Chapter XXIII
End-to-End Security Comparisons Between IEEE 802.16e and 3G Technologies

Sasan Adibi
University of Waterloo, Canada

Gordon B. Agnew
University of Waterloo, Canada

ABSTRACT

Security measures of mobile infrastructures have always been important from the early days of the creation of cellular networks. Nowadays, however, the traditional security schemes require a more fundamental approach to cover the entire path from the mobile user to the server. This fundamental approach is so-called end-to-end (E2E) security coverage. The main focus of this chapter is to discuss such architectures for IEEE 802.16e (Mobile-WiMAX) and major third generation (3G) cellular networks. The E2E implementations usually contain a complete set of algorithms, protocol enhancements (mutual identification, authentications, and authorization), including the very large-scale integration (VLSI) implementations. This chapter discusses various proposals at the protocol level.

INTRODUCTION

Mobile-WiMAX (802.16e) is a fourth generation (4G) candidate for mobility and is expected to address many of the current issues we face in 3G technologies. E2E security scheme is one of the major issues, which is currently addressed in variety of forms using IP security (IPsec), secure socket layer (SSL)/transport layer security (TLS), OpenPGP, and S/MIME (Gallop, 2005). The E2E architectures of major 3G technologies including global system for mobile communications (GSM), general packet radio service (GRPS), and code division multiple access (CDMA) and 802.16e will be discussed in this chapter.

The management of the sections is as follows: the next section will discuss details about the ultimate security features attributed to 3G technologies. The GSM section will discuss the security weakness in GSM's initial draft and the E2E solution to overcome its weakness. The fourth and fifth sections talk about GPRS and CDMA respectively. The Mobile-WiMAX section opens the discussion on 802.16e, the candidate for the 4G wireless systems, which contains the security weakness of 802.16e's initial draft and the E2E solution. A thorough comparison and references will be given in the last two sections.

OBJECTIVES OF SECURITY FEATURES FOR 3G/MOBILE-WIMAX

Before discussing security weaknesses of individual 3G technologies, we briefly discuss the objective of 3G security features. These features are (Campbell, Mckunas, Myagmar, Gupta, & Briley, 2002):

- **Mutual authentication:** Authentication is a method to verify that the claimed identity of an entity is genuine. Authentication is a fundamental security service and other necessary services often depend on proper authentication. Many protocols offer a one-way authentication. That is, only the client has to authenticate itself to the server and the server is not required to authenticate itself to the client. A one-way authentication is prone to an attack, so-called; *impersonation*, in which an illegitimate entity could pose as a legitimate one and start a new communication with another legitimate entity or take control an already started conversation. A two-way authentication scheme (mutual authentication) resolves impersonation attack. An E2E security scheme uses a balanced mutual authentication technique. A balanced technique requires equal effort by both entities for authenticate themselves to other entities. This decreases the chance of attacker's success
- **Data integrity:** This guarantees that the data received has not been altered by an unauthorized entity. One method of doing this is through the application of a hash function to the data stream
- **Security between networks:** Networks are interconnected using secure wired links, mainly using IPSec tunneling mechanism.
- **Secure international mobile subscriber identity (IMSI) usage:** The first-time user is assigned an initial IMSI number by the home network.
- **Stronger security scope:** Security is based within the radio network controller (RNC) rather than the base station (BS). An RNC is responsible for controlling and managing the multiple BSs including the utilization of radio network services.
- **User- and mobile-station authentication schemes:** Both user and mobile station share a secret common key, which is called the PIN. This is used for authentication.
- **Secure services:** These services protect the infrastructure against usage and access misuses.
- **Security in applications:** This is critical for mobile-based application security.
- **Fraud detection:** Mechanisms to detect and combat fraud in roaming situations.
- **Flexibility:** As technologies evolve, security features are extended and enhanced as required by new services and threats.
- **Service availability and configurability:** Users are to be notified whether security is on and the available level of security.
- **Multiple cipher and integrity algorithms:** The mobile user and the network negotiate and agree on the best available cipher and integrity algorithms (e.g., KASUMI).
- **Lawful interception:** Mechanisms should be provided to authorize agencies with certain necessary information about subscribers.
- **GSM compatibility:** GSM subscribers should be able to roam in 3G networks and cope with the extended security needed via GSM security context.