Packet-Level Signatures for Smart Home Devices

Rahmadi Trimananda, Janus Varmarken,
Athina Markopoulou, and Brian Demsky

UCI University of
California, Irvine

Home

Smart Home

Smart **Plugs**

Smart Home

Smart **Plugs**

Light Bulbs

UCI University of California, Irvine

Smart Home

Smart **Plugs**

Light Bulbs

Thermostats

Smart Home

Smart **Plugs**

Light Bulbs

Thermostats

Cameras

Smart Home

Smart **Plugs**

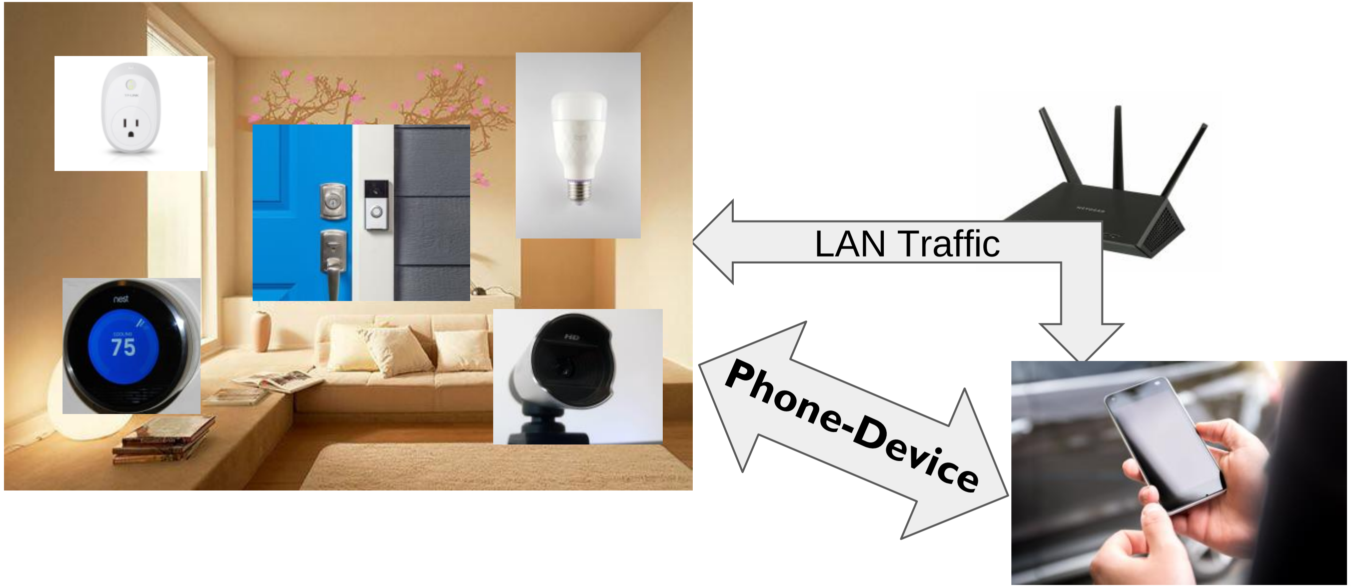
Light Bulbs

Thermostats

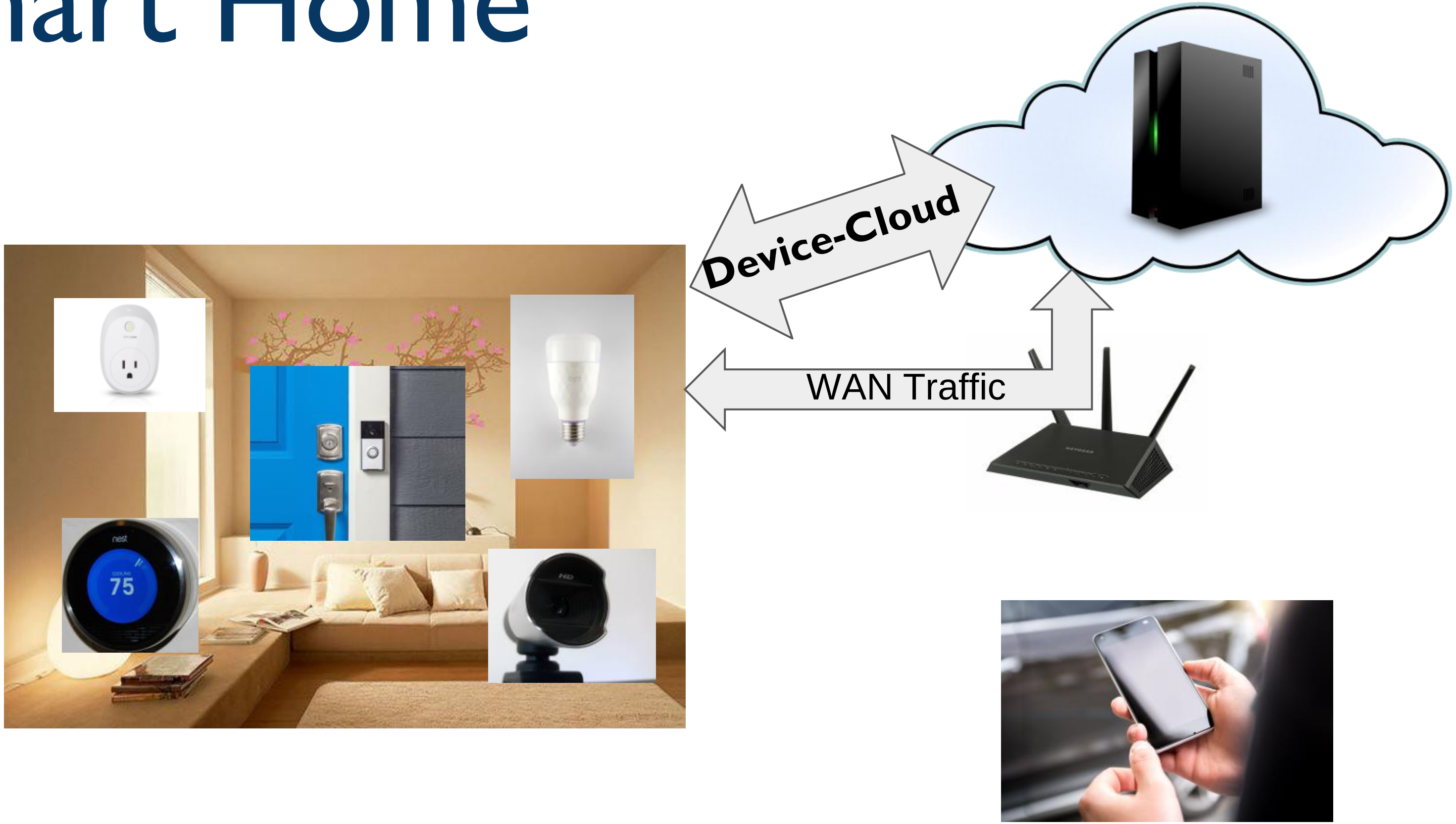
Cameras

Doorbells

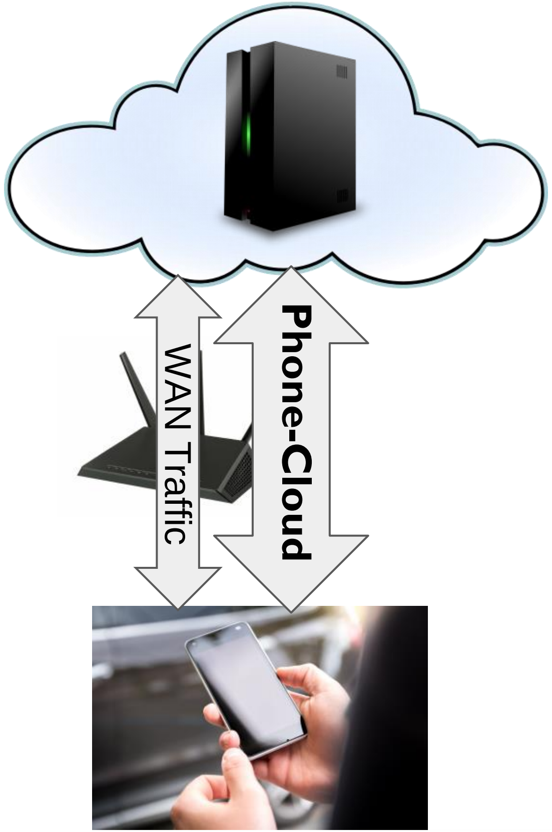
Smart Home



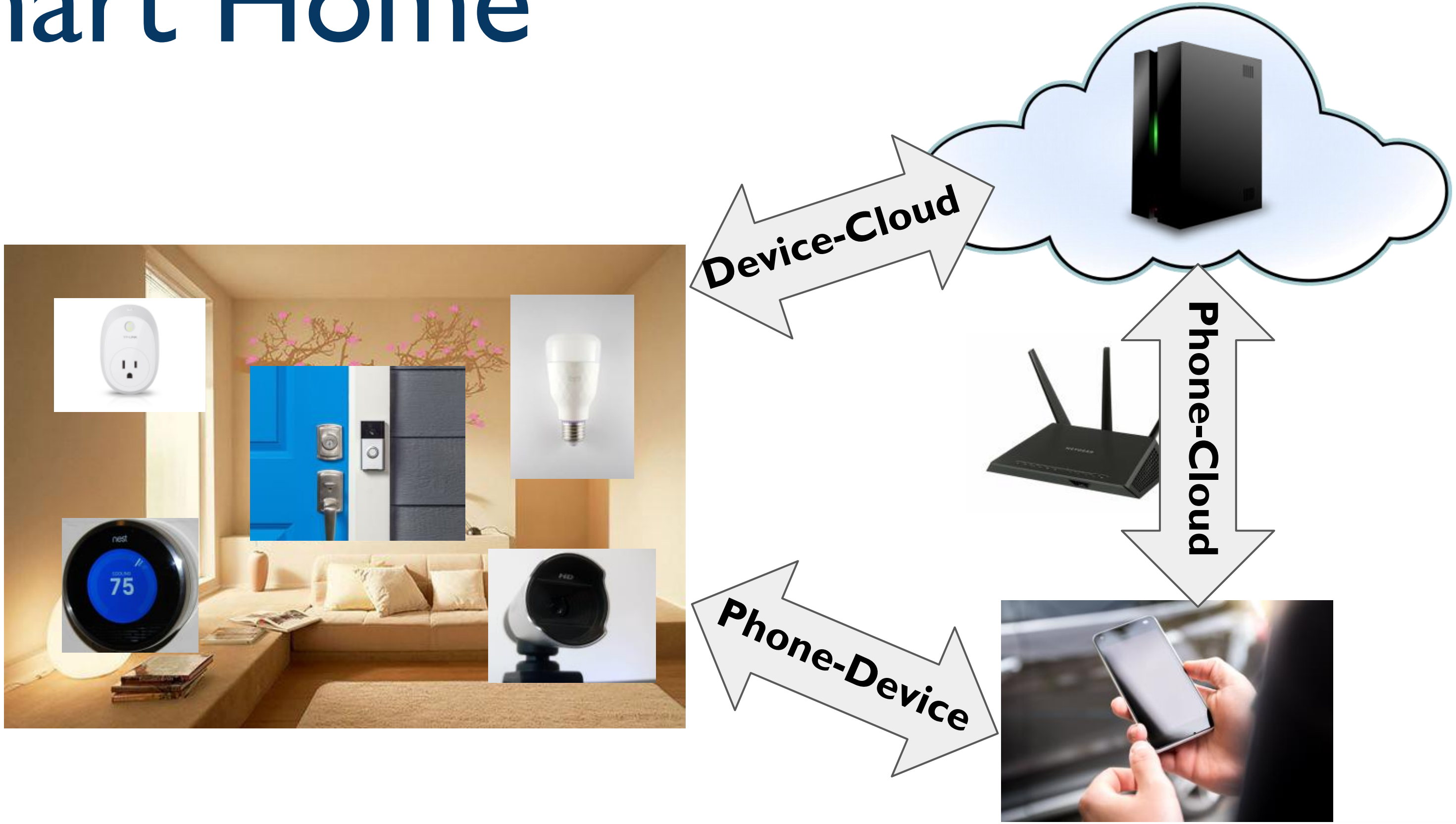
Smart Home



Smart Home



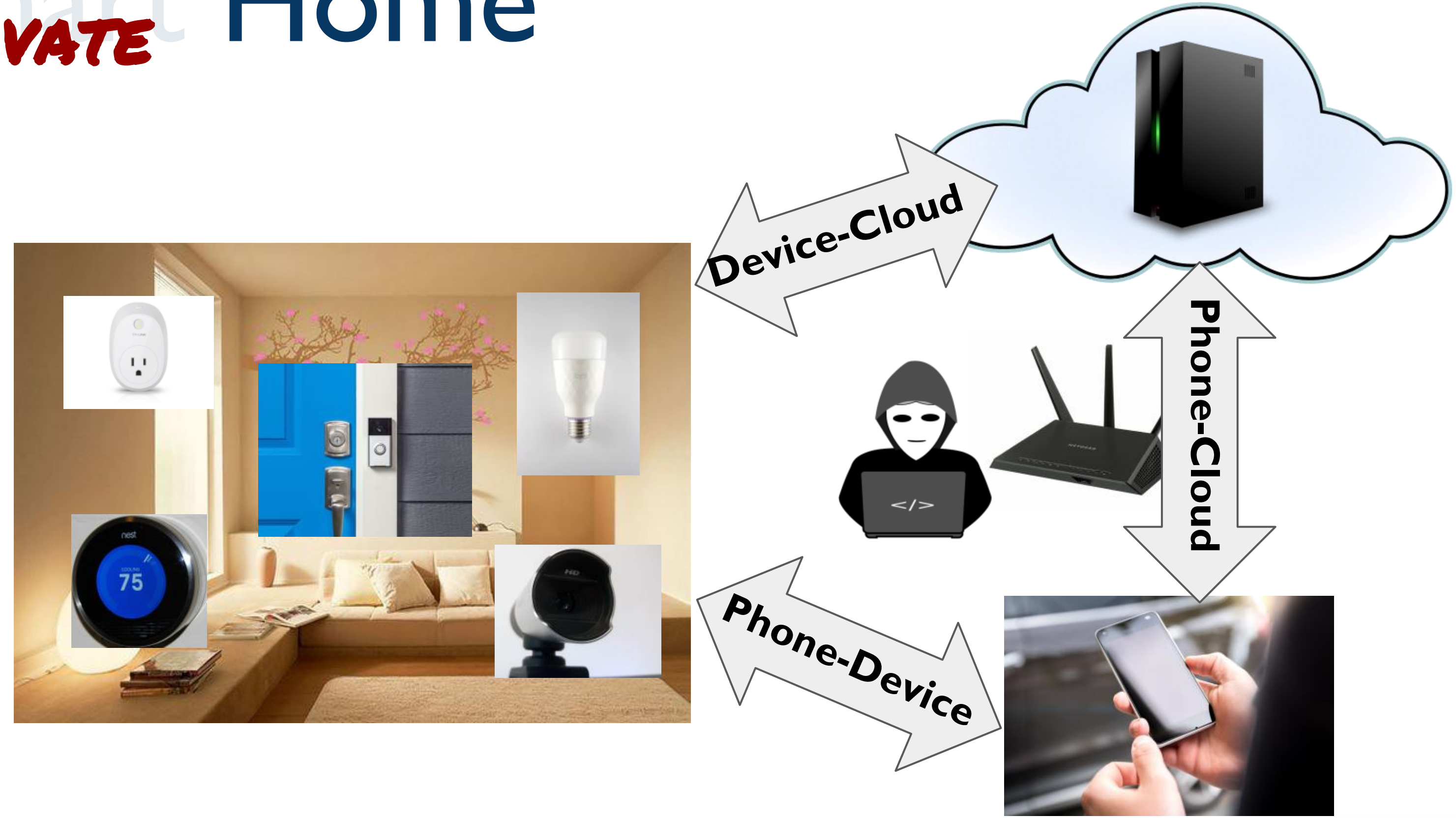
Smart Home



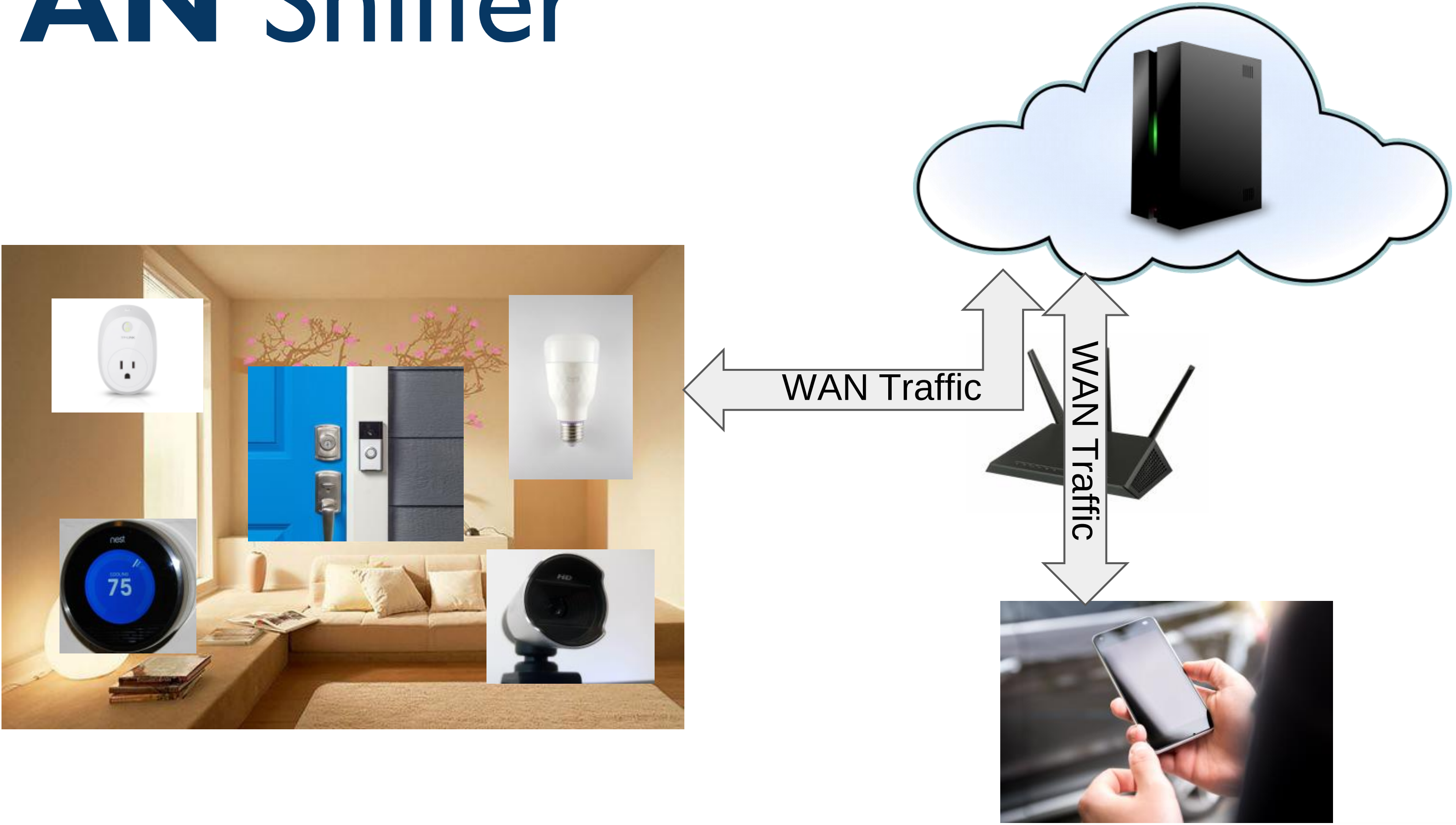
UCI University of California, Irvine

NOT-SO PRIVATE

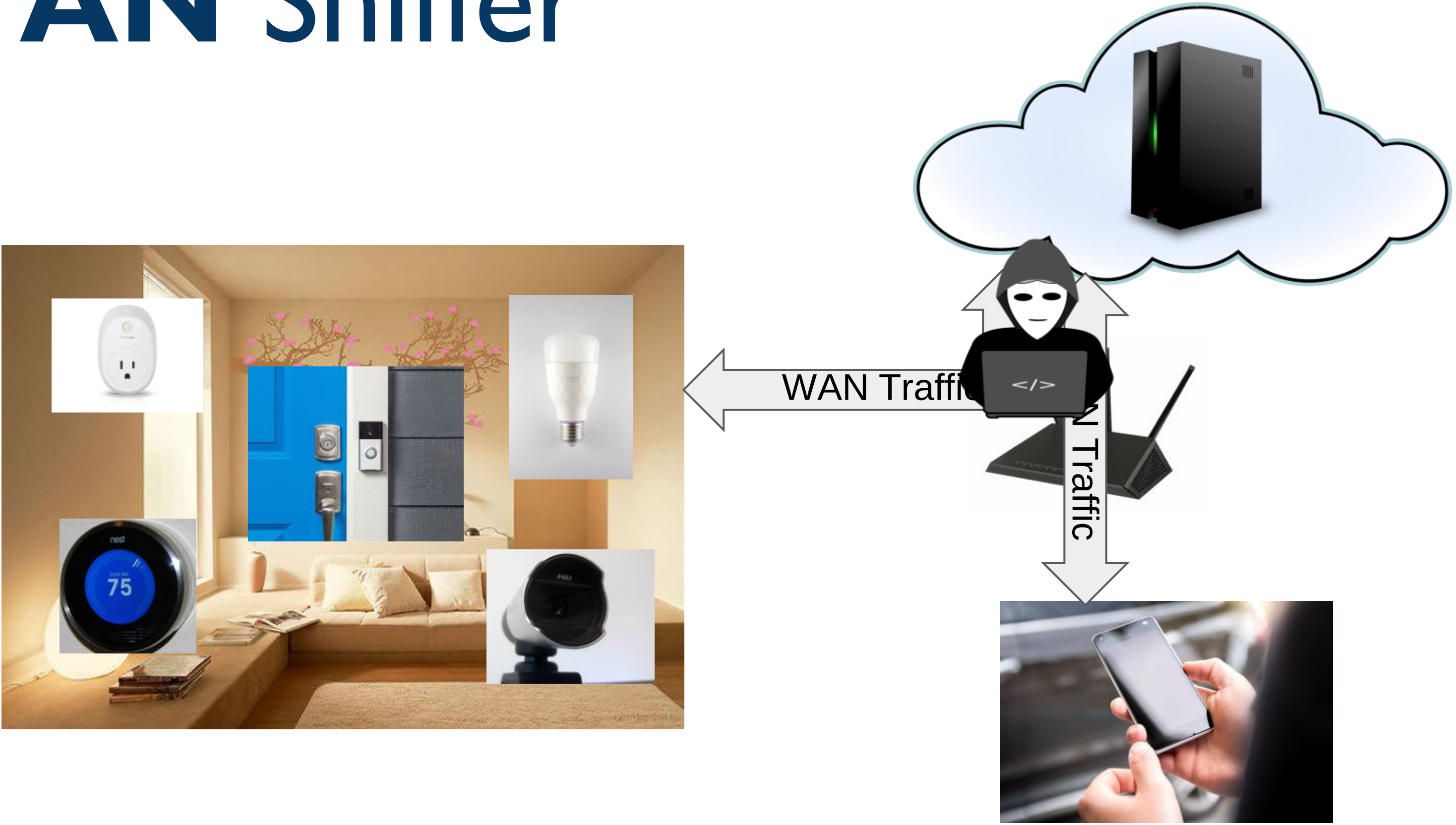
Smart Home



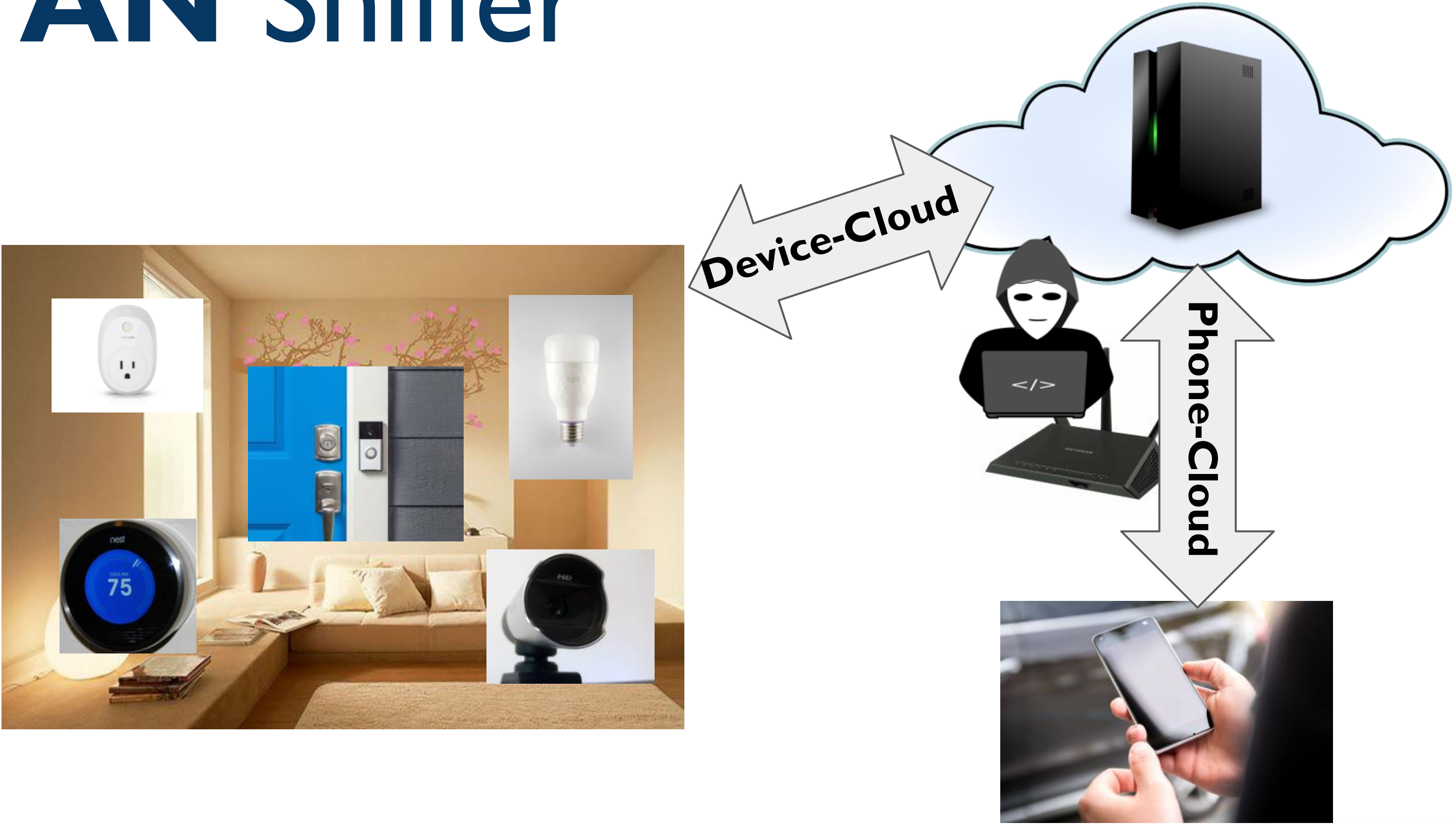
WAN Sniffer



WAN Sniffer

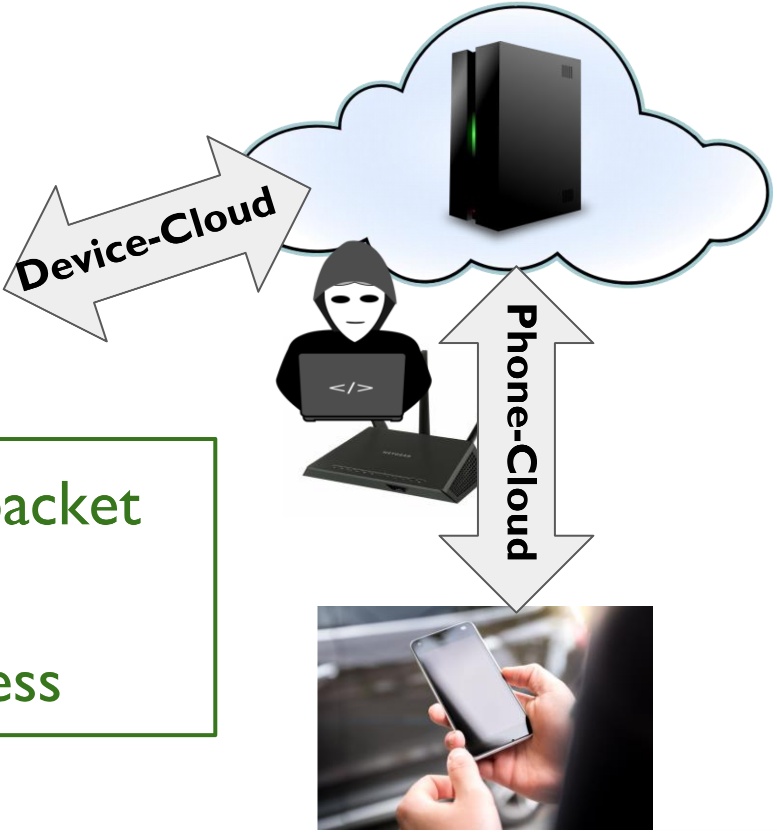


WAN Sniffer

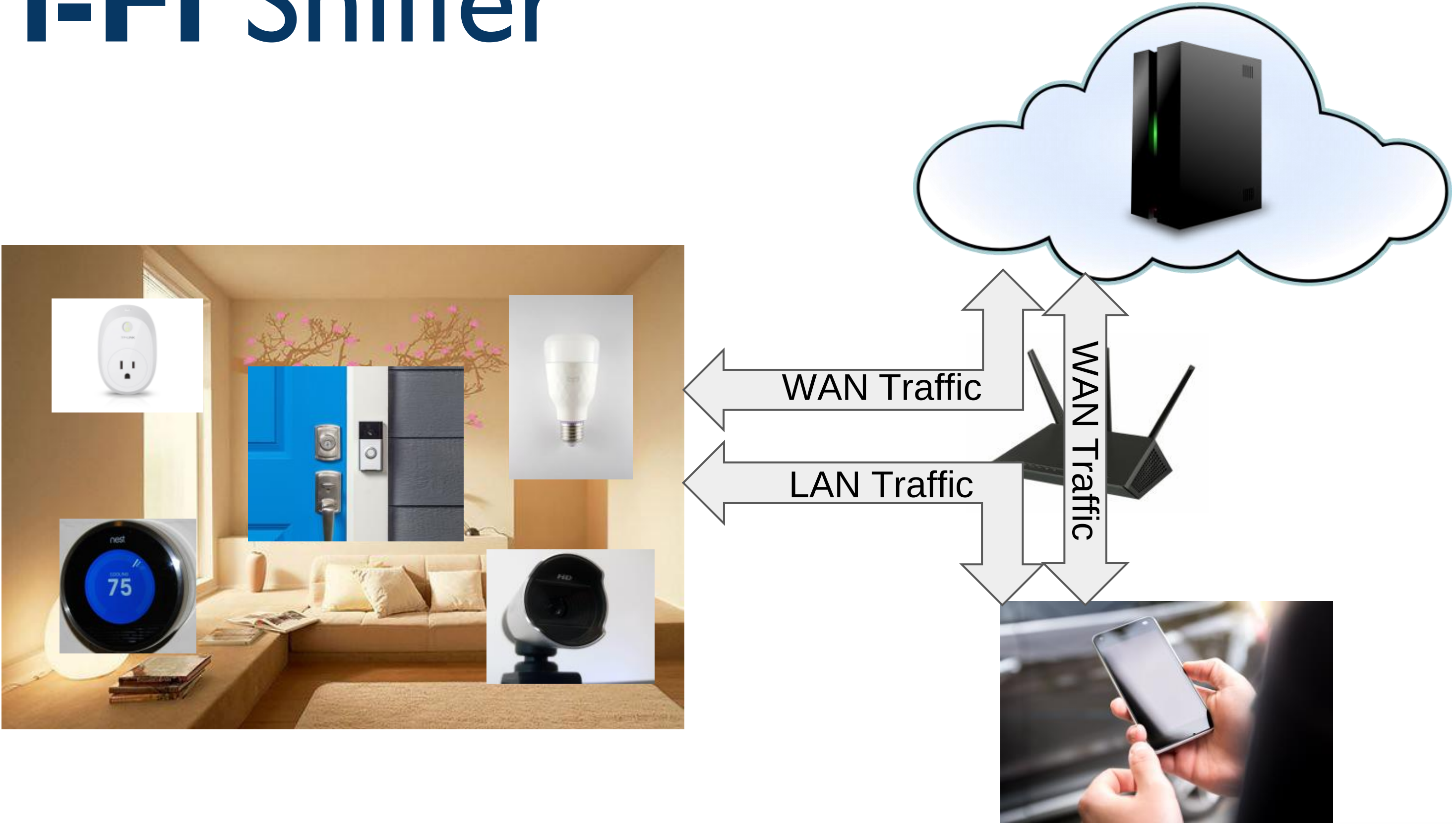


WAN Sniffer

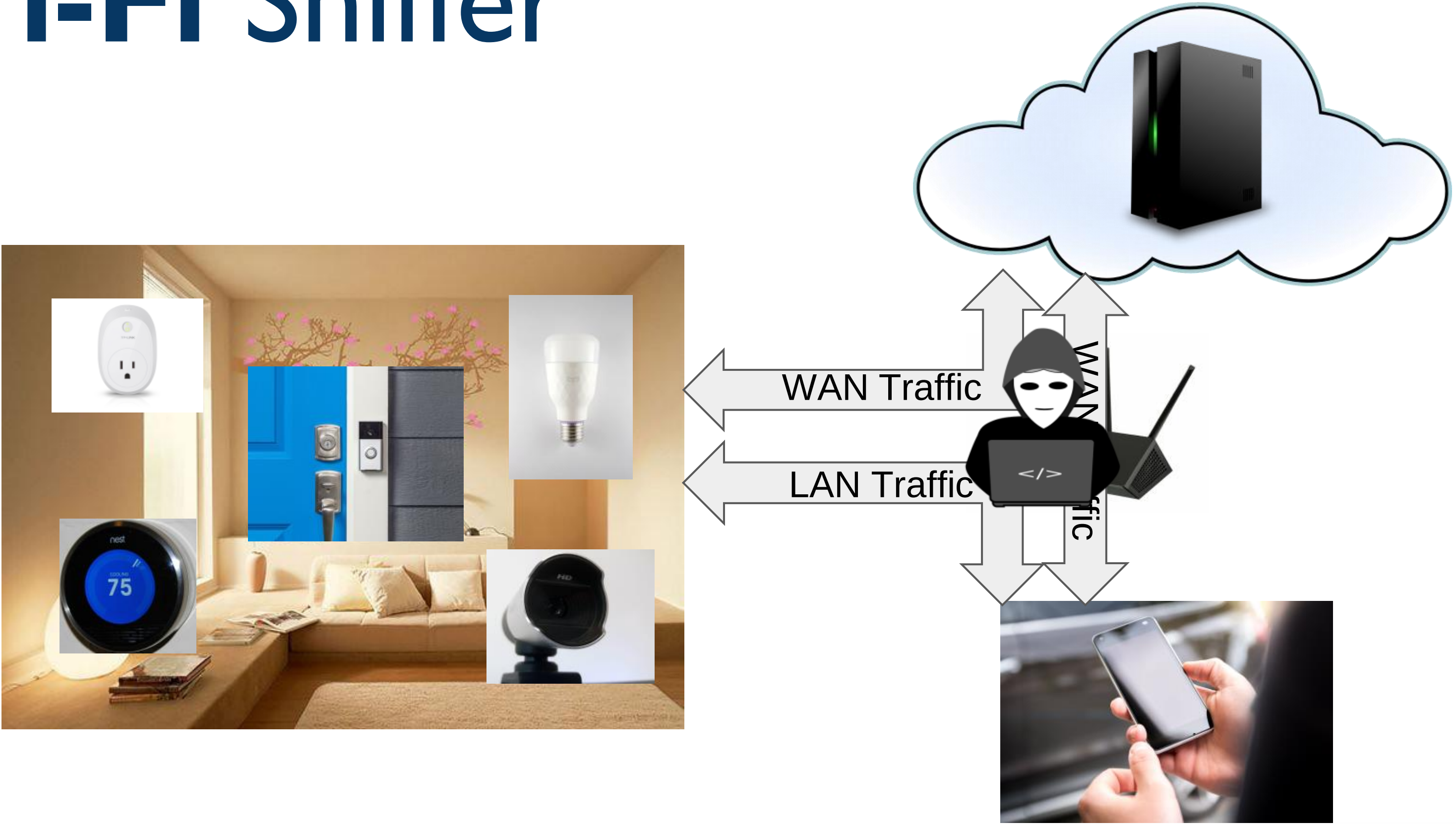
1) Can look into TCP/IP packet
2) Can see IP address
3) Cannot see MAC address



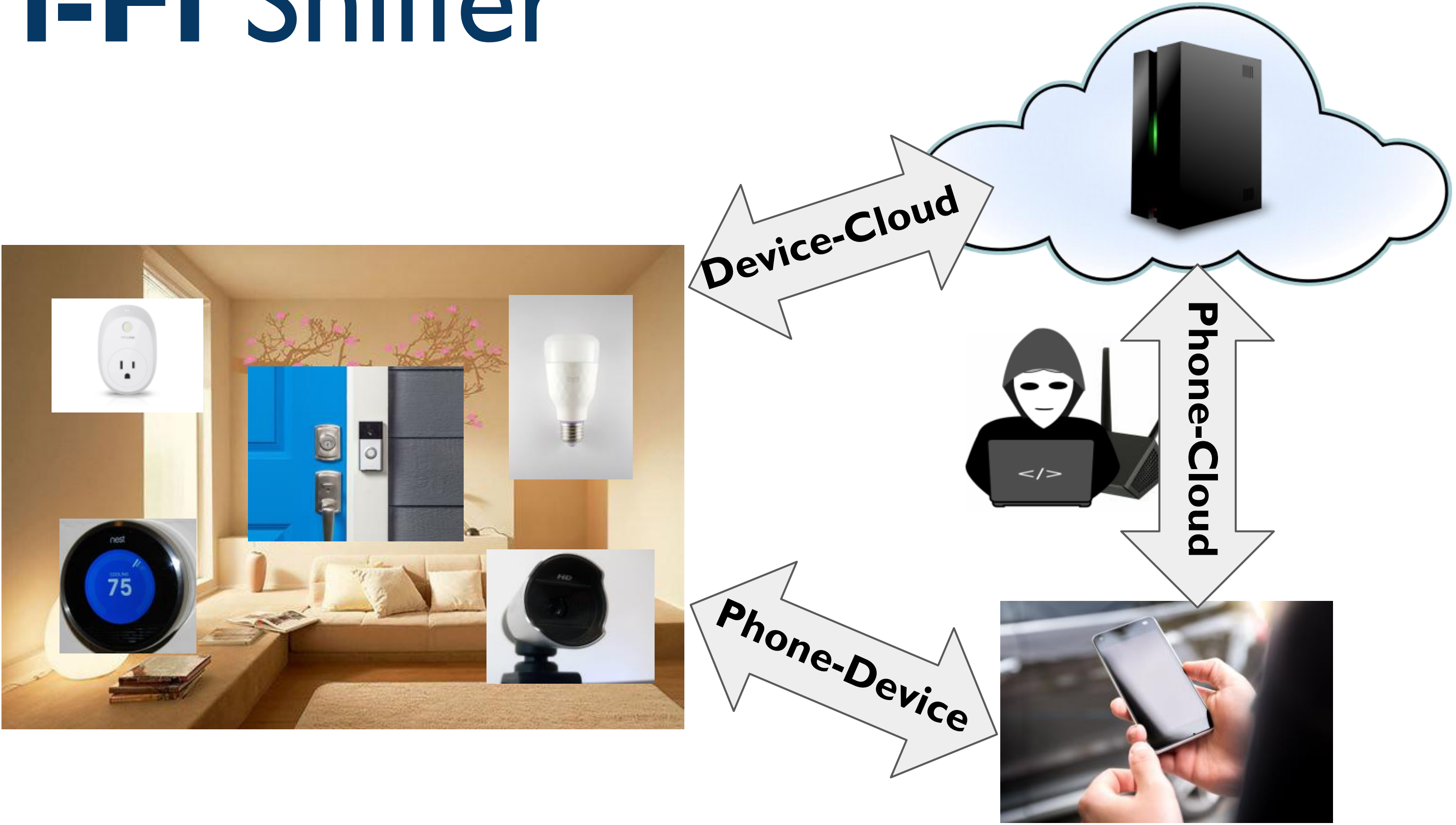
Wi-Fi Sniffer



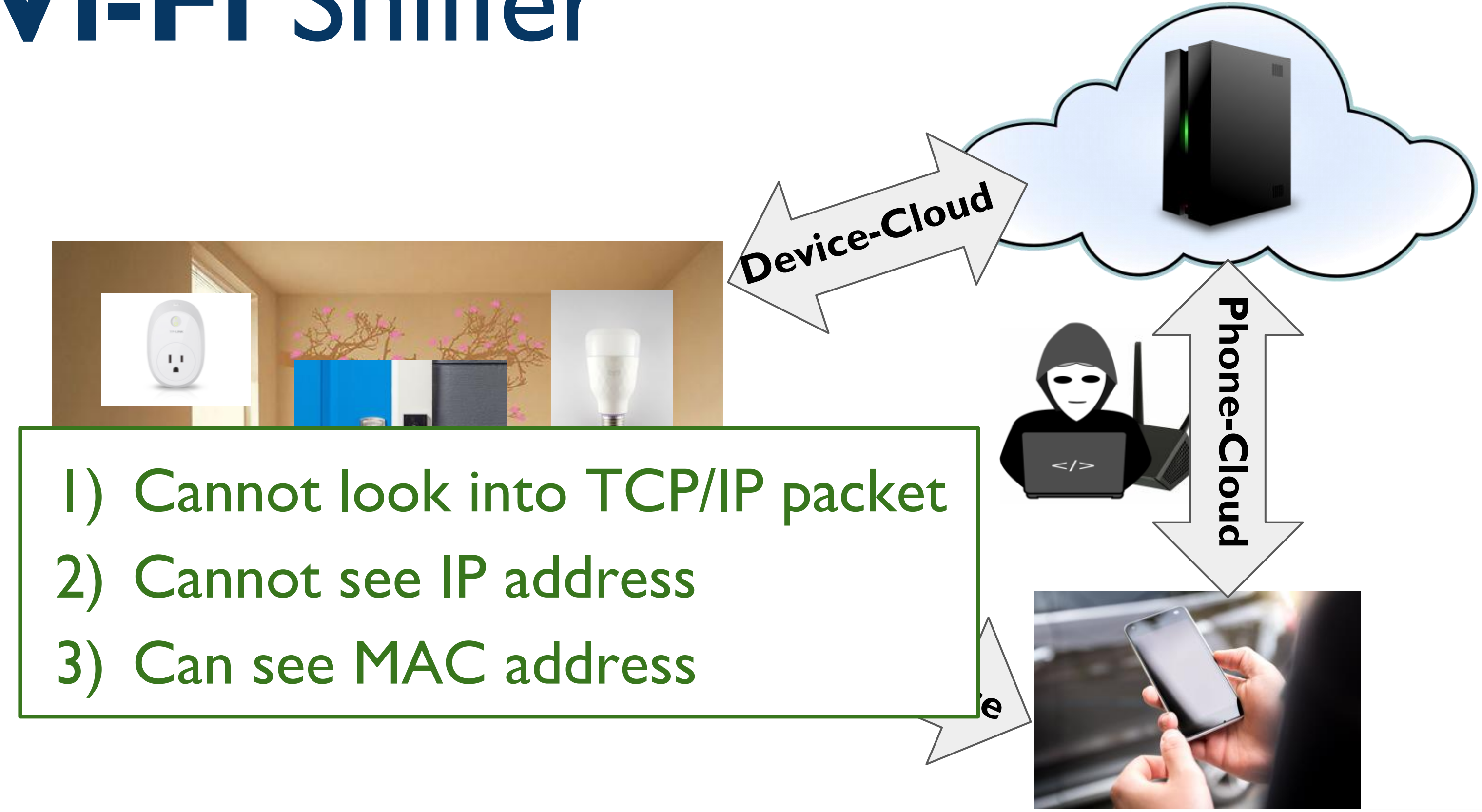
Wi-Fi Sniffer



Wi-Fi Sniffer



Wi-Fi Sniffer



1) Cannot look into TCP/IP packet
2) Cannot see IP address
3) Can see MAC address

State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)$^{\text{Homonit [CCS'18]}}$
- Volume-based$^{\text{Apthorpe et al. [PETS'19]}}$
- ML-based approaches$^{\text{HomeSnitch [WiSec'19]}}$
- IoT datasets$^{\text{Ren et al. [IMC'19], Alrawi et al. [S\&P'19]}}$

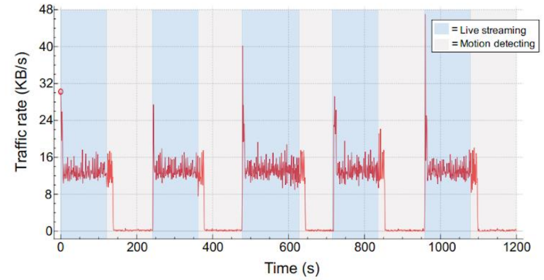
State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)[Homonit [CCS'18]]
- Volume-based[Apthorpe et al. [PETS'19]]
- ML-based approaches[HomeSnitch [WiSec'19]]
- IoT datasets[Ren et al. [IMC'19], Alrawi et al. [S&P'19]]

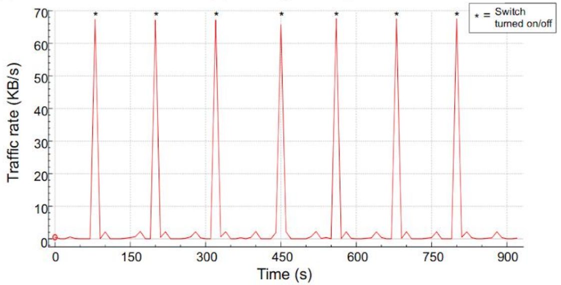
State-of-the-Art

- Specific protocols (ZigBee/Z-Wave) Homonit [CCS'18]
- Volume-based Apthorpe et al. [PETS'19]
- ML-based appr
- IoT datasets Rer

(a) Nest security camera – Video monitoring

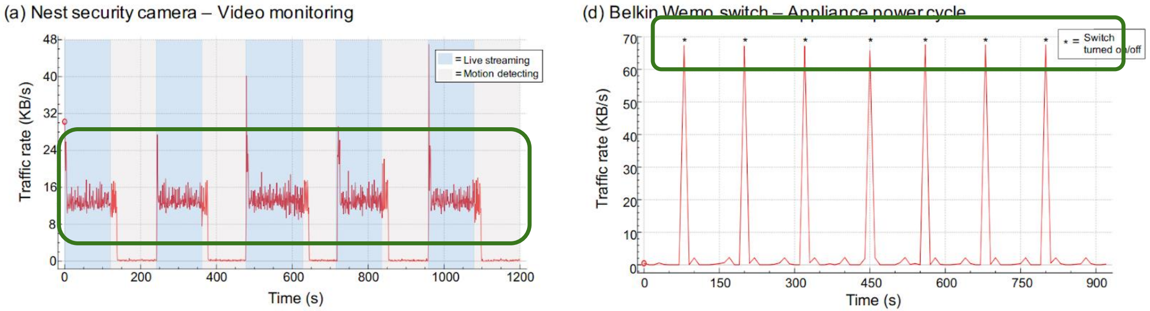


(d) Belkin Wemo switch – Appliance power cycle



State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)Homonit [CCS'18]
- Volume-basedApthorpe et al. [PETS'19]
- ML-based appr
- IoT datasetsRer



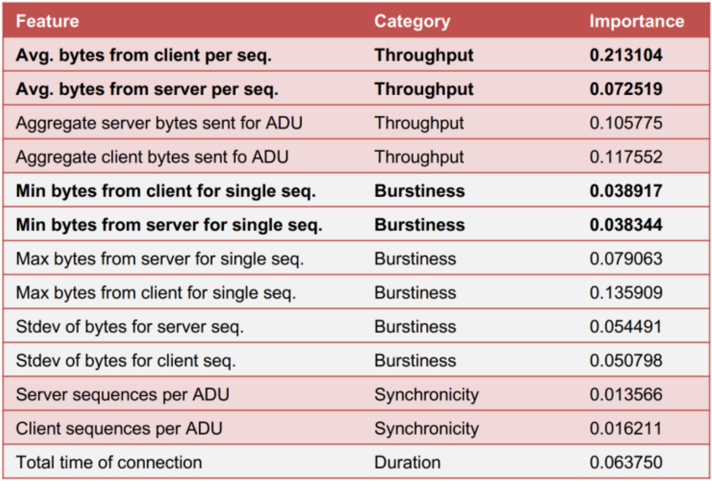
Volume spike is event

State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)$^{\text{Homonit [CCS'18]}}$
- Volume-based$^{\text{Apthorpe et al. [PETS'19]}}$
- ML-based approaches$^{\text{HomeSnitch [WiSec'19]}}$
- IoT datasets$^{\text{Ren et al. [IMC'19], Alrawi et al. [S\&P'19]}}$

State-of-the-Art

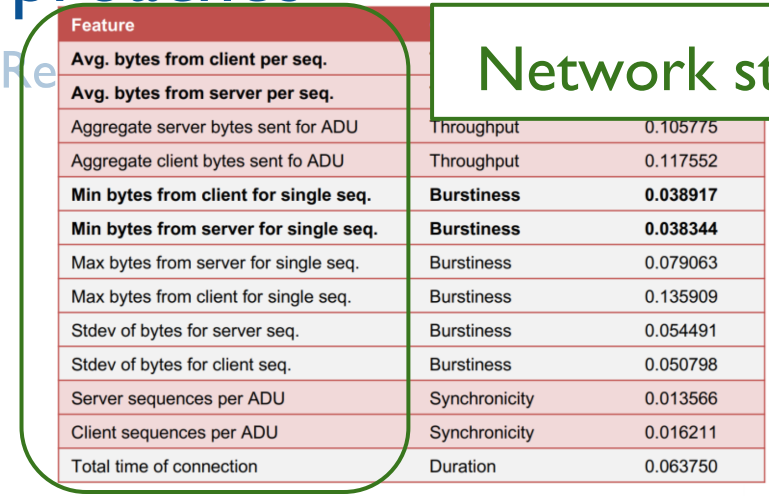
- Specific protocols (ZigBee/Z-Wave) Homonit [CCS'18]
- Volume-based Apthorpe et al. [PETS'19]
- **ML-based approaches** HomeSnitch [WiSec'19]
- IoT datasets Re &P'19]



Feature	Category	Importance
Avg. bytes from client per seq.	**Throughput**	**0.213104**
Avg. bytes from server per seq.	**Throughput**	**0.072519**
Aggregate server bytes sent for ADU	Throughput	0.105775
Aggregate client bytes sent fo ADU	Throughput	0.117552
Min bytes from client for single seq.	**Burstiness**	**0.038917**
Min bytes from server for single seq.	**Burstiness**	**0.038344**
Max bytes from server for single seq.	Burstiness	0.079063
Max bytes from client for single seq.	Burstiness	0.135909
Stdev of bytes for server seq.	Burstiness	0.054491
Stdev of bytes for client seq.	Burstiness	0.050798
Server sequences per ADU	Synchronicity	0.013566
Client sequences per ADU	Synchronicity	0.016211
Total time of connection	Duration	0.063750

State-of-the-Art

- Specific protocols (ZigBee/Z-Wave) Homonit [CCS'18]
- Volume-based Apthorpe et al. [PETS'19]
- ML-based approaches HomeSnitch [WiSec'19]
- IoT datasets Re



Feature		
Avg. bytes from client per seq.		
Avg. bytes from server per seq.		
Aggregate server bytes sent for ADU	Throughput	0.105775
Aggregate client bytes sent fo ADU	Throughput	0.117552
Min bytes from client for single seq.	**Burstiness**	**0.038917**
Min bytes from server for single seq.	**Burstiness**	**0.038344**
Max bytes from server for single seq.	Burstiness	0.079063
Max bytes from client for single seq.	Burstiness	0.135909
Stdev of bytes for server seq.	Burstiness	0.054491
Stdev of bytes for client seq.	Burstiness	0.050798
Server sequences per ADU	Synchronicity	0.013566
Client sequences per ADU	Synchronicity	0.016211
Total time of connection	Duration	0.063750

Network statistics as features

UCI University of California, Irvine

State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)Homonit [CCS'18]
- Volume-basedApthorpe et al. [PETS'19]
- ML-based approachesHomeSnitch [WiSec'19]
- IoT datasetsRen et al. [IMC'19], Alrawi et al. [S&P'19]

State-of-the-Art

- Specific protocols (ZigBe
- Volume-based Apthorpe et al. [
- ML-based approaches Hom
- IoT datasets Ren et al. [IMC'19], Alrawi et al. [S&P'19]

- Device study
  - Network traffic characteristics
- Public datasets
  - Mon(IoT)r
    https://moniotrlab.ccis.neu.edu/imc19/
  - YourThings
    https://yourthings.info/

Outline

I. Background and Problem Statement

II. Key Observation: Packet-Level Signatures

III. The PingPong System

IV. Conclusion

Outline

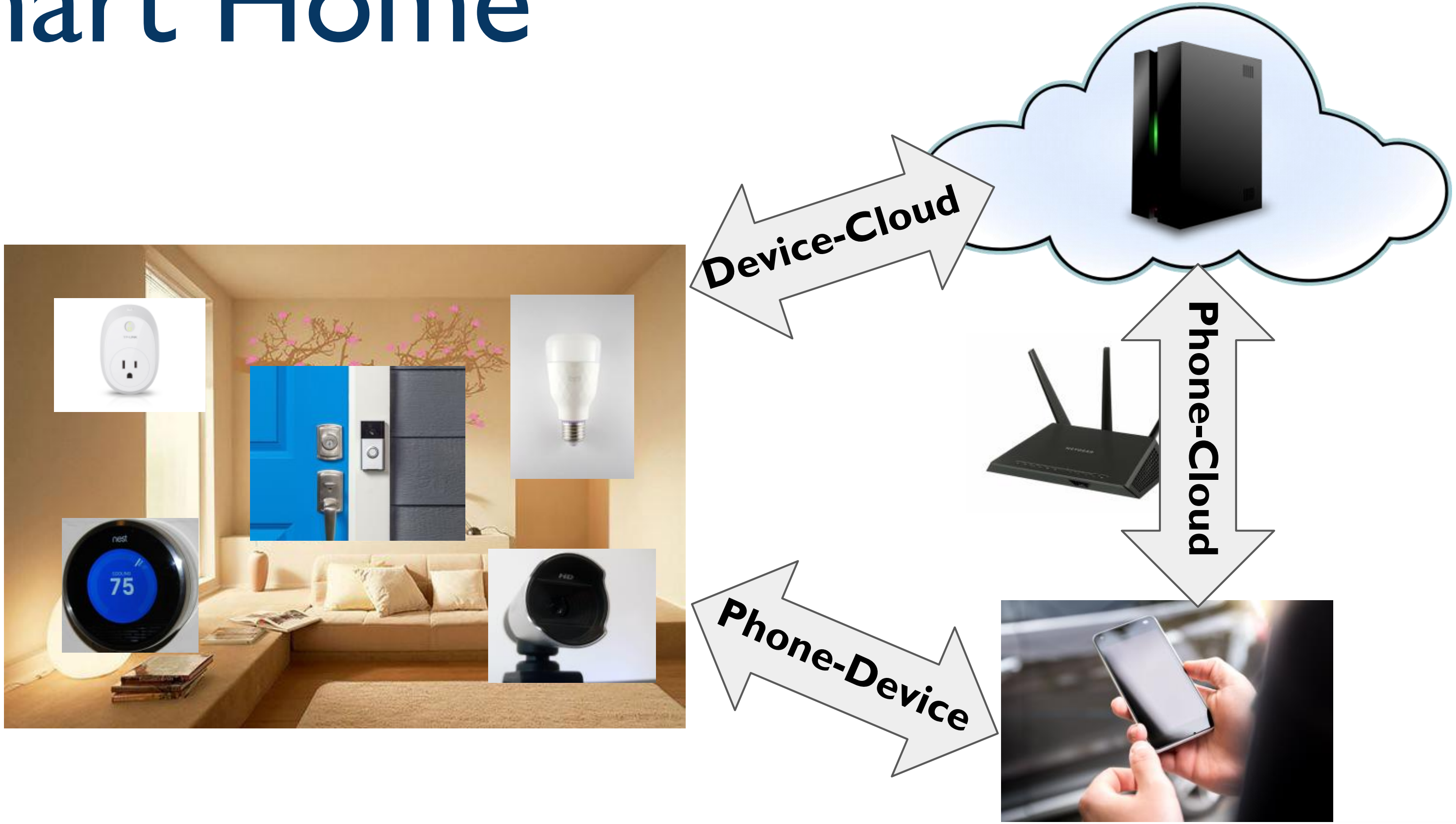
I. Background and Problem Statement

II. Key Observation: Packet-Level Signatures

III. The PingPong System

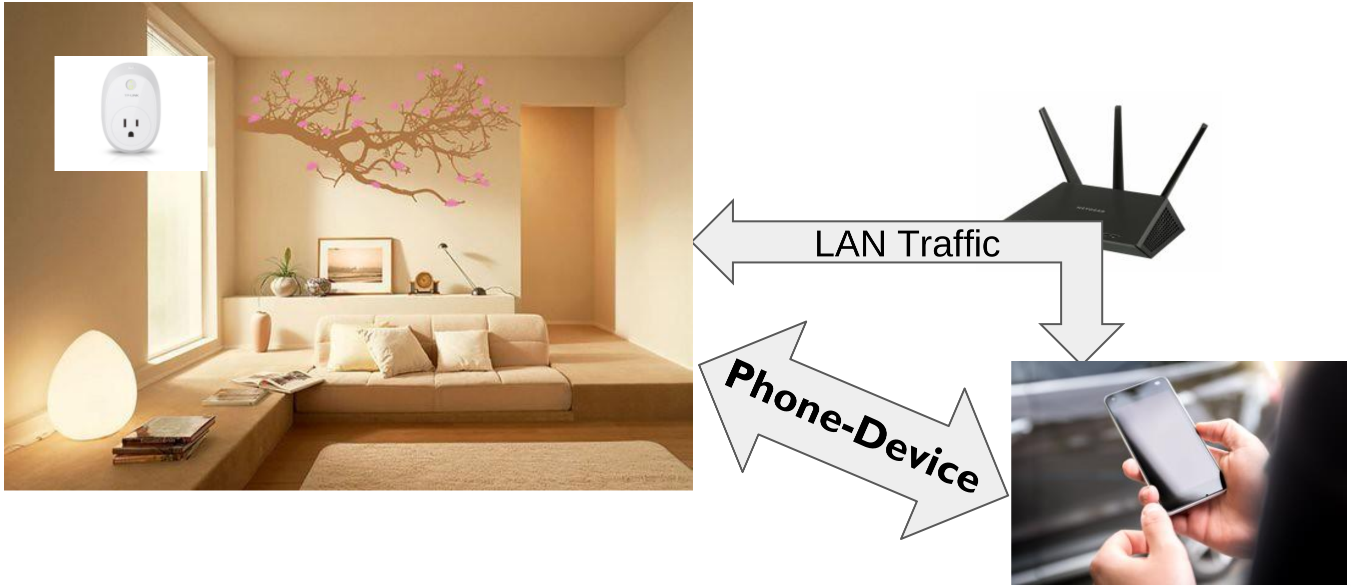
IV. Conclusion

Smart Home



Local Phone

Toggle ON Plug

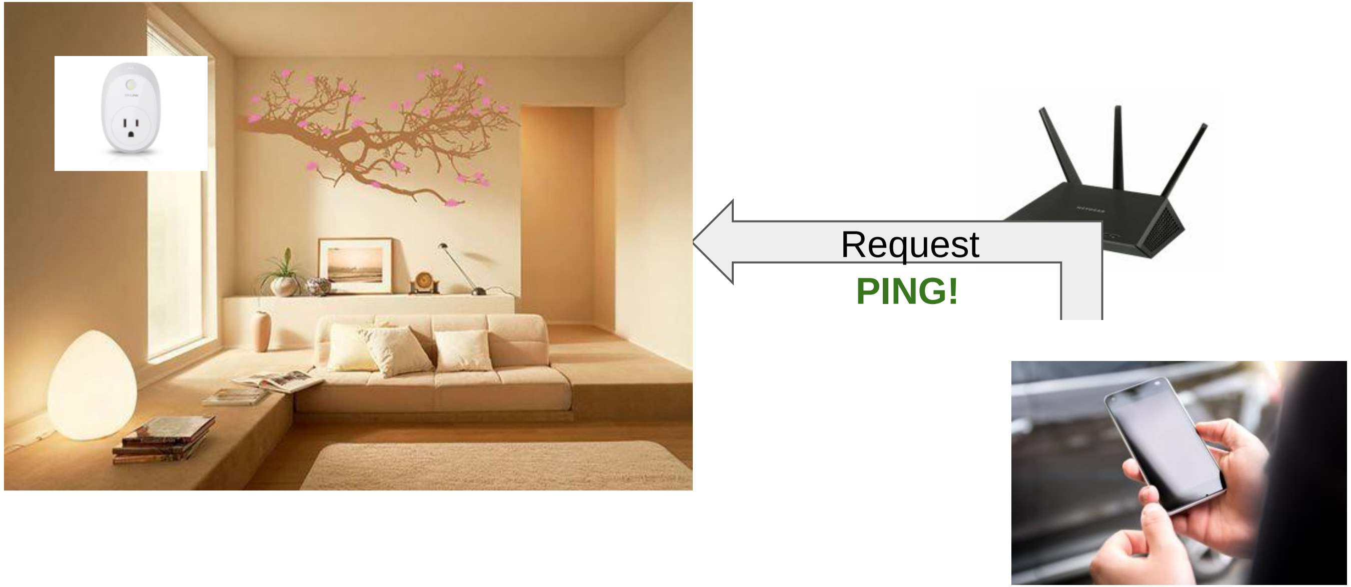


LAN Traffic

Phone-Device

Key Observation: Ping-Pong

Toggle ON Plug

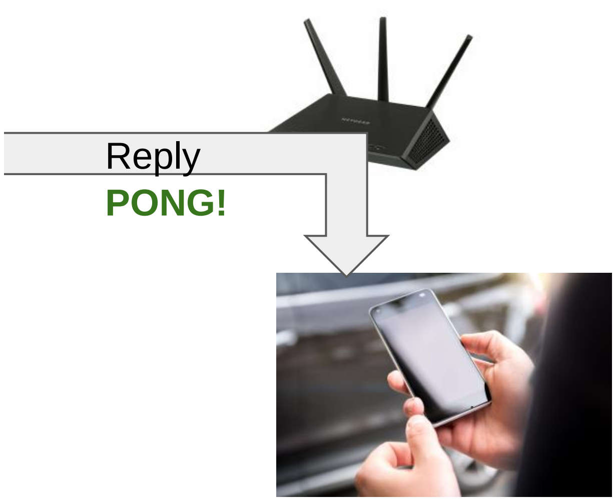


Request

PING!

Key Observation: Ping-Pong

Toggle ON Plug

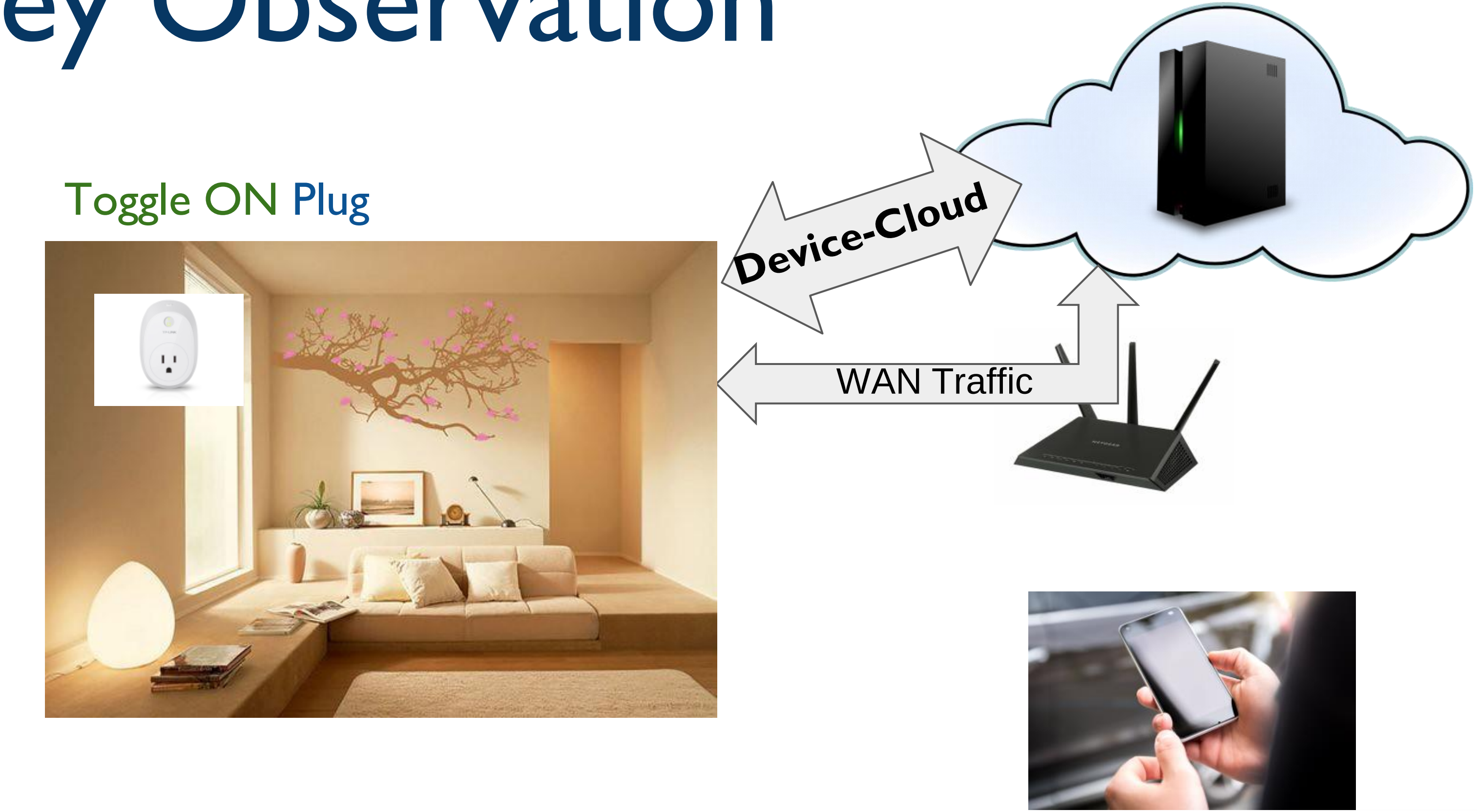


Reply

PONG!

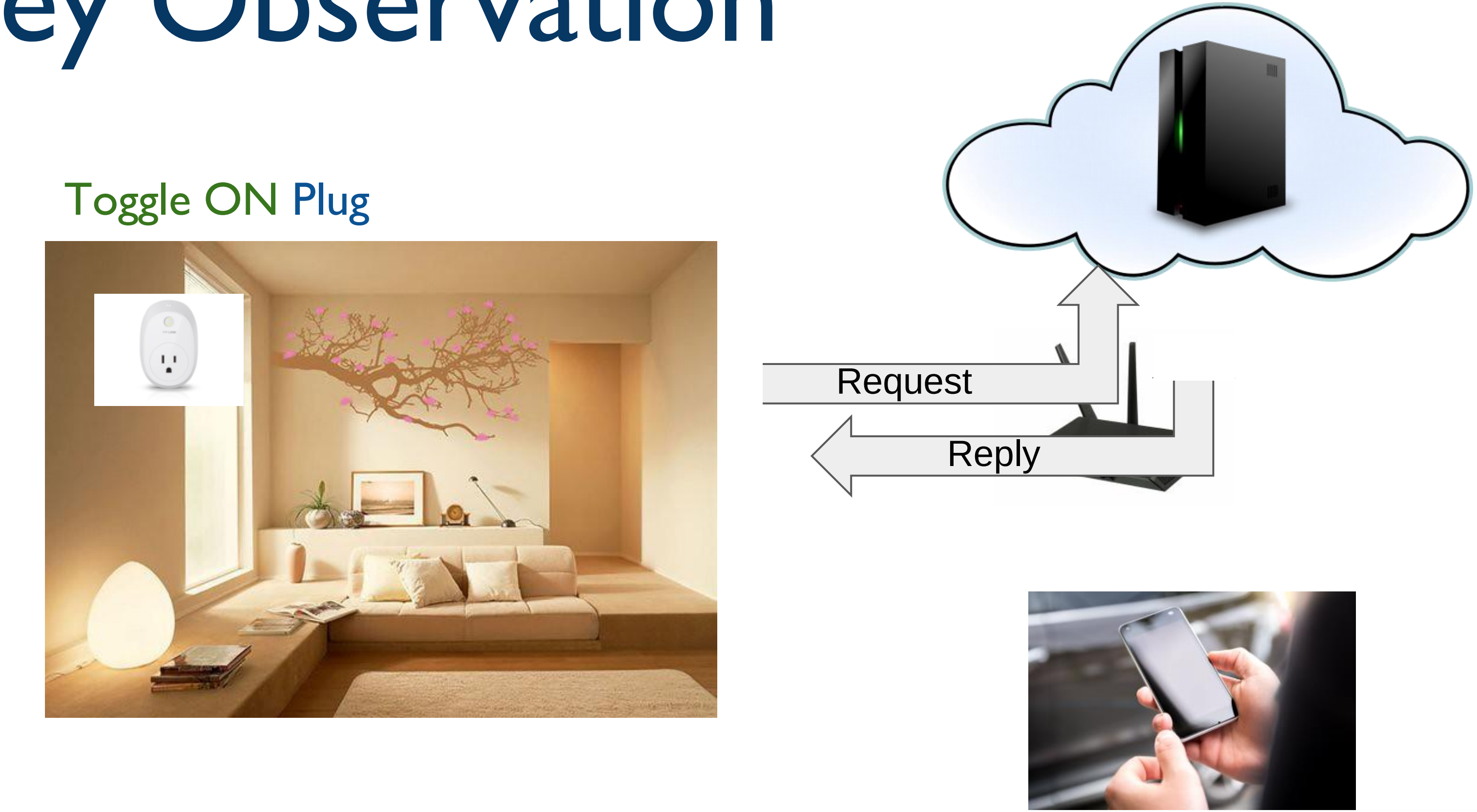
Key Observation

Toggle ON Plug



Key Observation

Toggle ON Plug

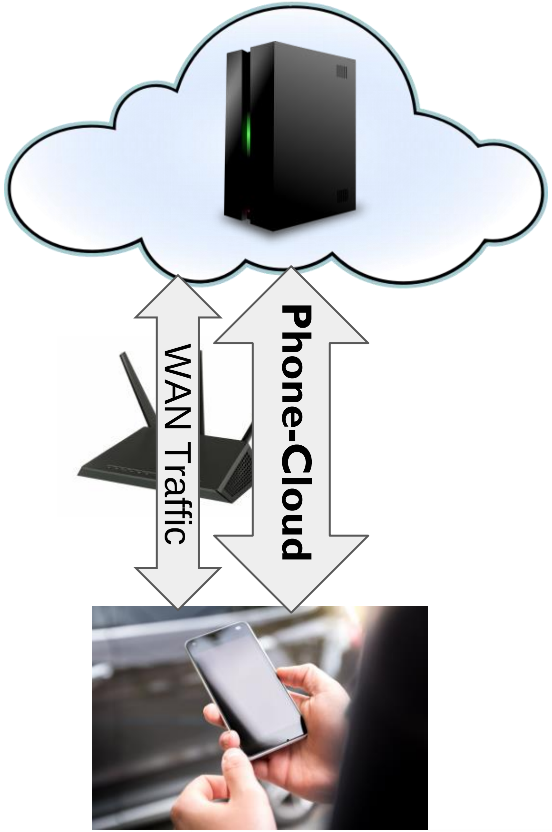


Request

Reply

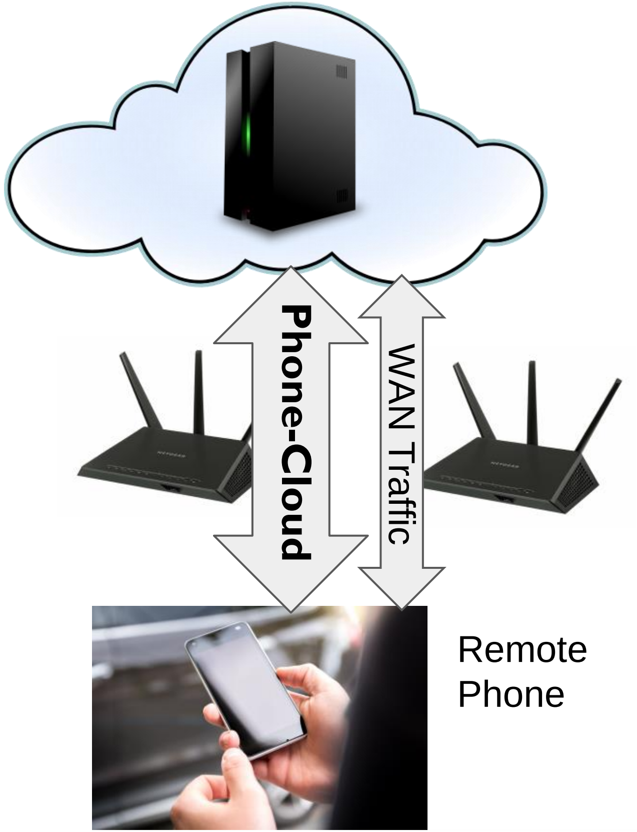
Remote Phone

Toggle ON Plug



Remote Phone

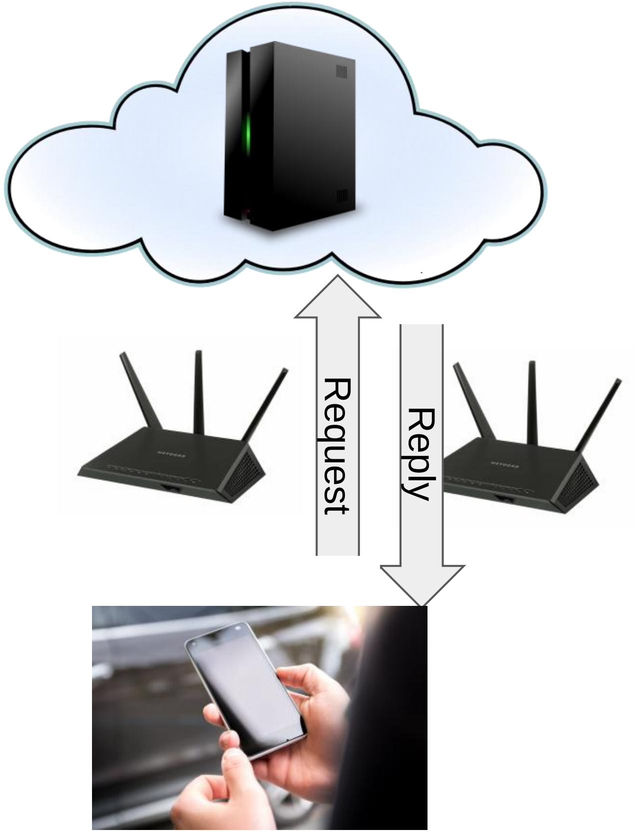
Toggle ON Plug



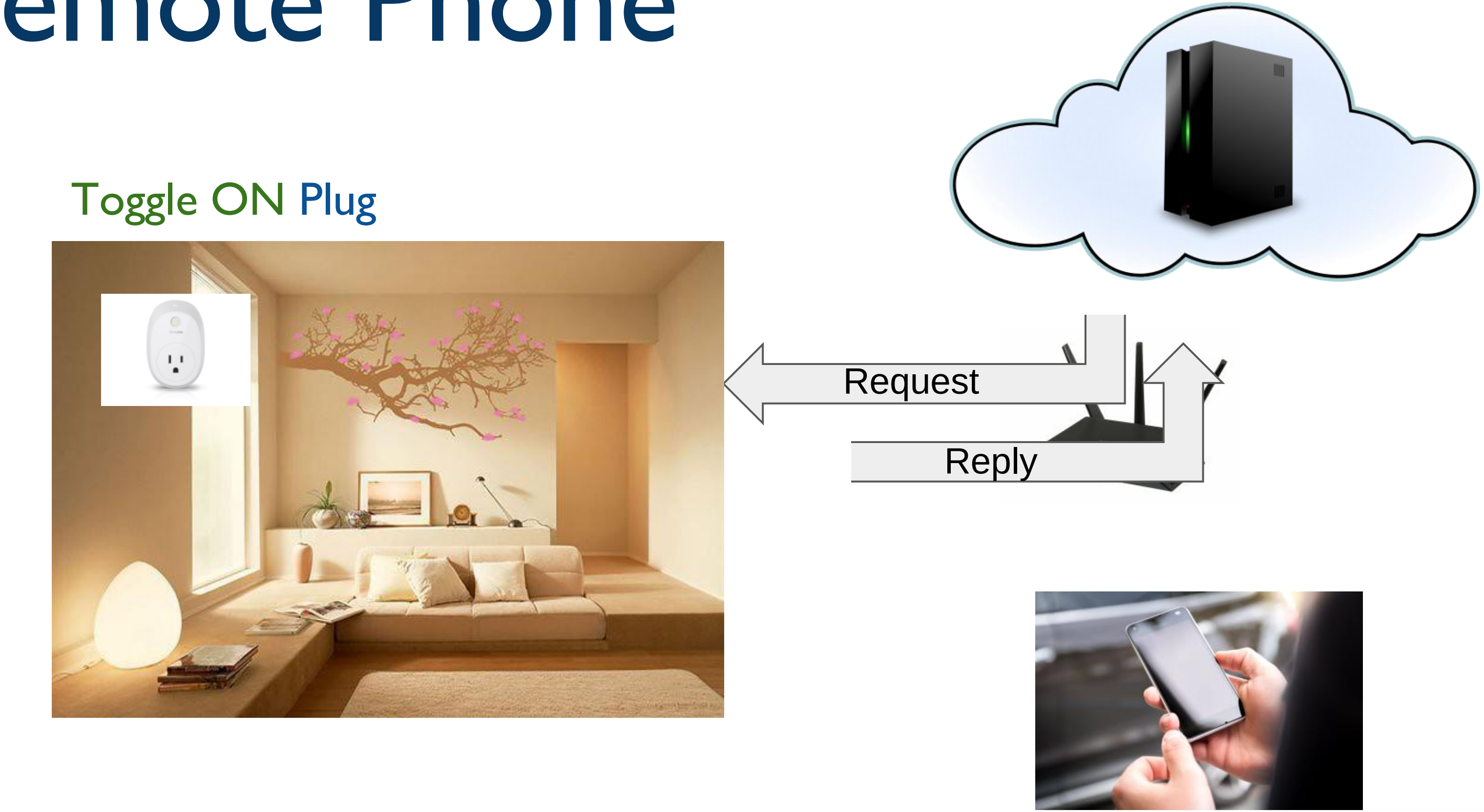
UCI University of California, Irvine

Remote Phone

Toggle ON Plug



Remote Phone



Toggle ON Plug

Request

Reply

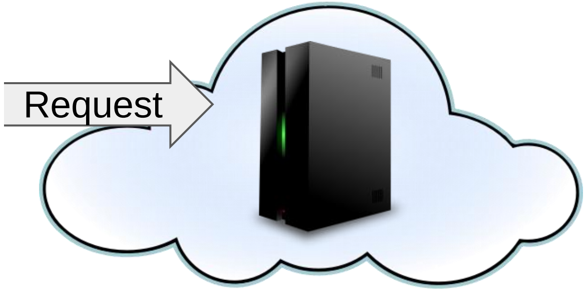
Home Automation

Home
Automation

Toggle ON Plug

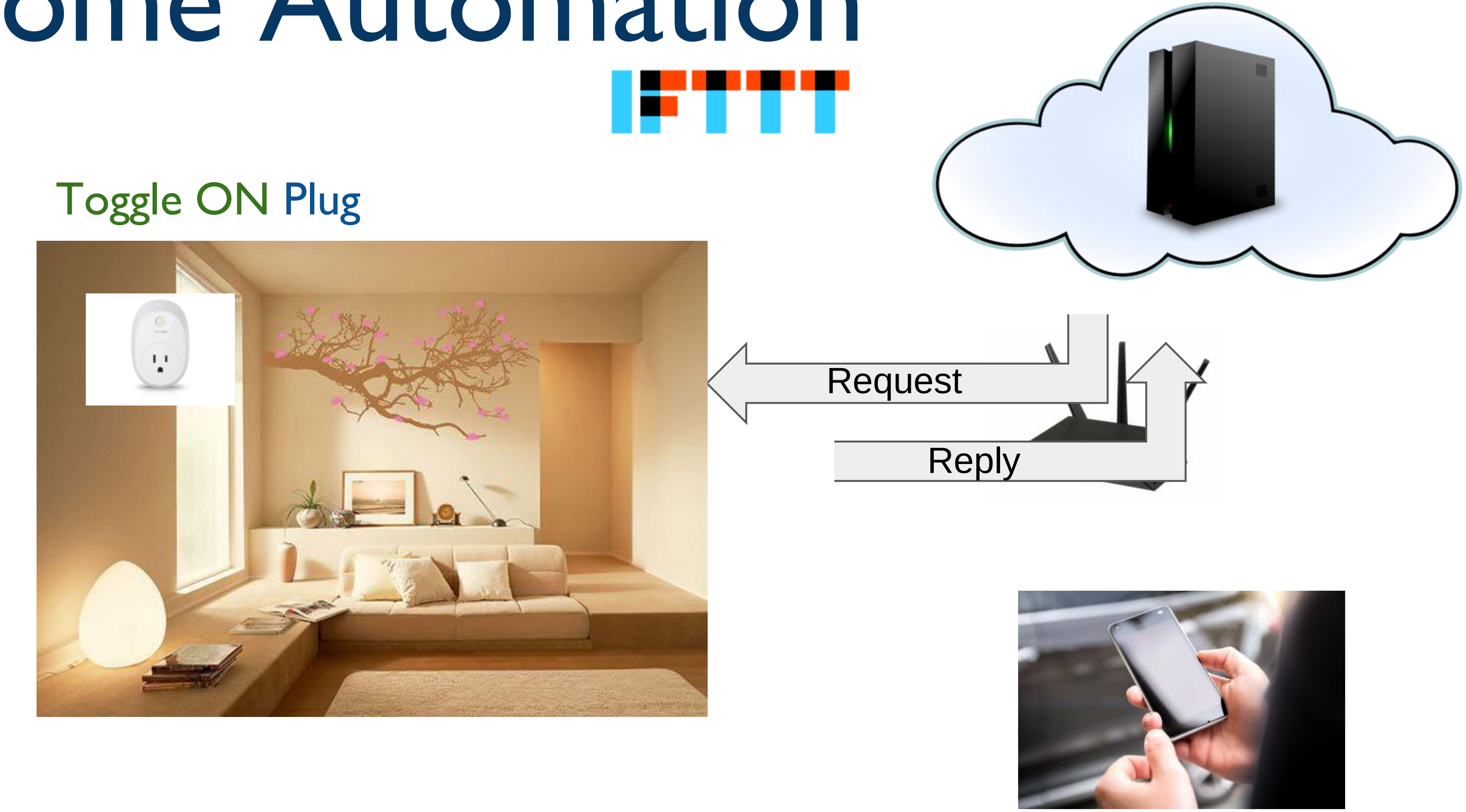
Home Automation

IFTTT

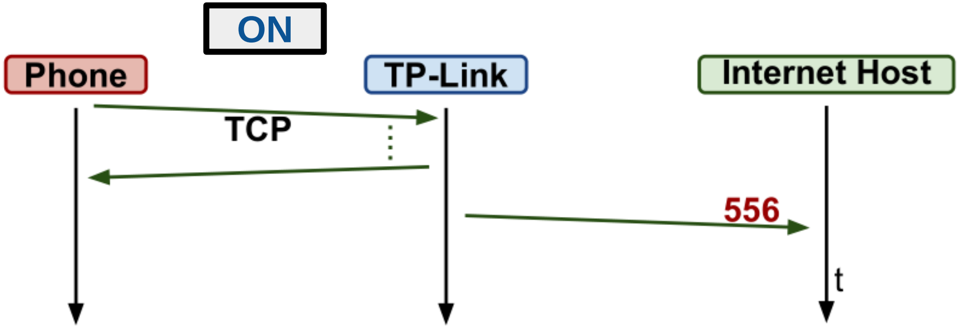


Toggle ON Plug

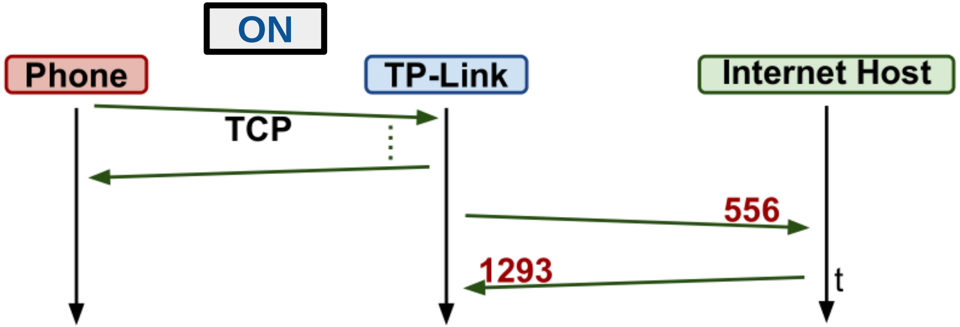
Home Automation



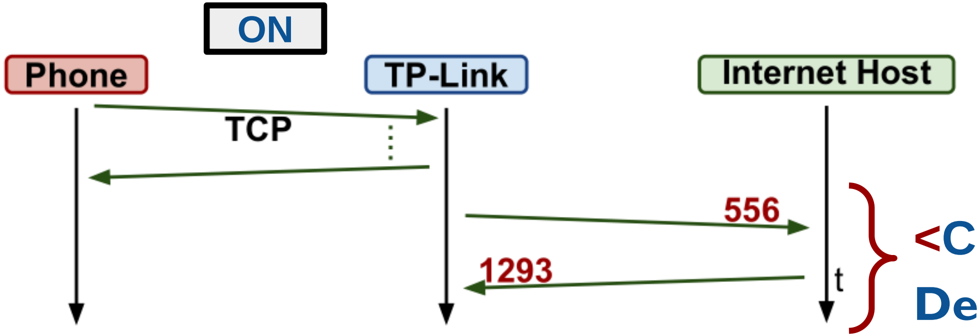
Ping-Pong in TP-Link Plug



Ping-Pong in TP-Link Plug



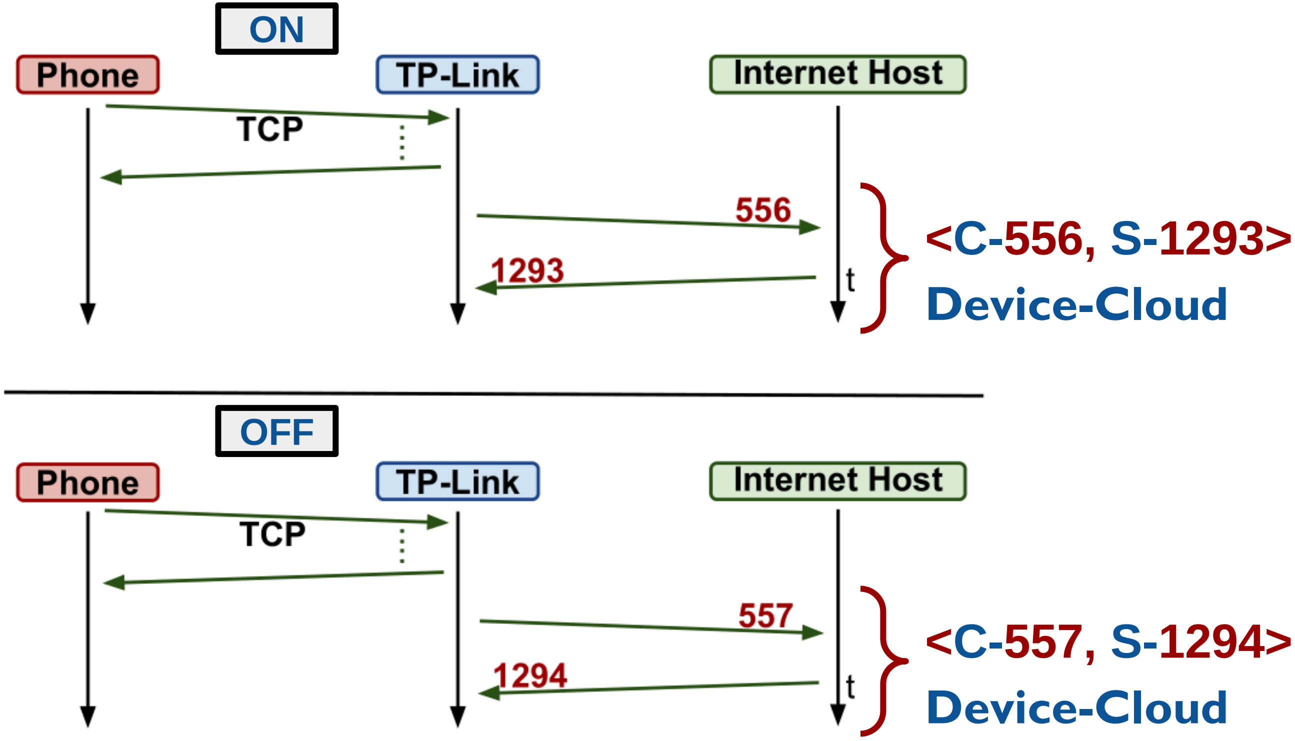
Ping-Pong in TP-Link Plug



<C-556, S-1293>

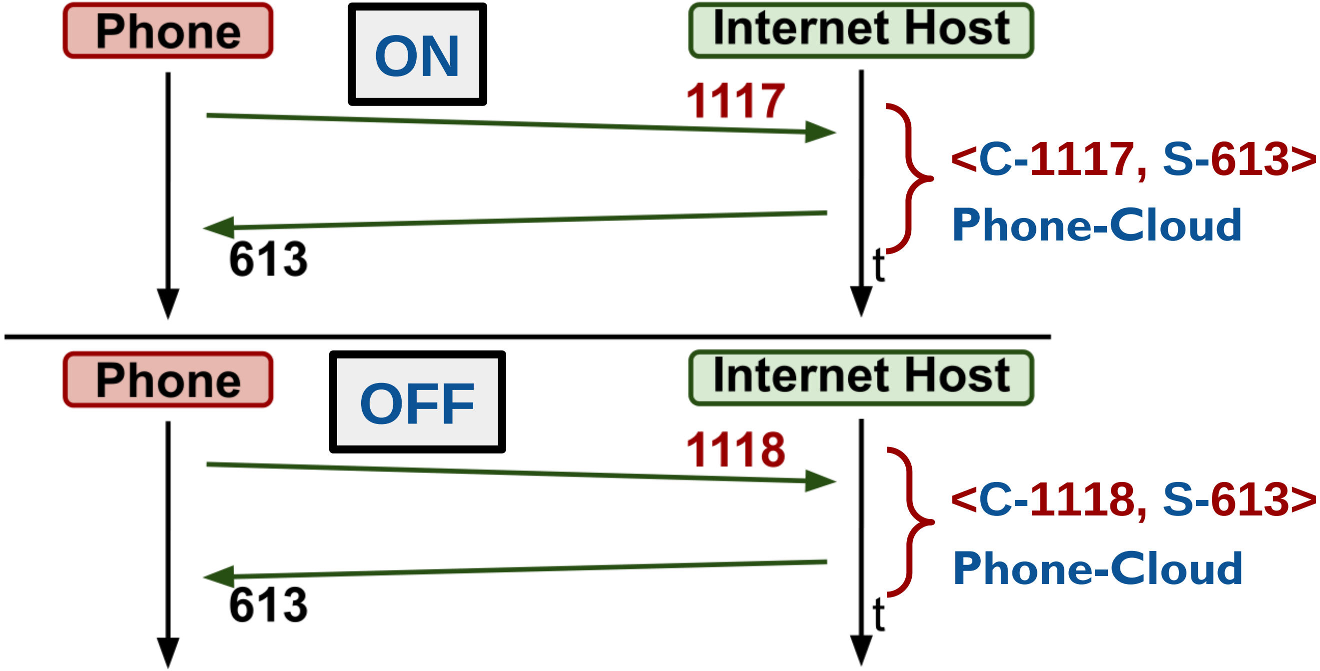
Device-Cloud

Ping-Pong in TP-Link Plug



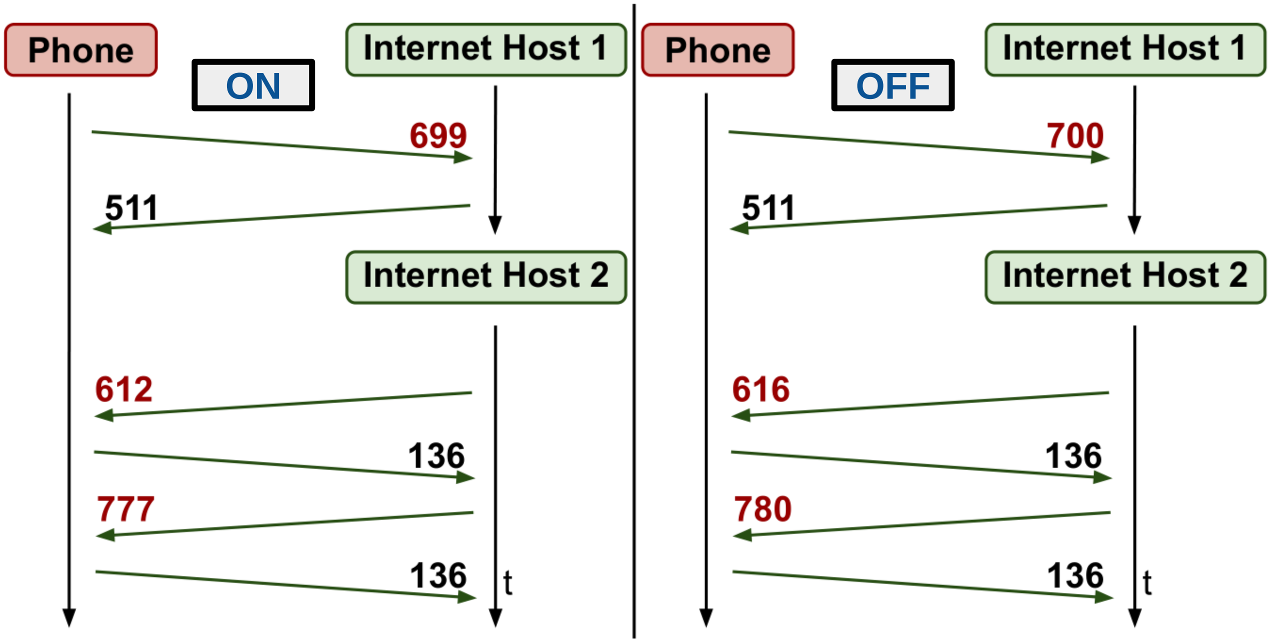
UCI University of California, Irvine

Ping-Pong in D-Link Plug



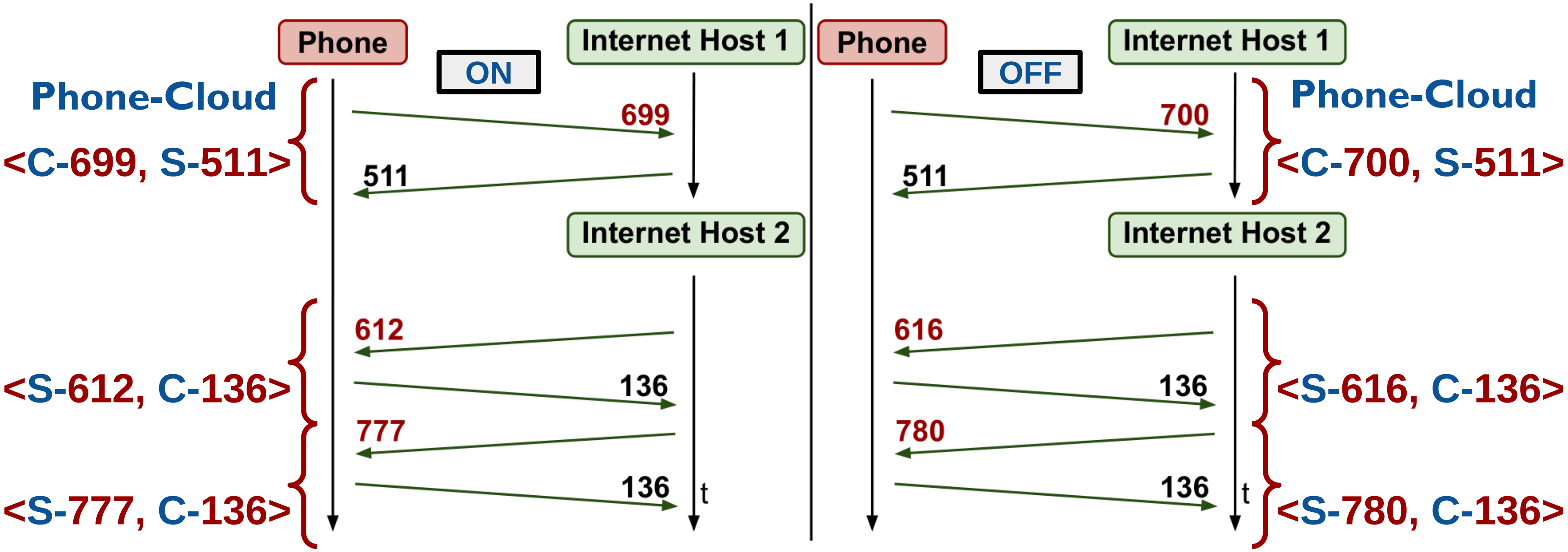
UCI University of California, Irvine

Ping-Pong in SmartThings Plug



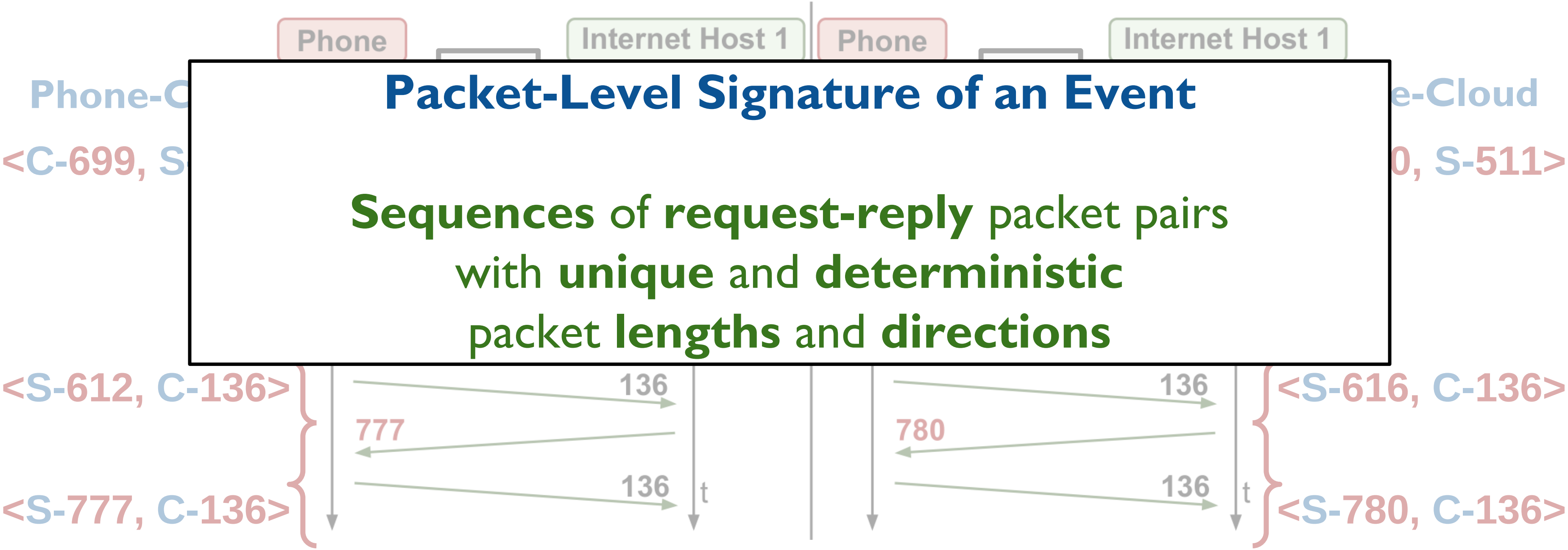
UCI University of California, Irvine

Ping-Pong in SmartThings Plug



UCI University of California, Irvine

Ping-Pong in SmartThings Plug



Packet-Level Signature of an Event

Sequences of **request-reply** packet pairs with **unique** and **deterministic** packet **lengths** and **directions**

Research Questions

- How to **automatically** extract packet-level signatures?
- How **universal** are packet-level signatures?
- How **unique** are packet-level signatures?

Research Questions

- How to **automatically** extract packet-level signatures?
- How **universal** are packet-level signatures?
- How **unique** are packet-level signatures?

Outline

I. Background and Problem Statement

II. Key Observation: Packet-Level Signatures

III. The PingPong System

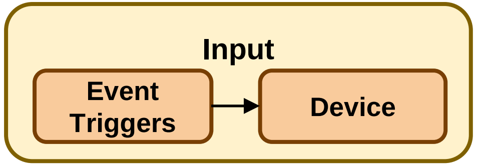
IV. Conclusion

Automated Extraction

- **Extract** these pairs
- Form **longest** possible **sequences**
- Use them as a **signature**

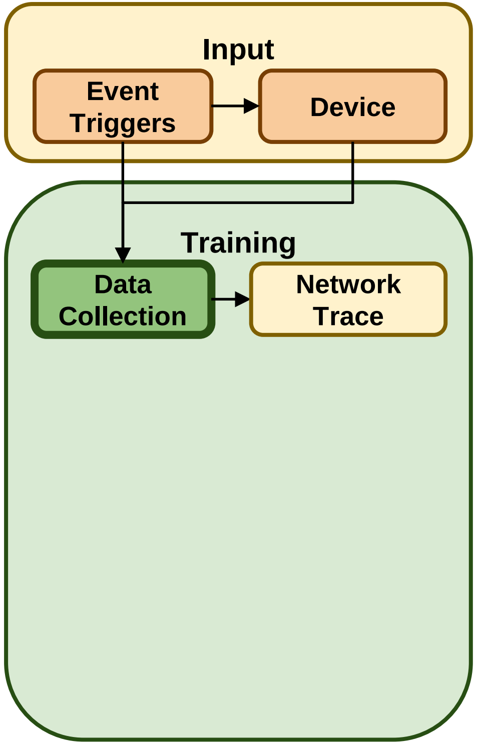
PingPong Training

The PingPong System



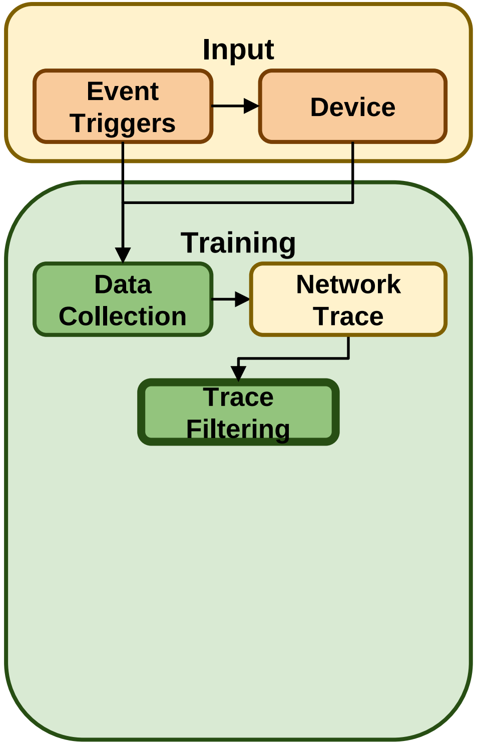
PingPong Training

The PingPong System



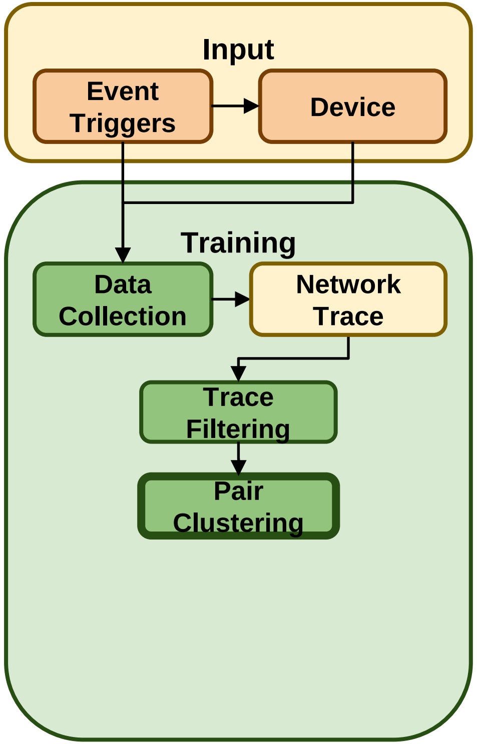
PingPong Training

The PingPong System



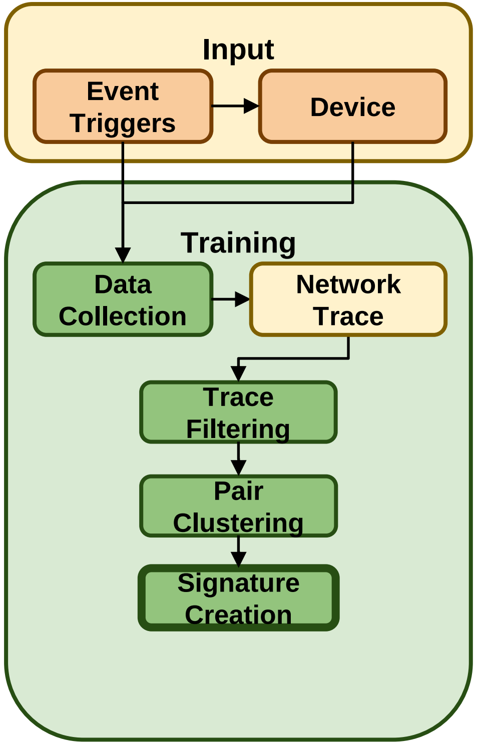
PingPong Training

The PingPong System



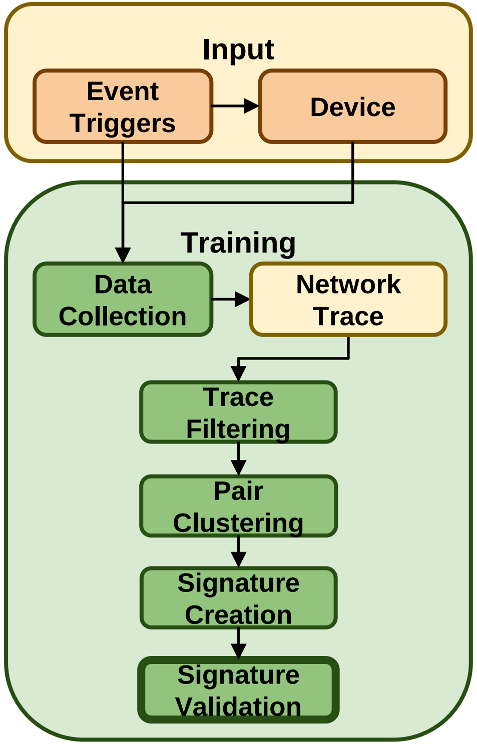
PingPong Training

The PingPong System



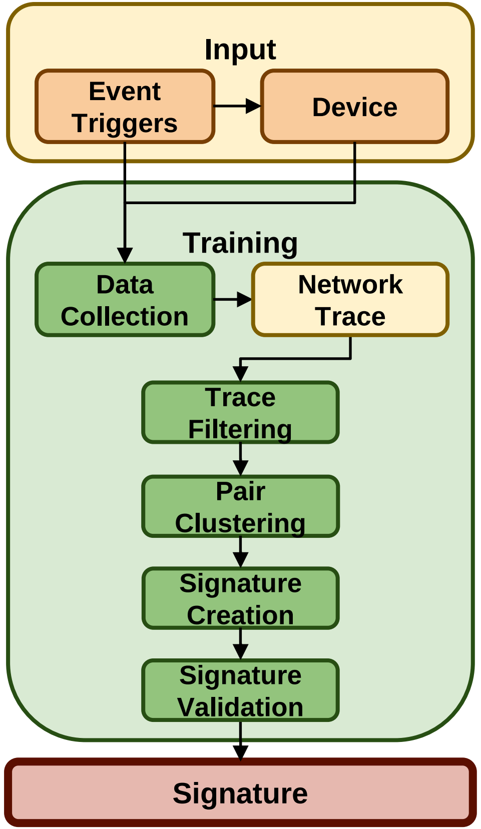
PingPong Training

The PingPong System



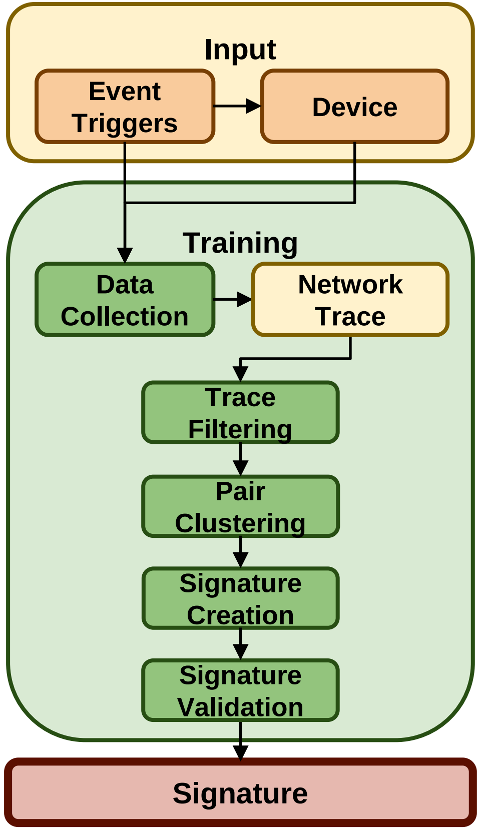
PingPong Training

The PingPong System



PingPong Training

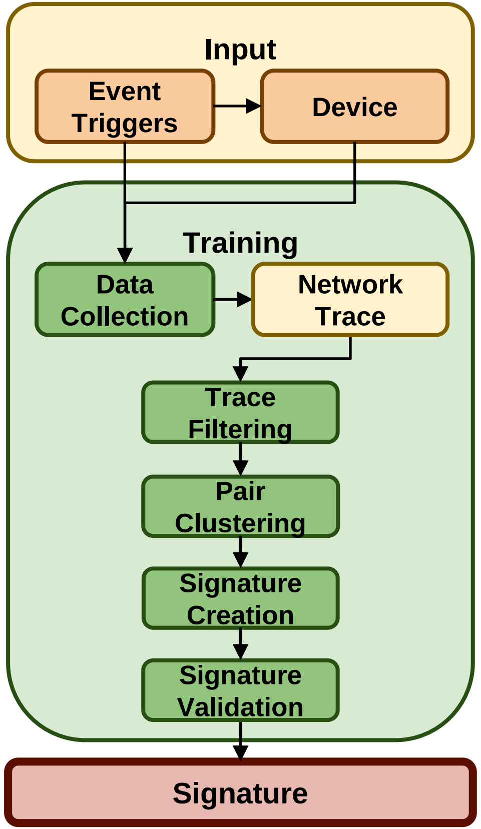
The PingPong System



C-556 S-1293

PingPong Training

The PingPong System



Input

Event Triggers

Device

Training

Data Collection

Network Trace

Trace Filtering

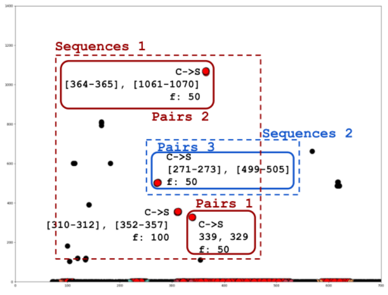
Pair Clustering

Signature Creation

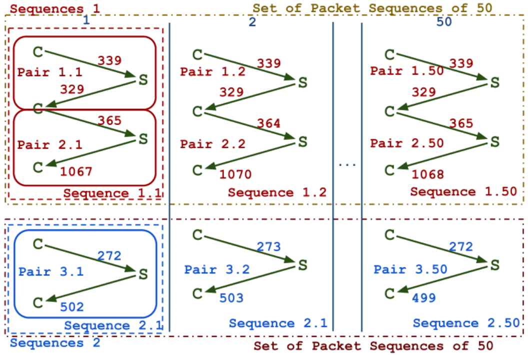
Signature Validation

Signature

C-556 S-1293



(b) Arlo Camera

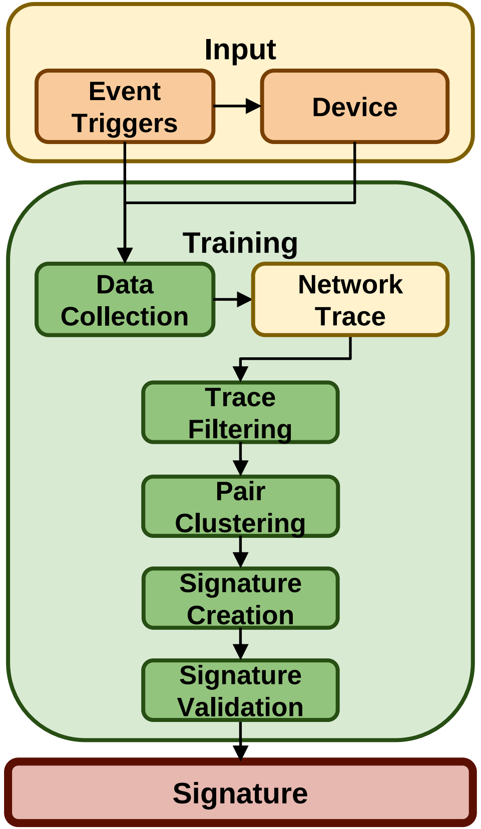


C-339 S-329 C-[364-365] S-[1061-1070]

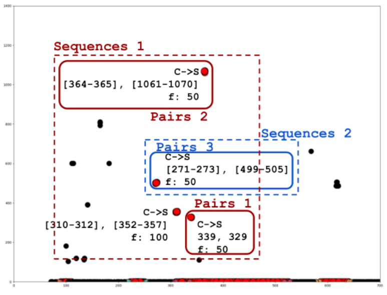
C-[271-273] S-[499-505]

PingPong Training

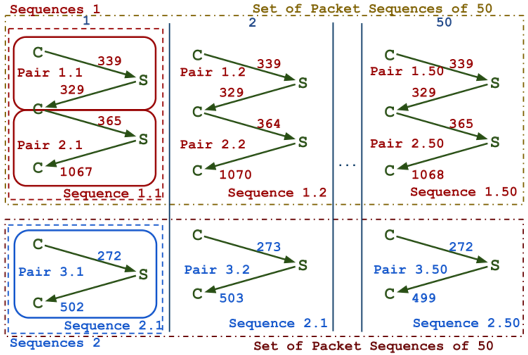
The PingPong System



C-556 S-1293



(b) Arlo Camera



C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

UCI University of California, Irvine

Research Questions

- How to **automatically** extract packet-level signatures? ✓
- How **universal** are packet-level signatures?
- How **unique** are packet-level signatures?

Research Questions

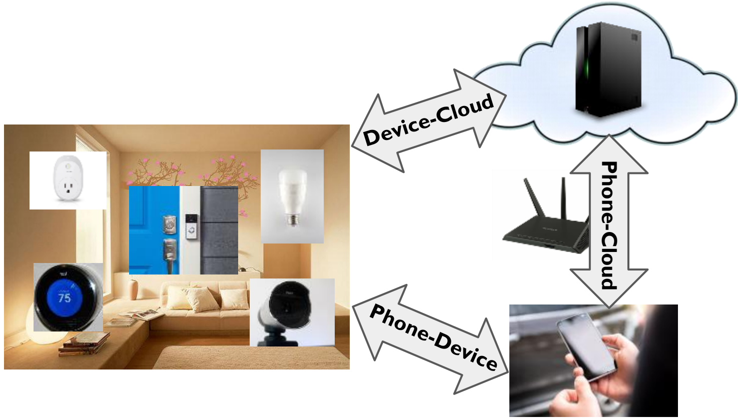
- How to **automatically** extract packet-level signatures? ✓
- How **universal** are packet-level signatures?
- How **unique** are packet-level signatures?

Universal Signatures

- **Three** communications

Universal Signatures

- **Three** communications



Universal Signatures

- **Three** communications
- **Two** adversaries
  - **WAN** and **Wi-Fi** sniffers

Universal Signatures

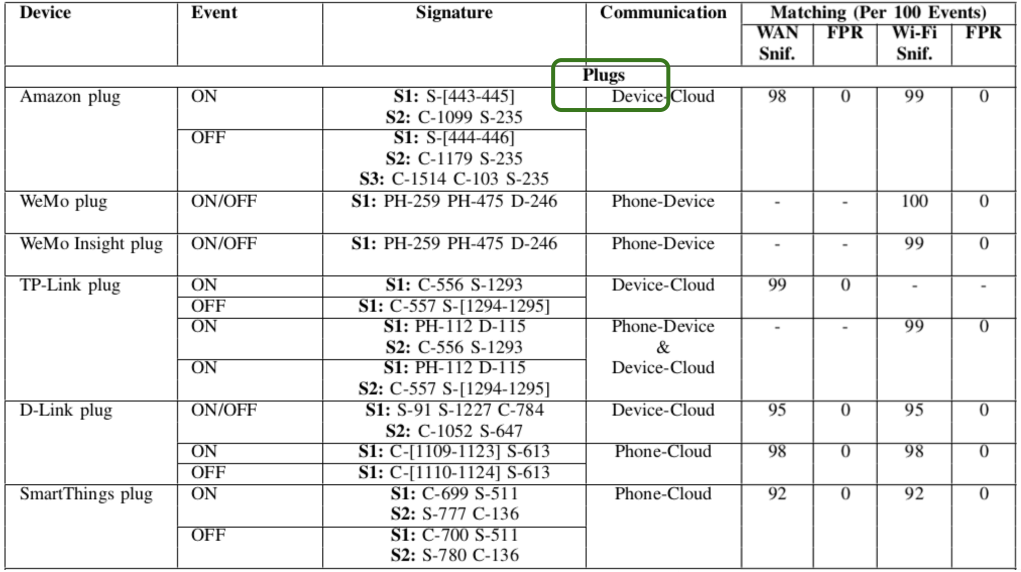
- **Three** communications
- **Two** adversaries
  - **WAN** and **Wi-Fi** sniffers
- Different triggers
  - **Local**-Phone

Universal Signatures

- Applies to many devices
  - Our corpus: **18** devices

Universal Signatures

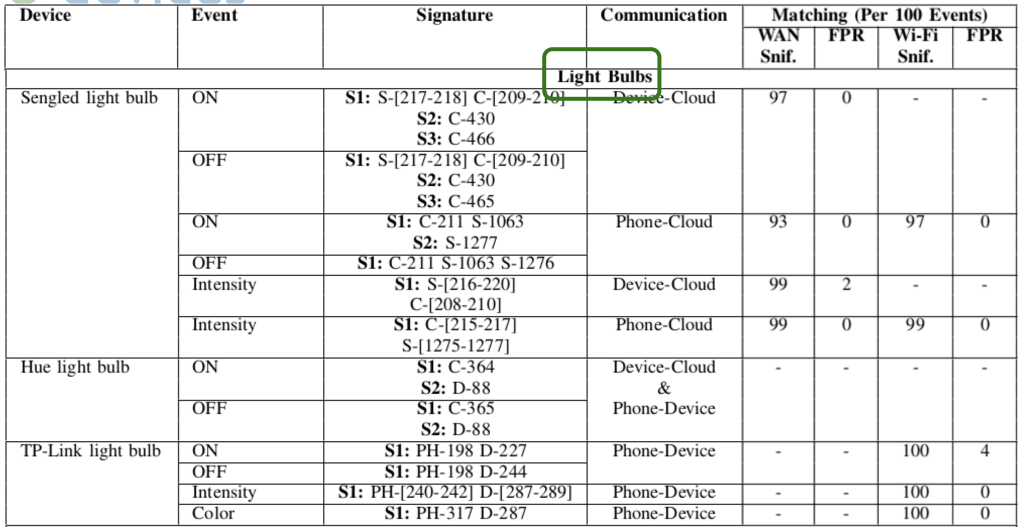
- Applies to many devices
  - Our corpus: 18 devices



Device	Event	Signature	Communication	Matching (Per 100 Events)			
				WAN Snif.	FPR	Wi-Fi Snif.	FPR
			Plugs				
Amazon plug	ON	**S1:** S-[443-445] **S2:** C-1099 S-235	Device-Cloud	98	0	99	0
	OFF	**S1:** S-[444-446] **S2:** C-1179 S-235 **S3:** C-1514 C-103 S-235					
WeMo plug	ON/OFF	**S1:** PH-259 PH-475 D-246	Phone-Device	-	-	100	0
WeMo Insight plug	ON/OFF	**S1:** PH-259 PH-475 D-246	Phone-Device	-	-	99	0
TP-Link plug	ON	**S1:** C-556 S-1293	Device-Cloud	99	0	-	-
	OFF	**S1:** C-557 S-[1294-1295]					
	ON	**S1:** PH-112 D-115 **S2:** C-556 S-1293	Phone-Device & Device-Cloud	-	-	99	0
	ON	**S1:** PH-112 D-115 **S2:** C-557 S-[1294-1295]					
D-Link plug	ON/OFF	**S1:** S-91 S-1227 C-784 **S2:** C-1052 S-647	Device-Cloud	95	0	95	0
	ON	**S1:** C-[1109-1123] S-613	Phone-Cloud	98	0	98	0
	OFF	**S1:** C-[1110-1124] S-613					
SmartThings plug	ON	**S1:** C-699 S-511 **S2:** S-777 C-136	Phone-Cloud	92	0	92	0
	OFF	**S1:** C-700 S-511 **S2:** S-780 C-136					

Universal Signatures

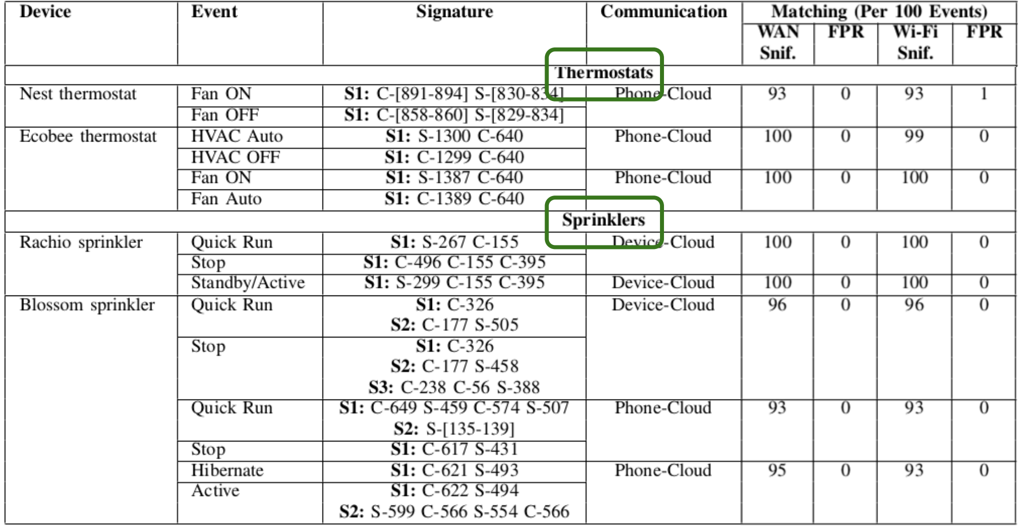
- Applies to many devices
  - Our corpus: 18 devices



Device	Event	Signature	Communication	Matching (Per 100 Events)			
				WAN Snif.	FPR	Wi-Fi Snif.	FPR
		Light Bulbs					
Sengled light bulb	ON	**S1:** S-[217-218] C-[209-210] **S2:** C-430 **S3:** C-466	Device-Cloud	97	0	-	-
	OFF	**S1:** S-[217-218] C-[209-210] **S2:** C-430 **S3:** C-465					
	ON	**S1:** C-211 S-1063 **S2:** S-1277	Phone-Cloud	93	0	97	0
	OFF	**S1:** C-211 S-1063 S-1276					
	Intensity	**S1:** S-[216-220] C-[208-210]	Device-Cloud	99	2	-	-
	Intensity	**S1:** C-[215-217] S-[1275-1277]	Phone-Cloud	99	0	99	0
Hue light bulb	ON	**S1:** C-364 **S2:** D-88	Device-Cloud & Phone-Device	-	-	-	-
	OFF	**S1:** C-365 **S2:** D-88					
TP-Link light bulb	ON	**S1:** PH-198 D-227	Phone-Device	-	-	100	4
	OFF	**S1:** PH-198 D-244					
	Intensity	**S1:** PH-[240-242] D-[287-289]	Phone-Device	-	-	100	0
	Color	**S1:** PH-317 D-287	Phone-Device	-	-	100	0

Universal Signatures

- Applies to many devices
  - Our corpus: 18 devices

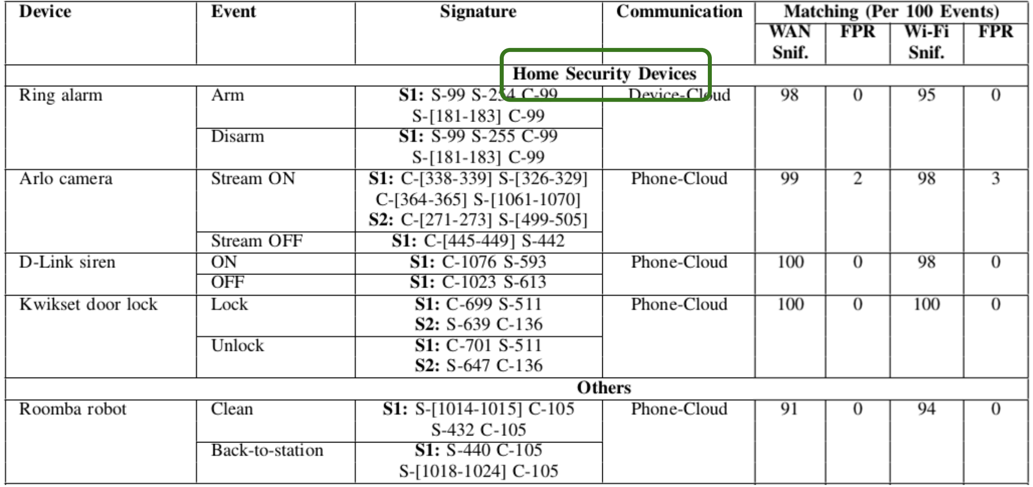


Device	Event	Signature	Communication	Matching (Per 100 Events)			
				WAN Snif.	FPR	Wi-Fi Snif.	FPR
Thermostats							
Nest thermostat	Fan ON	**S1:** C-[891-894] S-[830-834]	Phone-Cloud	93	0	93	1
	Fan OFF	**S1:** C-[858-860] S-[829-834]					
Ecobee thermostat	HVAC Auto	**S1:** S-1300 C-640	Phone-Cloud	100	0	99	0
	HVAC OFF	**S1:** C-1299 C-640					
	Fan ON	**S1:** S-1387 C-640	Phone-Cloud	100	0	100	0
	Fan Auto	**S1:** C-1389 C-640					
Sprinklers							
Rachio sprinkler	Quick Run	**S1:** S-267 C-155	Device-Cloud	100	0	100	0
	Stop	**S1:** C-496 C-155 C-395					
	Standby/Active	**S1:** S-299 C-155 C-395	Device-Cloud	100	0	100	0
Blossom sprinkler	Quick Run	**S1:** C-326 **S2:** C-177 S-505	Device-Cloud	96	0	96	0
	Stop	**S1:** C-326 **S2:** C-177 S-458 **S3:** C-238 C-56 S-388					
	Quick Run	**S1:** C-649 S-459 C-574 S-507 **S2:** S-[135-139]	Phone-Cloud	93	0	93	0
	Stop	**S1:** C-617 S-431					
	Hibernate	**S1:** C-621 S-493	Phone-Cloud	95	0	93	0
	Active	**S1:** C-622 S-494 **S2:** S-599 C-566 S-554 C-566					

UCI University of California, Irvine

Universal Signatures

- Applies to many devices
    - Our corpus: **18** devices



Device	Event	Signature	Communication	Matching (Per 100 Events)			
				WAN Snif.	FPR	Wi-Fi Snif.	FPR
Home Security Devices							
Ring alarm	Arm	**S1:** S-99 S-254 C-99 S-[181-183] C-99	Device-Cloud	98	0	95	0
	Disarm	**S1:** S-99 S-255 C-99 S-[181-183] C-99					
Arlo camera	Stream ON	**S1:** C-[338-339] S-[326-329] C-[364-365] S-[1061-1070] **S2:** C-[271-273] S-[499-505]	Phone-Cloud	99	2	98	3
	Stream OFF	**S1:** C-[445-449] S-442					
D-Link siren	ON	**S1:** C-1076 S-593	Phone-Cloud	100	0	98	0
	OFF	**S1:** C-1023 S-613					
Kwikset door lock	Lock	**S1:** C-699 S-511 **S2:** S-639 C-136	Phone-Cloud	100	0	100	0
	Unlock	**S1:** C-701 S-511 **S2:** S-647 C-136					
Others							
Roomba robot	Clean	**S1:** S-[1014-1015] C-105 S-432 C-105	Phone-Cloud	91	0	94	0
	Back-to-station	**S1:** S-440 C-105 S-[1018-1024] C-105					

Universal Signatures

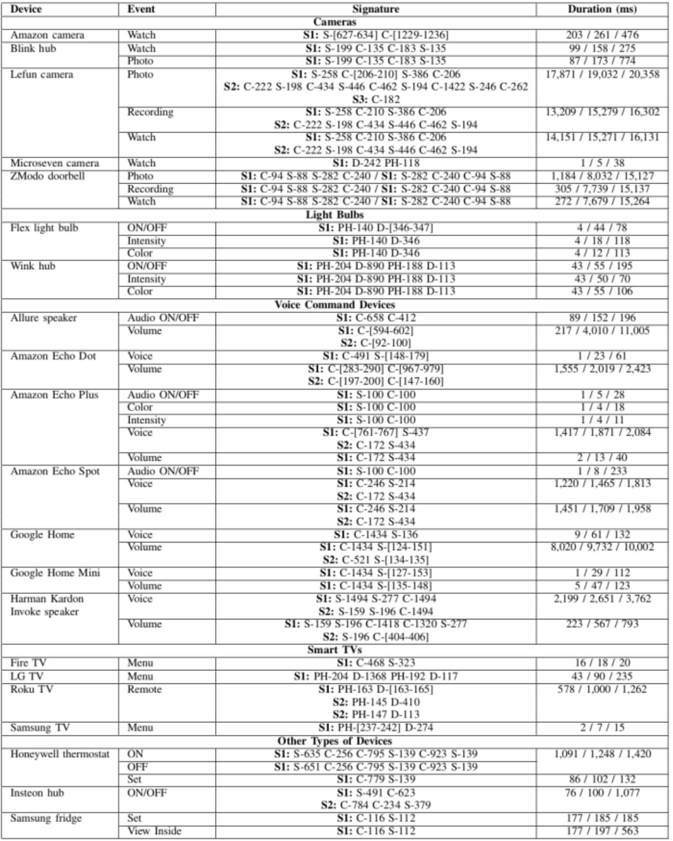
- Applies to many devices
  - Our corpus: **18** devices

Universal Signatures

- Applies to many devices
  - Our corpus: **18** devices
  - Public dataset Mon(IoT)r
    - Extraction for **21 new** devices

Universal Signatures

- Applies to ma
  - Our corpus:
  - Public dataset
    - Extraction fo



Device	Event	Signature	Duration (ms)
Cameras			
Amazon camera	Watch	**S1:** S-[627-634] C-[1229-1236]	203 / 261 / 476
Blink hub	Watch	**S1:** S-199 C-135 C-183 S-135	99 / 158 / 275
	Photo	**S1:** S-199 C-135 C-183 S-135	87 / 173 / 774
Lefun camera	Photo	**S1:** S-258 C-[206-210] S-386 C-206 **S2:** C-222 S-198 C-434 S-446 C-462 S-194 C-1422 S-246 C-262 **S3:** C-182	17,871 / 19,032 / 20,358
	Recording	**S1:** S-258 C-210 S-386 C-206 **S2:** C-222 S-198 C-434 S-446 C-462 S-194	13,209 / 15,279 / 16,302
	Watch	**S1:** S-258 C-210 S-386 C-206 **S2:** C-222 S-198 C-434 S-446 C-462 S-194	14,151 / 15,271 / 16,131
Microseven camera	Watch	**S1:** D-242 PH-118	1 / 5 / 38
ZModo doorbell	Photo	**S1:** C-94 S-88 S-282 C-240 / **S1:** S-282 C-240 C-94 S-88	1,184 / 8,032 / 15,127
	Recording	**S1:** C-94 S-88 S-282 C-240 / **S1:** S-282 C-240 C-94 S-88	305 / 7,739 / 15,137
	Watch	**S1:** C-94 S-88 S-282 C-240 / **S1:** S-282 C-240 C-94 S-88	272 / 7,679 / 15,264
Light Bulbs			
Flex light bulb	ON/OFF	**S1:** PH-140 D-[346-347]	4 / 44 / 78
	Intensity	**S1:** PH-140 D-346	4 / 18 / 118
	Color	**S1:** PH-140 D-346	4 / 12 / 113
Wink hub	ON/OFF	**S1:** PH-204 D-890 PH-188 D-113	43 / 55 / 195
	Intensity	**S1:** PH-204 D-890 PH-188 D-113	43 / 50 / 70
	Color	**S1:** PH-204 D-890 PH-188 D-113	43 / 55 / 106
Voice Command Devices			
Allure speaker	Audio ON/OFF	**S1:** C-658 C-412	89 / 152 / 196
	Volume	**S1:** C-[594-602] **S2:** C-[92-100]	217 / 4,010 / 11,005
Amazon Echo Dot	Voice	**S1:** C-491 S-[148-179]	1 / 23 / 61
	Volume	**S1:** C-[283-290] C-[967-979] **S2:** C-[197-200] C-[147-160]	1,555 / 2,019 / 2,423
Amazon Echo Plus	Audio ON/OFF	**S1:** S-100 C-100	1 / 5 / 28
	Color	**S1:** S-100 C-100	1 / 4 / 18
	Intensity	**S1:** S-100 C-100	1 / 4 / 11
	Voice	**S1:** C-[761-767] S-437 **S2:** C-172 S-434	1,417 / 1,871 / 2,084
	Volume	**S1:** C-172 S-434	2 / 13 / 40
Amazon Echo Spot	Audio ON/OFF	**S1:** S-100 C-100	1 / 8 / 233
	Voice	**S1:** C-246 S-214 **S2:** C-172 S-434	1,220 / 1,465 / 1,813
	Volume	**S1:** C-246 S-214 **S2:** C-172 S-434	1,451 / 1,709 / 1,958
Google Home	Voice	**S1:** C-1434 S-136	9 / 61 / 132
	Volume	**S1:** C-1434 S-[124-151] **S2:** C-521 S-[134-135]	8,020 / 9,732 / 10,002
Google Home Mini	Voice	**S1:** C-1434 S-[127-153]	1 / 29 / 112
	Volume	**S1:** C-1434 S-[135-148]	5 / 47 / 123
Harman Kardon Invoke speaker	Voice	**S1:** S-1494 S-277 C-1494 **S2:** S-159 S-196 C-1494	2,199 / 2,651 / 3,762
	Volume	**S1:** S-159 S-196 C-1418 C-1320 S-277 **S2:** S-196 C-[404-406]	223 / 567 / 793
Smart TVs			
Fire TV	Menu	**S1:** C-468 S-323	16 / 18 / 20
LG TV	Menu	**S1:** PH-204 D-1368 PH-192 D-117	43 / 90 / 235
Roku TV	Remote	**S1:** PH-163 D-[163-165] **S2:** PH-145 D-410 **S2:** PH-147 D-113	578 / 1,000 / 1,262
Samsung TV	Menu	**S1:** PH-[237-242] D-274	2 / 7 / 15
Other Types of Devices			
Honeywell thermostat	ON	**S1:** S-635 C-256 C-795 S-139 C-923 S-139	1,091 / 1,248 / 1,420
	OFF	**S1:** S-651 C-256 C-795 S-139 C-923 S-139	
	Set	**S1:** C-779 S-139	86 / 102 / 132
Insteon hub	ON/OFF	**S1:** S-491 C-623 **S2:** C-784 C-234 S-379	76 / 100 / 1,077
Samsung fridge	Set	**S1:** C-116 S-112	177 / 185 / 185
	View Inside	**S1:** C-116 S-112	177 / 197 / 563

Universal Signatures

- Applies to many devices
    - Our corpus: **18** devices
    - Public dataset Mon(IoT)r
        - Extraction for **21 new** devices
        - Comparison for **5 common** devices

Universal Signatures

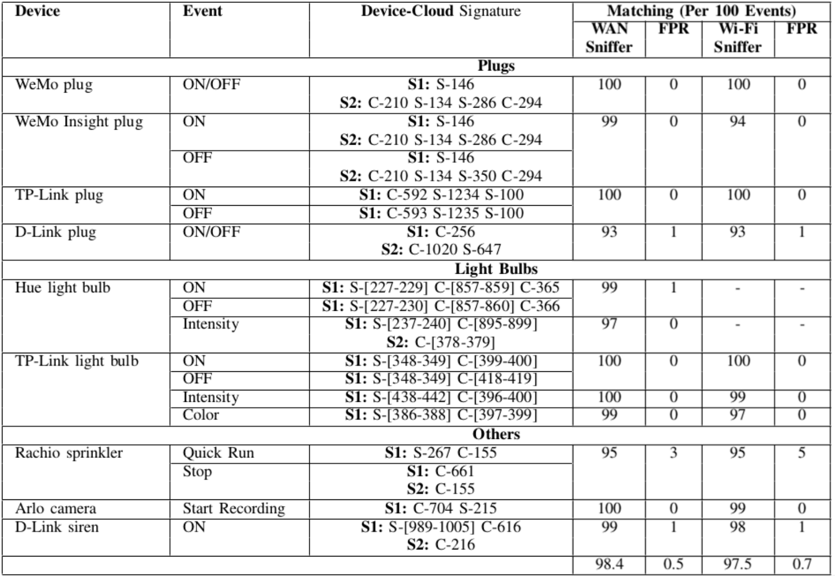
- **Three** communications
- **Two** adversaries
  - **WAN** and **Wi-Fi** sniffers
- Different triggers
  - **Local**-Phone

Universal Signatures

- **Three** communications
- **Two** adversaries
  - **WAN** and **Wi-Fi** sniffers
- Different triggers
  - **Local**-Phone
  - **Remote**-Phone, and
  - Home **Automation**

Universal Signatures

- Three communications
- Two a
  - WA
- Differe
  - Loc
  - Rem
  - Home Automation



Device	**Event**	**Device-Cloud** Signature	**Matching (Per 100 Events)**			
			WAN Sniffer	**FPR**	**Wi-Fi Sniffer**	**FPR**
		Plugs				
WeMo plug	ON/OFF	**S1:** S-146 **S2:** C-210 S-134 S-286 C-294	100	0	100	0
WeMo Insight plug	ON	**S1:** S-146 **S2:** C-210 S-134 S-286 C-294	99	0	94	0
	OFF	**S1:** S-146 **S2:** C-210 S-134 S-350 C-294				
TP-Link plug	ON	**S1:** C-592 S-1234 S-100	100	0	100	0
	OFF	**S1:** C-593 S-1235 S-100				
D-Link plug	ON/OFF	**S1:** C-256 **S2:** C-1020 S-647	93	1	93	1
		Light Bulbs				
Hue light bulb	ON	**S1:** S-[227-229] C-[857-859] C-365	99	1	-	-
	OFF	**S1:** S-[227-230] C-[857-860] C-366				
	Intensity	**S1:** S-[237-240] C-[895-899] **S2:** C-[378-379]	97	0	-	-
TP-Link light bulb	ON	**S1:** S-[348-349] C-[399-400]	100	0	100	0
	OFF	**S1:** S-[348-349] C-[418-419]				
	Intensity	**S1:** S-[438-442] C-[396-400]	100	0	99	0
	Color	**S1:** S-[386-388] C-[397-399]	99	0	97	0
		Others				
Rachio sprinkler	Quick Run	**S1:** S-267 C-155	95	3	95	5
	Stop	**S1:** C-661 **S2:** C-155				
Arlo camera	Start Recording	**S1:** C-704 S-215	100	0	99	0
D-Link siren	ON	**S1:** S-[989-1005] C-616 **S2:** C-216	99	1	98	1
			98.4	0.5	97.5	0.7

Universal Signatures

- **Three** communications
- **Two** adversaries
  - **WAN** and **Wi-Fi** sniffers
- Different triggers
  - **Local**-Phone
  - **Remote**-Phone, and
  - Home **Automation** IFTTT
- Matching with recall **> 97%**

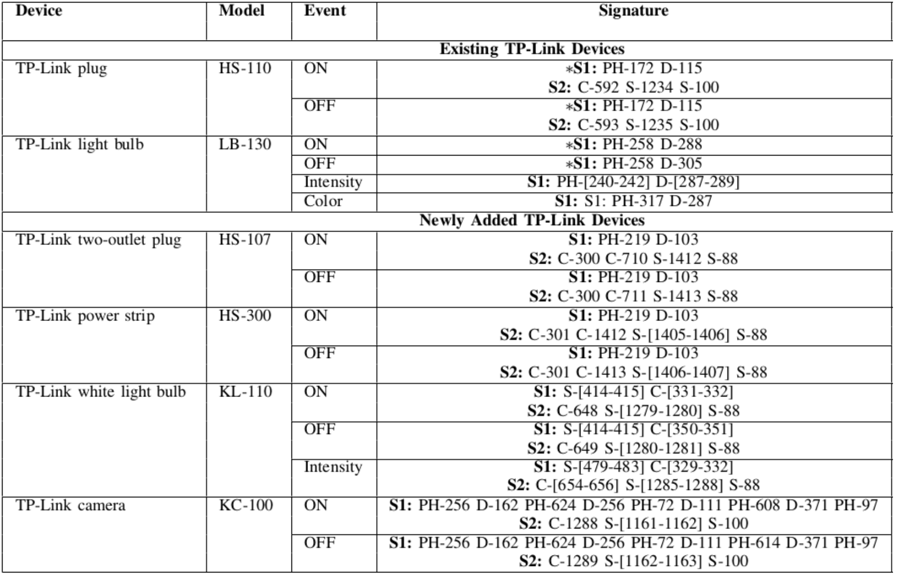
UCI University of California, Irvine

Unique Signatures

- Distinguish
  - **Device type**
  - **Event type:** binary and non-binary
  - Same-vendor devices

Unique Signatures

- Distinguish
  - ○ **Devic**
  - ○ **Even**
  - ○ Same-



Device	Model	Event	Signature
Existing TP-Link Devices			
TP-Link plug	HS-110	ON	⁎**S1:** PH-172 D-115 **S2:** C-592 S-1234 S-100
		OFF	⁎**S1:** PH-172 D-115 **S2:** C-593 S-1235 S-100
TP-Link light bulb	LB-130	ON	⁎**S1:** PH-258 D-288
		OFF	⁎**S1:** PH-258 D-305
		Intensity	**S1:** PH-[240-242] D-[287-289]
		Color	**S1:** S1: PH-317 D-287
Newly Added TP-Link Devices			
TP-Link two-outlet plug	HS-107	ON	**S1:** PH-219 D-103 **S2:** C-300 C-710 S-1412 S-88
		OFF	**S1:** PH-219 D-103 **S2:** C-300 C-711 S-1413 S-88
TP-Link power strip	HS-300	ON	**S1:** PH-219 D-103 **S2:** C-301 C-1412 S-[1405-1406] S-88
		OFF	**S1:** PH-219 D-103 **S2:** C-301 C-1413 S-[1406-1407] S-88
TP-Link white light bulb	KL-110	ON	**S1:** S-[414-415] C-[331-332] **S2:** C-648 S-[1279-1280] S-88
		OFF	**S1:** S-[414-415] C-[350-351] **S2:** C-649 S-[1280-1281] S-88
		Intensity	**S1:** S-[479-483] C-[329-332] **S2:** C-[654-656] S-[1285-1288] S-88
TP-Link camera	KC-100	ON	**S1:** PH-256 D-162 PH-624 D-256 PH-72 D-111 PH-608 D-371 PH-97 **S2:** C-1288 S-[1161-1162] S-100
		OFF	**S1:** PH-256 D-162 PH-624 D-256 PH-72 D-111 PH-614 D-371 PH-97 **S2:** C-1289 S-[1162-1163] S-100

Unique Signatures

- Distinguish
  - **Device type**
  - **Event type:** binary and non-binary
  - Same-vendor devices
- Negative control experiment
  - Three public datasets: **>440 million** packets
    - YourThings, UNSW, UNB
  - FPR: **one FP** per **40 million packets**

UCI University of California, Irvine

Packet-Level Signatures

- Can distinguish event types ✓

Packet-Level Signatures

- Can distinguish event types ✓
- Minimal set of traffic features ✓

Packet-Level Signatures

- Can distinguish event types ✓
- Minimal set of traffic features ✓
- Two adversaries ✓

Packet-Level Signatures

- Can distinguish event types ✓
- Minimal set of traffic features ✓
- Two adversaries ✓
- Applicable to many devices ✓

Packet-Level Signatures

- Can distinguish event types ✓
- Minimal set of traffic features ✓
- Two adversaries ✓
- Applicable to many devices ✓
- Resilient to traffic shaping & VPN encryption ✓
- Defended against by packet padding ✓

Packet-Level Signatures

- Can distinguish event types ✓
- Minimal set of traffic features ✓
- Two adversaries ✓
- Applicable to many devices ✓
- Resilient to traffic shaping & VPN encryption ✓
- Defended against by packet padding ✓
- Profiling and network monitoring ✓

Limitations

- Need device to train
- Signatures may vary over time
- Apply to **95%** of devices
  - UDP-based
  - Repetitive pairs for an event

Outline

I. Background and Problem Statement

II. Key Observation: Packet-Level Signatures

III. The PingPong System

IV. Conclusion

Conclusions

- Packet-level signatures
  - **Request-reply** pattern
  - Packet **lengths** and **directions**
- Automation: **PingPong**
  - Extraction and detection
- Signatures are **universal** and **unique**

Thank You!

- Paper
  https://www.ndss-symposium.org/ndss-paper/packet-level-signatures-for-smart-home-devices/
- Software and datasets
  http://plrg.ics.uci.edu/pingpong/

UCI University of California, Irvine

Additional Slides

Signature Variations

- Signatures with no variation
- Signatures with ranges
- Signatures that vary
  - Signature evolution
  - Signatures that vary in certain packets
    - App’s username and password

C-556 S-1293

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

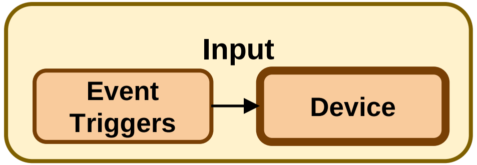
C-556 S-1293 2018

C-592 S-1234 S-100
C-605 S-1213 S-100
2019

UCI University of California, Irvine

PingPong Training

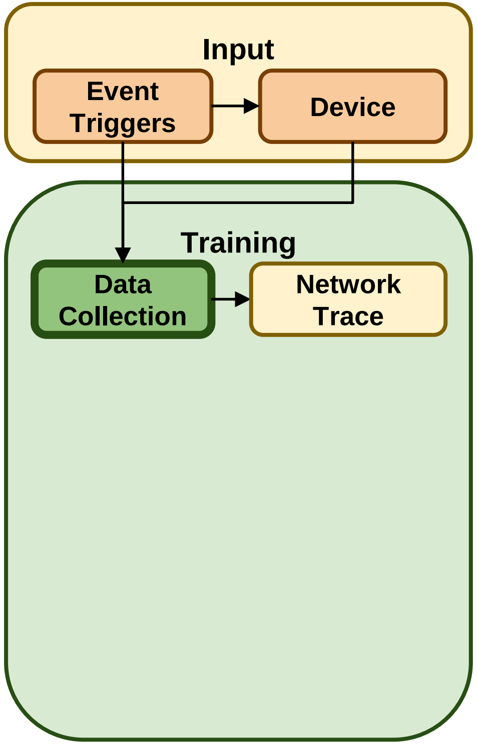
The PingPong System



Toggle ON for TP-Link Plug

PingPong Training

The PingPong System

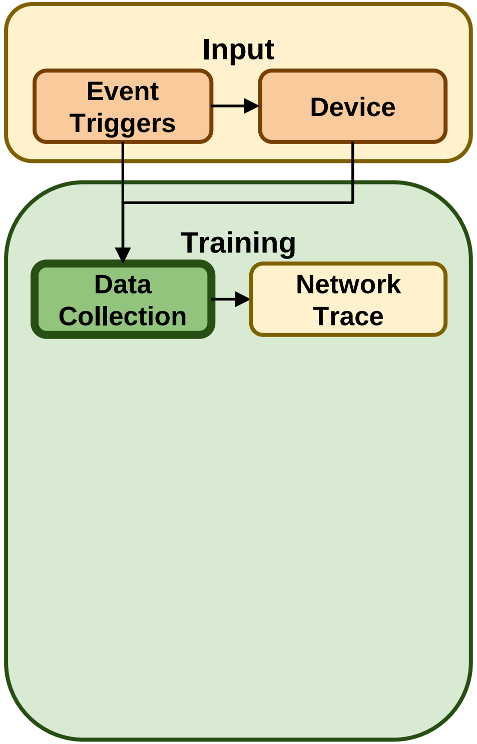


Toggle ON for TP-Link Plug

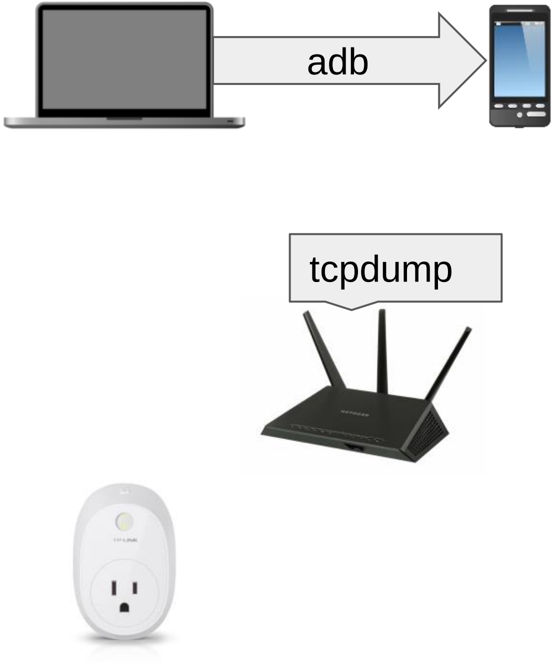
UCI University of California, Irvine

PingPong Training

The PingPong System

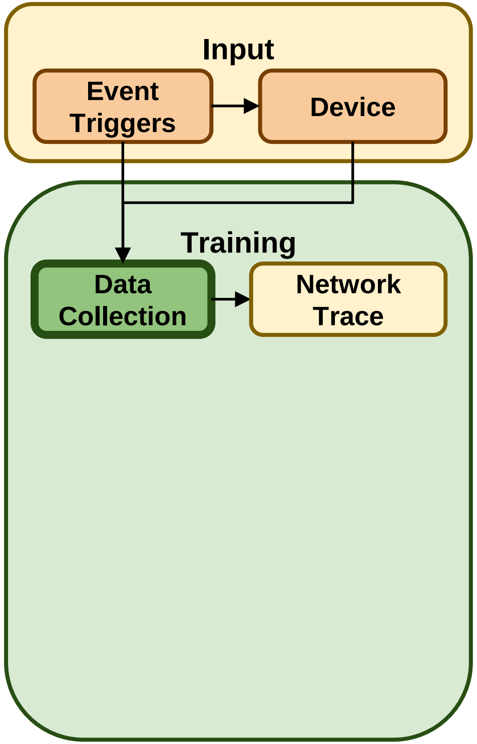


Toggle ON for TP-Link Plug

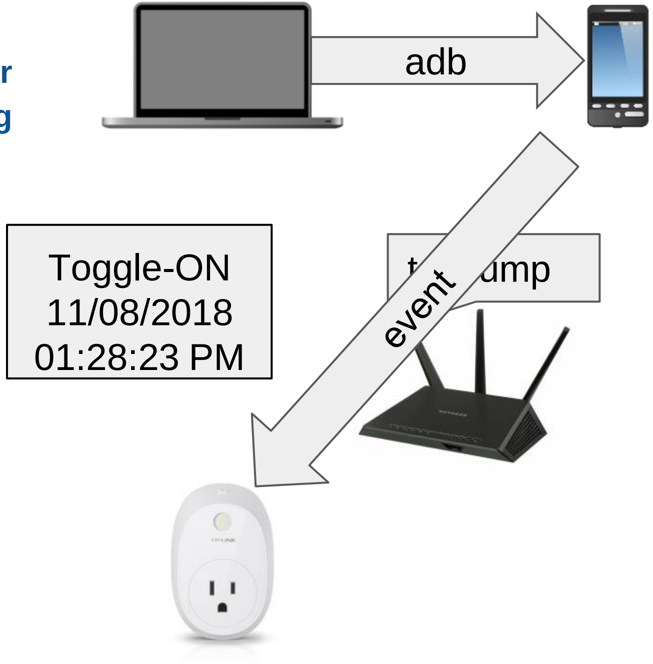


PingPong Training

The PingPong System



Toggle ON for TP-Link Plug

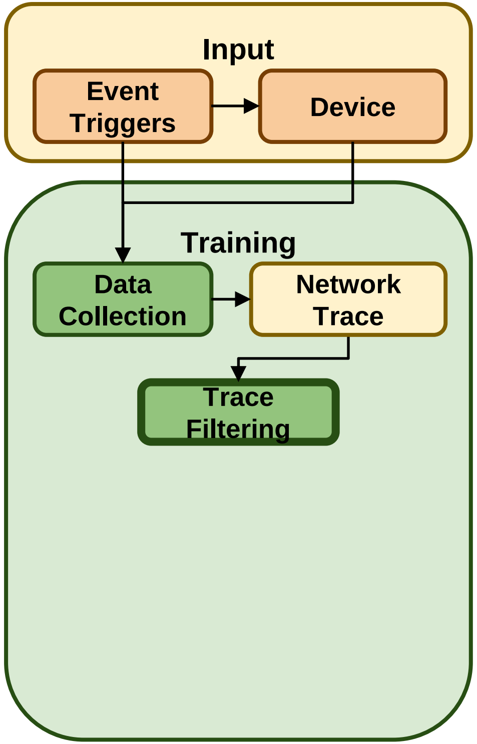


Toggle-ON
11/08/2018
01:28:23 PM

UCI University of California, Irvine

PingPong Training

The PingPong System



Toggle ON for TP-Link Plug

PCAP file

...

… C-123 S-456 … C-234 S-567
… C-345 S-678 ...

… C-556 S-1293 ... C-238 S-826
… C-129 S-123 ...

… C-123 S-456 … C-234 S-567
… C-345 S-678 …

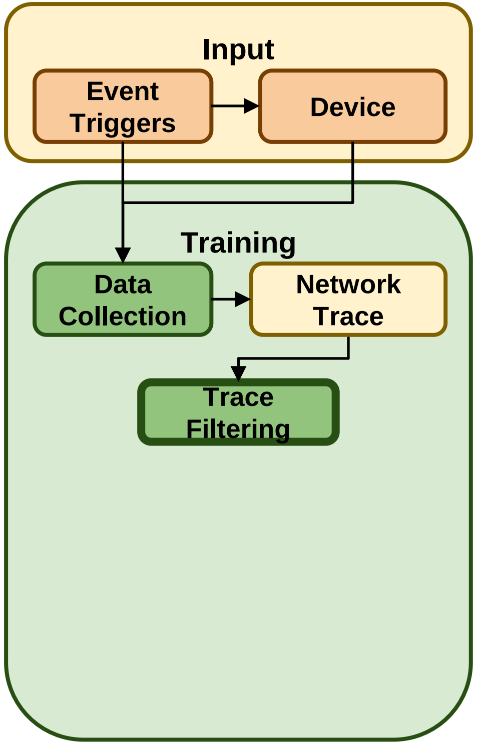
...

t

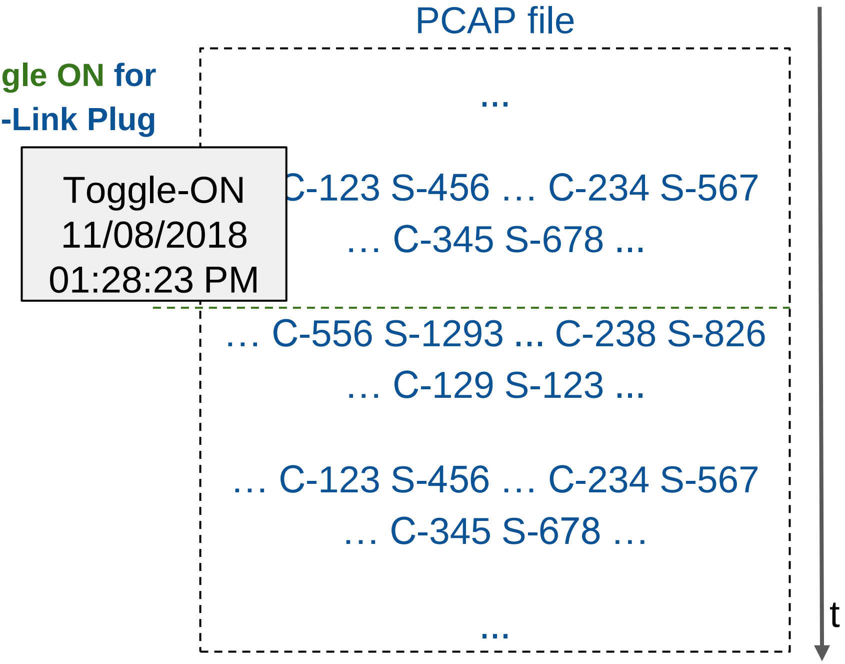
UCI University of California, Irvine

PingPong Training

The PingPong System



Toggle ON for TP-Link Plug



Toggle-ON
11/08/2018
01:28:23 PM

...

C-123 S-456 … C-234 S-567
… C-345 S-678 ...

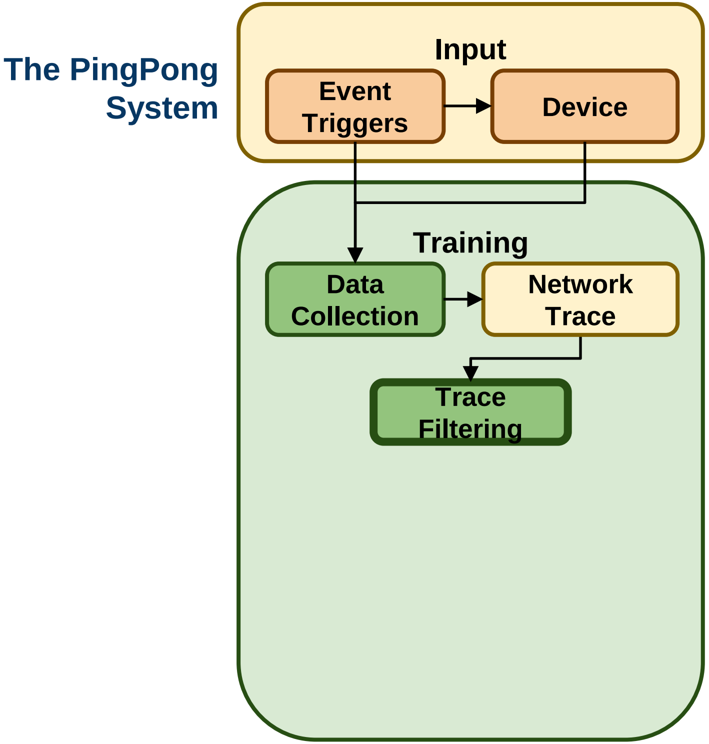
… C-556 S-1293 ... C-238 S-826
… C-129 S-123 ...

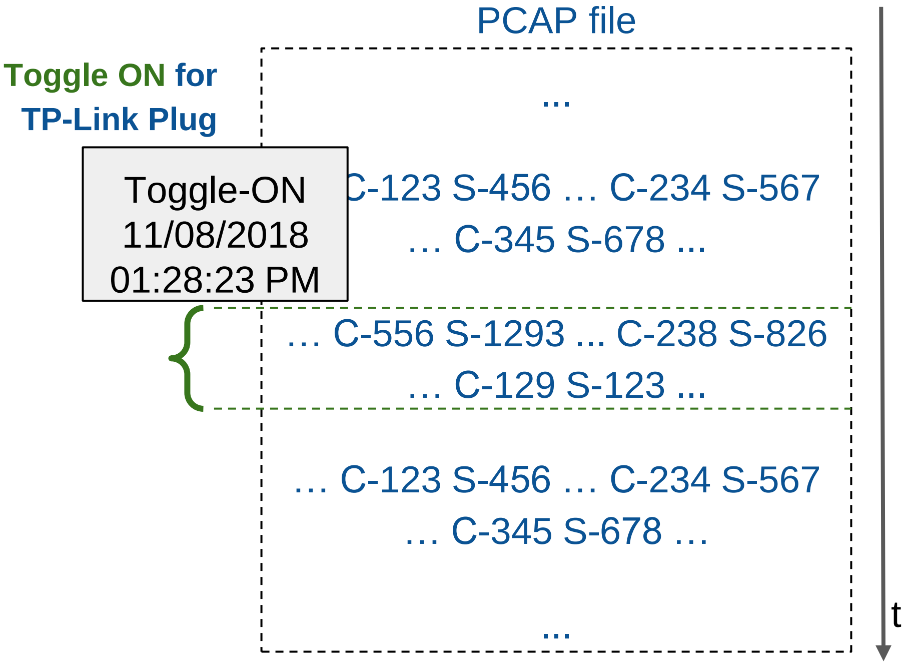
… C-123 S-456 … C-234 S-567
… C-345 S-678 …

...

UCI University of California, Irvine

PingPong Training

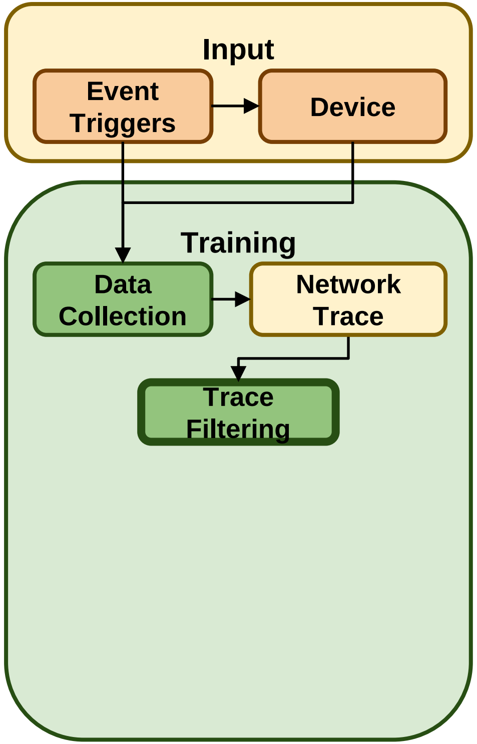



PCAP file
Toggle ON for TP-Link Plug
Toggle-ON 11/08/2018 01:28:23 PM
…
C-123 S-456 … C-234 S-567
… C-345 S-678 …
… C-556 S-1293 … C-238 S-826
… C-129 S-123 …
… C-123 S-456 … C-234 S-567
… C-345 S-678 …
…
t

UCI University of California, Irvine

PingPong Training

The PingPong System

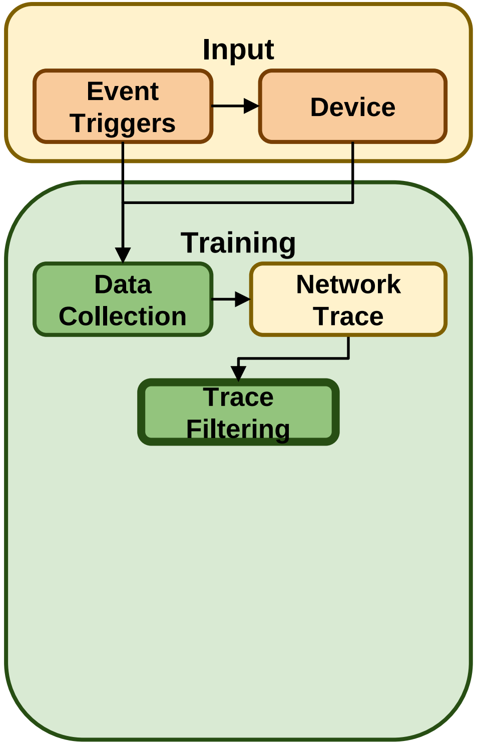


Toggle ON for TP-Link Plug

… C-556 S-1293 ... C-238 S-826 … C-129 S-123 ...

PingPong Training

The PingPong System



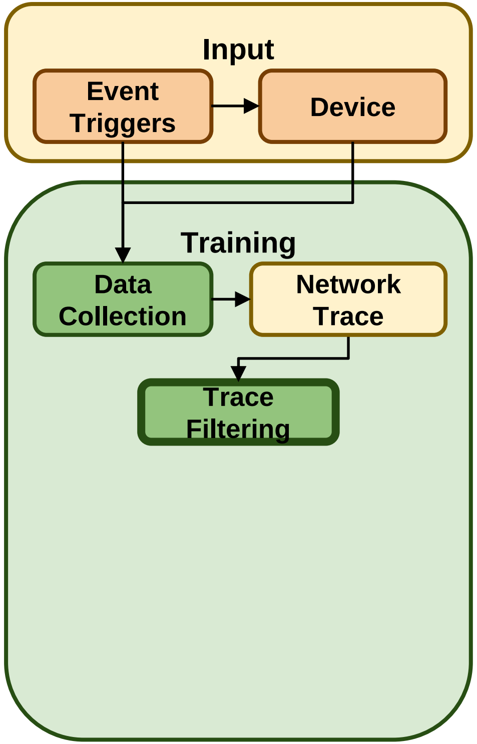
Toggle ON for TP-Link Plug

… C-556 S-1293 ... C-238 S-826
… C-129 S-123 ...

TCP Conn.1 … C-556 S-1293 ...

PingPong Training

The PingPong System



Toggle ON for TP-Link Plug

… C-556 S-1293 ... C-238 S-826
… C-129 S-123 ...

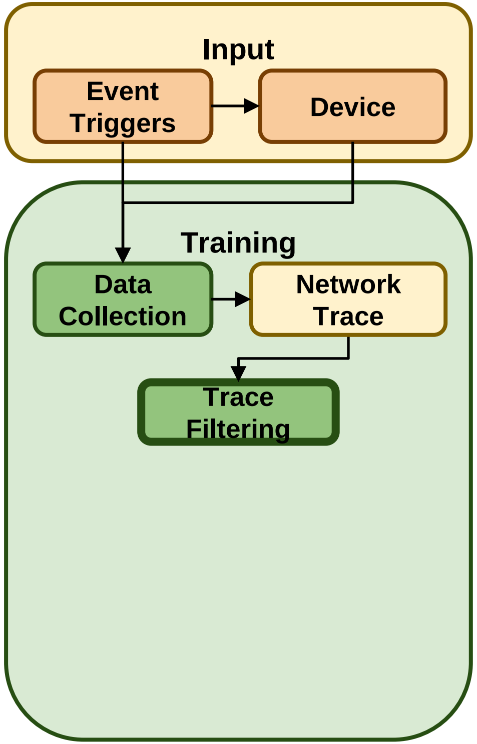
TCP Conn.1 … C-556 S-1293 ...

TCP Conn.2 … C-238 S-826 ...

UCI University of California, Irvine

PingPong Training

The PingPong System



Toggle ON for TP-Link Plug

… C-556 S-1293 … C-238 S-826 … C-129 S-123 ...

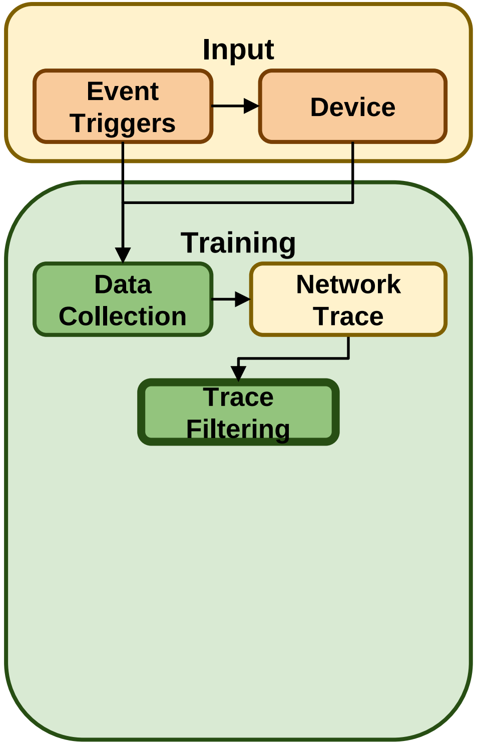
TCP Conn.1 … C-556 S-1293 ...

TCP Conn.2 … C-238 S-826 ...

TCP Conn.3 … C-129 S-123 ...

PingPong Training

The PingPong System



Toggle ON for TP-Link Plug

… C-556 S-1293 ... C-238 S-826 … C-129 S-123 ...

Packet Pairs

<...,...> <C-556, S-1293> <...,...>

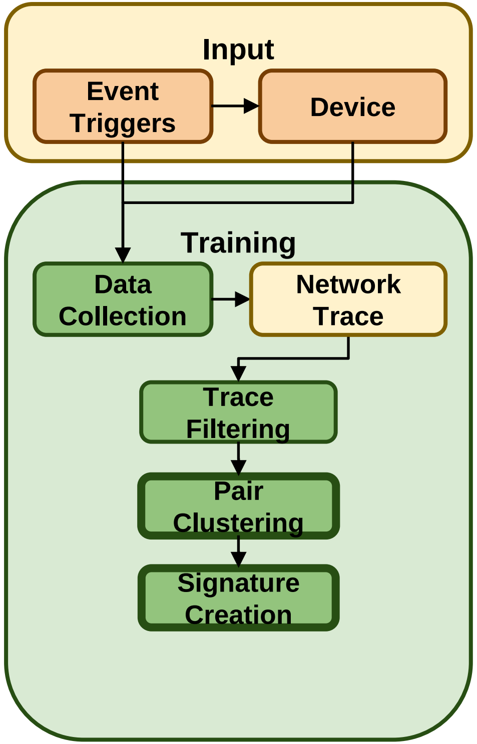
<...,...> <C-238, S-826> <...,...>

<...,...> <C-129, S-123> <...,...>

UCI University of California, Irvine

PingPong Training

The PingPong System



Toggle ON for TP-Link Plug

Packet Pairs

<...,...> <C-556, S-1293> <...,...>

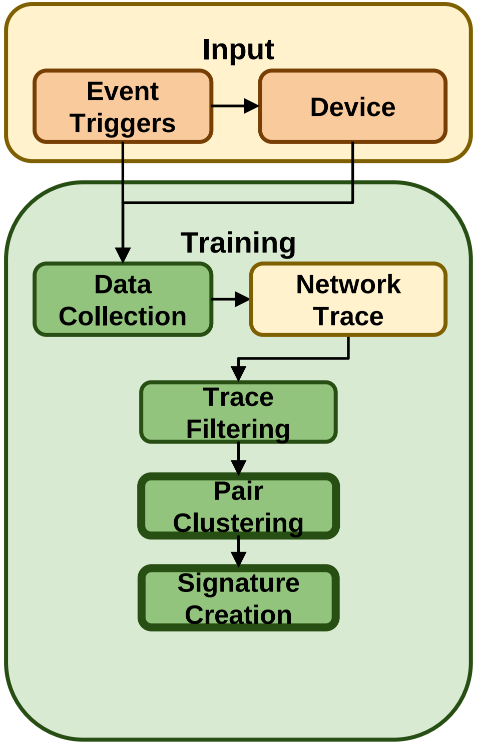
<...,...> <C-238, S-826> <...,...>

<...,...> <C-129, S-123> <...,...>

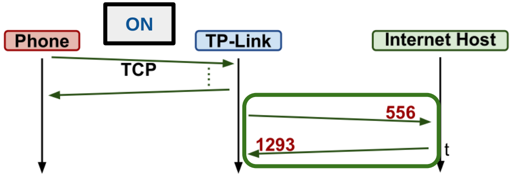
UCI University of California, Irvine

PingPong Training

The PingPong System



Toggle ON for TP-Link Plug



Packet Pairs

<...,...> <C-556, S-1293> <...,...>

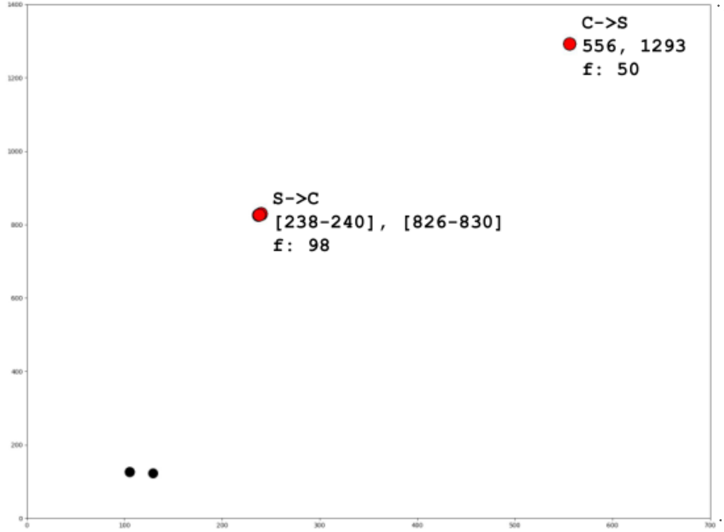
<...,...> <C-238, S-826> <...,...>

<...,...> <C-129, S-123> <...,...>

UCI University of California, Irvine

PingPong Training

Pair Clustering



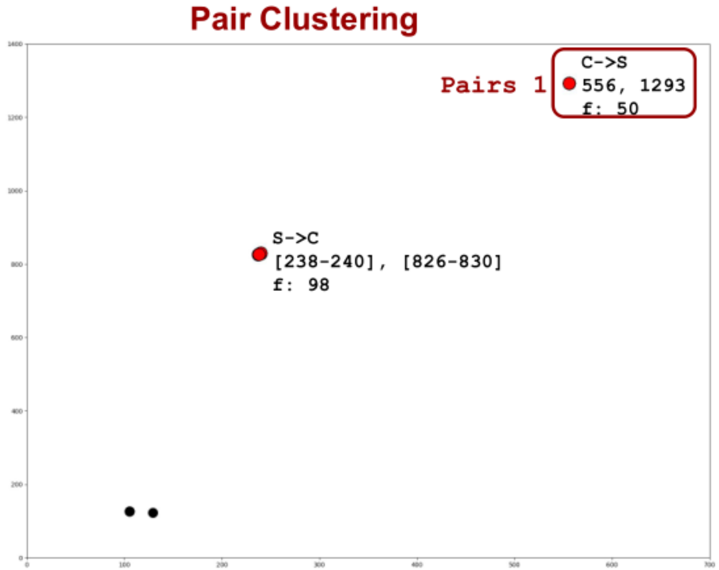
(a) TP-Link Plug

<...,...> <C-556, S-1293> <...,...>

<...,...> <C-238, S-826> <...,...>

<...,...> <C-129, S-123> <...,...>

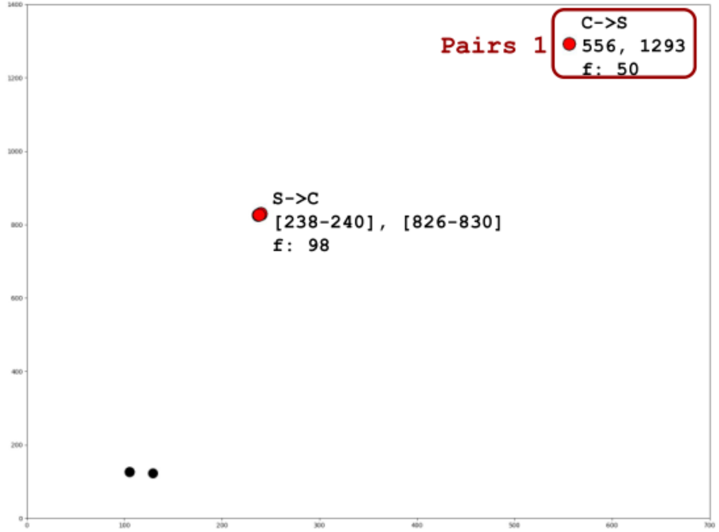
PingPong Training



(a) TP-Link Plug

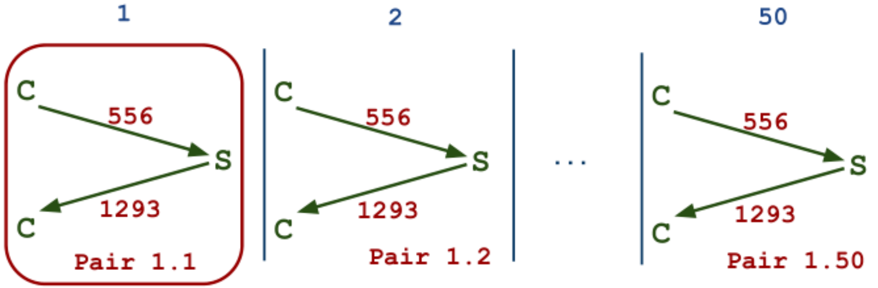
PingPong Training

Pair Clustering



(a) TP-Link Plug

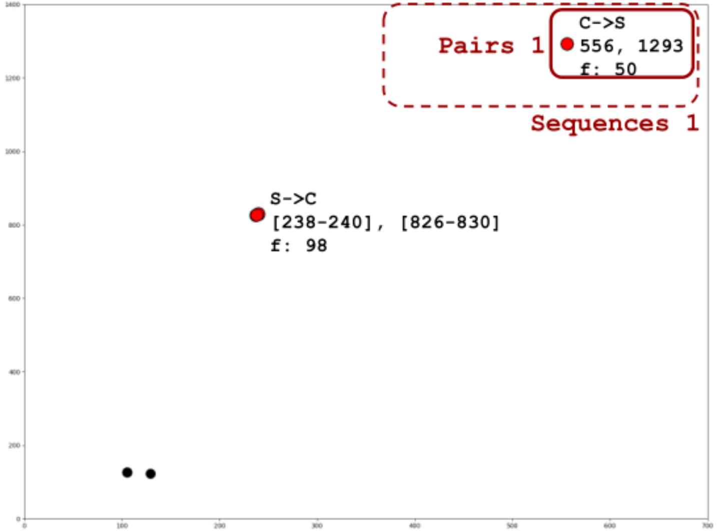
Signature Creation



UCI University of California, Irvine

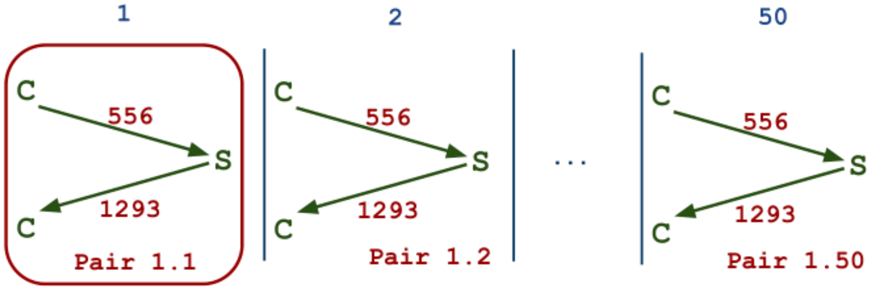
PingPong Training

Pair Clustering



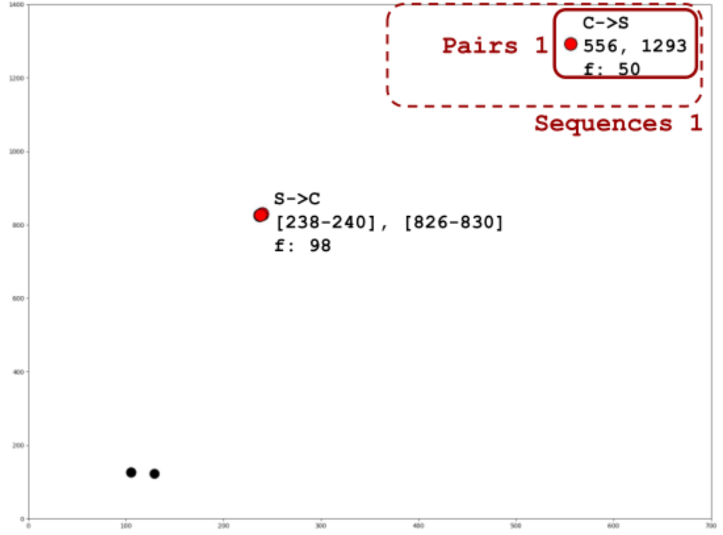
(a) TP-Link Plug

Signature Creation



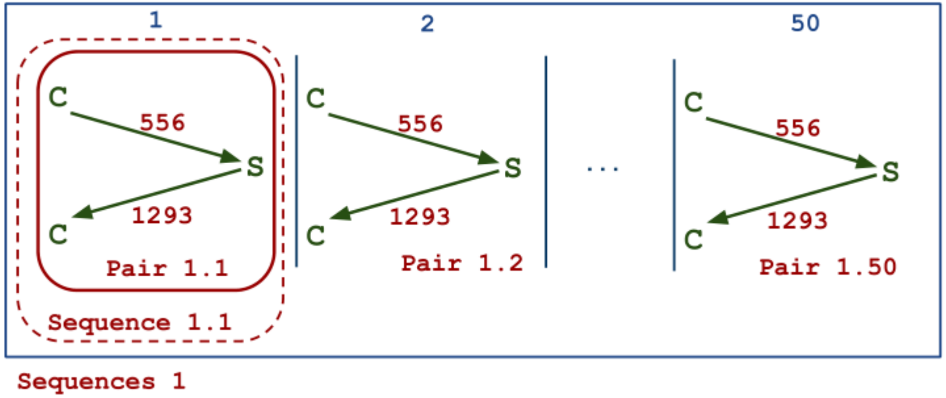
PingPong Training

Pair Clustering



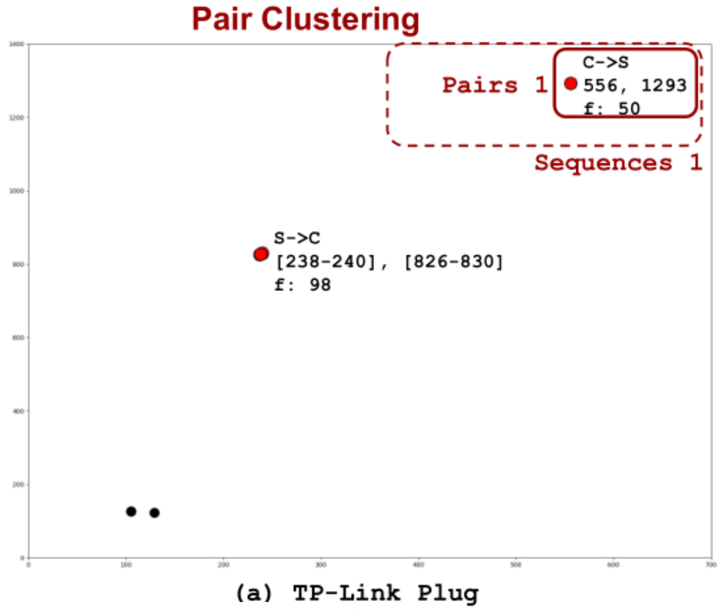
(a) TP-Link Plug

Signature Creation

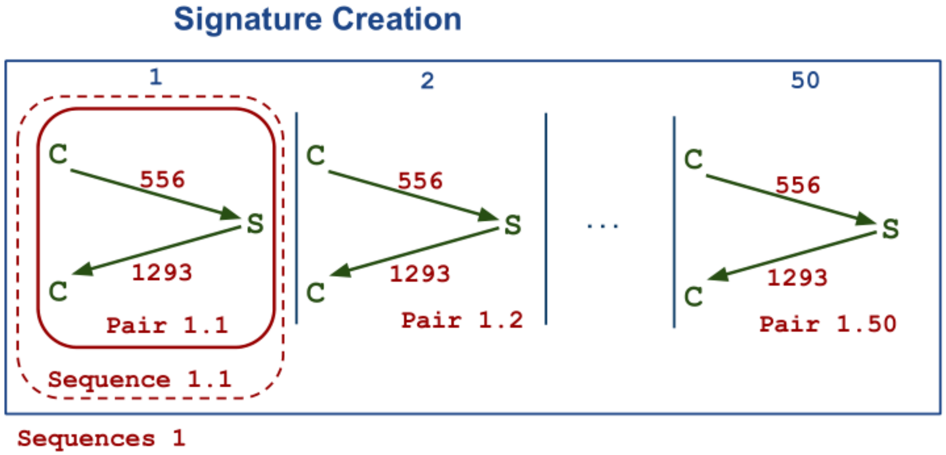


UCI University of California, Irvine

PingPong Training

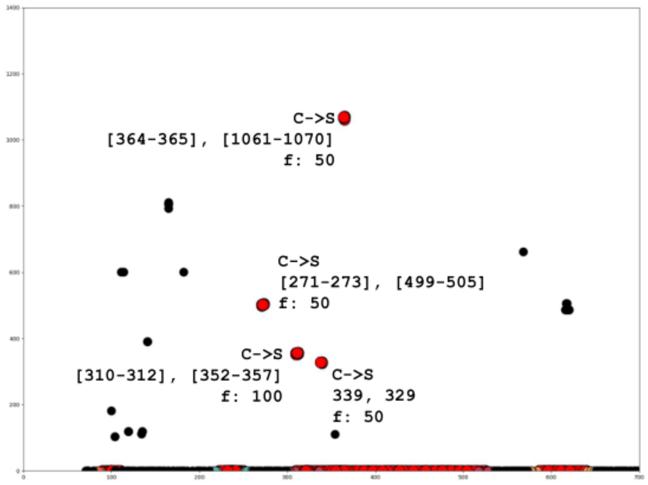


(a) TP-Link Plug



C-556 S-1293

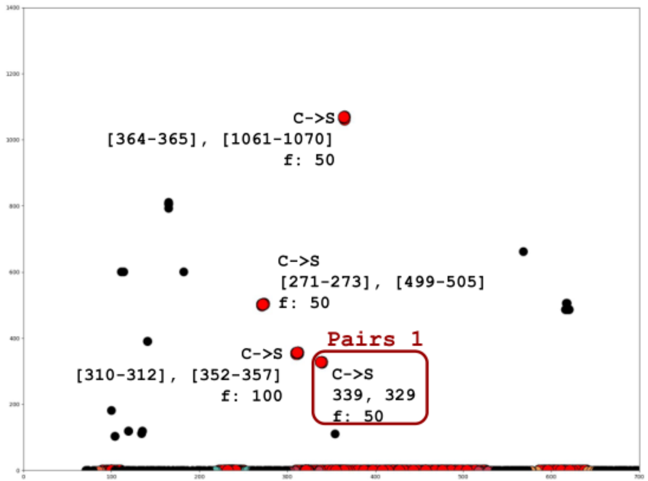
PingPong Training



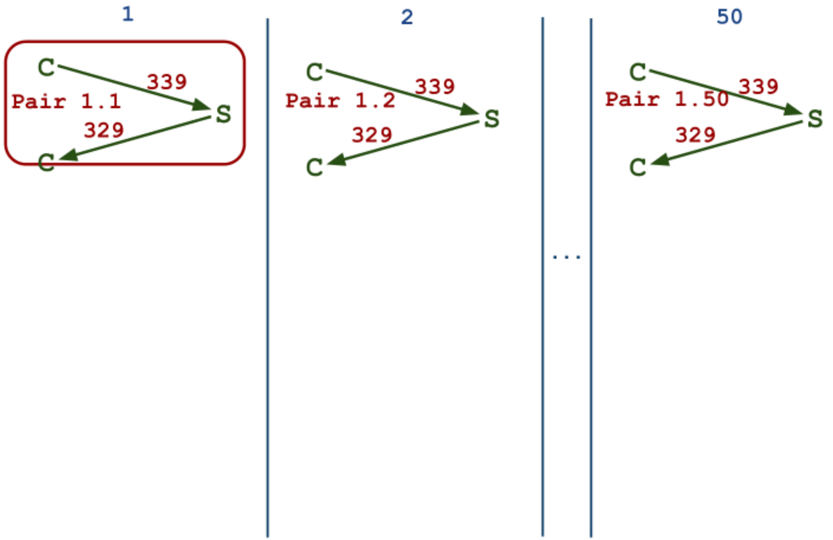
(b) Arlo Camera

arlo

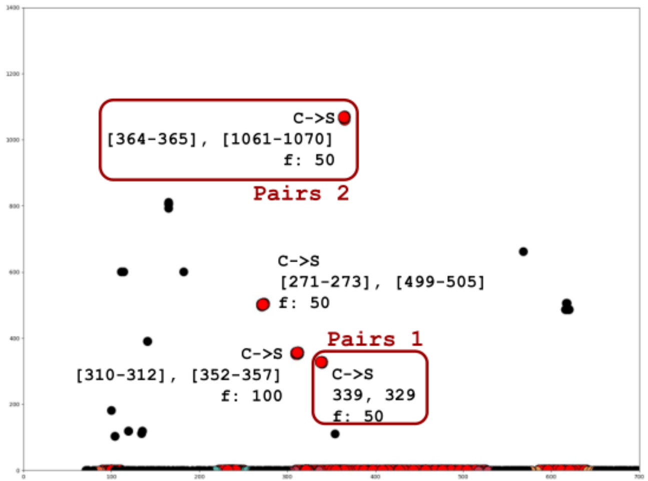
PingPong Training



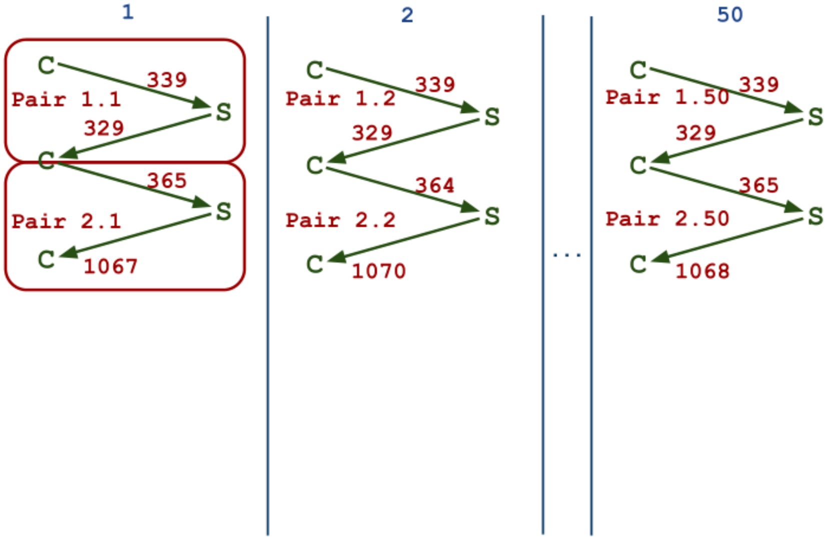
(b) Arlo Camera



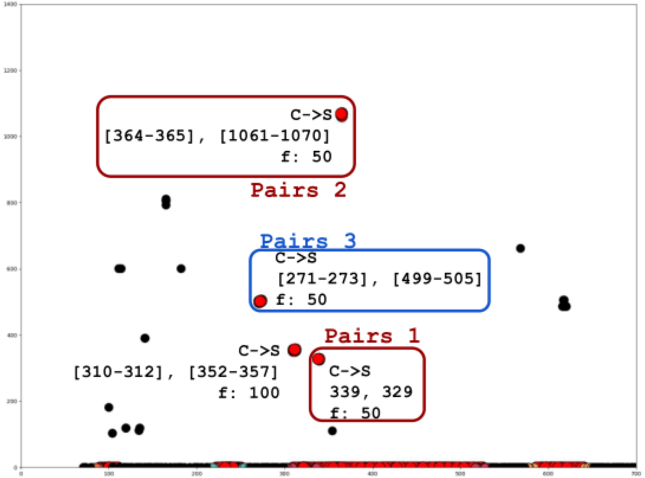
PingPong Training



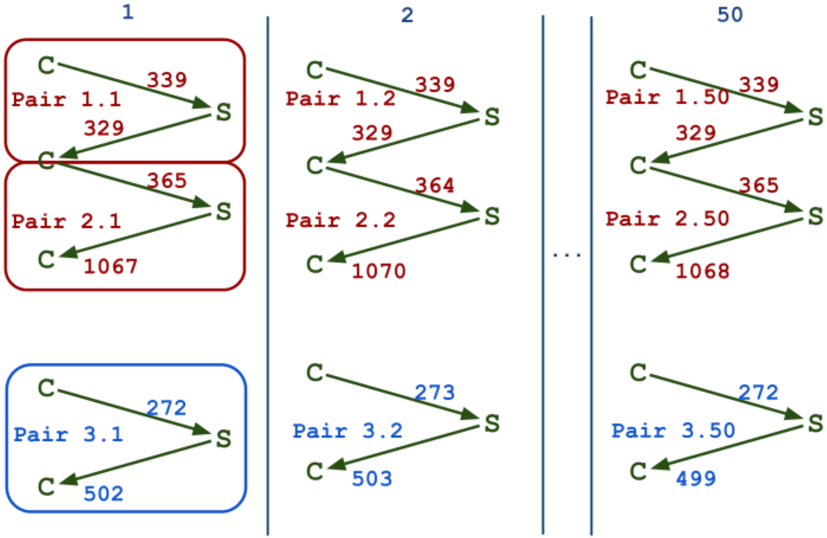
(b) Arlo Camera



PingPong Training

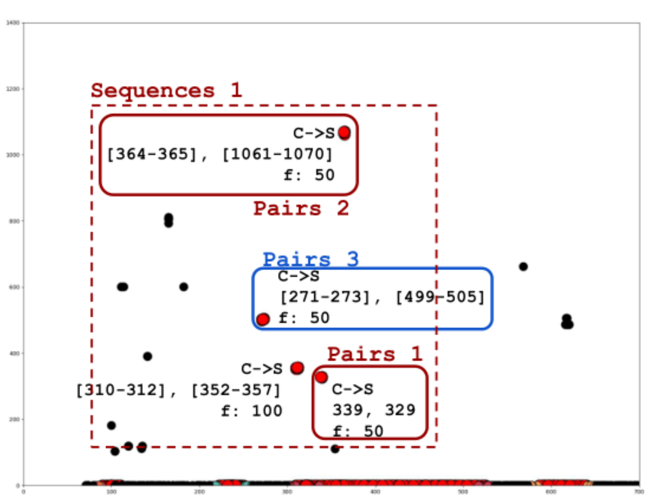


(b) Arlo Camera

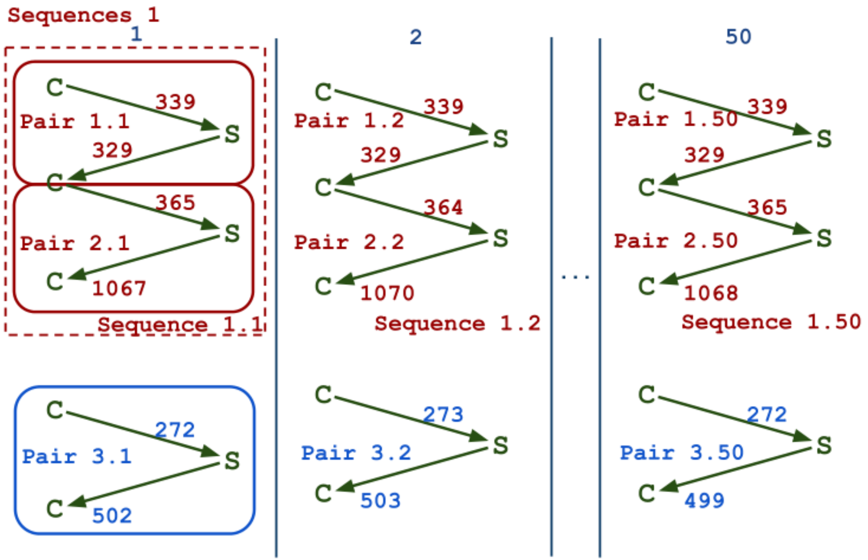


UCI University of California, Irvine

PingPong Training

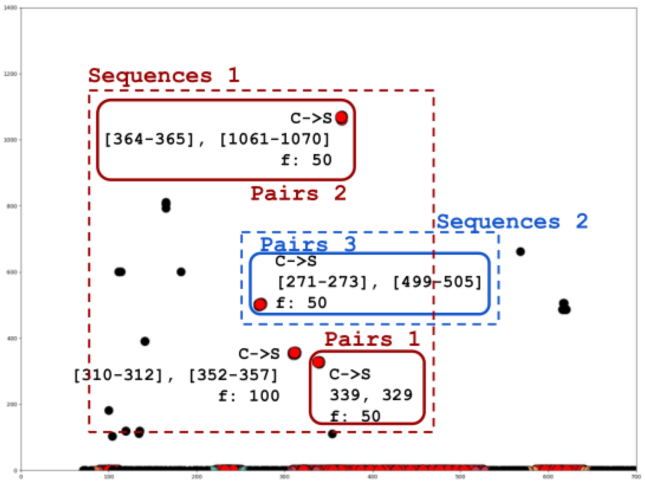


(b) Arlo Camera

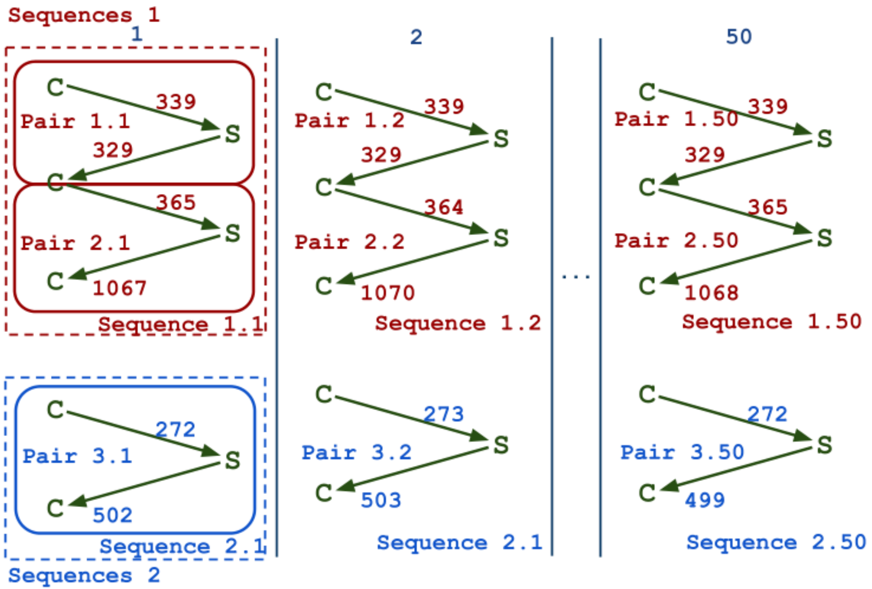


UCI University of California, Irvine

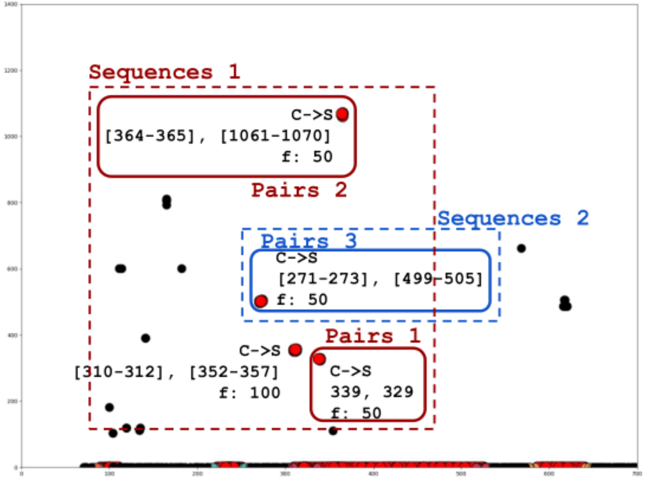
PingPong Training



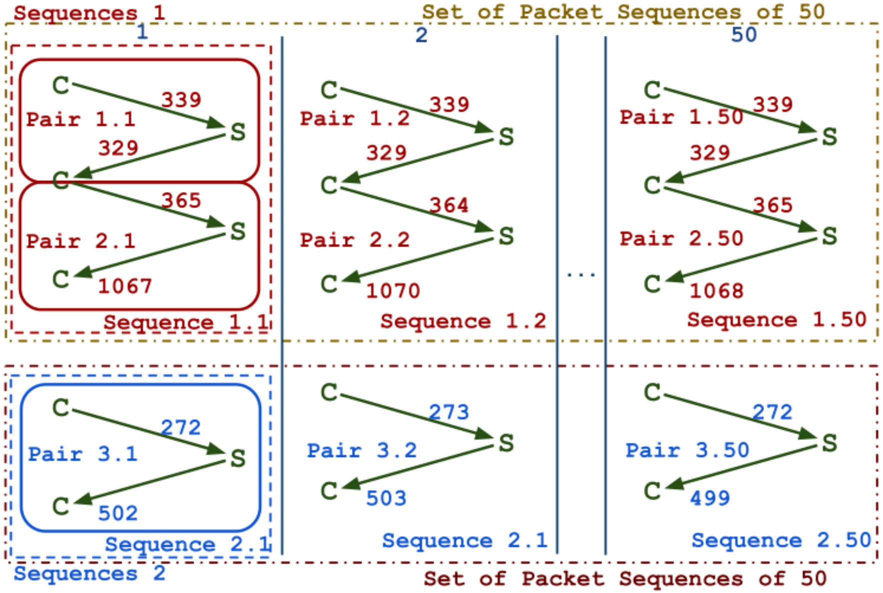
(b) Arlo Camera



PingPong Training

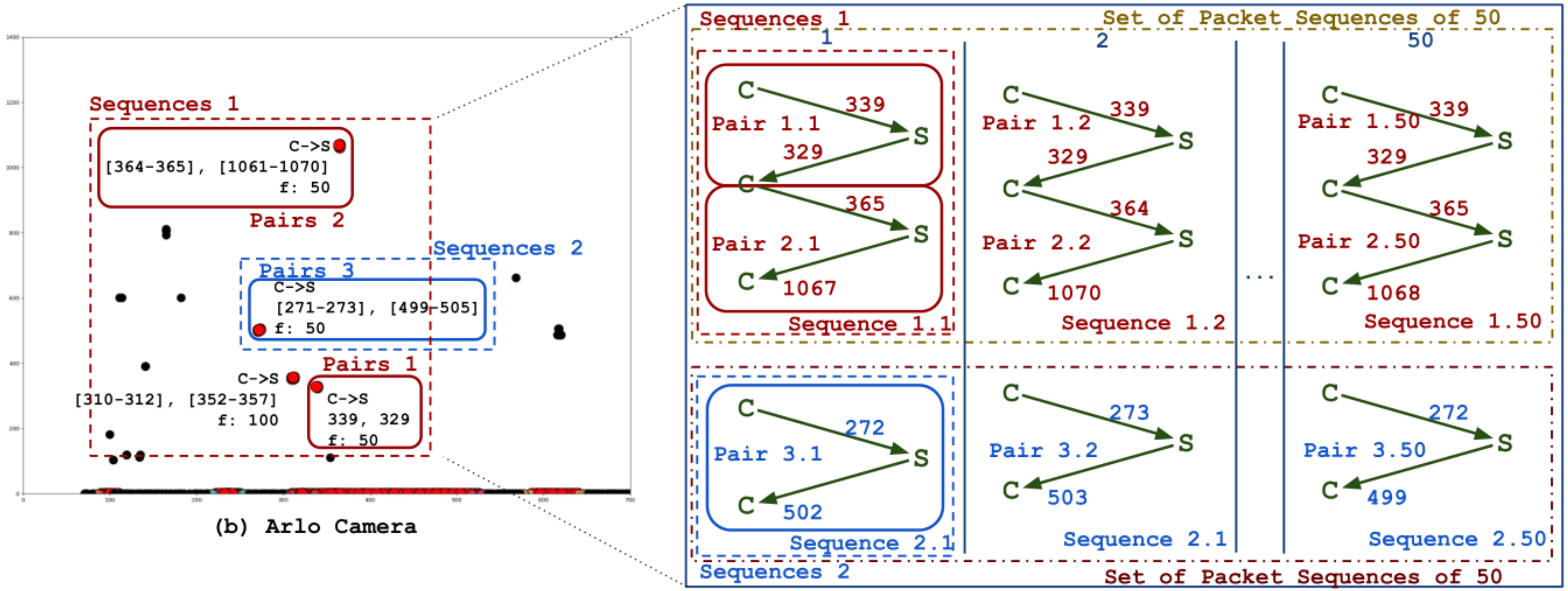


(b) Arlo Camera



University of California, Irvine

PingPong Training



(b) Arlo Camera

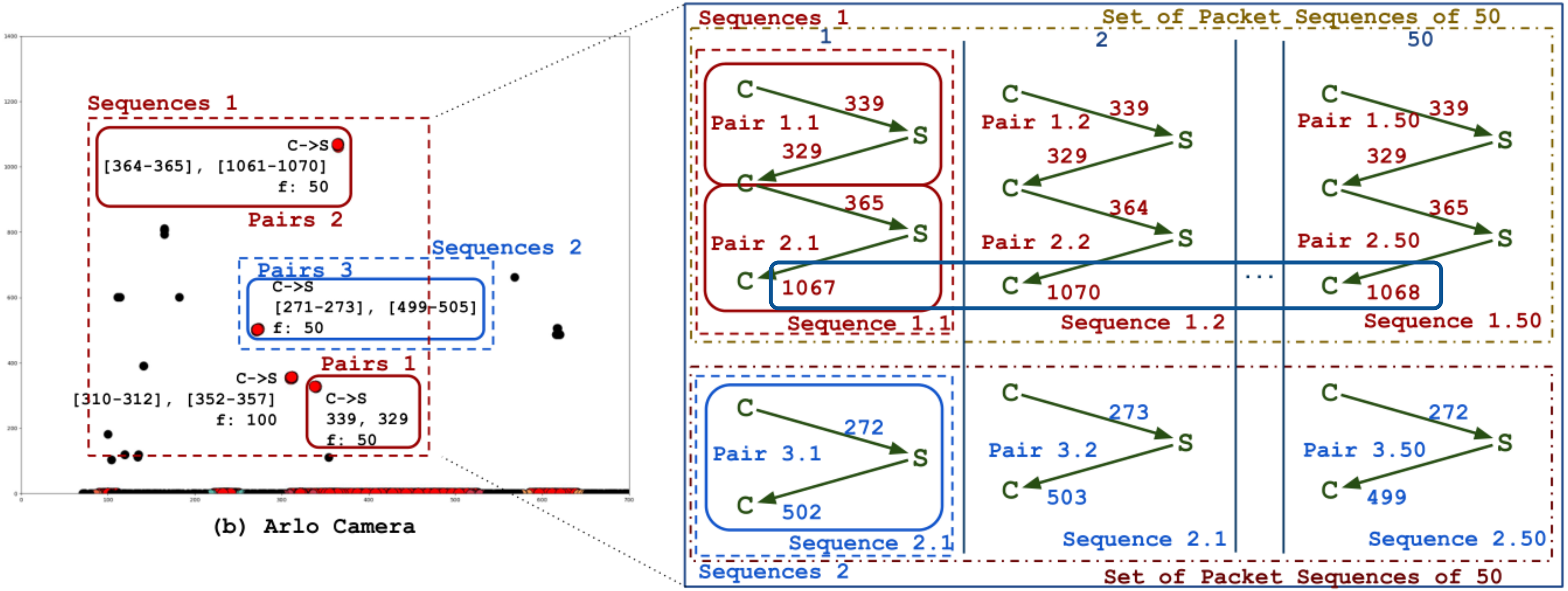
List of Packet Sequence Sets (= Packet-level signature)

C-339 S-329 C-[364-365] S-[1061-1070]

C-[271-273] S-[499-505]

UCI University of California, Irvine

PingPong Training



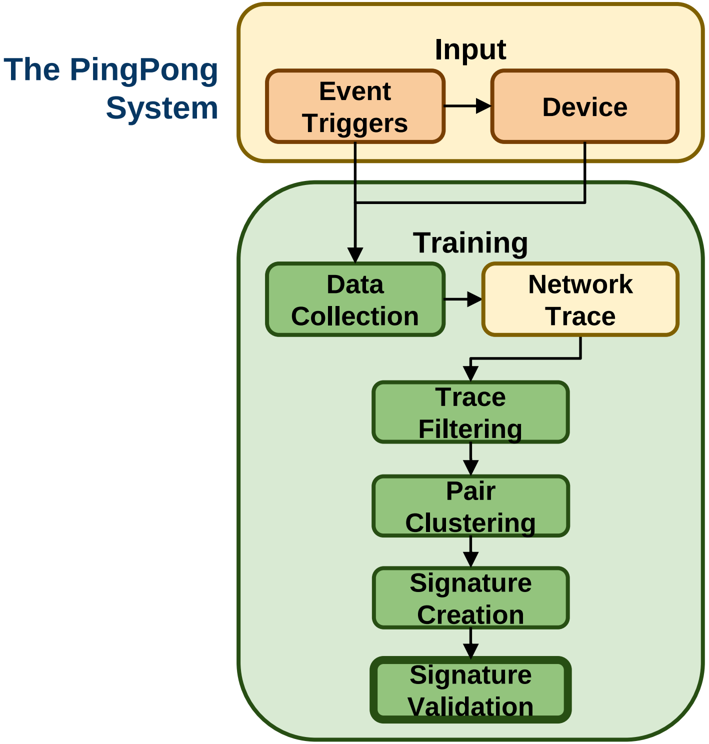
(b) Arlo Camera

List of Packet Sequence Sets (= Packet-level signature)

C-339 S-329 C-[364-365] S-[1061-1070]

C-[271-273] S-[499-505]

PingPong Training



- Run detection
  - Same PCAP file
- Valid signature iff
  - **n** detected events
  - **n** triggered events
  - **Matching** timestamps

UCI University of California, Irvine

PingPong Detection

Signature

Arlo Camera

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

PingPong Detection

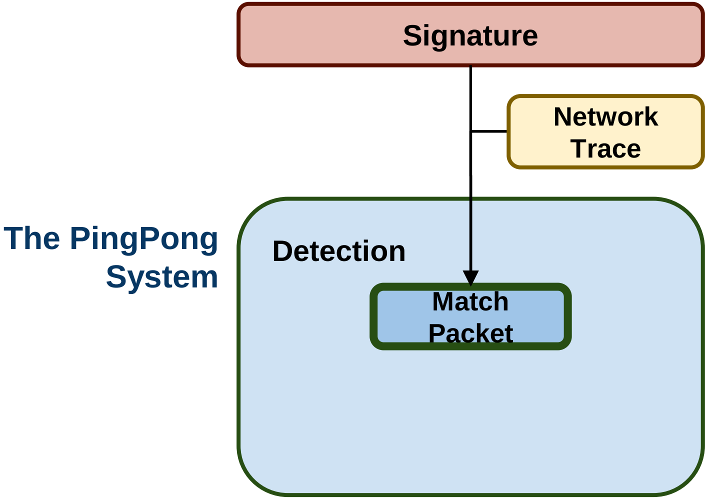
Signature

Network Trace

`C-339 S-329 C-[364-365] S-[1061-1070]`
`C-[271-273] S-[499-505]`

...

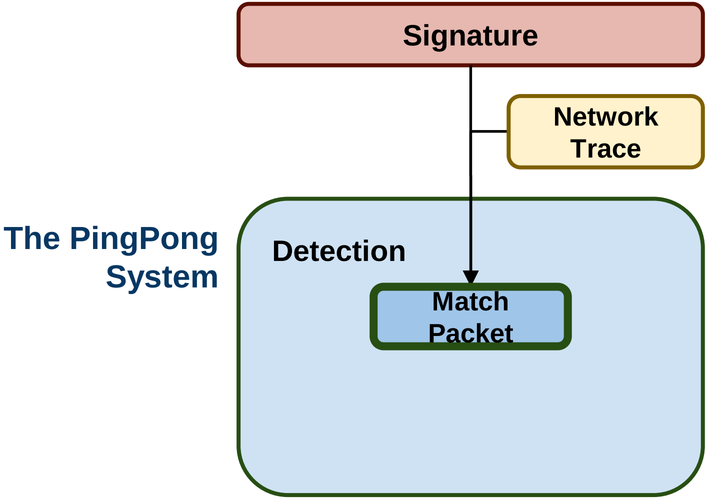
PingPong Detection



C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

... C-339

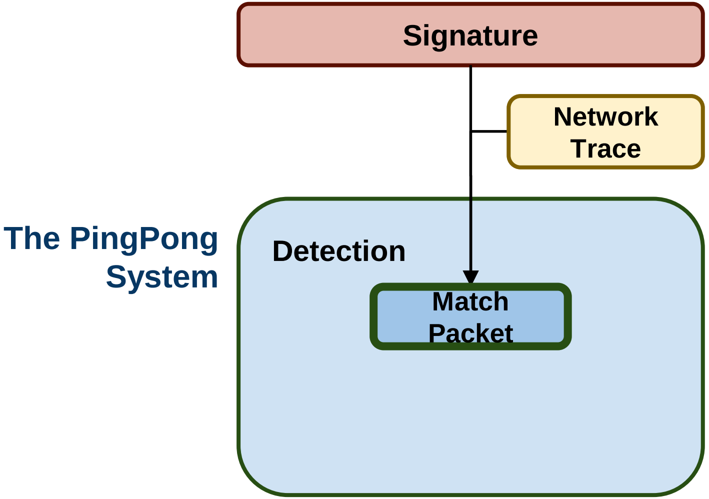
PingPong Detection



```
C-339 S-329 C-[364-365] S-[1061-1070]
      C-[271-273] S-[499-505]

         ... C-339 S-329
```

PingPong Detection

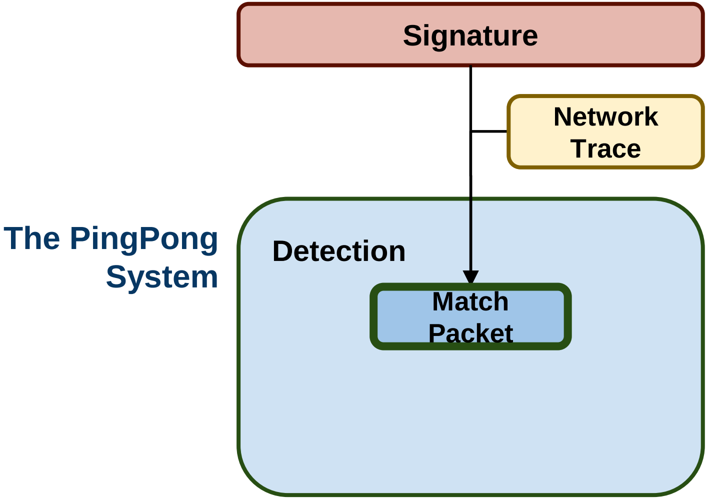


Range-based Matching

```
C-339 S-329 C-[364-365] S-[1061-1070]
            C-[271-273] S-[499-505]

      ... C-339 S-329 C-365
```

PingPong Detection

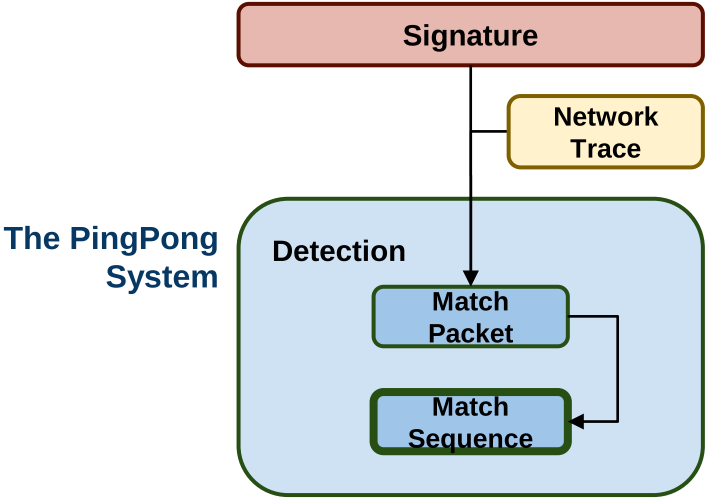


Range-based Matching

```
C-339 S-329 C-[364-365] S-[1061-1070]
      C-[271-273] S-[499-505]

   ... C-339 S-329 C-365 S-1065
```

PingPong Detection

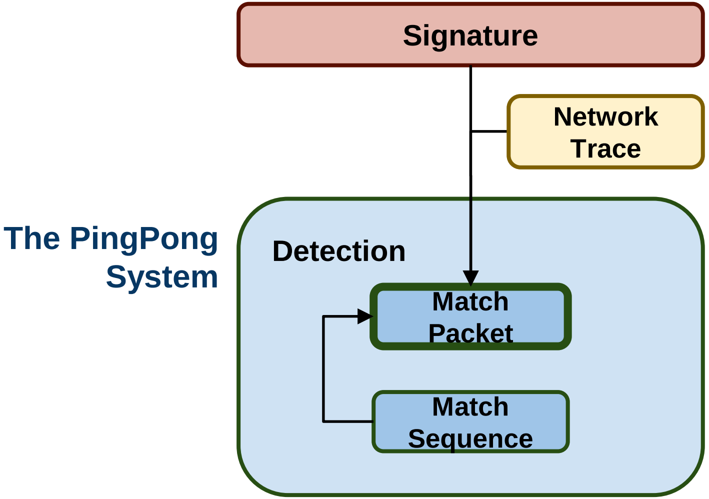


First Sequence Matched

```
C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]
```

```
... C-339 S-329 C-365 S-1065
```

PingPong Detection

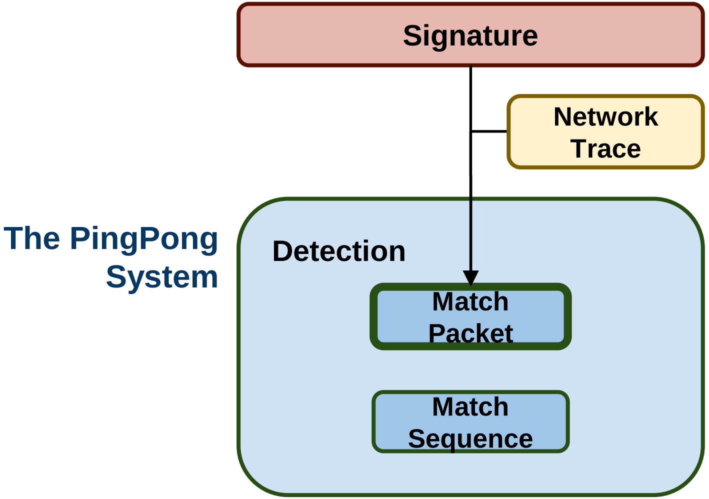


Range-based Matching

```
C-339 S-329 C-[364-365] S-[1061-1070]
     C-[271-273] S-[499-505]

   ... C-339 S-329 C-365 S-1065
           ... C-272
```

PingPong Detection

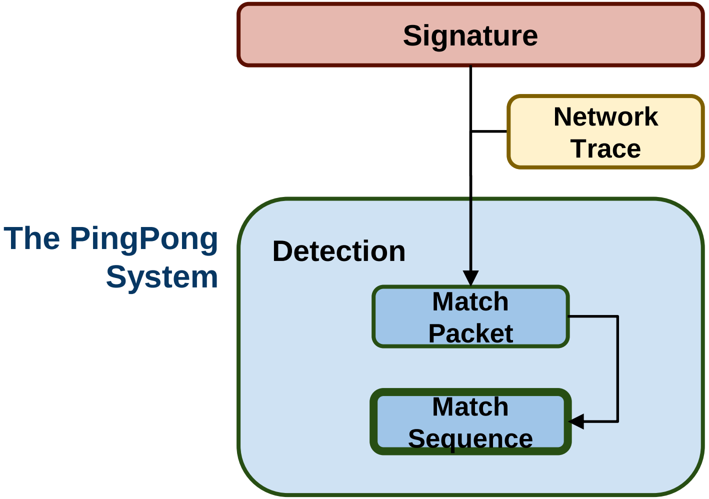


Range-based Matching

```
C-339 S-329 C-[364-365] S-[1061-1070]
      C-[271-273] S-[499-505]

   ... C-339 S-329 C-365 S-1065
         ... C-272 S-500
```

PingPong Detection



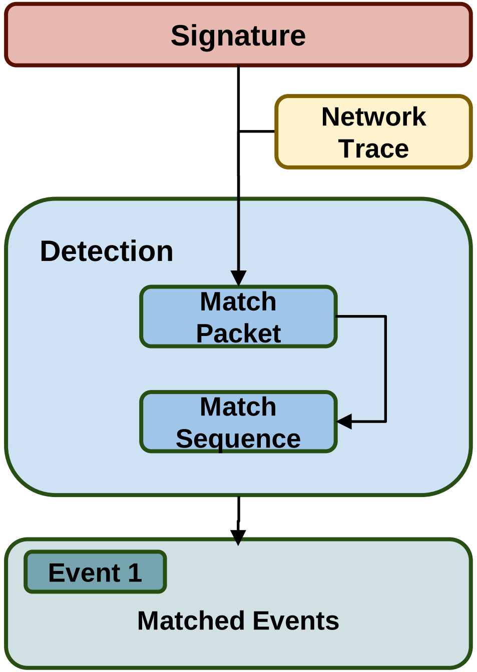
Second Sequence Matched

```
C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

... C-339 S-329 C-365 S-1065
... C-272 S-500
```

PingPong Detection

The PingPong System



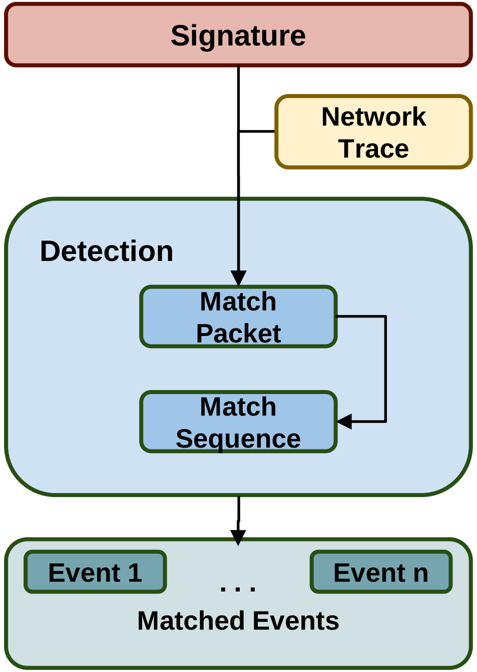
Event Match

```
C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]
```

```
... C-339 S-329 C-365 S-1065
... C-272 S-500
```

PingPong Detection

The PingPong System



Signature

Network Trace

Detection

Match Packet

Match Sequence

Event 1 . . . Event n

Matched Events

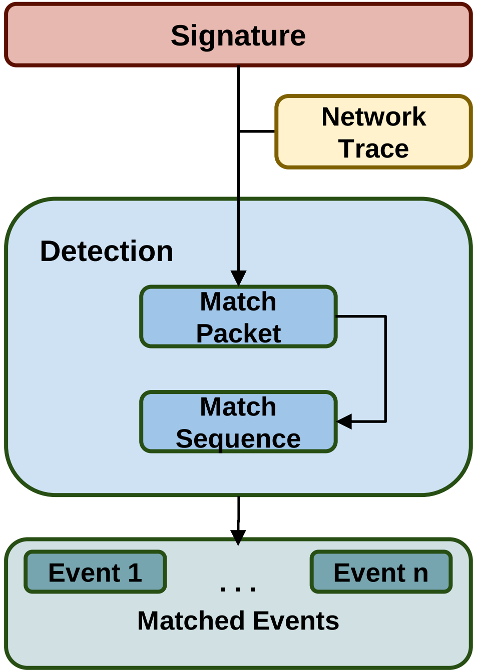
Event Match

```
C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]
```

```
... C-339 S-329 C-365 S-1065
... C-272 S-500
```

PingPong Detection

The PingPong System



Signature

Network Trace

Detection

Match Packet

Match Sequence

Event 1 . . . Event n

Matched Events

Event Match

```
C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]
```

```
... C-339 S-329 C-365 S-1065
... C-272 S-500
```

See paper for more detail

Possible Defenses

- Seemingly not effective defense
  - VPN
  - Traffic injection and shaping

Possible Defenses

- Seemingly not effective defense
    - VPN
    - Traffic injection and shaping
- More effective defense
    - Packet padding
        - Obfuscate packet lengths

Possible Defenses

- Not too effective defense
  - VPN
  - Traffic injection and shaping
- More effective defense
  - Packet padding
    - Obfuscate packet lengths
- **See paper** for detail