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

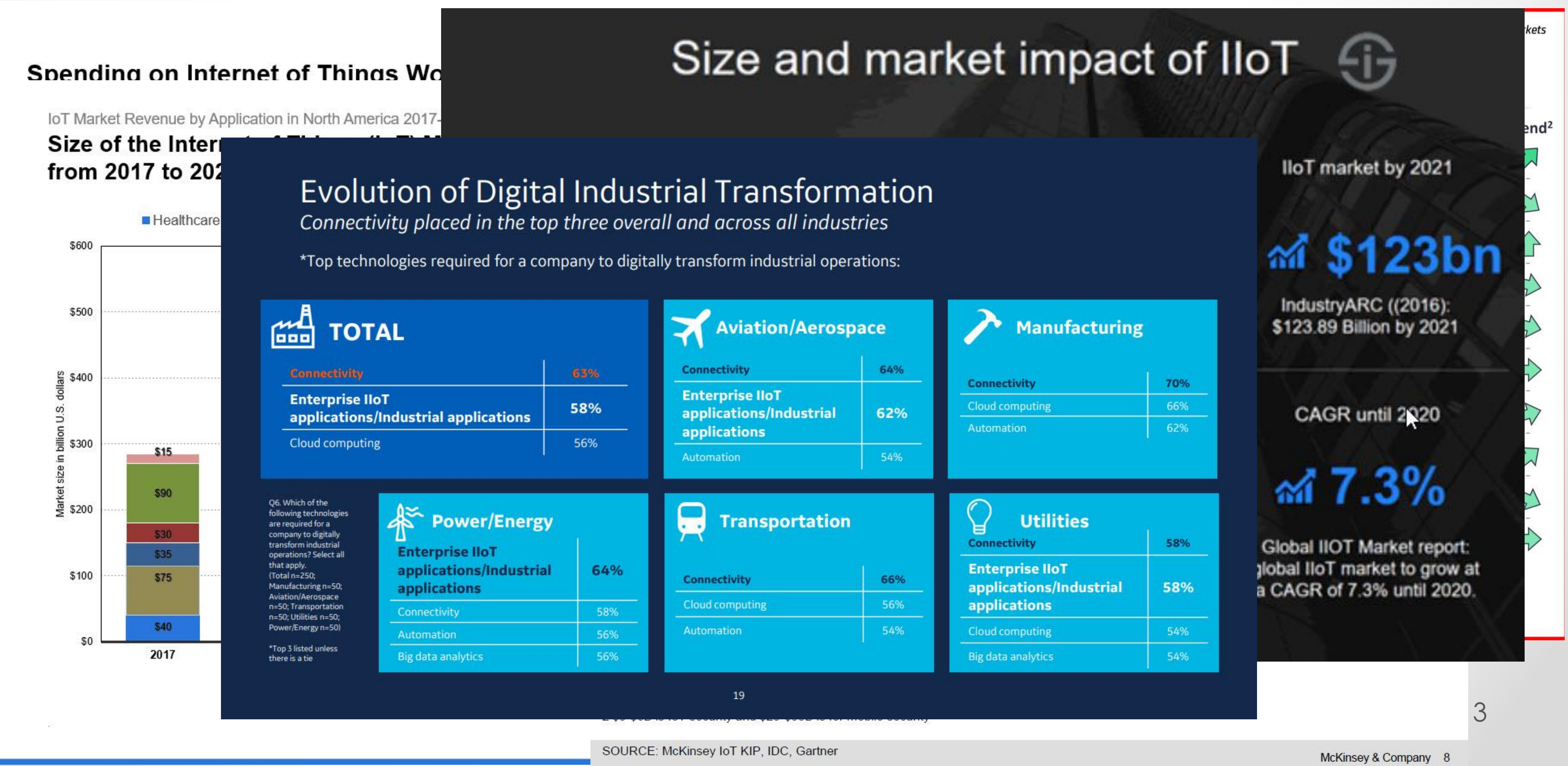
Samuel Mergendahl

Center for
Cyber Security and Privacy
University of Oregon

Table of Contents

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


KrebsonS
In-depth security news and in

WIRED
The Reaper IoT Botnet Has Already Infected a Million Networks
ANDY GREENBERG SECURITY 10.20.17 05:45 PM

ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

INTERNET OF BROKEN THINGS —

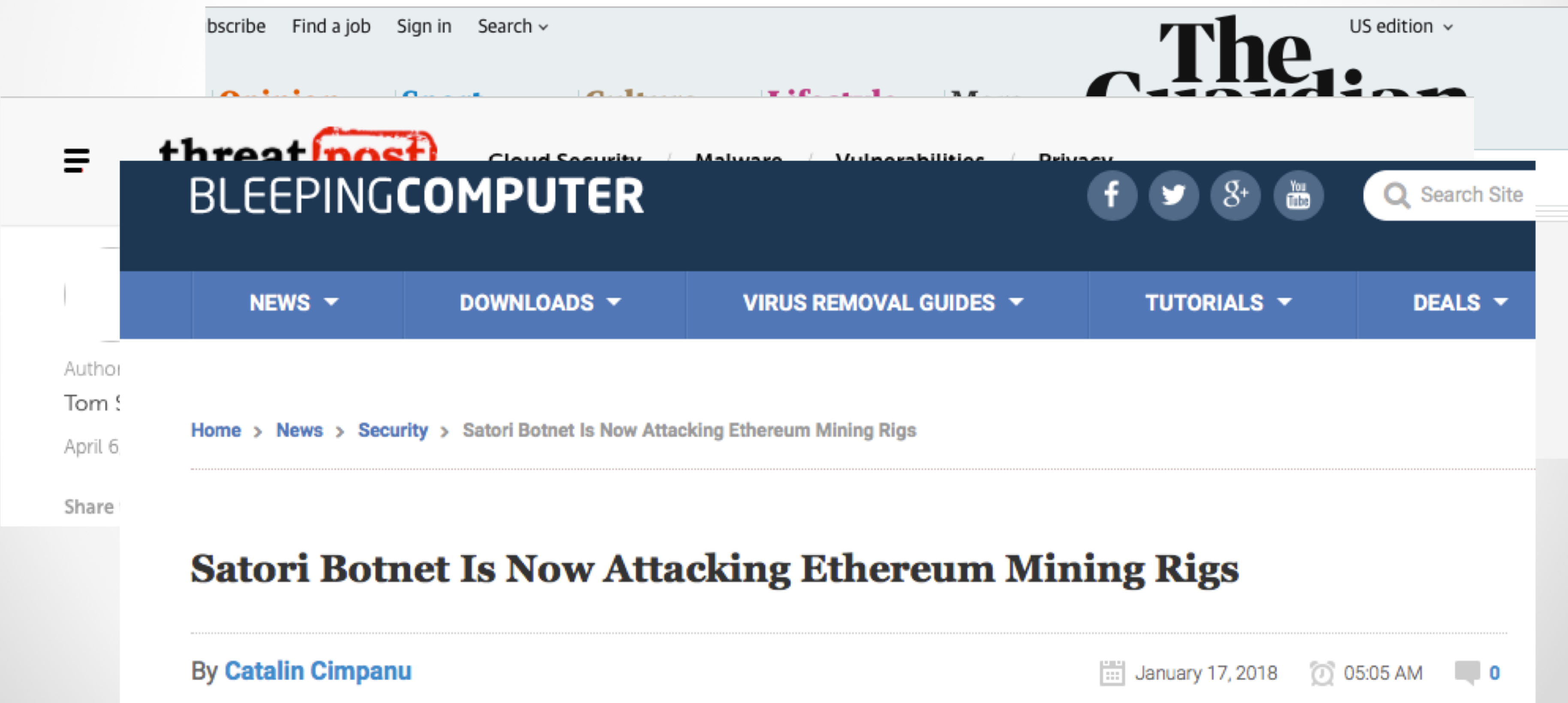
A potent botnet is exploiting a critical router bug that may never be fixed

With Internet stability hanging in the balance, router maker maintains radio silence.

DAN GOODIN - 2/14/2018, 2:10 PM

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
  - Easier to properly handle DDoS attacks near the attack sources
  - 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
  - False positive = misidentifying a benign connection as malicious
  - 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
  - False negative = misidentifying a malicious connection as benign
  - 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

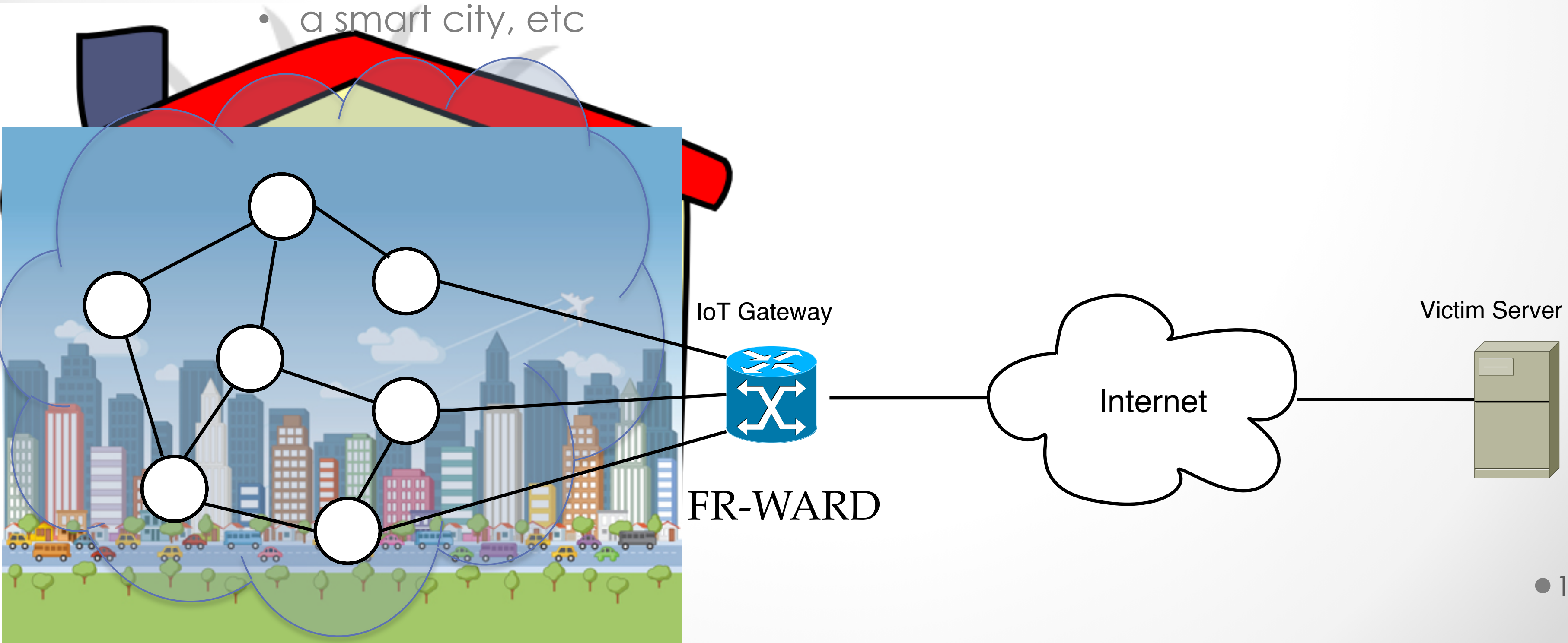
- A source-end DDoS defense will unavoidably encounter traffic it must label with low confidence
  - We call this traffic ***suspicious***
- If the defense filters the suspicious traffic:
  - It inevitably filters some good traffic
  - Leads to unwanted negative effects on benign traffic in IoT networks
- If the defense allows safe passage for the suspicious traffic:
  - It inevitably allows safe passage for some bad traffic
  - Fails to comprehensively mitigate an attack
- We need an efficient–but effective–***response*** to suspicious traffic

Table of Contents

1. Introduction
   - The Internet of Things
   - Source-end Distributed Denial-of-Service Defense
   - Difficulties of Source-end Defense for the Internet of Things
2. FR-WARD
   - Threat Model & Assumptions
   - Basic Design
   - Labeling Procedure
   - Signaling Mechanism
   - Defending Against Smart Attackers
   - Extending the Signaling Mechanism
3. Evaluation
   - Effects on Benign Traffic
   - Effects on Malicious Traffic

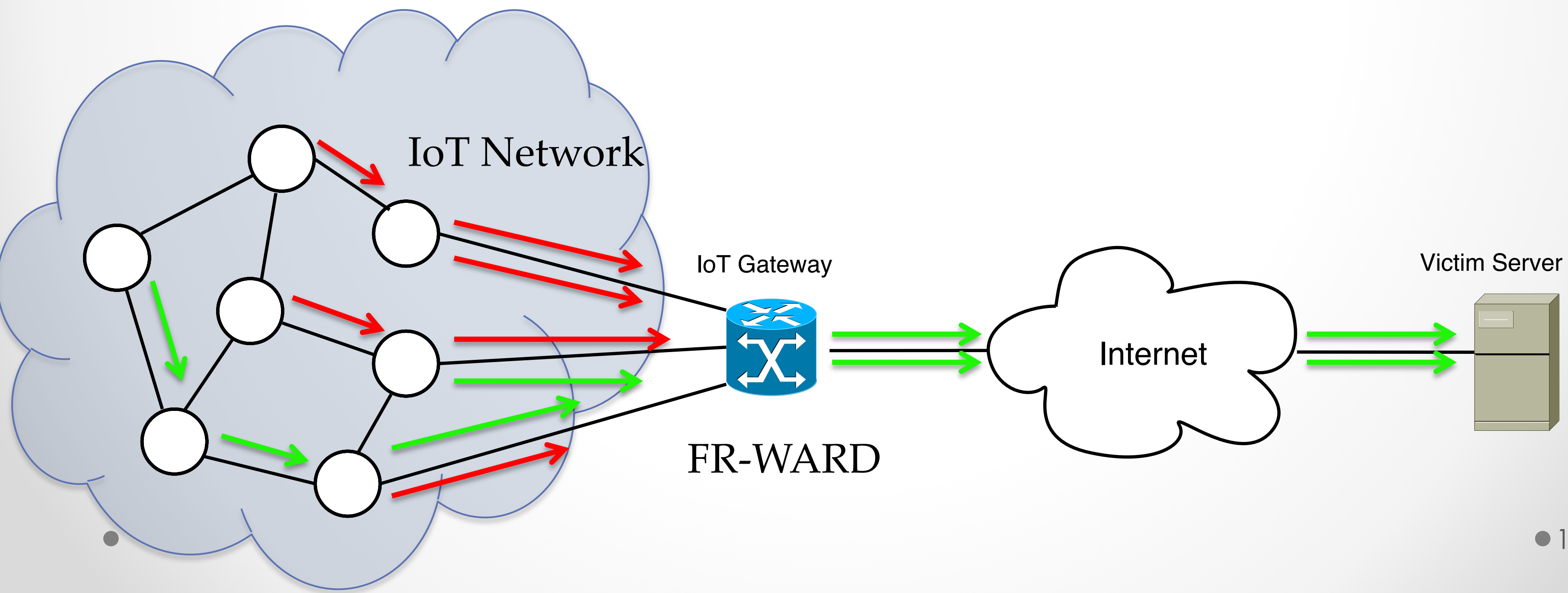
Threat Model & Assumptions

- 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



Threat Model & Assumptions (cont.)

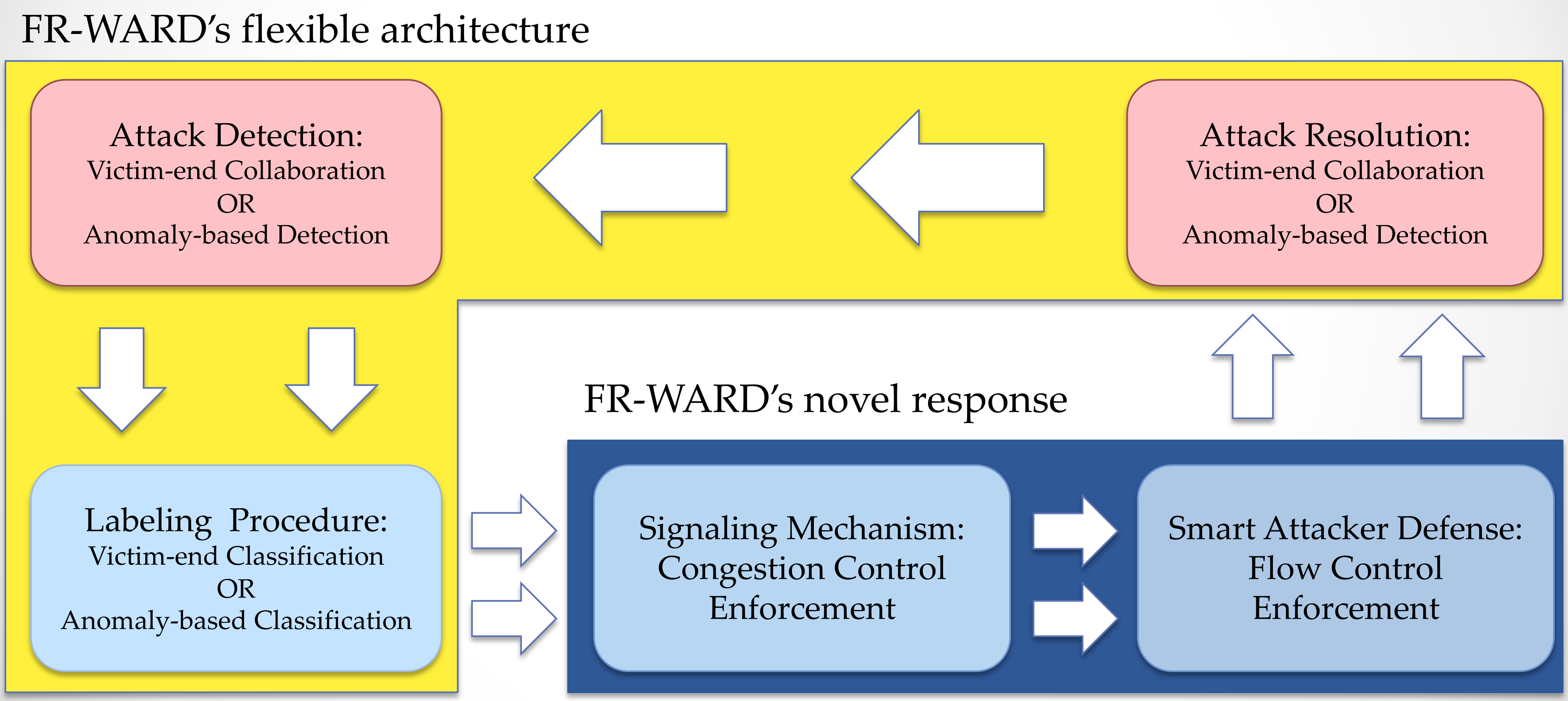
- FR-WARD has two main goals:
  1. Throttle **all** malicious DDoS traffic that attempts to leave the policed network to harmless sending rates
  2. Throttle **no** benign traffic that attempts to leave the policed network during this process



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

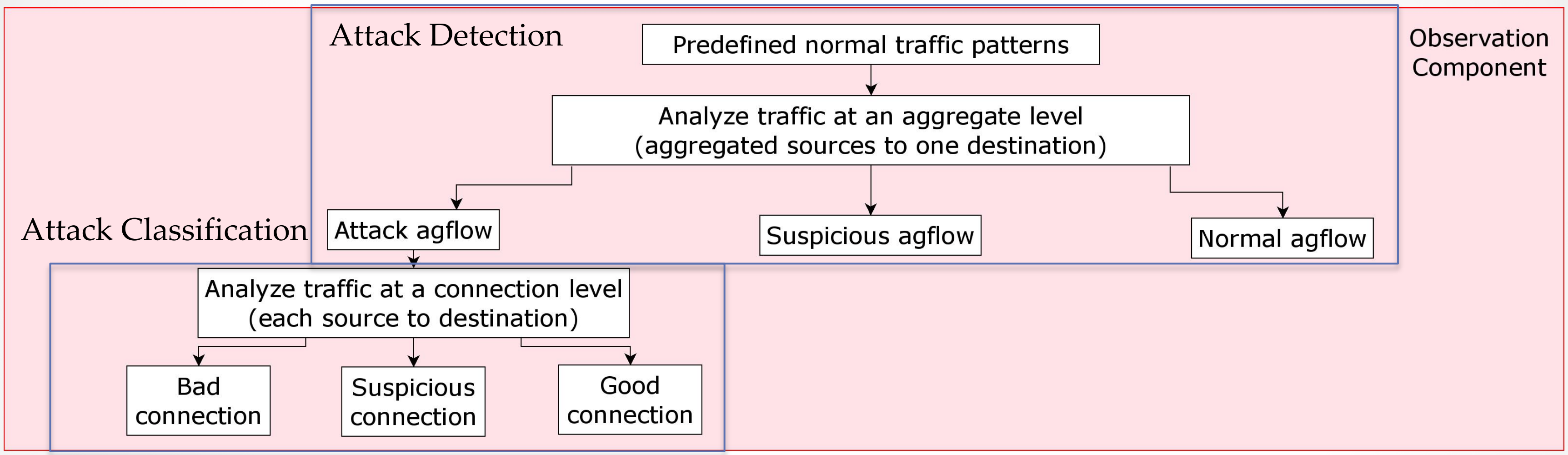
Basic Design (cont.)



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

Labeling Procedure (cont.)

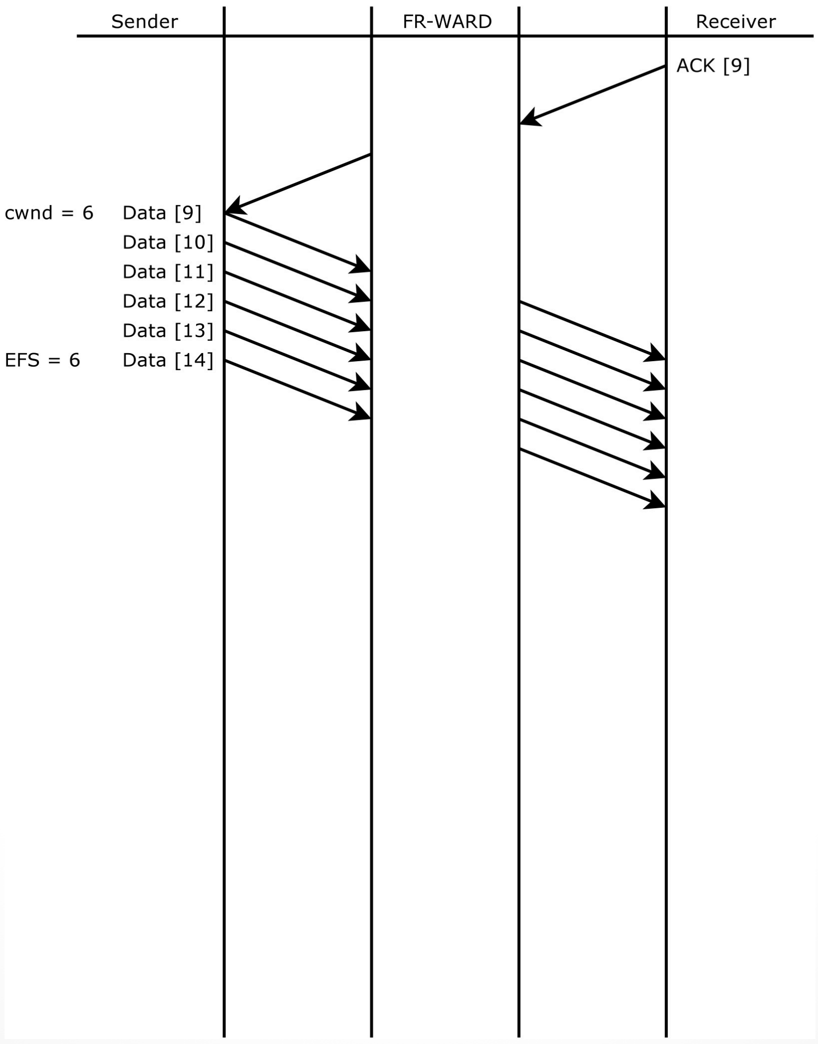


- D-WARD monitors traffic at two levels of granularity:
  1. Classifies the aggregate traffic from the *entire* source network to a particular host as an **agflow**
     - Labels deviations from a predefined normal model as *attack agflows*
  2. Further classifies the aggregate traffic from *one node* in the source network to a particular host as an **connection**
     - Labels deviations from a predefined normal model *as bad connections*

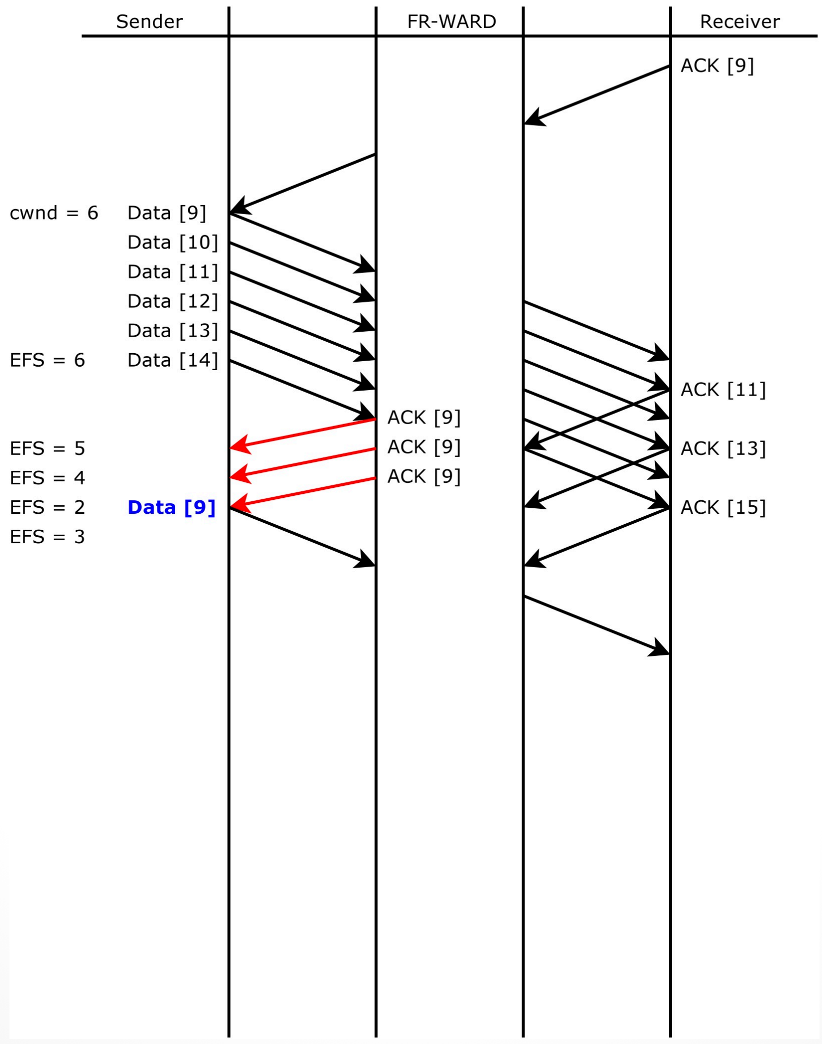
Signaling Mechanism

- Good and bad connections are easy to respond to:
  - Throttle bad connections and allow safe passage of good connections
- FR-WARD must also respond to suspicious connections
  - 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
  - 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**

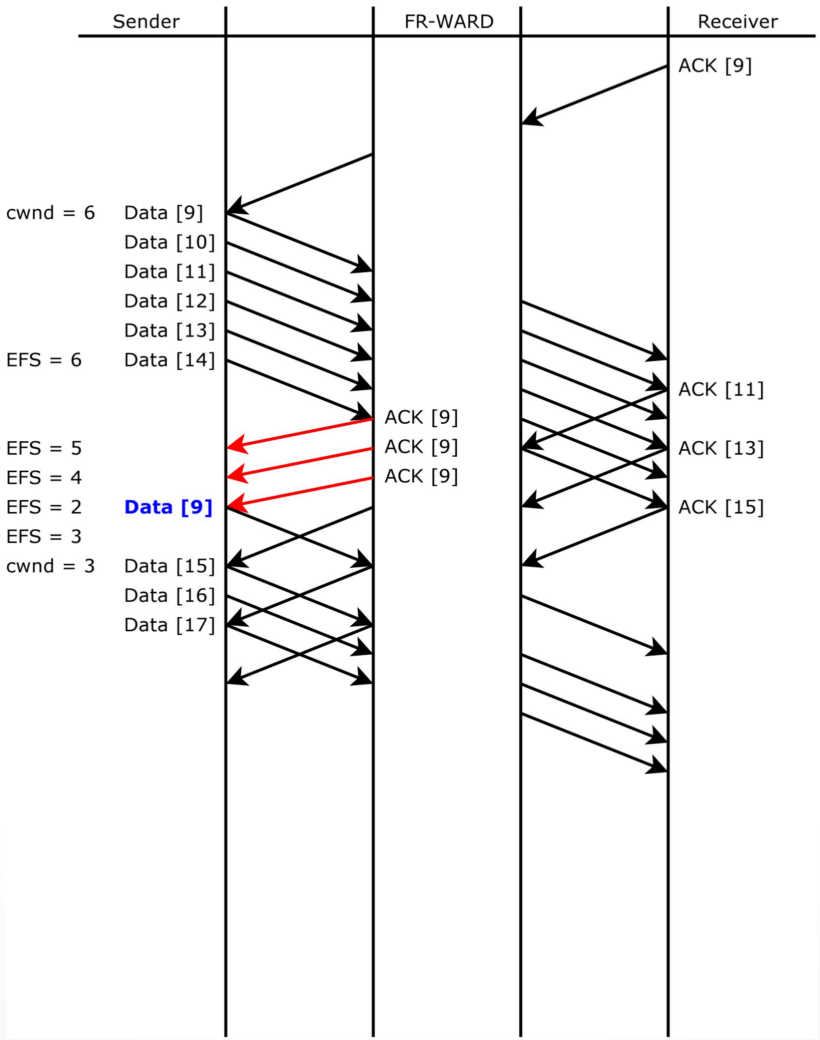
Signaling Mechanism: TCP Reno



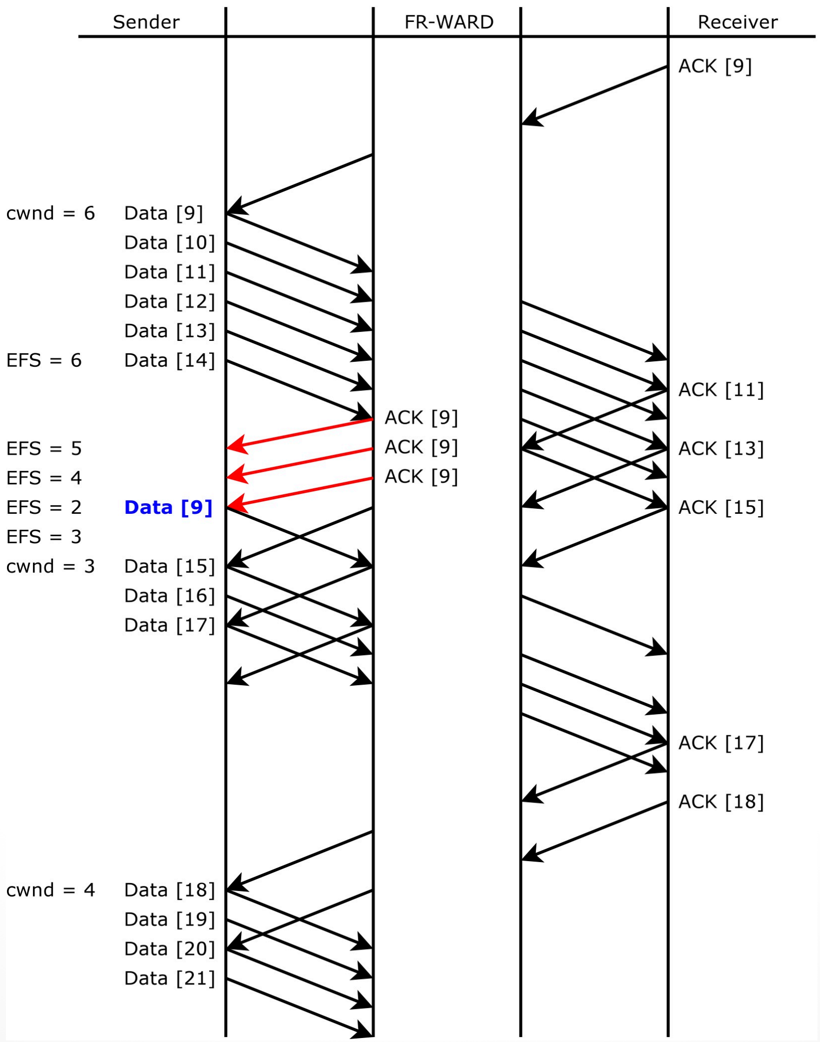
Signaling Mechanism: TCP Reno



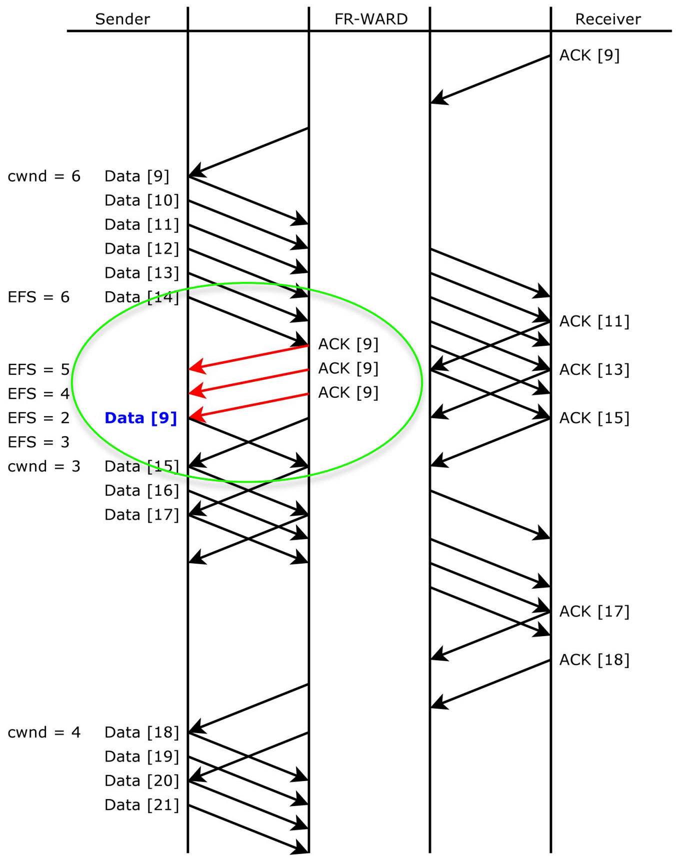
Signaling Mechanism: TCP Reno



Signaling Mechanism: TCP Reno

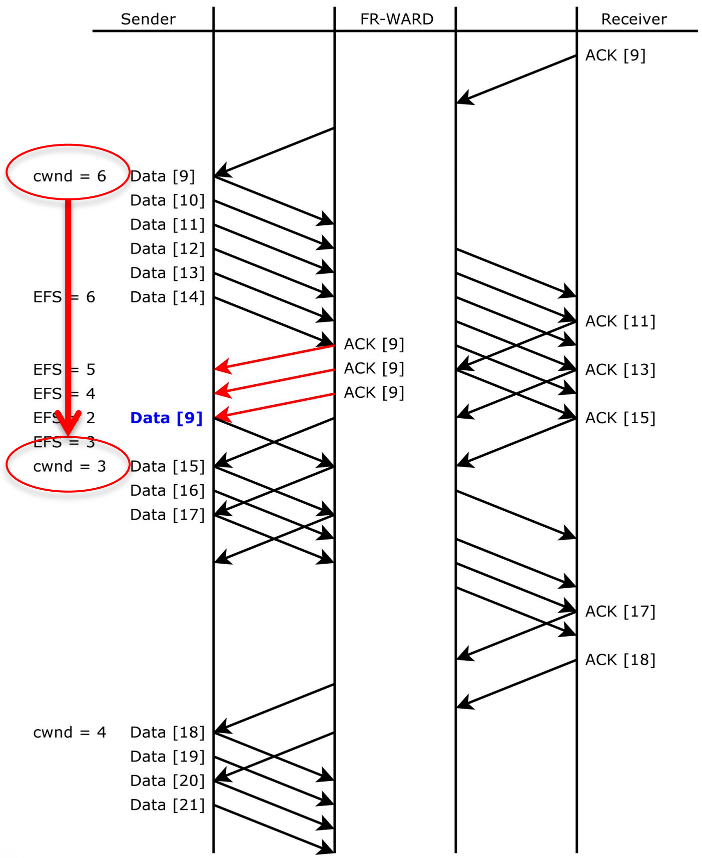


Signaling Mechanism: Benefits



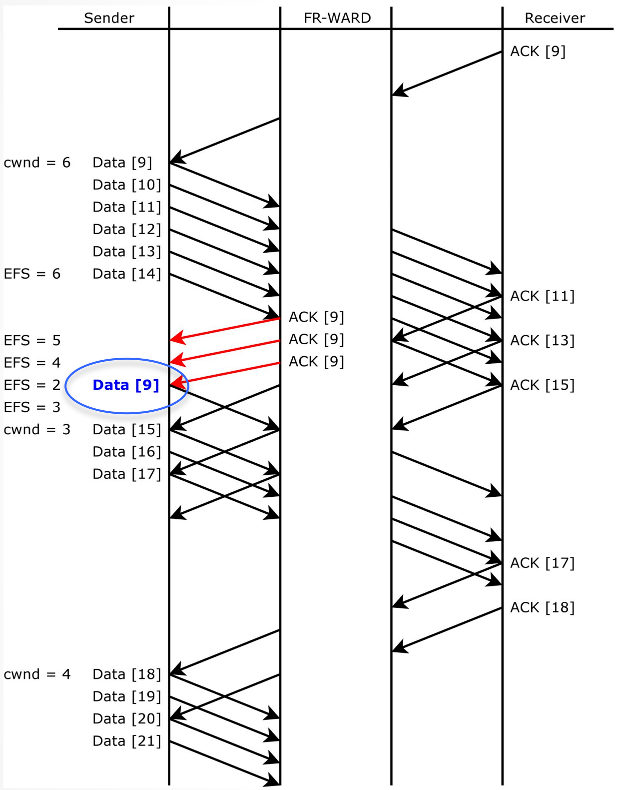
1. Identifies compliance with congestion control
   - FR-WARD can relabel non-compliant connections as bad within one RTT and begin to throttle them

Signaling Mechanism: Benefits

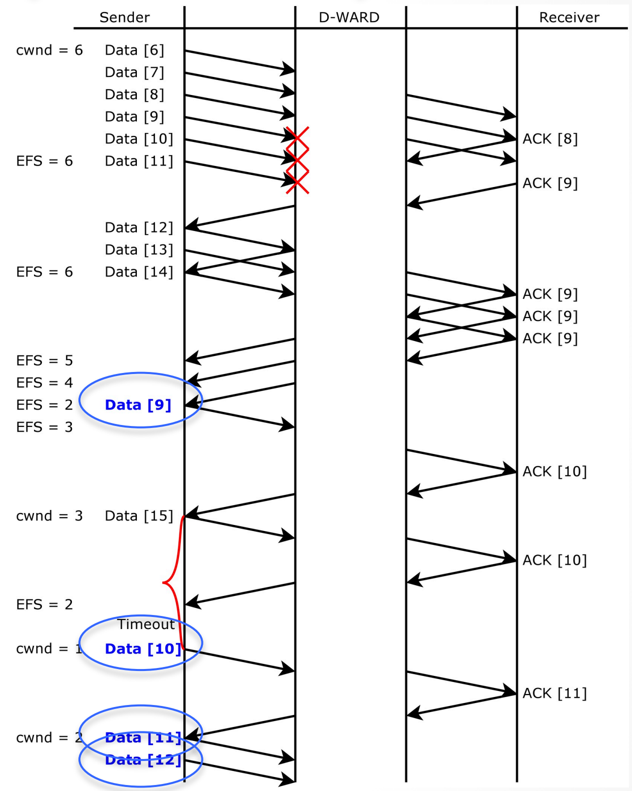


2. Decreases the transmission rate of malicious connections
   - FR-WARD must mitigate attack traffic as soon as possible
   - Passively checking compliance may not be fast enough

Signaling Mechanism: Benefits (cont.)



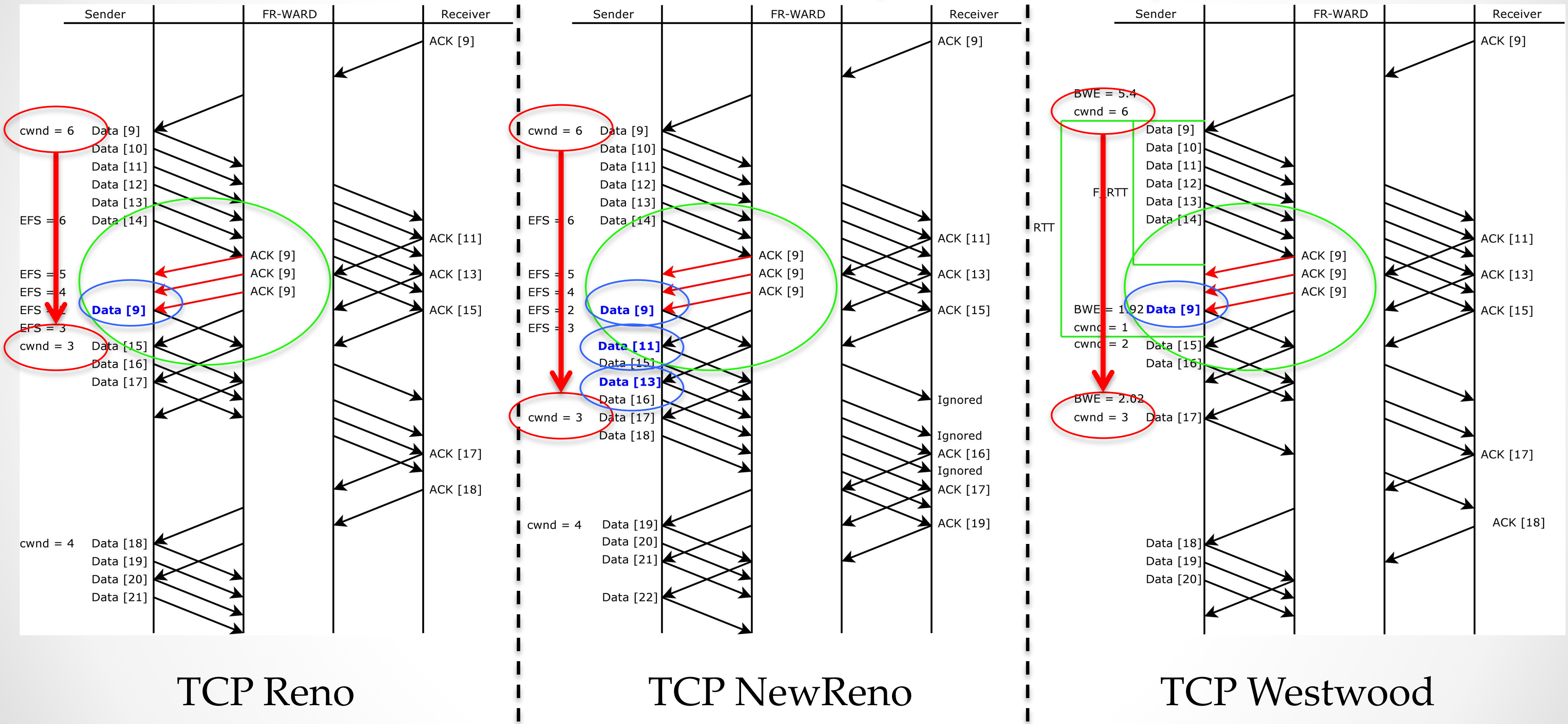
Signaling Mechanism



Throttling

3. Reduces energy consumption for benign connections
   - Reduces retransmission and increases goodput compared to throttling

Signaling Mechanism: Benefits (cont.)



TCP Reno | TCP NewReno | TCP Westwood

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

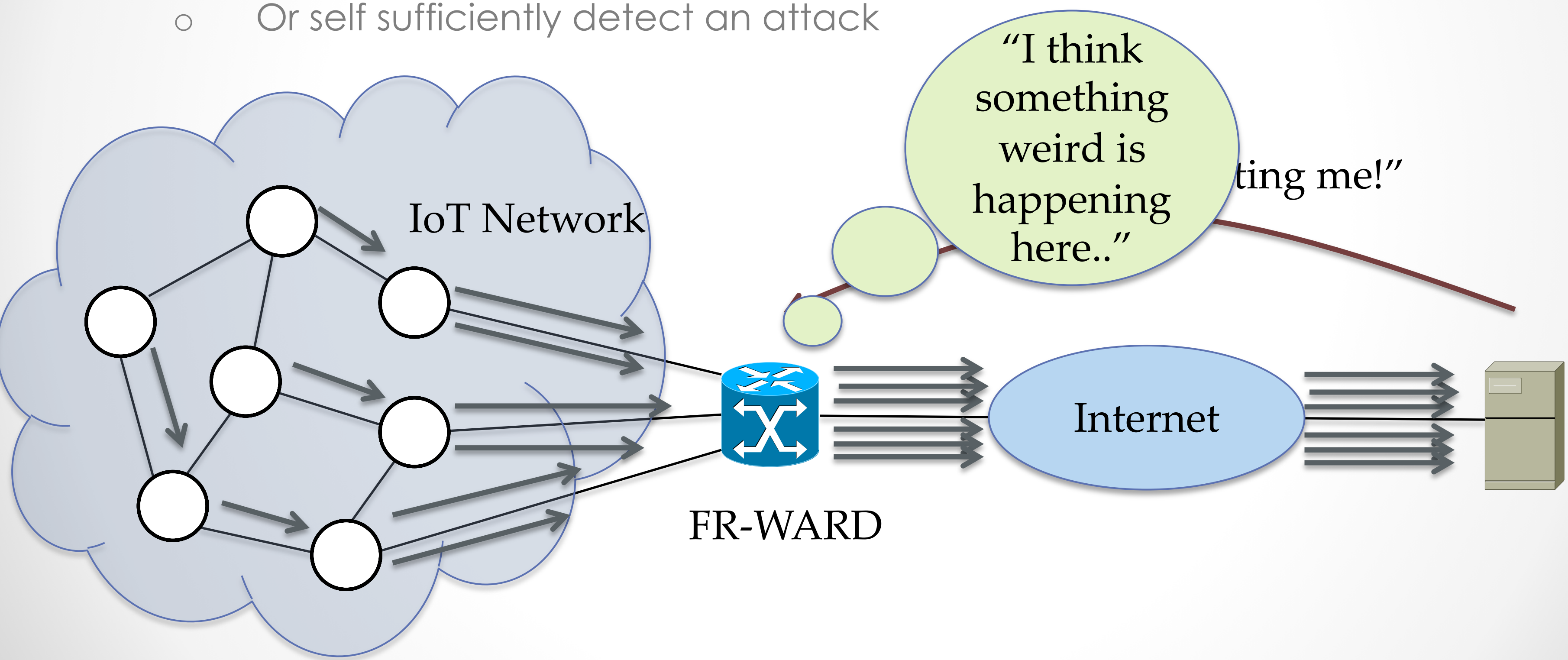
- An attacker may design an attack specifically to evade FR-WARD
  - (e.g.) an attacker could follow congestion control and comply with FR-WARD's signals
  - If FR-WARD only sends signals to initially mitigate the attack, the attacker could quickly return to a high sending rate
- FR-WARD defines an allowed transmission rate for each suspicious connection
  - 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
  - In TCP, the receiver provides a flow control service in the form of a receive window, or *recw*
  - *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
  - 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
  - Utilizing flow control requires expensive operations and state maintenance
  - FR-WARD maintains the flow control state only when necessary

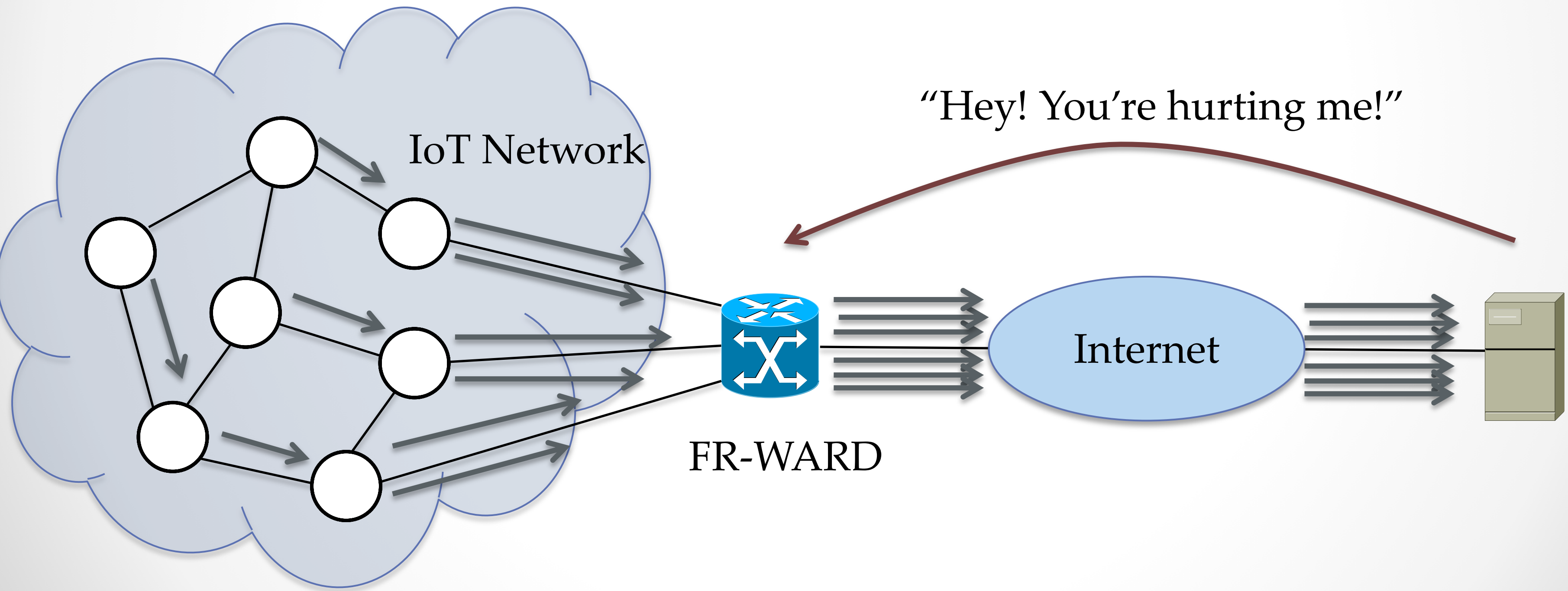
FR-WARD Overview

1. Attack Detection
   - Detect an attack through victim-end collaboration
   - Or self sufficiently detect an attack



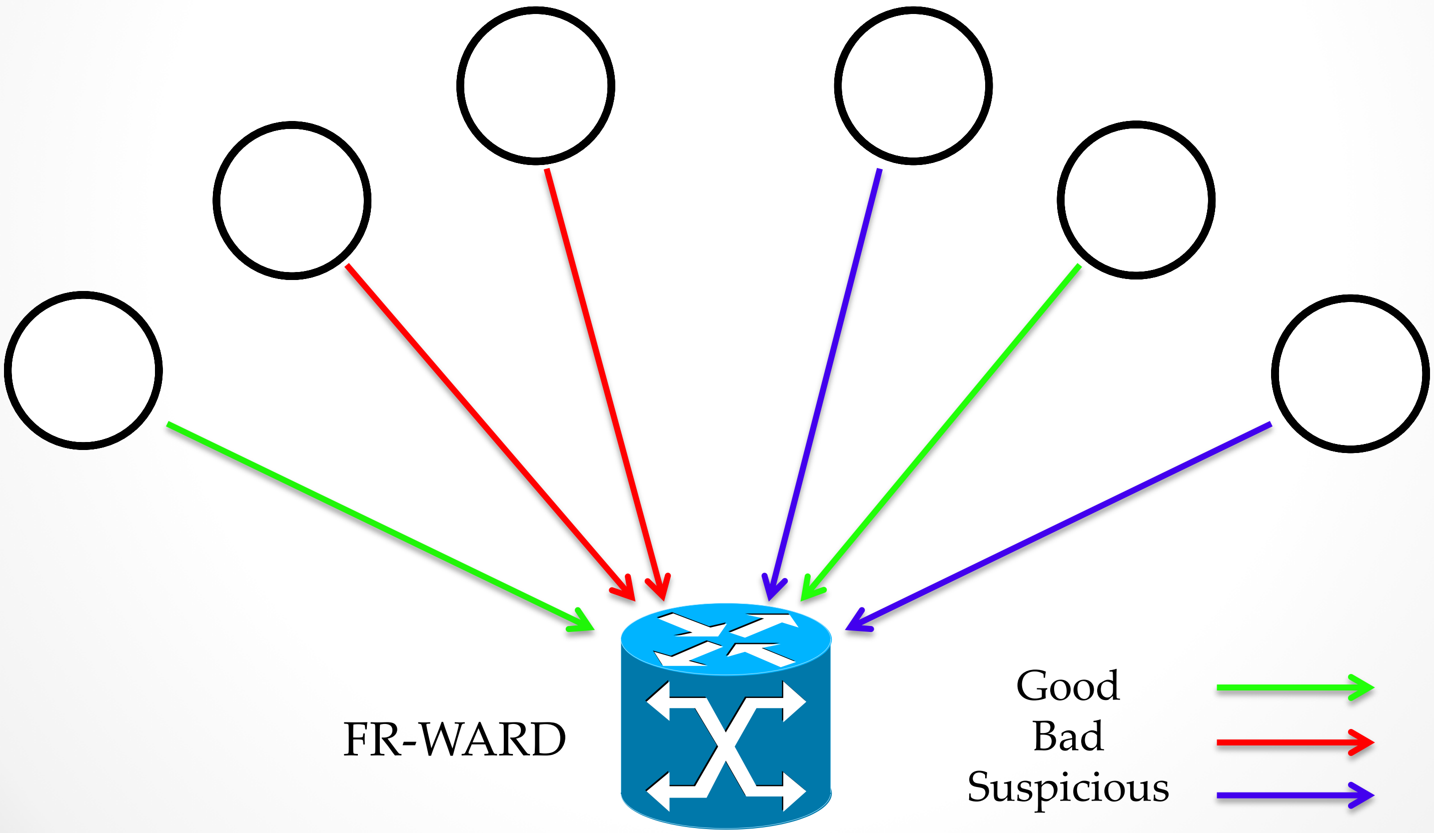
FR-WARD Overview (cont.)

2. Labeling Procedure
   - Label each connection in the attack agflow as good, bad, or suspicious



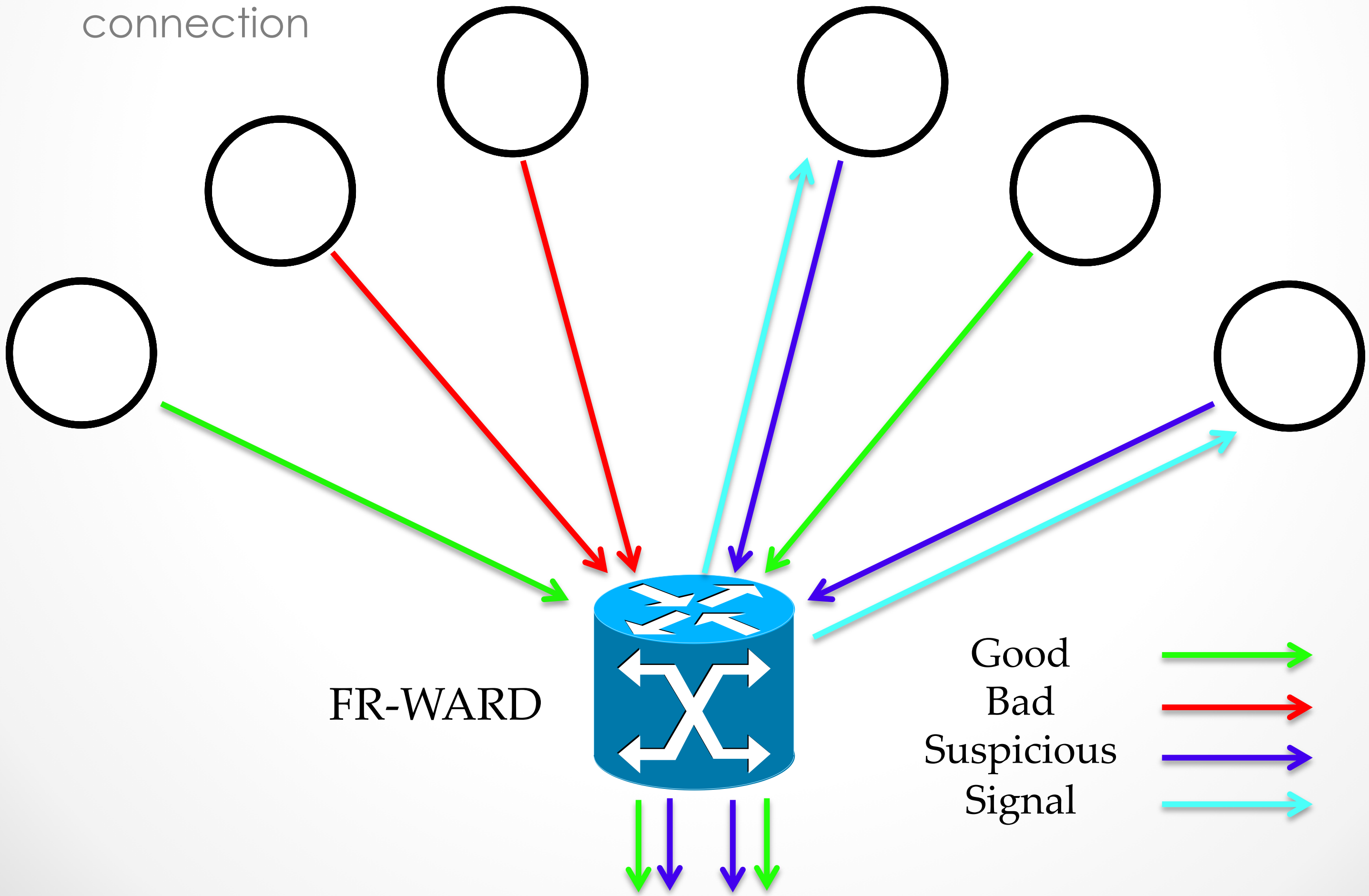
FR-WARD Overview (cont.)

2. Labeling Procedure
   - Label each connection in the attack agflow as good, bad, or suspicious



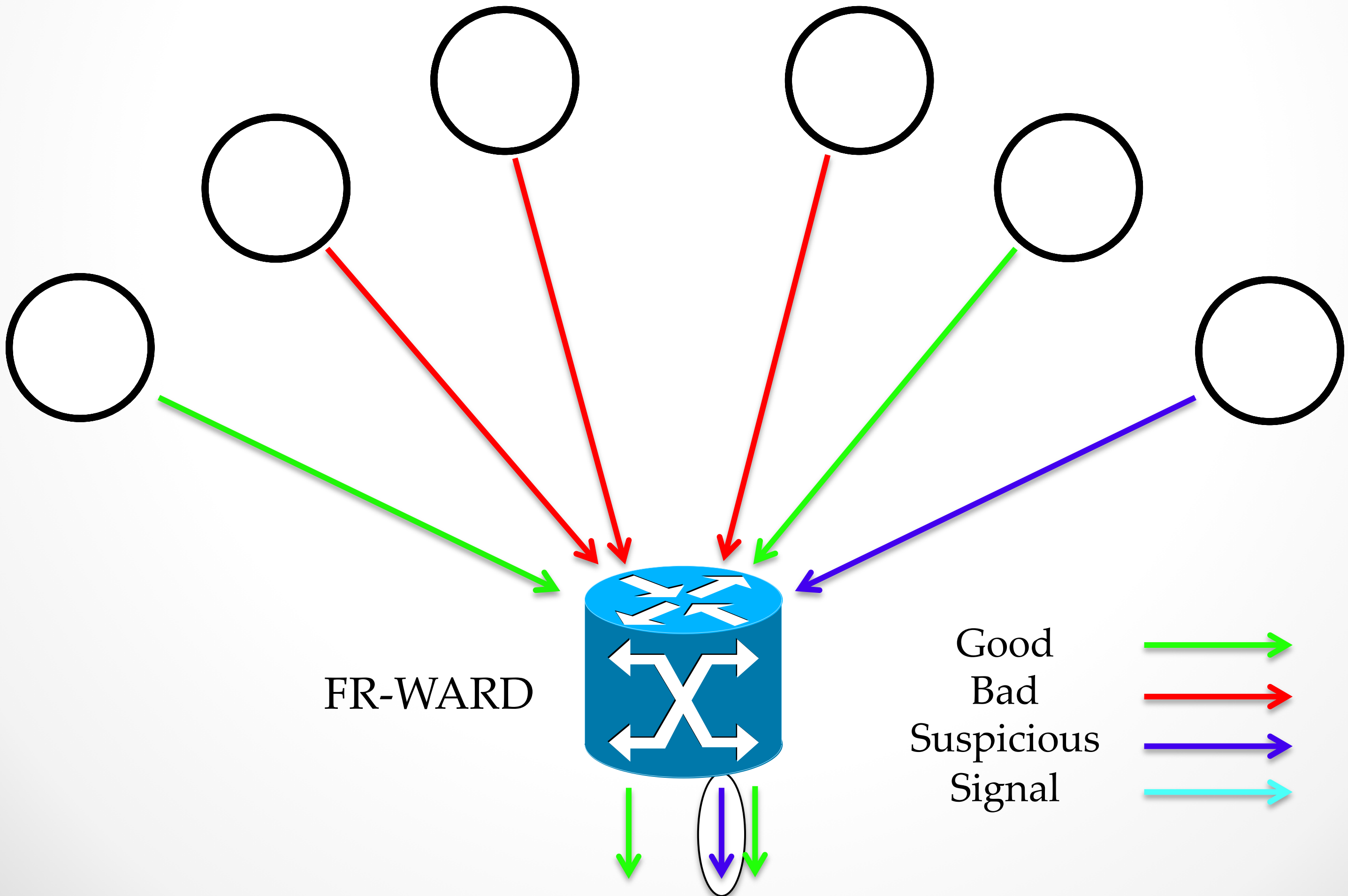
FR-WARD Overview (cont.)

3. Signaling Mechanism
   - Allow good, throttle bad, and send a signal to each suspicious connection



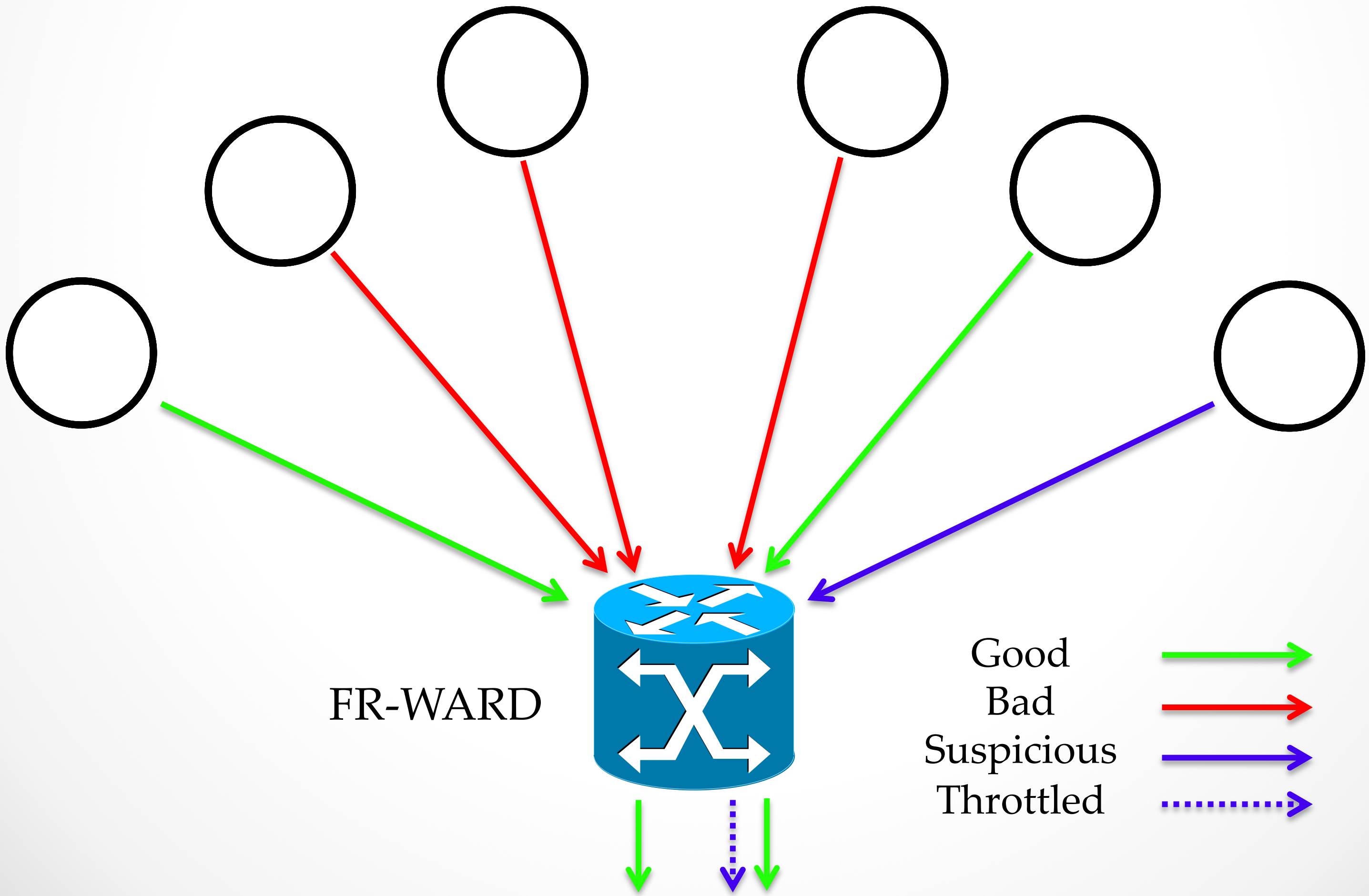
FR-WARD Overview (cont.)

3. Signaling Mechanism
   - Relabel each non-complient connection as bad



FR-WARD Overview (cont.)

4. Smart Attacker Defense
   - Throttle any suspicious connections that attempt to send more than *recw*



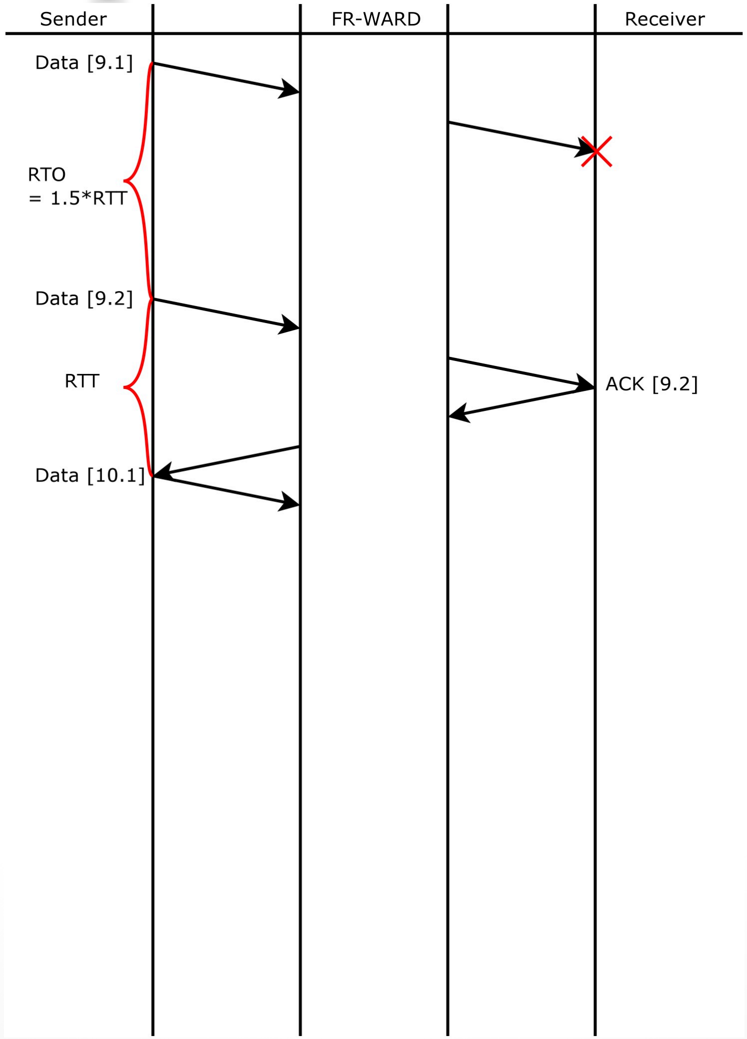
Extending the Signaling Mechanism

- FR-WARD is based on aspects of TCP
  - Want to show that FR-WARD can extend to any type of connection
- Traditionally, an application uses UDP if unreliable communication is sufficient
  - (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
  - 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
  - It can simply throttle the connection since retransmission is not required

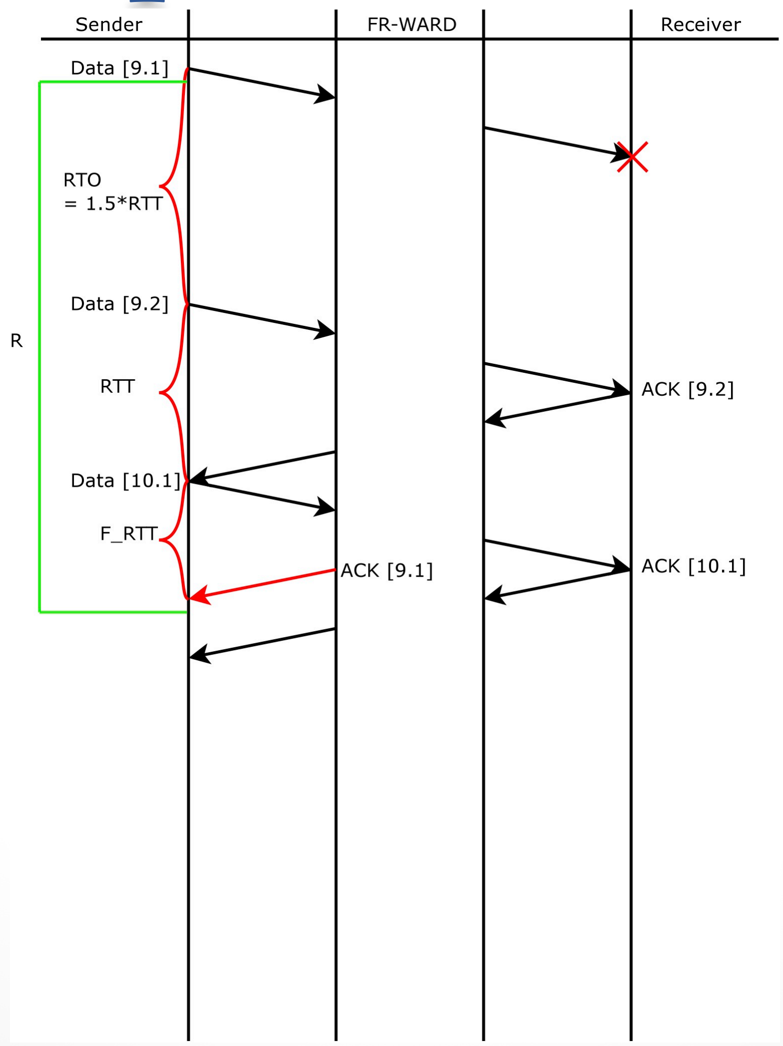
Extending the Signaling Mechanism (cont.)

- But, many IoT applications desire the reliability of TCP but with the overhead of UDP
  - (e.g.) CoAP, DTLS
  - These connections will retransmit lost packets similar to a TCP connection
  - 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
  - FR-WARD can create its signaling mechanism based on this acknowledgement

Signaling Mechanism: pCoCoA



Signaling Mechanism: pCoCoA



Signaling Mechanism: pCoCoA

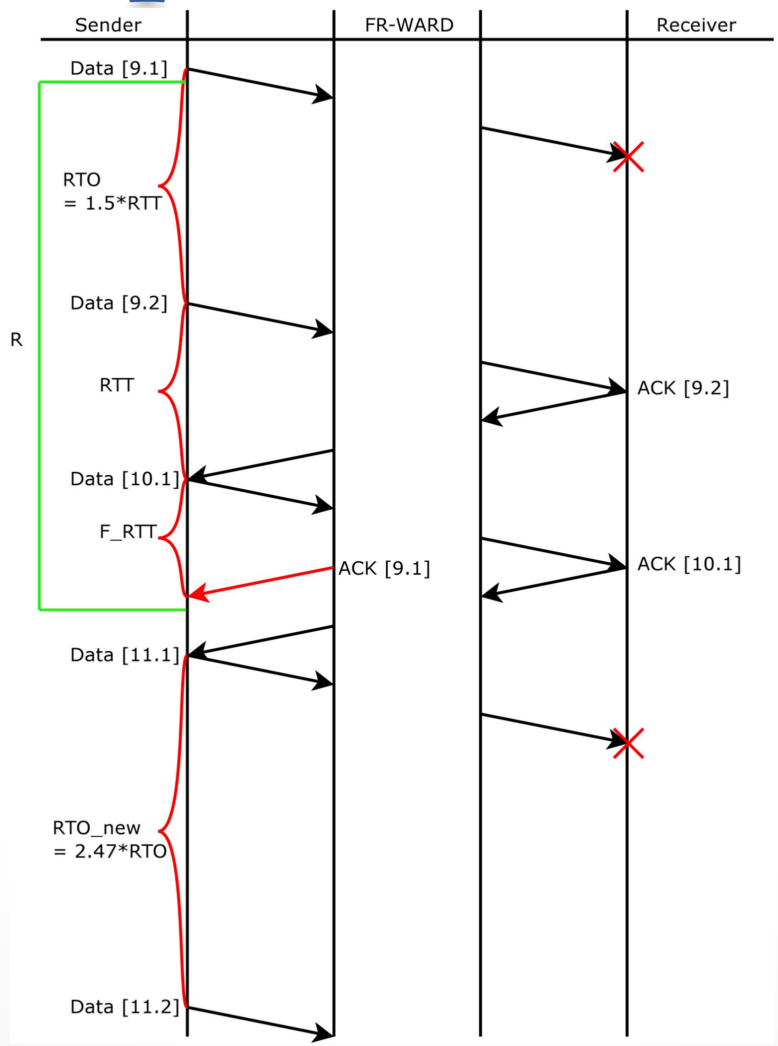
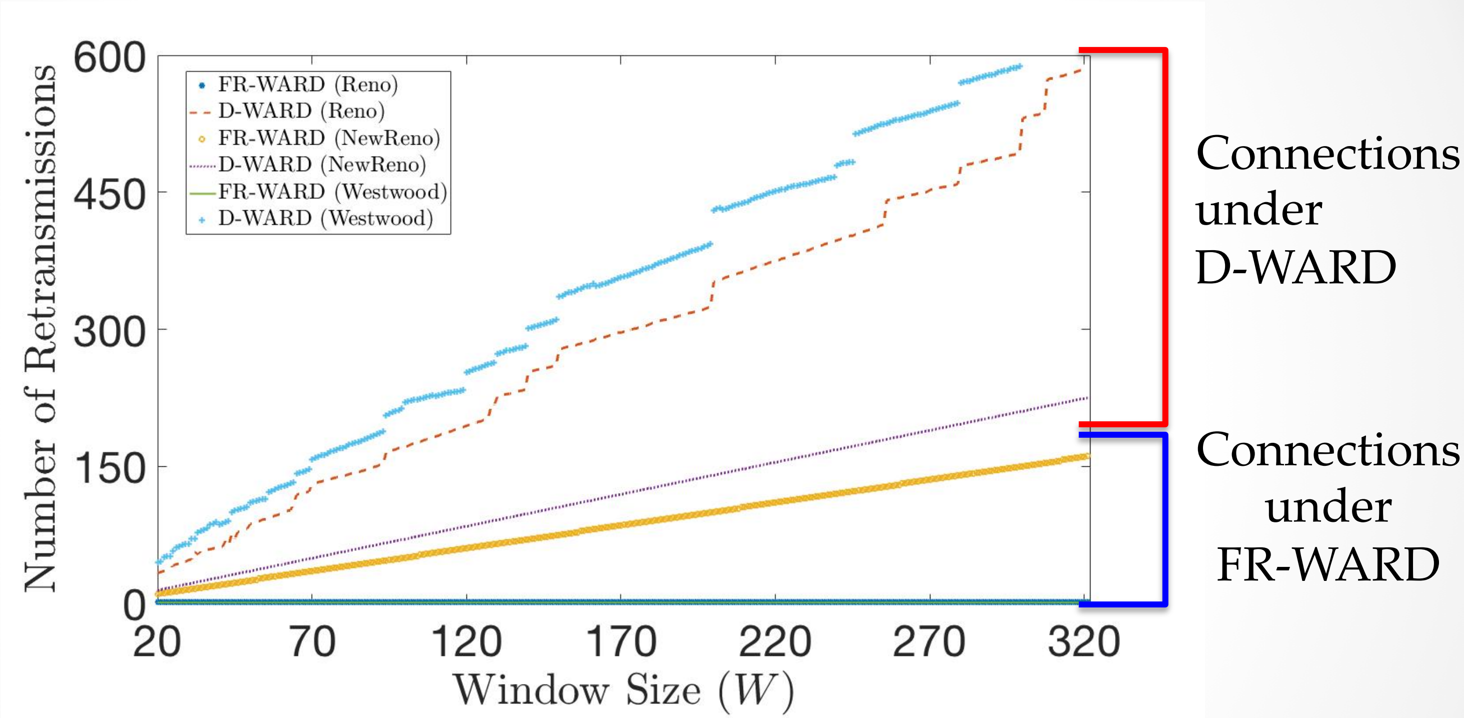


Table of Contents

FR-WARD Evaluation

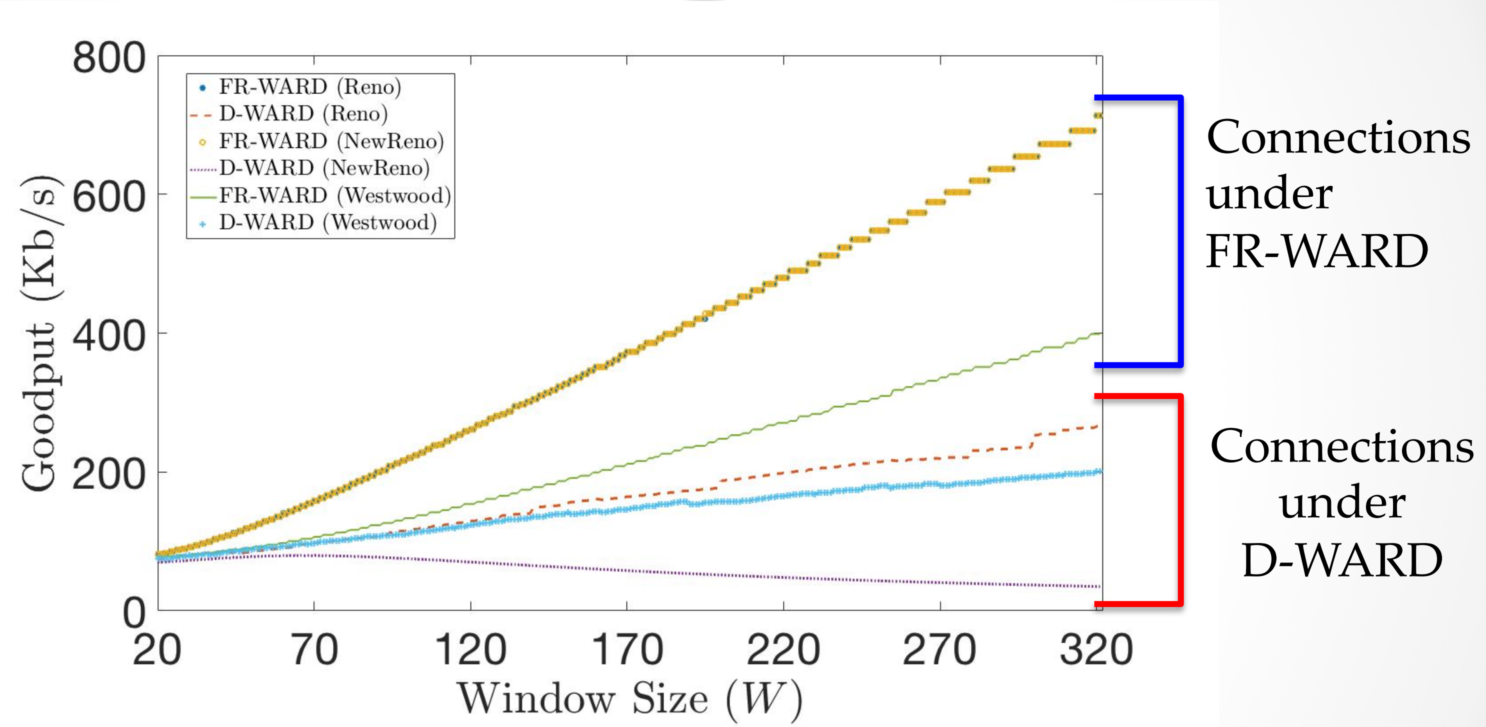
- We compare FR-WARD's performance against the previous source-end DDoS defense system, D-WARD
  - We expect FR-WARD to have the same accuracy and detection as D-WARD, so we do not evaluate them in this work
- We simulate mathematical models to estimate FR-WARD's effect on benign traffic
  - Retransmission, Goodput, Energy Consumption
- We use real-time experiments to estimate FR-WARD's ability to mitigate DDoS attacks
  - TCP SYN-flood attack, "Smart" TCP flood attack

Effects on Benign Traffic: Retransmission



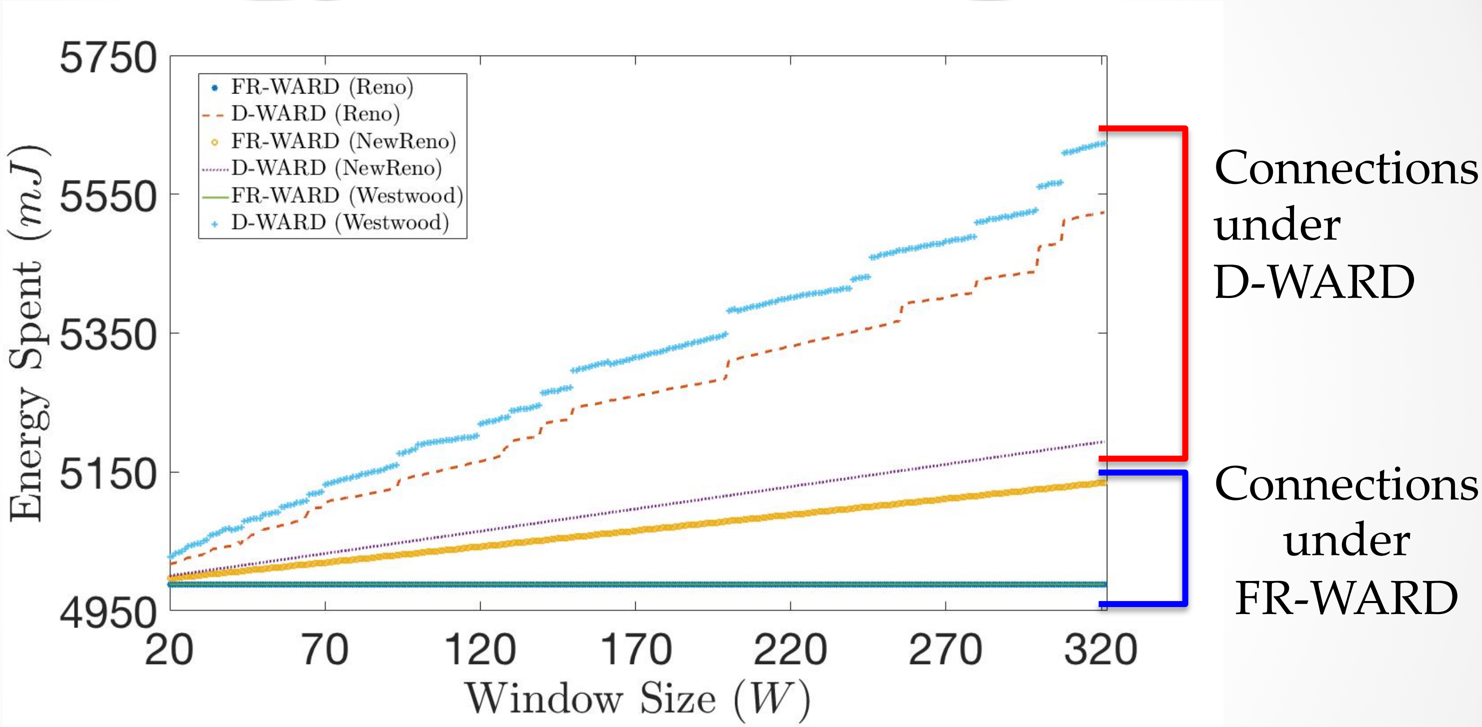
- As the window size (at the time of the attack detection), increases, D-WARD drops more packets initially
  - FR-WARD never drops suspicious traffic, and causes close to zero retransmissions
- On average, FR-WARD reduces retransmissions by a factor of 203

Effects on Benign Traffic: Goodput



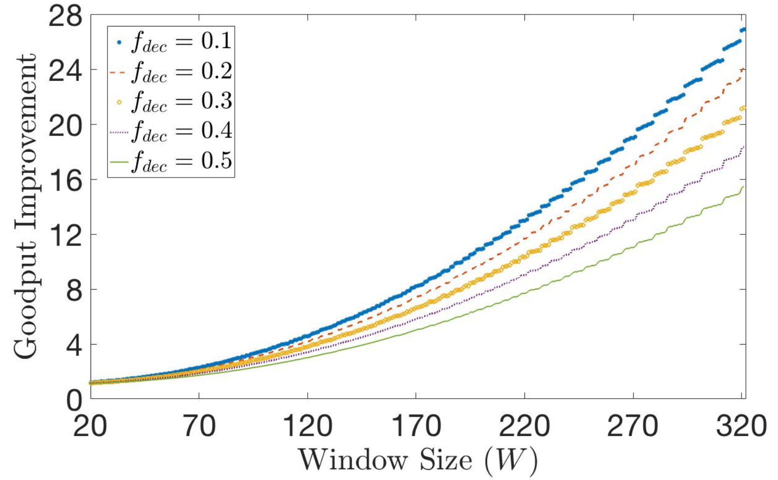
- As D-WARD drops more packets, it also causes the connection to slow down
  - Muddled with retransmissions, time wasted waiting for negative ACKs
- On average, FR-WARD increases goodput by a factor of
- 3.8

Effects on Benign Traffic: Energy Consumption

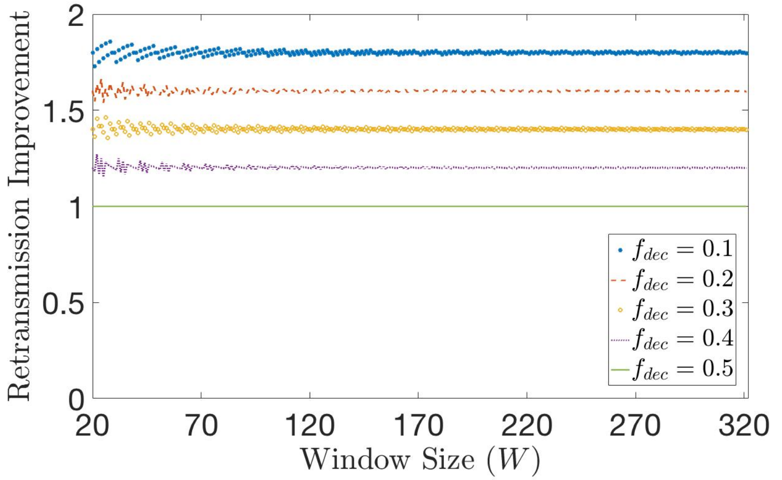


- Because FR-WARD reduces retransmissions, a benign device consumes much less energy than under D-WARD
  - Less packet transmission
- Because FR-WARD increases goodput, a benign device consumes much less energy than under D-WARD
  - Less active transmission time

Effects on Benign Traffic: D-WARD Parameters



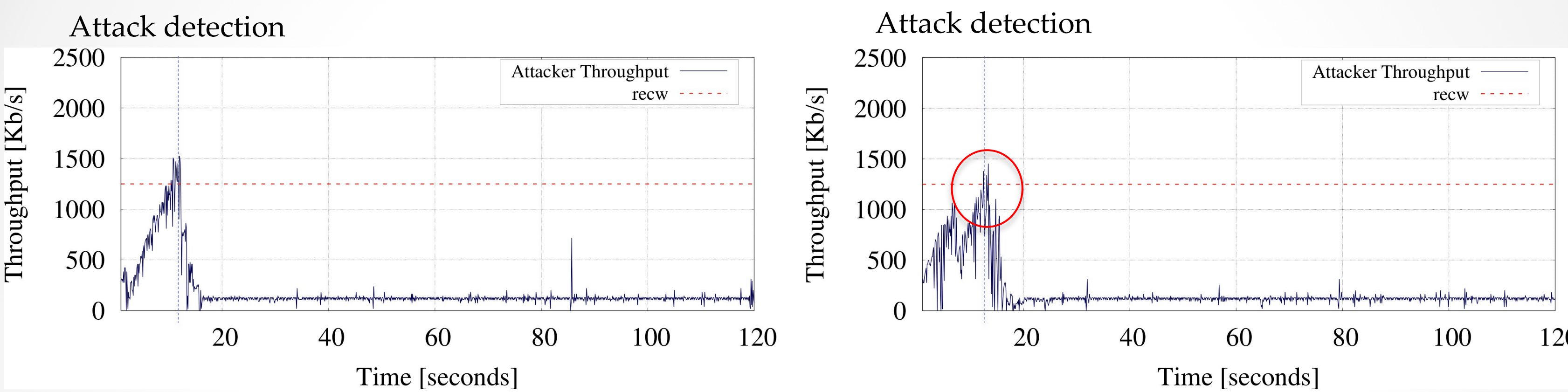
(c) The magnitude FR-WARD improves Goodput under TCP NewReno.



(c) The magnitude FR-WARD improves retransmissions under TCP NewReno.

- We evaluate the effect of D-WARD's parameter, fdec
  - fdec 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

Effects on Malicious Traffic

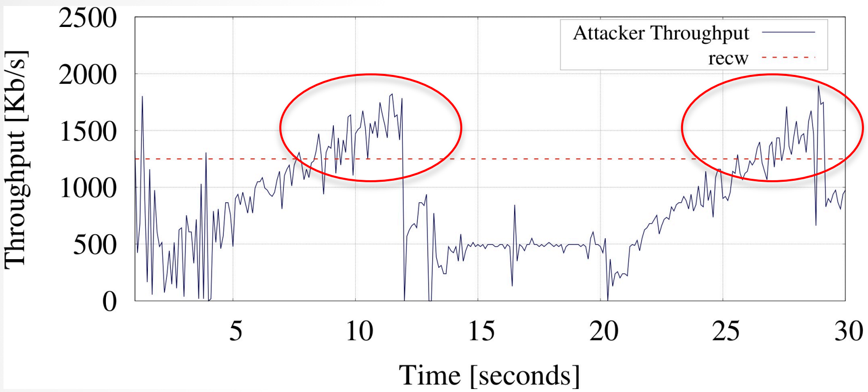


(a) The throughput of a naive attacker under D-WARD.

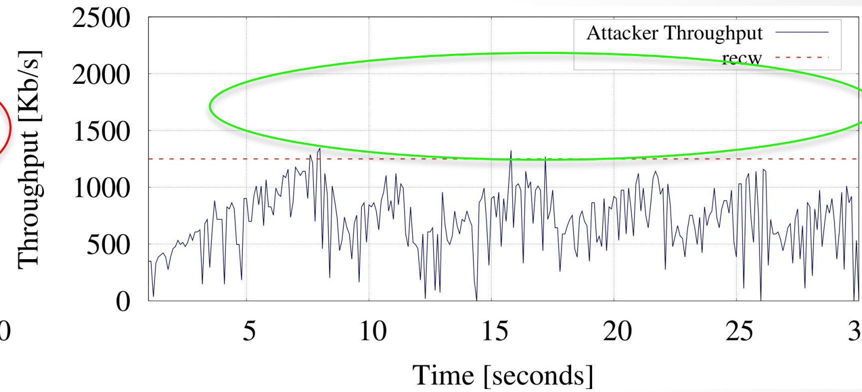
(d) The throughput of a naive attacker under FR-WARD.

- 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

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:
  - Devkishen Sisodia, Jun Li, and Hasan Cam

- For more details, check out our publication:
  - Mergendahl, S., Sisodia, D., Li, J., & Cam, H. (2018, July). FR-WARD: Fast Retransmit as a Wary but Ample Response to Distributed Denial-of-Service Attacks from the Internet of Things. *In 27th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-9). IEEE.

- Thank you for listening!