Chapter 83
Security and Mobility Aspects of Femtocell Networks

Suneth Namal
Center for Wireless Communication, Finland

Andrei Gurtov
Center for Wireless Communication, Finland

ABSTRACT

This chapter discusses security and mobility aspects of femtocell networks, given protocol level descriptions in the subsections. The connectivity between FAP and core network has a high risk of being compromised. The chapter discusses how Host Identity Protocol (HIP) can be adapted in femtocell technology to improve security and mobility issues. This chapter presents several enhancements to the femtocell technology such as strong authentication, service registration, identity verification, and node multihoming. In addition, Encapsulating Security Payload (ESP) is used to provide confidentiality, data origin authentication, connectionless integrity, anti-replay service, and limited traffic flow confidentiality. Furthermore, enhanced mobility support by means of locator/identity separation and node multihoming is discussed in the scope of 3GPP femtocells.

INTRODUCTION

The evolved communication technology introduces wide-spreading residential access points that enable mobile communication through the residential networks. The mobile networks can be widely spanned with the introduction of femtocells extending the operator network to subscriber residence. The home based Femtocell Access Points (FAPs) enable access to cellular networks over the broadband connectivity. FAPs are 3G hot-spots to which the mobile users can connect over the same Global System for Mobile Communications (GSM) band. Rather, FAPs may be WiFi enabled to support dual band handsets. LTE focuses on the extensive use of subscriber installed FAPs for improved network coverage and high-speed connectivity using Evolved Packet Core (EPC)

DOI: 10.4018/978-1-4666-4707-7.ch083

architecture which is based on all-IP concept. FAP establishes secure associations in either direction through the backhaul to protect the communication from attacks. It is realized, the connectivity between FAP and Femtocell Gateway (FeGW) is vulnerable to attacks since, both control and data traffic is carried over broadband access medium or public Internet which has no guarantee of security. Thus, protecting femtocell backhaul is a crucial requirement for secure communication.

Increasing number of mobile nodes attached to FAP may degrade service quality or prevent desired subscribers accessing operator network. Therefore, access control is a critical requirement in femtocell technology. On the other hand, close access FAPs filter subscribers using Closed Subscriber Groups (CSG) though; it may reduce the overall performance of the system (Novaczki et al., 2008). The existing femtocell architecture demands globally unique routable identity to be assigned on each connected device. In case of lacking IP addresses, mobile nodes that demand addresses to configure on it will not be served. For this reason, some operators implement address translation and address mapping in certain devices along the path. When it comes to mobility, IP addresses as identifiers result problems in user mobility. Therefore, identity, locator separation is highly demanded in mobile applications. HIP introduces a new identifier which obligates the rules of Domain Name Service (DNS). Thus, the change in IP address corresponds to the point of attachment may not affect transport layer associations.

In this chapter we have discussed the security and mobility aspects of the femtocell networks. By nature femtocells are very much prone to attacks. The backhaul between access point and the core network is vulnerable to threats as we are discussing in the coming sections. Furthermore, we have discussed few mobility protocols such as MOBIKE, PMIPv6 and HIP and the advantage over IP/Locator separation is emphasized.

BACKGROUND

Femtocell security architecture consists of three major stratums such as access security stratum, UE access control stratum and mobile network security stratum. FAP access security is provided in terms of mutual authentication, establishment of secure association, authorization, location looking mechanisms and the SeGW located in the border of the core network. Network domain security includes the security communication between SeGW and the core network whereas, UE access security includes access control based on Close Subscriber Groups (CSG) applicable legacy UEs. However, FAP authentication and message encryption across unreliable Internet or broadband access are major security considerations in femtocell networks.

Femtocell backhaul is vulnerable to any external attack since; there is no guarantee of security by the network provider. The femtocell security aspects are not yet standardized according to the 3GPP specifications (Akyildiz, Xie, & Mohanty, 2004). Thus, there are many ongoing research efforts to enable an end-to-end secure communication in femtocell technology. FAP authentication is a major consideration in femtocell security. In general, FAP authentication is performed using Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA), certificate or as a combination of both. The 3GPP standard presumes validation and authentication to be performed sequentially. Thus, during the initial power-up, FAP gets authenticate to the core network. If the certificate based authentication is used, the mutual authentication between the FAP and the core network is performed with X.509 certificate which is already configured at FAP and SeGW. Rather, Universal Integrated Circuit Card (UICC) that defines the identity of the secondary hosting party is used for the authentication (Akyildiz, Xie, & Mohanty, 2004).