2005 한국경영과학회/대한산업공학회 춘계공동학술대회
2005 5 월 13 일~14 일, 충북대학교

Ad-Hoc 네트워크 상에서 침입 탐지 시스템의 게임 이론적 접근

A Game Theoretic Approach to Intrusion Detection System in Wireless Ad-hoc Networks.

정영옥, 김세헌
한국과학기술원 산업공학과

Abstract

현대의 정보사회는 인터넷의 발전과 더불어 급속히 팽창하고 있으며 그에 따른 편리함과 더불어 악의적인 사용으로 인한 부작용도 함께 늘어나고 있는 추세이다. 특히 Ad-Hoc 과 같은 무선 네트워크 시스템의 경우 무선이 갖는 여러 가지 특성과 더불어, 전파를 전송 매체로 사용하기 때문에 유선 네트워크 시스템보다 더 많은 보안상의 취약성을 내포하고 있다. 전체적인 네트워크 측면에서 볼 때 이러한 네트워크 상 보안 문제는 시스템에 침입하려는 공격자와 그 침입을 막으려는 침입 탐지 시스템 간의 문제로 볼 수 있으며, 동시에 각자의 이익을 극대화하기 위한 게임의 측면으로 볼 수 있을 것이다. 본 연구에서는 이러한 쌍방 간의 관계를 무선 Ad-Hoc 상에서 게임 이론적으로 접근하여 해석해보고자 한다.

1. 서론

무선 네트워크는 레이아웃 변경의 편리성, 무선 네트워크가 가능한 반경 내에서의 이동성, 설치 및 유지보수의 확장성, 네트워크 구축의 유연성 등 유선 네트워크에서와는 다른 많은 장점을 가지고 있다. 그 중 무선 Ad-Hoc은 각 이동 단말기들이 통신하고자 할 때 임시로

'본 연구는 대학 IT연구센터 육성지원사업의 연구결과로 수행되었음'

짧은 시간 안에 하나의 소규모 네트워크를 구성하여 상호 정보를 교환하는 방식으로 이루어진다. 따라서 일반 네트워크가 Access Point를 중심으로 하는 데 비해 무선 Ad-Hoc은 Access Point없이 무선 노드들만으로 충분히 구현이 가능하다는 장점이 있다. 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.

그러나 무선 Ad-Hoc은 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. 지금까지 무선 Ad-Hoc 상에서의 보안 연구들은 대부분 침입 탐지 시스템(Intrusion Detection System: IDS)의 입장에서 악의적인 침입자를 효과적으로 판별하는 시스템 구조를 구상 및 방법에 그 초점이 맞추어져 왔다. 물론, 침입을 빠르고 정확하게 판별하여 침입을 최소화하는 것이 보안의 가장 중요한 목적이지만, 보안으로 얻고자 하는 궁극적인 목적이 침입에 따른 손해의 최소화 또는 이익의 극대화라는 점을 생각해보면, 침입자와 침입 탐지 시스템 간의 손해와 이익의 상호관계의 측면에서 문제를 바라보는 것이 더 바람직할 것이다.

2에서는 네트워크 상에 적용될 수 있는 게임 이론의 간단한 모형에 대해 설명할 것이고 3에서는 기존에 무선 Ad-Hoc 상의 침입 탐지와 관련된 연구 사례들을 언급할 것이며, 4에서는 연구에서 다루고자 하는 네트워크의 모형 수립 및 분석, 그리고 마지막으로 5에서는 이를 통해 결론을 도출해내고자 한다.

2. 게임 이론 모형

게임 이론은 본래 경제학에서 파생되어 나온 하나의 분야로, 경제적으로 상호관계에 있는 개체들에게 게임의 결과로 초래되는 이해관계를 예상하게 함으로써 가장 최적이라 판단되는 선택을 할 수 있도록 수학적인 근거를 통해 도출한다. 무선 Ad-Hoc 상의 침입 탐지 문제에 있어서도, 침입자와 침입 탐지 시스템을 각각 독립적인 주체라고 본다면, 각자 자신의 이익을 최대화하는 하나의 게임의 형태로 설명이 가능하다. 각 게임의 주체가 선택할 수 있는 전략을 S라고 한다면, 모든 전략의 집합을 $S = \{S_1, S_2, S_3, \cdots S_n\}$으로 표현가능하고, 이것을 침입자와 침입 탐지 시스템에 적용시킨다면, 하나의 침입자와 하나의 침입 탐지 시스템이 있는 모형에서 전략은 다음과 같을 것이다.

$S_{attacker}$ = {침입, 비침입}

S_{IDS} = {공격 탐지, 공격 미탐지}

여기서 전략을 선택하는 기준은 그것을 선택함으로써 받는 이익의 극대화이고 각 개체는 자신의 이익을 최대화하기 위한 선택을 한다는 가정을 포함한다.

여기서 문제를 접근하는 방식은 크게 세 가지로 나누어보기로 한다. 첫 번째는 정보의 공개성 여부로 정보가 일부의 개체에게만 공개되어 있고 다른 개체에게는 알려져 있지 않는 불완전정보게임(Incomplete Information Game)인지, 아니면 모든 개체에게 똑같은 정보가 공유되고 있는 완전정보게임(Complete Information Game)인지에 따라 분류한다. 두 번째는 순서의 여부로 각 개체가 동시에 선택을 하는 동시이동게임(Simultaneous Moving Game)인지, 하나의 또는 몇 개의 개체가 선택을 한 뒤, 다른 개체가 그 선택의 결과를 보고 자신의 선택을 하는 반복 이동게임(Repeated Moving Games)인지에 따라 분류한다. 마지막으로 살펴볼 문제는 선택의 순수성 여부이다. 즉, 각 개체의 선택이 상대방의 어떠한 선택에 대해서도 항상 최적이 되는 해가 존재하는지의 여부로 만약 상대방이 선택하는 전략에 따라 최적의 해가 달라진다면 이 문제는 강열등전략(Strictly dominated strategy)이 존재하지 않는다는 의미이고, 혼합 전략(Mixed strategy)으로 생각해야 한다. 이러한 세 가지 조건으로 볼 때 본 연구의 침입 게임 문제는 이익에 관련된 정보를 침입자와 침임 탐지 시스템 두 객체가 공평하게 공유하는 상태에서 동시에 선택을 하는 경우로 가정하기로 하며, 일반적인 경우의 침입 게임은 강열등 전략이 존재하지 않으므로, 혼합 전략의 측면에서 살펴보기로 한다.

3. 기존 연구 사례

현재까지 게임 이론을 네트워크에 적용한 사례는 많은 경우 대역폭 문제에 집중되어 있고, 네트워크에 게임이론 적용 시 침입자와 침입 탐지 시스템 간의 대립 구조로 보는 것은 거의 공통적으로 같으나 해결하고자 하는 문제의 목적에 있어서는 대역폭 설정, 라우팅(Routing), 가격 정책, 그리고 상호 이익 문제 등 그 종류가 다양하다. 침입 탐지 시스템에 적용하여 연구한 사례의 대부분의 경우도 유선 네트워크에 초점이 맞추어져 있다.

그 중 침입자와 침임 탐지 간의 이익 측면에서 살펴본 연구는 유선 네트워크 상에서 하나의 침입 노드와 하나의 피해 노드를 설정하여 침입이 이루어졌을 때와 그렇지 않은 경우, 그리고 침입 탐지를 하였을 때와 하지 못했을 경우의 2×2 행렬의 형태로 나타낸 것이 기본 형태로, 여기서 얻어낼 수 있는 중요한 결과는 침입자와 침입 탐지 시스템 간의 확률 값이다. 즉, 이 게임에서 두 개체는 각각의 경우에 얻을 수 있는 서로의 이익 값은 알고 있지만, 침입확률과 침입 탐지 확률을 알지 못하는 상태이며, 앞서 언급했다시피 강열등전략이 존재하지 않는 혼합 전략의 문제이기 때문에 상대방의 이익 값을 통해 상대방의 이익이 최대일 때의 확률 값을 유도해낸다. 이 확률 값을 통해 침입 탐지 시스템은 침입 확률 기대치를 얻고

침입자는 침입 탐지 확률 기대치를 얻는다. 하지만 기존의 논문에서는 유선 네트워크의 상황에서 침입 노드가 하나이고 침입 탐지 시스템이 있는 노드 또한 하나인 1-1 유형에서 침입 탐지 시스템의 하위 노드가 1개와 2개일 때까지를 다루었으므로 본 연구에서는 무선 Ad-Hoc 상황에서 하위 노드가 N개일 때까지의 경우로 확장하여 다루기로 한다.

4. 문제 정의 및 분석

4.1 기본 모형

본 연구에서 다루고자 하는 모형은 2계층 구조를 가진 무선 Ad-Hoc이다. 즉, 상위 계층에 있는 노드에 침입 탐지 시스템을 설치하고 하위 계층의 노드들의 침입 탐지를 감시하는 형태로 공격자는 반경 내의 어느 노드 중 하나를 선택하여 공격할 수 있다. 본 연구에서는 하나의 공격 노드와 하나의 피해 노드의 경우로 한정하기로 한다. 이 때 가장 기본적인 경우는 네트워크 상에 하나의 피해 노드와 하나의 공격 노드가 있는 경우이다. 이러한 경우, 상호 이익 행렬은 <표1>과 같이 주어진다.

	A	NA
D	(I_b, A_p)	(I_{pf}, 0)
ND	(I_n, A_n)	(0, 0)

<표1 > 1-1 유형 이익 행렬

여기에서 행은 침입자 전략 집합이고, 열은 침입 탐지 시스템 전략 집합이며, 각 기호의 의미는 다음과 같다.

I_b : 침입시 침입 탐지를 하는 경우, 침입 탐지 시스템이 갖는 이익, 양의 값

I_n : 침입시 침입 탐지를 하지 못하는 경우, 침입 탐지 시스템이 갖는 이익, 음의 값

I_{pf},: 침입이 아닐 때, 침입으로 판단하는 경우, 침입 탐지 시스템이 갖는 이익, 음의 값

A_p : 침입시 침입 탐지를 하는 경우, 침입자가 갖는 이익, 음의 값

A_n : 침입시 침입 탐지를 하지 못하는 경우, 침임자가 갖는 이익, 양의 값

위의 이익 행렬에서 전략의 수를 n, 최적의 전략을 S^*라고 하고 B(S)를 S라는 전략을 선택했을 때의 이익 값이라고 한다면, 다음의 식을 만족하는 S를 S^*라고 한다.

$B(S^*_{attacker}) \geq B(S_{attacker})_i \quad (1 \leq i \leq n)$

$B(S^*_{IDS}) \geq B(S_{IDS})_i \quad (1 \leq i \leq n)$

p를 침입 탐지 시스템이 침입 탐지를 하는 확률, q를 침입자가 침입할 확률이라고 놓는다면, 기존의 논문의 결과와 같이, 다음의 p와 q값을 이익을 최대로 할 때의 각각의 확률 값으로 얻는다.

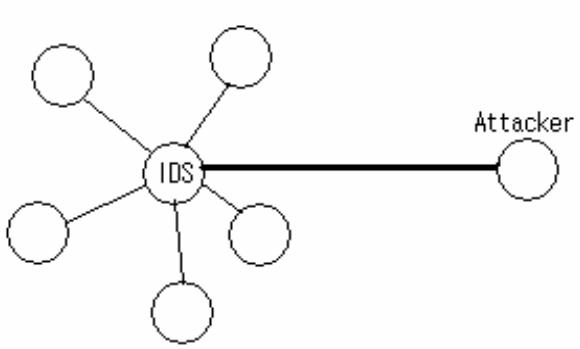
$q^* = I_{pf} / I_{pf} - I_b + I_n$

$p^* = A_n / A_n - A_p$

여기에서 침입자가 침입할 확률은 침입 탐지 시스템이 침입이 아닐 때에 침입으로 헛경보를 울릴 때의 이익과 침입을 침입이 아닌 것으로 판단하여 울리지 않을 때의 이익에서 침입을 정확하게 탐지해 내었을 때의 이익을 뺀 값 중 침입이 아닐 때에 침입으로 헛경보를 울리는 비율로 나타내어지고, 침입 탐지 시스템이 침입 탐지를 할 확률은 침입자가 침입을 성공적으로 하였을 때 얻는 이익에서 침입을 탐지 당하였을 때의 이익을 뺀 값 중 침입을 성공적으로 하였을 때의 이익 값의 비율이라는 것을 알 수 있다. 즉, 각각의 확률 값은 상대방의 이익에 의하여 그 값이 변해간다.

4.2 무선 Ad-Hoc 모형

2계층 구조의 무선 Ad-Hoc 시스템에서 침입 타지 시스템은 상위 계층의 노드에 설치하기로 하자. 이 구조는 여전히 하나의 침입자와 하나의 침입 탐지 시스템으로 이루어진 1-1 대응 구조의 게임이지만, 기본 모형과는 달리 침입 탐지 시스템은 특정한 하위 노드의 침입피해를 다른 하위 노드의 침입 피해로 오탐하는 경우가 발생한다. 이러한 경우를



<그림1> 2계층 무선 Ad-Hoc 네트워크>

I_{nf}로 정의하기로 한다. 또한 이 경우, 침입자가 얻는 이익을 A_b로 하자. 각 경우의 확률 값은 독립적이고 동일한 분포라고 가정하면, 다음과 같은 성질을 만족한다.

$p_1 = p_2 = \cdots = p_n = p$

$q_1 = q_2 = \cdots = q_n = q$

그러면 n개의 하위 노드를 가진 침입 탐지 시스템과 침입자의 이익 관계는 다음과 같이 주어진다.

	A_1	A_P	A_N	NA
D_1	(I_b, A_p)	(I_{nf}, A_b)	(I_{nf}, A_b)	(I_{pf}, 0)
D_P	(I_{nf}, A_b)	(I_b, A_p)	(I_{nf}, A_b)	(I_{pf}, 0)
D_N	(I_{nf}, A_b)	(I_{nf}, A_b)	(I_b, A_p)	(I_{pf}, 0)
ND	(I_n, A_n)	(I_n, A_n)	(I_n, A_n)	(0, 0)

<표2 > n-1 유형 이익 행렬

각자 이익이 최대일 때의 값은 상대방의 확률 값이 최대일 때를 가정으로 구한다. 예를 들어 침입자의 최대 이익은 침입 탐지 시스템의 확률이 최대라는 가정 아래 침임 확률 q의 최대값을 구하는 것으로 아래 식과 같은 형태를 만족시킨다.

$$\sum_{i=1}^{n} q^*(n p^* A_p + (1-np^*) A_b) \geq$$

$$\sum_{i=1}^{n} q(n p^* A_p + (1-np^*) A_b)$$

그리고 침입 탐지 시스템의 경우, 최대 이익 시 침입자가 최대 이익을 어든 다는 가정 하의 침입 탐지 확률 p^*는 아래의 식을 만족시킨다.

$$\{\sum_{i=1}^{n-1} p^*(q^* I_b + nq^* I_{nf} + (1-nq^*) I_{pf})\} + (1-np) nq^* I_n \geq$$

$$\{\sum_{i=1}^{n-1} p(q^* I_b + nq^* I_{nf} + (1-nq^*) I_{pf})\} + (1-np) nq^* I_n$$ 두

식의 함수는 2차 미분시 음의 값을 가지므로, 1차 미분의 값이 이 함수의 최대값이 되고, 따라서 이를 통해 각각의 p와 q값을 구하면 다음과 같다.

$q^*(n) = I_{pf} / nI_{pf} - I_b + nI_n - (n-1)I_{nf}$

$p^*(n) = A_n / nA_n - A_p - (n-1)A_b$

여기서 n은 대역폭의 범위 내에서 가능한 값이며 결과값은 각 주체가 최대 이익을 추구한다는 가정 하에 예상되는 상대방의 확률 값이다.

4.3 결과 분석

각각의 확률들은 상대방의 이익 값에 따라 그 값이 변한다는 특성을 가진다. 침입 탐지 시스템의 입장에서 생각해보면, n, I_{pf}, I_b, I_n, I_{nf}값의 변화에 따라 침입의 확률이 변한다는 것을 알 수 있다. 먼저, n이 증가하면, 전체적인 네트워크의 침입 확률은 다음과 같다.

$q^*(n) = nI_{pf} / nI_{pf} - I_b + nI_n - (n-1)I_{nf}$

$= I_{pf} / I_{pf} - I_b / n + I_n - (n-1)/nI_{nf}$

따라서 만약 $I_b = I_{nf}$라면, n의 변화에 따른 전체적인 네트워크의 침입 확률은 변하지 않지만, $I_b \geq 0$이고, $I_{nf} \leq 0$이므로 같을 확률은 극히 적다. 만약 $I_{nf} << 0$이라면, 분모의 값이 증가하고, 따라서 전체적인 공격 확률은 낮아진다. 침입을 탐지했을 시에 얻는 이익인 I_b은 양의 값으로 증가할수록 전체 네트워크의 침입 확률을 감소시키지만, 1/n이 곱해진 정도기 때문에 큰 영향을 미치지 않는다. 경보를 아예 울리지 않았을 때에 얻는 I_n의 경우, 음의 값으로 증가할수록 전체 네트워크의 확률을 감소시킨다. 이것은 즉,

침입이 발생한 경우에도 침입을 탐지하지 못한 때에 얻는 이익인 I_{pf}는 분자와 분모 모두 영향을 미치기 때문에 음의 값으로 증가할 경우 낮은 비율로 전체 네트워크의 침입 확률을 마찬가지로 감소시킨다. 마지막으로 다른 노드가 공격받은 것으로 오탐을 했을 시에 얻는 이익인 I_{nf}는 음의 값으로

증가할수록 전체 네트워크의 공격 확률을 증가시킨다. 위의 분석 결과로 볼 때, 전체 하위 노드들의 침입 확률이 작기 위해서는 침입 탐지 시스템이 침입을 발견했을 때의 이익이 크거나, 침입이 아닌 경우에 경보를 울리거나 아예 침입 경보를 울리지 않았을 때의 손해가 큰 경우에 이루어진다.

4.4 앞으로의 연구

현 모형에서는 침임 탐지 시스템이 단지 상위 노드에 설치되어 있고, 침입 노드가 하나인 경우를 채택하여 분석해 보았다. 하지만 현재 악의적인 공격 유형으로는 하나의 노드가 여러 노드를 공격하거나 여러 노드가 함께 다른 노드를 공격하는 경우, 여러 노드가 하나의 노드를 공격하는 경우 등 그 종류는 다양하게 나타나고 있으므로 이러한 유형에 따른 분석 또한 의미 있을 것이다. 또한 무선 Ad-hoc의 민감한 특성인 에너지 문제나 라우팅 문제 등을 고려한 게임 이론적 접근 방법도 가능할 것이다.

5. 결론

본 연구는 2계층 무선 Ad-Hoc 네트워크 상에서 하위 노드의 개수를 n으로 확장하였을 때의 침입 노드와 피해 노드 간의 상호 관계를 게임의 측면으로 고찰해 보았다. n이 증가할수록 각각 하위 노드들의 침입 확률은 작아지지만, 전체 하위 노드들의 집합으로 보았을 때 그 확률 값은 침입 탐지 시스템의 상황에 따른 이익에 따라 각기 다른 비율로 침입 확률을 감소 또는 증가시킨다는 것을 알 수 있었다. 또한 동시에 침입 탐지 기대 확률은 침입자의 이익에 따라 그 값이 달라진다는 것도 알 수 있다.

참고문헌

[1] Alpcan, T.; Basar, T, “A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection”, Proceedings of 42nd IEEE Conference on Decision and Control, 2003, Vol. 3, pp 2595 - 2600

[2] Murali Kodialam, Lakshman, T.V, “Detecting network intrusions via sampling: a game theoretic approach: A Game Theoretic Approach”, Proceedings of 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, 2003, Vol. 3, pp 1880 - 1889

[3] Rextin, A.T.; Irfan, Z.; Uzmi, Z.A, “Game Network Play A Game Theoretic Approach to Networks”, Proceedings of the 7th International Symposium on Parallel Architecture, Algorithm and Networks. 2004

[4] Mishra, A.; Nadkarni, K.; Patcha, A., ”Intrusion detection in wireless ad hoc networks”, Wireless Communications, IEEE, Vol. 11, Issue 1, pp 48 - 60

[5] M. Y. Huang, R. J. Jasper, and T. M. Wicks, “A large scale distributed intrusion detection framework based on attack strategy analysis”, in Intl. Symp. on Recent Advanced in Intrusion Detection(RAID), Louvain la Neuve, Belgium, 1998, pp 121-124

[6] Robert Gibbons, *A Primer in Game Theory*, New York, Harvester Wheatscheaf, 1992

[7] T. Basar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd ed. Philadelphia, PA:SIAM, 1999

[8] G. Owen, *Game Theory*, 3rd ed, New York NY:Academic Press, 2001

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

[10] Toh, C.-K., *Ad hoc mobile wireless networks : protocols and systems,* Prentice Hall PTR, c2002