41. mHealth over "Medical Grade" High Quality of Service Mobile Networks

Michael Kedar

Mobilexchange Ltd., 1131A Leslie Street, Suite 401, Toronto, Ontario (Canada) M3C 3L8
mike.kedar@mobilexchange.ca

Keywords: Mobile infrastructure, Broadband 700 MHz Mobile Networks, Ubiquitous Telemedicine, Public Real-Time Social Services, Interoperability, Industry Canada - IC, Federal Communications Commission - FCC, Quality of Service - QOS, Wireless Body Area Network-WBAN, Bring Your Own Device - BYOD.

1 Introduction

This chapter is focused on discussions of a number of issues and challenges associated with the underlying infrastructure of mHealth, including: regulation of medical devices/smartphones, network security and privacy, interoperability, scalability, ubiquity, data management and ownership, remote monitoring, and the importance of end-to-end Quality of Service (QoS) for full reliance on mHealth technology in medicine.

The rapidly accelerated adoption of broadband mobile technology in healthcare will have significant impact in transforming the industry; [4] in this chapter we will address the criticality to the medical profession of developing sufficient confidence in the accuracy and security of the underlying wireless infrastructures.

A pervasive expansion of mHealth is already occurring:

- Within hospitals and clinics, over unlicensed private Wi-Fi networks.
- Over ubiquitous wide area carriers' mobile networks owned by commercial public wireless networks.

We will review the evidence indicating that interfaces among these networks are commonly insecure. They are typically interconnected at the smartphone level, where medical patients' records and real-time, life-dependent monitoring data are interchanged from one network to another.

This chapter will show that the most important aspect of mHealth is the ability of the mobile/wireless infrastructure to reliably and accurately accommodate large amounts of end-to-end real-time data. Thus, dependability and end-to-end QoS of the underlying Radio Frequencies (RF) infrastructure are paramount.

> ***"As more and more wireless technologies and systems are introduced and rolled out in the hospital, proper management of this fundamental resource has never been more important."*** **[3]**

© Springer International Publishing Switzerland 2015

S. Adibi (ed.), *Mobile Health*,
Springer Series in Bio-/Neuroinformatics 5, DOI: 10.1007/978-3-319-12817-7_41

mike.kedar@mobilexchange.ca

We will see how mHealth is situated at the intersection of Electronic Health (IT) and smartphone technology. The discussion will center on the infrastructure behind smartphone technology.

In order to evaluate the present and future QoS issues and challenges of mHealth, a review is included as to how mobile communications technologies and smartphone technology came to be used in healthcare.

Imagine the following scenario:

A major train derailment occurs, injuring hundreds of people spread over two city blocks. Within minutes first responders arrive and immediately use their two-way radios to call for all equipped ambulances within 30 kilometers to rush to the scene. Hundreds of local residents untouched by the disaster rush to the derailment site to help in the rescue. Suddenly, hundreds of cell phones are turned on, jamming the four-cell site serving the two affected city blocks. Police and fire crews, as well as all the ambulance paramedic teams, start attending to the injured while communicating over their own radios to their individual headquarter dispatchers.

No direct radio communication is possible between the police, fire and paramedic crews on the scene because each of their radio networks operate on a different frequency.

In the ensuing chaos, many of the injured require urgent medical attention. Paramedics do their best to attend to these cases. They use the EMS (Emergency Medical Service) protocol to deal with simple injuries, but to obtain instructions to deal with the most serious injuries they need to connect to the local hospital emergency medical staff. As the cellular network is now jammed, they call their dispatchers, who in turn relay their requests to the hospital ER staff.

Now let's zoom in. A middle aged man is lying motionless without any signs of bleeding. He has a very weak pulse and shallow breathing. He appears to be having a cardiac arrest. The attending paramedic uses his portable radio and calls the dispatcher who is busy with many other calls. Eventually, he gets a response and reports, "We have a 50-something year old male, no signs of bleeding, weak pulse, shallow breathing and possible cardiac arrest, but we have no data on him. What is the safest approach to revive his heart in addition to providing CPR?" The dispatcher relays his interpretation of the hospital's recommendations, translated over the busy telephone. The message is, "Use Epinephrine 10 mg IV/IO every 3-5 minutes." "Are you sure?" asks the paramedic. "Yes" replies the dispatcher. The procedure is administered and the patient dies.

The amount of the Epinephrine should have been 1 mg and not 10 mg; however, due to the poor communication quality, the dosage was misunderstood and, ultimately, caused the patient to die.

This emergency event scenario shows how, in real-time situations, medical personnel are critically dependent upon dedicated, reliable, broadband, end-to-end communication infrastructure.

mike.kedar@mobilexchange.ca

2 Brief History of Mobile Communications in Healthcare

Wireless communications came to the healthcare industry as an ad hoc phenomenon, introduced some twenty-five years ago along with the introduction of commercial cellular radios. Doctors and other healthcare providers, having taken personal subscriptions on public commercial cellular carrier networks, imported their devices into "work," thereby commencing mHealth through the back door.

The use of personalized wireless phones and other mobile devices at work is now called "BOYD" – Bring Your Own Device. This phenomenon presents serious headaches to hospital IT departments who have to accommodate devices operating on foreign networks totally out of their control. The initial BOYD deployment in healthcare was limited to voice communications and was managed through privacy hospital rules and procedures. That has changed, however, since the mid-1990 when data was added to these devices and hospitals and clinics started to deploy Wi-Fi networks: "wireless local area networks" (WLAN) (Reference #5). We will review the evolution of indoor and various wide area wireless networks and their "medical grade" suitability in this section.

Mobile communication over a wide area has been deployed by Public Real-Time Social Services (PRTSS) agencies such as police, fire, ambulance (EMS) and others since the invention of the two-way radio in the 1920s. Two-way communication devices, "radios", were installed in vehicles to allow instant communication from headquarters (dispatchers) to their operating fleets. Public safety and social service agencies have deployed private two-way radio systems for over eighty-five years. Mobile radios became a fundamental "tool of the trade" for the PRTSS industry.

Public safety, airlines, the military, and other real-time operations have customized and deployed mobile networks over dedicated Radio Spectrums licensed by governments, based on the unique requirements and specifications which met their voice communication needs.

These private mobile networks were independently deployed by each agency in municipalities across the country and all over the world. Deployments in big metropolitan cities and small rural areas were individually undertaken on a variety of narrow band mobile channels in the LB spectrum (L Band used by the military), VHF (Very High Frequency), and UHF (Ultra High Frequency). Diverse frequency bands and serendipitous governmental channel allocations created a series of mostly short-term patches rather than a consistent, integrated system. Visionary planning to coordinate statewide, countrywide and, ultimately, worldwide interoperability needs during major emergencies were completely overlooked.

mike.kedar@mobilexchange.ca

3 The Mobile Communication Gap

Following the September 11, 2001 (9/11) catastrophe in the U.S.A., the FCC and Industry Canada set aside dedicated spectrum for first respondents that includes the fundamental broadband (voice data and video) design requirements to enable regional and countrywide co-ordination and interoperability.

Unfortunately, despite the availability today of advanced broadband mobile technologies, nothing has dramatically changed over the twelve years since 9/11. In many wide areas, natural or manmade disasters, of serious local, regional or multiple wide area situations, such as fire, flood, and terrorism attacks, the PRTSS agencies are still unable to perform "real-time end-to-end" broadband communications. Communication from victim field locations to hospital Emergency Rooms (ER) is still available only over commercial cellular networks.

Victims of major emergencies are attended to by paramedics who are unable to directly interface with hospital ER personnel. Typically, during emergencies, public cellular networks are totally jammed, preventing real-time access by rescue workers. Consequently, they must depend upon the only wireless communication available: The old narrow-band, two-way radios, capable of providing only voice and rudimentary data between them and their base dispatchers.

Hospitals are rarely equipped with PRTSS mobile base stations to accommodate such communications. So the link ends up flowing from the injured patient to the dispatcher to the dispatcher's landline (internet) to the hospital.

When local cellular networks are blocked or in failure mode, current radio systems cannot provide real-time, direct co-ordination between the field PRTSS personnel and the landline-connected institutions.

As private PRTSS radio systems evolved, their vehicular and portable radio devices, operating on different frequency bands, between different agencies, in different regions, created a chaotic mélange of products. In addition, as might be expected, unit cost structures soared. Volume production for these radios is in the thousands, unlike popular cellular phones, which are standardized all over the world and are produced in millions per annum, and have a significant lower unit cost. A police "walkie-talkie" could cost over $2,500.00 in comparison to a much more sophisticated "smart cellular phone" at less than $500.00.

As a result of budgetary and regulatory constraints that impede the allocation of dedicated public safety/healthcare spectrum and their subsequent deployment, many PRTSS agencies now rely upon commercial cellular mobile and local area Wi-Fi unlicensed networks for their operations. These include hospitals and telemedicine practitioners who employ commercial third-party networks not only for day-to-day correspondence but for emergency and life-dependent real-time operations as well.

mike.kedar@mobilexchange.ca

4 Public Discussions

The growing reliance on commercial wireless networks is one of the most critical challenges of the burgeoning mHealth and its related "first responders" emergency operations.

To illustrate this critical point a CBSNEWS article from September 2011 and a Bloomberg BusinessWeek article from April 2013 have been reprinted below:

On September 11, 2011 CBSNEWS reported: [11]

WASHINGTON – Amid the chaos of the Sept. 11 attacks in 2001, emergency responders found they could not communicate with each other. That problem persists 10 years later, according to a review of the 9/11 Commission's recommendations.

A National Preparedness Group report released Wednesday concludes that the recommendation that a nationwide broadband network for emergency responders be created "continues to languish."

"Despite the lives at stake, the recommendation to improve radio interoperability for first responders has stalled because of a political fight over whether to allocate 10 MHz of radio spectrum ... directly to public safety for a nationwide network, or auction it off to a commercial wireless bidder who would then be required to provide priority access on its network dedicated to public safety during emergencies," says the report, whose authors include 9/11 Commission chairmen Lee Hamilton and Thomas Kean.

Law enforcement and emergency responders around the country have long supported the creation of the communication network. In January, President Obama announced his support for allocating the radio space, known as the D-block spectrum, to police and other emergency workers.

Bills that would set aside the D-block and create a communication network have been introduced in both the House and the Senate this year, but so far have not been passed in either chamber.

Several big wireless carriers have supported auctioning off the airwaves to the wireless industry, a move that the government has estimated would raise about $3.1 billion. That could help pay to build a public safety communication network.

The Federal Communications Commission has tried to auction off the D-block before, but that 2008 auction required that the winning bidder help build a network to be shared by first responders and give them priority in an emergency. It did not attract any serious bidders.

The National Preparedness Group report stated, "...statewide communications, interoperability plans, and the creation of a national emergency communication plan have improved emergency co-ordination across different jurisdictions. More work needs to be done and the ultimate resolution is to follow the 9/11 Commission's recommendation and create a nationwide communication network."

mike.kedar@mobilexchange.ca

A more recent article following the Boston Marathon bombing in April 2013; Bloomberg BusinessWeek (Technology by Brad Stone April 16, 2013) [8]

Toward the bottom of the list of disturbing aspects about Monday's bombing at the Boston Marathon was this: Cellular networks in the area almost immediately slowed down and, for a period of time, appeared to stop working altogether. Runners and their loved ones could not connect, and victims had trouble communicating with emergency responders.

That frustrating scene has become familiar, evoking disasters from the Sept 11th attacks in 2001 to Hurricane Sandy in 2012. We rely on cell phones to run our lives, but they tend to be useless-or at least far from useful-when we need them most.

Initial reports suggested that authorities deliberately shut down mobile networks in Boston to avoid the possibility that mobile devices could be used to trigger more bombs.

The Associated Press reported this and then quickly reversed itself. Spokespeople from the major wireless carriers denied it, saying their networks were simply suffering from congestion: Too many people were trying to use their phones at the same time in order to get help or tell family and friends they were O.K.

"Thinking of those at Boston Marathon," AT&T tweeted at around 5:30 p.m. East Coast time. "For those in the area, please use text & we ask that you keep non-emergency calls to a minimum."

A Verizon Wireless spokesperson also suggested that customers in the area use text messages or e-mail to free-up capacity for public safety officials.

The science behind these failures in wireless connectivity isn't complicated. In every city, each mobile carrier operates hundreds or thousands of cell towers, which route calls and data to the carrier's backbone network. Each tower is designed to accommodate a set number of calls per second, per a certain geographic area. In a crisis, when everyone naturally reaches for their phone, that limit is quickly surpassed and the radios on the tower get sluggish. Mobile analyst, Chetan Sharma, who estimates that a cell site can handle 150 to 200 calls per second per sector: "We've all had the experience of a fast-busy signal. That is the network telling you, "Sorry, but your cell is overloaded. There is no more space."

In these situations, sending texts or e-mail is a better option because messages can be queued up and delivered as capacity becomes available. Twitter is especially efficient because information can be spread quickly and widely. Until it was debunked, the rumor that police deliberately shut down cell networks was an intriguing one. This is almost unheard of. When it has occurred, the practice has been controversial. In April 2011, public transit authorities in the San Francisco Bay Area on the region's BART subway system used to prevent activists from

mike.kedar@mobilexchange.ca

coordinating their activities as they protested shooting by BART police. The shutdown led to criticism that police were hindering the activists' right to free speech, spurring a further round of protests. The police argued that they acted to protect the public safety.

Monday's situation was different, of course. ABC News reported in a tweet that police were asking people on the scene not to use cell phones because they might set off other explosive devices. Still, it does not appear there was any widespread directive from law enforcement to shut down cell networks, and authorities appear to believe that cell phones do more to help than hurt in an emergency. "The belief is that much more good comes from networks being available than the risk of them being utilized for bad intentions," says Charles Golvin, an analyst at Forrester Research.

Can anything be done to improve network performance during tragedies such as Monday's bombing? Probably not much. Carriers could engineer networks to handle these situations by adding radios and towers and amplifying connections from the towers to the network's backbone.

But a vast majority of that extra capacity would then be wasted. "Over the years, a lot of research has gone into analyzing the trade-off between cost and capacity, and today's networks are designed to provide enough capacity during the vast majority of 'normal' conditions," says Golvin.

Just as land line networks were never meant to allow every person with a phone to place a call at the same time, wireless networks are designed to align resources with normal peak call volumes in the most efficient manner possible. As a result, hearing a loved one's voice in the tense minutes after an emergency may always be difficult. Perhaps it's best to hope we have fewer and fewer of these kinds of tragedies in the first place.

5 The Urgent Need for Dedicated Broadband Mobile Networks

As seen from these articles, national dedicated networks have not been deployed for neither first responders in the "public safety" arena, nor for mHealth and Healthcare in general. All real-time broadband wireless transactions are still shared with non-urgent media and voice networks without due priorities.

Dedicated broadband wireless networks were designed exclusively and deployed for public safety/healthcare and other real-time services; PRTSS, will overcome the serious shortcomings of current commercial wireless services. These shortcomings include poor availability, inadequate coverage, and, above all, the lack of priority access during emergencies.

Network infrastructure requirements for PRTSS communications include:

- Broadband applications to facilitate real-time responses by providing simultaneous voice and data images, including video.

mike.kedar@mobilexchange.ca

- Coverage of the entire country, ensuring service to meet PRTSS emergencies anywhere.
- Voice communication capabilities, to be used as backup to real-time critical voice channels on other frequencies, including one-to-one and one-to-many connectivity.
- Network software that provides traffic management services such as prioritizing. (If multiple networks were built separately and then linked together, interoperability and nationwide roaming would need to be ensured.)
- Mobile broadband applications designed for PRTSS. In particular, radio chipsets need to be developed for wireless devices that can connect to a Long Term Evolution (LTE) network.
- Secure authentication software to regulate access to the PRTSS networks; to achieve large volume, unit cost reductions. Such software must be incorporated into standard, commercially available "smart" phones.
- Network cell towers that are strengthened against natural hazards and furnished with back-up power supplies that can outlast extended power outages.
- Robust backhaul, high capacity, landline communication networks. Backhaul (which typically refers to the connections between the air interface access points between cell towers) is an essential component of wireless network infrastructure.

The increasing demand of data traffic on commercial wireless networks worldwide is fast exceeding governments' abilities to allocate more spectrums to public carriers as well as carriers' capabilities to build adequate capacity. [13, 15]

The result is already being noticed by consumers, as the frequency of dropped calls and delayed data transfer (emails) increases with ever more regularity. In other words, the carrier grade Quality of Service (QoS) of commercial cellular networks in large metropolitan areas is degrading. The existing commercial wireless infrastructures, which were originally designed for voice, are hard pressed to carry simultaneously vast amounts in real-time configurations of broadband mobile data and multimedia technology resulting from exponentially increasing usage.

A recent CTIA semi-annual data survey [14] shows more than 69% year-over-year growth in the amount of mobile data traffic (bytes) handled. The 2011 domestic traffic was more than 633 million Mbytes over a six month period ending in June 2012.

To put it into a slightly different perspective, in 2011, every person in the US was receiving more than 11 Mbytes/day. The well respected Cisco Global Mobile Traffic Data Forecast, 2011-2017, is predicting a 66% [15] compound annual growth rate for North America. This forecast would result in every American's receiving more than 200 Mbytes/day by 2017, nearly a twentyfold increase in just four years.

mike.kedar@mobilexchange.ca

Weak RF signal levels coupled with this tremendous growth in demand will further diminish the reliability of these commercial wireless carriers. The variety and complexity of scenarios involving wireless devices will require thorough analysis. The variable signal strengths of disparate wireless sources, in conjunction with separate, co-existing wireless systems can clearly lead to potential interference and degradation of overall system performance.

The existing commercial wireless infrastructures, which were originally designed for voice alone, are hard pressed to carry increasingly vast amounts of broadband, mobile and multimedia data, all simultaneously. Constant internet browsing, on a daily basis, increasing exponentially worldwide, is pushing the limits of current wireless infrastructures.

- **The Network requirements for mHealth**

The growth of mHealth diagnostic services radically increases the demand for wireless capacity. Sending real-time detailed images, such as MRIs, will require significant additional real-time digital bandwidth throughout, which the current carriers will not always be able to provide, particularly at peak hours.

Today's wireless network operators also do not provide priority assurances for real-time urgent communications. They provide only marketing Quality of Service (QoS) information about their networks. They refuse to give any detailed information to mobile users. Some mobile applications even use a network's signal strength to estimate QoS rather than capacity. Signal strength, of course, does not provide any information related to actual network congestion.

Taking into consideration that the mHealth users are moving in space and time, the task of managing the QoS by figuring out and trying to anticipate QoS levels of the underlying wireless networks on a continuous basis is impossible. Reliance on inappropriate metrics leads to worst case scenario assumptions and lowers the usability of real-time mHealth applications.

- **Real-Time, Real Life Example**

Let us take a real life situation, one of many thousands occurring every day, not in major emergencies involving large communities as we discussed earlier, but a typical day-to-day telemedicine/mHealth, doctor-patient remote interaction.

A 30-year old male is recovering from a surgical procedure and has developed an alarming infection. He is being treated by an antibiotic drip and is being monitored remotely by his Doctor who is presently working in another facility. The drip is being remotely operated; the patient's temperature is transmitted constantly and a camera is pointed to the infected area for monitoring on demand. The information is collected either continuously or on demand via a WBAN [16] (Wireless Body Area Network).

mike kedar@mobilexchange.ca

WBAN is a low-powered wireless communication and physiological sensor eco-system that has developed over FCC's specially assigned low power spectrum (40 MHz of spectrum at 2360-2400 MHz) using tiny, lightweight, ultra-low power monitoring devices. WBAN with sensors consuming extremely low power is used to monitor patients in critical conditions inside hospitals. Outside the hospital, the network can transmit patients' vital signs to their physicians over internet in real time.

In our example, the data is being collected wirelessly over the WBAN by a small computer connected to a cellular device: The "Collector/Operator". The Collector/Operator can be interrogated for information by the distant doctor to periodically check on the condition of his patient and remotely activate and change the drip rate of the antibiotic medicine. The system also allows for continuous monitoring on the distant doctor's smart phone screen.

Now, let's look at the wireless infrastructure and risk factors associated in this example of day-to-day telemedicine.

The information hub, the Collector/Operator is situated at the hospital within ten meters of the patient's bed, probably at the nursing station.

Cellular signal strength at that location is usually good; however, today, unannounced by the commercial cellular carrier to which the device is registered, a failure requiring maintenance has shut off the cell site covering the hospital.

Cellular commercial networks are consumer oriented operations with no direct interaction protocol between the users and the network operators, regardless of the situation.

So without notice, the distant doctor has lost his ongoing control and monitoring of his patient.

Very likely he will resort to a telephone to alert the hospital and to arrange alternative supervision, but the critical emphasis here is that there are no "medical grade" technology standards. Mobile networks are operated and managed by consumer oriented companies without any 'medical grade" QoS obligations.

- **The Network Regulatory Impairments**

The sad reality is that, in the twenty-first century, there are no end-to-end wireless standards for a "medical grade" mobile infrastructure. [10]

In "Medical Grade Wireless Utility Case Study for Hospitals – By Ed Cantwell- Oct 28, 2011" [12] various networks' are categorized by quality of service:

mike.kedar@mobilexchange.ca

Network	Consumer Grade	Enterprise Grade	Medical Grade
Coverage The % of the "area" that has wireless signal	Best Effort 85%	Engineered 95%	Guaranteed 100% Clinical Space
Signal Strength Received at device in presence of RF interference	Nominal Will Vary	Engineered Prioritized	Engineered Guaranteed
Capacity Available to the "devices" within the area	Shared	Prioritized Not Dedicated	Engineered Guaranteed Per unit area
Security Physical, Over the Air, and Digital measures to protect	Best Effort	By Policy Engineered	Comprehensive
Certainty Ability of protocol to operate in the area's RF environment	Vary Widely	Engineered Prioritized	Very High Mission & Life Critical

Source: Gary & Mary West Wireless Health Institute

The FDA and its equivalents in many other countries have strict compliance rules regarding medical devices; similarly, the FCC and its global equivalents have strict regulations regarding spectrum utilization and management. **Yet there is no domestic or international organization that has the responsibility to establish end-to-end "medical grade" [5, 6, 9, 12] mobile network infrastructure standards.**

mike.kedar@mobilexchange.ca