Use Cases for MLM Language in Modern Wireless Networks

SDRF-08-P-0009-V1.0.0

Approved 28 January 2009

TERMS, CONDITIONS & NOTICES

This document has been prepared by the MetaLanguage for Mobility Working Group to assist The SDR Forum (or its successors or assigns). It may be amended or withdrawn at a later time and it is not binding on any member of The SDR Forum or on the SDRF MetaLanguage for Mobility Working Group.

Contributors to this document that have submitted copyrighted materials (the Submission) to The SDR Forum for use in this document retain copyright ownership of their original work, while at the same time granting The SDR Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter’s copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to SDR Forum participants to copy any portion of this document for legitimate purposes of the SDR Forum. Copying for monetary gain or for other non-SDR Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

Contributors

Aden, Michelle; Sun
Bickle; Jerry; Prism Tech
Caimi, Frank; SkyCross
Cooklev, Todor; Purdue University
Cummings, Mark; enVia
Das, Subir; Telcordia Technologies
Del Torto, Dave; CryptoRights Foundation
Einseidler, Hans; Deutsche Telecom
Fette, Bruce; General Dynamics
Frantz, Fred; L-3 Com
Ginsberg, Allen; Mitre
Greenwood, Ed; SDR Forum Staff
Hope, Stephen; France Telecom
Kempf, James; NTT Do Co Mo
Kokar, Mieczyslaw; Northeastern University
Kovarik, Vince; Harris
Li, Shujun; Northeastern University
Lyles, Bryan; Telcordia Technologies
Normoyle, Bob; DRS Technologies
Skomra, Stewart; Qualcomm
Strassner, John; Motorola
Subrahmanyam, P. A.; Stanford University
Tiainen, Seppo; TeliaSonera

Many other individuals both within and outside of the SDR Forum helped with the creation of this document

INDEX

Document History

Version	Date	Editor	Description
V.0.0.0	5 September, 2008	Rachel Li	First release of the document. Submitted to Technical Committee voting.
V.0.0.1	22 January, 2009	Rachel Li Mitch Kokar	Comments from the Technical Committee voting incorporated: 1. Figure 1 redrawn. 2. The role of "sub-component" explained in a footnote. 3. The scope of the ontology for an example explained.

1. Introduction

The evolution of Software Defined Radio (SDR) is leading to more reconfigurable and heterogeneous systems. The design, deployment and management of these systems require communication and interaction between different components in the system (both within SDR and/or the infrastructure). Therefore it is important to have a modeling language (we will call it the Modeling Language for Mobility, or MLM), which can provide the ability to negotiate and control the reconfigurable systems. The modeling language enables a uniform way to describe the attributes of system components, Air Interface Standards (AIS) or waveforms, types of information being carried and characteristics of the end users. The design of such a modeling language must fully meet the goals and objectives of all roles in the wireless value chain across the entire life cycle, including Network Operators, Equipment Vendors, Software Vendors, Semiconductor Vendors, Component Vendors, Regulators and End Users.[1] Ongoing efforts in many other organizations such as E2R, W3C and IEEE 802. also have similar objective requirements. Figure 1-1 shows the roles of all members in the value chain. [1]

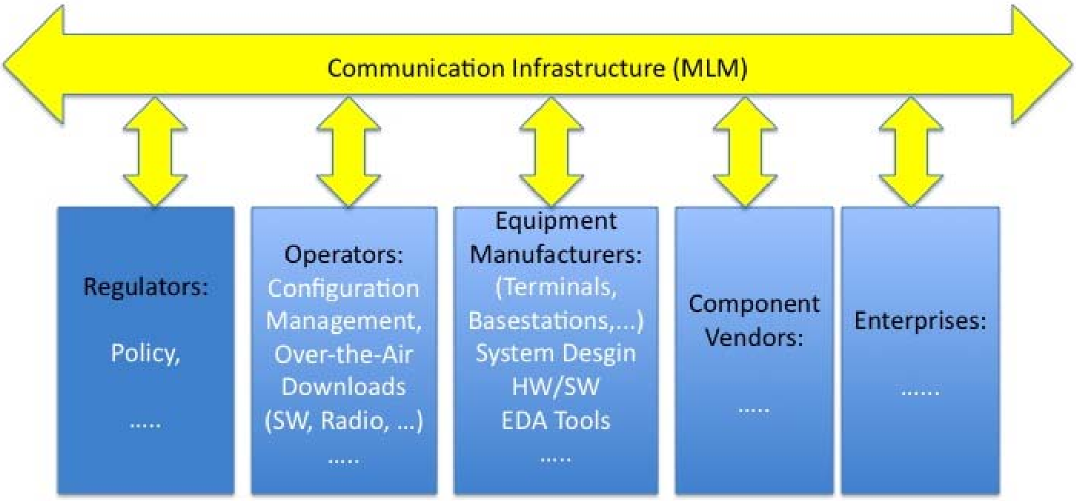

Figure 1-1. The Roles of the Members in the Value Chain

This document is intended to summarize the use cases within the context of multiple scenarios based on actual or credible events relevant to public safety and commercial applications. The analysis of each scenario will show: (1) how cognitive radio capabilities could enhance the ability to communicate under the challenging conditions of a major event or incident; (2) how modeling language might function in these contexts; (3) the issues that must be considered and addressed (in the system/radio/infrastructure) to realize the enhanced communication capabilities.

The following cognitive capabilities will be identified through the analysis of each scenario:[2]

1. Extend existing network coverage when individual radios move outside the coverage footprint of the communication system;
2. Dynamically allocate spectrum to provide greater capacity for overloaded networks;
3. Dynamically prioritize communications to better manage load;
4. Dynamically reconfigure the network to include non-first responders;
5. Provide distributed control for end users with different roles;
6. Provide load balancing in congested locations.

Furthermore, a number of functional capabilities that could enable the realization of these use cases will be identified, at both network level and subscriber level.

2. Public Safety Use Cases

The Public Safety Special Interest Group is one of several special interest groups within the SDR Forum that bring together developers, users, regulators, and educators to address issues specific to the application of SDR technology to a particular domain or market area. The goals of the Public Safety SIG are to interface with the public safety community (including both users and vendors), to raise awareness of SDR, to publicize the activities of the Forum in addressing those issues, and to increase participation of the public safety community in the SDR Forum. The Public Safety SIG also interacts with other committees and working groups within the Forum to provide the public safety community's inputs into the publications and initiatives undertaken by the Forum.[2]

In the Report on Software Defined Radio Technology for Public Safety,[1] the following potential observations were made on the potential role of cognitive radio capabilities for public safety:

1. The first responder can better focus on the incident/threat by eliminating radio operations ranging from routine to complex through the use of cognitive radio applications to:
    a. Be aware of its RF environment (e.g., vicinity of public safety incident);
    b. Detect available and authorized RF resources;
    c. Decide how to best operate within the existing infrastructure/network;
    d. Use geolocation, spectrum, and network awareness to minimize interference;
    e. Automatically reconfigure and connect; and
    f. Learn how to perform these steps better the next time.[2]
2. Cognitive radios offer a broad range of RF techniques to improve performance, interoperability, and efficiency.
3. Cognitive radio is becoming a significant concept for future communications systems and devices for two fundamental reasons:
    a. It enhances spectrum efficiency and improves access by making dynamic channel assignments, taking specialized measures to avoid harmful interference to others, and maximizing utility of available channel seconds.
    b. It enables "intelligent" self-configuring, auto-adapting systems and devices that can handle the growth trend of complex waveforms and user requirements.

[1] Use Cases for Cognitive application in Public Safety Communications Systems – Volume 1: Review of the 7 July Bombing of London Underground. November 8, 2007, SDRF-07-P-0019-V1.0.0

[2] The details of the learning step are not addressed in this document.

4. Public Safety must carefully balance spectrum efficiency benefits against the critical need for system reliability, robustness, security, “instant on,” and other application-specific requirements of the first responder.

In this section, two scenarios for public safety will be given. An actual event of the London Bombing on 7 July 2005 will be analyzed in Section 2.1 illustrating four use cases. This scenario was developed by the Public Safety Work Group. The analysis of a hypothesized event of a fire at a chemical plant in an urban environment will illustrate another use case in Section 2.2. This use case was developed by the MLM Work Group.

2.1. London Bombing Use Cases

In the morning of July 7, 2005, bombs were detonated in three crowded subway trains and aboard a London bus. The explosions were spread out across several incident sites. At least 52 people died, along with four bombers, and 700 were injured. This event provides a real-world scenario that illustrates the significant challenges in responding to a terrorist event. The purpose of section 2.1 is to use the sequence of events that occurred on that day and the communications that occurred as part of the response to identify circumstances in which future cognitive radio capabilities could provide more efficient and effective communications in similar situations.[2]

2.1.1. Use Case 1: Network Extension for Coverage and Reachback

Cognitive radio capabilities could be used to automatically reconfigure radios to create peer-to-peer links and repeater functions that can link those radios to infrastructure when radios are cut off from their infrastructure, particularly during initial response to an incident prior to additional communication resources being deployed.[2]

2.1.1.1 Description of Use Case

Bombs exploded on three London Underground trains inside tunnels with varying distances to the nearest station. There was no light. The only escape was by walking through the tunnel to the nearest station. Responders had to walk to the scene through the tunnel. Once police and fire responders went into the tunnels, their radios lost connectivity to the above-ground infrastructure. The only means for responders to communicate back to their respective command centers and any above ground personnel was to walk to the nearest station and position themselves at the entrance to the Metro system. It took 15 minutes to walk from the scene to the entrance. Though responders had adequate authority to communicate on their own networks, individual radios were not capable of exploiting peer-to-peer capabilities to provide network extension to connect isolated nodes to the network.

The agencies that responded to the emergency included Metropolitan Police, British Transport Police, the London Fire Brigade, and London Ambulance. They entered the tunnels through the nearest station.

Cognitive radio technology could be

implemented to reconfigure responders' radios to create an extension to the existing network. This network extension would allow transmissions to be passed back and forth from the incident site along a network of individual responder radios operating in peer-to-peer mode to a radio which can communicate with the main radio system/network. The concept is illustrated in Figure 2-1. As shown, communications is enabled between personnel at the opening of the tunnel to dispatch and emergency management centers, but not from responders at the scene of the explosion in the tunnels. The impact of the network extension capability is that on-scene responders would have direct communications to command centers without leaving the incident scene or resorting to runners that delayed communications by as much as 15 minutes. The use case diagram is shown in Figure 2-2.

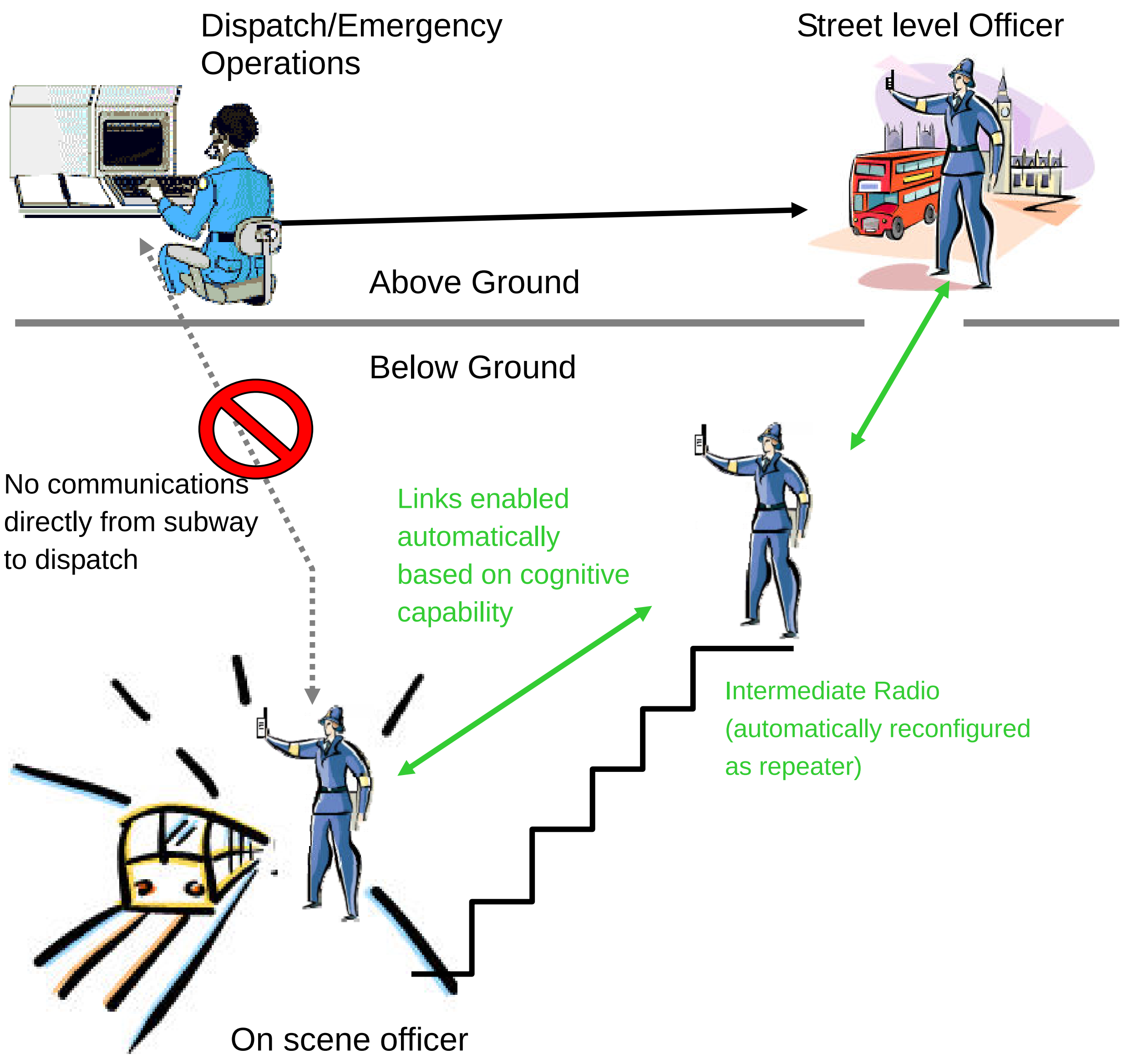
Dispatch/Emergency Operations
Street level Officer
Above Ground
Below Ground
No communications directly from subway to dispatch
Links enabled automatically based on cognitive capability
Intermediate Radio (automatically reconfigured as repeater)
On scene officer

Figure 2-1. Network Extension Use Case Example

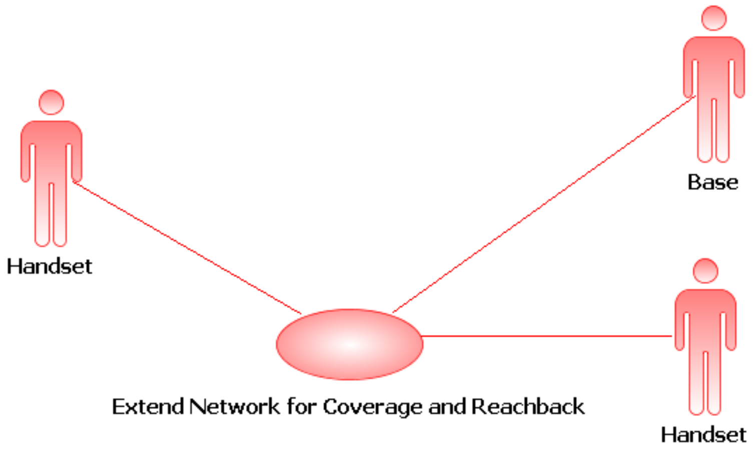

Figure 2-2. Network Extension Use Case Diagram[3]

Responders would maintain connectivity with their network at all times regardless of where they were located. Note that it would be possible to achieve the same effect by deploying repeaters at strategic locations to create the necessary extension. However, the cognitive capability has significant advantages that justify this use case:

- Cognitive capabilities and the ability to reconfigure radios would provide the network extension immediately, rather than after the period of time necessary to deploy repeaters.
- Cognitive capabilities would automatically determine appropriate network configuration. Repeaters would require manual determination of the repeater location, frequencies, and so on.
- Cognitive capabilities would allow the network extension to accommodate the dynamics of the response, as users arrive and leave, as the physical location of the responders changes, and so on.

2.1.1.2 Functional Capabilities

There are a number of functional capabilities assumed by this cognitive use case. First, the radios must be capable of being reconfigured to function as a network extension (e.g., the radios can operate on appropriate spectrum; the radios have reconfiguration algorithms, and so on). Second, there must be some level of cognitive capability for a collection of radios to “understand” that they have lost their ability to communicate with the system infrastructure. More specifically, radios must be capable of:

- Determining that one or more radios are disconnected from the system infrastructure;
- Finding and identifying peer radios;
- Identifying and authenticating compatible reconfigurable radios;

[3] The people images in the use case diagram represent actors in the UML representation. We assume that there are people associated to handset radios in these images.

- Determining which radios are within coverage of the infrastructure;
- Forming a satisfactory network extension route to the infrastructure from each affected radio using non-interfering frequencies for each “hop”;
- Adjusting the network topology as responders arrive and depart from the area where coverage is unavailable;
- Preserving the level of security of the baseline network in the network extensions;
- Providing either full duplex (simultaneous receive and transmit) operation or including a “store and forward” capability for user voice and/or data communications.

There are a number of approaches that could be utilized to achieve the network extension, such as ad hoc or mesh networks. The feasibility of existing protocols to accomplish this is a relevant research topic.

2.1.1.3 Assumptions

Below we describe the sequence of events as they might occur in this scenario. It is assumed that:

- The headsets in this network extension use case and the base stations have multiple air interface standard and cognitive radio capabilities (spectrum sniffing, adaptive power control, etc.).
- Since the focus of this document is not the protocol, a simplified version of proactive ad-hoc routing protocol is used. Each radio maintains a fresh list of destinations and their routes by periodically distributing routing tables throughout the network. In addition, next-hop is assumed to be a single radio.
- Figure 2-3 shows a typical topology of the network. The circles indicate the communication radius of each radio.
- Radios are preregistered with the base station.

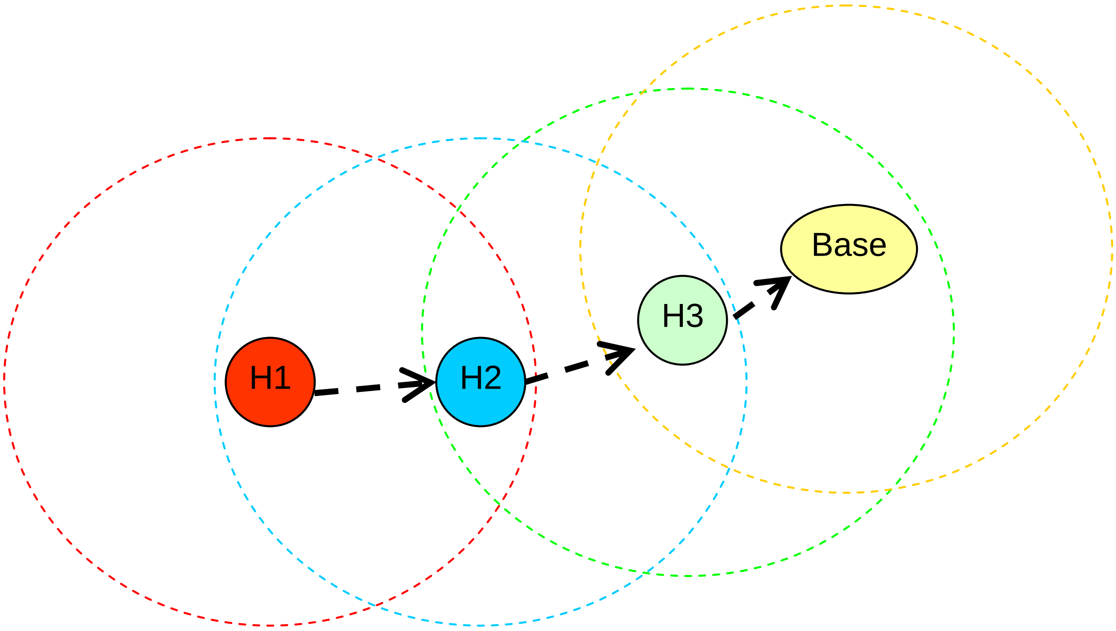

Figure 2-3. Topology of the Network

2.1.1.4 Timeline

1. **First-Responder's radio is disconnected from the infrastructure**
   a) The first-responder's radio (H1) scans the RF environment. The term scans means scanning the group of forward control channels in search of the strongest base station signal. The forward control channel is used for transmission of control messages from the base station to the mobile. If none of the control channels has signal strength above a usable level, the radio determines it's disconnected from the base station.
2. **First-Responder's radio sets up a peer-to-peer link to the base station**
   a) H1 broadcasts a query message to its neighbors for their information. Each radio maintains a route to each other radio in the network. The routing table contains ID (for example, IP address, MAC address, etc), next-hop ID, destination ID, and hop count. Initially, next-hop ID and hop count are set to a reasonable hop limit.
   b) In the mean time, H2, one of H1's neighbors, scans the RF environment and determines that it is disconnected from the base.
   c) H2 receives the query message from H1 and sends back an answer message to H1. In the mean time, H2 re-broadcasts the same query message to its neighbors. The answer message contains its own ID, spectral information, geographic or relative position and so on.
   d) H1 receives the answer message from H2 and updates its routing table. There are different criteria to choose the next-hop.
   e) In the mean time, H3, one of H2's neighbors, scans the RF environment and determines that it is connected to the base.
   f) H3 receives the query message from H2 and sends back an answer message to H2. In the mean time, H3 sends a message to the base, commanding the base to update its routing table.
   g) The base receives the command

message from H3 and updates its routing table.

h) H2 receives the answer message from its neighbors and updates its routing table.

i) Repeat (a) to (g) until the H1 finds a path to the base.

j) The base station sends a route reply message traversing back along the desired path to H1.

k) Route discovery is finished when the route reply message is received by H1.

3. First-Responder's radio transmits data packet to the base station

a) H1 sends a data message to H2.

b) H2 receives the data message and forwards the data to the next-hop (H3).

c) When the data message arrives at the destination, the destination radio sends back a confirm message (acknowledgement) to H1.

d) If H1 receives the confirm message within a predefined period of time, then the data transmission is finished. Otherwise, the data is considered to be lost; then the system repeats (a) to (d).

The topology of the network is dynamically changing as responders arrive and depart from the area where coverage is unavailable. Therefore, the radios must enable both periodic and event-triggered routing table updates. At every time interval, each radio broadcasts an update message to its neighbors with its current connectivity along with any routing table updates. After receiving an update message, the neighbors utilize the information to compute their routing table entries using an appropriate algorithm (e.g. iterative distance vector approach). In addition to periodic update, the radio should have the ability to announce important link changes, such as link removal when a responder departs from the area. Event-triggered updates ensure timely discovery of routing path changes.

The events are also represented in the UML Sequence Diagram in Figure 2-4. The boxes at the top of the figure represent radios involved in the use case. The vertical lines represent "life lines" or "time lines" of the radios with the time direction pointing downwards. Interactions between particular radios are shown by horizontal arrows annotated with the message types. All radios must have the knowledge of how to respond to particular types of events. All messages are expressed in the modeling language that all the radios can "speak".

Note that there are two kinds of arrows in the sequence diagram:

- An arrow from Radio1 (H1) to itself annotated with text in the form "< p > (< m >)", where p stands for a property and m stands for an element of the range of the property.
  - This arrow represents a sentence that can be expressed as a triple[4] <H1 p m>
  - Example: **scan(ForwardControlChannel_H1)**
    - *scan* is an *object property* which links the instances of *Radio* class to the instances of *Channel* class. This is illustrated in Figure 2-5.

[4] Triple is a sentence in the Resource Description Framework (RDF) language. It consists of a *subject*, a *predicate* and an *object*. The subject and object denote *resources* (*things* in the domain of discourse), and the predicate denotes a relationship between the subject and the object.

        - *H1* is an instance of *Radio* and *ForwardControlChannel_H1* is an instance of *Channel*.
        - Thus, the triple, <H1 scan ForwardControlChannel_H1>. It expresses the fact that H1 scans ForwardControlChannel_H1.
    - Example: **isConnectedToBase(false)**
        - *isConnectedToBase* is a *data type property* which links the instances of *Radio* class to an Boolean value.
        - The triple is <H1 isConnectedToBase false>
- An arrow from Radio1 (H1) to Radio2 (H2) annotated by "p(m)":
    - H1 invokes property p of H2. The triple is <H2 p m>
    - This type of arrow (in this case) represents the transmission of packet m from H1 to H2. m is an instance of *Packet* class. *Packet* class has properties such as *hasOriginatingAddress* and *hasTxMode*. Thus, the triples are <m hasOriginatingAddress H1> and <m hasTxMode TxMode>
    - *TxMode* can be unicast, broadcast, or multicast.
    - Example: **receive(Packet_queryRoutingTbl)**
        - *receive* is an *object property* which links the instances of *Radio* class to the instances of *Packet* class.
        - *H2* is an instance of *Radio* and *Packet_queryRoutingTbl* is an instance of *Packet*. Thus, the triple is <H2 receive Packet_queryRoutingTbl>
        - In this scenario, *H1* broadcasts *Packet_queryRoutingTbl* to all its neighbors. Hence, <Packet_queryRoutingTbl hasTxMode broadcast>, <Packet_queryRoutingTbl hasOriginatingAddress Address_H1>

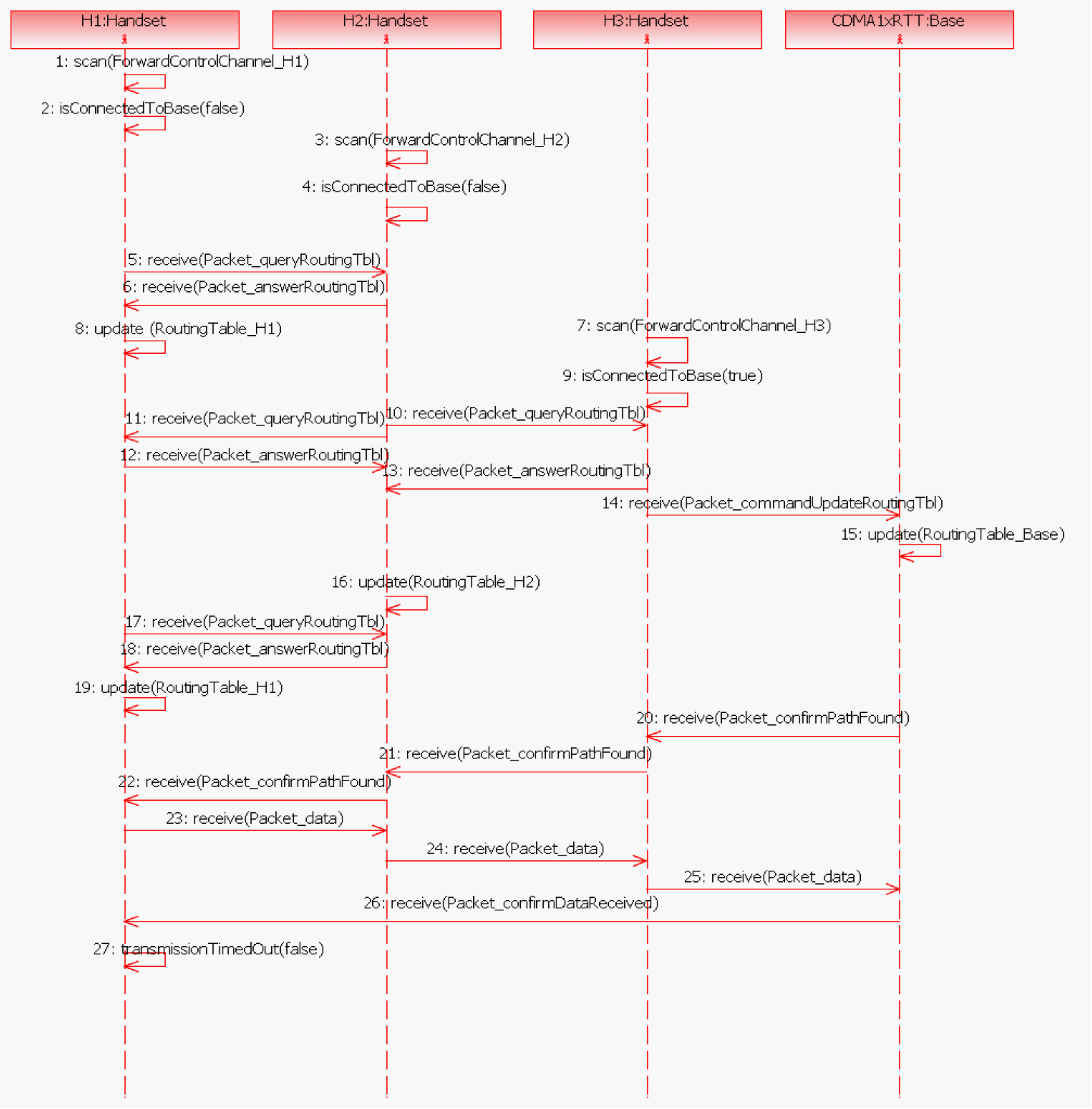
H1:Handset
H2:Handset
H3:Handset
CDMA1xRTT:Base
1: scan(ForwardControlChannel_H1)
2: isConnectedToBase(false)
3: scan(ForwardControlChannel_H2)
4: isConnectedToBase(false)
5: receive(Packet_queryRoutingTbl)
6: receive(Packet_answerRoutingTbl)
8: update (RoutingTable_H1)
7: scan(ForwardControlChannel_H3)
9: isConnectedToBase(true)
11: receive(Packet_queryRoutingTbl)
10: receive(Packet_queryRoutingTbl)
12: receive(Packet_answerRoutingTbl)
13: receive(Packet_answerRoutingTbl)
14: receive(Packet_commandUpdateRoutingTbl)
15: update(RoutingTable_Base)
16: update(RoutingTable_H2)
17: receive(Packet_queryRoutingTbl)
18: receive(Packet_answerRoutingTbl)
19: update(RoutingTable_H1)
20: receive(Packet_confirmPathFound)
21: receive(Packet_confirmPathFound)
22: receive(Packet_confirmPathFound)
23: receive(Packet_data)
24: receive(Packet_data)
25: receive(Packet_data)
26: receive(Packet_confirmDataReceived)
27: transmissionTimedOut(false)

Figure 2-4. Sequence Diagram of Network Extension Use Case[5]

2.1.1.5 OWL Ontology Representation

All the messages written above the arrows in Figure 2-4 are expressed in terms coming from an ontology. This ontology was developed for the sole reason of formalizing the Network Extension use case, thus we call it here the Network Extension Ontology. A graphical representation of this ontology

[5] The figure shows an example of end to end acknowledgement

is shown in Figure 2-5. The ontology was formalized in OWL using the Protégé tool[6]. Each rectangle in this figure represents a class. The first row in the rectangle shows the name of the class, followed by several rows, each of which shows a property of that particular class, either a *dataType property* or an *object property*. Arrows between classes are annotated by *property names*. Such arrows represent *object properties*. Each arrow can be read as a triple <Class1 propertyName Class2>, e.g. <Radio hasComponent RadioComponent>. An arrow connecting two classes annotated by "isa" represents subclass relationship, e.g. RoutingTable is a subclass of RadioComponent[7].

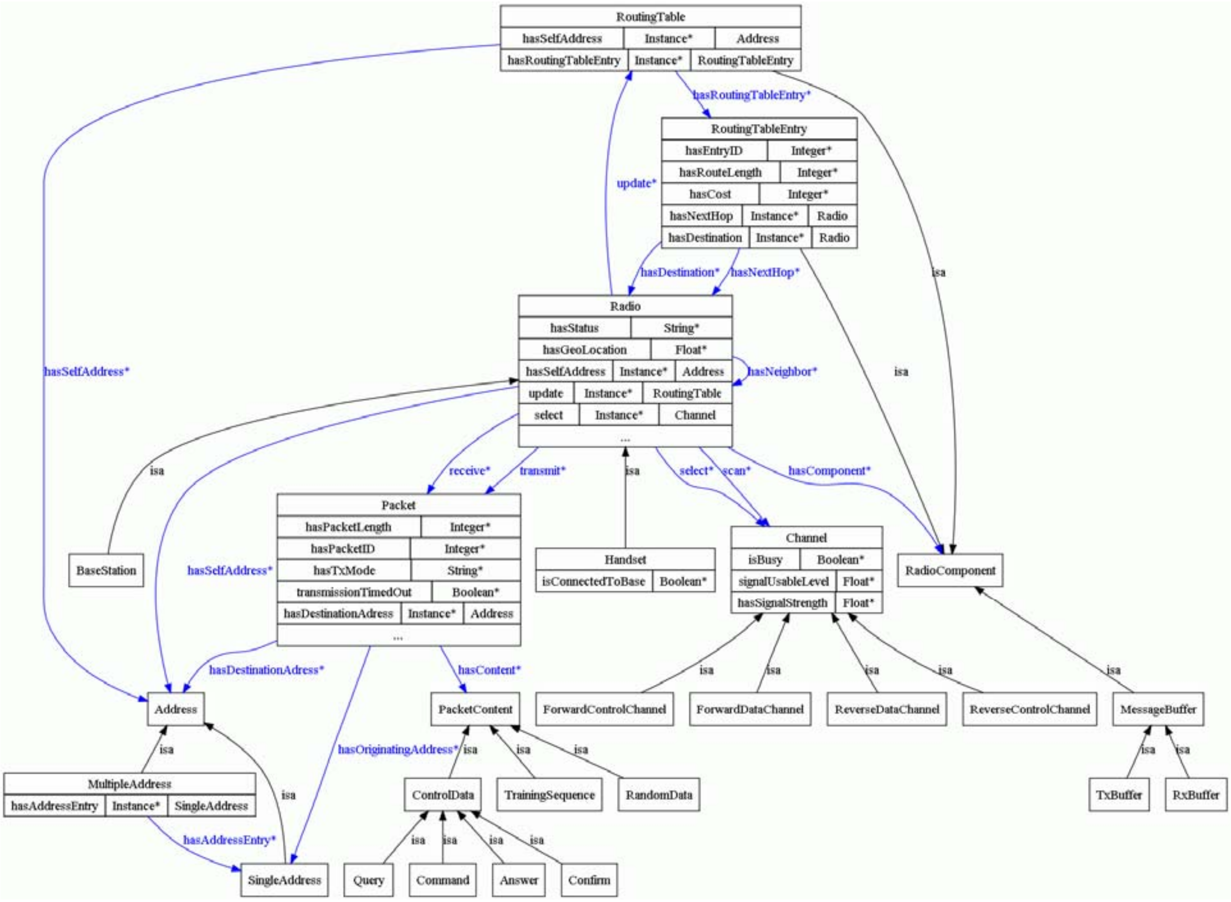

Figure 2-5. Ontological representation of the Network Extension Use Case. Isa arrows are black. Other arrows are blue.

2.1.2. Use Case 2: Dynamically Access Additional Spectrum

Dynamic spectrum access, or the ability of cognitive radios to identify and exploit unused or underutilized spectrum, could be a solution in the scenario when the system is overloaded. E.g., the

[6] Protégé is available at http://protege.stanford.edu.The OWL file for this ontology is available from the SDR Forum at http://groups.sdrforum.org/p/do/sd/sid=95&type=0.

[7] Note that a sub-component of another component is also a sub-component of a whole, like a bolt is a sub-component of wheel, but at the same time also a sub-component of a car. A complete ontology would have many other types of component, not just the ones shown in this figure.

commercial cellular system that is in its normal use, but is also used by the first responders. This use case is about providing a means for expanding capacity when needed [2].

2.1.2.1 Description of Use Case

This use case, shown in Figure 2-6, involves identifying and utilizing spectrum not normally utilized by the system (not within the air interface standard being used).

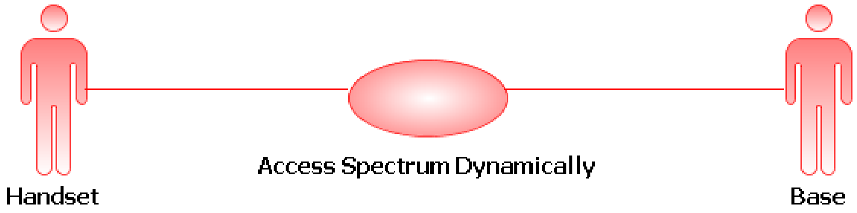

Figure 2-6. Dynamic Spectrum Access Use Case Diagram

There are three different approaches that can be considered to realize this use case, as outlined (underlined) below:

Pre-defined agreement among organizations: One approach to dynamic spectrum access is to establish agreements among organizations that would allow a non-licensed authorized user to utilize additional spectrum under defined circumstances and by mutual agreement. There is a broad range of potential types of agreements under which spectrum could be dynamically accessed. The following provides a range of possibilities:

- Dynamic spectrum access that is triggered by a pre-defined event, such as reaching a capacity limit;
- Dynamic spectrum access that occurs when one organization requests access and the licensed organization grants it (e.g., spectrum mutual aid).
- Dynamic spectrum access granted to another user (spectrum leasing) or to a secondary user on a non-interfering basis.

Emergency declaration: Another approach to dynamic spectrum access is to establish rules by which some spectrum is accessed for emergency response under a governmental declaration. The cognitive capability may be limited to identifying the load circumstances under which access of additional spectrum is appropriate, or may be used to manage network and subscriber reconfiguration to enhance spectrum utilization.

Identify unused or underutilized spectrum not licensed to the network: Another approach to dynamic spectrum access is to monitor spectrum utilization in frequencies not licensed to the network, identify spectrum which is unused or underutilized ("white space"), and reconfigure the network and subscriber equipment to utilize that spectrum. Clearly this type of dynamic spectrum access would be limited to emergency situations and only be allowed under clearly defined circumstances (such as a governmentally allowed policy). Cognitive capabilities would be required to identify available spectrum and to reconfigure the network and subscribers accordingly.

In this scenario, the network congestion would be relieved by providing more spectrum for use by all network users including first responders. If the infrastructure has a cellular architecture, it may be possible to dynamically reallocate the channel distribution to create additional capacity in the afflicted cells. Alternately, there may be a place in nearby spectrum where some other service can be pre-empted to satisfy the demand.

There are a number of procedural decisions involved in implementing this use case. Key procedures include determining at what point to invoke dynamic spectrum access procedures, procedures for identifying spectrum that can be utilized, and when to release the bandwidth.

The approach that allows spectrum to be accessed for emergency response may not be embodied in existing regulations and would need to be added to allow this approach. These regulatory changes can involve sweeping changes to how spectrum is utilized in emergency situations, and that crafting rules which balance the needs of emergency response and other legitimate uses of spectrum during emergencies will require extensive research, development, and public discussion.

This kind of spectrum sharing would require a significant amount of advanced detail planning. Plans can have varying degrees of dynamic range. Switching from one fixed plan to another is easier than dynamic cognitive problem solving in real time, but more likely would result in less efficient spectrum utilization.

2.1.2.2 Functional Capabilities

Dynamic spectrum access implies a number of functional capabilities, as described below.

- The base station and/or associated management infrastructure (or similar network component for systems that do not designate a base station) (called network below) must be able to identify capacity loading that exceeds whatever criteria are in place to initiate the dynamic spectrum access.
- The network must be capable of identifying spectrum resources that can be utilized to offload some calls. There are two possible approaches to identifying additional spectrum.
    - First, there may be established agreements in place that under certain circumstances spectrum normally used for one purpose is made available to support communications networks being utilized in an emergency. Such identification could be based on established agreements among spectrum “owners” or based on allocation of spectrum for emergency use in the event of a certain level of emergency.
    - Alternatively, cognitive radio nodes can search for underutilized spectrum (“white space”) that could be dynamically accessed. Note that in this case a scheme must be implemented to manage the hidden node problem. Also, the network must be able to support the ability to de-conflict the situation if multiple users attempt to access the same available spectrum “white space”.
    - The system must perform a spectrum and air interface rendezvous process for radio

nodes of the network.

- The network infrastructure must be able to reconfigure itself to use the new spectrum. If the system is a trunked system, the network must be able to incorporate additional frequency options into the system. Network transmitters and receivers must be able to be reconfigured to utilize the additional spectrum. If the additional spectrum is based on a pre-defined agreement, frequencies may be pre-programmed, in which case only an execution command is required to access the additional spectrum.
- Subscriber equipment must be able to reconfigure to use the new spectrum, i.e., must be able to transmit and receive on the additional frequencies.
- Reconfiguration information must be communicated among the radios and the network infrastructure to coordinate the utilization of additional spectrum.
- Dynamic access of spectrum must be consistent with the regulatory requirements of that spectrum (e.g., in terms of bandwidth, out of band emissions, power management, location based rules) to ensure that other users in that service are not adversely impacted by use of a specific frequency.

2.1.2.3 Timeline

Below we describe the sequence of events as they might occur in this scenario. It is assumed that the radios in this scenario and the base stations have the necessary cognitive radio capabilities. The events are also represented in the UML Sequence Diagram in Figure 2-7.

.

1. The Base Station periodically scans the RF environment and updates the spectrum utilization information (given as SpectrumUtilizationTbl in Figure 2-7)
2. When the capacity demand exceeds the available capacity, it is determined that the system is over-loaded. Dynamic spectrum access is triggered.
3. A user’s radio (H1) sends a request to the base station for a voice call initialization.
4. The base station identifies the unused or underutilized spectrum and chooses a channel (channel_H1) as the forward and reverse voice channel pair.
5. Base station sends a command message to H1 and configures channel_H1 as H1’s reverse voice channel.
6. Base station configures channel_H1 as its reverse voice channel.
7. H1 sends a command message to base station, asking if it is ready to receive data.
8. Base station sends back a confirm message to H1.
9. H1 starts to send data traffic to the base station.
10. When the data message arrives at the base station, the base station sends back a confirm message (acknowledgement) to H1.
11. If H1 receives the confirm message within a predefined period of time, then data transmission is finished. Otherwise, the data is considered to be lost, and then steps (3) to (10) would be repeated.

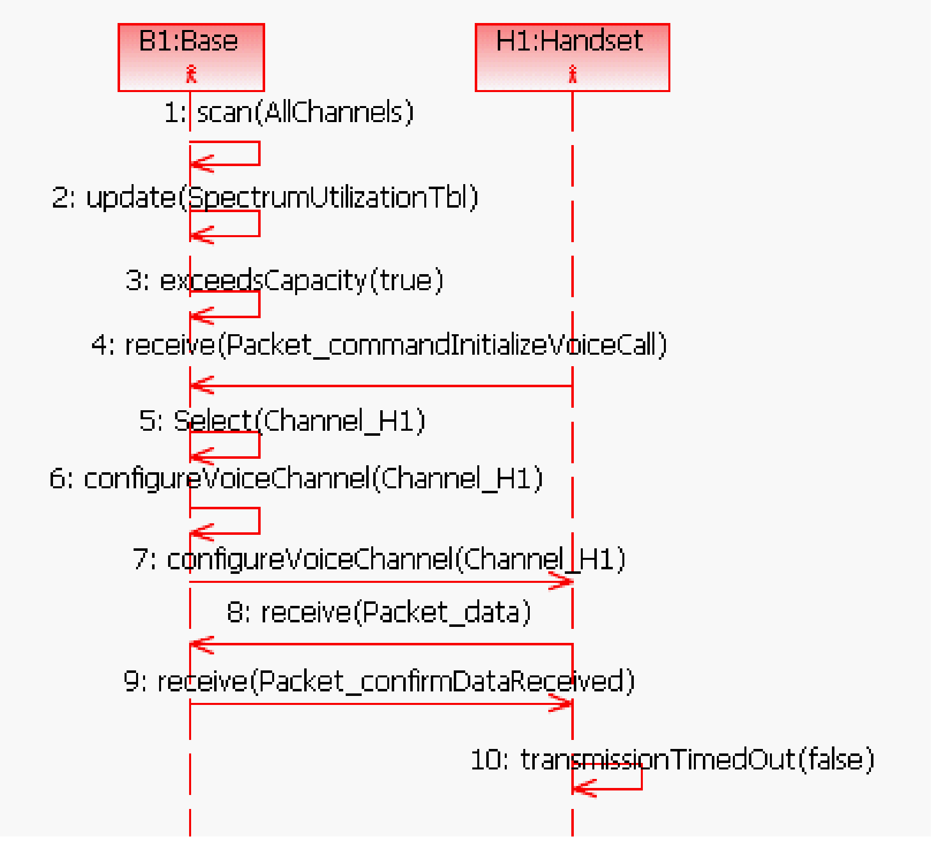
B1:Base
H1:Handset
1: scan(AllChannels)
2: update(SpectrumUtilizationTbl)
3: exceedsCapacity(true)
4: receive(Packet_commandInitializeVoiceCall)
5: Select(Channel_H1)
6: configureVoiceChannel(Channel_H1)
7: configureVoiceChannel(Channel_H1)
8: receive(Packet_data)
9: receive(Packet_confirmDataReceived)
10: transmissionTimedOut(false)

Figure 2-7 Sequence Diagram for Dynamic Spectrum Access

2.1.3. Use Case 3: Temporarily Reconfigure First Responder Communication Device Priorities

Cognitive radios (in this case, referring to cell phones) might be able to be temporarily reconfigured with higher priorities based on the circumstances of the emergency responder.[2]

2.1.3.1 Description of Use Case

The dynamic prioritization use case, shown in Figure 2-8, exploits cognitive capabilities to adjust the priorities of responders based on the ongoing communications activity as well as the dynamics of incident response.

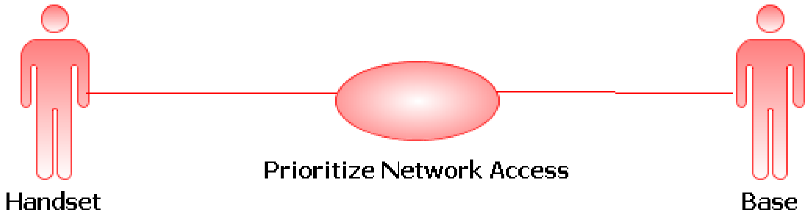

Figure 2-8. Dynamic Prioritization Use

Case Diagram

Priority schemes are implemented in today's public safety and commercial cellular systems. The application of cognitive capabilities provides the opportunity to adjust those priorities to accommodate unanticipated priorities or to manage priority access in real-time.

In a crisis situation, as demands for system resources rise, it may become necessary to manage access to the system based on the relative importance of the user and the communication being transmitted. The concept of this use case is to be able to change those priorities in real-time as an event unfolds. In the case of emergency responders using a commercial cell phone network, an example of priority access may be public safety users getting priority access over commercial users in the event of emergency situations.

The role of cognitive capabilities here is in the ability to adjust those priorities in real time based on the unfolding events of the incident, communications resources demands and availability, and the changing roles of individual responders over the course of an event. In the case of the London bombing scenario, a capability that would have enabled responders who did not have Access Overload Control (ACCOLC)-enabled devices (cell phones) would be to have devices reconfigured over-the-air and in real time. This could have eliminated the risk of responders being denied access to the system in the event that ACCOLC was invoked. These cognitive capabilities could provide more sophisticated and dynamic access management for radio/cellular systems.

First responders would be assigned a priority based on their role[8] in support of the response. Priority modifications would be downloaded to the first responders' mobile phones as needed. In addition, cognitive capabilities in the network management would recognize the increasing load level and congestion levels and block access to lower priority calls as needed. User mobile phones would also have a cognitive capability that indicates that user access has been blocked so that the system loading is not made worse by persistent access attempts.

Appropriate procedures will be needed, and depend on what particular approach is followed. For example, if individual responders are allowed to change (or request to change) their priority, policies and procedures need to be defined to govern the circumstances and steps to be followed by responders. Likewise, policies and procedures for any request approvals or assignment of priorities as described in the following section will be required.

2.1.3.2 Functional Capabilities

A number of capabilities must be available in order to realize this cognitive use case. First, there must be a mechanism to determine those public safety responders who have a legitimate need to have priority access to the communications network. Access to the network itself has already been established, i.e., the network has already recognized and authenticated the first responder's cell phone (responder's device). The required capability is to establish that the circumstances of that particular user warrant a level of priority greater than the priority level

[8] Other types of priority (including based on information type, environmental conditions, pre-existing service agreement, etc) may be required, but are not considered in this use case.

currently granted to the responder’s device.

The definition and assignment of priorities can incorporate a number of different elements of incident response and management. For example, priority assignments could be based on:

- The roles within the response that have been assigned to the individual responder’s device;
- Physical location of the responder’s device;
- Service of the responder’s device (e.g., EMS priority over law enforcement);
- Type of data being communicated;
- Role of the user in the communications process.

There is a potentially broad range of complexity and sophistication of the cognitive capabilities implied by this use case. Relatively simple cognitive capabilities could be implemented to associate priorities with responder assignments, physical location, and/or service. More sophisticated cognitive capabilities could assign priorities automatically based on a variety of parameters associated with the communications of the response, or even in a predictive mode to anticipate, rather than react to, the dynamic needs of the responders.

The advantage of role based priorities (supplemented by other ad hoc assignable methods) is that preplanning can determine the appropriate priorities for each role in a variety of situations of varying complexity. Cognitive capabilities might be able to assess the level of complexity involved and select a suitable priority. All of this is supplemented by the user controlled methods delineated as follows.

One approach to considering the different functional capabilities for handling priority assignments is to consider that there are three possibilities for requesting changes in priority—the responder, some central authority (e.g., incident command, incident communications leader), and the communication network itself. Note that in the case of the communications network, the actual functionality could be distributed between the subscriber unit and the network infrastructure, but the request or the authorization is made automatically without human initiative. Each of these entities may also authorize the requested priority change. This leads to six possible approaches to priority assignment as shown in Table 2-1.

Authorized by **Requested by**	**Individual Responder**	**Central Authority**	**Network**
Individual Responder	Priority is defined by individual responder	Individual requests are granted "manually" by central authority, would not require cognitive capabilities.	Cognitive capabilities in the communications network evaluate requests initiated by individual responder
Central Authority	Priority changes are initiated by central authority and "accepted" by individual responder.	Central authority makes unilateral decisions regarding its own resources.	Cognitive capabilities in the communications network evaluate requests initiated by central authority
Network	Cognitive capabilities in network "recommend" priority change to individual responder who must "accept" the change.	Cognitive capabilities in network "recommend" priority changes to central authority who must "accept" the change.	Fully automated capability for priority management with no human in the decision loop.

Table 2-1. Possible Dynamic Prioritization Approaches

While any of the above approaches is possible, we recognize that not all approaches will be appropriate for all situations, and user requirements for a specific system may well dictate that only one of the above approaches be implemented in a particular system. In addition, we recognize that an investment may be required to maintain information on responder credentials and to establish general policies as well as specific priorities associated with roles assigned to individual responders. Also note that there are ongoing and planned efforts in developing responder credential infrastructure to support incident management that can be leveraged to support this use case.

The other significant functional capability is the capability to reconfigure such a responder's device. In this situation involving a GSM-based cellular network, when ACCOLC is invoked, only cell phones with a SIM with priority authorization can access the system; other devices are blocked. The proposed cognitive use case assumes that either the SIM can be provisioned over the air for properly authenticated users, such that the phone would function with priority access. Alternatively, the system could determine that the user was a priority user based on the device ID (as opposed to the priority access code in the SIM) and allow access that way as well; however, the system computational effort to determine whether a call is being initiated by a priority user may involve substantial computational requirements.

We recognize that assignment of priorities presents challenges in making the determination of what communications are more important than others. Part of the ACCOLC decision criteria is the understanding that implementing ACCOLC would deny access to the network for responders (or for victims and observers who are providing critical information or notifying others). The ability to prioritize communications as proposed in this use case does not guarantee that all critical or important calls are made—there are physical limitations to the capacity of any system. However, this use case provides the opportunity to utilize cognitive radio capabilities to implement the best decisions that can be made with the available information.

In addition to the changes to dynamically modify user priority, it is also important to be able to restore default, or other pre-defined conditions, such as when the user no longer requires priority access. Different mechanisms for restoration may be implemented but could be similar to the same mechanisms used to implement dynamic prioritization. Restoration could be executed based on a variety of mechanisms, for example user request, incident command direction, and location if the user moves out of the incident area.

2.1.3.3 Timeline

Below we describe the sequence of events as they might occur in this scenario. It is assumed that the radios in this scenario and the base stations have the necessary cognitive radio capabilities. The events are also represented in the UML Sequence Diagram in Figure 2-9.

1. The first responder’s radio (H1) arrives.
2. H1 scans the RF environment and determines there is a base station nearby.
3. H1 registers with the base station as an incident leader.
4. The base station sends a command message to H1, and authorizes H1 with high-priority.
5. A second radio (H2) arrives.
6. H2 scans the RF environment and determines there is a base station nearby.
7. H2 registers with the base station as an ordinary user.
8. The base station sends a command message to H2, and authorizes H2 with low-priority.
9. H2 sends a command message to the base station requesting a voice call initialization.
10. Since H2 has low priority, the base station sends a command message to H2, indicating the service to H2 has been blocked.
11. H2 indicates to the user that the access has been blocked because the network is congested.

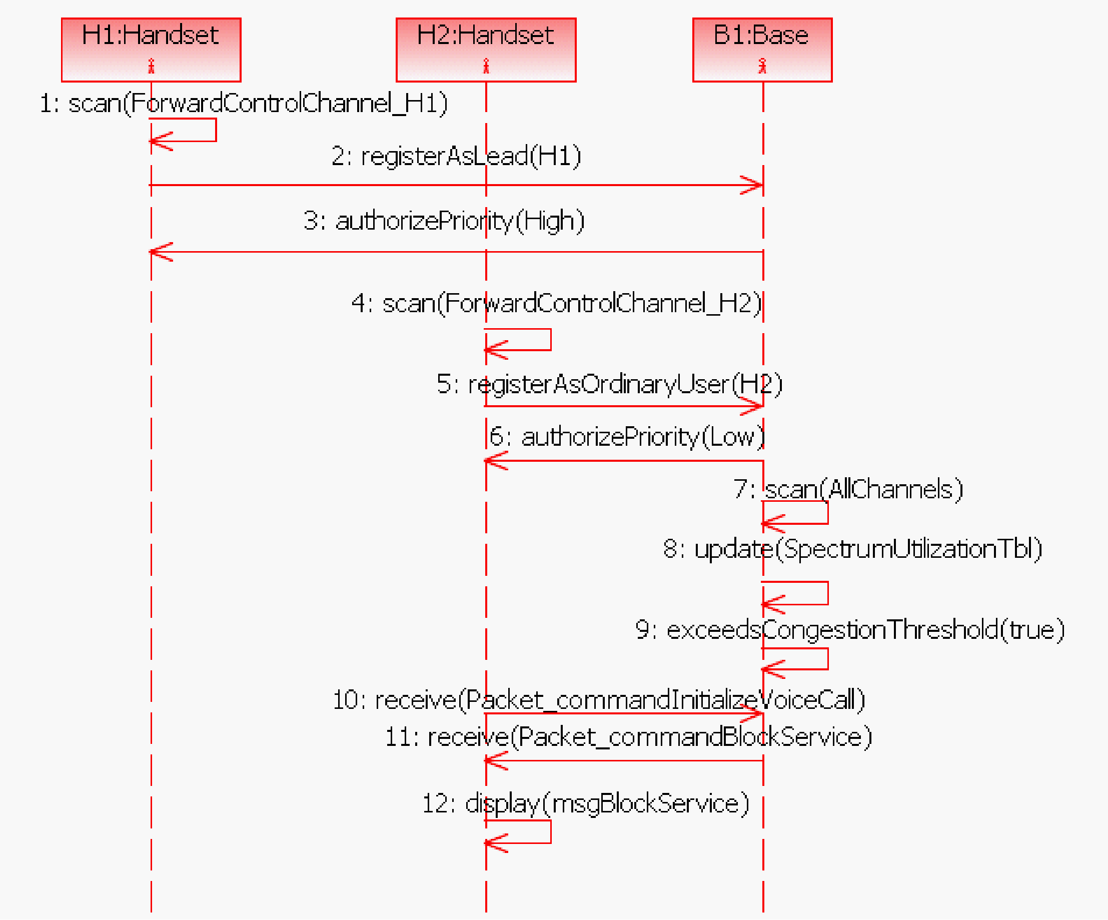
H1:Handset
H2:Handset
B1:Base
1: scan(ForwardControlChannel_H1)
2: registerAsLead(H1)
3: authorizePriority(High)
4: scan(ForwardControlChannel_H2)
5: registerAsOrdinaryUser(H2)
6: authorizePriority(Low)
7: scan(AllChannels)
8: update(SpectrumUtilizationTbl)
9: exceedsCongestionThreshold(true)
10: receive(Packet_commandInitializeVoiceCall)
11: receive(Packet_commandBlockService)
12: display(msgBlockService)

Figure 2-9. Sequence Diagram for the Dynamic Prioritization Use Case

2.2. Urban Fire Use Case

2.2.1. Description of Use Case

In this scenario there is a fire at a chemical plant in an urban environment. The use case diagram is shown in Figure 2-10. We will be concerned with three first responders and their radios. The three are an Incident Commander (Leader), a Fire Service Person and an Emergency Medical Technician (Medic).[1]

The Leader arrives with a portable radio which can be configured as a CDMA 1X RTT cellular, WiFi (2.4 GHz), or WiMax (5GHz) radio. The Fire Person arrives with a specialized fire network radio that can be configured to support CDMA 1X RTT cellular, WiFi (2.4 GHz), WiMax (5GHz) if correct S/W is downloaded. The Medic arrives with a specialized fire network radio that can be configured to support CDMA 1X RTT cellular, WiFi (2.4 GHz), WiMax (5GHz) if correct S/W is downloaded. Each of these contains a Control Point that can be enabled. All or a portion of a Control Point can be enabled. Only one Control Point, or portion thereof, is enabled at a time to prevent contradictory Cotrol Point messages from circulating in the network. Table 2-2 provides the radio capabilities that each role possesses.

Role	Radio Capabilities
Incident Commander (Leader)	• 800 (806 -824) MHz Voice Communications (FM conventional digital voice encoding) • CDMA 1X RTT cellular • WiFI (2.4 GHz) • WiMax (5GHz) radio
Fire Service Person	• 800 (806 -824) MHz Voice Communications (FM conventional digital voice encoding) • CDMA 1X RTT cellular • WiFi (2.4 GHz) • WiMax (5GHz)
Emergency Medical Technician (Medic)	• UHF (450-470MHz) • Voice Communications(FM conventional digital voice encoding) • CDMA 1X RTT cellular • WiFi (2.4 GHz).

Table 2-2. Radio Capabilities of Each Role

It is assumed that the radios of all of the human actors in this scenario and the base stations have the necessary cognitive radio capabilities.

1. **The Incident Commander Arrives on Scene.**
   a) Incident commander activates the emergency function on his radio, causing his location to be captured, his support infrastructure to be notified, and alerting the radio to apply emergency situational context
   b) The responder’s radio scans the RF environment and determines that there is a CDMA 1XRTT base station in the area with some bandwidth available and a functioning unsecured WiFi access point with connectivity to the Internet.
   c) The responder’s radio determines that the Cellular Base Station is likely to provide the most reliable connectivity at this location.
   d) The responder’s radio registers with the base station.
   e) The responder’s radio checks if there is any leader present and determines that he is the leader
   f) The leader’s radio informs the base station that it has a Leader radio role, and enables that portion of the Control Point appropriate to an incident commander.

2. **The Fire Person Arrives on Scene.**
   a) The fireman seeks connectivity with a Leader. His radio first seeks a leader on the specialized Fire AIS. Finding none, the radio starts downloading other AISs over the Fire AIS and starts sensing for the other AISs.
   b) The radio detects a CDMA base

station pilot, registers with the CDMA base station and requests (using MLM) connection to a leader.

c) The fireman's radio connects with the Leader's radio identifying itself (current configuration and potential configurations), its user, and requests instructions via an async data session.

d) The Fire Person's radio requests detailed maps / plans of the site, lists of dangerous chemicals likely to be on site. The Leader will need streaming video from the close vicinity of the fire and the leader and the Fire person will require a voice channel.

e) The Leader's radio indicates that there will be a large number of responders, so the radio determines that the best use of available spectrum is for the Fire Person's radio to initially use the 5GHz WiMax band configured for streaming video, async data and VOIP. It instructs the Fire Person's radio over CDMA 1XRTT channel to switch to 5GHz WiMax.

f) The Fire person's radio determines that given the impending arrival of a large number of responders, the best way to obtain the required WiMax S/W is to switch to the previously detected WiFi access point (after authorization/association) and download it that way. Using its modeling language definition of its existing hardware and S/W platform, it finds the appropriate software on the appropriate network to allow it to reliably operate on 5GHz WiMax and downloads it.

g) The Fireman's radio checks the downloaded S/W modules against its MLM configuration description. If the Fireman's radio determines that the module will operate correctly, not cause any problems on the local radio and will not emit any spurious emissions, etc, the radio loads it and registers with the WiMax access point.

h) The Fireman's radio then initiates a WiMax VOIP and streaming video session with the Leader.

i) The Fire person's radio is downloading site maps / plans and lists of likely dangerous chemicals via the specialized fire AIS and supporting infrastructure.

j) As soon as the Leader's radio detects that it is in VOIP / streaming video session with the Fire Person, the leader and the Fire Person discuss the best direction / means to approach the fire from.

k) The Fire Person approaches the fire.

l) The leader observes the streaming video.

3. **The Medic Arrives on scene**.

a) The Medic's radio seeks connectivity with a Leader. His radio first seeks a leader on the specialized Medic AIS. Finding none, the radio starts downloading other AIS's using the Medic AIS and starts sniffing for other AIS's.

b) The radio detects a CDMA base station pilot, registers with the CDMA base station and requests (using MLM) a connection to a leader.

c) The Medic's radio connects with the Leader's radio identifying itself (current configuration and potential configurations), its user, and requests instructions via an async data session.

d) The Leader's radio knows (using appropriate policies expressed in MLM) that the Medic's radio will likely need detailed maps / plans of the site, lists of dangerous chemicals likely to be on site and that the Leader will likely need an async data channel to direct the Medic to injured people.

e) The Medic's radio determines that the best use of available spectrum, given that there are likely to be a large number of responders, is for the Medic's radio to initially use the WiFi band configured for async data and VOIP. It requests the Fire Person's radio over a CDMA 1XRTT channel to switch to 2.4GHz WiFi.

f) The Medic's radio determines that given the impending arrival of a large number of responders, the best way to obtain the required WiFi S/W is to switch to the specialized Medic AIS and download it that way. Using the MLM definition of its existing hardware and S/W platform, it finds the appropriate software on the Medic infrastructure to allow it to reliably operate on 2.4GHz WiFi and downloads it.

g) The Medic's radio checks the downloaded S/W modules against its MLM configuration description. If the Medic's radio determines that the module will operate correctly, not cause any problems on the local radio and will not emit any spurious emissions, the radio loads it. It then initiates a WiFi VOIP and async data session with the Leader.

h) Simultaneously with the WiFi VoIP, the Medic's radio is downloading site maps / plans and lists of likely dangerous chemicals via the CDMA 1XRTT AIS from the Fireman's radio.

i) The Leader's radio seeing this pattern of usage, instructs the CDMA 1XRTT base station to cache the maps / plans and lists of dangerous chemicals and deliver them to all Firemen and Medic's who arrive at the incident.

j) The Medic's radio sends the list of dangerous chemicals using its specialized Medic AIS to its infrastructure requesting precautions and initial treatment for each.

k) As soon as the Leader's radio detects that it is in async and VOIP session with the Medic, the Leader tells the Medic he will send directions to injured people and any available information about their injuries via the async data channel and then disconnects from voice contact. Both radios shut down the VOIP session.

As more Fire people and Medics arrive, control may be distributed with a Fire Leader and a Medic Leader. At the same time, people with different roles will begin arriving. Crowd control, air traffic control, etc. may become involved. With a little imagination, the reader can see that these intelligent radios, with MLM describing what the capabilities of the radios are, what the characteristics of their users are and the type and flow of information they can provide, will enable efficient communication. Further complexity can be introduced by allowing radios to move into unoccupied spectrum allocated to other users.

2.2.2. Actors

The Actors in this Use Case are:

H1 - Leader Radio (shown as Leader in Figure 2-10)

H2 - Fire Person's Radio (shown as FireP)

H3 - Medic's Radio (shown as Medic)

B1 - 1XRTT Basestation & Infrastructure (shown as Base)

B2 - WiFi Access point & Infrastructure (shown as WiFiAP)

B3 - WiMax Access Point & Infrastructure (shown as WiMaxAP)

B4 – Fire Public Safety AIS Basestation & Infrastructure (shown as FireNet)

B5 - Medic Public Safety AIS Basestation & Infrastructure (shown as MedNet)

Control Point (shown as CP1 in Figure 2-11) – Because all the actors contain a Control Point which may or may not be active, the Control Point is not shown as an Actor in this Use Case. Instead, the Time Line and Sequence diagrams show only which actor's Control Point has been enabled.

The actors in this use case are diagramed in Figure 2-10.

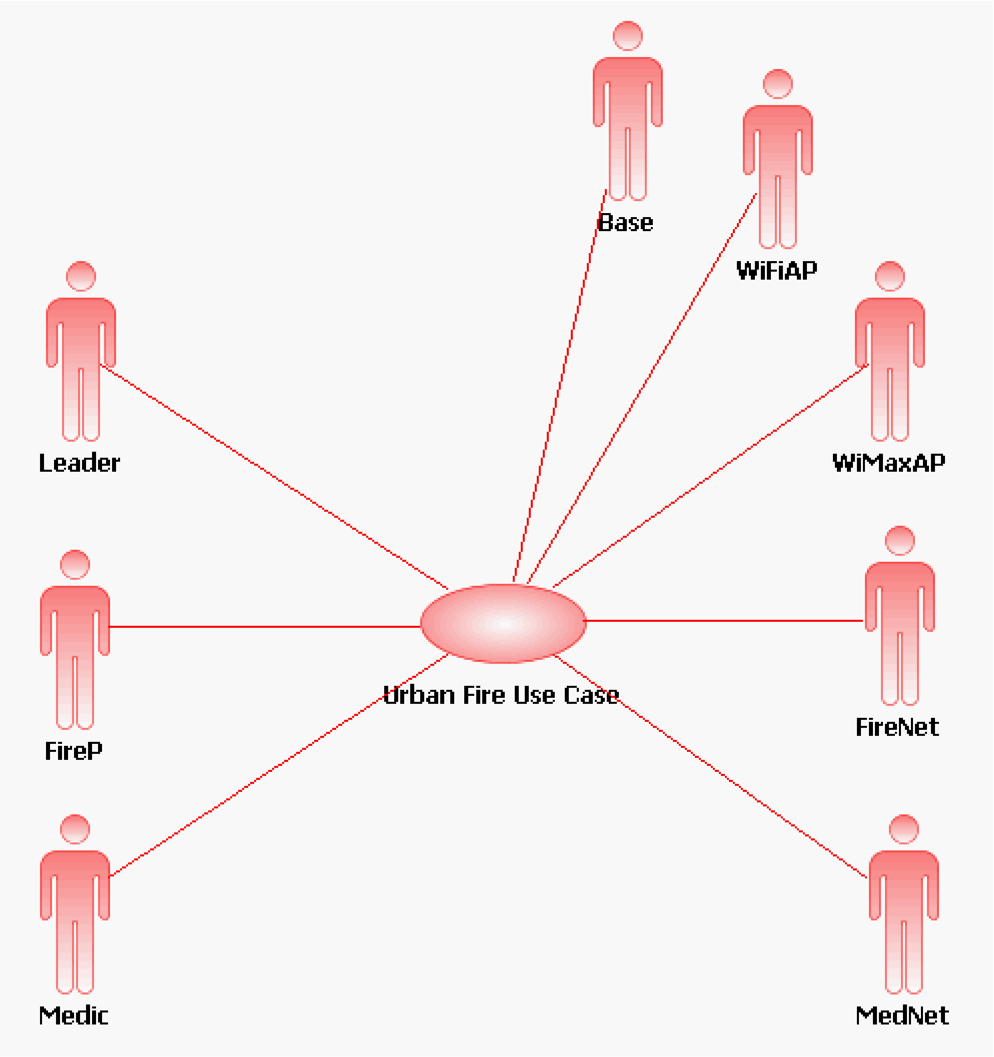

Figure 2-10. Urban Fire Use Case Diagram

2.2.3. Timeline

The Time Line for this Use Case is simplified for ease of understanding. The reader should refer back to the scenario for a full understanding of the inferences based on MLM descriptions that guide critical steps. Before this Time Line starts, B1's Control Point has been enabled.

1. **H1 arrives on scene**.
   a) H1 sniffs the spectral environment, infers that B1 provides best connectivity and requests registration on B1.
   b) B1 registers H1.
   c) H1 asks B1 if there is a leader present
   d) B1 answers that there is no leader present
   e) H1 requests the enabling of CP1 on H1
   f) B1 enables CP1 on H1
2. **H2 arrives on scene.**
   a) H2 is handed over to B4 and asks B4 if it has CP1
   b) B4 replies that it does not
   c) H2 sniffs the spectral environment, infers that B1 has the highest probability of having CP1 and requests registration with B1
   d) B1 registers H2
   e) H2 asks B1 if it has CP1
   f) B1 replies no, but that it transferred CP1 to H1
   g) H2 requests connection to H1
   h) B1 connects H2 to H1
   i) H2 asks H1 if it has CP1
   j) H1 replies that it does
   k) H2 requests base station assignment from CP1
   l) CP1 assigns H2 to B3
   m) H2 determines that it does not have S/W for WiMax (B3's AIS)
   n) H2 having sniffed the spectral environment, infers that the best way to obtain S/W is via B2
   o) H2 requests registration with B2
   p) B2 registers H2
   q) H2 requests S/W
   r) B2 delivers S/W to H2
   s) H2 examines the MLM description of itself and of the new S/W (including security info described in a later Use Case) and infers that loading the S/W has a high probability of achieving the desired results
   t) H2 installs the S/W
   u) H2 requests registration with B3
   v) B3 registers H2
3. **H3 arrives on scene.**
   a) H3 is handed over to B6 and asks B6 if it has CP1
   b) B6 replies that it does not

c) H3 sniffs the spectral environment, infers that B1 has the highest probability of having CP1 and requests registration with B1

d) B1 registers H3

e) H3 asks B1 if it has CP1

f) B1 replies no, but that it transferred CP1 to H1

g) H3 requests connection to H1

h) B1 connects H3 to H1

i) H3 asks H1 if it has CP1

j) H1 replies that it does

k) H3 requests base station assignment from CP1

l) CP1 assigns H3 to B2

m) H3 determines that it does not have S/W for WiFi (B2's AIS)

n) H3 having sniffed the spectral environment, infers that the best way to obtain S/W is via B6

o) H3 requests registration with B6

p) B6 registers H3

q) H3 requests S/W

r) B6 delivers S/W to H3

s) H3 examines the MLM description of itself and of the new S/W (including security info described in a later Use Case) and infers that loading the S/W has a high probability of achieving the desired results

t) H3 installs the S/W

u) H3 requests registration with B2

v) B2 registers H3

2.2.4 Sequence Diagram

Figure 2-11 shows the sequence diagram of this scenario. The boxes at the top of the figure represent radios of particular human actors involved in the use case. The vertical lines represent "life lines" of the radios with the time direction pointing downwards. Interactions between particular radios are shown by horizontal arrows annotated with the message types. Initiation of the communication is triggered by either the actions of particular human actors, e.g., "push a button", or by messages arriving from other players. All radios must have the knowledge of how to respond to particular types of events. All messages are expressed in the modeling language that all the radios can understand.

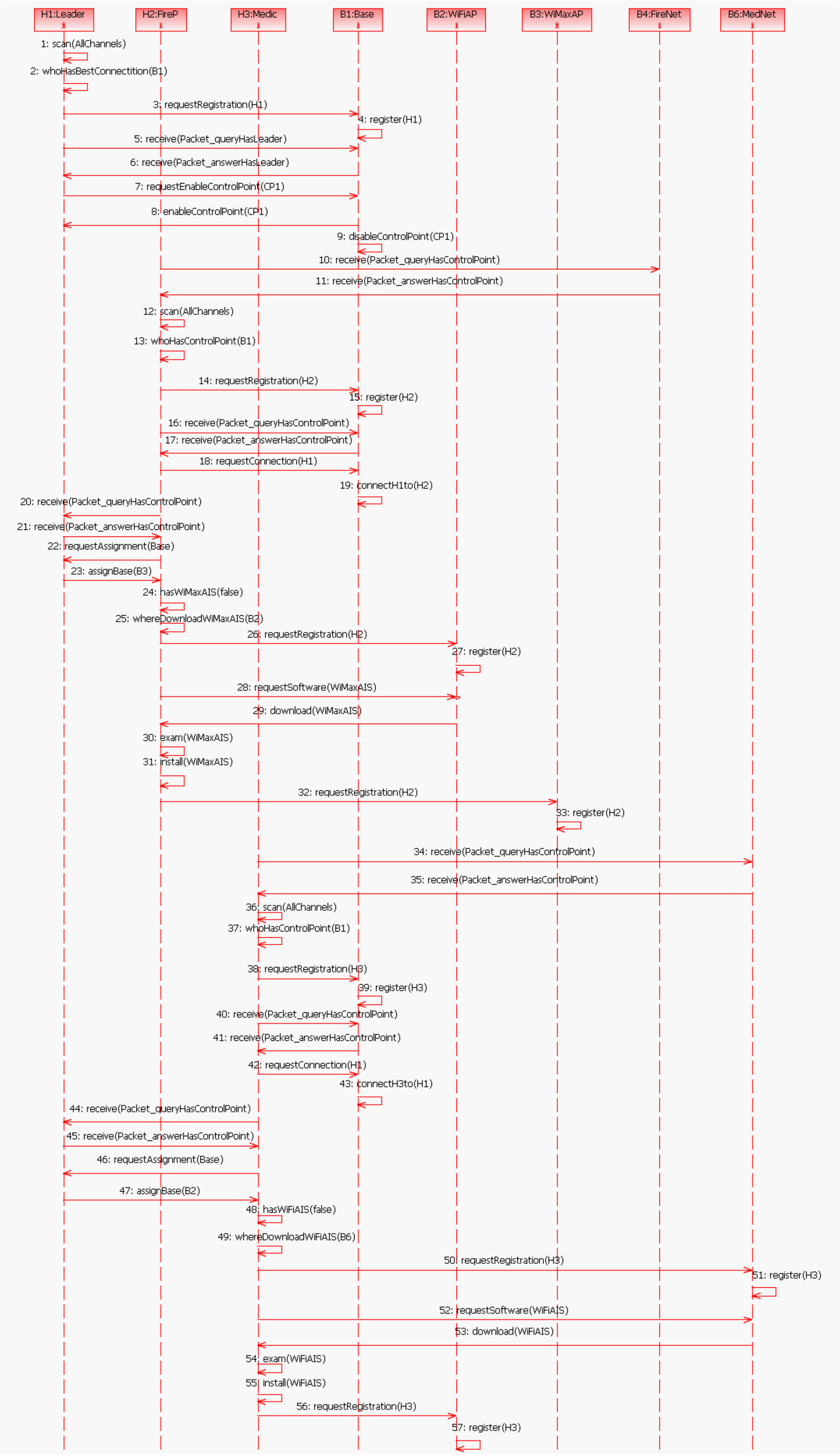
H1:Leader
H2:FireP
H3:Medic
B1:Base
B2:WiFiAP
B3:WiMaxAP
B4:FireNet
B6:MedNet
1: scan(AllChannels)
2: whoHasBestConnectition(B1)
3: requestRegistration(H1)
4: register(H1)
5: receive(Packet_queryHasLeader)
6: receive(Packet_answerHasLeader)
7: requestEnableControlPoint(CP1)
8: enableControlPoint(CP1)
9: disableControlPoint(CP1)
10: receive(Packet_queryHasControlPoint)
11: receive(Packet_answerHasControlPoint)
12: scan(AllChannels)
13: whoHasControlPoint(B1)
14: requestRegistration(H2)
15: register(H2)
16: receive(Packet_queryHasControlPoint)
17: receive(Packet_answerHasControlPoint)
18: requestConnection(H1)
19: connectH1to(H2)
20: receive(Packet_queryHasControlPoint)
21: receive(Packet_answerHasControlPoint)
22: requestAssignment(Base)
23: assignBase(B3)
24: hasWiMaxAIS(false)
25: whereDownloadWiMaxAIS(B2)
26: requestRegistration(H2)
27: register(H2)
28: requestSoftware(WiMaxAIS)
29: download(WiMaxAIS)
30: exam(WiMaxAIS)
31: install(WiMaxAIS)
32: requestRegistration(H2)
33: register(H2)
34: receive(Packet_queryHasControlPoint)
35: receive(Packet_answerHasControlPoint)
36: scan(AllChannels)
37: whoHasControlPoint(B1)
38: requestRegistration(H3)
39: register(H3)
40: receive(Packet_queryHasControlPoint)
41: receive(Packet_answerHasControlPoint)
42: requestConnection(H1)
43: connectH3to(H1)
44: receive(Packet_queryHasControlPoint)
45: receive(Packet_answerHasControlPoint)
46: requestAssignment(Base)
47: assignBase(B2)
48: hasWiFiAIS(false)
49: whereDownloadWiFiAIS(B6)
50: requestRegistration(H3)
51: register(H3)
52: requestSoftware(WiFiAIS)
53: download(WiFiAIS)
54: exam(WiFiAIS)
55: install(WiFiAIS)
56: requestRegistration(H3)
57: register(H3)

Figure 2-11. Sequence Diagram for the

3. Commercial Use Cases

Many cellular network operators, metropolitan areas and ISP's are deploying WiFi mesh networks. Many of them anticipate upgrading a portion or all of their networks to WiMax. In such a case we can consider a scenario using the same three AIS's as described in section 2.2.1 (1XRTT, 2.4 GHz WiFi, 5 GHz WiMax).

In this section we outline three use cases: Load Balancing use case, Software Download use case and Software Certification use case.

Instead of going through the whole of each of these scenarios, we will focus here on the differences between this Commercial Scenario and the Public Safety Scenarios described earlier in this document.

In each of these scenarios the Control Point is in the network operator's infrastructure. It may move around within that infrastructure, but it never moves out of it. The number and variety of hardware / software platforms in the field is much greater and therefore the complexity of matching the correct S/W download to the correct platform becomes more difficult, while the potential damage to the network of a mismatch becomes much higher.

In the network upgrade scenario the time constraint is greatly relaxed. In the load balancing scenario, the time constraint can be much greater.

Cost is an important issue in commercial systems. There are two cost components that tend to dominate in these scenarios. One is the cost associated with human intervention. When automated systems break down, network operators typically fall back on customer service personnel. This is costly and therefore to be avoided. The second is the impact of failure to meet QoS expectations on the consumers' part. Failure here can lead not only to directly lost customers, but also indirectly lost customers through degraded reputation.[1]

3.1. Load Balancing Use Case

3.1.1. Description of Use Case

In this scenario, a sporting event is being held at a stadium in an urban core. It is expected that one of the participants will be breaking a long held and honored record. 60,000 people are expected to be in the stadium. Another 10,000 are expected to congregate outside the stadium. There will be 1,000 public safety officials posted to the stadium and its immediate area to service these crowds. Of the 70,000 people in the crowd, 55,000 are expected to be carrying cell phones. 30% of the cell phones will likely have video camera capability. 20% of the phones will have Digital Multimedia Broadcasting (DMB - video receive service). 60% will have still cameras. 90% will have short message system (SMS). 30% will have Multimedia Message system (MMS). 25% will have full internet access

(10% with modest two way data bandwidth, 10% with medium speed to the handset and modest bandwidth to the base station, and 5% with medium bandwidth in both directions).

Additionally, there will likely be 40,000 WiFi, and 20,000 WiMax devices. Many of the WiFi and WiMax devices will have VOIP capability. Some portion of these WiFi and WiMax devices will be combination cell phones and some will be additional devices carried by people who also carry a cell phone. Some of the devices that have internet access are IPTV users. There are three network operators providing service in this area. The network operator we are focusing on has licenses in the DMB, Cellular, PCS and WiMax bands; WiFi hotspots (two bands) covering some or all of the stadium, depending on traffic load, population density and positioning of temporary structures in the stadium. The operator also has access through brokers to 700MHz spectrum which can be used under applicable regulatory policies. The network operator has roaming agreements, and some fractions of the people attending are expected to be subscribers to other providers and roaming on this network. In addition, there are WiFi access points in the area that are open to the public and not part of the network operator's hotspot service. Some of these access points may be operated by local businesses, others by metropolitan networks.

Some of the people attending will be both watching the live action and watching special video / etc, coverage via DMB or IPTV. At the time of the record breaking event, many of the attending people will call friends; send SMS's, MMS's, emails, still photos, video clips, etc. In addition to the wide array of device types outlined above, there will be a wide array of subscription types amongst the network's subscribers. Many subscriber devices will have capabilities that have not been activated because the subscriber has not subscribed to the subscription which uses them, they may be locked out, or they may need additional S/W downloads to be activated.

The network operator can make some assumptions about the number and types of subscribers, subscriptions, and devices that will be active in and around the stadium. Based on those assumptions, the network operator has developed a strategy of moving all video phones to WiMax, moving all still camera phones to WiFi, and moving all non video / non camera phones to cellular. Based on this strategy, the network operator can use information gathered from the devices as they arrive, using the MLM description and interface. As capacity becomes insufficient, the network operator starts reconfiguring devices to move them to AIS's that they would not normally be able to access, and starts bidding on 700 MHz spectrum.

Now we get to the period when capacity demand is peaking, driving a significant portion of the 700MHz brokered spectrum to be in use, and there is an explosion and fire in the immediate vicinity of the stadium. The 700MHz spectrum is claimed by first responders, the remaining brokered spectrum dramatically increases in cost and the network operator has to reconfigure the commercial network. MLM is used again to support network reconfiguration and to the extent necessary, triage.[9] Triage steps, will include restricting WiFi and WiMax bandwidth to effectively shut off VOIP.

In the timeline and sequence diagrams that follow, a simplified subset of the above scenario is used. The reader can use the full scenario to extrapolate to the full scenario with all of its

[9] Triage is the process of prioritizing users in a way allowing as many as possible to be serviced when resources are insufficient for all to be serviced the same time.

complexity in combinations and permutations of types of radios, types of users, types of information, etc. and large numbers.

3.1.2. Actors

The actors in this use case are:

H1 – Cellular (800-900 MHz) handset with WiFi, WiMax MMS, and Video Camera

H2 - Cellular (800-900 MHz) handset with WiFi, WiMax SMS, and Video Camera

H3 – Cellular700MHz handset with WiFi and SMS

H4 – Public Safety handset with Public Safety AIS and Alternate 700MHz Capability

B1 - Cellular Basestation (both 800-900 & 700MHz) Operated by Carrier A

B2 - WiFi Access Point Operated by Carrier A

B3 - WiMax Access Point Operated by Carrier A

B4 – Public Safety AIS Basestation with Alternate 700MHz Capability

I1 – Carrier A's Operation Infrastructure

The actors bare shown in the diagram in Figure 3-1. Note that H1, H2 and H3 are shown as Cellular Handset; H4 is shown as Public Safety Handset; B1 is shown as Cellular Base by Carrier A; B2 is shown as WiFiAP by Carrier A; B3 is shown as WiMaxAP by Carrier A; B4 is shown as Public Safety AIS Base.

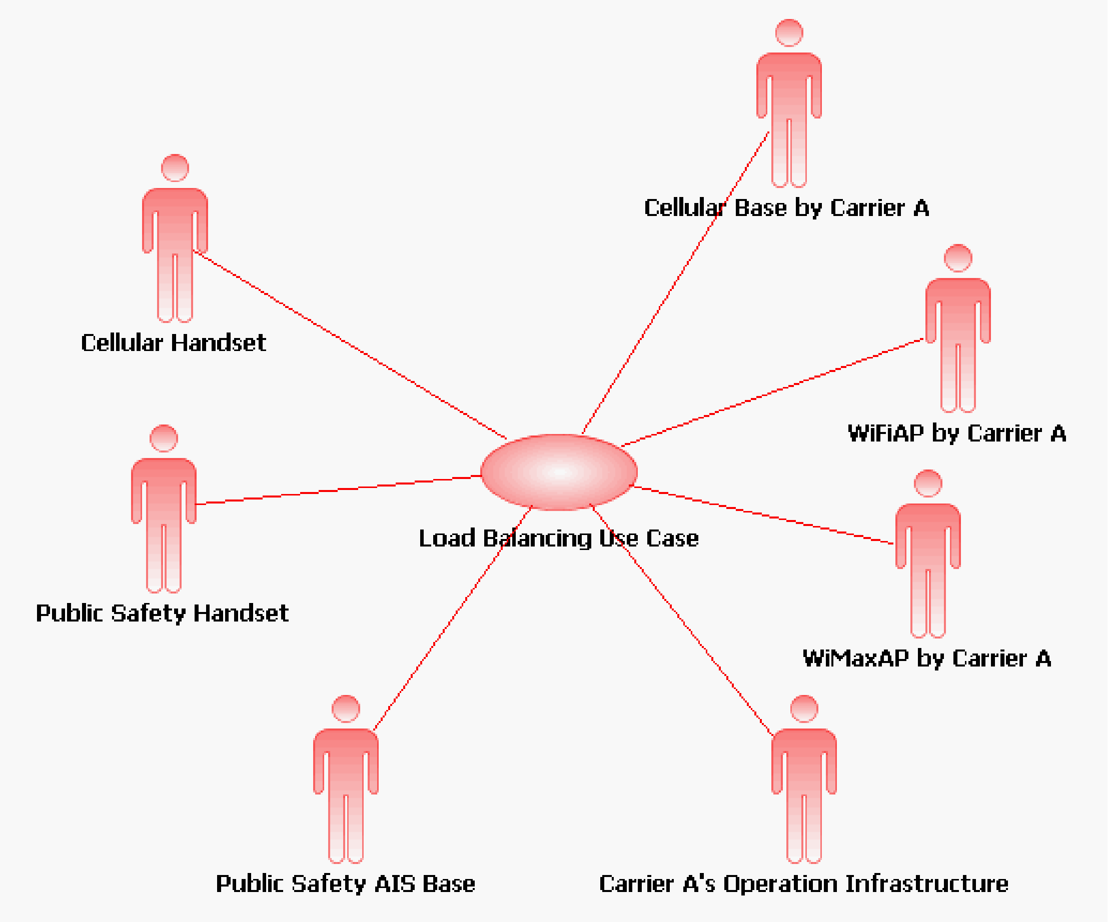

Figure 3-1. Use Case Diagram for the Load Balancing Use Case

3.1.3. Timeline

1. I1 becomes aware of the Situation likely to occur at the stadium

2. H1 arrives at the Stadium and is Handed-Over to B1

3. B1 assesses the Situation plus H1’s MLM description and instructs H1 to register with B3 and deregister with B1

4. H1 registers with B3 and deregisters with B1

5. H2 arrives at the Stadium and is Handed-Over to B1

6. B1 assesses the Situation plus H2’s MLM description and instructs H2 to register with B2 and deregister with B1

7. H1 registers with B2 and deregisters with B1

8. H3 arrives at the Stadium and is

Handed-Over to B1

9. B1 assesses the Situation plus H3's MLM description and issues no reconfiguration instructions

10. H4 arrives at the Stadium and is Handed-Over to B4 on the Public Safety AIS

11. B4 assesses the Situation plus H4's MLM description and issues no reconfiguration instructions

12. I1 receives Situation update informing it that a fire in the vicinity of the stadium has broken out

13. I1 assesses the new Situation and the MLM descriptions of all handsets connected to its networks in the stadium vicinity and concludes that it needs to release 700 MHz spectrum for public safety users

14. B1 instructs H3 to register with B2 and deregister with B1

15. H3 registers with B2 and deregisters with B1

16. B4 assesses the new Situation and the MLM descriptions of all handsets connected to its networks in the stadium vicinity and concludes that it needs to move handsets to 700 MHz spectrum

17. B4 instructs H4 to move to 700MHz

An outline of a sequence diagram for this use case is shown in Figure 3-2.

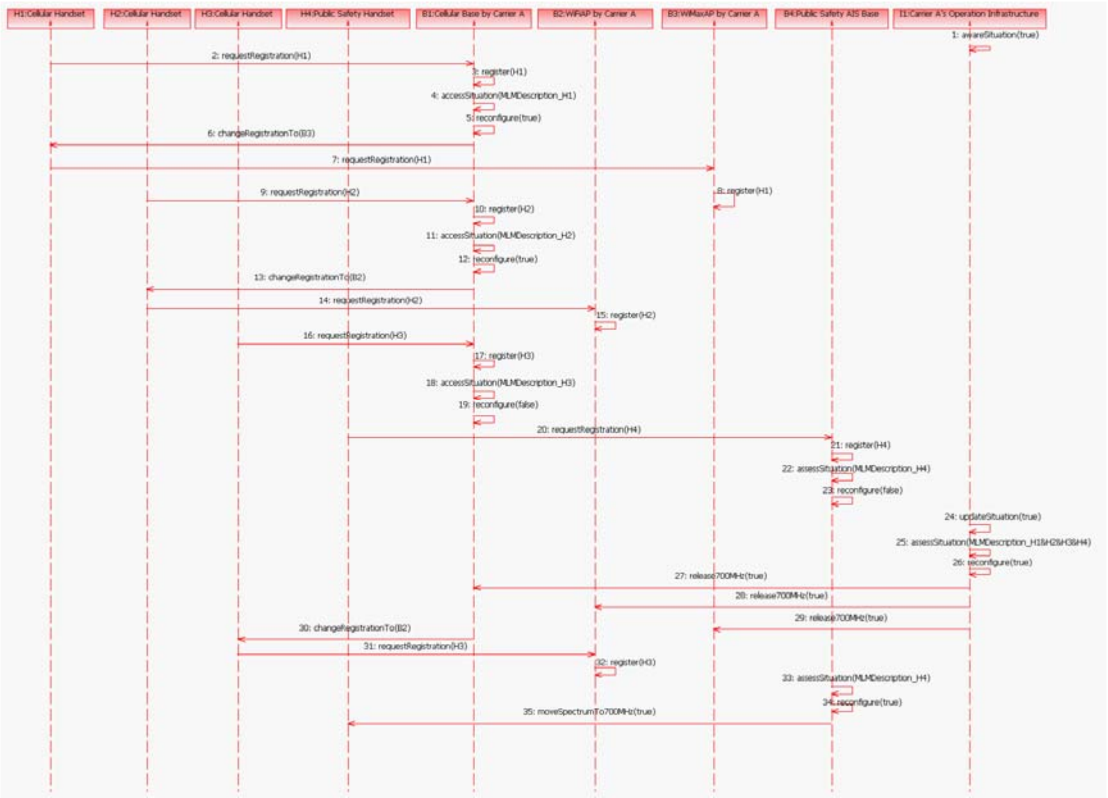
H1:Cellular Handset
H2:Cellular Handset
H3:Cellular Handset
H4:Public Safety Handset
B1:Cellular Base by Carrier A
B2:WiFiAP by Carrier A
B3:WiMaxAP by Carrier A
B4:Public Safety AIS Base
I1:Carrier A's Operation Infrastructure
1: awareSituation(true)
2: requestRegistration(H1)
3: register(H1)
4: accessSituation(MLMDescription_H1)
5: reconfigure(true)
6: changeRegistrationTo(B3)
7: requestRegistration(H1)
8: register(H1)
9: requestRegistration(H2)
10: register(H2)
11: accessSituation(MLMDescription_H2)
12: reconfigure(true)
13: changeRegistrationTo(B2)
14: requestRegistration(H2)
15: register(H2)
16: requestRegistration(H3)
17: register(H3)
18: accessSituation(MLMDescription_H3)
19: reconfigure(false)
20: requestRegistration(H4)
21: register(H4)
22: assessSituation(MLMDescription_H4)
23: reconfigure(false)
24: updateSituation(true)
25: assessSituation(MLMDescription_H1&H2&H3&H4)
26: reconfigure(true)
27: release700MHz(true)
28: release700MHz(true)
29: release700MHz(true)
30: changeRegistrationTo(B2)
31: requestRegistration(H3)
32: register(H3)
33: assessSituation(MLMDescription_H4)
34: reconfigure(true)
35: moveSpectrumTo700MHz(true)

Figure 3-2. Sequence Diagram for the Load Balancing Use Case

3.2. Software Download Use Case

3.2.1. Description of Use Case

In this scenario shown in Figure 3-3, a user requests a service from the handset (Service requests can come from the infrastructure or from the radio in response to environmental conditions. For simplicity these are not considered in this use case.). If the requested service is within the handset's currently configured capabilities, the service is initiated. If not, the MLM reasoner[10] searches its local Repository for software code modules (Software) that will allow satisfaction of the request. If such Software is found, the MLM reasoner installs it. If not, the MLM reasoner asks the infrastructure if it can provide the Software for the requested service. If yes, the Software is uploaded. The MLM reasoner then checks the Software to determine that the Software is from a Trusted Source (indicated by the appearance of a cryptographically protected certificate, then checks the Software's Message Authentication Code (MAC) to determine that the Software and its attached MLM description has not been changed in transit, and finally using the Software's MLM description and the radio's MLM description determines that there is a high probability that installing the Software on that particular radio will provide the desired result in both achieving desired functionality and avoiding undesired functionality. If all of these "tests" are satisfied, the Software is installed and the requested service is established. The actors involved in this use case are: User, the user's handset radio containing an MLM reasoner and a base station (Base). In this simplified case the Base fulfills all the functionality of a complete infrastructure.

[10] In earlier literature, the SDR Forum has called this function the MLM reasoner (see SDR Forum TR2.1 for the basic MLM reasoner architecture. *The internal structure of the MLM reasoner to support MLM was presented at the 2006 SDR Technical Conference, but it did not appear in the Proceedings In that presentation the role of the MLM Reasoner is shown.*). Current cognitive radio literature call it the MLM reasoner [ref fette], and it monitors functional requests and manages the air interface standard.

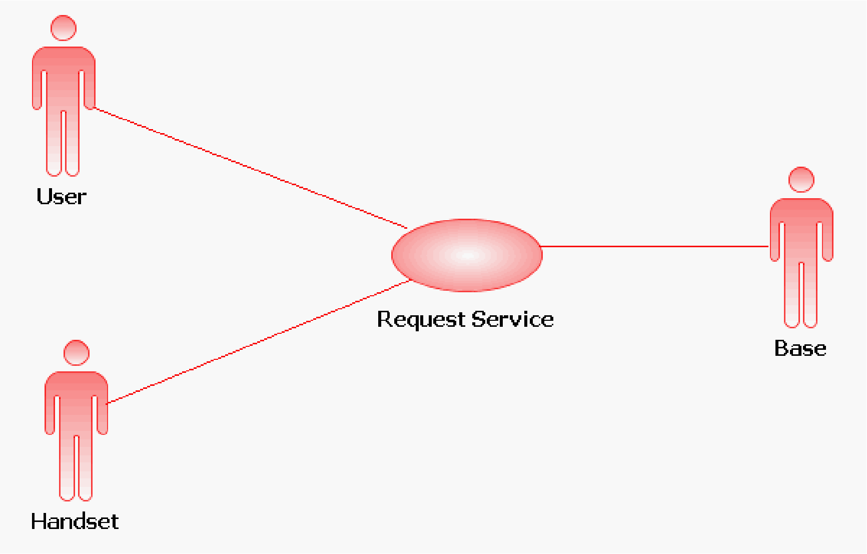

Figure 3-3. Software Download Use Case Example

3.2.2. Timeline

Figure 3-4 shows the sequence diagram for this use case:

1. User requests a particular type of service from the handset.
2. If the handset determines that the handset in its current configuration can deliver the requested service, it initiates the service.
3. Otherwise the handset checks local repository for Software that would allow this service.
4. If yes, then the handset is reconfigured and service initiated.
5. If no, then the handset communicates with the Base, to determine if it can provide the Software.
6. If no, then a negative reply is sent by the base to the handset, and the handset displays this to the user.
7. If yes, then the Software is uploaded
8. The received Software is “tested” by the handset for a valid trusted source certificate, a valid MAC and using the MLM definition of the Software and the MLM definition of the radio to assure a high probability of providing desired functionality and avoiding undesired functionality.
9. If any of these tests fail, the Software is not installed and the radio returns to step 5 above.
10. If yes the Software is installed and service established.

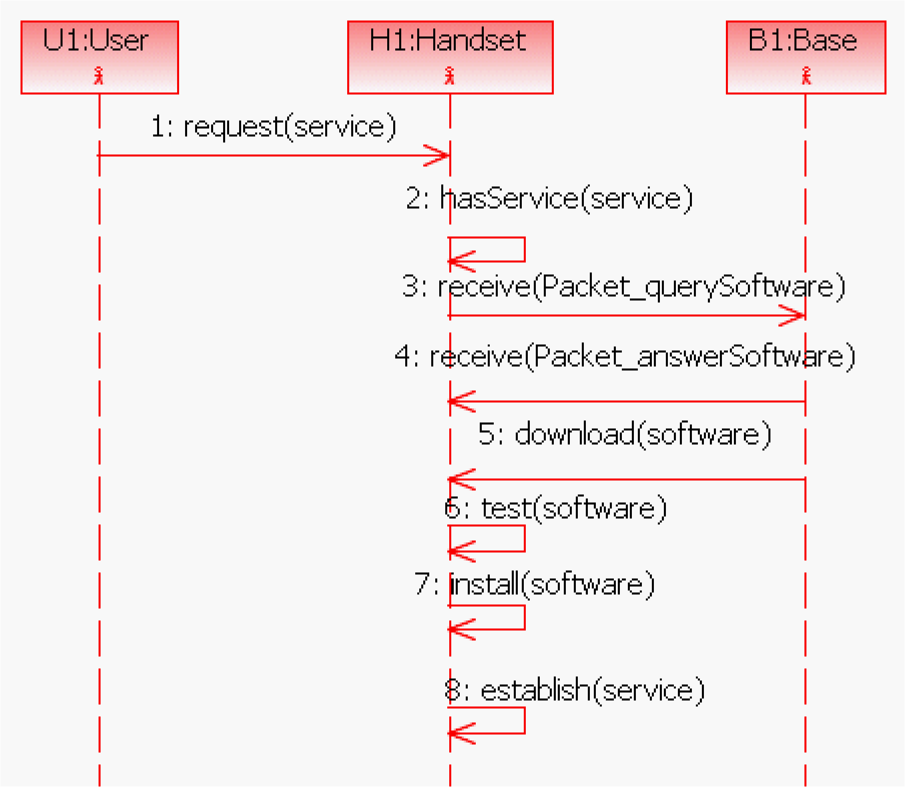

Figure 3-4. Sequence Diagram for Software Download Use Case

3.3. Software Certification Use Case

3.3.1. Description of Use Case

In this scenario, shown in Figure 3-5, a software vendor (SW Vendor) creates a new Software module and then presents its Software and its MLM description to an Approved Certification Lab. The Certification Lab checks whether the vendor is certified. If true, the Certification Lab tests the software to determine if the MLM description is accurate and adequate. The Certification Lab may install the module on a selected set of radios and/or simulate its operation on a selected set of MLM descriptions of radios. If the Lab finds that the SW Vendor's MLM description is accurate and adequate, it approves release of the Software with the approved MLM. The SW Vendor releases the Software with its attached MLM description all MAC protected.

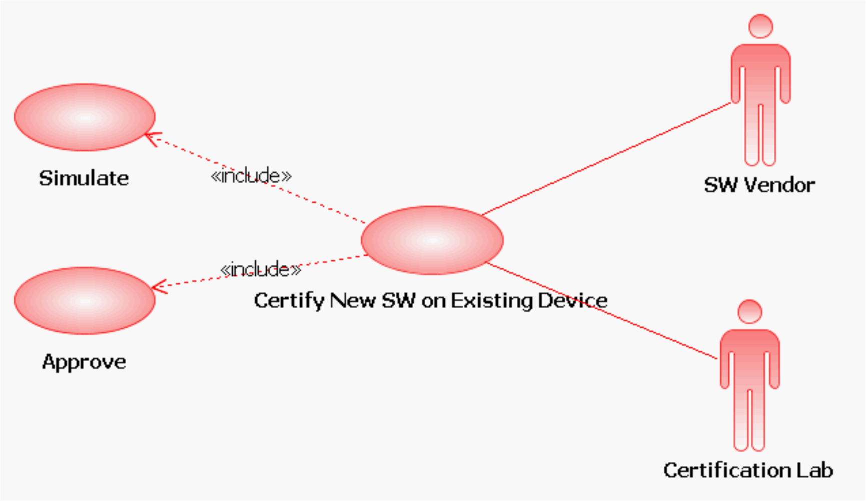

Figure 3-5. Software Certification Use Case Example

3.3.2. Timeline

Figure 3-6 shows the sequence diagram of this use case:

1. SW Vendor submits Software module with an accompanying MLM description to a conformance lab for testing.
2. Certification Lab checks whether Vendor is certified.
3. If true, then Certification Lab tests the software.
4. If test positive, then Certification Lab sends permission to release the software back to Vendor.
5. Vendor combines the software and MLM description of the permission and releases the software.

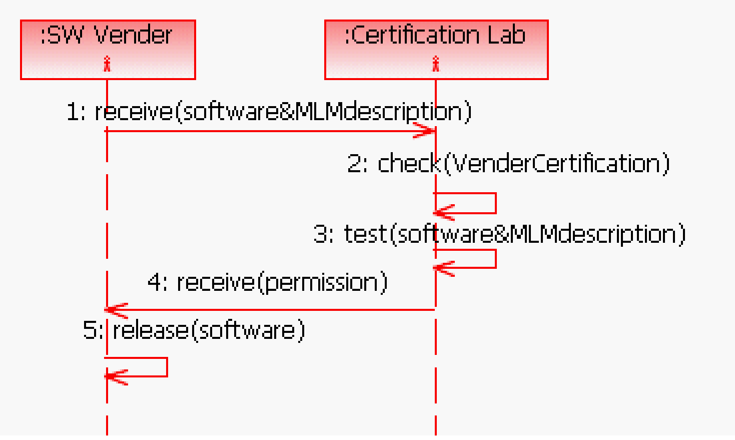
:SW Vender
:Certification Lab
1: receive(software&MLMdescription)
2: check(VenderCertification)
3: test(software&MLMdescription)
4: receive(permission)
5: release(software)

Figure 3-6. Sequence Diagram for the Software Certification Use Case

4. Summary and Next Steps

This document has described a series of scenarios that highlight the function and value of MLM. These scenarios were used as the basis for a series of Use Cases. These Use Cases informed a set of UML Sequence Diagrams. For one case (Network Extension Use Case), the messages in the Sequence Diagram were expressed as an Ontology developed for this particular Use Case. This Ontology is included as an example to show how an Ontology can be used to express other Use Cases.

This document will be circulated as widely as possible. This is likely to result in suggestions for modifications of the Use Cases and suggestions for additional Use Cases. This feedback is likely to result in revisions to this document.

At the same time, the MLM Working Group will start to develop a comprehensive Ontology that can be tested with the rest of the Use Cases in this document. Throughout this work the MLM Working Group will seek and incorporate, as appropriate, feedback from the largest possible community.

References:

[1] Mark Cummings; P.A. Subrahmanyam; “The Role Of A Metalanguage In The Context of Cognitive Radio Lifecycle Support”; SDR Technical Conference, Orlando, November 16, 2006.

[2] Public Safety Special Interest Group, “Use Cases for Cognitive Applications in Public Safety Communications Systems, Volume 1: Review of the 7 July Bombing of the London Underground”, Working Document SDRF-07-P-0019-V0.0.3, Version 1.0.0, pp., September 18, 2007.

[3] Mark Cummings; Todor Cooklev; Bryan Lyles; P. A, Subrahmanyam; "Commercial Wireless Metalanguage Scenario", SDR Technical Conference, Denver, Co. Nov. 2007.

[4] Mieczyslaw M. Kokar; Donald Hillman; Shujun Li; Bruce Fette; Preston Marshall; Mark Cummings, Todd Martin, John Strassner; “Towards a Unified Policy Languages for Future Communication Networks”, IEEE DySPAN Conference, Chicago, Oct. 2008.

[5] Bruce Fette; Mieczyslaw M. Kokar; Mark Cummings; "Next-Generation Design Issues in Communications", Portable Design Magazine, No.3, pages 20 - 24, 2008.