Handling Mobility Across WiFi and WiMAX

Anand Padmanabha Iyer
Cisco Systems, Inc.
170 W Tasman Drive
San Jose, CA 95134, USA
anapadma@cisco.com

Jayaraman Iyer
Cisco Systems, Inc.
170 W Tasman Drive
San Jose, CA 95134, USA
jiyer@cisco.com

ABSTRACT

Performance of wireless data networks can be improved by integrating heterogeneous networks. Hence, emerging wireless Internet networks consist of heterogeneous wireless networks working in synergy. WiFi and WiMAX are particularly interesting in their ability towards mobile data oriented networking, and a scheme that enables mobility across these two would provide several advantages to end-users, wireless operators as well as Wireless Internet Service Providers (WISPs). In this work, we propose a novel, cost-effective and end-user friendly mobility scheme. Our approach does not require additional client software to handle WiFi-WiMAX mobility, or hardware changes in any of the network entities involved. We demonstrate the feasibility of our solution by developing an actual prototype.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design

General Terms

Design, Management, Measurement

Keywords

WiMAX, WiFi, mobility

1. INTRODUCTION

Wireless access has seen exponential growth in the past few years due to the popularity and cost effectiveness of IEEE 802.11 standard [15]. WiMAX, also known as the IEEE 802.16 standard [5], has been emerging as a broadband wireless technology. Both these technologies have their respective strengths - 802.11 offers a higher throughput wireless network mostly on unlicensed spectrum, and 802.16 offers a larger wide area coverage network over a licensed spectrum.

IWCMC '09, June 21−24, 2009, Leipzig, Germany.

Recent trends indicate that future wireless Internet will consist of heterogeneous wireless networks working in synergy. Since overall spectrum is inherently limited, it helps to improve the overall performance of wireless data networks by complementing an unlicensed and licensed technology such as WiFi and WiMAX. This fact has already been exploited in building cost-effective WiFi mesh networks with WiMAX back-haul [12]. However, the question of mobility across both as two access networks still does not have concrete answers. A scheme that enables mobility across both these networks would provide several advantages to end-users as well as Wireless Service Providers.

1.1 Challenges

A mobility management scheme in a heterogeneous environment invites several challenges in the form of open questions. We examine a few these challenges below:

1.1.1 Differences in Wireless Standards

Wireless standards for different radio links tend to be a lot different, causing complexities of varying degrees. For example, network entry and network exit procedures are significantly different in 802.11 and 802.16. 802.11 networks use management frames to do client addition and hand-off, while 802.16 networks use initial network entry procedure. How does a mobility management scheme address effective hand-offs, especially when a user is roaming?

1.1.2 Definition of Mobility parameters

What are the important mobility parameters that needs to be defined? For instance, since authentication and hand-off techniques differ across networks, latency is one important issue. How does a mobility management scheme accommodate such parameters?

1.1.3 Client Complexities

Accommodating multiple radios which are completely heterogeneous, puts complexities at multiple layers. Apart from the multi-radio organization at the device layers, typically intelligent client software is required to allow roaming across different networks. Additional client intelligence will be required to offer application transparency. Each of the access networks may require a different authentication technique to be used, creating additional complexity and delays.

1.1.4 Network Architecture Challenges

Disparate networks such as WiFi and WiMAX may end up using entirely different architectures. This makes it a harder problem to accommodate roaming and hand-overs

with an assured latency. The two networks may use entirely different authentication schemes to authorize clients. In such situations, providing end-user transparent authentication is a key challenge, especially when the end user is mobile, and switches between networks.

1.2 Contributions

We propose an architectural approach to handling mobility across WiMAX and WiFi networks in a seamless fashion. We explore the space of authentication mobility which has not been focused previously by extending the *message mapping* technique, and find that it plays a key role in reducing hand-off latency in our mobility solution. Our approach tries to hide the client facing differences across WiFi and WiMAX at the network layer, and the resultant solution offers an elegant way to use an unlicensed technology such as WiFi to augment effective coverage to a WiMAX network.

1.3 Outline

The rest of the paper is organized as follows: We describe the motivation behind the problem in section 2. In section 3, we provide a brief overview of the two technologies. In this section, we also provide an overview of different frames in 802.11, with emphasis on management frames since they are of most interest to this work. Section 4 describes the architectural details of this work in detail. Implementation details are discussed in section 5. We analyze the effect of our scheme on mobility parameters and provide evaluation results in section 6. A brief summary of related work is presented in section 7. Finally, we conclude and discuss future work in section 8.

2. MOTIVATION

Consider a service scenario where a user, Bob, has a handheld device such as a PDA or a laptop with both 802.11 and 802.16 capabilities. Bob signs up with a provider that offers connectivity using 802.11 or 802.16. The provider offers Bob a connectivity option package, *"Any access, Always connected"*. Bob, being a business person, is on constant move, and expects a seamless experience to all the services including voice.

The provider wants to facilitate a seamless roaming experience across WiFi and WiMAX. Many of the indoor areas is covered using 802.11, and outdoor with 802.16, and a seamless experience can exploit this to facilitate a lower cost radio network.

Three questions need to be answered here: (i) How does the 802.11 network interact with WiMAX provider's 802.16 network? Is there a cost-effective model that facilitates a partner WiFi access point to be connected to the WiMAX provider's network? (ii) How is mobility handled across 802.11 and 802.16, and latency kept to a minimum (iii) How can two sets of credentials, one for WiFi and one for WiMAX, be avoided?

To deliver a seamless experience for moving between the 802.11 and 802.16 networks, all the three questions need to be addressed.

3. OVERVIEW

We now present an overview of both standards, stressing on control plane messages in each. Common in both standards, control plane messages are used to establish and tear down connections between different entities in a network.

3.1 IEEE 802.11

The IEEE 802.11 standard defines various frame types for communication between wireless devices. Management frames enables stations to establish and maintain connections. The standards define a number of management frames.

An access point (AP) periodically sends information about its presence through a `Beacon`. A `Probe Request` is used to obtain information from a station, usually an AP. This request is acknowledged by a `Probe Response`. `Authentication Frame`s are used by the AP to accept or reject radio NICs. An authenticated session is terminated using a `Deauthentication Frame`. An `Association Request` enables an AP to allocate resources to a client, and to synchronize with it, whose success is indicated by an `Association Response`. In case a client associated with a particular AP roams away from it, or it finds another AP with stronger beacon, it will send a `Re-Association Request` frame to the new AP. The outcome of this is indicated by `Re-association Response`. Finally, an association is terminated using a `Disassociation Frame`.

3.2 IEEE 802.16/WiMAX Network Architecture

The network architecture beyond the MAC/PHY for WiMAX is defined by the Network Working Group (NWG) [23]. As per this architecture, mobility in the WiMAX access network is handled by an Access Service Network Gateway (ASNGW). An ASNGW typically resides at the operators premise, connecting and servicing multiple WiMAX Base Stations (BS). A WiMAX network architecture is logically represented by Network Reference Model (NRM), which identifies key functional entities and reference points over which a network interoperability framework is defined. The interaction between entities is through reference points. In particular, the interaction between ASNGW and BS is through reference point R6. The reader is referred to IEEE 802.16e specification [5] for further details and [18] for an exhaustive description of these reference point messages. The following are the important R6 messages that we utilize in this work:

`MS Pre-attachment Request` is used by the BS to indicate the ASNGW about arrival of a new Mobile Station (MS). A `MS Pre-attachment Response` is used to communicate the authentication policy, and this is acknowledged by a `MS Pre-attachment Acknowledgment`. An `EAP Transfer` consists of a series of messages used to transfer the authentication procedure messages. On successful completion of EAP authentication procedure, the ASNGW sends a `Key Change Directive`. This directive is acknowledged by a `Key Change Acknowledgment`. A `MS Attachment Request` is initiated by the BS which contains the MS registration context. The completion of MS attachment with the ASNGW is indicated by `MS Attachment Response`. The `MS Attachment Ack` serves as an acknowledgment to the ASNGW indicating the completion of MS attachment, and hence trigger service flow creations.

4. PROPOSED ARCHITECTURE

We propose an architecture with a common `WiFi/WiMAX mobility service agent` for use across WiFi and WiMAX access. In a WiMAX network, an Access Service Network (ASN) gateway is a network element that provides mobility in conjunction with multiple WiMAX base stations. By incorporating a correct mapping mechanism between WiFi

and WiMAX, a WiFi Access Point can also interface to the WiMAX ASNGW. This enables a `WiFi/WiMAX mobility service agent` to be easily created using a ASN Gateway. Thus, in our architecture, the problem of handling mobility across WiFi and WiMAX boils down to the problem of handling mobility across WiMAX base stations which already has concrete solutions. This specific design choice yields several advantages towards handling a low latency mobility scheme.

4.1 WiFi-WiMAX Mapping Function

Essentially, our mobility scheme proposes the use of a WiFi Access Point (AP) as a WiMAX base station. In particular, our solution consists of a WiFi AP with an appropriate mapper function for handling mobility across WiFi and WiMAX. The purpose of the mapper function is to map events between 802.11 and R6 events, thus allowing the device to appear as a normal AP to the client, and a normal WiMAX base station to the ASN gateway. An added advantage to this approach is that the client and the ASN gateway are completely oblivious to the mapping taking place in the AP. Hence, we can avoid any hardware or software changes at these entities.

As indicated earlier, the ASN gateway provides mobility support in WiMAX networks by servicing multiple base stations. We further extended this concept of an anchored mobility service based on SSID membership, allowing flexibility to enable or disable WiFi/WiMAX mobility based on configuration. Additionally, it also provides the capability for a single AP to interface to multiple mobility service agents.

4.2 Connection Establishment

As described in section 3, both WiMAX and WiFi uses special messaging to set up and tear down connections. We propose the use of an event-based model. Specifically, we establish relationships between the various events in WiFi and WiMAX. For instance, a WiMAX connection establishment is initiated using a `pre-attachment request` as described in reference point R6 [5]. A WiFi client initiates it's attachment process with an AP using `association request`. Hence, we can directly map a WiFi `association request` to a WiMAX `pre-attachment request`. Similarly, we map various events that happen upon connection establishment in WiFi and WiMAX. A complete overview of various mappings used in our scheme is given in Table I.

Figure 1 describes the various events that occur during the connection establishment phase. The connection establishment ends when an `association response` is received at the client.

4.3 Handling Authentication Across Heterogeneous Networks

One of the major advantages of our proposal is that it can handle authentication across heterogeneous networks. To our knowledge, none of the earlier work support authentication mobility.

We apply the same event-based approach in this case too by mapping different events in 802.1x authentication in 802.11 with those in 802.16. Since both the networks use the same authentication server, our scheme is able to support authentication mobility which helps us avoid complete authentication while roaming between these networks and help reduce latency.

4.4 Handling IP Addresses

How should IP addresses be assigned to a multi-mode client? Of course, the easiest solution is to assign separate IP address to each interface. However, this solution requires IP address assignment handling when the client switches from one access interface to the other, and adds latency. The proposed architecture enables the same IP address to be used across both the WiFi and the WiMAX network interfaces, and keeps it seamless from an application perspective.

4.5 Data Flow

Once a station is attached to the network, data plane is set up by assigning an IP address. The IP address assignment in our scheme is taken care by the `WiFi-WiMAX mobility service agent`. This IP address could be obtained from an external DHCP server, or from a DHCP server internal to the service agent. Since the service agent acts as an anchor, this assignment helps in obtaining the same address when the client connects through either interface.

The AP merely acts as a relay for the DHCP messages exchanged between the client and the DHCP server, starting with the request made by the client.

The WiMAX R6 data plane utilizes *Generic Routing Encapsulation* (GRE) to route packets. Thus, in addition to the mapper function, it is also necessary for the AP to be able to encode and decode GRE packets.

5. IMPLEMENTATION

To evaluate the viability of our proposal, we implemented a prototype of the model. In this section, we describe our implementation details.

5.1 Hardware Setup

Our prototype used Cisco's 7300 series router loaded with Cisco's Access Service Network Gateway (ASNGW) software as the WiFi-WiMAX gateway. Cisco's Aironet 1240 Access Point running Cisco IOS serves as our AP. Our proposed modifications are incorporated into the AP's image.

5.2 The WiFi-WiMAX Event Mapper

The WiFi-WiMAX event mapper forms the core of our implementation. This service runs as a daemon/service inside our AP which gets activated upon boot up. Essentially, it acts as a middle man, triggering appropriate WiMAX R6 events using WiFi triggers and vice-versa as described in the earlier sections.

For control plane modifications, since reference point R6 uses UDP packets over a default port (port 5000 in our implementation), the mapper incorporates logic to understand reference point R6 events, and also WiFi events. For this purpose, it implements a number of state machines which simulate the WiMAX behavior for every WiFi client connecting to the AP. These state machines are similar to the 802.11 state machines. We then incorporated the state relation between WiFi and WiMAX into these state machines. Hence, every client connecting to the AP is virtually converted as a WiMAX client for the WiFi-WiMAX gateway by the mapper.

For the data plane, WiMAX stipulates the use of IP packets encapsulated in GRE tunnels. Since the version of IOS running in our AP natively supports GRE tunnel, we did not require any additional modifications to the image.

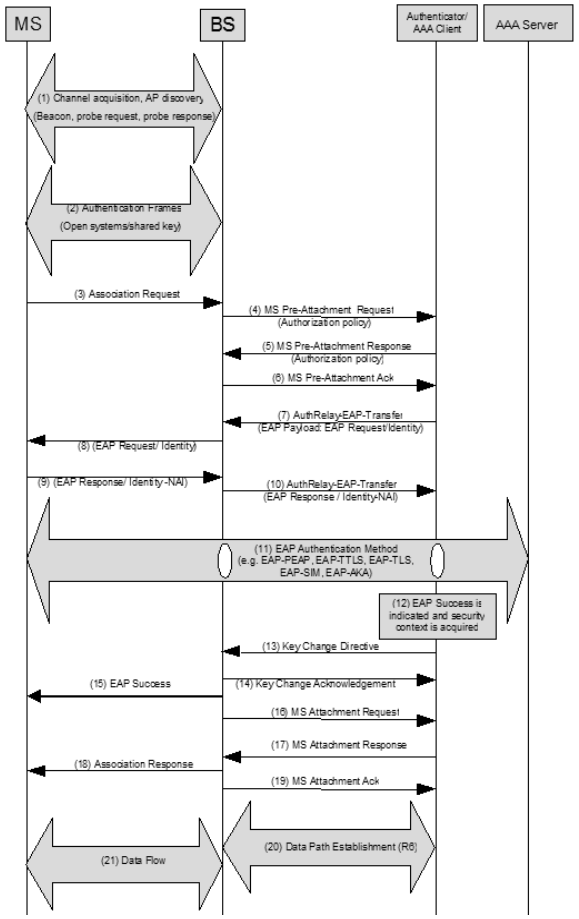

Figure 1: Mappings between WiFi and WiMAX events for Initial Network Entry.

Table 1: Typical latency for different events as measured in our experiments and by recent works.

Event	Latency
Discovery and connection	200-300 ms
Authentication (EAP TLS)	1.82 seconds
Reauthentication (EAP TLS)	few ms
DHCP (initial)	2 sec
DHCP (subsequent)	few ms, depends on adapter

6. EVALUATION

In this section, we analyze how our scheme affects mobility parameters. Since any mobility scheme would effectively result in disruption in connection at least for a short period of time during hand-off, latency is an extremely important parameter that needs to be addressed. This issue gains particular importance when networks are expected to support voice and video applications which demand extremely low latency. Typically, a wireless hand-off procedure comprises of 3 major events - *discovery*, *connection* and *data plane setup*. First, the mobile node must scan and discover potential networks to connect to. Once this has been done, it now has to connect to the selected network. The final step is to set up the data plane by obtaining an IP address through DHCP. That is, let T be the total delay during hand-off,

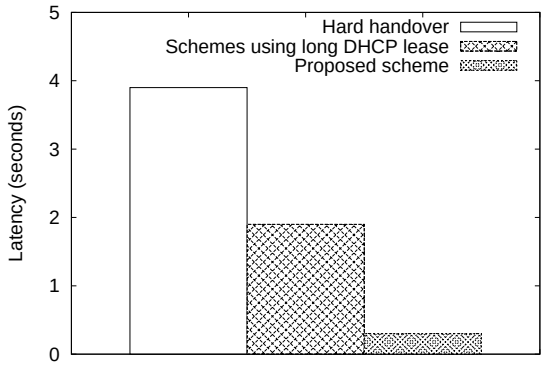

Figure 2: Comparison of hand-over latency for different schemes.

then

$$T = t_{discover} + t_{connect} + t_{dhcp}$$

During the connection phase, the mobile node is required to (re)associate and authenticate. Thus:

$$t_{connect} = t_{associate} + t_{authenticate}$$

Typical authentication in enterprise WiFi networks are done using 802.1x with Extensible Authentication Protocol (EAP).

Every event during the handover process accounts for significant delays. We performed a few experiments to estimate the delays during each of these phases, and our findings are given in Table II. It can be seen that authentication and DHCP events account for a major chunk. Lot of research has gone into optimizing each of these delays. For instance, the DHCP delay can be optimized by increasing lease times. Similarly authentication delays could be reduced significantly by using cached keys. However, none of these techniques work in heterogeneous network hand overs. Thus, a typical hand-over from WiFi to WiMAX would result in a latency of about 4 seconds which completely deters the purpose of a mobility solution (this huge delay is the result of two major components - DHCP delay and authentication delay). On the other hand, our mobility scheme achieves significant improvements over this hand-over delay because it saves on DHCP and authentication delays. This is possible because DHCP and authentication are central to our scheme. Further improvements are possible by the reuse of same session keys. Typical reduction in our scheme is in the range of 3.5 seconds compared to a solution that requires both DHCP and authentication to be done afresh and 1.5 seconds compared to solutions that take advantage of long DHCP leases. This is depicted in Figure 2.

7. RELATED WORK

Macro and micro mobility in all-IP networks have gained attention as a topic of importance in the past [4, 16, 8] with the emergence and popularity of heterogeneous wireless networks. Since WiMAX is a recent technology, macro and micro mobility in hybrid networks involving WiMAX has not been explored to a great extend.

Proxy Mobile IP (PMIP) [10] and Hierarchical Mobile-IP (HMIP) [9] are two schemes proposed to address local mobility management in all IP networks. We wish to note how

our scheme differs from these schemes: First, both PMIP and HMIP require the use of an additional network entity for mapping purpose. Second, PMIP and HMIP are layer 3 solutions where our architecture can be deployed at layer 2, layer 3 or a combination of layer 2 and layer 3. Third, both PMIP and HMIP study the problem in isolation without much focus to authentication considerations. Thus, neither PMIP nor HMIP offers a solution to the authentication problem across heterogeneous networks. Additionally, these schemes introduce additional signaling overhead which may not be insignificant.

[7] proposes an architectural solution for hand over between 802.11 and 802.16 networks. However, this solution requires the use of new network entities WiFi Gateway and extended-ASN Gateway. Again, this solution does not address authentication.

Multi-technology devices have been proposed in the past [3]. However, our work differs from them in the sense that we leverage the synergy between technologies to efficiently address hand-over issues in heterogeneous wireless networks.

A decent amount of work has been done in the area of mobility management in heterogeneous wireless networks. [2] is a qualitative comparison of different mobility management schemes. The authors also propose a new architecture for mobility management. [13] addresses major issues in mobility support for IP-based networks. [6] discusses the challenges associated with mobility management in hybrid wireless networks. Although this work analyzes many facets of mobility management, special stress has been given to hand-off management which, according to the authors, is one of the most challenging issues in mobility management. Many hand-off systems have also been proposed for use in hybrid wireless networks [11, 14].

Finally, security issues and authentication in IEEE 802.16 networks have been investigated recently [1, 17].

8. CONCLUSION

A mobility scheme allowing seamless hand over across WiFi and WiMAX promises convenient broadband access solution by providing several advantages to both end-users and operators. In this work, we propose a solution in this direction, and develop a prototype implementation. Our proposal is simple to deploy, and has immediate business value as indicated in section 2. Experimental measurements indicate that the scheme can shave off significant amount of time in hand over by smartly reducing the authentication latency. It also takes a first step in addressing seamless authentication across heterogeneous wireless access. Research in this direction, we believe, would also prove beneficial in a broader perspective since it will also address some of the issues in end-user transparent authentication.

We envision several areas for future work. First, we wish to extend our model as a platform to handle mobility across heterogeneous networks in a broader perspective. Second, we would like to evaluate the performance of our scheme with latency dependent applications such as voice and video.

9. REFERENCES

[1] A. Adibi, B. Lin, P.-H. Ho, G. Agnew, and S. Erfani. Authentication authorization and accounting (aaa) schemes in wimax. *Electro/information Technology, 2006 IEEE International Conference on*, pages 210–215, 7-10 May 2006.

[2] I. Akyildiz, J. Xie, and S. Mohanty. A survey of mobility management in next-generation all-ip-based wireless systems. *Wireless Communications, IEEE [see also IEEE Personal Communications]*, 11(4):16–28, Aug. 2004.

[3] P. Bahl, A. Adya, J. Padhye, and A. Walman. Reconsidering wireless systems with multiple radios. *SIGCOMM Comput. Commun. Rev.*, 34(5):39–46, 2004.

[4] A. T. Campbell and J. Gomez-Castellanos. Ip micro-mobility protocols. *SIGMOBILE Mob. Comput. Commun. Rev.*, 4(4):45–53, 2000.

[5] C. Eklund, R. Marks, K. Stanwood, and S. Wang. Ieee standard 802.16: a technical overview of the wirelessmantm air interface for broadband wireless access. *Communications Magazine, IEEE*, 40(6):98–107, Jun 2002.

[6] F. Siddiqui, S. Zeadally. Mobility management across hybrid wireless networks: Trends and challenges. *Computer Communications*, 29(9):1363–1385, May 2006.

[7] R. Fracchia. Architecture for Handover between 802.11 and 802.16. *Motorola White Paper*, 2007.

[8] C. Guo, Z. Guo, Q. Zhang, and W. Zhu. A seamless and proactive end-to-end mobility solution for roaming across heterogeneous wireless networks. *Selected Areas in Communications, IEEE Journal on*, 22(5):834–848, June 2004.

[9] IETF. Hierarchical Mobile IP. *RFC*, 2005.

[10] IETF. Proxy Mobile IP. *RFC*, 2008.

[11] R. Inayat, R. Aibara, and K. Nishimura. A seamless handoff for dual-interfaced mobile devices in hybrid wireless access networks. *Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on*, 1:373–378 Vol.1, 2004.

[12] Intel Corporation. Understanding Wi-Fi and WiMAX as Metro-Access Solutions. *White paper*.

[13] J. Li and H.-H. Chen. Mobility support for IP-Based networks. *Communications Magazine, IEEE*, 43(10):127–132, Oct. 2005.

[14] J. Nie, J. Wen, Q. Dong, and Z. Zhou. A seamless handoff in ieee 802.16a and ieee 802.11n hybrid networks. *Communications, Circuits and Systems, 2005. Proceedings. 2005 International Conference on*, 1:383–387 Vol. 1, 27-30 May 2005.

[15] L. M. S. C. of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Standard 802.11*, 1999.

[16] C. E. Perkins. IP Mobility Support. *RFC 2002*.

[17] H.-M. Sun, Y.-H. Lin, S.-M. Chen, and Y.-C. Shen. Secure and fast handover scheme based on pre-authentication method for 802.16/wimax infrastructure networks. *TENCON 2007 - 2007 IEEE Region 10 Conference*, pages 1–4, Oct. 30 2007-Nov. 2 2007.

[18] WiMAX Forum. WiMAX Forum Network Architecture - Stage 3: Detailed Protocols and Procedures.