전술용 인터넷의 보안 기술 연구*

김 점 구**

요 약

차세대 군 전술용 정보 네트워크는 상용 인터넷 기술을 기반으로 전술환경에서 데이터, 음성 및 영상 등의 다양한 정보 제공을 목표로 하는 전술용 인터넷(TI : Tactical Internet)으로 발전되는 추세이다. 한편, 미군(美軍)을 중심으로 전술용 인터넷에 상용 정보통신 기술의 도입이 급속히 진행됨에 따라 전술용 인터넷에 대한 위협과 공격유형은 점차 다양한 형태로 변화하고 있다. 본 논문에서는 차세대 전술용 정보 네트워크로써 전술용 인터넷을 수용하는 경우, 고려할 수 있는 보안요소 및 기술들을 살펴보고 이를 기반으로 전술용 인터넷에 대한 보안 방안에 대해 논하고자 한다.

Security Technology in Tactical Internet

Jeom Goo Kim*

ABSTRACT

There is a tendency that next-generation tactical information network for the military has been developed from tactical environment based on commercial Internet technology to Tactical Internet(TI) of which purpose is providing various informations such as data, voice and image. On the other side, with an introduction of commercial information communication technology onto Tactical Internet had progressed rapidly on the basis of U.S. Army, threats and attack patterns against Tactical Internet have changed into various types gradually. In this paper, we will examine security factors and technologies to be considered in case of accepting Tactical Internet as a next-generation tactical information network, and discuss its countermeasures with those technologies for a basis.

Key words : Tactical Internet, Security

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2006-C1909-0603-0027).

** Dept. of Computer Sciene, Namseoul University

1. 서 론

최근 정보화 사회로의 변화가 급격히 진행됨에 따라 21세기 전장의 패러다임은 기동력 및 화력 중심에서 정보전과 체계 통합전 형태로 바뀌어 가고 있다. 이와 함께 전술용 전장 환경에서 '정보우위의 확보'가 매우 중요한 요소로 대두되고 있으며, 이를 달성하기 위해 전장의 디지털화에 관한 연구가 활발히 진행 중에 있다.

이를 통해 나타난 개념인 전술용 인터넷(TI: Tactical Internet)은 전장의 시스템 및 전투원에게 효과적이고 빠른 지휘 명령과 전술 정보를 전달하기 위해 다양한 무선통신 방식이 통합된 형태의 디지털 정보 네트워크를 말한다. 이러한 전술용 인터넷은 TCP/IP 프로토콜 기반의 상용 인터넷과 유사한 기능을 수용하면서 전술 환경에서 음성, 데이터 및 영상 등의 다양한 종류의 원활한 정보 제공을 목표로 하고 있다[1].

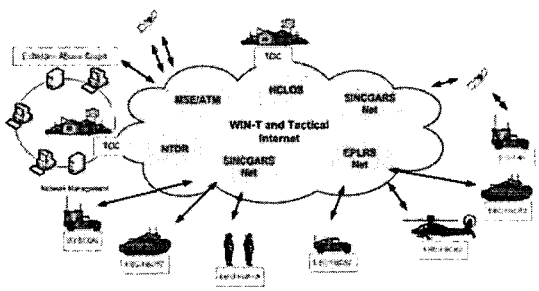
상업용 통신망과 달리 군사용 통신망은 보안 사항이 가장 중요시되는 통신망이다. 따라서 상업용 통신 기술을 도입하게 되는 전술용 정보 네트워크의 위험 요소를 분석하고 이를 통한 보안 방안에 대한 연구가 활발히 진행되고 있다. 그러나 지속적으로 정밀화 되고 있는 사이버테러 및 정보전에 대한 대응 방안은 여전히 미흡한 상태이며, 상용 인터넷 체계와의 연동으로 인한 군사 정보시스템 및 전술정보에 대한 보안 정책과 구조에 대한 연구의 부족으로 인해 효율적인 보안 방안이 도출되지 못하고 있는 상황이다.

본 논문에서는 미군(美軍)의 차세대 전술용 정보 네트워크로서 고려되고 있는 전술용 인터넷에 대한 구조와 위험요소를 살펴보고 이를 바탕으로 전술용 인터넷에 적용 가능한 보안 방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 전술용 인터넷의 구조를 살펴보고 제 3장에서는 전술용 인터넷상의 다양한 위협 형태와 보안상의 문제점을 간략하게 살펴보고, 이를 통해 전술용 인터넷의 보안 방안을 제안한다. 제 4장에서는 결론 및 향후 연구과제에 대해 논한다.

2. 전술용 인터넷

전술용 인터넷의 목적은 전장의 시스템을 디지털화하면서 전략적으로 배치한 상위 제대(battalion)와 하위 여단(brigade)간의 효율적인 명령 체계 및 제어 능력, 그리고 다양한 통신 서비스를 요구하는 전장의 전투병에게 신뢰성 있는 정보 전송 능력을 제공하는 것이다. 이러한 전장 디지털화를 지원하기 위해서는 디지털 통신 기술과 정보 관리 기술이 수평적, 수직적으로 통합된 디지털 정보 네트워크가 요구되며, 전술환경에서 안전한 통신 서비스 제공을 위해 높은 신뢰성과 안정된 접속을 보장해야 하는 등, 전술적 사용자들에게 적합한 일정 성능 이상을 제공할 수 있어야 한다. (그림 1)은 전술용 인터넷의 구조를 보여주고 있다.



(그림 1) 전술용 인터넷의 구조

(그림 1)에서 전술용 인터넷은 상위 전술용 인터넷과 하위 전술용 인터넷으로 구분되며 상위 전술용 인터넷은 상급부대와 분산된 부대들간 원활한 정보 교환을 가능하게 하는 통신자원들로 구성되고 하위 전술용 인터넷은 여단 및 이하 급 단위의 통신을 지원하는 시스템들로 구성된다. 상위 전

술용 인터넷에는 기존의 ATM(Asynchronous Transfer Mode)기술을 기반으로 하는 MSE(Mobile Subscriber Equipment) 전술용 패킷망(TPN : Tactical Packet Network)과 상용 IP기술을 기반으로 WIN-T(Warfighter Information Network-Tactical)가 포함된다. 하위 전술용 인터넷에서 사용되는 통신시스템에는 주로 여단(brigade) 및 이하 급 지휘체계(FBCB 2 : Force XXI Battle Command, Brigade and Below)의 컴퓨터들, EPLRS, NTDR, SINCGARS 등이 포함된다. 그러나 현재 개발이 진행 중에 있는 SDR 기반의 합동 전술 무선 시스템(JTRS : Joint Tactical Radio System)과 무선랜(WLAN) 등이 향후 NTDR, SINCGARS 및 EPLRS 등의 대체 시스템으로 예상되고 있다[2, 3, 4].

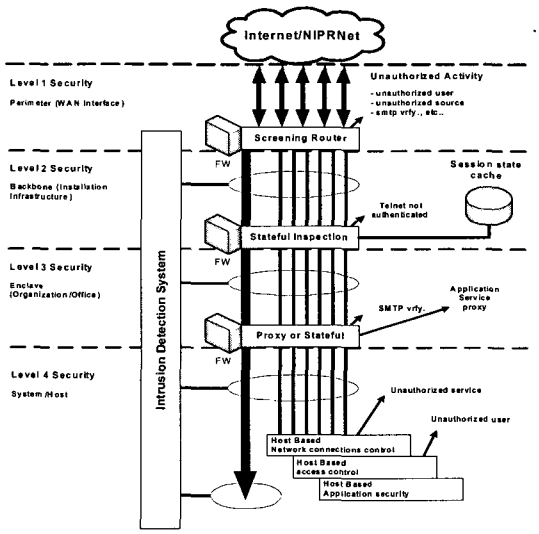
3. 전술용 인터넷의 보안방안

전술용 인터넷상의 정보 및 정보 시스템을 보호하기 위한 개념은 기존의 수동적 보안 형태인 "정보보호(Information Security)"에서 적극적 개념인 "정보보증(Information Assurance)"으로 강화되어야 한다. 정보보증이란 정보 및 정보 시스템의 가용성, 무결성, 인증, 비밀성 및 부인방지를 보장하여 정보 및 정보 시스템을 보호하고 방어하는 것을 의미하며, 외부로부터의 침입으로부터 중요 정보통신 기반을 보호하고 침입을 탐지하고 침입에 대한 능력 배가 및 이의 조화에 의하여 정보 시스템을 복원하는 능력이 포함되어야 한다[5].

또한 전술용 인터넷은 1급 비밀(classified type 1)정보와 SBU(sensitive but unclassified, classified type 2) 정보를 안전하게 전송하는 것을 보장하고 전술작전본부(TOC : Tactical Operation Center)와 여단(brigade) 및 그 이하의 작전 단위 사이에 이동성(mobility), 보안성(security), 생존성(survivability)등의 특성을 갖는 통신 서비스를 제공하는 전술용 통신 시스템이다. 여기서 SBU란 1급 비밀로 분류되지는 않았지만 정보의 누출이 국가 안보에 영향을 줄 수 있는 정보를 의미한다. 정보의 신뢰성과 보안성을 제공하기 위해서는 네트워크 보안(Network Security)과 통신 보안(Communication Security)을 고려할 수 있다[6].

3.1 정보 보증(IA : Information Assurance)

전술용 인터넷의 정보보증 방안은 NSIP(Network Security Improvement Program)의 I3A(Installation Information Infrastructure Architecture) 프로젝트에서 제시하는 심층 방어(defense in depth) 개념을 도입함으로써 전술용 인터넷의 백본망과 군사용 통신 장비를 보호하기 위한 수단으로 고려될 수 있다. I3A 심층 방어의 핵심은 특정 위협요소와 취약점에 대한 대응방안으로 전술용 인터넷의 구성요소들을 4계층(system/host, enclave, backbone, perimeter)으로 구분하고 요구 사항에 따라 계층별 특정 보안 솔루션(solution)을 제공하는 것이다.



(그림 2) I3A 심층 방어 기반의 정보보증 구조

(그림 2)에서 볼 수 있는 I3A 심층 방어 기반의

정보보증 구조의 기본적인 원리는 단계 1(Level 1)의 원거리 통신망 인터페이스부터 단계 4(Level 4)의 종단 시스템/호스트까지 데이터가 이동할 때 각 단계별 보안 등급을 설정하여 허용 가능한 데이터의 특성을 제한하는 것이다. 이러한 계층적인 보안 접근 방안은 각 단계에서 시스템들이 요구하는 보안사항들과 통신 장비들 간의 호환성(interoperability)을 유지해야 하며, 구현되는 보안 솔루션의 적합성이 고려되어야 한다.

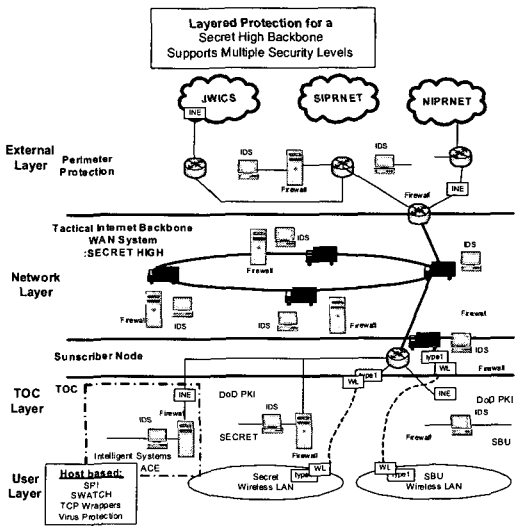
이러한 접근방법에 기초한 정보 보증 원리는 인증된 사용자(user)의 제한적인 정보 및 서비스로의 접근을 허용하는 동시에 외부 공격자로부터 내부 시스템 및 통신 자원을 보호하는 것이 목적이다. 따라서 (그림 2)와 같은 정보보증 구조는 외부 공격자가 단계 별 잠재적인 위협 요소와 취약점을 통해 내부 시스템 및 통신 자원으로의 접근 하는 것을 방지하거나 위협의 완화 혹은 제거하기 위한 방안을 제공해야 한다. 또한 악성 바이러스(virus)에 의한 감염과 의도적 독립 코드(e.g. Active X, Java, Javascript)와 같은 다른 형태의 공격으로부터 기간 시설을 보호하기 위해 지속적인 위험 요소의 측정도 이루어져야 한다[7].

3.2 네트워크 보안

전술용 인터넷의 보안체계는 I3A 심층 방어 기반의 정보보증 구조를 적용하는 방안이 고려될 수 있다. 즉 전술용 인터넷과 외부 네트워크와의 연결을 제공하는 라우터로부터 내부 정보 시스템에 이르기까지 각각의 영역에 적합한 특정한 보안 솔루션을 적용함으로써 가용성, 무결성, 인증, 기밀성 및 부인방지 등 보안 요구 사항들을 만족해야 한다.

3.2.1 네트워크 계층별 보안 구조

전술용 인터넷의 네트워크 보안은 I3A 심층 방어 개념을 도입한 것으로 다중 보안 장벽을 구축하여 외부 침입자와 내부 공격자에 대응한다. 이러한 장벽들은 보호, 탐지, 반응(reaction) 등의 특성을 갖춰야 하며, 일부 네트워크 계층이 손상 되더라도 나머지 계층들이 필요한 보안 대책을 마련할 수 있게 한다.



(그림 3) 전술용 인터넷 계층별 보안 구조

(1) 외부 계층

전술용 인터넷의 외부 계층은 국방정보통신망의 비화망(SIPRNET : Secret Internet Protocol Router Network), 비비화망(NIPRNET : Non-classified Internet Protocol Router Network)과 같은 외부 네트워크들과의 경계를 말하며 외부로부터의 침입을 방어하기 위한 보안 계층으로서 보안이 가장 강한 층이다. 외부 계층의 방어 초점은 외부에서 내부를 보호하는 것인데 일부 내부에서 외부로 시도한 공격도 고려되어야 한다.

(2) 네트워크 계층

전술용 인터넷의 네트워크 계층은 전술용 인터넷 백본망을 구성하는 유무선 LAN, MSE/TPN, NTDR(Near Term Data Radio) 네트워크 등 최고

의 보안이 요구되는 계층이며, 방어의 초점은 침입 탐지 기능을 통한 네트워크 모니터링으로써 통신 시스템에 대한 공격과 의심스러운 동작을 식별하는 능력을 제공한다.

(3) 사용자 계층

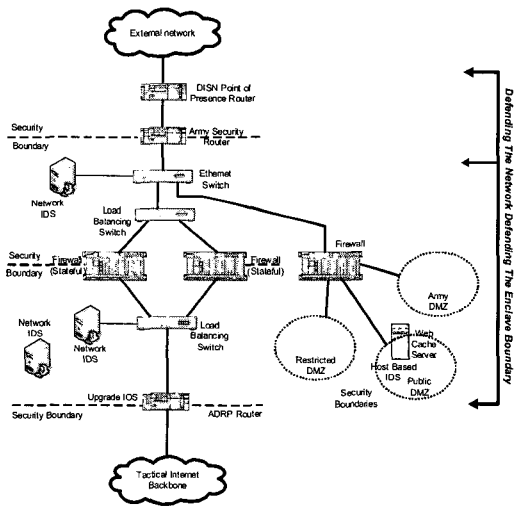
전술용 인터넷의 사용자 계층에서의 방어 초점은 작전본부의 컴퓨터들과 전장에서 사용하는 전술용 단말들을 보호하는 것으로써 바이러스 백신과 Secure OS 등 호스트 기반의 보안 솔루션들이 적용되며, 서버와 종단 시스템에 호스트 기반 모니터링 기능을 상주시켜 기타 호스트부터의 공격을 탐지한다. 또한 전술용 단말에 인증 서비스를 제공하기 위한 PKI 기술도 적용될 수 있다.

3.2.2 보안 기술 적용 방안

I3A 심층 방어 기반의 정보보증 개념을 전술용 인터넷에 적용하는 경우, TLA와 DMZ 구조를 고려할 수 있다.

TLA(Top Level Architecture)는 전술용 인터넷의 백본망과 국방정보통신망 사이의 네트워크 경계에 위치하며, ASR(Army Security Router), ADRP (Army Defense Information Systems Network Router Program) 라우터, 이더넷 스위치, 침입탐지시스템 등 보안 시스템으로 구성된다. ASR는 외부 네트워크에서 전술용 인터넷으로의 제한적인 접근을 제공함으로써 ASR의 라우팅 테이블(routing table)내에 접근제어리스트(ACL : Access Control List)를 참조하여 의심되는 특정 포트에 대한 응답 서비스를 차단한다. 이더넷 스위치와 침입탐지시스템은 의도적인 공격의 신속한 탐지와 대응을 위해 실시간의 감시 능력을 제공한다. ADRP 라우터는 ASR과 동일한 기능을 수행하며, ADRP 라우터의 접근제어리스트는 전술용 인터넷의 네트워크 관리자에 의해 관리됨으로써 ASR보다 더 강력한 접근통제 기능을 수행하게 된다.

DMZ(DeMilitarized Zone)는 전술용 인터넷 백본망의 구성요소 중, 물리적 혹은 논리적으로 구분되어 질 수 있는 통신장비들을 이용하여 보다 높은 보안 등급의 네트워크를 구성하는데 적용될 수 있으므로 DMZ를 이용한 네트워크 구성은 외부 사용자와 시스템들에 대해 보안사항이나 접근제어를 강화하기 위한 방안이라고 볼 수 있다. DMZ 내에 위치해야 하는 전술용 인터넷상의 요소는 외부 시스템과의 인터페이스 역할을 수행하며, 전술용 인터넷으로의 제한적인 접근을 허용하는 시스템과 접근을 허용하지 않는 시스템이 있다.



(그림 4) Enhanced TLA

최근 전술용 정보네트워크로의 공격빈도가 점차 증가하고 정교해짐에 따라 독립적인 TLA 혹은 DMZ를 이용한 보안 구조로는 전술용 인터넷과 내부 시스템의 보안 요구 사항들을 충족시키기엔 부족한 점이 있다. 이러한 측면에서 (그림 4)는 DMZ 구조가 TLA에 부가되어 보안 기능을 향상시키는 방안으로 고려될 수 있다[7].

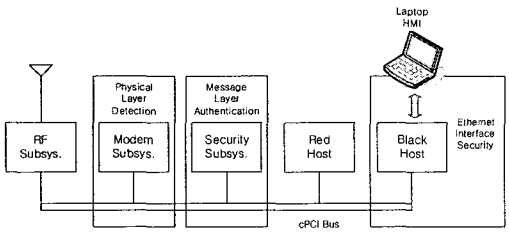
3.3 통신 보안

전술용 인터넷의 통신 보안은 SDR, 무선랜 등

의 상용통신 기술의 도입으로 인한 보안 문제점에 주안점을 둘 수 있다. 일반적으로 SDR, 무선랜 등의 무선통신은 전송장비와 단말들을 통과하는 음성이나 데이터를 보호하기 위해 주파수 도약(FH : Frequency Hopping)과 시분할(TD : Time Division) 등의 기술들이 사용된다. 또한 무선통신 상에서 송/수신 되는 정보를 보호하고자 LPI(Low Probability of Intercept) 기술, 주파수 도약, 대역 확산(spread spectrum) 등의 전송 기술, 벌크 암호화/복호화(bulk encryption/decryption) 기술들을 적용하여 정보의 노출, 수정 및 차단을 방지한다[8].

3.3.1 SDR 보안

기존 무선분야 정보전(IW : Information Warfare)의 영역에서 대부분의 공격 행위(cyber attack)는 물리적인 취약점에 대한 공격에 집중하였으나, 최근의 공격 유형(type of attack)은 전파 파형(RF waveform), 통신 신호 그리고 무선망의 백본망 침투를 통해 전파 신호 분열에 주안점을 두는 보다 진보된 전략을 추구하고 있다. 따라서 접근제어(access control), 메시지 인증, 그리고 근거리통신망 보안을 고려한 SDR 시스템의 설계방안은 SDR 환경의 정보전에서 외부 공격에 대한 보호와 탐지를 위한 핵심 사항이라고 볼 수 있다.



(그림 5) SDR 시스템 보안 구조

(1) 물리적 계층 탐지

SDR 시스템에서 외부의 공격의 침입에 대해서는 안정성이 강화된 파형(waveform)의 적용을 통해 위험성이 다소 완화될 수 있을 것이다. 따라서 주파수 호핑과 분산(spreading) 그리고 전파(RF : Radio Frequency) 장애를 제한시키는 파형들에 대한 적용방안이 SDR 시스템을 보호하는 방안으로 볼 수 있다.

(2) 메시지 계층 인증

SDR 시스템의 보안 사항 중, 메시지(message) 인증 절차는 외부 공격에 다소 취약한 하위 시스템들을 목표로 하는 공격 행위로부터 보호하기 위한 것이며, 임의의 메시지를 수신하는 경우, 사전에 규정된 사항을 검사하여 인증 여부를 확인하기 위한 절차가 필요하다. 이러한 인증 절차는 물리적 계층에서 방해 전파(jamming)를 탐지한 후에 이에 대응할 수 있는 보안 능력을 지원하기 위한 것이다.

(3) 이더넷(Ethernet) LAN 보안

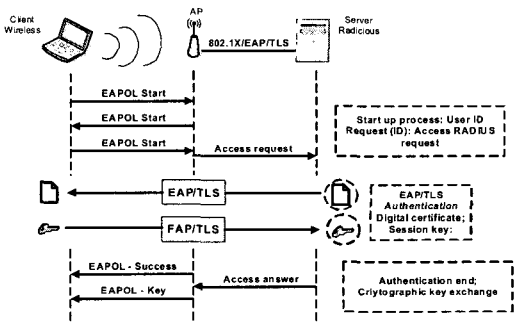
SDR 시스템은 원격 제어 및 근거리 통신망에 대한 제한적인 접근을 허용하기 위해 설계된 이더넷 포트를 적용하고 있다. SDR 시스템을 이용하여 전술작전을 전개하는 전장(battlefield)의 전술작전본부(TOC : Tactical Operation Center)의 경우, 이더넷을 이용하여 근거리 통신망을 구축하고 SDR 시스템의 무선링크를 통해 인증되지 않은 공격자가 내부 네트워크로 접근하는 것을 제한하도록 하고 있다[9].

3.3.2 무선랜(WLAN) 보안

전술 환경에서 무선랜 시스템의 안전한 보안체계를 구축하기 위해 EAP/TLS 보안 프로토콜을 이용한 RADIUS 서버의 적용 및 IEEE 802.1x의 듀얼 도어 액세스(dual door access) 기반의 인증 메커니즘의 적용이 고려될 수 있다[10]. 여기서 듀얼 도어 액세스는 액세스도어(access door), 서비스도어(service door)로 구성되며, 액세스도어는 액세스포인트, 서비스도어는 인증서버(RADIUS)를

의미한다.

이러한 무선랜 보안 체계를 통해 전장의 전투원을 포함한 사용자(user)들이 전술용 인터넷에 액세스(access)하는 경우, 사용자 인증 과정 중에는 액세스도어(access door)을 통해 인증과 신원확인 서비스로의 접근은 가능하지만 전술용 인터넷과 무선랜을 통한 통신 서비스는 제공되지 않는다. 그러나 액세스도어와 서비스도어를 통해 성공적인 인증절차를 완료한 경우, 전술용 인터넷과 무선랜을 통해 필요로 하는 통신 서비스를 제공받을 수 있다[11].



(그림 6) 전술용 무선랜 인증 절차

(그림 6)은 RADIUS 인증 서버를 사용하여 인증절차를 수행하는 전반적인 과정을 보여주고 있으며, 디지털 인증을 위한 EAP/TLS 통신 프로토콜을 이용하여 보다 강화된 보안계층(security layer)을 적용하고 있다. 여기서 EAP/TLS는 인터넷 전송계층에 암호채널을 형성하고자 하는 사용자(user)들이 핸드쉐이킹(handshaking) 기법을 통하여 상호인증 및 키 분배를 수행한 후, 송수신 되는 모든 메시지를 대상으로 기밀성을 제공하는 보안 프로토콜이다. 무선단말과 인증서버는 상호인증을 위한 디지털 인증서(digital certificate) 및 세션키(session key)를 EAP/TLS 통신 프로토콜을 이용하여 할당 받는다. 무선단말은 이 키를 이용하여 무선단말과 액세스포인트간의 무선링크 상에서 교환되는 메시지를 암호화하여 전송하게 된다[12].

4. 결 론

본 논문에서는 미군(美軍)에서 고려하고 있는 전술용 인터넷의 구조 및 통신기술들을 살펴보고 이에 따른 위협요소 및 보안상 취약점을 살펴보았다. 그리고 전술용 인터넷에서 고려할 수 있는 보안기술로서 방화벽, 침입탐지 시스템, 침입방지 시스템, SDR 보안, WLAN 보안 등의 정보보호 기술을 분석하여 전술용 인터넷에 필요한 보안 기술을 제시하였으며, I3A 심층분석 기반의 정보보증 체계의 분석을 통해 전술용 인터넷에 적용 가능한 정보보증 구조 및 체계를 제시하였다.

최근 IETF의 NEMO WG을 중심으로 IPv6 기술의 도입을 통해 네트워크 이동성(Network Mobility)의 지원을 위한 구조와 프로토콜에 대한 연구가 진행되고 있으며, 군사 분야에서도 이의 도입을 통한 IPv6 기반의 통신 체계로의 전환을 준비중에 있다. 따라서 전술용 인터넷의 체계가 IPv6 기반의 체계로 전환되는 경우, 발생할 수 있는 보안사항에 대한 분석을 통해 보다 안전하고 고급화된 통신 서비스를 제공할 수 있는 방안에 대한 연구가 필요할 것으로 보인다.

참 고 문 헌

[1] David A. Hall, Tactical Internet System Architecture for Task Force XXI, IEEE MILCOM 1996.

[2] Igal P. Sharret, WIN-T-The Army's New Tactical Intranet, IEEE MILCOM 1999.

[3] Pual Sass, Communications Networks for the Force XXI Digitized Battlefield, Baltzer Science Publisher 1999.

[4] Lt Col J. Place, D. Kerr, and D. Schaefer, Joint Tactical Radio System, IEEE MILCOM 2000.
[5] IATF, Information Assurance for the Tactical Enviroment, IATF Document 2002.
[6] Keith Rohwer, Timothy Krout, Multiple Level of Security in Support of Highly Mobile Tactical Internet-ELB ACTD, IEEE MILCOM 2001.
[7] Ted Hendy, An Information Assurance Architecture for Army Installations, IEEE MILCOM 2000.
[8] D. Torrieri, "Frequency Hopping and Future Army Mobile Communications", Proceedings, ATIRP Annual Conference, University of Maryland, 1997.
[9] Scott Chuprum, Chad Bergstrom, Bruce Fette, SDR Strategies for Information Warfare and Assurance, IEEE MILCOM 2000.
[10] Marco Carli, Andrea Rossetti, Alessandro Neri, Integrated Security Architecture for WLAN, IEEE Telecommunications 2003.
[11] C. Rigney, Remote Authentication Dial In User Service(RADIUS), IETF RFC 2865, June 2000.
[12] P. Calhoun et al, PPP EAP TLS Authentication Protocol, IETF RFC 2794 Mar 2000.

김 점 구

광운대학교 전자계산학과 이학사
광운대학교 전자계산학과 이학석사
한남대학교 컴퓨터공학과 공학박사
(주) 제성프로젝트 연구원
(주) 시사컴퓨토피아 인터넷사업본부장
현재 남서울대학교 컴퓨터학과 교수
관심분야 : 정보보호, 컴퓨터 네트워크, 무선통신