Defending Against New-Flow Attack in SDN-Based Internet of Things

Xu, Gau, Dong, Zhang, Heng FOH, Chao

Presented by: Preston Barbare, Tyler Wagner, Taylor Morris

Overview

- IoT
- Software Defined Networks, SDNs
- New Flow Attacks
- Smart Security Mechanism, SSM
- Conclusion
- Research Proposal

IoT: Internet of Things

- Infrastructure of interconnected smart devices
- Can collect and exchange data with each other and to the Internet
- Has many promises

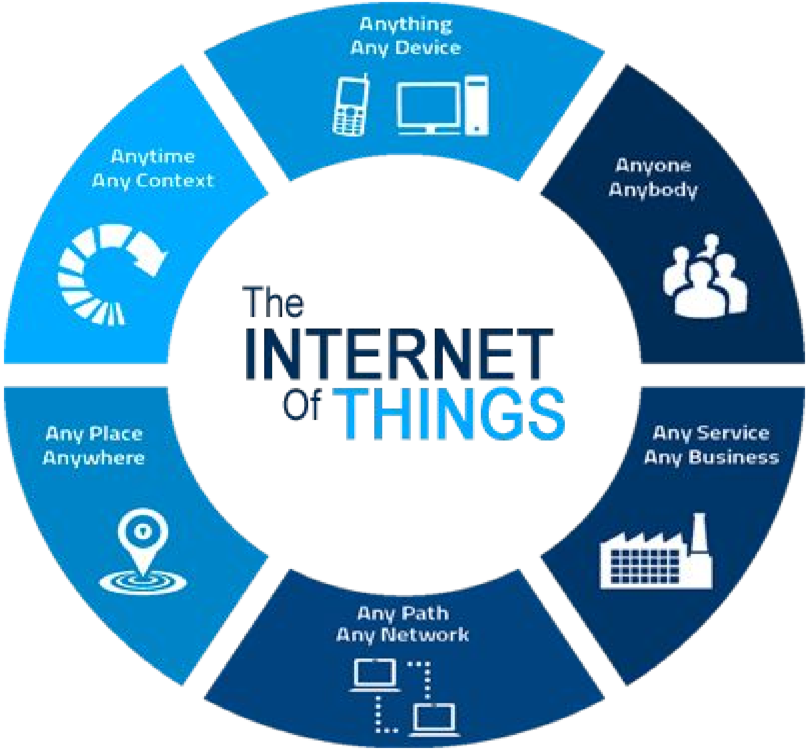


Photo Credit to: Intersog

The ‘Things’

Cyber Systems

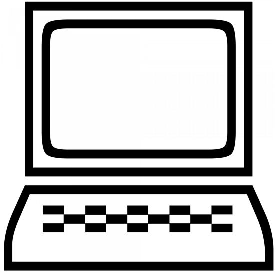


Photo Credit: Public
Domain Pictures

Photo Credit: MC Server Hosting

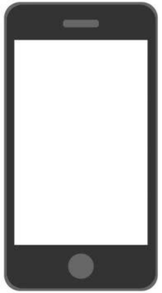


Photo Credit: Shutterstock

Cyber-Physical Systems

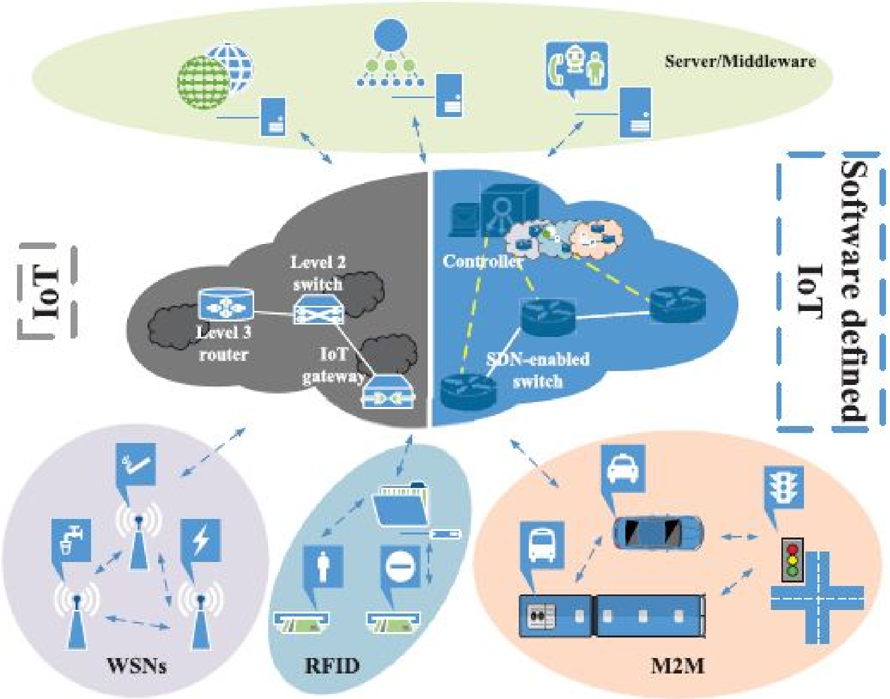
MR-Magic Smart Lightbulb

Kuka Manipulator

GOJI Smart Door Lock

SDN: Software Defined Network

- A newer approach to computer networking
- Paved the way to connect the many protocols in IoT
- Allows an easily customizable and dynamic change of network behavior
    - Higher flexibility and scalability of networking resources



SDN’s Problem

- Cyber attacks have cut the link between the devices and servers of IoT
  - Infrastructure layer DoS attack
  - Controller-switch communication flooding
  - Switch flow table flooding

The SDN Architecture, OpenFlow Protocol, and the New Flow Attack

SDN Layout

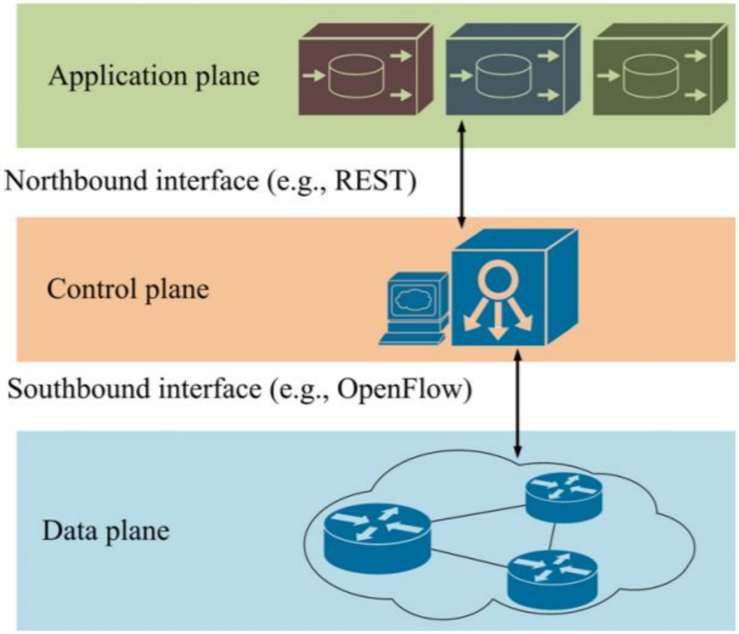

Application plane
Northbound interface (e.g., REST)
Control plane
Southbound interface (e.g., OpenFlow)
Data plane

FIGURE 2. The SDN architecture.

- Idea: split up control and data
- 3 layers
  - Application
  - Control
  - Data/Switches
- North and South communications interfaces

OpenFlow Protocol (Southbound)

- Allows control and data to be split up
  - Switches send info about flows to control plane
  - Control plane sends instructions for handling flows to switches
- Asynchronous Messages
  - Packet-In Message
  - Flow Removed Message
- Controller-to-Switch Messages
  - Multi-part, statistics gathering

New Flow Attack

- Similar to DoS attacks
- Execution:
  - Send unmatched packet
  - Packet-in message sent to control
  - New flow entry created
  - Controller-to-Switch messages sent to switches
  - Repeat
- New Flow attack test attempt

Smart Security Mechanism (SSM)

SSM (Smart Security Mechanism)

Resides in the application layer

Monitors & Mitigates

- New-flow Attack
- Via standard southbound and northbound interfaces

Recall...

Architecture:

Application Plane

Control Plane

Data Plane

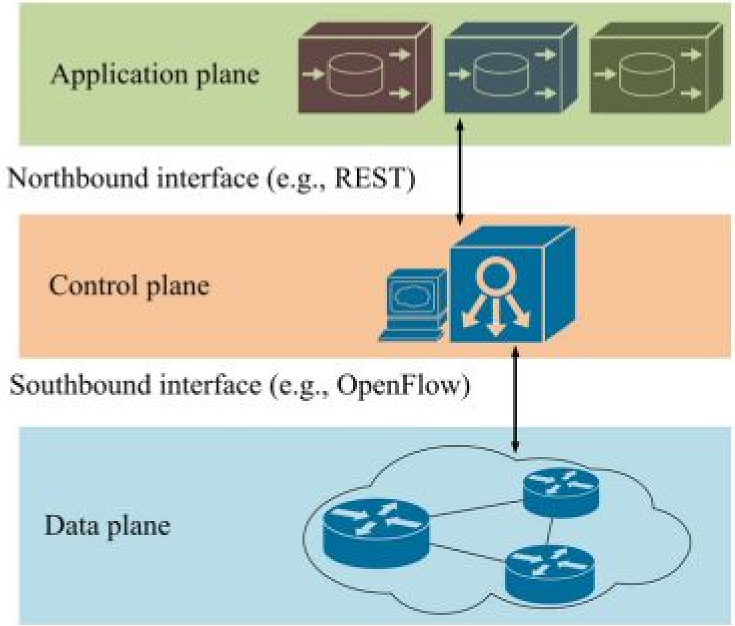

Application plane
Northbound interface (e.g., REST)
Control plane
Southbound interface (e.g., OpenFlow)
Data plane

FIGURE 2. **The SDN architecture.**

Recall…

Unmatched Packets

- Packet-in-message
- Flow removed message
- Multipart Message

What SSM attempts to prevent

New Flow Attack

- Unmatched Packets
    - Sends packet-in message as well as controller-to-switch message

SSM (Smart Security Mechanism): two parts

Detection Module

- Monitors new-flow attack by listening to Asynchronous Messages on control link
- Notifies Mitigation Module

Mitigation Module

- Assigns dynamic access control rules

SSM: Detection Module

Challenges:

- TCP nor IP handles arbitrary packets
- Monitoring cost is limited
- Must give info to mitigation process quickly

SSM: Detection Module

Compare

- Request rate of switch
- Match efficiency of switch

Differentiates between

- New-Flow attack
- Normal flow burst

SSM: Detection Module

1. Establish baselines (during no sign of attacks)
2. Determine the victim port location

SSM: Mitigation Module

Challenge:

- Cannot assign a flow entry for each attack flow

Solution:

- Redirect suspicious flows from the victim port to security middleware

SSM: Mitigation Module

Challenge:

- With redirected suspicious flows in the security middleware,
  - Security middleware cannot report filtering logs to controller via Southbound interface

Solution:

- Gather all outports to the security middleware
- Gather all inports from the security middleware
- Compare the packets of the outport vs. inport to determine illegal/malicious packets

Conclusion

- The IoT is become extremely popular
- Software-Defined Networks paved a way to connect the heterogeneous connection types
  - Downfalls on security
- Smart Security Module adds additional security components to the SDNs
  - Low-cost and easily implementable

Research Proposal

Problem

- IoT Smart Device Security

Proposed Solution

- Finding the best security scheme for these smart devices in IoT setting
  - Applying industrial grade best practices
- Encourage vendors to ship smart devices to consumers with this security

Questions
?

References

- T. Xu, D. Gao, P. Dong, H. Zhang, C. H. Foh and H. C. Chao, "Defending Against New-Flow Attack in SDN-Based Internet of Things," in *IEEE Access*, vol. 5, no. , pp. 3431-3443, 2017.