4 Security Protocols for Fast BSS Transition

Abstract  Along with the rapid deployment of WLAN, the density of the wireless AP will increase dramatically. In this circumstance, the continuity of service requires the wireless system to provide enough credence for those frequent handoffs among different base stations. Taking audio services over WLAN for example, the capacity should be guaranteed that the mobile client devices can establish a new association with another new AP as soon as possible after they terminate the connection with the former one. The latency derived from a handoff process is composed of three parts, including time for probing and detection, authentication and service re-association. If the latency exceeds 50 ms, the interruption will be sensed obviously by ears. Nevertheless, the latency in the present IEEE 802.11 network is usually several hundred milliseconds on average, which may lead to negative influences, such as the occasional transmission interruption, connection loss and deteriorated audio quality, and so forth. Therefore, the fast handoff protocol plays an essential part in the extensive deployment of audio services over IEEE 802.11 networks. In this chapter, according to a close scrutiny to IEEE 802.11r, which specifies fast handoff among APs in a WLAN ESS, the used security protocols are presented. To make up the deficiency in DoS-resilience of the scheme in the standard, we propose two new secure fast handoff schemes, which are MIC based and Hash chain based. At last, we present the secure and fast handoff solution based on location. This solution is characterized by the following functions, QoS guaranteeing, location probing, and location based fast switching.

4.1 IEEE 802.11r

In recent years, demands for access services from users turn to broadband, mobility, portability, etc. The broadband WLAN technology, on the basis of IEEE 802.11, caters to people’s requirement of broadband access during the
movement. Thanks to the standard series of IEEE 802.11, which have solved incompatibility among different air interfaces, the WLAN technology acquires powerful impetus to enhance the interconnection between WLAN terminals and AP. Therefore, the cost of wireless devices decreases rapidly. The broadband WLAN technology, which provides the multimedia and mobile communication services accompanied with Internet access, has been a hotspot in the research.

4.1.1 Introduction

In order to support the mobility of STA, IEEE 802.11 workgroup firstly propose IEEE 802.11f, i.e., IAPP [1], as the protocol for exchanging the related information among APs, which specifies the roaming function of STA among several APs in the same network segment. A handoff occurs when STA moves to the boundary of two BSSs’ coverage. At that time, STA re-associates with the new AP and terminates the association with the original one. The system to achieve a handoff among different APs in the same ESS is depicted in IEEE 802.11f, consisting of STA, multiple APs, DS, and RADIUS Server. If a STA needs to initiate a handoff because of the wireless link, it must enforce the re-authentication and re-association with the new AP before the normal communication. IAPP is an up-layer protocol operating above the IP layer. To provide secure communication among APs, the APs that are compatible with IAPP should register themselves in the RADIUS Server, and establish secure connection among APs. The exchanged information between an AP and RADIUS Server includes a mapping from BSS ID to the IP address. Based on the mapping, keys can be sent by the RADIUS Server for secure communication among APs. When a STA initiates a handoff, it needs to send the association or the re-association frames to the new AP, and then the new AP begins to exchange information with RADIUS Server to achieve the mapping between its new BSS ID and its IP address; meanwhile, the RADIUS Server conveys the corresponding keys to the new AP. Because an AP has to carry out the information exchanges with RADIUS Server at every time when a handoff occurs, the latency during a handoff will be relatively long. Though, the IEEE 802.11 committee launch work group TGr to study Fast BSS Transition (FBT) in order to fulfill the demands from those delay-sensitive services [2].

IEEE 802.11r specifies the holistic communication flow when a STA accomplishes a handoff with a new AP in the same ESS (including key verification), achieving a fast roaming protocol for wireless data and audio services. The STA handoff among APs from different ESS is out of scope of this standard. The IEEE 802.11r technology is independent of the IEEE 802.11i RSN and IEEE 802.11e network.

When a handoff occurs, the connection with the current AP is cut off; meanwhile, the new association with the new AP is started, which may lead to a transient connection loss, packet loss, and re-transmission in up layers, the ultimately