Executive Summary

Preamble.

This presentation outlines the benefits of this active body of work for large OEMs, network equipment manufacturers, smart phone app developers, low cost/low power device manufactures, all of whom have a market share interest in "Massive IoT". I have contended this cannot be achieved without Nature's approach to "Chirp" messaging and how super-organisms (Ants, Bees) flourish. Blog post

My previous company, ACG, was contracted by the US Air Force and NIST to work on Supervised Autonomy for remote robots (telerobotics), see Technical Paper. When commercial radios became more affordable, ACG became Meshdynamics and we began work on robust real-time connectivity for remote military machines.

In 2002, SPAWAR/DARPA funded a multi-year NRE contract for us to develop a device/protocol agnostic mesh control layer for use on military gear- from tree-based mobile backhauls (802.11) to body area networks (802.15). We must also provide the transport for real time, terse, Non-IP "Stealth Chirps" securely over IP backbones. This Hybrid Mesh must provide time-sensitive bridging across both tree and non-tree sub networks, running proactive periodic "shuttle" services.

Rationale for "Chirp Networks".

Nature's messaging systems, like pollen, are Receiver-Oriented. It is openly published because only the intended subscribers (flowers) can decipher the code. Because it is so open, it is also lightweight and can use all available transports – e.g. wind, bees. But the message must reach recipient in spring or its useless. So Pollen floods the transports during Allergy season. Sender-oriented systems (IP) hate storms. And quasi-synchronous traffic is bothersome. More

As in Nature, digital versions of birds MUST "chirp" freely. "small data" flows are heard by all. And new events discovered : "the cat is now here". These digital versions also need "Big Data" supervisory loops- periodic north bound shuttles needed. "Massive IoT" needs a "Natural" approach. Sender-based, IP transport are neither suitable nor scalable. ZDNet Podcast

The Journey.

Taking cues from Nature, this work began with trees connecting to edge networks using a common mesh control layer. We used VOIP to emulate "Chirps" – terse and periodic not favored by IP, and hence the need for timed transport.

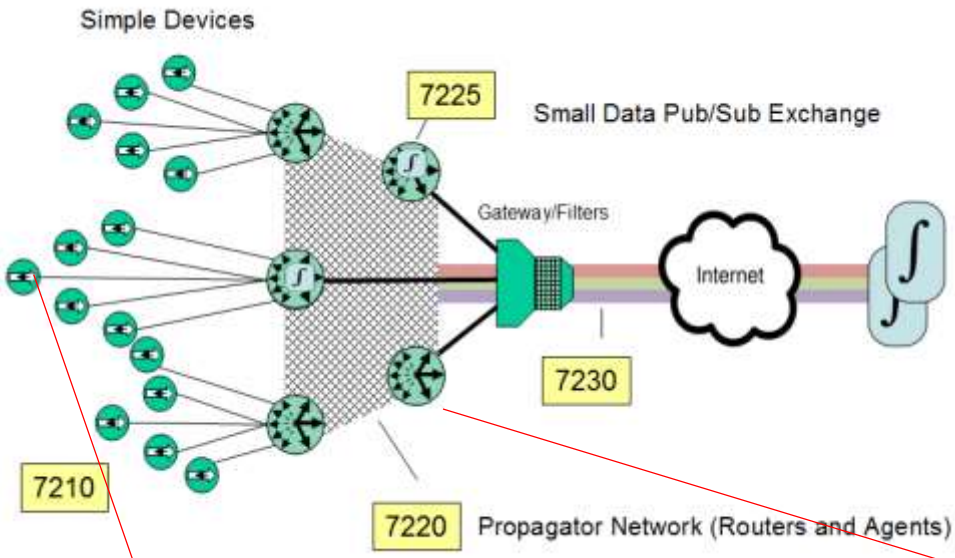
In 2012 I started the blog to reflect an alternate approach to the IOT hype. Intel sponsored the book. It received the 2014 Dr. Dobbs Jolt Award. The book moves on from trees to terse messaging by pollen, bees, ants and birds – "chirp protocols" and the work flow automation within collaborative chirp family ecosystems.

The patents cover essential facets of these emerging digital ant ecosystems and the machine control architectures they need.
My IP legal counsel is available to answer questions on issued patents listed here .
And, as always, your feedback and suggestions are welcomed. Thank you

Francis daCosta, Jan 2022 .

Podcast LinkedIn YouTube

Chirp Devices Are Already Here.



This Chirp life Is 14 days

This Mobile Propagator may publish its protocol on secure Non-IP Chirp Channels for trusted Chirp aware devices

No need for Round Trip

1. Sensor is applied

Most CGM sensors are tiny self-applied devices that sit partially beneath the skin.[1] They come with an inserter and have built-in adhesive to help them stick to your skin.[1]

2. Data is collected

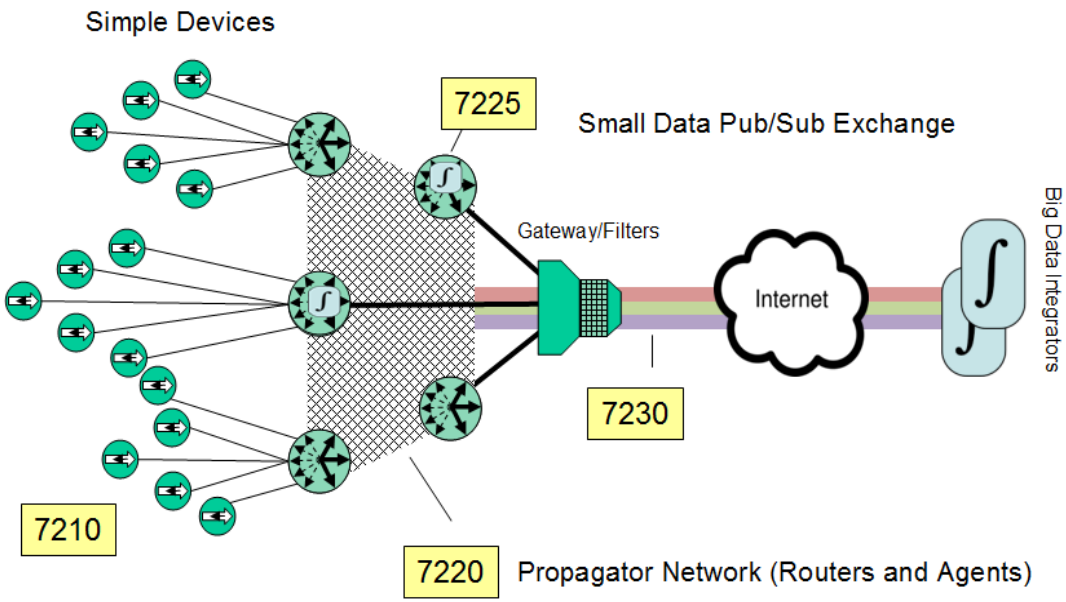
The sensor measures glucose levels at regular intervals and stores the readings.

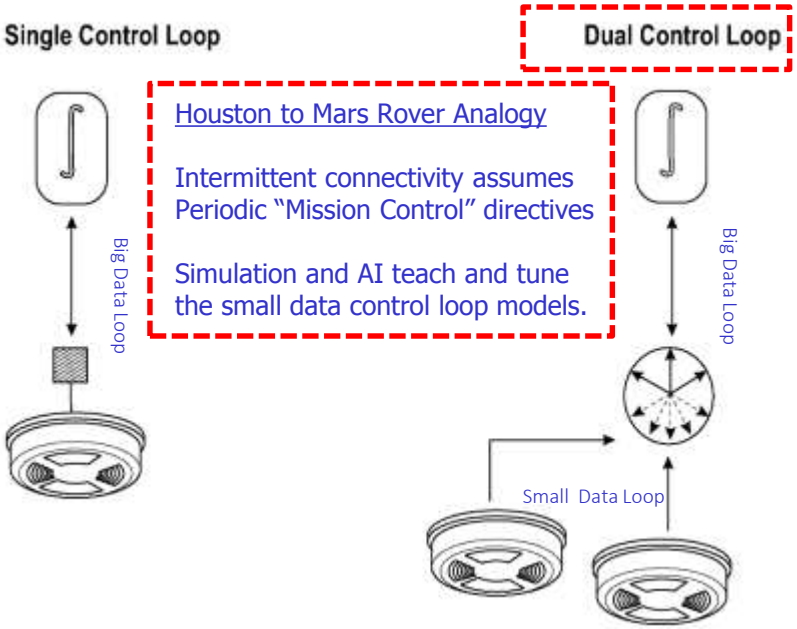
https://www.freestyle.abbott/us-en/what-is-cgm.html

3. Scan using a reader or smartphone[ll]

A handheld reader allows you to scan the glucose sensor to collect your information. You may be able to use a smartphone app[l] so that you don't have to carry around an extra device.

Chirp Devices, Propagators, Small Data (IoT), Dual Control Loops



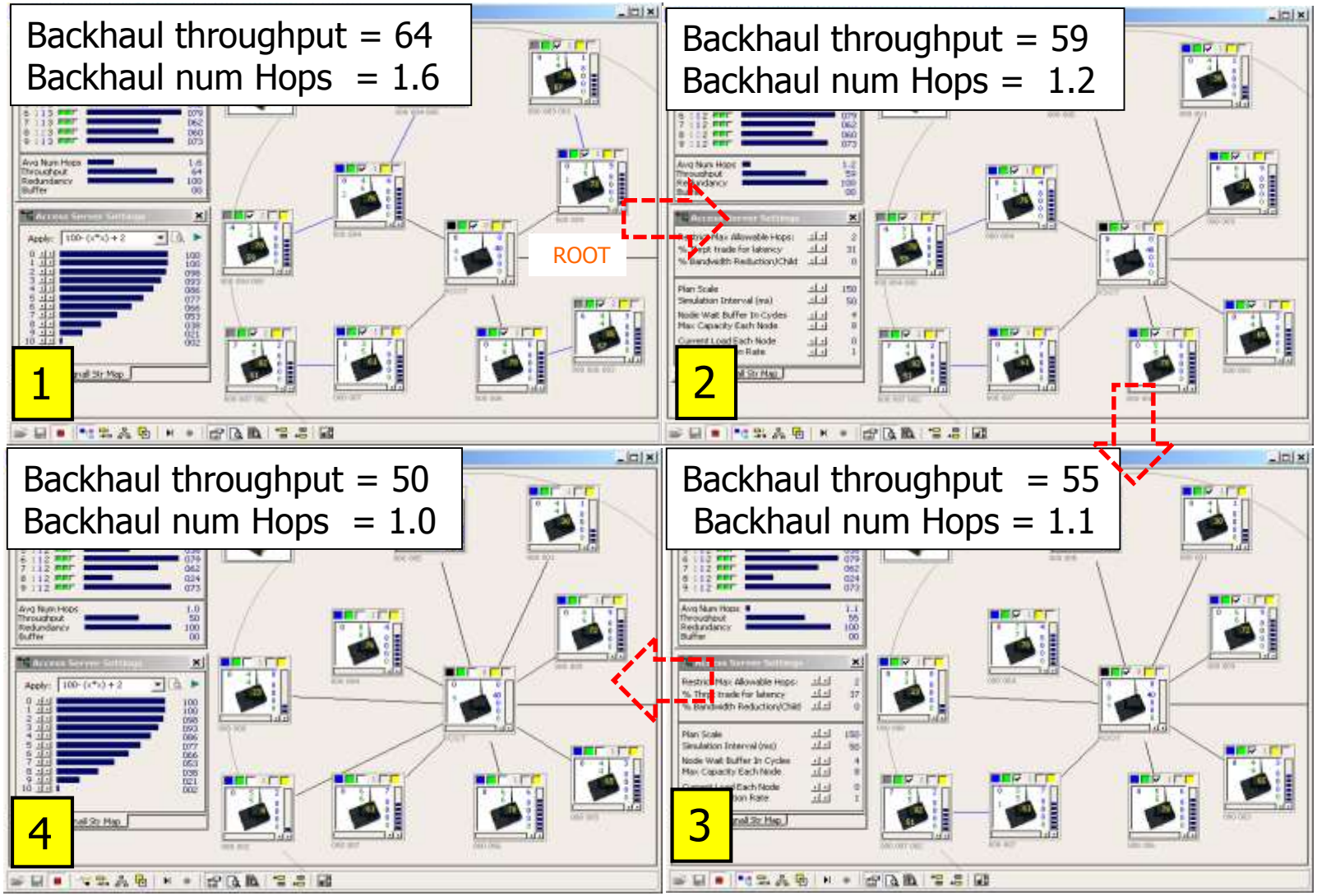


Patents: US8923186B1-chirp-networks.pdf
US9258765B1-chirp-networks.pdf
US9363651B1-chirp-networks.pdf
US9730100-terse-message-mesh-networks.pdf
US9819747-Chirp-networks.pdf
US10785316-Evolutionary-Wireless-Networks.pdf

"Meshdynamics' propagator node software allows us to deploy WiFi networks today with minimal additional wiring and also incorporate emerging Internet of Things devices on the same infrastructure today and in the future." Mr. Arai Yuji, GM, Communication Division, Sharp Electronics, Japan.

"Meshdynamics Scalable and Open Pub Sub enables us to rapidly integrate with Enterprise Class, OMG (Object Management Group)-approved, industry- standard messaging systems from RTI (Real-Time Innovations), PRISMTECH, OpenDDS, and others to provide assured real time end to end performance, even if we scale to billions of devices at the edge." Curtis Wright, Sr. Research Systems Engineer, Space and Navy Warfare Center.

Structured Mesh™ Self-tuning Topology



https://meshdynamics.com/documents/FloodingAnimation.pdf
Video https://www.youtube.com/watch?v=rrY7ExbWzws

Patents US 7,420,952 and US 8,462,747 and extensions for Mobility and Shuttle buses for small payload, periodic "Chirps".

Shuttle-Bus and Filter Services for Terse Messages (e.g. VOIP)

7150

7110

7130

Chirps to-and-from local devices

Buses to and from different integrator functions

Internet

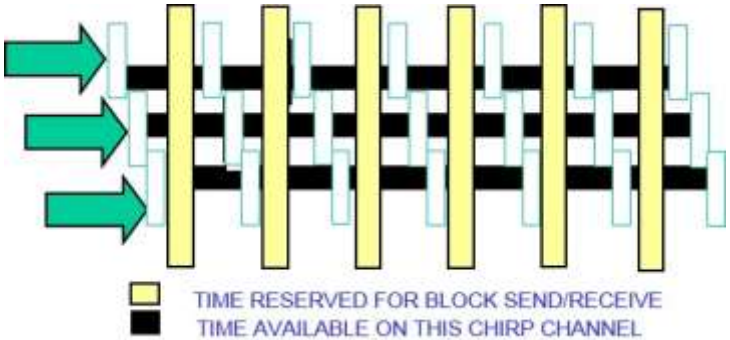
7140

7120

Buses to/from different Destinations

Propagator Node

Chirps unloaded, sorted, pruned, reloaded



https://meshdynamics.com/real-time-mesh-network.html
Patent Managing Jitter and Latency et el – See "Chirp Network" Patents.

https://meshdynamics.com/documents/Mesh-Dwgs-CollabScheduling.pdf
Patent Collaborative Logistics Ecosystem: An Extensible Framework for ..

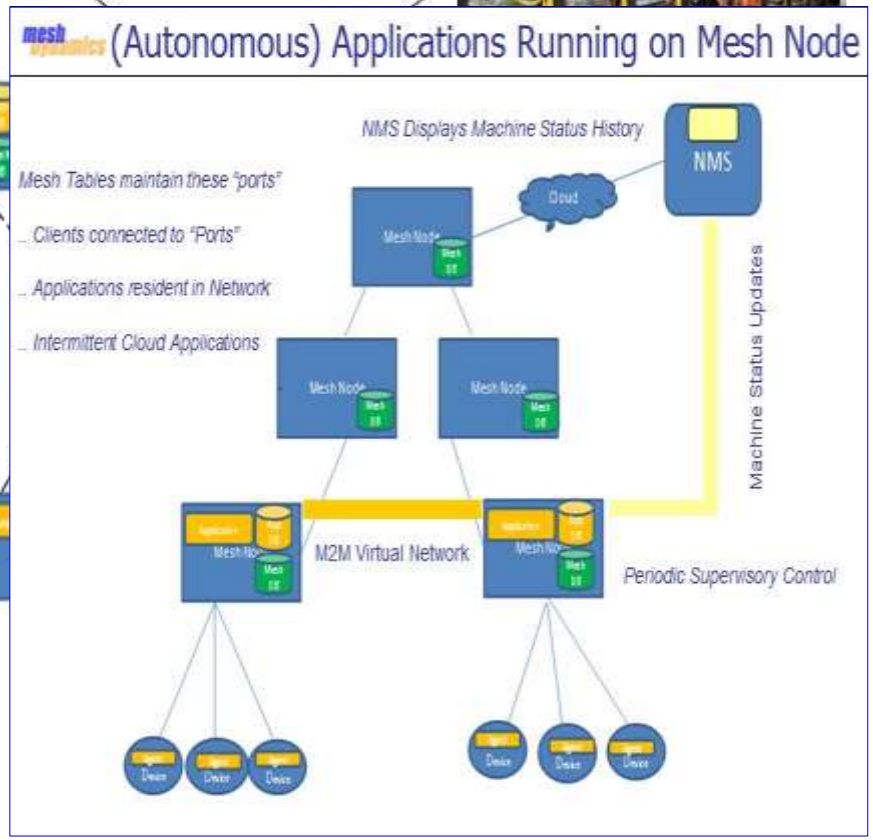
The Protocol Agnostic Network for IIoT

"I am talking to a secure IP-based SDN Aware Fabric"

https://meshdynamics.com/abstracted-network-for-industrial-internet.html

"I am talking to a Power Line

"I am talking to a PLC Controller



Evolutionary "Smart Networks"

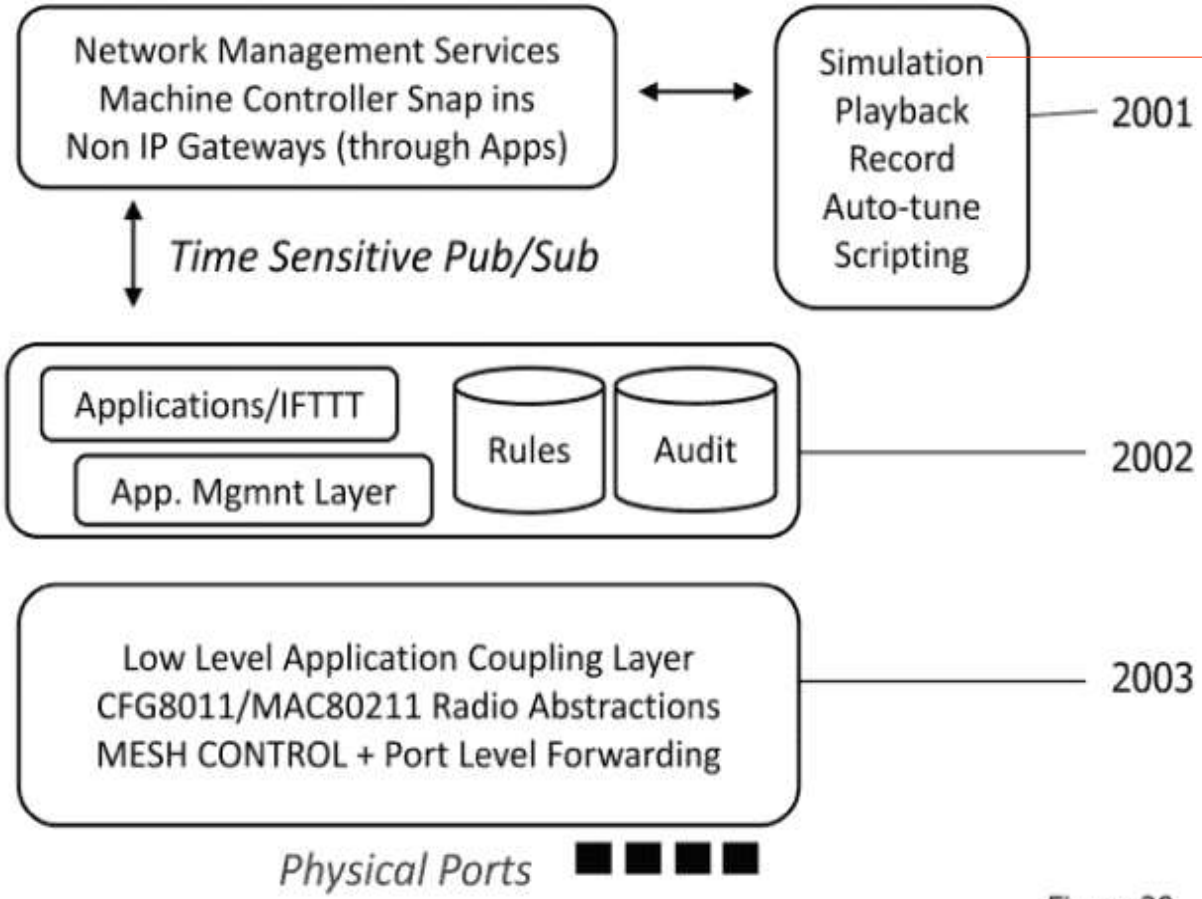
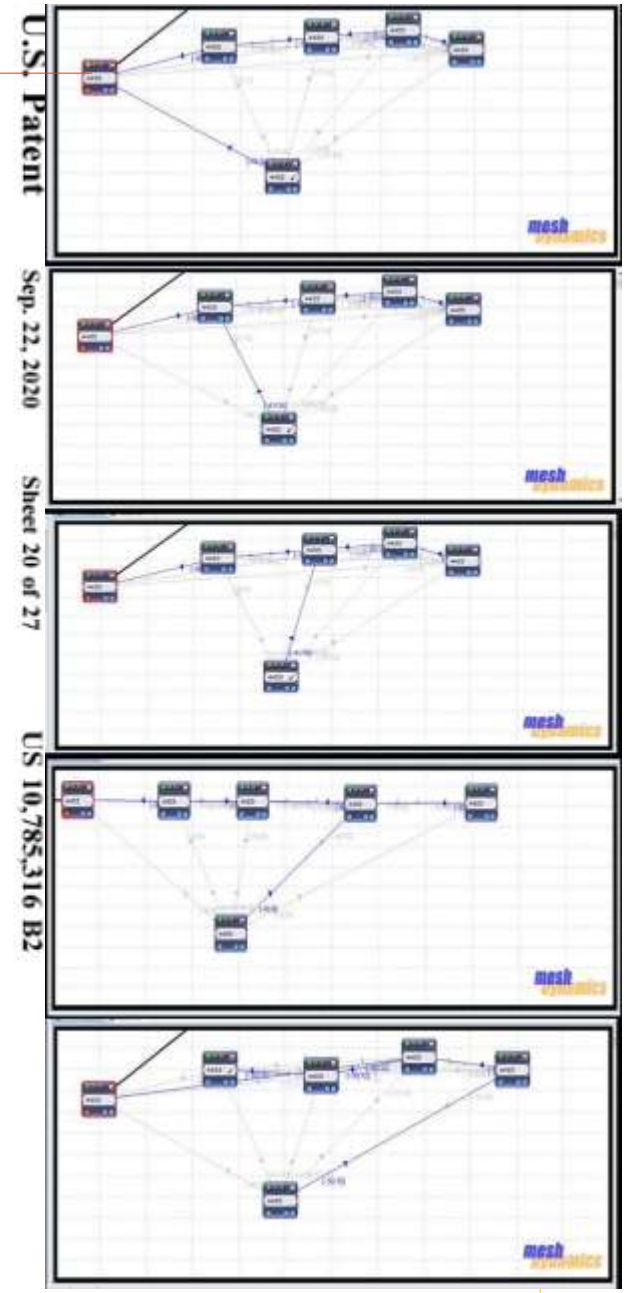


Figure 20



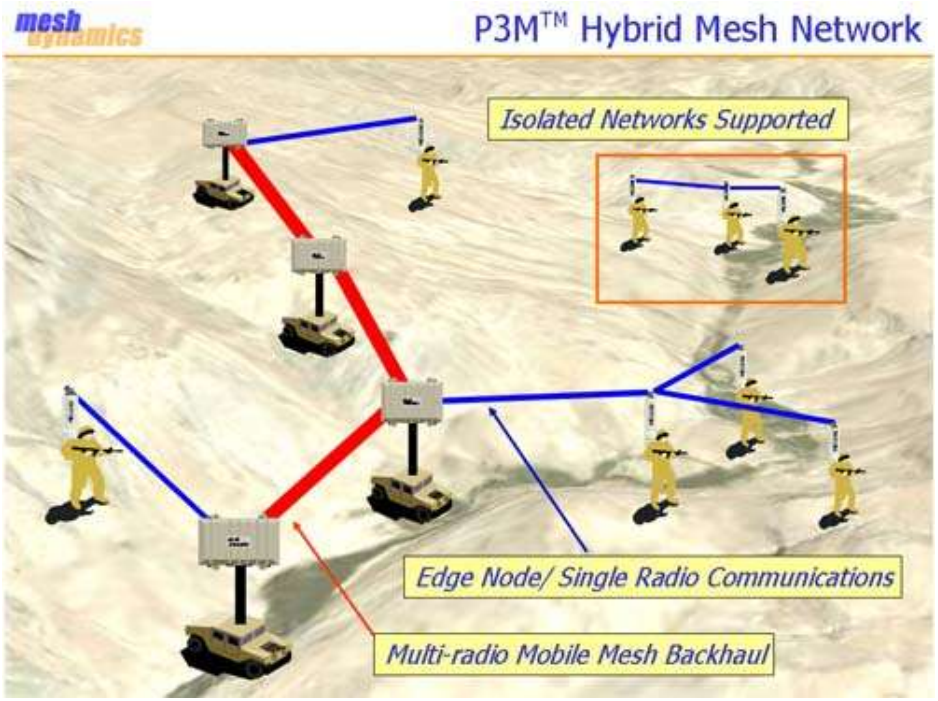
Abstracted-network-for-industrial-internet.html

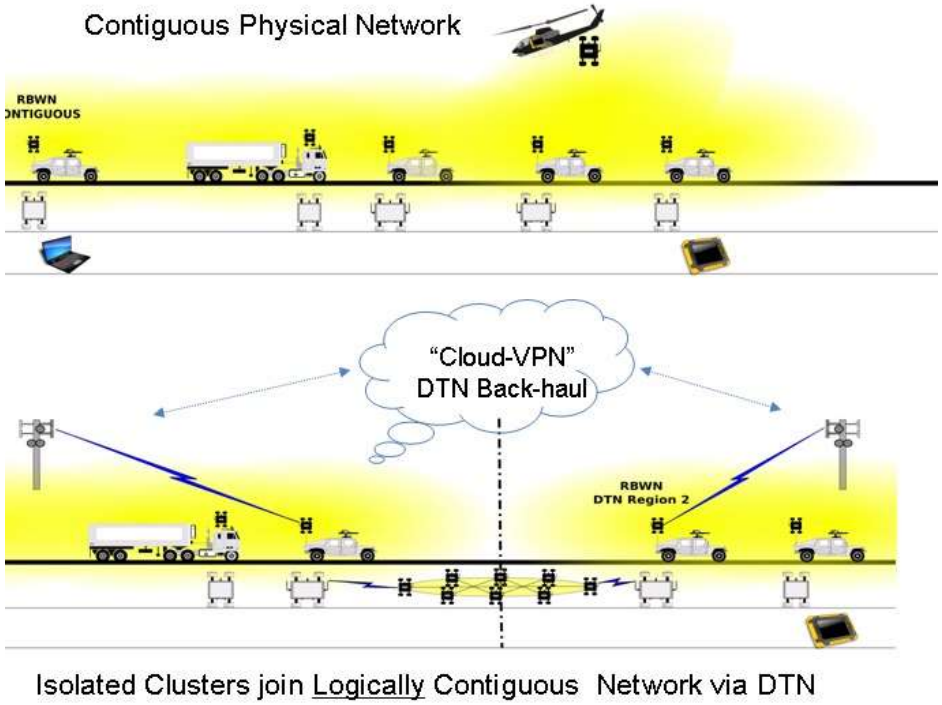
FloodingAnimation.pdf

Meshsuite/MD_Wifi_Sim_User_Guide.pdf

Patent Evolutionary Wireless Networks

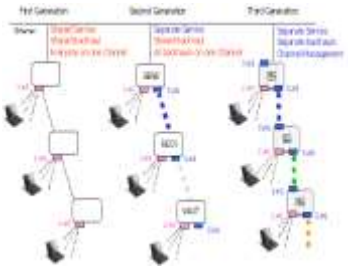
Mobility and Disruption Tolerance Extensions

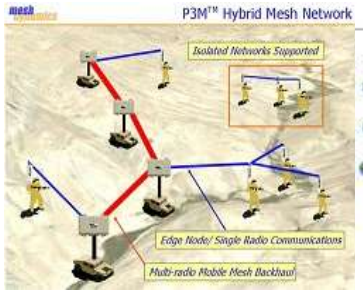


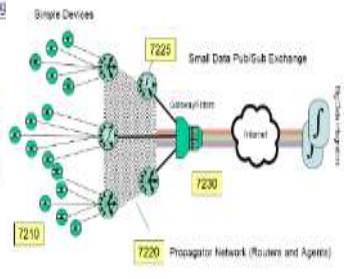


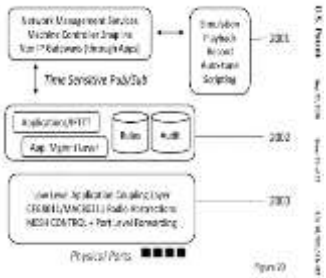
https://meshdynamics.com/military-mesh-networks.html
Video https://www.youtube.com/watch?v=I1prct6Xxzw
Patent Mobility Extensions for Wireless Multiple Radio Mesh

https://meshdynamics.com/abstracted-network-for-industrial-internet.html
https://meshdynamics.com/documents/MeshdynamicsDisruptionTolerantNetworks.pdf
Patent Evolutionary Wireless Networks









What is MeshsuiteTM ?

"Massive IoT" and 5G redefines "Wire-less" Mesh Networks

Existing Industrial Wi-Fi mesh networks bridge the gap from wired to wireless, providing last mile "edge" connectivity.

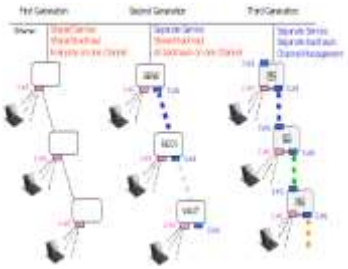
These Enterprise class wireless mesh networks must now support low latency bridging for 5G and "massive IoT".

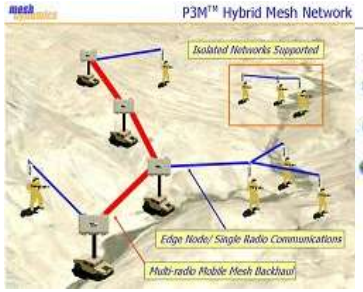
Cloud connectivity may be intermittent, mandating both local and remote control loops for the Industrial Internet.

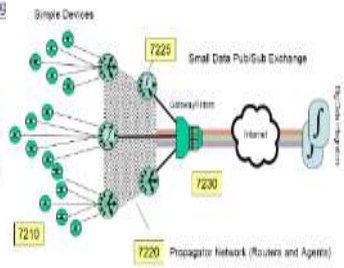
MeshSuiteTM is for OEMs building connected IoT aware devices/families/ecosystems

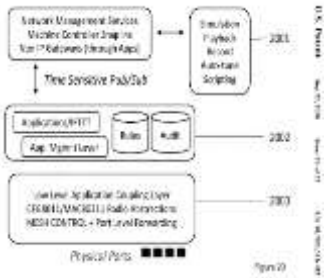
Our MeshSuiteTM IP and source code is useful to all tree-based mesh network equipment manufacturers. It includes

1. Our patented tree based radio backhaul and its embodiments
2. The mobility and low latency patented extensions developed for military mission critical applications.
3. IoT "Chirp" device integration as explained in the "Rethinking the Internet of Things" and multiple patents.
4. The Dual control loop for Industrial IoT as explained in "Evolutionary Networks" and its 3-tiered Architecture.
5. The Chirp protocols and its use to engender industry specific collaborations within Chirp family ecosystems.
6. Integrate Commercial AI tools to tune network topology, timing charts based on realistic simulations/ "experience".









Meshsuite™ enables "Massive IoT" Infrastructure

"Meshdynamics' propagator node software allows us to deploy WiFi networks today with minimal additional wiring and also incorporate emerging Internet of Things devices on the same infrastructure today and in the future." Mr. Arai Yuji, GM, Communication Division, Sharp Electronics, Japan.

SHARP

Sharp-QX-C300-Series-Press-Releases.pdf

Wireless Smart Network

Wireless Backhaul Access Point QX-C300 Series

for Japan domestic market

Suggested retail price: 335,000 JP Yen + tax

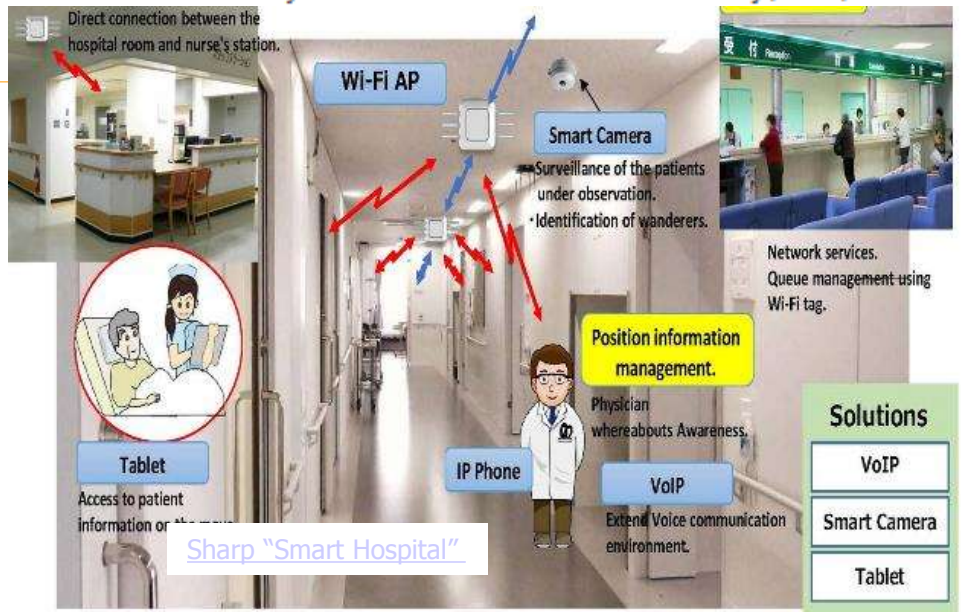
New information service will be implemented in smart network society by high-speed wireless LAN environment

■ **High-speed, Stable & Smooth Network Connection made possible by Wireless Backhaul Access Point**

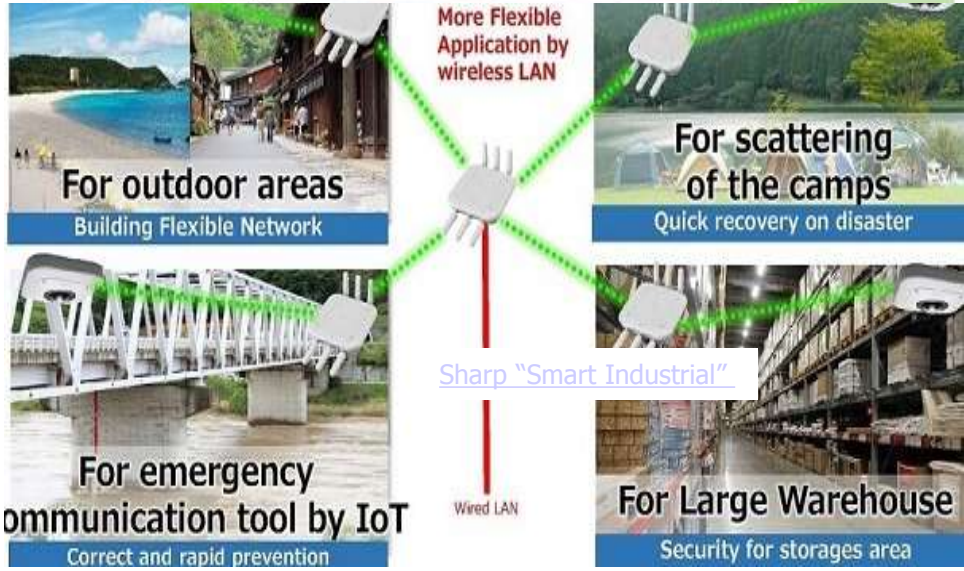
- IEEE802.11ac (3x3 MIMO), High-speed Data Transfer
- 1.3Gbps Link Speed (max): Approx 3X (max) speed of IEEE802.11n Access Point (*)
- 4.9GHz Model Available (Less Radio Wave Interference): Total of 4 models available to support customers use cases.
- Concurrent Connection: Up to 126 units per 1 Access Point
- Flexible Relocation and Extension of Access Points

(*) : theoretical value

http://www.sharp.co.jp/business/smartnetwork/products/qxc300.html



Sharp "Smart Hospital"



Sharp "Smart Industrial"

Foreword

Foreword, CTO GE's IIOT
Introduction
2014 Dr. Dobbs Jolt Award
Amazon Review (Leigh Chintz)
Net Of things (Blog)

With the rise of machines talking with machines in the Internet of Things, a new category of applications will demand evolutionary changes in the infrastructure of networks. Traditional networks were built to keep the enterprise at the center, resulting in star topologies and round-trip communications from edge devices to the servers at the center of the network. The Internet was similarly designed around information at the center of the network connected to people at the edges.

But machines are different from people, with different communications needs. Machines operate more independently in real-time and their actions affect the physical world immediately. Feedback and control of these local actions is critical for top performance and safety. Unlike the traditional end-to-end Internet, the Internet of Things must address these deterministic local control loops to insure business process reliability.

The different needs of machine communications can be seen in three aspects: real-time response, deterministic performance, and security and safety. All three aspects make demands on networking – closed control loops near the machines (to reduce latency), reduced costs of data transmission (in light of the rapidly expanding population of machines), and segregation of communications (to reduce noise and increase security).

With the increased number of devices and variety of applications, Metcalfe's Law is exploding with the number of new machines and the amount of data they generate. The only way for technology to keep up with the coming expansion of the Internet of Things is to manage the machine data flows differently from the way human application-oriented traffic has been handled with current protocols.

This book describes a critical new approach for the Internet of Things that makes it possible to extract meaning in context from the billions of new data sources that will emerge. This new approach recognizes the different demands of machine-to-machine networks and proposes an evolutionary three-tiered architecture to enable the next phase of the Internet.

Francis daCosta is distinctively qualified to develop this new IoT architecture. His diverse background in autonomous robotics, embedded systems, big data analysis, and wireless networking places him at the center of the all of the different technologies which must combine to address the Internet of Things. When Francis talks about communications realms, segregation of data streams, determinism, security, and control loops, I know that he is taking an innovative and disruptive approach in the evolutionary world of networks. This new architecture provides the urgently needed tools to address the expanding needs of the machines that join the physical world to the digital world in the Internet of Things.

Alok Batra
CEO, MQIdentity, Inc.
Former CTO & Chief Architect, GE Global Software Center, Industrial Internet Platform

Introduction

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 the machine social network (comprised of sensors and an unimaginable number of other devices) from the drag of human interaction, there is tremendous potential for creating autonomous communities of machines that require only occasional interaction with, 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 all of 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 of all sizes worldwide building moisture sensors, streetlights, and toasters lack the technical 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. ...(more)

Thanks!