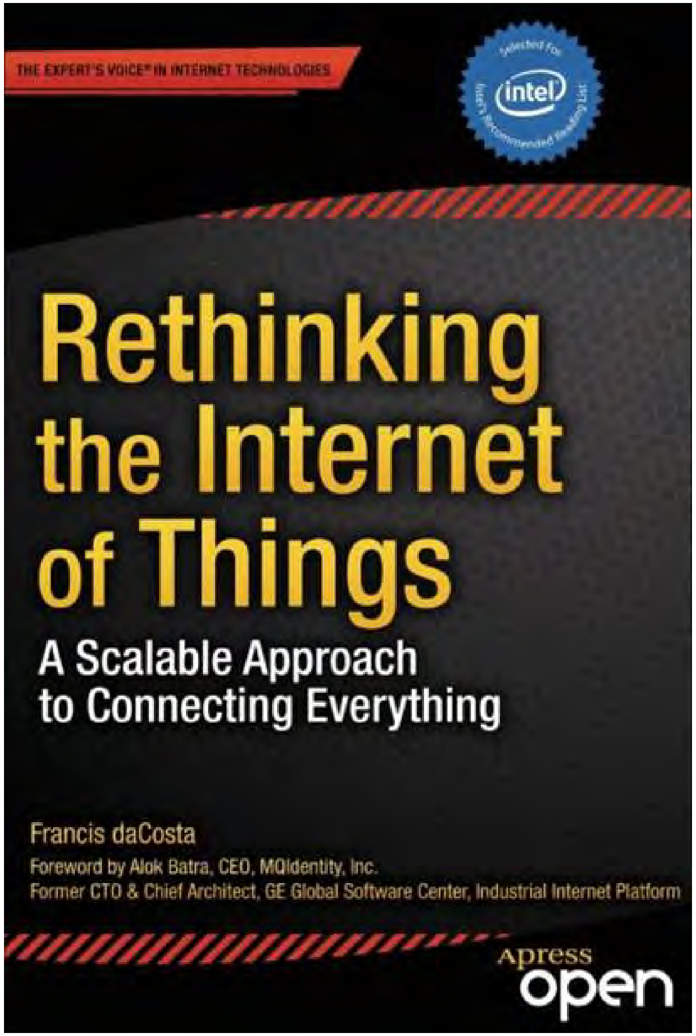
Open Source

For

Rethinking IoT

Francis da Costa



Francis daCosta: Past Experience and Expertise

- Real time Embedded systems and control
- Robotics, Machine Learning
- Distributed networking intelligence
- Real time Publish / Discover / Subscribe
- Real time Scheduling at network level.

- Founder/CTO; MeshDynamics (Mesh networking)
- Founder/CTO; Knowmadic (“Big” Data)
- Founder/CTO: Advanced Cybernetics Group (Robotics)
- IoT Stealth Startup: (Chirp Networks)

http://www.linkedin.com/in/francisdacosta/

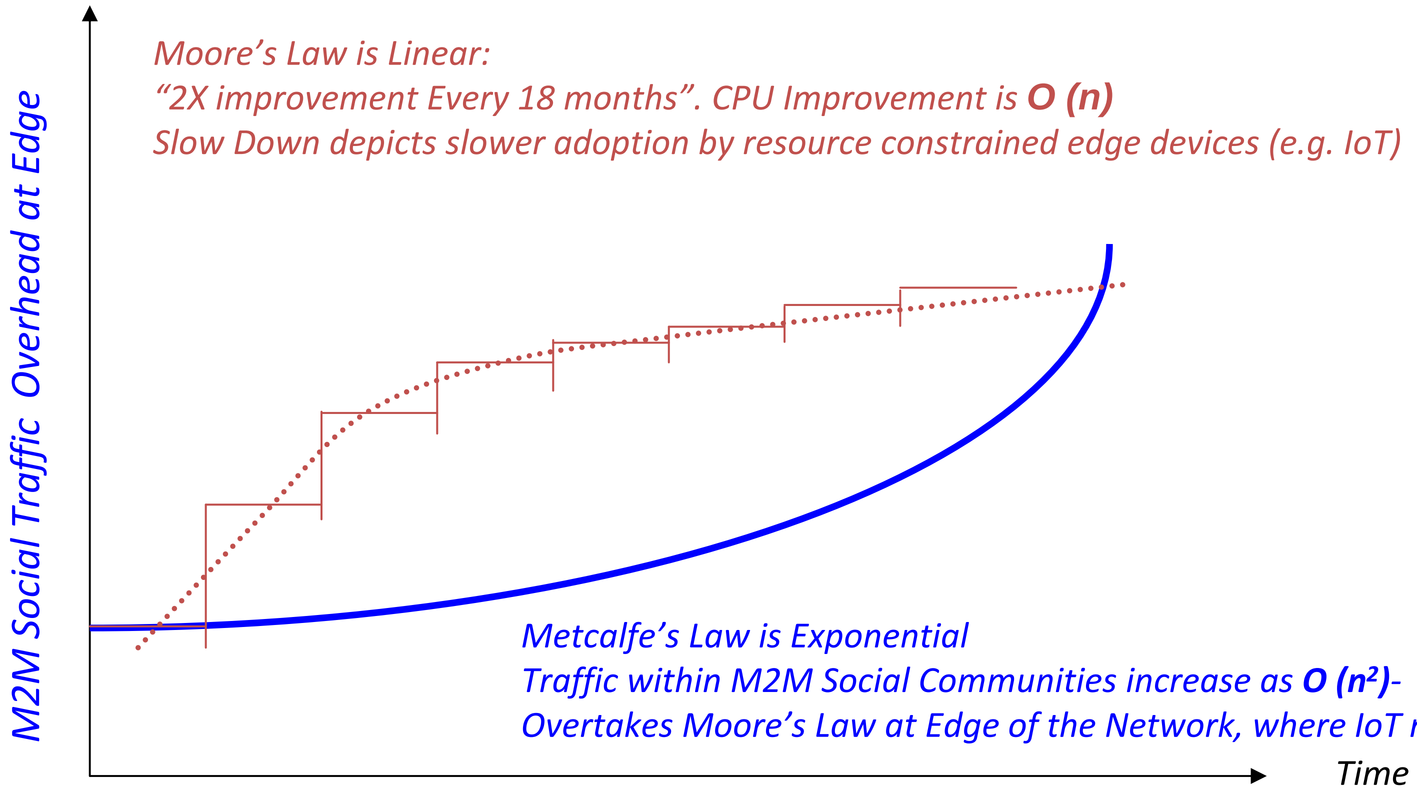
Why Open Source is *Essential* For IoT

Its Different Out There:

The IoT won’t be much like the traditional Internet:

- Scope – it’s 100 times bigger
- Simple – majority of end devices “dumb”
- Scalable – All control cannot be centralized
- Subscription-based – too much data otherwise
- Security – must be incremental
- ***Standards*** – Must be Open-Source with privacy extensions

The Challenge: Moore's Vs Metcalfe's at the Edge (IoT)



A new approach is needed for networking at the "Edge"

Simpler Devices Must Rule

Next wave of the Internet is Machines to Machines Ecosystems

Humans Oriented Ecosystem

- Lots more Processor, Memory, Protocol stacks
- Human Oriented Consumption (external)
- Assumed often "Always On"
- Centrally-managed naming (MACID, et al)

Machines Oriented Ecosystem

- Often Limited to microcontrollers etc.
- Consumption for local use (Internal)
- Many remote with Intermittent power
- Built by millions of manufacturers worldwide

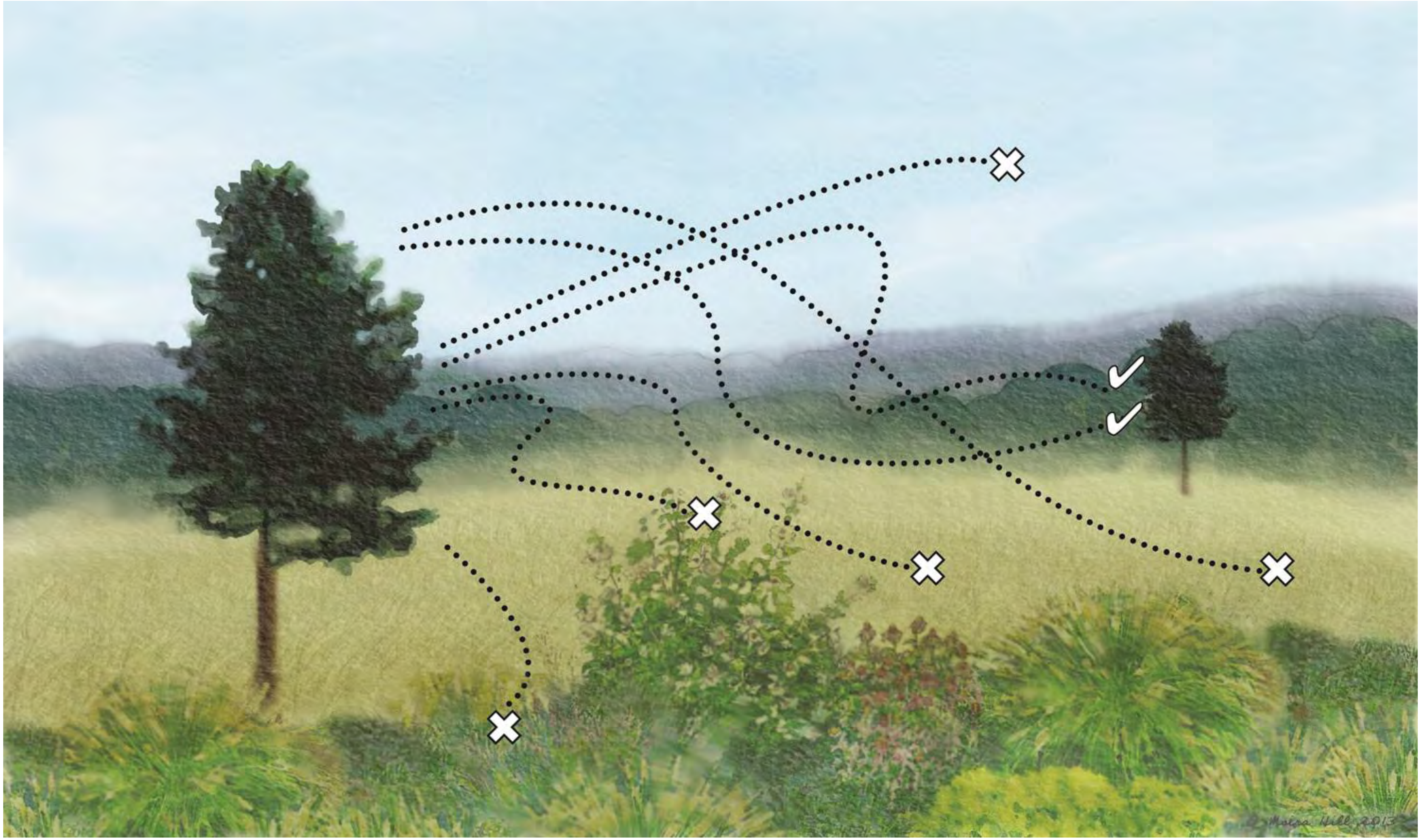
… many *cannot afford* traditional IP protocol overhead

IoT Data Characteristics

Machine to Machine (M2M)

- Terse – not oriented to humans
- Repetitive
- Individual messages not critical
- Meaning comes from *combination* with other data sourcoes – “Small Data”
- Consumption and Generation is mostly Local – M2M communities
- Often unidirectional,
- **Self-classified** – new and necessary concept

Self-Classification Lesson from Nature: Pollen "Chirps"



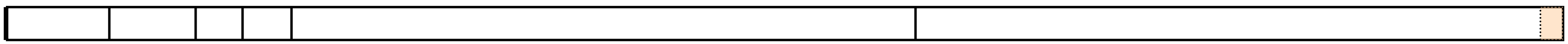
Pollen propagates everywhere, but only *specific* receivers decode "message"

Self Classification Lesson from Nature: Birdsong “Chirps”

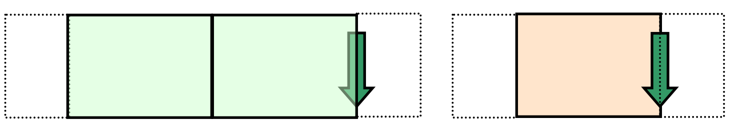
All birds derive some information, but only *specific* receivers fully participate

IoT Data is Different, Protocol Must be Different: Chirps

IPV6 Overhead = 40 bytes, 1 byte payload



Chirp Overhead = 4 bytes, 1 byte payload



Public Chirp Classification *Private payload*

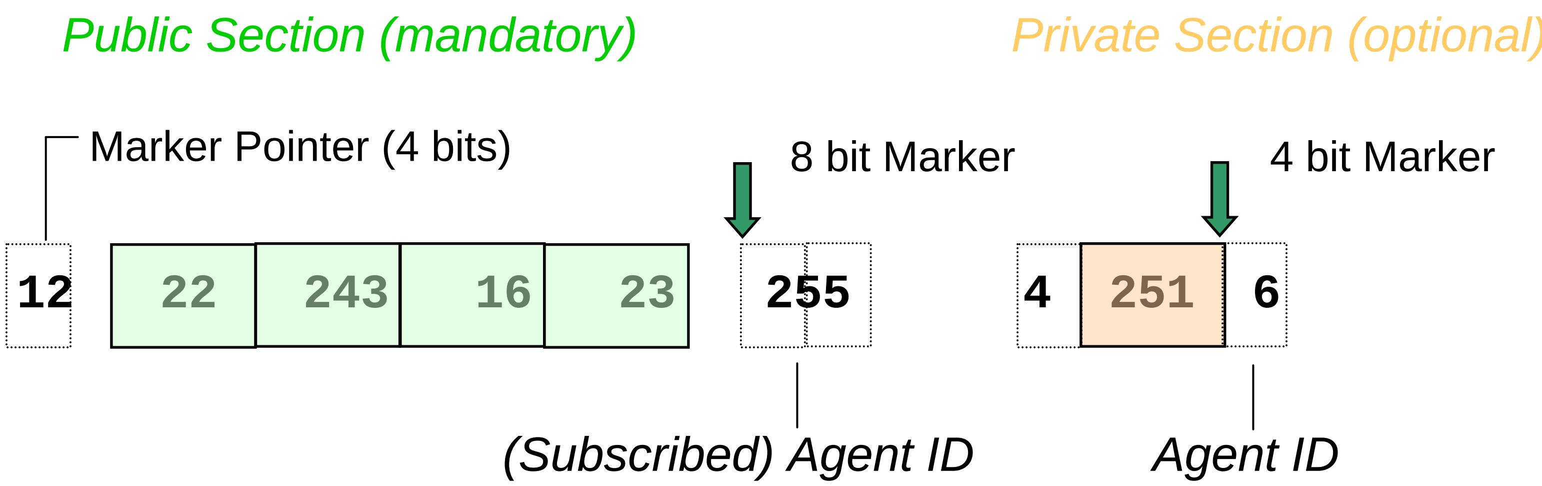
Note that Chirp *lacks*:

- Universally unique ID

- Error correction/retransmission

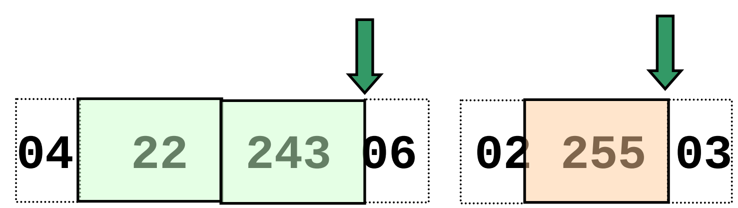
Minimal overhead for end device, but it must be applied *elsewhere*:
-"Propagator" Nodes/Network (discussed later)

Self-Classification “Pollen/Birdsong” for IoT: Chirps



Total chirp length with 2 Byte Public Field, 4 bit Marker, 1 Byte Payload = 5.0 bytes

5.0 Bytes with 1 Byte Payload
6.0 Bytes with 2 Byte Payload
7.0 Bytes with 3 Byte Payload
8.0 Bytes with 4 Byte Payload



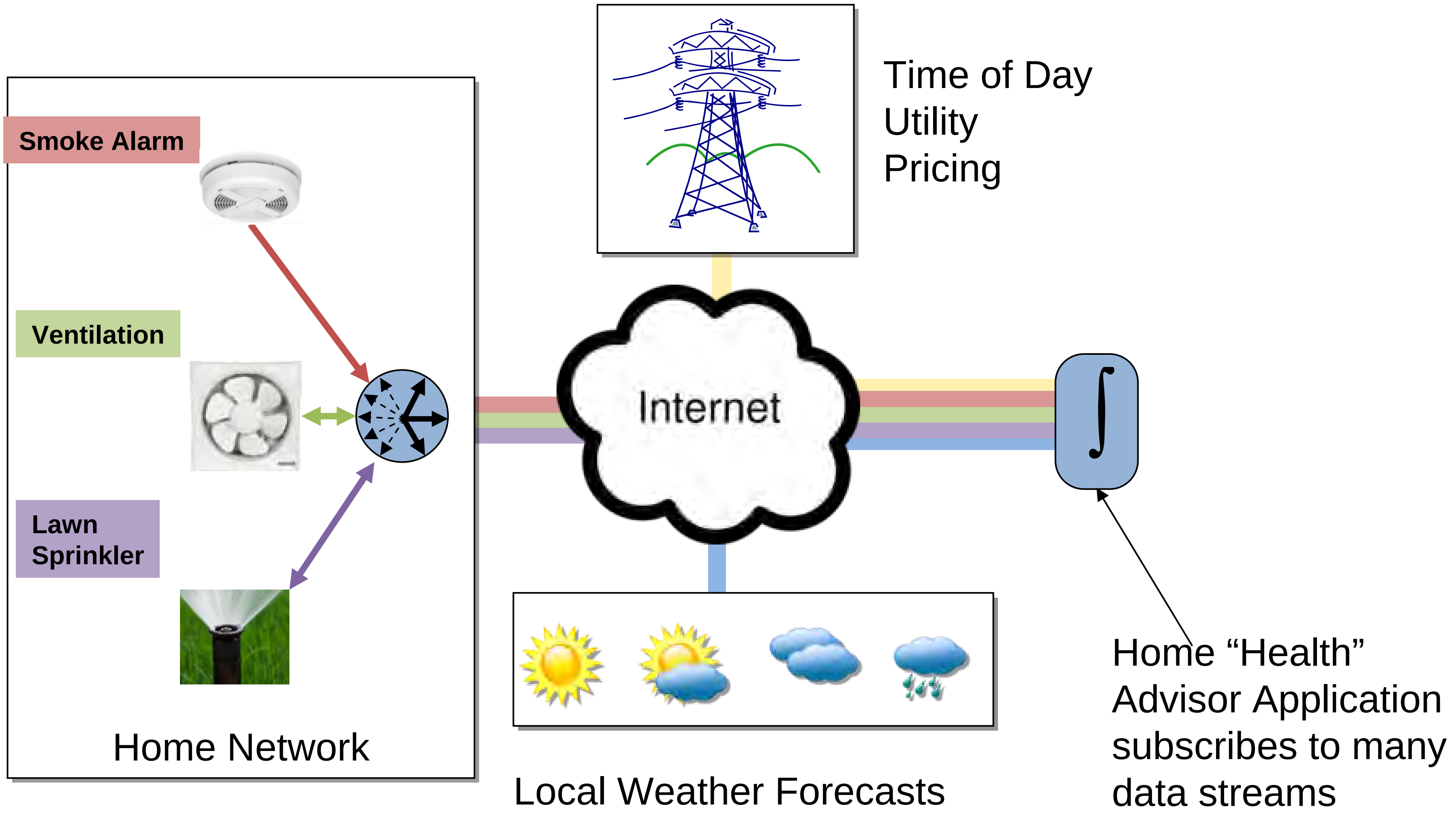
Self-Classification is Key to Discover / Subscribe

- Massive amounts of data published from trillions of devices
- Servers ("Integrator Functions") will discover and subscribe to interesting small data flows
- This requires self-classification at end device
  - Basic: Type of device (moisture sensor, streetlight, etc.) from <u>open-source</u> taxonomy
  - Incremental: unlimited additional classification through private fields
- Published data may be open to all *or* proprietary

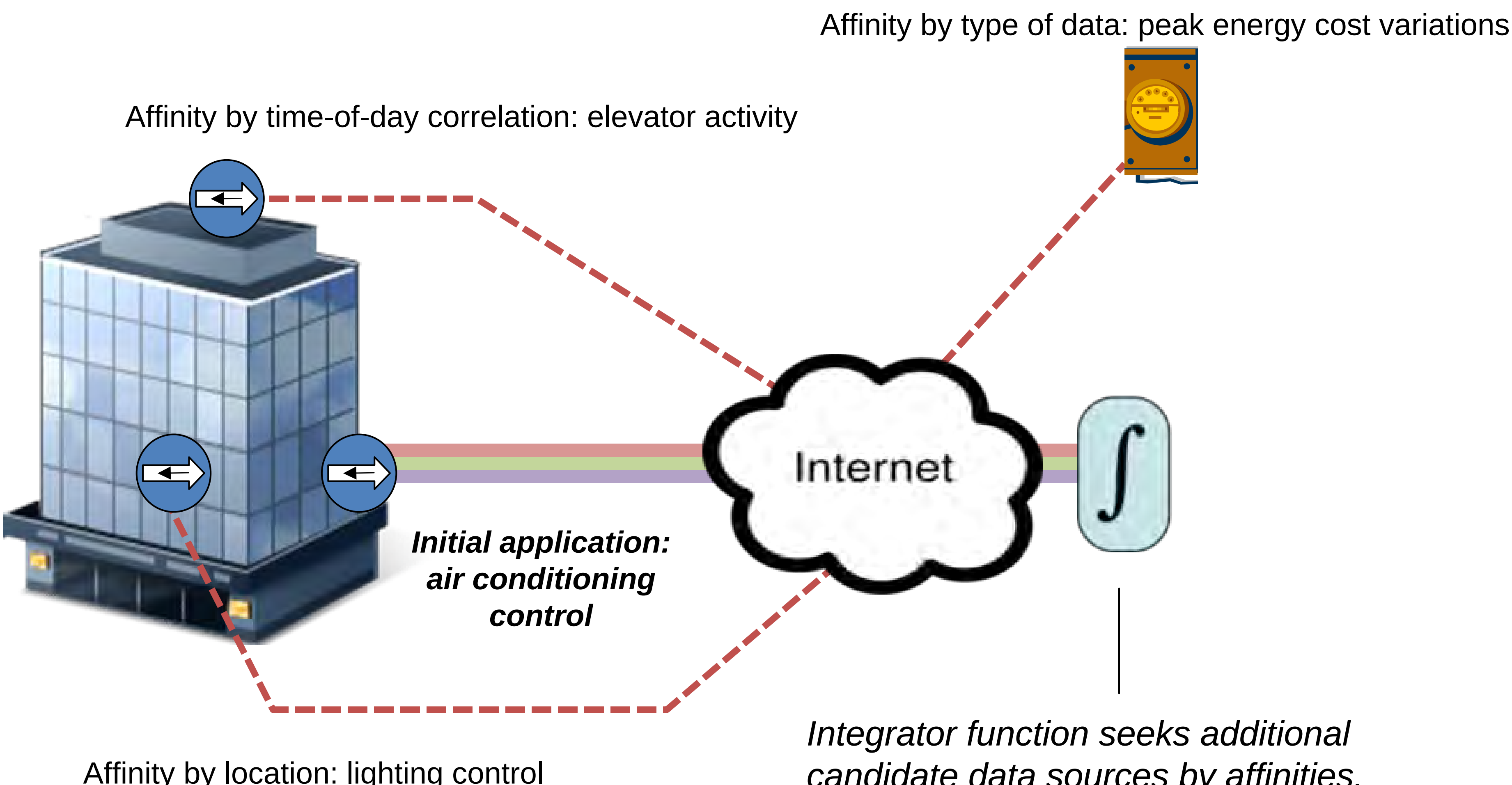
Discover/Publish/Subscribe Lesson from Nature: Affinities

Underlying event not seen, but *affinities* are visible.

Known Publish/Subscribe Affinities ("Pollen")



Discovered Publish/Subscribe Affinities (“Pheromones”)



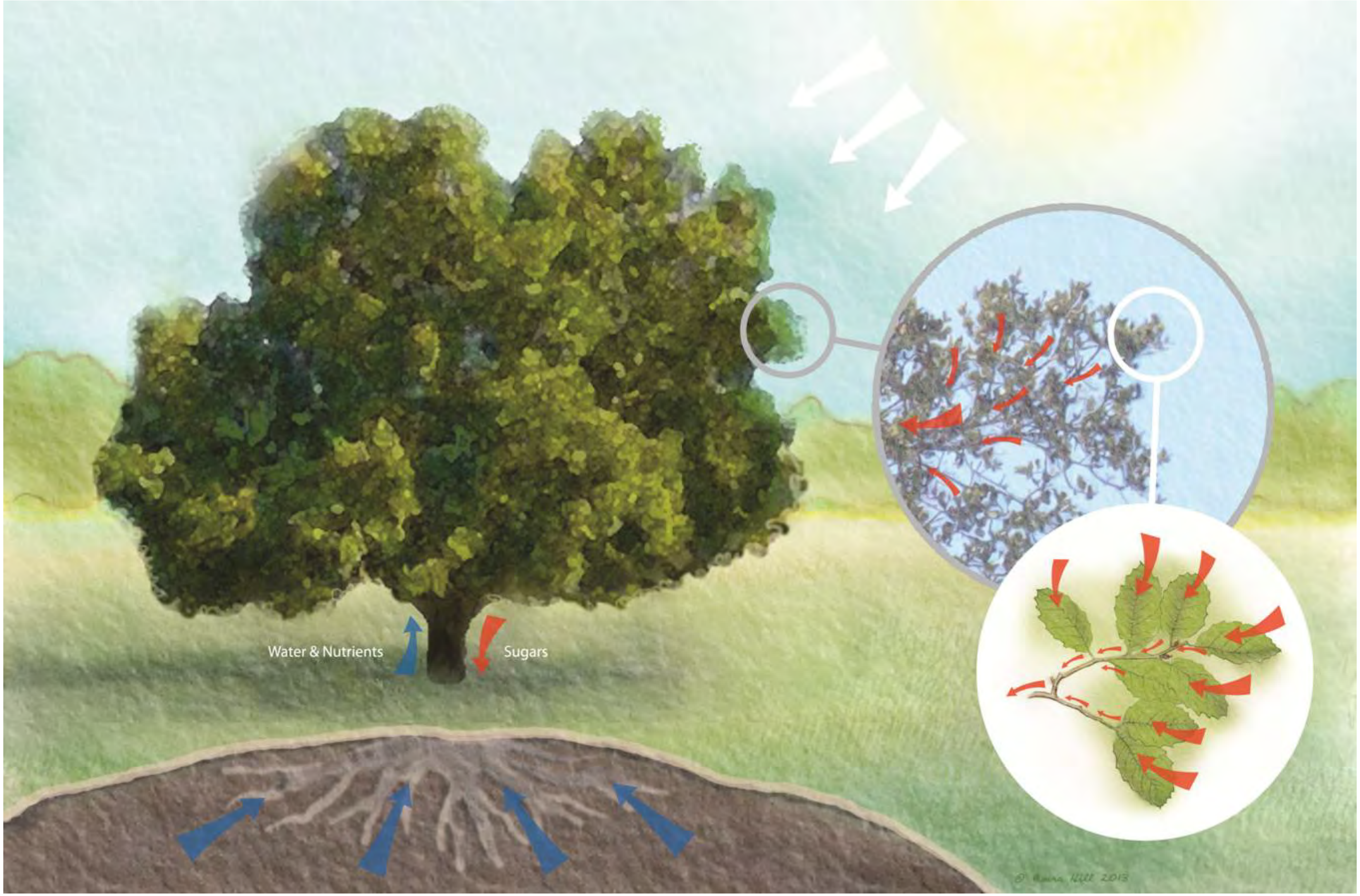
Integrator function seeks additional candidate data sources by affinities.

Builds more refined causal models. Accelerate Learning through Affinities

Publish / Subscribe for the IoT

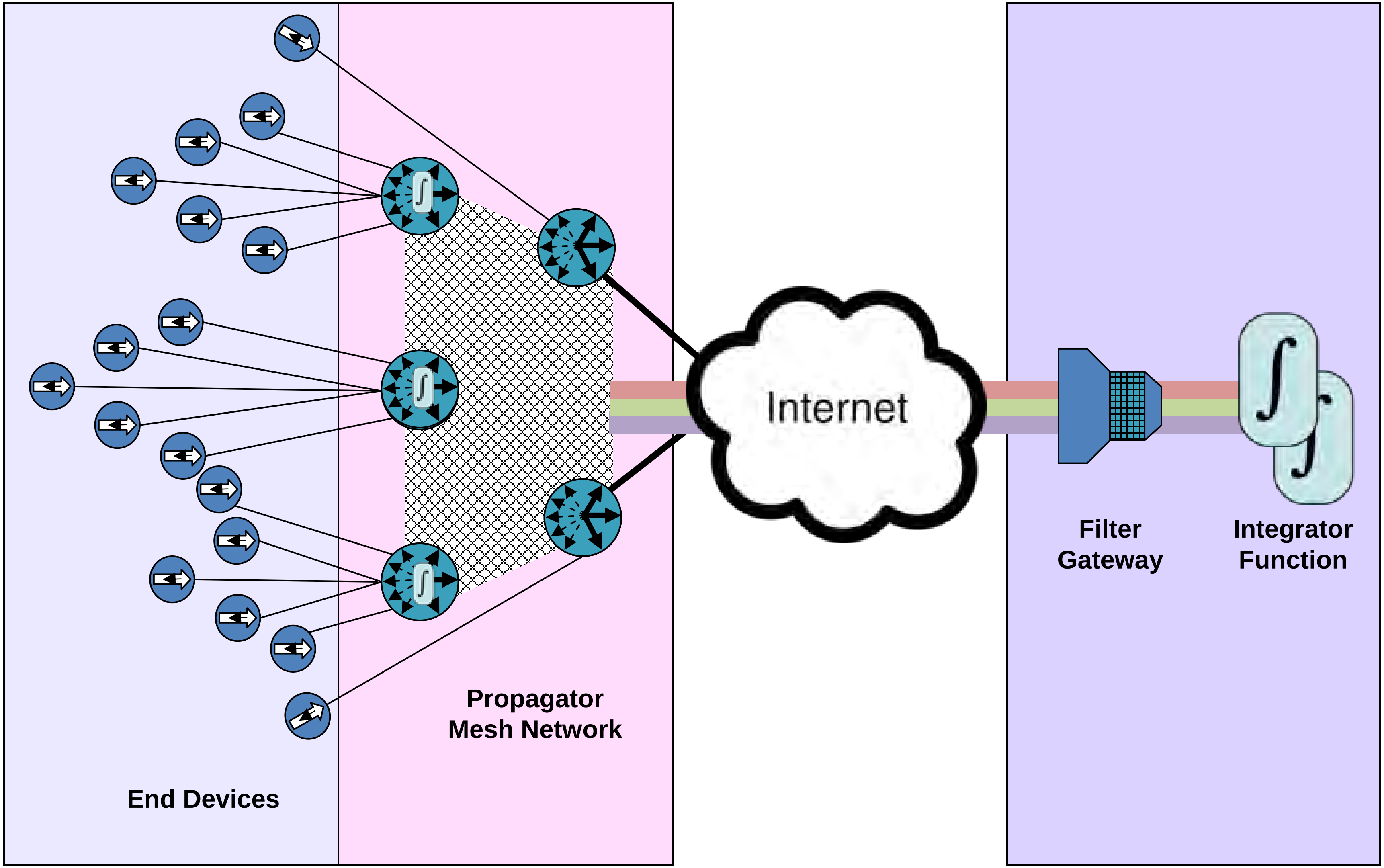
- Discovery: Many useful data sources may be unknown.
  - Self-classification ("Pressure sensor", "irrigation valve", "Flow Sensor" etc.) permits discovery of data "<u>affinities</u>**"**
  - Open Source top-level taxonomy crucial to scale and discovery
- Subscriber Based: Small data flows may be discovered, selected, and incorporated by Integrator Functions
- Dynamic: New flows may be added and existing sources aged-out over time
- Primarily for *Local* Consumption at Edge: "Small" data.

Scalability Lesson from Nature: Trees



End devices don't communicate with one another, so "tree" better than "web"

Emerging IoT Architecture

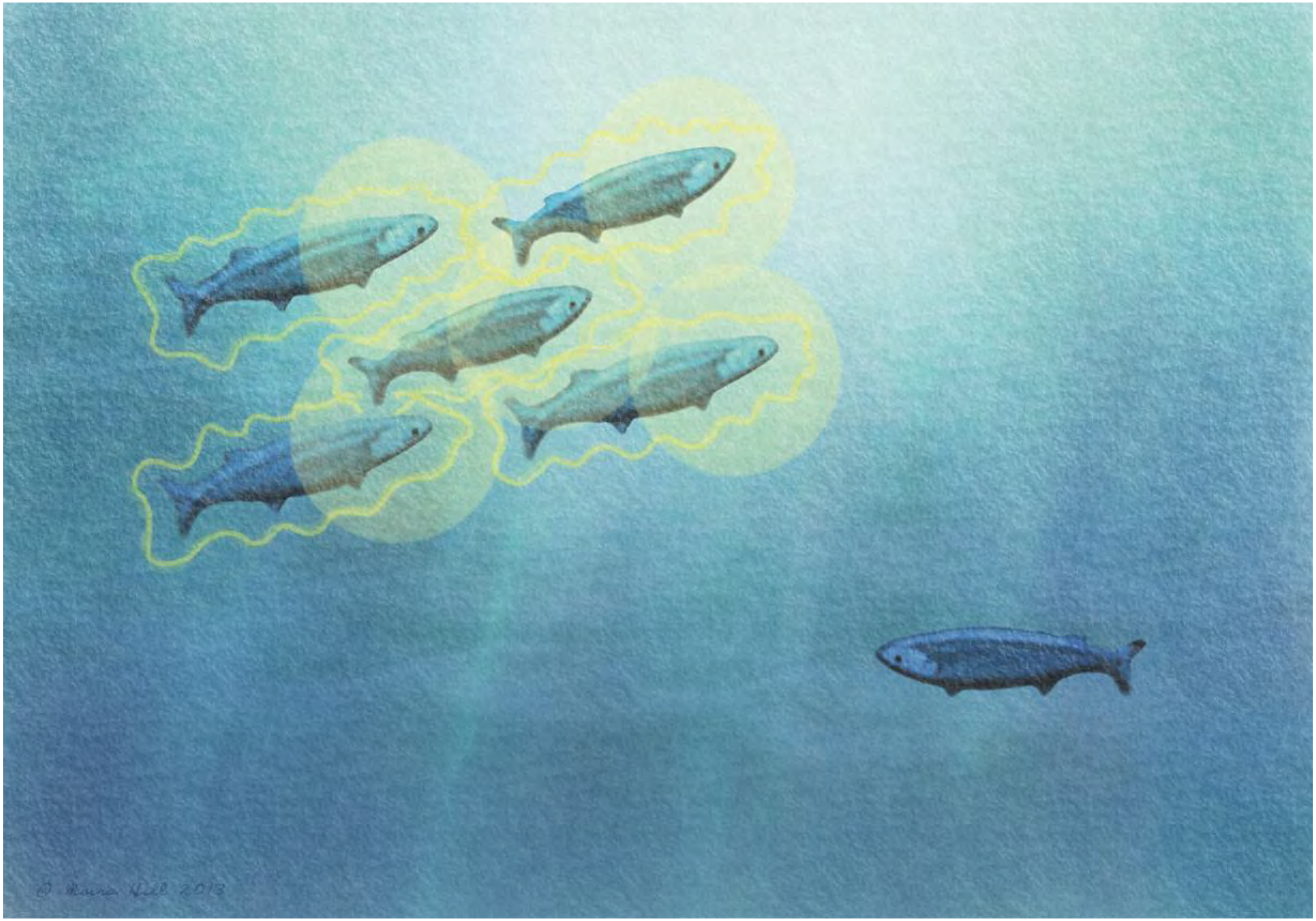


Chirp Data Streams **“Small” Data Flows** **“Big Data” Analysis**

Scalability of IoT Architecture

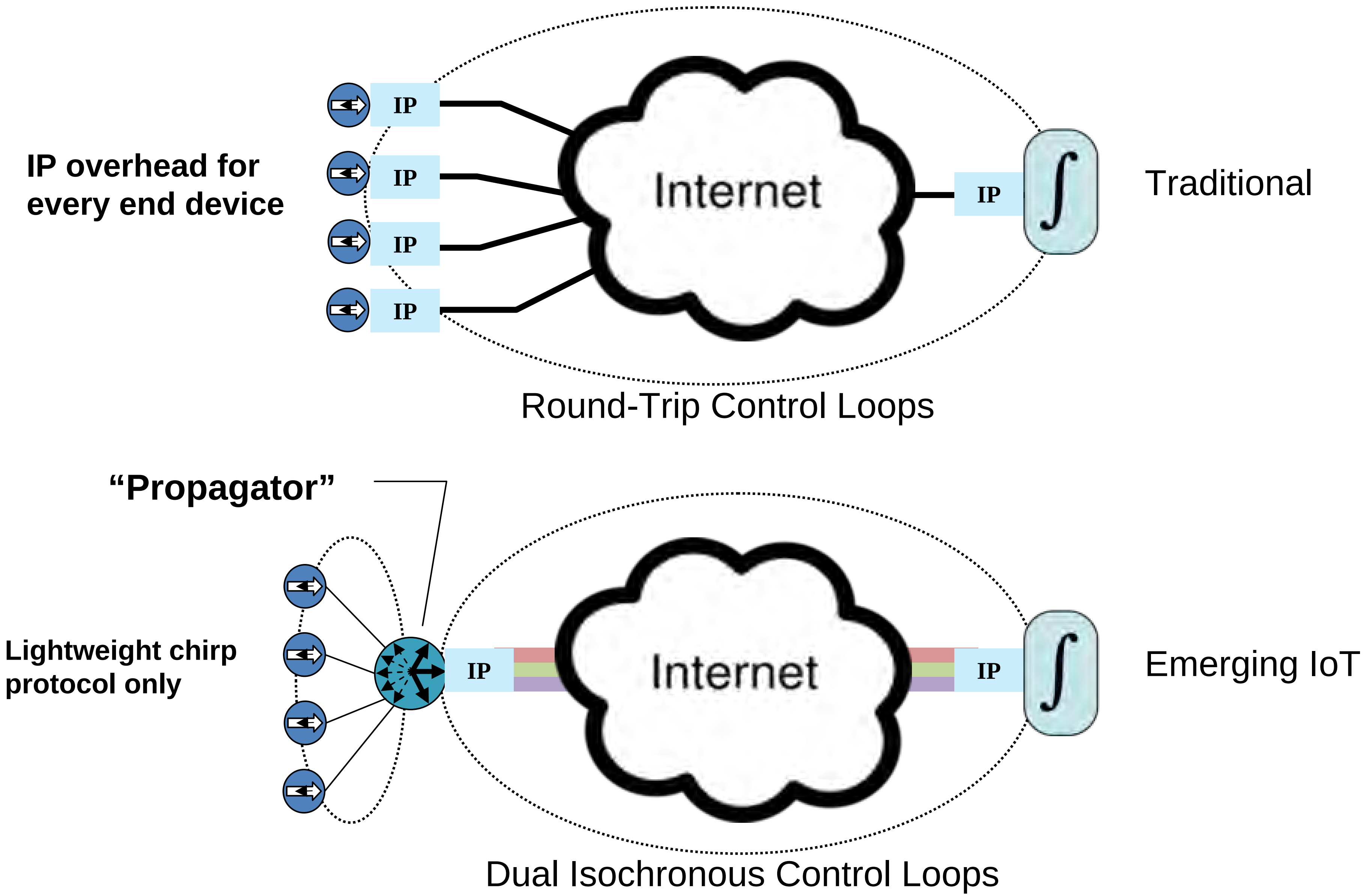
- End Devices can be cheap, simple, low power, unmanaged
- Protocol sophistication only in Propagator Nodes
- Prune and trim broadcasts – building “buses”
- Optional distributed intelligent agents in Propagator Nodes
  - Extend subscription preferences of Integrator Functions
  - Add security and proprietary functions
  - Extends “Software Defined Network” publish/ subscribe functionality to edge of network

Lesson from Nature: *Local* Autonomy



Devices operate independently, but may act in concert with external “cues”

Managing *Local* Autonomy



Importance of Open Source

- Basic Chirp self-classification taxonomy will be (and must be) Open Source for broad dissemination
  - Some number of top-level classifications
  - Sensors, appliances, actuators, etc.
- Working groups and SIGs may refine sub-classifications
  - Most also open to public for non-local consumers
- Enterprises and OEMs may develop custom and proprietary extensions for Private fields
- Open Source networking implementations (OpenWrt, et al) to accelerate large scale deployment

Even "Closed" Flows Will Offer Open Source Information

- Specifics of data stream may be private, but "affinities" are still observable
  - Information about number, location, and activity of devices (and much more)
  - Adds information to Open Source Taxonomy
- Analogous to CAPTCHA™ environment

- Every additional end device potentially adds to Open Source knowledge base

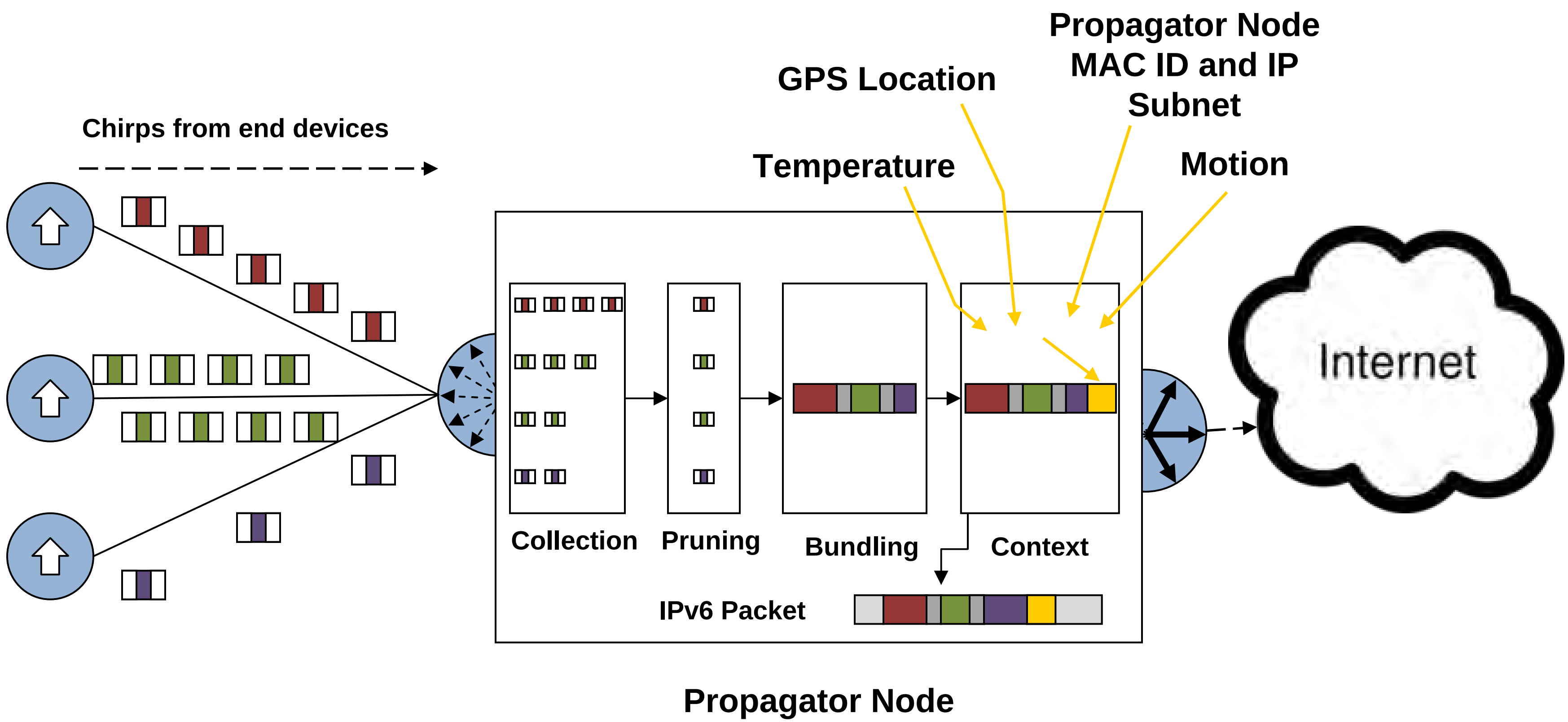
Internet of Things can only Happen through Open Source

- Too big, too much data, too unmanageable
- Lessons from nature
  - Only publish /discover / subscribe can scale
  - Self-classified data needed so receivers may select
- Open Source taxonomy
- Rapid proliferation of Propagator Nodes Functionality

- Chirp Networks is developing prototype for military.
  - Leverages Open Source (OpenWRT, MAC802.11)

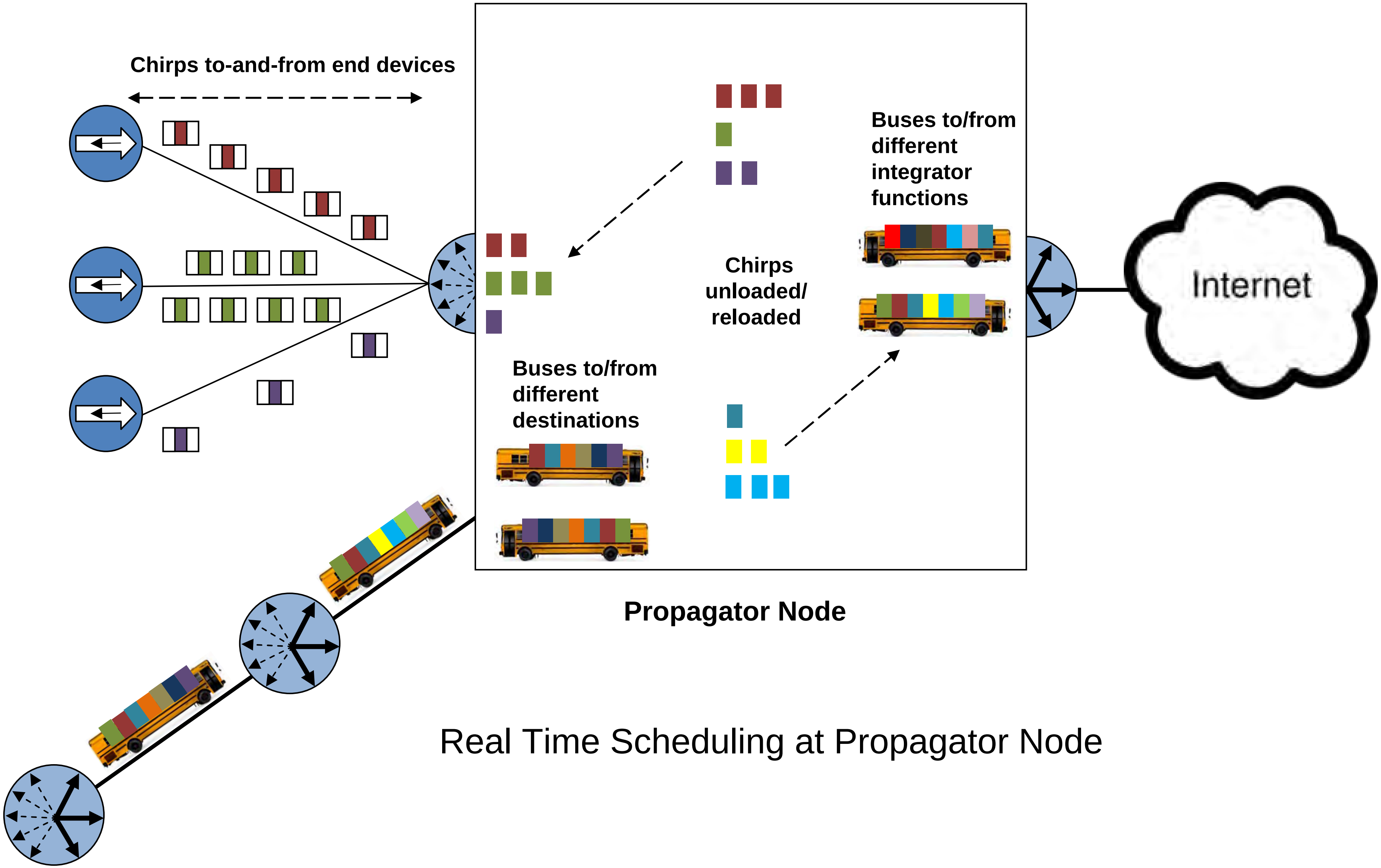
Support Slides

Scalability: Managing Broadcasts, Distribution, Addressing



Propagator Nodes create "Small Data" flows from Chirp data streams

Scalability: Loading "Buses"



Real Time Scheduling at Propagator Node

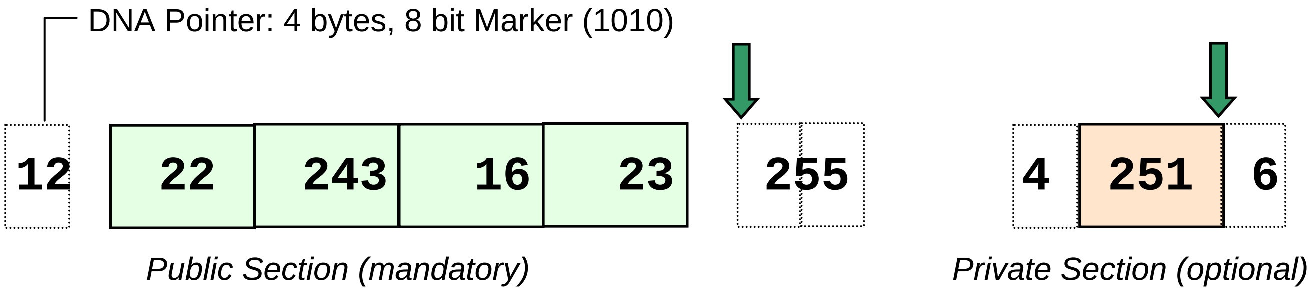
Propagator Nodes –Networking Capabilities

- Developed on Open Source platform: OpenWrt, et al
- Build structured trees among themselves
  - Path discovery, routing, redundancy, fail-over
  - Simplicity through “near-optimal” routing
- Manage multicast: pruning, forwarding, spoofing, etc.
- Optional integrated Publishing Agents participate in publish/subscribe bus, machine learning
- Offer wide variety of end device interfaces: wired, wireless, optical, etc.

Security Must be Incremental to Open Source Format

- Basic Chirp published and open to all
  - As in nature's pheromones, pollen and birdsong
- Private fields within Chirp may create "lock-and-key" relationship in OEM and proprietary applications
  - As in pollen – *receiver* determines
- Further security achieved through distributed agents in Propagator Nodes
- Secure data may still flow through Propagator Node network with open data, but is unintelligible
  - From nature: air transports both *proprietary* (e.g., pollen) and *open* "signals" (e.g., pheromones)

Security Must be Incremental



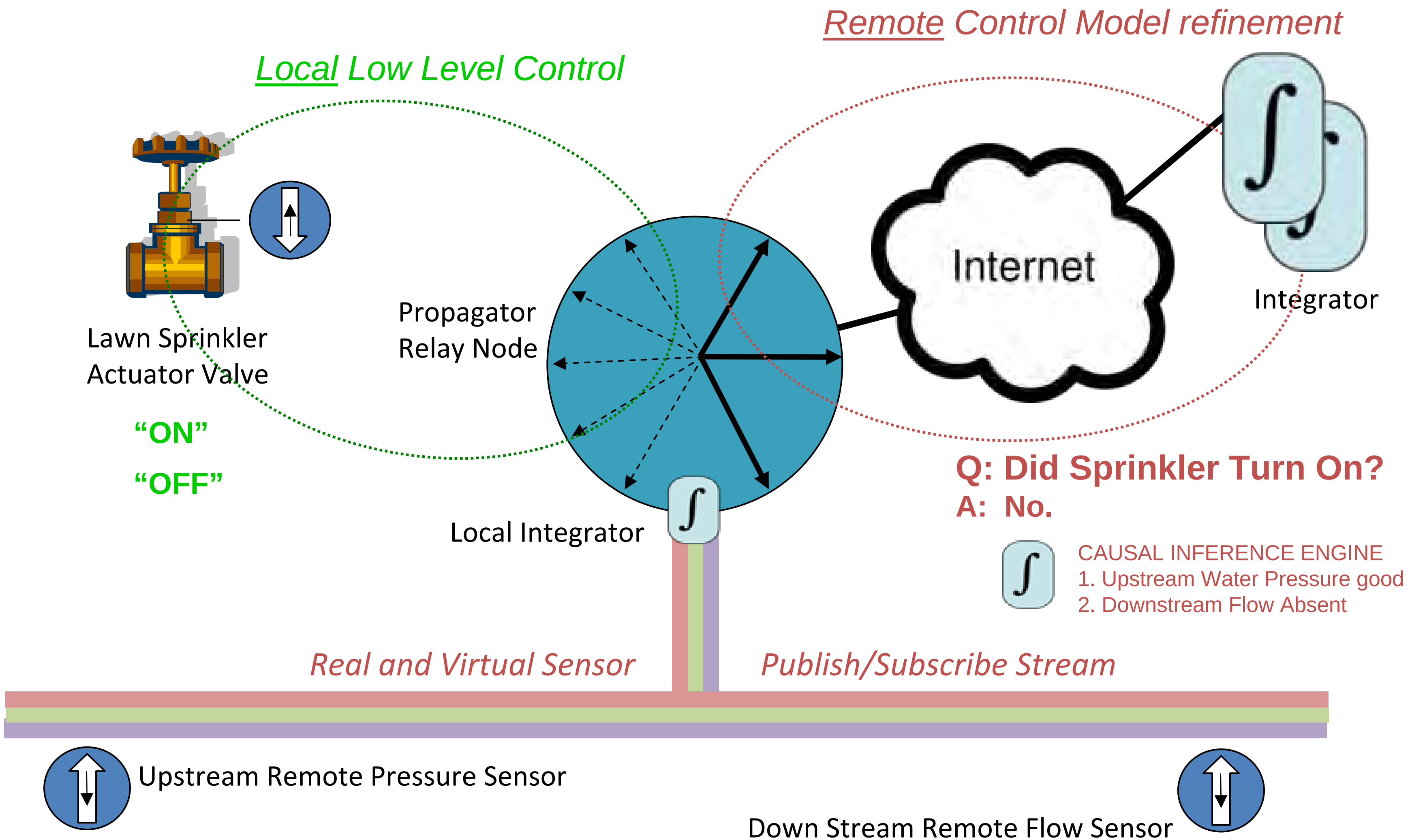
Public Agent ID is 4.8.255 (4 byte Public, 8 bit Marker, DNA 255
(Subscribed) Agent states: Classification is 8.8.8.8 (1 byte each)
Decrypted Chirp Class: 4.8.22.243.16.23.

Its payload requires another Agent
Private Agent 1.4.6 (specific for 4.8.22.243.16.23) decodes (251)

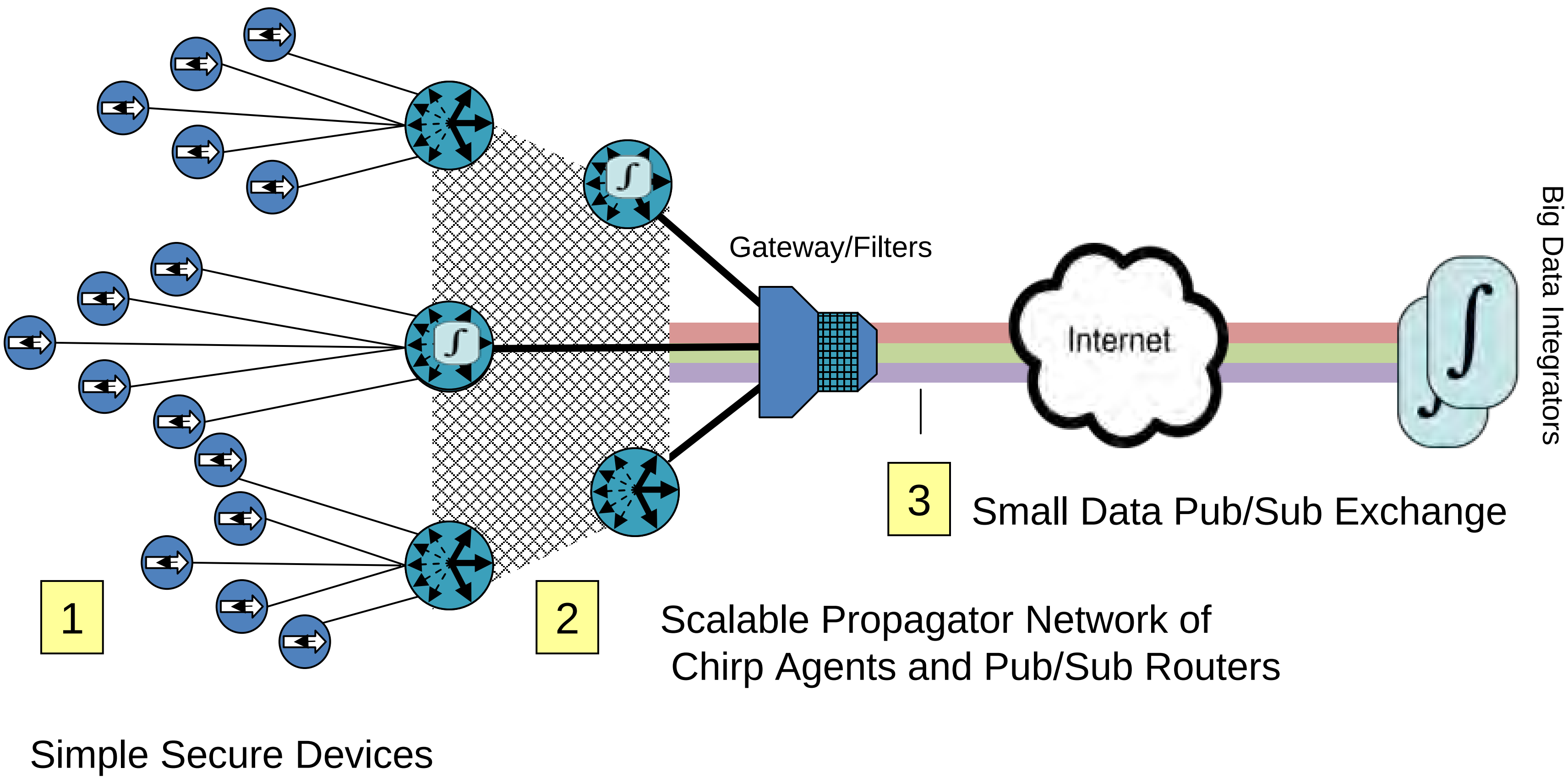
Chirp with public (open) payloads have shorter classifications
e.g. Chirp Class 4.8.22: Temp=243F Pressure=16psi Humidity=23%.

Larger Packets intended for slower transport.
Enterprises may define their (internal) classification schemes.
Discovery of “unknown” chirp classes detected, addressed in SIGs.
Distributed, organic growth of chirp classification taxonomy.

Local and Remote Control Loops



Chirp Networks: *Scalable* Publish/Subscribe for the Edge



<u>Chirp Networks are</u>

- *Scalable* with Moore's Law (linear)
- *Secure:* Chirp to IP bridging is through distributed agent network
- *Dynamic*: Supports Temporal M2M communities through logical mesh
- *Reliable*: Deterministic Latency and Jitter through tree based topology
- *Practical:* Economies of Scale favor moving M2M overhead to Propagators