CREATING THE VALUE PROPOSITION FOR MSO AND CONSUMER ALIKE IN THE MORE CONNECTED HOME – A GUIDEBOOK TO SUCCESS

Mark Francisco, Comcast Cable
Charles Cheevers, ARRIS

Abstract

The even more connected home is quickly becoming a reality. Much has been discussed about the rise in the number of connected devices in the home to increase from 10 today (on average); to 40 in five years with more than 40 billion connected devices on the planet.

Yet, we have seen the slow progress to mass adoption of home automation, Home Control, home security, and other home connectivity solutions. Why is this stuck and how can it be unstuck to gain a more saturated deployment level of 80% of US homes with one or more new connected home devices?

This paper takes a look at the following key elements in this growing and important area:

- *The current status of technology enablers and how technology can move the needle now to help the overall value proposition*
- *The key technical building blocks required to create an MSO led Internet of Things (IoT) architecture and unify much of the elements of the connected home*
- *The importance of simplicity and curation of the service in this area – and the pros and cons of Do it Yourself (DIY) vs. Managed Connected Home/IoT services*
- *Standards and proprietary solutions – how they intermix and can there be only one or does the MSO have to look at embracing and adding value to the Do it Yourself devices?*
- *The Value and Cost equation with a close look at Effort and Cost vs. Return – why some of the current approaches to getting consumers to spend more of their money on these lifestyle, comfort, or convenience solutions don't work and how to focus on the value returns that do work*

THE INEVITABLE PROGRESSION TO A MORE CONNECTED LIFESTYLE

We are entering the "peak of inflated expectations" for the Internet of Things where there is a huge expectation that we are moving towards a world of more automation of tasks and lifestyle through connected smart devices that can be united together to provide a relevant and important new task that improves costs, efficiency, people's lives or in some cases makes the task completely transparent to the beneficiary.

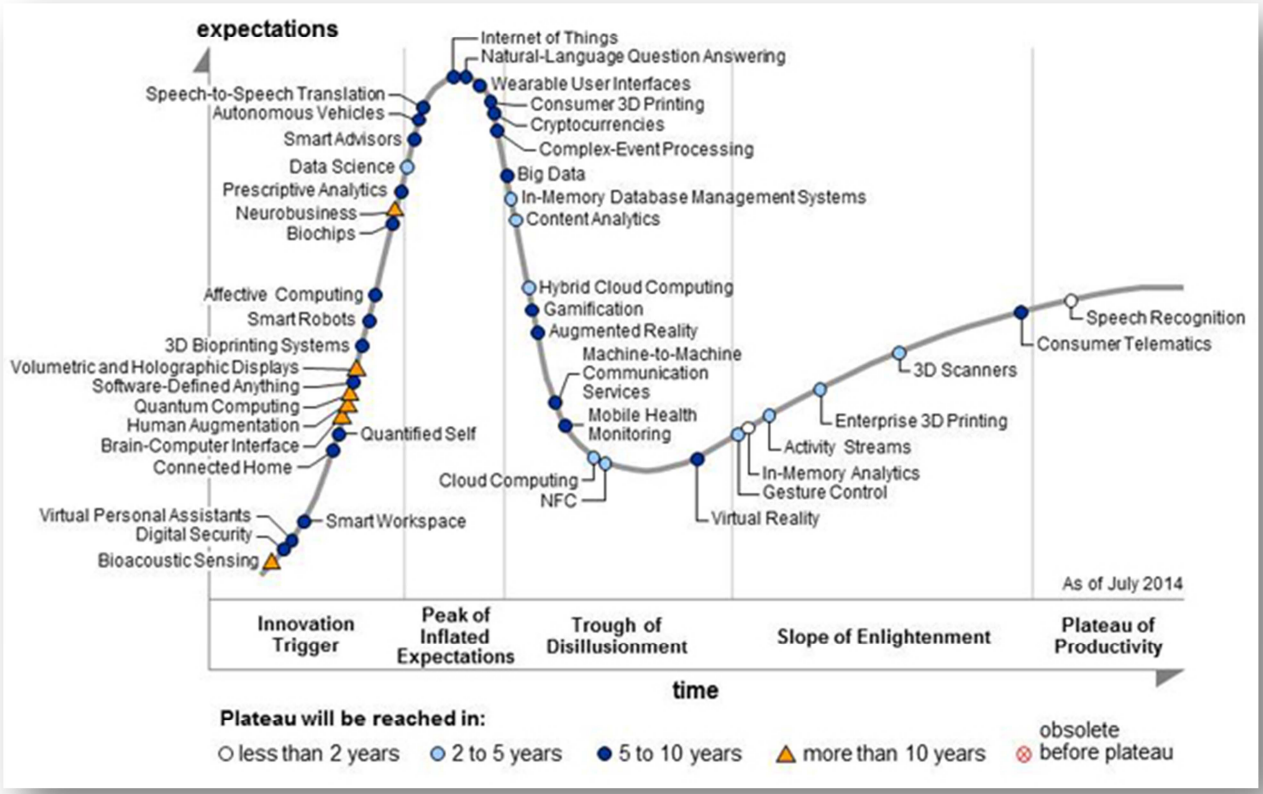

Figure 1 – Gartner's 2014 Hype Curve

We see new connected devices emerge daily ranging from the connected 'fork' to the myriad of wearable devices that record all facets of someone's health and exercise habits.

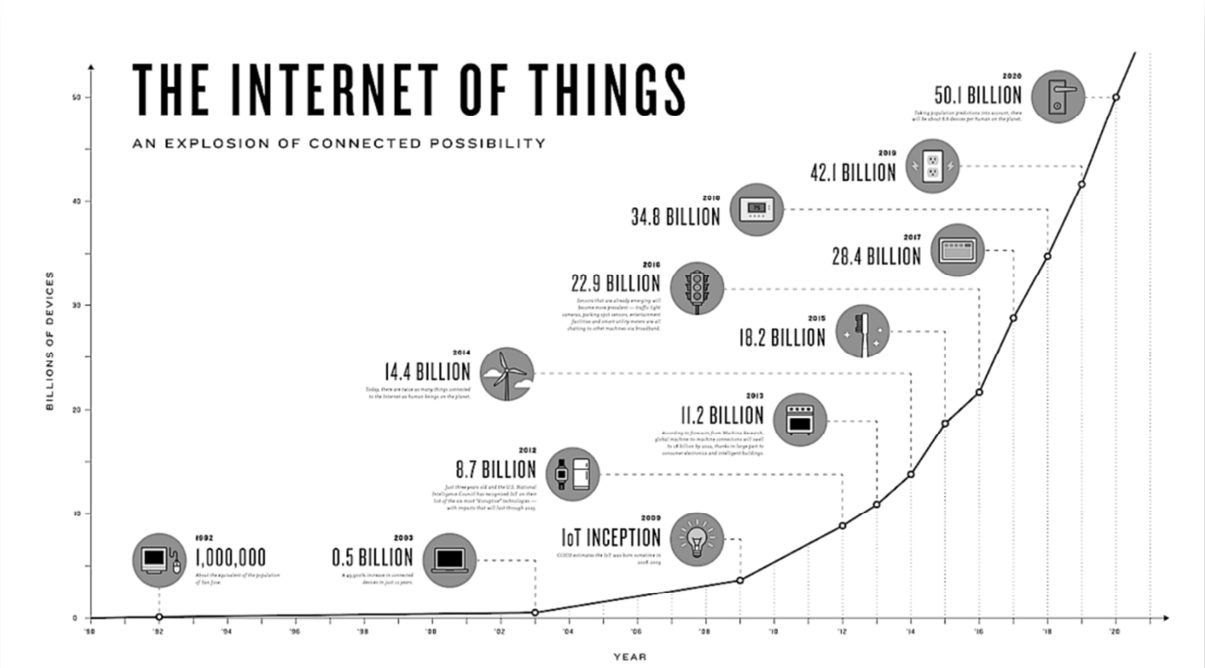

Figure 2 – The projected connected devices curve

There is also critical momentum in a number of areas that shows that the technology is readying to enable the next phase of IoT driven services. These technology pillars include:

- Effective price points at scale for wireless technologies and silicon development with attractive processing power and energy consumption
- Sensor technology and harvesting energy solutions allowing wireless sensors to become more ubiquitous in the home and city environment
- Protocol standards emerging to unite the application space for connected devices
- Cloud-to-Home architectures that can also provide low latency communication for home applications
- Smartphone applications that can drive IoT interaction and provide simple dashboard to monitor or trigger events
- Data analytics and intuitive rules engines for value to consumer, retailer and service provider

There is also a desire in the services sector to leverage the increase in connectivity and connected device to increase their visibility to the consumer or provide Business-to-Consumer (B2C) or Business-to-Business-to-Consumer (B2B2C) services through direct connectivity or Cloud-to-Cloud exchanges.

Typical areas include:

- Energy Management
- Water, Gas and Utility Management
- Medical and Health Management
- Insurance and Wealth Management
- Security and Automation
- Education
- And others

These areas funnel existing spend into the IoT derived services or in some cases generate new sources of income.

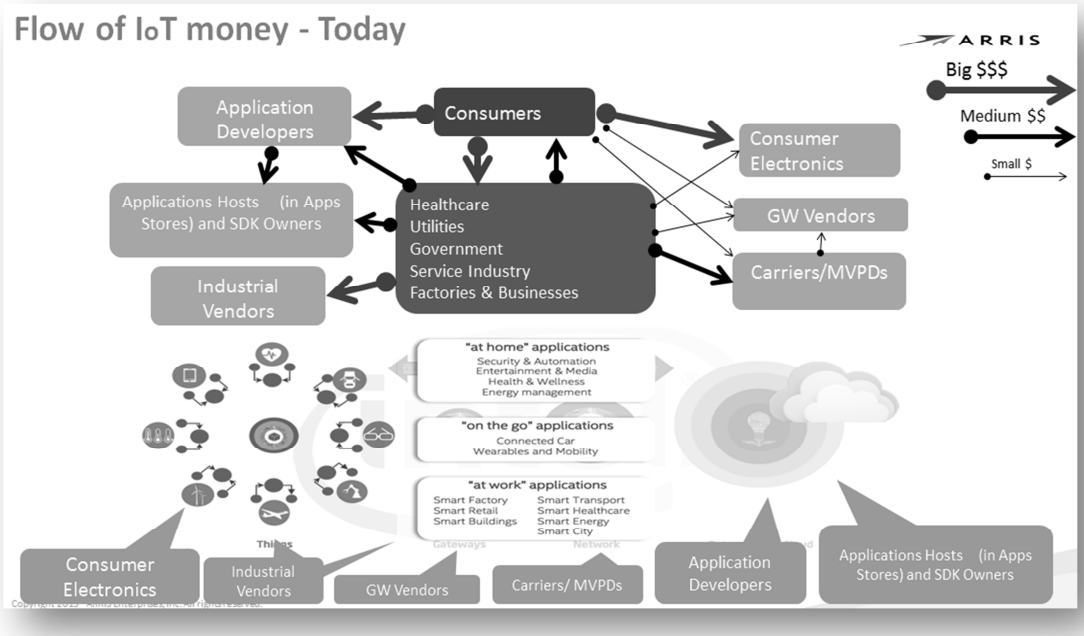

Figure 3 – The flow of money in the IoT ecosystem

There are several macro segments of IoT derived revenue:

- Industrial and Machine-to-Machine
- Smart Cities
- Wearables
- Medical
- And many, many more…

The above segments account for over 66% of the estimated five-year revenue of $5 billion globally. However, the connected home segment is the sweet spot for the MSO and one where the projected revenue in 5 years is about $2 billion of which Smart Energy and Home Security services account for about $1.8 billion of the total.

It's clear that the MSO cannot ignore this trend of connecting more and more devices in the home. Rather than let it just be a burden on the connectivity infrastructure that the MSO has invested in – it seems that there is real opportunity to drive new revenue opportunities from onboarding these new devices and creating value-add elements in the connectivity and service ecosystem.

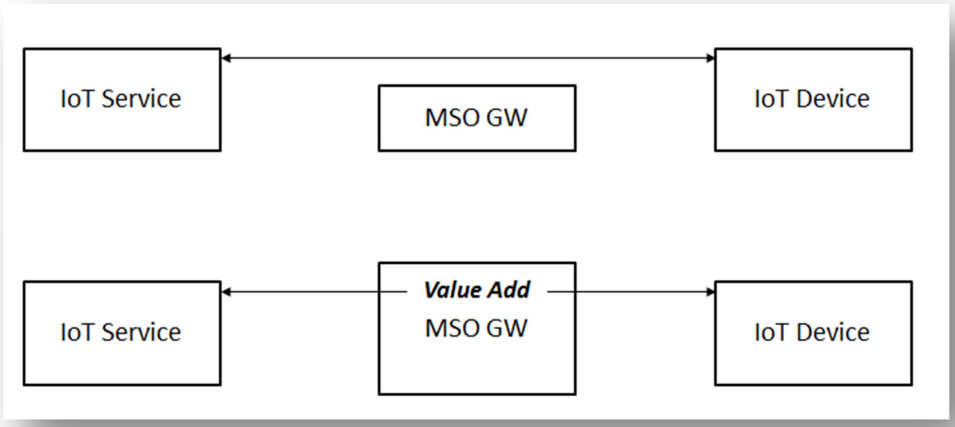

Figure 4 – Creating MSO value-add demarcation to IOT services

This value-add insertion in the IoT service chain is something that the MSO can achieve for many services that could otherwise run Over-the-Top (OTT) from IoT service providers to the MSO's own customer. The remainder of this paper will suggest the path forward for an MSO to evolve a revenue generating position in this growth area of connected things.

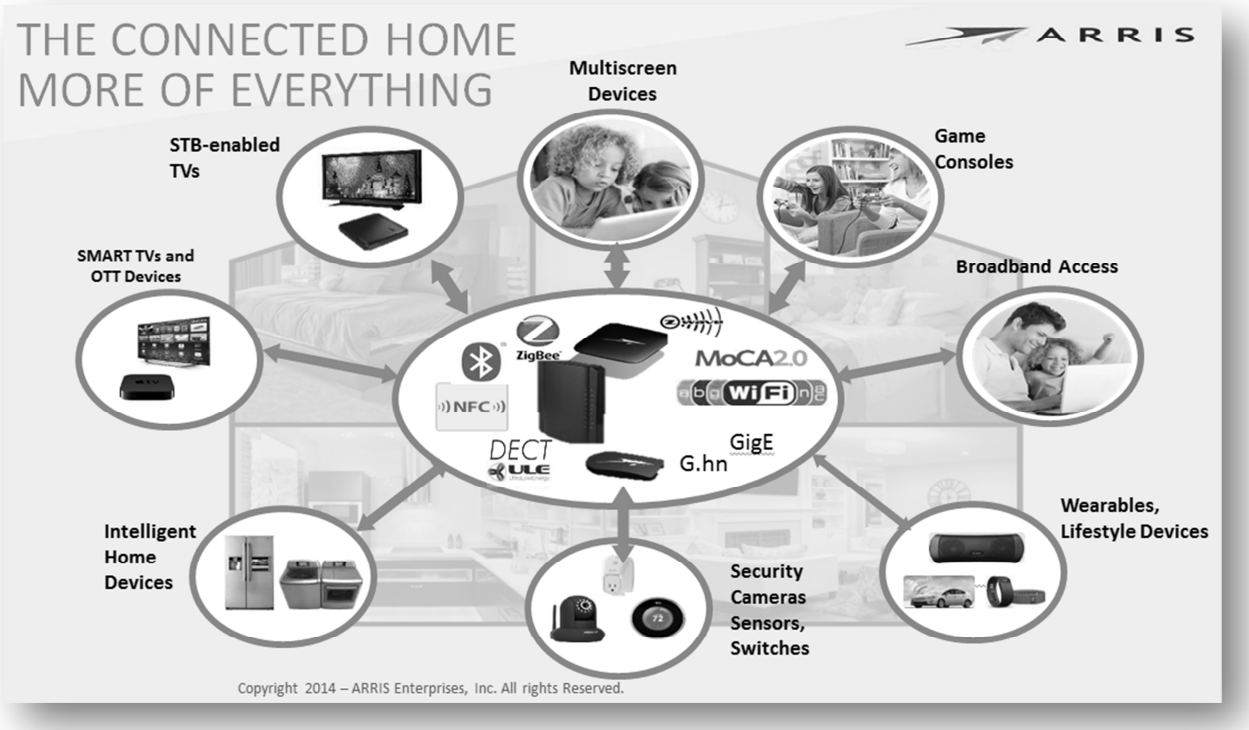

Figure 5 – The Connected Home: Service provider opportunity from their existing devices

The Cable Ecosystem's Role

A service provider may create the Internet to the home connectivity upon which all IoT solutions need to ride. The following set of capabilities that can be leveraged for IoT based services:

- Connectivity infrastructure to Internet
- Technician resources
- Existing devices in the home with wireless connectivity
- Prominent definition of TV user experience
- Existing base and products in market offering home security and automation solutions

The operator is positioned well to extend more into services that touch the end subscriber. In particular, the above set of capabilities really does allow the MSO to enable a faster adoption of connected services.

To baseline potential new solutions, let's take a quick look at the current home security and automation service offered by many service providers.

We typically see the following three services:

1) Home security solution – For example, a comprehensive package of home security solutions that require a typical CAPEX investment of estimated $500-$800 and at a typical monthly payment of up to $39.95 can have an ROI on CAPEX of ~21 months. This type of service requires longer service contracts or requires the customer to purchase some or all of the devices initially.

2) Home automation solution – a smaller package of sensors and switches and cameras that provide home automation services. Typically being offered for a lower subscription cost and a shorter ROI than that of a full security solution.

3) Lower end introductory to (1) or (2) such as a camera solution having a lower subscription cost offering a typical 9 month ROI on CAPEX investment.

Home security and automation services often require professional installation so additional costs of truck roll and technician time and cost increase the ROI by another 2-6 months based on labor and time. Added to this is the network operations center (NOC) and customer support costs causing an even higher time to ROI on CAPEX investment.

The penetration rates of these services have been typically below 5% of the homes served by an MSO. What might be the issue with these service offerings?

It is primarily the customers' view of the cost/value equation of the service. These services, particularly security – have inertia factors from cost-per-month to the hassle factor of installation in the home. These services are typically also not integrated into the MSO's own gateway and TV experience thus they do not leverage any real CAPEX synergies to improve the ROI or capability to lower the overall cost per month.

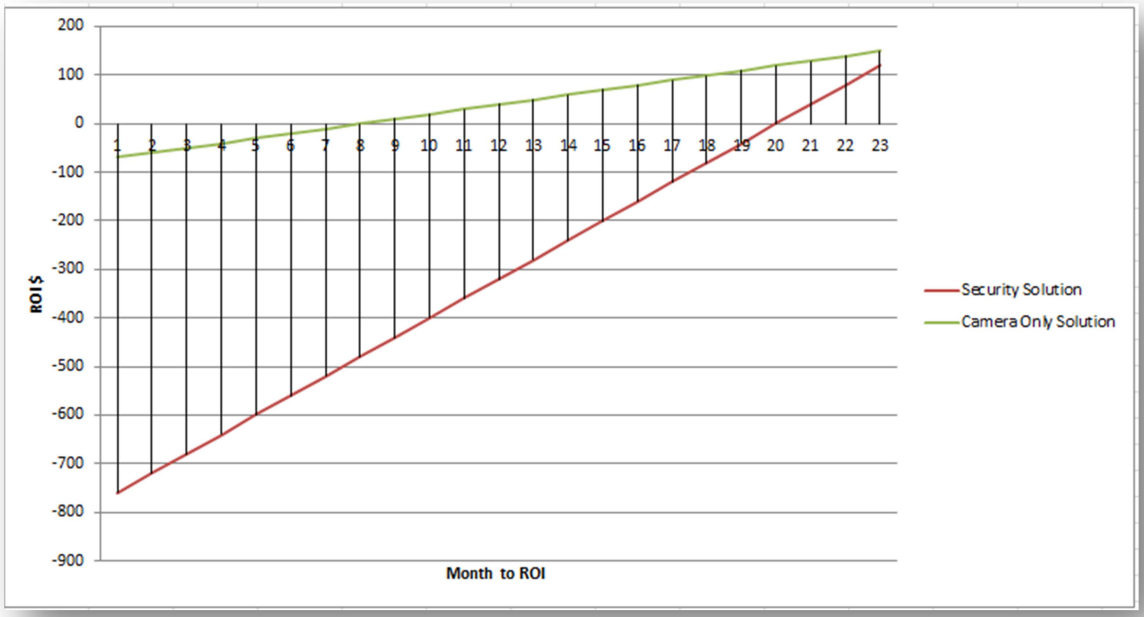

Figure 6 – Home automation/security logjam

How can an MSO improve the potential for revenue for the more traditional connected home services and also begin to also pull in non-traditional revenues in supporting health, energy, utilities, wealth and education services – each of these with large new potential vertical revenue opportunities?

Here are a couple of fundamental stepping stones:

- The inclusion of more IoT radio solutions supporting 802.15.4 and Bluetooth low energy (BLE) as well as Wi-Fi
- Integration of radio solutions in MSO devices such as the gateway (GW), Wi-Fi extender, set-top box (STB) and remote control
- Development of onboarding software solutions to create MSO gateway hub(s)
- Development of the new IoT services that are derivatives of the home automation directions but made simpler and coupled with the voice, video, and data solutions of an MSO

Figure 7 – Service providers have IoT hubs already

Additional to the more traditional connected home revenue opportunities, there is the potential for the MSO to move their connectivity and IoT home presence solution to work with the large vertical opportunities of

- Medicine and Home Health
- Energy
- Utilities – including Water, Gas, and Garbage Disposal etc.
- Health
- Wealth
- Education
- Smart Cities
- Industrial
- Machine-to-Machine

Table 1 and Table 2 below outlines a series of incremental revenue creating capabilities and opportunities that in some cases are unique to each service provider. They leverage absorption of cost of deployment across voice, video, and data and now home automation and IoT services.

<u>The service provider call to action for IoT opportunities</u>

The cost/value tradeoff for the consumer is something that the cable operator can help with by drive providing a value proposition for the consumer.

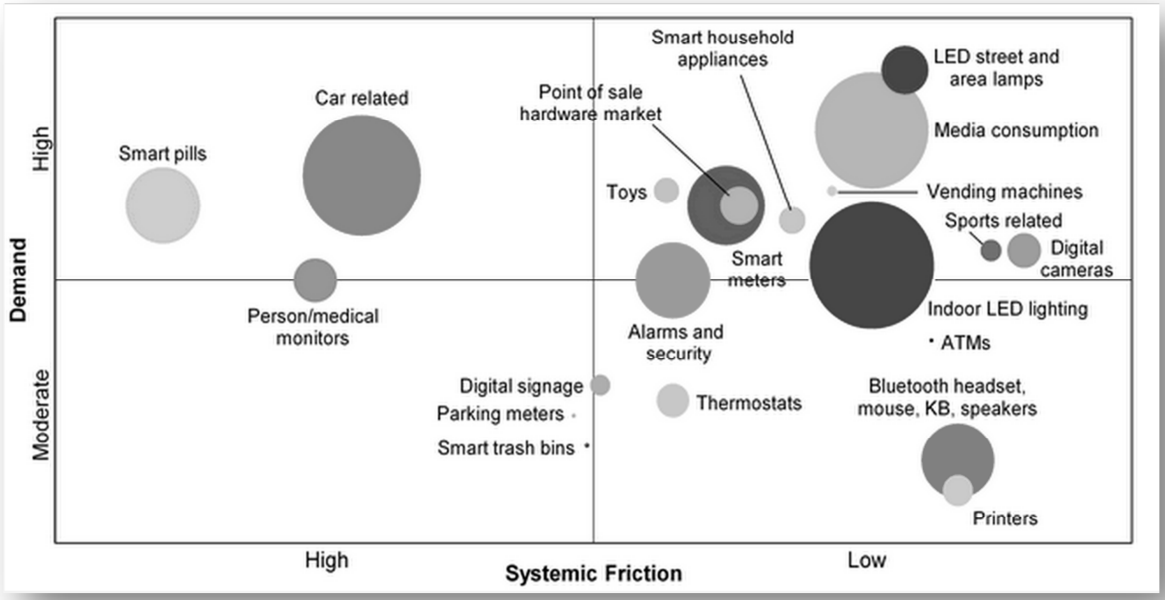

Figure 8 – IoT Service demand and systemic friction

As we can see above, services like alarms and security are relatively low on the friction axis and moderate to high on the demand axis. However, services like Medical Monitors and Smart Pills are highly desirable to automate but are high on the system friction axis – as they require a large change in philosophy, business models, trust, technology, and other factors.

Another component of the cost/value proposition is the absorption of the acquisition costs for any IoT service. These costs can be leveraged by using the MSO installer resources to also support IoT services and can be blended across the MSO's other business of voice, video, and data to leverage the touchpoints that are factored into the operating expenses of its business.

A key element of the MSO capabilities to drive a successful value chain for IoT services is its technician resource base to both support IoT devices and also upsell services when on callout for video, data, and voice installations. This may require potential retooling and reskilling.

Table 1 – MSO key areas of IoT engineering

Potential Action	Description
Reduce the CAPEX investment for home security and automation devices Drive down the ROI time OR decrease the monthly charge to the consumer	Integrate more functionality into gateway, extender, and set-top box for IoT Leverage consumers own devices like tablets, smartphones and TVs more Offer virtualized environments in gateway devices to providers of OTT services
Leverage the technician installs of broadband voice and video services to upsell and install IoT services	Reduce the truck roll costs for connected home services Retrain the technician staff to sell connected home services
Integrate 802.15.4 and BLE into other devices like gateway, extenders, set-top boxes and even remote controls	The service provider can own the radio/PHY level onboarding of the majority of connected devices
Add LTE backup solution to homes requiring security or high availability medical applications	Leverage low usage data rates for LTE call out when required
Offer one set of service provider branded connected home devices – supporting many applications	Provide a service provider branded connected home experience with range of own devices
Support onboarding of BYO devices into the connected home environment	Through supporting the main IoT protocols allow integration of the users own BYOD with service provider solution and the Entertainment system
Develop collaborative value-add applications for integration of service providers and BYOD devices	Create partnerships with different device and solutions to onboard into the service provider curated home experience. Integrating smartphone applications to a single console. Creating IFTTT rules that work across different solutions.
Develop a range of solutions and services that fit into all budgets • CAPEX only investment entry • <$5 per month services • <$20 per month services • <$50 per month • High Value services like Aging-in-Place > $50 per month	Allow subscribers to enter the connected home environment with no monthly fee and CAPEX only services Design a set of applications and services that run without the addition of any specific dedicated device or users own device that range from $1-$5 per month Upsell the consumer to solutions in the $20 range including targeting something like a Security service as a $20 p/m service with reduced CAPEX investment to ROI High Tier multiple services in the $50 range Specific subsidized services like Aging-in-Place commanding $50-$300 per month depending on the level of service

The big adjacent market opportunities from the service providers current baseline

Additional to the traditional connected home derived services above, the following are potentially larger revenue services and the ones that need a deeper look to drive the big step function changes in how a service provider adds new overlay services.

Table 2 – Potential overlay services

Potential Service	Description
Medicare and telemedicine services	Significant dollars are available from insurance companies and government agencies to provide monitoring and future drug administration services Integration of the collector gateway into the service provider gateway as well as using STB/TV instead of tablet devices reduces CAPEX. Adding reminder applications through the TV UX also improve monitoring frequency
Virtual Machine access and APIs to service providers to add application to service provider gateways, extenders and entertainment services	Ability to sell to IoT service providers either client access in home devices or Cloud interfaces
Brokerage for services interfaces for utility and digital services.	Creation of a M2M or B2B2C interface where consumer can broker their utilities to different providers and get lowest and off peak service rates Offer the pool pump 4 hour run to the brokering service and receive the best rate/time from the utility
Analytics and telemetry from the home	Selling telemetry data from the home including supporting Big Data monetizing opportunities
Location and presence triggers and services	For better and more accurate targeted advertising. Can be a source of additional revenue to service provider
Accessibility and voice controlled services	Another specific market to create a more accessible home environment for the blind with voice controlled services
Education services	Leveraging the entertainment, connectivity, and multiscreen control the service provider has to drive a better home education solution including creative task reward interaction with kids the TV and access to the Internet

Integrate 802.15.4 and BLE into other devices like broadband gateway, home network extenders, set-top boxes, and even remote controls

Getting presence of a device in the home is a difficult thing to achieve. Google is moving from its presence in PCs, tablets, and smartphones to other home devices through its acquisitions of NEST, Dropcam, and the recent addition of the Revolv HUB solution.

Apple is advancing its position from its presence in smartphones, desktop, laptop, and tablets. They also supply airport access points, Wi-Fi enabled storage devices and Apple TV. With the addition of HomeKit to IoS, Apple has indicated its strategy to add HomeKit functionality to wireless attached devices and create opportunities for new home control and automation applications which interact with media experiences. One can also see in the Apple Store the rise of partnered IoT and connected devices and solutions.

Consider the general connected home use case for security, in particular where the initial investment of capital items includes a ZigBee Hub Protocol converter, a touch panel, and LTE radio. The potential exists to absorb these radios and functions into products like the:

- Home gateway – already Wi-Fi based yet now add 802.15.4 and BLE support
- Wi-Fi extender – an important emerging additional device in the connection to services. There is an opportunity to add the additional 802.15.4 and BLE radios to the extender device
- Set-top box – perhaps the most powerful addition to the IoT ecosystem because of its presence near consumers as well as having the TV screen to drive integrated IoT based-applications

In particular, the strategy to add 802.15.4 and BLE radios to the gateway, extenders and set-tops – at a small additional cost to those devices to reduce any additional cost of protocol/PHY conversion is key. This allows for the easy onboarding of any service provider IoT devices or consumers own purchased wireless smart devices.

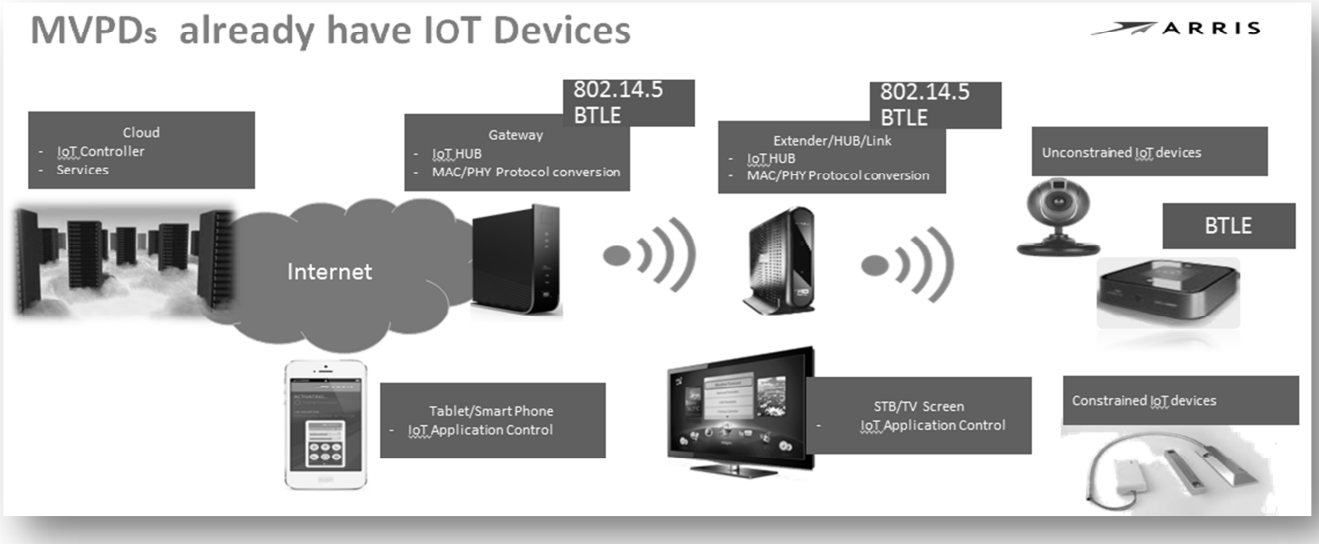

Figure 9 – The service provider's IoT devices

In current proprietary IoT solutions there are those devices that require low power wireless solutions:

- ZigBee and ZWave, for example, are commonly used for low power sensors and inexpensive solutions that run from coin cell battery solutions. They often harvest energy from leakage or kinetic energy
- Bluetooth Low Energy is a popular physical layer of many medical and wearable devices

These solutions typically require the addition of a Hub/Link or protocol convertor from 802.15.4/BLE to Wi-Fi and from ZigBee to IP. This hub is both an additional cost item and an additional device in the home. It takes the data path typically in an over-the-top trajectory. The integration of this device into existing MSO devices is a key part of the MSO strength in the IoT ecosystem and home.

Why 802.15.4

802.15.4 supports the physical layer of ZigBee based devices and aligns with the PHY layer selection of the Thread group of companies in the IoT space. It is likely to be used for low power and more constrained IoT devices, but also emerging with Thread promoting 6LoWPAN direct IP connectivity.

The ZigBee group is also advancing solutions for ZigBee IP and 920IP as well as a 6LoWPAN so another option to consider.

Why BLE

Almost every wearable and hold-able device supports a Bluetooth interface. BLE and BT4.2 are the right interception points to allow the onboarding and presence detection of devices. It provides a good low power solution and offers an opportunity to the service provider to also combine the use of Bluetooth with remote control and set-tops. This allows the cost of BLE addition to the set-top to be amortized over both remote functionality and IoT connectivity to wearables, and also to afford location and presence detection to applications for advertising and other security solutions.

In particular, adding the BLE support into a set-top makes it a more likely solution to connect to BLE devices and wearables when consumers are in the main rooms of their homes. Those rooms typically have a set-top box present. Additionally, applications that allow interaction between the consumer's BLE IoT devices and the TV screen can be developed.

One further big BLE/BT4.2 opportunity is in the Medicare and Wellness area. Typically, most of the monitoring devices connect via Bluetooth to send readings and there is a large opportunity to support Medicare solutions just by adding an IP set-top with BLE to the home.

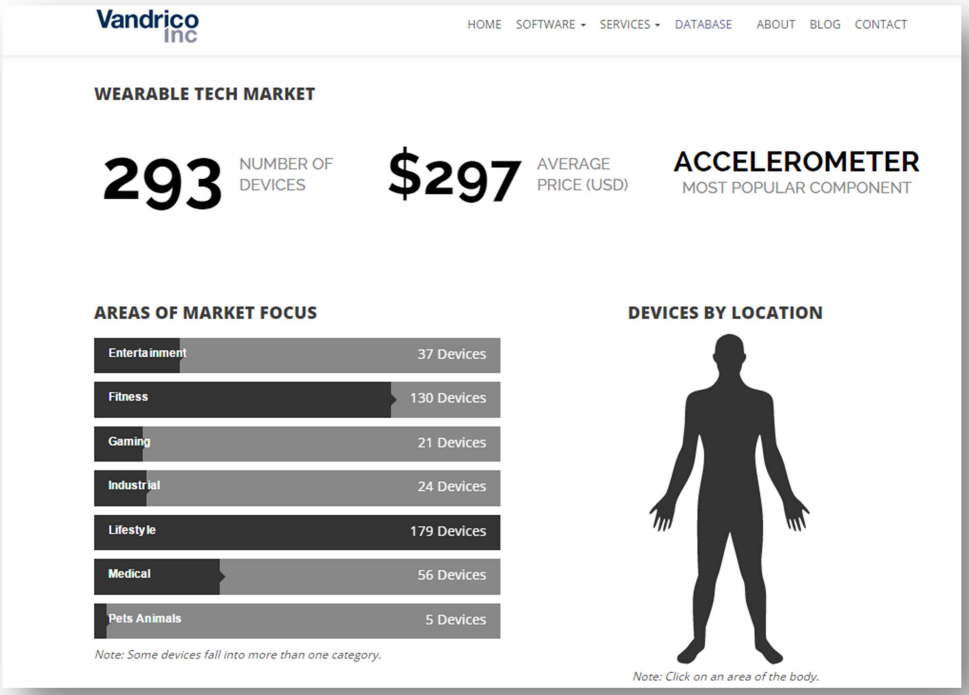

Figure 10 – Almost 300 wearable devices already exist

Add LTE backup solutions to homes requiring security or high available medical applications

While the reliability of the cable network is high, a backup path is required to provide high availability solutions like security and some medical applications.

A 3G/LTE backup has typically been a separate device integrated into either the control panel for security or in medical applications a device like the Qualcomm 2Net device that provides dedicated connection to network side database.

The pricing models for SIM based devices are changing to allow very cost effective 'rarely used' data connections and in many applications the LTE radio can be powered off until needed not requiring additional power overhead in steady state operation.

Leverage the technician installs of broadband voice and video services to upsell and install IoT services

This is a key aspect of a service provider's ability to accelerate adoption of connected home and other IoT services.

One truck roll and $150 investment in technician time could be offset by the following re-engineering of the technician install process.

For example, if a technician is installing a new gateway or set-top, the truck roll cost may also be amortized over any additional connected home installs or upsells.

As another example, if the service provider also partners with water, gas or electric companies, either company can also install metering devices as part of the one visit install.

Even if an MSO doesn't initially partner with any utility companies – the MSO can make an investment in installing devices such as gas leak detection, water flow meters, HVAC systems, and even sprinkler or pool pump systems as part of a larger brokering of service or selling of analytics or telemetry data.

The consumer would have to approve the installation of these devices and opt-in on the sending of information to utilities or insurance company – something that can be managed to high opt-in rates from consumers.

The amortization of multiple activities in the home by the field technician would potentially:

- Decrease the present cost of IoT services install and OPEX considerably
- Incur initial capital outlay for devices like water flow monitors that could be offset with substantial potential monthly fees from insurance companies for leak damage mitigation
- Incur initial capital outlay for items like sprinklers, pumps, HVAC controllers and energy management devices, however brokerage fees and utility pass through of revenue sharing to the service provider would be possible and potentially profitable

The process and amortization changes could enable the viability of a cable operator based IoT solution and its associated services.

<u>Offer one set of service provider branded connected home devices – supporting many applications</u>

It is important for each service provider to create and provide a set of appropriate devices that identify that service with the service provider offering it. In the case of current home automation and security solutions, partnering with home security and automation companies – and leveraging their software solutions – allows for an MSO to enter the market and deploy the solution on its own devices. However, service provider branding may ensure that the consumer identifies more with the service provider than the security company. The other devices that link into the controlling device or hub are many and varied. Typically the current focus devices include

- Thermostats
- Cameras
- Contact and Motion Sensors
- Lights and Light Switches

Future potential additional devices and services include additional devices on the list below.

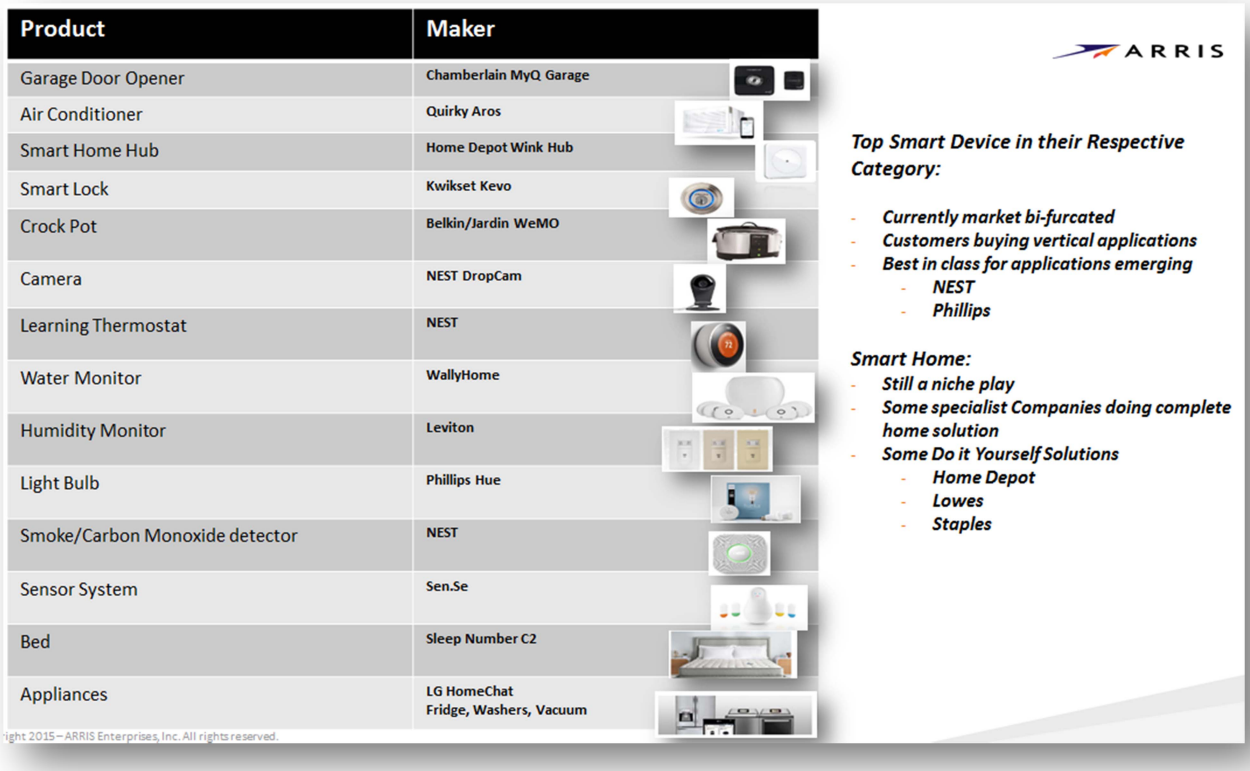

Figure 11 – The top IoT device and service opportunity

Support onboarding of third party IoT devices

There are literally a 100 different solutions for IoT applications – and all come with proprietary protocols. In some cases, they converge on ZigBee or Zwave for non-IP devices but generally, companies like Belkin/WeMO, Insteon, PeQ, Phillips HUE, Withings, Google NEST, Quickset, Chamberlain, Kwikset and Apple/HomeKit all have their own solutions built around many different protocols. This has caused fragmentation in the application space for IoT and has created user experience issues where the consumer needs to use multiple applications and interfaces to access their home automation, control or IoT solutions.

There is an opportunity to make a "Home" experience rather than a WeMo or Google experience and aggregate the different solutions to one interface – an MSO application on smartphones, tablets, PCs, and the set-top box for a user experience which is part of the complete MSO TV experience.

To do this requires the support of more than one framework and/or set of protocols. The logical choice is to:

- Adopt one protocol for each service providers own solution
- Support the protocols moving the herd (market) and closest to standardization or major adoption
- Support protocols which are open standards or on a path to OpenSource
- On a solution by solution basis, if the business analysis dictates, add support for other solutions
- For hardware enabled solutions like Apple's HomeKit, make decisions on the inclusion of the security module in some or all of the onboarding solutions
- Develop strong relationships with the Top 10 BYOD (Bring your own device) and BYOS (Bring your own service) providers

- Develop a value-added proposition for third party solution providers to integrate their solution into a singular home experience. Examples include:
  - Smart Oven – notifications on TV that something is burning
  - Smart Garage Door open – notifications on TV that the garage door is open
  - Integrate audio and voice control into IoT devices
  - Integrate into the MSO Entertainment Platform for integration with video, voice, and data services

The primary IoT protocols that fit the criteria above are:

- Open Internet Connect
- Alljoyn/Allseen Alliance
- Thread
- ZigBee
- UPnP

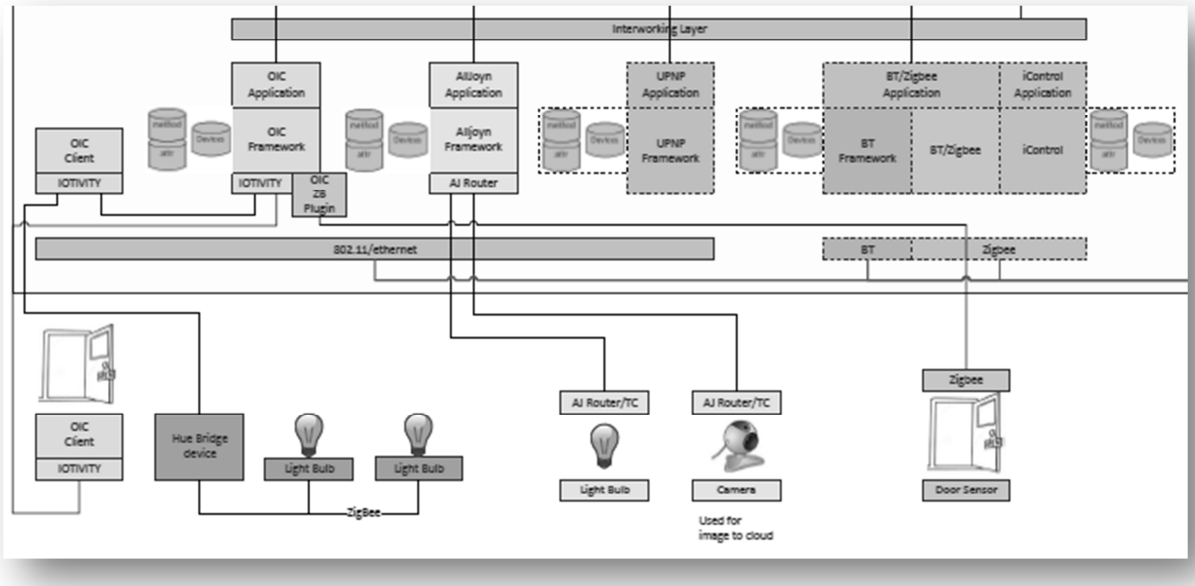

Figure 12 – Multi IoT protocol stack for an MSO gateway

The Business Decision inputs for this multi-protocol support include:

- Can the service provider afford not to provide this feature? If the value-add to the service provider solution is to aggregate fragmented IoT solutions then targeting the high runners for inclusion in a single MSO controlled solution is important
- What is the cost of supporting many different protocols?
  - Each solution has to be weighed on its popularity, opportunity and ROI
  - Additional code overhead has to be reviewed for RAM and Flash implications on devices
  - Supporting the main OpenSource standards solution seems a prudent decision
  - Partnering with the high runner proprietary IoT devices and service providers on a mutually beneficial basis
  - Additional software and testing resources for multiple combinations of protocol and device may be prohibitive

- How are these protocols maintained and integrated into the gateway, extender, and set-top box?
  - One proposal could be to develop a solution that works with the RDK-B architecture. This could be an abstracted and containerized architecture that messages to the RDK-B framework and keeps the IoT modules – modular and protected from the connectivity operations of the gateway
  - Integrate OIC, AllJoyn and Thread and others into the runtime as needed
  - Develop a common data model, since each has very different protocols in their implementation and coverage,
  - Leverage templates from UPnP and the machine-to-machine IoT standardization work
  - Dynamically load as the devices are sensed in the home

<u>Develop collaborative value-added applications for the integration of MSO and BYOD devices</u>

As defined in the preceding section, one of the key strategies for a service provider is to ensure that from a physical layer all major IoT devices and applications can make their way into the ecosystem of the service provider.

To add value to the third party solution, the protocol of the solution must be:

- Part of the supported protocols in the stack – examples OIC, Alljoyn, and Thread
- Partnered disclosure with the solution provider

The opportunities for increased revenue and application opportunity are to:

- Aggregate a single dashboard experience on the single service provider's application. In the case of MSO, the TV UX application becomes the single interface point to both MSO and Third party devices. For the MSO provided set-top boxes, the UX based dashboard and interface to the home experience is offered
- Charging subscribers for an aggregated experience of their third party and MSO-based solutions can be done through the purchase of an application. For example, a nominal monthly fee could be charged for using each MSO provided IoT portal application

Examples of such applications are could include:

- Smart Garage Door opener – The added value is having the event from garage door also sent into the MSO Home Framework and being able to display notifications on the standard TV or TV UX. In addition, if the MSO has a voice services on their TV platform, those services could also be leveraged to close the garage door from the smartphone or a remote control application
- Adding all the IoT service and devices into a singular dashboard where the devices can be viewed for connectivity health without having to fire up multiple smartphone applications.
- Being able to monitor and control the use of security cameras from third parties to help address some of the privacy concerns consumers have about the use of cameras and sensors in the home

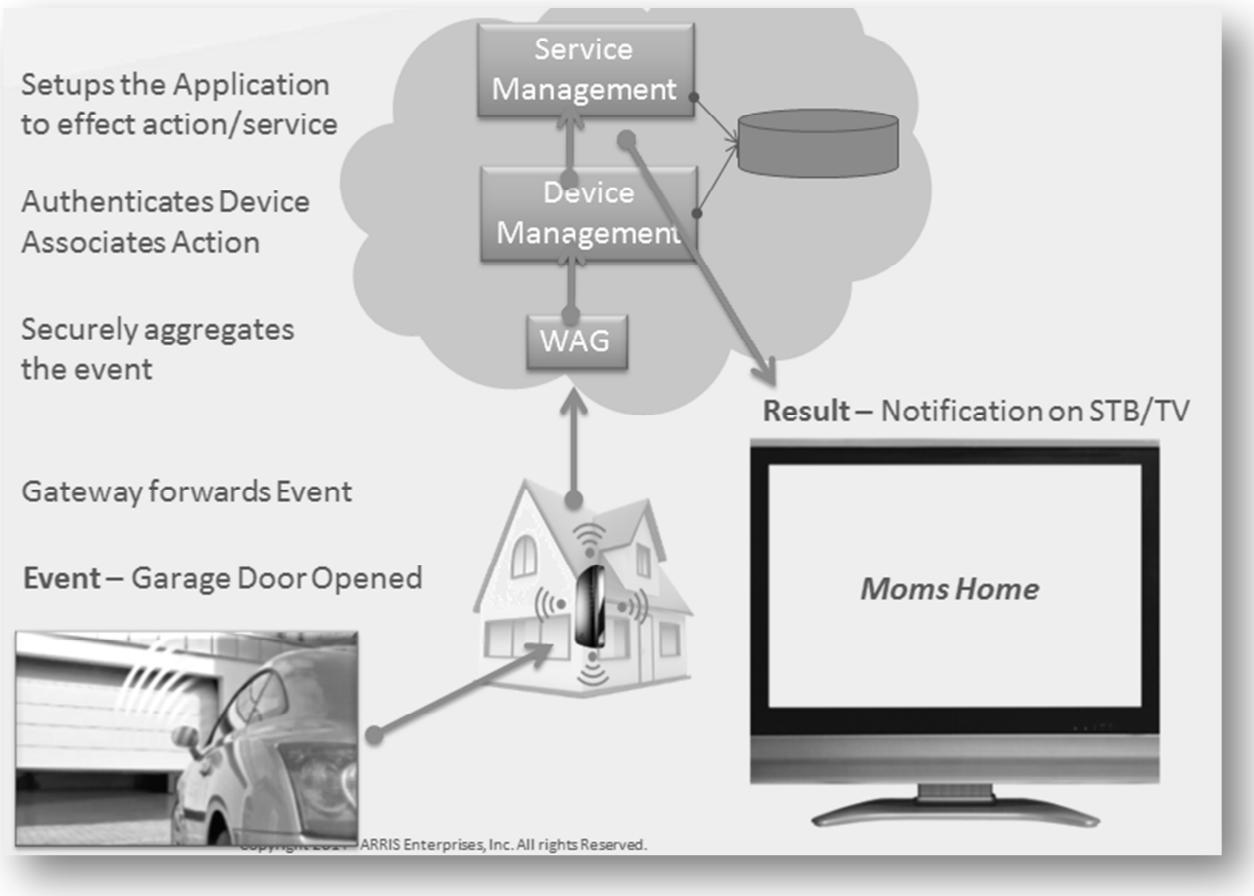

Figure 13 – Onboarding a notification service from third party application using Cloud Services Architecture

Develop a range of solutions and services that fit into all budgets

A key change in the current home automation and home security solutions of the service provider is to create something for everyone's budget in the connected home and IoT space.

Current MSO home security and automation solutions approximate range per month:

- $9.95 per month for camera IoT solutions
- Home automation and control solutions at $19.95 per month with a limited number of IoT devices and sensors
- Entry level security solution at $19.95; a home security solution with provided devices
- Deluxe security solution for $39.95; a home security solution with additional devices

As we have mentioned earlier – these solutions currently have:

- Low penetration with customer base
- ROI ranging from 8 to 20 months
- Requirements for 2+ year minimum contracts
- Have technician installation costs

There is opportunity to improve either ROI or base monthly cost by leveraging the integration of functionality into other devices like gateways, extenders, and set-top boxes.

Additionally, there are some new models that could allow everyone to dip their toes

into the IoT, connected home and security services. These include:

- Zero $ per monthly fee onboarding solutions
  - CAPEX only purchase of IoT device
  - Free giveaways to customers of IoT Switches Sensors to tease them into additional IoT services
- $1-$5 applications that are pay once with no monthly fee
  - Modesty protection for camera; enabling this feature on the MSO home security/automation application
- $1-$5 applications – per month
  - Onboarding your BYOD into the MSO home security/automation application
  - Enabling voice control of IOT devices
  - Elderly panic button based on RF4CE or BLE remote control
  - Adding security cameras including BYO cameras to the TV dashboard
  - $1-$5 per month for each additional IoT devices to the initial bundled packages
- $5-$30 per month applications
  - $30 per month for the MSO security package and "all you can eat" application services from lower tiers
  - $15 per month for a home automation package
  - Second home/vacation home packages
  - Direct to water utility sprinkler solutions leveraging IFTT based weather and sensor information to optimize to a fixed monthly fee for water use and lawn perfection
- Higher end per month fee bundles for MDU and SMB environments

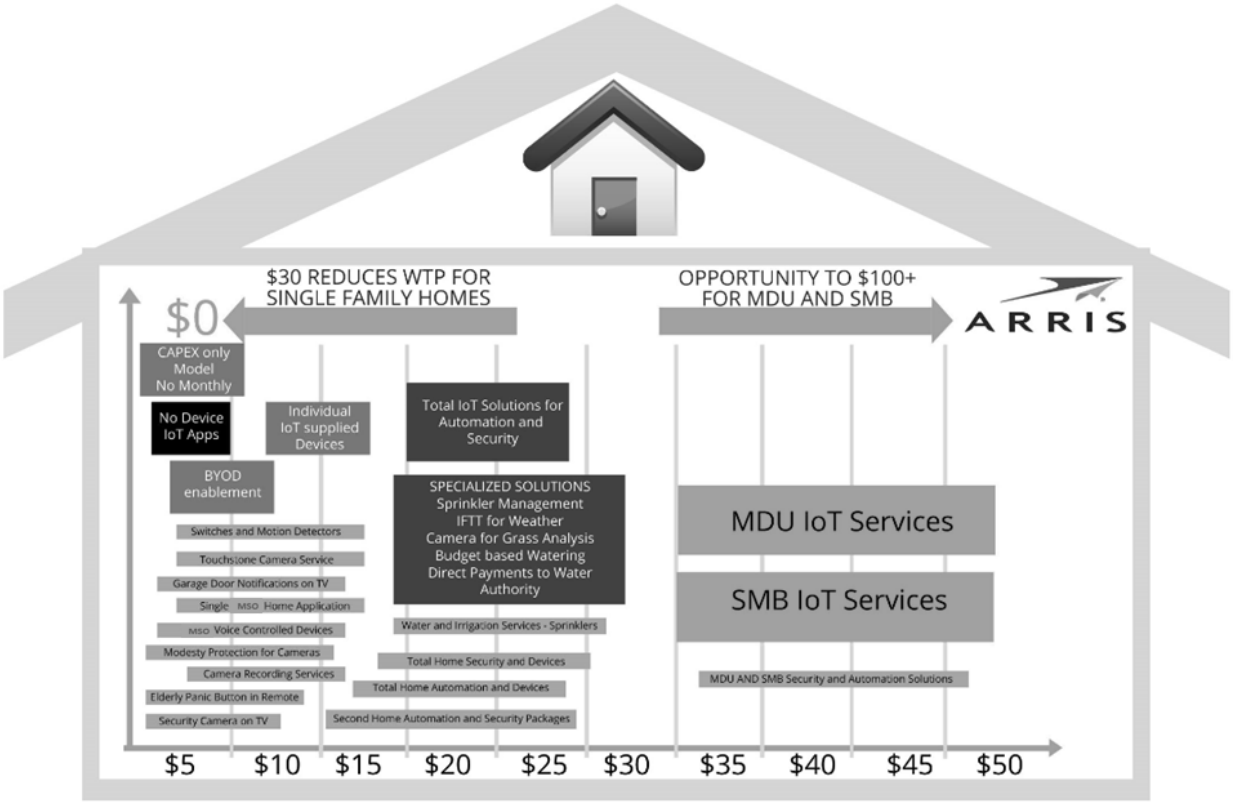

Figure 14 – Potential range of IoT services for everyone

Figure 15 – Simple monthly panic solution using RF4CE and BLE remote

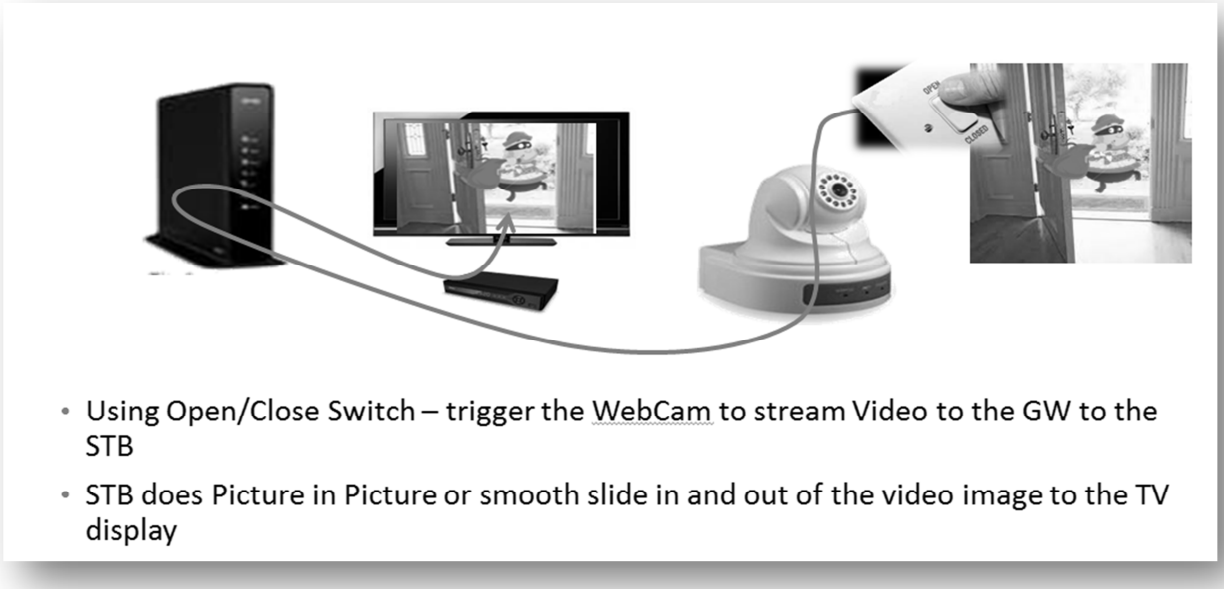

Figure 16 – The better integration of a third party camera

MEDICARE AND TELEMEDICINE SOLUTIONS

One of the most exciting opportunities for the service provider is the Telemedicine, Medicare, and Aging-in-Place business opportunity.

Aging-in-Place services focus on monitoring the elderly and ensuring that clear communications and connectivity are provided to caregivers.

Typically most applications require monitoring and use specific hub devices to connect to Bluetooth-based health monitoring devices from weighing scales to blood pulse-oxygen monitors. There is now even progress in monitoring the drug administration itself from sensors that detect medicine packaging access activity to devices that are worn by the patient and are connected to the Pharmaceutical or Caregiver drug administration system.

There are service provider opportunities to reduce the capital expenditure on the Medicare equipment by using gateways, extenders, and set-top boxes with BLE to connect to the wireless Medicare device. This could effectively create a solution where the patient is checked to see if they are a MSO subscriber with a 'Medicare Ready' home package. They are then sent home with just the monitoring devices – and not the hub device.

Figure 17 – Service provider Medicare solution

A service provider could create the best solution to gather the daily readings by incorporating the service providers TV platform into the solution. This would also allow for training about the medication and devices to be given through the TV platform.

An MSO TV platform typically has many accessibility features to aid any disabled patients. Features might include syncing the patient's monitoring schedule to the TV system; the TV could prompt the patient to take their readings. Strong stick (and even some carrot opportunities) could be created by pausing TV content to force the patient to take a reading. Additionally, blood sugar checks and insulin reminders could be given on the TV, again with a forced pause until the patient completes the requested action item (reminder).

Aging-in-Place communities could be serviced by a single MSO deployment, because of the integration of some of the Medicare solutions. The revenue opportunity for the MSO would be in addition to the already existing voice, video, and data services they might be providing that community, or end up providing that community by winning an Aging-in-Place service bid.

Virtual Machine (VIM) access and APIs add applications to service provider gateways, extenders, and entertainment services

The opportunity is to offer third party companies the ability to have access to the customer's device(s) as part of an overlay service that the third party offers. Services could be potentially hosted in the Cloud with only one service provider interface in the home gateway since VM architecture in the gateway potentially offers the scope for a more hands-off pass-through approach to some specific services.

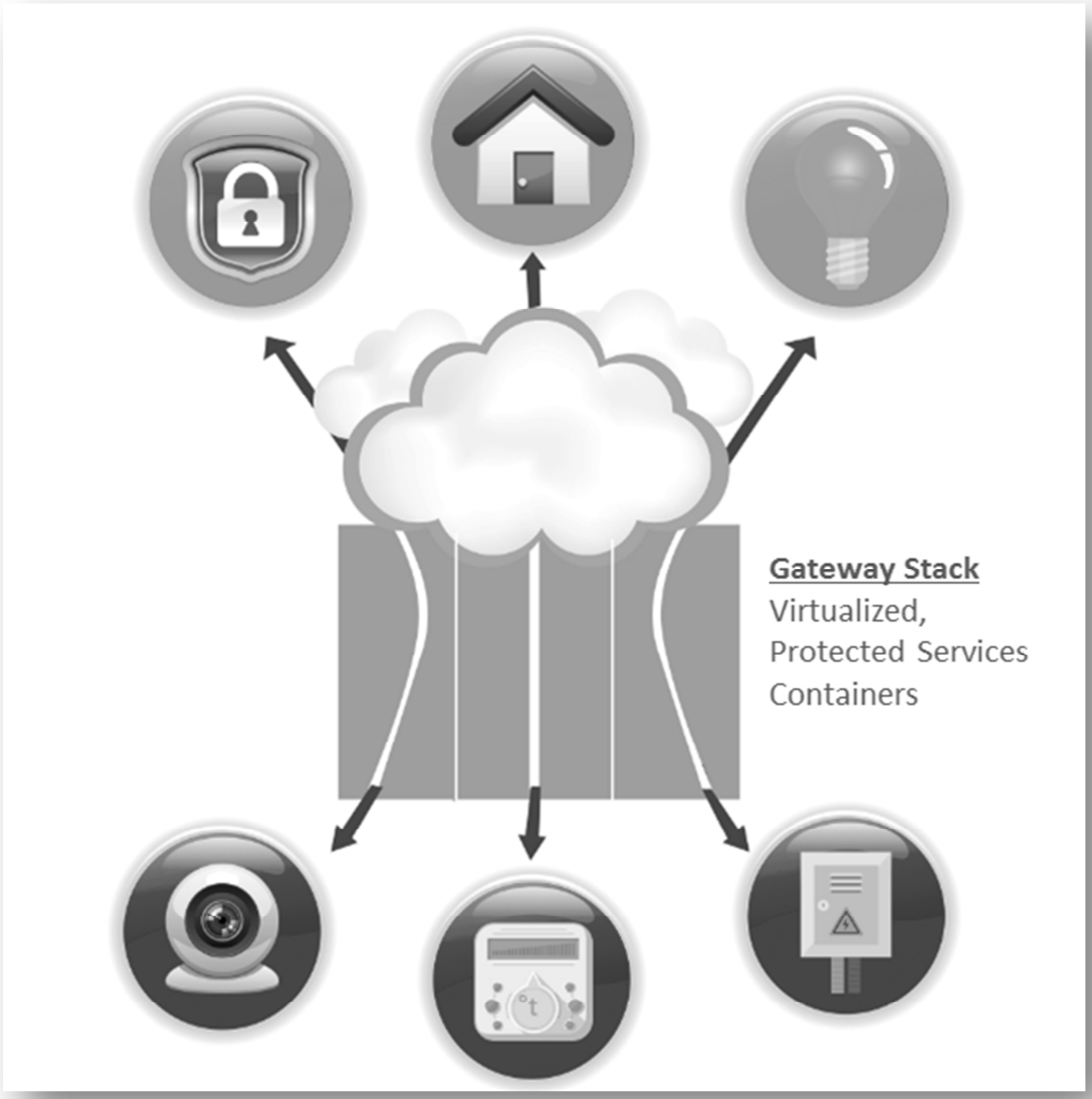

Figure 18 – Hosting third party applications in the IoT gateway

The revenue opportunity is to charge for access to the VM in the gateway and other devices. Fees could be application or service based. The opportunity costs include the development of the VM hosting model, along with the associated APIs and Web services that would allow a third party service provider to access the home information.

For example, offering any security company the ability to leverage the gateway for access to Wi-Fi, 802.15.4, and BLE services, as well as LTE radios in the future, by overlaying their own devices into the home, could be a service that mutually benefits both companies. The service provider doesn't have to get into the security business, yet could make revenue from the devices they have in the home.

The Virtual Machine makes this type of application possible – allowing the service provider and third party to protect each other's services and not impact the consumer experience.

Brokerage for services interfaces for utility and digital services

The commercial model for service provider is to create this brokering service ecosystem. By leveraging its position as the connection to the consumer's IoT devices, the offer/bid solution is to create an automated switching of utilities to the consumer on a monthly or lower granularity. Whether this can be done on a per device or per service basis should also be reviewed. The MSO would then take a percentage of the transaction for providing the brokering of the services.

The MSO also provides onboarding of the utilities as well as details of the power or water or gas requirements of the home through intelligent monitoring.

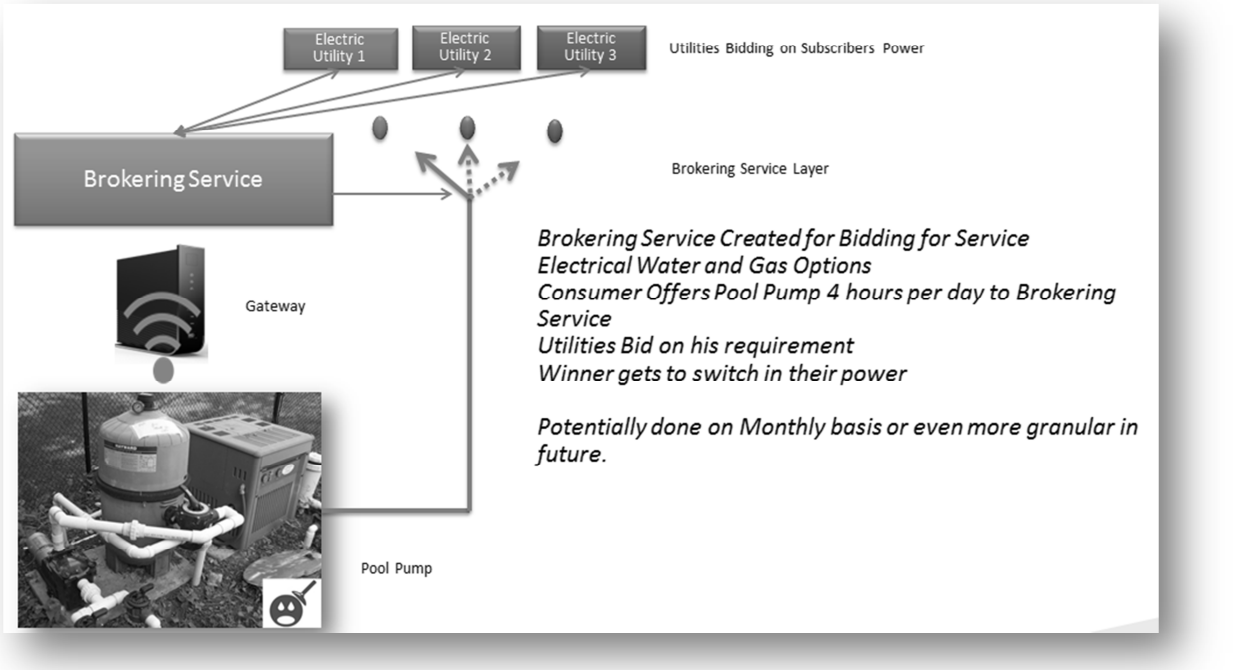

Figure 19 – Example simple brokering architecture

Show me the (IoT) money!

If we take a hypothetical look at a YoY projection – for an IoT revenue stream from the above services example and the resale and use of analytics from the home – the following graph could potentially be the ramp projection of IoT services for an MSO with over 1,000,000 subscribers. The may generate potentially upwards of $50 of revenue, on average, across the entire customer base.

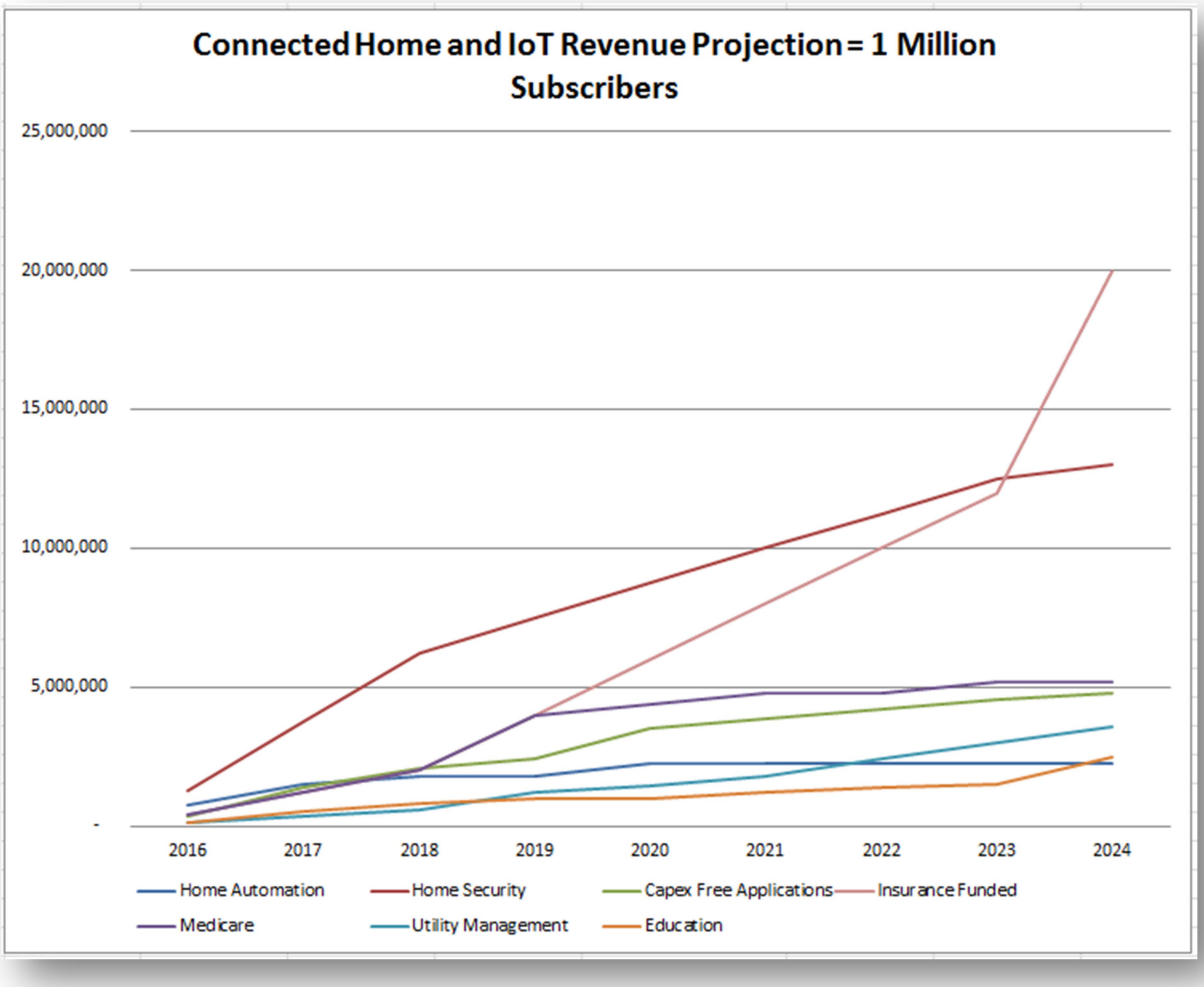

Figure 20 – Hypothetical model of IoT revenue growth by service

	Per Year adoption								
	2016	2017	2018	2019	2020	2021	2022	2023	2024
Home Automation									
<$20 p/m Service	5%	10%	12%	12%	15%	15%	15%	15%	15%
Home Security									
<$30 p/m Service	5%	15%	25%	30%	35%	40%	45%	50%	52%
$5pm Applications	5%	20%	30%	35%	50%	55%	60%	65%	68%
Insurance Funded	1%	3%	5%	10%	15%	20%	25%	30%	50%
Medicare	1%	3%	5%	10%	11%	12%	12%	13%	13%
Utility Management	1%	3%	5%	10%	12%	15%	20%	25%	30%
Education	1%	5%	8%	10%	10%	12%	14%	15%	25%
Analytics/Big Data	25%	50%	75%	85%	86%	86%	86%	87%	87%

Figure 21 – YoY % of IoT service growth

This model illustrates a hypothetical revenue stream from the selling of new IoT based services and could potentially have some of the following market penetration and revenue characteristics to:

- Drive security and home automation to ~ 67% take rates with decreased per month cost and CAPEX investment
- Drive up to ~70% of subscribers to spend about $7 per month on IoT CAPEX free applications based on presence and existing hardware
- Get insurance funding for ~50% of homes for preventative measures
- For Assisted Living / Aging-in-Place and sent home to recuperate applications we may get ~13% take rates with an average of $40 per month service to insurance companies and care providers
- Providing energy and other utility connectivity and monitoring, and analytics may yield another $12 per month and take rates to 30%
- Other Big Data analytics sales of connected home data for about $2 per month (conservative) and ~85% take rate (opt-in typical % number)

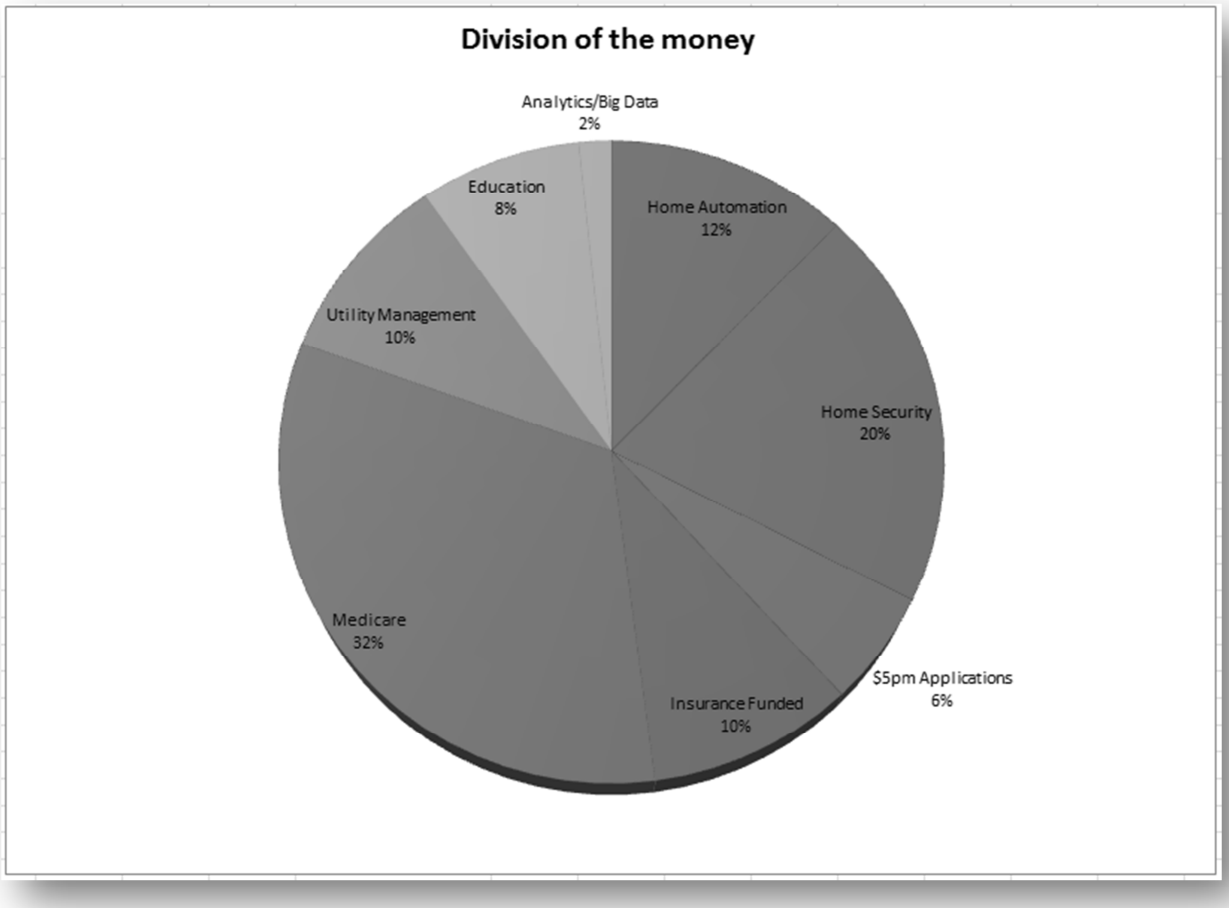

Figure 22 – Breakdown per IoT service in $

Location and presence triggers and services

As we discussed, the connected home needs the connected person to affect some or many of the services that may be desirable to have as a consumer. To be able to create that simple and best positioned and directed user experience – device and people location and presence is a big part of a successful home solution.

The best IoT services will be the services that don't require any specific intervention using smartphone or applications and are driven by ones presence and location. Many home 'scenes' or regular routine actions may be automatically learned or triggered to execute.

For example, the home security lockdown action could simply be done by sensing the TV being turned off, no presence in the bottom floor of the house, or the time of day, etc. Alarm setting and security lockdown could be triggered from the TV being turned off or a number of additional events. In the case of the last TV off at night this could also present the user with a quick camera scan, sensor/contact status, garage door open notification and even police or other social media information relating to the neighborhood or district

As another example, sprinkler systems would not have to use rain detectors. They could instead be driven from cloud IFTTT

weather applications and even soil/moisture analysis sensors.

Additionally, an application could automatically open the garage door when presence is detected via a designated device or set of devices.

There are even more interesting presence and location services that can also be achieved. Consider that as you move from room to room – your home application interface on your tablet or smartphone also changes. When you are in a room with set-top box and TV – the remote for the TV may be presented as the first and landing zone application. When you are in a room with audio speakers, you may be presented with the Playlist and speaker control app as first on your control application landing page.

Who is in the room, vicinity of each other and in front of the TV? There are many ways to try and define who – but one of the easiest is to use iBeacon technology with Bluetooth to declare a person's presence with a smartphone or potentially a wearable fitness device. This allows interesting applications particularly with the service providers TV user experience. For example:

- Recommendations can be done without cameras being required
- Personal preferences can be loaded in the TV UX

Interesting applications can be built as the consumer leaves one room and goes to another room. For example, a TV notification could offer to resume where a consumer stopped viewing a program when they left the other room, even if they forgot to pause the DVR.

ACCESSIBILITY AND VOICE CONTROLLED SOLUTIONS

One of the strongest assets in the MSO IoT play is the integration of an IoT service with the TV experience. This integration provides access for the IoT devices to a visual feedback portal (STB generated TV UX) and input methods to the IoT services. These inputs might be through a TV remote control, an MSO application on TV and smartphone/tablet, and with the increase in voice control of the TV experience the integration of this voice control into the whole home ecosystem.

As was mentioned in the last section, the ability for the MSO to detect presence and movement in the home can also be leveraged into the overall smoothness and integration of the complete home experience.

If we envisage a home with both audio and motion sensors, we can create a simpler interaction with the IoT services and devices through detection of presence and the use of voice control. There is a growing use of applications for "always on" audio sensors – where the user is hands-free and speaks naturally; in this case typically using a code word to trigger the action sequence.

This audio sensor can be positioned in MSO devices like set-tops, gateways, and extenders, and in particular devices like remote controls to pick up the user commands. Of course, the same application can be built on PC, tablet and smartphone using the audio inputs on those devices and leveraging an MSO 'soft' presence through applications on those devices. Voice recognition is particularly useful for control, authentication, and personalization and thus has an important role to play in the future MSO and IoT home.

The growth of IoT is critically dependent on both simplicity of user interaction with any specific device, as also that the complexities of user interaction grow very slowly with the number of devices. In that context, voice is a good modality as it allows for users to interact with IoT devices while doing other things

(e.g. watching TV), thus enabling the user to multiplex IoT interactions with other (media) manipulation. Because IoT interaction in a home setting is likely to be repetitive and with a bounded set of devices, the voice interaction problem in the home has some distinct characteristics from general purpose voice UXes (e.g. the 'Siri' problem on Apple devices).

Companies like Wit.AI are attacking the 'Voice for IoT' problem by making bounded vocabulary command and control interfaces easy to create. Bounded vocabulary command and control recognition is also likely to be more resilient in noisy settings than unbounded voice recognition. Another opportunity for an industry value-added service is the creation and distribution of curated command libraries for commonly used commands (and associated diverse and colloquial utterances).

The use of voice as a modality also solves the input friction in authentication. Given that there are a bounded set of voices in a household, the act of interacting with an IoT device also enables implicit user authentication (and personalization) without explicit effort from the end user.

B2B2C services

It's clear that there will be a number of macro business models in the IoT value-add and revenue chain. These include:

- IoT service direct to Consumer as B2C but OTT to the MSO
- IoT service direct to Consumer as B2B2C with the MSO adding value with relationships with IoT service provider
- MSO Direct to Consumer – as B2C
- B2B2C with Cloud-to-Cloud exchanges between MSO Cloud services and IoT services providers own Cloud infrastructure

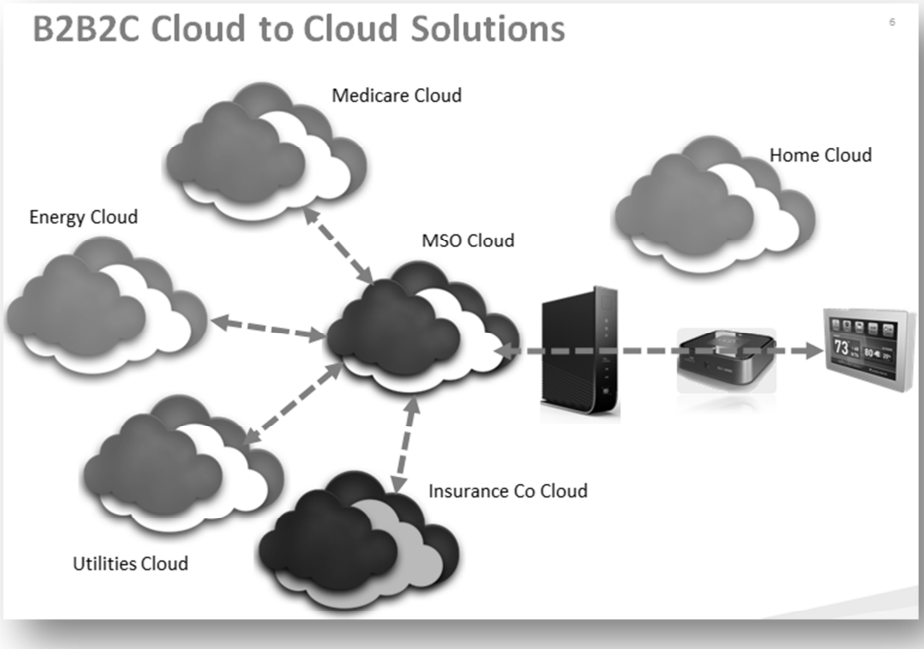

Figure 23 – B2B2C possible IoT services network

The development of these Cloud-to-Cloud interfaces and interchanges will take time. However, the potential exists for an MSO to partner with many of the current services vying to provide connectivity based IoT services to the subscriber. The MSO may optimize the cost and investment chain to provide the service. In particular, as has been mentioned throughout this document, the MSO may also leverage the existing CAPEX investment in device hardware as the IoT gateway and its fleet of technicians.

Data mining and the revenue opportunity for analytics

IoT technology needs to be strongly data driven for two reasons: the superior and personalized user experience, and monetizability.

On the former, IoT operations need to auto configure to a user's 'typical' expectations and context. Take the simple example of a smart light bulb. User expectation of the speed of light bulb operations (e.g. on/off) can range from 50 to 500 msec. Further, the likelihood that the automated turning on of a light may be positive or disruptive (waking up a sleeping spouse already in the room) is a function of social and personal context. Data collection and mining enables a self-learning capability (with potentially periodic or seasonal adjustments) for IoT devices that adjusts to the evolving behavior of users.

On the monetization front, data collection and mining enables the MSO to monetize (and subsidize) IoT services via the creation of third party relationships, both advertising and commerce. As articulated in http://wfoa.wharton.upenn.edu/perspective/venuvasudevan/, proactively understanding a consumer's use of a device like a washing machine enables an MSO to create just-in time advertising relationships with the detergent advertising companies, or Angie's list style intermediaries for periodic repair.

Supporting services

Assuming IOT is valuable enough that a subscriber finds benefits in a service tier to support it, the tier may include associated services such as data archival, security, rules engines, remote and mobile access, expedited customer service, etc. This is the place that consumers pick their own (hopefully standards-based) devices and they are discovered and integrated into the MSO management and presentation

The network and network management

How does the MSO scale for the millions of devices creating billions of transactions on the network?

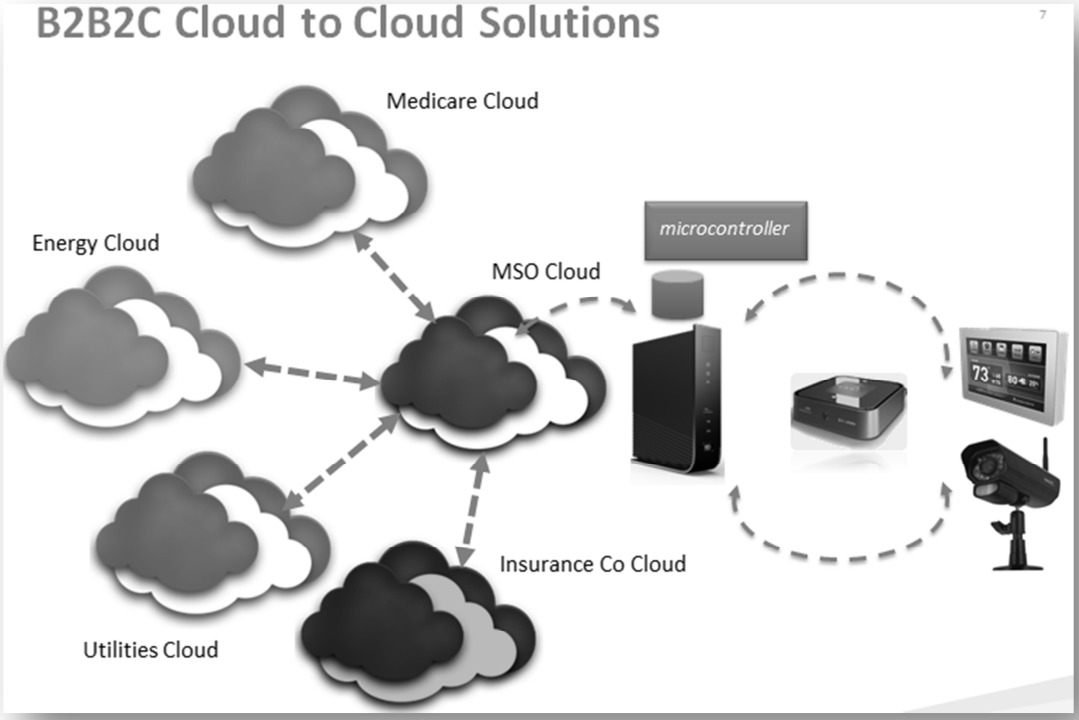

Figure 24 – Leveraging the gateway to scale transactions

There are many performance requirements for IoT services and devices. Some require very low latency, for example turning off and on a light switch (<500ms for action/response desirable). Some require lots of bandwidth, like HD security cameras, most of the devices are 'chirpy' and require maintenance level information to make sure they are still alive and ready to trigger an IoT action or service.

Some of the services require high reliability and availability, such as security and high end Medicare monitoring services, where they need reliable home and network connections and in some cases require an additional LTE backhaul capability in case both the primary Wi-Fi and MSO Internet connection is down. The creation of Wireless Personal Area Networks (WPANs) will generate a significant amount of new traffic for the MSO. With IPv6 addressability like 6LoWPAN architectures, there will also be an increase in addressing scope.

Protocols such as ZigBee have been designed to minimize the power used by a protocol like IP (Internet Protocol) and create their own connection over a home network that sleeps/wakes to preserve power in the end device. Other protocols such as AllJoyn, OIC, and Thread are TCP-IP/UDP-IP based and drive the power requirements of the end devices higher and are more suited to unconstrained devices with higher power and higher MIPS capabilities.

One of the key elements for consideration in IoT architecture is the MSO Gateway. As we have seen when the 802.15.4 and BLE radios are added to the Wi-Fi radios – it becomes the complete IoT gateway with capabilities to:

- Onboard the IoT devices for connectivity
- Provide protocol conversion at both the PHY and the software protocol level with the addition of the main IoT stacks

- Provide the scope to become a microcontroller for the IoT devices and to provide WPAN functions locally. These functions:
  - Minimize latency for in house trigger/actions
  - Provide a local rules capability to improve IoT experience and minimize the traffic to the cloud
  - Cache local IFTTT actions for improved latency and robustness when the Internet is down
  - Work more efficiently with Cloud IoT controller and rules based systems

While there will undoubtedly be more upstream and downstream traffic to/from the home because of IoT, the MSO can provide a local WPAN microcontroller in the gateway to minimize this traffic while simultaneously adding value with lower latency and robustness in the absence of the Internet. Additional to latency improvements, there is also an added value to security by having the gateway play a proactive role in securing IoT; a topic covered later in this paper.

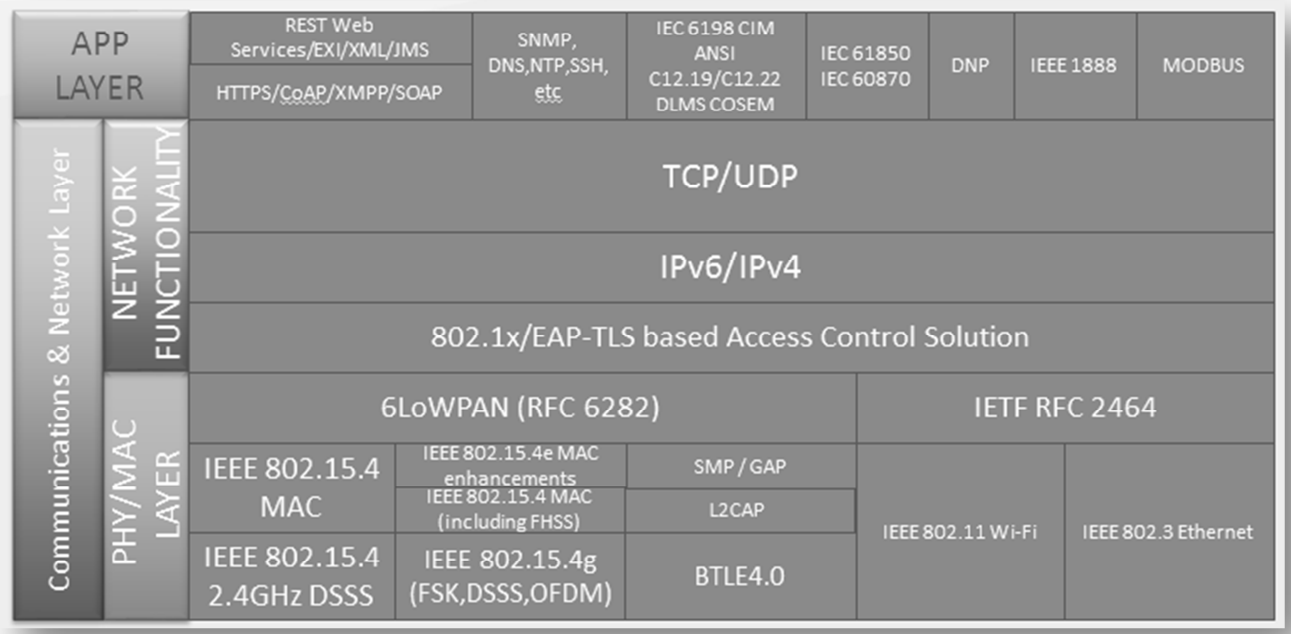

Figure 25 – Example of the IoT protocol stack

IOT will involve a number of different physical layers, primarily focused on low power per transaction. Running an IPv6 protocol over 802.15.4, Bluetooth low energy, and potentially 802.11ah low power Wi-Fi, may all need to be supported at the Gateway in this MSO IoT architecture. While Cloud control of these services is desirable and required in some applications, it will be key to ensure that the gateway supports the ability to apply IoT rules locally to the WPAN.

Data aggregation

The Big Data repository will certainly reside in the Cloud. This will be a key learning and analytics point for macro level views of large data sets. Performance will be

critical as the cloud IoT aggregation service will accept literally billions of transactions per day, some with very low latency demands.

If the actual number of IoT devices even remotely approaches the 26 billion estimate, then the resulting data deluge presents a formidable problem. But is this a 'vanilla' big data (i.e. lots of data) problem, or are there unique characteristics to IoT Big Data? The local gateway microcontroller will be the arbiter for this and ensure that only the true unique data is sent to the cloud aggregator.

Taking patterns, usability, and societal impact perspectives suggests the following distinctive components:

- IoT data is likely to be bursty, both because people and place activity is, and also that anomalous situations (e.g. a storm) are likely to cause large step function changes in data traffic
- Unlike some other data sets (e.g. e-commerce), IoT data can contain long stretches of boring 'life as usual' data, where collection and distribution costs might overshoot the user and business benefit
- Almost all IoT data is personal, so the privacy implications of any breach or misuse are disproportionately high. Even at this early stage in the industry evolution, this issue has caught the attention of the Federal Trade Commission (FTC) who are concerned with these issues
- Given the fragmentation of IoT platforms and devices, any single entity is likely to only have a partial IoT view of the connected home

These characteristics of home IoT data suggest the following attributes to the data aggregation architecture:

- Decentralized data aggregation architecture with CPE level intelligence (and 'Fog Networks'; a contrasting architecture to the cloud in the home) to filter and aggregate 'life as usual' data in latency and cost minimized ways. This augmented with edge intelligence to deal with locale specific responses in low latency ways.
- Dealing with security and privacy concerns via 'limited data window' aggregation technologies in the cloud (and subsequent deletion of the raw data) and edge node summarization techniques that limit the collection and transmission of raw data to the cloud
- An ability to rapidly move data processing functions between cloud, edge and customer premise in response to exogenous network or environmental conditions

IoT and Security and Privacy

The recent press has numerous articles concerning the impacts of poor security practices, as well as on attacks on systems thought to be secure. Introducing new IoT devices that are connected to the outside world magnifies the problem of security.

These devices have access to new data about the home, and about the people living there, report that data, and exert controls on the home environment. Security for the Internet of Things is absolutely an essential aspect to provide, or the IoT will be a source of new attacks compromising consumer privacy and device functionality. For devices that relate to medical data, or significant environmental control, security weaknesses could even create serious consequences for the consumer. Additionally, we see that 20% of people are not comfortable with adding devices because of security and privacy concerns. Privacy is front of mind of many consumers and probably one of the biggest inertia factors for use of sensor devices with video (cameras) and audio.

What should the attributes of a secure IoT implementation be? At a high level, a secure IoT system must protect the privacy of the individual, and by extension, all sensor data collected that pertains in any way to that individual. When an infrastructure server element must process such data, only the required data should be provided for the functions expected, and any Big Data examination of such data must be anonymized. For IoT devices that exert some control over the environment, control commands must be protected against hacking. Entry points to the home for any specific control must be minimized to that system exerting that specific control. The following sections provide specifics.

Privacy and IoT Devices

Even with device robustness, communication security, and public key identities, IoT devices require an additional type of protection. Quite often, the patterns of sensor reports themselves can convey information that needs protection. For example, if cameras are set to report movement only, then the absence of reports may indicate the home is not occupied , and a convenient target for criminals. In such a case, occasional (encrypted) reports need to be issued that in fact report no movement, to break these patterns. Another type of attack might involve moving devices between homes to spoof information or behavior. Location needs protection by including environmental information to assist in proving identity. As an example, a router might report the networks it discovers near the home, including SSIDs and RF channels.

This sort of information is only "approximate" in the sense that it is not repeatable. However, algorithms exist to determine enough similarity to identify location in this fuzzy logic sense.

Key elements in the privacy model that need additional work may include some or all of the following:

1) Leveraging the security models built into solutions like AllJoyn, OIC, and Thread, but not relying exclusively on them.

2) Adding additional security layers over the standard solutions may be a way of adding additional differentiation to the service provider's IoT solution. A particular device or protocol may report being hacked in some OTT environments. However, it may not be hacked in the MSO additional security layer.

3) Making it more difficult to hack an MSO IoT solution using additional information about the home relationship to the device particularly for onboarding could be a key value-add differentiator. The service provider already has trusted elements like a gateway and set-top to use to validate the correct presence of the new device and aid in the security of both onboarding and persistent communications.

4) Developing anti-spoofing solutions for IoT devices to make sure they are authenticated and the right connection chain authenticates their authorization in the home environment.

5) Developing solutions to mitigate against repetitive 'tell all' patterns that may determine who is home alone, if anyone is home could be an important security and privacy solution.

6) In particular, for video and audio devices, ensure that this traffic is transparent for the user with leverage of TV UX for camera and audio sensor transmissions. Also, include gateway and IP level traffic blockers when the home owner is not comfortable with camera and audio sensor devices from third party sources.

7) Make this easy to do and potentially incorporate a privacy button on a remote control, offer modes that when there is presence of one or more of the inhabitants no external transmission of camera information is made.

Communication

All communications between IoT devices and any related servers must be encrypted and authenticated. Typically, for IP end points, web security standards such as SSL and IP-Sec should be employed. All end points should have X.509 public key certificates and keys, signed by accepted and validated trust authorities. Unfortunately, many simpler constrained IoT sensors and devices are not IP and security capable and may use other protocols like ZigBee to a hub that then provides security solution. This IP gateway node in the home serves as an intermediary, providing the IP security desired for the node, and the translation to simpler forms of networks and security.

Consumer Data Access Management

All sensor or media related data collected within the home, and intended for processing in an infrastructure server, belongs to the consumer. The consumer must be able to define its permitted usage in all respects. Some collected data remains within the home for access by the consumer; other data must be passed out to a server node for processing and response. Typically, different device classes are associated with different such servers. Thus, the consumer must be able to set which data can go to which server, and permit specific controls to return from specific servers. This data access management function is akin to the permissions requested for each Android and iOS application installation. However, too often those requests are simply "rubber stamped" by the consumer. In the IoT system, data management has to be available in a user-friendly manner, clearly setting forth the impacts and purposes of the devices in question, and the related data and control. In many cases, the consumer would not understand the subtleties of data management.

Fortunately, recent federal laws are helping IoT component manufacturers steer clear of deceptive practices. IoT devices will be held to the higher standard of identifying clearly the data required as mandatory for the device to work, and optional for additional functions. Further, this minimum access set must be the default set-up. Once the data is processed at the server, any use of that data in a Big Data aggregate is optional, and must be agreed in advance by the consumer. If so agreed, the data still can never be identified as to the consumer it is associated with, without additional agreements in place.

Remote Access

In many use cases for IoT devices, the consumer can remote access infrastructure servers or in-home gateways to effect control or check status. Such communications falls within the "always encrypted and authenticated" regimen described above, but often the mobile devices used are generic non-IoT devices, and access of this type is quite often logon/password in nature. This should not be the preferred mechanism for remote access, as it is subject to hacking and attack. Password attacks are well described in the literature. Fortuitously, the Wi-Fi standards community has created a new approach based upon installed certificates and keys, called Passpoint. IoT remote access should employ a similar public key identity based approach, or perhaps Passpoint itself.

Device Robustness

Often security systems focus on the communications between devices, and not on the devices themselves. However, in commercial video delivery, very robust in-

home platforms have been built cost effectively, where all devices boot securely, have only signed authorized code on them, and where physical access to keys and cryptographic functions is prevented. This should be the high ground for all in-home IP connected nodes for IoT systems. For devices that conform to simpler standards, robust designs should be encouraged as an evolutionary path.

SUMMARY

The Internet of Things (IoT) is at the peak of inflated expectations. With even a small percentage of the predicted numbers of devices involved and potential revenue realized, the benefits are substantial to consumers in terms of lifestyle and businesses in terms of productivity and profitability. Additionally, the impacts to the interconnecting networks will be considerable as the trends are already pointing to tens, if not hundreds of devices, connected per person. The opportunity to excel at or surrender to the impact of IoT will be based on designs with consumer value in mind, scalable network architecture, meaningful data analytics, and attention to matters of data integrity. A sound model for security and privacy of devices through the life of the device and the end user has not been developed and should be point of focus both in technical and business policy synthesis.

The MSO has several differentiated capabilities to leverage their success while participating in the IoT. Cable networks are well positioned to handle the new influx of telemetry and control points. Big Data capabilities already in place for triple-play services can be adapted for the new commodity of sensor data. Operations, Administration, Management and Provisioning (OAM&P) facilities provide the foundation for onboarding and service assurance of IoT devices, although currently are not capable of accepting the wide variety of device types. MSOs have a prominent position on the screen most used in the home, the television. Coupled with voice control and eventually voice response, the television is very convenient and useful, particularly with the graying of our population.

A business plan for the IoT related business should involve facilitating a wide range of consumer-selected devices to offer data and control to and through the cable network. This step allows both the collection of data sets for analytics and the ability to integrate into MSO provided user interfaces on television, mobile, web and telephone. The business models discussed in this paper suggest the need to reduce the equipment costs associated with today's smart home solutions to allow ease the ability to achieve large-scale deployment and allow profitability with one or more services that generate revenues in the order of a few dollars / month. Large-scale deployment is needed to collect a sufficient data set to attract advertisers and other target markets for B2B2C opportunities.

The technical solutions outlined in the paper involve several recommendations for standard technologies involved with communications and device ecosystems. These areas are relatively immature and likely to see entrants, exits, and consolidation therefore a pluggable architecture is recommended. A set of recommendations for fundamental inclusion of robust security capabilities is key to ensuring the emergent IoT remains in positive light during its formative state.

Contributing Authors

Paul Moroney
Venu Vasuvedan
Ian Wheelock
Wade Carter
Mark Bugajski
Eli Baruch