Demystifying and exploiting IoT Timeout Behaviors in Smart Home

Chenglong Fu

Assistant Professor

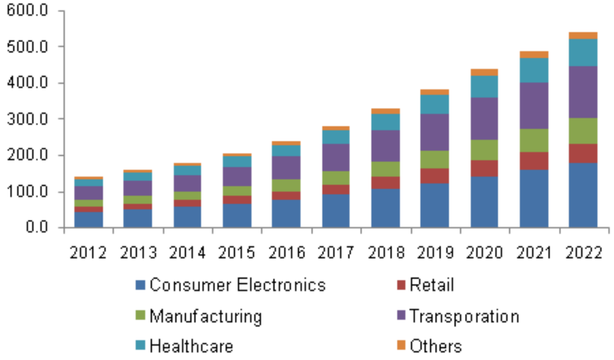
Department of Software and Information Systems

UNC Charlotte

chenglong.fu@uncc.edu

CHARLOTTE
COLLEGE OF COMPUTING AND INFORMATICS

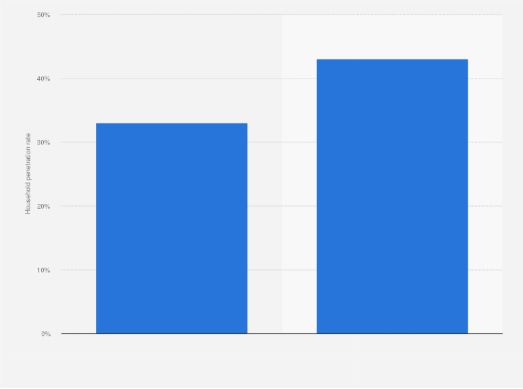
CAE
IN CYBERSECURITY
COMMUNITY



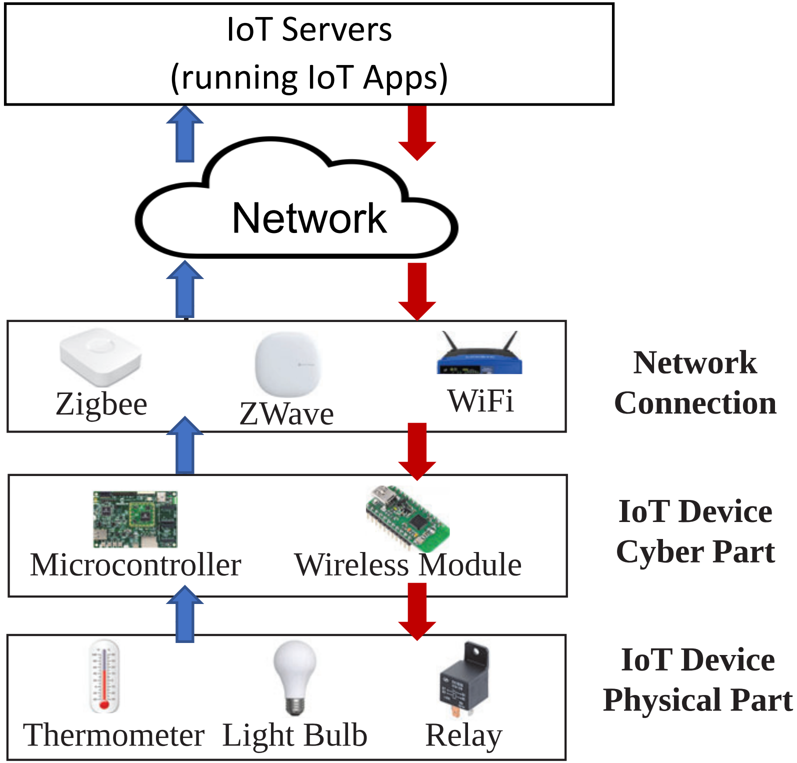
Global Internet of Things (IoT) Market Size To Hit USD 1,842 Billion by 2028 at a 24.5% CAGR Growth (with COVID-19 Analysis): Facts & Factors

Booming of the Internet of Things Market

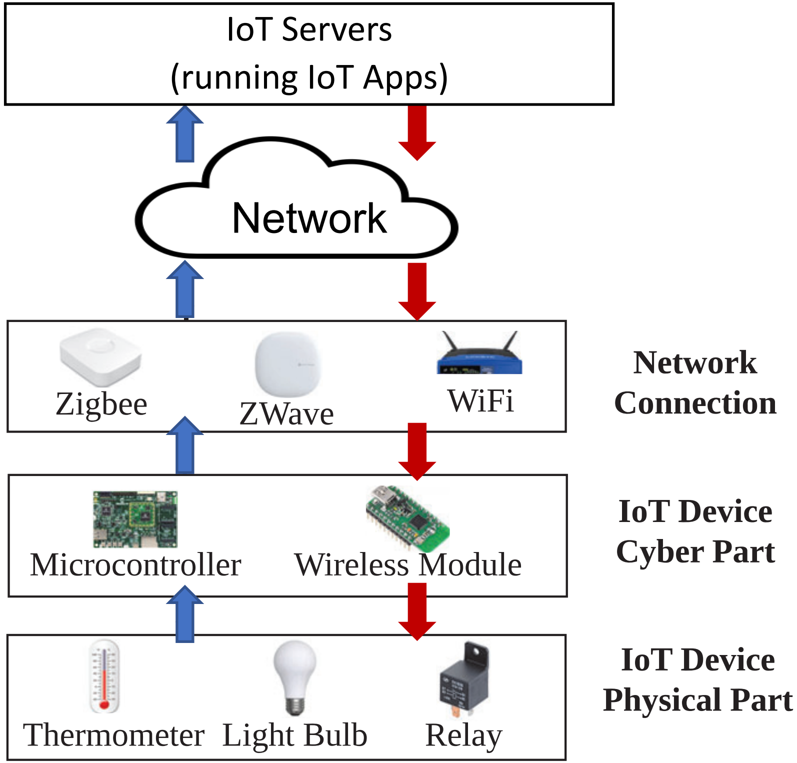
- More than 10 billion active IoT devices
- $400 billion IoT market size
- 43% smart home device household penetration rate



Background: IoT Architecture

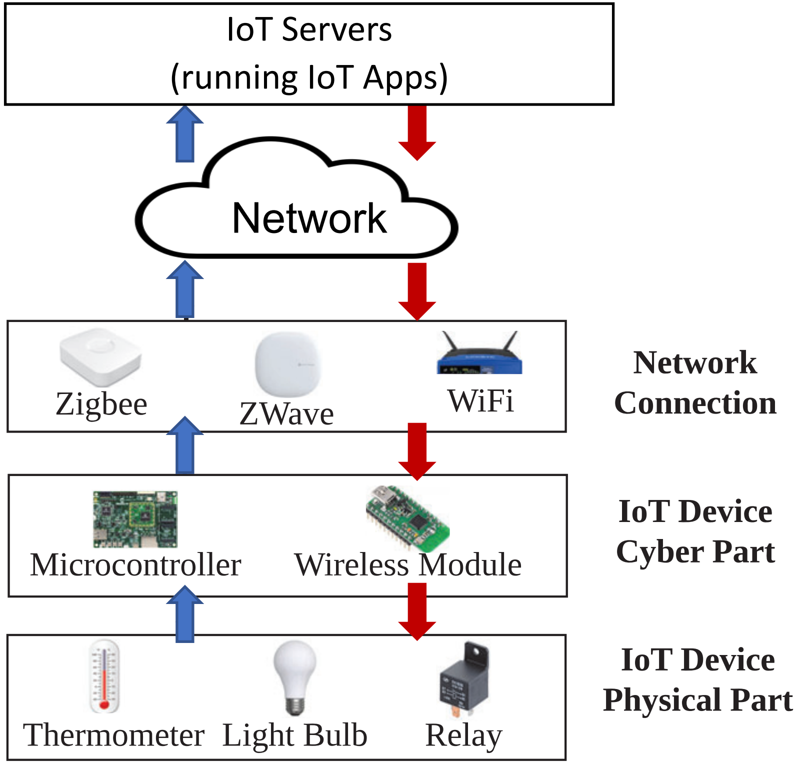


Background: IoT Architecture



- ⬆ IoT Event
  - E.g., lock status
  - Flow from device to server
- ⬇ IoT Command
  - E.g., unlock door
  - Flow from server to device

Background: IoT Architecture



IoT Servers
(running IoT Apps)

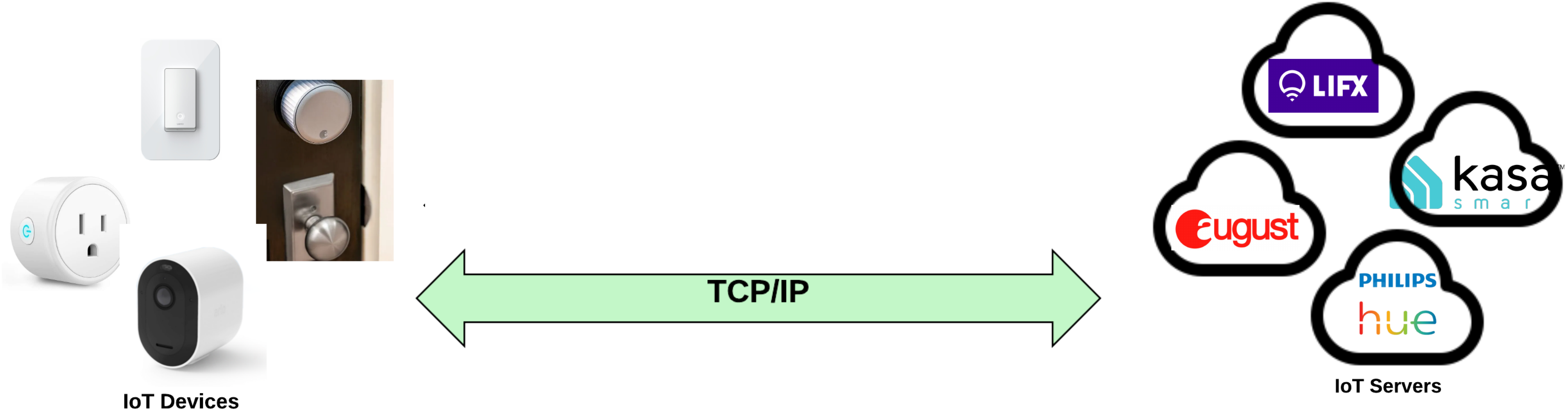
Network

Zigbee ZWave WiFi — Network Connection

Microcontroller Wireless Module — IoT Device Cyber Part

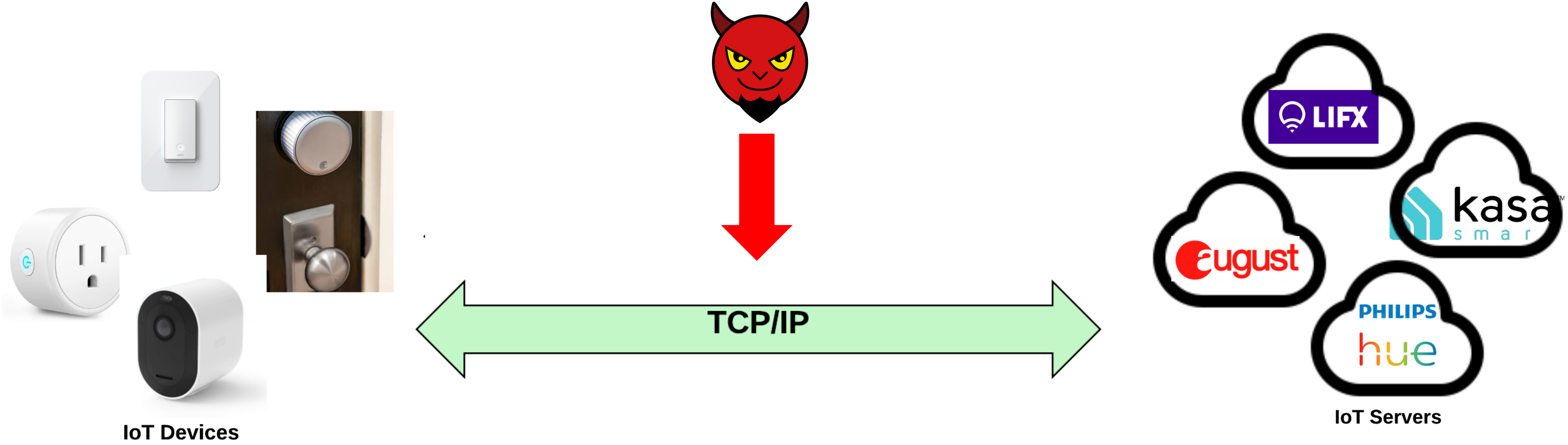
Thermometer Light Bulb Relay — IoT Device Physical Part

- ⬆ IoT Event
  - E.g., lock status
  - Flow from device to server
- ⬇ IoT Command
  - E.g., unlock door
  - Flow from server to device
- IoT App (aka, smart app/routine/rule)
  - **Trigger**: *when motion-on* ***(event)*** *is received*
  - **Condition:** *if presence sensor is present*
  - **Action:** *turn off indoor-camera* ***(command)***



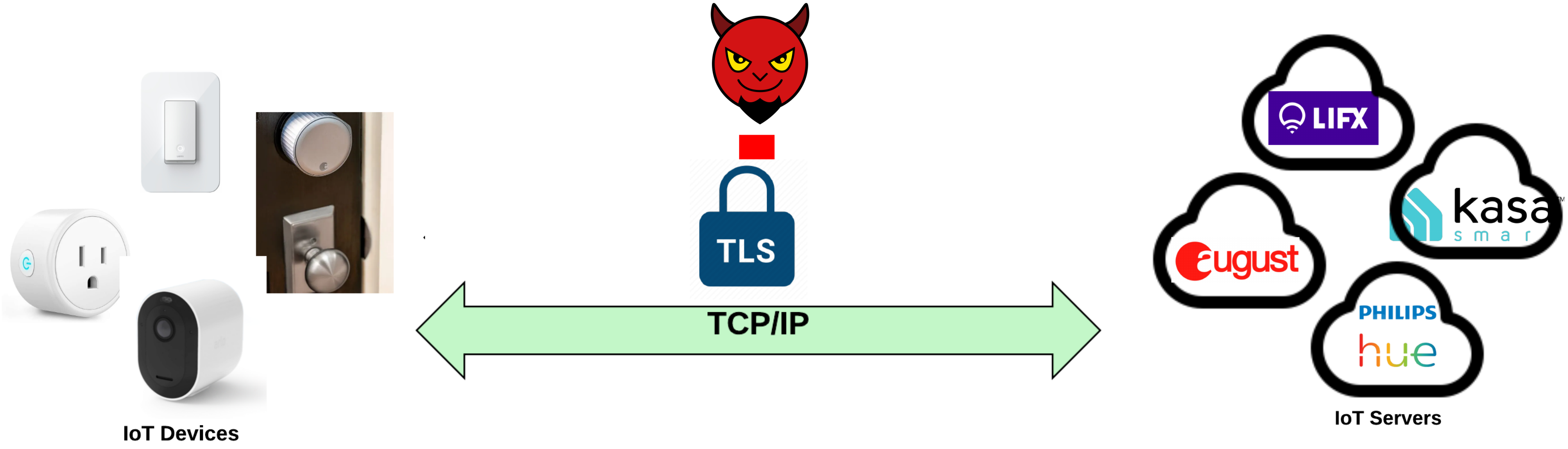
74% of IoT devices use TCP/IP

Zigbee and ZWave devices are connected to IoT hubs, which also use TCP/IP



74% of IoT devices use TCP/IP

Zigbee and ZWave devices are connected
to IoT hubs, which also use TCP/IP

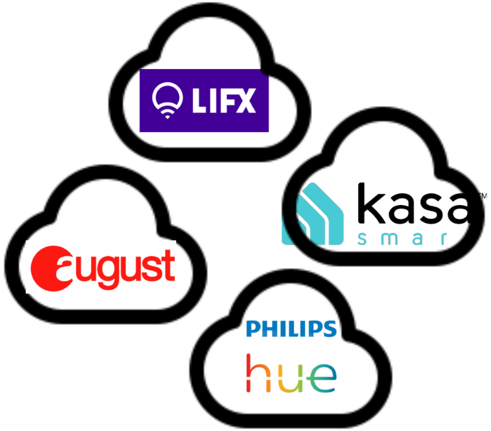


Message Integrity Protection

Tampering attempts: alert, session termination

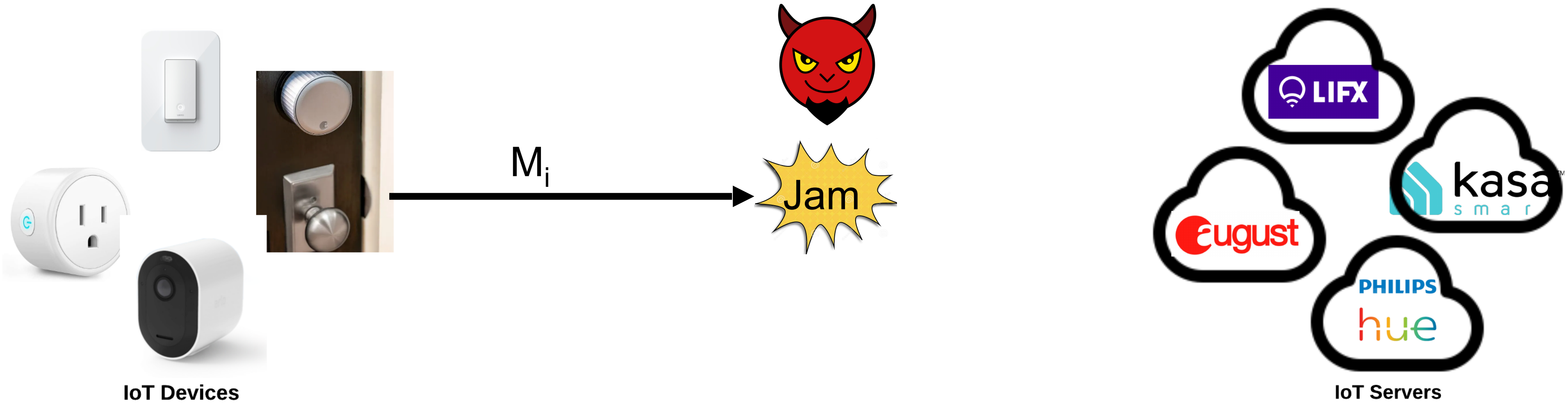
TLS Message Integrity Protection

IoT Devices



IoT Servers

TLS Message Integrity Protection



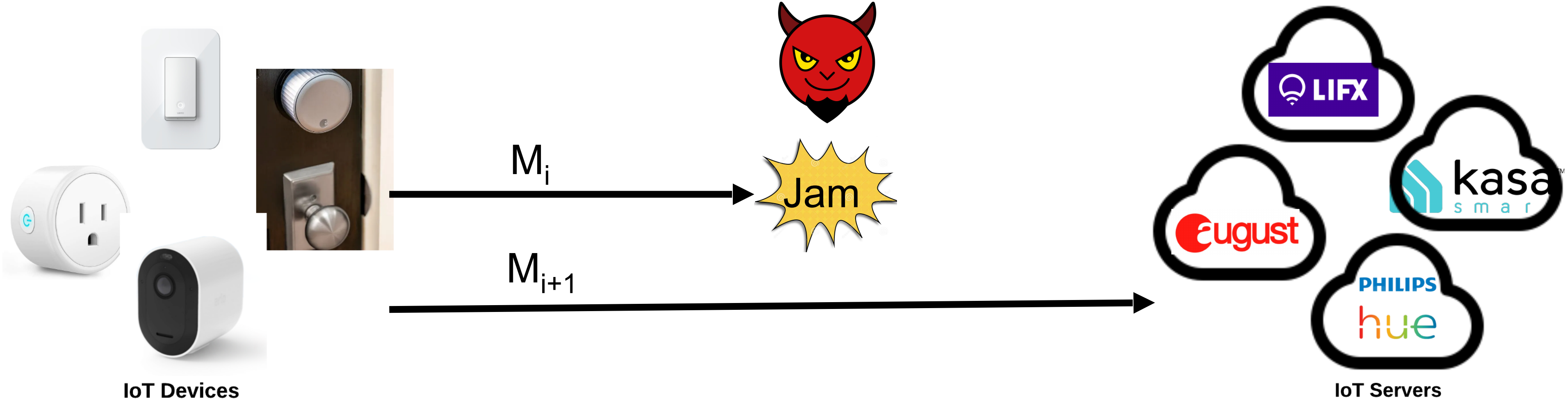
M_i

Jam

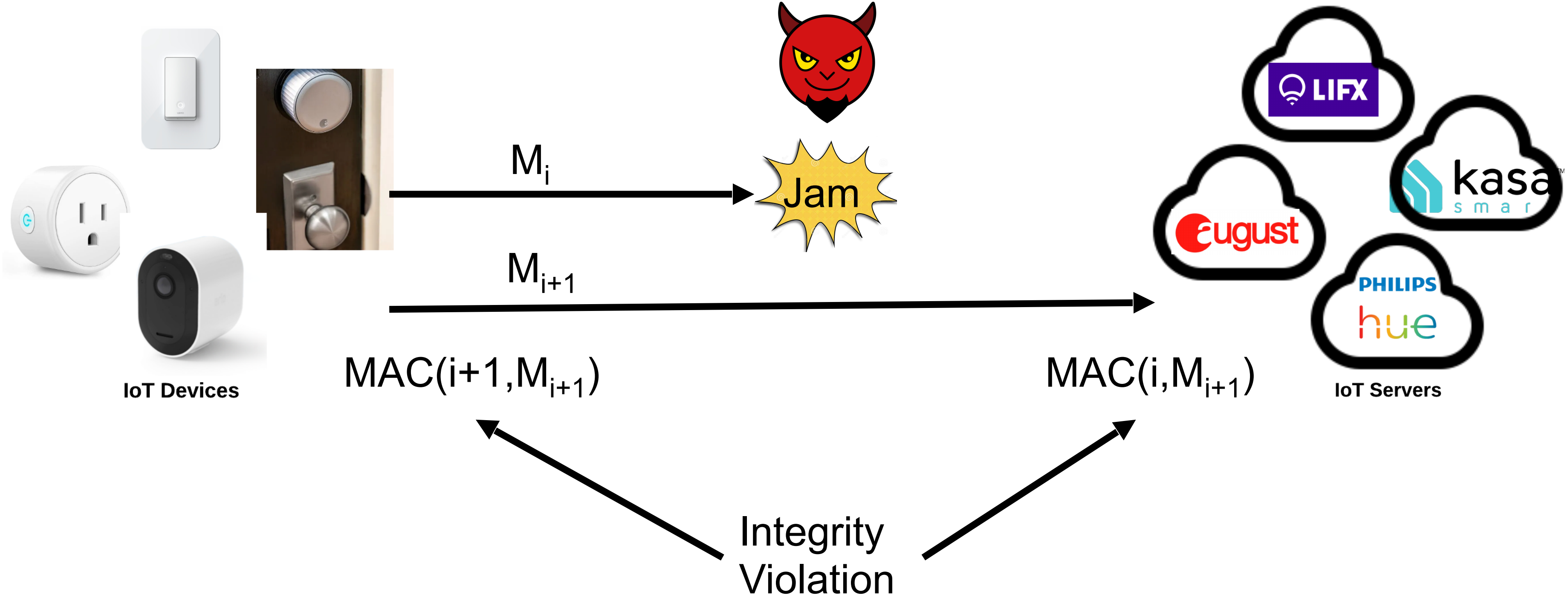
IoT Devices

IoT Servers

TLS Message Integrity Protection



TLS Message Integrity Protection



IoT Devices

M_i

Jam

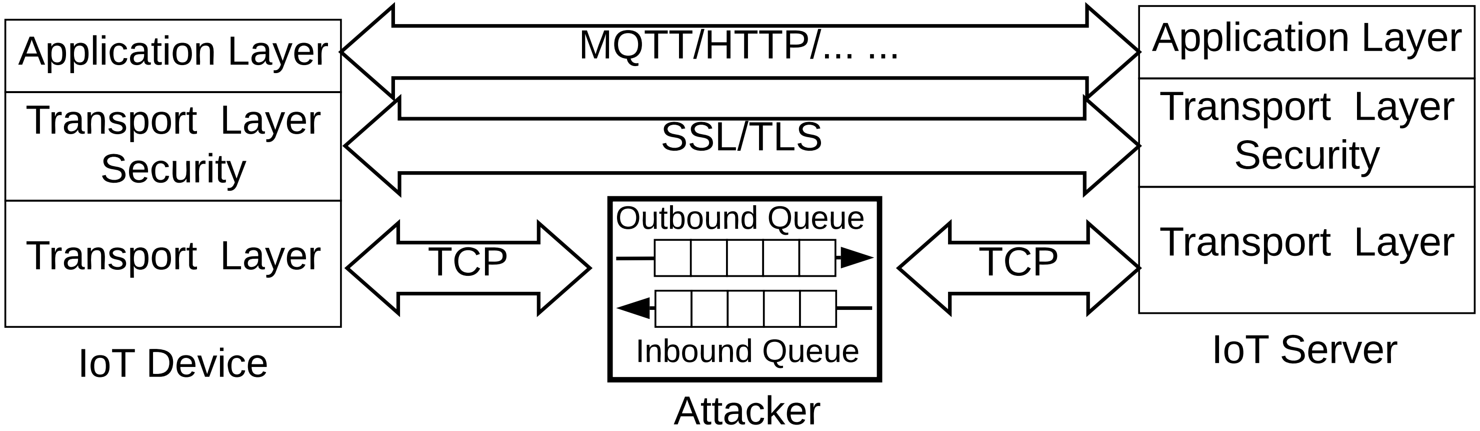
M_{i+1}

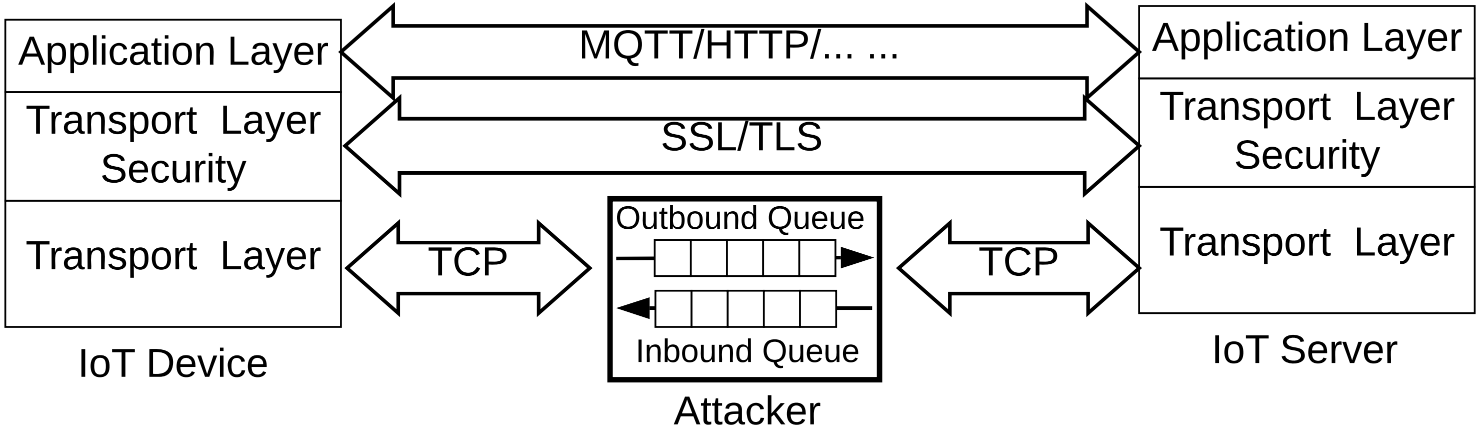
$\mathrm{MAC}(i+1, M_{i+1})$

$\mathrm{MAC}(i, M_{i+1})$

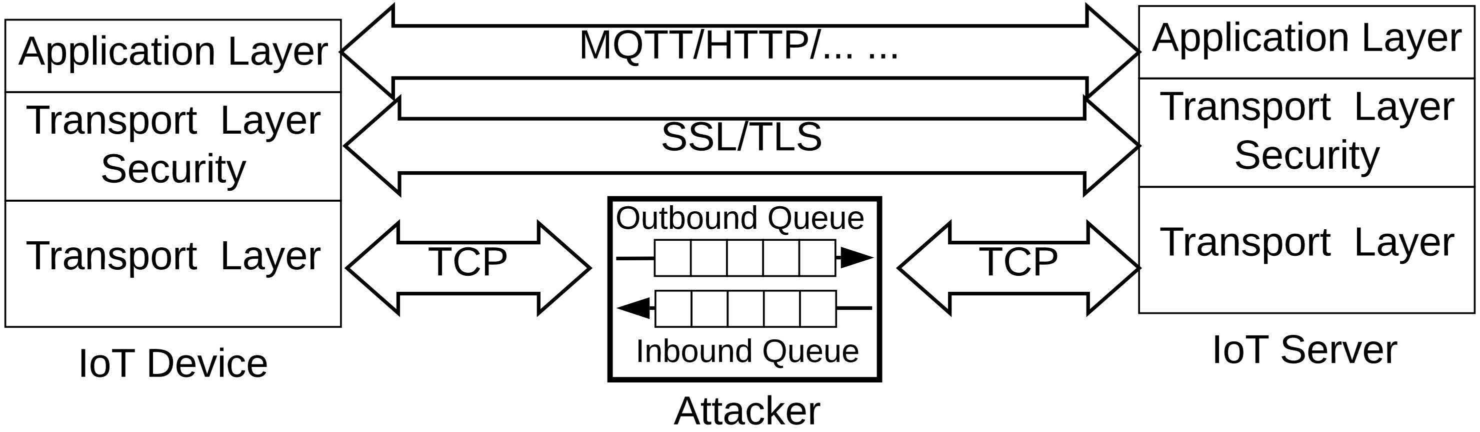
IoT Servers

Integrity Violation

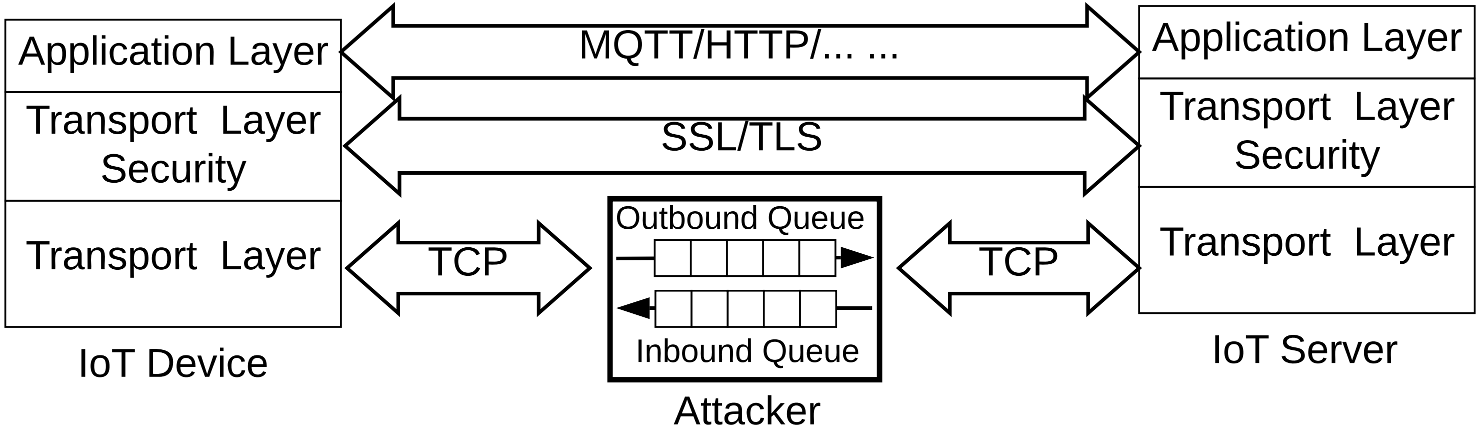

Application Layer
MQTT/HTTP/... ...
Application Layer
Transport Layer Security
SSL/TLS
Transport Layer Security
Transport Layer
TCP
Outbound Queue
Inbound Queue
TCP
Transport Layer
IoT Device
Attacker
IoT Server



- TCP
  - *"picky"* about delay



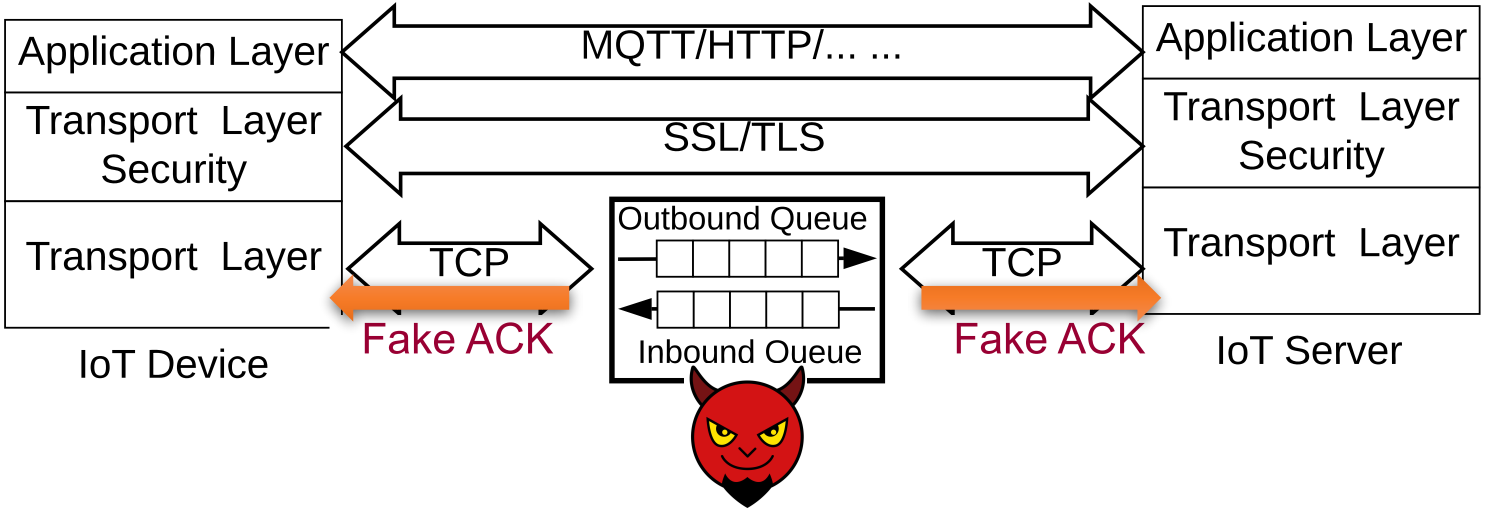
- TCP
  - *“picky”* about delay
- TLS (Transport Layer Security)
  - Cannot drop, inject, modify or disorder data packets

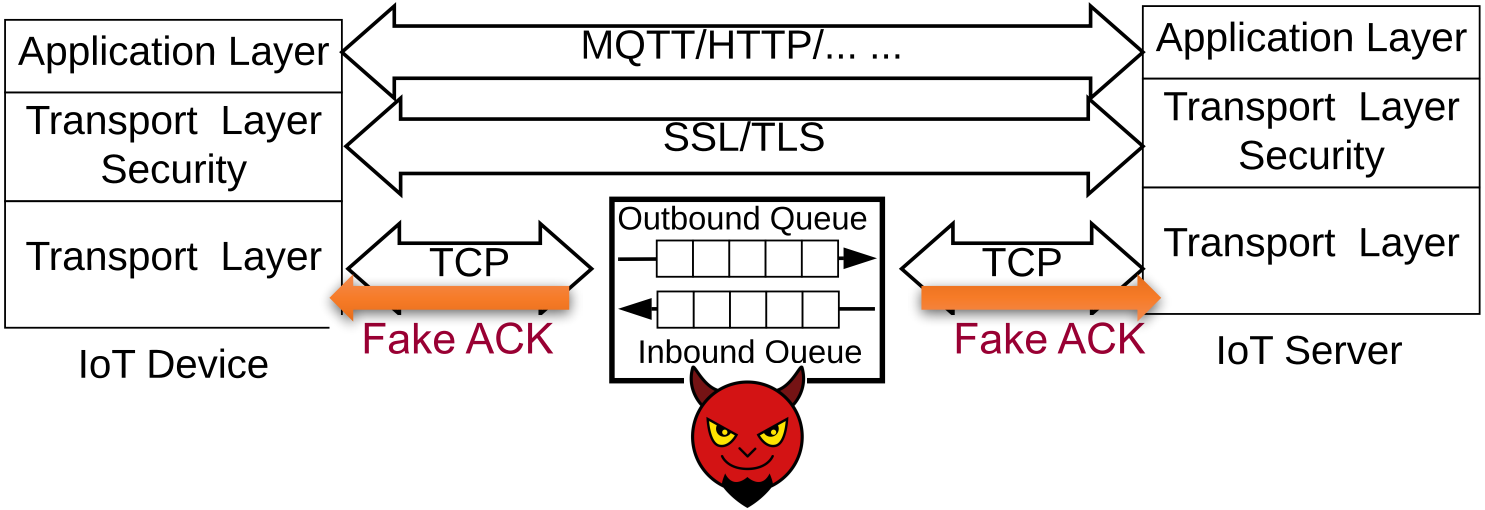


- TCP
  - *"picky"* about delay
- TLS (Transport Layer Security)
  - Cannot drop, inject, modify or disorder data packets

Key Insight 1:

Delay detection in the TCP layer is decoupled from data protection by TLS


Application Layer
Transport Layer Security
Transport Layer
IoT Device
MQTT/HTTP/... ...
SSL/TLS
TCP
Fake ACK
Outbound Queue
Inbound Queue
TCP
Fake ACK
Application Layer
Transport Layer Security
Transport Layer
IoT Server



What if the attacker injects fake TCP ACK packets and delays TLS packets?

TCP will not complain!

TLS will not complain either!

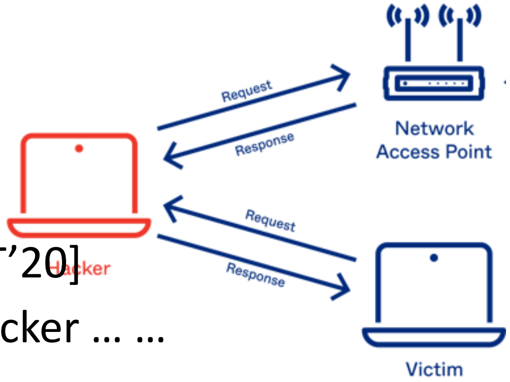
The delay is only constrained by the Application layer, which we find is quite **insensitive** to delay

Questions…

- How to hijack the TCP traffic?

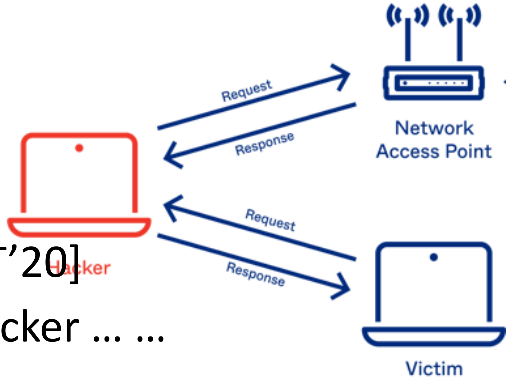
Questions…

- How to hijack the TCP traffic?
  - ARP spoofing: easy to launch [IoTInspector: IMWUT’20]
  - Shared network, Hotel, office, campus, remote attacker … …
- How to infer IoT messages from encrypted traffic?



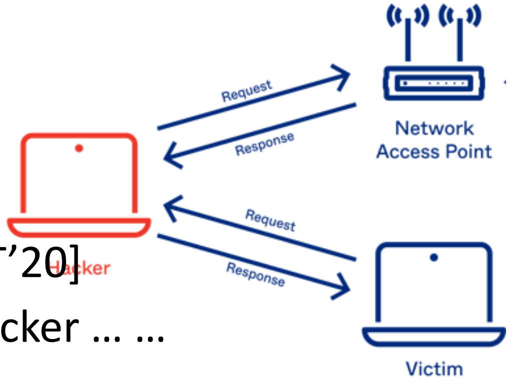
Questions…

- How to hijack the TCP traffic?
  - <u>ARP spoofing</u>: easy to launch [IoTInspector: IMWUT'20]
  - Shared network, Hotel, office, campus, remote attacker … …
- How to infer IoT messages from encrypted traffic?
  - <u>Side-channel attacks</u>: *packet length, DNS query, …*
  - Accuracy: 97% [PingPong: NDSS'20]
- What is the delay constraint imposed on the App layer?

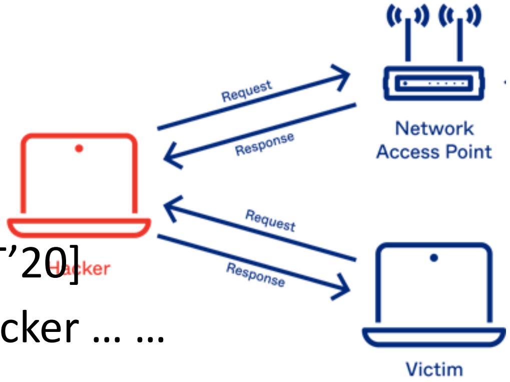


Questions…

- How to hijack the TCP traffic?
  - ARP spoofing: easy to launch [IoTInspector: IMWUT’20]
  - Shared network, Hotel, office, campus, remote attacker … …
- How to infer IoT messages from encrypted traffic?
  - Side-channel attacks: *packet length, DNS query, …*
  - Accuracy: 97% [PingPong: NDSS’20]
- What is the delay constraint imposed on the App layer?
  - Challenges: diverse IoT devices + proprietary protocols



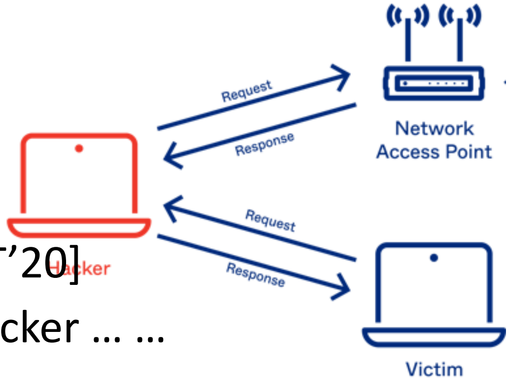
Questions…



- How to hijack the TCP traffic?
    - ARP spoofing: easy to launch [IoTInspector: IMWUT'20]
    - Shared network, Hotel, office, campus, remote attacker … …
- How to infer IoT messages from encrypted traffic?
    - Side-channel attacks: *packet length, DNS query, …*
    - Accuracy: 97% [PingPong: NDSS'20]
- What is the delay constraint imposed on the App layer?
    - Challenges: diverse IoT devices + proprietary protocols
    - The first large-scale study of IoT timeout behavior

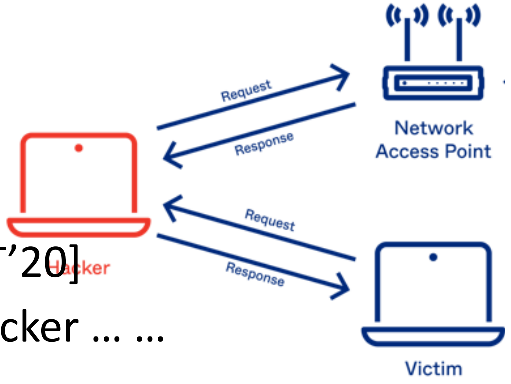
Questions…

- How to hijack the TCP traffic?
  - ARP spoofing: easy to launch [IoTInspector: IMWUT’20]
  - Shared network, Hotel, office, campus, remote attacker … …
- How to infer IoT messages from encrypted traffic?
  - Side-channel attacks: *packet length, DNS query, …*
  - Accuracy: 97% [PingPong: NDSS’20]
- What is the delay constraint imposed on the App layer?
  - Challenges: diverse IoT devices + proprietary protocols
  - The first large-scale study of IoT timeout behavior
    - A normal message must be ack-ed within a threshold?

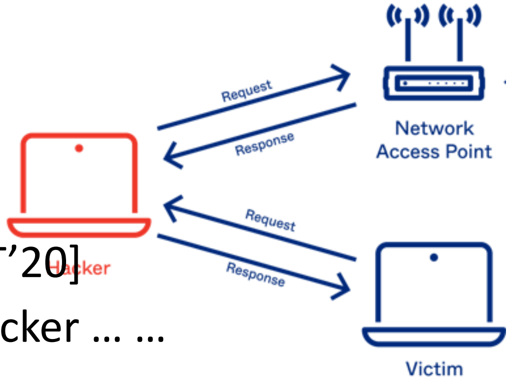


Questions…

- How to hijack the TCP traffic?
  - ARP spoofing: easy to launch [IoTInspector: IMWUT’20]
  - Shared network, Hotel, office, campus, remote attacker … …
- How to infer IoT messages from encrypted traffic?
  - Side-channel attacks: *packet length, DNS query, …*
  - Accuracy: 97% [PingPong: NDSS’20]
- What is the delay constraint imposed on the App layer?
  - Challenges: diverse IoT devices + proprietary protocols
  - The first large-scale study of IoT timeout behavior
    - A normal message must be ack-ed within a threshold?
    - A keep-alive message must be ack-ed within a threshold?



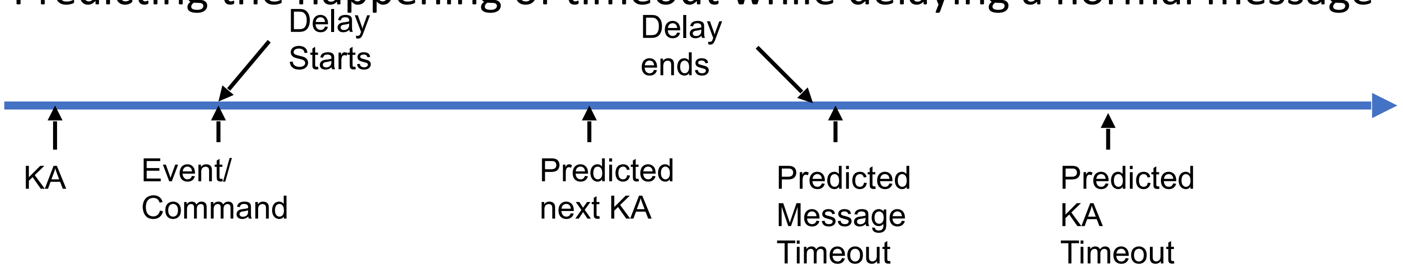
Questions…

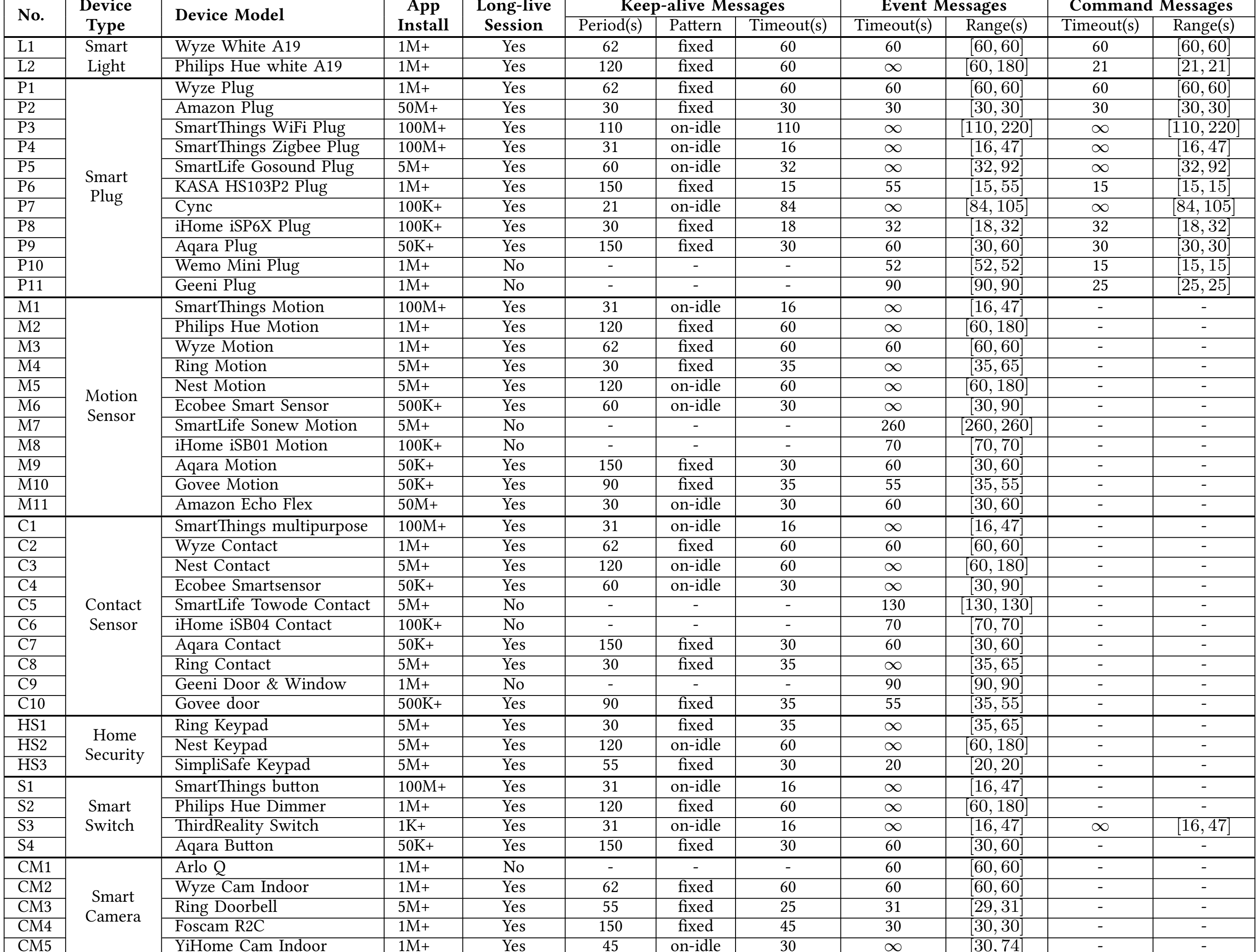


- How to hijack the TCP traffic?
  - ARP spoofing: easy to launch [IoTInspector: IMWUT’20]
  - Shared network, Hotel, office, campus, remote attacker … …
- How to infer IoT messages from encrypted traffic?
  - Side-channel attacks: *packet length, DNS query, …*
  - Accuracy: 97% [PingPong: NDSS’20]
- What is the delay constraint imposed on the App layer?
  - Challenges: diverse IoT devices + proprietary protocols
  - The first large-scale study of IoT timeout behavior
    - A normal message must be ack-ed within a threshold?
    - A keep-alive message must be ack-ed within a threshold?
    - Categorization?

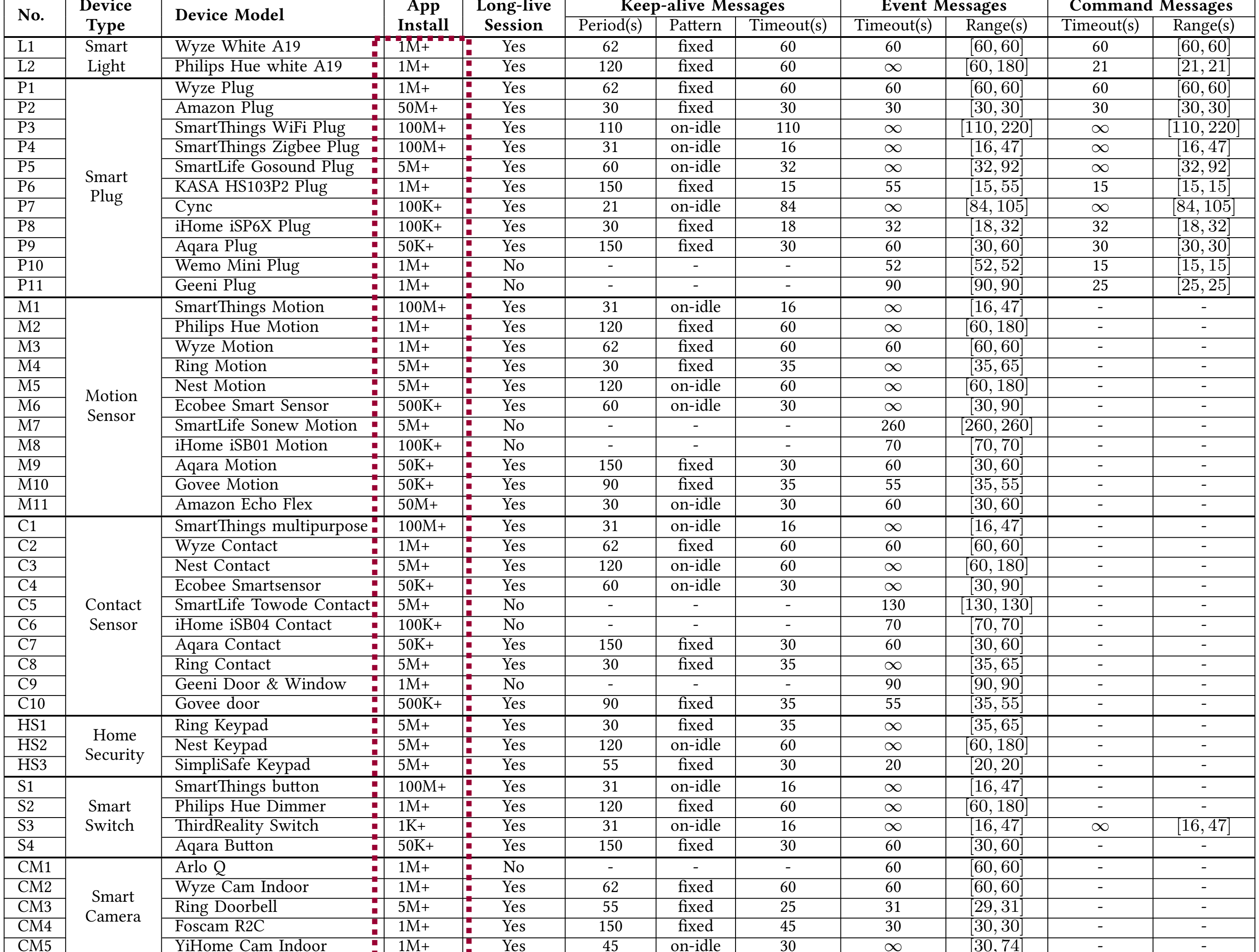
Application Layer Timeout Behavior

- Two types of messages
  - Normal messages: on occurring of events/commands
  - Keep-alive messages: periodically exchanged
- Timeout Behavior Measurement
  - Keep-alive pattern: on-idle/periodic, length of period
  - Message timeout
    - Normal message timeout
    - Keep-alive message timeout
- Predicting the happening of timeout while delaying a normal message

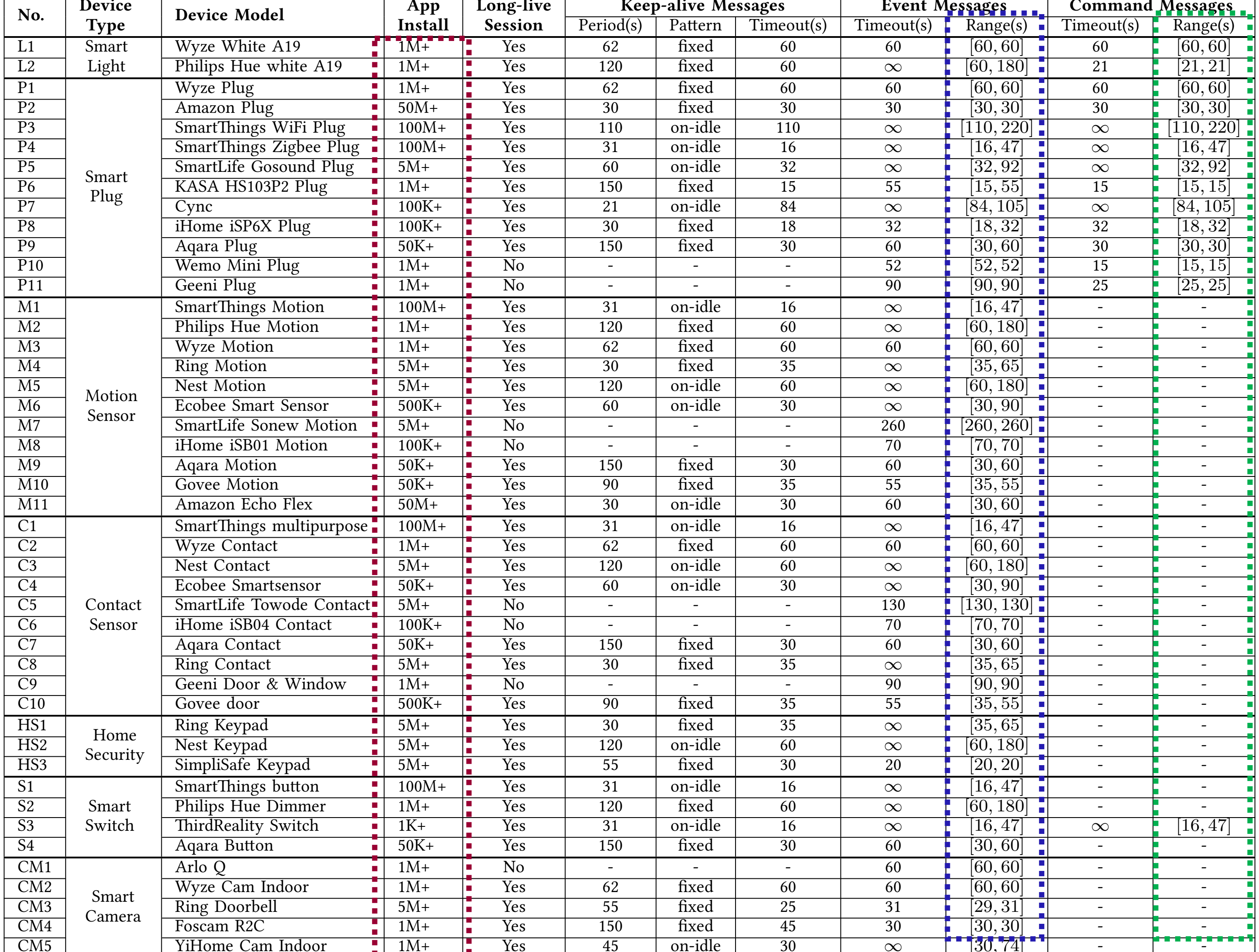




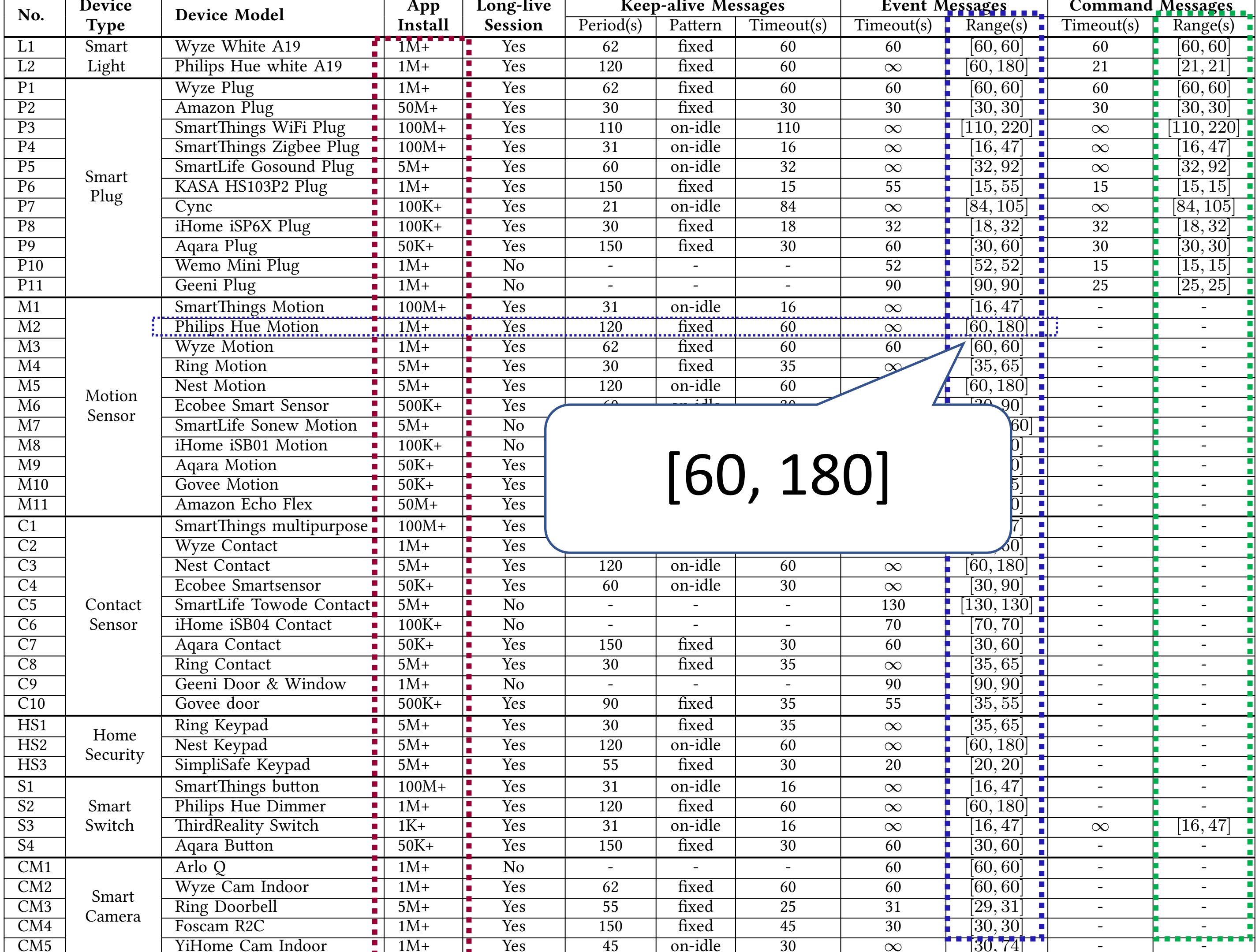
No.	Device Type	Device Model	App Install	Long-live Session	Keep-alive Messages			Event Messages		Command Messages	
					Period(s)	Pattern	Timeout(s)	Timeout(s)	Range(s)	Timeout(s)	Range(s)
L1	Smart Light	Wyze White A19	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
L2		Philips Hue white A19	1M+	Yes	120	fixed	60	∞	[60, 180]	21	[21, 21]
P1	Smart Plug	Wyze Plug	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
P2		Amazon Plug	50M+	Yes	30	fixed	30	30	[30, 30]	30	[30, 30]
P3		SmartThings WiFi Plug	100M+	Yes	110	on-idle	110	∞	[110, 220]	∞	[110, 220]
P4		SmartThings Zigbee Plug	100M+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
P5		SmartLife Gosound Plug	5M+	Yes	60	on-idle	32	∞	[32, 92]	∞	[32, 92]
P6		KASA HS103P2 Plug	1M+	Yes	150	fixed	15	55	[15, 55]	15	[15, 15]
P7		Cync	100K+	Yes	21	on-idle	84	∞	[84, 105]	∞	[84, 105]
P8		iHome iSP6X Plug	100K+	Yes	30	fixed	18	32	[18, 32]	32	[18, 32]
P9		Aqara Plug	50K+	Yes	150	fixed	30	60	[30, 60]	30	[30, 30]
P10		Wemo Mini Plug	1M+	No	-	-	-	52	[52, 52]	15	[15, 15]
P11		Geeni Plug	1M+	No	-	-	-	90	[90, 90]	25	[25, 25]
M1	Motion Sensor	SmartThings Motion	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
M2		Philips Hue Motion	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
M3		Wyze Motion	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
M4		Ring Motion	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
M5		Nest Motion	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
M6		Ecobee Smart Sensor	500K+	Yes	60	on-idle	30	∞	[30, 90]	-	-
M7		SmartLife Sonew Motion	5M+	No	-	-	-	260	[260, 260]	-	-
M8		iHome iSB01 Motion	100K+	No	-	-	-	70	[70, 70]	-	-
M9		Aqara Motion	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
M10		Govee Motion	50K+	Yes	90	fixed	35	55	[35, 55]	-	-
M11		Amazon Echo Flex	50M+	Yes	30	on-idle	30	60	[30, 60]	-	-
C1	Contact Sensor	SmartThings multipurpose	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
C2		Wyze Contact	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
C3		Nest Contact	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
C4		Ecobee Smartsensor	50K+	Yes	60	on-idle	30	∞	[30, 90]	-	-
C5		SmartLife Towode Contact	5M+	No	-	-	-	130	[130, 130]	-	-
C6		iHome iSB04 Contact	100K+	No	-	-	-	70	[70, 70]	-	-
C7		Aqara Contact	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
C8		Ring Contact	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
C9		Geeni Door & Window	1M+	No	-	-	-	90	[90, 90]	-	-
C10		Govee door	500K+	Yes	90	fixed	35	55	[35, 55]	-	-
HS1	Home Security	Ring Keypad	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
HS2		Nest Keypad	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
HS3		SimpliSafe Keypad	5M+	Yes	55	fixed	30	20	[20, 20]	-	-
S1	Smart Switch	SmartThings button	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
S2		Philips Hue Dimmer	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
S3		ThirdReality Switch	1K+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
S4		Aqara Button	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
CM1	Smart Camera	Arlo Q	1M+	No	-	-	-	60	[60, 60]	-	-
CM2		Wyze Cam Indoor	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
CM3		Ring Doorbell	5M+	Yes	55	fixed	25	31	[29, 31]	-	-
CM4		Foscam R2C	1M+	Yes	150	fixed	45	30	[30, 30]	-	-
CM5		YiHome Cam Indoor	1M+	Yes	45	on-idle	30	∞	[30, 74]	-	-



No.	Device Type	Device Model	App Install	Long-live Session	Keep-alive Messages			Event Messages		Command Messages	
					Period(s)	Pattern	Timeout(s)	Timeout(s)	Range(s)	Timeout(s)	Range(s)
L1	Smart Light	Wyze White A19	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
L2		Philips Hue white A19	1M+	Yes	120	fixed	60	∞	[60, 180]	21	[21, 21]
P1	Smart Plug	Wyze Plug	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
P2		Amazon Plug	50M+	Yes	30	fixed	30	30	[30, 30]	30	[30, 30]
P3		SmartThings WiFi Plug	100M+	Yes	110	on-idle	110	∞	[110, 220]	∞	[110, 220]
P4		SmartThings Zigbee Plug	100M+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
P5		SmartLife Gosound Plug	5M+	Yes	60	on-idle	32	∞	[32, 92]	∞	[32, 92]
P6		KASA HS103P2 Plug	1M+	Yes	150	fixed	15	55	[15, 55]	15	[15, 15]
P7		Cync	100K+	Yes	21	on-idle	84	∞	[84, 105]	∞	[84, 105]
P8		iHome iSP6X Plug	100K+	Yes	30	fixed	18	32	[18, 32]	32	[18, 32]
P9		Aqara Plug	50K+	Yes	150	fixed	30	60	[30, 60]	30	[30, 30]
P10		Wemo Mini Plug	1M+	No	-	-	-	52	[52, 52]	15	[15, 15]
P11		Geeni Plug	1M+	No	-	-	-	90	[90, 90]	25	[25, 25]
M1	Motion Sensor	SmartThings Motion	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
M2		Philips Hue Motion	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
M3		Wyze Motion	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
M4		Ring Motion	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
M5		Nest Motion	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
M6		Ecobee Smart Sensor	500K+	Yes	60	on-idle	30	∞	[30, 90]	-	-
M7		SmartLife Sonew Motion	5M+	No	-	-	-	260	[260, 260]	-	-
M8		iHome iSB01 Motion	100K+	No	-	-	-	70	[70, 70]	-	-
M9		Aqara Motion	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
M10		Govee Motion	50K+	Yes	90	fixed	35	55	[35, 55]	-	-
M11		Amazon Echo Flex	50M+	Yes	30	on-idle	30	60	[30, 60]	-	-
C1	Contact Sensor	SmartThings multipurpose	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
C2		Wyze Contact	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
C3		Nest Contact	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
C4		Ecobee Smartsensor	50K+	Yes	60	on-idle	30	∞	[30, 90]	-	-
C5		SmartLife Towode Contact	5M+	No	-	-	-	130	[130, 130]	-	-
C6		iHome iSB04 Contact	100K+	No	-	-	-	70	[70, 70]	-	-
C7		Aqara Contact	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
C8		Ring Contact	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
C9		Geeni Door & Window	1M+	No	-	-	-	90	[90, 90]	-	-
C10		Govee door	500K+	Yes	90	fixed	35	55	[35, 55]	-	-
HS1	Home Security	Ring Keypad	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
HS2		Nest Keypad	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
HS3		SimpliSafe Keypad	5M+	Yes	55	fixed	30	20	[20, 20]	-	-
S1	Smart Switch	SmartThings button	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
S2		Philips Hue Dimmer	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
S3		ThirdReality Switch	1K+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
S4		Aqara Button	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
CM1	Smart Camera	Arlo Q	1M+	No	-	-	-	60	[60, 60]	-	-
CM2		Wyze Cam Indoor	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
CM3		Ring Doorbell	5M+	Yes	55	fixed	25	31	[29, 31]	-	-
CM4		Foscam R2C	1M+	Yes	150	fixed	45	30	[30, 30]	-	-
CM5		YiHome Cam Indoor	1M+	Yes	45	on-idle	30	∞	[30, 74]	-	-

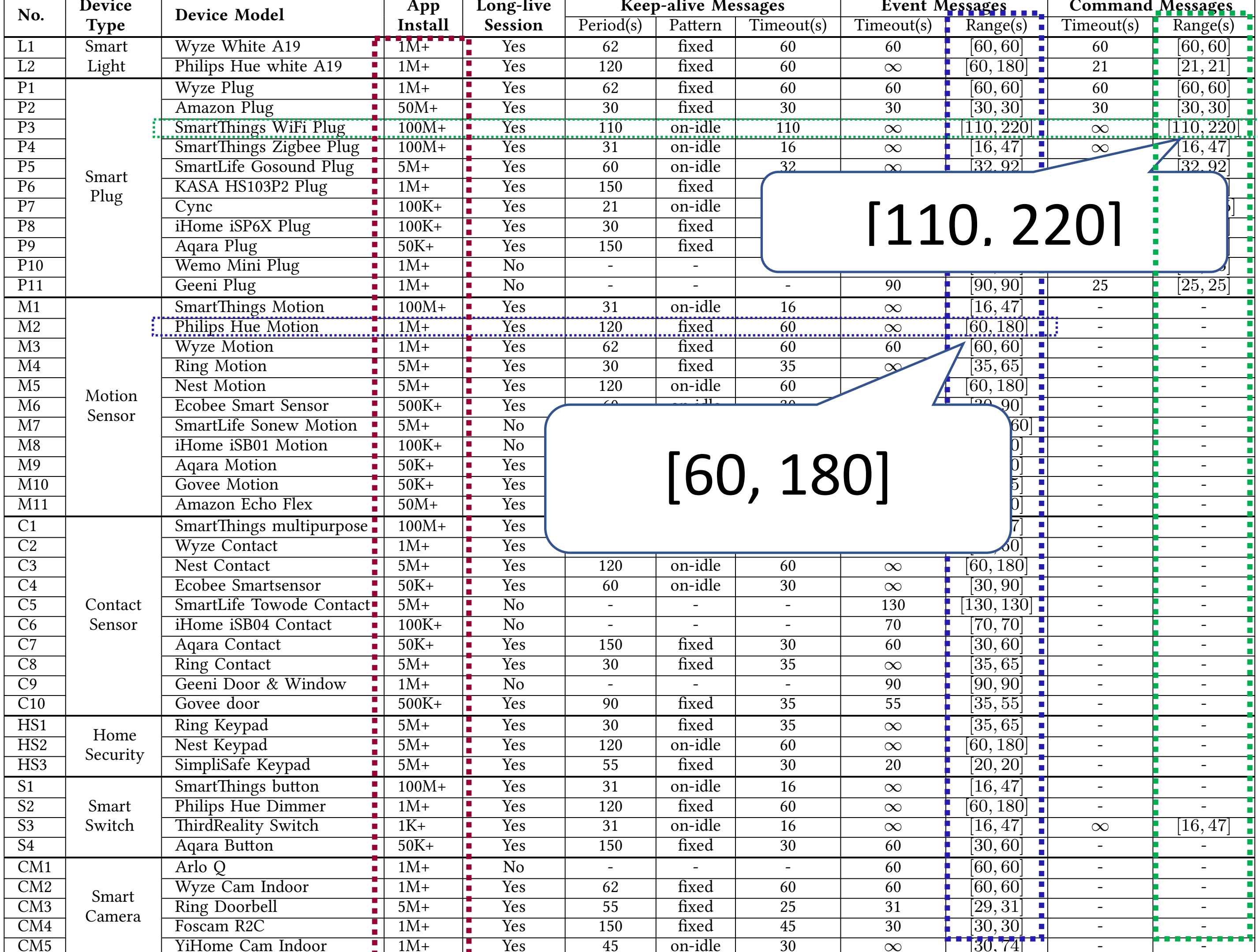


No.	Device Type	Device Model	App Install	Long-live Session	Keep-alive Messages			Event Messages		Command Messages	
					Period(s)	Pattern	Timeout(s)	Timeout(s)	Range(s)	Timeout(s)	Range(s)
L1	Smart Light	Wyze White A19	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
L2		Philips Hue white A19	1M+	Yes	120	fixed	60	∞	[60, 180]	21	[21, 21]
P1	Smart Plug	Wyze Plug	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
P2		Amazon Plug	50M+	Yes	30	fixed	30	30	[30, 30]	30	[30, 30]
P3		SmartThings WiFi Plug	100M+	Yes	110	on-idle	110	∞	[110, 220]	∞	[110, 220]
P4		SmartThings Zigbee Plug	100M+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
P5		SmartLife Gosound Plug	5M+	Yes	60	on-idle	32	∞	[32, 92]	∞	[32, 92]
P6		KASA HS103P2 Plug	1M+	Yes	150	fixed	15	55	[15, 55]	15	[15, 15]
P7		Cync	100K+	Yes	21	on-idle	84	∞	[84, 105]	∞	[84, 105]
P8		iHome iSP6X Plug	100K+	Yes	30	fixed	18	32	[18, 32]	32	[18, 32]
P9		Aqara Plug	50K+	Yes	150	fixed	30	60	[30, 60]	30	[30, 30]
P10		Wemo Mini Plug	1M+	No	-	-	-	52	[52, 52]	15	[15, 15]
P11		Geeni Plug	1M+	No	-	-	-	90	[90, 90]	25	[25, 25]
M1	Motion Sensor	SmartThings Motion	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
M2		Philips Hue Motion	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
M3		Wyze Motion	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
M4		Ring Motion	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
M5		Nest Motion	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
M6		Ecobee Smart Sensor	500K+	Yes	60	on-idle	30	∞	[30, 90]	-	-
M7		SmartLife Sonew Motion	5M+	No	-	-	-	260	[260, 260]	-	-
M8		iHome iSB01 Motion	100K+	No	-	-	-	70	[70, 70]	-	-
M9		Aqara Motion	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
M10		Govee Motion	50K+	Yes	90	fixed	35	55	[35, 55]	-	-
M11		Amazon Echo Flex	50M+	Yes	30	on-idle	30	60	[30, 60]	-	-
C1	Contact Sensor	SmartThings multipurpose	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
C2		Wyze Contact	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
C3		Nest Contact	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
C4		Ecobee Smartsensor	50K+	Yes	60	on-idle	30	∞	[30, 90]	-	-
C5		SmartLife Towode Contact	5M+	No	-	-	-	130	[130, 130]	-	-
C6		iHome iSB04 Contact	100K+	No	-	-	-	70	[70, 70]	-	-
C7		Aqara Contact	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
C8		Ring Contact	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
C9		Geeni Door & Window	1M+	No	-	-	-	90	[90, 90]	-	-
C10		Govee door	500K+	Yes	90	fixed	35	55	[35, 55]	-	-
HS1	Home Security	Ring Keypad	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
HS2		Nest Keypad	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
HS3		SimpliSafe Keypad	5M+	Yes	55	fixed	30	20	[20, 20]	-	-
S1	Smart Switch	SmartThings button	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
S2		Philips Hue Dimmer	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
S3		ThirdReality Switch	1K+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
S4		Aqara Button	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
CM1	Smart Camera	Arlo Q	1M+	No	-	-	-	60	[60, 60]	-	-
CM2		Wyze Cam Indoor	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
CM3		Ring Doorbell	5M+	Yes	55	fixed	25	31	[29, 31]	-	-
CM4		Foscam R2C	1M+	Yes	150	fixed	45	30	[30, 30]	-	-
CM5		YiHome Cam Indoor	1M+	Yes	45	on-idle	30	∞	[30, 74]	-	-



No.	Device Type	Device Model	App Install	Long-live Session	Keep-alive Messages			Event Messages		Command Messages	
					Period(s)	Pattern	Timeout(s)	Timeout(s)	Range(s)	Timeout(s)	Range(s)
L1	Smart Light	Wyze White A19	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
L2		Philips Hue white A19	1M+	Yes	120	fixed	60	∞	[60, 180]	21	[21, 21]
P1	Smart Plug	Wyze Plug	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
P2		Amazon Plug	50M+	Yes	30	fixed	30	30	[30, 30]	30	[30, 30]
P3		SmartThings WiFi Plug	100M+	Yes	110	on-idle	110	∞	[110, 220]	∞	[110, 220]
P4		SmartThings Zigbee Plug	100M+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
P5		SmartLife Gosound Plug	5M+	Yes	60	on-idle	32	∞	[32, 92]	∞	[32, 92]
P6		KASA HS103P2 Plug	1M+	Yes	150	fixed	15	55	[15, 55]	15	[15, 15]
P7		Cync	100K+	Yes	21	on-idle	84	∞	[84, 105]	∞	[84, 105]
P8		iHome iSP6X Plug	100K+	Yes	30	fixed	18	32	[18, 32]	32	[18, 32]
P9		Aqara Plug	50K+	Yes	150	fixed	30	60	[30, 60]	30	[30, 30]
P10		Wemo Mini Plug	1M+	No	-	-	-	52	[52, 52]	15	[15, 15]
P11		Geeni Plug	1M+	No	-	-	-	90	[90, 90]	25	[25, 25]
M1	Motion Sensor	SmartThings Motion	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
M2		Philips Hue Motion	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
M3		Wyze Motion	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
M4		Ring Motion	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
M5		Nest Motion	5M+	Yes	120	on-idle	60	[illegible]	[60, 180]	-	-
M6		Ecobee Smart Sensor	500K+	Yes	60	on-idle	30	[illegible]	[30, 90]	-	-
M7		SmartLife Sonew Motion	5M+	No	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
M8		iHome iSB01 Motion	100K+	No	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
M9		Aqara Motion	50K+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
M10		Govee Motion	50K+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
M11		Amazon Echo Flex	50M+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
C1	Contact Sensor	SmartThings multipurpose	100M+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
C2		Wyze Contact	1M+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
C3		Nest Contact	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
C4		Ecobee Smartsensor	50K+	Yes	60	on-idle	30	∞	[30, 90]	-	-
C5		SmartLife Towode Contact	5M+	No	-	-	-	130	[130, 130]	-	-
C6		iHome iSB04 Contact	100K+	No	-	-	-	70	[70, 70]	-	-
C7		Aqara Contact	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
C8		Ring Contact	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
C9		Geeni Door & Window	1M+	No	-	-	-	90	[90, 90]	-	-
C10		Govee door	500K+	Yes	90	fixed	35	55	[35, 55]	-	-
HS1	Home Security	Ring Keypad	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
HS2		Nest Keypad	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
HS3		SimpliSafe Keypad	5M+	Yes	55	fixed	30	20	[20, 20]	-	-
S1	Smart Switch	SmartThings button	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
S2		Philips Hue Dimmer	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
S3		ThirdReality Switch	1K+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
S4		Aqara Button	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
CM1	Smart Camera	Arlo Q	1M+	No	-	-	-	60	[60, 60]	-	-
CM2		Wyze Cam Indoor	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
CM3		Ring Doorbell	5M+	Yes	55	fixed	25	31	[29, 31]	-	-
CM4		Foscam R2C	1M+	Yes	150	fixed	45	30	[30, 30]	-	-
CM5		YiHome Cam Indoor	1M+	Yes	45	on-idle	30	∞	[30, 74]	-	-

[60, 180]



No.	Device Type	Device Model	App Install	Long-live Session	Keep-alive Messages			Event Messages		Command Messages	
					Period(s)	Pattern	Timeout(s)	Timeout(s)	Range(s)	Timeout(s)	Range(s)
L1	Smart Light	Wyze White A19	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
L2		Philips Hue white A19	1M+	Yes	120	fixed	60	∞	[60, 180]	21	[21, 21]
P1	Smart Plug	Wyze Plug	1M+	Yes	62	fixed	60	60	[60, 60]	60	[60, 60]
P2		Amazon Plug	50M+	Yes	30	fixed	30	30	[30, 30]	30	[30, 30]
P3		SmartThings WiFi Plug	100M+	Yes	110	on-idle	110	∞	[110, 220]	∞	[110, 220]
P4		SmartThings Zigbee Plug	100M+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
P5		SmartLife Gosound Plug	5M+	Yes	60	on-idle	32	∞	[32, 92]	[illegible]	[32, 92]
P6		KASA HS103P2 Plug	1M+	Yes	150	fixed	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
P7		Cync	100K+	Yes	21	on-idle	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
P8		iHome iSP6X Plug	100K+	Yes	30	fixed	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
P9		Aqara Plug	50K+	Yes	150	fixed	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
P10		Wemo Mini Plug	1M+	No	-	-	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
P11		Geeni Plug	1M+	No	-	-	-	90	[90, 90]	25	[25, 25]
M1	Motion Sensor	SmartThings Motion	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
M2		Philips Hue Motion	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
M3		Wyze Motion	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
M4		Ring Motion	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
M5		Nest Motion	5M+	Yes	120	on-idle	60	[illegible]	[60, 180]	-	-
M6		Ecobee Smart Sensor	500K+	Yes	60	on-idle	30	[illegible]	[30, 90]	-	-
M7		SmartLife Sonew Motion	5M+	No	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
M8		iHome iSB01 Motion	100K+	No	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
M9		Aqara Motion	50K+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
M10		Govee Motion	50K+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
M11		Amazon Echo Flex	50M+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
C1	Contact Sensor	SmartThings multipurpose	100M+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
C2		Wyze Contact	1M+	Yes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-	-
C3		Nest Contact	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
C4		Ecobee Smartsensor	50K+	Yes	60	on-idle	30	∞	[30, 90]	-	-
C5		SmartLife Towode Contact	5M+	No	-	-	-	130	[130, 130]	-	-
C6		iHome iSB04 Contact	100K+	No	-	-	-	70	[70, 70]	-	-
C7		Aqara Contact	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
C8		Ring Contact	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
C9		Geeni Door & Window	1M+	No	-	-	-	90	[90, 90]	-	-
C10		Govee door	500K+	Yes	90	fixed	35	55	[35, 55]	-	-
HS1	Home Security	Ring Keypad	5M+	Yes	30	fixed	35	∞	[35, 65]	-	-
HS2		Nest Keypad	5M+	Yes	120	on-idle	60	∞	[60, 180]	-	-
HS3		SimpliSafe Keypad	5M+	Yes	55	fixed	30	20	[20, 20]	-	-
S1	Smart Switch	SmartThings button	100M+	Yes	31	on-idle	16	∞	[16, 47]	-	-
S2		Philips Hue Dimmer	1M+	Yes	120	fixed	60	∞	[60, 180]	-	-
S3		ThirdReality Switch	1K+	Yes	31	on-idle	16	∞	[16, 47]	∞	[16, 47]
S4		Aqara Button	50K+	Yes	150	fixed	30	60	[30, 60]	-	-
CM1	Smart Camera	Arlo Q	1M+	No	-	-	-	60	[60, 60]	-	-
CM2		Wyze Cam Indoor	1M+	Yes	62	fixed	60	60	[60, 60]	-	-
CM3		Ring Doorbell	5M+	Yes	55	fixed	25	31	[29, 31]	-	-
CM4		Foscam R2C	1M+	Yes	150	fixed	45	30	[30, 30]	-	-
CM5		YiHome Cam Indoor	1M+	Yes	45	on-idle	30	∞	[30, 74]	-	-

[110, 220]

[60, 180]

Phantom-Delay Attack Primitives

- IoT Event Message Delay (E-Delay)
- IoT Command Message Delay (C-Delay)

IoT events and commands can be delayed **without**

(1) relying on any implementation bugs: usable

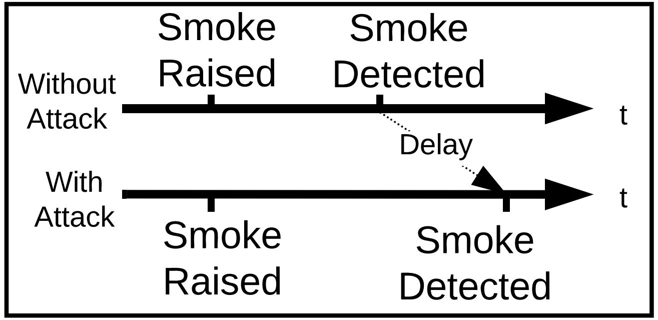
(2) cracking any TLS session keys: easy-to-apply

(3) triggering any alerts in any layers: stealthy

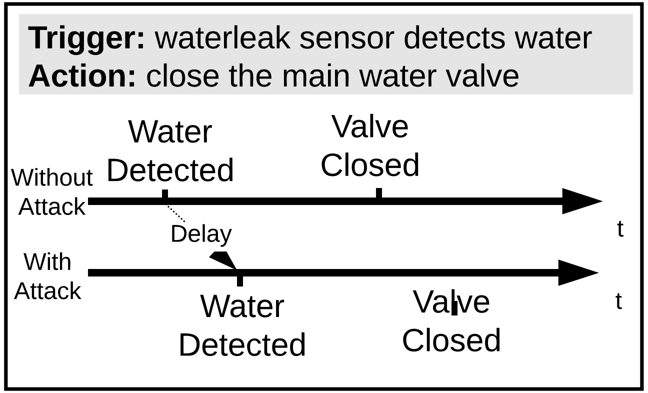
IoT Phantom Delay Attacks

- What are the new attack primitives? ☑
  - E-Delay; C-Delay
- What simple attacks can be launched?
- What sophisticated attacks can be launched?
- What are the possible countermeasures?

- State-Update Delay Attacks

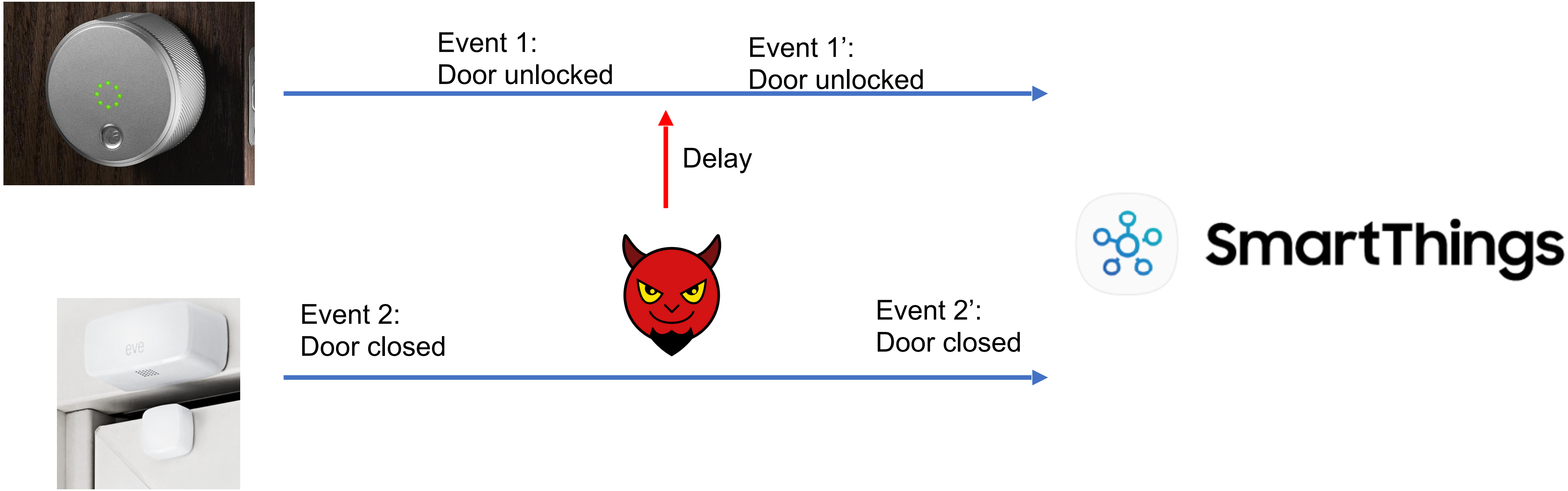


- Action Delay Attacks


Trigger: waterleak sensor detects water
Action: close the main water valve

IoT Phantom Delay Attacks

- What are the new attack primitives? ☑
  - E-Delay; C-Delay
- What simple attacks can be launched? ☑
  - *“Fire alarm is delayed”, “Remedy actions delayed”*
- What sophisticated attacks can be launched?
- What are the possible countermeasures?



Event 1:
Door unlocked

Event 1':
Door unlocked

Delay

Event 2:
Door closed

Event 2':
Door closed

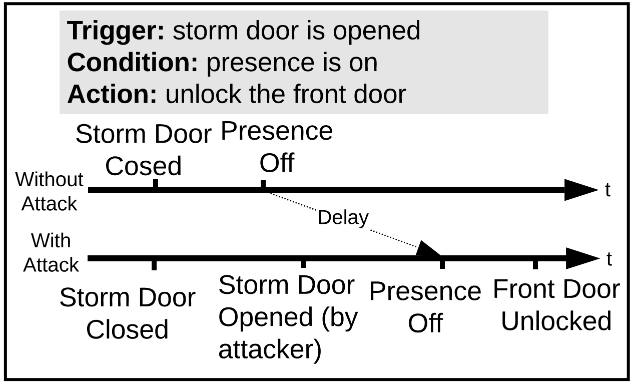
SmartThings

Key Insight 2:

Each device has an individual TCP-TLS session to its IoT server

Selective Delay → Message Out-of-order

- Spurious Execution



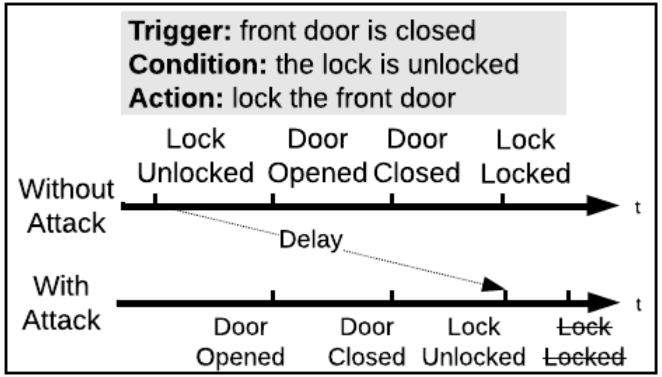
Trigger: storm door is opened
Condition: presence is on
Action: unlock the front door

Without Attack: Storm Door Cosed — Presence Off — t

Delay

With Attack: Storm Door Closed — Storm Door Opened (by attacker) — Presence Off — Front Door Unlocked — t

- Disabled Execution

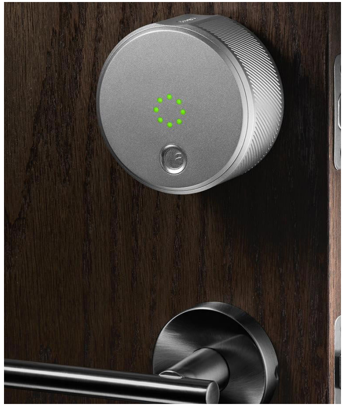


Trigger: front door is closed
Condition: the lock is unlocked
Action: lock the front door

Without Attack: Lock Unlocked — Door Opened — Door Closed — Lock Locked — t

Delay

With Attack: Door Opened — Door Closed — Lock Unlocked — ~~Lock Locked~~ — t

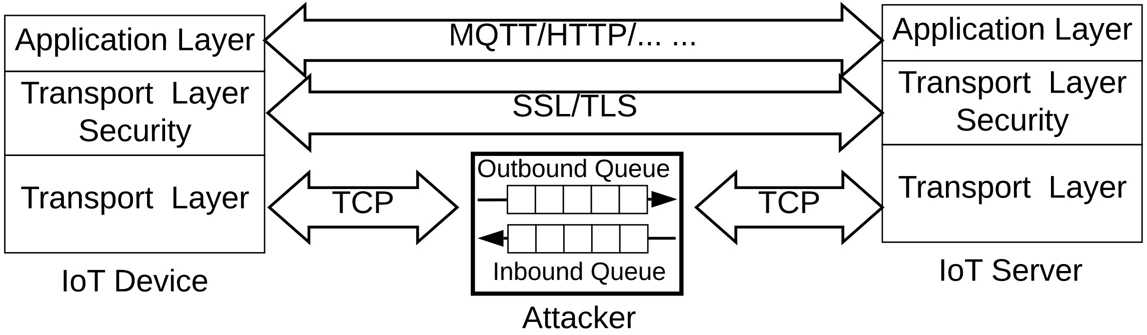


IoT Phantom Delay Attacks

- What are the new attack primitives? ☑
    - E-Delay; C-Delay
- What simple attacks can be launched? ☑
    - *“Fire alarm is delayed”, “Remedy actions delayed”*
- What sophisticated attacks can be launched? ☑
    - *“Spurious unlock”, “Door lock override”*
- What are the possible countermeasures?

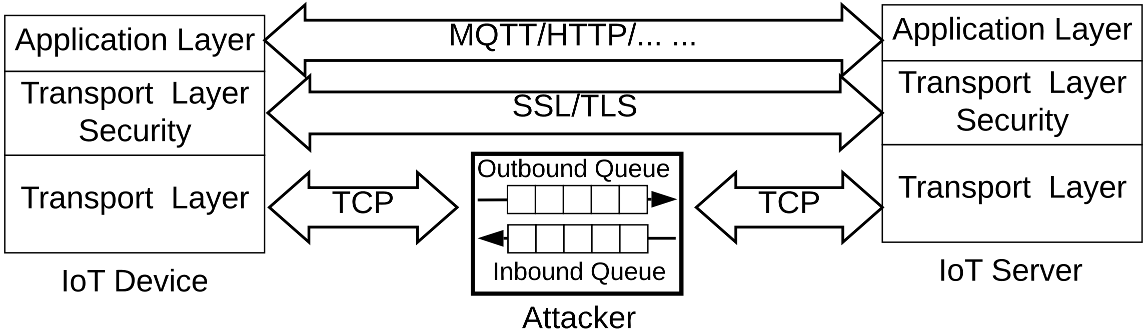
Possible Countermeasures

- Checking timestamp upon receiving a message
  - Limitations: post-attack detection; clock sync
- Tightening the app-layer delay constraint
  - Limitations: traffic and energy consumption; false positives



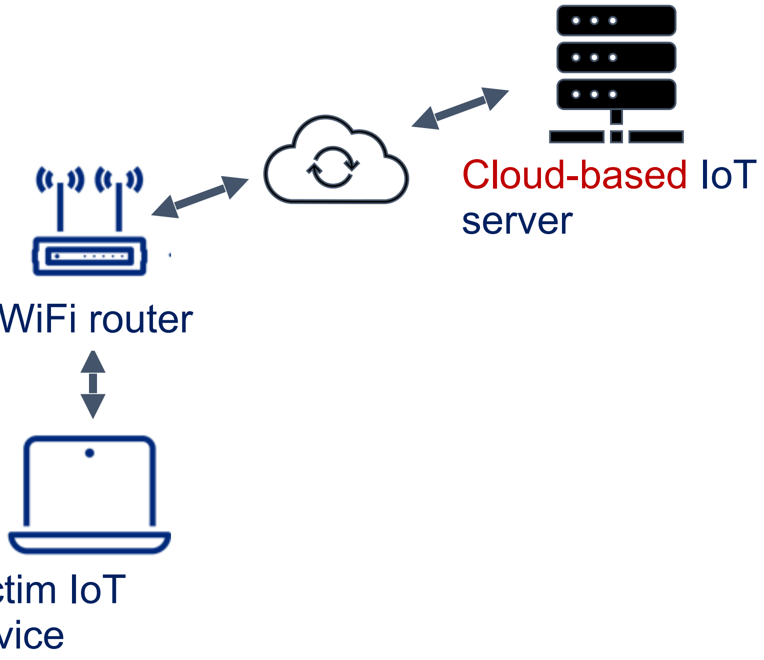
Possible Countermeasures

- Checking timestamp upon receiving a message
  - Limitations: post-attack detection; clock sync
- Tightening the app-layer delay constraint
  - Limitations: traffic and energy consumption; false positives

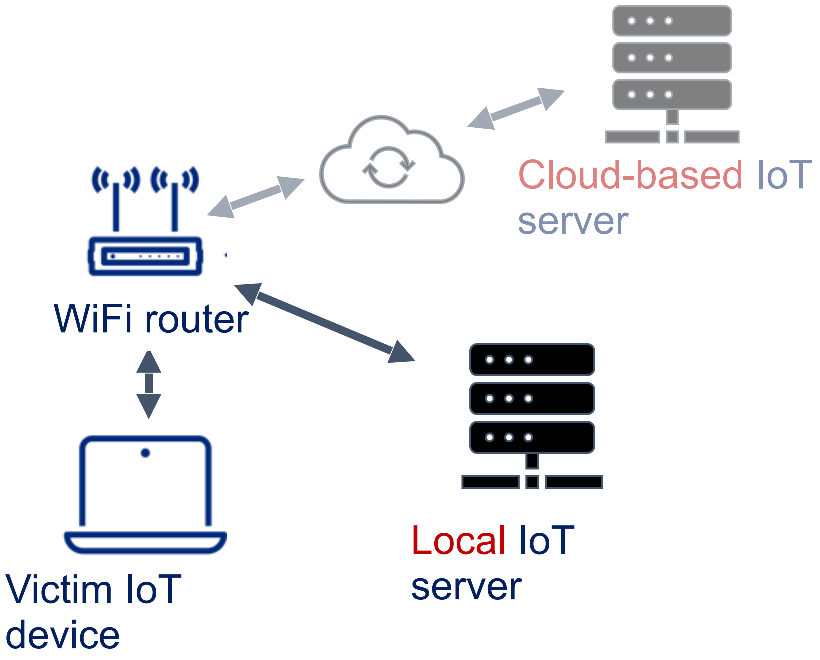


Common Limitation: the countermeasures need to update the firmware of billions of IoT devices

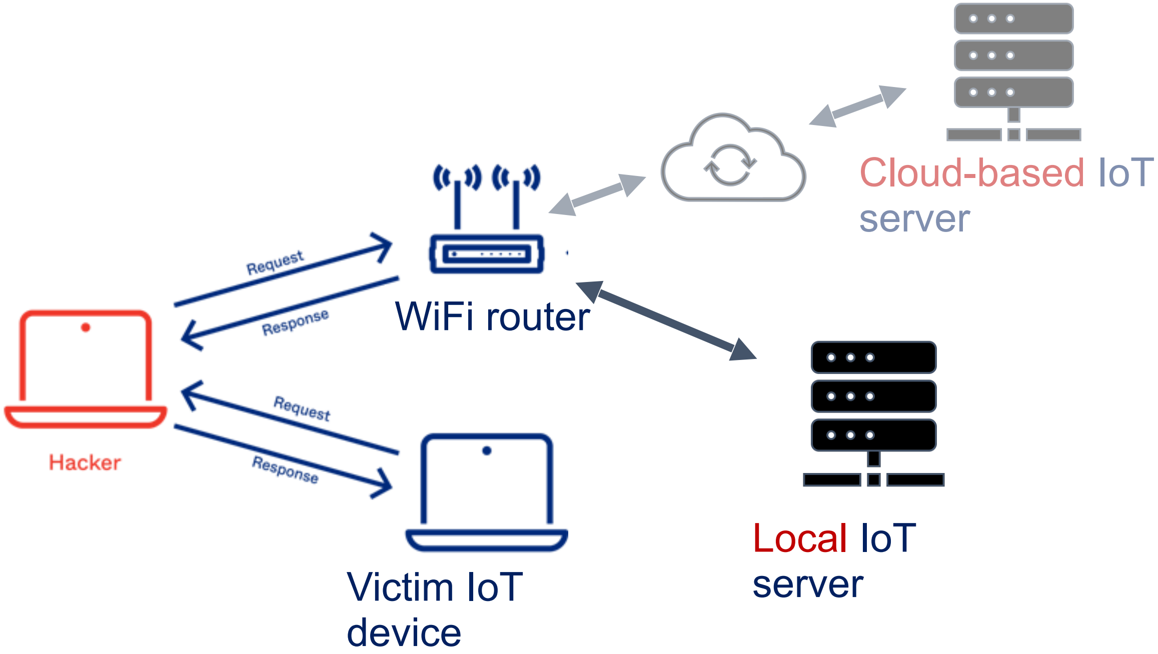
Local IoT Server: Not a Countermeasure



Local IoT Server: Not a Countermeasure

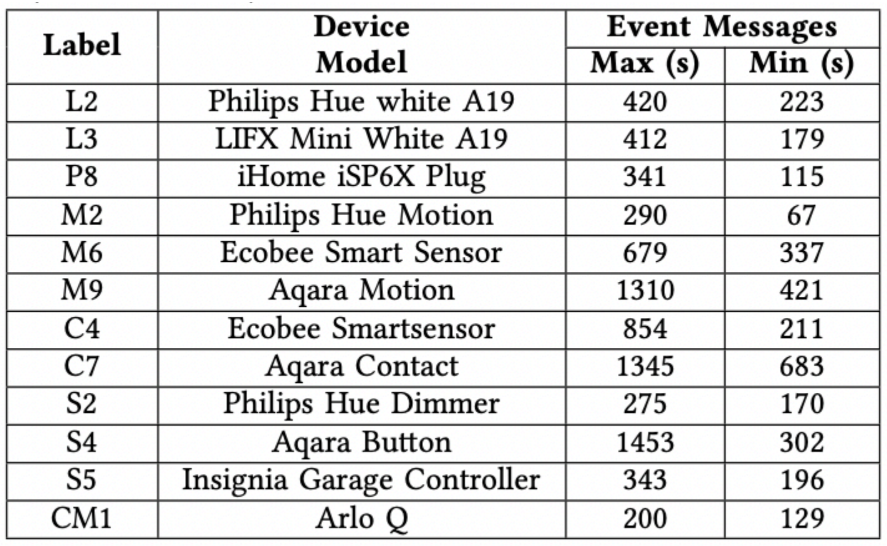


Local IoT Server: Not a Countermeasure



Case Study: Apple Homekit

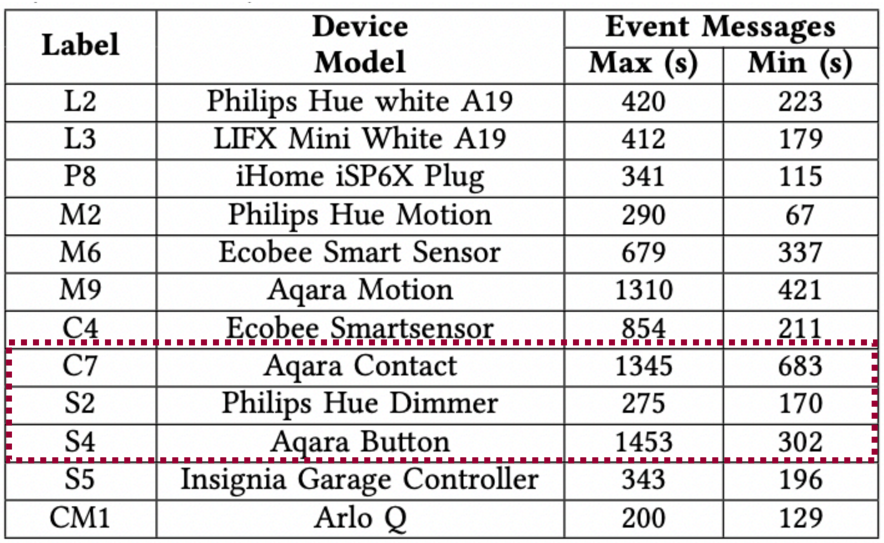
- Local IoT servers: HomePod, Apple TV, or iPad
- No application layer event ack (HAP specification)
- No keep-alive messages
- Unlimited delay until the hub occasionally polling



Label	Device Model	Event Messages	
		Max (s)	Min (s)
L2	Philips Hue white A19	420	223
L3	LIFX Mini White A19	412	179
P8	iHome iSP6X Plug	341	115
M2	Philips Hue Motion	290	67
M6	Ecobee Smart Sensor	679	337
M9	Aqara Motion	1310	421
C4	Ecobee Smartsensor	854	211
C7	Aqara Contact	1345	683
S2	Philips Hue Dimmer	275	170
S4	Aqara Button	1453	302
S5	Insignia Garage Controller	343	196
CM1	Arlo Q	200	129

Case Study: Apple Homekit

- Local IoT servers: HomePod, Apple TV, or iPad
- No application layer event ack (HAP specification)
- No keep-alive messages
- Unlimited delay until the hub occasionally polling



Label	Device Model	Event Messages	
		Max (s)	Min (s)
L2	Philips Hue white A19	420	223
L3	LIFX Mini White A19	412	179
P8	iHome iSP6X Plug	341	115
M2	Philips Hue Motion	290	67
M6	Ecobee Smart Sensor	679	337
M9	Aqara Motion	1310	421
C4	Ecobee Smartsensor	854	211
C7	Aqara Contact	1345	683
S2	Philips Hue Dimmer	275	170
S4	Aqara Button	1453	302
S5	Insignia Garage Controller	343	196
CM1	Arlo Q	200	129

More than 20 mins delay!

Is TCP+TLS really suitable for IoT?

Is TCP+TLS really suitable for IoT?

A Flaw:

We cannot trust the TCP layer to detect network delays (as it is decoupled from the data protection by TLS)

Is TCP+TLS really suitable for IoT?

A Flaw:

We cannot trust the TCP layer to detect network delays (as it is decoupled from the data protection by TLS)

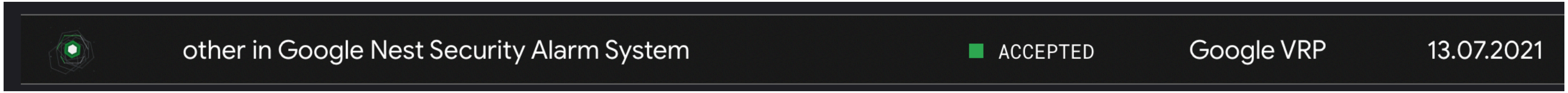
A Dilemma:

We should not use the Application layer to detect network delays (as its timeout threshold needs to take into consideration scheduling, automation processing, and constrained devices)

Not an issue of one or two IoT platforms or devices;
all IoT platforms we tested have it

Attack script and detailed steps to reproduce the attack is available at https://github.com/infinitywings/IoT-Phantom-Delay-Attack

Responsible Disclosure



other in Google Nest Security Alarm System	🟩 ACCEPTED	Google VRP	13.07.2021

“We will report this vulnerability to the product team and reduce the value of timeout” — SimpliSafe

“We appreciate your suggestions and will evaluate our TLS keep alive and connection timeout strategy for our current timeout thresholds. We also have a mitigation strategy in place so in the future it will be harder for an attacker to discern commands based on packet size or TCP segment length. ” — Ring

Contributions

- The **first** work that studies IoT timeout behaviors and their exploitability
  - Revealed a critical design flaw

- **IoT phantom-delay attack primitives**
  - No alerts; no packet loss; no disconnection; no bugs

- **Rich attacks: delay, disable, override automation**

- **Uniqueness** (compared to delays in distributed systems)
  - Zero implementation bugs vs. specific bugs
  - IoT over TCP/IP vs. specialized systems

Thanks!

Q&A