情報保護學會論文誌
第20卷 第5號, 2010. 10

메모리 사용 감소를 통한 802.11i 4-Way Handshake에서의 DoS 공격 차단 기법

김 정 윤,[1†] 김 인 환,[2] 최 형 기[1‡]
[1]성균관대학교, [2]LG전자

DoS attack prevention using methods for reduction of memory usage in 802.11i 4-Way Handshake

Jung-Yoon Kim,[1†] In-Hwan Kim,[2] Hyoung-Kee Choi[1‡]
[1]Sungkyunkwan University, [2]LG Electronics

요 약

무선 서비스의 하나인 Wireless LAN(WLAN)은 기존의 cellular network보다 높은 데이터 전송 율을 가지며 편리한 무선 인터넷 접속을 제공하여, 사용량이 지속적으로 증가하고 있다. 그럼에도 불구하고 802.11는 무선 환경이 가지는 고유의 특성으로 인해 많은 공격에 노출되어 있다. IEEE는 이러한 문제점을 해결 하기 위해 802.11i 보안 표준을 발표하였다. 그러나 802.11i의 키 분배 과정의 취약성으로 인해 공격 대상이 되는 단말에게 지속적으로 메시지를 보내면 단말은 메모리 고갈현상이 발생하게 되고, 정상적인 무선랜 서비스를 받지 못하게 된다. 본 논문에서는 이러한 문제점을 해결하기 위한 방법을 제시하고 기존에 제안되었던 방법과 시뮬레이션을 통해 비교 분석 하였다. 제안하는 기법은 단말의 메모리 소비를 최소화 함으로써 단말의 메모리 고갈 현상을 제거한다.

ABSTRACT

Wireless LAN (WLAN) is type of wireless service that has higher data transmission than current cellular networks. The usage is continually increasing. There are a lot of vulnerabilities in wireless network, due to the properties of the wireless environment, regardless of its popularity. IEEE announced the 802.11i security standard to solve these problems. The vulnerable point of messages used in the process of key distribution for 802.11i makes the target node attacked lose memory through continuous messages and blocks the legitimate WLAN service. In this paper, we proposed new schemes to solve this problem and compared our proposals with the current process. The proposed protocol eliminates the memory exhaustion problem on the client side by using methods for reduction of memory usage.

Keywords: 4-way handshake, 802.11i, wlan security, denial of services, security

I. 서 론

무선랜은 설치가 용이하며 쉽게 인터넷에 접속할 수 있는 장점을 지니고 있어 점점 그 사용이 늘어나고 있다. 이러한 인기에도 불과하고 무선랜은 제 3자에게 데이터가 쉽게 노출될 수 있다는 무선 환경의 특성을 그대로 따르고 있어, 각종 공격들에 대해 심각하게 노출되어 있다. 무선 환경에서 암호화 기능의 제공에 따른 기밀성과 무결성을 보장하지 않는다면, 모든 데이터가 제3자에게 그대로 노출 되거나 변조될 수 있다. 또한, 사용자 인증 메커니즘이 취약하다면, 공격자는 정상적인 사용자나 서비스 제공자로 위

접수일(2010년 1월 9일), 수정일(1차: 2010년 3월 25일, 2차: 2010년 5월 11일), 게재확정일(2010년 5월 18일)
† 주저자, steal83@ece.skku.ac.kr
‡ 교신저자, hkchoi@ece.skku.ac.kr

장하여 사용자의 통신을 도청 할 수 있게 된다. 따라서 무선랜 서비스는 기밀성과 무결성을 보장하고 안전한 사용자 인증을 제공하여야 한다.

IEEE는 무선랜에서의 암호화 통신과 상호인증을 제공하기 위해, Wired Equivalent Privacy (WEP)[1]와 802.1x[2]를 발표하였다. 그러나 WEP의 암호학적 취약점이 발견되었으며, 802.1x역시 개인 정보가 침해되거나, man-in-the-middle 공격 등이 가능한 취약점이 알려지게 되었다.

이에 따라, IEEE는 보다 강화된 무선랜 보안을 제공하기 위한 802.11i[3]를 발표하였다. 802.11i는 강력한 암호화 방식과 세션 키 분배 방식, 상호 인증 메커니즘을 제공하고 있다. 그러나 802.11i의 세션 키 분배를 위한 4-way handshake[4][5]과정의 취약점이 발견되었고, 이를 통해 공격자가 지속적으로 단말에 메시지를 보내게 되면 단말에 대한 Denial of Service (DoS) 공격이 가능해지고 결과적으로 정상적인 무선랜 서비스를 제공받지 못하게 되는 문제점이 존재 하게 되었다.

본 논문은 802.11i의 세션 키 분배를 위한 4-way handshake 과정에 초점을 맞추고 있으며, 4-way handshake과정의 취약점과 이를 악용한 공격을 보여주고 공격에 대한 해결책들을 제시하며, 기존의 대안들과 시뮬레이션을 통한 비교 분석 결과를 보여준다. 제안하는 해결책은 단말 측이 저장해야 하는 값을 최소화 함으로써 단말 측의 메모리 고갈 가능성을 제거한다. 즉, 기존 802.11i에서 단말이 저장해야 하는 정보 (SNonce)를 제안하는 해결책에서는 더 이상 단말이 저장할 필요가 없으며, 그 대신 Access Point가 해당 SNonce를 단말에게 되돌려주는 방법을 사용함으로써 메모리 고갈현상을 제거할 수 있다.

본 논문의 2장은 관련 연구로 이루어져 있고, 3장은 4-way handshake 전반에 대한 분석과 보안 취약성에 대한 분석을 다루고 있으며, 4장은 본 논문이 제안하는 해결책에 대한 설명하고 있다. 5장은 실제 무선랜 환경 구현을 통한 해결책들에 대한 비교 분석을 포함하고 있다. 6장은 논문의 결론에 대해서 설명하고 있다.

II. 관련연구

802.11i는 기존의 WEP와 802.1x의 취약점을 보완하고, 더욱 강력한 보안을 제공하기 위해 암호화 방식, 상호인증 메커니즘과 세션 키 분배 방식을 정의하고 있다. 현재 802.11i의 취약점을 분석하고 이를 보완하기 위한 많은 연구가 진행 중이다.

Changhua He들은 802.11i 인증 과정 중 세션 키 분배 과정인 4-way handshake에서 발생할 수 있는 공격에 대해서 분석하고 이를 막기 위한 해결책을 제시하였다[4]. 4-way handshake 과정에서 단말과 AP는 키 생성에 필요한 인자들을 교환하는데, 세션 키는 2개의 메시지를 교환 후에 비로소 유도가 가능하게 된다. 따라서 첫 번째 메시지는 아직 세션 키가 생성되지 않아서 무결성이나 기밀성을 보장하지 못하게 되어, DoS 공격의 원인이 되고 있다. 공격자는 단말에 마치 서로 다른 많은 수의 AP로부터 첫 번째 메시지가 보내진 것처럼 위장하고, 단말의 메모리 자원을 공격하는 DoS 공격을 가하게 된다. 이 DoS 공격을 막기 위해 그들은 세션 키를 생성할 때 필요한 인자 중에서 단말의 랜덤 값을 고정하여 단말이 여러 개의 첫 번째 메시지를 받아도 각각의 첫 번째 메시지에 대해 메모리를 할당하지 않게 하는 방법을 제시하였다. 그러나 이들이 제안하는 기법은 랜덤 값이 고정되어 있다는 특성에 의해, key freshness를 보장하지 못한다. 즉, 단말과 AP 사이에 생성되는 세션키는 매번 같은 랜덤 값에 의해 생성되기 때문에, 공격자가 키 및 암호문에 대한 각종 공격을 수행함으로써 키 및 평문 일부를 도출해낼 가능성이 존재한다.

또한 Changhua He들은 4-way handshake외에도 802.11i 각 절차에서 발생할 수 있는 다양한 보안 취약점들을 분석하고, 이를 제거하기 위한 방법들을 보여주며 최종적으로는 802.11i의 총체적인 변화 방안을 제안하였다[5]. 현재 802.11i 표준에 따르면 802.11i 각 절차를 수행 중에 문제가 발생하게 되면, 진행되고 있던 모든 절차가 취소되며 802.11i의 처음부터 다시 실행하게 된다. 따라서 그들은 각 절차 속에서 문제가 발생하더라도 진행 중이던 절차 이전 절차로 돌아가서 해당 절차부터 다시 실행되도록 하고, 802.11i의 보안취약점을 제거할 수 있는 해결책들과 결합하여 새로운 802.11i를 제안하였다. 그러나 이들이 제안하는 기법은 802.11i에 대해 많은 수정을 필요로 하며, 따라서 현실에 적용하기 어렵다는 단점이 존재한다.

Hayrie Altunbasak들은 4-way handshake에 사용되는 메시지 교환 횟수와 시간 지연을 줄이기 위한 연구를 진행하였다[6]. 그들은 4-way handshake의 마지막 메시지가 단순히 세 번째 메시지를 제대로

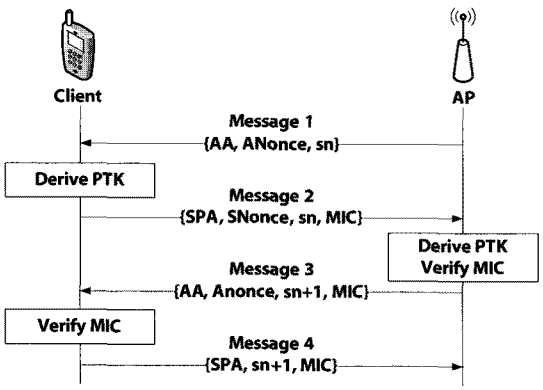
받았음을 확인하는 의미 밖에 없다는 점에 착안하여 마지막 메시지를 제외하고 timer를 사용한 3-way handshake를 제안하였다. 또한 세션 키 생성을 위한 인자를 간소화 하여 2-way handshake도 가능함을 보여 주었다. 그러나 그들이 제안한 3-way handshake의 경우, 3번째 메시지를 수신한 이후에 AP는 일정시간을 기다려야 한다는 단점이 존재한다. 이는 공격자에 의한 또 다른 DoS 공격이 가능함을 의미한다. 그리고 2-way handshake의 경우 PTK를 생성함에 있어서 단말이 전혀 관여하지 않기 때문에, 단말은 PTK의 fressness 및 안전성을 확신할 수 없다는 문제가 발생한다. 예를 들어, AP의 암호모듈에 문제가 발생할 경우, 키는 다른 사용자들에게 노출될 가능성이 존재하며, 단말은 이러한 위협을 방지할 수 없게 된다.

Romano Fantacci들은 무선랜 환경에서 안전하면서 효율적인 handover 방법을 제안하였다[7]. 현재 802.11i에서는 단말이 기존의 AP에서 handover하여 새로운 AP와 통신하는 경우, 새로운 AP와 단말은 802.11i과정을 처음부터 다시 실행해야 하였다. 이로 인해 handover 시간이 길어지며, VoIP같은 QoS를 보장하여야 하는 서비스를 이용하는 경우 서비스를 정상적으로 이용할 수 없게 된다. 따라서 그들은 802.11i 인증과정에서 생성되지만 사용되지 않고 있던 키를 이용하여, handover가 일어나는 경우 인증서버가 이 키를 사용하여 새로운 AP와 인증에 필요한 정보가 담긴 토큰을 생성해 단말이 802.11i 모든 과정을 다시 시작할 필요 없이 토큰의 정당성만 확인하고 바로 통신을 재개할 수 있는 방법을 제시하였다. 해당 연구는 802.11i에서의 handover에 관한 연구로서, 본 논문에서는 다루지 않는 범위이므로 해당 연구와의 상세한 비교 및 분석은 생략한다.

Jing Liu 등은 4-way handshake 과정의 보안성을 formal method를 이용하여 증명하였으며, 그 결과 기존 802.11i의 4-way handshake 과정이 DoS 공격에 취약하다는 사실을 밝혀냈다[8]. 즉, Changhua He 등의 연구에서 밝힌바와 같이, 4-way handshake에서의 첫 번째 메시지는 보호받지 못하기 때문에 위조된 첫 번째 메시지에 의한 DoS가 발생할 수 있음을 주장하였다. Jing Liu 등은 PTK가 생성되기 이전에 단말과 AP가 공유하고 있는 PMK를 이용하여 메시지를 보호하는 방법을 제안함으로써, 송수신 되는 메시지 개수를 2개로 줄이면서 DoS 공격의 위협을 방지할 수 있는 대책을 제안하였다. 그들은 제안하는 기법이 재전송 공격 (replay attack)을 차단할 수 있다고 주장하였으나, 그들의 기법이 재전송 공격을 차단하기 위해서는, 단말은 모든 AP에 의해 송신되는 모든 ANonce를 저장하고 있어야 한다. 그렇지 않으면 공격자는 과거에 AP에 의해 송신된 첫 번째 메시지를 재전송함으로써 단말이 새로운 PTK를 설치하도록 유도할 수 있다. 이는 결과적으로 DoS를 유발하게 될 수 있다. 만약 단말이 모든 ANonce를 저장한다면, 이는 메모리 고갈에 의한 또 다른 DoS를 유발할 수 있다. 따라서 이들이 제안하는 기법은 DoS 공격의 취약점이 존재한다.

Kemal Bicakci 등은 PHY계층과 MAC계층에서 발생할 수 있는 각종 공격들에 대해 소개하고, 일부 공격들을 막을 수 있는 방법을 제안하였다[9]. 그들에 따르면 802.11 네트워크는 무선통신에 기반하기 때문에 jamming attack에 취약하다. 그러나 jamming attack을 암호기법으로 막는 것은 불가능하며, 이를 막기 위해서는 PHY계층에서의 대안이 필요하기 때문에, jamming attack에 대한 고려 및 대책 논의는 본 논문에서는 다루지 않는다. Kemal Bicakci 등은 802.11의 MAC계층에서의 취약점으로서 deauthentication attack의 가능성을 제시하였다. 이러한 deauthentication attack은 802.11의 관리프레임이 보호되지 않기 때문에 발생하는 것으로서, 802.11i가 적용되어도 이 문제는 해결되지 못한다. 한편, 그들은 각 계층별로 존재하는 취약점들을 제거하기 위한 방법들을 통합적으로 제시하였다. 즉, 그들이 제안하는 솔루션은 PHY계층, MAC계층, 그리고 상위 계층에서의 보안 기법들을 모두 결합하고 있다. 그들이 제안하는 기법은 강력한 보안성 향상을 기대할 수 있으나, 공격 가능성 및 효과가 낮은 사소한 위협들을 모두 제거하기 위해 성능 및 비용의 과다한 소모를 유발한다. 이는 해당 기법이 현실적으로 적용되기 어려움을 의미한다.

Sung-Hyun Eum 등은 802.11i 및 4-way handshake의 보안성에 대해 분석하고, hash chain 메커니즘을 활용하여 DoS 공격을 차단할 수 있는 대책을 제안하였다[10]. 그들이 제안하는 해결책에서는 인증서버가 미리 다수 개의 hash chain을 생성한 다음, 해당 hash chain의 마지막 값을 인증과정에서 차례대로 사용한다. 즉, 다항 시간 내에 hash의 역을 계산할 수 없다는 hash의 속성에 의해 인증 서



〔그림 1〕 802.11i 4-way handshake

버가 아닌 다른 개체는 해당 hash chain을 생성할 수 없음을 인증에 활용하는 기법이다. 해당 기법을 적용하기 위해서는 hash chain의 마지막 값을 인증서버와 단말이 공유하고 있는 키로 암호화 하거나 무결성을 검증할 수 있는 방안이 함께 제공되어야 한다. 또한, 단말과 인증서버의 상호인증 이후에 단말이 4-way handshake를 수행하게 되면 인증서버는 해당 hash chain 값을 AP에게 전달하여 단말과 AP가 해당 hash chain을 이용해 계속 인증을 진행할 수 있도록 해야 한다. 그들의 기법은 hash chain의 싱크가 깨어질 경우, 인증이 완전히 취소되고 4-way handshake 이전 단계 (단말과 인증서버 간 상호인증)부터 새롭게 인증을 시작해야 한다는 문제점이 존재한다. 즉, 그들의 기법이 현실에서 적용되기 위해서는 hash chain의 싱크가 깨어질 경우를 대비한 대책이 요구된다. Hash chain의 싱크가 깨지는 문제는 hash chain을 활용하는 기법들의 전형적인 취약점이다.

III. 4-way handshake 분석

4-way handshake는 802.11i 인증 과정에서 단말과 AP의 상호인증과 세션 키 유도 및 검증을 담당하는 핵심적인 과정이다. 4-way handshake의 주요 역할은 단말과 AP간에 동일한 Pairwise Master Key (PMK)를 소유하고 있음을 확인하고 세션 키인 Pairwise Transient Key (PTK)를 생성하는 것이다.

3.1 4-way handshake 개요

4-way handshake[4][5]는 〔그림 1〕 과 같이 Message 1에서 Message 4까지의 4개의 메시지를 사용하여, 단말과 AP 사이의 PMK 소유 여부를 확인하고, 무선 구간의 보호를 위한 키인 PTK를 생성하게 된다.

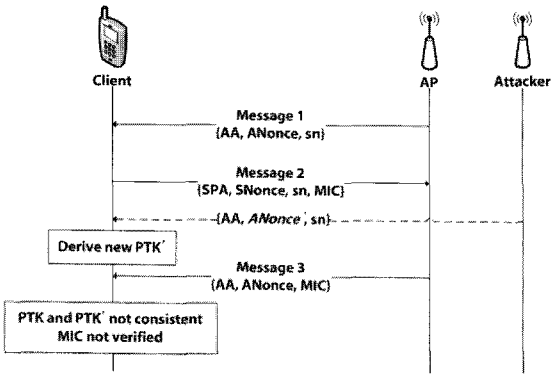
AP가 단말에게 메시지를 보내면서 4-way handshake는 시작된다. 이 메시지에는 AP의 MAC 주소인 AA와 AP가 선정한 랜덤 값 ANonce, 그리고 재전송 공격을 방지하기 위한 counter로 sequence number (sn)이 포함되어 있다. Message 1을 받은 단말은 임의의 랜덤 값인 SNonce를 생성한다. 생성한 SNonce, 단말의 MAC주소인 SPA, AP가 보낸 Message 1에 포함되어 있던 AA, ANonce 그리고 PMK 이렇게 5개의 인자를 사용하여 PTK를 생성한다. 그리고 SPA와 SNonce와 Message Integrity Code (MIC) 가 포함된 Message 2를 AP에게 전송한다. MIC는 단말과 AP가 송수신하는 메시지의 무결성을 증명하기 위해 사용되며, 메시지를 PTK로 암호화 한 것이다. 즉, Message 2에 포함된 MIC는 SPA, SNonce, 그리고 sn의 무결성을 증명하기 위해 사용된다.

Message 1을 AP가 보내는 시점에는 PTK를 생성하기 위한 5개의 인자가 모두 확보된 상태가 아니므로, AP는 PTK를 생성할 수 없게 되고, 첫 번째 메시지는 평문으로 전송되며 보호되지 않는다.

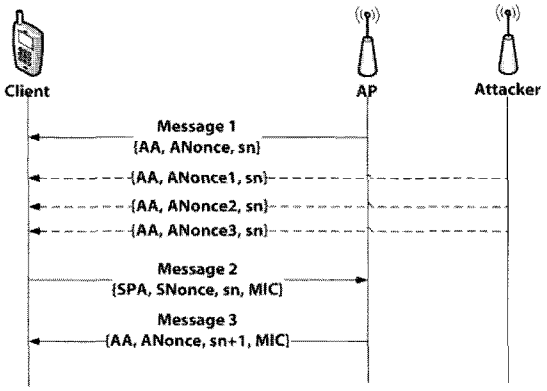
단말로부터 Message 2를 받은 AP는 SPA와 SNonce를 획득하게 되므로, AP도 단말과 같은 PTK를 생성 할 수 있게 된다. AP는 PTK를 생성하고, 생성된 PTK를 사용하여 Message 2의 MIC를 검증 한다. AP는 전달되어온 메시지를 PTK로 암호화하여 수신된 MIC와 비교하여 메시지의 무결성을 확인한다. 이 작업을 통해 AP는 단말이 동일한 PMK를 소유하고 있음을 확인하게 된다.

Message 3 역시 Message 2와 유사한 과정을 거친다. 단말은 수신된 Message 3의 MIC를 검증해 봄으로서, AP가 단말과 동일한 PMK를 소유하고 있음을 확인한다. 또한, 세 번째 메시지에는 AP가 생성한 Group Temporal Key (GTK) 가 포함 될 수 있는데, 이는 AP가 브로드캐스트하는 beacon 등의 프레임을 보호하기 위해 사용된다. Message 3에는 sn 대신 sn+1이 포함됨으로써, 공격자에 의한 재전송 공격 (replay attack)의 가능성을 제거한다.

네 번째 메시지는 단순히 단말이 세 번째 메시지를 제대로 전송 받았음을 알려주는 간단한 의미를



〔그림 2〕 One-message Attack



〔그림 3〕 Memory exhaustion attack

지닌다.

한편, PTK는 다음과 같은 식에 따라 생성된다.

PTK = PRF-512 (PMK, "pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || ANonce || SNonce).

PRF-512는 512비트의 결과를 출력하는 의사난수 생성기 (Pseudo Random Function)를 의미한다.

3.2 4-way handshake 취약성 분석

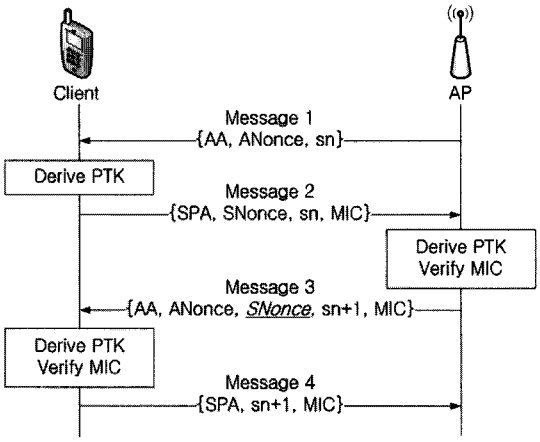
4-way handshake 과정에서 AP는 현재 몇 번째 메시지를 보내고 받았는지 저장하며, 현재 기다리고 있는 메시지가 일정시간 동안 도착하지 않는다면 이전의 메시지를 보내어 정확한 응답을 기다린다. 단말은 AP와 다르게 현재 몇 번째 메시지를 보냈는지, 몇 번째 메시지를 받아야 하는지에 대한 정보를 저장하지 않는다. 단말이 현재 상태에 대한 정보를 저장하고 특정 메시지를 기다리게 되면, 다음과 같은 상황들이 발생했을 때, 교착 (deadlock) 상태가 발생하게 되고 4-way handshake 과정은 더 이상 진행되지 않는다.

첫 번째는 단말이 보낸 Message 2가 패킷 손실로 인해 AP에게 전송되지 않는 상황이 발생하는 경우이다. AP는 일정시간 후 단말에게 Message 1을 다시 전달하지만 단말은 Message 3을 기다리고 있기 때문에 해당 메시지를 받아들이지 않고 버리게 된다. 또 다른 상황은 공격자가 위조된 Message 1을 보내 4-way handshake과정을 시작하는 경우이다. 이 후, AP가 정상적인 Message 1을 보내더라도 단말은 Message 3을 기다리고 있기 때문에 이를 받아들이지 않게 된다. 이 두 가지 상황이 발생하게 되면 4-way handshake 과정은 중단되고, 802.11i 과정은 실패하게 된다. 그러므로 단말은 단순히 수신되는 Message 1에 대한 중복만을 확인한다. 또한, Message 1이 전송되는 시점에서 단말과 AP 모두 PTK를 생성하지 못한 상태이므로 MIC를 첨부 할 수 없어 단말은 전송되어오는 모든 Message 1에 대해 매번 PTK를 생성하고 메시지에 대한 ANonce와 PTK를 저장한다.

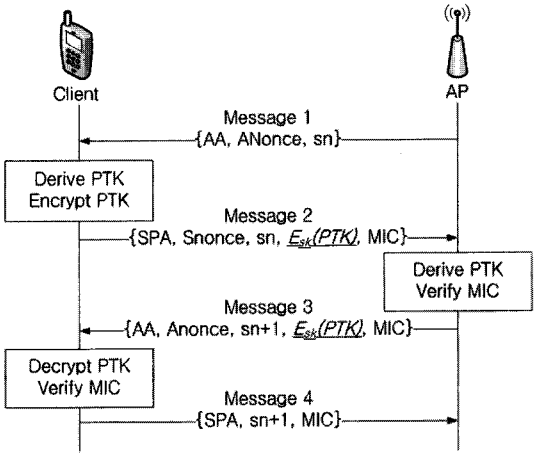
〔그림 2〕 와 같이 정상적인 Message 1과 Message 3 사이에 공격자가 단말에게 AP가 보낸 Message 1에서 단순히 ANonce 값만 변경하여 재전송하게 될 경우, 단말은 PTK를 새로 생성하게 된다. 이후 AP가 정상적으로 Message 3를 전송하게 되면, 공격자로 인해 PTK가 변경되었기 때문에 MIC의 검증에 실패하게 되고, 4-way handshake의 blocking이 발생하게 된다.

이 공격을 막기 위해서는 단말은 전송되어 오는 모든 Message 1에 대해서 일시적인 PTK를 생성하고, 이후 세 번째 메시지를 받고 MIC를 검증하여 일치하면 PTK를 설치해야 하며 단말은 각 ANonce 값에 대하여, 해당하는 모든 PTK를 생성, 저장해야 한다. 이는 〔그림 3〕 과 같은 정상적인 첫 번째 메시지와 세 번째 메시지 사이에 공격자가 다수의 첫 번째 메시지를 보내어 단말의 자원을 소모시키는 공격이 가능해진다[5].

공격자가 위조해서 보낼 수 있는 첫 번째 메시지의 수는 이론적으로 한계가 없으므로, 단말의 ANonce와 PTK를 저장하는 메모리의 한계를 초과시켜 4-way handshaking blocking이 가능해진다. 4-way handshaking blocking은 공격의 성립이 쉽고, 공격이 성공하는 경우, 이전의 802.11i 모든 인증과정이 취소되기 때문에 심각한 문제를 야기할



〔그림 4〕 AP가 SNonce를 전송



〔그림 5〕 암호화 된 PTK 전송

수 있다.

IV. 제안하는 4-way handshake

4-way handshake 과정에서 단말은 전송되어오는 모든 Message 1에 대해 받아들이고 ANonce와 생성되는 PTK를 메모리에 저장하게 된다. 따라서 공격자가 다수의 위조된 메시지를 보내게 되면, 단말은 이에 대해 모두 메모리를 할당하게 되고, 메모리 소모로 인한 4-way handshake blocking이 발생한다.

본 논문은 4-way handshake blocking을 막을 수 있는 2가지 해결책을 제시한다. 각 해결책은 단말이 Message 1에 대해 ANonce와 PTK를 저장하지 않게 하기 위하여, Message 3을 수신 한 후, PTK를 획득할 수 있도록 한다. 첫 번째 방법은 AP가 Message 3에 추가적인 인자를 삽입하는 것 이며, 두 번째 방법은 쿠키〔11〕의 개념을 사용하는 것이다.

4.1 AP가 Snonce를 전송

4-way handshake blocking을 막는 첫 번째 해결책은 〔그림 4〕와 같이 AP가 Message 2를 통해 획득한 SNonce를 Message 3에 삽입하여 전송해 주는 것이다. 이에 대한 자세한 설명은 다음과 같다.

Message 1을 받은 단말은 기존의 4way-handshake와 동일하게 PTK를 생성하고 Message 2를 AP에게 전송한다. 즉, PTK는 다음 식과 같이 생성된다.

PTK = PRF-512 (PMK, "pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || ANonce || SNonce).

그러나 단말은 AP가 전송한 ANonce와 생성된 PTK를 저장하지 않고, 메모리에서 지운다. Message 2를 받은 AP는 PTK를 생성하고, Message 2의 MIC 검증을 통해 단말의 PMK 소유 여부를 확인한다. 이 때, Message 2에 포함된 MIC는 SPA, SNonce, sn의 무결성을 증명하기 위한 것이며, MIC는 이 메시지들을 PTK로 암호화 한 결과값이다. 이 후, AP는 단말이 전송한 SNonce를 Message 3에 삽입하여 다시 단말에게 전송한다. 한편, Message 3에는 기존 802.11i와 달리 sn 대신 sn+1이 포함된다. 이는 공격자에 의한 재전송 공격(replay attack)의 가능성을 완전히 제거하기 위함이다. 즉, Message 2를 수신한 공격자가 해당 메시지를 Message 3을 수신한 단말은 PTK를 다시 생성하게 되고, Message 3의 MIC 검증을 통해 AP가 단말과 같은 PMK를 소유 하고 있음을 확인한다. MIC의 검증이 정상적으로 이루어진다면 해당 PTK를 설치하고, Message 4를 AP에게 전송한다.

AP가 세 번째 메시지를 통해 ANonce, SNonce, AA 모두를 전송해주기 때문에 기존 4-way handshake의 메모리 소모를 제거할 수 있다. Message 3이 수신되면, 단말은 SPA와 PMK를 알고 있기 때문에 PTK를 생성하기 위한 5가지 인자를 모두 확보하게 된다. 따라서 PTK를 다시 생성할 수 있게 되고, 이 PTK를 통해 Message 3의 MIC를 검증한다. 이 방식은 기존의 4-way handshake에 비해 PTK를 다시 생성하는 연산이 추가로 요구된다.

4.2 암호화된 PTK 전송

두 번째 해결책은 [그림 5] 와 같이 단말이 PTK를 저장하지 않고 쿠키로 만들어서 전송하는 방식이다. 이 방법 역시 앞에서 설명한 방법과 마찬가지로 단말이 Message 3를 수신한 이후에 PTK를 획득 할 수 있게 하여, 메모리 소모를 제거하였다. 이에 대한 자세한 설명은 다음과 같다.

Message 1을 받은 단말은 기존의 4-way handshake방식과 동일하게 PTK를 생성한다. PTK를 생성한 단말은 랜덤 값(sk)를 생성한다. sk는 단말만이 아는 비밀 값으로서 PTK를 암호화 하는데 사용된다. 단말은 sk로 PTK를 암호화한 쿠키를 Message 2에 포함시켜 보낸다. Message 2를 받은 AP는 단말과 동일하게 PTK를 생성하고, 2번째 메시지에서 받은 쿠키를 다시 Message 3에 포함시켜 전송한다. Message 3를 받은 단말은 자신의 비밀키로 쿠키를 복호화 하고, 복호화를 통해 획득한 PTK로 MIC를 검증한다. 이후 MIC의 검증이 정상적으로 이루어지면 해당 PTK를 설치한다.

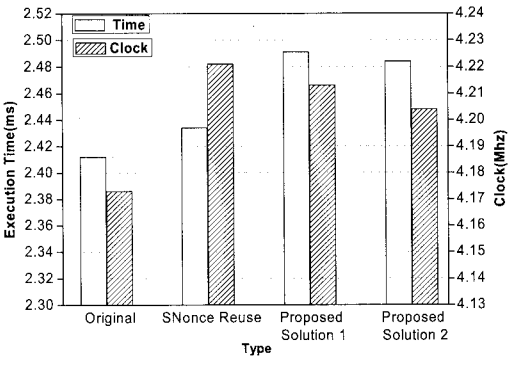
이 방식은 ANonce들과 해당 PTK들을 저장하지 않기 때문에, 메모리 소모를 제거할 수 있다. 다만, PTK를 암호화하고 복호화하는 추가적인 연산이 필요하며 단말의 비밀 키를 설정해줘야 한다.

V. 평 가

앞 장을 통해 기존 4-way handshake의 보안 취약점을 악용하여 발생하는 DoS 공격을 막을 수 있는 해결책들을 제안하였다. 제안한 해결책들은 공격을 막기 위해 추가적인 연산들이 요구 된다. 따라서, 본 장에서는 실제 무선랜 환경을 구성, 성능 측정을 통해 제안한 2가지 해결책들이 기존 4-way handshake와 비교하여 성능 저하가 거의 없음을 보여줄 것이다.

우리는 제안한 2가지 해결책, Changhua He 등이 제안하였던 SNonce Reuse[4] 그리고 기존 802.11i 4-way handshake를 직접 구현하여 성능 측정을 진행하였다.

기존 802.11i 4-way handshake에서 단말은 Message 1들이 수신 될 때마다 SNonce 값을 변경하며 새로운 PTK를 생성하였다. Changhua He 등이 제안하였던 SNonce Reuse 기법의 경우, SNonce 값이 변경되지 않도록 하여, 모든 Message 2에 포함되는 SNonce가 동일한 값을 갖도록 하였다. 즉, Message 1에 대한 메모리 할당을 하지 않게 하였다. 고정되어 있는 SNonce와 Message 3에 전송되어오는 ANonce를 이용, Message 3수신 후에 다시 PTK를 계산하는 방법이다.



[그림 6] 알고리즘별 clock 및 시간 비교

성능 측정을 위해 리눅스용 오픈 소스인 hostap[12] 와 xsupplicant[13] 를 표준 x86 processor에 설치하여, 실제 무선랜 환경을 구축하였다. Hostap는 무선랜의 AP의 기능을 수행하며, xsupplicant는 단말의 기능을 수행한다. SNonce Reuse 와 제안한 2개의 해결책의 구현을 위하여, xsupplicant와 hostap의 소스 코드들을 수정하였다. 이를 통해 새로운 802.11i 인증과정을 실시하였으며, 4-way handshake를 수행하는데 필요한 시간과 소모되는 clock을 단말 쪽에서 측정하였다. [그림 6] 은 측정된 시간과 clock 비교 결과를 보여준다. 각 알고리즘 별로 1200번을 수행하여 평균 값을 구하였으며, 실제 측정된 수치 값과 overhead는 [표 1] 에 나타나있다. 각 overhead는 기존 4-way handshake를 1로 놓고 계산하였다.

[표 1] 이 나타내는 바와 같이 논문에서 제안한 해결책들 모두 0.1ms이하의 추가적인 시간 overhead와 0.1Mhz이하의 추가적인 clock overhead를 가진다. 이러한 overhead는 기존 4-way handshake의 보안적 취약점을 제거하기 위해 추가적으로 필요한 연산으로 생기는 차이이며, 이는 기존 4-way handshake 전체 과정과 비교하여 매우 미비한 수준이다.

Changhua He등이 제안한 SNonce Reuse 같은 경우 제안한 해결책들과 비교하여 시간 측정에 있어서는 좀 더 나은 결과를 보여주지만, clock 측정에 있어서는 그렇지 않은 결과를 보여준다. 이러한 차이는 우리가 제안한 해결책들이 4-way handshake 내의 메시지에 새로운 값을 추가하여 메시지 길이가 길

어져 발생하는 차이이며, 전체적인 성능 면에서는 차이가 없다고 할 수 있다. 그러나 SNonce Reuse는 기존 4-way handshake 그리고 제안한 해결책들과 다르게 SNonce값이 고정되어 있어 key freshness를 보장하지 못하는 잠재적인 취약점이 존재하고, 이는 새로운 공격을 유도할 수 있다.

한편, 제안하는 해결책들의 보안성을 평가하면 다음과 같다. AP가 SNonce를 다시 전송해주는 해결책의 경우, 공격자가 SNonce를 도청하거나 변조하려고 시도할 수 있다. 그러나, SNonce는 랜덤 값 이외의 다른 의미를 갖지 않기 때문에 도청을 당하더라도 아무 의미가 없으며, 공격자가 SNonce를 변조할 경우 적절한 MIC를 생성할 수 없기 때문에 이는 공격자에게 아무런 의미가 없다. 암호화 된 PTK를 전송하는 해결책의 경우, PTK를 암호화 하는데 사용된 키가 단말만이 알고 있는 값이기 때문에, 공격자는 도청 및 변조를 수행할 수 없다. 따라서 제안하는 해결책은 DoS 공격을 차단할 수 있을 뿐 아니라, 그 의외의 측면에서 802.11i와 동일한 보안성을 갖는다.

제안하는 해결책들의 안전성 분석 결과는 다음과 같다. AP가 SNonce를 다시 전송해주는 해결책의 경우, 기존 802.11i 표준에 제시된 4-way handshake와 비교하였을 때, AP가 단말에게 송신하는 Message 3에 SNonce가 추가된 것을 제외하면 기존 4-way handshake와 동일하다. 따라서 본 해결책에서 Message 1, Message 2, Message 4는 기존 4-way handshake와 동일한 안전성을 갖는다. 한편, Message 3의 경우, 기존 4-way handshake에서 송신된 AA, ANonce, sn+1 뿐 아니라 본 해결책에서 추가된 SNonce도 모두 MIC를 이용하여 무결성을 보장한다. 제안하는 해결책에서 사용하는 MIC 알고리즘의 안전성은 기존 4-way handshake에서 사용되는 MIC 알고리즘을 그대로 사용하기 때문에, 기존 4-way handshake와 동일한 안전성을 갖는다. 결과적으로, AP가 SNonce를 다시 전송해주는 해결책의 경우, PTK를 모르는 공격자는 적절한 MIC를 생성하거나 변조할 수 없기 때문에, SNonce의 추가에 따른 메시지 위변조 등의 공격을 수행할 수 없다. 한편, SNonce는 아무 의미가 없는 난수이기 때문에, SNonce가 평문으로 노출되는 것은 어떠한 의미도 없으며 어떠한 프라이버시도 침해되지 않는다. 따라서 SNonce의 암호화는 불필요하다. 본 해결책에서 단말은 Message 3에 포함된 ANonce와 SNonce를 이용하여 PTK를 생성할 수 있기 때문에, PTK와 Nonce값들을 미리 저장하고 있을 필요가 없으며, 따라서 기존 4-way handshake에서 발생하는 메모리 고갈에 따른 서비스 거부 공격을 차단할 수 있다. 암호화 된 PTK를 전송하는 해결책의 경우, 기존 4-way handshake와 비교하면, Message 2와 Message 3에 E_{sk}(PTK)가 추가되었다. Message 2와 Message 3에는 각각 MIC가 포함되기 때문에, MIC의 검증에 사용되는 PTK를 모르는 공격자는 E_{sk}(PTK)를 위조하거나 변조할 수 없다. 제안하는 해결책에서 MIC 생성에 사용되는 알고리즘은 기존 4-way handshake에서 사용되는 MIC 알고리즘과 동일하기 때문에, 제안하는 해결책에서의 MIC의 안전성은 기존 4-way handshake와 동일하다. 그리고 E_{sk}(PTK)는 Advanced Encryption Scheme (AES) [14]과 같은 안전성이 검증된 대칭키 기반 암호화 알고리즘을 사용하여 PTK를 암호화 하는 함수를 의미한다. 이 때 암호화에 사용되는 대칭키 sk는 128비트 혹은 256비트의 크기를 갖으며, 이는 수많은 응용에서 안전성이 검증된 크기의 키 길이이다. 즉, 제안하는 해결책에서 사용하는 암호화 알고리즘은 안전성이 검증된 암호화 알고리즘과 키 길이를 사용함으로써, 학문적, 실용적으로 안전성이 검증되었다고 볼 수 있다. 본 해결책에서 단말은 기존 4-way handshake와 달리, 생성되는 PTK들과 Nonce값들을 모두 저장하고 있을 필요가 없으며, 대신 대칭키 sk 하나만 저장하고 있으면 Message 3을 통해 PTK를 추출할 수 있다. 즉, 제안하는 해결책에서는 다수의 PTK와 Nonce값들을 저장하는 대신 sk 하나만 저장함으로써, 단말의 메모리 고갈 문제를 방지할 수 있으며, 이를 통해 서비스 거부 공격을 차단할 수 있다.

VI. 결 론

802.11i는 기존 무선랜의 취약점을 제거하고 더 나은 보안을 제공하기 위해 제안되었다. 그러나 802.11i의 세션키 유도 과정인 4-way handshake에서의 보안 취약점이 발견되었으며, 본 논문에서는 이를 이용한 DoS 공격이 가능함을 보여주었으며 이를 막기 위한 2가지 해결책을 제시하였다. 제안한 해결책들은 기존의 802.11i의 4-way handshake와는 다르게 단말이 Message 3를 수신하고 PTK를 획득할 수 있게 하여 Message 1에 대해

〔표 1〕 알고리즘 별 성능 비교

Type	Time (ms)	Time overhead	Clock (Mhz)	Clock overhead
4-way handshake	2.412	1	4.173	1
SNonce reuse [4]	2.434	1.009	4.221	1.011
Proposed solution 1	2.491	1.032	4.213	1.009
Proposed solution 2	2.484	1.029	4.204	1.007

메모리를 할당하지 않게 하였다.

제안한 2가지 해결책과 SNonce Reuse[4]를 구현하여 실제 무선랜 환경을 구성하였으며, 이를 통해 4-way handshake의 수행에 필요한 시간과 소모되는 clock을 각각 측정, 비교하였다.

본 논문에서 우리는 실제 성능 측정을 통해 제안한 2개의 해결책이 기존의 4-way handshake와 비교하여 성능 차이가 거의 없음을 보여 주었다. 또한, 제안한 해결책들은 SNonce Reuse에서 제공하지 못하는 key freshness를 제공하면서도 기존의 4-way handshake에 가능한 DoS 공격을 막을 수 있음을 보여주었다.

참 고 문 헌

[1] M. Jagetia and T. Kocak, "A novel scrambling algorithm for a robust WEP implementation," Vehicular Technology Conference(VTC) 2004-Spring, pp. 2487-2491, May 2004.

[2] IEEE Computer Society, "Port-Based Network Access Control", IEEE Std 802.1X-2010, Feb. 2010.

[3] IEEE Computer Society, "Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specification : Medium Access Control(MAC) Security Enhancements", IEEE Std 802.11i/D4.1, Jul. 2003.

[4] Changhua He and John C. Mitchell, "Analysis of the 802.11i 4-Way Handshake," Proceeding of the Third ACM International Workshop on Wireless Security, pp. 43-50, Oct. 2004.

[5] Changhua He and John C. Mitchell, "Security analysis and improvements for IEEE 802.11i," The 12th Annual Network and Distributed System Security Symposium, pp. 90-110, Feb. 2005.

[6] Hayriye Altunbasak and Henry Owen, "Alternative Pair-wise Key Exchange Protocols for Robust Security Networks (IEEE 802.11i) in Wireless LANs," IEEE SoutheastCon, pp. 77-83, Mar. 2004.

[7] Romano Fantacci, Leonardo Maccari, and Tommaso Pecorella, "Analysis of Secure Handover for IEEE 802.1x-Based Wireless Ad Hoc Networks," Wireless Communications, vol. 14, no. 5, pp. 21-29, Oct. 2007.

[8] Jing Liu, Xinming Ye, Jun Zhang, and Jun Li, "Security verification of 802.11i 4-way handshake protocol," ICC 2008, pp. 1642-1647, May 2008.

[9] Kemal Bicakci and Bulent Tavli, "Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks," Computer Standards & Interfaces, vol. 31, no. 5, pp. 931-941, Sep. 2009.

[10] Sung-Hyun Eum, Sung-Jae Cho, Hyoung-Kee Choi, and Hyunseung Choo, "A Robust Session Key Distribution in 802.11i," ICCSA 2008, pp. 201-206, Jun. 2008.

[11] W. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, Aug. 2007.

[12] http://hostap.epitest.fi

[13] http://open1x.sourceforge.net

[14] C. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in a Public World, 2nd Ed., Upper Saddle River: Prentice Hall PTR, 2002, ch. 2-3.

〈著者紹介〉

김 정 윤 (Jung-Yoon Kim) 학생회원
2006년 8월: 성균관대학교 컴퓨터공학전공 학사졸업
2008년 2월: 성균관대학교대학원 전자전기컴퓨터공학과 석사졸업
2008년 3월~현재: 성균관대학교대학원 휴대폰학과 박사과정
〈관심분야〉 차량 간 통신 보안, Pay-TV 보안, 무선통신망 보안

김 인 환 (In-Hwan Kim) 정회원
2008년 2월: 성균관대학교 컴퓨터공학전공 학사졸업
2010년 2월: 성균관대학교대학원 전자전기컴퓨터공학과 석사졸업
2010년~현재: LG전자 연구원
〈관심분야〉 차량 간 통신 보안, 무선통신망 보안

최 형 기 (Hyoung-Kee Choi)
1992년 2월: 성균관대학교 전자공학과 학사졸업
1996년 2월: Polytechnic University in Brooklyn, NY 석사졸업
2001년 2월: Georgia Institute of Technology in Atlanta, GA 박사졸업
2001년~2004년: Lancope 근무
2004년 3월~현재: 성균관대학교 정보통신공학부 부교수
〈관심분야〉 네트워크보안, Traffic characterization and modeling