Ad-Hoc 네트워크 상에서의 계층적 침입 탐지 시스템
A Hierarchical Intrusion Detection System in Wireless Ad-hoc Networks.

정영옥, 김세헌
한국과학기술원 산업공학과

Abstract

침입탐지시스템(Intrusion detection system)은 외부에서 시스템의 자원을 불법으로 사용, 변조, 제거하는 것을 막기 위해 설치된 시스템으로 현대의 네트워크가 점점 발전해가고 그에 따른 악의적인 사용자의 수도 증가하면서 그 중요성이 더해가고 있다. 특히 Ad-hoc 을 기반으로 한 무선 네트워크에서는 무선이 갖는 특성으로 인해 유선 네트워크보다 더 많은 보안상의 위험에 노출되어 있을 뿐만 아니라, 시스템의 자원인 에너지가 한정되어 있다는 특성을 갖는다. 따라서 자원을 가능한 효율적으로 사용하면서 보안상의 위협도 최소화 시킬 수 있도록 침입 탐지 시스템을 구현하는 것이 적절할 것이며, 이를 위해 보안 위협의 정도와 자원 위협의 정도를 고려한 계층적인 보안 시스템을 구축하고자 한다.

1. 서론

무선 Ad-hoc 네트워크는 고정된 유선기반이 없는 상태에서 각 이동 단말기들이 통신하고자 할 때 임시로 짧은 시간 안에 하나의 소규모 네트워크를 구성하여 통신을 하는 망을 일컫는다. 이러한 통신 방식은 레이아웃 변경의 편리성, 무선 네트워크가 가능한 반경 내에서의 이동성, 설치 및 유지보수의 확장성, 네트워크 구축의 유연성 등 유선 네트워크에서와는 다른 많은 장점을 가지고 있다. 또한 일반 네트워크가 Access Point를 중심으로 하는 데 비해 무선 Ad-Hoc 네트워크는 Access Point없이 무선 단말들만으로도 충분히 구현이 가능하다. 이것은 무선 Ad-Hoc 네트워크에서 각 단말 노드는 하나의 라우터 기능을 하기 때문이다. 원래 이 통신방식은 군사 통신망 구축과 같은 군사적 목적으로 개발되었으나 현재는 군사적 목적 이외에서도 재난 구조나 로봇 협동 작업, 회의장과 같이 공공 및 산업적 목적으로도 많이 쓰이고 있다.

그렇지만 무선 Ad-Hoc 네트워크는 유선 네트워크에 비해 보안상 훨씬 더 많은 위험에 노출되어 있다. 즉, Ad-Hoc과 같은 무선 네트워크는 전파를 매체로 사용하기 때문에 전파간섭, 다중링크로 인한 보안상 취약성을 가지게 되는 것이다 이러한 무선 Ad-Hoc 상의 보안 문제는 정보화 사회로의 발전과 더불어 공공 및 개인 정보 보호 인식이 높아져 감에 따라 점점 더 중요한 문제로 다루어지고 있다. 기존의 침입 탐지 시스템(Intrusion Detection System: IDS)의 대부분은 유선 네트워크를 기반으로 연구되어 왔다. 하지만 이 시스템을 그대로 무선 Ad-hoc 네트워크 상의 각 단말에 적용하기에는 무선 Ad-hoc 만이 가지고 있는 몇 가지 특성

'본 연구는 대학 IT연구센터 육성지원사업의 연구결과로 수행되었음'

때문에 여러 문제점이 발생한다. 그 중 하나가 자원의 제약성이다. 대부분의 무선 Ad-hoc 네트워크의 단말에서 밧데리와 같은 자원은 한정되어 있고 이것이 고려되지 않은 채 침입 탐지 시스템(Intrusion Detection System: IDS)을 설치한다면 네트워크의 보안의 효율성을 위해 네트워크의 수명을 단축시키는 결과를 가져오게 될 것이다. 따라서 본 연구에서는 무선 Ad-hoc 네트워크의 특성 중 한정된 자원 상황을 고려하여 그에 맞는 보안 설정을 최적화하고자 한다.

서론에 이어서 2에서는 기존에 무선 Ad-Hoc 상의 침입 탐지와 관련된 연구 사례들을 언급하고, 3에서는 본 연구에서 제시하고자 하는 침입 탐지 시스템(Intrusion Detection System: IDS)을 소개하고 4에서는 간단한 예시를 통해 보안 수준의 변화를 살펴볼 것이다. 그리고 마지막으로 5에서는 분석한 내용을 토대로 향후 연구 과제 및 결론을 기술하고자 한다.

2. 기존 연구 사례

무선 Ad-hoc 네트워크 상에서 보안을 하는 가장 기초적인 방법은 모든 단말 노드에 침입 탐지 시스템(Intrusion Detection System: IDS)을 설치하여 실행하는 방식이다. [1] 이 시스템에는 기존 유선 네트워크 상의 침입 탐지 시스템(Intrusion Detection System: IDS)과 비슷하게 먼저 데이터를 수집하고, 칩임 탐지 엔진을 통해 수집된 데이터를 분석한 뒤, 침입이라고 여겨지는 데이터에 대해서 접근 통제나 거부 등의 직접적인 대응을 하거나 단순히 노드에 침입 정보를 알려주는 등의 소극적인 대응을 한다. 기본적으로 각 노드들은 효과적인 보안을 위해 상호 협력을 하며 각 노드의 자원의 제약성은 고려하지 않고 있다. 자원의 제약성을 고려하여 연구된 것으로는 침입 탐지 시스템(Intrusion Detection System: IDS)을 전체 노드가 아닌 일부 노드에 설치하여 전체 네트워크의 자원의 효율성을 고려하였다. 즉, 가장 연결성이 좋은 노드를 일정한 시간마다 투표하여 선정된 노드만이 침입 탐지 시스템(Intrusion Detection System: IDS)을 설치하거나[2], 일정한 시간마다 에너지가 가장 많이 남아있는 노드에 침입 탐지 시스템(Intrusion Detection System: IDS)을 설치하는 방법[3] 등이다. 이러한 방법들은 모든 노드에 시스템을 설치하는 것보다 자원을 효율적으로 사용할 수 있는 장점은 있지만, 노드 간의 상호 협력은 내부 노드가 악의적인 노드가 아니어야 한다는 가정을 우선적으로 필요로 한다. 하지만 무선 Ad-hoc 네트워크는 일시적으로 네트워크의 형성과 소멸이 반복되는 특성을 가지고 있고, 제 3기관의 인증을 받는 것도 어렵기 때문에 노드 간의 협력을 우선적으로 고려하는 것은 무리가 있다. 오히려 이러한 점에서는 모든 노드마다 침입 탐지 시스템(Intrusion Detection System: IDS)을 설치하는 것이 침입에 더 안전하다고 말할 수 있을 것이다.

3. 침입탐지시스템

3.1 환경적 요소

무선 Ad-Hoc 네트워크의 각 노드가 앞서 언급했듯이 자기자신을 제외한 모든 다른 모드를 잠정적인 악의 노드라고 생각한다면, 기본적으로 각 노드는 자신을 보호할 침입 탐지 시스템(Intrusion Detection System: IDS)을 설치하는 것이 바람직하다. 하지만 어느 정도의 보안수준을 설정하여 칩임을 대비할 것인지는 유선 네트워크에서 침입 탐지

시스템을 설치할 때와는 달리 자원의 제약성을 고려하여 결정해야 한다. 본 연구에서는 단말 노드들이 어느 정도의 이동성을 가지고 분산된 1-tier 네트워크를 형성하는 것을 기본적인 무선 Ad-hoc 네트워크로 가정한다. 또한 자원의 효율을 효과적으로 보여주기 위해 공격의 유형을 DoS(Denial of Service)로 한정한다.

3.2 침입확률

노드의 적절한 보안을 위해 침입확률을 아는 것은 중요하지만 그 근거를 도출하는 기준은 아직 불명확하다. 본 연구에서는 무선 Ad-hoc 네트워크가 가진 특성 중의 하나인 노드의 이동성을 그 기준으로 삼고자 한다. 시간이 따라 변해가는 노드의 개수가 침입확률의 지표이며, 주변 노드의 개수가 많으면 침입확률이 높고, 적으면 침입확률이 낮은 것이다. 이 확률은 기본적으로 주변 노드가 잠정적 악의 노드라는 관점에서 볼 때 타당성을 가진다. 따라서 N(t)를 시간 t 시점에서의 주변 노드의 개수라고 본다면 침입확률 p는 다음과 같다.

$p = 1 - [1/N(t)]$ (단, $0 \le p \le 1$)

여기에서 N(t)의 분포는 임의의 노드에서 하나의 새로운 노드가 연결되는 시간을 포아송 분포로 생각하고, 그 노드가 연결되어 있는 시간을 지수분포라고 생각한다면, 시스템에서 고객들의 도착이 포아송 과정으로 일어나고 서비스 시간이 지수 과정으로 일어나는 경우와 같으므로 M/M/1 대기행렬의 경우를 채택한다. 아 때, 시간 $t \to \infty$로 본다면, Little's law를 적용하여 $E[N(t)]$ = 시스템 도착률×시스템에 머무는 평균시간 = $\lambda \times E(T)$이고 따라서 $p = [1/\lambda \times E(T)]$이다.

3.3 최적해 도출

무선 Ad-hoc 네트워크 상에서 노드의 에너지 자원의 최적화를 목적으로 한다면 임의의 노드에 공격이 발생하거나 침입 탐지 시스템(Intrusion Detection System: IDS)을 설치하는 데에 에너지가 소모가 일어난다. 특히, DoS(Deinal of Service)와 같은 공격이 발생하면 노드의 에너지 소모가 극도하게 일어나고 이를 방지하기 위해 침입 탐지 시스템(Intrusion Detection System: IDS)의 설정을 과다하게 한다면 이 또한 에너지 비효율을 초래할 것이다. N을 보안 수준의 개수라고 하고 이 개수는 공격 개수와 같다고 한다면, 목적식은 공격을 받았을 때의 에너지 소모와 임의의 보안수준을 설정했을 때의 에너지 소모 비용을 최소화하도록 설정한다. 따라서 전체적으로 다음과 같은 식을 얻는다.

$$\min.\ p \times \{ \sum_{i=1}^{N} E(A_i) \times (\sum_{k=i+1}^{N} x_k) \} + \sum_{i=1}^{N} C(A_i) \times x_i$$

$$\text{s.t.} \sum_{i=1}^{N} x_i = 1 \text{ (단, } x_i \text{는 정수)}$$

$$p = \max[0, 1 - [1/N(t)]]$$

$E(A_i)$: i번째 공격 유형에 따른 에너지 소모 비용

$C(X_i)$: x등급 보안수준을 유지하는 데 드는 에너지 소모 비용

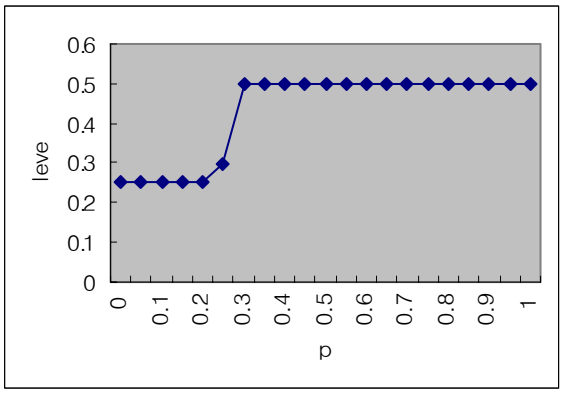
x_k: x등급 보안 수준 설정여부, (단, $x_k > x_{k+1}$)

$\sum_{i=1}^{N} x_i = 1$를 통해 노드는 0또는 1의 값을 가지며, 단 하나의 보안 수준만을 설정하게 된다. 침입확률은 0보다 작을 수 없으므로 $p = \max[0, 1 - [1/N(t)]]$을 통해 0과 예측된 값 중에서 큰 값을 선택하도록 설정하였다. 또한, 위 식을 일정한 시간마다 계산하여 보안 수준을 변화시킨다.

4. 침입 모델

DoS 공격의 세 가지 유형이 발생하는 에너지 소모를 무선 네트워크 상에서 분석한 연구[5]를 토대로 간단하게 위의 최적해를 구해보면 다음과 같다.

min. p{0.8(x2+x3)+0.15(x3)} +
{0.6x1+0.4x2+0.2x3}
s.t. x1+x2+x3 = 0



위의 그래프에서 침입확률 p가 증가함에 따라 보안 수준이 가장 작은 1에서부터 3으로 변해가는 것을 볼 수 있고 이 때의 보안 수준이 에너지 비용을 가장 최소화하는 값이다.

5. 향후 연구 과제 및 결론

본 연구에서는 무선 Ad-Hoc 네트워크 상에서 네트워크 상황에 맞는 계층적 침입 탐지 시스템(Intrusion Detection System: IDS)을 설치하여 각 노드에서의 자원의 최적화를 도출해내고자 하였다. 이를 통해 적절한 보안 수준을 유지하면서도 자원을 효율적으로 사용할 수 있을 것이다.

차후 논의될 수 있는 연구 과제로 노드의 이동성 외에 다른 Ad-hoc 네트워크 의 특징을 반영하여 침입확률을 도출하거나, 에너지 비용의 수치를 변화시키거나, 더 고려해야 할 에너지 비용을 추가하거나, 목적식을 계산하는 단위 시간을 변화시키는 것 등이 가능할 것이다.

참고문헌

[1] Y. Zhang, W. Lee, Y, A. Huang,, *"Intrusion Detection Techniques for Mobile Wireless Networks"*, Wireless Networks 9(2003), pp545–556.

[2] Kachirski, O., Guha, R., *"Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks"*, Proceedings of the 36th Hawaii International Conference on System Sciences, 2003, pp57-64.

[3] H.Y. Kim, Y.O. Jung, S.H. Kim, *"A Lifetime Maximizing Scheme for Intrusion Detection in Wireless Ad-hoc Networks"*, Proceedings of the 33rd International Conference on Computers and Industrial Engineering, 2004

[4] Alampalayam, S., Kumar, A., Srinivasan, S., *"Mobile ad hoc network security – a taxonomy"*, Proceedings of the 7th International Conference on Advanced Communication Technology, Volume 2, 2005, pp839 – 844

[5] T Martin,, M Hsiao,, D Ha,, J Krishnaswami, "Denial-of-Service Attacks on Battery-powered Mobile Computers", Proceedings of the IEEE International Conference on Pervasive Computing and Communications, 2004, pp309 – 318

[6] Ilyas and Mohammad, *The handbook of ad hoc wireless networks*, CRC Press, 2002.

[7] D.J.Marchette, *Computer Intrusion Detection and Network Monitoring*, Springer, New York, 2001