Chapter 11

PORTABILITY ARCHITECTURE FOR NOMADIC WIRELESS INTERNET USERS AND SECURITY PERFORMANCE EVALUATION

Mustafa M. Matalgah\textsuperscript{1}, Jihad Qaddour\textsuperscript{2}, Omar S. Elkeelany\textsuperscript{3} and Khurram P. Sheikh\textsuperscript{4}
\textsuperscript{1} University of Mississippi \textsuperscript{2} Illinois State University \textsuperscript{3} University of Missouri, Kansas City \textsuperscript{4} Sprint

Abstract A value added service to broadband wireless network is the remote access virtual private network (VPN). The corporate legitimate portable users can connect to their offices through a wireless network from different locations and get secure services as if they were connected to the corporate local area network. One of the main challenges is to block illegitimate wireless users’ requests. Registration and authentication functions should be implemented with highly secured wireless connection. These functions are accomplished by tunnelling the user information in a secured form to the corporate authentication server through the Internet traffic. The Corporate Authentication Server then grants or denies the user access. This chapter addresses various portability scenarios, architectures, implementation, and requirement issues for portable wireless Internet access systems. Moreover, performance evaluation and comparison are presented for the state-of-the-art security and authentication techniques.

Keywords: Wireless Internet, portability architecture, remote wireless authentication and security, VPN tunnelling.

1. Introduction

One of the most important requirements for high-speed fixed wireless Internet services is to support customer premises equipment (CPE) self install feature. This provides the user the ability to move around his location and re-establish radio and Internet protocol (IP) sessions easily. This is the simplest form of portability that can be supported to nomadic
users. In mobility it is required to keep the radio and IP sessions connected continuously. Whereas, for portability when a user moves from one regional base station to another then a hard handoff is experienced between the two regional base stations that belong to two different radio network controllers (RNC) in European networks (or mobile switching centers in American networks (MSC)). Different handoff scenarios and requirements need to be defined for both IP session handoff via a routing gateway, and radio network (RN) handoff via the radio link controller (RLC). If the user moves from one base station to another that belongs to the same RNC or MSC, then cell reselection need to be accomplished to reconnect the portable device at the new location. In mobility, cell reconnection for this scenario is performed smoothly without reestablishing a new session with the new cell. However, a new IP address reassignment might need to be established if subnet has changed.

When a portable device moves from one base station to another that belongs to a different RNC or MSC, then a new radio link protocol (RLP) signaling session with the new base station is needed for cell reselection. User registration and authentication is also needed if each RNC has its own server for Remote Authentication Dial In User Service (RADIUS). This server is used for dial-up security management.

This chapter addresses the following: 1) End-to-end element functions that meet portability requirements. 2) Various portability scenarios, architectures and implementation issues in fixed wireless Internet access systems. One of the major issues to be addressed is how to complete a secured time-bounded authentication, authorization and accounting when a user travels from one wireless market area to another through an IP network. 3) Private end-to-end architecture between the home and visited market network to complete a secured time-bounded portability requirement.

2. System Authentication

When a portable device moves from one base station to another that belongs to a different RNC, two methods are proposed for user registration and authentication (assuming each RNC belongs to a different RADIUS). In one method, since a different RADIUS serves each RNC, the new RNC will verify the user eligibility through its local (primary) RADIUS database, using tunnelling and routing protocols, for registration and authentication. The local RADIUS will then send interrogation signaling messages to all the RADIUSs in the network to verify the eligibility of that user. The RADIUS with the database that the user belongs to, will then reply with the eligibility status of that user to ac-