FR-WARD: Fast Retransmit as a Wary but Ample Response to Distributed Denial-of-Service Attacks from the Internet of Things

Samuel Mergendahl

Center for Cyber Security and Privacy
University of Oregon
Table of Contents

1. Introduction
   o The Internet of Things
   o Source-end Distributed Denial-of-Service Defense
   o Difficulties of Source-end Defense for the Internet of Things

2. FR-WARD
   o Threat Model & Assumptions
   o Basic Design
   o Labeling Procedure
   o Signaling Mechanism
   o Defending Against Smart Attackers
   o Extending the Signaling Mechanism

3. Evaluation
   o Effects on Benign Traffic
   o Effects on Malicious Traffic
The Internet of Things - Growth

- The Internet of Things (IoT) continues to rapidly expand in size and capability.
The Internet of Things - Botnets

- But many IoT devices often remain unprotected and targets of botnets.
The Internet of Things – DDoS

- IoT botnets can launch large-scale distributed denial-of-service (DDoS) attacks
The Internet of Things (cont.)

- DDoS attacks increased 91% in 2017 thanks to IoT
  - Criminals can now attack and take down a company for less than $100

Image: iStockphoto/daoleduc
Source-end DDoS Defense

• Detects and thwarts attack traffic before the traffic leaves its original network
  o Easier to properly handle DDoS attacks near the attack sources
  o Can play a pivotal role in collaborative DDoS defenses
    • Guarantees impunity when a collaborator is under attack

• Source-end DDoS defenses operate in three main phases:
  1. Attack Detection
    • (eg) receive an attack notification from a collaborator
  2. Traffic Classification
    • (eg) label current connections as good or bad
  3. Attack Response
    • (eg) filter the bad connections and allow safe passage for the good
Source-end DDoS Defense in IoT Networks

• False positives are significantly detrimental in IoT environments
  o False positive = misidentifying a benign connection as malicious
  o Filtering a benign connection results in:
    • Unnecessary retransmission
    • Reduced goodput
    • Excessive energy consumption (loss of precious battery life)

• Must still maintain close to zero false negatives
  o False negative = misidentifying a malicious connection as benign
  o Allowing safe passage of malicious connections fails to mitigate an attack

• Categorically labeling traffic as good or bad becomes extremely difficult
Crux of the Problem

• A source-end DDoS defense will unavoidably encounter traffic it must label with low confidence
  o We call this traffic **suspicious**

• If the defense filters the suspicious traffic:
  o It inevitably filters some good traffic
  o Leads to unwanted negative effects on benign traffic in IoT networks

• If the defense allows safe passage for the suspicious traffic:
  o It inevitably allows safe passage for some bad traffic
  o Fails to comprehensively mitigate an attack

• We need an efficient—but effective—**response** to suspicious traffic
Table of Contents

1. Introduction
   o The Internet of Things
   o Source-end Distributed Denial-of-Service Defense
   o Difficulties of Source-end Defense for the Internet of Things

2. FR-WARD
   o Threat Model & Assumptions
   o Basic Design
   o Labeling Procedure
   o Signaling Mechanism
   o Defending Against Smart Attackers
   o Extending the Signaling Mechanism

3. Evaluation
   o Effects on Benign Traffic
   o Effects on Malicious Traffic
Threat Model & Assumptions

- FR-WARD is placed at the gateway of a generic IoT environment
  - The IoT network maintains wireless connectivity between low power, energy constrained devices
  - The IoT network could be:
    - a smart home
    - a Wireless Sensor Network (WSN)
    - a smart city, etc
FR-WARD has two main goals:
1. Throttle **all** malicious DDoS traffic that attempts to leave the policed network to harmless sending rates
2. Throttle **no** benign traffic that attempts to leave the policed network during this process

![Diagram showing IoT network, IoT gateway, FR-WARD, Internet, and Victim Server.](image)
Basic Design

• The design of FR-WARD is driven by the fundamental characteristics of an IoT environment.

• It follows two principles:
  1. It adopts a conservative approach to avoid dropping benign traffic
     • FR-WARD will **not** drop any traffic it cannot definitively discern as malevolent
     • Instead devises a signaling mechanism to handle suspicious connections
  2. The defense cannot rely on installation of new hardware or software on IoT devices
     • Instead relies only on protocols and functions that the IoT devices already support
FR-WARD’s flexible architecture

**Basic Design (cont.)**

**FR-WARD’s novel response**

- **Labeling Procedure:**
  - Victim-end Classification
  - Anomaly-based Classification

- **Attack Detection:**
  - Victim-end Collaboration
  - Anomaly-based Detection

- **Attack Resolution:**
  - Victim-end Collaboration
  - Anomaly-based Detection

- **Signaling Mechanism:**
  - Congestion Control Enforcement

- **Smart Attacker Defense:**
  - Flow Control Enforcement
Labeling Procedure

- It is not the main focus of FR-WARD to improve detection or classification of an attack
  - Connection labels act as an input to the FR-WARD system

- FR-WARD uses the observation component of the previous source-end DDoS defense solution D-WARD
  - Can instead rely on any connection labeling procedure that categorizes traffic into good, suspicious, or bad
  - (e.g.) Victim-end collaboration, machine learning, etc
• **D-WARD** monitors traffic at two levels of granularity:
  1. Classifies the aggregate traffic from the *entire* source network to a particular host as an **agflow**
     - Labels deviations from a predefined normal model as **attack agflows**
  2. Further classifies the aggregate traffic from one node in the source network to a particular host as an **connection**
     - Labels deviations from a predefined normal model as **bad connections**
Signaling Mechanism

• Good and bad connections are easy to respond to:
  o Throttle bad connections and allow safe passage of good connections
• FR-WARD must also respond to suspicious connections
  o Employs the fast retransmit mechanism from TCP congestion control to reduce their sending rate
• FR-WARD sends three duplicate acknowledgements of an “in-flight” segment to the suspicious connection
  o The sender cuts its window size in half and immediately retransmits the “in-flight” segment
    • In accordance to multiplicative decrease and fast retransmit
• We call this set of duplicate acknowledgements a signal
Signaling Mechanism: TCP Reno

cwnd = 6
Data [9]
Data [10]
Data [11]
Data [12]
Data [13]
Data [14]

EFS = 6

Sender
FR-WARD
Receiver

ACK [9]
Signalizing Mechanism: TCP Reno
Signaling Mechanism: TCP Reno

<table>
<thead>
<tr>
<th>Sender</th>
<th>FR-WARD</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>cwnd = 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [10]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [11]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [12]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [13]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [14]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EFS = 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EFS = 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EFS = 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EFS = 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EFS = 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cwnd = 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [15]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [16]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [17]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cwnd = 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [18]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [19]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [20]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data [21]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


ACK [17] → ACK [18]
**Signaling Mechanism: Benefits**

1. Identifies compliance with congestion control
   - FR-WARD can relabel non-compliant connections as bad within one RTT and begin to throttle them

<table>
<thead>
<tr>
<th>Sender</th>
<th>FR-WARD</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>cwnd = 6</td>
<td>Data [9]</td>
<td>ACK [9]</td>
</tr>
<tr>
<td>EFS = 2</td>
<td>Data [13]</td>
<td>Data [14]</td>
</tr>
<tr>
<td>EFS = 3</td>
<td>Data [15]</td>
<td>Data [16]</td>
</tr>
<tr>
<td>cwnd = 3</td>
<td>Data [17]</td>
<td>Data [18]</td>
</tr>
<tr>
<td>cwnd = 4</td>
<td>Data [19]</td>
<td>ACK [17]</td>
</tr>
<tr>
<td></td>
<td>Data [20]</td>
<td>ACK [18]</td>
</tr>
<tr>
<td></td>
<td>Data [21]</td>
<td></td>
</tr>
</tbody>
</table>
2. Decreases the transmission rate of malicious connections
   - FR-WARD must mitigate attack traffic as soon as possible
   - Passively checking compliance may not be fast enough
Signaling Mechanism: Benefits (cont.)

3. Reduces energy consumption for benign connections
   - Reduces retransmission and increases goodput compared to throttling
4. The same signaling mechanism works across TCP variants
   - Signal achieves aforementioned benefits under each algorithm
   - Simplifies design of FR-WARD
Defending Against Smart Attackers

• An attacker may design an attack specifically to evade FR-WARD
  o (e.g.) an attacker could follow congestion control and comply with FR-WARD's signals
  o If FR-WARD only sends signals to initially mitigate the attack, the attacker could quickly return to a high sending rate

• FR-WARD defines an allowed transmission rate for each suspicious connection
  o Enforces this transmission rate until the attack agflow is relabeled normal
Defending Against Smart Attackers (cont.)

• FR-WARD employs the flow control mechanism of TCP to define a suspicious connection’s allowed rate
  o In TCP, the receiver provides a flow control service in the form of a receive window, or recw
  o recw informs the sender the amount of available space in the receiver’s buffer

• This provides a precise definition for FR-WARD’s allowed transmission rate
  o If a sender transmits more than recw, the receiver’s buffer will overflow, thus constituting a DDoS attack

• FR-WARD waits to observe recw values until after sending its initial signals
  o Utilizing flow control requires expensive operations and state maintenance
  o FR-WARD maintains the flow control state only when necessary
FR-WARD Overview

1. Attack Detection
   - Detect an attack through victim-end collaboration
   - Or self sufficiently detect an attack
2. Labeling Procedure
   - Label each connection in the attack agflow as good, bad, or suspicious
2. Labeling Procedure
   - Label each connection in the attack agflow as good, bad, or suspicious
3. Signaling Mechanism
   - Allow good, throttle bad, and send a signal to each suspicious connection
3. Signaling Mechanism
   - Relabel each non-compliant connection as bad
4. Smart Attacker Defense
   - Throttle any suspicious connections that attempt to send more than receive.
Extending the Signaling Mechanism

• FR-WARD is based on aspects of TCP
  o Want to show that FR-WARD can extend to any type of connection

• Traditionally, an application uses UDP if unreliable communication is sufficient
  o (e.g.) if an IoT device wishes to send its location to a server, it can periodically provide the server its location with UDP datagrams
  o Even after a lost datagram, the server can still infer the device’s location based on previous and future information

• FR-WARD does not need to provide an efficient response to such connections
  o It can simply throttle the connection since retransmission is not required
Extending the Signaling Mechanism (cont.)

• But, many IoT applications desire the reliability of TCP but with the overhead of UDP
  o (e.g.) CoAP, DTLS
  o These connections will retransmit lost packets similar to a TCP connection
  o FR-WARD cannot simply throttle these types of connections when they are labeled suspicious

• Any connection that requires reliable transportation uses some type of an acknowledgment
  o FR-WARD can create its signaling mechanism based on this acknowledgement
### Signaling Mechanism: pCoCoA

<table>
<thead>
<tr>
<th>Sender</th>
<th>FR-WARD</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data [9.1]</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>RTO = 1.5*RTT</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>Data [9.2]</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>RTT</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>Data [10.1]</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>ACK [9.2]</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
</tbody>
</table>

---

36
Signaling Mechanism: pCoCoA
Signaling Mechanism: pCoCoA

Diagram:
- Sender
  - Data [9.1]
  - RTO = 1.5*RTT
  - Data [9.2]
  - RTT
  - Data [10.1]
  - F_RTT
  - Data [11.1]
  - RTO_new = 2.47*RTO
  - Data [11.2]
- FR-WARD
- Receiver
  - ACK [9.1]
  - ACK [9.2]
  - ACK [10.1]
Table of Contents

1. Introduction
   o The Internet of Things
   o Source-end Distributed Denial-of-Service Defense
   o Difficulties of Source-end Defense for the Internet of Things

2. FR-WARD
   o Threat Model & Assumptions
   o Basic Design
   o Labeling Procedure
   o Signaling Mechanism
   o Defending Against Smart Attackers
   o Extending the Signaling Mechanism

3. Evaluation
   o Effects on Benign Traffic
   o Effects on Malicious Traffic
FR-WARD Evaluation

• We compare FR-WARD’s performance against the previous source-end DDoS defense system, D-WARD
  o We expect FR-WARD to have the same accuracy and detection as D-WARD, so we do not evaluate them in this work

• We simulate mathematical models to estimate FR-WARD’s effect on benign traffic
  o Retransmission, Goodput, Energy Consumption

• We use real-time experiments to estimate FR-WARD’s ability to mitigate DDoS attacks
  o TCP SYN-flood attack, “Smart” TCP flood attack
Effects on Benign Traffic: Retransmission

- As the window size (at the time of the attack detection) increases, D-WARD drops more packets initially.
  - FR-WARD never drops suspicious traffic, and causes close to zero retransmissions.
- On average, FR-WARD reduces retransmissions by a factor of 203.
Effects on Benign Traffic: Goodput

- As D-WARD drops more packets, it also causes the connection to slow down
  - Muddled with retransmissions, time wasted waiting for negative ACKs
- On average, FR-WARD increases goodput by a factor of 3.8
Effects on Benign Traffic: Energy Consumption

- Because FR-WARD reduces retransmissions, a benign device consumes much less energy than under D-WARD
  - Less packet transmission
- Because FR-WARD increases goodput, a benign device consumes much less energy than under D-WARD
  - Less active transmission time
Effects on Benign Traffic: D-WARD Parameters

- We evaluate the effect of D-WARD’s parameter, $f_{\text{dec}}$
  - $f_{\text{dec}}$ represents the rigor of D-WARD
  - (ie) How much traffic does D-WARD drop after a detected attack
- As D-WARD becomes stricter, it drops more segments
  - Increases retransmissions further
  - Decreases goodput further

(c) The magnitude FR-WARD improves Goodput under TCP NewReno. (c) The magnitude FR-WARD improves retransmissions under TCP NewReno.
Effects on Malicious Traffic

- The naive attacker uses the hping3 command-line tool to flood the receiver with TCP-SYN segments.
- After detecting an attack, both defense systems successfully throttle the attacker’s throughput.
- The graphs look almost identical.
  - But FR-WARD’s signaling mechanism allows a negligible extra instant of DDoS traffic.

(a) The throughput of a naive attacker under D-WARD.

(d) The throughput of a naive attacker under FR-WARD.
Effects on Malicious Traffic

(a) The throughput of the smart attacker under D-WARD.

(d) The throughput of the smart attacker under FR-WARD.

- The smart attacker follows TCP congestion control
  - But still attempts to flood the receiver with TCP segments
- The attacker can achieve bursts of successful DDoS traffic under D-WARD
  - The attacker follows congestion control but not flow control
- FR-WARD never allows the smart attacker to transmit more than the receiver can handle
  - The smart attacker either must transmit at a manageable rate or become detected
Acknowledgements

• Special thank you to the co-authors on this work:
  o Devkishen Sisodia, Jun Li, and Hasan Cam

• For more details, check out our publication:

• Thank you for listening!