Network and Security Monitoring in the IoT and Fog Computing Age

Luca Deri <deri@ntop.org>
@lucaderi

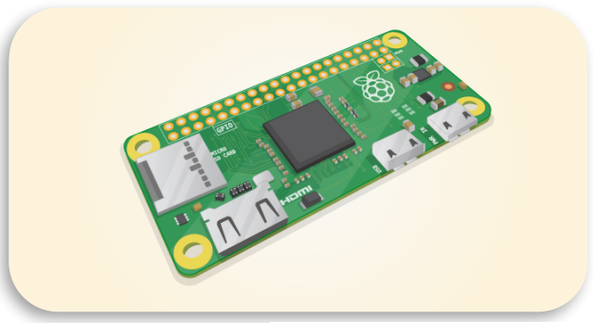
ntop

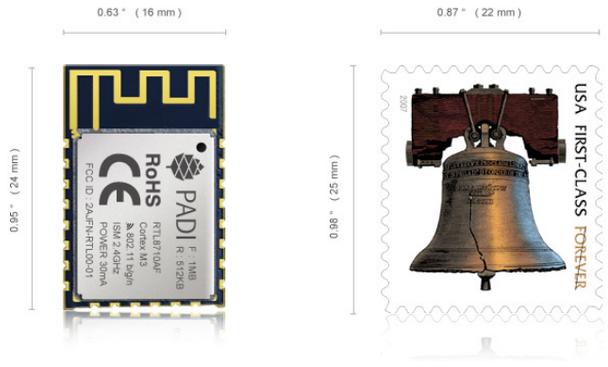
About ntop

- ntop develops open source network traffic monitoring applications, part of major Linux/BSD software distributions.
- ntop (circa 1998) is the first app we released and it is a web-based network monitoring application.
- Today our products range from traffic monitoring, high-speed packet processing, deep-packet inspection (DPI), IDS/IPS acceleration, and DDoS Mitigation.
- See http://github.com/ntop/

It all Started with a sub-5$ Computer…

- Building low-cost devices able to run full fledged OSs (e.g. Linux) enabled computing to become really pervasive.
- No more excuses for not automating tasks, or rethinking existing processes in a more intelligent fashion.

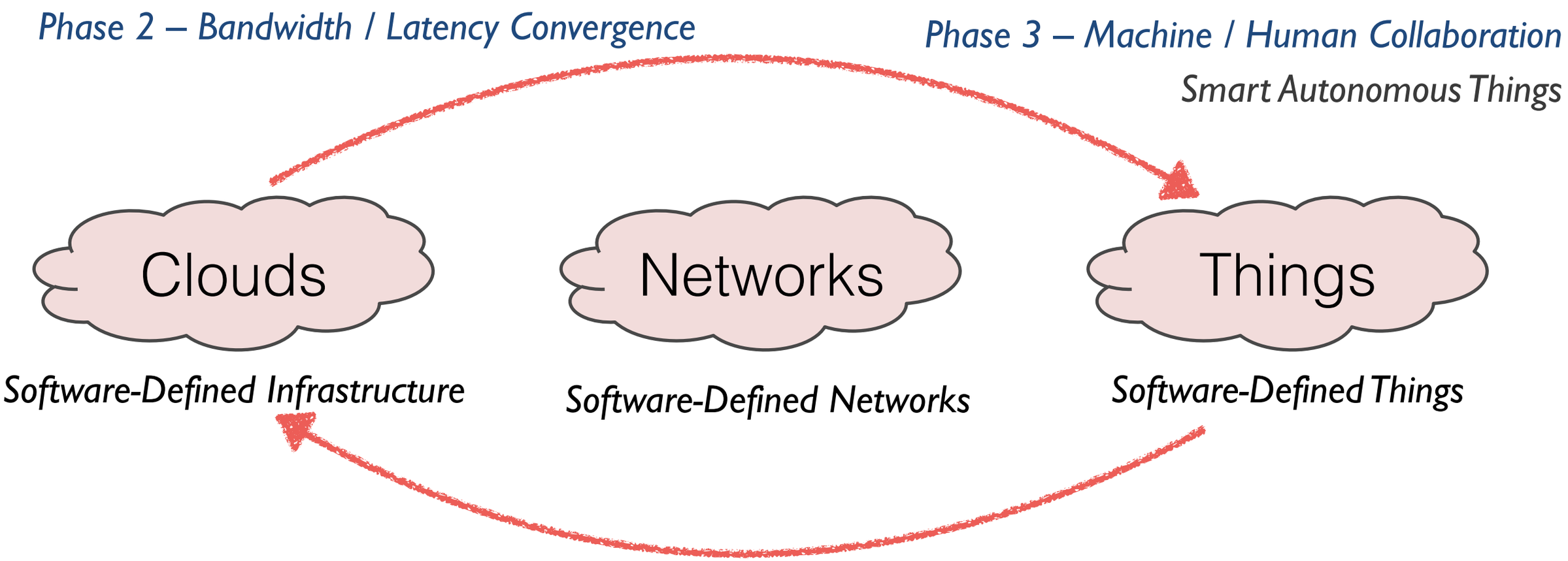




- 1Ghz, Single-core CPU
- 512MB RAM
- Mini HDMI and USB On-The-Go ports
- Micro USB power
- HAT-compatible 40-pin header
- Composite video and reset headers

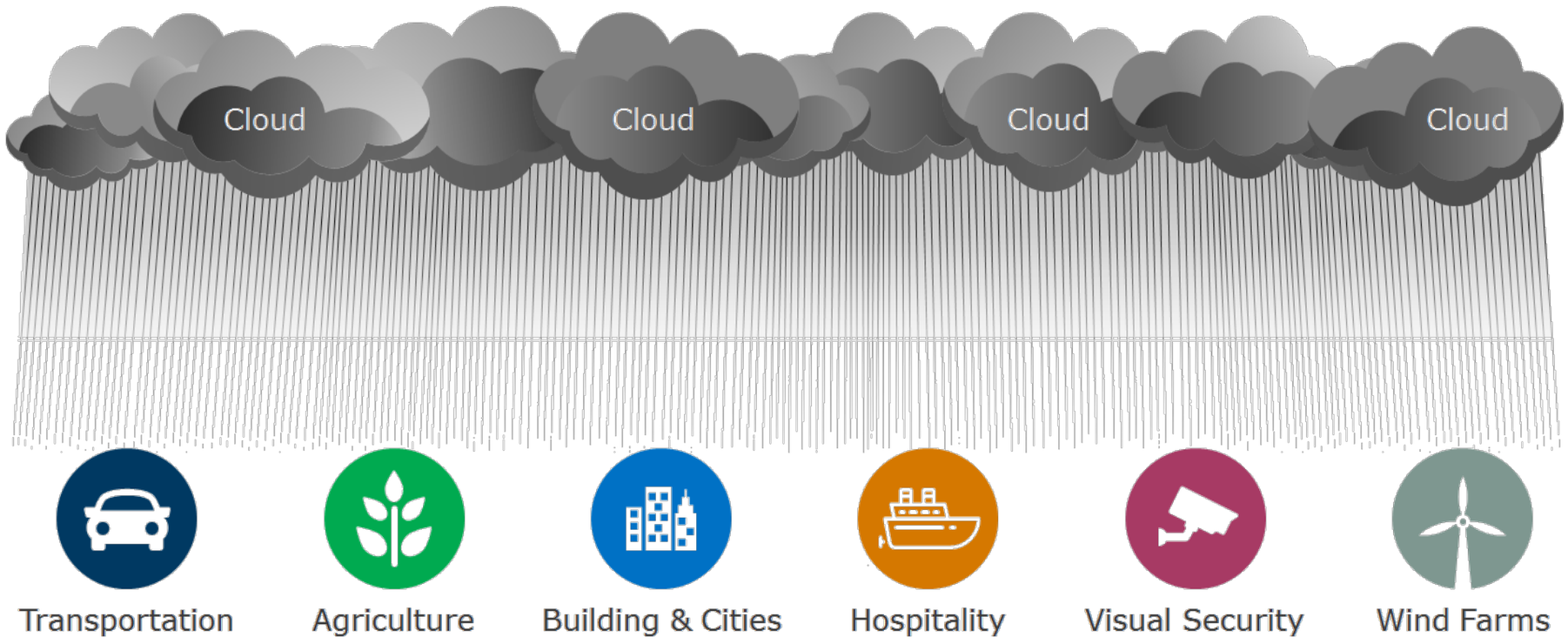
Raspberry PI zero (US$ 5)
Pine64 PADI IoT (US$ 1.99)

IoT Transformation



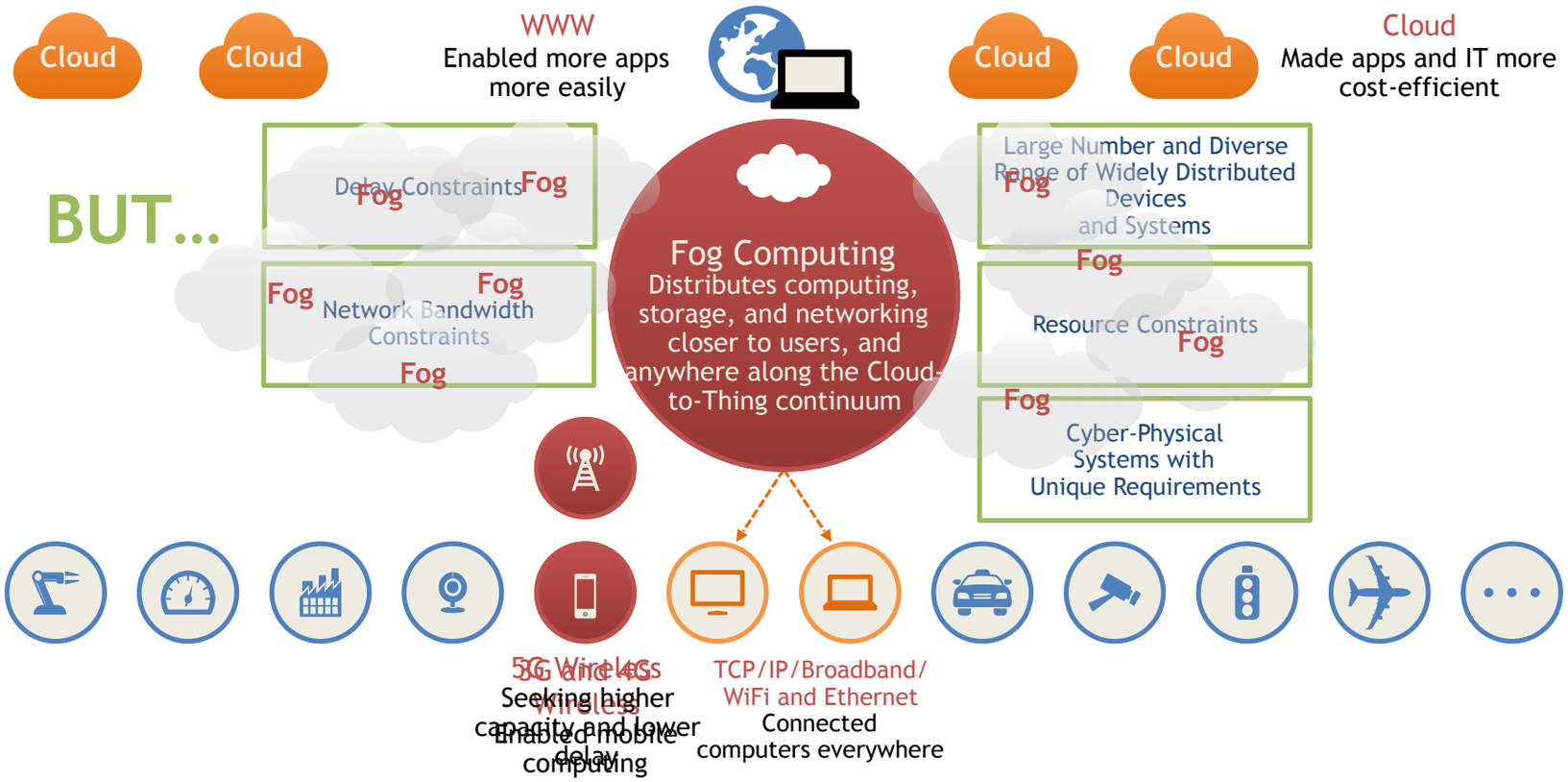
However All This Cannot Scale…

- The cloud alone cannot support the **IoT momentum**.
- There is a need for **filtering** and **processing** *before* the Cloud.

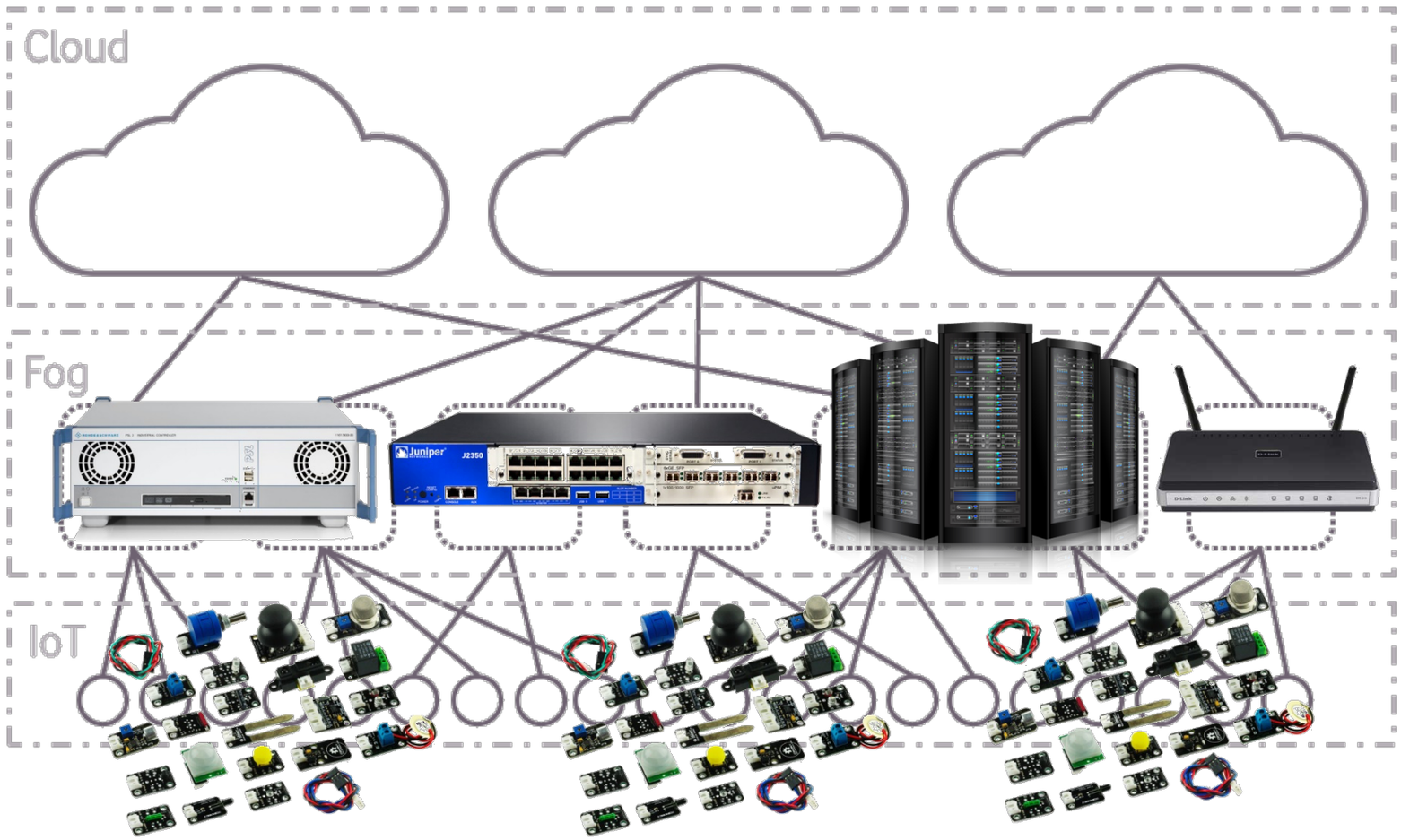


50 billion of connected devices by 2020 (Source Intel)

Towards Fog Computing



What is Fog Computing

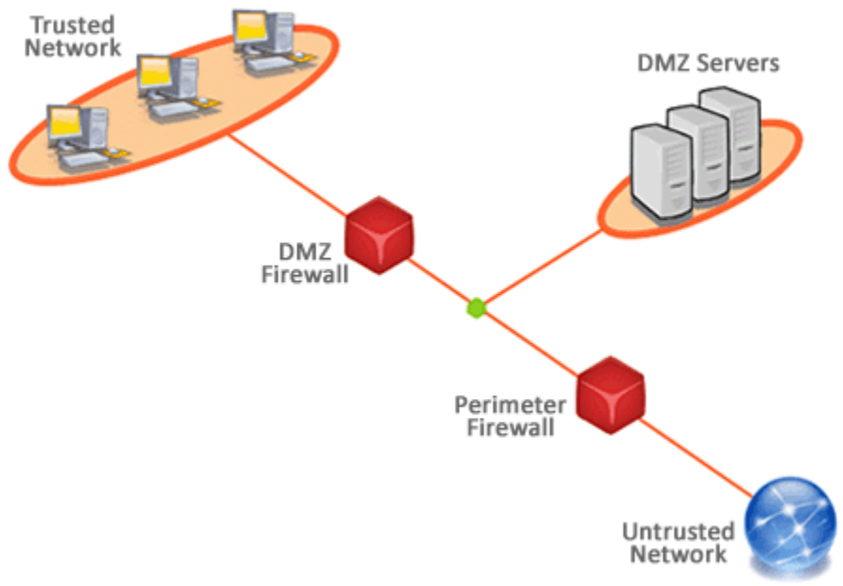


FOG COMPUTING: a system-level horizontal architecture that distributes computing, storage, and networking closer to users, and anywhere along the Cloud-to-Thing continuum

A Broken Security Model [1/3]

"Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job."

Jerome Saltzer



- Procedural Security
- Logical Security
- Physical Security

Denning's Least Privilege Principle

A Broken Security Model [2/3]

- The Low-voltage Environment:
  - Wide-spread use of IoT devices.
  - Increasing interconnection between edge devices and corporate networks: an edge device has important topological privileges.
  - Edge devices lack built-in security features: too simple, yet easy to attack or replace with "trojan" devices.
  - Physical location renders networks vulnerable to external attack – even without Internet connection

A Broken Security Model [3/3]

- Unsecured low-voltage devices:
  - Access control
    - Unauthorised opening of gates/doors, false attendance information.
  - Video surveillance cameras
    - Manipulation of video camera streams, unauthorised viewing or disabling video edge-device elements.
  - Building-management/Fire-alarm systems
    - False readings, disabling or blinding.
  - Perimeter IP-based sensors
    - False readings, disabling or blinding.
  - DDoS (Distributed Denial of Service) attacks, can disrupt network operations and thus break a complex system/factory.

Traditional Network Monitoring Is Becoming Outdated…

- Popular metrics such as bytes, packets, best-match routing are being revisited since users care about latency and application service time.
- Polling-based protocols (e.g. SNMP) are being replaced by push-oriented approaches (e.g. Cisco Telemetry).
- Binary/custom protocols (e.g. NetFlow/IPFIX) are being replaced by (less efficient yet more flexible/ open) JSON-based data sources so that data can be shared across components.

Basically We Need to Monitor…

- Dynamic network topologies and moving components.
- Identify IoT devices and threat them differently from "generic" computers (e.g. laptops or tablets)
- Tag network traffic with application protocol and monitor it continuously overtime looking at specialised metrics (e.g. HTTP return code) in addition to generic ones (e.g. jitter and bandwidth).
- As IoT devices are not installed in "controlled environments" (e.g. a rack on a datacenter vs on a corridor) physical security needs also to be monitored.

IoT Monitoring: Device Profile

- A device profile is a pair
  < < Mac, IP, Port >, < Service IN, Service OUT > >

ARP Monitoring

SNMP Device/Bridge Monitoring

L7 services provided by a device
(e.g. RTP streaming for a camera)

L7 services used by a device
(e.g. SMTP for sending notifications)

IoT Monitoring: Traffic Profile

- A traffic profile is a pair
  < < Device, Service, Latency, < Thpt $_{UP}$, Thpt $_{DOWN}$ >,
  Protocol Metadata > >
- Device: subject of the communication.
- Service: Layer 7 (DPI) protocol identification.
- Latency: service time (slow response is a problem for devices such as burglar alarms).
- Throughput: create baseline (e.g. low throughput for a camera is an indication of a problem/attack).
- Metadata: used to pinpoint a problem (e.g. error reported).

Monitoring IoT (Security) [1/2]

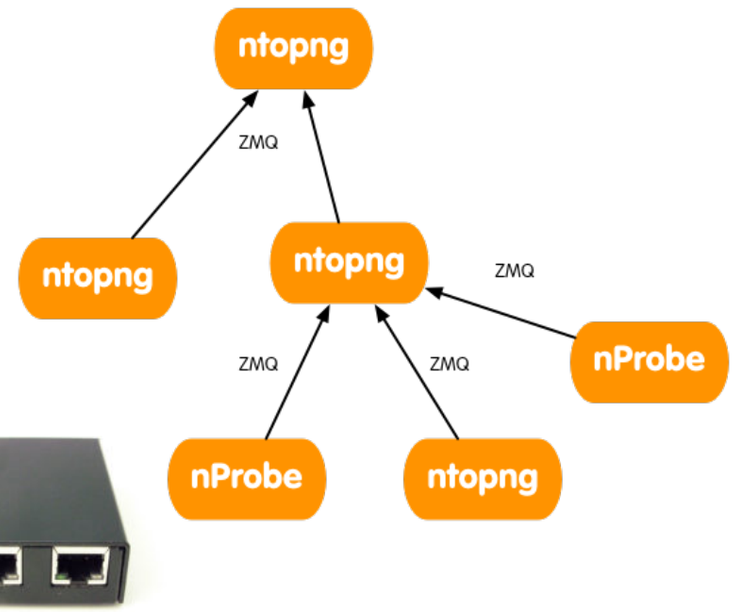
- Learning
  - Identify network elements (discovery), assign them a role (e.g. a printer).
- Profiling
  - Bind a device to a profile (e.g. a printer cannot Skype or share files using BitTorrent) and enforce it via alarms or traffic policy enforcement.
- Continuous Monitoring
  - Physical constraints (e.g. MAC/IP binding and switch port location), traffic constraints (e.g. a new protocol serviced by a device or throughput above/under its historical baseline can be an indication of a problem).

Monitoring IoT (Security) [2/2]

- In IoT monitoring traffic patters are rather static and thus once a model is created it must be observed regularly overtime, if not alert.
- Triggers notifications if devices fail due to electrical, software, mechanical or other faults: active monitoring/ polling is compulsory (passive is not enough).
- Threats
  - External: monitor/detect breaches in the low-voltage network.
  - Internal: monitor/detect network threats through unauthorised use (e.g. HTTP access to a device from a client that never did that before).

Solution Overview [1/3]

- Software-only, low-cost sensors that can be embedded in devices or deployed at the network edge, to create a collaborative monitoring infrastructure.



- Tag devices, traffic, and users.

SIP	0 B	7.06 KB	Rcvd	7.06 KB	0 %
SNMP	4.5 MB	4.18	Sent Rc	8.67 MB	1.54 %
SSH	593.4 KB	4.11 MB	Sen Rcvd	4.69 MB	0.83 %
SSL	3.26 MB	4.17 MB	Sent Rcvd	7.43 MB	1.32 %
Skype	0 B	11.54 KB	Rcvd	11.54 KB	0 %
Tor	37.34 KB	58.7 KB	Se Rcv	96.04 KB	0.02 %

What do we need to hide here?

Ingress but no egress traffic: service scan?

Solution Overview [2/3]

All Layer 2 Devices

ARP Stats

10 ▾ Filter MACs▾ Manufacturer▾

MAC Address	Manufacturer	Hosts	ARP Sent	ARP Received	Seen Since	Breakdown	Throughput	Traffic
80:2A:A8:8D:69:2C	Ubiquiti Networks Inc.	269	38	8	4 min, 32 sec	Sent Rc	9.1 Kbit	4.36 MB
C4:2C:03:06:49:FE	Apple, Inc.	1	10	8	4 min, 32 sec	Se Rcvd	8.75 Kbit	4.37 MB
CC:2D:8C:F6:C7:39	LG ELECTRONICS INC	1	5	2	4 min, 30 sec	Sent R	95.88 bps	14.62 KB
54:4E:90:BA:EC:84	Apple, Inc.	2	5	0	2 min, 16 sec	Sent	361.17 bps	10.22 KB
AC:87:A3:16:3E:30	Apple, Inc.	1	0	0	4 min, 6 sec	Sent	0 bps	2.61 KB
80:2A:A8:8D:2B:EE	Ubiquiti Networks Inc.	1	0	0	3 min, 30 sec	Sent	0 bps	228 B
26:A4:3C:FF:4C:D7	n/a	0	0	0	2 min, 24 sec	Sent	0 bps	468 B
28:57:BE:E3:D7:CF	Hangzhou Hikvision Digital Technology Co.,Ltd.	1	0	0	4 min, 31 sec	Sent	0 bps	13.6 KB
24:A4:3C:FE:4C:D7	Ubiquiti Networks Inc.	1	0	0	2 min, 22 sec	Sent	0 bps	1.45 KB

Showing 1 to 9 of 9 rows

Hosts Monitoring

Physical Location

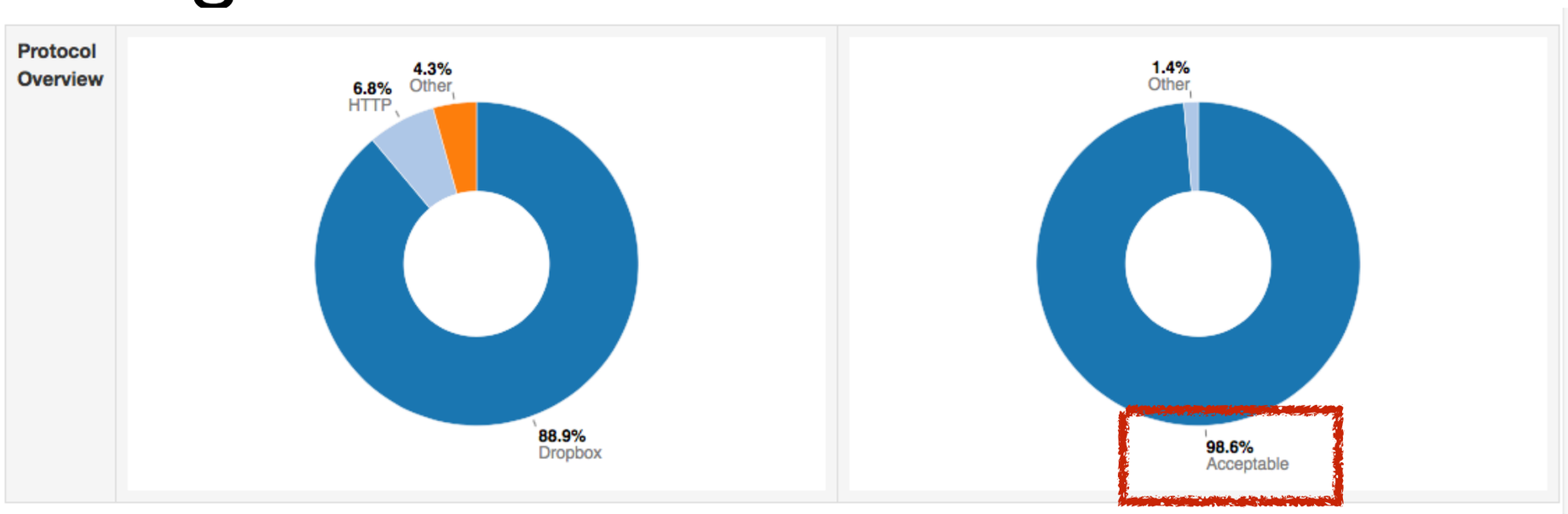
Mac: 80:2A:A8:8D:69:2C

MAC Address	80:2A:A8:8D:69:2C (Ubiquiti_8D:69:2C) [Show Hosts]	80:2A:A8:8D:69:2C Save
First / Last Seen	02/04/2017 19:28:54 [4 min, 35 sec ago]	02/04/2017 19:33:26 [3 sec ago]
Sent vs Received Traffic Breakdown	Sent	Rcvd
Traffic Sent / Received	5,111 Pkts / 3.71 MB	4,558 Pkts / 666.24 KB
Address Resolution Protocol	**ARP Requests**	**ARP Replies**
	38 Sent / 0 Received	0 Sent / 8 Received

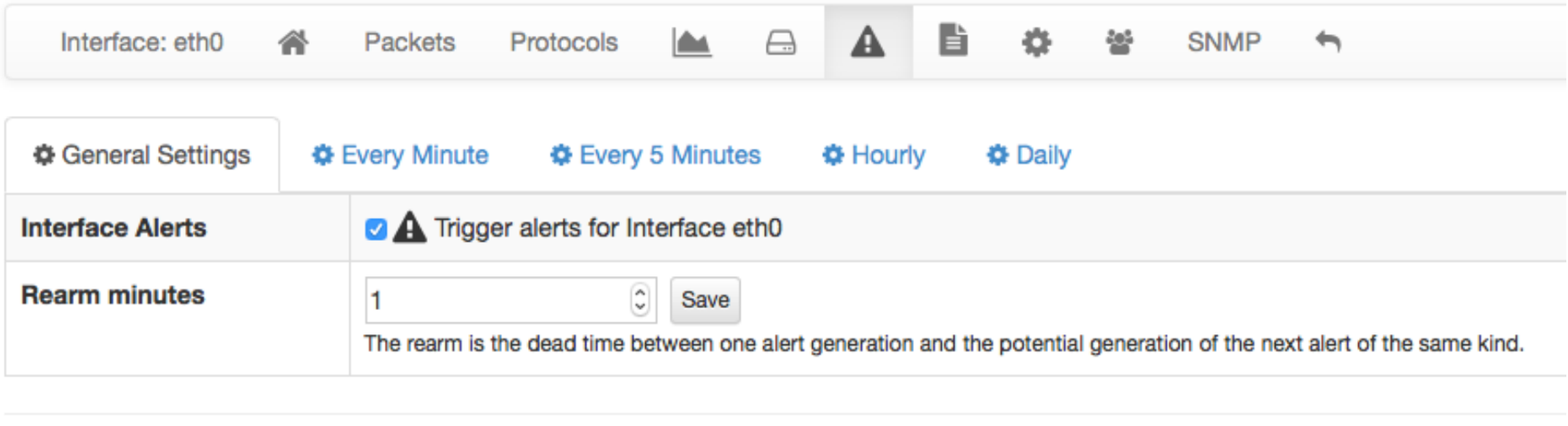
Device Port	
600	ge-0/1/0 trunk
324	ge-0/1/0 trunk
572	ge-0/0/35

Solution Overview [3/3]

- Baselining



- Alerting



Final Remarks

- IoT and Fog computing create new monitoring challenges and require an *integrated monitoring* approach: element + periodic active scans + permanent passive traffic monitoring.
- Monitoring hundred/thousand devices require *scalability* and *intelligence* in the monitoring platform (analytics and big data is not enough, platform must be reactive, distributed, multi-tenant).
- Bytes+Packet-based monitoring must be *complemented* with specialised metrics, DPI, realtime telemetry monitoring, flexible (on-the-go) alerting.

Credits: Antonio Cisternino, Stefano Forti, Ohad Kleinman.