MAC 및 LLC Layer의 특성을 이용한 Mobile Ad hoc 네트워크에서의 침입탐지에 관한 연구

이재상* 김동성* 박종서*

*한국항공대학교, 컴퓨터공학과

Intrusion Detection System for Mobile Ad hoc Network using Characteristics of MAC & LLC Layer

Jae-Sang Lee* Dong-Sung Kim* Jong-Sou Park*

*Department of Computer Engineering at Hankuk Aviation Univ.

요 약

Mobile Ad hoc망의 경우 단말기에서 무선접속 인터페이스만 있으면 침입자로 하여금 쉽게 접속이 가능하게 하며, SSID와 WEP Key를 쉽게 취득하여 네트워크의 일원으로 참여할 수 있는 보안상의 취약성이 존재한다. 보안 취약성을 극복하기 위해서는 한정된 에너지 자원과 프로세서를 가진 무선 단말기로 침입탐지를 수행하기에는 문제점들이 존재한다. 따라서 본 논문에서는 프로세스 부하를 줄이는 IEEE802.11 Frame헤더의 Sequence Number 분석방법과 효과적으로 침입을 탐지할 수 있는 RF Monitoring을 이용하여 Mobile Ad hoc 환경에 적합한 침입탐지 시스템을 제안한다.

I. 서론

1. Mobile Ad hoc 네트워크

1) 개요

Mobile Ad hoc Network는 기반 망과는 달리 중앙관리자가 존재하지 않으므로 각각의 노드들이 Self-Routing으로 인접노드들과 통신을 한다. 그림 1에서 보면 각 노드들(Mobile Node)은 이동성을 가지기 때문에 새로운 노드의 생성, 네트워크 내부에서의 노드의 이동, 노드의 소멸 등은 네트워크의 토폴로지를 시간에 따라 동적으로 변화시킨다. 각 노드는 주기적으로 자신의 존재를 브로드캐스팅하며, 직접적으로 통신이 가능한 이웃 노드의 정보를 항상 유지하고, 이웃 노드의 정보에 따라 라우팅정보를 갱신한다. 이는 라우팅 프로토콜에 의해서 생성 및 관리된다[1].

2) 특성

분산 운영 , 각 노드의 보안 및 라우팅 기능은 분산된 조건 하에서도 효율적으로 운영될 수 있어야 한다[2].

다이나믹한 네트워크 형태 , 노드가 이동성을 가지기 때문에 네트워크 형태가 다양해진다. 그러나 네트워크 연결은 유지되어야한다.

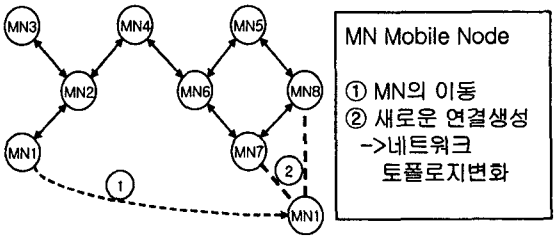

그림 1 Mobile Ad hoc 네트워크[2]

불규칙한 링크 용량 , 모든 링크 오류의 합이 멀티홉 경로에 영향을 미치기 때문에, 높은 비트 오류 율이 미치는 영향은 멀티홉 ad hoc 네트워크에서 더욱 명확히 나타난다.

소전력 기기 . 대개 네트워크 노드는 건전지로 작동되기 때문에 전력 여유가 별로 없다. 이는 곧 CPU 프로세싱, 메모리, 신호처리 등의 전력소모적인 부품에 영향을 미친다.

2. Wireless IDS

무선은 유선과는 환경이 다르기 때문에, WIDS 설계 시에는 다음의 사항을 고려해야 한다[3].

첫째, 무선환경은 유선망과는 달리 제한된 대역폭을 가지므로 통신 지연 등의 문제점을 발생시킨다. 둘째, 유선환경에서 처럼 정상과 비정상의 구분이 쉽지 않다. 셋째, 각각의 노드의 IDS 에이전트(Agent)들 사이에는 보안 채널이 필요하다. 넷째, 개방네트워크의 특성은 보안 취약성을 높인다. 개방성은 새로운 사용자가 네트워크에 쉽게 참여할 수 있는 장점이 있는 반면에 침입자로 하여금 쉽게 네트워크에 접근할 수 있다는 단점도 존재한다.

Ⅱ. 본문

1. 기존연구

무선네트워크에서의 침입탐지에 관한 연구는 크게 두 가지로 나눌수 있다.

첫째, DARPA의 프로젝트로써 프로토콜을 개발하거나 active network기술을 적용하는 방안에 대한 연구이다. 각 보안요소들을 하나의 보안프로토콜로 연결하는 IDIP(Intruder Detection and Isolation Protocol)와 침입자에 대한 능동적인 대응의 AN-IDR(Active Networks Intrusion Detection and Response)이 대표적이다[4].

둘째, 학계위주의 연구로서, 기존의 네트워크 보안기술을 무선네트워크에 적용하거나 이동형 에이전트 기술을 이용하여 침입자 탐지하여 위치를 추적하는 방안에 대한 연구이다[5].

위 연구들의 결과를 Mobile Ad hoc 네트워크에 적용시키기 위해선 제한된 자원을 지닌 무선노드를 신중하게 고려해야 한다. Mobile Ad hoc 네트워크의 무선노드에서는 제한된 에너지 자원의 효율적인 사용과 프로세스 과부하 방지가 필수적인 요건들이다. 이 문제점들을 고려해서 보면, 프로세스의 처리가 많아 에너지 자원을 쉽게 고갈시키는 Application이나 Transport Layer에서의 연구보다는 하위 레이어 인 MAC이나 LLC Layer에서의 연구가 필요하다[6].

1) Sequence number

표1에서 Mobile Ad hoc 네트워크에서 침입탐지 시스템이 고려해야 할 LLC Layer 분석의 특성요인들을 나열하였다. 이중에서 중요한 특성요인은

표 1 LLC Layer 분석의 특성요인

특성요인
Sequence number
Control Type and Subtype
Destination MAC
Service Set Identifier(SSID)
Organizationally Unique Identifier(OUI)
Data Payload, LLC Protocol Type Field
LLC Protocol ID

Sequence Number이다. Sequence Number는 IEEE802.11 Frame 헤더의 Sequence Control Block에 위치하고 있는 것으로, 12비트의 크기를 가지고 있다. 이는 하나의 카운터로서 0부터 시작하여 modulo 4096까지 카운트 한다(그림 2 참조).

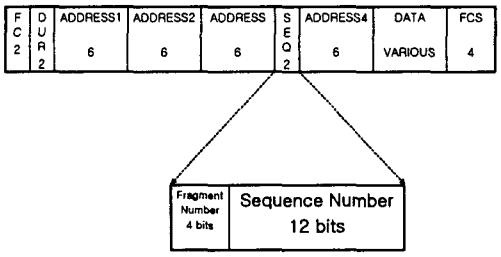

그림 2 Sequence Control Block[6]

네트워크에 침입자가 MAC Spoofing을 통해서 공격한다면, 우리는 이 침입자를 네트워크의 구성원과 구별해내기 힘들다. 하지만 IEEE802.11 Frame을 분석해보면 이 문제점을 해결할 수 있다. 그림3에서 보면 모니터링으로 캡쳐한 Frame의 분석 결과가 나와있다. 결과를 보면 네트워크의 어느 한 구성원과 동일한 MAC Address를 사용하면서 전혀 다른 Sequence Number를 가진 Frame이 존재한다. 이 Sequence Number는 무선네트워크상에서 각 호스트의 무선인터페이스가 생성해 내는 것으로, 동일한 호스트가 아니면 같을 수 없다. 그러므로 프레임 분석결과 동일한 MAC Address를 가지면서 서로 다른 Sqauence Number을 가진 Frame의 발생은 침입자가 MAC Spoofing 공격을 통하여 네트워크에 침투하였다고 판단할 수 있다. Sequence Number는 이러한 분석을 통해서 네트워크에 침입자가 발생했을 시에 일반 사용자와 침입자를 구별할 수 있는 주요한 factor가 된다[7].

2) RF Monitoring

RF Monitoring은 무선 환경에 있어서 주파수를 이용하여 주변의 이용 가능한 시그널을 모니터링 한다. 이용가능 시그널에 대한 정보를 수집한 이후에 연결요청 프레임과 요청응답 프레임을 주고

```
tecra:~ $ tethereal -r airjack.dmp -n -R "wlan.sa eq 00:e0:63:82:19:c6"
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
    BSS Id: 00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
    Fragment number: 0
    Sequence number: 2966

IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
    BSS Id: 00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
    Fragment number: 0
    Sequence number: 2967

IEEE 802.11
    Type/Subtype: Probe Response (5)
    Destination address: 00:60:1d:f0:91:56 (00:60:1d:f0:91:56)
    Source address: 00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
    BSS Id: 00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
    Fragment number: 0
    Sequence number: 2968

IEEE 802.11
    Type/Subtype: Deauthentication (12)
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
    BSS Id: 00:e0:63:82:19:c6 (00:e0:63:82:19:c6)
    Fragment number: 0
    Sequence number: 1335
IEEE 802.11 wireless LAN management frame
    Fixed parameters (2 bytes)
        Reason code: Previous authentication no longer valid (0x0002)
```

그림 3 IEEE802.11 Frame 분석

받음으로서 링크를 연결시킬 수 있다. 이와 같이 노드 간에 connection을 만드는 RF 시그널의 특성을 보면 다음과 같다.

첫째, 시그널의 강도는 거리에 반비례한다. Source에서 거리가 멀수록 시그널의 크기가 작아지고, 가까우면 시그널의 크기가 커진다(그림 4참조).

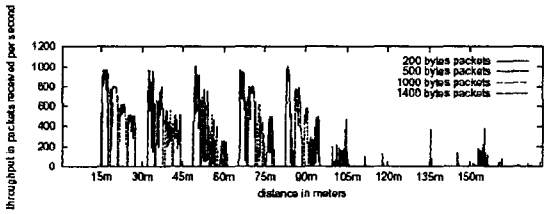

그림 4 거리에 따른 시그널의 강도[8]

둘째, 노드의 이동에 따라서 시그널의 크기가 동적으로 변화한다. Ad hoc 환경의 각 노드는 이동성을 가지므로, 노드가 이동함에 따라 시그널의 크기도 변화한다.

셋째, 노드상의 무선인터페스의 방향에 따라 방향성이 달라진다. 무선인터페이스의 시그널은 직진성을 가지므로 그 위치에 따라서 방향성이 달라진다(그림5 참조).

그림 5 무선인터페이스의 방향성[8]

기존연구에서 밝혀진 바와 같이 Mobile Ad hoc 네트워크에서 침입탐지시스템을 구축할 시에는 여러 가지 고려되어야 할 사항들이 있다. 그중에서도 특히 무선단말기의 자원이 한정적이라는 점은, Mobile Ad hoc 네트워크 상에서의 WIDS를 구축할 시에는 큰 요인으로 작용한다. 이 문제점들을 보완하기 위해서는 많은 프로세스 처리량을 발생시키는 네트웍의 상위 Layer 특징분석보다는 비교적 처리양이 적은 하위레이어의 특성을 이용하는 것이 보다 효율적인 침입탐지를 가능케 한다. 여기에 무선네트워크의 시그널 특성을 이용한 RF Monitoring을 이용한다면, 보다 효과적으로 침입자를 탐지해 낼수 있다. 이에 본 논문에서는 Mobile Ad hoc 네트워크에서의 효율적인 침입탐지시스템 구축을 위한 네트워크 하위 레이어의 특성에 대한 연구를 제시하고자 한다.

2) 제안 모델

침입탐지 시스템은 크게 모니터링과 대응 두 가지의 행동으로 나누어진다. 이 두 가지 모두 중요하지만 특히 효율적인 모니터링은 침입탐지 시스템에 있어서 필수적이다.

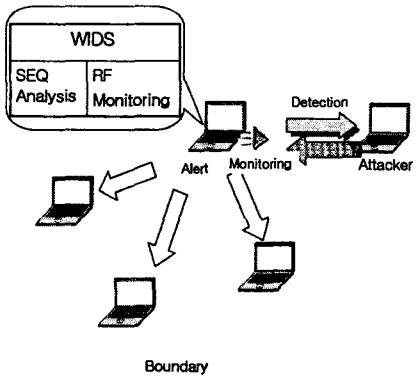

그림 6 제안모델

현재의 모니터링 기술은 주로 패킷 모니터링에 의존하고 있다. 패킷 모니터링의 경우 모든 패킷을 분석해야 하기 때문에 프로세스 처리량이 많고 데이터베이스의 양 또한 커지므로, 제한된 자원의 무선 단말기에서 수행함에 있어 어려운 점이 많다. 또한 모니터링시의 Audit point의 부재는 전체 패킷을 수집함에 있어서, 네트워크의 각 노드에게

빈번한 라우팅을 생성시킴으로 프로세스 과부하를 준다. 이뿐만 아니라 무선네트워크에서 주요한 로긴 정보인 MAC Address는 네트워크 상에 노출되어 있기 때문에 침입자로 하여금 MAC Spoofing 공격을 가능하게 한다.

침입자를 구별하긴 위해선 패킷의 정보 분석에 802.11 Frame 헤더에 있는 Sequence의 정보를 이용하면 효율적이다. Sequence Number는 frame의 헤더에 있는 정보로, 분석 시에 다른 레이어의 frame보다 Decapsulation 과정을 덜 거치게 되므로 프로세스 처리량이 많지 않아 효율적인 모니터링을 가능하게 해준다. 뿐만 아니라 TCP계층의 Frame Sequence Number와는 달리, 펌웨어에 의해서 생성되므로 펌웨어 프로그램 지식을 가진 전문가가 아니라면 변조를 할 수가 없다.

이러한 Sequence Number도 시스템상의 fault로 인하여 잘못된 정보를 전하거나 정보의 전달을 방해 받을 수 있다. 하지만 정상적인 네트워크 상에서 침입자 분류과정의 Feature로써 Sequence Number의 이용은 효과적이다[7].

특수한 목적의 Ad hoc 네트워크를 구축할 시에 Boundary의 설정은 매우 중요하다. 이는 네트워크의 구성원으로 하여금 이웃노드와의 연결을 유지하게 해줌과 동시에 침입자로 하여금 네트워크에 접근하지 못하도록 하는 물리적인 보안성을 제공한다. Boundary의 설정은 시널 강도의 상한선과 하한선을 결정함으로써 가능하다. 이는 Noise로 식별될 수 있는 신호를 차단함으로써 노드 간에 우수한 링크를 보장해 준다. 이렇게 설정된 Boundary안에서 RF Monitoring을 수행함으로서 훨씬 더 효과적으로 침입자를 탐지해 낼 수 있다. 그림6에서 보면 침입자가 구축되어 있는 네트워크로의 진입을 시도시 적정 시그널 범위 내에 위치하여야 하며, 이는 물리적으로도 가까운 위치임을 뜻한다. 이러한 상황에서 침입자가 네트워크에 진입 시도시 RF Monitoring으로 색출이 가능하고, 네트워크 진입에 성공한다 하더라도 Sequence Number를 적용한 WIDS로 탐지가 가능하다. 또한 GPS를 도입한다면 침입자의 정확한 위치 파악까지도 가능하다.

Ⅲ. 결론 및 향후연구

본 논문에서는 Mobile Ad hoc Network에서의 효과적인 침입탐지 시스템을 위한 MAC과 LLC Layer의 특성에 대해 제시하였고, 특히 침입자를 가려내는 방법에 있어서 LLC Layer의 특성인 Sequence Number와 MAC layer의 특성인 RF Monitoring을 중점적으로 다루었다. Sequence Number를 이용한 효율적인 WIDS와 효과적으로 침입자를 탐지할수 있는 설정 Boundary내에서의 RF Monitoring은 각각 독립적이 아니라 상호 보완적으로 개념으로 작용한다. 이러한 두가지 개념의 복합성은 Mobile Ad hoc 네트워크 상에서의 뛰어난 침입탐지 시스템을 구현 가능케 한다. 그러나 이 두 가지 개념이 결합된 침입탐지 시스템은 무선노드에 프로세스 과부하라는 단점을 완전히 해결하지는 못하고 있다.

이 문제점 개선을 위해서는 Mobile Ad hoc 네트워크에 트래픽이 집중되는 Centralized Manage Device를 세워, 무선노드에 탑재된 Monitoring 기능을 이식함으로써 각 노드로부터 프로세스 과부하를 생성시키는 모니터링 기능을 분리해내는 방법에 대한 연구가 필요하다.

Acknowledgement

본 논문은 과학기술부·한국과학재단 및 경기도의 RRC 사업 연구비 지원에 의해 수행되었음.

참고문헌

[1] C. K. Toh, "Ad Hoc Mobile Wireless Networks : Protocols and Systems", Prentice Hall PTR, 2002.

[2] C. E. Perkins, "Ad Hoc Networking" Addison-Wesley, 2001.

[3] Wenken Lee, Yongguang Zhang, Yi-An Huang, "Intrusion Detection Techniques for Mobile wireless networks"

[4] Active Network project DARPA

[5] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, MobiCom' 2000,

[6] Joshua Wright, "Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection" 2002

[7] Joshua Wright, "Detecting Wireless LAN MAC Address Spoofing", 2003

[8] D. Dhoutaut, I. Guerin-Lassous(Equipe ARES / CITI/FR), "Experiments with 802.11b in ad hoc configurations", Madnet Conference 2003