차세대 전술정보통신체계에서의 무선 메쉬 MSAP 노드 간 상호 인증 기법

준회원 손 유 진*, 배 병 구*, 정회원 손 태 식*, 고 영 배*, 임 광 재**, 윤 미 영**

Mutual Authentication Method between Wireless Mesh Enabled MSAPs in the Next-generation TICN

Yu-Jin Son*, Byoung-Gu Bae* *Associater Members*,
Taeshik Shon*, Young-Bae Ko*, Kwang Jae Lim**, Mi-Young Yun** *Regular Members*

요 약

차세대 전술정보통신체계(TICN)에서 전술이동통신체계는 이동통신가입자처리부(MSAP)에 포함된 전술용 다기능 단말기(TMFT)의 지휘 통제 및 통신 수단을 제공하는 역할을 한다. 차기 이동통신가입자처리부는 고정 지향성 안테나인 LCTR(Low Capacity Trunk radio)과 HCTR(High Capacity Trunk Radio)을 통해 기간망을 구성할 수 있고, WMN(Wireless Mesh Network) 모듈을 통해 무선 메쉬망을 형성하여 상호운용 된다. 즉, 이동 중에 끊김 없는 데이터 송·수신을 지원하기 위해서 MSAP간 WMN 모듈을 사용하여 망을 구성한다. 이러한 환경에서 신뢰성 있는 데이터 전송을 보장하기 위하여 단말 간 상호 인증을 수행하고 데이터를 암호화 할 수 있는 기술이 필요하다. 본 논문에서는 MSAP 단말간 인증서버를 통해 분산적으로 인증을 수행하여 보다 비용과 효율성 측면에서 장점을 갖는 상호 인증 기법을 제안한다.

Key Words : IEEE 802.16m, EAP-TLS, Distributed Authentication, 전술이동통신체계

ABSTRACT

The tactical mobile communication network, which comprises a part of the next-generation Tactical Information and Communication Network (TICN), provides means of communication and control for Tactical Multi-Functional Terminals (TMFT) belonging to a Mobile Subscriber Access Point (MSAP). The next-generation of MSAP is capable of constructing a backbone network via LCTR and HCTR directional antennas. At the same time, WMN modules are used to create and manage a wireless mesh backbone. When directional antennas are used in mobile environments, seamless services cannot be efficiently supported as the movement of the node prevents the angle of the antenna to constantly match. Therefore, data communication through the wireless mesh networks is required to provide direct communication between mobile MSAPs. Accordingly, mutual authentication and data encryption mechanisms are required to provide reliable data transmission in this environment. To provide efficient mutual authentication between MSAP devices, the process of verifying a certificate of the other MSAP device through its own authentication server is required. This paper proposes mutual authentication mechanisms where the MSAP requiring authentication and the MSAP that permits it initiates low-cost and efficient authentication in a distributed

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2012-(H0301-12-2003))
* 아주대학교 컴퓨터 공학과 유비쿼터스 네트워크 시스템 연구실({yujin, byounggu}@uns.ajou.ac.kr, {tsshon, youngko}@ajou.ac.kr)
** ERTI 한국전자통신연구원 모바일응용통신연구팀({kjlim, myyun}@etri.re.kr)
논문번호 : KICS2011-11-570, 접수일자 : 2011년 11월 30일, 최종논문접수일자 : 2012년 5월 7일

way. More specifically, we propose a method of applying EAP-ELS (Extensible Authentication Protocol-Transport Layer Security) in the next-generation TICN.

Ⅰ. 서 론

차세대 전술통신 체계인 전술정보통신체계(TICN: Tactical Information and Communication Network)는 실시간적으로 수집한 정보를 바탕으로 전장의 상황에 따라 빠른 대응 및 정보 전달을 할 수 있는 대용량 통신기반이다. TICN 체계를 구축하면 기간망의 무선전송용량이 현재 수준 대비 10배로 증가하고 가입자 데이터 단말의 무선전송용량도 수십 배 이상 늘어나게 될 것으로 예상된다.

현재 TICN 체계는 그림 1과 같이 기능에 따라 기간망 전송체계, 기간망 교환접속체계, 망제어체계, 전투무선망체계, 전술이동통신체계로 구분한다. 그 중에서 전술이동통신체계는 지휘소 내부 및 주변지역에 위치한 전술용다기능단말기(TMFT: Tactical Multi-Functional Terminal)에게 지휘 통제 및 통신 수단을 제공하는 것을 목적으로 한다. 이를 위하여 전술이동통신체계는 이동통신가입자처리부(MSAP: Mobile Subscriber Access Point)라는 교환 접속 체계를 활용하여 기동 중인 TMFT 단말이 다양한 음성 및 데이터 전송 등의 실시간 멀티미디어 서비스를 제공 받을 수 있는 기능을 지원해준다. MSAP은 이를 지원하기 위한 수단으로 기간망 교환접속체계인 소용량 무선전송체계(LCTR: Low Capacity Trunk Radio)와 대용량 무선전송체계(HCTR: High Capacity Trunk Radio)를 이용하여 외부 전송로를 구성한다[1]. 이러한 외부 전송로를 통하여 MSAP은 타 부대와의 정보를 교환할 수 있는 통신 수단을 구축할 수 있다. MSAP 단말과 TMFT 단말 간의 연결 및 통신은 WiBro(Wireless Broadband)기술을 활용하여 대대급 네트워크를 형성하게 된다[2].

기존의 전술이동통신체계에서 고정 지향성 안테나 방식인 LCTR과 HCTR로 통신망을 구성하는 경우 처리 성능은 보장될 수 있지만 실시간적으로 변화하는 상황에 빠른 대응을 할 수 없다는 문제점이 발생한다. 왜냐하면 지향성 안테나를 통해 구축된 무선전송체계는 신호의 접점을 만들기 때문에 신호는 강할 수 있으나, 일정 범위의 안테나 각도에서만 전송이 가능하기 때문에 항상 고정된 방향을 유지해야하는 문제점이 있기 때문이다. 그 결과, MSAP이 이동을 하거나 장애물 또는 지리적 특성으로 인하여 안테나의 지속적인 연결이 끊어지는 현상이 빈번히 발생하게 된다. 이러한 문제점들을 해결하기 위하여 차기 MSAP에서는 내부적으로 WMN (Wireless Mesh Network) 모듈을 추가하고 MSAP 간 메쉬망을 형성하여 이동 중에도 끊김 없는 서비스를 지원할 수 있도록 하는 방안이 고려되고 있다. 그림 2는 TICN에서의 차기 전술이동통신체계 구성도이다. 인증서버, 이동전술용라우터, 제어국(ACR)이 포함된 이동교환장비, 무선접속장치, 운용컴퓨터 외에 추가적으로 WMN 모듈을 장착함으로써 타 MSAP과의 연결성을 보장할 수 있게 된다. 그러므로 WMN을 통해 MSAP 간의 무선 멀티 홉 통신, 분산 협업 등의 기능들을 수행할 수 있음과 동시에 네트워크 확장성 및 관리를 용이하게 할 수 있다[3].

이렇게 LCTR과 HCTR이 연결되는 전술 무선망과 MSAP 노드들 간 WMN 모듈로 구성되는 메쉬망이 함께 운용되는 상황에서 구축된 네트워크에 접속하기 위한 초기 가입 및 연동 방안 연구는 현재 진행되고 있지 않다. 이러한 방법이 혼용되어 사

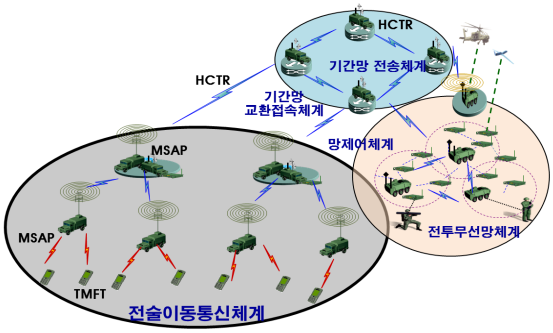

그림 1. 전술정보통신체계(TICN)와 전술이동통신체계 구성도
Fig 1. Architecture of TICN and MSAPs

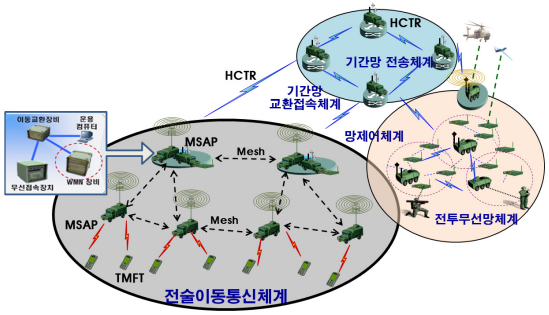

그림 2. 전술정보통신체계(TICN)와 차기 전술이동통신체계 구성도
Fig. 2. Architecture of TICN and next-generation MSAPs

용될 때, 타 MSAP과의 멀티미디어 서비스를 제공하기 위해서는 군 환경에 적합한 인증방안 정립이 필요하다. MSAP은 무선 메쉬망을 구성함으로 MSAP간 직접적인 멀티 홉 통신이 가능해졌지만, 데이터 도청 또는 부인방지 등의 위험에 쉽게 노출될 수 있다는 문제점이 있다. 따라서 전술이동통신체계에서 단말 간 상호 인증과 데이터 암호화는 매우 중요한 이슈로 볼 수 있다.

본 연구에서는 기존의 TMFT-MSAP간 사용하는 EAP-TLS(Extensible Authentication Protocol - Transport Layer Security)인증 기법[4]을 MSAP-MSAP간 상호 인증 기법에 도입함으로 무선 환경에서 발생할 수 있는 보안적 요소를 강화하고자 한다. 인증서버를 갖춘 단말의 인증과 같은 특수한 군 환경의 특수성을 고려하고, 이러한 문제점을 해결하기 위한 상호 인증 기법에 대해 제시한다.

Ⅱ. 관련 연구

2.1 무선 메쉬망에서의 상호 인증

무선 메쉬 네트워크의 표준 기술인 802.11s[5]는 802.11i[6] 보안 표준을 바탕으로 제정하고 있기 때문에 실제 메쉬망의 구성원인 MP(Mesh Point) 인증 과정은 802.11i와 유사하다. 인증을 위한 요소로는 사용자의 인증을 요청하는 단말, 망에 접근할 수 있도록 서비스를 제공하는 AP(Access Point)와 실제적인 인증 역할을 수행하는 AAA(Authentication Authorization Accounting) 인증서버로 구성된다. 802.11i에서는 EAP를 사용하여 EAP 헤더에 다양한 종류의 인증방식(MD5-Challenge[7], TLS[8]등)을 명시할 수 있도록 확장성을 부여한다. 인증방식에 해당하는 메시지를 교환하고 인증결과에 따라 상호 인증을 수행한다.

802.11i에서는 통신을 위한 키 생성을 하고 AP와 인증서버간 EAP 메시지로 보호했다면, 802.11s에서는 AP의 역할을 하는 MA(Mesh Authenticator)과 키 생성 및 관리 기능을 담당하는 MKD(Mesh Key Distributor), MKD와 인증을 수행하는 AAA 인증서버 간 EAP를 통해 메시지 암호화를 수행한다.

2.2 EAP-TLS 인증 프로토콜

IEEE 802.16 표준은 MAC 계층 안에 PKM(Privacy Key Management)이라고 하는 보안 부계층을 정의한다. 이는 PKMv1과 PKMv2로 구분되며, 먼저 PKMv1은 단방향 인증 및 기밀성 기능을 제공하며 IEEE 802.16 표준에 기본적으로 적용되어 있다. 그러나 PKMv1의 보안성에 대해 의문을 제기하였고, 단말과 기지국간의 양방향 상호 인증을 제공하는 PKMv2가 제안되었다[9]. PKMv2의 EAP 인증은 IEEE 802.1x 포트 기반의 가입자 인증 데이터 전송을 위한 표준 프로토콜로 다양한 인증 프로토콜을 지원한다. EAP-TLS는 X.509 인증서를 기반으로 단말의 양방향 인증을 수행하며, TMFT와 MSAP 단말 모두 인증서를 보유하기 때문에 이를 통해 인증을 수행한다. 그 결과에 의해서 상호 공유하는 비밀 키를 생성하여 이후 전송하려는 데이터를 보호하여 전달할 수 있다.

2.2.1 EAP-TLS 인증 절차

Step 1. 시스템 초기 등록 단계

최초 단말은 초기 링크 동기화 및 협상을 하기 위해 Ranging과정을 수행한다. 먼저 주변에 위치한 MSAP을 탐색하고 단말이 자신의 ID를 인증서버로 전송하여 TLS 연결을 기지국에 알린다.

Step 2. 상호 인증 단계

단말과 인증서버 간에 일반적인 TLS 연결절차로 각자의 인증서를 사용한 상호 인증 과정을 수행한다. 이 과정에서 단말은 Premaster Secret 키를 임의로 생성하여, TMS(TLS Master Secret)를 공유하게 된다.

Step 3. 키 분배 및 4-way 핸드쉐이킹 단계

공유된 키를 가지고 단말과 인증서버는 무선구간 데이터 암호 키를 생성하기 위한 키인 MSK(Master Session Key)를 생성한다. 인증서버는 생성된 MSK를 기지국에 전달하고, 이로부터 데이터 암호 키를 생성한 후, 4-way 핸드쉐이킹을 수행한다.

2.3 EAP 기반의 키 생성 및 전달

일반적으로 EAP 기반의 인증방식은 2가지 용도의 키를 공통적으로 생성한다. TLS 연결 시 랜덤하게 생성하는 Premaster Secret 키와 무선구간 암호용 키를 생성한다. 무선구간 암호용 키는 단말과 기지국이 공유하게 되는 키로부터 PMK(Pair-wise Master Key)를 설정하게 된다. 이를 통해 유니캐스트 프레임 보호용 키와 브로드캐스트 프레임 보호용 키를 생성할 수 있다. 그리고 인증이 완료된 후 무선구간 보호용 암호 키를 생성 할 수 있는 MSK를 전달하는 과정이 있다.

Ⅲ. 제안 기법

차기 MSAP은 WMN 모듈을 통해 무선 메쉬 네트워크를 형성하게 된다. 새롭게 진입한 MSAP이 이미 형성된 MSAP 네트워크에 접근할 경우 기존 네트워크의 정보를 공유할 수 있는 정당한 MSAP 인지를 판별하기 위한 인증을 수행하게 된다. 모든 MSAP 내부에는 각각의 인증서버인 AAA Server를 보유하고 있다는 구조적인 특성 때문에 신뢰된 인증기관으로부터 발급된 타 MSAP의 X.509 인증서를 관리 및 검증 할 수 있다. 기존의 EAP-TLS 기반 인증 방식은 단말과 서버의 구조에서 상호 인증을 제시하고 있기 때문에 서버와 서버간의 인증에 그대로 적용할 수 없다. 제안된 기법에서는 타 MSAP의 인증서 관리를 인증서버에서 수행하지만, 자신의 인증서를 갖는 주체에 따라 분류된다. 따라서 본 연구에서는 이러한 특수한 환경에서의 인증 절차를 수행하기 위한 기법을 제시한다.

3.1 MSAP 내부 구조적 특징

상호 인증을 통한 네트워크 인증은 신뢰된 정보를 관리하는 주체에 따라 크게 중앙 집중형과 분산형 두 가지로 구분한다. 중앙 집중형의 경우에는 중앙에 서버를 정의하여 신뢰된 정보를 관리하고, 서버에서 정보를 생성함과 동시에 폐기 및 인증, 키 분배 등을 담당한다. 반면, 분산형 인증 방식의 경우에는 중앙에 서버의 도움 없이도 네트워크상에 분산된 기기 간의 상호 인증을 수행하여 신뢰된 정보를 관리한다.

기존에 구성된 네트워크에 새로운 MSAP이 접근하기를 원할 경우에는 정당한 MSAP인지를 판별하는 것은 매우 중요하다. 이 과정을 용이하게 하기 위하여 중앙에 신뢰된 서버를 설치하여 인증 및 키 분배를 하는 것은 여러 가지 측면에서 어려움이 발생할 수 있다. 손쉽게 모든 MSAP을 서버를 통해 한 번에 제어를 할 수 있다는 장점이 있는 반면, 모든 MSAP이 단일 인증서버를 접근하기 위해서는 WMN 모듈을 이용한 멀티 홉 통신 환경을 추가로 고려하여 관리해야 한다. 뿐만 아니라 인증서버를 별도로 구축하여 운용하는 측면에서도 서버 자체를 탈취 당할 경우, 큰 타격이 가해질 수 있다는 문제점이 있다. 군 환경에서는 적군에 의한 공격을 예방하고 기밀 유출을 막아야하기 때문에 차기 전술이동통신체계에서는 MSAP간 상호 인증을 수행하기 위해 분산형으로 단말 간 협업을 통해 신뢰된 정보

그림 3. WMN을 통한 내부 연결 구조
Fig. 3. Internal link structure through WMN

교환하는 방식을 도입해야한다.

그림 3은 MSAP의 내부 연결 구조도이다. 차기에는 WMN 모듈을 이용하여 MSAP과 MSAP이 메쉬망을 구축하여 분산적인 인증을 수행한다면 MSAP의 이동 유·무에 상관없이도 보안에 보다 강력한 시스템을 구축하여 안전한 데이터 전송이 가능하게 된다.

최초에 MSAP이 네트워크에 진입하여 링크가 활성화 된 뒤, WMN 모듈에서 인증 요청 메시지를 전송하게 된다. 타 MSAP에서 수신된 메시지는 WMN 모듈을 통해 중계 역할을 담당하는 ACR을 거쳐 MSAP의 인증서버인 AAA Server에게 전달된다. MSAP-TMFT 단말간 인증을 위해서는 기지국 역할을 하는 RAS를 통해 메시지가 인증서버로 수신되기 때문에 본 제안 절차에서 생략한다.

3.2 EAP-TLS 기반 MSAP간 상호 인증

3.2.1. 시나리오1: MSAP의 내부 인증서버-인증서버간 인증 절차

그림 4는 MSAP의 내부 인증서버-인증서버 간 인증 절차를 나타낸 흐름도이다. 인증서버에서는 EAP 메시지를 송·수신하며 자신의 X.509인증서와 모든 MSAP의 인증서를 관리하는 주체가 된다. 그러므로 인증서버에서는 TMFT 단말의 인증 요청 메시지와 WMN 모듈로부터 전달되는 MSAP의 인증 요청 메시지를 처리해야 한다.

Step 1. 시스템 초기 등록 단계

최초 Ranging 작업 후에 본 인증 절차가 시작된다. 초기 등록 단계는 인증허가 MSAP인 MSAP1의 WMN 모듈이 인증요청을 하려는 MSAP2의 Identity를 요구하는 EAP-Request /Identify 메시지를 PKMv2-RSP/EAP-Transfer 메시지에 캡슐화 하여 전송한다. 이 메시지를 수신한 MSAP2의 WMN은 PKMv2-RSP/EAP-Transfer 메시지로부터 EAP-Request/Identify 메시지를 추출한다.

MSAP1 WMN → MSAP2 WMN :

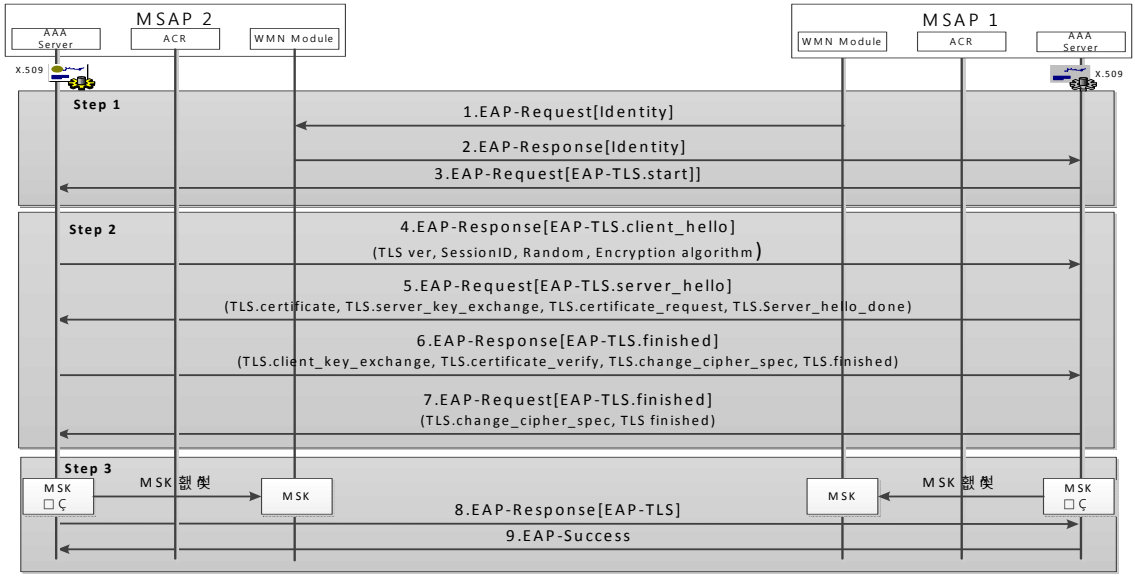

그림 4. MSAP의 내부 인증서버-인증서버간 인증 절차
Fig. 4. The authentication process between MSAP's internal authentication server

PKMv2-RSP/EAP-Transfer(EAP-Request/Identity)…(1)

이후 인증요청 메시지를 수신한 MSAP2는 자신의 ID를 담은 EAP-Response/Identity 메시지로 응답하고, 이를 수신한 MSAP1의 WMN 모듈은 ACR에게 전달하고 메시지 중계를 통해 인증서버로 전송된다. 이때 ACR과 AAA Server간은 RADIUS 프로토콜[10]을 통해 메시지를 송·수신을 수행한다.

MSAP2 WMN → MSAP1 WMN :

PKMv2-REQ/EAP-Transfer(EAP-Response/Identity)…(2)

Step 2. 상호 인증 단계

인증을 허가하는 MSAP1의 인증서버에서 EAP-Response/Identity 메시지를 수신하면 먼저 ID를 식별하여 검증되었을 경우에는 EAP-Request/EAP-TLS.Start 메시지를 생성하여 ACR로 전송한다. 이 메시지 내에는 별도의 데이터 없이 전송되며, MSAP2의 WMN 모듈과 ACR을 거쳐 인증서버로 전달된다.

MSAP1 AAA Server → MSAP2 AAA Server :

PKMv2-RSP/EAP-Transfer(EAP-Request/EAP-TLS.Start)…(3)

MSAP2는 EAP-Request/EAP-TLS.Start 메시지를 수신 한 뒤, MSAP1에게 응답 메시지를 전송하기 위해 EAP-Response/EAP-TLS.Client_Hello 메시지를 생성하여 MSAP1에게 전송한다. 이 메시지의 내부에는 지원하는 TLS 버전과 세션 ID, 랜덤 넘버 및 암호화 알고리즘들을 포함한다. 그리고 MSAP1의 WMN 모듈이 수신하여 ACR를 거쳐 인증서버로 전달한다.

MSAP2 AAA Server → MSAP1 AAA Server :

PKMv2-REQ/EAP-Transfer(EAP-Response/EAP-TLS.Client_Hello)…(4)

그리고 MSAP1은 EAP-Request/EAP-TLS.Server_Hello 메시지 생성하여 ACR을 거쳐 WMN 모듈로 전달한다. MSAP1의 WMN 모듈은 이 메시지를 MSAP2에게 전송하고, 이를 수신한 MSAP2는 자신의 ACR을 거쳐 인증서버로 전달한다. 이 메시지 내부에는 TLS Server_Hello, MSAP1의 본인 인증서가 포함된 TLS Certificate, TLS Server_Key_Exchange, TLS Certificate_Request, TLS Server_Hello_Done로 구성된다. MSAP2은 MSAP1의 인증서인 X.509 인증서를 검증한다.

MSAP1 AAA Server → MSAP2 AAA Server :

PKMv2-RSP/EAP-Transfer(EAP-Request/EAP-TLS.Server_Hello)…(5)

MSAP2의 인증서버에서 MSAP1의 X.509 인증서를 검증하여 성공했을 경우, Premaster Secret, TEK(Traffic Encryption Key)를 생성하고 EAP-Response/EAP-TLS.Finished 메시지를 전송한다. 이 메시지 내부에는 상호 인증을 수행하기 위해 인증을 요청하는 MSAP2의 인증서를 포함하며 TLS Certificate, Premaster Secret이 포함된 TLS Client_Key_Exchange, TLS Certificate_Verify,

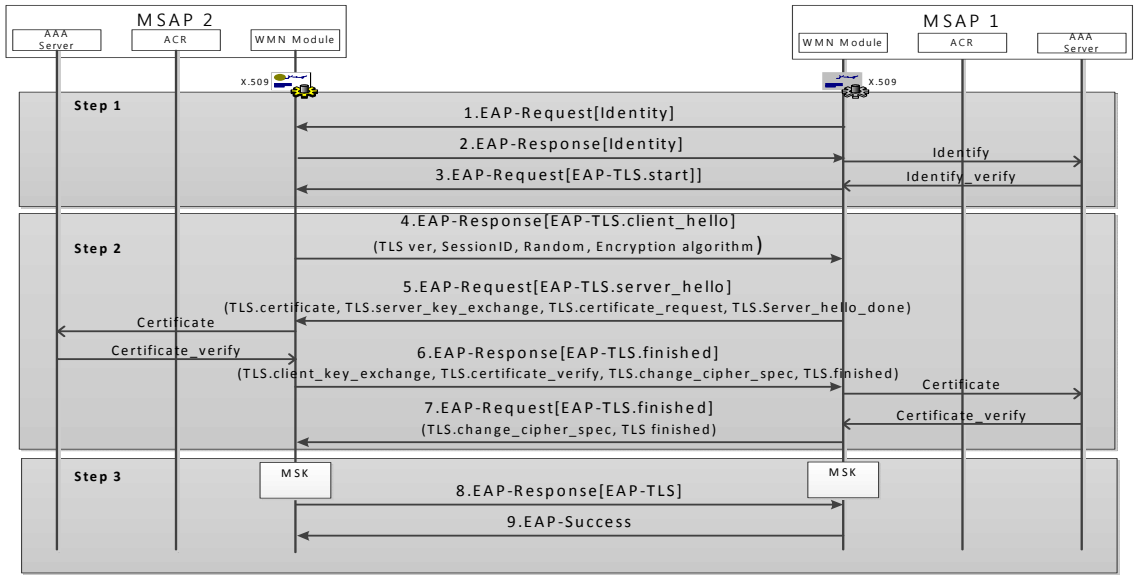

그림 5. MSAP의 내부 WMN-WMN 모듈간 인증 절차
Fig. 5. The authentication process between MSAP's internal WMN modules

TLS Change_Cipher_Spec, TLS Finished로 구성된다.

MSAP2 AAA Server → MSAP1 AAA Server : PKMv2-REQ/EAP-Transfer(EAP-Response/EAP-TLS.Finished)…(6)

Step 3. 키 분배 및 메시지 암호화 단계

상호 인증 단계를 위해서 MSAP1이 EAP-Response/EAP-TLS.Finished 메시지를 수신하였을 때, MSAP2의 인증서와 TLS Certificate등을 통해 인증을 수행한다. MSAP1의 인증서버는 MSAP2의 인증서 내부에서 X.520 Common Name RDN에서 MAC 주소와 모델명을 추출할 수 있어야 하며, 추출한 MAC 주소를 RADIUS Access-Request 메시지의 Calling-Station-Id의 MAC 주소와 비교하여 불일치하는 경우 인증과정을 종료해야 한다. MSAP2의 인증이 성공하면, 수신된 Premaster Secret을 이용하여 TEK를 생성하고 이 후의 메시지는 모두 TEK로 암호화해서 교환한다. TLS Change_Cipher_Spec, TLS finished로 구성된 EAP-Request/EAP-TLS.Finished 메시지를 생성하여 MSAP2의 인증서버로 전송한다.

MSAP1 AAA Server → MSAP2 AAA Server : PKMv2-RSP/EAP-Transfer(EAP-Request/EAP-TLS.Finished)…(7)

각 MSAP은 Finish 메시지를 송·수신 한 후에 TMS와 인증요청 MSAP의 랜덤 넘버와 인증허가 MSAP의 랜덤 넘버를 이용해 MSK를 생성한다. MSAP1의 인증서버와 MSAP2의 인증서버에서 MSK를 생성한 후, 각각의 WMN 모듈에게 ACR 중계를 통해 전달한다.

MSAP1 AAA Server → MSAP1 WMN : MSK…(8)

MSAP2 AAA Server → MSAP2 WMN : MSK…(9)

키를 생성하여 WMN 모듈에게 성공적으로 전달하였을 경우에는 MSAP2의 인증서버에서 데이터가 포함되지 않은 EAP-Response/EAP-TLS 메시지를 생성하여 MSAP2의 WMN 모듈에게 전달한 다음 메시지를 MSAP1의 인증서버로 전송한다.

MSAP2 AAA Server → MSAP1 AAA Server : PKMv2-REQ/EAP-Transfer(EAP-Response/EAP-TLS)…(10)

MSAP1의 인증서버는 WMN 모듈과 ACR을 거쳐 EAP-Response/EAP-TLS 메시지를 수신하면, EAP-Success 메시지를 생성하여 MSAP2의 WMN 모듈에게 전달한다. MSAP2가 성공적으로 EAP-Success 메시지를 수신하였다면 MSAP간 상호 인증 과정이 정상적으로 수행된 것이다. 더불어 인증과정에서 도출한 키를 이용하여 메시지를 암호화하여 전송한다.

MSAP1 AAA Server → MSAP2 AAA Server : PKMv2-RSP/EAP-Transfer(EAP-Success)…(11)

3.2.2 시나리오 2: MSAP의 내부 WMN-WMN 모듈간 인증 절차

그림 5는 MSAP의 내부 WMN-WMN 모듈간 인증 절차를 나타낸 흐름도이다. WMN 모듈에서는 EAP 메시지를 송·수신하며 자신의 X.509 인증서 관리를 하는 주체가 된다. 인증서버에서는 TMFT 단말의 인증 요청 메시지와 WMN 모듈로부터 타 MSAP의 인증서 검증을 위한 메시지를 처리하게 된다. MSAP 인증 메시지를 처리하는 WMN 모듈 내에는 자신의 X.509 인증서를 포함해야 한다.

Step 1. 시스템 초기 등록 단계

시나리오 2의 시스템 초기 등록 단계는 시나리오 1의 동작 과정과 동일하다. 초기 등록 단계는 인증허가 MSAP인 MSAP1의 WMN 모듈이 인증요청을 하려는 MSAP2의 Identity를 요구하는 EAP-Request /Identify 메시지를 PKMv2-RSP/EAP-Transfer 메시지에 캡슐화 하여 전송한다.

MSAP1 WMN → MSAP2 WMN :

PKMv2-RSP/EAP-Transfer(EAP-Request/Identity)…(1)

이후 인증요청 메시지를 수신한 MSAP2는 자신의 ID를 담은 메시지인 EAP-Response/Identity 메시지로 응답하고, 이를 수신한 MSAP1의 WMN 모듈은 ACR에게 전달하고 메시지 중계를 통해 인증서버로 전송된다.

MSAP2 WMN → MSAP1 AAA Server :

PKMv2-REQ/EAP-Transfer(EAP-Response/Identity)…(2)

Step 2. 상호 인증 단계

MSAP1의 인증서버에서는 EAP-Response/Identity 메시지를 전달받아 먼저 ID를 식별하여 검증되었을 경우에 EAP-Request/EAP-TLS.Start 메시지를 생성하여 ACR로 전송한다. 이 메시지 내에는 별도의 데이터 없이 전송되며, MSAP1의 WMN 모듈에서 MSAP2의 WMN 모듈로 전송된다.

MSAP1 AAA Server → MSAP2 WMN :

PKMv2-RSP/EAP-Transfer(EAP-Request/EAP-TLS.Start)…(3)

MSAP2의 WMN 모듈에서 EAP-Request / EAP-TLS.Start 메시지를 수신 한 뒤, 인증서버의 확인 없이 바로 응답 메시지를 전송한다. MSAP2의 WMN은 EAP-Response/EAP-TLS.Client_Hello 메시지를 생성하여 MSAP1에게 전송한다. 이 메시지의 내부에는 지원하는 TLS 버전과 세션 ID, 랜덤 넘버 및 암호화 알고리즘들을 포함한다.

MSAP2 WMN → MSAP1 WMN :

PKMv2-REQ/EAP-Transfer(EAP-Response/EAP-TLS.Client_Hello)…(4)

그리고 MSAP1의 WMN 모듈은 EAP-Request/EAP-TLS.Server_Hello 메시지 생성하여 MSAP2에게 전송한다. WMN 모듈에서 자신의 인증서를 가지고 있기 때문에 인증서버의 도움 없이 바로 전송이 가능하다. 전송된 메시지는 MSAP2의 WMN 모듈이 수신하게 된다. 이 메시지 내부에는 TLS Server_Hello, MSAP1의 본인 인증서가 포함된 TLS Certificate, TLS Server_Key_Exchange, TLS Certificate_Request, TLS Server_Hello_Done로 구성된다. MSAP2의 WMN 모듈은 메시지를 ACR에게 전달하여 인증서버에서 MSAP1의 인증서인 X.509 인증서를 검증한다.

MSAP1 WMN → MSAP2 AAA Server :

PKMv2-RSP/EAP-Transfer(EAP-Request/EAP-TLS.Server_Hello)…(5)

MSAP2의 인증서버에서 MSAP1의 X.509 인증서를 검증하여 성공했을 경우, 인증된 단말임을 알려주는 Certificate_Verify 메시지를 WMN 모듈로 전달한다. WMN 모듈에서는 Premaster Secret, TEK(Traffic Encryption Key)를 생성하고, 본인의 인증서를 담은 EAP-Response/EAP-TLS.Finished 메시지를 전송한다. 이 메시지 내부에는 상호 인증을 수행하기 위해 인증을 요청하는 MSAP2의 인증서를 포함하며 TLS Certificate, Premaster Secret이 포함된 TLS Client_Key_Exchange, TLS Certificate_Verify, TLS Change_Cipher_Spec, TLS Finished로 구성되며 ACR을 통해 WMN 모듈에게 전달되어 MSAP1에게 전송된다.

MSAP2 AAA Server → MSAP1 AAA Server :

PKMv2-REQ/EAP-Transfer(EAP-Response/EAP-TLS.Finished)…(6)

Step 3. 키 분배 및 메시지 암호화 단계

상호 인증 단계를 위해서 MSAP1이 EAP-Response/EAP-TLS.Finished 메시지를 수신하였을 때, MSAP2의 인증서와 TLS Certificate를 인증서버에게 전달하게 된다. 인증서 검증을 수행한 뒤 Certificate_Verify 메시지를 통해 MSAP2의 인증을 여부를 WMN 모듈에게 알려준다. MSAP1은 MSAP2의 인증서 내부에서 X.520 Common Name RDN에서 MAC 주소와 모델명을 추출할 수 있어야 하며, 추출한 MAC 주소를 RADIUS Access-Request 메시지의 Calling-Station-Id의 MAC 주소와 비교하여 불일치하는 경우 인증과정을 종료해야 한다. MSAP2의 인증이 성공하면, 수

신된 Premaster Secret을 이용하여 TEK를 생성하고 이 후의 메시지는 모두 TEK로 암호화해서 교환한다. TLS Change_Cipher_Spec, TLS finished로 구성된 EAP-Request/EAP-TLS.Finished 메시지를 생성하여 MSAP2의 WMN 모듈로 전송한다.

MSAP1 AAA Server → MSAP2 WMN :

PKMv2-RSP/EAP-Transfer(EAP-Request/EAP-TLS.Finished)…(7)

각 MSAP은 Finish 메시지를 송·수신 한 후에 TMS와 인증요청 MSAP의 랜덤 넘버와 인증허가 MSAP의 랜덤 넘버를 이용해 MSK를 WMN 모듈 내에서 생성한다.

MSAP1 WMN : MSK…(8)

MSAP2 WMN : MSK…(9)

성공적으로 MSK가 생성하였을 때에는 MSAP2의 WMN 모듈에서 데이터가 포함되지 않은 EAP-Response/EAP-TLS 메시지를 생성하여 MSAP1에게 전송한다.

MSAP2 WMN → MSAP1 WMN :

PKMv2-REQ/EAP-Transfer(EAP-Response/EAP-TLS)…(10)

MSAP1의 WMN 모듈에서 EAP-Response / EAP-TLS 메시지를 수신하면, EAP-Success 메시지를 생성하여 MSAP2의 WMN 모듈에게 전달한다. MSAP2가 성공적으로 EAP-Success 메시지를 수신하였다면 MSAP간 상호 인증 과정이 정상적으로 수행된 것이다. 더불어 인증과정에서 도출한 키를 이용하여 메시지를 암호화하여 전송한다.

MSAP1 WMN → MSAP2 WMN :

PKMv2-RSP/EAP-Transfer(EAP-Success)…(11)

Ⅳ. 제안된 시나리오 검증

4.1 성능 분석

4.1.1 제안 기법의 상호 인증 성능 분석

MSAP-MSAP의 두 가지 상호 인증 절차는 인증 주체에 따라 분류할 수 있다. 표 1은 상호 인증 절차를 수행하기 위해 제안된 시나리오 별 인증기법을 비교한 표이다. 시나리오 1의 경우에는 인증서버-인증서버간 인증을 수행하기 때문에 MSAP의 모든 인증서 검증, 관리 및 키 생성, 분배를 AAA Server에서 하게 된다. 인증서버에서 타 인증서 관리뿐만 아니라 본인의 인증서를 관리하기 때문에 기기에 대한 신뢰성이 보다 향상된다. 그러나 메시지를 송·수신하게 될 경우에는 메시지를 인증서버까지 전달해야하기 때문에 지연시간이 시나리오 2보다 높다. 결과적으로 메시지 교환 횟수를 비교하였을 때에도 시나리오 2보다 총 9회 이상의 추가적인 메시지 처리량이 발생하였다. 시나리오 2에서는 타 인증서에 대한 검증 메시지를 전달하는 것 외에는 WMN 모듈에서 처리하기 때문에 수신된 메시지에 바로 응답할 수 있다. 또한 WMN 모듈간 인증에서는 인증서버의 에이전트(Agent) 역할이 되어 수행하기 위해 키 생성, 분배 및 본인의 인증서 관리를 WMN 모듈에서 한다. 이로 인하여 인증서버에서 관리하는 것 보다는 신뢰성이 낮지만 인증서버의 부담을 줄일 수 있다는 장점이 있다.

4.1.2 기존 기술과 비교

표 2에서는 제안 기법인 군 환경에서의 TLS 기법과 일반적인 TLS 기법 및 확장된 TLS 기법(EAP-TLS)간의 보안 요소를 비교하고 있다. 표를 통해 군 환경 TLS 기법에서는 상호인증을 수행하기 위하여 클라이언트 단말의 인증서가 요구가 된다는 것을 알 수 있다. 하지만 기존의 TLS 기법은 서버와 클라이언트 단말이 서로 상호인증을 수행하지 않고, 서버가 클라이언트 단말을 인증하기 때문에 서버를 위장하여 공격할 수 있다는 단점이 있다.

표 1. 인증 절차 시나리오 별 비교

Table 1. Comparison of authentication process for each scenario

제안방법	Number of Message Exchanging	Processing Delay	Authentication and Key Derivation Subject
시나리오 1	24회	Yes	AAA Server
시나리오 2	15회	No	WMN Module

표 2. EAP-TLS 상호 인증 기법 비교

Table 2. Comparison of EAP-TLS mutual authentication schemes

	Mutual Authentication	Require Client Certificates	Generation of Keying Material	User Identity Hiding
군 환경 TLS 기법	Yes	Yes	Not required	Yes
일반 TLS 기법	No	Yes	No	No
확장된 TLS 기법	Yes	Yes	Not required	Yes

또한 일반적인 TLS 기법에 비하여 확장된 TLS 기법을 도입한 군 환경 TLS 기법은 기본적인 EAP 메시지에 암호화하여 전송한다. 그렇기 때문에 인증을 수행하기 위해 초기 단말의 ID(Identify)를 전송할 때에도 사용자의 식별을 암호화하여 전송할 수 있게 된다.

4.2 안전성 분석

본 절에서는 제안 기법의 안정성에 대해 간략한 분석 결과를 기술한다. 제안된 기법에서는 단말 간 상호 인증을 수행하여 도출된 키는 암호화된 난수를 통해 이루어지므로, 공격자가 통신 내용을 취득하기 위해서는 암호화된 패킷을 해독할 수 있어야 한다. 그리고 신뢰받은 기관으로부터의 X.509 인증서를 발급받기 때문에 전송된 인증서에 대한 상호 인증이 가능해 지며 최초에 비대칭 키(Asymmetric Key)를 사용하기 때문에 부인 방지기능이 포함된다.

EAP 프로토콜을 사용하여 메시지 암호화를 통해 기밀성을 제공하고 있으며 인증을 요청하는 MSAP과 허가하는 MSAP 단말 사이에서의 생성된 키를 사용하기 때문에 무결성 측면에서 예방할 수 있는 기법이라고 생각된다. 그 외에도 전송된 메시지를 공격자가 중간에서 위·변조 할 수 없음으로 MITM (Man-in-the-middle) Attack 등에 대해서는 안전하다고 판단된다.

Ⅲ. 결 론

전술이동통신 체계에서 사용되는 MSAP은 TMFT 단말의 실시간 서비스를 지원하기 위한 핵심적인 역할을 담당한다. MSAP의 보다 높은 신뢰성, 실시간성을 지원하기 위하여 MSAP 자체에 WMN을 지원할 수 있는 모듈을 장착하는 방안이 제시되고 있으며, 이러한 MSAP간의 안전한 통신을 지원하기 위한 상호 인증방법이 필요하다. 본 논문에서는 기존 MSAP과 TMFT 단말간의 인증을 위해 사용된 EAP-TLS 상호 인증 기법을 분석하고, 이를 MSAP과 MSAP 단말 간 상호 인증을 위해 적용하는 방법을 제시하였다. 또한 제시한 방법론을 비교하여 성능을 분석하였고, 현재 제안된 시나리오에서는 인증의 주체가 다르다는 특성이 있기 때문에 성능과 구현에서 차이가 발생할 수 있다. 향후 계획으로는 제안된 기법의 실제 군 환경에 적용 시 발생할 수 있는 음영 지역 문제 등에 대한 대응 방안에 대해 보완 하도록 하겠다.

참 고 문 헌

[1] 박귀순, 황정섭, “미래 전장 환경변화에 따른 TICN 체계 요구 기능 및 능력,” Telecommunications Review, 제20권 2호, pp.196-206, 2010.

[2] 유정훈, 조정호, 권오주, 박귀순, “Mobile WiMAX 기반의 전술이동통신체계 테스트베드 성능분석,” 한국통신학회지, 제 26권 제3호, pp.9-15, 2009.

[3] F. Akyildiz, X. Wang, W. Wang, “Wireless mesh networks: a survey,” Computer Networks. vol 47, no.4, pp.445-487, 2005.

[4] [EAP-TLS] RFC 5216, http://www.ietf.org/rfc/rfc5216.txt

[5] IEEE P802.11sTM/D7.0, Amendment 10: Mesh Networking, July. 2010.

[6] IEEE P802.11iTM/D10.0, MAC security enhancements, amendment 6 to IEEE Standard for local and metropolitan area networks part 11: Wireless MAC and PHY specifications. April. 2004.

[7] [MD5 Algorithm] RFC 1321, http://wwwwww.ietf.org/rfc/rfc1321.txt

[8] [TLS] RFC 2246, http://www.ietf.org/rfc/rfc2246.txt

[9] D. Johnston and J. Walker, “Overview of IEEE 802.16 Security,” IEEE Security & Privacy, magazine May/June 2004.

[10] [RADIUS] RFC 2865, http://www.ietf.org/rfc/rfc2865.txt

손 유 진 (Yu-Jin Son) 준회원

2010년 8월 아주대학교 정보 및 컴퓨터공학부

2010년 9월~현재 아주대학교 컴퓨터공학과 석사 재학 중

<관심분야> 무선 네트워크, 군 전술 네트워크

배 병 구 (Byoung-Gu Bae) 준회원

2003년 2월 3사관학교 전산정보처리학과

2010년 3월~현재 아주대학교 NCW 석사 재학 중

<관심분야> 전술통신체계, 컴퓨터 네트워크

손 태 식 (Taeshik Shon) 정회원

2000년 2월 아주대학교 정보및컴퓨터공학부

2002년 2월 아주대학교 컴퓨터공학 석사

2005년 8월 고려대학교 정보보호대학원 박사

2004년 2월~2005년 2월 University of Minnesota, Research Scholar

2005년 8월~2011년 2 삼성전자 DMC 연구소 책임연구원

2011년 2월~현재 아주대학교 정보컴퓨터 공학부 조교수

<관심분야> 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지

고 영 배 (Young-Bae Ko) 정회원

1991년 2월 아주대학교 전자계산학과

1995년 2월 아주대학교 경영대학원 경영정보학과 석사

2000년 7월 텍사스 A&M 대원 컴퓨터공학과 박사

2000년~2002년 미국 IBM T.J 왓슨 연구소 전임연구원

2002년 9월~현재 아주대학교 정보컴퓨터 공학부 정교수

<관심분야> Mobile Ad Hoc Networks, 무선 메쉬 네트워크, 군 전술네트워크 등

임 광 재 (Kwang Jae Lim) 정회원

1992년 2월 인하대학교 전자공학과

1994년 2월 인하대학교 전자공학과 석사

1999년 2월 인하대학교 전자공학과 박사

1999년 3월~현재 한국전자통신연구원 모바일응용통신연구팀장

<관심분야> 이동 및 무선 통신

윤 미 영 (Mi-Young Yun) 정회원

1999년 2월 충남대학교 컴퓨터학과

2001년 2월 충남대학교 컴퓨터학과 석사

2000년 12월~현재 한국전자통신연구원 모바일응용통신연구팀

<관심분야> 이동 및 무선 통신