[11-62]

Fast Handoff Support In 802.11i Environment: Extended Key Distribution Tunnel

정요셉, 이종협, 송주석
연세대학교 컴퓨터과학과
{joyfully, jhlee, jssong}@emerald.yonsei.ac.kr

Fast Handoff Support In 802.11i Environment: Extended Key Distribution Tunnel

Joseph Jung, JongHyup Lee, JooSeok Song
Department of Computer Science Yonsei University

Abstract

WLAN is widely used and its security fault becomes a significant problem. 802.11i specification is issued for supporting security services in 802.11 networks. When EAP-TLS scheme is used in 802.1x authentication framework, the full authentication is needed at every handoff. However the full authentication takes too long time to satisfy the requirements of the real-time applications like VoIP. We propose a fast handoff scheme in 802.11i environment, called "Extended Key Distribution Tunnel". It avoids the full authentication on handoff by generating the new PMK based on the current PMK. Because it can avoid most of the full authentication, the performance can be improved dramatically.

I. Introduction

Wireless Local Area Networks (WLANs) have quickly become part of everyday life. The need for security solutions for a wide variety of users has become inevitable with the rapid growth of the wireless systems. The IEEE 802.11i task group has proposed a new security architecture called Robust Security Network (RSN) to improve the security of the current 802.11 MAC. This new architecture utilizes the IEEE 802.1X standard for access control and Advanced Encryption Standard (AES) for encryption. 802.11i uses a pair-wise key exchange protocol utilizing 802.1x for mutual authentication and key management process.

Specifically, it is desirable to minimize the number of messages so as to reduce the delay during the handoff process as well as reducing the channel contention. In 802.11i, since the full authentication is needed every time a user associates/re-associates with an access point and during a handoff process to setup new keys it contributes to the delay and the channel contention in the system.

We propose a fast handoff scheme in 802.11i environment, called "Extended Key Distribution Tunnel". It can avoid the full authentication on handoff, the performance can be improved dramatically.

II. Related Works

A. IEEE 802.11i

The 802.11i task group is expected, in late 2003, to generate what will become a new 802.11 specification that addresses these issues and defines how secure wireless connectivity products must operate. 802.11i defines the concept of an RSN. An RSN makes extensive use of protocols above the IEEE 802.11 MAC layer to provide authentication and key management. This allows IEEE 802.11 to take advantage of work already done in other standards groups and avoid duplicating functions at the IEEE 802.11 MAC that are already performed at higher layers.

The 802.11i work is focused in two areas:

- Defining an overall architecture for wireless security. This will include the use of technologies such as EAP, 802.1x, RADIUS, and certificates.
- How the architecture should be implemented for current and future products.

B. EAP-TLS

The Transport Layer Security protocol as described in RFC-2246 provides strong authentication and encryption at the transport level. The authentication part of TLS has been exported as an authentication mechanism over EAP in EAP-TLS RFC 2716. This is