant buffer overflows, resulting in missed beacon signals from the AP
- Frequent beacon losses decrease the perceived Received Signal Strength Indication (RSSI) value over time
- When the RSSI drops below a certain threshold, the victim device initiates the roaming process and disconnects from the original AP

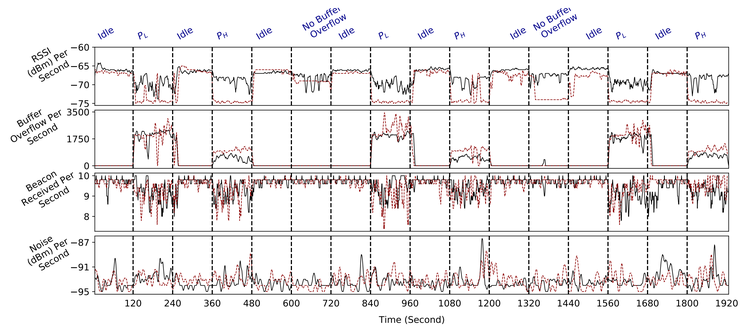

Figure 2. Internal status of victim device (the DevBoard) under TCP-SYN closed port DDoS attack

Findings on E-DDoS attacks

To assess the influence of factors such as communication protocol and port states on energy consumption, victim devices are subjected to attacks for 30 minutes

- 1400 B (P_H) causes higher energy consumption at lower attack rates compared to 0 B (P_L)

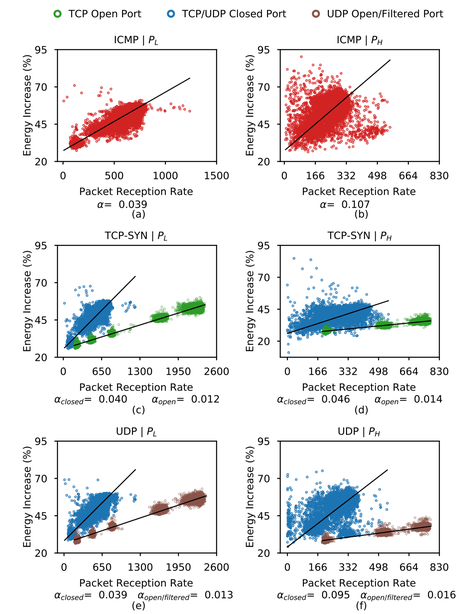

Figure 3. Google Home under E-DDoS attacks shows maximum energy consumption and received attack rate for 1400 B ICMP and 0 B TCP-SYN open port attacks, respectively

Key observations

- Effective DDoS attacks: 0 B payload TCP-SYN/UDP attacks on closed ports or ICMP attacks if the victim responds to ICMP packets
- Effective E-DDoS attacks: 1400 B payload UDP attacks on closed ports or ICMP attacks if the device responds to ICMP packets, maximizing energy consumption without disconnection
- Among voice assistants, Google Home is more susceptible to DDoS attacks, while Alexa is more vulnerable to E-DDoS attacks
- Among video cameras, Nest Cam is more prone to DDoS attacks, while Ring Cam is more vulnerable to E-DDoS attacks