SCTE•ISBE CABLE-TEC EXPO® VIRTUAL EXPERIENCE » OCTOBER 12-15 2020

2020 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS®

A Better Platform to Facilitate Remote Patient Monitoring

A Technical Paper prepared for SCTE•ISBE by

Jason Page
Principal Engineer
Charter Communications
6360 Fiddlers Green Circle, Denver, CO 80111
720-699-6236
jason.page@charter.com

Table of Contents

List of Figures

1. Introduction

Cable companies are positioned to enable remote monitoring of patient data through connected medical devices. The remote needs of customers due to Coronavirus highlighted the need to offer healthcare services outside of traditional brick and mortar medical facilities. Existing solutions that enable the wireless transfer of data from connected medical devices suffer from numerous shortcomings that limit the adoption of this technology.

The predominant means of wireless connectivity for in-home medical devices is Bluetooth Low Energy. Most manufacturers require the use of a smartphone and a proprietary application to transmit vitals measurements from healthcare devices. This places a heavy burden on a patient's ability to purchase a smartphone and then have the technology savvy to download an application and connect with the healthcare devices. These proprietary applications also lead to data siloes and inconsistent security practices. To overcome this limitation some device manufacturers and service providers resort to using expensive cellular radios and data plans. As a result of these steep barriers many of the most vulnerable patients are unable to participate in the use of this technology.

There is a better way. IoT radios, such as Bluetooth Low Energy (BLE), should be included in traditional Ethernet and Wi-Fi routers. These common access points are a natural bridge between Personal Area Networks (PAN) that are used for most constrained IoT devices' wireless communication and traditional IP based Local Area Networks (LAN) and Wide Area Networks (WAN). This should be combined with a flexible software platform that can provide interfaces for IoT device provisioning, command and control, and telemetry transport.

Utilizing this approach to fulfill remote patient monitoring use cases would enable devices to be onboarded with little or no user intervention. It would also ensure that sensitive healthcare measurements can be sent directly to secure whitelisted endpoints. As administrators of the platform, Cable companies can implement industry standard security practices and provide advanced monitoring and troubleshooting services. This solution removes the technological barriers to entry, improves connection reliability, and can be provided at a much cheaper price point than using cellular.

This paper describes a prototype of a router-based remote patient monitoring system which will be much more effective than the current approaches. It introduces OpenSync, a cloud-agnostic open-source software for the delivery, curation, and management of services for the modern home and the IoT extensions that need to be added to it. It describes the enhancements that must be made to the router and its software stack, as well as what cable companies can do as an industry to enable this new line of business.

2. What is Remote Patient Monitoring (RPM)

Remote Patient Monitoring (RPM) is a new technology in the rapidly evolving world of digital healthcare delivery. RPM allows for the collection of patient data outside of traditional brick and mortar healthcare facilities. The ability to regularly take readings of vitals and other physiological measurements enables healthcare professionals to provide custom tailored

treatments and intervene more quickly if patients are not progressing as expected. There are other uses as well: consumers can track their own wellbeing, research and analytic companies can collect anonymized data to improve overall healthcare and design new therapies.

RPM has been enabled by the continual miniaturization of electronics and by the evolution of IoT. Most connected medical devices are battery operated, constrained devices. They typically use Bluetooth Low Energy for wireless communications but sometimes come with cellular or Wi-Fi radios. Most of the devices specialize in taking a single medical measurement and generally attempt to transmit the value as soon as it is available. Examples of RPM devices include connected blood pressure cuffs, pulse oximeters, scales, thermometers, glucometers, and more.

A diverse set of stakeholders is required for RPM to achieve general acceptance and provide value to users. The major stakeholders in the space are patients, doctors, device manufacturers, electronic medical records providers, insurers, patient engagement companies, healthcare exchanges, and many more. Each stakeholder has different interests and responsibilities. These competing factors often lead to data being siloed with a single entity causing patients to get less value from the technology. Coordinating access to medical data and ensuring proper authorization can become very complex. Cable companies can play the coordination role.

3. Why Should Cable Operators Care

Currently there exists no standard for transporting data from connected medical devices to backend systems in the cloud where the data can be used and stored. Cable companies are well positioned to influence the creation of standards and be the connectivity bridge. Cable already has a presence in nearly every home across the country and provides connectivity for millions of connected devices. The next evolution of this connectivity should be to connected medical devices that use personal area networks.

The potential benefits to Cable companies are vast. Cable companies stand to enhance the relationship with their customers and improve their overall reputation by being the guardians to sensitive health information. Internet and advanced wireless connectivity packages can be made stickier since they play a vital role in directly ensuring our customer's wellness. There also exists new lines of revenue through the direct administration of remote patient monitoring services or through partnerships with healthcare systems and providers. This technology also presents an opportunity to engage in the wider smart home industry.

4. Current Implementations and Their Shortcomings

Remote patient monitoring requires the transfer of sensitive data from medical devices to the internet. To facilitate this data transfer two general approaches have been adopted. The first and most common approach is to use a smartphone as a hub and the second approach is to equip medical devices with cellular radios. Each carries its own shortcomings that limit the adoption of this technology.

The smartphone as a hub approach works by utilizing the Bluetooth radio that is ubiquitous in smartphones today. The smartphone acts as a central device and is able to connect to nearby BLE medical devices. Once connected to the medical device the smartphone is able to retrieve readings from the device and send them to the cloud or store them locally. Generally the process of connecting to the device and retrieving measurements is done through a proprietary application provided by the device manufacturer.

The smartphone as a hub approach suffers from a few shortcomings. The first is that it requires users to have a smartphone. Patients are also required to download proprietary applications, turn on Bluetooth, create accounts, adjust permissions and settings, and perform a range of other tasks that may not be simple for many of the most needy. The proprietary nature of the application required to interact with the device often leads to data siloes. Having medical devices from different manufacturers also generally requires separate applications.

To overcome these limitations the second approach of using cellular radios has been adopted. This approach generally places cellular radios directly in connected medical devices. Rather than requiring a hub to enable the transfer of data to the cloud the device can directly transfer the data itself. While this approach eases the technological burden on patients it increases the cost of connected medical devices and requires expensive recurring data plans. It also increases the complexity of the device and leaves the security implementation completely at the discretion of the device manufacturer.

5. A Better Connectivity Solution

An ideal connectivity solution for remote patient monitoring must retain the cost effectiveness of inexpensive Bluetooth radios while minimizing the technical role a user must play. It should provide the patient the ability to authorize access to their medical data but otherwise be transparent to them. The nuance involved in connecting the medical device to a network, controlling the device, and ultimately transmitting readings to the cloud should be automated. The user interface for patients to interact with their medical data should be completely decoupled from the application that transfers data from device to cloud. All device provisioning and association with a particular user should be done by backend systems that require little or no patient involvement.

To have the widest adoption the software should be open source and the router components should be hardware agnostic. An open source solution would allow every connectivity provider and medical device manufacturer to deploy the solution. A hardware agnostic platform would allow components to be cost competitively sourced and limit the leverage of any given vendor. This helps drive down the total bill of materials and avoid procurement obstacles.

6. Why Use a Router

The router is a natural replacement for the use of a smartphone as a hub and its always on nature provides many additional advantages for the collection and transfer of medical data. The router is a relatively inexpensive and common piece of equipment for most households. It currently serves to connect ethernet and Wi-Fi capable devices to the internet. With addition of IoT radios the

router can also be a bridge to connected medical devices and facilitate the transfer of data to the cloud.

Using a router to provide access to the internet for connected medical devices provides an inexpensive connectivity option. This also ensures that existing BLE medical devices can participate. Routers can be centrally and remotely administrated. The always-on access point lends itself nicely to regular collection of connectivity diagnostics. Remote administration can assist in troubleshooting malfunctioning equipment.

7. Why Use the OpenSync Platform

Equipping routers with additional IoT radios is only part of the solution. In addition to the necessary hardware to communicate with connected medical devices a software platform to interact with the devices is also required. Such a platform must be capable of being remotely managed, have a secure pipeline to facilitate telemetry, and be capable of being run on routers. In addition, the software must be deployed to millions of routers and bulletproof.

OpenSync is a software platform that meets the requirements to enable remote patient monitoring. It has baked in support for JSON RPC, a synchronized bi-directional database, and MQTT. These components make the platform extremely flexible, extensible, reliable, and secure. OpenSync and all of its components are open source. It can be run on OpenWRT, RDK, and other Linux based operating systems. OpenSync has also been thoroughly vetted and underpins the routing platforms of a number of major companies.

8. BLE Telemetry

To facilitate the transmission of data from a connected medical device, some means of uniquely identifying the device and some means of communicating with the device are required. In the majority of RPM devices, the means of communication is Bluetooth Low Energy and the device can be uniquely identified by its MAC address. Additional pieces of information that are required for the BLE protocol are the GATT service UUID that is broadcast in advertisement packets, and GATT characteristic UUID(s) that stores the device's value(s) of interest. Additional information is helpful but not necessarily required.

All BLE transactions begin with a device advertising itself. Information included in the advertisement packet is the MAC address of the device and usually a GATT service UUID. The service UUID can effectively be used to determine what type of device is advertising while the MAC address can be used to uniquely identify the exact instance of the device type. Any scanning devices that hear this advertisement can then issue a connect request to the remote device if they are interested in interacting with it. Upon establishment of the connection the central device can then issue commands to the peripheral device. These commands can assist in learning more about the capabilities of the device, reading values from the peripheral, writing values to the peripheral, or enabling notifications.

In a remote patient monitoring use case a typical transaction begins with a device turning on when a user engages it. This could be a user stepping on a scale, pressing a button on a blood pressure cuff, or placing a pulse oximeter on their finger tip. The device begins taking a measurement and when the first reading becomes available the device begins advertising itself. Nearby devices that are listening for these advertisements can issue a connection request in response. When the listening device connects it enables notifications on the medical device and the medical device then transmits values as they become available. This could be a stream of values as is the case with a pulse oximeter or a single value as is the case with a weight scale. When the medical device is done taking its measurement or otherwise disengaged by the user it disconnects from the listening device and goes to sleep. Transactions can grow more complicated when adding in authorization or bonding but this is the basis for the transfer of readings from a connected medical device to an internet connected device.

9. Proof of Concept

To prove the viability of RPM on a router and through OpenSync, the Emerging Technology team at Charter Communications designed and implemented a proof of concept. The design used a Raspberry Pi to act as a router and added a Silicon Labs Bluetooth capable radio via USB. The main software component is a custom build of OpenSync with extensions for IoT. These extensions included schema updates, a Bluetooth Low Energy hardware abstraction layer (HAL), a centralized RPM manager, and specialized plugins to assist the manager application. Supporting software components included a RESTful API, MQTT to Kafka connector, WebSocket server and a simple user interface.

The system works by allowing applications to issue commands in response to events generated by the Bluetooth Low Energy hardware abstraction layer or by updates made to configuration tables in the synchronized database. The BLE events that were exposed for the proof of concept include: advertisement packet received, connection established, service discovered, characteristic discovered, notifications enabled, and new value received. The BLE commands that were exposed include: enable scanning, connect to device, discover services, discover characteristics, and enable notifications. This simple set of commands and events allowed for interactions with four different types of medical devices. They include a blood pressure cuff, pulse oximeter, scale, and thermometer. Each device was made by a different manufacturer.

Every device interaction begins with provisioning a specific medical device to a customer account through the RESTful API. The RESTful API exposes resources that are capable of performing database transactions. These database transactions are then replicated down to the Raspberry Pi via the magic of OpenSync. The information needed for provisioning the specific device is it's MAC address, the UUID of the GATT service it advertises, and the UUID of the GATT characteristic that stores the value of interest.

When the RPM manager code running on the Raspberry Pi detects the provisioning of a new device it enables scanning through the BLE HAL. The HAL then begins to pass received advertisement packets up to the RPM manager code. If the manager finds an advertisement packet with a matching MAC address it then issues a connect request to the device.

Upon successful connection the manager then begins a process of attribute discovery on the device. If one of the discovered attributes happens to match the UUID of the GATT characteristic value of interest, the manager issues an enable notifications command. The device will then begin transmitting measurements to the Raspberry Pi as they become available. When a new value is received the manager code takes the raw bytes and transmits them to the cloud via MQTT. Once in the cloud the data is then able to be ingested by any stakeholders that have authorized access.

The main steps for getting data off the medical device can be broken down into three basic processes. The first process is establishing a connection between the medical device and router. The second process is discovering the attributes that the device exposes if this is not already known. The third process is enabling notifications and receiving values of interest. Below are sequence diagrams depicting the main processes that take place.

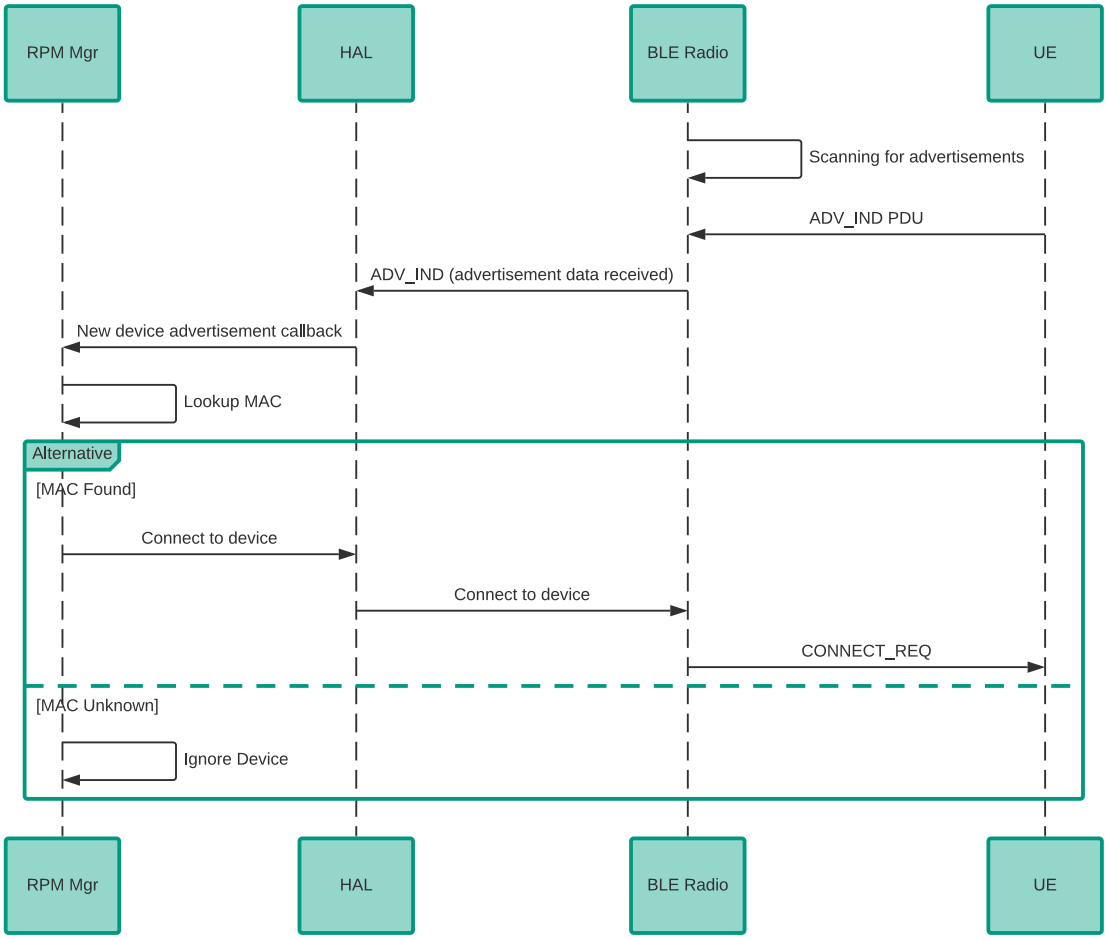

Figure 1 – Device Discovery and Connection

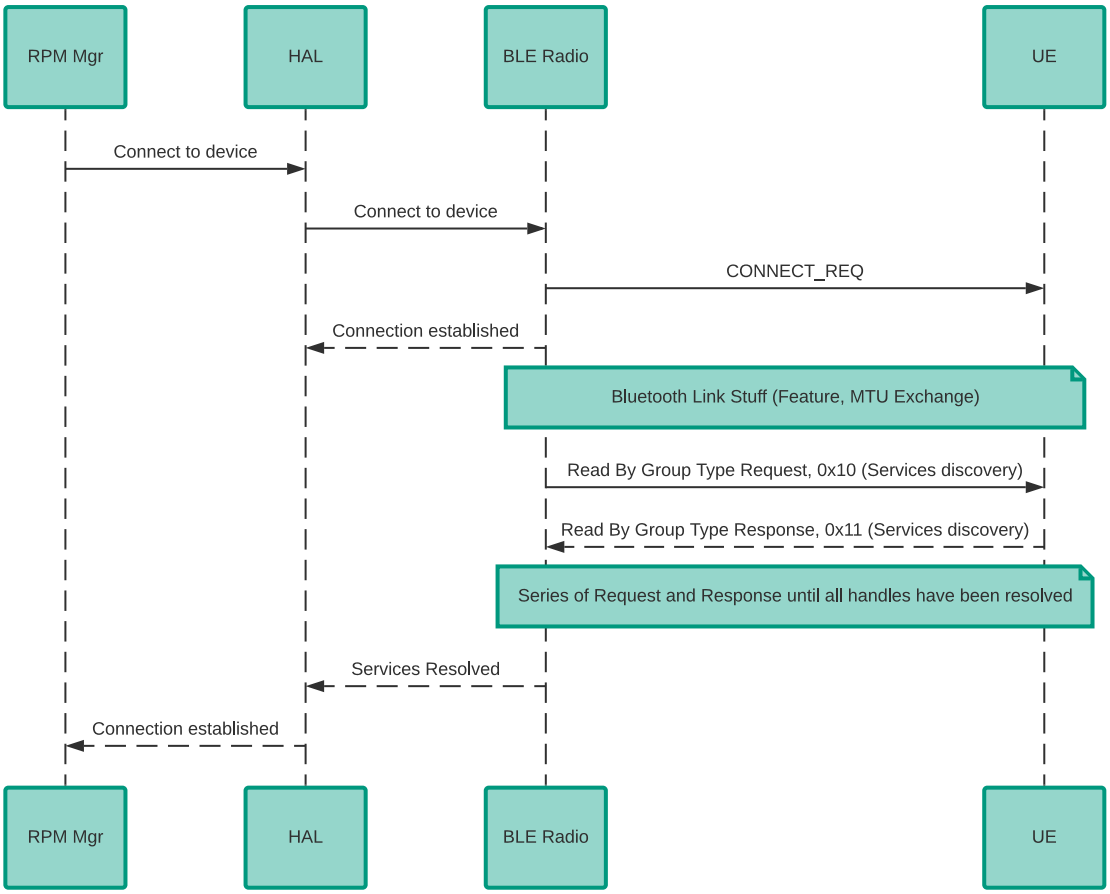

Figure 2 – Device Connection and Attribute Discovery

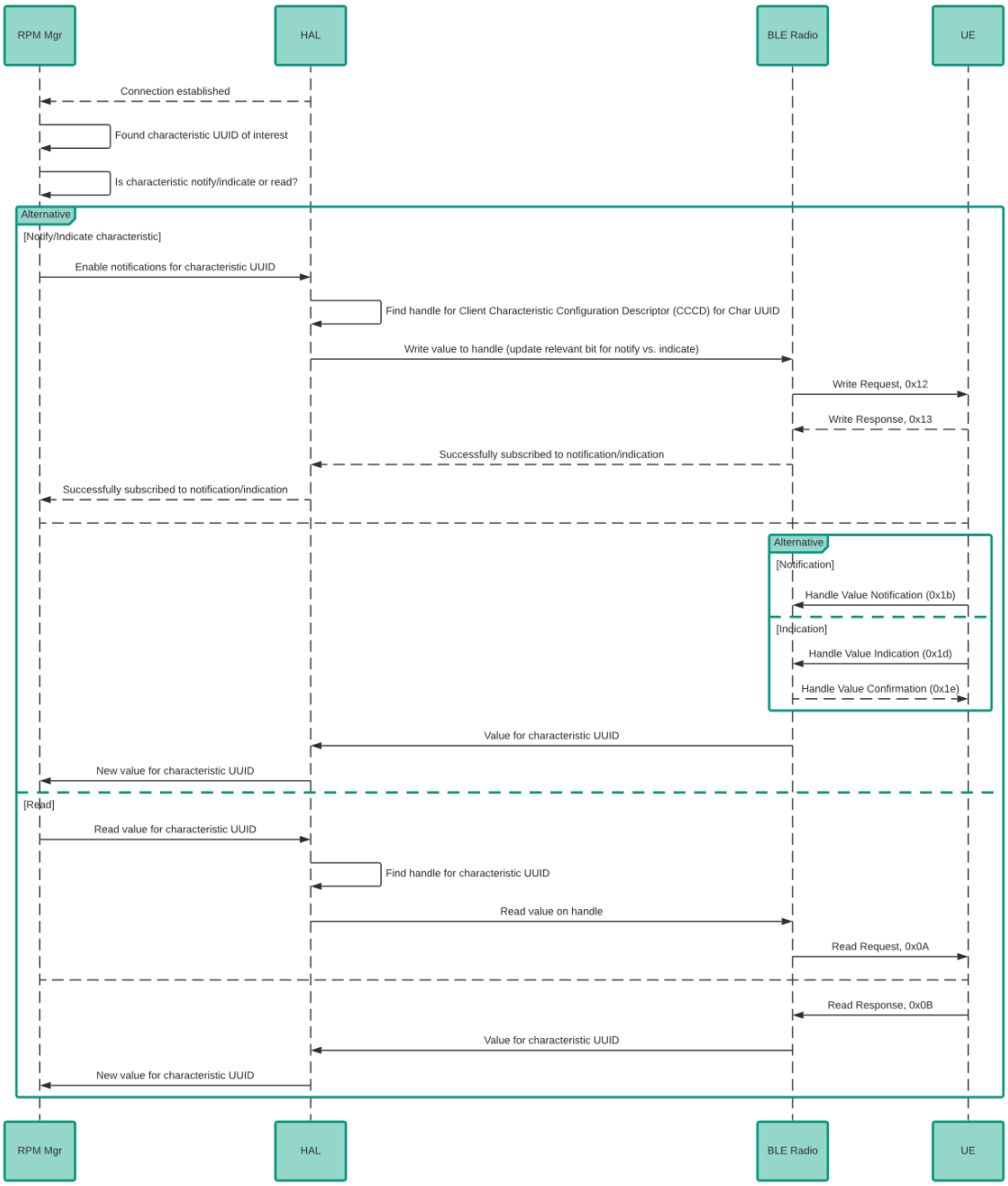

Figure 3 – Data Transfer

10. Areas Requiring Additional Work

The RPM proof of concept demonstrated the bare minimum required to facilitate the transfer of data from connected medical devices. The above outlined approach does not address security. Utilizing the outlined components, security can be centrally administered, data can be guaranteed to be encrypted while in transit from the router to the cloud, and additional best practice security standards can be employed.

In addition to work done around security, a more robust set of interfaces to provision devices and ingest data should be designed. The simple user interface created for the proof of concept allowed for manual provisioning of devices to a single customer account and the ability to view measurements in real time. A more effective interface would allow the process of device provisioning and data access to be automated at the point of sale or when prescribed by a doctor. It should allow the customer to elect where their data should be transferred and should require consent for all third party access.

While the proof of concept shows that a router can be used for remote patient monitoring, it has not been tested with day to day use. Potential areas that can improve performance would be bonding with devices and maintaining device information such as mappings from a GATT UUID to an attribute handle. Additional systems can also be created to track battery levels, device connectivity history, and RSSI values.

11. Potential Concerns with the Outlined Approach

The approach outlined above will work well for the majority of remote patient monitoring use cases. However, it suffers from two potential concerns. The first concerns placement of the router and signal range of the protocol. Bluetooth low energy has a range of 100 meters but in practical usage this is generally closer to 25 to 50 meters. In large homes or MDUs with lots of interference, the router may not be situated in an ideal location to accommodate these restrictions. In such situations placing IoT radios in Wi-Fi mesh access points would be an excellent approach. These can be small devices that create Personal Area Networks with a Wi-Fi data backhaul to the main router. In addition to providing extended IoT coverage they can also improve general Wi-Fi coverage.

The second concern relates to specific use cases requiring real time transmission of readings taken outside of a user's home. In this situation cable operators may be able to use a smartphone to serve as a hub for gathering and transmitting measurements with a companion app that complements the in home service. As Cable companies venture more into the mobile space this becomes a practical approach.

12. Conclusion

Remote patient monitoring is an emergent technology in the delivery of healthcare that holds great potential. To fully capitalize on this potential a better platform for the transfer of data from connected medical devices is needed. The benefits of the approach described in this paper are more reliable connectivity, stricter security, cost efficacy, decoupling of data acquisition and data interaction, and an improved user experience. Cable companies are in a strong position to

leverage existing and enhanced infrastructure to support RPM technology. The rewards for implementing an RPM platform will be increased customer loyalty, new potential streams of revenue, and an opening to play a larger role in the broader smart home space. If Cable companies work together to create an open source standard many device manufacturers and RPM service providers will welcome the opportunity to use it.

Abbreviations

IoT	Internet of Things
BLE	Bluetooth Low Energy
PAN	personal area network
LAN	local area network
WAN	wide area network
RPM	remote patient monitoring
MAC	media access control
UUID	universal unique identifier
GATT	Generic Attribute Profile
HAL	hardware abstraction layer