전술네트워크 및 전장관리체계 사이버 공격 및 방어 기술

김보성, 안효춘, 노병희
아주대학교

요 약

미래 전장 환경이 네트워크 중심전으로 진화되어 가면서, 전술네트워크의 구축은 필수적이다. 군사 분야의 선진 각국은 이의 구축을 위하여 막대한 인력과 비용을 들여 추진하여 오고 있다. 우리 군에서도 전술통신 네트워크인 TICN을 구축하여 오고 있으며, 이는 다양한 복합 전술 및 전투 체계를 광대역 고속 통신 네트워크로 연결하여 정보의 적시 전달을 통하여 통합 전투력의 최대 발휘를 목표로 한다. 유무선 네트워크와 이에 연결된 시스템들을 대상으로 한 다양한 형태의 사이버 공격들은 개인과 기업은 물론 국가 기반시설까지를 대상으로 하고 있으며, 전술네트워크 또한 공격 목표 대상중의 하나이다. 본 고에서는 전술네트워크에서의 사이버 공격의 형태와 특징에 대하여 살펴보고, 이에 대응하기 위한 방어 방법들에 대하여 고찰한다.

Ⅰ. 서 론

네트워크 중심전 (Network Centric Warfare, NCW) 환경에서는 전쟁의 주체가 되는 부대 및 체계를 포함하는 모든 요소들이 네트워크로 연결되는 것을 전제로 한다[1]. 전술네트워크는 GIG (Global Information Grid) 체계 관점에서 보면 가장 엣지 (edge) 부분에 위치한다. 그러나 정보를 수집하고 이를 활용하여 전투를 수행하는 대부분의 사용자는 전술네트워크에 연결되어 있고, 운영 환경이 매우 열악하므로, 각국에서는 이의 구축을 위하여 막대한 인력과 비용을 들여 추진하여 오고 있다.

우리나라에서는 전술네트워크로서 TICN (Tactical Information Communication Network)를 구축하고 있다. TICN은 NCW 환경에서 감시정찰, 지휘통제, 정밀타격체계 (C4ISR-PGM)의 통합 전투력 발휘에 필요한 고속 대용량 정보를 기동 간에도 실시간 유통을 보장하는 것을 목표로 한다[1]. TICN은 대용량 무선전송체계, 소용량 무선전송체계, 교환접속체계, 전투무선체계, 전술 이동통신체계, 망제어체계 등의 복합적인 부체계들로 구성된다[2]. 그리고, 육군전술지휘정보체계 (Army Tactical Command Information System, ATCIS)[3], 대대급 이하 전투 지휘체계 (Battalion Battle Command System, B2CS)[4], 군사정보 통합 처리체계 (Military Intelligence Management System, MIMS)[5] 등 전장관리체계를 TICN과 연계하여 구축하여 공통상황 인식 및 전장관리 능력을 극대화한다.

최근, 다양한 형태의 사이버 공격들이 발생하고 있으며[6], 이는 유무선 네트워크와 이에 연결된 개인과 기업은 물론 국가 기반시설까지를 대상으로 하고 있다. 향후, 사이버 위협은 개인과 기업 및 국가 기반시설을 넘어서 지휘통제 수단과 관련된 군사 시설 및 정보기반체계, 그리고 위성을 비롯한 감시정찰, 정밀타격 무기체계로까지 확대될 것으로 예상 된다.

TICN은 무선을 기반으로 하여 통신을 지원하는 복합체계들로 구성되고, 다양한 전장관리체계들을 수용하게 되므로, 유선 기반의 C4I 체계들보다 더 많은 취약점을 잠재적으로 내포하고 있어, 이를 이용한 사이버 공격에 노출되기 쉽다.

기존의 전술네트워크를 대상으로 한 사이버 위협에 대한 연구들은 MANET (Mobile Ad-hoc Network)에서의 공격 및 방어 기술들[7]에 집중되어 왔다. 그러나, TICN에서는 MANET의 요소를 갖는 주요 부체계는 전투무선망으로서, 이는 대대급 이하를 기반으로 한다. 그리고, 군단에서 여단급까지는 HCTRS와 LCTRS의 광대역 무선 백본망을 제공하는 부체계들을 기반으로 운영된다. 따라서, TICN에 대한 사이버 공격 및 방어에 대한 연구 및 기술적 접근을 위하여 전통적인 상용무선망이나 MANET에서의 방법들을 그대로 적용하는 데는 한계를 갖는다.

본 고에서는 우리나라의 전술네트워크인 TICN의 특징을 소개하고, 이를 대상으로 한 사이버 공격 및 대응 기술들을 살펴본다. 그리고, 전장정보를 교환하고 관리하는 전장관리체계들을 소개하고, TICN과 연계하여, 이들 전장관리체계들을 대상으로 한 사이버 공격 위협의 형태와 특징에 대하여 살펴보고, 이에 대응하기 위한 방어 방법들에 대하여 고찰한다.

Ⅱ. 배 경

1. 전술정보통신체계(TICN)

TICN체계는 〈그림 1〉과 같이 대용량 무선전송 체계 (HTCRS, High Capacity Trunk Radio System), 소용량 무선전송 체계(LCTRS, Low Capacity Trunk Radio System), 교환접속 체계(TIPS, Tactical Internet Protocol System), 전투무선 체계(CNRS, Combat Network Radio System), 전술 이동통신 체계(TMCS, Tactical Mobile Communication System), 망제어 체계(NCS, Network Control System) 등의 부체계들로 구성되어 있다.

이들 부체계들 중에서 HCTRS와 LCTRS는 각각 여단(연대)급 이상과 대대급 부대통신소간의 고속 대용량 무선 전송 능력을 제공한다. 그리고, CNRS는 전장에서 직접 전투를 지휘하는 지휘관들과 전투원들 간에 정보를 주고받기 위해 다대역 다기능 무전기인 TMMR (Tactical Multi-band, Multi-role Radio)이 주 장비로 사용된다.

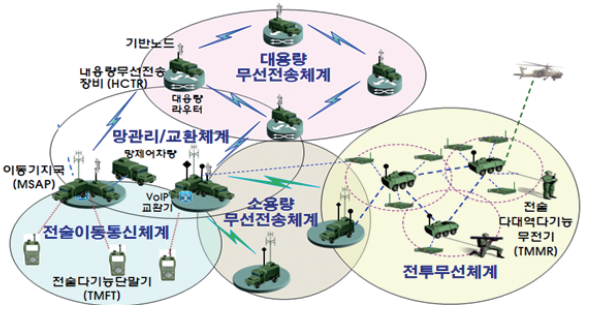

그림 1. TICN 구성도

2. 전장관리체계

전장관리체계란 C4I의 각 요소를 유기적으로 통합 하여 지휘관에게 부여된 임무 달성을 위해 가용한 자원을 최적의 장소와 시간에 할당하여 전투력 상승 효과를 발휘할 수 있도록 지원하는 총체적인 수단과 절차를 지칭한다[8]. 전장관리체계의 주요 능력은 다음과 같다.

- 전장공간 가시화 및 전장인식 공유
- 자체진단 및 복구능력 보유
- 신속 정확한 결심 및 계획수립 지원
- 제 전장기능별 운영체계 통합
- 수직 · 수평적 실시간 연동
- 자료입력 및 정보유통 자동화

한국군의 전장지휘체계는 지상전술C4I체계로 호칭되고 있는 육군전술지휘정보체계인 ATCIS[3], 대대급 이하 전투지휘체계인 B2CS[4], 그리고 군사정보통합처리체계인 MIMS[5] 등으로 구성된다.

ATCIS는 육군의 전술제대의 제 전투력을 통합하고 지휘관의 의사결정을 지원하여 전투력 발휘의 승수 효과를 달성하기 위해 감시 및 타격체계와 연동하여 운용되는 전장관리체계 중 하나다. 각 제대의 다양한 전투력 수단들을 효과적으로 운용하고, 전투 수행절차를 자동화하여 신속하고 효율적인 지휘통제로 전투력 승수효과를 발휘할 수 있도록 지휘통제를 지원 하는 기능을 담당한다. 또한, OO급 이상 제대에 배치하여 제대 및 기능별로 상호 연동하여 지휘통제 수단으로 운용하며, 각 제대 지휘관의 지휘결심 사항과 관련된 각종 현황 및 상황을 지휘결심 자료로 지원한다.

B2CS는 핵심 전장상황 파악 지휘통제를 위한 정보를 실시간으로 공유하고, 기동 간 지휘통제를 보장하기 위한 체계이다. TMMR를 모뎀으로 활용하여 경량화, 기동화된 체계를 확보한다. TMMR이 게이트웨이와 네트워크가 단절되더라도 Ad-Hoc 기능으로 독자 망을 구성하여 운용할 수 있다. 대대급 이하 부대들의 단말기 데이터들이 상급부대의 B2CS 서버로 전달되고 연동 서버를 통해 B2CS 서버와 ATCIS 단말기가 연동된다.

Ⅲ. 전투무선체계 대상의 사이버 공격 및 방어 기술

TICN의 부체계 중 TMMR을 기반으로 하는 전투무선체계는 신속한 부대 전개 및 기동을 위해 MANET 기술 적용이 고려된다. 전투무선체계의 사이버 보안 측면에서 MANET이 가지는 특성과 고려하여야 할 사항들은 다음과 같다.

- **동적 토폴로지** – 단말들은 독단적으로 자유롭게 이동한다. 따라서 멀티 홉의 네트워크 토폴로지는 예측할 수 없는 시간에 임의로 빠르게 변화한다.
- **대역폭 제한 및 가변 용량 링크** – 무선 링크는 단말들에 저장된 내용보다 상대적으로 적은 용량을 제공한다. 또한, 이 용량은 다중 접속, 페이딩, 잡음, 간섭 등의 조건에 따라 최대 전송률에 비해 떨어질 수 있다.
- **에너지의 제한된 운용** – MANET 환경의 몇몇 또는 모든 단말들은 배터리 또는 소모성 에너지 수단에 의존하여 운용이 된다. 이러한 단말들의 가장 중요한 최적화된 설계 기준은 에너지 관리가 될 것이다.
- **제한된 물리적 보안** – 유선 네트워크에 비해 모바일 무선

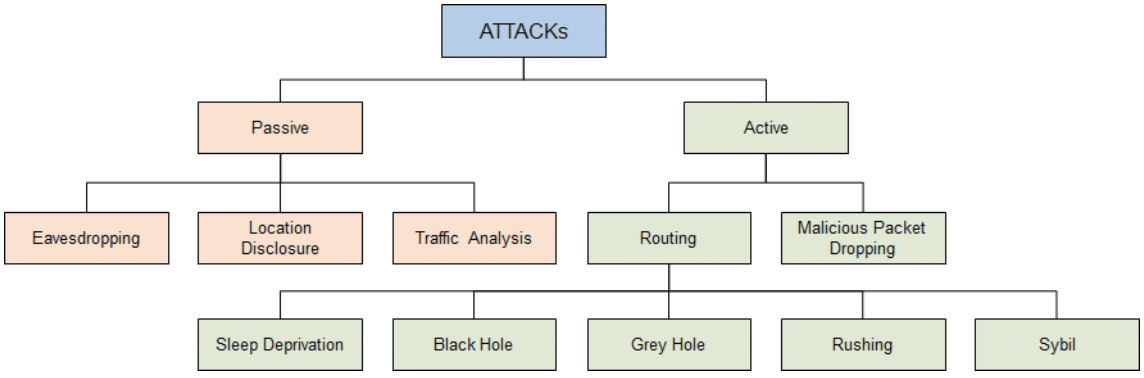

그림 2. MANET에서의 네트워크 공격 분류

네트워크는 물리적인 보안 위협을 받기 쉽다. 도청, 스푸핑, 서비스 거부 등의 공격을 받을 수 있으므로 이에 대비가 필요하다.

- **기반 시설 및 중앙 모니터링 부재** – MANET은 기반시설 제공이 어렵기 때문에 인증 기관과 온라인 서버를 기반으로 한 기존 기법의 적용이 어렵다. 또한, 중앙에서 관리하는 모니터링 시스템이 없어 대규모의 MANET에서 트래픽 모니터링이 어려워 전송 장애와 악의적인 패킷 폐기 공격 등을 받기 쉽다.

1. 전투무선체계 사이버 공격 기술

MANET 환경의 특수성을 활용한 사이버 공격 기법은 〈그림 2〉와 같이 수동형과 능동형 공격으로 분류될 수 있다[7].

수동형 공격은 라우팅 프로토콜의 동작에는 지장을 주지 않고, 도청이나 트래픽 분석을 통하여 가치 있는 정보를 찾아내는 시도들을 말한다. 결국, 네트워크 토폴로지, 단말들의 위치, 또는 중요 단말들의 신원 등과 네트워크 또는 단말들의 중요정보가 노출될 수 있다.

능동형 공격을 시도하는 비정상 행위 노드들 (misbehaving nodes)은 이기적인 노드 (selfish node)와 악의적인 노드 (malicious node)로 구분할 수 있다. 이기적인 노드는 자신의 패킷 전송은 하면서도 인접 단말의 패킷 전송은 하지 못하도록 하는 단말로서 대표적인 공격 유형은 패킷 폐기(packet dropping) 공격이 있다. 반면에, 악의적인 노드는 네트워크 단절 및 인접 노드의 자원 고갈을 유도하며, 대표적인 공격 유형은 정상 노드를 비정상 노드로 허위 지목하여 해당 노드를 고립시키는 거짓 지목(false accusation) 공격이 있다.

MANET에서는 정보전달을 위한 라우팅의 역할이 매우 중요하며, 라우팅 프로토콜을 대상으로 한 공격은 네트워크 인프라 및 운용에 지장을 초래한다. Sleep Deprivation Attack, Black Hole Attack, Gray Hole Attack, Rushing Attack, Sybil Attack들은 매우 잘 알려진 MANET에서의 라우팅 프로토콜을 대상으로 하는 공격들이며, TICN의 TMMR 단말들도 이러한 공격의 피해를 입을 수 있다.

2. 전투무선체계 사이버 공격 방어 기술

본 절에서는 MANET을 대상으로 하는 사이버 공격에 대응하는 방어 기법들을 소개한다[7].

데이터 패킷 폐기 공격의 경우, 매우 다양한 연구가 이루어졌다. 협동 참여(cooperative participation), 이웃 감시 시스템(NWS, Neighbor Watch System), 흐름 보존(flow conservation) 원리 기반 방어 기법들과 비정상행위 노드 탐지 및 회피 기법인 Watchdog과 Pathrater가 제안됐었다.

Sleep Deprivation Attack 은 이 공격을 제안한 저자가 이웃 감시를 기반으로 RREQ 플러딩 방어 기법도 함께 제안하였다. 공격 중에도 파워 보존이 가능한 아키텍처와 공격을 탐지할 수 있는 경량의 중간층 프로토콜도 제안됐었다.

Black Hole Attack 공격에 대한, 다양한 방어 기법들이 존재한다. 토폴로지 정보 획득이 가능한 경우에 동작이 가능한 TOGBAD 기법, 고정 임계치를 기반으로 한 블랙홀 탐지 기법, RREP 시퀀스 번호를 기반으로 한 블랙홀 공격 탐지 기법 등이 있다.

Gray Hole Attack에 대한 방어를 위하여 전달한 패킷의 근거를 기반으로 하여 라우팅 프로토콜 차원에서의 탐지 기법이 제안된 바 있다. Rushing Attack 에 대응하는 방법으로는 안전한 이웃 탐지, 안전한 경로 탐지, 무작위 RREQ 전달과 같은 일반적인 알고리즘을 활용한 기법들이 제안되고 있다.

Sybil Attack의 경우는 인증서를 활용한 방어 기법, IP 주소 또는 MAC 주소를 추적하여 이동성을 식별하는 방어 기법, 단말의 무선 자원 테스트를 통한 방어 기법들이 제안되었다.

표 1. 전술네트워크 주요 공격 및 위험요소 분석

주요공격		취약성정도	공격효과	위험성	대응기술	공통방어방법론
수동형 (passive)	Eavesdrop	Low	High	Low	Cryptography	• Cryptography • Authentication • Tunneling • Anti-Jamming • Cross-layer Approach • Policy-driven Management
	Traffic Analysis	High	Low	Medium	Traffic Obfuscation	
능동형 (active)	DoS	Low-High	High	Low-High	Layer specific mechanisms	
	Masquerade	Low	Very High	Medium	Trust System Cryptography	
	Modification	Low	High	Low	Cryptography	
	Jamming	High	High	High	Anti-Jamming Cognitive Radio	

Ⅳ. 기간접속체계 대상의 사이버 공격 및 방어 기술

전술한 바와 같이, TICN의 부체계들 중 HCTRS와 LCTRS는 각각 여단(연대)급 이상과 대대급 부대 통신소간의 고속 대용량과 소용량의 무선 전송 능력을 제공한다. 이들 HCTRS와 LCTRS 부체계들은 TMMR과 같은 이동성을 제공하지 않고, 백본 무선 전송로의 기능을 제공한다. 본 고에서는 HTRS와 LCTRS를 기반으로 하는 군단급 네트워크를 기간접속체계로 칭하기로 한다.

1. 기간접속체계 대상의 사이버 공격

〈표 1〉에는 기간접속체계를 대상으로 하는 주요 공격 및 위험요소를 분석하여 정리하였다[9][10]. 〈표 1〉에서 보는 바와 같이 기간접속체계를 대상으로 한 공격 유형은 크게 수동형과 능동형으로 구분 가능하다.

수동형 공격의 대표적인 형태는 **도청(Eavesdropping)**과 **트래픽 분석(Traffic Analysis)**이다. 기간접속체계를 통하여는 지휘관들과 전투원들간의 명령 및 보고 정보, C4I의 지휘통제체계와 각종 무기체계 정보들, 그리고 공통상황인식과 제어를 위한 전장관리체계 정보들이 전달되므로, 이에 대한 도청이나 트래픽 분석 공격은 치명적일 수 있다.

서비스 거부(Denial of Service, DoS) 공격은 능동형 공격의 대표적인 형태들 중의 하나이다. 서비스 거부는 기간접속체계를 구성하는 각 통신장비를 대상으로 또는 전장관리체계를 대상으로 하여 전술운용의 인프라에 지장을 주는 치명적인 요소가 될 수 있다.

가장(Masquerade)은 네트워크 내의 노드를 가장하여 행동하는 공격이다. 전술망에서의 중요 정보에 직접 접근하는 것은 어려워 보이지만, 만약 중요한 정보를 수집하고 정보를 조작하는 것이 성공할 경우 기밀성과 무결성에 치명적인 영향을 미칠 수 있다[10].

조작(Modification)은 네트워크에서 전송되는 정보를 가로채서 자신에게 유리하도록 조작하는 공격이다. 공격자는 이를 위해서 네트워크의 구성원으로 인증되어 있어야 한다. Masquerade 공격이 이를 위해 활용될 수 있다. 전술 네트워크의 기간접속체계에서 정보 조작이 이루어질 경우 정보의 기밀성과 무결성이 손상되어 큰 피해를 입힐 수 있다.

재밍(Jamming) 전술에는 공격 대상에 따라 여러 가지로 나눌 수 있다. 초고주파 에너지를 방사함으로써 특정 주파수나 전파의 사용을 거부하도록 교란하는 형태 또는 허위 정보를 전송하도록 하는 기만 형태로 나눌 수 있다. HTCRS와 LCTRS의 대용량의 장거리 무선 전송로를 제공하는데, 이를 대상으로 한 재밍(Jamming) 공격은 무선 전송로의 용량 저하가 발생할 뿐만 아니라, 라우팅 경로의 불안정을 초래하게 된다. 우회 라우팅에 의하여 특정 노드나 무선링크에 트래픽이 집중되는 다수의 혼잡 링크 구간 형성과 자원 분배의 불균등이 발생할 수 있다. 또한 작전 수행을 위해 신뢰성, 적시성, 안정성, 수용성, 지속성 등의 요소를 필요로 한다.

2. 기간접속체계 대상의 사이버 공격 대응 기술

암호화(Cryptography)는 적이 통신 내용을 가로채더라도 정보를 확인할 수 없게 함으로써 작전 수행 간 생존성 및 기밀성을 보장할 수 있다. NCW 전장 환경으로 변화 되면서 암호 체계에 대한 관리가 중요시되고 있다. NCW 환경은 유/무선은 물론 위성통신을 결합하여 전장 정보를 공유하므로 안전하게 네트워크를 통해 전달하기 위해 데이터 암호화 기법을 사용한다.

인증(Authentication)을 위한 국방인증체계는 모든 국방인력

을 대상으로 공개키 인증서를 발급, 관리하므로 신원관리, 식별 및 인증의 공통 인프라 역할을 담당한다. 유기적인 네트워킹과 정보의 공유가 강조되는 NCW 환경에서는 네트워킹에 참여하는 사용자 및 개체들의 신원을 정확히 확인, 검증할 수 있는 인증 체계가 필수적으로 요구 된다.

보안 터널링(Tunneling)은 공격자가 네트워크 패킷을 수집하거나 가로채기 어렵도록 무선매체를 보호하여 준다. 공격자가 터널 내부에서 교환되는 정보를 파악하기 어렵고, 패킷을 획득하더라도 헤더부분까지 보호가 되어있어 프로토콜 등을 분석하는 것이 어렵다. 차세대 전술통신망은 ALL IP 기반으로 구축되기 때문에, 다양한 종류의 단말들의 종단간 보안을 실현하기 위해 IPSec 기반 터널링이 사용될 것으로 예상된다.

항재밍(Anti Jamming)은 주로 대역 확산이 주로 사용되고 있으나, 채널부호화, Interleaving 등의 보수적 기법 그리고 Clipping, Erazing, 필터링 등의 적극적 기법도 활용되고 있다. 또한 지향성 안테나를 사용하여 빔 형성에 의한 널링도 강력한 대응의 하나로 자리매김하고 있다. 고속의 데이터 통신을 위해 개발된 OFDM 기술은 광대역 통신으로 주목 받고 있으나 그 기법만으로는 재밍에 매우 취약하여 재밍 존재 시 심각한 성능 열화가 존재한다. 이를 보완하기 위해 Multi-carrier 기법 등도 연구 적용되고 있다.

정책기반관리(PBM, Policy-Based Management) 기술은 전술 운용 및 서비스 차원의 관리 정책을 정의하고 이를 기반으로 네트워크 및 서비스를 일관된 정책에 의하여 자동으로 관리하는 기술이다[11]. 특히, 전술 네트워크의 급변하는 통신 환경에 적응하고, 다양한 사이버 공격에 대응하기 위하여, 각국의 전술 네트워크에는 PBM의 적용을 우선적으로 고려하고 있다[12].

Ⅴ. TICN 기반 전장관리체계 유통 시 사이버 공격 특징 분석

본 장에서는 전장관리체계를 대상으로 한 사이버 공격 가능성을 분석하고자 한다. 이를 위하여, 앞서 구분한 바와 같이, HCTRS과 LCTRS를 사용하는 대형 · 중형 부대 중심의 전술네트워크 체계인 기간접속체계와 TMMR을 기반으로 하는 대대급 이하의 소부대 전술네트워크 체계인 전투무선체계로 구분하기로 한다.

1. 기간접속체계 전장관리체계 대상 공격 특성

〈그림 3〉은 전술한 기간접속체계에서의 전형적인 정보 전달 형태를 보여준다. 하급 제대 단말기들로부터의 정보는 상위 부대의 서버에서 통합되고, 이 통합된 정보들은 다시 또 상위의 부대 서버로 전달되어 통합된다. 마지막으로 최상위 부대의 통합 서버로 모든 정보가 집중되어 전장 상황에 대한 공통 인식이 가능해지게 된다. 또한, 상급 부대에서는 필요한 정보들을 가공하여 하급 부대로 하향으로 전달하게 된다.

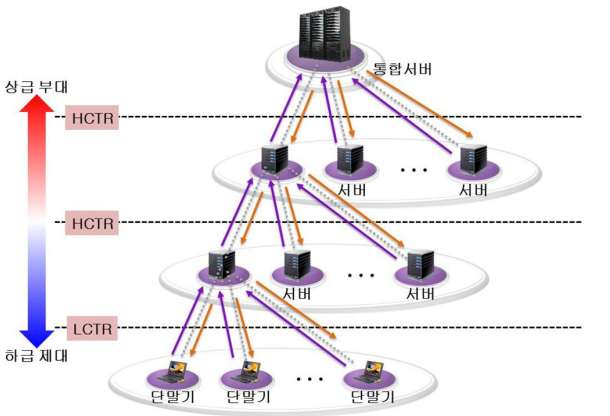

그림 3. 기간접속체계의 전장정보 전달 구조

〈그림 3〉에서 보는 바와 같이, 기간접속 체계에서의 지휘통제 체계 정보 전달은 하급 제대에서 상급 부대로 정보가 모이는 중앙집중형의 Stove-Pipe식의 Bottom-UP 구조로 구성되어 부대 편제에 따라 계층적인 구조를 갖는다. 이러한 네트워크 구조는 상급 부대에서 넓은 범위에 퍼져 있는 하급 제대들을 지휘통제하기에 용이하지만, 상급 부대로 갈수록 몰려드는 데이터의 양으로 인해 부하량이 증가하고, 상급 부대에서 네트워크에 이상이 생길 경우 하급 제대들이 모두 단절되는 등의 피해를 입을 수 있는 위험성을 가지고 있다.

이러한 중앙집중형 네트워크 구조는 상급 부대 또는 같은 소속 부대로 데이터를 전송할 경우 모두 직속 상급 부대를 거쳐서 전달하게 된다. 이는 중앙에 있는 서버로 모든 제어 정보와 데이터 트래픽이 집중되기 때문에 상급 부대로 갈수록 트래픽 과부하가 심해져 네트워크 장애 혹은 고장에 대한 위험 부담이 커진다. 뿐만 아니라, 극단적인 경우로 코어 역할을 하는 부대에 이상이 발생하거나 공격을 받을 경우 하위에 있는 모든 부대의 통신이 마비될 수 있다. 반면 데이터가 각 상급 부대를 거치면서 분석 및 재검토되기 때문에 중간에 공격 트래픽이 확산되는 것을 발견하여 대처하기에 용이하다.

2. 전투무선체계 전장관리체계 대상 공격 특성

TICN의 엣지(edge)에 위치하는 부체계인 전투무선 체계는 전술 MANET의 형태와 이의 특징을 갖는다.

전투무선체계는 적과 직접 대면하여 전투를 수행하는 체계로

전쟁의 성패를 좌우하는데 지대한 영향을 미칠 수 있으며, 따라서 이러한 전장 정보를 신속하고 정확하게 전달하는 것이 매우 중요하다.

〈그림 4〉는 전투무선체계에서의 전장정보 전달 과정을 보여준다. TMMR 장비에 연결된 단말로부터의 정보는 MANET 구조의 전투무선체계 네트워크를 통하여 통제단말기에 전달된다. 이 정보는 연동서버를 통하여 ATCIS 단말기에 전달되어, 앞 절에서 설명한 방법에 의하여 기간접속체계의 전장관리체계에 연동되게 된다.

전투무선체계에서의 전장정보전달 체계도 기간접속체계에서와 마찬가지로 하위제대 단말기에서 상급 부대 서버로 전달되는 중앙집중형의 Stove-Pipe식의 Bottom-UP 구조를 갖는다. 그러나, 기간접속체계에서와 같이 명시적인 노드간 경로보다는 MANET의 라우팅에 의하여 동적인 노드간 릴레이를 통하여 정보 전달이 이루어진다. 이러한 MANET의 라우팅 과정을 통하여 상급 부대로 정보가 전달되는 과정에서 문제가 발생하면 하급 제대들이 모두 정보 공유와 전장상황 인식의 장애를 입을 수 있다. 또한, 네트워크 장애 측면에서 문제를 야기할 수 있다. 중앙에 있는 서버로 모든 제어 정보와 데이터 트래픽이 집중되기 때문에 상급 부대로 갈수록 트래픽 과부하가 심해져 네트워크 장애 또는 고장에 대한 위험 부담이 증가한다. 극단적인 경우에는 코어 역할을 하는 부대의 통합 서버에 이상이 발생하여 공격을 받을 경우 모든 하위 제대들의 통신이 마비될 수 있다.

전투무선체계는 다른 부체계와는 달리 MANET의 특징을 가지므로, 이로 인하여 보안에 매우 취약한 특징을 갖는다. 따라서 이를 고려한 사이버 공격 및 방어 기법들의 고려가 필요하다.

전투무선체계는 제한된 무선 주파수 대역을 사용하므로 라우팅 오버헤드를 줄이고, 플러딩과 주기적인 메시지 발생을 최소화해야 할 필요가 있다. 이러한 오버헤드는 전장 정보의 적시 전달에 장애를 줄 수 있으므로, 이에 대비하여야 한다.

특히, 전장관리에서는 위치의 인식이 매우 중요하므로, 빠르게 움직이는 TMMR들의 정확한 위치 인식이 필요하고, 이의 정보를 오도하기 위한 공격에 대하여도 대비하여야 한다. Stove-Pipe 식의 정보 전달 구조에서 하급 제대의 정보들을 통합하는 노드들에 대한 보호 체계를 고려하여야 한다.

Ⅵ. 결 론

본 고에서는 전술네트워크 및 전장관리 체계를 대상으로 하는 사이버 공격의 형태와 특징에 대하여 살펴보고, 이에 대응하기 위한 방어 방법들에 대하여 고찰하였다.

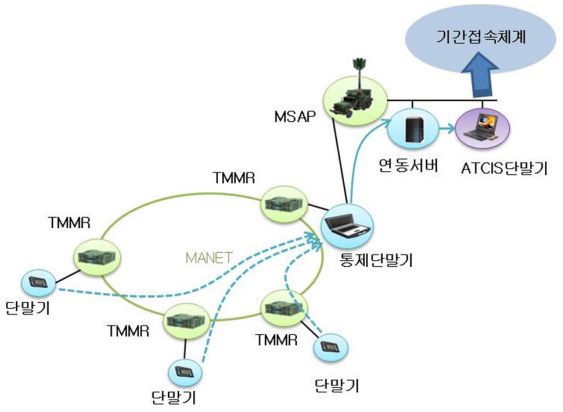

그림 4. 전투무선체계에서의 전장정보 전달 구조

우선적으로, 전술정보통신체계인 TICN 구조, 전장관리체계들, 그리고 이들의 특징을 소개하였다. 전술네트워크와 전장관리체계는 군의 고유한 계층구조에 따른 Stove-Pipe 식의 상향식 정보교환 구조를 가지므로, 기존의 상용망이나 상용서비스 대상의 사이버전 위협과는 다른 문제가 발생하게 될 수 있음을 보였다. 특히, TICN은 부체계의 종류와 네트워크 구조, 그리고 링크의 능력에 따라 HCTRS와 LCTRS를 기반으로 하는 대형 · 중형 부대 중심의 기간접속체계와 TMMR을 기반으로 하는 소부대 전투무선체계로 구분하여 사이버 공격의 연구에 필요한 접근 방법론을 제시하였다.

현재 우리군에서는 TICN과 전장관리체계의 구축을 진행하고 있다. 모든 요소들이 네트워크에 연결되는 NCW 환경은 전장정보의 신속한 전달과 공유를 통한 통합 전투력 향상을 제공하여 주지만, 사이버 공격의 위협을 동시에 내포하고 있다. 기존에 많은 일반 및 상용 네트워크나 서비스를 대상으로 하는 사이버 공격에 대한 연구는 많이 이루어지고 있으나, 본 고에서 소개한 바와 같이, 전술네트워크는 그 특성상 이러한 기존 연구들을 그대로 적용하는 데는 한계가 있다. 또한, 국방 선진 각국의 전술네트워크는 국가마다 고유의 전술운용 개념들이 반영되므로, 타국의 결과를 우리나라 경우에 그대로 적용하는 것은 무리가 있을 수 있다. 따라서, 우리 군의 전술네트워크 운용개념과 전장정보 전달구조를 고려한 독자적인 사이버전 대응 전략 수립과 이에 대한 연구가 필요하다.

Acknowledgement

본 연구는 국방과학연구소의 지원을 받는 “사이버전 모의를 위한 모델 설계 및 구현 기술” 연구의 일환으로 수행되었음.

참 고 문 헌

[1] 김종철, 정종관, 노병희, “전술통신 네트워크와 QoS 기술,” 전자공학회지, 제35권 제10호, pp.40-52, 2008년 10월

[2] 하영석, 정영철, 임용환, 양현상, "전술 정보통신 체계를 위한 공중중계용 UAV 개발에 관한 연구," 한국통신학회, 2009년 하계 학술대회 논문집, 2009년 6월

[3] 김혜진, 이상훈, "육군 전술 지휘정보체계 (ATCIS) 장애요인분석," 한국정보과학회, 2014년 동계 학술 발표회 논문집, 2014년 12월

[4] 방승호, 이태억, "NCOE구축을 위한 B2CS 정보 공유 체계 모델링 및 작전운용 효율성 분석," 대한산업공학회, 2015년 춘계공동학술대회 논문집, 2015년 4월

[5] 오행록, 김성용, 신석철, "군사 정보 통합 처리 체계 소개 및 발전 방향," 한국 방위산업 진흥회, 국방과기술, 제377권, pp.90-97, 2010년 7월

[6] J. Andress, and S. Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 2nd ed., Syngress, 2011

[7] A. Nadeem and M. P. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, Fourth Quarter, 2013.

[8] 박승, "전장관리체계 운용을 위한 전투지휘용 차량의 성능개량 개념," 한국군사과학기술학회지, 제11권, 제2호, pp.16~22, 2008년 4월

[9] R. S. Ross, “Managing Information Security Risk: Organization, Mission, and Information System View,” Special Publication (NIST SP) - 800-39, Mar. 2011

[10] D. Kidston, L. Li, H. Tang, and P. Mason, “Mitigating Security Threats in Tactical Networks,” Communications Research Centre (CRC), White Paper, Sep. 2010

[11] 한국통신학회 군통신연구회, 군통신시스템, 제5장 전술네트워크 QoS 및 망관리 기술, 홍릉과학출판사, 2014년 1월

[12] R. Chadha, L. Kant, Policy-Driven Mobile Ad-Hoc Network Management, John Wiley & Sons, Inc. 2008

약 력

김 보 성

2009년 아주대학교 정보컴퓨터공학부 학사
2015년 아주대학교 컴퓨터공학과 박사
2015년~현재 아주대학교 정보통신연구소 선임연구원
2012년 IWUCA ’2012 최우수논문상 수상
2014년 KCC ’2014 우수발표논문상 수상
관심분야: 정보보안, 국방전술통신, 사물인터넷, 센서네트워크, 인지무선통신, 멀티미디어통신, 위성통신, 모델링과 시뮬레이션

안 효 춘

2010년 State University of New York 공학석사
2015년 아주대학교 공학박사
2000년~현재 육군 정보통신장교
관심분야: 정보보안, 사물인터넷, 인지무선통신, 국방전술통신

노 병 희

1987년 한양대학교 공학사
1989년 한국과학기술원 공학석사
1998년 한국과학기술원 공학박사
1989년~1994년 한국통신 통신망연구소 연구원
1998년~2000년 삼성전자 연구원
2005년 StonyBrook University 방문교수
2014년 국방과학연구소 겸임연구원
2000년~현재 아주대학교 교수
2011년~현재 서울어코드활성화지원사업 책임자
관심분야: 모바일 멀티미디어 통신, 사물인터넷(IoT) 플랫폼 및 응용서비스, 미래인터넷, 네트워크 보안, 국방사이버전, 전술네트워크