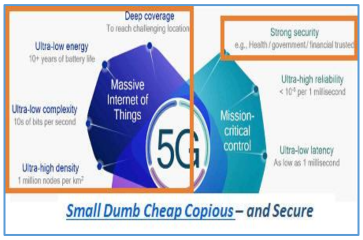
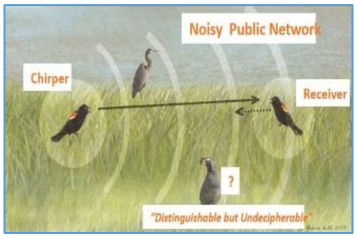
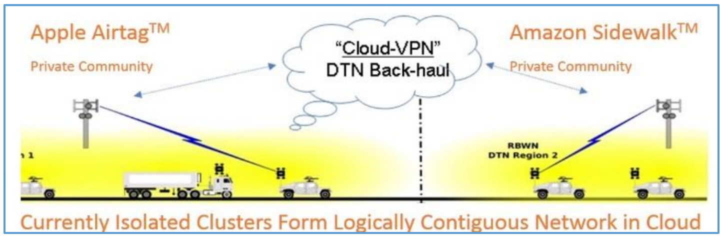
0. Table of Contents and Comments

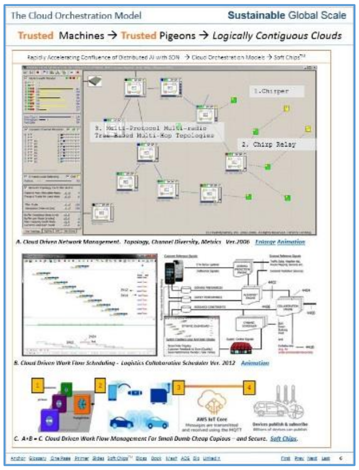
Thumb nails.

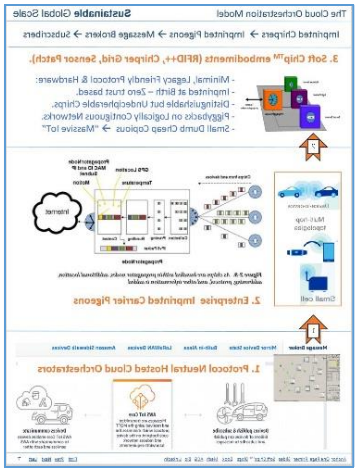
Of Salient Figures to proposal and conjectures. Click for more

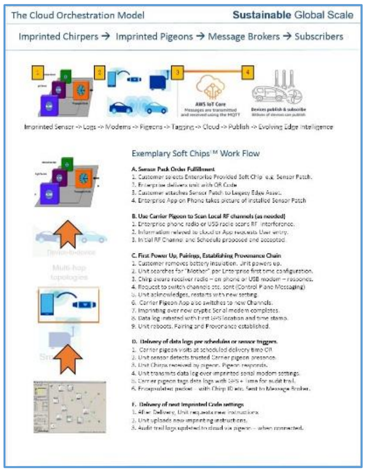


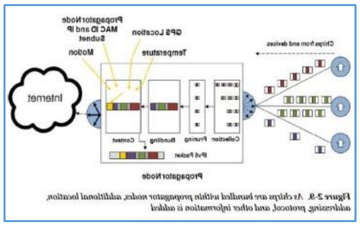





The Cloud Orchestration Model
Sustainable Global Scale
Trusted Machines → Trusted Pigeons → Logically Contiguous Clouds
1. Chirper
2. Chirp Relay
A. Cloud Driven Network Management. Topology, Channel Diversity, Metrics
B. Cloud Driven Work Flow Scheduling – Logistics Collaborative Schedules
C. A+B = C. Cloud Driven Work Flow Management For Small Dumb Cheap Copious – and Secure.




The Cloud Orchestration Model
Sustainable Global Scale
Imprinted Chirpers → Imprinted Pigeons → Message Brokers → Subscribers
AWS IoT Core
Exemplary Soft Chips™ Work Flow



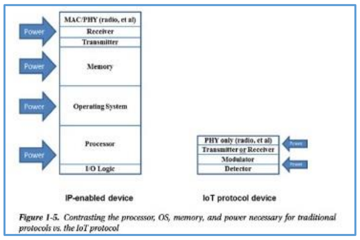
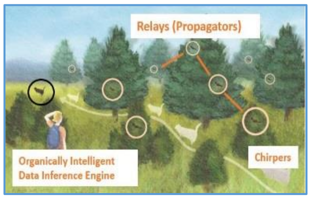
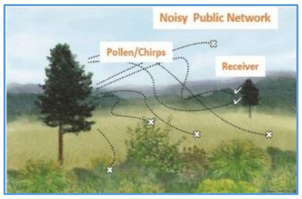
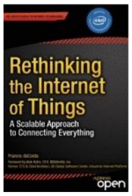


Figure 1-5. Contrasting the processor, OS, memory, and power necessary for traditional protocols vs. the IoT protocol

1
2
3
4
AWS IoT Core
Messages are transmitted and received using the MQTT
Devices publish & subscribe
Billions of devices can publish






Rethinking the Internet of Things
A Scalable Approach to Connecting Everything
open

■ 1. GLOSSARY

Excerpts from Web Glossary (for Offline Viewing)

Carrier Pigeons, **Pigeons**, **Propagators**. The packet transport from rudimentary edge protocol to cloud. RFID readers encapsulates the raw signals into a useful format. Similarly Pigeons, over a rudimentary - and legacy supported - serial modem, take in Chirp packets, tag and prune them and put them on a shuttle bus to interested subscribers. Illustration.

Chirps. Taking cues from Nature, (digital) Chirps are terse, cryptic receiver oriented messaging. Birds chirp - and while we can distinguish species of birds we do not understand the meaning. Distinguishable yet Undecipherable. Innately secure. Combined with imprinting at birth, this ensures end-to-end security. Chirp Devices **-** 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. Imprints provide an end-to-end trusted Topic based addressing system – see Pub/Sub. .

Cloud Orchestration. See Illustration, The Cloud manages collision avoidance proactively by:

- RF channel diversity and network topology management - as in scalable O(nLogn) tree structures. More
- Cloud application awareness - when data from the edge is needed - time window of relevance. More
- Addressing conflicting objectives or RF interference by re-imprinting RF channel and schedules. More

Cloud >Edge Thinking .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. See Evolutionary Mesh Networks.

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

Edge. Low power consumption IoT devices in remote, harsh, hostile or under-developed regions that:

- Need minimal power usage - use terse protocols and infrequent data log deliveries
- No one single piece of sampled data is critical - delivery that don't sometimes happen is OK.
- Regions serviced are remote - carrier pigeons visit infrequently and schedules may slip.
- Data logs delivered on a best efforts intermittent connectivity basis and it suffices.
- The primitive Ant-like intelligence is reprogrammable by Cloud agents – the carrier pigeons.

Edge->Cloud thinking. Last mile connectivity is challenging in logistic supply chains because pick up and delivery are predicated on available bulk transport (planes, trucks, ships) and distribution from hubs. As a result IoT radios use congested and short range BLE. Phones - Ubiquitous Pigeons - support it. The cost is "heavier" hardware and power usage. This is edge to cloud thinking and is not sustainable.

Imprinting. Right after birth, a bird is imprinted and thus learns cues that differentiate friend (mother) from foe (predator). It is fundamental to their survival. Next, birds of a feather flock together - form trusted private communities. While everyone hears their chirp, it is cryptic and only they know the full meaning of what is being said. Illustration. Distinguishable - for routing - but Undecipherable. Imprinting establishes **Provenance.** No third party pre-assigned ID (RFID, MAC) needed. Enterprise defines the topic headers that it needs to have the topic based addressing scheme to deliver where requested.

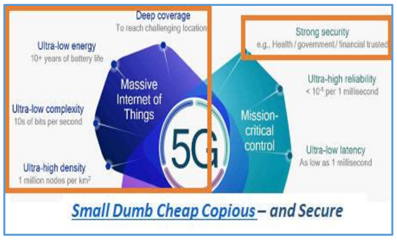
Provenance. Chirp products are imprinted – establishing provenance to "Mother". On power up chirp devices first scan/listen for "Mother" on private channels and cryptic protocols. Receiver radios inside phones or USB attached respond, then imprint devices. If RF or schedule interference occurs, the cloud directs them to other channels or schedules - teaches them new tricks. Imprints provide an end-to-end trusted system. Establishing **provenance** of sourced materials - which tree in which forest - has to come from imprinted tags that follow the tree from the forest to the lumber yard and onwards to Consumer. Provenance chains kick in when the tree is first felled - **go back to birth.**

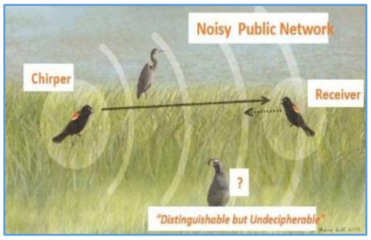
Security. Chirp protocols are receiver oriented. Cloud driven scheduling provides dynamic collision avoidance in both time and RF channels. Thus both the USB powered receiver radio pigeon unit and the chirpers have to know both when, where or how to chirp- both being imprinted by trusted hosted PaaS. Additionally, Chirpers don't use MAC ID or other third party UUID Identification. See MAC spoofing and Man in the Middle Attack for reasons why. Instead, Chirpers provide a minimal Chirp-ID - the species ID. Carrier Pigeons fill in authenticated tagging - GPS location, timestamps and route the IPV6 packet. The Chirp-ID may be generated by the cloud based on the deployed environment. If less than 255 unique species are operating at the same schedules and RF channels ranges - Co-location in time and RF space - then 1 byte suffices as a Chirp-ID. Soft Chips Work Flows and Cloud Orchestration Models leverage cloud intelligence.

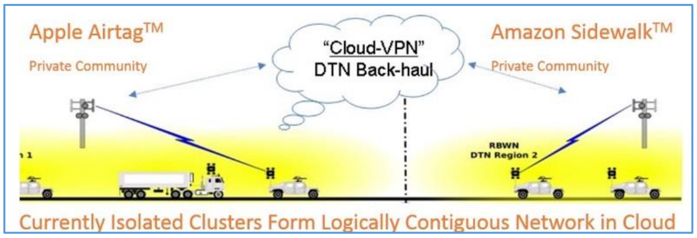
Soft Chips. Chirp protocols are generic and intentionally rudimentary. However simple ant-like edge intelligence is easily imprinted to provide When-this-then-that and If-when-this-then-that processes. Soft Chips are a set of sensors that can be activated by imprinted code to perform specific tasks e.g. make data logs, relay "fire!" alerts. The chipsets may be made in millions because they support multiple use cases.

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**.

■ 2. EXECUTIVE SUMMARY







Left: Challenges to massive IoT deployments are: simplicity, cost, energy, and security Enlarge

Center: Nature's messaging is receiver oriented. Distinguishable yet Undecipherable to others. Enlarge

Right: Previously walled gardens may extend their reach through messaging at the Cloud Level. Enlarge

Note: Links in **bold** define terms differently to be able to describe a new **Cloud->Edge Thinking**. Related: Glossary .

Over the next several decades, billions of IoT devices will need to be monitoring assets of interest (hardware, infrastructure, farms,…) as well as natural resources (forests, water, mines, extraction fields, etc.) frequently in remote locations with little to no access to power and only sparse or intermittent internet connectivity.

Today's IoT approach utilize the IPV6 and MAC based protocols. However, this "heavy" approach requires more processing power at the radio end – adversely affecting cost and scalability. We propose here an alternative approach based on nature's strategies for transmitting information. The IPV6 protocol is sender-oriented and heavy – 40 bytes for the header alone. In sharp contrast, Nature's messaging is light, **receiver-oriented,** and innately secure.

The **lightness and elegance of pollen** is it can piggyback on all available transports such as wind, insects, and animals. Pollen is receiver oriented and innately secure: only intended recipient species of flower can decode the "message". Taking cues from Nature we propose an approach using terse "chirp" communications with 1-2 byte topic headers that can piggyback on global, untrusted networks and with messages understood only by intended parties. The carrier pigeons use the topic headers to route the chirp packets (header and payload) to intended cloud subscribers. We can now enable massive IoT even in areas with little to no infrastructure. Our combination of hardware and software in the chipsets creates secure trust communications that can operate in regions with intermittent connectivity or can utilize current and future walled-garden "networks."

This approach shifts away from "heavy" Edge -> Cloud solutions. Instead, it brings to bear lessons learnt in our deployments of Cloud managed Global Scale **mesh military networks** and the supervision of **Edge** devices in remote, harsh, hostile regions:

1. Edge devices (chirpers) don't need IPV6 heavy OSI stack -> minimal power and cost (cents vs dollars)
2. Massive edge deployments without the MAC constraints of IPV6 – low cost and long life deployments
3. Software Defined networking at Edge -> Moves Chirping Intelligence to Cloud – Economies of Scale, Secure.
4. "**Imprinted**" chipsets enable use of untrusted networks or across walled gardens – Reprogrammable, Multi-use.

Some aspects of this proposal have been previously demonstrated. "Chirps" were developed for SPAWAR for stealth terse (1-2 bytes) messaging across untrusted networks. Sharp Corp. licensed the intellectual property and software for dual use deployments in Japan and Southeast Asia. The key features of Cloud Orchestrated Model described later are:

. *Agnostic*.	Chirps are radio & protocol agnostic. May use multiple transports and networks.
. *Low power consumption*.	Ultra-Low wireless usage leads to low power/long battery life
. *Dumb, Cheap Devices.*	Ant-like purpose driven capabilities Re-programmable, multi-purpose.
. *Copious*.	Can now be copiously spread for Early Warning Systems: e.g. Forest Fires
. *No central standards needed*.	Chirp protocol easily extensible by Enterprise.
. *Flexible Collaborations*.	Walled gardens can share messaging from their devices with others.
. *Innately secure*.	Imprinting process is End-to-End and zero trust required.

■ 3. ABSTRACT SUBMITTED DoD SBIR 2023.4: A2D-1380 - Soft Chips Solutions for Ultra Low Power Edge Intelligence

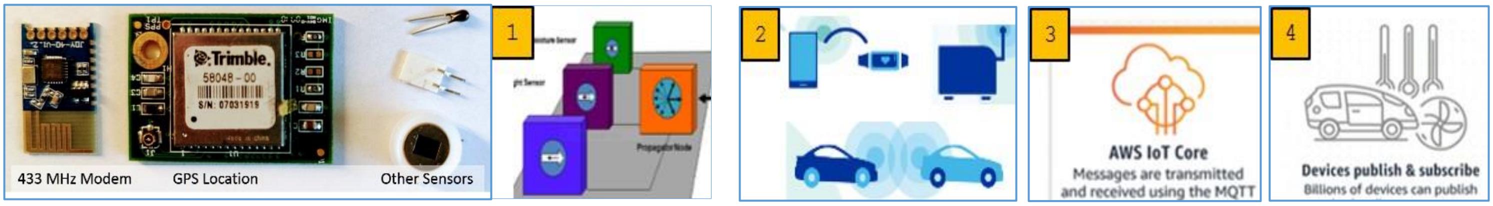
MODERNIZATION PRIORITIES: Advanced Computing and Software | Advanced Materials | Human-Machine Interfaces | Integrated Network Systems-of-Systems | Integrated Sensing and Cyber | Microelectronics | Trusted AI and Autonomy

KEYWORDS: logistics; supply chain; climate; internet of things; information collection; data collection; sensing; communications; autonomy; artificial intelligence; sensors; AI/ML; xTech; xTechPrime;

OBJECTIVE: XTechPrime is seeking novel, disruptive concepts and technology solutions with dual-use capabilities that can assist in tackling the Army's current needs and apply to current Army concepts. The intent is to provide the Army with transformative technology solutions while enabling cost savings throughout the Army systems' life cycle. Critical technology focus areas include Artificial Intelligence/Machine Learning (AI/ML); Autonomy; Climate and clean Technologies; Immersive/Wearables; and Sensors.

This proposal is relevant to highlighted words in ARMY BAA A234-P015 above. Since 2002, we have focused on last mile connectivity for semi-autonomous machines at the "Edge". These are remote, hostile, harsh, underdeveloped regions often energy constrained and communication compromised. Here we rely on authenticated information from trusted remote devices.

Over next decades, billions of IoT devices will be monitoring farms, forests, oceans, and other natural resources with sparse and *intermittent* cloud connectivity. As our machines become more autonomous, sparse or intermittent connectivity is sufficient and *ubiquitous.* Leveraging this ubiquity, simplified remote "Edge" sensors may provide data logs for pickup per schedules - a logistics supply chain paradigm. Taking cues from Nature, "Chirps" was developed for SPAWAR for terse stealth assured messaging. It was licensed by Sharp Corp. It has widespread uses for asset tracking, food systems and climate – on a Global scale.


Trimble.
58048-00
S/N: 07031918
433 MHz Modem
GPS Location
Other Sensors
1
2
3
AWS IoT Core
Messages are transmitted and received using the MQTT
4
Devices publish & subscribe
Billions of devices can publish

Imprinted and Reprogrammable Sensor Pack -> Data Logs -> Ubiquitous Carrier Pigeons -> Cloud -> Edge Intelligence

Today's last mile is crippled by Edge->Cloud thinking with proprietary transport protocols, not scalable or sustainable.

1. Today: Radios with BLE, Zigbee, Lora.. => Proprietary Gateways. => Fractured Markets and Silos => Not Scalable.
2. Chirp: Simple Modem, Low Power/Cost => All available Carrier Pigeons. => Globally Contiguous Clouds => Massively Scalable.

Key Points – related to Cloud->Edge thinking and its Cloud Orchestration Model are.

A. Soft Chips^{TM} – low cost, low power reprogrammable chips, embodying Chirps are imprinted by the Cloud to manage RF channels (how) and schedules (when) for packet delivery – using a familiar, Global scale logistics supply chain paradigm.

B. Ubiquitous Carrier Pigeons – phones, drones - pick up, GPS tag and time stamp and then forward to IoT hosted services.

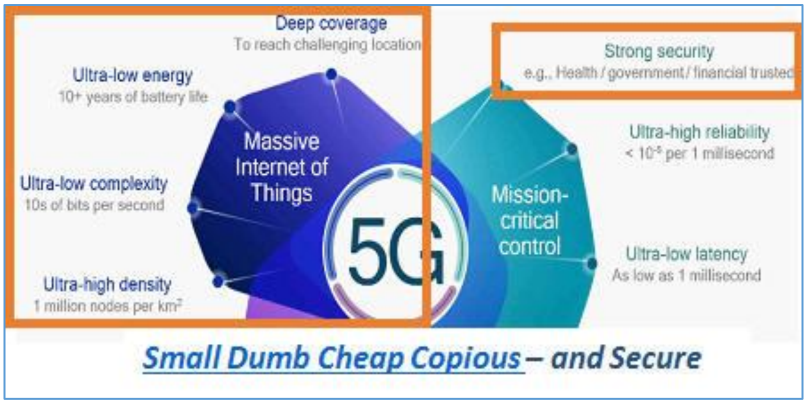
C. Soft Chips^{TM} use simple – and legacy supported - wireless serial modems. They can run on solar energy, in remote, harsh, hostile areas – providing crucial, trusted Edge Intelligence with low cost of deployment and reusable programmable chips.

D. At the cloud end of the supply chain: Logically contiguous clouds join walled garden boundaries - engendering "Massive IIoT".

Related Army Multi-domain Operations & Smart Dust are relevant to Abstracted Network Scalable IoT GreyNet PCN

■ 4. PICTORIAL TOUR (ABCD)

Illustrations A-B-C-D to explain Cloud Orchestrated Models



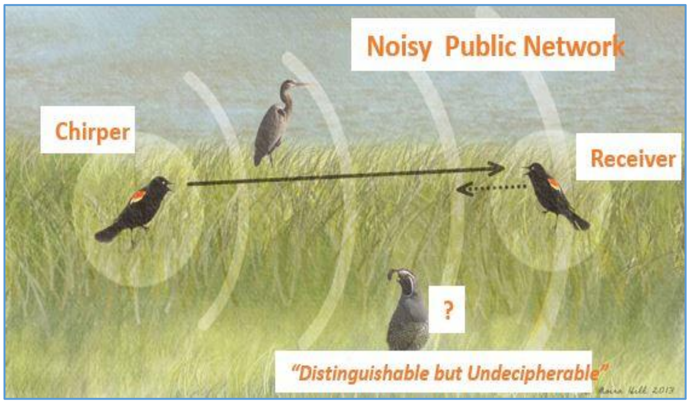
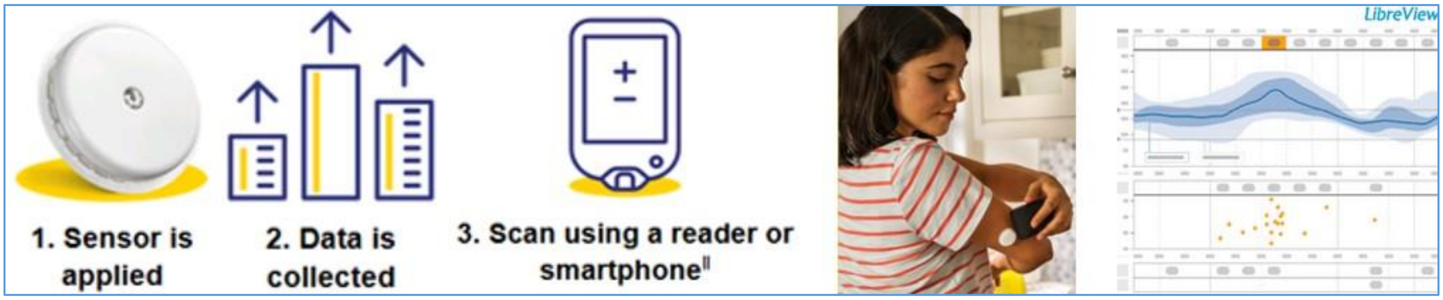


Fig. A. Left: Key Challenges to "Massive IoT": Energy, Complexity, Density + Security. In incumbent offerings massive deployment - density, simplicity, low power, and remote hostile environments conflict high security, requiring processing power.

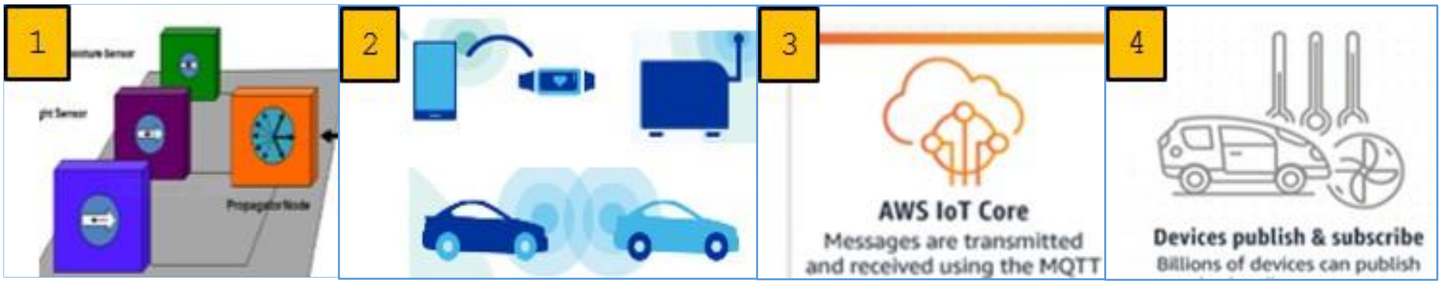
Fig. B. Right: Nature based approaches to Massive messaging are receiver biased. While all birds hear it only intended recipients can decode it. Distinguishable - for routing - yet undecipherable. Cryptic terse transmissions also not easily detected.

Fig. C. Below is a Consumer example of a secure and purpose driven Edge Sensor to Cloud work flow.



Medical Sensor Patch -> collects data. -> Specific Purpose Carrier Pigeon Transports -> Cloud -> Edge Intelligence

Fig. D. Below is an Enterprise Version: Sensor follows similar work flow as above but is cheap and innately secure.


1
2
3
4
Moisture Sensor
pH Sensor
Propagator Node
AWS IoT Core
Messages are transmitted and received using the MQTT
Devices publish & subscribe
Billions of devices can publish

Enterprise Imprinted Sensor "Patch" -> collects data -> Carrier Pigeon Transports -> Cloud Messaging-> Edge Intelligence.

Explanation for A-B-C-D. This approach leverages all available carrier pigeons (phones, drones). Like Pollen, Chirp packets are lightweight (minimally 1-2 bytes) and protocol agnostic – to piggyback on all available wireless transports. Our Sensor patches also use ubiquitously supported serial modem protocols. *This is a Quantifiable Cost Difference.* A modem costs 10 cents vs $20 for this WiFi radio. *And* CSMA/CA etc. are inherently inefficient . Chirps thus cleanly cut through Gordian knots in Fig. A

Simple Upgrades Across all Radio Protocols: All Edge radios can transport Chirp packets. Chirp protocol handlers are activated when existing radios on carrier pigeons detect Chirps - undecipherable to other supported protocols and so passed on to Chirp processing firmware – and if not there, the receiver radio simply discards it - Pollen Image. Otherwise packets are forwarded. This secure framework- with the upgraded firmware -and field tested by the military, is the Cloud Orchestration Model.

Lightweight and low-power leveraging all available transports. Simple Imprinted Devices managed by Cloud Orchestrators

■ 5.1 PROPOSAL DETAILS Page 1/6

Simple Devices Speaking Simply Securely and Copiously.

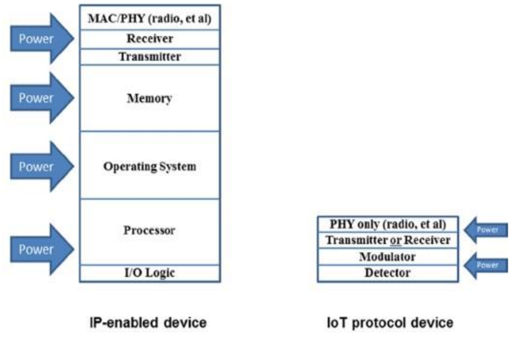


Figure 1-5. Contrasting the processor, OS, memory, and power necessary for traditional protocols vs. the IoT protocol

Soft Chips don’t need the full OSI stack

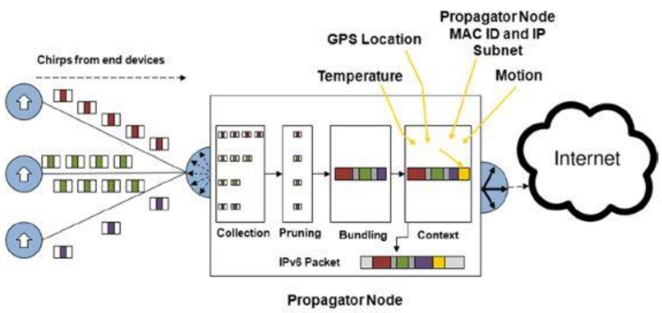


Figure 2-9. As chirps are bundled within propagator nodes, additional location, addressing, protocol, and other information is added

Pigeon has the full OSI stack -> does tagging and routing.

Minimal power consumption. Chirp Protocols shift radio intelligence and costly processing to the receiver end - phones, drones or any powered carrier pigeons that already run the full OSI stack (above left). These tag and forward Chirps. Chirp now need only simple wireless modems. Power usage are minimized by shorter packet sizes (1-2 bytes vs 40+ bytes), simpler processors and inherently more efficient transmissions over serial modems. Cost of end-to-end secure edge radio hardware plummets. Batteries can last decades. Solar is feasible for green deployments.

Shifting radio intelligence to the receiver and cloud is functionally equivalent to CSMA/CA and DCF for low power and cost Edge devices. Human driven RF chatter required smarts in phones and computers operating in congested, dynamic RF. BLE IoT devices also used MAC-based protocols and RF bands (e.g. 2.4 GHz) – their carrier pigeons (phones, computers) support it. But in *remote or rural, non-urban spaces, RF interference is not chaotic*. Cloud Orchestrators monitor RF patterns and sets RF channels for simple devices - scheduled when to listen, chirp or relay and on what non-interfering RF channels - collision avoidance in both time and RF space. **Small** (footprint), **Dumb** (processing power) **Cheap** (minimal hardware). Potentially **Copious**. More

Imprinting at Birth. MAC ID or other UUID Identification Schemes are supplied by third party vendors to enterprises. They cannot customize it to be topic based – how pub/sub messages are transported within large scale enterprises to interested subscribers. In contrast, imprint empowers enterprises to use their own ID schemes. Additionally, imprinting happens in the field when the soft chip is being deployed and is attached to the asset. This establishes **provenance** and trust chains – See RFID++ for more.

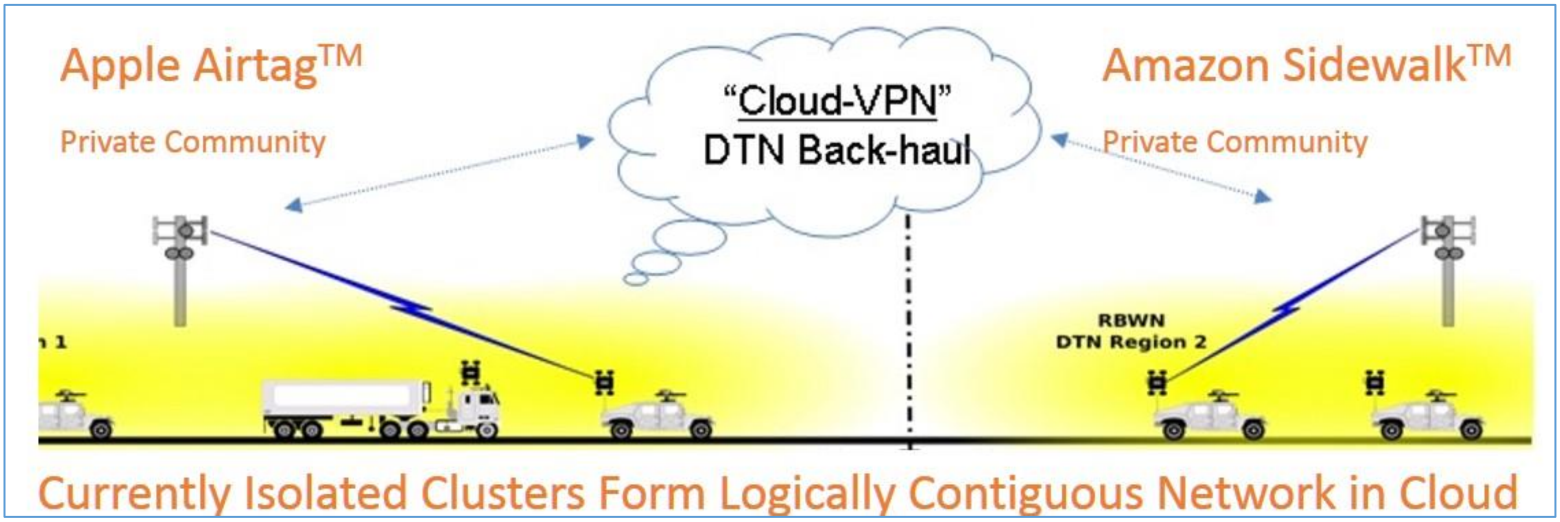
Security. Chirpers don't use MAC ID or other UUID Identification Schemes. See MAC spoofing and Man in the Middle Attack for reasons why. Instead, Chirpers provide a minimal Chirp-ID - the digital bird species ID. Carrier Pigeons then fill in tagging - GPS location, timestamps and route the IPV6 packet. Image. Even the Chirp-ID may be generated based on the environment. If less than 255 unique species are operating at the same schedules and RF channels ranges - Co-location in both time and RF space - then 1 byte suffices. Detecting a 1-2 byte packet when channel, time or handshaking are all unknown makes Chirps innately secure. And even if detected it will be changed at the next encounter between the pigeon and device.

Soft Chips. Ant-like intelligence is imprinted to provide When-this-then-that and If-this-then-that processes. Soft Chips are a set of sensors that are activated by imprinted code to perform specific tasks e.g. make data logs, relay "fire!" alerts, monitor pollution or detect intrusion detection through simple means. Designed Features - and value - in Soft Chips is in them being:

Small.	Small Radio Power Usage and Footprint - Long Battery life. Solar only, feasible.
Dumb.	Purpose Specific Ant-like processing capabilities - but re-programmable
Cheap.	Intended to be produced in millions - since multi-use and re-purposed
Copious.	Intended to be used like seeding crops - deep ground truth verification
Secure.	Imprinting process is innately secure. USB modems for even security.
Organic.	No central standards committee needed. Enterprises make up their own.
Agnostic.	Chirps are protocol agnostic. Software Fix to coexist with other protocols.

■ 5.2 PROPOSAL DETAILS Page 2/6

Cloud Orchestrated Models 1/2



Products in Walled Garden Ecosystems can be connected by Trusted Messaging between their Clouds- Global Edge Intelligence

Apple AirTag^{TM} Asset tracking devices “trust” Apple Smart phones and its network to covertly provide secure location tracking services. They do not currently connect to Amazon Sidewalk^{TM} network. They do not share proprietary firmware and software handshaking protocols. Now consider a low cost Chirp version of AirTag^{TM} – made by Apple but using long range Sub 1 GHz radios. Apple Phones don’t support that radio but simple USB radio modems are a simple fix.

Chirp protocols are radio & protocol agnostic. Both Apple and Amazon may provide Chirp aware products, on their own Chirp protocols, no standards committees needed. At the Cloud end **networks can coalesce across previously walled gardens.** Chirps are then published to interested subscribers –now a *logically contiguous Global cloud* through Pub/Sub messaging services.

Edge->Cloud Thinking. Today’s last mile is crippled by proprietary transport protocols, not sustainable. Edge to Cloud thinking focused on smarts at the radio end to manage collision avoidance by segmenting collision domains in RF space (channel diversity) and time (time reservation slots). Current IoT Radios have to be “smart” because they use phones and computers as carrier pigeons to connect. These devices, intended for humans are rechargeable and thus not energy constrained. They can afford more power hungry communication protocols. In order to communicate. Thus some IoT edge devices must also confirm to protocols and radio frequencies phones and computers support – or build out proprietary mesh networks and Gateways.

Conversely, in **Cloud->Edge thinking**, we let the Cloud manage ant-like reprogrammable intelligence at the Edge – purpose driven, minimal smarts low power and cheap so it can be copiously deployed – as in dense sensor grids for intrusion detection..

Minimal Deployment Costs. The cost of Dual Band radio is $20. 433 MHz Wireless modems are 10 cents. MAC based radios use 45 bytes to transport a 4 byte data packet. Chirpers do it in 5 bytes with one byte for ID tagging. Communication power usage and product cost are both minimal and fraction of current Edge->Cloud radio systems. The current Edge radios and their proprietary protocols have resulted in fractured markets and unscalable networks. Since Chirp is protocol agnostic, all wireless networks may support Chirp products through protocol handlers – thus extending their network beyond current boundaries.

Further, Chirp devices use **Topic Based Addressing** – not device or protocol specific. Hosted services managing such devices can “connect” similar Chirp species to Carrier Pigeon services available – birds of a feather may now flock together. Amazon IoT Core hosting knows where devices under its care are and what RF channels are being used by them. It can thus Orchestrate elements of this logistics supply chain. A new Chirp device, joining this network will be assigned non- interfering channels and schedules.

Since all co-located Chirp products share the same RF space, the Cloud manages which non-interfering channels to use for what and when devices must be silent in time slots reserved. Collision avoidance – in time and space - is now **Cloud Orchestrated.**

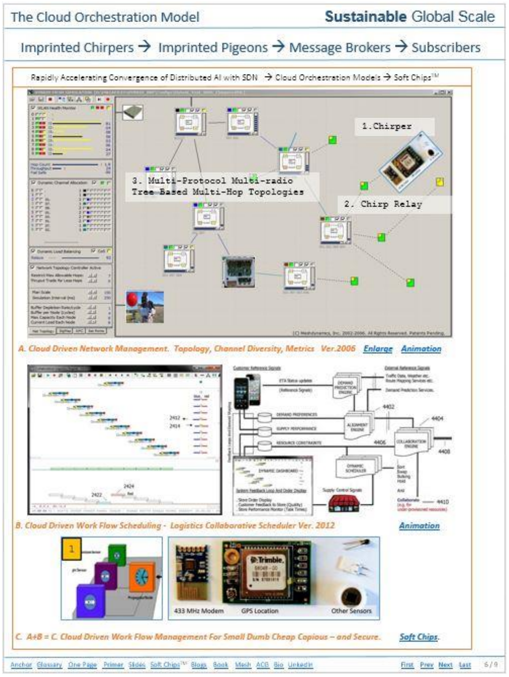
■ 5.2 PROPOSAL DETAILS Page 3/6 *Cloud Orchestrated Models 2/2*

Today's last mile is crippled by **Edge→Cloud** thinking with proprietary transport protocols, not scalable or sustainable.

1. Today: Radios with BLE, Zigbee, Lora → Proprietary Protocols & Systems →Fractured Markets and Silos→Not Scalable.
2. Chirp: Radio Modem + Imprinting → Any available Chirp aware Pigeon→Globally Contiguous Clouds→Massively Scalable

Edge->Cloud thinking must shift to more sustainable, scalable, secure **Cloud->Edge thinking.**

A. Global-Scale "Edge" challenges are: simplicity, cost, energy & (as always) security.
B. Chirpers don't need heavy OSI stack -> minimal cost and power usage 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 IoT - with no legacy systems left behind - burgeons. See Slides or click below for overviews.


The Cloud Orchestration Model **Sustainable** Global Scale

Imprinted Chirpers → Imprinted Pigeons → Message Brokers → Subscribers

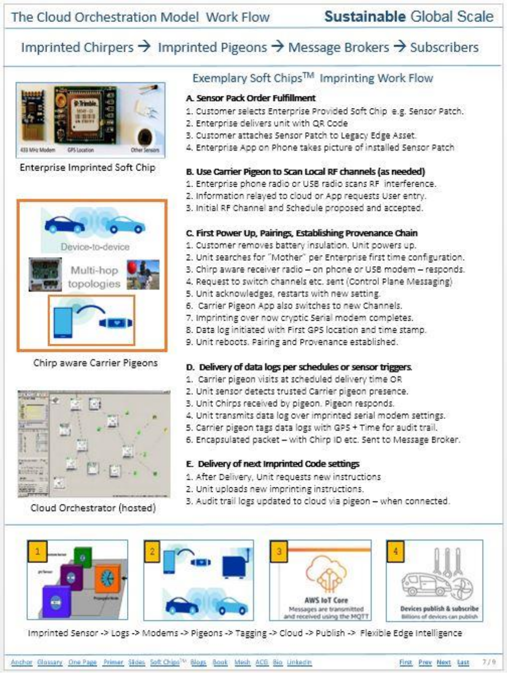
Rapidly Accelerating Convergence of Distributed AI with SDN → Cloud Orchestration Models → Soft Chips™

A. Cloud Driven Network Management. Topology, Channel Diversity, Metrics Ver.2006 Enlarge Animation

B. Cloud Driven Work Flow Scheduling - Logistics Collaborative Scheduler Ver. 2012 Animation

C. A+B = C. Cloud Driven Work Flow Management For Small Dumb Cheap Copious – and Secure. Soft Chips.

Anchor Glossary One Page Primer Slides Soft Chips™ Blogs Book Mesh ACG Bio LinkedIn First Prev Next Last 6 / 9


The Cloud Orchestration Model Work Flow **Sustainable** Global Scale

Imprinted Chirpers → Imprinted Pigeons → Message Brokers → Subscribers

Enterprise Imprinted Soft Chip

Chirp aware Carrier Pigeons

Cloud Orchestrator (hosted)

Exemplary Soft Chips™ Imprinting Work Flow

A. Sensor Pack Order Fulfillment
1. Customer selects Enterprise Provided Soft Chip e.g. Sensor Patch.
2. Enterprise delivers unit with QR Code
3. Customer attaches Sensor Patch to Legacy Edge Asset.
4. Enterprise App on Phone takes picture of installed Sensor Patch

B. Use Carrier Pigeon to Scan Local RF channels (as needed)
1. Enterprise phone radio or USB radio scans RF interference.
2. Information relayed to cloud or App requests User entry.
3. Initial RF Channel and Schedule proposed and accepted.

C. First Power Up, Pairings, Establishing Provenance Chain
1. Customer removes battery insulation. Unit powers up.
2. Unit searches for "Mother" per Enterprise first time configuration.
3. Chirp aware receiver radio – on phone or USB modem – responds.
4. Request to switch channels etc. sent (Control Plane Messaging)
5. Unit acknowledges, restarts with new setting.
6. Carrier Pigeon App also switches to new Channels.
7. Imprinting over now cryptic Serial modem completes.
8. Data log initiated with First GPS location and time stamp.
9. Unit reboots. Pairing and Provenance established.

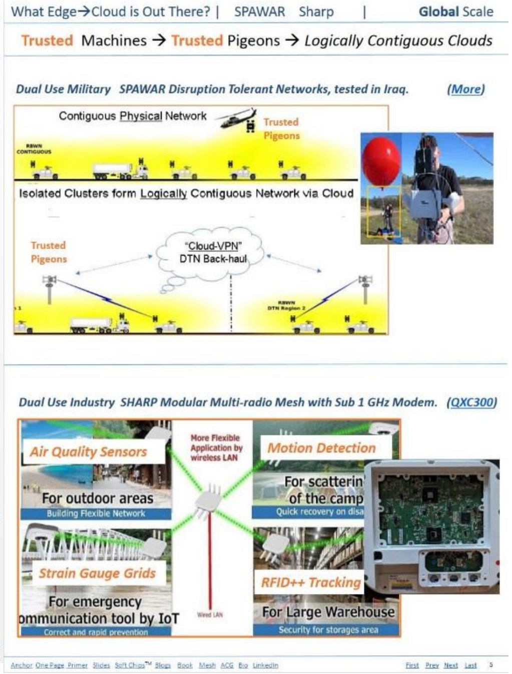
D. Delivery of data logs per schedules or sensor triggers.
1. Carrier pigeon visits at scheduled delivery time OR
2. Unit sensor detects trusted Carrier pigeon presence.
3. Unit Chirps received by pigeon. Pigeon responds.
4. Unit transmits data log over imprinted serial modem settings.
5. Carrier pigeon tags data logs with GPS + Time for audit trail.
6. Encapsulated packet – with Chirp ID etc. Sent to Message Broker.

E. Delivery of next Imprinted Code settings
1. After Delivery, Unit requests new instructions
2. Unit uploads new imprinting instructions.
3. Audit trail logs updated to cloud via pigeon – when connected.

433 MHz Modem
GPS Location
Other Sensors
Device-to-device
Multi-hop topologies
1
2
3
AWS IoT Core
Messages are transmitted and received using the MQTT
4
Devices publish & subscribe
Billions of devices can publish

Imprinted Sensor -> Logs -> Modems -> Pigeons -> Tagging -> Cloud -> Publish -> Flexible Edge Intelligence

Anchor Glossary One Page Primer Slides Soft Chips™ Blogs Book Mesh ACG Bio LinkedIn First Prev Next Last 7 / 9


What Edge→Cloud is Out There? | SPAWAR Sharp | **Global** Scale

Trusted Machines → Trusted Pigeons → *Logically Contiguous Clouds*

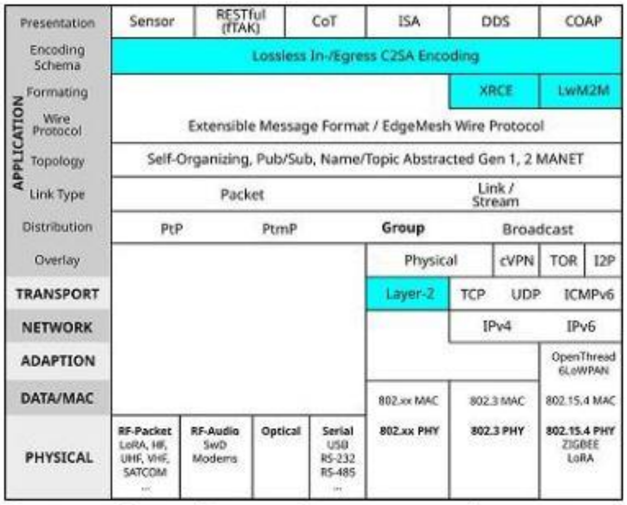
Dual Use Military SPAWAR Disruption Tolerant Networks, tested in Iraq. (More)

Contiguous Physical Network
Trusted Pigeons
RBWN CONTIGUOUS
Isolated Clusters form Logically Contiguous Network via Cloud
Trusted Pigeons
"Cloud-VPN" DTN Back-haul
RBWN DTN Region 2

Dual Use Industry SHARP Modular Multi-radio Mesh with Sub 1 GHz Modem. (QXC300)

Air Quality Sensors
For outdoor areas
Building Flexible Network
More Flexible Application by wireless LAN
Motion Detection
For scatterin of the camp
Quick recovery on disa
Strain Gauge Grids
For emergency ommunication tool by IoT
Correct and rapid prevention
Wired LAN
RFID++ Tracking
For Large Warehouse
Security for storages area

Anchor One Page Primer Slides Soft Chips™ Blogs Book Mesh ACG Bio LinkedIn First Prev Next Last 5


APPLICATION

Presentation: Sensor | RESTful (fTAK) | CoT | ISA | DDS | COAP

Encoding Schema: Lossless In-/Egress C2SA Encoding

Formating: XRCE | LwM2M

Wire Protocol: Extensible Message Format / EdgeMesh Wire Protocol

Topology: Self-Organizing, Pub/Sub, Name/Topic Abstracted Gen 1, 2 MANET

Link Type: Packet | Link / Stream

Distribution: PtP | PtmP | **Group** | Broadcast

Overlay: Physical | cVPN | TOR | I2P

TRANSPORT: Layer-2 | TCP | UDP | ICMPv6

NETWORK: IPv4 | IPv6

ADAPTION: OpenThread 6LoWPAN

DATA/MAC: 802.xx MAC | 802.3 MAC | 802.15.4 MAC

PHYSICAL: **RF-Packet** LoRA, HF, UHF, VHF, SATCOM … | **RF-Audio** SwD Modems | **Optical** | **Serial** USB RS-232 RS-485 … | **802.xx PHY** | **802.3 PHY** | **802.15.4 PHY** ZIGBEE LoRA

Chirp port forwarders reside on pigeon radios at Layer I.

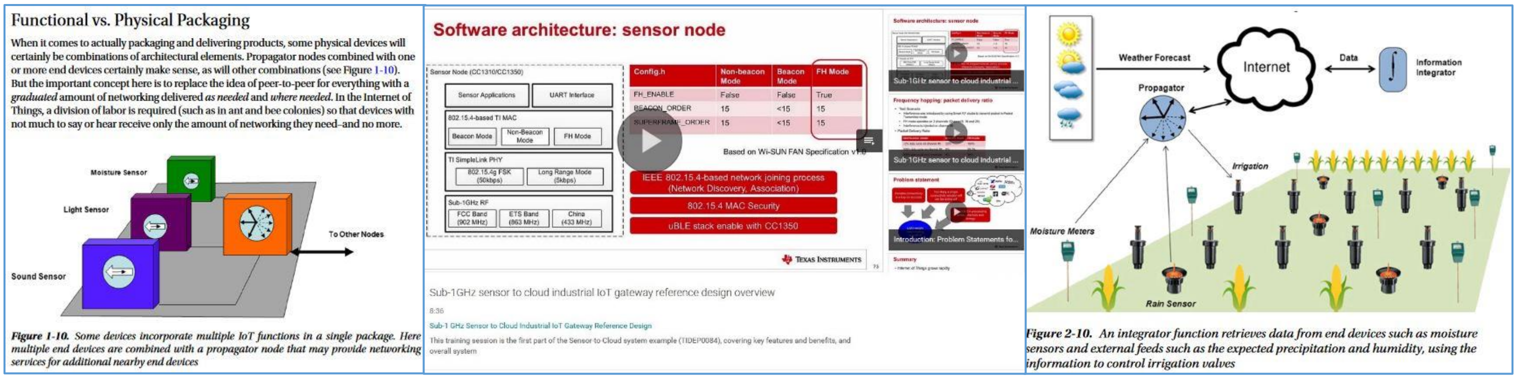
Pigeons then port chirps to other radios and form logical Layer 2 network.

Soft Chips – as the name suggests – may be imprinted to provide diverse behaviors. They can use any carrier pigeon radio that supports serial modem communications and can detect, with a Chirp protocol handler chirps. Enterprise customized **imprinted** code directs sensors in the multi-use sensor pack. Imprints thus mimic primitive ant-like edge intelligence – small dumb cheap copious – and secure. Low power 16 bit microcontroller with a modem hand off to pigeons. The Chirp protocol uses rudimentary - legacy supported – modems. All pigeons can support it. **Benefits**: *Lightweight and low-power leveraging all available transports – protocol agnostic. Low cost modem and processing unit minimizes costs and battery life*

Established Provenance. Chirp products are imprinted at birth – establishing provenance to "Mother". On power up chirp devices first scan/listen for the Cloud "Mother" on private channels and cryptic protocols. Intended Receiver radios inside phones or USB modems respond, then imprint devices, see Image. Imprints provide an end-to-end trusted system. Establishing **provenance** of sourced materials - which tree in which forest - has to come from imprinted tags that follow the tree from the forest to the lumber yard. Trust chains begin when the tree is first felled and an RFID++ tags is attached to it- with GPS location and time tagging through the imprinting process with a phone or USB Modem used to transmit imprint instructions (code) . RFID++ tags thus establish provenance for regulatory agencies and also provide a record of travel conditions e.g. for vaccines and food.

We are in conversations with two US Chipmakers to use existing development tools and COTS products to engender Chirp aware IoT ecosystems. They can provide multi-use Soft Chips prototypes containing GPS, Accelerometer, Temperature, microphone etc. Sensors are activated by imprints to run schedules (Cron) or on triggers. Minimal versions of Free RTOS suffice. More. Three use cases - **RFID++** for asset tracking, **Chirper Grid** for early warning systems and **Sensor Patch** for legacy assets will be imprinted – and demonstrate different behaviors. Two U.S. chipmakers will validate vendor neutral, nature of chirp protocols & architecture.

1. RFID++$^{TM.}$ RFID is a static GUID identification scheme. The tags is applied to boxes in transit and when energized, transmit a code to the reader. Similarly, a RFID++ tag is an active tag applied to perishable items, for example. It builds a data log of the item in transit, based on IR, temperature, sound and accelerometer sensors. Logs are released to readers when a handshake signal is received by microphone or IR sensors. This rechargeable RFID++ tag thus minimally contains sensors, no MAC and simple Sub 1GHz modem. RFID++ chirps are 1-2 bytes vs. IPV6 40+. Schedules ensure collision avoidance. CSMA/CA need not apply.



Functional vs. Physical Packaging

When it comes to actually packaging and delivering products, some physical devices will certainly be combinations of architectural elements. Propagator nodes combined with one or more end devices certainly make sense, as will other combinations (see Figure 1-10). But the important concept here is to replace the idea of peer-to-peer for everything with a *graduated* amount of networking delivered *as needed* and *where needed*. In the Internet of Things, a division of labor is required (such as in ant and bee colonies) so that devices with not much to say or hear receive only the amount of networking they need–and no more.

***Figure 1-10.** Some devices incorporate multiple IoT functions in a single package. Here multiple end devices are combined with a propagator node that may provide networking services for additional nearby end devices*

Software architecture: sensor node

Sensor Node (CC1310/CC1350)

Sensor Applications | UART Interface

802.15.4-based TI MAC: Beacon Mode | Non-Beacon Mode | FH Mode

TI SimpleLink PHY: 802.15.4g FSK (50kbps) | Long Range Mode (5kbps)

Sub-1GHz RF: FCC Band (902 MHz) | ETS Band (863 MHz) | China (433 MHz)

Config.h	Non-beacon Mode	Beacon Mode	FH Mode
FH_ENABLE	False	False	True
BEACON_ORDER	15	<15	15
SUPERFRAME_ORDER	15	<15	15

Based on Wi-SUN FAN Specification v1.0

IEEE 802.15.4-based network joining process (Network Discovery, Association)

802.15.4 MAC Security

uBLE stack enable with CC1350

Texas Instruments 73

Sub-1GHz sensor to cloud industrial IoT gateway reference design overview

8:36

Sub-1 GHz Sensor to Cloud Industrial IoT Gateway Reference Design

This training session is the first part of the Sensor-to-Cloud system example (TIDEP0084), covering key features and benefits, and overall system

Software architecture: sensor node
Sub-1GHz sensor to cloud industrial ...
Frequency hopping: packet delivery ratio
Sub-1GHz sensor to cloud industrial ...
Problem statement
Introduction: Problem Statements fo...
Summary
Weather Forecast
Internet
Data
Information Integrator
Propagator
Irrigation
Moisture Meters
Rain Sensor

***Figure 2-10.** An integrator function retrieves data from end devices such as moisture sensors and external feeds such as the expected precipitation and humidity, using the information to control irrigation valves*

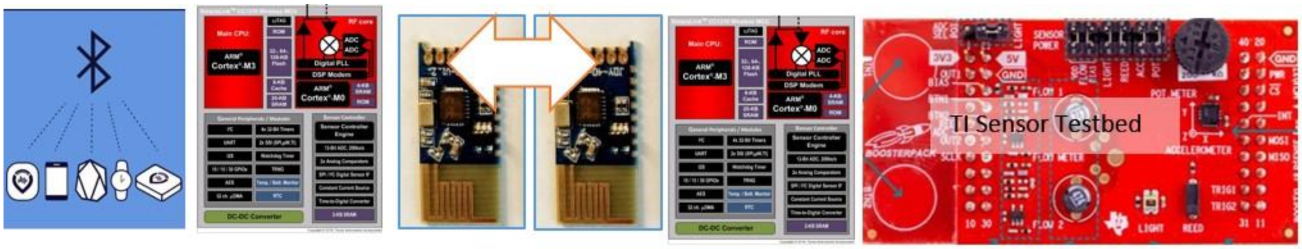
L-R. Soft chips packaging of sensors and modem, Exemplary low power OS development, Chirper Grids for copious seeding.

2. Chirper Grid^{TM} is a variant which is event and relay based. Heat sensors trigger chirps over staggered (jitter) intervals so many chirpers, hearing this, relay it quickly so the entire grid goes "live", see Flooding. Patrol drones or phones with USB modems are pigeons to bring it into the cloud and galvanize the fire protection services, saving us billions. Military versions, for mobile asset tracking and intrusion detection, have been field tested as part of a disruption tolerant real time military mesh network.

3. Sensor (Legacy) Patch. Legacy Edge assets - pump motors - will have a non-invasive sensor patch attached to them that provide Edge → Cloud data logs. Vibration and sound sensors logs will be analyzed in the cloud for proactive predictive maintenance – e.g. "bushings needs oil". Such scheduled and purpose driven sensing drives new efficiencies in servicing assets.

■ 5.4. PROPOSAL DETAILS Page 5/6

Minimal Viable Product Leveraging Ubiquitous SMS



```
Apps on Connected Devices    Orchestrate
 |
 |- To Cloud Message Brokers (e.g. SMS)
 |- Download Configured Exemplary Templates
 |
 |- Network Extension Support:
 |- Provide Simple Relays over BLE Mesh
 |- Connect to Covert Global Scale Networks
 |- Restrict or extend network reach.
 |- Leverage Tree based scalable networks.

Imprinting and Delivery Schedules
 |
 |-Imprinted with Schedules
 |-Told when to listen and speak
 |-Data logs erased on pick up
```

(excerpted from Chirp Primer).

A minimal viable Soft Chip work flow may use SMS as message broker and BLE/USB on pigeons to store and forward. *More* Consider a potential use case for a farmer in rural Africa. His phone has no connectivity in the field where the sensors are. A store and forward mechanism is needed – see this email based thin device for Asian rural distribution chains. We also want to leverage SMS like free messaging services so we must limit the total payload to 160 bytes for SMS transmissions. There will also be tagging at the Smart phone application end before it is transmitted to SMS message brokers – when the farmer has connectivity. We thus further limit data log payload to be no more than 110 bytes, with 10 bytes reserved for Chirp-ID etc. The 100 byte data log will be sent on SMS, so we may further restrict it to ASCII and CSV-like format.

For the 100 bytes payload (the data log) our options are based on how many samples and each sample size in bytes :

#Samples : Sample_Size_in_Bytes: 100:1, 50:2, 25:4, 20:5, 10:10, 5:20, 4:25, 2:50, 1:100 (100 bytes each).

Thus 4 sensors, each providing 1 byte may be sampled 25 times during pigeon pickup sessions. This specific Chirp payload framing is thus fleshed out to be 25 samples of |Sensor_1|Sensor_2|Sensor_3|Sensor_4| = 25 *4*1 bytes. This is generous because 2 bits (0 through 3) can define "black or dead", "red", "yellow", "green" mapping to programmed sensor data ranges. Thus 4 sensor feeds can be condensed to one byte (8 bits). Edge intelligence can be terse yet meaningful- especially in receiver-oriented communications. In military stealth uses for asset tracking and intrusion detection 1-2 bytes were used - and no Chirp-ID (obfuscation mode).

When pigeons arrive, data logs are transferred based on handshaking supplied in the imprinting protocols- and could be as simple as an obfuscated version of Chirp-IDs. Recall schedules and protocol framing are private and can be changed each trip - using temporal keys and frequency hopping. Innately Secure.

After data logs are delivered, the data log is erased and effectively a soft reboot begins the next data logging schedule - which may include a new programs or framing. The soft chip may not have GPS to conserve both cost and power, but pigeons may - then time/location are synched. Mobile asset tracking at this granularity may suffice.

The farmer transfers the data log (110 bytes) from the pigeon to apps on his phone with BLE pairing between his phone and the BLE radio on the pigeon. The phone app can add GPS and time stamp tags and eventually forwards it to message brokers - SMS, WhatsApp etc. These trusted community networks may include oversight agencies who rely on remote ground data to drive forecasting etc.

A minimal viable - and self-sufficient - product emerges which may also leverage existing BLE connectivity, already in use for indoor IoT to connect with BLE mesh on local WLANs. The farmer's phone may thus use other phones in the network to connect to cloud services.

Consider now two WhatsApp accounts on the farmer's phone. One is admin protected and provides programs and schedule templates. The phone app adds jitter settings so soft chips avoid collisions and generates new imprints for all Soft Chips on the farm- a poor man's Cloud Orchestrated Model. The pigeon- like postal workers - carry community "mail" and distributes it. Data logs from soft chip grids, collected through the region are sent to another SMS or WhatsApp account to collectively provide actionable intelligence available to digital and human subscribers - operating at a globally relevant scale. Thus two messaging accounts, an intermittently connected device and store-and-forward pigeons support dense sensor grids relevant to food supply, climate preparedness, asset tracking etc.

5.5. PROPOSAL DETAILS Page 6/6

CHIPS, COTS Support and Supervised Autonomy

5.5.1 Soft Chips™ and CHIPS initiatives.

"Business is War Watered Down"

Soft Chips embodiments are intended for dual use (military and industrial) since the security is in the imprinting services provided by trusted cloud agents. Two ends of wireless modems must "match" - know of each other's' schedules and RF channel usage and cryptic handshakes. Thus a military version uses a USB wireless modem and soft chips using military RF channels. ***End-to-End and zero trust are integral to this Nature based imprinting work flow.*** CHIPS initiatives - "*integral to America's economic and national security*" will benefit because only trusted radios will have essential Chirp protocol handlers installed.

5.5.2 Soft Chips™ and COTS products availability.

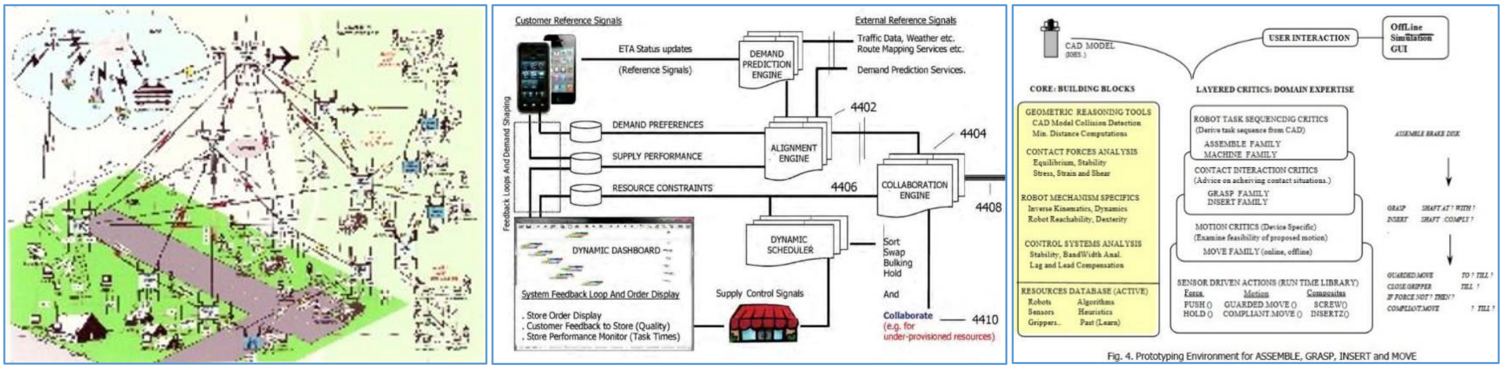
COTS Support for Co-existing Chirp IoT.

Above L-R: TI Sensor Controller Studio for MCU Sensor Controller & Sensors and Modem Elements.

In 2016 a developer in Europe demonstrated a version on Raspberry PI with a two byte Chirp. We now generalize it – innately secure, cloud orchestrated Cloud->Edge Global Scale messaging. The Sensor Controller Studio, supports a plethora of radios - all of which can be made Chirp aware. These MAC based radios need a simple protocol handler, running at the Lower Level MAC, to detect Chirps and then forward them. These radios are already on our ubiquitously available carrier pigeons and they run the full OSI stack. Where a specialized radio is needed, a USB attachment - Enterprise or Government Imprinted - is a simple fix. Military and Industry are deploying Software Defined Radios. Sub-1 GHz radios used by Amazon Sidewalk. Chirp extends this network to farms forests, rural, remote regions through software - Sustainable Global Impact.

5.5.3 Soft Chips™ and Supervised Autonomy

In 1992 a Supervised Autonomy Architecture (video) was deployed in multiple dual use cases. In 2003 Soft Chips™ Concepts were developed for Military stealth intrusion detection. Last mile connectivity for remote assets had its challenges: Mobility, Scalability, and Logically Contiguous network infrastructure to service these stealth devices was addressed first. Chirps were first discussed here. The combined power of Distributed AI and SDN then prompted this shift to Cloud Orchestration Models.


Customer Reference Signals
External Reference Signals
ETA Status updates
(Reference Signals)
DEMAND PREDICTION ENGINE
Traffic Data, Weather etc.
Route Mapping Services etc.
Demand Prediction Services.
4402
4404
DEMAND PREFERENCES
SUPPLY PERFORMANCE
RESOURCE CONSTRAINTS
ALIGNMENT ENGINE
4406
COLLABORATION ENGINE
4408
Feedback Loops And Demand Shaping
DYNAMIC DASHBOARD
DYNAMIC SCHEDULER
Sort
Swap
Bulking
Hold
And
System Feedback Loop And Order Display
. Store Order Display
. Customer Feedback to Store (Quality)
. Store Performance Monitor (Task Times)
Supply Control Signals
Collaborate
(e.g. for under-provisioned resources)
4410
CAD MODEL
USER INTERACTION
OffLine Simulation GUI
CORE: BUILDING BLOCKS
LAYERED CRITICS: DOMAIN EXPERTISE
GEOMETRIC REASONING TOOLS
CAD Model Collision Detection
Min. Distance Computations
CONTACT FORCES ANALYSIS
Equilibrium, Stability
Stress, Strain and Shear
ROBOT MECHANISM SPECIFICS
Inverse Kinematics, Dynamics
Robot Reachability, Dexterity
CONTROL SYSTEMS ANALYSIS
Stability, BandWidth Anal.
Lag and Lead Compensation
RESOURCES DATABASE (ACTIVE)
Robots
Sensors
Grippers..
Algorithms
Heuristics
Past (Learn)
ROBOT TASK SEQUENCING CRITICS
(Derive task sequence from CAD)
ASSEMBLE FAMILY
MACHINE FAMILY
CONTACT INTERACTION CRITICS
(Advice on acheiving contact situations.)
GRASP FAMILY
INSERT FAMILY
MOTION CRITICS (Device Specific)
(Examine feasibility of proposed motion)
MOVE FAMILY (online, offline)
SENSOR DRIVEN ACTIONS (RUN TIME LIBRARY)
Force
Motion
Composites
PUSH ()
HOLD ()
GUARDED MOVE ()
COMPLIANT MOVE ()
SCREW()
INSERTZ()
ASSEMBLE BRAKE DISK
GRASP
INSERT
SHAFT AT ? WITH ?
SHAFT COMPLY ?
GUARDED MOVE
CLOSE GRIPPER
IF FORCE NOT ? THEN ?
COMPLIANT MOVE
TO ? TILL ?
TILL ?
? TILL ?
Fig. 4. Prototyping Environment for ASSEMBLE, GRASP, INSERT and MOVE

Above L-R: Mobile Mesh Networks, Collaborative Scheduling, Digital Domain Experts (Critics).

■ 6. STATEMENT OF WORK (SOW). *Validating Soft Chips and Cloud Orchestration Models.*

Time estimates based on work on the NIST sponsored Unified Tele-robotics Architecture Program and similar multi-year NRE contracts from SPAWAR and other military system integrators that focused on supervised autonomy for remotely operated devices. Related: Publication and Video.

■ 6.1 Phase I 6 months. *Prototype Soft Chips Package with COTS Free RTOS, 16 Bit MCUs etc.*

This phase will include selecting two serial modem chipset manufacturers, with sensors on the chipset or easily added via serial modem-like inputs from external sensor streams. Phase I demonstrates that Chirp packets – using rudimentary and legacy supported serial modem protocols – are detected and forwarded by existing radios on ubiquitous carrier pigeons – phones, drones, delivery trucks, farm tractors - on supported frequency bands on their radios ***or*** by inserting USB powered wireless serial modems. Conversations in progress with their applications groups. (Existing carrier pigeons can thus be Chirp aware through a software upgrade **or** USB radio. The USB modem is also imprinted by Enterprises or Regulatory Agencies and their agents).

Sub 1 GHz radios are not currently supported on phones – our ubiquitous carrier pigeons. A USB modem is a simple fix and will be demonstrated. Thus any smart phone can now extend the reach of simple serial modem based edge devices. Military radios can install chirp protocol handlers at the Lower Level MAC (LLMAC) just above the PHY layer - to detect and forward stealth chirps. We are in conversations with two US Chipmakers to use existing development tools and COTS products to engender Chirp aware IoT ecosystems. They will provide multi-use Soft Chips prototypes containing GPS, Accelerometer, Temperature, microphone etc. Sensors are activated by imprints to run schedules (Cron) or on triggers. Minimal versions of Free RTOS suffice.

■ 6.2 Phase II 6 months. *Chirp Protocol Handlers coexisting with other radio protocols.*

A developer in Europe implemented a version of Chirps on Raspberry PI with a two byte Chirp. We now take this to the next level – innately secure, cloud orchestrated Chirp messaging. The Cloud Orchestrator, running on a hosted IIOT service like Amazon IoT Core, will be tested on digital clones emulating the Soft Chips. Next the code that imprint edge devices from hosted IOT services will be tested - the same imprinting code on two US sensor & radio chipmakers. As an example, per this demonstration Texas Instruments, Honeywell, Amazon Sidewalk radios will continue to use existing protocols. In addition, those same radios will detect and forward Chirp packets. Proactive Collision Avoidance - Temporal and Channel Diversity – will be tested in the cloud.

■ 6.3 Phase III 6 months. *Exploring applications for copious soft chips use – "billions".*

Edge->Cloud thinking 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".

Here we explore dual case uses of Imprinted Work Flow: Edge→Modem→Pigeon→Cloud→Subscribers

. Explore types of edge intelligence transported through imprinting.
. Demonstrate scalability and security through field tests.
. Explore the set of use cases that together justify making billions of Soft Chips.
. These chipsets support software extensions in existing radios on carrier pigeons – or USB.
. Explore packaging options for simplified Master control unit (MCU), Sub 1 GHz modem.
. Define sets of wide purpose sensor suites that are activated based on imprinting directives.
. Explore commercialization of Soft Chips Embodiments – Related Content: Soft Chips

■ 7. ABOUT US

Key Personnel and **Meshdynamics Technology.**

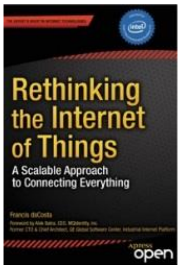
■ 7.1 Key Personnel, Francis daCosta (Northrop, MITRE).

The emerging Internet of Things architecture and Meshdynamics mesh networking technology has been influenced by the Robotics and Machine Control background of Francis daCosta. In 1992 Francis founded Advanced Cybernetics Group and developed dual use control systems protocol and architecture for semi-autonomous robotics see ACG Video.

In 2002, Meshdynamics was formed to focus on stealth chirp protocols for military machines in remote, harsh and hostile environments. In 2012 Intel sponsored Rethinking the Internet of Things, based on his IoT blogs. Francis has a Masters from Stanford University, post-graduate work in AI from UCLA, a bachelors from IIT-Delhi. He has authored 24 awarded patents.

His journey is a convergence of overlapping and inter connected interests in Edge and Cloud. Bio Slides

1982-2002 Robots → Add Sensors → Add Tele-robotics → Add Automated Programming
2002-2012 Add Time Sensitive Networks (last mile, mesh networks, mobility, Chirp)
2012-2022 Re-thinking the Internet of things, Proving Cloud Orchestration models


Rethinking the Internet of Things
A Scalable Approach to Connecting Everything
Francis daCosta
open

■ 7.2 Key Personnel, Curtis White (AFRL, SPAWAR).

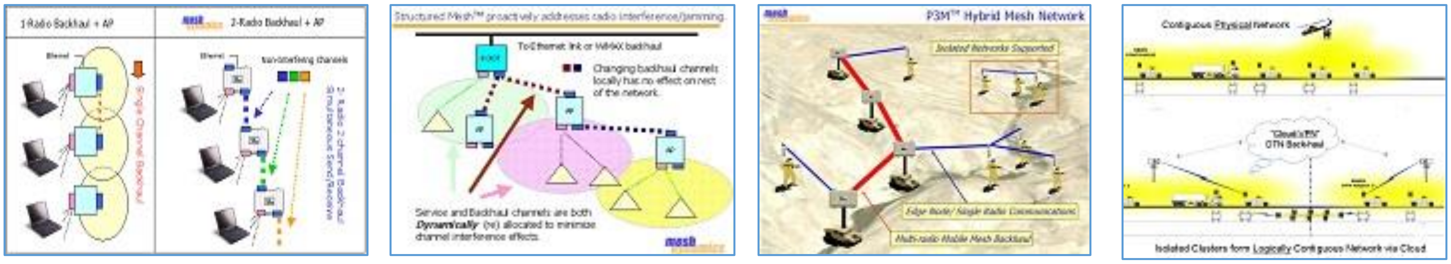
Curtis has been intimately involved in Meshdynamics and its military applications since 2002. He has recently retired as Sr. Research System Engineer at SPAWAR-LANT/SAT. Curtis will continue to explore military and commercial uses for “Chirp”.

■ 7.3 Key Personnel Alok Batra (GE, Cisco)

Formerly the CTO and Chief Architect for General Electric (GE) Industrial Internet Initiatives. Deep domain expertise in Edge-to-Cloud connectivity for IIoT and its global scale challenges. Wrote foreword for Francis’s book on Rethinking IoT.

■ 7.4 About Meshdynamics Technology

Our Experience base relevant to this proposal.


1 Radio Backhaul + AP
2-Radio Backhaul + AP
Single Channel Backhaul
Non-interfering channels
2-Radio 2-channel Backhaul Simultaneous Send/Receive
Structured Mesh™ proactively addresses radio interference/jamming.
To Ethernet link or WiMAX backhaul
ROOT
AP
Changing backhaul channels locally has no effect on rest of the network.
Service and Backhaul channels are both Dynamically (re) allocated to minimize channel interference effects.
P3M™ Hybrid Mesh Network
Isolated Networks Supported
Edge Node/ Single Radio Communications
Multi-radio Mobile Mesh Backhaul
Contiguous Physical Network
"Cloud's PN" OTN Back-haul
Isolated Clusters form Logically Contiguous Network via Cloud

Above: Technology field tested on SPAWAR and USAF AFRL contracts. Click on pics for more.

Meshdynamics' technology expertise includes multi-radio mesh networking, extremely lightweight Internet of Things (IoT) protocols for simple devices, and Software-Defined Networking capabilities for large networks. The company is focused on high-performance wireless networking for IoT and enterprise applications with substantial patented and patent-pending Intellectual Property. We bring value to Industrial OEMs with requirements for bringing IoT devices into larger enterprise networks coordinated with SDN, as well as Government agencies with security, monitoring, performance and surveillance needs for IoT devices at the edge of the network. Meshdynamics has licensing partnerships with OEMs, enterprises, and government agencies with requirements to integrate very large numbers of sensors, actuators, at the network edge. We are a UK, US and Canada government approved network equipment supplier. FIPS 140/2 certified. Related Links: Technology and Patents.

CAGE Code 47W66. UEI CM3KJEVQDV59. SBC 002491091. DUNS 603023537. EIN 46-1618665.
Work to be performed at Meshdynamics, by US citizens with Classified Clearances, as needed.

■ 8 CONCLUSIONS AND KEY CONJECTURES.

The only systems on earth that have ever scaled to the size and scope of the Internet of things are natural systems: pollen distribution, ant colonies, redwoods, and so on. This proposal outlines how Massive IoT may be achieved by rethinking last mile connectivity. Today's last mile is crippled by proprietary transport protocols, not scalable or sustainable.

Small, dumb, cheap and copious. Edge intelligence must provide data needed to address global scale challenges in Climate preparedness, agriculture and food supply, detecting forest fires, lifetime tracking of remote assets and cost effective Cloud driven predictive maintenance. The confluence of Distributed AI + SDN has prompted this shift to ***Cloud Orchestration Models***. Edge devices are imprinted by owners directly - no third parties needed. They form logically contiguous networks across previously walled garden boundaries. **Authenticated ground sensors address global scale challenges for our planet.**

Small. IPV6 is heavy– 40 bytes for the header alone. In sharp contrast, Nature's IoT messaging is light, **receiver-oriented** and self-classifying. Thus pollen is light so it can piggyback on available transports - wind, bees. It is receiver oriented - only intended recipients – flowers can decode the "message". **Distinguishable but Undecipherable. Innately Secure**. More Encryption optional.

Dumb. Edge to Cloud thinking focused on smarts at the radio end to manage collision avoidance by segmenting collision domains in RF space (channel diversity) and time (time reservation slots). IoT Radios are "smart" because they use phones and computers as their carrier pigeons to talk to clouds. Conversely, in Cloud to Edge thinking, we let the Cloud manage Ant-like intelligence at the Edge – purpose driven, limited processing power and cheap. The Edge can be small dumb and cheap. A modem costs 10 cents vs $20 for this WiFi radio. *And* CSMA/CA etc. are inherently inefficient . Heavy power usage and costs deter ***Copious*** use of densely populated sensor grids needed to detect forest fires, pollution etc. Related: Smart Dust.

Chirp protocols and their simplified hardware are **Cloud Managed** and thus cleanly cut through all Gordian knots shown here. Soft Chips are **imprinted** to send trusted Edge data as requested. They piggyback on ubiquitous intermittent connectivity to be -

Small.	Small Footprint, Ultra-Low Wireless Usage. Long Battery life. Simpler Processor.
Dumb.	Ant-like purpose driven processing capabilities - but re-programmable.
Cheap.	Intended to be produced in millions - since multi-purpose, multi-use., rechargeable.
Copious.	Intended to be used like Smart Dust – copiously spread over wide regions.
Secure.	Imprinting process is innately secure, End-to-End and zero trust required.
Organic.	No central standards needed. Chirp protocol easily extensible by Enterprise.
Agnostic.	Chirps are radio and protocol agnostic. Coexists with software handler.

Key Conjectures when thinking shifts from traditional Edge->Cloud paradigms 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 IoT – burgeons and with AI helps address our Globally Relevant Challenges.

Our Globally Relevant Challenges in Climate preparedness, Air and Ocean pollution, and verifying provenance chains are all indirectly based on asset or natural resource tracking and monitoring with wireless networks at the Edge. Small dumb cheap and copiously spread sensors are essential to collecting corroborated fine grain ground truth. Edge intelligence demands dense sensor grids to corroborate events in remote, harsh and hostile regions. This mandates ultra-low power use - long battery life or solar - and the ability to re-purpose IoT Edge behaviors through cloud driven imprinting and Cloud managed collision avoidance.

More details in this Chirp Primer. Thank you for your consideration. Your feedback is welcomed. Francis daCosta Jan 2024.

■ 9. REFERENCES.

Excerpts from Web Anchor (for Offline Viewing)

Links are references in the rationale behind Cloud-->Edge thinking and Soft Chip^{TM} embodiments.

A. How SDN and Distributed AI redefine thinking about Cloud->Edge Connectivity.

1. Glossary. for what is meant by Ants Chirps Edge Orchestration Pigeons Provenance etc.
2. One Page. Executive Summary. How low power Edge devices engender Massive IoT
3. Primer and Slides. Describes Reprogrammable Ant-like actionable Edge Intelligence
4. Soft Chips. Family of radio hardware and protocol agnostic multi-use sensor packages.

B. Previously Published on Rethinking the Internet of Things and related Blogs.

1. Small Dumb Cheap Copious Benefits of Massive IoT, Published 2016 PDF.
2. The Abstracted Network for the Industrial Internet Rationale for Cloud Driven SDN
3. Cloud Orchestration related FloodingAnimation.pdf & AnimationCollabScheduling.pdf
4. Rethinking-Internet-Of-Things-Book Also: Blog , Jolt Award , Amazon Reviews
5. Think like an Ant. See also deterministic finite automation. Purpose built machines

C. Exemplary Edge Ecosystems (Apple, Amazon) that could be extended to Global Scale.

1. Making 5G NR a reality. Qualcomm © 2018. See Fig. 3, Challenges of "Massive IoT"
2. Apple's Air tag. Operates in its trusted communities, see Also Gear Patrol article.
3. Amazon Sidewalk Trusted communities using TI chipsets for Sub 1GHz longer range
4. Amazon IoT Core Exemplary, potential, globally relevant PaaS service provider

D. Related to Security, Authentic Lifetime Provenance Chains ("Imprinting").

1. Zero trust Security Model. Business is war watered down. Now Globally Relevant.
2. Man in the Middle Attack, see also MAC Spoofing and Hidden Node Problem
3. Ground truth based on trusted sensors and corroborated PHY-PHY link connectivity.
4. How do MAC Spoofing Attacks Work, endemic to all MAC (UUID) based edge connectivity.
5. End to End Encryption See also Zero trust. Essential to military level security.
6. CHIPS Initiative - "*integral to America's economic and national security*".
7. Imprinting - as part of Cloud managed provenance chaining *PDF*
8. Provenance. Needed to establish or certify where natural resources came from.
9. Friend to Friend Networks See also Pub/Sub and Logically Contiguous Clouds.

E. COTS Available Technologies relevant to Soft Chips Data work flow paradigms.

1. Radio chirp data incorporated in an MQTT environment 433 MHz radio & Raspberry PI. *PDF*.
2. Software Defined Networking (SDN.) See also Distributed AI and Software Defined Radio.
3. Free RTOS. Exemplary Low power OS. Widely used. Minimal Version for Soft Chips
4. Comparing MQTT Brokers for the Industrial IoT (SCADA -> Pub/Sub -> Cloud Services.)
5. Top 15 SCADA Companies in the World (SCADA Solutions connect Edge IoT to the Cloud.)
6. 18 Wireless Modem Manufacturers in 2023 (Sensor -> Wireless Modem -> SCADA.)
7. Top-10-PaaS-providers-and-what-they-offer-you Platform as a Service (PaaS) Providers.
8. TI Low power Sensor controller (Video) and Sensor Controller Studio. Imprinting code.
9. Texas Instruments CC1125 low cost wireless modem, fractional dollar in volume.
10. Sub 1 GHZ Bands – (Longer range, Sparse RF, Cloud Managed.) Related: Sidewalk
11. Diversifying the IoT with Sub-1 GHz technology See also CC1310 MCU and Tutorial
12. UART: A Hardware Communication Protocol – extensible for diverse chirp protocols.
13. Radio-frequency identification (RFID). RFID++ in an active ID tag. See Provenance.
14. What is Pub/Sub Pub/Sub Messaging within Enterprises, see also MQTT, AWS IoT-Core
15. Service Level Agreement (SLA) Relevant to Networks for Logistic Supply chains.

F. Related to low power MAC based Radios and Protocols at the Edge

1. Inexpensive Low Data Rate Links for the Internet of Things. See Table at end
2. Low Power Wireless Technologies for Your Future Device Typical Selection Guide
3. Bluetooth 2.4GHz low range connectivity for smartphone supported radio protocols.
4. IPV6 Packet Header. Why IPV6 sender oriented messaging is heavy. See Also OSI
5. CSMA/CA OSI and DCF. Why MAC-based protocols are inherently inefficient and heavy.

6, Machine to Machine (M2M) Intentionally succinct and purpose driven. See Cryptic.

7. Radio Frequency Interference The core reasons for CSMA/CA OSI DCF and MAC.