FR-WARD: Source-end Distributed Denial-of-Service Defense from the Internet of Things

Samuel Mergendahl
University of Oregon

Devkishen Sisodia
University of Oregon

Jun Li
University of Oregon

Hasan Cam
Army Research Laboratory

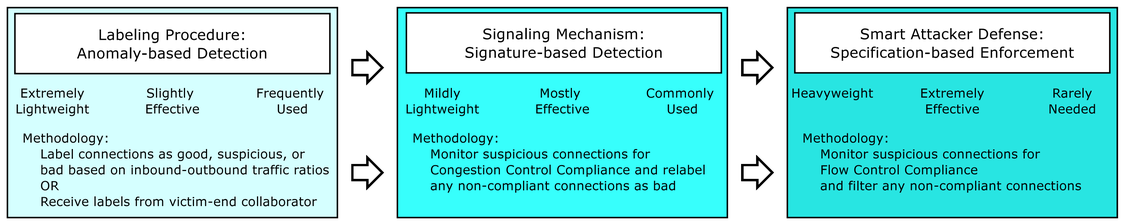
Motivation

- Many Internet of Things (IoT) devices become compromised and launch destructive distributed denial-of-service (DDoS) attacks.
- Previous DDoS defense solutions are unsuitable for deployment in IoT.
- They can mistakenly throttle or filter benign traffic which leads to unnecessary battery loss on IoT devices.

Objectives

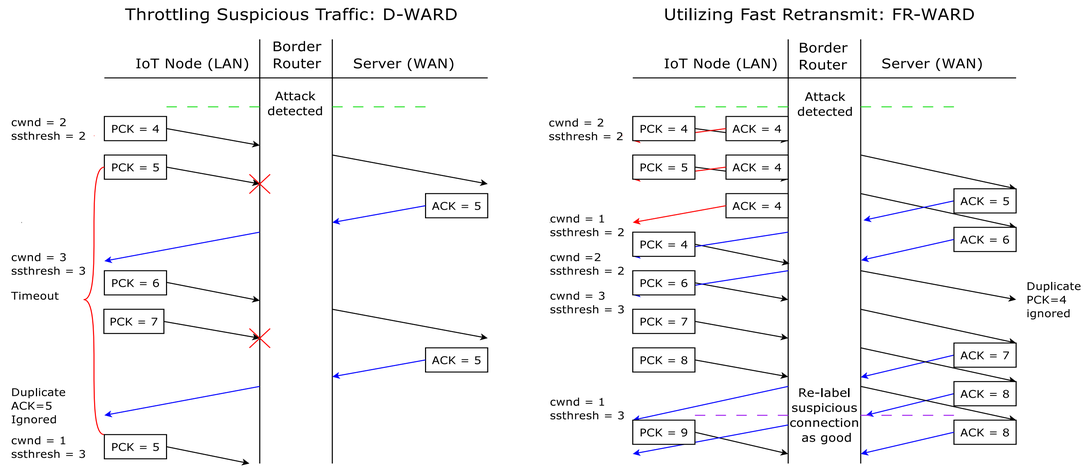
- FR-WARD must mitigate DDoS traffic that attempts to leave the policed network, but also avoid resource penalties on benign devices.
- Benign traffic should transmit at the quickest allowable rate, but malicious traffic must always transmit at a manageable rate.
- FR-WARD cannot rely on installation of new hardware or software on IoT devices.

Basic Design



- FR-WARD identifies and mitigates DDoS attacks in three phases to avoid filtering benign traffic.
- Its novel response to traffic too difficult to categorically label as good or bad saves IoT battery life without sacrificing attack mitigation.

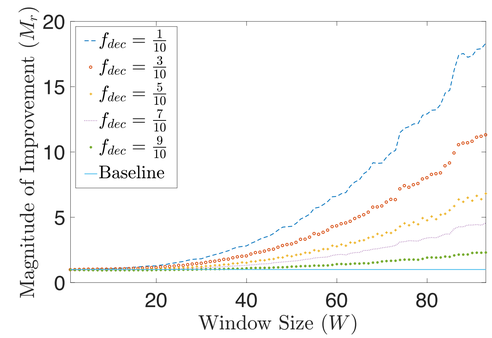
Signaling Mechanism



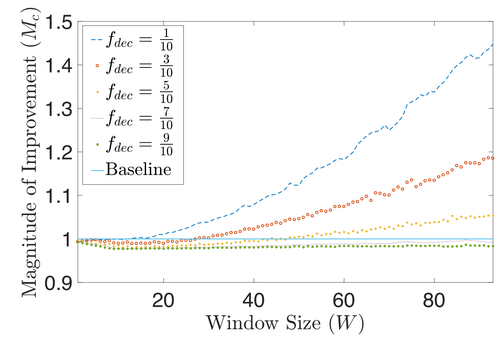
- FR-WARD uses fast retransmit as a signaling mechanism to reduce the transfer rate of suspicious connections and identify congestion control compliance without the negative effects of throttling.

Results

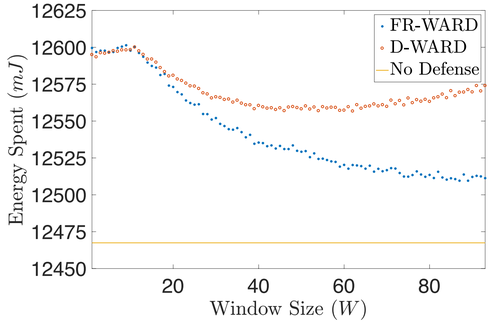
Effects on Benign Traffic



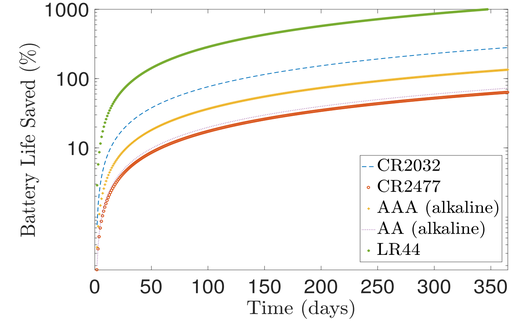
(a) The magnitude that FR-WARD reduces retransmissions.



(b) The magnitude that FR-WARD reduces connection duration.

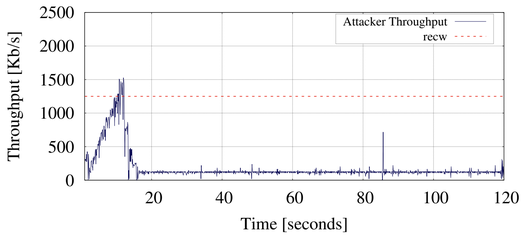


(c) The energy consumption of a benign IoT device.

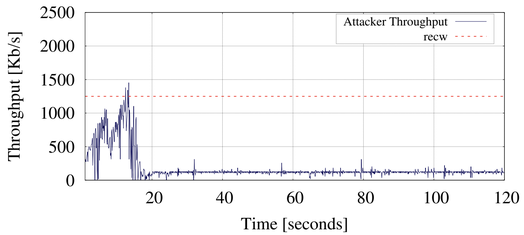


(d) The extent that FR-WARD saves IoT battery life during one year.

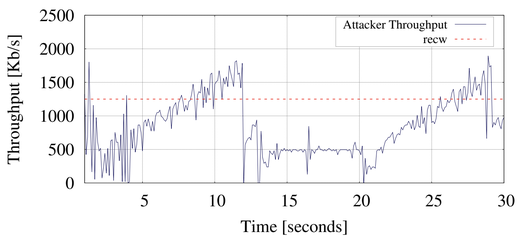
Effects on Malicious Traffic



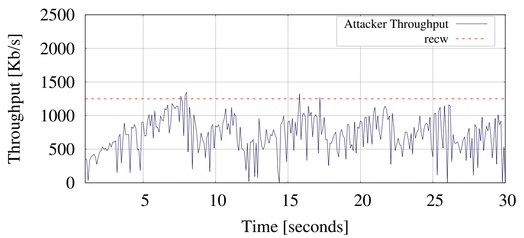
(a) Throughput of a naïve attacker under D-WARD.



(b) Throughput of a naïve attacker under FR-WARD.



(c) Throughput of a smart attacker under D-WARD.



(d) Throughput of a smart attacker under FR-WARD.