KIICE 한국정보통신학회지 13권 2호
THE MAGAZINE OF KIICE
http://www.kiice.org

전술 MANET 시큐리티 동향 및 전망

김영동

동양대학교 국방기술대학 정보통신공학과

목 차

Ⅰ. 서 론

스마트 폰의 대중화로 특징 지워지는 정보통신 시대는 3G(3rd Generation)시대를 넘어LTE(long term evolution)로 불리는 모바일 스마트 기술 시대로 진입하고 있다.

모바일 스마트 기술은 음성통화 서비스라는 고유의 목적을 넘어 인터넷과 각종 멀티미디어 서비스 기능을 탑재하고 개인의 일상 생활 영역 뿐만 아니라 우리 사회 각 전문적인 영역으로 그 활용범위가 확대되어 이른바 모바일 빅뱅(Mobile Big Bang)이라고 불리는 대혁신을 가져오고 있다.

스마트 단말기의 급속한 보급과 활용의 확대는 스마트폰이 갖는 강력한 연산기능과 고속의 통신기능 그리고 다양한 입출력 기능에 기반한 것이며, 하드웨어 기술의 지속적 발전과 소프트웨어 제작기술의 일반화 및 대중화라는 현재의 경향으로 미루어 볼 때 앞으로도 상당한 기간 동안 정보 단말기로서의 우월적 위치를 고수할 것으로 판단된다.

그러나, 이런 현상은 긍정적 요인 못지않게 부정적 요소를 동반하거나 증폭시키는 요인으로 작용하고 있다. 강력한 연산기능은 각종 소프트웨어의 실현의 수월성을 확보하는 긍정적 요인이 되는 반면에 정보침해 소프트웨어의 기능이 강력해질수 있는 토대를 제공하고 있으며, 고속의 통신 기능은 단말기가 정보통신망으로부터 다양한 정보를 수월하게 수집하고 활용할수 있응 수단을 제공하는 반면에 자신이 정보침해의 대상이 될수 있는 외부로부터의 공격통로가 넓어짐을 의미한다. 마지막으로 입출력장치의 다양화는 정보를 부정적 방법으로 획득하기 위한 입력수단과 획득한 정보의 손쉬운 열람이라는 악용 요소를 제공한다.

특히 이동정보 단말기에 활용에 대한 부정적 영향은 단말기가 사용되는 특정의 통신망에서 더 크게 나타날 수 있다.

서버급의 통신장치의 지원이 비교적 쉬운 기반 네트워크 통신에 접속한 단말기의 경우 방화벽을 비롯한 기타 침해대응 기능을 활용하기 수월하다. 반면에, 군사용이나 탐험/탐사 같은 목적으로 제한된 지역에서 사용되는 임시망으로서 단말기만으로 구성되는 애드-혹 통신에서는 서버급 장치의 지원이 수월치 못하기 때문에 단말기만으로 정보침해에 대비해야 한다. 따라서 애드-혹 네트워크에서의 시큐리티 문제는 비록 단말기의 고성능화가 지속적으로 추진되고 있다 하더라도 시큐리티 문제를 스스로 해결해야 하는 구조적 문제점으로 인해 인프라네트워크에 비해 매우 심각할 수 밖에 없다[1].

애드-혹 네트워크의 여러 응응 가운데 군사용인 전술 모바일 애드-혹의 경우 시큐리티 문제의 심각성은 일반 애드-혹 네트워크에 비해 더욱 가중된다. 보호대상을 넘어 비밀로 처리되어야하는 통념상 의미의 오프라인성의 군사 정보 보호가 정보통신망이라는 전달체

계의 안정화와 단말기의 이동성이라는 이용 환경의 동적 요인과 같은 여러 요소들이 동시에 작용하는 곳에서 전자화된 정보유통체계를 대상으로 시큐리티 문제를 해결해야 하기 때문이다.

이 글에서는 이런 현상들을 고려해서 군사용으로 사용되는 전술 MANET(Mobile Ad-hoc Network)의 시큐리티 문제 해결을 위한 최근의 동향과 앞으로의 전망에 대해서 살펴본다.

이 글은 I장의 서론에 이어 II장에서 모바일 시큐리티의 동향, III장에서 애드-혹 네트워크 시큐리티 기술, IV 장에서 전술 MANET 시큐리티 전망 그리고 V장에서 결론의 순서로 구성한다.

Ⅱ. 모바일 시큐리티 동향

모바일 환경을 비롯한 IT분야에서 시큐리티 문제는 일반적으로 가용성(Availability), 인증(Authentication), 기밀성(Confidentiality), 무결성(Integrity), 부인봉쇄(Non-Repudiation)의 속성으로 다루어져 왔다.

- 가용성 : 네트워크 또는 장비에 대한 공격이 있다 하더라도 정보 송수신이 가능
- 인증 : 정당하게 허가된 사용자만이 하드웨어 및 소프트웨어 자원의 사용이 가능
- 기밀성 : 보관되어 있거나 이동중인 정보에 대한 부정한 판독의 불가능
- 무결성 : 보관되어 있거나 이동중이 정보에 대한 부정한 변경의 불가능
- 부인봉쇄 : 시큐리티 침해 행위 수행에 대한 부인의 불가능

시큐리티 속성간의 상호 작용은 그림 1과 같다.

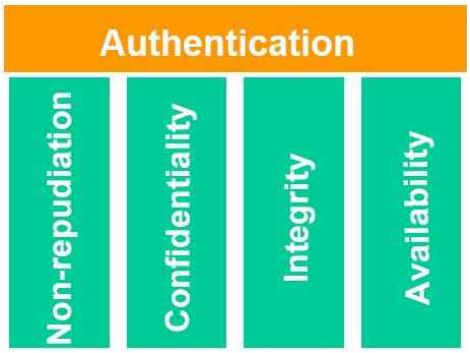

그림 1. 시큐리티 속성[2].

시큐리티 속성들을 고려한 모바일 환경에서의 침해 대응 보호 요소들은 그림 2와 같이 단말보호, 네트워크 보호, 서비스 보호, 콘텐츠 보호 등으로 구성되며 각각은 다음과 같이 정의된다[2].

- 단말보호 : 모바일 단말에서 기업·개인 정보유출, 부정·불법 사용, 임의 조작등을 유발 시키는 위험으로부터 보호
- 네트워크 보호: 무선 네트워크 전송 구간(WiFi, 블루투스, 3G/4G, WiBro)에서 발생되는 비인가 접속 및 DDoS 공격 같은 네트워크 침해 사고로부터 보호
- 응용 서비스 보호 : 모바일 클라우딩 컴퓨팅, mVoIP, mIPTV, SNS 등의 모바일 서비스에 대한 불법사용, 거부·오용에 대한 위협으로부터 보호
- 콘텐츠 보호 : 모바일을 통해 유통·이동되는 콘텐츠에 대한 불법 유출·삽입을 일으키는 저해 요소로부터 보호

그림 2에 의하면 각 영역별 침해 유형으로 단말영역의 악성코드감염, 단말동작 마비, 단말 분실과 그로 인한 정보유출, 네트워크 영역의 무선기기에 대한 공격, 무선기기 비인증 사용, 응용서비스 영역의 개인정보유출, 모바일 시스템 해킹, 모바일 서비스 중단, 콘텐츠 영역의 디지털 저작권 침해, 유해·불법 정보의 유통 등이 있다.

그림 2. 모바일 4대 영역별 보안 위협[3].

이에 대하여 모바일단말 보안강화, 무선네트워크 안정성 확보, 모바일 서비스·콘텐츠 보호로 구성되는 모바일 서비스·인프라 보안품질 향상, 다음으로 모바일 개인정보보호 및 위치정보 보호 강화, 모바일 스팸방지 및 최소화, 모바일 유해정보 유통방지로 구성되는 모바일 이용자 프라이버시 보호, 마지막으로 모바일 정보보호 기반 조성 등으로 나누어 대응 방안이 추진되고 있다.

Ⅲ. MANET 시큐리티 기술

모바일 스마트 단말기로 구현 가능한 응용 분야 중에 하나로 MANET이 있다. MANET은 통신기반구조의 활용이 어려운 환경에 설치·운용되는 임시통신망으로서 학술, 레저, 탐험·탐사, 긴급통신 및 군사통신 등에 사용되고 있으며, 고성능 스마트 단말기 보급 확대로 그 활용이 증가할 것으로 예상된다.

모바일 스마트 기술이 발전되어 MANET 활영에 유리한 환경이 조성되고 있으나 여전히 발생되고 있는 MANET의 취약점을 살펴보면 시큐리티 약점, 통신 기기 크기의 한계, 배터리 수명 문제, 통신 환경의 가변성, 데이터 이동 속도 및 대역의 제약 등 다양한 형태로 나타나고 있다[4].

특히, MANET 시큐리티 문제는 인프라네트워크에 비하여 매우 심각하다. MANET의 경우에 서버와 같은 통신기반구조의 지원이 용이하지 못하고, 단말기의 고성능화가 이루어진다 하더라고 성능 개선의 한계가 있고, 단말기라는 기기 구조상 제약점으로 인해 서버 급의 침해 대응 방안 갖추는 것이 수월치 않아 시큐리티 문제에 매우 취약한 약점이 있다.

MANET에서 시큐리티 취약점에는 표 1과 같이 크게 능동공격과 수동공격이 있다.

능동공격은 기기나 기능에 대하여 직접 공격을 가하여 피해를 일으키는 공격유형으로, 공격기기가 피공격 기기에 공격을 가하여 기기의 기능을 마비 또는 오동작을 발생시키거나, 장치에 저장된 데이터나 네트워크를 통하여 이동중인 데이터를 위조·변조시키거나, 네트워크 기능에 변화를 주어 정상적인 데이터 유통을 방해하여 공격자의 의도대로 진행되게 하는 유형의 공격으로 공격대상기기에 직접적인 피해를 일으키는 공격을 의미한다.

이와는 반대로 수동공격은 기기나 기능에 대하여 직접적인 공격이 아니라 이동중인 데이터를 감시 또는 관찰하거나 기기가 전송하는 데이터를 분석하는 등 정보습득을 목적으로 수행되는 공격으로 기기나 데이터에 대하여 직접적인 피해를 일으키는 않는다.

표 1. MANET 시큐리티 취약점 분류.

분 류	공 격 유 형
능동공격	위조, 변형, DoS, 스푸핑, 시빌공격, 싱크홀공격, 웜홀공격, 블랙홀공격, 그레이홀 공격 등
수동공격	도청, 트래픽분석, 감시 등

MANET에서 발생되는 공격유형을 네트워크 계층 구조와 관련시켜 살펴보면 표 2와 같이 물리계층에 대한 공격으로부터 응용계층 그리고 다중계층공격에 이르기까지 매우 다양하다.

표 2에서 몇가지 대표적인 유형의 공격을 살펴보면 다음과 같다.

- MAC 붕괴 : MAC 프로토콜을 공격하여 정상적인 데이터 이동을 방해
- 웜홀공격 : 특정 패킷들을 한 지점에서 다른 지점으로 이동
- 블랙홀공격 : 패킷을 특정 지점으로 이동시킨 후 이를 폐기함으로서 데이터의 정상적인 이동을 방해

- 그레이홀공격 : 패킷을 특정지점으로 이동시킨 후 이중 일부의 특정 패킷만을 폐기하고 나머지는 목적지로 전달

- 플러딩공격 : 특정 메시지를 지속적으로 발생시켜 네트워크의 전송기능을 방해. 라우팅 플러딩과 SYN 플러딩으로 분류

- 세션하이제킹공격 : 획득한 공격대상자 정보를 사용하여 정상적인 세션을 가로챈 다음 이를 이용하여 공격을 시도

- 데이터손상공격 : 응용계층에 발생되는 유형의 공격으로 바이러스나 웜 소프트웨어에 의한 데이터 변경

- DoS 공격 : 대규모의 데이터를 네트워크에 발생시켜 네트워크의 전송기능을 마비시키거나 데이터의 정상적인 이동을 방해

표 2. MANET 프로토콜 계층별 공격 유형[5].

계 층	공 격 유 형
다중계층	DoS, 메지지 가로채기, 위장, 재전송
응용계층	부인, 데이터 손상
전송계층	세션 하이제킹, SYN 플러딩
네트워크계층	웜홀, 블랙홀, 그레이홀, 라우팅 플러딩, 자원소모
데이터링크계층	트래픽 분석, 감시, MAC 붕괴
물리계층	재밍, 가로채기, 도청

이와같은 다양한 종류의 공격에 대한 시큐리티 대책을 프로토콜 계층 구조상에서 살펴보면 표 3과 같다. 표 3에 제시한 계층별 시큐리티 대책은 일반응용, 긴급통신, 전술용, 센서네트워크 등 MANET 응용환경에 따라 적절한 방식으로 구현되어질 수 있다.

표 3. MANET 프로토콜 계층별 시큐리티 대책[6].

계 층	시큐리티 대책
응용계층	바이러스, 웜, 악성코드, 응용기능 남용의 검출 및 방지 대책
전송계층	인증수단의 확보 종단간 안전한 통신 방안 확보
네트워크계층	애드혹 라우팅 및 포워딩 프로토콜 보호 방안
데이터링크계층	무선 MAC 보호방안, 링크계층 시큐리티 지원 방안
물리계층	신호 재밍 방지 방안

Ⅳ. 전술 MANET 시큐리티 전망

MANET은 설치, 확장, 축소 및 철수의 용이성 등으로 인하여 군사적 목적에 많이 활용되고 있다. 군사적 목적으로 활용되는 MANET을 전술 MANET이라 하는데 군사적 용도의 여러 통신 서비스를 아우르는 개념으로 사용되고 있으며 T-MANET(Tactical MANET) 또는 M-MANET(Military MANET)이라 불리기도 한다.

전술 MANET은 민간용 MANET에 비하여 네트워크의 안정성과 신뢰성이 강조된다. 전술 MANET의 안정성은 시큐리티 문제와 직결되는 것으로서 기기나 네트워크의 동작에 대한 신뢰성과 유통되는 정보의 보호를 포괄하는 개념으로 볼수 있다. 전술 MANET의 시큐리티는 정보영역, 이동영역, 장비영역으로 나누어 구성된다.

정보영역은 전술 MANET에서 저장·이동·활용되는 정보자체에 대한 보호를 의미하는 것으로서 기밀성과 무결성이 중요 보호 속성이 된다. 정보가 노출되어도 판독되지 못하도록 생성·관리되어야 함을 의미한다.

이동영역은 정보가 이동하는 네트워크 측면의 시큐리티 문제이다. 이 단계에서는 인증, 기밀성 및 무결성이 강조되는데, 특히 무결성이 중요한 요소이다. 전술 MANET의 경우 습득한 정보의 위변조가 미치는 영향이 매우 크기 때문이다.

마지막으로, 장비영역은 일반 MANET과는 달리 전술 MANET에서 특히 중요시되는 요소로서 전술 MANET에 연결된 각종 정보기기가 정상적인 작동상태를 유지하도록 보호하는 기능을 의미한다. IT 기술

을 사용한 지능형 장비인 경우 사소한 하나의 기능 장애가 발생하더라도 전체 장비의 활용에 치명적인 문제점을 유발할수 있다. 따라서 전술 MANET에 사용되는 각종 지능형 IT 장비의 가용성을 확보하는 것은 매우 중요한 시큐리티 문제이다.

전술 MANET 시큐리티 세 영역 가운데 정보영역과, 이동영역은 일반 MANET과 크게 다르지 않으므로 이 장에서는 장비영역에 대한 시큐리티를 중심으로 살펴본다.

장비에 대한 시큐리티 공격은 장비운용에 대한 공격과 장비자체에 대한 공격으로 나누어진다. 장비운용과 관련된 시큐리티 공격은 장비의 운용과 관련 통신체계에 혼란을 주거나 수집된 데이터를 위·변조하여 장비가 목적한 데로 운용되지 못하도록 하는데 목표르 두고 있다. 바이러스나 스팸 또는 트로이목마와 같은 악성 소프트웨어를 사용하여 공격을 시도하거나 데이터를 탈취하여 공격자가 원하는 데이터로 위·변조하여 삽입시키는 것을 의미한다. 이런 형태의 침해는 동시에 광범위하게 다발적으로 발생되게 할수도 있지만 지정된 시간에 소규모로 발생시키거나 또는 랜덤한 시간에 랜덤한 형태로 실행하도록하여 장비운영에 어려움을 발생시킬수도 있다.

장비자체에 대한 공격은 센서나 통신기능 또는 전원 기능과 같은 장비의 특정 부분을 전통적인 화력이 아니라 정보기술을 활용한 소프트웨어적 또는 하드웨어적 방법으로 공격하여 무력화시키는 형태로 발생되어진다.

예를 들면 특정 센서에 한계용량을 초과하는 동작을 지속적으로 일으키도록 하여 감지기능 자체를 무력화하거나 잘못된 감지결과를 전송하게 만들거나, 간헐적으로 오동작시켜 장비에 대한 신뢰성을 낮추도록 만드는 등의 방법이 있을 수 있다.

장비에 대한 공격으로 발생할 수 있는 몇몇 주요 시큐리티 문제를 살펴보면 다음과 같다[7].

- 센서도청 : 유·무인 장비에 설치된 센서에서 발생되는 데이터를 가로채어 분석하고 이를 역활용하는 공격형태. 필요하면 공격자가 의도하는 데이터로 교체하여 혼란을 초래

- 배터리소진 : 공격대상 장치에 대하여 지속적인 데이터 전송 요청 시도 등의 방법을 통하여 짧은 시간 내에 배터리를 소진하게 하여 더 이상 사용하지 못하게 하는 공격형태. 무인 소형탐지기 등에 유효한 공격

- 무선재밍 : 무선 주파수 대역에 대한 공격으로 재밍신호를 사용하여 해당 주파수를 통한 데이터 전송을 방해. 통신기능 자체를 파괴하지는 않으나 동작을 무력화함으로서 장비 불능을 초래하는 공격형태

- 탬퍼링(tampering) : 장비의 하드웨어를 파괴하거나 분해는 공격형태

전술 MANET에 대한 시큐리티 공격은 단말기 중심으로 구축되는 MANET 자체로서 해결하기 쉽지 않다. 특히 안정성이 전제되어야 하는 군사적 목적의 MANET에서 있어서는 시큐리티 문제를 해결하기 위해서는 인프라네트워크나 특수목적의 통신체계의 지원이 필요하다.

교란 억제 네트워크라고 불리우는 DTN (Disruption-Tolerant Network)이 대표적인 예이다[8]. DTN은 정보체계에 대한 침투 및 교란을 위한 공격용 기술에 대한 정보체계와 정보를 보호하기 위한 기술로서 무선구간의 전파방해, 스푸핑(spoofing), DoS 공격뿐만 아니라 네트워크 차체에 대한 공격에 대하여 신뢰성있는 통신수단을 제공할 목적으로 개발되고 있다. DTN을 확대하여 다양한 형태로 나타나는 전술 MANET의 시큐리티 문제에 대응하려는 노력들이 시험적으로 전개되고 있다.

전술-MANET의 시큐리티 문제는 방어를 통한 자원의 정상적인 작동을 보장하는 초기 단계를 넘어 상대 자원을 무력화하는 단계로 진입하고 있으며, 궁극적으로는 상대 자원을 자신의 자원으로 활용하는 단계로 발전해 나갈 것으로 생각된다.

Ⅴ. 결 론

이 글에서는 설치·운용의 수월성으로 인해 군사용으로 전술 MANET의 시큐리티 문제의 동향과 전망에

대하여 개략적으로 살펴보았다. 전술 MANET의 시큐리티 문제는 일반 MANET 과는 달리 안정성에 우선하고 있은데 이 안정성은 장비운영과 장비자체에 대한 시큐리티 문제로 나타나고 있음을 볼 수 있었다.

전술 MANET의 시큐리티 확보를 위한 다양한 방안이 있을수 있으나 대표적인 예로서 DTN을 활용하는 방안에 대하여 살펴보았다.

점차 지능화되고 있는 정보기술이 군사적 공격 수단으로 사용될 경우 화력을 사용한 공격못지 않은 결과를 초래할 것으로 생각된다. 따라서 전술 MANET의 시큐리티 문제에 대한 관심과 연구가 더욱 필요할 것이다.

참고문헌

[1] 김영동, "블랙홀 공격이 있는 MANET에서 VoIP 트래픽의 전송성능", 한국해양정보통신학회, 종합학술대회 논문집, 15권 2호, 2011.10.

[2] H.Tang, M.Salmanian, C.Chang, "Strong Authentication for Tactical Mobile Ad Hoc Networks", Technical Report, Defence R&D Canada – Ottawa, 2007.

[3] 박철순, "스마트 모바일 시큐리티 정책방향", TTA Journal, Vol. 133, 2011.

[4] K.Sharma, N.Khandelwal. Prabhakar.M, "An Overview of Security Problems in MANET", http://psrcentre.org/images/extraimages/155.pdf

[5] Z.Ishart, "Security issues, challenges & solutions in MANET", IJCST Vol. 2, Issue 4, 2011.

[6] H.Yang, H.Luo, F.Ye, S.Lu, L.Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, Vol. 11, Issue 1, 2004.

[7] 한국정보통신기술협회, "USN 위협 및 공격 시나리오 분석", 정보통신기술보고서, TTAR-06. XXXX, 2009.

[8] W.Webb, "Wireless Communications The Future", John Wiley and Sons, 2007.

저자소개

김영동 (Young-Dong Kim)

1984년 2월 광운대학교 전자통신공학과 (공학사)

1986년 2월 광운대학교 대학원 전자통신공학과 (공학석사)

1990년 8월 광운대학교 대학원 전자통신공학과 (공학박사)

1989년 3월 ~ 1995월 2월 대덕대학교 정보통신공학과

1995년 3월 ~ 현재 동양대학교 정보통신공학과

2003년 3월 ~ 2004년 2월 UCSC(UC Santa Cruz) Visiting Research Associate

※관심분야 : MANET, VoIP, Simulation, Security, Protocol