한국산학기술학회논문지
Vol. 8, No. 4, pp. 788-794, 2007

NCW환경의 보안 프레임워크 기술에서 암호통신 중계영향 분석

홍진근[1*]

The Analysis of Crypto Communication Relay Effect in the Security Framework Technique of Network Centric Warfare Environment

Jin-Keun Hong[1*]

요 약 미 국방성의 정책은 NCW 개념 구현으로 방향을 이동하고 있다. NCW는 일반적으로 4개의 즉, 지휘통제, 센서 시스템, 교전시스템, 네트워크와 같은 핵심적인 상호종속적인 요소들의 통합과 동기화로 설명할 수 있다. 그러므로 한국군의 군사정책은 적용가능한 NCW 통신환경 및 암호통신 정책에 대한 접근과 연구가 필요하다. 본 연구에서는 미국을 중심으로 추진되는 네트워크 중심 전쟁에서 보안 프레임워크를 살펴보았다. 네트워크 중심전쟁에서 고려되는 핵심 기술을 소개하였으며 이 핵심 기술인 보안 요구조건, GIG, JTRS, NCES, TCS의 보안 특성과 같은 보안 프레임워크를 고찰하고 NCW 환경에서 노드간 암호통신 중계영향을 분석하였다. 본 결과는 NCW의 다양한 암호통신 연구분야에서 환경적인 영향 요소들을 고찰하는데 도움을 제공한다.

Abstract The policy of US DoD is moving towards implementation of Network Centric Warfare(NCW) concepts. NCW is commonly described as the integration and synchronization of four key interdependent elements such as command and control, sensor system, engagement systems and the network. Therefore the military policy of Korea military is needed to access and examine the policy of NCW communication environment and crypto communication, which is able to apply it. In this case study, We are reviewed the security framework of the concept of network centric warfare in the centering around the US. It is introduced the core technology in the network centric warfare, and it is reviewed the security framework such as, the requirements of security, the characteristics security of global information grid, joint tactical radion system, net centric enterprise services, transformational communication satellite, in the basis of core technology, and analysis the effect of crypto communication relay between command node and surbornate node in NCW environment. This report support the assistance, which is considered the elements of surrounding effects in the varied crypto communication research area of NCW.

Key words : Information, 네트워크, Model, Structure, Security

1. 서론

미 국방성이 추진하는 네트워크 중심 전쟁은 21세기 정보기술, 정보 공유, 전투력 간의 상호관계성을 가지고 추진되고 있다. 강인하게 네트워크화된 전투력은 정보공유를 개선시키고 정보공유는 정보의 품질과 공유된 상황인식 능력을 개선시킨다. 또한 공유된 상황인식 능력은 자기 동기화를 가능하게 하며 지휘체계의 지속성과 신속성을 개선시킨다. 이를통해 드라마틱한 작전의 효과를 유발할 수 있다[1][2]. 네트워크 중심 작전의 개념적인 프레임워크는 office of force transformation(OFT)와 office of the assistant secretary of defense for networks and information integration(OASD)에 의해 보다 세부적으로 제시되고 있다. OFT와 OASD는 RAND에 공대공 전투작전에 대한 NCO를 어떻게 수행할 것인지에 대한 연구를 위임하여 처리하고 있다. 네트워크 중심전 환경 구축을 위해서는 global information grid, 네트워크 중심 엔터프라이즈 서비스 구조, joint tactical & radio system, 위성통신 기술, 정보보증 서비스와 같은 핵심적인 요소기술이 확립되어야 한다. 이 가운데 가장 중요한 정보보증 서비스는 다차원적의 계층화된 정보보증 전략으로 심층방어

[1]백석대학교 정보통신학부
*교신저자: 홍진근(jkhong@bu.ac.kr)

프로그램, 침입탐지 기술의 적용, 산업체와 전략적인 파트너쉽을 통한 보안이 가능한 상용제품 개발, 개방된 보안 프레임워크 마련, 국가차원의 보증 파트너쉽(CC 평가) 추진, 글로벌과 상호연동이 가능한 보안관리 구조를 마련하고, 고수준 인증제품 및 시스템에 대한 연구개발, 실시간 모니터링과 데이터 수집, 분석 및 가시화를 위한 연구개발 등이 요구된다. 본 연구에서는 네트워크 중심전을 성공적으로 수행하기 위해 요구되는 핵심기술을 살펴보았으며, 이 기술을 중심으로 정보보호 프레임워크를 고찰하였다. 2장에서는 네트워크 중심 작전을 위해 요구되는 핵심 기술에 대해 언급하였고, 3장과 4장에서는 네트워크 중심작전에서 요구되는 보안 프레임워크를 고찰한 후, NCW 중심 작전환경에서 노드간 암호통신 중계 영향을 분석하였으며 5장에서 결론을 맺었다.

2. 네트워크 중심 작전을 위한 핵심 기술[3][4]

네트워크 중심 전쟁을 수행하기 위해 요구되는 핵심 기술로는 광대역의 위성통신기술, GIG 구조, joint tactical & radio system(JTRS), 네트워크 중심 엔터프라이즈 서비스, 정보 보증 및 수평적인 융합 기술이 있다. 광대역 위성통신 기술은 이동 및 전술 사용자들에게 유비쿼터스 통신 능력을 제공하며 GIG 구조는 보안 기능이 제공되고 강인한 광 IP 지상망을 제공한다. JTRS 는 개방형 통신 구조를 갖는 소프트웨어 재 프로그램이 가능한 무선 장비 패밀리를 제공하며 전술 광대역의 IP 통신 능력을 제공한다. 넷 중심의 엔터프라이즈 서비스는 네트워크 중심 엔터프라이즈에 널리 사용되는 폭넓은 범위의 어플리케이션 및 데이터를 지원하기 위한 서비스 인프라를 제공한다. 또한 정보보증 기술은 넷이 강인하고 신뢰성이 있으며 트러스트한 것을 보증하기 위한 모든 노력을 의미하며 수평적인 융합 기술은 전장에서 교차되는 복잡하고 애매모호한 상황 감지 능력을 갖는 분석가 및 전투원들에게 보다 확신을 가지다 주는데 필요한 넷 중심의 어플리케이션이나 콘텐츠를 제공하는 기술을 의미한다.

2.1 Net centric enterprise services(NCES)

NCES는 에지에 있는 사용자들에게 유비쿼터스한 접속을 통해 적시에 안전하며 결심에 요구되는 수준정도의 품질정보를 제공하는 인프라 구조를 갖도록 하는 능력을 제공하는 것이 중요하다. 넷 중심성은 신속하게 적시에 정확한 전투원에게 정확한 정보를 제공하기 위한 모델로써 서비스 중심 구조를 가능하게 하는 것이 네트워크 엔터프라이즈 서비스이다. 엔터프라이즈 서비스에서 서비스 생산자는 데이터와 어플리케이션을 다양한 서비스를 거쳐 접속함으로써 활용가능하게 하고 이때 사용되는 메타 데이터는 생산자의 포맷을 근거로 하는 서비스를 추가하게 된다. 정보생산자는 메타데이터를 사용하여 콘텐츠를 설명하고 탐색 하기위해 카달로그에 메타데이터를 붙이며 서비스로서 데이터와 어플리케이션을 디스플레이한다. 서비스 소비자는 메타 데이터를 사용하여 데이터 서비스의 자동화된 검색을 수행하며 흥미있는 데이터를 가지고 온다. 이때 생산자를 기반으로 정보형식과 정의 항목을 등록하고 적합한 구조로 변환한다. 또한 소비자의 입장에서는 데이터 서비스를 검색하기 위해 메타 카달로그를 검색하며 검색결과로부터 찾은 메타데이터를 분석하고 파악된 메타데이터를 근거로 선택된 데이터를 가져오게 된다. 그러나 이러한 NCES 서비스를 제공하기 위해서는 문제점들이 대두되고 있다. 소비자 입장에서는 어떤 데이터가 존재하며, 어떻게 데이터에 접근할 수 있는지, 이 데이터가 내가 필요로 하는 데이터인지, 내가 필요로 하는 데이터임을 내가 어떻게 다른 사람에게 말할 수 있는지? 등에 대한 사항들을 해결해야 하고, 생산자 입장에서는 내가 생산한 데이터를 다른 사람과 어떻게 공유할 지, 내가 설명한 데이터를 다른 사람이 어떻게 이해할 수 있을지에 대한 해결점이 필요하다. 넷 상의 정보 리소스는 통합관리를 위해 보안기능이 제공되어야 한다. 또한 사용자 요구에 신속하게 응답하도록 진화방안이 마련되어야 한다.

2.2 혁신적인 통신 프로그램

통신 구조는 GIG-BE, transformational communication satellite (TCS), JTRS와 같은 혁신적인 통신 프로그램이 요구되는데 광대역폭, 유비쿼터스 IP 서비스, 웹 베이스의 제품과 서비스가 허용되어야 한다. NCES 는 이 계층 구조에 중간 계층에 속하며 각 구성품이 다른 부분들을 개선시키는 역할을 한다. 초기화를 할 때 거대한 IP 베이스의 인트라 넷을 가지고 DoD 사용자를 위해 공개되고 제공되어야 한다. GIG는 통합된 정보 인프라를 제공하며 정보 서비스 및 전달, 서비스 에이전트, 인텔리젼트하며 통합된 통신 인트라 넷, 적응적이고 동적인 리소스를 제공해야 한다. GIG에서 제공되는 서비스는 항법 GEO positioning, 군수 보급지원, 감시정찰, 정보작전, 지휘통제, 군 개선 프로그램 등이 있다. IP를 기반으로 하는 GIG 서비스는 정보 유형과 서비스로 전화 서비스, 멀티미디어 서비스, 비디오, 데이터 서비스 등이 있다. 하부 구조는 IP 서비스를 네트워크 계층에서 제공하며 전달매

체로 구리선, 광케이블, 위성, 무선 통신 등을 제공한다. GIG 서비스는 전 세계에서 수용가능하며 사용가능하고 패킷 교환 구조의 인터넷 전송구조에 공통 사용자 및 통합 서비스 프레임워크를 제공한다. 또한 어플리케이션과 전달계층 서비스 사이의 표준화된 인터페이스 제공과 함께 이더넷, ATM, WAP 등과 같은 다수의 네트워크 레벨의 프로토콜 상에서 사용되도록 지원해야 한다. 미 국방성의 비젼은 우주, 항공 및 지상 노드 간의 전달 구조가 인터넷과 같은 구조로 진화해 가며 통합된 우주, 항공 지상 네트워크 구조를 갖는다. RF 및 레이져 통신네트워크를 통한 증가된 용량과 연결성이 요구된다.

3. NCO를 위한 보안 프레임워크[4-7]

미 DoD는 DoD 8500.1에 정보보증(information assurance)에 대한 정의를 "가용성, 무결성, 인증, 기밀성, 부인봉쇄에 의해 정보나 정보시스템을 보호하고 방어하는 대책"으로 내리고 있으며 이 개념에는 보호, 탐지 및 대응 능력을 통한 정보 시스템의 복구를 포함하고 있다. 넷 중심 서비스에서 정보보증을 위해 구성된 위원회에는 DoD, McDonal Bradley, Green Hills Software, Oracle, Boeing, Northrop Grumman, The Open Group, Booz Allen, Eagan Mc Allister, MITRE Corp. 등과 같이 정부기관과 민간업체가 있다. 이 가운데 IA 프로그램의 대두되는 위협요소에 대한 관리는 DoD에 의해 이루어지며 NSA, STRATCOM, DISA 등의 기관이 조정한다.

3.1 NCW에서 보안 요구사항[8-9]

보안 스코프의 경우 역할, 책임성 및 보안 수준은 사용자의 수준에 따라 정의되고 집중화된 거버넌스나 통제에 의해 결정되어야 하며 물리적인 차원에서 보호 기술이 제공되어야 하며 공학적인 관점에서 메시지 필터링 기술 등으로 보장되어야 한다. 평가의 경우 넷 중심 서비스를 위한 보안을 어떻게 평가할 것인지, 이 평가의 종결은 어디에서 이루어질 것인지 등에 관한 부분들이 정리되어야 한다. 보안 서비스는 네트워킹 인프라 구조, 고립 경계영역, 컴퓨팅 환경을 보호하기 위한 계층별 심층암호, PKI 및 KMI 보호, 탐지 및 대응능력이 제공되어야 한다. 이와 같은 보호 방안에는 인증된 접근통제, 데이터 무결성, 견고한 시스템, 여분의 경로, 강한 암호방식, 트래픽 흐름 보호 대책, 접근통제와 필터링을 위한 디바이스, 분배된 침입탐지, 어플리케이션 보안, PKI, 백업 및 복구, 선택적인 경로, 물리적인 보안 및 다른 보안 대책, 은닉채널을 베이스로 하는 네트워크 등이 있다. 데이터 계층 및 패킷 계층에서 보안 서비스가 제공되어야 하는데, 패킷 계층 서비스 보안은 트래픽의 기밀성을 위해 노드 간에 IPSEC /SSL 벌크 암호를 제공해야 한다. 데이터 계층 서비스 보안에서 사용자와 데이터 소스간에 기밀성 데이터 암호화를 위해 사용되는 XML과 같은 암호 표준을 사용할 경우 해결이 되지 않는 경우가 있으므로 이에 대한 해결책이 필요하다. 신분 식별과 계정을 위한 관리 서비스에서는 X.509 인증서를 사용하고 보안 역할이나 클리어런스, 허용 가능한 일에 관련하여 기술적으로는 구현가능하나 누가 증명서를 관리할 것인지에 대한 정책 부분이 해결되어야 한다. 보안 정책에서는 누가 접근통제 정책을 관리할 것인지, 접근통제 정책 및 데이터 소스에 대한 관리정책의 유연성이 아울러 요구된다. 집중적으로 관리되는 계정 서버가 제시되어야 하며 데이터 소스들에 대해 데이터 소스의 특정 규칙을 확장하기 위한 기회가 마련되어야 한다. 다중 저장된 데이터로부터 수집된 콘텐츠 검색의 경우 사용자의 보안 역할이나 분류 수준에 근거하여 필터 처리 방안이 요구되며 기술적으로 simple object access protocol 필터 수준을 수행할 수 있으나 새로운 분류에 의해 생성된 동적인 콘텐츠는 어떻게 분류할 것인지에 대한 부분도 해결되어야 한다. 또한 신속하고 유연한 보안 솔루션이 요구되는데 비록 네트워크 중심 구조라 할지라도 각 네트워크 호에 따라 보안 성능 이슈가 실현되어야 한다. 각 보안 기능에 대한 웹 서비스를 제공할 때 각 네트워크 호에 대한 암호학적인 보호가 요구되며 각 웹 서비스 메시지의 응답은 호출자에 의해 디지털 서명되거나 승인되어야 한다. 네트워크가 다운되거나 웹 서비스가 공격 받을 때 어디에 보안 로그를 설정할지 등의 문제를 결정해야 한다. 개개 컴포넌트나 네트워크 베이스 서비스를 제공하는 곳에서 보안 컴포넌트를 갖는 호환성 있는 구조를 제공해야 하며 보안 컴포넌트와 네트워크 중심 서비스간에 유연한 구조가 제시되어야 한다. 이때 각 컴포넌트는 서명 인증 및 정책 결정 서비스를 위한 보안 웹 서비스 능력을 가져야 한다. 네트워크 중심전 환경에서 유비쿼터스를 지향하는 정보보증 서비스는 임시 네트워크에서 브로드캐스트 환경을 고려한 무결성이 지원되어야 하며, 전원관리를 동시에 고려한 DoS 공격탐지 및 대응을 고려한 가용성 서비스, 오프라인에서 온라인 상태로 단속적인 환경변화에서도 적용할 수 있는 인증 서비스, 낮은 성능이나 낮은 에너지가 제공되는 환경과 같은 곳에서의 기밀성 서비스, 사용자 존재 탐지, 기억된 사용자 기호 및 행동을 토대로 지능적인 응용 환경이나 익명성, 추적성과 트래픽 분석 방안 등이 마련되어야 한다. 지속적으로 네트워크는 침해 받기 쉽고 침해가 사실

상 증가하는 실정이므로 네트워크 중심환경에 적합한 동적인 IA 전략의 수립이 요구되고 있다. 이러한 전략 수립에는 중심을 보호하는 툴, 작전 구성에서 중심을 방어할 수 있는 그리고 중심의 상황을 인식할 수 있는 능력 제공, 중심의 생존성을 유지하는 프로세스 제공, 중심을 전적으로 신뢰하게 할 수 있는 IA 능력이 제공되어야 한다. 미 DoD는 IA 전략의 솔루션을 다차원적으로 접근하고 있으며, 교육 및 훈련 받은 인력, 개선된 작전 수행 능력, 기술의 이노베이션, 결정적인 인프라 요소에서 정보기술 중요성 해결 등에 초점을 맞추고 있다. 운용적인 관리요소에서는 통합된 정보보증 정책 프로그램, 정보보증 취약성 경고 프로세스, 서비스 및 에이젼스 컴퓨터 긴급응답팀 운용, DoD와 연합된 다른 정부기관, 부서의 연합 테스크 포스 운영, 지속적인 취약성 분석 및 평가 프로그램, 보호 탐지, 응답 능력 테스트를 위한 실행 프로그램이 실시되고 있다. DoD GIG 인터넷은 GIG 코어와 에지 노드에 서버 어플리케이션으로 접속하며 인트라넷은 보안 서버를 운용하여 IPSEC, TLS, PKI 등을 서비스 하며 IPv6를 지원한다. GIG 보안 서비스는 단대단 정보보증 서비스, 콘텐츠 베이스 정보 보호, PKI에 의한 접근통제, 글로벌 네트워크 방어, 강력한 훈련 및 인증을 제공한다. 단대단 정보보증 서비스 구조는 NSA, TC/GIG IA에 의해 개발되며 사용자와 사용자간 데이터를 보호하는 전달계층 보안, 링크 레벨 공격에 대비한 TRANSEC를 제공하고 IA 기술적인 워킹 그룹으로 구성되어 있다. 콘텐츠 베이스 정보보호는 메타 데이터의 보안 테그 설정, 암호화된 동적인 공유, 연합군이나 협력 파트너와의 유연성을 지원한다. PKI에 의한 접근통제는 동적인 커뮤니티를 지원하기 위해 확장하며 리소스에 대한 사용자의 강한 인증과 접근통제 기능을 제공한다. 글로벌 네트워크 방어는 경계 외부와 내부 고립지역에 대한 강인한 엔터프라이즈 센서 그리드 구조를 가지며 C2를 갖는 심층방어 접근과 취약성 관리 서비스를 지원한다. GIG 보안 측면에서 암호의 혁신적인 변화부분에는 Black IP Fabric 구조 제공, 강한 식별, 인증 및 계정 부여 기능 제공, High assurance IP encryptor 개발, PKI 개발 및 적용, 보안 관리 인프라 구조 등을 포함하고 있다. TCS에서의 보안 서비스는 우주선 및 지상 장비의 보호, 시스템 내에 포함된 정보 및 데이터 보호, 통신 및 데이터 처리 서비스의 보호가 존재하며, 우주 임무 보호 서비스는 넷 상호 연결성이 증가할수록 중요도가 높아진다. 우연히 발생된 사건에 대해 결코 보안 사고는 기다리지 않으며 우주 임무 어플리케이션은 반드시 보호되어야 한다. 또한 상호운용성 및 호환성을 만족시키기 위해 보안 표준이 이루어져야 하고 보안 서비스를 위해 다양한 계층에서 보안이 가능해야 한다. 우주 임무에 있어서 위협에는 space elements를 위협하는 replay 공격, 트래픽 분석, DoS/Jamming이 있으며, 시스템 및 네트워크를 위협하는 replay 공격, 데이터 절취와 가로채기, 소프트웨어 위협, 트래픽 분석 및 인가되지 않은 접근 위협이 있다. 통제에는 인가되지 않은 접근위협, 트래픽 분석, 소프트웨어 위협, 사용자를 위협하는 데이터 절취 및 소프트웨어 위협이 존재한다. DoD에서 고려하는 TCS에서 보안대책은 보안 기능이 있는 우주 네트워킹으로 소스와 우주의 신뢰된 게이트웨이간, 그리고 우주의 신뢰된 게이트웨이와 목적지간 암호처리 구조를 고려하고 있다. 단대단 보안은 소스와 목적지간 보안을 수행하고 라우팅을 위해서는 암호화되지 않은 헤더 구조를 갖는다. 그러므로 네트워크 계층이나 전송계층 상위에서 암호화를 수행한다. 적용가능한 보안표준은 IPSEC으로 지상의 대역폭 가용성을 고려할 때 보다 가벼운 구조가 필요하다. SCPS-SP(Space communication protocols suite-security protocol)는 국방성과 NASA에 의해 우주 통신 프로토콜에서 적용가능한 보안 프로토콜로 개발되었으며 보다 경량화된 구조를 갖는다. Consultative committee for space data systems layer 2는 패킷 텔리메트리/원격명령으로 전송 프레임 위 또는 아래 보안 계층이다. HAIPE는 고속 IP 암호장비로 네트워크 중심성의 비젼을 지원하기 위한 라우팅 구조에 대한 적용가능한 암호구조를 지원한다. 전술 네트워크는 동적인 라우팅 구조를 적용할 때 확장성과 용이성이 해결되어야 하며 IP 암호화를 위한 현재 프로토콜 구조는 GIG 비젼을 지원하는데 규모의 확장성이 부족한 것으로 지적되고 있다. IP 암호화 사용이 증가하고 있는 상황에서 주요 프로그램이 IP 암호화를 의존하고 있으므로 GIG-BE 환경에 적합한 구조가 설계되어야 한다. 그러므로 통합에 적용가능하고 구현이 쉬운 IP encryptor 개발이 요구된다. 엔터프라이즈 서비스를 위한 엔드 포인트 보안의 핵심적인 요구사항에는 정책 가이드 라인을 만족시키는 패스워드, 스마트카드, 토큰 등의 강한 사용자 인증방안이 요구되며, 디바이스에 저장된 데이터의 자동적이고 투명하며 실시간으로 암호 처리가 가능해야한다. 또한 플로피 디스크, USB 디바이스, CF, SD, MMC 등과 같이 제거 가능한 미디어 암호를 지원해야한다. 따라서 네트워크 중심전 환경에서 정보보호 서비스는 다음과 같은 사항들이 만족되어야 한다. 먼저, 메타데이터 구성 및 글로벌로 공유된 서비스를 기본으로 정보와 서비스는 권한이 있는 사용자들에게 유비쿼터스하게 접근 가능해야한다. 두 번째로 현재 사용자에 대한 확인과 현재 사용자 및 사용자 위치를 근거로 하는 접근통제 환경이 제공되어야 한다. 세 번째로 융합된 음성, 비디오, 데이터 및 이미지 서비스가 제공되어야 하며

민감한 임무 사용자의 요구사항을 지원하는 높은 수준의 통신 능력과 충분한 보안성을 제공해야 한다. 고정 및 임시 커뮤니티에 대한 동적이고 적응적이며 자기 구성이 가능한 구조를 가져야 하며 이를 통해 전체 IP를 근간으로 하는 높은 가용성을 보장하는 네트워크를 제공해야 한다. 네 번째로 seamless하고 보안성을 제공하는 단대단 상호접속된 정보 환경이 마련되어야 하며 다섯 번째로 DoD, Intelligence community, 다른 정부기관, 산업체, 국제 파트너와 정보의 상호 운용성이 보장되어야 한다. 여섯 번째로 네트워크 관리, 성능 모니터링, 보안관리, 공격탐지 및 대응 등의 공통 인프라를 지원할 수 있어야 하며 마지막으로 국방성에 민감한 임무 요구사항이 가용성이나 기밀성, 무결성을 통해 서비스되며 상용기술이 레버리지된 강한 포커스를 제공해야 한다. DoD는 네트워크 중심전 환경 구축을 위해 GIG BE 구축을 제시한다. 이 통신 인프라를 위한 GIG 구축 항목에는 광 IP 망과 통합 GIG 망 구축, 통신 백본 구축, 고속이며 보안 및 신뢰성을 제공하는 광범위한 연결성을 제공하는 구조를 포함하고, TCS 구축 항목에는 광범위한 gap filter, BLOS 통신 구조를 요구한다. JTRS를 위한 투자항목에는 소프트웨어 프로그래머블한 무선장비, 무선 라디오 장비 및 네트워킹 시스템, 백본(음성, 비디오, 데이터 통신)이 포함되어 있으며, NCES를 위한 투자계획에는 핵심 엔터프라이즈 서비스, 어플리케이션 프로그램 인터페이스를 지원하며 정보의 품질을 결정하기 위해 적시성, 보안성, 유비쿼터스 능력을 제공할 수 있도록 한다. 수평적인 융합을 위한 투자항목에는 작전 정보 데이터의 응용 프로세스로 사용자에 의한 데이터 요구 및 융합이 가능한 IP를 베이스로 하는 수단이나 툴을 마련하는 것을 포함하고 있다. 분산된 공동 지상 스테이션과 심층방어 연구 개발, 정보보호(통신, 전송 보호) 개발, 암호 프로그램 개발에 관련된 정보보증에 투자가 아울러 이루어지고 있다. 특히 IPv6로의 전이가 현재 진행 중이다. IPv6는 단대 단 연결성, 멀티캐스트, 이동성, 호스트 멀티 호핑, IPSec을 기반으로 하며 NCO에서 보안은 IPv6 설계와 적용 관점에서 반드시 고려되어야 한다. IPv6 흐름 레벨에서의 보안 고려 사항은 서비스 거부나 절취의 문제, 터널링과 IPSec에서의 상호작용문제, 트래픽 분석, 방화벽 등이 있다. 암호 무결성 체크는 터널모드에서 내부 흐름을 보호할 수 있으나, AH의 경우 외부 흐름 레벨은 보호 할 수 없다. IPv6 네트워크 구조측면에서 보호는 NAT(network address translation) 보다는 NAP(network architecture protection)가 요구되고 있다. NAT는 대부분의 라우터나 방화벽에 의해 제공되는 상태 패킷 필터 기능을 제공하고 IPSec 구조와 결합될 수 있으며 내부 및 외부 간에 게이트웨이를 제공한다. 이 경우 IPv6 라우터는 유일한 로컬 주소 prefix가 사이트 내에서 광고되고 prefix 상에 들어오는 그리고 나가는 패킷에 대한 필터링을 수행하며 DHCPv6 prefix는 서비스 제공업자로부터 글로벌 라우터 prefix를 얻기 위해 사용된다. NAP는 RFC 3041 표준에 정의된 바대로 IPv6에서 상태 정보가 없는 주소의 자동구성을 위한 프라이버시 확장문제를 DHCPv6와 DNS로 구현될 수 있고, 유일한 로컬 주소는 사이트 규모에서 제공되며, RFC3633 표준대로 DHCPv6 prefix 옵션을 정의하고 있다. IPSec VPN은 ESPv3와 함께 사용될 수 있으며 IPv6 방화벽은 존재하나 아직도 미성숙하며 방화벽 모델은 진화되고 있는 중이다.

4. NCW 환경에서 노드간 암호통신 중계 영향 분석[5-7]

넷 중심의 전투부대 작전 상황인식 정보 전달 임무를 수행할 때 요구되는 주요 상황 인식정보는 부대원 voice 암호통신에 의한 직접 정보 중계 방식과 노드 교환기에 의해 중계되는 간접 중계방식으로 전달되는 문자암호통신으로 구분할 수 있으며, 이들 중계방식은 지형 등의 주위 환경요소에 의한 영향으로 인해 특히 암호통신의 경우 일반 평문통신에 비해 정보전달 지연요소 및 오류전파로 인한 재전송이 빈번히 발생된다. 일반적인 부대원에 의한 아날로그 스크램블러에 의한 voice 통신을 활용한 직접 상황정보 중계방식은 주위의 잡음 영향 등과 같은 통신장해에 따라 수신측에서의 음성 복호시 품질이 매우 저하되며 반면 디지털 보코더에 의한 voice 중계방식에 암호통신을 적용한 경우는 아날로그 스크램블러 방식보다 보다 나은 성능을 제공한다. 그러나 상황인식 정보를 문자 및 코드화하여 전송하는 교환기에 의한 간접중계 방식에서의 암호통신은 통신환경이 열악할 경우 직접 중계에 의한 암호통신 성능보다 열화되는 것을 살펴 보고자 한다. 본 논문에서는 voice 통신에 의한 직접 중계방식에서의 암호통신 성능과 교환기에 의한 간접 중계방식에서의 암호통신의 성능을 평가하였다. 그림1에서는 전투지휘부대 노드 교환기와 하급부대 노드간의 넷 중심 작전을 위해 상황인식 정보를 전달하기 위한 전달 구조의 예를 나타내고 있다. 영역 (Area) A에서 하급 노드의 경우 9.6Kbps 통신구간, 영역A와 B의 보안 통신구간은 19.2Kbps, 영역B의 경우 19.2Kbps, 영역 B와 영역 C의 보안 통신구간은 64Kbps, 영역C의 경우 64Kbps, 영역C의 지휘노드일 경우 1Mbps 전송속도를 제공한다고 가정한다.

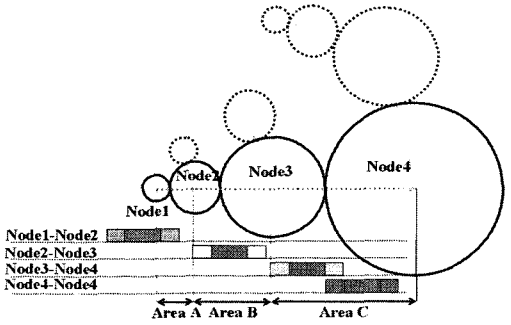


그림 1. 전투 지휘부대 노드 교환기와 하급부대망 노드간의 넷정보 전달구조

제시된 표 1에서는 영역A 노드와 영역B 지휘노드간 상황인식 정보를 전달할 때 부대원의 voice 암호통신을 이용한 직접중계 방식과 데이터 교환 노드에 의해 전달되는 간접중계 방식의 암호통신 성능을 비교한 것이다. 즉 Tree 넷으로 이루어진 넷 중심의 전투부대가 상황인식 정보를 상급부대 지휘관에 보고한다고 할 때, 3stage relay의 경우는 하급 부대의 지휘관이 상급부대 지휘관에 상황인식 정보를 전달하기 위해 3개의 노드 교환기를 거쳐 암호통신을 통해 전파되는 경우이다. 이때 간접중계 방식을 활용할 경우 3개의 노드 교환기를 거쳐 정보가 정상적으로 전달되기 위해서는 영역A에서는 9.6Kbps로 전달되고, 영역B에서는 19.2Kbps, 영역C에서는 64kbps 암호통신 전송속도로 전달된다. Voice 암호통신의 경우 아날로그스크램블러를 적용할 경우 채널환경이 열악하면 매 암호통신마다 수신시 평균 20~30msec 동안 정상적인 복호가 불가능하다. 이 채널의 경우 디지털 비트오류율로 변환하는 $2x10^{-2}$~$3x10^{-3}$ 정도가 된다. 동일한 환경에서 디지털 모뎀이 적용된 암호통신의 경우 비트오류율은 $1x10^{-2}$ 이며 50% 오버헤드 갖는 성능의 보코더 채널오류정정부호를 적용하면 $1x10^{-3}$ 정도이고 동일한 조건에서 암호통신을 적용하면 평균 비트오류율이 $5x10^{-2}$ 정도의 채널열화가 발생한다. 만일 간접중계에 의한 암호통신을 지원하면 간접중계 방식의 일반통신 비트오류율은 상황인식 정보가 문자단위(8비트)로 지원하므로 비트오류율은 $1.25x10^{-1}$이므로 50% 오버헤드를 갖는 보코더 채널오류정정부호를 적용하면 $6.125x10^{-1}$ 오류채널로 암호통신 채널환경이 매우 열악하다.

채널 환경이 열악한 환경에서는 아날로그 스크램블러를 이용한 voice 직접 중계 방식보다 디지털 모뎀을 적용한 voice 직접 중계 암호통신 방식이 적합하며, 디지털 모뎀을 적용한 voice 직접 중계 방식이 교환기에 의해 전송되는 상황인식 정보의 간접중계 방식을 적용한 암호통신보다 나은 성능을 제공한다.

표 1. 영역A와 영역B 지휘노드간 직접중계와 간접중계 상황인식정보의 암호통신 시 열악한 환경에서의 비트오류율(평문통신/암호통신BER)

구 분	평문통신 BER	평문통신BER (with ECC)	암호통신 BER
교환기 암호통신에 의한 간접 중계	$1.25X10^{-1}$	$1.25x10^{-2}$	$6.125x10^{-1}$
voice 암호통신에 의한 직접중계 (디지털보코더)	$1.0x10^{-2}$	$1.0x10^{-3}$	$5.0x10^{-2}$
voice 암호통신에 의한 직접중계 (아날로그스크램블러)	$2.0x10^{-2}$	-	$1.0x10^{-1}$

그림 2에서는 표 1로부터 주어진 각 중계방식의 암호통신 조건에서 비트오류환경에 대한 암호동기 검출능력을 나타낸 것이다. 비트오류 환경이 열악할 경우 voice 통신에 디지털 모뎀을 적용한 방식이 가장 우수한 검출능력을 제공하고 아날로그 스크램블러를 적용한 방식이 두 번째 성능을 제공한다. 한편 교환기를 통해 간접중계에 의한 암호통신은 각 stage 마다 재전송이 발생하고 아울러 동기검출 능력 측면에서도 비효율적인으로 나타난다. 넷 중심 작전은 신속한 시간에 정보가 수집, 전파되어 상급 지휘노드에서 결심할 수 있도록 유도하는 것이 매우 중요하다. 이러한 측면에서 상황인식 정보를 빠른 시간에 전파하기 위해서는 넷 중심 환경노드의 특성에 따라 암호통신에서 효과적인 중계방식을 운용하는 것이 중요한 것으로 판단된다.

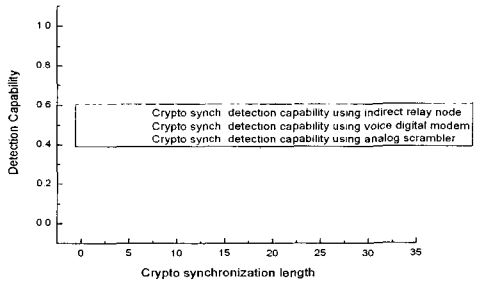


그림 2. 상황인식 정보 직접/간접중계시 암호통신의 암호동기 전송능력 비교

주어진 표 2에서는 영역A에서 영역C간 하급부대 노드에서 상급부대 노드로 상황인식 정보를 전파할 때, 암호통신에 소요되는 시간을 나타낸 것이다. 하급부대의 노드(영역A)는 채널환경이 매우 열악하고 상급부대(영역 B, C) 노드로 이동할수록 채널환경이 양호한 것으로 판단되며 이에 따라 영역에 따라 암호통신이 이루어질 때 영역

A에서 요구되는 소비시간은 교환기 암호통신에 의한 간접중계 방식에서는 2.5sec, voice 통신에 의해 직접중계를 하되 디지털 모뎀에 의한 암호통신은 1.05sec, 아날로그 스크램블러를 이용할 경우 1.11sec 의 전송시간이 평균적으로 소비된다.

표 2. 영역A, 영역B, 영역C 지휘노드간 직접중계와 간접중계 상황인식정보의 암호통신 소비시간(3단 중계, 전송비트=9600bits, 전송율=9.6Kbps/19.2Kbps/64Kbps)

구 분	Area A	Area B	Area C	Total
교환기 암호통신에 의한 간접 중계	2.5sec	2.5sec	0.15sec	3.15sec
voice 암호통신에 의한 직접중계 (디지털보코더)	1.05sec	0.47sec	0.15sec	1.67sec
voice 암호통신에 의한 직접중계 (아날로그스크램블러)	1.11sec	0.47sec	0.15sec	1.74sec

이때 아날로그 스크램블러를 사용할 경우 전송소비 시간측면에서는 디지털 모뎀을 활용할 경우와 유사하나 음성 품질 측면에서는 품질이 좋지 않다. 교환기에 의해 전송되는 간접중계 방식에서는 채널이 열악하므로 암호통신에서 암호동기 검출이 상대적으로 어렵고 한편 상황인식 정보의 식별이 음성 통신에 비해 어렵기 때문에 재전송이 많이 발생하기 때문인 것으로 분석된다. 본 논문에서는 NCW 환경에서 암호통신에서 발생할 수 있는 통신 영향 조건들을 연구분석함으로써 넷 중심 작전을 암호통신에 운용할 때 사용되는 직접중계 방식과 간접중계 방식의 효과성을 살펴보았다. 전송율측면이나 비트오류환경이 좋은 여건에서는 간접중계 방식을 적용하는 것이 적합할 것이나 전송환경이 열악한 환경에서는 부대원을 통해 상황인식 정보를 직접중계방식이 더 효과적인 것으로 판단된다.

5. 결론

본 연구에서는 미 국방성을 주도로 추진되고 운용되고 있는 네트워크 중심전 환경에서 정보보호 프레임워크를 주제로 다루었다. 현재 미 국방성이 네트워크 중심 작전을 수행할 때 반드시 요구되는 핵심 기술을 살펴보았으며 기술된 주요한 보안 요구사항으로는 정보보증 서비스 전략과 솔루션, GIG 보안특성, TCS 보안특성, NCES 보안특성, JTRS 보안특성 등을 고찰하였다. 또한 넷 중심작전을 운용할 때 하급부대의 노드에서 상급부대로 상황인식정보를 보고하거나 상급부대에서 하급부대로 지휘명령을 하달하고자 할 때 채널특성에 따른 소요시간, 동기검출 능력 등을 분석함으로써 암호통신 운용에 적합한 중계노드 방식과 관련하여 살펴보았다. 향후 연구과제에서는 최근 호주를 비롯한 뉴질랜드 등과 같은 NCW 운용체계에 대한 연구와 함께 NCW 각 요소에 대한 세부적인 연구동향 분석, 보안체계 메카니즘의 구현방향 등을 정립하고 연구분석하고자 한다.

참고문헌

[1] Alberts, David S., "Mission Capability Packages," Strategic forum, institute for national strategic studies, #14, Ja. 1995.

[2] Alberts, David S. and John J. Garstka, "Network Centric Warfare Department of Defense Report to Congress," July, 2001.

[3] Cebrowski, Vice Admiral Arthur K., and John J. Garstka, "Network Centric Warfare: Its Origin and Future," Proceedings, Jan., 1998.

[4] Daniel Gonzales, John Hollywood, Gina Kingstan, and David Signori," Network-Centric Operations Case Study," RAND National Defense Research Institute, 2005.

[5] Michele Knight, Les Vencel and Terry Moon, "A Network Centric Warfare compliance process for Autstralian Defence," DSTO-TR-1928, 2006.

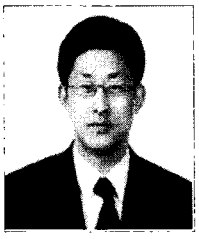
[6] Walt Okon, "NCES Information & Capabilities," DISA, NIID Day, 2006.

[7] Mort Rolleston, Lt Col John Pernot, Maj Tim Keeports, "The U.S. Air Force Transformation Flight Plan," HQ USAF/XPSC future concepts and transformation division, 2004.

[8] The White House, The National Security Strategy of the US of America, Sept. 2002.

[9] The White House, The National Strategy to Secure Cyberspace, Feb. 2003.

홍 진 근(Jin-Keun Hong) **[정회원]**



- 2000년 : 경북대학교 전자공학과 (공학박사)
- 현재 : 백석대학교 정보통신학부 교수

<관심분야>
정보보호, 텔레매틱스 시스템, 헬쓰케어시스템