The Rio-Las Vegas, Nevada

TMC MACHINE 2 MACHINE Evolution

Beyond traditional M2M to the IoT: Aggregating Disparate Data Protocols on the IoT

-Eshwar Pittampalli, Ph.D., Director, Market Development; OMA

August 11-14, 2014

Battle of the Platforms • Conference Sessions • Exhibit Hall

Outline

- Introduction
- OMA DM
- OMA LWM2M
- OMA GwMO
- Collaboration with oneM2M

Introduction

Beyond traditional M2M to the IoT: Aggregating Disparate Data Protocols* on the IoT

M2M to IoT- Connections:

- Device to Device (D2D)
- Device to Server (D2S)
- Server to Server (S2S)

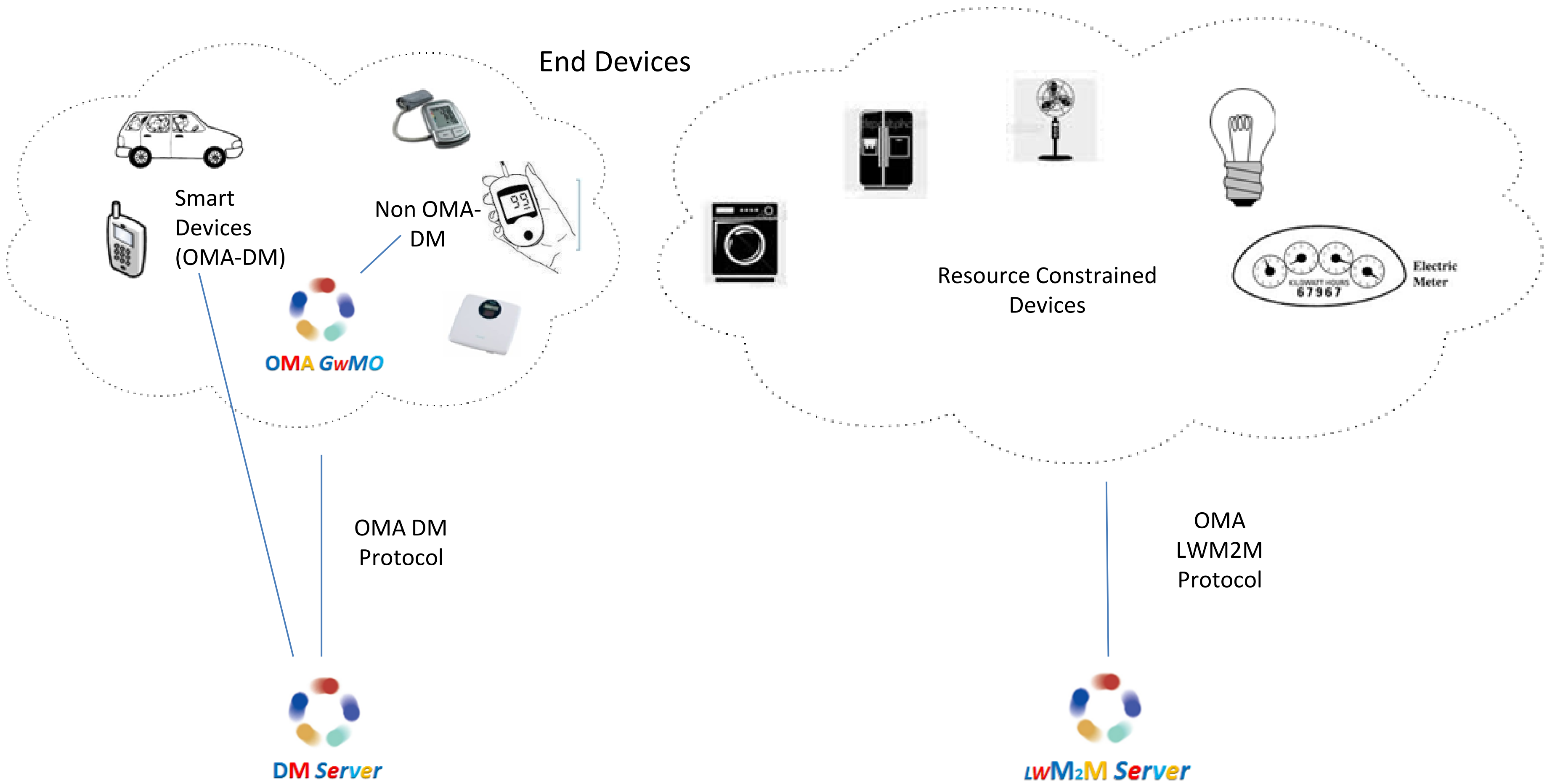
On top of this, if you add People (P), there are several more combinations

Disparate protocols - As a broad categorization of protocols, we see:

- OMA-DM/OMA LWM2M/MQTT/CoAP: a protocol for collecting device data and communicating it to servers (D2S)
- XMPP: connecting devices to people, a special case of the D2S
- DDS (Data Distribution Service): for integrating intelligent machines (D2D)
- AMQP (Advanced Message Queuing Protocol): connect servers (S2S)
- Others: UPnP DM, TR069, ZigBee, KNX, OpenWebNet, & Bluetooth), etc.

*6LowPAN, AllJoyn, BACnet, Bluetooth (including Bluetooth Low Energy), Cellular (including GSM/GPRS, W-CDMA, LTE), CoAP, Continua Health Alliance, DECT ULE, Eclipse Foundation, EnOcean, FI-WARE, GENIVI, HyperCat, LonWorks, M-Bus, MirrorLink, MQTT, OMA LightweightM2M, OneM2M, Open Interconnect Consortium (OIC), REST, Urban OS, Weightless, Wi-Fi, and Zigbee (and 802.15.4).

Aggregating Disparate Data Protocols on the IoT



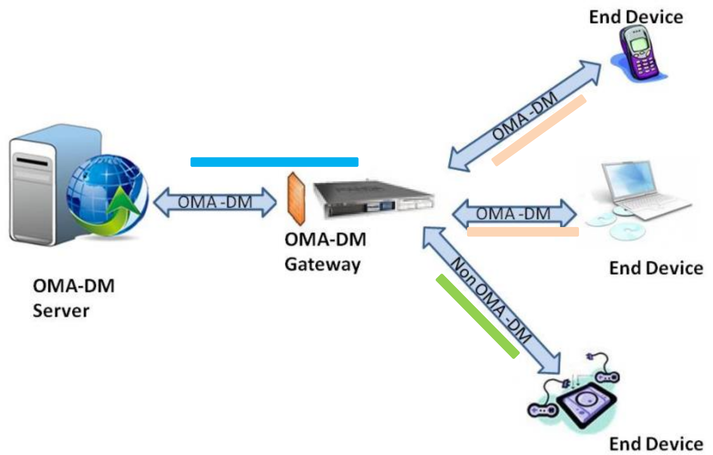
OMA-DM and OMA-LWM2M

- OMA DM
  - Enables device customization and services configuration remotely
  - Configuration and management is exposed in a Management Object(MO)within the Management Tree.
  - MO can be modified by DM Commands triggering of functional behavior in the device,
  - Examples include FUMO, SCOMO, etc.

- OMA LWM2M
  - Lightweight M2M is focused on constrained M2M devices, and is applicable to Cellular, 6LoWPAN, WiFi and ZigBee IP or any other IP based devices
  - Can be combined with existing DM offerings
  - OMA Lightweight M2M protocol supports both device management and service logic.

OMA DM Gateway Management Object (GwMO)-v1.1

- OMA DM GwMO (v1.0) provides a mechanism for OMA DM to manage devices indirectly, through a gateway, when:
  - Direct interaction between server and client is not possible
  - Device does not have a publicly routable address
  - Device may be sitting behind a firewall
  - Device supports a management protocol other than OMA-DM

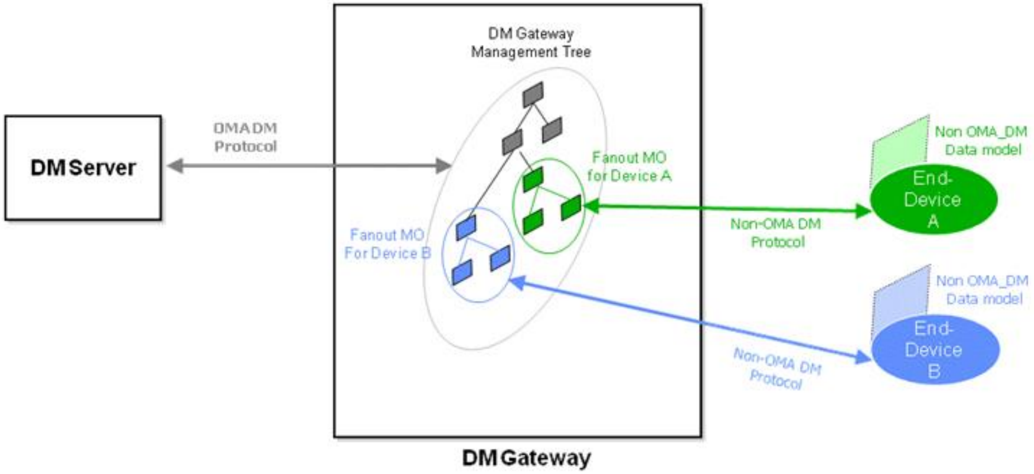


Three different supported modes:

- Transparent Mode: The DM Gateway assists the DM Server in sending a DM Notification to the End Device(s) behind the DM Gateway
- Proxy Mode: The DM Gateway manages End Device(s) behind the DM Gateway on behalf of the DM Server over DM protocol
- Adaptation Mode: Similar to the Proxy Mode with the difference that the DM Gateway manages End Device(s) behind the DM Gateway on behalf of the DM Server over non-OMA-DM protocols (such as UPnP DM, TR069, etc.)

DM Gateway Adaptation Mode

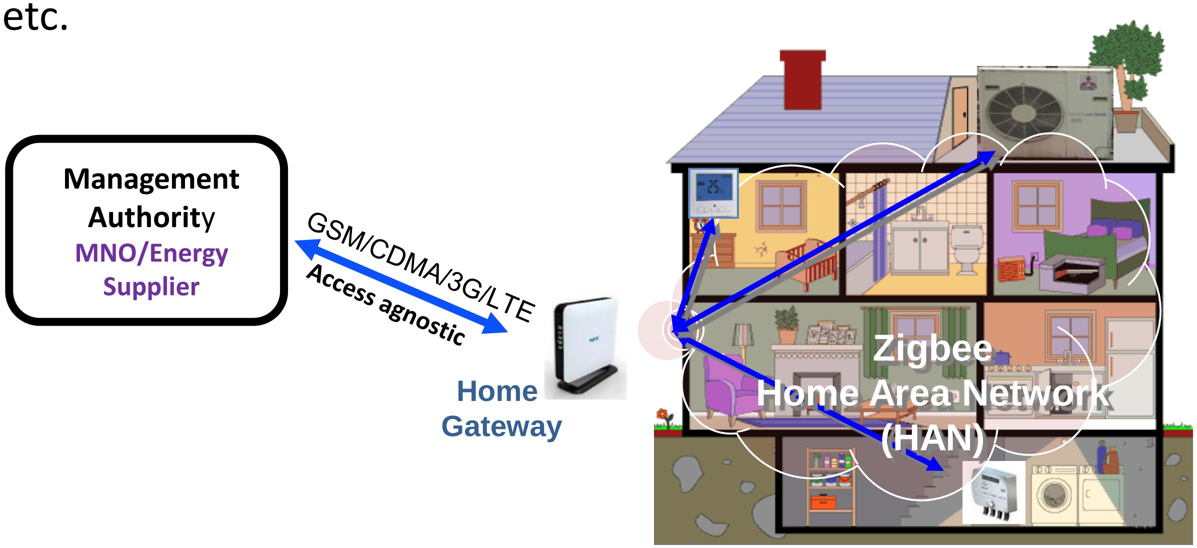
- Enables management of OMA DM and non-OMA DM devices behind a DM Gateway using OMA DM Server and DM Gateway pair.
- Adaptation functionality implemented in the management server or the Gateway.
- Existing OMA DM devices and new non-OMA DM devices can be easily and cost-effectively managed and provisioned by the Service Provider.
- Extend the use of OMA DM Server available in the Service Provider's network without additional installations or support or cost.



DM Gateway Adaptation Mode (Use case 1)

Device Management via DM Gateway

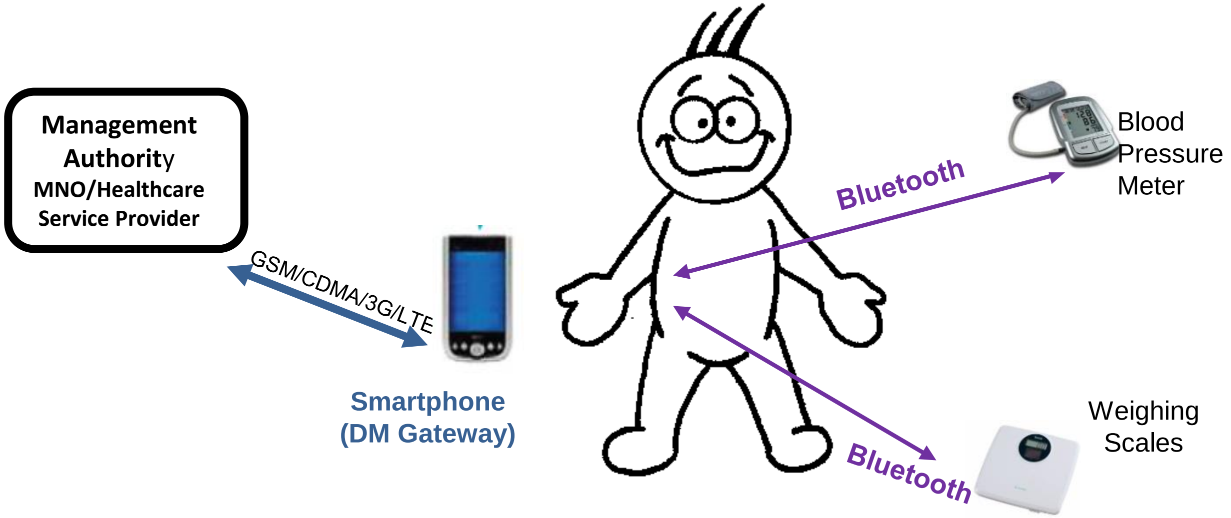
- A Zigbee Home Area Network (HAN) is composed of home appliances, e.g. Smart Meter, Air Conditioner, Programmable Communicating Thermostat (PCT)
- The Home Gateway with GSM/CDMA/3G/LTE connectivity acts as a DM Gateway. Note that many of GSM/CDMA/3G/LTE communication modules today implement OMA DM functionality.
- A Management Authority e.g. MNO or Energy Supplier configures remotely via DM protocols the HAN, then leverages that connection for demand-response, load-balancing, etc.



DM Gateway Adaptation Mode (Use case 2)

Continua (CHA/PCHA)-compliant Device Management via DM Gateway

- Some weight scales, Blood-Pressure Gauges which are compliant with Continua, transfer the data over Bluetooth (or USB, NFC) but these devices don't have GSM/CDMA /3G connectivity.
- A mobile handset with Bluetooth connectivity acts as a DM Gateway.
- A Management Authority (e.g. MNO or Health-care Service Provider) configures remotely via DM protocols the Bluetooth devices, then leverages that connection for diagnosis etc.



Collaboration with oneM2M

DM Collaboration – OMA & BBF

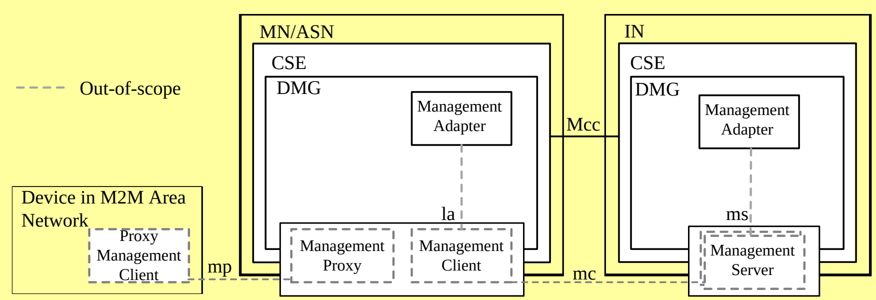
Group Name: WG5 - MAS
Source: Tim Carey, ALU, timothy.carey@alcatel-lucent.com
Meeting Date: 2013-09-30
Agenda Item: TP#7 MAS

Slide borrowed from: http://member.openmobilealliance.org/ftp/Public_documents/DM/2013/OMA-DM-2013-0112-INP_oneM2M_OMA_BBF_collaboration.zip

Collaboration between OMA &oneM2M- Not to add any more to existing disparate protocols

DM Collaboration – OMA & BBF

- **Discuss if we should begin to collaborate with OMA and BBF on DM Server Interaction**
  - **-Define a framework and requirements for the interaction between the M2M Service Layer and the Device Management Layer via the ms interface**



Slide borrowed from: http://member.openmobilealliance.org/ftp/Public_documents/DM/2013/OMA-DM-2013-0112-INP_oneM2M_OMA_BBF_collaboration.zip

Some of the questions investigated……….

1. How is a M2M Service Layer Session Established?
2. How does the DM Server Initiate Events to the M2M Service Layer?
3. How are resources discovered by the M2M Service Layer?

Summary

OMA is addressing:

- Smart end devices with OMA-DM new revisions
  - ✓ Gateway Management Object (GwMO) to support non OMA-DM protocol compliant devices
- Resource constrained devices with LWM2M
- Working in close cooperation with oneM2M to address evolving needs identified for various vertical applications

For more information, please contact me at epittampalli@omaorg.org
and visit our website: http://openmobilealliance.org/

Thank You!

Aggregating Disparate Data Protocols on the Industrial Internet of Things

Intelligent Network Connectivity

The Objective

Use data and information from (and beyond) the edge of networks to optimize utilization of assets and resources

Our customers face IoT challenges

- Market & Technology ***Fragmentation***
  - Hardware, software, protocols... all different, independent
  - Lack of integration…between devices, to enterprise systems
- M2M Development ***Complexity***
  - Many different skills required...
  - Hardware, Embedded, Software, IT, Telecom
  - No common architectural guidelines
  - Security risks
- Vendor ***Lock-In***
  - Proprietary SDKs, protocols
  - Device specific, application specific
- >85% of the billions of the forecasted new IIoT connections are existing devices & assets

Maturity model – a hill to climb

- Given the longevity of industrial assets, the bulk of the opportunity for the IIoT for the next 5-10 years hinges on finding economical models for connecting legacy devices
- Aggregated device volumes may be enormous, but individual projects vary widely in requirements
- These variables create cost challenges

Cost – Barrier to IIoT

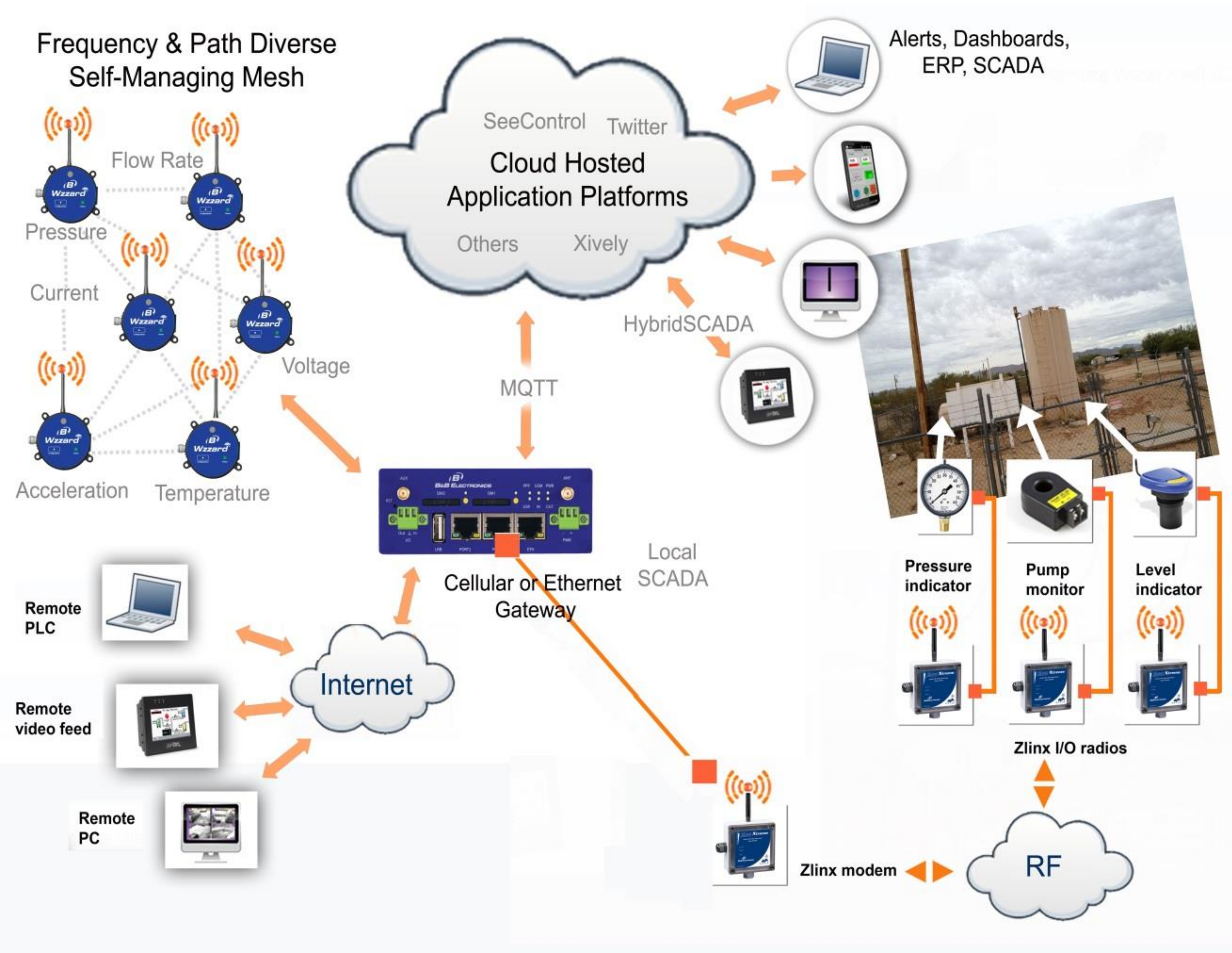
Rate of adoption constrained by our ability to reduce cost of solutions for legacy assets

- $ NRE – systems integration & application development
- $ COGs - Hardware cost for connectivity
- $ Installation cost
  - $ Physical installation, cabinets & wiring labor
  - $ Provisioning, support and troubleshooting costs, specialized labor
- $ Operations cost
  - $ Data plans
  - $ PaaS charges

Strategies for cost control

- Leverage high volume technologies
  - Ethernet, WiFi, Cellular, Bluetooth, mobile devices
- Overlay networks can be more cost-effective than adapting existing devices
- Design out installation costs
  - Mminimize both labor *and* skillsets required in the field
- Minimize operational costs
  - Intelligent Gateway-centric architectures
  - Lowest cost backhaul solutions, failover to higher cost
  - Intelligence at the edge - actionable information not raw data

Gateway-centric architecture



Intelligence at the edge - concepts

- Intelligent gateways backhaul via lowest cost connectivity path with failover to secondary networks
- Sensor networks that aggregate many data points through single gateways
- Applications hosted at the edge
  - Push filtering and decision-making to edge devices
  - Minimize bandwidth, power and data storage requirements
  - Most data isn't useful or even interesting - teach edge devices what is interesting
- Backhaul with scalable, efficient "IoT" type protocols vs. traditional SCADA. Pub-sub vs. client-server
- Security – extend system security design out to edge devices

Summary

- First generation of the IIoT will be dominated by existing assets
- Total Cost of Ownership of solutions is the largest factor influencing adoption rate
- Scalable, standardized platforms for hardware, middleware and applications are key to reducing TCO and speeding adoption of IIoT solutions

Thank you

Mike Fahrion
Director of New Product Development
B&B Electronics
(815) 434-8715
mfahrion@bb-elec.com

Intelligent Network Connectivity

The Rio-Las Vegas, Nevada

TMC

MACHINE M2M MACHINE Evolution

Conference & EXPO

August 11-14, 2014

Battle of the Platforms • Conference Sessions • Exhibit Hall

Connect with us
#M2MEvolution
@M2MEvolution

www.m2mevolutionexpo.com

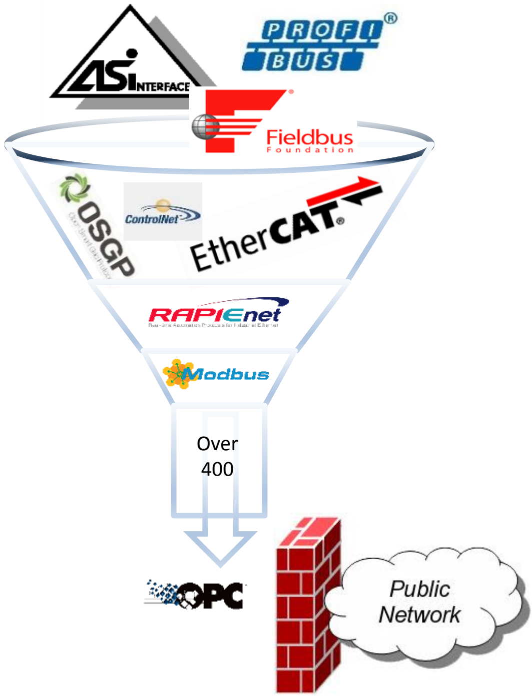
Aggregating Disparate Data Protocols on the Internet of Things

Xavier Mesrobian

VP Sales and Marketing Skkynet Cloud Systems

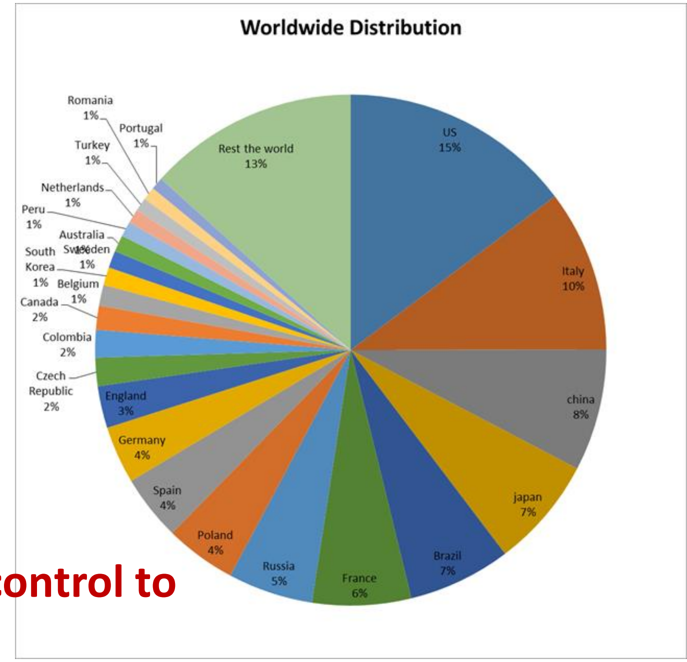
Networks of Things

- Industrial systems have been using networks of “things” since the 1970’s
  - PLCs
  - Direct I/O
  - Specialized protocols and networks
  - Local and centrally managed networks
  - High tag counts
  - High update rates
    - Not uncommon to see sub 1 ms updates
  - Low security requirements
    - The network is trusted, the devices are trusted



Networks of Things

- Manufacturing and Resources = 14.03M companies alone
  - 2015 IOT Industrial sector is projected to be $1.6T
  - 14M unique Implementations
  - 1.4M different hardware suppliers



The challenge = extend what we've learned in industrial control to networks that span the globe.

Internet of Things

- Unlike an industrial network
  - No central management – *things and networks are owned and operated by people or companies who are not acquainted*
  - There is a Strong security requirement
    - Jan 2014 Hackers gain 'full control' of critical SCADA systems Over 60,000 exposed control systems found online
    - Jan 2014 - Your Fridge is Full of SPAM: Proof of An IoT-driven Attack Over 750,000 messages came from IOT
    - May 2014 - DHS Confirms U.S. Public Utility's Control System Was Hacked Two separate incidents
    - July 2014 - Dragonfly hackers target 1000 Western energy firms, industrial control systems
    - …
  - Unreliable, relatively slow network (Internet)
  - No agreement on hardware communication protocols
  - Traditional server/client (master/slave) communication not appropriate (e.g., OPC)
  - Data aggregation and protocol conversion is key

Internet of Things

- Like an industrial network
  - Latency is crucial - improvements are non-linear
    - At some point a change in degree becomes a change in kind
    - When data latencies approach network propagation speeds, the Internet of Things changes from a reporting mechanism to a control mechanism. Process dynamics become visible.
  - Data can be modeled as (name,value,time) tuples (tags)
  - Need to support systems with tens of thousands of tags
  - Hardware from different manufacturers need to interoperate
  - Yet, existing capital equipment needs to be preserved and incorporated into the IoT to reach 14M companies

Little Things

- Limited resources
  - Tiny embedded devices – e.g., 64K RAM, no MMU, no FPU, no operating system
  - Small embedded devices – e.g., 8 MB RAM, no MMU, no FPU, uClinux O/S
  - Large embedded devices – e.g., 2 GB RAM, Intel or ARM, Embedded XP, Linux, QNX, etc.
- Dedicated application
- Proprietary data format
- Small tag count
- Low data rates

Big Things

- Effectively unlimited resources
  - PC, PLC, DCS
  - Choice of memory, CPU
- Standard or proprietary data formats
  - Usually convertible to standards like OPC
- Large tag counts
- High data rates





Data Aggregation

- Where do we do aggregation?
  - Hub systems in the cloud
- The hub system does not need to speak all protocols
  - Hub systems should speak one abstract protocol
  - Hub systems should not access the "things" – the "things" should access the hub.
    - Things should never offer an open port to the Internet
    - This principle disqualifies industrial protocols like OPC, Modbus
  - Convert-at-source is simpler – the "things" convert their data to the hub's abstract protocol before transmission, and convert from abstract protocol to private protocol on reception.

Data Aggregation (Protocol)

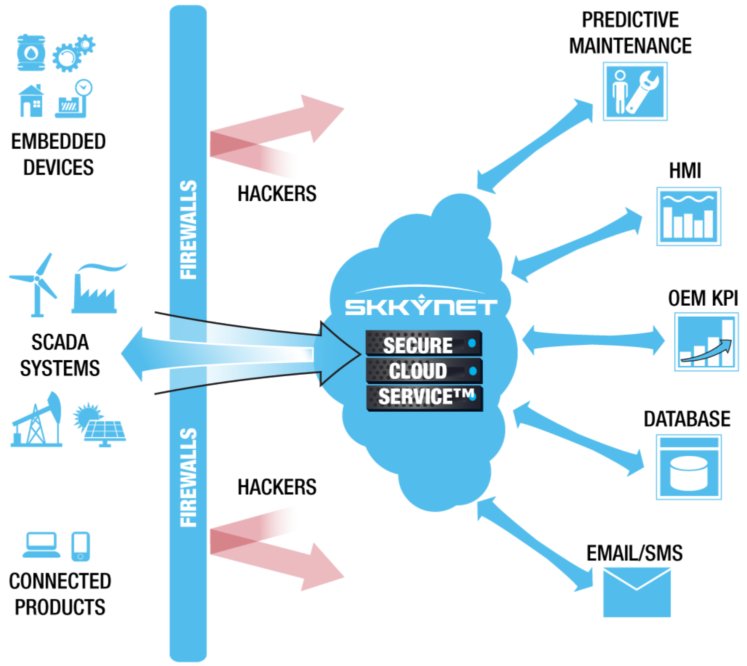
- Abstract data protocol must be simple
  - Suitable for tiny devices with <64 K RAM
  - Not dependent on bit/byte order or CPU architecture – ASCII
  - Simple to construct and parse with minimal CPU load
  - Low packet overhead
  - Streamable
  - Transport agnostic

Data Aggregation (Connection)

- The Internet is built on TCP – so must be the IoT
- Corporate security concerns
  - limit TCP ports, introduce outbound proxies and inbound firewalls
  - In reality, most TCP solutions will fail
- Forward-looking solution is WebSockets
  - Modern proxies can forward a WebSocket connection
  - WebSocket implementation can fit in 64K of RAM

About Skkynet Cloud Systems

- Available today
  - Provides real-time monitoring, supervisory control with no additional hardware, no VPN
  - No open firewall ports = No attack surface
  - Connects to industrial systems
    - Using open standard protocols (TCP, OPC,…)
  - ETK is available for qualified partners, with no run-time royalties or fees
    - Supports Linux, uClinux and TRON to name a few
    - Hosts on virtually any CPU, including resource-constrained MPUs with no floating point or MMU support.
    - ETK optionally supports IPV6, SSL, WebSockets and a built-in scripting language, allowing you to tailor the ETK to your application and the resources available.
    - The ETK manages a single data set while allowing multiple inbound and outbound connections, allowing multiple clients connected directly to the embedded device without the need for a gateway.
  - Includes a full featured Web-based HMI



Come see us at Booth 714

Thank You

Xavier Mesrobian

xavier.mesrobian@Skkynet.com

Booth 714