ABSTRACT

The wireless metropolitan area networks (WMANs) based on the 802.16 technology have recently gained a lot of interest among vendors and ISPs as the possible next development in wireless IP offering and a possible solution for the last mile Access problem. With the theoretical speed of up to 75 Mbps and with a range of several miles, 802.16 broadband wireless offers an alternative to cable modem and DSL, possibly displacing these technologies in the future. We discuss implementing security in wireless MANs with the PKM protocol that is used in 802.16 for key management and security associations management. Since device certificates are defined by the IEEE 802.16 standard, we briefly cover the issue of certificates and certificate hierarchies.

INTRODUCTION

In this chapter on wireless Metropolitan Area Network Security, we use the terms wireless MAN (WMAN), broadband wireless access (BWA), and WiMAX interchangeably to mean 802.16-based wireless networks and the technologies underlying these networks. The term broadband wireless access or BWA is the formal title used in the IEEE 802.16 standards documents, while WiMAX is the industry’s coined term for the technology (much in the same way that WiFi has been used for 802.11). We use the more general wireless MAN to mean both the technology and the industry around the technology. The aim is to provide enough context for discussions regarding security-related issues.

BACKGROUND ON 802.16 MANS

The basic arrangement of an 802.16 network or cell consists of one (or more) base stations (BSs) and multiple subscriber stations (SSs) (Hardjono, et al, 2005). Depending on the frequency of transmission,
the SS may or may not need to be in the line-of-sight of the BS antenna. In addition to base stations and subscriber stations, there might also be other entities within the network, such as repeater stations (RSs) and routers, which provide connectivity of the network to one or more core or backbone networks. The BS has a number of tasks within the cell, including management of medium access by the SS, resource allocation, key management and other security-related functions (Figure 1).

An implementation of an 802.16 network will typically deploy a fixed antenna for the SS, with the BS using either a sectored antenna or omnidirectional antenna. The BS would be installed in a location that can provide the best coverage, which would usually be the rooftops of buildings and other geographically high locations. Although a fixed SS would use a fixed antenna, with the future development of the mobile subscriber station (MSS), it is possible that an SS could be using an omnidirectional antenna. In practice, the cell size would be about 5 miles or less in radius. However, given suitable environmental conditions and the use of orthogonal frequency division multiplexing (OFDM), the cell radius can reach 20 or even 30 miles. In order to increase the range of a given implementation, a mesh topology can also be used instead of the point-to-point topology.

Figure 1. The 802.16 WiMAX network technology