Mobile WiMAX 네트워크에서 공유 인증 정보를 이용한 분산 서비스 거부 공격 방어

정회원 김 영 욱*, 종신회원 박 세 웅*

Prevention Scheme of DDoS Attack in Mobile WiMAX Networks Using Shared Authentication Information

Youngwook Kim* *Regular Member*, Saewoong Bahk* *Lifelong Member*

요 약

메시지 인증 코드 (Message Authentication Code, MAC)는 메시지의 변조를 확인하기 위하여 사용되고 Mobile WiMAX 네트워크에서는 관리 메시지 (management message)의 인증을 위하여 Cipher-based 메시지 인증 코드 (Cipher-based MAC, CMAC)를 사용한다. 이 때 계산된 CMAC값 128 비트 중 하위 64 비트만을 사용하고 상위 64 비트 값은 잘라내어 사용하지 않는다. 본 연구에서는 이렇게 사용되지 않는 CMAC의 상위 64 비트를 공유 인증 정보 (Shared Authentication Information, SAI)라 하고 Mobile WiMAX 네트워크에서 유휴 모드 (idle mode) 상의 보안 취약점을 이용한 분산 서비스 거부 공격을 방어하는 수단으로 사용한다. 공유 인증 정보는 CMAC 값 중 사용되지 않는 64 비트를 사용하는 것이기 때문에 CMAC 값과 같은 보안성을 제공하며 CMAC 값을 계산하는 과정에서 얻을 수 있기 때문에 추가적인 계산이 필요 없다. 또한 사용하기 전까지 무선 구간에서 전송되지 않아 노출될 염려가 없으며 CMAC 키를 아는 기지국, 접근 서비스망 게이트웨이 (Access Service Network Gateway, ASN GW), 무선 단말 사이에서만 공유되기 때문에 안전하다. 이런 특성들로 인하여 공유 인증 정보는 분산 서비스 거부 공격 시에 기지국과 접근 서비스망 게이트웨이의 부하를 줄임으로써 효율적으로 분산 서비스 거부 공격을 방어할 수 있다.

Key Words : Mobile WiMAX, idle mode, CMAC, DDoS, SAI

ABSTRACT

Message Authentication Code (MAC) assures integrity of messages. In Mobiel WiMAX, 128-bit Cipher-based MAC (CMAC) is calculated for management messages but only the least significant half is actually used truncating the most significant 64 bits. Naming these unused most significant 64bits Shared Authentication Information (SAI), we suggest that SAI can be applied to protect the network from DDoS attack which exploits idle mode vulnerabilities. Since SAI is the unused half of CMAC, it is as secure as 64bits of CMAC and no additional calculations are needed to obtain it. Moreover, SAI doesn't have to be exchanged through air interface and shared only among MS, BS, and ASN Gateway. With these good properties, SAI can efficiently reduce the overheads of BS and ASN GW under the DDoS attack.

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업 [2008-F-007-01, 3차원 환경에서의 지능형 무선 통신 시스템]과 대학 IT연구센터 지원사업 [IITA-2008-C1090-0803-0004]의 일환으로 수행하였음.

* 서울대학교 전기컴퓨터공학부, 뉴미디어통신공동연구소 (kiyewo@netlab.snu.ac.kr, sbahk@snu.ac.kr),

논문번호 : KICS2007-11-510, 접수일자 : 2007년 11월 13일, 최종논문접수일자 : 2008년 11월 27일

Ⅰ. 서 론

Mobile WiMAX와 같은 패킷 중심의 광대역 무선 시스템에서 발생할 수 있는 분산 서비스 거부 (Distributed Denial of Service, DDoS) 공격에 대한 연구는 아직 초기 단계에 있다. Mobile WiMAX 네트워크가 아직 설치 초기 단계일 뿐 아니라 기존의 셀룰러 네트워크들은 전화가 주요 서비스 대상이었기 때문에 분산 서비스 거부 공격을 할 수 있는 충분한 여건이 되지 않았다. 하지만 Mobile WiMAX 네트워크는 핸드폰, PDA, 랩탑과 같은 여러 종류의 단말을 대상으로 전화뿐 아니라 다양한 데이터 서비스를 제공하며 수율 (throughput) 또한 기존의 무선 데이터 망에 비하여 크게 향상되었다. 따라서 Mobile WiMAX 네트워크가 보편화되고 이를 이용한 데이터 통신이 늘어나면 광대역 무선 네트워크에서도 유선망에서 문제가 되었던 분산 서비스 거부와 같은 형태의 공격이 발생할 수 있으며 광대역 무선 네트워크가 보편화되기 시작하는 현 시점에서 이러한 문제를 살펴보고 이에 대한 대비를 하는 것이 필요하다.

현재까지 무선 네트워크에서의 분산 서비스 거부 공격에 대한 연구는 802.11 네트워크 혹은 ad-hoc 네트워크를 중심으로 활발히 이루어졌다. Bellardo와 Savage는 802.11 네트워크에서 인증 해제 (Deauthentication)와 가상 반송파 감지 (virtual carrier sensing)를 이용한 분산 서비스 거부 공격을 실험을 통해 입증하고 그 효과를 감소시키기 위해 '인증 해제' 메시지를 큐잉하거나 Network Allocation Vector (NAV)값의 범위를 제한하는 방식을 제안하였다[1]. Gupta, et al.은 혼잡(congetstion)에 기반한 매체 접근 제어 (Medium Acces Control, MAC) 계층 분산 서비스 거부 공격을 무선 ad-hoc 네트워크에서 연구하고 MAC 계층에서의 공정성 (fairness)을 이용하여 이 공격을 완화시키는 방법을 제시하였다[2].

무선 네트워크 프로토콜의 보안 취약점을 이용한 공격에 대한 연구와 무선 네트워크에서 보안 프로토콜이 서비스 품질 (Quality of Service, QoS) 등에 미치는 영향에 대한 연구도 진행되었다. Zhang과 Fang은 3GPP -AKA (3rd Generation Partnership - Authentication and Key Agreement) 인증 프로토콜의 보안 취약점을 분석하여 가짜 기지국 (false BS)을 통한 공격 가능성을 제시하였다 [3]. 한편 Liang과 Wang은 무선 네트워크에서 인증 과정이 QoS에 미칠 수 있는 영향을 인증 부하 (Authentication cost)의 측면과 인증 지연 (Authentication delay)의 측면에서 대기이론 (Queueing Theory)을 적용하여 분석하였다 [4].

하지만 이들 논문은 802.11 이나 ad-hoc 네트워크와 같이 중앙 관리자가 없는 무선 네트워크에서의 공격을 연구하거나 셀룰러 네트워크와 같이 전화서비스가 중심인 네트워크에서 보안 취약점이나 보안이 미치는 영향을 연구하였다.

본 논문에서는 광대역 무선 네트워크인 Mobile WiMAX 네트워크에서 일어날 수 있는 분산 서비스 거부 공격을 제시하고 이에 대한 방어 방법을 제안할 것이다.

본 논문은 다음과 같이 구성되어 있다. 섹션 II에서는 배경 지식을 설명한다. 섹션 III에서는 Mobile WiMAX 네트워크에서 발생할 수 있는 기지국 (Base Station, BS)와 접근 서비스망 게이트웨이 (Access Service Network Gateway, ASN GW)에 대한 분산 서비스 거부 공격을 설명하고 섹션 IV에서 이에 대한 해법으로 공유 인증 정보 (Shared Authentication Information, SAI)를 제안한다. 섹션 V에서 제안된 방법의 성능을 살펴보고 섹션 VI에서 결론을 맺는다.

Ⅱ. 배 경 지 식

2.1 Mobile WiMAX 네트워크 참조 모델

Mobile WiMAX 네트워크는 802.16e 표준을 기반으로 도심 지역에서 종단 연결(last mile access)을 위한 광대역 무선 접속 (BWA: Broadband Wireless Access) 시스템이다. 그림 1은 Mobile WiMAX 네트워크의 참

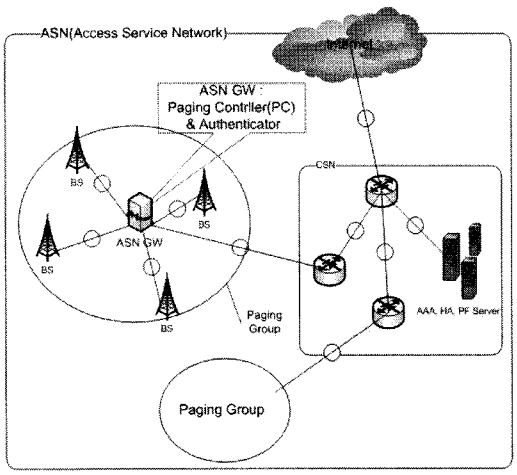


그림 1. Mobile WiMAX 네트워크 참조 모델

조 모델로 접근 서비스망 (Access Service Network, ASN)과 연결 서비스망 (Connectivity Service Network, CSN)으로 구성되어 있다. 접근 서비스망은 이동 단말에 무선 접속 서비스를 제공해 주기 위한 네트워크 구조로서 기지국과 접근 서비스망 게이트웨이로 구성되어 있다. 접근 서비스망 게이트웨이는 기지국들을 연결 서비스망으로 연결해 주는 역할을 하며 접근 서비스망 게이트웨이 프로파일 (Profile)에 의해 그 기능이 정의 내려진다. 본 논문에서는 프로파일 A 혹은 C를 참조하여 인증매개자 (Authenticator)와 페이징 제어기 (Paging Controller, PC) 기능이 접근 서비스망 게이트웨이에 있다고 가정한다.

2.2 인증매개자 (Authenticator)

Mobile WiMAX 네트워크에서 인증매개자는 인증 서버와 이동 서비스 가입자 (Mobile Subscriber, MS) 사이에서 인증을 대행해 주는 역할을 한다. 즉, 이동 서비스 사용자가 처음 네트워크에 진입하여 인증서버와 인증을 마치면 이 사용자의 인증 정보는 인증매개자에 저장되어 있다가 사용자가 다른 기지국으로 이동하거나 하는 경우에 새 기지국에 인증키 컨텍스트 (Authentication Key context, AK context)를 포함한 사용자의 인증 정보를 알려주는 역할을 한다.

2.3 페이징 제어기 (Paging Controller, PC)와 유휴 모드 (idle mode)

페이징 제어기는 이동 서비스 가입자의 유휴 모드를 지원한다. 유휴 모드 이동 서비스 가입자를 지원하기 위해 각 기지국들은 페이징 그룹 (Paging Group)이라는 논리적인 그룹으로 나누어진다. 페이징 제어기는 바로 이 페이징 그룹 내의 기지국들을 관리하고 유휴 모드에 있는 이동 서비스 가입자들의 목록을 저장하며 이들을 페이징할 필요가 있으면 이동 서비스 가입자가 속해 있는 페이징 그룹 내의 기지국들에게 페이징하도록 지시하는 역할을 한다. 그림 1에서 접근 서비스망 게이트웨이를 중심으로 여러 개의 기지국들이 하나의 페이징 그룹으로 묶여 있으며 접근 서비스망 게이트웨이는 페이징 제어기로서 이 기지국들을 관리한다.

2.4 Cipher-based MAC (CMAC)과 공유 인증 정보

Mobile WiMAX에서는 관리 메시지의 무결성을 보장하기 위해 CMAC을 사용하며 그림 2와 같이 계산된다.

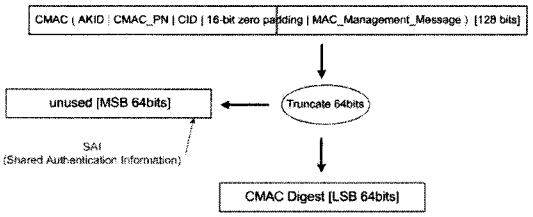


그림 2. CMAC 값의 계산과 공유 인증 정보

그림 2에서 보면 CMAC 알고리즘을 사용하여 계산한 결과 값은 128 비트이다. 하지만 802.16e 표준에서는 이 128 비트 중에서 하위 64 비트만 잘라내어 CMAC 값으로 사용하고 상위 64 비트는 사용하지 않는다. 본 논문에서는 이 버려지는 상위 64 비트를 공유 인증 정보 (Shared Authentication Information, SAI)라 부르고 이를 이용하여 Mobile WiMAX 네트워크에서 발생할 수 있는 분산 서비스 거부 공격을 방어할 것이다.

Ⅲ. 기지국과 접근 서비스망 게이트웨이에 대한 분산 서비스 거부 공격

Mobie WiMAX 네트워크에서 위치 갱신 (Location Update, LU)을 하는 유휴 모드 이동 서비스 가입자는 Ranging 구간에서 ranging code를 전송하고 대역폭을 할당받아 RNG-REQ 메시지를 전송한다. 이 때 대역폭을 할당하는 과정에서 이동 서비스 가입자에 대한 인증을 따로 하지 않기 때문에 임의의 이동 서비스 가입자가 대역폭을 할당 받아 사용할 수 있다. 이러한 프로토콜 상의 취약점을 이용하여 악의적인 이동 서비스 가입자는 기지국 및 접근 서비스망 게이트웨이의 자원을 악용할 수 있다.

먼저 Mobile WiMAX에서 관리 메시지의 CMAC 검증 과정을 알아보자. CMAC 값을 검증하기 위해서는 기지국과 이동 서비스 가입자 사이에 CMAC 키를 포함한 이동 서비스 가입자의 인증키 컨텍스트가 공유되어야 한다. 기지국은 이러한 정보를 인증매개자로부터 받아온다. 즉 기지국은 페이징 제어기를 통해 인증매개자에게 인증키 컨텍스트를 요청하고 인증매개자는 이동 서비스 가입자의 인증키 컨텍스트를 생성하여 페이징 제어기에 전송한다. 페이징 제어기는 이를 기지국에 전송하고 기지국은 CMAC 값을 계산하여 검증하게 된다.

따라서 위 취약점을 이용하여 대역폭을 할당 받은 악의적인 이동 서비스 가입자가 CMAC을 포함

한 RNG-REQ 메시지를 조작하여 전송하면 CMAC을 검증하는데 기지국과 접근 서비스망 게이트웨이(인증매개자와 페이징 제어기)의 자원을 악용할 수 있다.

기지국은 수십 혹은 수백 대의 이동 서비스 가입자를 관리하며 접근 서비스망 게이트웨이는 다시 몇몇의 기지국을 관리하므로 접근 서비스망 게이트웨이는 수 백 혹은 수천 대의 이동 서비스 가입자를 관리하게 된다. 따라서 다수의 악의적인 이동 서비스 가입자가 RNG-REQ 메시지를 조작하여 전송한다면 기지국과 접근 서비스망 게이트웨이의 자원 중 상당 부분이 이런 메시지를 처리하는 데 소비되는 분산 서비스 거부 공격으로 이어질 수 있다.

Ⅳ. 공유 인증 정보

본 장에서는 공유 인증 정보를 접근 서비스망 게이트웨이와 이동 서비스 가입자사이의 인증정보로 이용하여 분산 서비스 거부 공격을 방어하는 방법을 설명한다. 공유 인증 정보는 이동 서비스 가입자와 기지국이 주고받은 관리 메시지의 CMAC을 계산하는 과정에서 이동 서비스 가입자와 기지국이 각자 CMAC의 남은 부분을 이용하는 것이기 때문에

1) 공유 인증 정보를 얻기 위한 추가적인 계산이 필요 없다.

또한 이동 서비스 가입자와 기지국은 관리 메시지만 주고받으면 이 메시지의 CMAC을 통해 각자 공유 인증 정보를 얻을 수 있기 때문에

2) 공유 인증 정보를 이동 서비스 가입자와 기지국이 공유하기 위해 무선 인터페이스 상으로 공유 인증 정보를 직접 교환할 필요가 없다.

3) 이동 서비스 가입자와 기지국이 주고받는 메시지의 CMAC 값을 계산할 수 없는 다른 네트워크 개체들은 이 값을 알 수 없다.

4) CMAC의 사용되지 않는 64 비트를 사용한 것이므로 CMAC과 동등한 보안성을 보장한다..

5) 공유 인증 정보를 관리 메시지에 TLV (Type, Length, Value)로 추가할 수 있어 표준에 변화 없이 구현할 수 있다.

는 장점이 있다. 본 연구에서는 위치 갱신 과정에서 공유 인증 정보를 이용하는 분산 서비스 거부 공격을 방어한다. 구체적인 절차는 다음과 같다.

4.1 공유 인증 정보를 이용한 분산 서비스 거부 공격 방어

4.1.1 공유 인증 정보 저장

유휴 모드로의 진입은 이동 서비스 가입자가 DREG-REQ 메시지를 기지국으로 전송하거나 기지국이 DREG-CMD 메시지를 이동 서비스 가입자에 전송함으로써 시작된다. 이동 서비스 가입자가 유휴 모드를 시작하는 경우는 이동 서비스 가입자가 먼저 DREG-REQ 메시지를 기지국에 전송하고 기지국이 이에 대한 응답으로 DREG-CMD 메시지를 보낸다. 반면 네트워크가 시작되는 유휴 모드로의 진입은 기지국이 DREG-CMD 메시지를 보내고 이동 서비스 가입자가 이에 대한 응답으로 DREG-REQ 메시지를 보낸다. 따라서 공유 인증 정보값을 얻기 위한 메시지로 이동 서비스 가입자가 시작하는 유휴 모드 진입 과정에서나 기지국이 시작하는 유휴 모드 진입 과정에서 공통적으로 사용되는 DREG-REQ와 DREG-CMD 메시지를 이용할 수 있다. 여기서는 설명의 편의를 위해 이동 서비스 가입자가 시작하는 유휴 모드에서 DREG-REQ 메시지를 이용하는 경우를 예로 들어 설명한다. 이동 서비스 가입자가 시작하는 유휴 모드 진입과정의 경우 이동 서비스 가입자는 DREG-REQ 메시지를 보내면서 계산한 CMAC 값의 상위 64 비트를 공유 인증 정보로 저장해두고 나머지 하위 64 비트를 CMAC 값으로 붙여서 보낸다. 기지국은 수신한 DREG-REQ 메시지를 검증하면서 이에 대한 CMAC 값을 계산하게 되고 이 중 하위 64 비트를 먼저 DREG-REQ에 포함된 CMAC 값과 비교하여 DREG-REQ 메시지를 검증하고 이상이 없으면 상위 64 비트를 공유 인증 정보로 저장한다.

기지국은 이동 서비스 가입자의 등록 해지 정보(De-Registration)를 MS-info REQ 메시지로 페이징 제어기에 전송하면서 자신이 저장하고 있는 이동 서비스 가입자의 공유 인증 정보값을 이동 서비스 가입자의 MAC 주소와 같이 전송한다. 페이징 제어기는 이 값을 저장하고 있다가 검증 단계에서 이용한다. 한편 페이징 제어기는 MS-info REQ 메시지를 처리하고 등록 해지를 요청한 이동 서비스 가입자에 대한 결과를 MS-info RSP로 기지국으로 전송한다. 기지국은 이 결과를 DREG-CMD 메시지를 통해 이동 서비스 가입자에 보낸다. 이동 서비스 가입자는 DREG-CMD 메시지를 수신하고 유휴 모드로 진입하게 된다.

4.1.2. 공유 인증 정보 전송

공유 인증 정보 저장 단계에서 이동 서비스 가입자와 페이징 제어기는 공유 인증 정보를 서로 공유하였다. 이러한 상태에서 유휴 모드에 있던 이동 서비스 가입자는 주기적으로 깨어나서 RNG-REQ 메시지와 RNG-RSP 메시지를 이용하여 위치 갱신을 수행한다. 이 때 공유 인증 정보를 TLV로 포함하여 RNG-REQ 메시지를 전송한다.

4.1.3 공유 인증 정보 검증

이동 서비스 가입자가 보낸 RNG-REQ 메시지를 받은 기지국은 이 메시지에 포함되어 있는 공유 인증 정보를 페이징 제어기에 전송하여 1 단계에서 저장된 공유 인증 정보값과 비교 한다. 이동 서비스 가입자가 이동하여 다른 기지국에서 안전한 위치 갱신(Secure Location Update)을 진행하고 다시 기존의 기지국으로 돌아온 경우 기존의 기지국이 가지고 있는 공유 인증 정보값은 잘못된 값이 되므로 정확한 공유 인증 정보값의 검증을 위해 공유 인증 정보의 검증은 페이징 제어기에서 이루어진다. 이 때 기지국과 페이징 제어기 사이의 정보 교환은 LU REQ와 LU RSP 를 통해 이루어진다. 페이징 제어기는 전송되어온 공유 인증 정보값이 자신이 저장하고 있는 공유 인증 정보값과 같은지를 판단하여 이 값이 같으면 인증매개자에 인증키 컨텍스트를 요청하고 이를 받아와 기지국으로 전송하고 같지 않다면 인증 실패를 알리는 메시지를 전송한다.

4.1.4 공유 인증 정보의 갱신

한 번 사용된 공유 인증 정보는 RNG-REQ 메시지에 평문으로 전달되었기 때문에 다음번에 그 값을 그대로 사용할 수 없다. 위치 갱신 도중 공유 인증 정보의 갱신은 RNG-RSP 메시지를 이용하여 이루어진다. 위치 갱신을 하는 이동 서비스 가입자는 RNG-REQ 메시지를 전송하고 그에 대한 응답으로 RNG-RSP를 받는다. 이 때 기지국은 RNG-RSP 메시지에 포함될 CMAC 값을 계산하는데 이 값의 상위 64 비트 값을 다음 번 위치 갱신을 위한 공유 인증 정보 값으로 사용한다. 따라서 기지국은 RNG-RSP 메시지를 보내면서 이 공유 인증 정보값을 페이징 제어기에 전송해야 하며 이동 서비스 가입자는 수신한 RNG-RSP의 CMAC 값을 계산하고 이 과정에서 상위 64 비트를 저장해야 한다. 그림 3은 공유 인증 정보의 저장, 전송, 검증 및 갱신이 이루어지는 과정을 나타낸다.

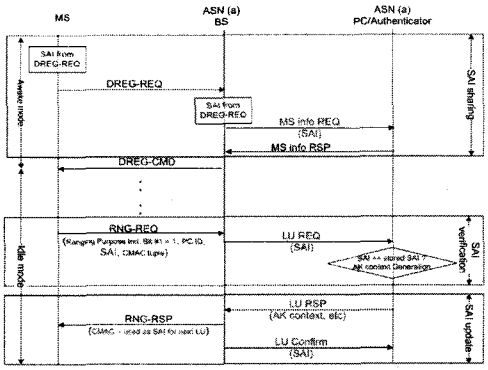


그림 3. 공유 인증 정보 저장, 전송, 검증 및 갱신

V. 모의실험 결과 및 분석

본 장에서는 공유 인증 정보를 사용하여 얻게 되는 효과를 CMAC 생성부하, 전송 부하 및 인증키 컨텍스트 생성 부하 측면에서 분석하고 이를 통해 향상되는 네트워크 지연시간을 계산한다.

5.1 모의실험 환경

본 연구에서는 공격 상황에서 공유 인증 정보를 사용함으로써 얻을 수 있는 기지국과 접근 서비스망 게이트웨이의 부하 감소와 정상 상황에서 공유 인증 정보를 사용함으로써 나타나는 기지국과 접근 서비스망 게이트웨이의 부하 증가를 시뮬레이션을 통해 알아보고 공유 인증 정보를 구현하지 않았을 때의 부하와 비교해 보았다. 이를 위해 AES128-CMAC 알고리즘과 dot16KDF 함수 (인증키 컨텍스트 생성에 이용)를 C로 구현하고[5,6,7] Pentium CPU의 rdtsc 명령어를 사용하여 이들의 평균 부하를 CPU 클록 주기 (clock cycle)로 측정하였다. 평균값은 각 부하를 1000번씩 반복하여 측정한 것이다. 모의실험에 사용된 환경을 표 1에 정리하였다.

표 1. 시뮬레이션 환경

인자 (parameter)	값
CPU	Pentium IV 2.4 GHz
Memory	512 MB
OS	Windows XP
RNG-REQ Message Size	64 바이트
block cipher	AES
AES key size	128 비트
C compiler	lcc v4.0
모의실험 코드	
AES algorithm	Linux WPA/WPA2 supplicant[5]
CMAC algorithm	RFC 4493[6]
dot16KDF	David Johnston's home[7]

5.2 CMAC 생성 부하

CMAC을 생성하는데 필요한 CPU 클록 주기 (clock cycle) 수를 측정하기 위하여 임의의 64 바이트 RNG-REQ 메시지와 임의의 128 비트 키를 생성하고 CMAC을 계산하였다. 여기서 RNG-REQ 메시지의 크기는 실제 RNG-REQ 메시지의 크기와 AES 블록의 크기를 고려하여 64 바이트로 정하였다. 측정 결과 20116 주기 (cycle)가 필요했다 (2.4 GHz CPU에서 8.4 us).

5.3 전송 부하

기지국 혹은 접근 서비스망 게이트웨이가 메시지를 전송하는 부하를 측정하기 위하여 64 바이트의 임의의 메시지를 생성하여 Windows Socket을 통해 전송하고 이 때 필요한 CPU의 클록 주기 수를 측정하였다. Mobile WiMAX에서는 기지국과 접근 서비스망 게이트웨이 사이의 전송 프로토콜 (transport protocol)로 UDP를 사용한다.

전송부하는 메시지를 커널의 송신 버퍼에 저장하는데 걸리는 시간, 전송 시간 (transmission time)과 전송 지연 (propagation delay)으로 계산할 수 있으며 메시지를 커널의 송신 버퍼(send buffer)에 저장하는데 72009 주기가 필요하였다 (2.4 GHz CPU에서 30 us). 전송 시간은 기지국과 접근 서비스망 게이트웨이가 100Mbps ethernet으로 연결되어 있다고 가정하고 공유 인증 정보를 구현한 경우와 구현하지 않은 경우로 나누어 LU REQ, LU RSP의 전송 시간을 계산하였다. LU REQ와 LU RSP는 공유 인증 정보를 구현하지 않은 경우 각각 44 바이트와 232 바이트이며 공유 인증 정보를 구현한 경우 56 바이트와 52 바이트이다. 여기에 Ethernet/IP/UDP 헤더를 포함하여 전송 시간을 계산하면 공유 인증 정보를 구현하지 않은 경우 각각 6.88us/21.92us가 되며 구현한 경우 7.84us/7.52us가 된다.

한편, 전파 지연은 접근 서비스망 게이트웨이와 기지국 간의 평균 거리를 12 Km로 가정하여 한 홉 당 40 us로 잡았다.[4]

따라서 총 전송부하는 30 + 6.88/7.84/21.92/7.52 + 40 = 76.88/77.84/91.92/77.52 us가 된다.

5.4 인증키 컨텍스트 생성 부하

인증키 컨텍스트는 이동 서비스 가입자의 AK, CMAC_KEY_U, CMAC_KEY_D, KEK, EIK 등으로 구성되어 있으며 이 중 AK, AKID, CMAC_KEY_U, CMAC_KEY_D, KEK 항목을 생성하는 부하를 측정하기 위하여 이들을 생성하고 이 때 필요한 CPU 클록 주기 수를 측정하여 표 2에 정리하였다.

표 2. 인증키 컨텍스트 생성 부하 비교

정상 상황			공격 시		
w/o SAI	w/ SAI	ratio	w/o SAI	w/ SAI	ratio
106423 (44.34us)	106530 (44.39us)	1.001	106423 (44.34us)	8 (0.003us)	0.001

정상적인 상황에서는 공유 인증 정보를 구현한 경우 접근 서비스망 게이트웨이에서 공유 인증 정보 값을 비교하는 추가 부하가 있으므로 구현하지 않은 경우에 비해 107 주기가 더 필요했으며 이는 인증키 컨텍스트를 생성하는데 필요한 클록 주기 수의 약 0.1%정도이다. 따라서 공유 인증 정보를 구현하더라도 정상적인 상황에서 크게 부하가 되지 않는다.

한편 공격 상황에서는 공유 인증 정보를 구현한 경우에는 공유 인증 정보 값을 비교하는 연산만을 수행하게 되지만 공유 인증 정보를 구현하지 않은 경우는 인증키 컨텍스트를 생성하게 되므로 CPU 클록 주기 수에 큰 차이를 보였다. 공유 인증 정보를 구현하지 않은 경우에는 106423 주기를 소모하는 반면 구현한 경우에는 이의 0.1%에 해당하는 8 주기만을 소모하였다. 따라서 공유 인증 정보는 공격 시에 효과적으로 접근 서비스망 게이트웨이를 보호할 수 있다.

5.5 총 부하 비교

본 절에서는 공유 인증 정보를 구현한 시스템과 공유 인증 정보를 구현하지 않은 시스템의 부하를 비교해 본다. 시스템의 부하는 기지국 부하와 접근 서비스망 게이트웨이 부하의 합으로 표현하였다.

공격 상황에서 공유 인증 정보를 구현하지 않은 경우 인증키 컨텍스트를 생성 부하와 CMAC 검증 부하를 모두 받는 반면 공유 인증 정보를 구현한 경우 이러한 부하를 줄일 수 있다. 이를 정리하면 표 3과 같다.

표 3. 공격 상황에서의 공유 인증 정보 부하 비교

공격 시	
w/ SAI	BS 부하 : 77.84 us ASN GW 부하 : 0.003+77.52 = 77.523 us Total 부하 : 77.84+77.523 = 155.363 us
w/o SAI	BS 부하 : 76.88 + 8.4 = 85.28 us ASN GW 부하 : 44.34+91.92 = 136.26 us Total 부하 : 85.92+136.26 = 221.54 us
ratio	155.363 / 221.54 * 100 % = 70.13%

표 4. 정상 상황에서의 공유 인증 정보 부하 비교

정상 상황	
w/ SAI	BS 부하 : 77.84+8.4 = 86.24 us ASN GW 부하 : 91.92+44.39 = 136.31 us Total 부하 : 86.24+136.31 = 222.55 us
w/o SAI	BS 부하 : 76.88 + 8.4 = 85.28 us ASN GW 부하 : 44.34+91.92 = 136.26 us Total 부하 : 85.92+136.26 = 221.54 us
ratio	222.55 / 221.54 * 100 % = 100.46%

표 3를 보면 공격 상황에서 공유 인증 정보를 구현한 경우의 부하가 공유 인증 정보를 구현하지 않은 경우에 비하여 약 29.87% 가량 감소함을 알 수 있다.

한편 정상적인 상황에서 공유 인증 정보를 구현하지 않은 경우의 부하는 공격 상황에서 공유 인증 정보를 구현하지 않은 경우와 같으며 공유 인증 정보를 구현한 경우는 여기에 공유 인증 정보를 검증하는 부하만이 더해진다.

표 4을 보면 정상적인 상황에서 공유 인증 정보를 구현하더라도 총 부하는 원래의 시스템 부하의 약 0.46%만 증가하는 것을 알 수 있다. 따라서 공유 인증 정보는 정상적인 상황에서 추가적인 부하가 거의 없음을 알 수 있다.

VI. 결 론

본 논문은 Mobile WiMAX 네트워크에서 유휴 모드 상태에 있는 단말들에 의한 분산 서비스 거부 공격 가능성을 염두에 두고 이를 방어하기 위한 방법으로 공유 인증 정보를 제시하였다.

공유 인증 정보는 CMAC의 사용되지 않는 부분을 이용하기 때문에 공유 인증 정보 값을 얻는데 추가적인 계산이 필요치 않으며 이동 서비스 가입자와 기지국 사이에 공유하기 위해 무선 인터페이스 상으로 전송할 필요가 없다. 또한 간단한 비교만으로 이동 서비스 가입자의 인증이 가능하기 때문에 평상시에도 CPU에 거의 부하를 주지 않으며 공격 시에는 효과적으로 공격을 차단할 수 있다.

참 고 문 헌

[1] J. Bellardo, S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Usenix 2003, June 2005.

[2] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial-of-Service Attacks at the MAC Layers in Wireless Ad Hoc Networks," MILCOM 2002, October 2002.

[3] M. Zhang, Y. Fang, "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans. on WIRELESS COMMUNICATIONS Vol. 4 No. 2, pp. 734-742, March 2005.

[4] W. Liang, W. Wang, "Quantitative Study of Authentication and QoS in wireless IP networks," INFOCOM 2005, March 2005.

[5] <http://hostap.epitest.fi/wpa_supplicant/>

[6] J. H. Song, R. Poovendran, J. Lee, and T. Iwata, "The AES-CMAC Algorithm," RFC 4493, June 2006.

[7] <https://www.deadhat.com/wmancrypto/>.

[8] "WiMAX End-to-End Network Systems Architecture - Stage 3: Detailed Protocols and Procedures," WiMAX Forum, August 2006.

[9] "Standard for Local and Metropolitan area networks- Part16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," IEEE Std 802.16e-2005, February 2006.

[10] "Standard for Local and Metropolitan area networks- Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE std 802.16-2004, October 2004.

[11] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," NIST Special Publication 800-38B, May 2005.

[12] J. Arkko, H. Harverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement(EAP-AKA)," IETF RFC 4187, January 2006.

[13] Y. Kim, H. Lim, and S. Bahk, "SAI: Shared Authentication Information for Preventing DDoS attacks in Mobile WiMAX Networks," CCNC 2008, January 2008.

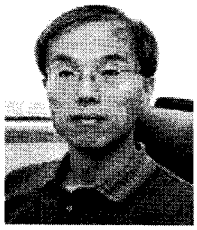
김 영 욱 (Youngwook Kim) 정회원

2003년 서울대학교 전기공학부 학사

2009년~현재 서울대학교 전기컴퓨터공학부 석박사 통합과정

<관심분야> 프로토콜 보안, 무선 네트워크

박 세 웅 (Saewoong Bahk) 종신회원



1984년 서울대학교 전기공학과 학사

1986년 서울대학교 전기공학과 석사

1991년 Univ. of Pennsylvania 박사

1991년~1996년 AT&T Bell Lab.

1994년~현재 서울대학교 전기컴퓨터공학부 교수

<관심분야> 차세대 무선 네트워크, 네트워크 보안