SCTE·ISBE CABLE-TEC EXPO 2018 ATLANTA, GA OCTOBER 22-25

2018 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS

Internet of Things Dynamics: Opportunities and Challenges for Broadband Network Operators

A Technical Paper prepared for SCTE•ISBE by

Tim Johnson
Director, Global Product Management
Alpha Technologies
360-392-2234
Tim.Johnson@alpha.com

Arun Ravisankar
Sr Engineer
Comcast
215-286-7558
Arun_Ravisankar@cable.comcast.com

J. Clarke Stevens
Principal Architect
Shaw Communications
587-393-0605
Clarke.Stevens@sjrb.ca

Chris Bastian
SVP/CTO
SCTE-ISBE
610-594-7304
cbastian@scte.org

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

Introduction

Cable network operators are always looking for ways to add services for their customers, especially so since the 1990s. To name a few: Data over cable, then voice, then DVR evolving to nDVR, were added to the service bundle. More recently home monitoring and security services have also been offered by many operators. [1]

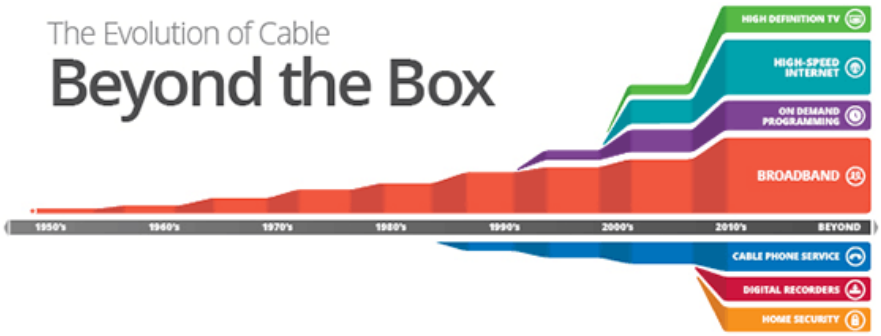

Figure 1 - Evolution of Cable Beyond the Box

Source: calcable.org

The Internet of Things is loosely defined as Internet-connected sensors in homes, businesses and public spaces, as well as the data analytics monitoring of those sensors back in the data center. With the Internet of Things, there is an opportunity to rapidly open up entirely new service opportunities that can differentiate cable network operators from their competition. However, the primary challenge will be to smoothly install, operate and integrate these new services with the operator's existing service bundle.

Cable network operators are uniquely positioned to offer IoT services to new and existing customers. They have four characteristics that industry start-ups and OTT service providers covet:

- Existing service location in millions of homes, businesses, and public spaces
- High speed and reliable network connectivity
- Power for sensors and gateways
- An existing and localized/in-market fleet of fulfillment technicians

Cable network operators have a well-established presence in the home including cable modems, home gateways, set top boxes, Wi-Fi extenders and home security hubs, however the evolution to new services - such as connected healthcare, and smart homes – will require new devices and sensors, as well as increased care to ensure the highest network performance while preventing security breaches.

1. The IoT Service Opportunity

Gartner, Inc. forecasts that 8.4 billion Internet-connected things were in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020. Total spending on endpoints and services will reach almost $2 trillion by 2020. [2]

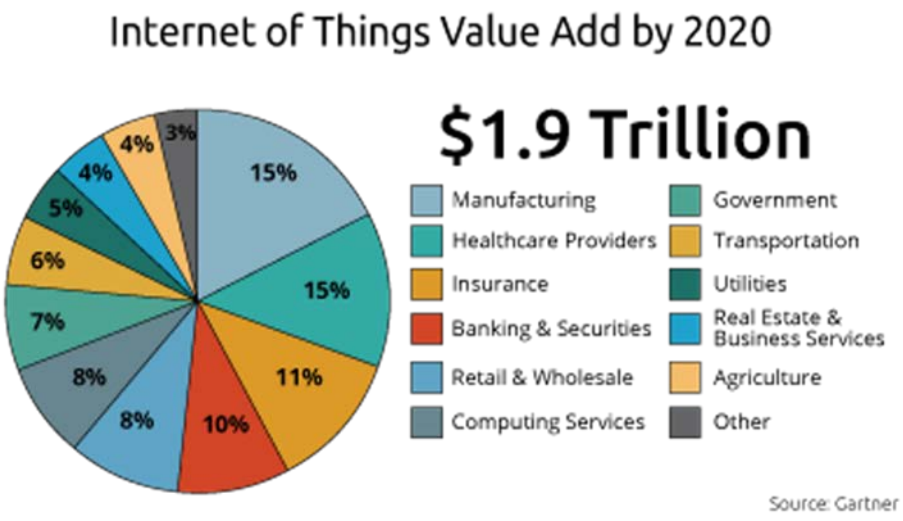

Figure 2: Internet of Things Value Add by 2020

How big of this market share will the cable network operators capture? The service cases are expanding, as are the number of customers. Will the cable industry focus on these service sectors? Recent press releases seem to indicate that they will. Comcast launched its low power, wide area network, machineQ, in July 2017 [3], and Cox followed suit with Cox2M in March 2018 [4], each focused on rapidly introducing IoT services to their customers.

The SCTE Data Standards Subcommittee, and Internet of Things Working Group

SCTE·ISBE STANDARDS

Established in 1996, the Data Standards Subcommittee (DSS) develops standards for the delivery of digital service supporting high-speed data, video, VoIP, and other services over cable networks.

The Internet of Things working group was announced on October 31, 2016 as an entity under DSS, and conducted its first meeting on November 16, 2016. [5]

The IoT working group's charter is to facilitate communication between service providers and industry partners to standardize new IoT-based services. The working group aims to make standards and operational practices deployable and manageable for service providers, as well as focusing on the vast use cases available in the IoT community to support service providers' business objectives. The early focus of the working group was to develop use case descriptions, which will be outlined in the following sections.

1. IoT Use Case Descriptions

One of the leading categories in IoT use cases is in home monitoring, and specifically home automation, home security, and connected healthcare. This section details those use cases.

1.1. Home Monitoring

The Home Monitoring use case mainly spans two broad sets of applications, described here.

1.1.1. Home Automation

Home automation applications provide services that augment the capabilities of devices and sensors in a home, and help customers to seamlessly access these services. Automation is intended to provide ease of use and access to products and services, while simultaneously helping with overall energy conservation.

Home Automation may include managed devices, like Door/Window Sensors, Motion Detectors and the building of rules engines that could operate and control other devices. For example, some use cases could be to detect motion, operate lights/STB/TV, or to open/close a garage door.

Home automation also plays an important role in providing safety-related features, like smoke detectors and flood sensors. These sensors can trigger actions which include raising alarms for appropriate help as needed.

Home automation applications include integration with personal voice assistants, and other smart devices in the home that are capable of connecting to a network and exposing APIs to control their actions. Examples include smart speakers, thermostats, washers, bulbs and many more. Figure 3 captures many home monitoring devices.

Figure 3 - Devices in a Home Monitoring Use Case

1.1.2. Home Security

Home Security, as the name implies, is designed to secure the premise with the use of IoT sensors. Customers could opt in to receive alerts when certain anomalies detected. Additionally, a third-party service can provide verification of any events or activities, and possibly contact the user or law enforcement based on the indications/events.

The evolution of IoT and smart home applications has increased the demand for residential security products. Apart from traditional security requirements, IoT security is also gaining importance to ensure

data and device integrity in a smart home. Various research findings suggest an increased need for home security systems to reduce burglary-related emergencies. In most cases where burglaries have been reported, one of the major causes is that the home owner has forgotten or neglected to close doors or windows. A typical home security system, when set in "armed" mode, will detect any such anomalies and alert the user. This is a huge relief for the home owner, and illustrative of the tacit benefit that is peace of mind.

It is important for any Home Security system to have redundancy in backhaul connectivity in case there is an attempt to sabotage the primary internet connection, which is the broadband cable internet. Home Security systems tend to have backup cellular connectivity in case there is a drop in broadband connectivity.

Figure 4 shows the behavior of a home security system when an event occurs. The system, when in "Armed" mode, detects if any door/window is opened and alerts the user. However, there are efforts underway to use AI and Machine Learning tools to analyze data from all sensors in a home to determine if there is no one in home and if the customer has forgot to "Arm" the system.

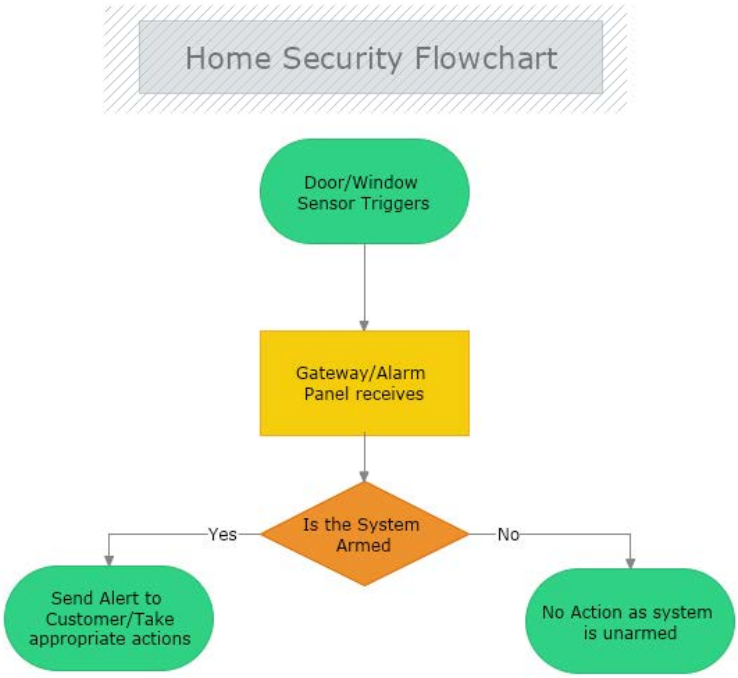

Figure 4: Home Security System Flowchart

1.2. Connected Healthcare

IoT technologies can impact a lot of healthcare use cases and can bring peace of mind to customers. These technologies could also assist Medicare professionals by augmenting them with information when providing medical care to patients.

Health and wellness applications, generic or specific, could target a large set of population. Examples include fitness-based applications that help consumers track and organize their health data, and to plan daily activities and exercise routines.

Another major area where IoT could play a major role is in eldercare. Studies show that there is significant growth in the senior population in the coming years, as the Baby Boomer generation enters its twilight years. IoT is poised to offer applications that facilitate aging-in-place -- because personal independence is a high priority for Senior citizens.

Healthcare use cases include the following:

- *Home Health and Tele-Medicine Applications:* Bridging between FDA-approved home health devices (blood pressure cuffs, glucometers, asthma dispensers, etc.) and medical professionals/caregivers, via Bluetooth-to-LPWAN adaptors.
- *Health and Wellness applications:* To meet and extend people's health/wellness goals.
- *Remote Patient Monitoring:* To extend the reach of Internet-connected devices by bridging between short- and long-range networks.
- *Aging in Place applications:* To extend the range of ADL (Activities of Daily Living) that are often stressed by age-related consequences, such as falling.
- *Responding to Emergencies:* To make it faster and easier to get urgent care.

Various studies indicate a gradual increase of Internet users among people aged 75 years and older, as well as an increased level of smartphone ownership. This growing segment of connected Seniors similarly indicates that IoT could play a major role in enhancing lifestyles. Notably, the population of those aged 65 and over has increased from 36.2 million in 2004, to 46.2 million, in 2014 -- a 28% increase. The Senior population is projected to more than double, to 98 million, by 2060. [6]

As Internet adoption increases within the Senior community, it represents a major tool for providing value-based services:

- Applications like ADL monitoring and remote patient monitoring would help reduce the number of visits to a care provider. This would also help reduce the burden on conventional healthcare systems (such as hospitals and clinics.)
- Medicare has begun implementing incentives to reduce hospital re-admissions, which has stimulated the growth of remote patient monitoring. Efforts like the Hospital Readmission Reduction Program (HRRP) actually penalizes hospitals, financially, if they exhibit high rates of Medicare readmissions. [7]
- Remote patient monitoring could be used to source and convey health and wellness information, so as to:
    - Provide first-hand information to users and care providers (family members, medical personnel)
    - Encourage patient adherence to medical protocols (medications, exercise)
    - Enable caregivers and medical providers to plan and adjust the course of action
    - Help individuals to make lifestyle choices fueled by individualized data
- Apart from eldercare, these technologies could also be tailored to assist patients or otherwise vulnerable family members with chronic conditions.

Connected health applications offer services to consumers and caregivers (professionals & personal/family members.) These applications provide a platform on which the patient and caregiver could interact, exchange data and configure alerts. Such services would provide appropriate information and alerts to a family member or care provider, so that corrective action could be taken. For instance, it is an invaluable peace of mind for a son or daughter who no longer lives near an aging parent, to know that

medications are being taken as scheduled, or that something abnormal or problematic is happening (or, preferably, not happening!)

Remote patient monitoring typically includes:

- *Activity Monitoring:* Tracking activities and detecting abnormal or emergency situations, like a fall event or an incapacitation. Fall detection or incapacitation could be used to trigger a PERS (Personal Emergency Response Systems) event. Figure 5 shows how activity monitoring applications could be used to monitor activity of elders for an aging-in-place application. These could also be used for fall detection and raise alerts for help when such an incident occurs.
- *Biometric Monitoring:* Measuring body vitals, like blood sugar, BP (blood pressure), weight; establishing a secure health data record which is monitored constantly; predicting future anomalies; reducing risks. Figure 6 shows examples of devices that are used to monitor body vitals. These devices are BLE- (Bluetooth Low Energy) enabled and data could be sent and analyzed by medical care providers.
    - Data collected could be put into analytic engines and trends could be analyzed. Figure 7 shows a sample trend related to Blood Pressure.
    - These trends indicate the progress and well-being of the patient.
    - Use of AI/ML combined with IoT technologies could help bring *Sensors to Insights*
- *Patient Adherence:* Ensuring that patients follow their doctor's orders; providing appropriate reminders to patients and family members, such as for medication refills.
- *Virtual Visits:* Meeting doctors or care providers over a video conference, rather than a face-to-face meeting, which with Seniors often involves collapsible wheel chairs and a considerable amount of extra effort for everyone involved.
- Other applications include access to electronic health records (EHRs), to help doctors and care providers optimize a patient's health with vital information.

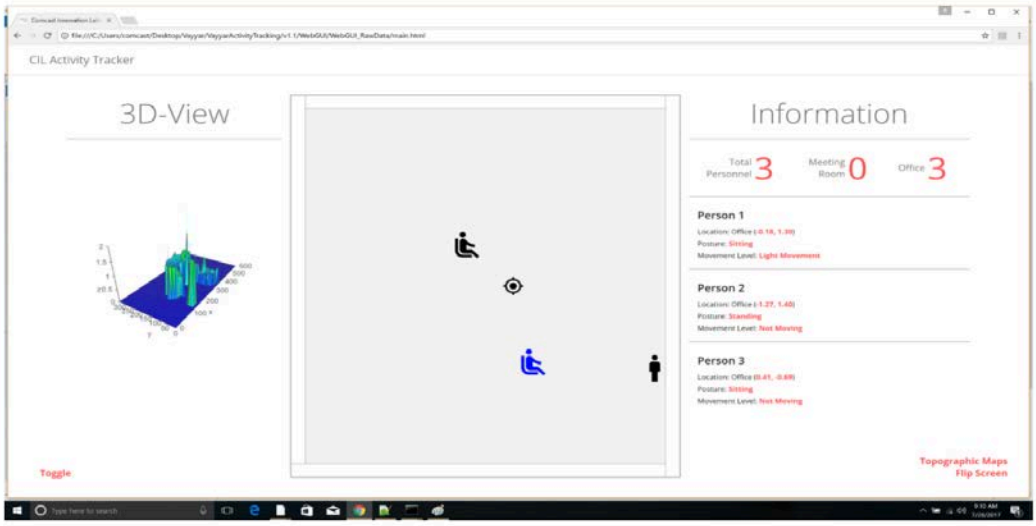

Figure 5: Activity Monitoring Applications

Figure 6: Biometric Devices used for Remote Patient Monitoring

Figure 7: Trend Capture and Monitored Data

1.3. Smart Cities/Mobility

In December 2015, the U.S. Department of Transportation (U.S.D.O.T.) launched the *Smart City Challenge*, asking mid-sized cities (200,000 – 800,000) across America to share their ideas for how to create an integrated, first-of-its-kind smart transportation system that would use data, applications, and technology to help people and goods move faster, cheaper, and more efficiently. [9]

By challenging American cities to use emerging transportation technologies to address their most pressing problems, the Smart City Challenge aimed to spread innovation through a mixture of competition, collaboration, and experimentation. But the Smart City Challenge was about more than just technology. The U.S. Department of Transportation (USDOT) called on mayors to define their most pressing transportation problems and envision bold new solutions that could change the face of transportation in U.S. cities by meeting the needs of residents of all ages and abilities; and *bridging the digital divide* so that everyone, not just the tech-savvy, can be connected to everything their city has to offer.

Of the approximately 100 cities which fit this criteria, 78 quickly activated cross-organizational (City; State; Private Enterprise; NFP, etc.) teams to submit comprehensive applications for the $40M which the USDOT put forth for the winning bid. [9]

The powerful two-fold message of this fact:

1. The USDOT recognizes that the "Smart Transportation/Mobility" is at the core of the Government's perspective on what is foundational for a "Smart City".
2. The vast (78%!) majority of cities either have, or are rapidly seeking to have, leadership and/or funding in place to immediately enact Smart City initiatives.

The relevance ("so what") for the Cable Industry, MSOs and supporting eco-system?

In order to enact many of the use cases which are associated and envisioned for "Smart Mobility/Smart Cities", there are fundamentally three core infrastructure attributes which are required:

1. Power
2. Communications Backhaul
3. Real Estate (site)

Enter the HFC Network. Given the near ubiquity of this network throughout America (either aerial or subterranean) the enablement of strand-mounted "gateway" devices provides the opportunity for rapid and cost-effective deployment of several types of Smart Mobility-effecting IP-based devices, including, but not limited to: small cells (NB-IoT); Wi-Fi access points; IoT (LoRa), and Security Cameras.

The diagrams below demonstrate the architecture, based on actually deployments, of two of these areas:

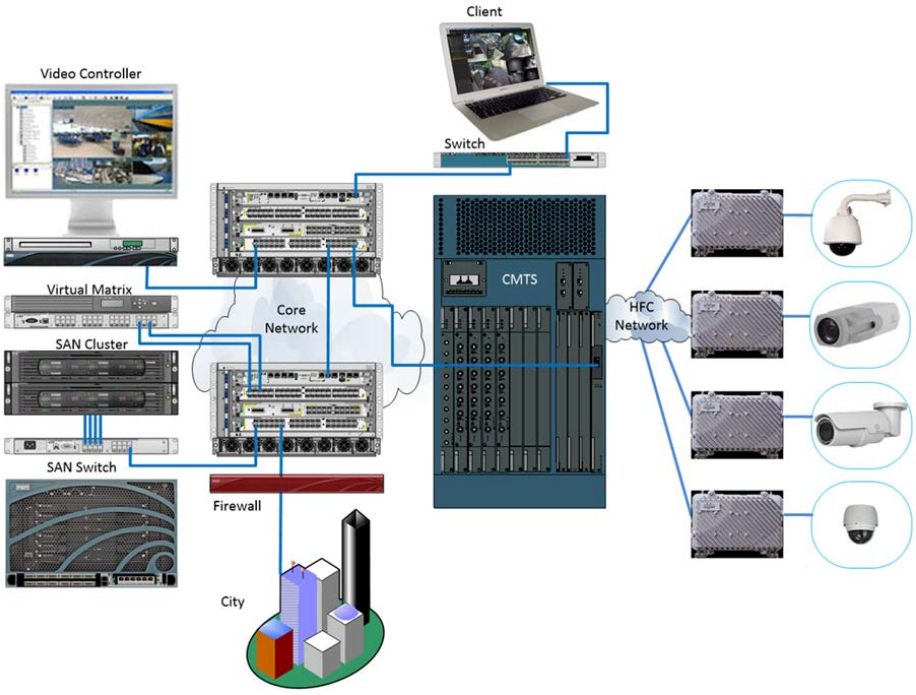

Figure 8: Network architecture supporting Security Cameras

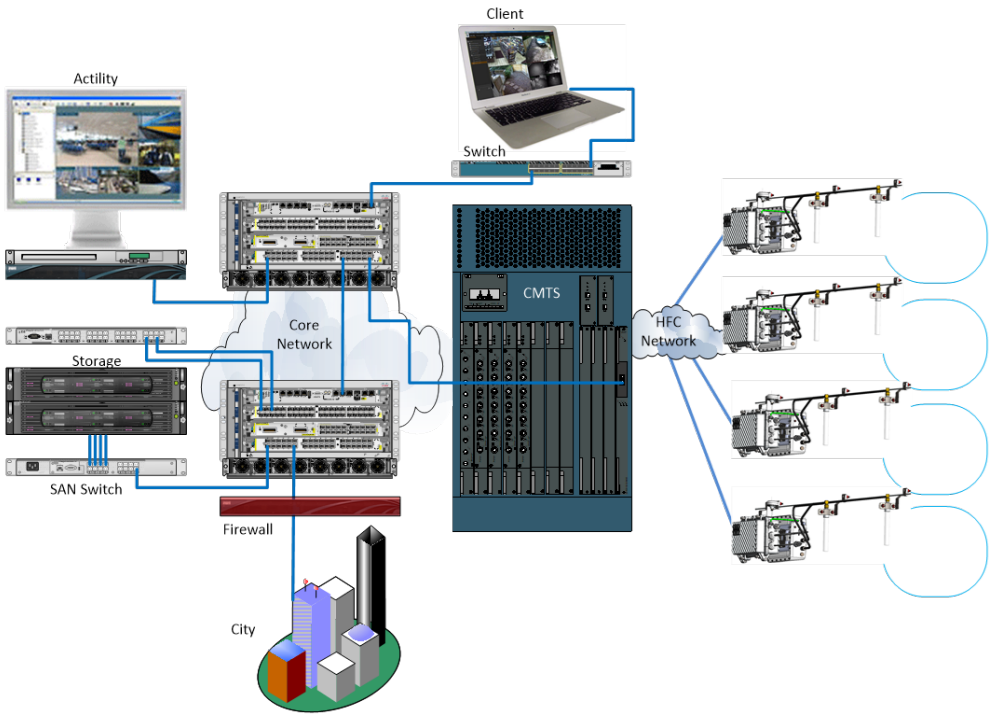

Figure 9: Network architecture supporting LoRaWAN

Question:

In addition to these "ready to deploy" Smart Mobility/Smart City technologies, what could be the next BIG thing that the HFC could enable across the country?

One Answer:

Digital Short Range Communications (DSRC) to promote safer, more intelligent transportation systems.

DSRC is a two-way short-to-medium-range wireless communications capability that permits very high data transmission critical in communications-based active safety applications. The Federal Communications Commission set aside 75 MHz of spectrum around the 5.9 GHz band (5.850-5.925 GHz) band in 1999 to be used for vehicle-related safety and mobility systems. [9]

The USDOT has identified more than 40 use cases for vehicle to infrastructure (V2I) technologies, such as:

- the ability to pay for parking and tolls wirelessly
- identifying when a car is approaching a curve too quickly and alerting the driver
- adjusting traffic signals to accommodate first responders in an emergency; and
- alerting drivers of conditions such as road construction, among many others

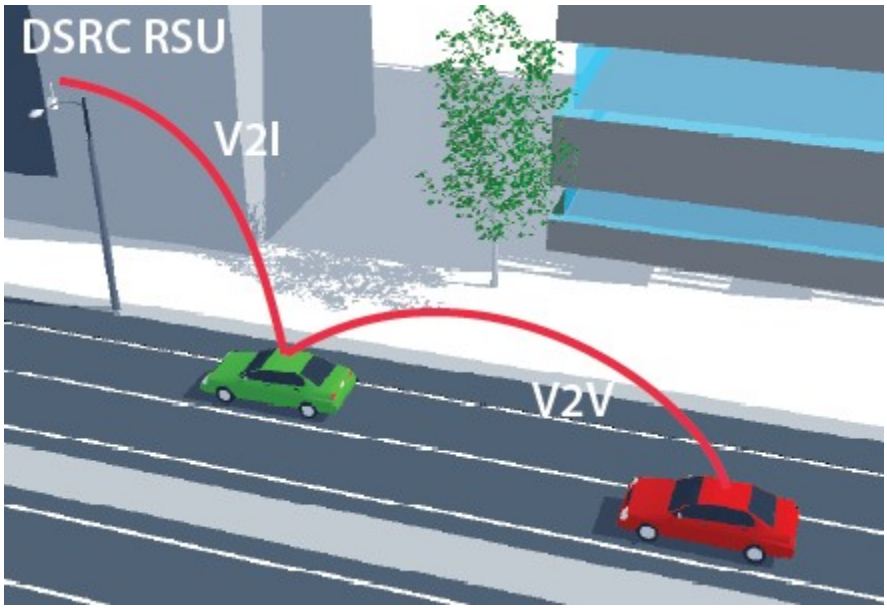

Figure 10: Demonstrating Vehicle to Infrastructure (V2I) and subsequent Vehicle to Vehicle (V2V) communications via DSRC and the network of Road Side Units (RSUs)

The current major roadblock in deploying the DSRC wireless network? The need for efficiencies in deploying Roadside Units, or RSUs, relative to three core attributes: Power, Backhaul, and Real Estate.

Current RSU deployment topology is focused on "traditional" sources of these needed ingredients, as portrayed below using a combination of Utility Power; available Street Furniture (such as traffic lights), and, more often than not, Wireless Backhaul:

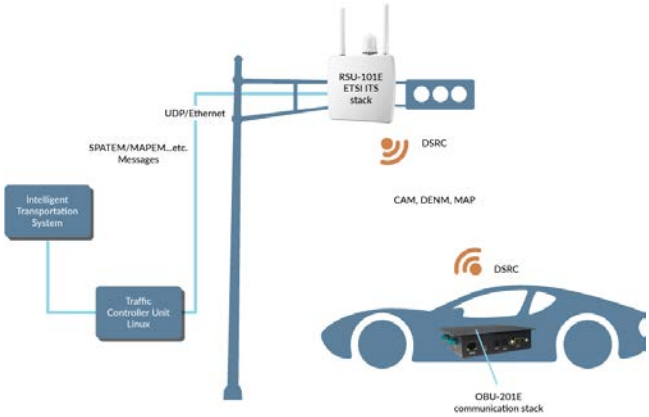

Figure 11: Traditional RSU deployment

This conventional wisdom is largely driven by a lack of general understanding of the value proposition offered here:

1. The HFC Network provides a high-speed, QoS-based, communications network, with diverse, backed-up power, provided via strand-mounted gateways which are deployed on "real estate" in an almost unlimited footprint of deployment choices.
2. RSU Devices are generally powered by PoE+ (under 50W load), and transmit approximately 300 Yards.

The *new message* which could/should be promoted to all stakeholders:

The HFC Network provides an ideal solution to quickly and efficiently deploy RSUs in the scale required to effectively realize the dream the USDOT envisioned in 1999…*Safer and Smarter* (more Intelligent) transportation systems for citizens across the country.

In summary, in order to enact a significant core of the most cutting-edge technologies and resulting Smart Cities/Mobility use cases, one of the most iconic and legacy infrastructures of the last century could and should be quickly re-energized to perform a vital 21st century service:

The over 1.5 million miles of America's HFC Network.

2. IoT Perspectives from Network Operators: Developing, Operating and Maintaining Consumer IoT Services

Estimates for the market size of IoT vary greatly. Most estimates show strong growth of around 20% year-over-year. Other predictions aren't nearly so conservative. One thing is for sure, almost all analysts see the market as big and growing. The variability is due in part to the virtually unlimited perspectives of the market. The smart home is perhaps the most visible manifestation of the IoT market to most people. (People have always talked to their appliances, but it's hard to avoid the wonder of having the appliances listen.) It seems that the home market is probably one of the less profitable sectors. Corporations have a financial incentive to use IoT to increase productivity and they have more cash to invest. It's true that knowledge is power and by that measure IoT is a revolution. It's not only feasible to know virtually everything about your product and its production instantaneously, the sheer volume of data and the automated analysis of that data allow for insights that a human is never likely to discover.

The good news is that this information and control is available to operators at a reasonable cost. The bad news is that it's available to your competitors at that same cost. So how can IoT be advantageous to cable? The key is to look at the differentiation cable has built through decades of intense investment in a service industry:

- Cable has a monthly financial relationship with the customer.
- Cable has a fleet of skilled technicians who visit customers in person at their homes.
- Cable has equipment in customers' homes and the physical plant to reach those homes. That equipment is connected to the headend twenty-four hours a day.

These advantages, however, come with challenges. A monthly bill has never been attractive to the customer paying it and increasingly, they are presented with options that are based on actual consumption.

Our skilled technicians are often not qualified in the skills that customers want. Engineers are not always great salespeople. The sheer volume of IoT devices makes it almost impossible to know which options will best serve the customer.

The physical plant is always in need of an upgrade and increasingly customers are choosing the freedom of wireless infrastructure that is also striving for continuous reliability improvements.

In order to understand how the cable infrastructure can be effectively leveraged, it is critical to look at customer pain points. Some of the most important include:

- *Lack of interoperability* – Customers are looking for solutions to their challenges. Those solutions often come from different vendors who rely on different ecosystems. This diversity is never going away, but that is a problem that providers must address. Consumers can't.
- *Security* – There is legitimate fear around the security of the network and IoT solutions. As IoT devices become more ubiquitous and easier to use, they pose an increasingly attractive resource for bad actors.
- *Management* – Most customers are unqualified to be system administrators and have no desire to assume that role, just as most drivers are unqualified to be auto mechanics. Operators need to find a way to economically provide this service.

The market is indeed big and growing. [10] Cable does have some intrinsic assets that provide an advantage. However, that advantage is a head start, not a reservation. MSOs need to quickly establish the efficient infrastructure to provide the best and most responsive service to customers while leveraging the very features of IoT to run that infrastructure efficiently.

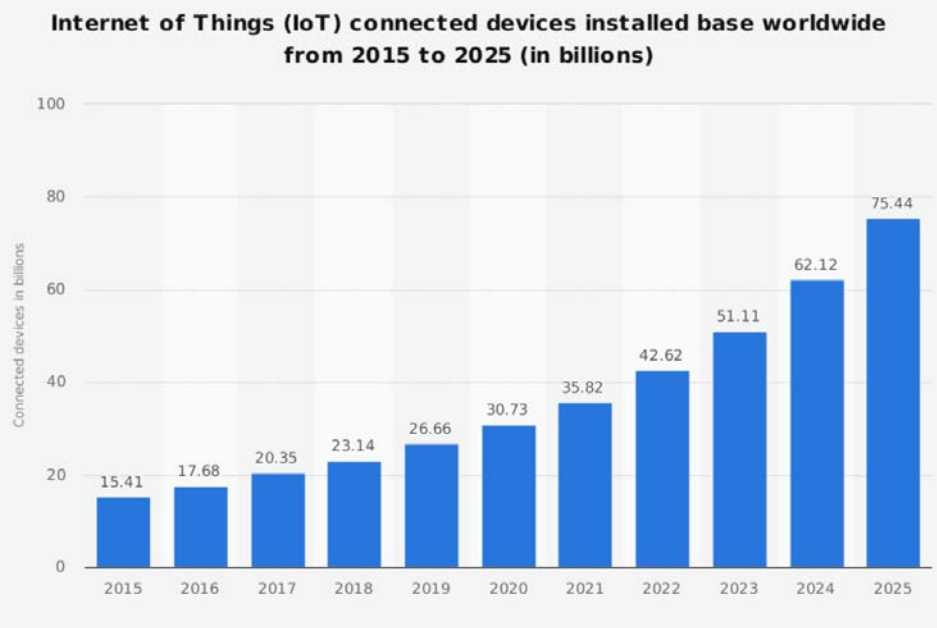

Figure 12: IoT connected device growth forecast

Source: Statista

3. Technical factors

3.1. Protocols and Standards

IoT applications use a wide variety of signaling protocols and standards. Most IoT devices today are based on the following communication protocols:

- Zigbee
- Bluetooth Low Energy (BLE)
- WiFfi-based devices

Figure 13 shows a typical representation of protocols that are generally associated with IoT applications. [11]

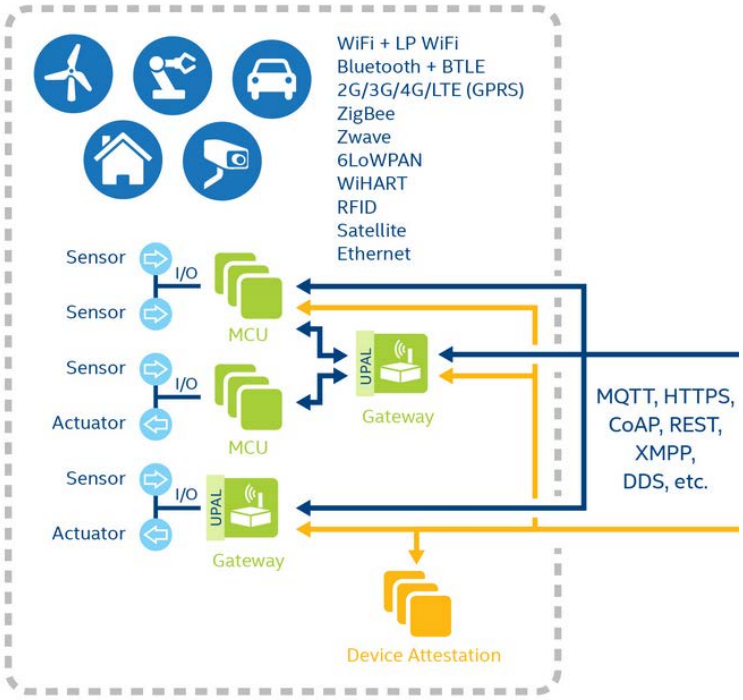

Figure 13: Network Protocols supporting IoT applications

As part of the application design, it is important that the service provider infrastructure supports these protocols and hence serve a large number of devices that connect to the network.

One of the major design aspects is the coexistence of all these protocols and how to best bridge them on to a network, as well as reliably transfer data for analytics and processing. Challenges include working with multiple protocols, hardware and software implementations. Signal interference is another challenge which leads to data loss and may impact some critical functioning of the system.

The action of "rules engines" and devices depends heavily on how each device in the system (home) functions, irrespective of its type, power source, or data model. It is very important to monitor all devices and to ensure all of the devices have the right configurations (software, settings, and battery level).

3.2. Security threats and security solutions/best practices

Systems and applications need to be secured from unauthorized access, and to protect sensitive information. Connected devices lead to an increased risk of being exposed to attacks, and as such need elaborate security measures to provide these safe and secure services to the customers.

Incidents are routinely reported where peripheral devices in an IoT network have been compromised by DDoS attacks.

The attack surface of IoT devices are greatly increasing as operating systems and communication stacks are becoming more complex. [12] Further, the IoT-related firmware typically includes open-source components, and code written by large distributed teams. It is the service provider's goal to ensure that

the number of penetration points and attack vectors are minimized for its deployed IoT devices. However, if the attacker manages to penetrate the device, the impact to other devices in the network should simultaneously be minimized.

Trusted devices, with a Root of Trust, provide additional security. Unmanaged devices could be monitored for the data patterns being sent and received by the device. For example, a thermostat which is expected to receive settings and report status could be suspicious if the device is suddenly observed to be generating heavy data traffic and communicating with unintended destinations.

Industry groups like OCF (Open Connectivity Foundation) help in specifying device attributes and helping monitor the network status.

3.3. Operational factors

3.3.1. Training the workforce to install and operate a network of home-based IoT sensors and objects

It is very important to effectively train the customer-facing workforce to address issues relating to IoT services. Conventionally, the service provider's call center receives calls when there is an issue with any of the devices (including unmanaged devices) in the premise. Our customer care professionals need to be equipped with the necessary tools to understand the problems associated with IoT services, so as to authentically help the customer in resolving the problem.

Another important aspect is installing and configuring devices on the network. Professional installation involves finding the right spots in the home to install devices like motion sensors and other IoT devices. The technician needs to consider such things as sensor range, number of sensors needed, and interference issues. The technician needs to be equipped with the tools which can help them effectively troubleshoot issues with both installation and maintenance.

Device configurations and software also need to be managed that include new feature updates and bug fixes.

3.3.2. IoT supporting IoT

One of the best ways to support a robust IoT infrastructure is to use IoT in that support. IoT can be viewed from two sides: One side looks at the benefits of connecting real-world devices to the Internet so that they can be monitored and controlled. The other side looks at the data that a constellation of IoT devices generates and sees that as a rich resource for understanding and improving IoT service.

There are the obvious observations of knowing when equipment is on and off, and the direct information that can be queried from an individual device. This sort of information is good for customer service personnel and can be directly leveraged on a customer call.

What may be more valuable, however, are inferences that can be made on an aggregate basis of massive amounts of data that are statistically evaluated to get insights that are less obvious. This information is yet another tool that can be used in the ongoing field of proactive network maintenance. While there are many benefits to the science of using tuned signals to isolate the location of a network fault, that information becomes even more valuable if the traffic traversing that network can be dynamically understood. If active elements in the network can be remotely controlled to instantly repair or avoid the breach automatically and without an immediate truck roll, the savings quickly accrue. If data can be used to provide a predictive diagnosis, potential problems can be avoided altogether.

IoT makes this possible by providing intelligence to all equipment connected to the network with a big data analytics infrastructure to collect, analyze and actuate the IoT network elements. Network operators are unlikely to be the creators of the various IoT devices on the network. However, they can define a common network infrastructure that will improve manageability for the operator and provide a target platform for vendors. For maximal efficiency, this platform should have the following features:

- *Interoperability* – While the different advantages of various network technologies ensure that there will never be one network that everyone agrees upon, the Internet has shown us that different networks can be made highly interoperable. The cable industry should adopt an upper-level IoT network that allows for these different technologies underneath, while providing the commonality required to make the technologies work together.
- *Security* – It is clear that operators will be expected by customers to insure the integrity of the network and a safe environment for their data. If MSOs will have to address any breaches, it makes far more sense to prevent those breaches in the first place.
- *Standards* – The challenge of providing a reliable, interoperable, and secure IoT platform is not something that can be done in isolation. Just as DOCSIS is responsible for the industry's broadband vibrancy, the next generation of the cable industry will rely on a standardized IoT infrastructure that can support consumers, businesses, government and industry. It will also benefit itself by providing the information and equipment to significantly maintain itself autonomously. The Internet of Things must be supported by international standards that address not only the needs of customers, but also the needs of operators, equipment makers, chip providers and every participant in the IoT chain.

4. Conclusion

The Internet of Things is viewed as many different things by different participants. However, one thing is clear: For cable operators, it is not simply a new product category, it is a new platform for products and services. Cable has been through this before. While many predicted the demise of cable, they neglected to acknowledge cable's evolution. Indeed, if cable were still based on analog television services, it would be irrelevant. But that's not what happened. Cable evolved to digital services, changed the basic structure of its network and became the premier operator of Internet access. Now it's time to evolve again to be the premier platform for the Internet of Things – a common platform that will serve consumers, businesses, government, industry and itself.

5. Abbreviations

ADL	Activities of Daily Living
AI	Artificial Intelligence
AP	Access point
BLE	Bluetooth Low Energy
DOCSIS	Data over coax service interface specification
DSRC	Digital short range communications
DSS	Data Standards Subcommittee
EHRs	electronic health records
HFC	Hybrid fiber coax
HRRP	Hospital Readmission Reduction Program
IoT	Internet of Things
ISBE	International Society of Broadband Experts
LoRaWAN	Long range wide-area network
LP-WAN	Low-power wide-area network

ML	Machine Learning
NB-IoT	Narrowband Internet of Things
nDVR	Network digital video recorder
OCF	Open Connectivity Foundation
OTT	Over The Top
PERS	Personal Emergency Response Systems
QoS	Quality of Service
RSU	Road side unit
SCTE	Society of Cable Telecommunications Engineers
STB	Set-Top Box
USDOT	United States Department of Transportation
V2I	Vehicle to infrastructure
V2V	Vehicle to vehicle

6. Bibliography & References

[1] https://www.calcable.org/

[2] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[3] https://corporate.comcast.com/news-information/news-feed/machineq-comcasts-enterprise-internet-of-things-service-expanding-to-12-major-us-markets

[4] http://newsroom.cox.com/cox_launches_cox2m_for_smart_cities_-smart_businesses

[5] https://www.multichannel.com/news/scteisbe-eyes-iot-standards-408241

[6] https://www.census.gov/content/dam/Census/library/publications/2015/demo/p25-1143.pdf

[7] https://www.cms.gov/medicare/medicare-fee-for-service-payment/acuteinpatientpps/readmissions-reduction-program.html

[8] https://www.transportation.gov/smartcity

[9] https://www.its.dot.gov/pilots/pilots_thea.htm

[10] https://www.statista.com/statistics/764051/iot-market-size-worldwide/ and

https://www.statista.com/study/27915/internet-of-things-iot-statista-dossier/)

[11] https://newsroom.intel.com/news-releases/intel-unifies-and-simplifies-connectivity-security-for-iot/

[12] https://www.techrepublic.com/article/as-iot-attacks-increase-600-in-one-year-businesses-need-to-up-their-security/)

