Chirp Primer (On the Cloud Orchestration Model)

Fig. 1. Challenges to "Massive IoT" : low energy, complexity, copious use.

The Rationale behind Small Dumb Cheap Copious

Over the next decade, billions of IoT devices will be monitoring farms, forests, oceans, and other (non-urban) natural resources with sparse and intermittent cloud connectivity.

As Edge IIoT becomes semi-autonomous, intermittent connectivity is both sufficient and ubiquitous.

Software Defined Mesh™ then drives a Cloud driven thinking where simple Edge devices are periodically imprinted to transmit or relay data on cloud managed schedules.

MAC based wireless protocols are sender oriented, extensions of protocols intended for (verbose) humans. In sharp contract Nature's "Massive" messaging is cryptic, receiver-oriented and self-classifying. Bird chirps are short (low power) and while distinguishable (routable) are undecipherable to most. Innately secure.

Digital Chirp Protocols minimize energy by shifting radio intelligence to the receiver end - ubiquitously available carrier pigeons - phones, drones, routers. These all run the full OSI stack, Fig. 2. Pigeons do the heavy lifting to route to Hosted IoT Services, Fig. 4, 5. More

Chirpers™, now, by contrast, Fig. 3, use only primitive -and legacy supported- wireless modems.

The battery lives on remote devices are extended by decades. The cost of edge radio hardware plummets.

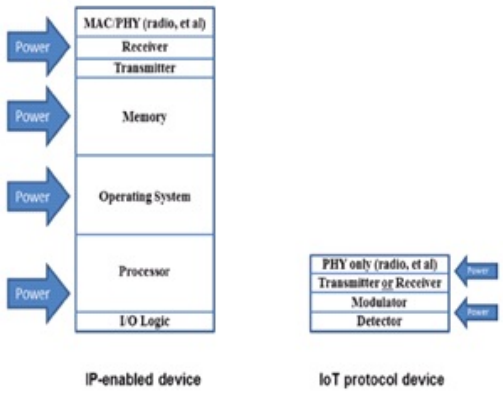

Figure 1-5. Contrasting the processor, OS, memory, and power necessary for traditional protocols vs. the IoT protocol

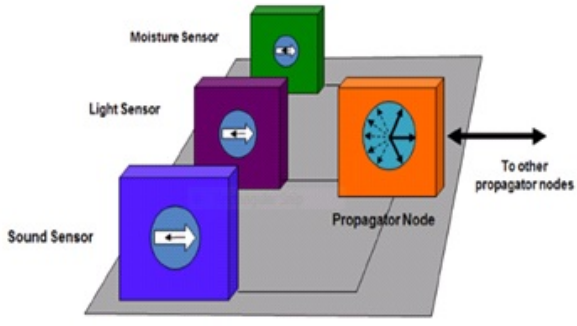

Figure 6-1. Combinations of different sensor types within one physical package, each generating uniquely marked chirp packets, are just one example of the benefits of self-classified chirp protocols. In this example, an on-board propagator node could efficiently combine the chirp streams into "busloads" of small data for interpretation by one or more integrator functions

Fig. 2, left. Chirpers don't need the full OSI stack -> minimizing power and cost
Fig. 3, right. Exemplary Chirper: sensors + ant-like logic + wireless serial modem

Inverted Cloud -> Edge Thinking

The challenges in Fig. 1 are exacerbated for currently un-connected Legacy machines. Consider:

1. RFID++™ Active Tags -like OCR labels - may be stuck on remote assets for actionable intelligence.
2. Car, Phone, Trucks and drones services serve as Edge chirp harvesters and propagators - Globally.

Edge->Cloud thinking then shifts to a more sustainable, scalable, secure **Cloud->Edge thinking**:

1. Cloud Orchestrator -> Trusted Pigeon -> Imprints Chirp with new Logic, Schedules.
2. Chirper -> Runs Logic -> dumb wireless modems -> Receiver Radios on Phones, Drones etc.
3. Receivers harvest Chirps -> Add tagging -> Pub/Sub messaging -> Cloud Subscribers.
4. Chirpers with Ant-like imprinted logic run on billions of chipsets -> "Massive IoT".

Key Takeaways when thinking shifts from Edge->Cloud to Cloud Orchestrated Flows:

A. Global-Scale "Edge" challenges are: simplicity, cost, energy & (as always) security.
B. Chirpers don't need heavy OSI stack -> minimal power and cost for connectivity.
C. Software Defined Networking for the Edge -> Moves Chirping Intelligence to Cloud.
D. Trusted walled gardens become globally relevant through our imprinted chipsets.
E. Massive IIoT - with no legacy systems left behind - burgeons.

Cloud Birthed Imprinting and Orchestration

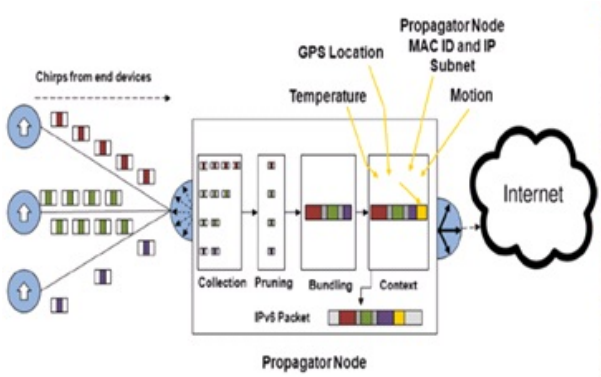

Figure 2-9. As chirps are bundled within propagator nodes, additional location, addressing, protocol, and other information is added

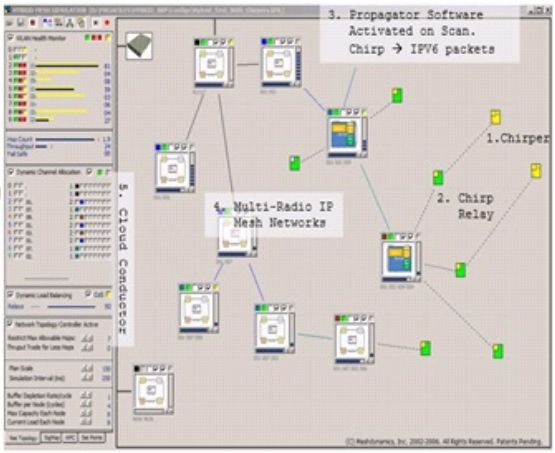

Fig.4 Left: Apps on receiver phones/drones Prune, Tag and Bundle Chirps for the Cloud.
Fig.5 Right: Cloud Orchestrator imprints chirpers/relays through heartbeats. Enlarge.

Shifting radio intelligence to the receiver and cloud is functionally equivalent to CSMA/CA and DCF for minimal power Edge. Human driven RF chatter required smarts in phones operating in congested, dynamic RF and this drove BLE etc. devices to use MAC based protocols. In non-urban spaces, RF patterns were learnt, predicted and drove schedules and channels. (For more please see: Evolutionary Mesh Networks)

Imprinting. Chirp products are imprinted – establishing provenance to "Mother". On power up chirp devices first scan/listen for "Mother" on private channels and cryptic protocols. Receiver radios on phones or drones respond and imprint the devices. If RF interference occurs, the cloud directs them to other channels or schedules - teaches them new tricks.

Scheduling. Control systems need timely inputs from the field – this is back scheduled from when carrier pigeons arrive, the size of the data logs to be stored etc. The entire data logistics supply chain is visible and used to imprints both sensors and pigeons. The Enterprise tunes it to avoid RF interference by changing channels and schedules.

Discovery. Digital version of Bird Call registries will empower discovery of hidden corroborating intelligence. Symbiotic signaling - as in Nature - is currently lost. More.

MAC-Less Protocols Chirp packets use locally unique addressing - a byte suffices to distinguish 255 chirp species operating at the same time and RF channels. Compare to IP headers of 40+ bytes.

Standards. Nature's Massive IoT grew organically, managing collision domains in time and region by evolved differentiated "tunes". The Chirp protocol does not need standards bodies - for these reasons.

Deployment Costs. The cost of 2.4GHz BLE radio is around a dollar. Wireless modems are 15 cents. MAC based radios use 45 bytes to transport a 4 byte data packet. Chirpers do it in 5 bytes with one byte for the core tagging. Next, CSMA/CA are inefficient compared to scheduled broadcasts. Coin batteries now last decades.

Global Relevance. Chirp Networks™ are device level authenticated. They are logically contiguous - over previously walled garden boundaries. Thus Chirps picked up by a receiver Apple Phone (with USB Modem) is propagated via Amazon trucks - because these devices have been opted in by federated hosted services.

Cloud->Edge thinking drives a new look at Global Scale Edge Connectivity. Simple Devices Speaking Simply.

Globally Relevant Use Cases

Shifting Radio Intelligence out of the Edge then burgeons a new breed of legacy supported IIoT messaging. Topic based addressing feeds directly into Enterprise Pub/Sub.

Example: The challenges in Fig. 1 are exacerbated for currently un-connected Legacy machines, a large market. RFID++™ Active Tags -like OCR labels - may be stuck on remote assets for actionable intelligence. Sensors on it monitor vibration, sound, temperature. Per imprinted directives, logs are made and picked up and analyzed by cloud services. Edge Sensor -> Data Logs -> Pigeons -> Tagging and Routing -> Cloud.

Chirpers are intelligently scheduled and imprinted to activate sensors per PaaS services. Today, drones are commonly used in remote or de-militarized zones. All delivery trucks are potentially carrier pigeons.

Small dumb cheap copious sensors address climate preparedness and edge asset tracking at Global Scale.

Lifetime service support for Legacy IIoT Edge alone - with a non intrusive sensor "Patch" - drives new business models where Chirper logs is integrated to drive new efficiencies in Edge Asset management.

Summary

The confluence of AI + SDN has prompted this shift to the Cloud Orchestration Model. Chirp enabled assets are imprinted by their owners directly. Chirpers coalesce to be logically contiguous across previously walled garden boundaries - this engenders Massive IoT.

1. Today: Edge with BLE, Zigbee, Lora => Fractured Markets and Silos => **Not** Massive.
2. Chirp: Imprinted Edge => Intermittent Pigeons => Contiguous Clouds => Massive.

Thank you for your time. All feedback is appreciated. LinkedIn

About the Author

The emerging Internet of Things architecture and wireless mesh networking technology has been influenced by the Robotics and Machine Control background of founder Francis daCosta. In 1992 Francis founded Advanced Cybernetics Group contracted to provide semi-autonomous control architectures and protocols for military use. In 2002, Meshdynamics was formed to focus on last mile MeshControl™ and mobile, stealth mode intrusion detection applications. In 2012, Intel sponsored Rethinking the Internet of Things, based on his blogs.

His 1982-2022 journey has been a confluence of overlapping interests in Edge and Cloud.

1982-2002 Robots > +Sensors > +Tele-robotics > +Automatic Task Level Programming
2002-2012 Time Sensitive Networks for remote machines (last mile, mesh networks)
2012-2022 Re-thinking the Internet of things, Proving Cloud Orchestration models

Addendum: Introduction, "Rethinking the Internet of Things", Intel Press, 2013.

I didn't set out to develop a new architecture for the Internet of Things (IoT). Rather, I was thinking about the implications of control and scheduling within machine social networks in the context of Metcalfe's Law. The coming tsunami of machine-to-machine interconnections could yield tremendous flows of information – and knowledge.

Once we free machine social networks (comprised of sensors and other devices) from the drag of human interaction, there is tremendous potential for creating autonomous communities of machines that require occasional interaction or reporting to humans.

The conventional wisdom is that the expansive address space of IPv6 solves the IoT problem of myriad end devices. But the host-to-host assumptions fossilized into the IP protocol in the 1970s fundamentally limited its utility for the very edge of the IoT network.

As the Internet of Things expands exponentially over the coming years, it will be expected to connect to devices that are cheaper, dumber, and more diverse. Traditional networking thinking will fail for multiple reasons.

First, although IPv6 provides an address for these devices, the largest population of these appliances, sensors, and actuators will lack the horsepower in terms of processors, memory, and bandwidth to run the bloated IP protocol stack. It simply does not make financial sense to

burden a simple sensor with the protocol overhead needed for host-to-host communications.

Second, the conventional implementation of IP protocols implies networking knowledge on the part of device manufacturers: without centrally authorized MAC IDs and end-to-end management, IP falls flat. Many of the hundreds of thousands of manufacturers, building moisture sensors, streetlights lack the expertise to implement legacy network technology in traditional ways.

Third, the data needs of the IoT are completely different from the global Internet. Most of the communications will be terse machine-to-machine interchanges that are largely asymmetrical, with much more data flowing in one direction (sensor to server, for example) than in the other. And in most cases, losing an individual message to an intermittent or noisy connection will be no big deal. Unlike the traditional Internet, which is primarily human-oriented (and thus averse to data loss), much of the Internet of Things traffic will be analyzed over time, not acted upon immediately. Most of the end devices will be essentially autonomous, operating independently whether anyone is "listening" or not.

Fourth, when there are real-time sensing and response loops needed in the Internet of Things, traditional network architectures with their round-trip control loops will be problematic. Instead, a way would be needed to engender independent local control loops managing the "business" of appliances, sensors, and actuators while still permitting occasional "advise and consent" communications with central servers.

Finally, and most importantly, traditional IP peer-to-peer relationships lock out much of the potential richness of the Internet of Things. There will be vast streams of data flowing, many of which are unknown or unplanned. Only a publish/subscribe architecture allows us to tap into this knowledge by discovering interesting data flows and relationships. And only a publish/subscribe network can scale to the tremendous size of the coming Internet of Things.

The only systems on earth that have ever scaled to the size and scope of the Internet things are natural systems: pollen distribution, ant colonies, redwoods, and so on.

From examining these natural systems, I developed the three-tiered IoT architecture described in this book: simple end devices; networking specialist propagator nodes, and information-seeking integrator functions.

In these pages, I'll explain why terse, self-classified messages, networking overhead isolated to a specialized tier of devices, and publish subscribe relationships formed are the only way to fully distill the power of the coming Internet of Things.

Francis daCosta LinkedIn
Santa Clara, California, 2013

Chirp Landing Page Chirp One Pager *Chirp Primer* Chirp Primer Slides