[11-59]

IEEE 802.11 환경에서의 Lightweight Packet 상호 인증

이근순, 김효진, 송주석
연세대학교 컴퓨터과학과
{soonlee, hyojin, jssong}@emerald.yonsei.ac.kr

A Mutual Lightweight Packet Authentication in IEEE 802.11

KeunSoon Lee, HyoJin Kim, JooSeok Song
Department of Computer Science, Yonsei University

요약

급속도로 증가하고 있는 데이터 트래픽을 현재의 무선 기술로는 감당할 수 없다. 그러므로 좀 더 무선 통신에 알맞고 간단하면서도 효율적인 통신 방법이 필요하다. 본 논문에서는 IEEE 802.11 표준을 따르는 통신 환경 하에서 Mutual Lightweight packet Authentication(MuLA)을 제안한다. MuLA는 일반적으로 First-hop으로 정의되는 station(STA)과 access point(AP) 사이에서 최소한의 비용으로 Access Control을 할 수 있는 방법을 제공한다.

1. 서론

한때 많은 주목을 받았으며 Wi-Fi(Wireless Fidelity)라고도 불리는 IEEE 802.11b 표준은 심각한 보안상의 문제점들이 지적되었기 때문에, 보안에 대한 전반적인 사항을 기술해 놓은 IEEE 802.11i 라는 표준이 새로 만들어지게 되었다. IEEE 802.11i는 일반적으로 First-hop[1]으로 정의되는 station(STA)과 access point(AP) 사이의 통신에서 사용되는 각종 보안 이슈들을 정리해 놓은 표준이다. IEEE 802.11i는 무선 통신은 전파를 조절할 수 없다는 고유의 특성 때문에 유선 통신에 비해 보안상으로 더욱 취약하다는 약점을 보완하였지만 overhead가 매우 많다.

대개 금융거래 등 철저한 보안이 필요한 작업이 있는 반면, 웹서핑과 같은 단순한 작업에는 IEEE 802.11i와 같은 강한 보안성을 제공하지만 overhead가 큰 기법이 필요하지는 않다.

기존에 소개된 Statistical One-Bit Lightweight Authentication(SOLA)[2]은 최소한의 overhead로 access control을 할 수 있는 방법으로, 인증되지 않은 STA이 AP에 부당하게 access를 시도하는 경우를 차단해 준다. 하지만, SOLA는 STA에서 AP로의 access 시도만을 고려하였을 뿐 그 반대의 경우는 고려하지 않았으며, 동시에 다수의 ACK(Acknowledgement)이 손실되어 동기를 맞추기 어려운 경우에 대한 고려를 하지 않았다. 그러므로 본 논문에서는 이에 대한 해결책으로 MUtual Lightweight packet Authentication(MuLA)을 제안한다.

2. First-hop과 End-to-End security

First-hop[1]인 STA과 AP 사이는 IEEE 802.11을 사용하여 무선으로 연결하고 AP부터 destination까지는 인터넷을 사용하여 유선으로 연결한다고 가정할 때, Alice가 Bob에게 이메일을 보내려한다면, 전송 도중에 악의적인 사람에게 그 내용이 유출되지 않도록 End-to-End security를 제공해 줄 필요가 있다. End-to-End security는 유선 도메인에서는 IPv6(Internet Protocol version 6)나 VPN(Virtual Private Networks) 등을 이용하여 제공해줄 수 있지만, 무선 도메인인 First-hop에서는 IEEE 802.11i가 사용된다. End-to-End security와 First-hop security 사이의 관계는 그림 1과 같다.

그림 2와 같이 IEEE 802.11i는 First-hop에서 강한 보안성을 제공하기 위해, End-to-End security를 위해 암호화한 패킷을 다시 암호화한다. 데이터 트래픽이 빠르게 증가하고 있는 현재의 상황에서 볼 때, 이와 같이 같은 패킷을 두 번 암호화하는 것은 많은 delay를 가져온다. 즉, 이러한 문제점을 해결하기 위해 SOLA[2]가 제안되었다.

3. SOLA

IEEE 802.11i는 First-hop에 거의 완벽한 보안성을 제공해주지만 overhead가 매우 많다. 무선 통신에서 overhead가 큰 것은 효율적이지 못하므로, 논문 [2]에서는 First-hop에서 IEEE 802.11i를 위한 암호화 과정을 생략하고 대신 SOLA를 도입할 것을 제안하였다.

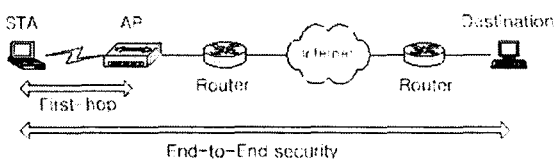

그림 1. First-hop과 End-to-End security