ENTERPRISE WIMAX
Building the Next Generation Enterprise Wireless Infrastructure with WiMAX

Kai X. Miao
Intel Labs China, Building A, Raycom Info Park, Beijing 100190, Beijing, Republic of China

Keywords: Enterprise WiMAX, WiFi, Authentication, EAP-TTLS, EAP-TLS, Mobile Virtual Network Operator, Mobile Enterprise Network Operator, MVNO, MENO, Handoff, Cloud, Network as a Service, NaaS.

Abstract: As an all-IP broadband wireless technology, WiMAX uniquely integrates well with existing enterprise network infrastructure, which allows an enterprise to either directly host a WiMAX network or, alternatively, use a public WiMAX network hosted by a network service provider for its enterprise services. In this paper, we will discuss these two different network hosting models for the enterprise. In particular, we will discuss 1) what the WiMAX network architecture should look like; 2) how can the security models of WiMAX be made stronger to serve the needs of enterprise users; 3) how WiMAX and WiFi can work together seamlessly to give the user a unified experience. The content in this paper is based on our recent research in this area.

1 INTRODUCTION

Although WiMAX was created almost exclusively with the consumer market in mind, it resembles WiFi in being designed as an all-IP wireless technology and for running IP applications and services, which makes WiMAX a potential candidate for enterprise usages. Recently, there has been a growing amount of interest in using WiMAX in different enterprise markets, with the goal to improve enterprise wireless coverage and roaming capabilities. There are on-going efforts in the industry on specific enterprise WiMAX usages in different markets, extending WiMAX for enterprise usage, and trial deployments to validate and demonstrate enterprise usages of WiMAX.

It is important to realize, when considering using WiMAX for the enterprise, the complementary nature between WiFi and WiMAX in some key aspects. While WiFi has a short coverage range of about 100 meters, WiMAX offers a significantly greater coverage in a range of 500 meters and beyond; while WiFi offers high raw data bandwidth with poor traffic control capabilities, WiMAX is capable of highly sophisticated traffic management and control. With the greater coverage, strong QoS capabilities, and superior mobility support natively built it, WiMAX is providing to us a potential for transforming enterprise wireless infrastructure not only in an office environment, but also in different market vertical environments such as a university campus, railways, oil fields, city roads and highways, etc.

Unlike WiFi, however, WiMAX largely works in *licensed* frequency bands, which, while making a WiMAX network more managed for ensuring better service performance, complicates how a WiMAX network can be hosted in an enterprise environment and how a WiMAX network should be actually deployed in any real situation. In other words, for WiMAX usages in an enterprise, both business model and network architecture can be very different from those of WiFi. IT can no longer easily own the network, as it does in the case of a network WiFi, and the involvement of a wireless service provider or government who owns the frequency spectrum is a critical part of a WiMAX network solution. This single fact makes the WiMAX usage by an enterprise significantly more complicated in terms of business model, network deployment, security model, roaming, and architecture considerations. Apparently, to fully resolve and clarify the issues surrounding the business model and network hosting architecture requires an industry level effort involving service providers, enterprise leaders, standard bodies, and government. In addition, as different countries may have different policies concerning spectrum allocation and ownership,

X. Miao K. (2010).
ENTERPRISE WIMAX - Building the Next Generation Enterprise Wireless Infrastructure with WiMAX.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 31-35
DOI: 10.5220/0002980400310035
Copyright © SciTePress

WiMAX usages may also differ from country to country.

In the following, we divide our discussion around two different architectural models, enterprise hosted vs. provider hosted enterprise. In the enterprise hosted WiMAX model, our primary goal is to develop a unified network architecture for WiFi and WiMAX. In the provider hosted WiMAX for the enterprise, our goal is to derive a network architecture that meets the requirement of an enterprise in terms of security and manageability.

2 UNIFYING WIMAX AND WIFI NETWORKS IN ENTERPRISE

In many enterprise environments, we need to consider WiFi and WiMAX as a whole, i.e. treating them as complementary and leveraging the strengths associated with each in the overall enterprise environment. In a university campus environment, e.g. WiFi can be used for supporting indoor high speed data applications and WiMAX can be used for outdoor coverage. As another example, in railway application scenarios, WiFi can be used inside a train for passengers to access various services and WiMAX on the other hand can be used for wireless connectivity between a train and the ground. In particular, WiMAX is well suited for voice and video applications indoor or outdoor, due to its strong QoS capabilities, to serve the critical needs in almost every vertical market for full multimedia communications and collaborations.

Figure 1 below shows an integrated WiFi and WiMAX network, consisting of typical network components in WiFi and WiMAX for client network access, client authentication, and client roaming.

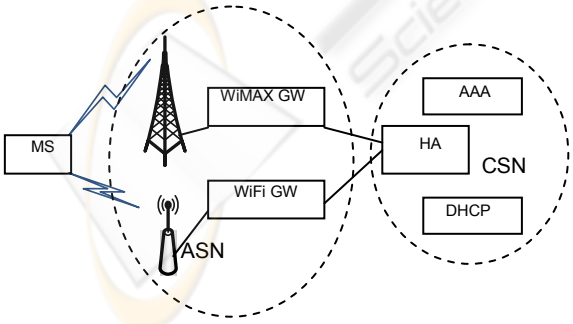

Figure 1: Integrated WiFi and WiMAX Network.

The integration of WiFi and WiMAX happens in both the access network layer and the core service network layer. In the core service network, common network servers (AAA, DHCP, and HA) are used for both WiFi and WiMAX. An AAA server is responsible for authenticating and authorizing the network access of a client, a Home Agent (HA) serves a user client when it roams from WiFi to WiMAX or vice versa, and a DHCP server works to provide IP addresses to a client device at the beginning of a network access or in a (Simple IP) handoff operation from one network to another. In the access network, we have defined two entities called WiFi Gateway and WiMAX Gateway, with their internal composition and subcomponents shown in Figure 2.

Note, a WiFi gateway (or a WiMAX gateway) defined in this paper is only a logical network entity, with a set of standard subcomponents in the industry. In addition, a WiFi gateway and a WiMAX gateway consist of almost exactly the same types of subcomponents except for their wireless network specific components, i.e. WiFi AC and WiMAX ASN, forming a logically unified layer for netowrk access.

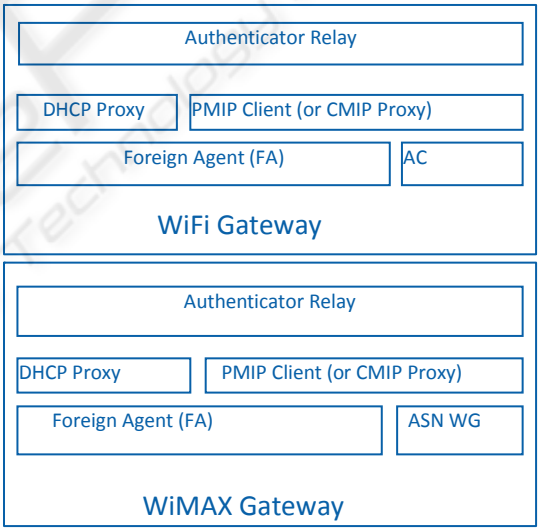

Figure 2: Composition of WiFi and WiMAX Gateways.

The subcomponents in a WiFi gateway or WiMAX gateway have been chosen to meet security and roaming requirements in an enterprise environment and the function of each subcomponent serves to provide a specific capability following its functionl definition in the industry.

Apparently, a number of issues deserve detailed attention under the unified WiFi and WiMAX architecture. More specifically, the certificates used in network and client authentication should be the same for both WiFi and WiMAX; the security model for WiMAX should be adequate for the enterprise,

i.e. providing enterprise level security. In our investigation, we developed two different authentication models for WiMAX in consideration of enterprise security requirements. In the first model, we adopted a modified version of EAP-TTLS defined in the WiMAX standard, in which enterprise certificates are used instead of certificates issued by VeriSign. In the second model, we introduced an additional layer of authentication for the enterprise on top of the WiMAX authentication which can be seen as the basic authentication layer. We will discuss these two authentication modles in more details later in this paper. Another important topic in this architecture is WiFi/WiMAX handoff for application mobility, which can be done via the HA and FAs in this architecture and a handoff engine inside the client. Due to space limitation in this paper, we are not able to provide detailed discussion on this topic.

3 PROVIDER HOSTED WIMAX

A provider-hosted mobile infrastructure for the enterprise may offer several key advantages in comparison to a mobile infrastructure hosted by an enterprise itself. First of all, an enterprise may benefit in network (equipment and maintenance) cost from a provider-hosted mobile enterprise infrastructure due to economies of scale. In this age of Cloud Computing today, provider-hosted wireless connectivity for the enterprise, which we may call Network as a Service or NaaS, seems quite straightforward to understand. After all, a Wireless Network Cloud is a resource that can be shared by multiple types of users just like a Compute Cloud. A public network is in fact a shared resource by different users (i.e. "multi-tenant") by definition, but *how a public network should be shared* by different enterprises has never been studied, which is the focus of our discussion here. In NaaS, a WiMAX network owned by a network provider would be shared by enterprise users (and consumers) for accessing services that belong to different enterprises (and other service providers). Therefore, the same value that drives Cloud Computing should also drive what we are proposing here as NaaS. The second potential advantage of a provider-hosted mobile architecture for the enterprise is *architecture unification*, which means an enterprise would no longer need to have isolated islands of on-campus mobile access networks geographically distributed on one hand and provider hosted access on the other, but a unified architecture on and off all campuses around the globe implemented over providers' networks. Apparently, with such a unified mobile infrastructure, comes true mobility, which is the third advantage.

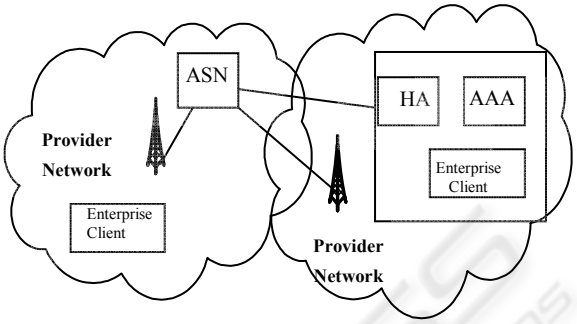

Figure 3: Provided hosted enterprise WiMAX.

With the NaaS vision for the provider-hosted mobile enterprise proposed in this paper, we now describe a WiMAX network architecture shown in Figure 3 which allows us to actually achieve NaaS. Before proceeding, however, it is important to point out that a sound security model is essential for a provider-hosted mobile enterprise infrastructure, thus should be a key focus, although we will not treat it as a separate topic below.

As shown in Figure 3, an enterprise network has all the core network components but it uses WiMAX networks of service providers for user mobile access to enterprise services both *on and off campus*. In the enterprise network, an AAA server is used for enterprise device and user authentication, a DHCP server is for dynamically distributing IP addresses to enterprise clients, a HA (Home Agent) is for Mobile IP (tunnel) management, and a IPSec gateway is for securing data in communication between a mobile client and a host in the enterprise network, *all* over a provider network. Upon entering a WiMAX network of a provider, a mobile client is authenticated by the AAA server of the enterprise network and the provider AAA server is acting as a proxy that forwards the authentication messages between the enterprise client and the enterprise AAA server. After successful authentication with IT certificates and other credentials, the client is given a Mobile IP address and a MIP tunnel is established between the HA and a FA (Foreign Agent) in the provider WiMAX network. A security association is then established between the IPSec gateway and the mobile client for carrying application traffic over a secure IP connection.

Such an architecture has several key features: 1) it enables full client mobility because it uses Mobile IP to allow a client to carry the application traffic in

real-time from one WiMAX network to another (or, to a WiFi network on campus!); 2) On-campus WiMAX coverage is done in the same way as off-campus coverage, all via providers' WiMAX networks; 3) Client authentication uses enterprise security factors (certificates etc.), rather than public (VeriSign) certificates; 4) IP addresses can be enterprise internal addresses, rather than public IP addresses; 5) Data security can be implemented either with IPSec tunnel model (i.e. IP VPN) or with IPSec transport mode; 6) Security and mobility are largely controlled by the enterprise rather than a provider.

Apparently, the central idea in the architectural direction of NaaS is enterprise managed mobility and security while leveraging providers' WiMAX networks for enterprise mobile access. In term of security, we could use provider's public authentication mechanism as the first authentication and then have a second enterprise specific authentication for further security, which was what we discussed earlier and actually implemented in our lab as Two-layer Authentication.

It is important to realize that a new business model, which formally defines the relationship between an enterprise and a provider and allows the enterprise to have sufficient control over enterprise services and data, is needed for this architecture In the cellular world, there is a type of service providers called MVNO (Mobile Virtual Network Operator), in which a virtual provider would offer services to real consumers out of the whole-sale subscriptions it acquired from large (real) providers. The MVNO model can be extended to a large enterprise, resulting in MENO, Mobile Enterprise Network Operator, for an enterprise that acts like a virtual provider. In MENO, an enterprise would provide real services to enterprise users as IT does it today, but it does not need to own any mobile networks. Like a MVNO, a MENO would acquire network accesses at whole-sale from service providers for its own enterprise users. Apparently, MENO and NaaS go hand in hand.

4 SECURITY CONSIDERATIONS

As shown in Figure 1, WiFi and WiMAX can have the same overall architecture in term of not only network access but also client and network authentication. This section discusses authentication of WiMAX for an enterprise environment.

Our effort on WiMAX authentication was motivated by: 1) to develop a few realistic authentication models in consideration of WiMAX enterprise usages so that enterprise grade authentication can be achieved for WiMAX; 2) to use the WiMAX standards as much as possible while making minor modifications or additions; and 3) to leverage existing components in enterprise authentication solutions such as that in WiFi.

The short coverage of WiFi provides a natural physical protection in network access as one has to be physically on premise to access a WiFi network. At Intel, we indeed take this into consideration and include physical location as one factor of authentication in addition to using IT defined certificates. For WiMAX, with its increased range of coverage, additional factors in WiMAX authentication need to be considered.

In our effort to find appropriate enterprise authentication models for WiMAX in mind, we investigated several possible models which we will discuss next.

1) WiMAX EAP-TTLS Model

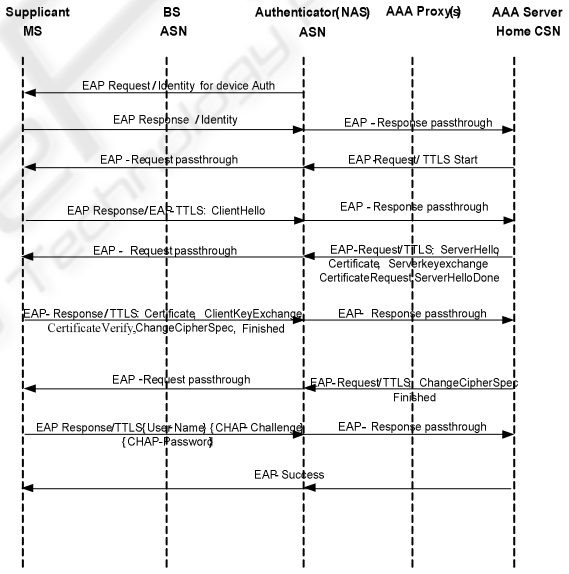

Figure 4: WiMAX EAP-TTLS.

The most straightforward approach to a model for enterprise WiMAX authentication is to evaluate how we can use authentication models as specified in the current WiMAX standard to find out if any of them can meet enterprise requirements and, if not, how we can adapt anything in these models to better meet the requirements but with minimal modifications. The WiMAX EAP-TTLS, which offers multiple authentication factors, appears to be a very likely option. The WiMAX EAP-TTLS is shown in Figure 4 below.

In WiMAX EAP-TTLS, MAC address, WiMAX certificates, and user name and password are used in the authentication process. In addition, it allows the use of network certificate only or both network certificate and client certificate in an authentication process, as a configurable option. A WiMAX certificate is one that is managed by WiMAX Forum with VeriSign as the 3rd party Certification Authority (CA).

Apparently, it is conceivable that we adapt in the way that EAP-TTLS is used with changing the protocol as defined by WiMAX Forum. For example, instead of using the VeriSign certificate in the hardware of a device, IT certificate or a TPM certificate can be used; instead of using MAC address, email address can be used; and, instead of using user name and password, a software ID or user finger print can be used. In our lab, we have built a system framework consisting of clients, BS, ASN, and AAA which allows the use of different device certificates and different user level information or secretes to carry out authentication operations as a research prototype.

In this approach, the use of EAP-TTLS can fall back to "public model" when the network is a provider network, i.e. to carry out authentication in exactly the same way as specified by WiMAX Forum.

2) Layered EAP Model

It is sometimes desirable to keep the use of EAP-TTLC as specified by WiMAX Forum and introduce additional authentication factors *independently* for increased enterprise security on top of WiMAX. In Layered EAP model, we introduce EAP over IP (EAPoUDP or EAPoIP) just for enterprise authentication which runs after the standard WiMAX EAP-TTLS in an authentication operation. This model can therefore be viewed as a two-stage authentication process, i.e. public network authentication followed by enterprise authentication. The advantage of this approach is the clear separation between the two stages with each dedicated to a particular type of network, which can conceivably translate into a clean AAA architecture. The questions associated with this model are how enterprise IT would be able to manage public certificates and if managing public authentication is indeed necessary in an enterprise environment.

3) Double EAP Model

A double EAP model is shown Figure 5. In this model, two different EAP TLS (or TTLS) form a single authentication process in the WiMAX layer, with a standard EAP-TLS authentication followed by an enterprise EAP-TTLS authentication, as specifically proposed here.

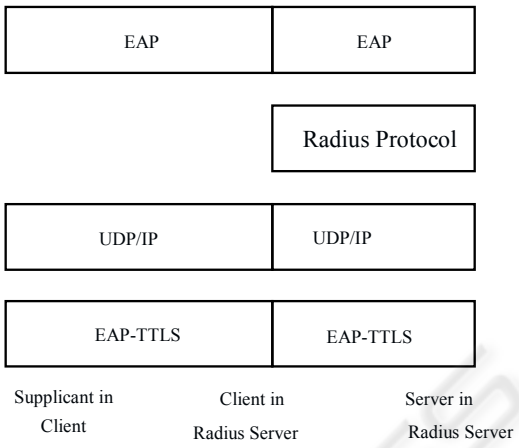

Figure 5: A Double EAP Model.

In addition, specific content in EAP-TTLS can be used in to make it more suitable for enterprise usages. In this approach, public network authentication is valid, when the network to be accessed is not an enterprise network, and can be automatically triggered during the access process.

5 CONCLUSIONS

WiMAX is no doubt important for the enterprise industry, although WiMAX as a standard was developed with the consumer market in mind. However, key challenges still exist today for Enterprise WiMAX in terms of network architecture and business models. In the conceptual framework of using WiMAX in an enterprise environment from technical viewpoint, the architectural discussion in this paper paves the way for the next generation Mobile Enterprise beyond local area network coverage for business users. The two different architecture models discussed can each play a role in the marketplace depending on whether an enterprise has the WiMAX frequency spectrum required to host a WiMAX network and what it prefers based on enterprise requirements and business considerations.

REFERENCES

WiMAX Forum, 2005, IEEE Standard 802.16e-2005
C. Perkins, 2002, IETF RFC 3344, IP Mobility for IPv4
S. Gundavelli, 2008, IETF RFC5213, Mobile IPV6