MANET에서 침입탐지 방법의 현황 및 선택 지침

오 선 진*　　배 인 한**

◈ 목 차 ◈

1. 서 론

차세대 무선망은 인프라구조 무선망과 인프라구조가 없는 모바일 애드 혹 망(MANET)을 포함할 것이다. MANET은 조만간 이동 상거래를 포함한 광역 이동 멀티 홉 무선과 개인 영역 망 등 모두에서 중요한 응용들을 가질 것이다.

이동 상거래는 정보, 서비스 또는 상품의 교환에 가치 전달의 결과로 무선 단말기나 데이터 연결을 사용한다[1, 24]. 이동 상거래는 거대한 주요 시장을 갖는다. 산업 연구가 GartnerGroup은 2005년까지 이동 채널에서 행해지는 전자 상거래의 규모가 1.8 백만조 달러에 이를 것이라고 예측하였다[4, 13].

MANET은 만약 이동 상거래를 위해 기존의 네트워크 기술이 사용된다면 이동 상거래의 비즈니스 모델에 혁명을 가져올 것이다. 애드 혹 특징의 MANET은 모바일 폰 망, 한 가지 종류의 인프라구조 무선망 그리고 주요 기존의 망 기술을 사용하는 현재의 이동 상거래와는 판이한 새로운 이동 상거래 모델을 만든다.

이동 상거래의 폭넓은 응용에 한 가지 중요한 도전은 보안이다[24]. 이동 상거래는 보안 문제가 완전히 해결될 때까지는 당분간 니치(niche) 시장에 머무를 것이다[5]. MANET에 대한 보안은 이동 상거래에서의 MANET 응용들에 매우 중요하다. MANET을 위한 모든 보안 척도들 중에서 침입탐지가 MANET이 유선망보다 보안에 대한 침입탐지가 더욱 의존적이기 때문에 중요한 문제이다.

Mishira[14]와 Brutch[2]는 MANET을 위한 두 가지 침입탐지 조사를 하였다. 두 조사 모두 MANET의 IDS에 대한 연구의 현재 상태에 대한 논의에 초점이 있고, 그리고 현재 논문들에서 제안된 IDS들을 분석하고 비교하였다.

본 연구는 우선 MANET에서 IDS에 대한 비교 연구를 위한 프레임워크를 제안하고 제안된 IDS를 통신과 의사결정 메커니즘과 같은 서로 다른 컴포넌트와 모듈들로 나누어 분석하는 것이다. 더욱이, MANET을 위한 IDS를 개발에서 다른 침입 탐지 방법 선택하는 다수의 지침 역시 첫 번째 시도이다. 이들 지침들은 목적 네트워크의 요구사항이나 자원에 기반 한다.

본 논문은 인프라 구조 없는 MANET에 초점을 맞추었으며 다음과 같이 구성되었다. 2장에서는 MANET을 위한 현존하는 침입탐지시스템(IDS)을 특징과 보안 문제 그리고 요구사항 등에 기초한 개요를 소개한다. 3장에서는 비교연구 프레임워크를 개발하여 MANET에서의 IDS를 입력, 출력, 프로세스 방법, 장점과 단점에 기초하여 비교연구를 보여준다. 4장에서는 MANET을 위한 침입탐지 방법을 선택하는 지침을 개발한다. 그리고 5장에서 결론을 맺는다.

* 세명대학교 정보통신학부 교수
** 대구가톨릭대학교 컴퓨터정보통신공학부 교수

2. 관련연구

2.1 MANET

MANET은 무선으로 연결된 수많은 무선과 이동 장치 노드로 구성된 IP 기반 망이다. 운영에서 이들 노드들은 어떠한 미리 정의된 인프라구조나 중앙 집중 관리에 영향을 받지 않는다. 이러한 망은 학술대회나 교실 또는 전장 등에서 사용될 수 있다. MANET에서 무선 범위 내의 노드들은 무선 링크를 통해 직접 서로 통신할 수 있지만 무선 범위를 벗어난 노드들은 그들의 메시지를 전달하기 위해 중간 노드를 필요로 한다. 각 노드는 호스트 뿐 아니라 라우터로도 실행할 수 있다.

MANET의 특징은 다음과 같이 정의될 수 있다[1, 18, 19].

- 자동 터미널(Autonomous terminal): MANET의 각 노드는 자동으로 라우터나 호스트 일 수 있다.
- 분산(Distributed): MANET은 라우팅, 호스트 설정 그리고 보안과 같은 작동이나 기능들이 분산된다. 예를 들어, 유선망과는 달리 MANET은 중앙집중식 방화벽을 가질 수 없다[1].
- 다중 홉 라우팅(Multi-hop routing): 메시지의 소스와 목적지가 한 노드의 무선 범위 밖이라면 다중 홉 라우팅이 필요하다.
- 동적 망 위상(Dynamic network topology): 노드들은 이동하며 언제나 망에 합류하거나 이탈할 수 있다. 따라서 위상은 동적이다.
- 링크 대역 변동(Fluctuating link bandwidth): 무선 링크의 안정성, 용량 그리고 신뢰성은 항상 유선 링크보다 더 떨어진다.
- 얇은 터미널(Thin terminal): 모바일 노드들은 종종 경량으로 덜 강력한 CPU와 메모리 그리고 전원을 갖는다.
- 동시성과 이동성(Spontaneous & mobile): 망의 환경설정에 최소의 방해가 요구된다. 라우팅 프로토콜은 망에서 사용자들이 통신하는데 적합해야 한다. 그리고 보안 역시 지원해야 한다.

암호화와 같은 유선망을 위한 현존하는 보안기술들은 MANET에서 사용될 수 있다. 그러나 MANET의 이동성과 애드 혹 특징 때문에 MANET 응용은 제한적이다. 방화벽과 같은 다른 기술은 중앙 집중화된 권한 부족으로 인해 MANET에 적용할 수 없다.

유선망과 마찬가지로 MANET은 도청(passive eavesdropping), 위장(spoofing) 그리고 서비스의 거부와 같은 보안 위협에 직면한다. 동시에 그의 애드 혹 특징 때문에 더욱 보안 위협을 겪는다. MANET에 대한 위협을 두 집단으로 분류할 수 있다.

- 애드 혹 특징으로 가중된 취약성: MANET의 위상은 주로 노드의 지리적 위치와 무선 범위에 의해 결정된다. 따라서 그것은 분명한 물리적 경계를 가지지 않는다. 유선망에서 중앙집중식 방화벽은 접근제어를 구현할 수 있다. 그러나 MANET에서는 접근제어가 중앙집중식 방화벽으로는 이루어 질 수 없다[1]. 서비스의 거부(DOS)와 같은 다른 공격은 여전히 MANET을 위협하며 유선망 보다 더욱 취약한데 그 이유는 MANET의 라우팅과 자동 환경설정 프레임워크가 그와 같은 공격에 더욱 취약하기 때문이다.
- 애드 혹 특징에 따른 취약성: MANET의 라우팅과 자동 환경설정 메커니즘은 더욱 공격할 기회를 부여하는데 그 이유는 이 두 메커니즘 모두에서 모든 노드들이 서로 모든 권한을 갖기 때문이다[1].

무선망에서 라우팅과 같은 다수 주요 프로토콜에서의 의사 결정은 상호 협력적이다. 공격은 알고리즘의 협력적인 특징을 이용할 수 있게 설계될 수 있으며, 시스템의 고장을 야기한다. 예를 들어, 무선망에서 MAC 계층 프로토콜은 고정 망에서의 그것보다 더욱 취약하다. 노드들은 누가 전송을 위한 통신 채널을 가지고 있으며 미리 정의된 프로토콜에 따라 어떻게 채널을 양도하는지를 결정하기 위해 서로 협력한다. 만약 한 노드가 침해하고 악의적으로 행동한다면 프로토콜은 작동하지 않게 되고 네트워크가 단절되어 서비스 거부를 초래한다. 유선망에서는 MAC 계층이 방화벽이나 게이트웨이와 같은 외부의 3 계층 장비들로

부터 고립되어 있기 때문에 이와 같은 일은 좀처럼 일어나지 않는다[26].

자동 환경설정 역시 취약성을 보여준다. 환경설정 메커니즘은 IP 주소를 계산하고 이 IP 주소가 이미 사용되고 있는지를 결정하기 위해 노드에 의해 주어진 정보를 사용한다. 그래서 악의적 노드는 진입노드의 IP 주소를 사용하는 척 할 수 있다. 이것이 진입노드가 망에 결합하는 것을 막는다.

MANET 노드는 항상 배터리 전원을 사용한다. 공격자는 패킷들을 강제로 전달하게 함으로써 노드가 자신의 전원을 소진하도록 할 수 있다. 이를 "수면 박탈 고문(sleep deprivation torture)"라 부른다[1].

무선망에서 외부 엔티티가 망에 연결하려고 할 때 물리적 연결이나 방화벽이나 게이트웨이와 같은 어떤 보안 방어선을 통과할 필요가 없기 때문에 무선망의 특징 그 자체가 공격에 더욱 취약하다. 공격은 어떤 장소에서든 올 수 있고 무선망 내부의 어떤 노드도 목표가 될 수 있다. 다시 말해 무선망에서는 방어선이 매우 모호하고 각 노드들이 침해될 위험에 노출되어 있다[26].

무선망은 노드들이 자율적이며 독립적인 단위로 이동을 허용한다. 따라서 노드들은 휴대장치 분실과 같은 물리적 보호의 부족으로 인해 도난이 일어나기 매우 쉬울 것이다. 대규모 망에서의 이동 노드들의 추적은 매우 어렵다. 따라서 공격은 더욱 타격을 주고 감지가 어려운 침해된 노드로부터 시작된다.

침입예방 기술의 사용은 그 효과 면에서 더욱 제한적이다. 예를 들어, 우리는 방어를 구현하기 위해 암호화나 사용자 인증을 사용할 수 있다. 그러나 유선망에서는 거의 일어나지 않지만 무선망에서는 휴대장치와 같은 어떤 노드들은 분실되거나 침해될 소지가 충분하다. 그리고 그런 노드들은 자신의 개인키를 가지고 있고 이것은 암호화 방어를 무력화 할 것이다.

MANET의 보안 목표는 가용성, 무결성, 인증, 기밀성, 부인방지(non-repudiation)를 포함한다. 가용성은 MANET이 서비스 거절 공격으로부터 생존할 수 있어야 함을 의미한다. 서비스 거절은 MANET의 어떤 계층에서도 발생할 수 있다. 예를 들어, 공격자는 망의 정지를 야기시키기 위해 네트워크 계층의 라우팅 프로토콜을 왜곡시킬 수 있다. 기밀성은 비밀정보를 비인증 사용자로부터 보호하는 능력을 의미한다. 무결성은 메시지가 전달 도중 오염되지 않아야 됨을 의미한다. 오염은 망 실패나 공격에 의해 초래된다. 인증은 노드가 피어 노드의 진짜 정체를 확인할 수 있어야 한다. 인증이 없으면 공격은 노드로 가장할 수 있으며 망에 비인증 접근을 획득할 수 있다. 그리고 부인방지는 메시지 송신노드가 메시지의 송신을 거절할 수 없음을 의미한다. 이것은 침해된 노드를 탐지하고 고립시키는데 유용하다[18].

이러한 취약성을 극복하고 보안 목표를 달성하기 위해 MANET은 다음의 보안 척도가 필요하다.

- 라우팅 메커니즘 보호(Protecting routing mechanism): 본 논문에서 MANET의 라우팅은 공격이 수월함을 보였다. 가능한 해결책은 암호화 방안을 사용하거나 보안 라우팅 프로토콜을 개발하는 것이다.
- 키 관리 방안 보호(Protecting key management scheme): MANET에서 키 분배 보안은 어렵다. 가능한 해결책은 비대칭 키 암호화에 기초한 방안이다.
- 침입탐지(Intrusion detection): 이것이 본 논문의 초점이며 뒤에서 자세히 설명할 것이다[18].

2.2 MANET에서 IDS

침입탐지 시스템은 컴퓨터 시스템에 대한 경고 메커니즘으로 서비스한다. 시스템은 컴퓨터 시스템에 발생할 보안 요소를 감지하고 사이트 보안 담당자에게 경고 메시지를 발생시켜 침입에 대한 어떤 조치를 취하도록 한다[20].

IDS는 시스템 내의 작동들을 추적하는 감시자료 수집 에이전트와 감시 자료를 분석하고 사이트 보안 담당자에게 출력 보고서를 발행하는 탐지기 등을 포함한다[20].

MANET에서 IDS를 설명하는데 침입탐지기술과 침입탐지구조의 두 가지 개념을 구분할 필요가 있다. 침입탐지기술은 이상 현상(anomaly)이나 오용 탐지(misuse detection)와 같은 개념을 말한다. 이들은 주로 얼마나 IDS가 어떤 알고리즘을 사용하여 주어진 감시 자료를

입력으로 어떻게 침입을 탐지하는가 하는 문제를 해결한다. 이것은 알고리즘처럼 보여 질 수 있다. 그러나 침입탐지 구조는 보다 큰 범위에서 문제를 다룬다.

침입탐지구조는 어떤 침입탐지기술을 모듈로 사용할 필요가 있다. 그러나 이것은 역시 망 내의 노드들이 침입탐지 의사결정에 어떻게 협력할 수 있는지에 대한 모듈과 같은 많은 다른 모듈들을 포함한다. 유선망에서는 노드가 항상 지역적으로 수집된 자료에 기반 한 침입탐지 결정을 할 수 있다. 따라서 침입탐지 기술은 그것이 노드에 배치되면 침입탐지에 대한 요구를 충족시킬 수 있다. 그러나 무선망에서는 지역적으로 수집된 자료에만 기반 한 노드의 침입탐지 결정은 매우 어렵다. 노드들은 침입탐지 결정을 위해선 적어도 협력하거나 자료를 교환해야만 한다. 따라서 무선 IDS에서는 서로 다른 노드의 역할을 정의하고 그들이 통신하는 방법을 정의하는 구조가 매우 중요하다.

침입탐지 기술은 기본적으로 구조나 환경에 독립적이다. 다시 말해, 이상 현상이나 오용탐지는 유선망에서 그것들이 사용되는 것처럼 무선 환경에서도 사용될 수 있다. 다만 구현에서의 차이점은 주로 알고리즘에 입력으로 무슨 감시 자료를 사용하느냐 하는 것이다. 그러나 MANET에서의 대부분의 IDS는 MANET의 특징 때문에 이상 현상 탐지를 사용한다.

MANET에서의 IDS에 대한 대부분의 논문들은 저자가 서로 다른 탐지 기술보다는 MANET에서의 IDS의 서로 다른 구조에 초점에 맞춰 재검토하고 있다. 많은 논문들은 사용된 탐지 기술을 자세히 언급하지 않는다. 어떤 것들은 심지어 이상 현상과 오용 탐지 기술 모두를 사용할 수 있다고 하기도 한다. 따라서 본 논문에서는 구조들이 사용하는 탐지 기술 보다는 IDS의 서로 다른 구조에 초점을 맞추고자 한다.

이 장에서는 우선 MANET에서의 공격을 설명하고 나서 MANET에서의 IDS의 보안 작업을 설명한다. 그리고 나서 MANET에서의 IDS의 요구사항을 알아보고 마지막으로 MANET에서의 IDS의 가능한 구조를 분석하였다.

2.2.1 MANET에서 공격

MANET에서의 공격은 결과와 기술에 따라 분류할 수 있다[8]. 중요성에 기초하여 공격은 다음과 같이 분류되어 진다.

- 블랙 홀(Black hole) : 모든 패킷들이 그들을 전혀 전달하지 않는 특수 노드로 라우트 된다.
- 라우팅 루프(Routing loops) : 라우팅 경로에 루프를 초래한다.
- 망 분할(Network partition) : 망은 노드들이 비록 그들 사이에 경로가 존재하더라도 서로 통신할 수 없는 서브 망들로 분리된다.
- 이기주의(Selfishness) : 노드가 다음 노드들을 위한 라우터로 서비스 하지 않는다.
- 수면 박탈(Sleep deprivation) : 노드는 자신의 배터리를 계속 사용하도록 강요된다.
- 서비스 거부(Denial of service) : 노드가 패킷 송신이나 수신이 금지된다[8, 27].

공격의 기술에 기초하여 그들을 다음과 같이 분류한다.

- 캐싱 중독(Cache poisoning) : 라우팅 테이블 내의 정보가 수정, 삭제되거나 또는 거짓 정보를 포함한다.
- 위조된 라우트 메시지(Fabricated route message) : 악의적 정보를 가진 라우트 요청이나 회신과 같은 라우트 메시지들이 망에 삽입된다. 그들은 다음과 같이 실행될 수 있다.
  (a) 거짓 소스 라우트(False source route) : 목적지가 어디던가 상관없이 라우트 비용을 1로 설정하는 것과 같은 거짓 라우트가 망 내에 방송된다.
  (b) 최대 순서(Maximum sequence) : 제어 메시지 내의 순서 필드를 최대값으로 수정한다.
- 러싱(Rushing) : MANET의 다수의 라우팅 프로토콜에서 단지 처음 도착한 메시지만이 수신자에 의해 받아진다. 공격자는 거짓 제어 메시지를 분배하여 뒤에 도착하는 정당한 메시지를 차단할 수 있다.
- 웜홀(Wormhole) : 두 노드 사이에 비밀로 패킷을 전송할 수 있는 경로가 생성된다.
- 패킷 폐기(Packet dropping) : 노드가 라우트 될 예정인 패킷을 폐기 시킨다.
- 위장(Spoofing) : 패킷이나 제어 메시지에 거짓

또는 변경된 소스 주소를 삽입한다.

- 악의의 플로딩(Malicious flooding) : 통상적이지 않게 많은 양의 패킷을 어떤 목적 노드들에 전송한다[8].

2.2.2 MANET에서 IDS의 보안 작업

Brutch와 Ko[2]는 MANET에서 IDS의 두 가지 보안 작업을 제안하였다.

라우팅 프로토콜에 대한 공격 탐지 : MANET에서 공격자는 내부의 노드들이 틀린 라우팅 정보를 전달하는 동안 네트워크 단절이나 과부하를 초래하기 위하여 라우팅 정보를 주입, 재생, 왜곡 할 수 있다[11, 12, 21, 22].

모바일 노드에 대한 공격 탐지 : 이것은 유선망에서와 같다. 우리는 개개의 워크스테이션을 보호할 필요가 있다.

2.2.3 MANET에서 IDS를 위한 요구사항

IDS 측면에서 유선과 무선망의 차이점은 다음과 같다.

- MANET을 위한 IDS는 지역적이고 부분적인 감시 자료로 작동해야 한다. MANET은 완전하고 전역 감시 자료를 수집하기 위해 유선망에서 사용되는 방화벽이나 게이트웨이와 같은 고정된 인프라구조를 가지고 있지 않기 때문에 MANET에서의 감시 자료는 항상 지역적이고 부분적이다[26].
- 네트워크 기반 IDS는 무선망을 위해 작동하지 않는다.
- MANET에서의 IDS는 정상과 침입 트래픽을 구분하기가 무척 어렵다. 무선망에서는 종종 정상과 비정상 행위의 분명한 구분이 없다. 무선망에서는 연결이 안정적이지 않고 이동 노드들은 언제나 망에 가입과 이탈이 이루어 질 수 있다. 예를 들어, 일시적으로 동기화에서 벗어난 노드는 공격 행위로 간주되는 패킷을 송신할 수 있다[26].
- IDS는 최소 자원을 사용해야 한다. 무선망은 안정적 연결을 가지지 않으며 대역폭과 전원과 같은 망의 물리적 자원이나 장비들은 제한적이다. 연결의 단절은 언제나 일어날 수 있다[26]. 더욱이 IDS 목적을 위해 노드 사이의 통신은 너무 많은 대역폭 자원을 차지해서는 안 된다.
- 통신에서 암호화는 활성화하기 힘들다. 서로 다른 노드 상의 IDS 사이의 통신은 그 통신에 접근하는 공격을 허용하지 않도록 안전해야 한다. 그러나 MANET에서의 암호화는 그 자체가 어려운 작업이다. 유선망에서는 접근을 위한 물리적 연결의 요구사항 때문에 이 문제가 덜 분명하다.
- IDS는 어떤 노드도 안전하다고 가정할 수 없다. 유선망에서와는 달리 MANET 노드들은 아마 침해될 것으로 보인다. 따라서 협력적 알고리즘에서 IDS는 어떠한 노드도 완전히 신뢰할 수 있다고 가정해서는 안 된다.
- IDS는 높은 거짓 경고 율 문제를 짚고 넘어가야만 한다. MANET의 대역폭이 유선망과 비교해서 상당히 제한적이기 때문에 침입탐지 결정을 위한 충분한 감시 자료의 확보가 어렵다. 결과적으로 MANET에서의 IDS는 너무 많은 거짓 경고나 많은 공격 분실의 결과를 쉽게 가져올 것이다[10].

여기에 언급해야만 할 3 가지 개발 문제가 있다.

- 무선망의 이동성과 애드 혹 특징에 잘 맞는 적당한 IDS의 구조를 찾아라.
- 이상 현상 탐지에서 무선망 내의 감시 자료 소스를 효율적으로 사용할 방법을 찾아라. 위에서 언급했듯이 무선망에서의 감시 자료는 종종 부분적이고 지역적이다.
- 정상 트래픽으로부터 공격 트래픽을 효율적으로 구분할 수 있는 방법을 찾아라. 특히 빈약한 연결성으로 인해 비정상처럼 보이것은 정상 트래픽을 식별할 수 있는 방법을 찾아라. 그렇지 않으면 IDS는 높은 거짓 경고 율을 가질 것이다[26].

Levente(2002)는 MANET을 위한 IDS의 요구사항을 다음과 같이 식별하였다.

- 완전히 분산시켜라. 이것은 IDS가 각 노드에서 침입을 탐지해야 하고 노드들은 경고를 할 것인지에 대한 결정에 협력할 수 있다.
- 지역적이고 부분적인 감시 자료를 다루기 위해서 IDS는 이상 현상이 발생한 것을 다른 홉에서 감지할 필요가 있다.
- 정상/비정상 사이에서 분명한 구분을 할 수 없는 문제를 다루기 위해서 IDS는 높은 탐지율과 낮은 거짓 경고를 획득할 필요가 있다.
- 무선망상의 주어진 자원 제약으로 IDS는 전원을 포함한 너무 많은 자원을 소비해서는 안 된다. 따라서 IDS는 런타임 효율성을 가져야 한다.

2.2.4 MANET에서 IDS를 위한 구조와 탐지 의사 결정 모델

MANET에서 현존하는 IDS의 가능한 구조는 독립 IDS, 분산 그리고 협력적 IDS 그리고 계층적 IDS를 포함한다.

- 독립형(Stand-alone) IDS : 이 구조에서는 각 호스트가 IDS를 가지고 독립적으로 공격을 탐지한다. 노드들 사이에서의 협력은 없고 모든 결정은 지역노드들에 의한다. 이 구조는 충분히 효율적이지는 않지만 모든 노드에서 IDS를 실행시킬 능력이 없는 환경에서 사용될 수 있다[2].
- 분산 및 협력(Distributed & Cooperative) IDS : 이 구조에서는 각 노드가 IDS 에이전트를 가지며 지역 탐지 결정을 한다. 동시에 모든 노드들이 전역 탐지 결정에 참여한다. 이것은 플랫 MANET에 적합하다[2].
- 계층적(Hierarchical) IDS : 이 구조는 다중 계층 MANET을 위해 설계되었다. 다중 계층 MANET에서는 클러스터 헤드(CH) 노드가 클러스터 내의 모든 노드들에 대한 중앙집중식 라우팅을 하며 IDS를 포함한 보안 측정을 지원할 수 있다. 더욱이, CH 노드는 또한 Byzantine CH 노드에 의해 만들어진 가상 백본 라우팅 프로토콜에 대한 공격을 탐지할 수 있는데 이것은 MANET에서 매우 중요하다[2].

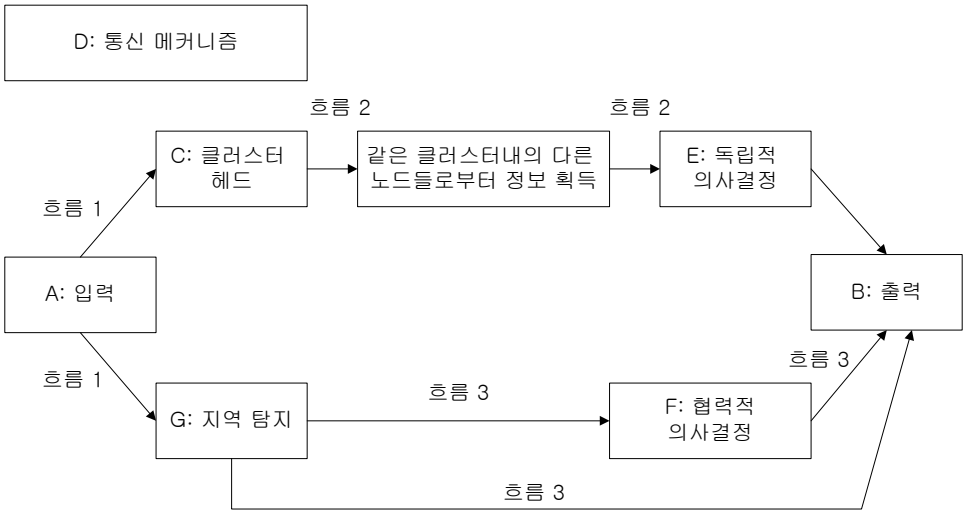
MANET에서 현존하는 두 가지의 침입탐지에 대한 의사결정 방법으로 협력적 의사결정과 독립적 의사결정을 포함한다.

- 협력적 의사결정(Collaborative decision making) : 각 노드는 침입탐지 프로세스에 활동적으로 참여한다. 일단 한 노드가 충분히 높은 신뢰도로 침입을 탐지하면 이 노드는 침입에 대한 대응을 시작할 수 있다. 이 설계의 간단한 구현에서 공격이 발생했는지를 결정하기 위해 다수결 방법(majority voting scheme)이 사용된다[25]. 이 설계는 또한 퍼지논리와 같은 좀 더 복잡한 의사결정 방안을 사용할 수 있다. 이 설계는 보안적인 측면에서 약간의 취약점이 있다. 이것은 서비스 거부나 위장 침입과 같은 공격을 쉽게 받을 수 있다. 위장 침입에서는 악의적 노드가 초강력 침입 대응을 유발하고 전체 망에 영향을 준다[9].
- 독립적 의사결정(Independent decision making) : 이 프레임워크에서는 어떤 노드들이 침입탐지를 위해 할당되었다. 이들 노드들은 다른 노드들로부터 침입 경고를 수집하고 망 내의 어떤 노드가 공격을 받았는지를 결정한다. 이들 노드들은 의사 결정에 다른 노드들의 참여를 필요로 하지 않는다. 이 설계 역시 취약점이 있다. 좋은 결정을 하기 위해서 의사 결정 노드는 다른 노드들로부터 많은 량의 자료를 수집해야만 한다. 그러나 그러한 수집은 망 자원이 특히 제한된 MANET에서는 매우 비용이 많이 든다[9].

3. MANET에서 IDS에 대한 비교 연구

3.1 비교 연구에 대한 프레임워크

그림 1은 MANET에서 침입탐지에 대한 비교연구를 위한 프레임워크를 보여준다. 그림 1에서와 같이 3개의 흐름과 7개의 컴포넌트로 구성된다. 이들 흐름과 컴포넌트에 대한 자세한 설명은 다음과 같다.



(그림 1) MANET에서 침입 탐지에 대한 비교 연구의 프레임워크

입력(Input): 자료는 IDS에 의해 수집된다. 이것은 주로 시스템 감시 자료, 네트워크 패킷 또는 라우팅 테이블 내에서의 갱신 통계와 같은 자료의 통계를 포함한다.

클러스터 노드(Cluster node): 어떤 알고리즘이 네트워크상에서 수행되어 망이 수개의 클러스터로 분리된다. 어떤 클러스터는 클러스터 헤드 노드를 일반적으로 갖는다. 망 분리와 클러스터 헤드 선택은 동적으로 이루어진다.

지역 탐지(Local detect): 단일 노드 상의 IDS 모듈이나 에이전트는 지역 노드에 침입이 발생했는지를 결정하기 위해 침입탐지 알고리즘을 구동한다.

다른 노드들로부터 정보 획득(Get information from other nodes): 이것은 일반적으로 클러스터 노드 상에서 발생한다. MANET의 분산과 애드 혹 특징 때문에 단일 노드 상의 지역 정보만으로는 종종 탐지 의사결정을 하는데 불충분하다. 따라서 IDS는 보다 정확한 탐지를 위해서 자신이 거주하는 노드가 아닌 다른 노드들로부터 정보를 수집할 필요가 있다.

독립적 탐지 의사결정(Independent detection decision making): 클러스터 헤드 상의 IDS는 필요로 하는 모든 정보를 가지고 침입결정을 한다.

협력적 탐지 의사결정(Collaborative detection decision making): 다수의 노드들이 침입 결정을 위해 투표를 하는 것과 같이 협력적 의사결정 프로세스에 참여한다. 통상적으로 투표를 하기 전에 각 참여 노드들은 이미 초기 결정을 한다. 그것들은 보다 정확한 그룹결정을 위해 초기 결정을 취합할 필요가 있다.

흐름 1: 첫 번째 입력은 IDS를 위해 수집된다. 그 다음 어떤 IDS는 망의 노드들을 클러스터나 지역(zone)으로 묶기도 하고 그룹으로 묶지 않기도 한다.

흐름 2: 클러스터 내의 IDS에서는 클러스터의 멤버 노드들은 항상 클러스터 헤드에 지역 보안 정보를 전달한다. 그 다음 클러스터 헤드는 수집된 정보에 기초하여 독립적으로 침입결정을 한다.

흐름 3: 클러스터가 없는 IDS에서는 두 가지의 탐지 의사결정 방법이 있다. 그 하나는 한 노드상의 IDS 모듈이 직접 결정을 하고 침입 경고를 발생시키는 것

이다. 그러나 지역 정보가 종종 침입 결정을 하기에 불충분하기 때문에 이 방법은 MANET에서는 거의 사용되지 않는다. 다른 방법으로는 협력적 의사결정을 하는 것이다.

표 1은 MANET을 위한 현존하는 침입탐지 방법들을 입력, 처리 방법, 출력, 그리고 장단점에 기초하여 자세히 비교 연구한 결과를 보여준다. 여기서 문자 A에서부터 G까지는 그림 1의 문자들과 관련된 것이다.

표 1에서는 현존하는 침입탐지 방법들을 보여준다. 방법 1은 효율적이며 대역폭 자각형(bandwidth-conscious)이다. 이것은 다중계층에서 침입을 목표로 하였고 MANET에 대한 IDS의 분산 특성에 잘 맞는다. 이 방법은 클러스터를 가지며 클러스터 헤드 상의 IDS는 다른 노드들로부터 정보를 수집한 후 독립적 의사결정 방법을 채택한다. 이것은 이동 에이전트를 노드들 사이의 통신을 위해 사용한다.

방법 2는 이상 현상 탐지에 지역과 협력적 의사결정을 구현한다. 이 접근 방법에서 개개의 IDS 에이전트는 독자적으로 작동하며 의사 결정하는데 협력한다. 각 IDS 에이전트는 노드 상에서 작동하며 지역 활동을 감시한다. 만약 노드가 강한 증거를 가지고 지역적으로 침입을 탐지하면 노드는 침입 발생을 결론지을 수 있으며 경고 대응을 시작한다. 그러나 증거가 충분히 강하지 않아 망 내의 보다 넓은 지역에서 조사가 필요하다면 IDS 에이전트는 분산 합의 알고리즘인 협력 프로시저를 시작할 수 있다[26].

방법 3에서 저자들은 클러스터 헤드가 이웃(시민 노드)에 있는 노드들의 그룹에 의해 선출되고 헤드 노드는 시민 노드들을 감시하는 클러스터 기반 방법을 제안하였다. 일단 클러스터 헤드가 선출되면 다른 노드들은 그들이 지역적으로 획득한 특징들을 클러스터 헤드에 전달할 필요가 있다. 이 IDS는 데이터 마이닝으로 구현된 이상 현상 탐지를 탐지 기술로 사용한다[11].

방법 4에서 각 노드는 지역 IDS를 구동한다. 각 노드는 침입을 지역적으로 탐지하고 탐지를 확인하기 위해 외부 자료를 사용한다. 노드들은 이동 에이전트를 통신과 협력을 위해 사용한다.

(표 1) 침입 탐지 방법에 대한 비교 연구

번호	방법	참고 논문	A: 입력	B: 출력	방법론									장점	단점
					C: 그룹핑 노드		D: 통신 메커니즘		의사 결정		G: 지역 탐지				
					클러스터 헤드	지역 헤드	모바일 에이전트	네트워크 메시지	E: 독립적	F: 협력적	비정상 행위	오용	명세		
1	모바일 에이전트 기반 IDS	[9]	네트워크 패킷, 시스템 또는 프로그램 수준 감시 자료	침입 경고와 대응	예		예		예		예			대부분 노드들을 위해 자원을 유지하고, 확장 가능하고 유연하다.	모바일 에이전트의 보안을 구현하는 것이 어렵다.
2	지역 협력적 의사결정 IDS	[26]	라우팅 테이블에서 갱신과 같은 지역 노드상에서 감시 자료 수집	침입 경고와 대응				예		예	예			지역 감시 자료를 분산 협력적으로 처리. 다른 입력 자료를 수용 가능.	Byzantine 노드가 공격에 취약. 의사결정이 다수결이다. 구현 및 검증되지 않았음.
3	협력적 IDS 프레임워크에서 클러스터 헤드	[8]	송수신된 다수의 패킷과 다수의 라우트 제어 메시지에 대한 통계	침입 탐지와 경고	예			예	예		예			CPU 사용과 망 오버헤드에서 IDS의 효율성 향상, 공격 종류 식별.	침해된 노드가 클러스터 헤드로 선출되는 것을 방지해야 한다.
4	시스템에 대한 지역 침입 탐지	[1]	관리 정보 DB에서 감시 자료	침입 경고			예		예					적은 망 트래픽, 확장성.	모바일 에이전트 생성과 관리에서 복잡성.
5	존 기반 IDS	[22]	라우팅 테이블에서 자료의 통계	식별된 침입 종류와 위치로 침입 경고		예		예		예	예			거짓 경고 감소, 탐지 향상, 다수의 침입 기법을 포함.	복잡한 구조는 조정을 위하여 많은 프로토콜이 필요하고, 존 설립을 위한 계산이 복잡하다.
6	패킷-단계 침입 탐지를 위한 사례-기반 에이전트	[6]	패킷 정보: 망 주소, 포트 등	침입 경고	예		예			예		예		효율적, 대역폭-의식 MMANET의 분산 속성을 고려하였다.	모바일 에이전트의 보안은 구현이 어렵고, 패킷 부하가 증가할 때 패킷 폐기율이 증가하고, 개선이 요구된다.
7	교차-특징 분석	[7]	패킷 폐기와 라우팅 테이블 변경간의 관계와 같은 패킷 통계	침입 경고							예			비정상 행위 모델 자동 구축	높은 계산 비용
8	명세 기반	[23]		라우팅 프로토콜에서 요청-응답 흐름				예					예	낮은 오버헤드	단지 하나의 라우팅 프로토콜을 위해 설계, ID 작업을 위하여 프로토콜 수정이 필요하다.
9	이웃 감시	[17]		하나의 노드와 다수의 노드 단계 에서 침입 경고,, 경고 결정을 위하여 투표가 사용되어진다,	예			예		예				이상적이고 진부하지 않은 지역 탐지 메커니즘	패킷이 각 홉에서 검사되므로 낮은 효율성
10	모듈라 구조	[16]	관리 정보 베이스(MIB)	침입 경고			예			예				원시 데이터는 통과되고 고급 메시지만 전달되므로 망 사용이 분산되고 효율적이다. 확장성. 다수의 단계: 시스템, 망 그리고 응용 단계에서 공격을 탐지할 수 있다.	모바일 에이전트, 보안, 계산 비용 그리고 관리에 속하는 문제들

방법 5는 이상 현상 탐지에 협력적 메커니즘을 사용하는 IDS를 구현한다. 이 모델에서 망은 지역적 존(zone)으로 나누어진다. 각 존은 게이트웨이 노드와 개별적인 노드들을 가진다. 개개의 노드들은 작동 중인 IDS 에이전트를 갖고 침입활동을 개별적으로 탐지한다. 일단 개별적인 노드가 침입을 탐지하면 경고 메시지를 생성한다. 게이트웨이 노드는 그 존에서 노드들에 의해 생성된 경고들을 수집하고 서로 관련시킨다. 경고의 속성에서 유사성을 기초로 경고들을 수집하는데 알고리즘이 사용된다. 단지 게이트웨이 노드들만이 초기의 경보를 위하여 경고를 사용할 수 있다[21, 22].

방법 6은 역시 독립적 의사결정을 적용하는데 클러스터와 클러스터 헤드를 사용한다. 이 방법은 또한 이동 에이전트를 노드들 사이의 통신에 사용한다. 침입탐지 엔진은 인공지능 원리로 설계된 사례기반 에이전트 이다.

방법 7은 주로 폐기된 패킷 개수와 라우팅 테이블에서의 변화 백분율 사이에서의 상관관계와 같은 패킷 통계 즉, 서로 다른 특징들 간의 관계를 사용하는 탐지 알고리즘을 제안하였다. 이 알고리즘은 다른 IDS 구조에서 침입탐지 엔진으로 사용될 수 있다.

방법 8에서 망에서의 중요한 객체의 정상 행위는 우선 정상 명세로 구축된다. 그리고 나서 실제 행위는 정상 명세와 비교된다. 이 방법은 라우팅 프로토콜에서 요청-응답 흐름을 추적하기 위해 분산 망 감시를 사용한다. 망 감시는 의사결정을 위해 명세 기반 탐지 알고리즘을 구동한다[15, 18].

방법 9에서는 패킷이 망 내에서 운행하는 동안 수정되지 않았다는 것을 확신하기 위해 한 노드의 두 이웃 노드들이 사용된다. 이것은 각 홉에서의 각 패킷내의 정보를 비교함으로써 이루어진다. 이 방법은 두 가지 모드를 갖는데 수동(passive) 모드는 단일 호스트를 보호하기 위한 것이고, 능동(active) 모드는 클러스터내의 노드들을 협력적으로 보호하기 위한 것이다. 능동 모드에서 클러스터 헤드는 실제 침입이 발생했는지를 결정하기 위해 투표 알고리즘을 시작한다.

방법 10에서 관리정보 베이스(Management information base: MIB)내의 정보는 입력 자료로 사용된다. 이 방법 역시 이동 에이전트와 협력적 의사결정 메커니즘을 사용한다.

3.2 입력

대부분의 방법들이 라우팅 테이블 내의 갱신 횟수나 망 내의 요청-응답 흐름과 같은 패킷이나 망 트래픽 관련 정보를 취한다.

패킷관련 정보를 사용하는 것들 중에 방법 6과 9는 망 주소나 포트 번호와 같은 패킷 헤더 내의 정보를 직접 사용한다. 패킷이나 망 트래픽 관련 정보를 주로 사용하는 다른 방법들은 수신되고 송신된 패킷 개수의 통계나 라우팅 테이블 내의 변경 통계와 같은 패킷 정보로부터 통계적 자료 프로세스를 사용한다. 방법 7은 예를 들어 누락된 패킷 개수와 라우팅 테이블에서 갱신 백분율간의 상관관계와 같은 패킷이나 트래픽 관련 통계로부터 유도된 통계를 사용한다.

방법 1과 2는 IDS가 다른 형태의 감시 자료와 작동하거나 서로 다른 종류의 감시 자료에 적응할 가능성을 허용한다. 이 성질은 가치가 있고 미래 IDS 설계에 중요 고려사항이 될 것이다.

3.3 출력

대부분의 구조는 침입이 발생했다는 사실만을 탐지한다. 어떤 방법들은 공격의 형태나 침입자의 위치와 같은 추가 정보를 획득하기도 한다. 예를 들어, 존 기반 IDS는 공격의 형태와 위치 모두를 감지할 수 있다.

3.4 클러스터 노드

방법 1, 3, 6 과 9와 같은 방법들은 클러스터 헤드와 게이트웨이 노드를 사용한다. 클러스터 헤드의 목적은 침입탐지와 같이 어떤 자원 소비를 하는 계산은 단지 망의 다수의 노드들에서만 수행될 수 있다. 따라서 거의 대부분의 다른 노드들은 네트워크 트래픽의 실제 작업에 초점을 맞출 수 있다.

클러스터 헤드는 항상 탐지결정을 위해 클러스터 멤버로부터 정보를 수집한다. 어떤 방법에서는 원래의 입력 자료가 클러스터 헤드에 보내지기 전에 더 처리 되거나 포맷된다. 이렇게 함으로써 그 자료를 전송하기 위한 망 트래픽이 감소한다. 클러스터 헤드 상에서의 계산은 멤버 노드로부터 유입되는 자료들이 IDS 사용을 위해 이미 포맷되었기 때문에 역시 감소될 수 있다.

클러스터 헤드와 그 멤버노드들 사이의 보안 통신은 연구에서 주목을 받고 있다.

3.5 지역 침입 탐지

방법 8을 제외한 다른 방법들은 이상 현상 탐지를 이용한다. 이상 현상 탐지는 MANET에서 오용 탐지보다 더욱 적절하다.

MANET에서 이상 현상 탐지는 정상 행위의 프로파일이 주기적으로 갱신되어야 하는 취약점을 갖는다. 이것은 제한된 망 자원에 무거운 짐을 지운다. 방법 7은 이상 현상 모델을 자동적으로 구축할 수 있다. 이것은 이 취약점에 해결책을 제공한다.

방법 8은 명세 탐지를 사용한다. 이론상 명세 탐지는 새로운 공격 형태를 탐지할 수 있고 낮은 거짓 경고 율을 달성할 수 있다. 방법 6은 기본적으로 오용 탐지를 사용한다.

3.6 통신 메커니즘

모든 구조는 서로 다른 노드들에서 실행되는 IDS 사이에 어떤 형태로든 통신이 필요하다. 통신은 이동 에이전트에 의해 이루어진다.

방법 1, 4, 6 그리고 10은 이동 에이전트를 사용한다. 이동 에이전트를 사용하는 목적은 망 트래픽을 줄이고 망의 실제 작업을 위한 더 많은 자원을 절약하기 위한 것이다. 그러나 그러한 구조에서 이동 노드들은 이동 에이전트가 이동 노드 상에서 계산을 수행하는 것을 허용하고 이동 에이전트들은 또한 공격에 대해 문을 열어준다. 따라서 악의적 코드로부터 노드를 보호하는 보안 메커니즘이 매우 중요하다. 그리고 그러한 메커니즘은 이동 에이전트를 덜 강력하고 덜 효율적이도록 하고 이것이 이동 에이전트를 사용하는 중요한 고려사항 중의 하나이다. 또한 이동 에이전트의 생성, 이동, 작동 그리고 종료와 같은 이동 에이전트 관리는 역시 매우 도전적인 과제이다.

이동 에이전트를 사용하지 않는 구조에서는 자료를 교환하고 침입 의사결정에 협력하기 위해 네트워크 프로토콜에 의존해야 한다. 그러한 프로토콜은 안전하고 강건해야만 한다. 동시에 그러한 통신은 MANET에서 매우 제한적인 대역폭 자원의 많은 부분을 사용한다.

3.7 협력적 의사결정과 독립적 의사결정

방법 2, 5, 9, 10은 침입탐지에 협력적 의사결정을 사용한다. 다른 것들은 독립적 의사결정을 사용한다. 방법 9를 제외한 클러스터를 사용하는 대부분의 방법들은 협력적 의사결정을 사용하지 않는다.

협력적 의사결정을 사용하는 목적은 의사결정을 하는데 다른 노드들로부터 정보를 포함하고자 하는 것으로 보다 정확한 결정을 하기 위한 것이다.

협력적 의사결정은 보안측면에서 취약점을 갖는다. 이것은 서비스의 거부나 위장 침입과 같은 공격을 더욱 쉽게 받을 수 있다.

3.8 장 · 단점

방법 1은 여러 종류의 감시 자료로 작동하는 프레임워크를 제공한다. 이것은 확장 가능하여 만약 IDS가 새로운 종류의 감시 자료와 작동을 필요로 한다면 단지 새로운 종류의 감시 자료를 감시 할 수 있는 추가 에이전트를 통합하여 해결할 수 있다. 그러나 불행하게도 그 성능은 어떠한 구현에 의해서도 증명되지 않았다. 일단 그 성능이 받아들여 질 수 있는 수준으로 제공된다면 더 많은 기능을 추가할 수 있는 가능성이 성공적인 제품을 위한 중요한 성질이기 때문에 이 프레임워크는 상업용 제품을 위하여 일반적이고 확장 가능한 구조로 서비스 할 수 있다. 이 방법은 클러스터 헤드를 사용하기 때문에 단지 일부 노드에서 IDS 목적을 위한 자원 사용을 제한함으로써 MANET을 더욱 효

율적으로 만들 수 있다. 그러한 프레임워크는 보안 요구 사항이 중간정도이고 효율성 요구사항이 높은 환경에 적용될 수 있다. 또한 이 방법은 다중 계층 MANET을 위해 쉽게 확장될 수 있다.

방법 2는 MANET의 분산 속성에 적합한 프레임워크를 제공한다. 그리고 또한 여러 종류의 감시 자료와도 작동한다. 만약 IDS가 새로운 종류의 자료와 작동을 필요로 한다면 이것은 IDS 에이전트에 더 많은 자료 수집 모듈을 추가할 수 있다. 이 방법은 데이터 마이닝을 지역 침입탐지 메커니즘으로 사용한다. 데이터 마이닝은 탐지율과 거짓 경고율 모두에서 우수함을 보인다. 또한 IDS는 이동 에이전트를 통신을 위해 사용하지 않기 때문에 Byzantine 노드들로부터 보호할 수 있는 효율적인 방법을 찾는다면 높은 보안 요구를 위해 설계될 수 있다. 이 프레임워크는 플랫 MANET을 위해 설계되었다. 대규모 다중 계층 MANET에서는 MANET의 하부 지역에서 작동할 수 있다.

방법 3은 단지 소수의 노드에서 IDS 목적을 위해 자원 사용을 제한함으로써 MANET의 효율성을 개선한다. 구현은 이 방법이 역시 만족할만한 수준의 탐지율을 달성할 수 있음을 보였다. 그러한 프레임워크는 보안 요구사항이 중간정도인 반면 효율성 요구사항이 높은 환경에 적용할 수 있다. 또한 이 방법은 쉽게 다중 계층 MANET을 위해 확장될 수 있다[3].

방법 4는 이동 에이전트를 사용하여 확장형 구조를 제공한다. 만약 IDS가 더 많은 기능을 필요로 한다면 이것은 더 많은 이동 에이전트를 새로운 태스크에 통합할 수 있다. 이 방법은 침입탐지 목적을 위해 네트워크 트래픽을 감소시킨다. 그러나 이 구조는 과중한 이동 에이전트의 사용에 의존하므로 모든 에이전트의 생성과 관리하는데 계산 복잡도를 야기한다. 이 구조는 그 성능을 증명하기 위해 구현이 필요하다.

방법 5는 모의실험에서 상당히 탐지율을 개선하였고 거짓경고를 감소시켰다. 이것이 MANET에서 IDS의 주요 성능 지시자이다. 그러나 특히 CPU 시간이나 대역폭과 같은 자원을 이 방법은 얼마나 필요로 하는지와 같은 런-타임 효율성에 대한 자료가 없다. 존 설립이나 침입탐지 목적을 위해 노드들 사이의 통신 프로토콜 알고리즘이 매우 복잡하게 보이기 때문에 이 구조는 상당한 량의 자원을 필요로 할 것이라고 믿는 것이 합리적이다. 이 방법은 이동 에이전트를 사용하지 않으며 클러스터 헤드처럼 작동하는 게이트웨이 노드를 가진다. 이 구조는 IDS 성능과 보안에 대한 요구사항이 높고 MANET 자원이 일반적으로 유용한 환경에 적용될 수 있다.

방법 6은 자동적으로 이상 현상 모델을 구축할 수 있으나 계산 비용이 높다. 방법 7은 오버헤드는 낮으나 단지 단일 라우팅 프로토콜을 위해 설계되어서 프로토콜의 수정이 요구된다. 방법 8은 일반적인 지역 탐지 메커니즘 없이 이상적이나 각 홉마다 패킷이 검사되기 때문에 낮은 효율성을 갖는다. 그리고 방법 10은 높은 확장성으로 사용 중 분산되고 효율적이며 다수의 단계에서의 공격 탐지가 가능하지만 이동 에이전트와 관련된 보안과 계산비용 그리고 관리 문제를 갖는다.

4. 지 침

이 장에서는 MANET에서의 침입탐지 방법을 선택하는데 도움을 주는 지침이 개발되었다.

지침 1: 높은 탐지율과 낮은 거짓 경고율 그리고 각 노드에 충분한 망 자원과 계산 자원을 가진 MANET에서는 IDS는 각 노드에서 지역 탐지 기법으로 데이터 마이닝이나 신경망을 사용해야 하고 노드들 사이에서는 협력적 의사결정을 사용한다.

지침 2: 망 자원이 제한적이며 IDS에 대한 보안 요구사항이 높지 않은 MANET에서는 이동 에이전트가 노드들 사이의 통신 메커니즘으로 사용되어야만 한다.

지침 3: 확장성과 보안 요구사항이 높지 않은 IDS를 위해 이동 에이전트는 각 노드에서 탐지를 수행하는데 사용되어야 한다.

지침 4: 여러 종류의 감시 자료로 작동하기 위해 확장될 수 있는 IDS와 보안 요구사항이 높지 않은 IDS를 위해 이동 에이전트는 각 노드 상에서 탐지를 수행하도록 사용되어야 한다.

지침 5: MANET의 주어진 특징으로 다른 노드들로부터의 정보수집 없는 지역 탐지는 사용되지 말아야 한다. 이것은 높은 거짓 경고율과 낮은 탐지율을 유도한다.

지침 6: 노드의 계산 자원이 풍부하고 공격 종류와 위치가 알려질 필요가 있는 MANET에서는 방법 5에서 개발된 공격 종류와 위치 탐색 알고리즘이 사용될 수 있다.

지침 7: 클러스터를 사용하는 IDS에서는 자료가 클러스터 헤드로 보내지기 전에 멤버 노드상의 원래의 감시 자료가 클러스터 상의 IDS에서 사용하기 위해 처리되고 포맷되어야 한다. 이것은 클러스터 헤드의 네트워크 트래픽의 계산 요구 모두를 감소시킨다. 만약 보안 요구사항이 높지 않으면 네트워크 트래픽을 더욱 줄일 수 있기 때문에 멤버 노드 상에서 작업하는데 이동 에이전트가 사용되어야 한다.

지침 8: 높은 거짓 경고율에 대한 요구사항을 가지지 않는 MANET에서는 협력적 의사결정이 서비스 거부와 IP 위장 공격에 취약하기 때문에 선호할 메커니즘이 아니다.

5. 결 론

본 논문의 목적은 MANET에서의 IDS에 대한 연구의 현재 상태의 큰 그림을 제공하는 것이며 MANET에서 IDS를 위한 침입탐지 방법을 선택하는 지침을 제공하는 것이다. 특별히 본 논문에서는 우선 IDS, MANET 그리고 MANET을 위한 IDS들에 대한 현존하는 논문들을 조사하였고 MANET에서 IDS의 요구사항을 고려하였다. 그 다음 현존하는 논문들에서 제안한 IDS의 구조를 분석하기 위해 프레임워크 비교 연구를 개발하였다. 비교 연구에서 본 논문은 제안된 구조를 그것들의 입력, 출력, 처리 방법, 장점과 단점 등에 따라 논의하였다. 처리 방법 분석은 MANET에서 IDS 구조에 대해 클러스터가 사용되는지, 노드들 사이에서 어떤 통신 메커니즘이 사용되는지, 어떤 탐지 의사결정 메커니즘이 사용되는지, 그리고 어떤 지역 탐지 기술이 사용되는지에 더욱 초점을 맞추었다. 본 논문은 또한 MANET에서 다른 방법론의 선택이 IDS의 속성에 어떻게 영향을 미치는지를 연구하였다. 마지막으로, MANET에서 다른 침입탐지 방법을 선택하는 다수의 지침을 제안하였다.

MANET에서 침입탐지 비교 연구와 지침은 이 분야의 연구자들이 MANET을 위한 새로운 IDS를 설계하는데 참조 프레임워크를 제공한다. 또한 그들의 MANET을 위해 적당한 IDS를 선택해야만 하는 보안 전문가와 같은 의사결정자에게 도움을 줄 수 있다. 본 연구의 결과는 무선 세계에서 정보 시스템 보안에 관심을 가진 교육 전문가나 산업 전문가에게 유용할 것이다.

참 고 문 헌

[1] A. Patrick and O. Camp, "Security in Ad hoc Networks: a general Intrusion detection architecture enhancing trust based approaches," Proceedings of the First International Workshop on Wireless Information System, 2002.

[2] Brutch, Paul and Calvin ko, "Challenges in Intrusion Detection for Wireless Ad-hoc Networks." Proceedings of 2003 Symposium on Applications and the Internet Workshop, 2003.

[3] Debar, H. and A. Wespi, "Aggregation and correlation of intrusion detection alerts." Proceedings of th 4th intl sympon recent advances in intrusion detection, pp. 85-103, 2001.

[4] Gartner Group, "Gartner unveils the shape of the wireless economy," Gartner press Release, September 11 2000.

[5] Gillick, Kevin and Randy Vanderhoof, "Mobile e-Commerce:

market place enablers and inhibitors." Smartcard Forum Annual Meeting, 2000.

[6] Guha, R., O.Kachirski and D.G. Schwartz, "Case-Based Agents for Packet-Level Intrusion detection in Ad Hoc Networks." Seventeenth international Symposium on Computer and Information Sciences, 2002.

[7] Huang, Y. W. Fan, W. Lee and P.S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies." Proceedings of the 23th International conference on distributed computing systems, pp. 478-487, 2003.

[8] Huang, Yi-an and Wenke lee, "A cooperative intrusion detection system for ad hoc networks." Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), 2003.

[9] Kachirski, Oleg and Ratan Guha, "Effective Intrusion Detection Using Multiple Sensor in Wireless Ad Hoc Networks." Proceedings of the 36th Hawaii International Conference on System Sciences, 2002.

[10] Kong, J., H. Lou, K. Xu, D. Gu, M. Gerla, and S Lu, "Adaptive Security for Multi-layer Ad-hoc Networks." Special Issue of Wireless Communication and Mobile Computing, 2002.

[11] Lee, Wenke, "Applying data mining to intrusion detection: the quest for automation, efficiency, and credibility, "ACM SIGKDD Explorations Newsletter. Vol. 4, No. 2, pp. 35-42, 2002.

[12] Marti, S., T. Giuli, K. Lai, and M Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks." Proceedings of the Sixth Annual International Conference on Mobile Communication and Networking, 2000.

[13] May, Paul, "Mobile Commerce: Opportunities, Applications, and Technologies of Wireless Business", United Kingdom: Cambridge University Press. p. 6, 2001.

[14] Mishra, Amitabh and Ketan Nadkarni, "Intrusion Detection in wireless Ad Hoc Networks." IEEE Wireless Communications, pp.48-60, February 2004.

[15] Okazaki, Y., I. Sato, and S Goto, "A new Intrusion detection method based on process profiling." Proceedings of 2002 Symposium on Applications and the Internet, 2002.

[16] Puttini, R. S, J-Mr. Percher, L Mé, O Camp, R. of Sousa Jr., C J. Barenco Abbas and L J Garcia Villalba, "Modular for Distributed IDS in MANET Structures." Proceedings of the 2003 International Conference on Computational Science and Its Applications (ICCSA), 2003.

[17] Rajavaram, Sowjanya and Hiren Shah, "Neighborhood Watch: An Intrusion Detection and Response Protocol for Mobile Ad-hoc Networks." Technical Report, UMBC, October 2002.

[18] Sekar, R, "Specification-based anomaly detection: a new approach for detecting network intrusion." Proceedings of the 9th ACM conference on Computer and communications security, pp. 265-274, 2002.

[19] Smith, Andrew B. "An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks." Proceedings of the 5th National Colloquium for Information System Security Education, 2001.

[20] Stefan Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy." Retrieved on March 26 2004 at Citeceer.com, 2000.

[21] Sun, B, K. Wu, and U. Pooch, "Routing anomaly detection in mobile ad hoc networks," Proceedings of the 12th International Confer3nce on Computer Communications and Networks, pp. 20-23, 2003.

[22] Sun, bo, Kui 쪄, and Udo Pooch, "Alert aggregation in mobile ad hoc networks." Proceedings of the 2003 ACM workshop on Wireless security, pp. 69-78, 2003.

[23] Tseng, Chin-Yang and Poornima Balasubramanyam, "A specification-based intrusion detection system for AODV." ACM Workshop on security of Ad Hoc and Sensor Networks, 2003.

[24] Wei, J., L. Liu, and K. Koong, "A Framework for Delivering Mobile Commerce Security System." Proceedings of International Conference for Pacific RIM Management: ACME Transaction, 2003.

[25] Zhang, Yongguan and Wenke Lee, "Intrusion detection

in wireless ad-hoc networks." Proceedings of the 6th annual International Conference on Mobile Computing and Networking, pp. 275-283, 2000.

[26] Zhang, Yongguan and Wenke Lee, "Intrusion detection techniques for mobile Manet." ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, pp. 545-556, 2003.

[27] Zhou, L. and Z.J. Haas, "Securing ad hoc networks." IEEE Network, 13(6), pp. 24-30, 1999.

◐ 저 자 소 개 ◑

오 선 진

1981년 한양대학교 공과대학(공학사)
1987년 미국 Wayne State University 컴퓨터과학과(이학사)
1989년 미국 University of Detroit 컴퓨터과학과(이학석사)
1993년 미국 Oklahoma State University 컴퓨터과학과(박사 과정)
1999년 曉星 Catholic University 전자계산학과(이학박사)
1994년~2000년 선린대학교 컴퓨터정보학과 교수
2000년~현재 세명대학교 정보통신학부 교수
관심분야 : 모바일 멀티미디어, 모바일 컴퓨팅, 무선 인터넷 등
E-mail : sjoh@semyung.ac.kr

배 인 한

1984년 경남대학교 전자계산학과(공학사)
1986년 중앙대학교 대학원 전자계산학과(이학석사)
1990년 중앙대학교 대학원 전자계산학과(공학박사)
1996년~1997년 Department of Computer Science and Engineering, The Ohio State University(Post-doc)
2002년~2003년 Department of Computer Science, Old Dominion University(Visiting Professor)
관심분야: 모바일 멀티미디어, 모바일 컨버전스, 모바일 컴퓨팅, 무선 인터넷 등
E-mail: ihbae@cu.ac.kr