모바일 애드 혹 네트워크에서의 실시간 침입탐지 노드 선택 방법에 관한 연구

A Real-Time IDS Node Selection Method in MANETs

길현준, 김세헌
산업 및 시스템공학과, 대전시 유성구 구성동 373-1 KAIST

Abstract

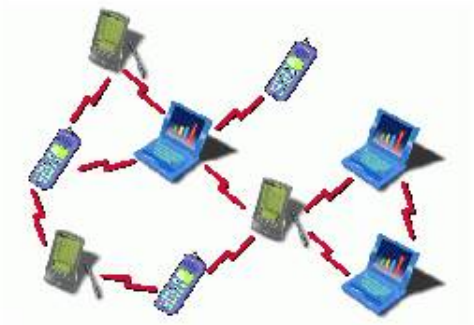
최근 들어 군사, 교통, 헬스 케어, 지능형 빌딩 등에서 모바일 애드 혹 네트워크(MANET)의 활용성이 부각되면서, 모바일 애드 혹 네트워크가 흥미롭고 장래 유망한 분야로 각광 받고 있다. 그러나 중앙통제센터의 부재, 잦은 토폴로지의 변화 등으로 네트워크의 보안상의 문제가 발생하고 있다. 이를 해결하기 위한 대안으로 침입 탐지 시스템 (IDS)이 도입되었는데, 기존의 연구들은 모바일 애드 혹 네트워크의 잦은 토폴로지의 변화 환경 하에서 복잡한 알고리즘과 많은 계산량 등으로 빠른 침입 탐지 시스템 노드의 배치가 어려웠다. 따라서 이번 연구에서는 다이나믹하게 변하는 네트워크 환경에서 간단하고 빠른 침입 탐지 시스템 노드의 배치 알고리즘을 제안하려고 한다.

1. Introduction

최근 들어 유선 통신과는 달리 무선 통신에서의 보안 문제가 빠른 속도로 증가하고 있다. 이것은 무선 랜, 이동 전화의 사용 인구가 기하급수적으로 증가하고 있기 때문인데, 이러한 무선 통신의 이용률 증가와 함께 부각되고 있는 것이 보안의 문제이다.

여러 가지 형태의 무선 통신 중에서도 최근 들어 군사, 교통, 헬스 케어, 지능형 빌딩 등에서의 활용성이 부각되고 있는 모바일 애드 혹 네트워크가 흥미롭고 장래 유망한 분야로 각광 받고 있다. 그러나 모바일 애드 혹 네트워크의 특성상 보안에 취약하다는 단점이 있는데, 이것은 모바일 애드 혹 네트워크를 구성하는 구성요소나 그것들의 구성 방법에 따른 것이다.

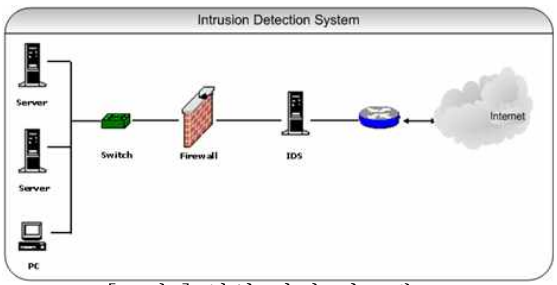
[그림1]과 같이 먼저 다른 무선 통신과는 달리 중앙의 통제센터가 없는 구조이기 때문에 전체의 네트워크 정보를 수집하고 관리할 수 없다. 또한 통신과 관련된 노드들의 출입이 자유롭기 때문에 토폴로지가 고정되어 있거나 어느 정도 정적인 것이 아니라 토폴로지의 변



[그림1] 모바일 애드 혹 네트워크

화를 예측할 수 없고 변화 주기도 짧다.

이러한 모바일 애드 혹 네트워크의 특성 때문에 악의적인 의도를 가진 사용자가 네트워크에 침입하면 보안상의 문제가 발생하게 되는데 이것을 해결하기 위해 도입된 것이 침입 탐지 시스템 (IDS) 이다.



[그림2] 침입 탐지 시스템

[그림2]와 같이 침입 탐지 시스템은 네트워크상의 특정 노드들에 설치되어 자신의 커뮤니케이션 범위를 지나가는 모든 패킷을 수집하고 검사하여, 특정한 노드가 이상 행동을 하면 관리자에게 알리는 역할을 한다. 이 과정에서 침입 탐지 시스템이 설치된 노드들은 그렇지 않은 노드들보다 추가의 배터리 파워를 소모하게 된다.

여기서 이러한 침입 탐지 시스템을 어떤 노드

들에 배치하여야 좀 더 효과적인 침입 탐지를 하고, 각각의 노드들의 배터리 파워를 효율적으로 사용하여 전체 네트워크의 지속시간을 연장 시킬 수 있는지의 문제가 발생한다.
따라서 이번 연구에서는 다이나믹하게 변하는 네트워크 환경에서 간단하고 빠른 침입 탐지 시스템 노드의 배치 알고리즘을 제안하려고 한다.이러한 문제를 해결하기 위해 기존의 연구에서 많은 방법들을 제시하였다. 그러나 이러한 방법들은 복잡한 알고리즘과 많은 계산량 등으로 모바일 애드 혹 네트워크의 특성인 잦은 토폴로지의 변화에 다이나믹하게 대응하지 못하는 단점이 있었다.

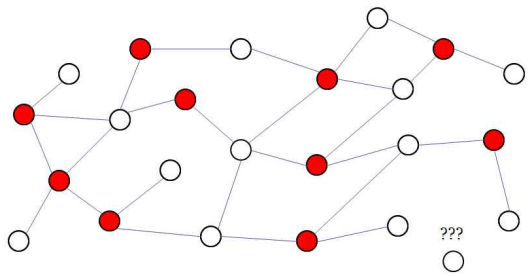
이 논문의 나머지 구성은 다음과 같다. 2장에서는 기존의 연구된 방법들을 간단하게 소개하고, 3장에서는 제안된 알고리즘을 소개한다. 4장에서는 결론을 제시하고, 마지막으로 5장에서는 향후 연구해야 할 과제를 소개하는 것으로 논문을 마치고자 한다.

2. Related works

모바일 애드 혹 네트워크에서 침입 탐지 시스템 노드의 배치 문제는 관련된 많은 연구자들의 관심을 끌어왔다.

이러한 침입 탐지 시스템 노드의 배치 문제에는 크게 모든 노드들의 이상행동 탐지와 함께 선택된 노드 수의 최소화, 선택된 노드의 배터리 파워를 고려한 전체 네트워크의 지속시간 연장 등이 연구되고 있다.

기존의 연구들을 살펴보면, 이웃 노드들의 배터리 파워를 고려한 침입 탐지 시스템 노드의 선택 방법[1]이나 최소걸침나무를 이용한 침입 탐지 시스템 노드의 선택 방법[2], 침입 탐지 시스템 노드의 탐지 범위를 고려한 선택 방법[3] 등의 연구가 있다. 이러한 연구들은 선택된 침입 탐지 시스템 노드를 최소화하거나 전체 네트워크의 지속 시간을 연장시키는 것에는 상당한 효과가 있으나 모바일 애드 혹 네트워크의 가장 큰 특징인 잦은 토폴로지의 변화에 다이나믹하게 대응하지 못하는 단점이 있다.



[그림3] 기존의 침입 탐지 시스템 노드 선택

즉, 모바일 애드 혹 네트워크에서는 노드의 출입이 자유롭기 때문에 [그림3]과 같이 이러한 변화가 생길 때마다 전체적인 네트워크를 대상으로 침입 탐지 시스템 노드를 다시 선택한다면, 복잡한 알고리즘과 많은 계산량 때문에 실시간으로 대응하기 힘들다. 따라서 이러한 잦은 토폴로지의 변화에 적용할 수 있는 간단한 알고리즘이 필요하다.

3. A Proposed algorithm

이 논문에서는 침입 탐지 시스템 노드의 선택 시에 전체 네트워크를 대상으로 하지 않고 각각의 패스를 대상으로 함으로써, 모바일 애드 혹 네트워크의 잦은 토폴로지의 변화에 대응하는 간단한 알고리즘을 제안하였다.

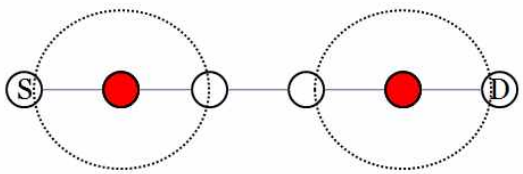
먼저 이 알고리즘에서는 모바일 애드 혹 네트워크의 환경에서 온-디맨드의 프로토콜을 사용하는 것을 가정하였다. 또한 여기서는 컨트롤 패킷 보다는 데이터 패킷에 중점을 두어 패스가 정해지고 난 후에 패스를 따라 흐르는 데이터 패킷의 무결성을 강조하였다. 이 알고리즘의 간단한 단계는 다음과 같다.

Step. 1
전체의 네트워크에서 데이터를 송수신하는 노드를 정하고, 특정한 프로토콜을 사용하여 패스를 선택한다.

Step. 2
선택된 패스 상에서 휴리스틱한 방법 또는 간단한 알고리즘을 이용한 최적 선택 방법을 이용하여 침입 탐지 시스템 노드를 선택한다. 이때 선택된 노드는 패스 상의 모든 노드들의 이상 행동을 탐지할 수 있어야 한다.

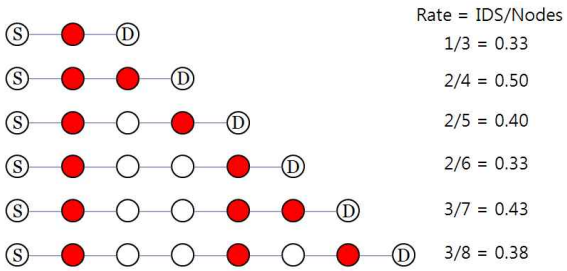
Step. 3
해당 패스를 이용한 데이터의 전송을 마치면 선택된 침입 탐지 시스템 노드들을 정상 노드로 반환한다.

Step. 2에서 침입 탐지 시스템 노드를 선택할 때 여러 가지 방법을 사용하여 선택할 수 있다. 여기서는 간단하고 직관적인 방법을 소개하고자 한다.



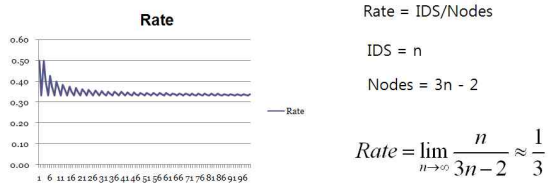
[그림 4] 침입 탐지 시스템 노드 선택 방법

[그림 4]와 같이 침입 탐지 시스템 노드의 탐지 범위가 1홉의 이웃노드까지라고 하면 패스상의 노드가 6개일 때 2개의 노드가 침입 탐지 시스템 노드로 정해진다. [그림 5]는 패스상의 노드의 수를 늘려가면서 나타내어 본 것이다.



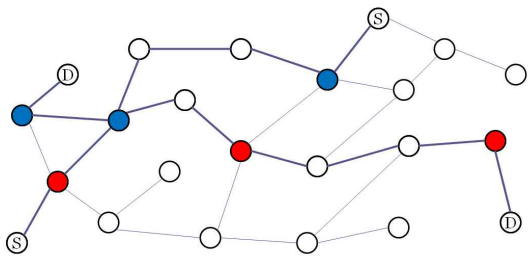
[그림 5] 침입 탐지 시스템 노드의 비율

[그림 6]은 패스상의 노드의 숫자를 100개까지 늘렸을 때의 결과인데, 대략 33.3%의 비율로 선택되는 것을 알 수 있다.



[그림 6] 침입 탐지 시스템 노드의 비율

이러한 간단한 선택 방법을 전체적인 네트워크에서 적용하여 보면 [그림 7]과 같다.



[그림 7] 간단한 선택 알고리즘의 적용 예

하나의 패스에서 전송을 하는 사이 다른 노드에서 전송을 하려고 패스가 설정되면 그 패스상에서 침입 탐지 시스템 노드가 선택된다. 만약 그 선택된 노드가 이미 선택된 노드라면 전체 네트워크에서 침입 탐지 시스템 노드의 비율이 작아질 수도 있을 것이다.

또한 전체 네트워크에서 모든 노드들이 전송을 하거나 침입 탐지 시스템 노드로 선택되어 활동을 하는 것이 아니라, 전송을 하고 있는 패스상의 노드만 활동을 하고 전송을 마치면 활동을 멈추기 때문에 각 노드의 배터리 파워와 전체 네트워크의 지속시간 연장 측면에서도 좀 더 효율적일 것이다.

앞에서 소개한 간단한 휴리스틱 방법 외에도 많은 방법들이 있을 것이다. 이러한 간단하고 빠른 침입 탐지 시스템 노드 선택 방법은 모바일 애드 혹 네트워크 환경하에서 전체 네트워크에서 선택하는 것보다 훨씬 더 효율적이고 다이나믹하게 대응할 수 있다.

4. Conclusion

이 논문에서는 모바일 애드 혹 네트워크의 잦은 토폴로지 변화 환경하에서 다이나믹한 침입 탐지 시스템 노드 선택 방법에 관한 간단하고 빠른 알고리즘을 제시하였다. 이 방법은 기존의 연구들에 비해 거의 실시간으로 토폴로지의 변화에 대응할 수 있다.

또한 전송에 관여하지 않는 노드들의 배터리 파워 소모를 최소한으로 줄임으로써 전체 네트워크의 지속시간의 연장을 가능하게 하였다.

그러나 전체 네트워크를 대상으로 하는 것이 아니라 전송이 이루어지는 패스별로 침입 탐지 시스템 노드를 선택함으로써 특정 프로토콜, 예를 들면 온-디맨드 방식의 프로토콜에 한정되는 약점이 있다.

5. Future works

이 논문에서는 아직 제안한 알고리즘에 대한 시뮬레이션이 진행 중이다. 따라서 제안한 알고리즘에 대한 성능을 측정할 수 있는 여러 가지 기준 즉, 전체 네트워크에서 침입 탐지 시스템 노드의 비율이나 노드를 선택하는 알고리즘의 속도, 복잡도 등을 측정할 수 있는 기준 등을 만들어 추가로 시뮬레이션을 해야 할 것이다.

또한 이 논문에서는 간단하고 직관적인 휴리스틱한 선택 방법을 소개하였다. 이러한 선택 방법 역시 앞으로 연구하고 시뮬레이션으로 성능을 측정해보아야 할 것이다.

< References >

[1] Hyunwoo Kim, Dongwoo Kim, Sehun Kim. Lifetime-enhancing selection of monitoring nodes for intrusion detection in mobile ad hoc networks. Int. J. Electron. Commun. (AEU) 60 (2006) 248 - 250

[2] Ha, Sung-chul. An Efficient Lifetime-Enhancing IDS Node Distribution Using Minimum Spanning Tree in Wireless Ad Hoc Networks

[3] Tran Hoang Hai, Eui-Nam Huh. Minimizing the Intrusion Detection Modules in Wireless Sensor Networks. International Conference on Computational Sciences and Its Applications ICCSA 2008