TICN(Tactical Information Communication Network) 정보보호 기술 개발 동향

김응준* · 김동규**

1. 서 론

정보통신 기술 및 네트워크 인프라의 발전으로 미래의 전장 환경은 플랫폼 중심에서 통신망과 응용체계가 통합된 네트워크 중심의 지휘통제가 이루어 지는 NCW(Network Centric Warfare : 네트워크 중심전)로 이동할 것이다. NCW는 현재 미 국방성의 전력변환에 있어 중요한 주제가 되고 있으며 유럽의 여러 국가는 물론 호주나 싱가폴에도 확산되어 군사발전의 중심점이 되고 있다. 우리나라도 NCW 의 필요성을 인식하고 한국적인 개념 정립과 구현을 추진 중에 있어 향후 미래 국방의 중심이 될 것은 자명한 것으로 보인다.

NCW환경에서 전술정보통신체계의 역할을 하고 있는 TICN(Tactical Information Communication Network: 군 전술정보통신체계)은 다원화된 군 통신망을 일원화하고 다양한 전장 정보를 적시 적소에 실시간으로 전달해 정확한 지휘통제 및 의사결정을 가능하게 하는 미래형 군 전술종합정보통신체계를 말한다.

또한, 현재 육군에서 운영 중인 SPIDER[1] 전술통신체계와 전투무선망을 2013년부터 대체해 고속, 대용량, 원거리, 무선중계 전송으로 발전시키기 위한 사업이다

정보통신기술의 발전으로 인해 전쟁의 패러다임은 근본적으로 변하고 있다. NCW환경의 TICN체계 내에서는 정보량이 급격히 증가하고 시스템 운용개념이 복잡해 짐에 따라, 정보보호 측면에서 위협과 취약성이 증가할 것으로 예상된다. 이에 따라 정보보호기술이 TICN에서의 임무수행에 있어 기본적이고 필수적인 기술이 되고

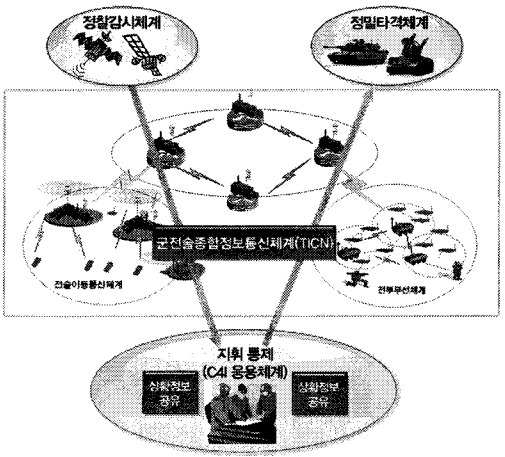


그림 1. NCW 수행 개념도

※ 교신저자(Corresponding Author) : 김동규, 주소 : 서울시 성동구 행당동(-), 전화 : 02)2220-2312, FAX : 02)2220-4312, E-mail : DQKIM@esslab.hanyang.ac.kr
* 한양대학교 전자통신컴퓨터공학과 석사과정 (E-mail : ejkim@esslab.hanyang.ac.kr)
** 한양대학교 전자통신컴퓨터공학과 부교수
※ "본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (IITA-2009-(C1090-0902-0003))

1) 현재 육군에서 운영 중인 격자형 지역지원 통신체계

있으며, 연구수행이 지속적으로 추진되고 있다.

본 논문 2절에서는 TICN체계의 역할과 함께 각 구성요소에 대한 특징을 간단히 살펴보고, 3절에서는 정보보증체계의 근간을 이루고 있는 정보보증 기술 프레임워크(IATF : Information Assurance Technical Framework)를 살펴볼 것이다. 그리고 4절과 5절에서는 TICN체계를 중심으로 진행되고 있는 정보보증 모델에 대한 정의를 통해 앞으로 TICN체계의 정보보호 전략을 제시하고자 한다.

2. TICN의 역할

TICN은 미래 NCW에서 정찰감시-지휘통제-정밀타격체계(C4ISR-PGM)로 이어지는 통합 전투력 발휘를 위해, 고속 대용량 전술정보를 실시간으로 소통시키는 전술통신기반체계로서 ALL-IP기반의 격자형 네트워크로 운용된다.

TICN장비체계는 TICN 내부 및 외부 체계의 멀티미디어 인터페이스를 담당하는 전술통신체계 연동장치, 대용량 무선전송을 담당하는 대용량 무선전송장치, 이동 가입자 연동을 위한 전술용 이동통신 가입자 처리부, 전투무선망을 위한 전술용 SDR, TICN 망 관리 및 제어를 위한 망 제어기 등 총 5개의 장비 체계로 구성되어 있다.

TICN은 총 3개의 무선통신체계와 이를 지원해주는 2개의 지원 기반 체계로 나누어진다.

무선 통신 체계는 전술 이동 간 무선통신을 지원하기 위한 전술이동통신체계, FM, AM과 같은 기존의 무선장비를 하나의 장비로 통합하여 통신하기 위한 전투무선체계, 그리고 대용량의 정보를 긴 거리를 통해 전송하기 위한 기간망 전송 체계, 이렇게 3개로 이루어진다.

지원 기반 체계로는 이 기종망간의 상호 연동을 위한 기간망 교환 접속 체계와 네트워크의 효율적인 제어를 위한 망 제어 체계, 이렇게 2개로 이루어진다.

2.1 전술이동통신체계

전술이동통신체계의 구성장비로는 기지국에 해당하는 M-SAP과 이동단말에 해당하는 TMFT, 이렇게 두 개로 구성되어 있다.

그림 3과 같이 하나의 기지국에 지정되어 있는 각 단말기는 지정되어 있는 기지국을 통해 서로 통신을 수행하며, 통화지역에 포함되어 있지 않은 단말기와 통신을 하기 위해서는 인근 기지국의

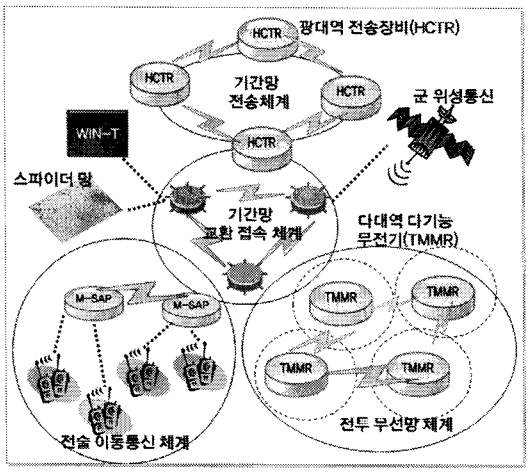


그림 2. TICN 체계 구성도

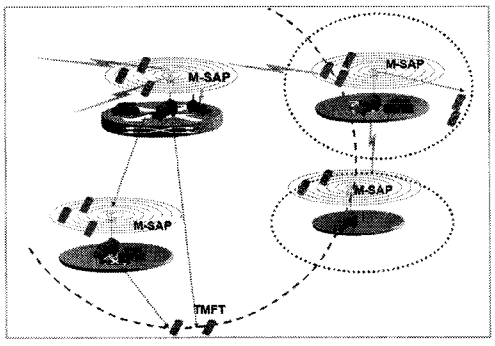


그림 3. 전술이동통신체계 운용개념

도움을 받아야 통신을 수행 할 수 있다.

구성장비의 주요 기능으로는 수Mbps에 달하는 전송용량과 수십 Km에 달하는 통달거리 능력을 보유하고 있다. 그리고 기지국에 해당하는 M-SAP은 이동 중 차량에 탑재되어 기동운용이 가능하며, 이동 중 핸드오버를 지원한다.

2.2 전투무선체계

전투무선체계는 전술인터넷 백본망 및 향상된 무전기를 제공함으로써 전투무선망 네트워킹 능력을 제공해 준다. 또한 기존의 군 무선 통신 체계인 SPIDER체계에서 사용되고 있는 FM, AM과 같은 무전기의 기능을 지원하며, 이대역간 중계역할을 담당한다.

그림 3과 같이 전투무선체계는 AM통신을 위한 HF통신과 FM통신을 위한 VHF통신을 사용하며 Ad-Hoc Network로 구성되어 있어 기반 망 없이도 순수 모바일 노드들만으로 통신이 가능하다.

구성장비의 주요 기능으로는 SDR[2]기반의 무전기 기능과 웨이브폼간 Cross-banding기능, 그리고 Ad-Hoc 네트워킹 기능을 지원한다.

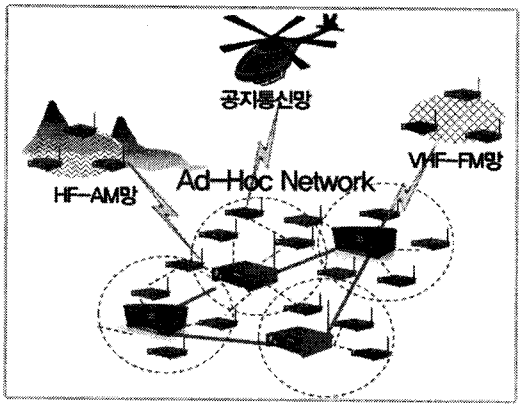


그림 3. 전투무선체계 운용개념

2.3 기간망 전송체계

기간망 전송체계는 노드와 노드, 부대와 노드를 무선으로 연결하는 대용량 전송장비로 대용량 간선 전송로를 제공해준다.

기간망 전송체계의 구성장비로는 RFU(Radio Frequence Unit)와 BBS(Digital Baseband Unit), 그리고 안테나 세트로 나누어 지며, 서로가 분리 운용되어 진다.

구성 장비의 주요 기능으로는 수십 Mbps 급 전송능력과 수십 Km 이상 통달거리를 지원하며, 전자전에 대비하기 위한 대전자전 기능이 운용되어 진다.

2.4 기간망 교환접속체계

기간망 교환접속체계는 통신소 내 유무선 가입자 및 전술이동통신망, 전투무선망 등 다양한 가입자망을 수용하며, 최적화된 경로 설정, 고속 라우팅 및 스위칭 기능을 수행하고 있다.

기간망 교환 접속체계의 주요 기능으로는 전술환경에 적합한 라우팅 기능과, 유무선 가입자 트래픽 교환기능, 전술환경의 특성을 고려한 Qos

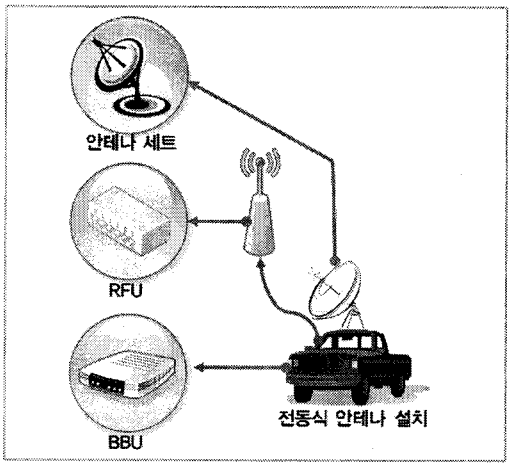


그림 4. 기간망 전송체계 운용개념

2) Software Defined Radio

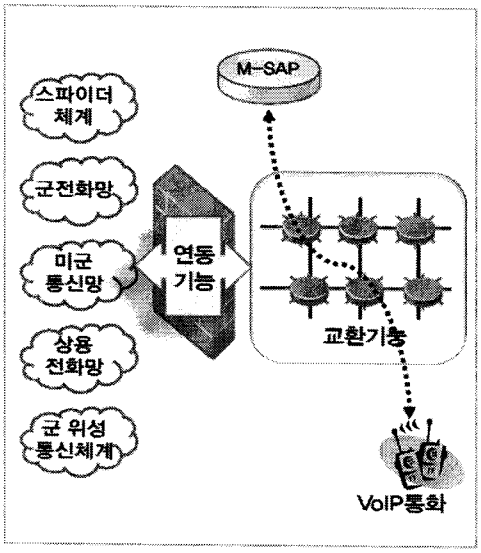


그림 5. 기간망 교환접속체계 운용개념

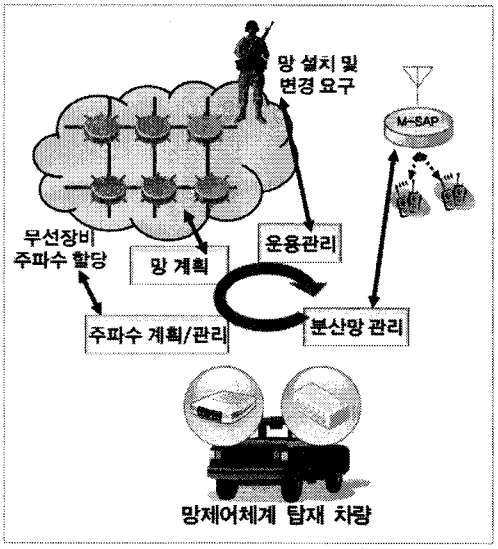


그림 6. 망 제어체계 운용개념

(Quality of System)를 제공해 준다. 또한 주소체계, 가입자 번호체계를 지원해 주며 가입자 와 망의 이동성을 지원해준다.

또한 그림 5 와 같이 다양한 외부체계를 연동해 주는 기능 또한 지원해 준다.

2.5 망 제어 체계

망 제어체계는 부대노드에 설치되어 망을 감시하고 제어를 수행한다.

망 제어 체계의 주요 기능으로는 통신소 업무처리와 자원관리 기능을 담당하며, 망 구성 및 장비 배치 시뮬레이션을 지원한다. 그리고 군단, 사단 단위 WAN/LAN 장비 감시 및 관리 기능과 무선장비 배치, 주파수 할당, 관리기능을 담당한다.

3. IATF의 정보보증

IATF는 미 정부내 보안 관련 부서 및 보안 산업체의 요구에 의하여 국가안보국(NSA: National Security Agency)에 의해 개발된 보안지침 문서로서 정보보증 정책, 기술, 환경 등의 내용을 담고 있다.

IATF는 보편적인 프레임워크를 적용하지 않으므로써 발생할 수 있는 정보시스템의 혼란을 해결하고자 그림 7과 같이 지역 컴퓨팅 환경(Enclave), 엔클레이브 경계, 네트워크 및 기반구조, 그리고 지원 기반구조의 4개 도메인으로 구분

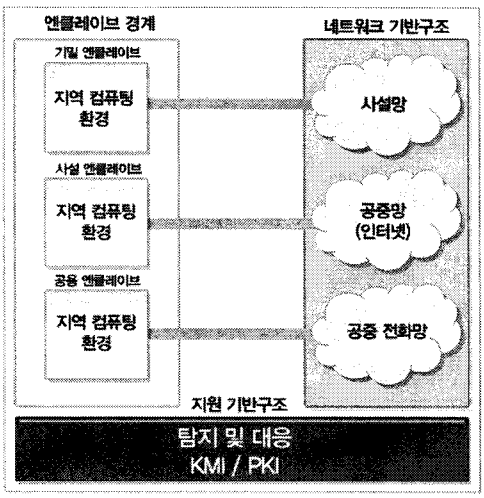


그림 7. IATF 정보보호 도메인

하여 정보시스템의 정보보증기술 양상을 구분하고 프레임워크를 제시하고 있다.

3.1 지역 컴퓨팅 환경 (Enclave)

지역 사용자의 컴퓨팅 환경은 일반적으로 서버, 클라이언트, 서버 및 클라이언트에 설치된 응용을 말한다. 대부분의 조직들은 그들의 임무를 수행할 수 있는 다양한 응용을 사용하고 있지만 현재의 컴퓨팅 환경 보안은 주로 운영체제 및 서버와 클라이언트 시스템에 집중되어 있다.

3.2 엔클레이브 경계 (Enclave Boundary)

엔클레이브는 일반적으로 근거리통신망을 통하여 지역 컴퓨팅 장비들과 상호 연결할 수 있도록 묶어놓은 하나의 지역이며 엔클레이브 경계는 엔클레이브 내부 또는 외부로부터의 정보고 나가고 들어가는 접점이다. 각 엔클레이브들은 외부의 네트워크를 통해 다양한 연결이 이루어 지기 때문에 엔클레이브 경계 보호막을 설치하여 외부정보의 유입이 조직의 시스템 운용이나 자료에 영향을 미치지 않도록 해야 한다. 엔클레이브 경계보호를 위하 가드(Guard), 방화벽 등이 이용되며, 원격접속으로부터의 보호를 위해 암호화를 사용한다.

3.3 네트워크와 기반구조 (Network and Infrastrcuture)

네트워크와 기반 구조는 엔클레이브로 둘러싸인 지역들 사이에 상호 통신 능력을 제공한다. 기반구조에는 운영지역 통신망 (OAN: Operational Area Network), 도시권 통신망(MAN: Metropolitan Area Network), 캠퍼스 통신망 (Campus Network), WAN, LAN 등이 있다. 네트워크는 또 다른 중요 요소로서 네트워크 관리, 도메인네임서버(DNS), 네트워크 침입탐지시스템 (IDS) 및 디렉토리 서비스를 포함한다.

3.4 지원 기반구조 (Supporting Infrastructure)

지원 기반구조의 역할은 시스템 보안관리와 보안서비스를 위헤 네트워크, 엔클레이브 및 컴퓨팅 환경에서 정보보증 메커니즘의 기초를 마련하는 것이다. 즉, 지원기반구조는 네트워크 서비스, 컴퓨터 사용자, 웹서비스, 응용, 파일, 도메인네임서버와 디렉토리 서비스 등에 보안서비스를 제공한다. 정보보증기술 프레임워크가 제시하는 지원 기반구조는 공개키기반구조(PKI: Public Key Infrastructure)를 포함하는 키관리기반구조(KMI: Key Management Infrastructure)와 탐지 및 대응 기반구조의 두 가지이다.

4. TICN 정보보증 모델

정보보증이란 용어를 사용하게 된 배경은 미국방부 지침에 따라서, 기존의 정보전에 대한 미국방부의 인식이 갱신되면서 제기된 개념이다. 미국방부에서 정보전이란 개념을 폐지하고 정보보증이란 용어를 사용하게 된 배경은 미국의 국가방위가 IT기술을 기반으로 하는 국가의 주요 기반구조에 의존한다는 사실을 인식하였기 때문이다.

우리나라 군 통신 또한 TICN 체계가 개발되면서 정보보증이라는 개념의 필요성이 대두되고 있다. TICN체계의 정보보증 또한 주요 기반구조를 구성·운영 및 통제하는 정보와 정보기술에 대한 보호, 신뢰성 및 가용성을 보장하는 의미에서 미국방부에서 사용되고 있는 정보보증의 개념과 같은 맥락에서 해석될 수 있다.

TICN 체계에서의 정보보증 체계는 그림 8에서

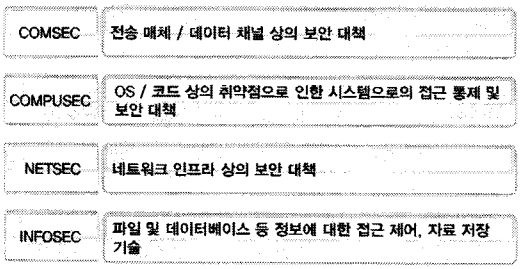


그림 8. TICN 정보보증 모델

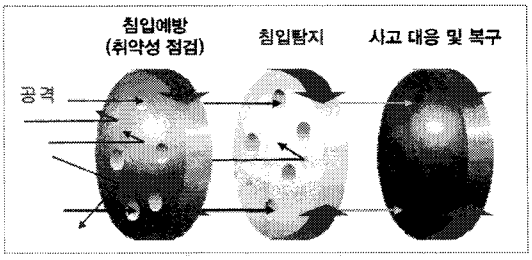


그림 9. 정보보증의 가용성

와 같이 크게 4가지로 나뉘어질 수 있다.

이와 같이 정보보증 체계를 크게 4가지로 나눈 이유는 통신 시스템 상에서 정보가 위협 받을 수 있는 모든 부분에서 공격을 차단하고 정보를 보호하겠단 것이다.

첫 번째로 Communication Security에 해당하는 COMSEC은 주로 전송 매체 혹은 데이터 채널 상과 같은 물리계층에서의 보안 대책을 의미한다. 전파교란과 같은 재망환경에 강인한 항 재밍 기술이나 Side Channel Attack에 강인한 기술과 같이 하위 계층상에서 발생 가능한 위협에 대해서 정보보증을 실시하여야 한다.

두 번째로 Computer Security에 해당하는 COMPUSEC은 주로 시스템의 운영체제나 코드 상의 취약점으로 시스템 내부로의 접근 통제와 관련된 보안 대책을 의미한다. TICN 장비체계의 대부분은 Software 기반의 SDR로 구성되어 있기 때문에 시스템 측면뿐만 아니라, 소프트웨어적인 측면에서도 취약성을 고려해야 한다. COMPUSEC에서의 대표적인 위협 유형으로는 악성코드나 바이러스와 같은 시스템 대상 공격이 대부분이다. 따라서 운영체제의 접근 제어 및 권한관리와 군 통신 장비에 맞는 백신이나 악성 프로그램 탐지 툴을 개발하여 정기적으로 업데이트를 시행해야 한다.

세 번째로 Network Security에 해당하는 NETSEC은 네트워크 인프라 자체를 보호하는 의미에서 COMSEC과 구별된다. 주로 네트워크 계층과 전송계층 상에서 활동하는 패킷의 암호화 프로토콜과 관련이 있으며 대표적인 프로토콜로는 네트워크 계층의 IPSEC (IP Security)과 전송계층의 SSL (Secure Socket Layer)이 있다.

네 번째로 Information Security에 해당하는 INFOSEC은 파일이나 데이터베이스에 대한 접근제어 또는 효율적인 자료저장 기술을 통한 정보 자체에 대한 보안 대책을 의미한다. 주로 어플리케이션 계층상의 보안과 관련이 있으며 계정과 패스워드 사용, 정보에 대한 효율적인 접근제어를 통하여 정보보증을 구현하여야 할 것이다.

위에서 제시한 4가지 정보보증 매커니즘 외에도 정보의 침해에 대한 보호, 더 나아가 신뢰성 및 가용성을 보장하여야 한다. 즉, 적의 침입이 성공해도 시스템의 중요 서비스를 지속적으로 제공할 수 있어야 하며, 침입 발생 후에도 정보의 기밀성과 완전성을 유지하여야 한다.

5. TICN 정보보증 기술 연구 동향

TICN을 도입함에 있어서 정보보증을 구현하는 일은 매우 중요하다. TICN 체계를 통해서 송수신될 모든 데이터들은 전시에 적에게 빼앗길 경우 매우위험한 정보가 될 수 있고, 작전 중 안전하게 그리고 아군의 정책에 맞게 정보가 각 군

전력에게 전달되지 않을 경우 작전 수행을 보장하기 어렵다. 종래의 정보보안은 전자의 문제점 만을 해결 할 수 있다. 따라서 정보보안의 개념을 확장한 정보보증의 개념을 도입하고, 이를 TICN 체계에 접목시키기 위한 아키텍처의 연구가 진행중이다. 정보보증은 정보를 사용함에 있어서 발생하는 모든 위험을 관리하는 것을 목표로 한다. 따라서 정보와 정보 시스템을 보호하기 위해서 관련된 모든 자원에서의 기밀성, 무결성, 진정성, 가용성, 부인방지 등의 보안 서비스를 보장하여야 한다. 여기서 관련된 모든 자원은 정보가 저장되는 공간, 처리되는 시스템, 전송되는 매체 등을 의미하며, 사고나 고의에 의해서 발생할 수 있는 위협 또한 정보보증의 구현에서는 제거되어야 할 대상으로 고려되고 있다.

5.1 종단간(End-to-End) 보안 터널 시스템

군의 통신 시스템에서 사용되는 모든 데이터 흐름은 종래에는 암호화를 통해서 보호되었다. 각 통신 링크 사이에 암호장비가 존재해 송/수신 전/후에 데이터를 암/복호화하는 방법이다. 이 방법은 지나치게 많은 오버헤드가 존재해 실제 네트워클 성능을 저하시키는 원인의 상당부분을 차지하였다. 또한 응용을 사용할 경우 응용에서 이미 데이터 보호를 위해서 암호화를 수행하므로 이중의 중복된 보호로 인해 비용의 낭비가 발생한다. 따라서 이런 복잡성을 피하기 위해 TICN에서 사용되는 데이터 트래픽을 보호하기 위해서 간단하면서도 안전한 새로운 방법을 개발할 필요가 있다.

이를 위해 종단간(End-to-End) 보안 터널을 통해서 단말과 단말, 단말과 서버사이에 발생하는 데이터 트래픽을 보호하고자 한다. 단대단 터널을 사용할 경우, 중간에 어떠한 노드도 내용을 살펴볼 수 없으므로 안전하게 트래픽을 보호할 수 있다.

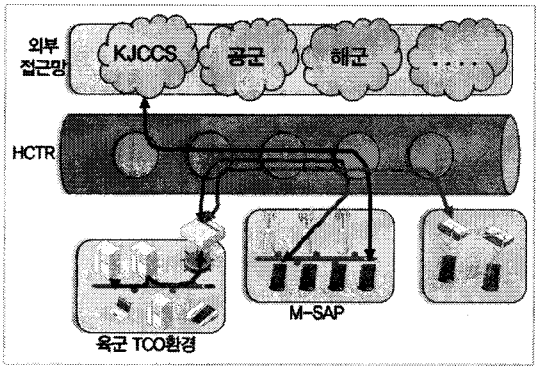


그림 10. TICN 종단간 보안터널 시스템

5.2 다계층 접근제어 시스템

군의 통신 시스템에서 사용되는 모든 자원은 허락된 사용자에게 허락된 권한 만큼만 할당되어야 한다. 따라서 TICN을 사용하는 모든 사용자는 필요한 경우 인증을 받아야 하며, 시스템에서는 권한을 검사하여 필요한 만큼의 자원을 할당할 수 있어야 한다. 이를 위해 각 사용자를 인증하는 방법과 사용자의 자원 사용 권한을 계급, 직무 등의 관점에서 다각도로 제어할 수 있는 형태의 시스템을 개발하여야 할 것이다.

본 시스템에서는 TICN체계의 효율성을 최대한 살리기 위해 높은 수준의 인증이 필요한 경우와 아닌 경우를 구분하고, 후자의 경우는 간단한 기기 인증만으로 제한된 자원을 사용 할 수 있도록 하며, 전자의 경우는 사용자 수준의 인증을 수행하도록 한다. 특히 응용체계를 사용하는 경우, 직무, 계급, 팀, 부대, 위치 등등의 다양한 조건을 통해서 다각도로 접근제어가 가능하도록 하되 효율적이고 간단한 방식을 개발할 필요가 있다.

6. 결 론

본 논문에서는 NCW환경의 전술정보통신체계인 TICN의 구성요소와 TICN 정보보증에 대한

설명과 기술동향에 대한 소개를 하였다. 그리고 TICN 체계에서의 정보보증 모델과 관련 연구 동향을 소개하였다.

TICN체계의 정보보증 아키텍쳐가 목표로 하는 기본 방향은 다음과 같다.

• 최대한 간단하게 구현하면서 보안 수준은 최대한 높일 수 있는 방안을 모색한다.

• TICN 체계의 성능을 고려하여 최대한 가볍게 기술을 개발하여 오버헤드를 줄인다.

• 최대한 현재 사용되고 있는 상용 기술 및 솔루션을 가능한 활용하되, 앞의 두 기본 방향을 만족하도록 최적화 및 개량화 시켜 TICN 체계에서 안정적으로 사용 될 수 있게 한다.

아직까지 정보보증 체계는 이론적이며 TICN 체계 또한 완전히 설계되지 않은 실정이다. 본 논문을 활용하면 향후 TICN체계에서 정보보호 확립에 많은 활용이 될 수 있을 것이다. 하지만 정보보증이 조금 더 명확해 지는 시점에서 조금 더 체계적인 정보보호 연구가 필요할 것으로 본다.

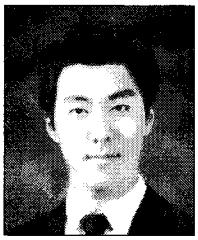
참 고 문 헌

[1] The Joint Staff, Information Assurance : Legal, Regulatory, Policy and Organizational Considerations, 3rd Ed., Sep, 1997.

[2] "IATF: Information Assurance Technical Framework, Release 3.1," National Security Agency, Sep. 2002.

[3] 이철원, 최석진, 이철수, "NCW를 위한 정보보증 프레임워크" 정보과학회지, 제 24권, 9호, pp. 57-63, 2006.

[4] 이철원, 김홍근, "정보보증: 컴퓨터 보안의 새로운 패러다임" 정보과학회지, 제18권, 1호, pp. 53-54, 2000.



김 응 준

• 2009년 충북대학교 정보통신공학과 (학사)
• 2009년~현재 한양대학교 전자통신컴퓨터공학과 (석사)
• 관심분야 : 모바일 인증, 암호화 알고리즘, 네트워크 보안

김 동 규

• 1992년 서울대학교 컴퓨터공학과 (학사)
• 1994년 서울대학교 컴퓨터공학과 (석사)
• 1999년 서울대학교 컴퓨터공학과 (박사)
• 2001년 부산대학교 컴퓨터공학과 조교수
• 2006년 한양대학교 전자통신컴퓨터공학과 조교수
• 2007년~현재 한양대학교 전자통신컴퓨터공학과 부교수
• 관심분야 : 모바일 인증, RFID/USN 보안 시스템, 암호화 알고리즘 및 Crypto coprocessor