논문 12-37C-11-01

한국통신학회논문지 '12-11 Vol.37C No.11
http://dx.doi.org/10.7840/kics.2012.37C.11.1011

차세대 전술이동통신체계 무선 MSAP 메쉬망을 위한 혼합형 인증기법

배 병 구◆, 윤 선 중*, 고 영 배°

A Hybrid Authentication Scheme for Wireless MSAP Mesh Networks in the Next-Generation TMCS

Byoung-Gu Bae◆, Sun-Joong Yoon*, Young-Bae Ko°

요 약

본 논문에서는 차세대 전술이동통신체계에서의 무선 MSAP 메쉬망에서 효율적으로 인증키를 관리하고 전술이동통신체계의 부하를 줄이는 새로운 혼합형 인증기법을 제안한다. 또한 각각의 MSAP와 TMFT가 인증받는 알고리즘이 다르므로 인증요청 받은 MSAP의 제어대(ACR)에서 EAP 패킷의 Code 부분을 확인하여 처리하는 방안도 제안한다. 기존의 방식에서 각 MSAP가 체계접속을 위해서는 중앙집중형 인증기법과 분산형 인증기법을 활용할 수 있는데 각각은 문제점을 안고 있다. 즉, 중앙집중형 인증기법은 MSAP의 빈번한 가입 및 탈퇴로 인한 과다한 지연문제가 있고 분산형 인증기법은 인증에 필요한 정보를 사전에 공유해야 하는 문제점이 있다. 이러한 문제점을 보완하는 동시에 전술적인 환경에서 악의적인 MSAP의한 접속거부와 네트워크 보안성을 극대화하기 위해서는 보다 효과적인 인증기법이 요구된다. 따라서 본 논문에서는 미 인증된 MSAP가 EAP-TLS 기법을 기반으로 전술이동통신 네트워크 진입시 초기 인증과 이웃 MSAP간의 상호인증 등 다양한 시나리오를 군의 특수한 환경에 맞추어 구체적으로 제시하고 성능평가를 통해 혼합형 인증기법이 군 전술환경에 효율적으로 적용될 수 있음을 보였다.

Key Words : TICN(전술정보통신체계), TMCS(전술이동통신체계), Authentication, EAP-TLS, Mesh

ABSTRACT

This paper presents a novel hybrid authentication scheme in the next-generation Tactical Mobile Communication Systems(TMCS) with wireless MSAP mesh networks. The existing centralized and distributed authentication methods for security between MSAPs may have their pros and cons. The centralized authentication method induces overhead from frequent MSAP association which leads to long authentication delay. On the other hand, the distributed authentication method requires initial sharing of the authentication information. Therefore, a more efficient authentication scheme is needed to protect the network from malicious MSAPs and also maximize efficiency of the network security. The proposed scheme provides a hybrid method of efficiently managing the authentication keys in the wireless MSAP mesh network to reduce the induced authentication message exchange overhead. Also, as the authentication method between MSAP and TMFT is different, a method of utilizing the ACR for handling the EAP packets is proposed. In overall, the proposed scheme provides efficient mutual authentication between MSAPs especially for tactical environments and is analyzed through performance evaluation to prove its superiority.

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2012-(H0301-12-2003))
◆ 주저자 : 아주대학교 일반대학원 NCW학과, byounggu@uns.ajou.ac.kr, 정회원
° 교신저자 : 아주대학교 소프트웨어융합학과, younko@ajou.ac.kr, 정회원
* 육군 전투지휘훈련단, sunjoong@uns.ajou.ac.kr, 정회원
논문번호 : KICS2012-09-417, 접수일자 : 2012년 8월 3일, 최종논문접수일자 : 2012년 10월 26일

Ⅰ. 서 론

오늘날 전장 환경은 재래식 무기에서 정보유통이 보장되는 네트워크 중심전장체계(NCW: Network Centric Warfare)로 발전하고 있다[1]. 네트워크 중심전이란 전장의 구성요소들인 감시체계와 지휘통신체계, 타격체계까지 네트워크로 연결하여 전장의 상황을 실시간으로 수집하고 수집된 정보를 바탕으로 지휘권자의 결심을 도와 전장 상황에 대한 빠른 대응을 할 수 있도록 하는 것이다. 전술정보통신체계(TICN: Tactical Information and Communication Network)는 이러한 네트워크 중심전에서 정보가 원활히 소통 되도록 하는 것을 목적으로 한다. 그림 1과 같이 전술정보통신체계는 그 기능에 따라 기간망 전송체계, 기간망 교환접속체계, 망 제어체계, 전투무선망체계, 전술이동통신체계(TMCS: Tactical Mobile Communication System)로 구분된다[2]. 이 중에서 전술이동통신체계는 주파수 효율 측면에서 강점이 있는 WiBro 기술를 기반으로 만들어진 체계이다. 즉 상용 기지국에 해당하는 이동통신가입자 처리부(MSAP: Mobile Subscriber Access Point)와 사용자 휴대기기에 해당되는 전술용 다기능단말기(TMFT: Tactical Multi-Functional Terminal)로 구성 된다. MSAP의 내부구조는 TMFT를 지원하기 위해 여러 요소들로 구성되는데, 보다 구체적으로는

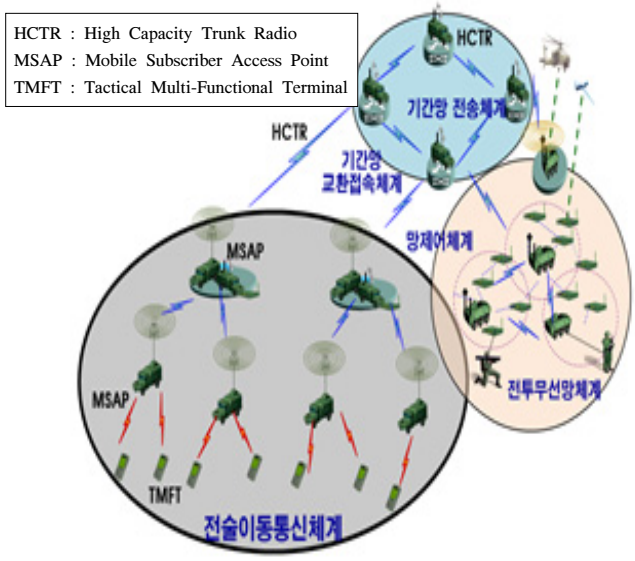


그림 1. 전술정보통신체계(TICN)
Fig. 1. Tactical Information and Communication Network (TICN)

무선접속장비(RAS: Radio Access Subsystem), 접속제어장비(ACR: Access Control Router), 인증서버(AAA: Authentication, Authorization, Accounting) 등이 있다[3]. 이러한 구조는 상용이동통신망과 달리 하나의 MSAP에 포함되어 운용된다. 또한 MSAP와 TMFT의 인증 및 보안 기술은 상용휴대폰에서 쓰는 EAP-AKA[4] (EAP-Authentication and Key Agreement)와 달리 TMFT의 X.509 인증서를 기반으로 하는 EAP-TLS[5] (Extensible Authentication Protocol Transport Layer Security)에 기반 한다.

육군은 기존의 전술이동통신체계보다 전술환경에 적합하도록 MSAP간 연결 구조를 기존의 1:N에서 통신망의 안정성을 보장하고 분산 협업 등의 기능을 수행할 수 있는 N:N 메쉬 구조의 차세대 전술이동통신체계(Next-Generation TMCS)를 연구 중에 있다. 즉, 기존의 전술이동통신체계는 소용량 무선전송체계인 LCTR(Low Capacity Trunk Radio)를 사용하여 중심이 되는 MSAP를 기준으로 1:N 전송로를 구성하는 방식이다. 고정 지향성 안테나 방식인 LCTR로 통신망을 구성하는 경우, 처리 성능은 보장될 수 있지만 실시간적으로 변화하는 상황에 빠른 대응을 할 수 없다는 문제점이 발생한다. 그리고 지향성 안테나를 통해 구축된 무선전송체계는 일정 범위의 안테나 각도에서만 전송이 가능함으로 항상 고정된 방향을 유지해야 하는 문제점이 발생한다. 그 결과, MSAP가 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) 장비를 추가하고 MSAP간 메쉬 토폴로지를 형성하여 이동 중에도 끊김없는 서비스를 지원한다. 일반적인 상용에서의 무선메쉬네트워크는 고정 혹은 이동성이 미미한 수준의 메쉬 라우터간에 형성되는 "메쉬 토폴로지 기반 네트워크"로, 무선 멀티 홉 통신을 사용하여 인터넷 및 멀티미디어 등 다양한 서비스를 고속으로 제공할 수 있는 무선 기간망이다. 이는 망 구성 및 유지 보수가 유선 기간망에 비해 간단하고, 확장이 용이하며 경제성 또한 높은 것으로 기대되기 때문에 미래 유망 네트워크 기술 중 하나로 대두되고 있다[6]. 그러나 상용과 달리 MSAP에 무선메쉬네트워크(WMN: Wireless Mesh Network)용 모듈 혹은 장비를 추가하여 이들 상호간 메쉬망을 구축하는 군용 무선메쉬네트워크는 이러한 무선 기간망의 역할보다는 기존의 LCTR

(Low Capacity Trunk Radio), HCTR(High Capacity Trunk Radio)로 이루어진 전술 무선백본 망과 연계되어 군용망 운용의 효율성 및 융통성을 높이는 방향에 주안점을 두고 있다.

차세대 전술이동통신체계에서 가장 문제화 되는 부분이 MSAP간 인증방식이다. MSAP간 무선통신 망임에도 불구하고 어떠한 인증절차 없이 통신망을 구성함으로서 보안에 취약한 문제점이 발생한다. 즉, 미 인증된 MSAP가 기존의 메쉬망에 최초 진입할 경우, EAP-TLS 기반 초기 인증과 이웃 MSAP간 인증 기법등 다양한 형태에서의 인증 시나리오를 군 전술환경에 맞게 아직까지 다루고 있지 않았다. 따라서 메쉬망을 기반으로 하는 차세대 전술이동통신체계에서 보안성이 강화된 군 특수한 환경에 맞는 혼합형 인증기법을 제안하고 이런 인증기법을 적용하기 위해서 TMFT와 MSAP간, MSAP와 이웃 MSAP간 인증시 다른 인증 시나리오를 따르므로 인증요청 받은 MSAP에서 2가지 인증요청 메시지를 처리하도록 망 연동 부분을 추가하였다.

본 논문은 다음과 같이 구성되어 있다. 2장은 전술이동통신체계에서 적합한 인증에 관련된 연구들에 대해 알아본다. 3장에서 각 상황에 적합한 혼합형 인증절차 및 MSAP의 내부에서 TMFT와 MSAP 각각을 인증하기위한 패킷구조의 망 연동을 살펴본다. 4장에서 혼합형 인증절차에 대한 성능평가에 대해 기술한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1. EAP-TLS 기반 MSAP간 인증 절차[7]

EAP-TLS는 X.509 인증서를 기반으로 단말과 인증서버가 모두 인증서를 가지고 있기 때문에 상호 인증을 수행한다. 그 결과에 의해서 상호 공유하는 비밀 키를 생성하고 이후 전송하려는 데이터를 보호하여 전달 할 수 있다. 위 과정을 구체적으로 설명하면, 시스템 초기 등록을 위해 최초 MSAP는 Ranging 과정을 통해 주변에 위치한 이웃MSAP가 탐색되면 자신의 ID를 이웃MSAP의 인증서버로 전송하여, TLS 연결을 무선접속장비(RAS)에 알리도록 한다. 그리고 MSAP와 이웃MSAP의 인증서버간에 일반적인 TLS 인증절차로 각자의 인증서를 활용한 상호인증 과정을 수행한다. 이 과정에서 MSAP와 이웃MSAP는 Premaster Secret 키를 임의로 생성하여, TMS(TLS Master Secret)를 공유하게 된다. 이제 공유된 키를 통하여 MSAP와 이웃 MSAP의 인증서버는 무선구간 데이터 암호 키를 생성하기 위해 MSK(Master Session Key)를 생성한다. 인증서버는 생성된 MSK를 무선접속장비(RAS)에 전달한다. 그리고 MSAP와 이웃MSAP는 MSK로부터 무선구간 데이터 암호 키를 생성한 후, 4-way Handshaking을 수행한다.

2.2 메쉬망 인증기법[8]

IEEE 802.11s에서 제안된 메쉬 노드들 간에 인증기법으로는 중앙집중형 인증기법과 분산형 인증기법이 있다. 중앙집중형 인증기법에서는 홉 간 인증을 수행하기 위해 메쉬 노드들 간에 상호인증할 때, 인증서버(AS: Authentication Server)로 상대 노드에 대한 인증을 요청하면 AS는 인증 검증을 수행한 후에 결과를 알려준다. 분산형 인증기법을 적용하기 위해서는 메쉬 노드들 간에 미리 인증에 필요한 정보를 공유해야 하며 복잡한 알고리즘을 사용하여 서로를 인증 한다.

Ⅲ. 제안 기법

전술정보통신체계는 논리적으로 계층적 구조를 갖고 있다. 즉, 하위부대들은 소속된 상위부대에 접속하여 통신망을 구성하고 상위부대의 통제를 받는다. 이러한 구조는 전술이동통신체계에도 적용되며 상위부대 MSAP를 모든 그림에서 중심MSAP로 표현하였다. 혼합형 인증기법은 분산형 인증에서 문제가 되었던 초기 이웃MSAP와 사전 인증정보 공유 문제를 해결하고 효율적인 인증관리를 위해 중앙집중형 인증기법을 사용한다. 또한 초기 인증 후 이웃 MSAP간 인증시 중앙집중형 인증에서 문제가 되었던 인증서버 부하를 감소시키고 빠른 상호인증을 위해 분산형 인증기법을 사용한다.

3.1. 군 환경에 적합한 혼합형 인증기법 제안

3.1.1. 초기 인증 절차

MSAP5가 전술이동통신 네트워크에 초기 인증을 받을 경우, 중앙집중형 인증기법을 사용한다. 그림 2에서 구체적인 인증 절차를 확인 할 수 있다. 첫째, MSAP5는 이웃MSAP들에게 인증요청을 한다. 이때 수신 세기가 강한 MSAP1을 선택하여 중심 MSAP의 인증서버에게 EAP-TLS 인증기법을 요청한다. 둘째, 중심MSAP의 인증서버는 MSAP5의 ID

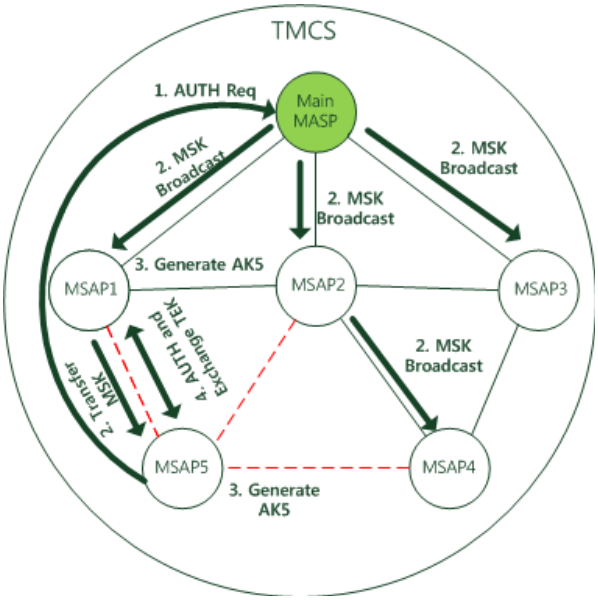


그림 2. 초기 인증 절차
Fig. 2 Initial authentication process

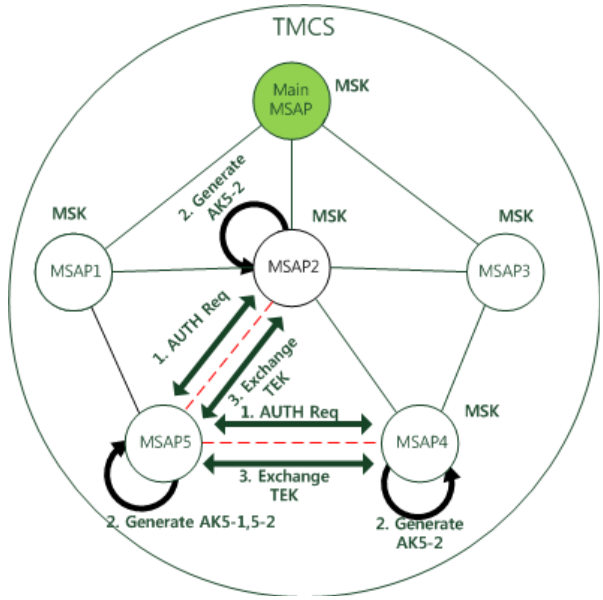


그림 3. 이웃 MSAP간 인증 절차
Fig. 3. Authentication process between neighboring MSAPs

를 확인 후 MSK(Master Session Key)를 생성하여 다시 전술이동통신 네트워크에 포함된 모든 MSAP에게 Broadcasting 한다. Broadcasting할 때 MSK는 기존의 MSAP간에 형성된 메쉬망에서 TEK(Traffic Encryption Key)를 통해 암호화 되어 전달된다. 셋째, MSAP1과 MSAP5는 각각 MSK를 활용하여 상호간에 유일한 AK(Authentication Key)를 생성함으로서 상호간의 인증을 완료한다. 그리고 중심MSAP는 이 정보를 갖고 전술이동통신 네트워크에 소속되어진 MSAP의 인증 테이블을 관리하게 된다. 마지막으로 MSAP1과 MSAP5는 상호 간에 안전한 데이터 전달을 위해 TEK로 암호화하여 전달한다.

3.1.2. 이웃MSAP간 인증절차

초기 인증 후 이웃MSAP간에 인증할 경우, 분산형 인증 기법을 수행한다. 내부구조 특성상 각각의 MSAP는 인증서버를 보유하고 있기 때문에 초기 인증에 의해 발생한 정보를 가지고 다른 인증키를 안전하게 생성할 수 있다. 그러므로 이웃MSAP간의 인증과 이동 후 인증할 경우에도 매번 중심MSAP에게 인증을 받을 필요 없이 이웃MSAP들은 Broadcasting된 MSK를 활용하여 신뢰성 있는 통신 구간을 빠르게 형성할 수 있다. 또한 초기 인증과 같은 복잡한 과정을 단축시키고 인증 확인 절차만으로 MSAP간 신뢰성 있는 통신망을 구성함으로서 신속한 인증이 가능하다. 그림 3은 초기 인증을 마친 MSAP5와 이웃MSAP간의 인증절차를 보이고 있다. 첫째, MSAP5는 이웃MSAP간 신뢰성 있는 통신 구간을 형성하기 위하여 이웃MSAP2와 MSAP4에게 인증을 요청하게 된다. 둘째, 이웃 MSAP2와 MSAP4는 MSAP5의 초기 인증 할 때 발생한 인증정보를 가지고 있으므로 확인절차를 통해 중심MSAP의 도움 없이 각각 고유한 AK5-1과 AK5-2를 생성한다. 마지막으로 각 구간 마다 신뢰성 있는 통신구간을 형성하고 TEK를 통해 데이터를 암호화하여 보내게 된다.

3.1.3. 타 전술이동통신 네트워크로 이동 후 인증절차

네트워크X의 중심MSAP와 네트워크Y의 중심MSAP간 35Mbps 용량의 HCTR(High Capacity Trunk Radio) 전송로가 연결된 전술 환경에서 전술이동통신 네트워크X에 있는 MSAP5가 타 전술이동통신 네트워크Y로 이동하였을 경우, 혼합형 인증기법을 수행한다. 그 이유는 군 전술망의 특성상 MSAP5가 전술환경에 따라 타 전술이동통신 네트워크Y로 접속하였다 하더라도 MSAP5는 네트워크X의 중심MSAP에 연결되어진 전술C4I 서버에 연결되어야만 하기 때문이다. 즉, 물리적으로 다른 네트워크에 있더라도 논리적으로는 현재 소속된 전술이동통신 네트워크에 연결되어 있어야 함으로 인증 또한 현재 소속된 X중심MSAP의 인증서버로 중앙집중형 인증을 요청한 후 이웃해 있는 MSAP6은 X중심MSAP에게서 전달받은 MSK를 가지고 분산형 인증을 수행한다. 그림 4에서 구체적인 인증 절차를

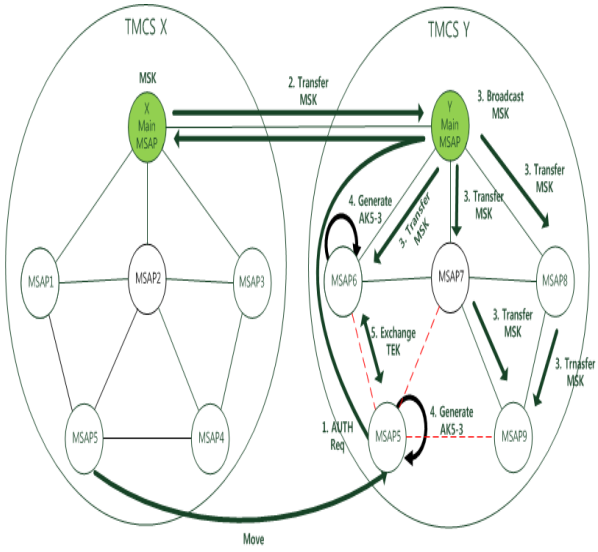


그림 4. 타 전술이동통신 네트워크로 이동 후 인증절차
Fig. 4. Authentication process after moving to another TMCS network

확인 할 수 있다. 첫째, MSAP5는 초기 인증과 같이 수신세기가 강한 이웃MSAP6을 거쳐 Y중심MSAP에게 인증을 요청한다. 하지만 Y중심MSAP는 MSAP5의 군단ID를 확인한 후 MSAP5에 대한 정보를 갖고 있지 않으므로 MSAP5의 전술이동통신 네트워크X를 찾아 인증정보를 요청한다. 이때 Y중심MSAP는 MSAP5의 군단급 단위로 고유한 군단ID를 식별하여 어느 제대의 장비임을 알 수 있다. 둘째, X중심MSAP는 MSAP5가 초기 인증 절차에 의해 발생된 인증정보를 갖고 있으므로 Y중심MSAP에게 전달한다. 셋째, Y중심MSAP는 이 같은 정보를 자신이 관리하는 전술이동통신 네트워크Y로 Broadcasting 함으로서 MSAP5에 대한 인증정보를 모든 MSAP에게 전달하게 된다. 이때 타 네트워크에 Broadcasting된 MSK는 Key 유효시간을 48시간으로 설정하여 급변하는 전장에서 MSAP의 이동에 따라 타 네트워크에 소속된 이웃MSAP들이 MSK의 보유여부를 판단하여 자동으로 제거할 수 있다. 또한 Key 유효시간을 설정 할 때, 짧게 설정할수록 빈번한 중앙집중형 인증을 통해 MSK를 전달받아야 하는 단점이 발생하므로 작전시간을 고려하여 충분한 Key 유효시간을 설정할 수 있도록 하였다. 넷째, MSAP6은 MSAP5와 신뢰성 있는 통신구간을 형성하기 위해 상호간에 고유한 AK5-3을 생성하여 통신망을 형성한다. 마지막으로 TEK를 통해 메시지를 암호화 하여 전달한다. 또한 이웃MSAP간 인증은 위에서 설명한 방식과 동일하다.

3.2. 망 연동 제안

차세대 전술이동통신체계에서 MSAP 인증시 혼합형 인증기법을 따르나 TMFT같은 경우, 와이브로 기반 인증을 따르기 때문에 각각 다른 인증 알고리즘으로 인증 받게 된다. 즉, 그림 5와 같이 TMFT는 자신이 소속된 MSAP의 인증서버에게 인증을 받으며 MSAP는 전술이동통신 네트워크에서 중심MSAP의 인증서버에게 인증을 받아야 한다. 그러므로 인증을 요청받은 MSAP는 TMFT에서 인증 요청된 것인지 MSAP에서 인증 요청된 것인지 구분하여 각각의 인증서버에게 인증 메시지를 전달하여야 한다. 전술이동통신체계를 망 연동 측면에서 용어를 정의하였다[7]. 즉, TMFT단말과 MSAP의 인증방식을 외부연동이라 정의 하고, MSAP와 MSAP의 인증 방식을 내부 연동이라고 정의 한다. 구체적으로 살펴보면, 그림 6과 같이 외부연동은 기존에 정의된 EAP-TLS 인증기법을 사용하여 MSAP의 이동기지국(RAS) 장비를 통해 수신된 인증 메시지를 제어국(ACR)에 전달하여 해당 MSAP의 인증서버와 상호 인증을 수행한다. 또한 내부연동은 WMN장비를 통해 수신된 메시지를 제어국(ACR)을 통해 전술이동통신 네트워크에서 중심MSAP의 인증서버와 상호 인증을 수행한 뒤, 신뢰된 망을 구축한다. 따라서 인증 요청받은 MSAP 내의 제어국(ACR)은 내·외부연동을 구별하기 위해 EAP 패킷의 구조 변경 없이 EAP Code 필드에 MSAP의 인증요청 메시지를 추가함으로서 구분할 수 있게 하였다. EAP

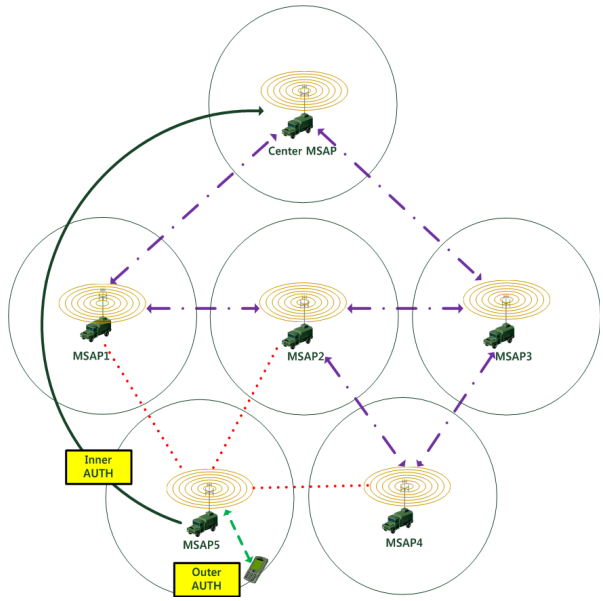


그림 5. 내·외부 인증 시나리오
Fig 5. Inner/Outer Authentication Process

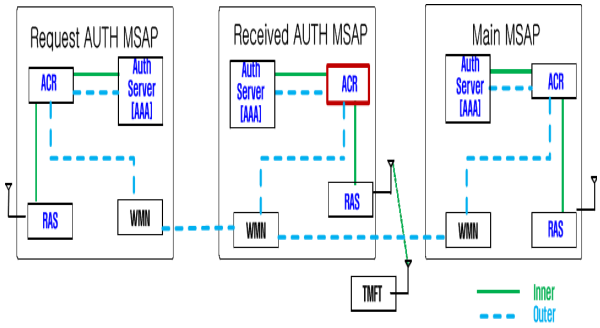


그림 6. 인증요청받는 MSAP의 내부 구조도
Fig. 6. Authentication Requested MSAP's Internal Architecture

패킷구조[4]는 그림 7과 같다. 1에서 4까지의 Code는 TMFT가 인증을 받을 때 송·수신되는 표준 내용과 같으며 추가로 5에서 8까지의 Code는 MSAP가 인증 받을 때 송·수신되는 메시지를 추가로 정의 하였다. 또한 그림 8은 인증요청을 받은 MSAP 내의 제어국(ACR)에서 EAP 패킷 메시지를 처리하는 순서도이다. 기존의 전술이동통신 네트워크를 구성하는 MSAP는 각각의 개체에 의해 인증요청을 받는다. 이때 인증요청 받은 MSAP는 제어국(ACR)에서 Code 필드를 확인한다. Code 필드가 5이하라면 TMFT 단말인증요청 EAP라 판단하고 해당 MSAP의 인증서버에서 상호인증을 하도록 전달한다. 하지만 5 이상이라면 MSAP간 인증이라 판단하여 다시 MSK의 존재여부를 확인 후 없다면 초기 인증인 중앙집중형 인증을 수행한다. 하지만 MSK가 있다면 초기 인증 후 이웃MSAP간 인증이라 판

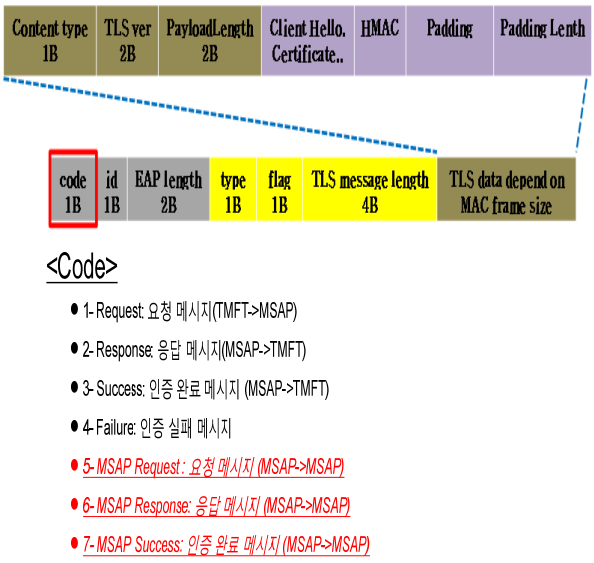


그림 7. EAP 패킷 구조
Fig. 7. EAP packet structure

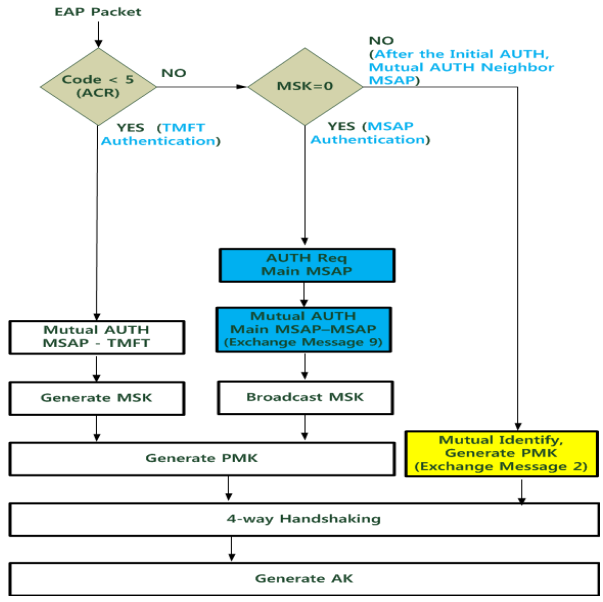


그림 8. 인증요청받는 MSAP의 메시지 처리 순서도
Fig. 8. A flowchart for Message Handling of Authentication Requested MSAPs

단하여 이웃MSAP와 분산형 인증을 수행한다.

Ⅳ. 제안된 시나리오 검증

MSAP와 이웃MSAP간 인증시 표1과 같이 중앙집중형[9] 인증기법의 경우, MSAP는 초기 인증뿐만 아니라 이웃MSAP간 인증에도 그림 9의 중앙집중형 인증기법과 같은 순서도에 의해 매번 인증서버에 접속하여 인증절차를 수행해야 한다. 그러므로 인증 과정에서 지연되고 인증 메시지 오버헤드가 발생하며 MSAP 이동시 이웃MSAP들간 인증에서도 똑같은 방식으로 인증함으로서 중심MSAP의 인증서버에 로드가 많아지는 문제가 있다.

분산형[10] 인증기법의 경우, 중앙집중형 인증기법과 달리 중심MSAP를 거치지 않고 각 MSAP들간 그림 9의 분산형 인증과 같은 순서도에 의해 Peer-To-Peer 인증을 수행한다. 분산형 인증기법을 적용하기 위해서는 각 MSAP간에 미리 인증에 필요한 정보를 공유하고 있어야 하는 보안상 문제점이 있으며 이웃MSAP와 협업을 통해 새로운 MSAP를 인증할 수 있으나 군 환경상 최악의 상황을 고려하여 1개의 메쉬망이 구성되었을 경우, 이웃MSAP간 협업을 통해 인증하면 보안상 매우 취약하고 주변 악의적인 MSAP들의 공모에 의해서도 보안상 취약할 수 있다.

개선된 분산형[7] 인증은 그림 9의 개선된 분산형

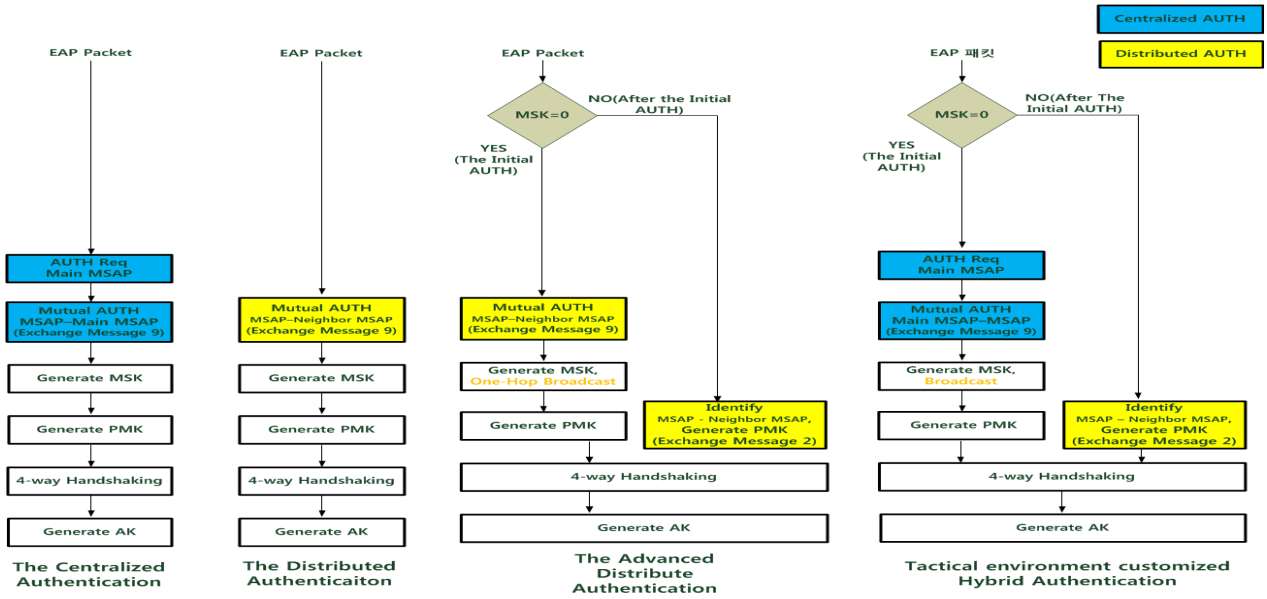


그림 9. MSAP간 각 인증별 인증요청 메시지 처리 순서도
Fig. 9. A flowchart for Authentication Request Messages in between MSAPs

인증기법과 같은 순서도에 의해 인증이 수행된다. 초기 인증시에는 기존의 분산형 인증절차와 동일하지만 이웃MSAP와 인증시 인증절차를 생략함으로서 인증처리시간을 단축시킬 수 있는 점이 다르다. 즉, 초기 인증시 9개의 인증 메시지를 교환하고 MSK의 생성 및 One-Hop Broadcasting 한다. 이를 통해 이웃MSAP간 인증은 9개의 인증 메시지를 교환 하는 것이 아니라 단지 확인절차상 2개의 메시지를 통해 신뢰성 있는 통신망을 구성한다. 따라서 기존의 분산형 인증절차 보다 적은 인증 메시지 교환으로 빠르게 인증 할 수 있다.

군 환경에 적합한 혼합형 인증기법은 MSAP가 초기 인증 받을 경우, 중앙집중형 인증기법을 수행함으로서 앞에서 설명한 분산형 인증기법의 문제점을 해결 할 수 있다. 또한 군의 특수한 전술환경상황에서 전술이동통신체계의 중심이 되는 MSAP만이 하위부대들의 인증을 담당하게 하여 MSAP가 적에 의해 피탈되었다 하더라도 전술이동통신체계의 접근을 효율적으로 차단할 수 있다. 그리고 MSAP가 메쉬망에서 빈번한 이동을 할 경우, 이웃MSAP간 신속한 인증을 받기 위해 분산형 인증기법을 병행하여 사용한다. 즉, 그림 9의 혼합형 인증과 같은 순

표 1. 각 인증기법 장·단점 분석
Table. 1. A Comparison of the Proposed Scheme with Other Authentication Schemes

	Centralized Authentication Methods[9]	Distributed Authentication Methods[10]	Advanced distributed Authentication Method[7]	Proposed, Hybrid Authentication Scheme for Tactical Networks
Advantages	· Efficient management of authentication · High level of security	· Fast mutual Authentication · Distribution loads of authentication server	· Fast mutual Authentication · Distribution loads of authentication server	· High level of security and Efficient management of authentication · Fast mutual Authentication
Disadvantages	· Additional response time · Increasing loads of authentication server	· Necessity of advanced neighbor MSAP · Possibility of mis-authentication by adversary nodes	· Necessity of advanced neighbor MSAP	· Overload of main MSAP for authentication

서도에 의해 초기 인증시 중앙집중형 인증기법으로 인증하고 MSK를 생성하여 전술이동통신 네트워크 내에 포함된 모든 MSAP에게 Broadcasting 한다. 그 이후 이웃MSAP간 인증시 기존의 중앙집중형 인증이 아닌 분산형 인증으로 단지 확인절차상 2개의 메시지를 통해 신뢰성 있는 통신망을 구성한다. 하지만 초기 인증할 경우, 중앙집중형 방식을 따라 중심MSAP가 전술이동통신 네트워크에 포함된 모든 MSAP들의 인증관련 정보를 관리하고 있으므로 적에 의해 피탈되면 모든 정보를 노출 될 수 있는 단점이 있다. 본 논문에서는 중심MSAP가 적과 조우지역에 위치한 위험한 제대를 선정한 것이 아니라 적 후방지역, 아군의 방어가 가능한 안전한 지역의 중심MSAP로 선정함으로서 이를 어느 정도 극복할 수 있다고 판단한다.

그림 10은 One-Hop내에 있는 MSAP들이 서로 메쉬망을 구성하려고 할때 MSAP의 수를 증가시키며 메시지 교환 횟수를 그래프로 분석하였다. 즉, X축은 MSAP의 수를 나타내고 Y축은 인증요청 메시지 교환 횟수를 나타내고 있다. M은 전체 인증메시지 교환 횟수라 정의하고 인증 메시지 교환 횟수를 계산하기 위해 중앙집중형 인증기법은 (1)과 같은 수식을 사용하였다. 초기 9개의 인증 메시지를 교환하고 이웃MSAP간 9개의 인증 메시지를 교환하는데 항상 중심MSAP를 다시 거쳐서 인증 받으므로 α(Hop 수)에 더하기 1를 하여 9개 메시지를 중심MSAP에게 전달하게 된다. 이웃MSAP의 수에 따라 위 같은 절차가 반복 되므로 β(이웃MSAP의 수)를 곱하여 MSAP의 인증 메시지 교환 횟수를 계산할 수 있다.

$$M = 9+((\alpha+1)*9)*\beta \quad (1)$$

분산형 인증기법은 간단하다. 인증정보를 모든 MSAP가 각각 보유하고 있기 때문에 이웃해 있는 MSAP의 수에 따라 인증 메시지 교환을 (2)와 같이 계산할 수 있다.

$$M = 9*\beta \quad (2)$$

개선된 분산형 인증기법은 (3)과 같이 초기 9개의 인증 메시지를 교환하고 이웃MSAP간 2개의 인증 확인 메시지를 교환함으로서 신뢰성 있는 통신망을 구성할 수 있다.

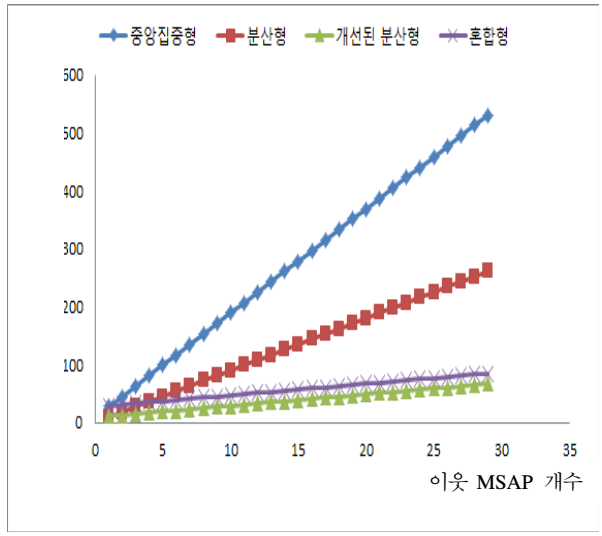


그림 10. 초기인증과 이웃MSAP간 인증
Fig. 10. Initial and authentication process between neighboring MSAPs

$$M = 9+(\beta*2) \quad (3)$$

혼합형 인증기법은 (4)와 같이 초기 9개의 인증 메시지를 교환하고 α(hop 수)에 의해 메시지 교환 횟수가 증가할 수 있으며 이웃MSAP간 2개의 인증 확인 메시지를 교환함으로서 신뢰성 있는 통신망을 구성할 수 있다.

$$M = 9+((\alpha+1)*9)+(\beta*2) \quad (4)$$

그림 10은 개선된 분산형과 혼합형 인증기법은 초기인증 후 이웃MSAP간에 인증시 인증절차를 단축시킴으로서 인증요청 메시지 교환 횟수가 상당히 줄었음을 알 수 있다. 비록 혼합형 인증기법이 개선된 분산형 인증기법보다 우수하지 않고 비슷한 성능을 보였으나 전술이동통신체계에서 MSAP의 기능을 발휘하기 위해 항상 중심MSAP에게 통신망이 구성되어 전술C4I체계에 접속해야 하므로 군 환경상 중심MSAP가 전술이동통신 네트워크 예하 MSAP들의 인증정보를 담당하여 보안을 강화하고 개선된 분산형의 성능과 비슷한 혼합형 인증기법이 차세대 전술이동통신체계에서 적합함을 알 수 있다.

Ⅲ. 결 론

본 논문은 차세대 전술이동통신체계에서의 MSAP간 메쉬망을 구성하는 환경에서 각각의 MSAP가 올바른 MSAP인지 인증하기 위해 군 전

술이동통신환경에 적합한 혼합형 인증기법을 제안함과 동시에 각각의 개체에 의해 인증 받는 알고리즘이 다르므로 인증요청 받은 MSAP의 제어대(ACR)에서 EAP 패킷의 Code 부분을 확인하여 처리하는 방안도 제안하였다. 이것은 위에서 설명했듯이 MSAP 특성상 각각의 MSAP가 인증서버를 갖고 있기 때문에 가능하였다. 따라서 혼합형 인증기법은 인증을 위한 네트워크 부하를 줄이고 인증키를 중심MSAP에서 관리함으로서 각각의 MSAP들이 전술이동통신 네트워크의 접근통제를 강화 할 수 있으며 군 환경에서 일어날 수 있는 적에 의한 MSAP피탈 및 주변 MSAP들의 공모에 의한 악의적 MSAP의 문제도 강력하게 대응할 수 있을 것이다.

참 고 문 헌

[1] C.W. Lee, S.J. Choi, C.S. Lee, “Information Assurance Framework For NCW,” KISE, vo.l 24, no. 9, pp.57-63, 2006.

[2] G.S. Park, J.s. Hwang, “TICN System Requirement and Capability for Future Warfare Environment”, Telecommunications Review, vol. 20, no. 2, 2010.5.

[3] Y.J Hoon, et al., “Mobile WiMAX based Performance analysis of Tactical Mobile Communication System Test bed ,” KICS, vol. 26, no. 3, pp. 9-15, 2009.

[4] [EAP-AKA] RFC 4187, http://www.ietf.org/rfc/rfc4187.txt

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

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

[7] Y.J. Son, B.G. Bae, et al., “Mutual Authentication Method between Wireless Mesh Enabled MSAPs in the Next-generation,” KICS, vol. 37, no. 5, May, 2012.

[8] Y. Lee, et al., “Design of Hybrid Authentication scheme and key distribution for mobile multi-hop Relay in IEEE 802.16j”, Proc. of Euro American Conference on Telematics and Information Systems, 2009.

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

[10] C. Kaufman. DASS Distributed Authentication Security Service, September 1993. RFC 1507.

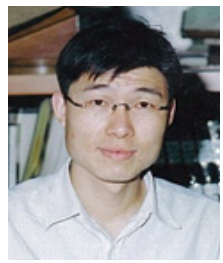
배 병 구 (Byoung-Gu Bae)

2003년 2월 3사관학교 전산정보처리학과

2010년 3월~현재 아주대학교 NCW 석사 재학 중

<관심분야> 전술통신체계, 컴퓨터 네트워크

윤 선 중 (Sun-Joong Yoon)



1997년 숭실대학교 컴퓨터학부

2004년 국방대학원 전산정보학과

2011년 아주대학교 일반대학원 NCW공학과 박사

2011년~현재 전투지휘훈련단

<관심분야> 군 전술네트워크(TICN, 전술데이터링크), 지오캐스팅, 무선 메쉬 네트워크, MANET 등

고 영 배 (Young-Bae Ko)

1991년 2월 아주대학교 전자계산학 학사

1995년 2월 아주대학교 MBA 경영정보학 석사

2000년 7월 Texas A&M Univ. 컴퓨터공학 박사

2000년~2002년 미국 IBM T.J 왓슨 연구소 전임연구원

2002년 9월~2011년 아주대학교 정보컴퓨터공학부 정교수

2012년 아주대학교 소프트웨어융합학과, 일반대학원 컴퓨터공학과 및 NCW학과 정교수

<관심분야> Wi-Fi Technology, MANET, 미래인터넷 CCN, 군 전술네트워크 등