情報保護學會論文誌
第19卷 第1號, 2009. 2

슈타켈버그 게임 기반 Anti-virus 백신 선택 모형*

성시일,† 최인찬‡

고려대학교 정보경영공학부

An Anti-Virus Vaccine Selection Model Based on Stackelberg Game*

Si-il Sung,† In-Chan Choi‡

Division of Information Management Engineering, Korea University

요 약

이 연구는 웹기반 시스템의 운영자와 침해자의 전략과 관계된 정보보안문제를 다룬다. 슈타켈버그 게임상황을 이용하여, 백신 선택 문제의 게임이론적 모형을 제시한다. 이 모형에서 운영자는 잠재적 시스템 침해자에 대응하는 백신조합을 선택하고, 침해자는 운영자의 백신 조합에 가장 효율적으로 침입할 수 있는 방법을 선택한다. 제시된 모형은 운영자의 예산, 시스템 성능 등을 고려한 추가적 현실제약조건을 동시에 고려한다. 더불어, 가정을 적용해 수정된 현실 데이터를 이용하여 2가지 시나리오 분석을 제시한다.

ABSTRACT

This paper deals with an information security problem that involves the strategies of both an attacker and an administrator of a web-based system. A game-theoretic model for the problem, based on an Stackelberg game environment, is presented. In the model, the administrator selects a set of anti-virus vaccines to cope with potential system attackers and the intruder chooses attacking modes that are most effective against the administrator's chosen set of vaccines. Moreover, the model considers a number of practical constraints, such as a budget limit on the vaccine purchase and a limit on the system performance. In addition, two different scenario analyses are provided, based on the results of the proposed model applied to a simulated pseudo-real-world data.

Keywords : Network Security, Stackelberg Game, Game Theory

Ⅰ. 서 론

다양한 종류의 상거래 및 서비스 제공 방식이 온라인 방식으로 변화함에 따라 컴퓨터 네트워크 보안 문제도 증가하는 추세에 있다[1]. 컴퓨터 네트워크 보안 문제 발생의 대표적인 예로써 2006년 9월말 다음(Daum)의 데이터베이스가 해킹당하면서 7만 명 이상의 개인정보가 유출되었으며, 2008년 2월에는 옥션 회원의 60%인 1천만 명 이상의 개인정보가 유출되는 사고도 발생한 바 있다. 또한 최근 GS칼텍스의 고객 정보가 유출되는 사고가 있었다.

이 연구는 특정 목적을 갖고 운영되는 웹기반 시스템

접수일(2008년 10월 16일), 수정일(2008년 12월 23일), 게재확정일(2009년 1월 23일)

* 본 연구는 지식경제부 및 정보통신연구진흥원의 IT신성장 동력핵심기술개발사업의 일환으로 수행하였음. (2007-019-02, 정보투명성 보장형 디지털 포렌식 시스템 개발]

† 주저자, kkk0710@korea.ac.kr

‡ 교신저자, ichoi@korea.ac.kr

의 보안 문제를 다룬다. 특정 목적을 가진 시스템은 공격자들의 여러 가지 공격방법 중에서 특수한 공격방법에 더욱 큰 피해를 입을 수 있다. 예를 들면, 광고 및 홍보 사이트 운영자는 접속자들의 접속을 방해하는 행위에 높은 비용을 지불하고, 중/소규모 전자상거래 사이트들은 가격 변조 행위에 의한 피해에 높은 비용을 지불한다. 따라서 운영자가 운영하는 웹기반 시스템의 특성에 따라 피해가 변동하는 상황을 고려하여 운영자의 개별 상황에 맞는 보안 방법론이 필요하다.

이 연구는 운영자의 보안 시스템 구성 방법으로 백신 선택 문제를 고려한다. 일반적으로 많은 사용자들이 백신간 충돌 문제로 인하여 1개의 백신을 사용하지만, Oberheide, J[11]의 연구를 살펴보면 1개 이상의 백신을 사용하는 경우 악성코드의 검색 성공률이 증가하는 것을 알 수 있다. 이 연구는 백신간 충돌문제를 해결하는 방법으로 백신 사용의 시분할 접근을 고려한다. 단위 시간당 1개의 백신만을 사용하는 시분할 접근을 이용하여 백신간 충돌문제를 방지하는 동시에, 운영자의 특수한 상황을 반영하는 백신 선택 문제를 고려한다. 이러한 백신 선택 문제는 운영자가 먼저 선택하는 특징을 가지는데, 시스템이 존재하지 않으면 공격자가 공격을 할 수 없기에, 시스템 운영자의 상황은 슈타켈버그 상황으로 표현가능하다[6,7]. 슈타켈버그 상황에서 시스템 운영자는 자신이 운영하는 웹기반 시스템의 목적에 부합하는 백신조합을 먼저 선택한다. 이때 백신은 백신 제조사별로 고유의 유전자(genetic)나 휴리스틱 알고리즘을 사용하는 특징을 가지는 점이 잘 알려져 있으며, 악성코드에 대한 검색 성공률과 점유하는 메모리 자원의 크기, 악성코드 탐색 속도, 거짓경보 발생횟수도 차이가 존재하는 점이 알려져 있다[2]. 따라서 이 연구는 백신 선택 문제 해결을 통해 ‘나의 상황에 맞는 백신 조합은 무엇일까’라는 질문의 한 가지 접근방식을 제시한다.

2장에서는 백신 선택 게임을 모형화하며 3장에서는 문제 해결의 접근 방식과 실험결과를 제시한다. 4장에서는 제시한 접근 방식을 이용해 시나리오로 분석하며 5장에서는 연구의 한계점과 추후 연구 방향을 제시한다.

Ⅱ. 문헌 연구

이 연구는 웹기반 시스템 보안문제를 게임이론의 시각에서 접근한다. GS칼텍스의 경우 유출 사고는 내부자에 의해 발생되었으나, 옥션과 다음의 경우는 인터넷을 통한 외부 침해자의 공격에 의해 발생하였다. 외부 침해자 공격의 경우, 침해자와 운영자간의 보호하여야할 데이터를 대상으로 한 게임으로 간주할 수 있다. 게임 시각에서 보안 문제를 접근한 연구는 최근에 시작된 연구로써, Kodialam과 Lakshman[5], Alpcan과 Basar[4], Xia와 Zhang[8], Mavronicolas [9], Lye와 Wing[10] 등의 연구가 있다.

Kodialam과 Lakshman[5]의 연구는 게임모형을 이용해 통신 네트워크에서 감지할 수 있는 악의적 패킷 검출 문제를 다룬다. 공격자의 전략은 악의적 패킷의 검출 확률을 최소화하는 패스 선택이며, 네트워크 운영자의 전략은 탐지기를 설치하는 위치이고. 각 경기자는 악의적 패킷이 검출되는 시간을 보수로 고려한다. Alpcan과 Basar[4]의 연구는 게임모형을 이용해 네트워크 보안과 유저의 접속 용이성 사이의 상충관계를 다룬다. 공격자의 전략은 시스템 공격 유무이고 운영자의 전략은 시스템 보안 수준의 강화나 완화, 유지이다. 이 경우 공격자는 공격성공과 공격탐지로 인한 피해를 보수로 고려하며, 운영자는 공격탐지 성공유무와 거짓 경보를 보수로 고려한다.

Xia와 Zhang[8]의 연구는 게임모형을 이용해, 공격자는 수비자에게 공격을 감행할 것이라고 위협하고 수비자는 이 위협에 대한 최선의 대응을 고려하는 상황을 다룬다. 보수에 대한 구체적 언급보다는 게임모형을 이용해 상황을 고려할 수 있음을 언급하고 있다. Mavronicolas 등의 연구[9]는 게임이론을 기반으로 네트워크를 구성하는 물리적 단말기에 설치하는 탐지설비의 최적 위치선정을 다룬다. 운영자의 전략은 탐지기를 설치하는 단말기의 위치 선택이며, 공격자는 공격을 감행할 단말기의 선택이다. 이 전략을 그래프이론을 사용하여 은행, 기업, 공공 기관의 네트워크 탐지설비의 게임이론적 균형을 제시하고 있다.

Lye와 Wing[10]은 공격자와 네트워크 운영자 사이에서 발생하는 보안 문제를 일반합 확률 게임으로 모형화하고 있다. 실제 네트워크 관리자들에 대한 인터뷰를 통해 공격자의 3개 시나리오를 도출하였고 이를 이용해 전략 선택에 따른 전이확률을 부여한다. 전이확률을 사용함에 따라 시스템 상태 공간이 크게 증가할 수 있다. 마지막으로 공격자와 운영자가 동시에 선택한 전략묶음에 의해 발생되는 결과에 보수를 부여한다. 이와 같은

[표 2] 보수 행렬: 실험 데이터 1번

백신번호	6	7	8	9	10	11	12	13
V	0.82,-1.64	0.98,-1.96	0.68,-1.36	0.82,-1.64	0.45,-0.9	0.4,-0.8	0.72,-1.44	0.80,-1.6
W	2.91-4.85	2.97,-4.95	2.73,-4.55	2.91,-4.85	2.70,-4.5	2.76,-4.6	2.16,-3.6	1.98,-3.3
B	4,-0.8	4.7,-0.94	2.4,-0.48	4,-0.8	2,-0.4	2.15,-0.43	3.35,-0.67	2.5,-0.5
T	4.25,-4.25	4.85,-4.85	3.25,-3.25	4.25,-4.25	2.9,-2.9	3.5,-3.5	3,-3	3.55,-3.55

과정을 통해 게임모형이 구성되고 단계별 상태에서 공격자와 운영자의 전략이 비교된다.

이 연구는 기존의 연구들과는 달리 백신 선택을 통한 운영자의 보안 문제를 다루고자 한다. 기존의 연구들은 Lye와 Wing[10]의 연구를 제외하고 대부분 데이터를 제시하지 않거나 자료 가공 과정을 다루는 수리적 부분이 빠져있다. 이 연구는 이들 연구와 달리, 백신 선택 모형 개발을 위해 자료를 가공한 과정과 운영자의 상황에 맞는 해법절차 개발을 포함하여 다룬다.

Ⅲ. 백신 선택 게임 모형

일반적으로 게임은 게임의 경기자, 경기자가 선택할 수 있는 전략들로 이루어진 전략공간, 그리고 전략선택에 따른 보수행렬로 구성된다[3,6]. 백신 선택 문제를 게임모형으로 구성하기 위해서는 다음과 같은 일반적인 게임 요소와 추가적인 제약을 정의할 필요가 있다. 모형의 경기자는 운영자와 공격자이며, 전략공간으로 공격자는 구분 가능한 공격방법을 전략으로 가지며, 운영자는 백신조합선택을 전략으로 가진다. 공격자와 운영자의 보수행렬은 공격이 성공할 확률에 공격방법별 가치를 곱한 값을 기대이윤(비용)으로 구성된다. 시스템 운영 상황에 현실을 반영하기 위해 이 모형에서는 추가적 제약 조건으로 백신별 탐색속도 하한과 거짓경보발생 횟수의 상한을 고려한다.

- **공격자의 전략공간:** 이 모형에서 다루는 공격자의 공격전략은 윈도우 바이러스, 웜, 백도어, 트로이목마로 조합할 수 있는 공격방법으로 구성된다. 문헌 [1]과 위키피디아(http://www.wikipedia.org)에 의해 각 공격

[표 1] 백신 제조사 및 백신별 특성 (참고문헌 [2])

백신별 특성 / 백신 제조사	백신번호	거짓경보 발생횟수	탐색속도 (MB/sec)	백신별 악성코드 선행탐지력(탐색 성공률, %)			
				바이러스	웜	백도어	트로이안
G-Data	1	8	4.8	0.64	0.05	0.65	0.38
Alwil	2	9	11.1	0.61	0.05	0.62	0.36
GriSoft	3	7	12.2	0.23	0.04	0.37	0.27
Softwin	4	19	11.3	0.41	0.13	0.59	0.50
DoctorWeb	5	35	2.9	0.54	0.05	0.64	0.39
MicroWorld	6	1	2.8	0.18	0.03	0.20	0.15
Fortinet	7	7	47.5	0.02	0.01	0.06	0.03
FriskSoftware	8	36	23.4	0.32	0.09	0.52	0.35
F-Secure	9	1	3.8	0.18	0.03	0.20	0.15
Kasper-sky Lab	10	5	4.9	0.55	0.10	0.60	0.42
McAfee	11	8	11.8	0.60	0.08	0.57	0.30
Microsoft	12	6	10.2	0.28	0.28	0.33	0.40
Norman ASA	13	6	9.4	0.20	0.34	0.50	0.29
Symantec	14	1	22.6	0.35	0.90	0.22	0.23
AEC	15	29	4.3	0.53	0.34	0.76	0.57
AVIRA	16	16	16.7	0.86	0.94	0.86	0.76
ESET	17	29	15.1	0.71	0.96	0.70	0.65

방법은 다음과 같이 정의할 수 있다.

- **바이러스:** 프로그램이나 메모리에 자신 또는 자신의 변형 코드를 복사하여 시스템 지연 또는 마비, 강제 종료 등과 사이트 변조를 일으킨다.
- **웜:** 네트워크에 기생하며 인터넷 접속 속도를 현저히 저하시키며 시스템에 과부하를 일으킨다. 이 연구에서는 분산서비스거부(DDoS)도 이 공격방법으로 간주하며 이는 백신을 통해서 방지할 수 있다.
- **백도어:** 공격자가 원격지에서 조정하며 정보 유출 및 시스템의 통제 권한을 유출시킨다.
- **트로이얀:** 백도어 방식과 유사하지만 공격자가 직접 통제하지 않는다.

• 운영자의 전략공간: 이 모형에서 다루는 운영자의 방어전략은 [표 1]에 제시된 17 종류 백신의 조합으로 구성된다.

• 보수행렬: 운영자와 공격자별 보수행렬을 구성하기 위해 [표 1]의 자료와 4가지 공격방법을 이용한다. 이 연구는 백신 조합(단일 백신 포함)을 하나의 전략으로 고려하여, 하나의 전략이 다른 전략보다 상대적으로 우월한지 판단하여, 조합 집합 안에서 가장 우월한 전략을 제시하는 것을 목적으로 한다. 또한 운영자의 비용과 공격자의 이득은 각 백신과 공격방법에 의해 검색되지 않는 비율에 공격방법 별 가치를 곱한 값을 이용해 구성하므로, 보수행렬은 확률의 특성을 가지기 보다는 기대보수의 특성을 가진다. 이러한 특성은 실험데이터 1을 통해 나타난다.

실험데이터 1은 공격자가 바이러스(V) 공격에 1천만 원, 웜(W) 3천만 원, 백도어(B)와 트로이얀(T)에 5천만 원의 가치를 부여하고 있으며, 운영자는 각각 -2, -5, -1, -5 천만 원의 가치를 부여한 상황을 다룬다. 각 셀의 왼쪽 숫자는 공격자의 보수이며 오른쪽은 운영자의 음의 보수(비용)이다. [표 2]의 자료 중 백신 번호 6을 자세히 살펴보면 다음과 같다. 6번 백신은 MicroWorld사의 백신으로 바이러스 공격 탐색 성공률이 0.18, 웜 0.03, 백도어 0.20, 트로이얀 0.15 이다. 공격자는 백신에 각 공격방법이 탐색되지 않았을 경우 1, 3, 5, 5천만 원의 이득을 얻을 수 있으므로 바이러스 공격을 통해 (1-0.18) X 1 천만 원인 8백 2십만 원을 기대이윤을 얻을 수 있으며 웜 공격은 (1-0.03) X 3 천만 원인 2천 9백 1십만 원의 기대이윤을 얻을 수 있다. 백도어와 트로이얀 역시 같은 방식을 통해 공격자의 기대이윤을 구할 수 있으며, 운영자의 경우 역시 마찬가지이다. 이와 같은 방법을 이용해 공격자와 운영자의 보수행렬을 구성한다.

• 추가 제약: 일반적인 게임모형은 다루지 않지만, 백신의 특성을 고려하기 위해 이 연구는 추가 제약으로써 거짓경보와 악성코드 탐색 속도를 고려한다. 이 모형은 운영자의 전략으로 선택된 백신의 수가 1개일 경우 개별 백신의 자료를 그대로 사용하고, 선택된 백신의 수가 2개 이상일 경우 기대치를 이용하여 거짓경보와 악성코드 탐색 속도를 고려한다.

- **거짓경보 발생 횟수:** 감염되지 않은 파일을 감염된 파일로 판단하여 동작을 막는 횟수로써 경보가 발생하면 시스템 운영 프로그램의 동작을 지연 혹은 멈추게 하는 문제를 야기한다. 따라서 발생할 수 있는 거짓경보 횟수의 상한을 제약조건으로써 고려한다.
- **악성코드 탐색 속도:** 백신이 사용하는 휴리스틱에 따라 탐색 속도가 다르며 MB/sec로 표현되는데 초당 탐색하는 데이터의 양이 많을수록 전체 시스템의 검색에 대한 탐색 시간이 감소한다. 따라서 전체 시스템 자원에 백신이 점유하는 시간이 감소하므로 탐색 속도의 하한을 제약조건으로 고려한다.

이 연구에서 다루는 공격방법별 운영자와 공격자의 보수는 공통지식(common knowledge)이라고 간주한다. 이는 공격자와 운영자는 서로 중시하는 가치와 이와 연관된 전략은 알고 있다는 일반적인 게임이론의 가정이다. 또한 현실적으로 네트워크를 공격하는 공격자는 어떠한 계기를 통해 운영자 집단에 속할 수 있다. 이를 통해 공격자가 중시하는 가치를 운영자가 알 수 있으며, 동시에 역의 관계도 알 수 있다.

모형의 단순화를 위해서 이 연구에서 제시하는 모형은 다음과 같은 가정을 가진다. 공격자들이 하나의 공격전략을 선택하면 다른 공격을 통해 발생되는 상태로 전이하지 않고, 한 가지 상황만 발생한다고 가정한다. 공격자의 공격방법이 각각 독립적이고 구분 가능하다(independent and identical)는 의미로, 예를 들면 백도어 프로그램을 사용하는 전략을 선택하면 시스템 통제는 발

생 가능하더라도 시스템 마비는 발생하지 않게 된다.

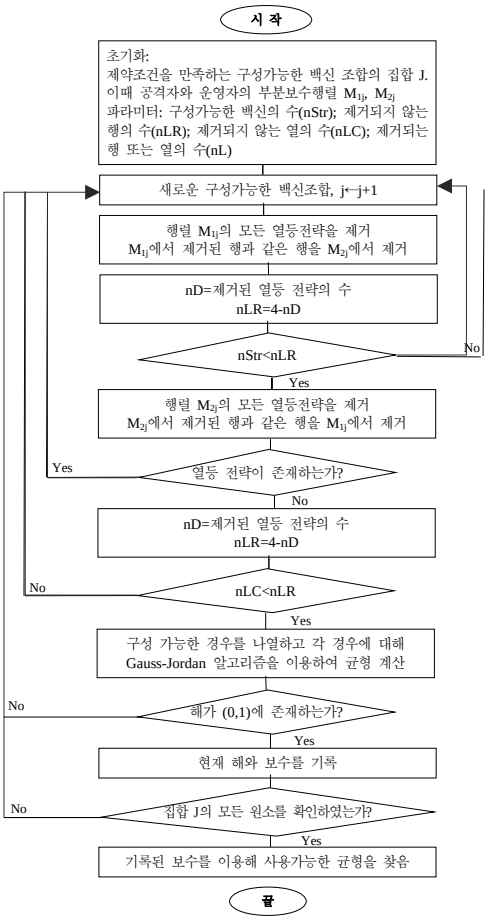
탐색속도와 거짓경보횟수는 제약조건으로써, 이를 만족하는 해를 고려한다. 시스템 자원은 한계가 존재하기에 백신조합의 구성 백신 수가 시스템 자원에 선형으로 영향을 준다고 고려할 수 있다. 운영자의 시스템에 다수의 백신 프로그램이 동시에 상주할 경우 시스템의 속도가 현저히 느려질 수 있고, 백신 간의 거짓경보 교차 발생 가능성이 존재하며, 다수의 백신을 유지/운영할 경우 구입비용 등이 발생하는 점에 기인한다.

Ⅳ. 균형점 탐색절차 및 실험결과

이 연구에서 다루는 슈타켈버그 게임 모형은 일반적인 게임 해법 절차를 통해 균형점을 찾기 어렵다. 따라서 다음과 같은 수정 해법 절차를 사용한다. 우선 하나의 가능한 백신조합을 선택한 후 선택된 백신조합에 대해 공격자의 대응전략을 찾아낸다. 다음으로 운영자의 백신조합이 공격자의 전략에 대응하는 대응전략조건을 만족하는지 검사하고 만족한다면 이를 가능해 집합에 추가하는데, 이는 백신 선택 게임모형이 슈타켈버그 게임 상황이기에 이탈할 유인을 확인하는 과정을 생략할 수 있다. 이렇게 구성된 가능해 집합에서 가장 좋은 보수를 주는 백신조합을 찾는다.

[표 2]의 자료를 이용해 균형점을 찾는 방법의 예제를 살펴보면 다음과 같다. 일단 구성 가능한 백신조합으로 선택된 6, 7번 백신을 선택한다고 가정하자. 이 경우 공격자는 다른 어떠한 전략보다 트로이얀 공격방법을 선택하는 전략이 유리하다. 이에 따라 운영자는 6, 7번 백신을 사용하지 않고 6번 백신만을 사용하게 됨으로써 6, 7번 백신을 사용한다는 가정에 모순이 생기고, 6, 7번 백신은 더 이상 고려하지 않는다.

다음으로 운영자가 8, 12번 백신을 사용한다고 가정하자. 이 경우 공격자는 바이러스와 웜 공격방법은 사용하지 않는다. 일단 바이러스 공격방법은 다른 공격방법보다 기대이윤이 작으므로 쉽게 제거되지만, 웜의 경우는 다르다. 웜 공격방법은 8번 백신을 사용하는 상황에서는 백도어 방식을 사용할 때보다 높은 기대 이윤을 주지만, 백도어와 트로이얀 방식을 혼합해서 사용할 때보다 확실히 기대이윤이 작음을 찾을 수 있다. 따라서 바이러스와 웜 공격방법은 고려하지 않고, 백도어와 트로이얀 공격방법만 고려한다. 백도어와 트로이얀으로



구성된 공격방법과 8, 12번 백신으로 구성된 백신조합이 일반적인 균형 조건을 만족하는지 확인한다. 조건을 만족하는지 확인한 결과, 균형 조건을 만족함을 찾을 수 있고, 그 결과 공격자는 백도어와 트로이얀을 각각 0.57, 0.43의 확률로 사용하고 운영자는 8번, 12번 백신을 각각 0.29, 0.71의 확률로 사용하며 운영자의 기대비용은 -1676만원 임을 계산할 수 있다.

여기서 운영자가 사용할 확률을 자세히 살펴보면 다음과 같다. 운영자는 앞면이 나올 확률이 29%이며 8이 적혀있고 뒷면이 나올 확률이 71%이며 12가 적혀있는 특수한 동전을 매 단위 시간이 시작할 때 던져서 결정된 백신을 해당 단위시간동안 실행한다는 뜻이다.

이러한 방식을 이용하여 가능해 집합의 구성 가능한 백신조합을 모두 확인하고 여기서 가장 작은 기대비용을 찾는다. 이 문제의 최종 결과(제약별 3종류)는 부록

[표 3] 실험결과(공격방법 별 동일 보수행렬)

해의 크기	공격자 전략선택 비율(%)	공격자 보수	운영자 전략선택 비율(%)	운영자 보수
3*3	V:0.03,W:0.32,B:0.65	561	2:0.44,13;0.16,14:0.40	-561*
3*3	V:0.08,W:0.29,B:0.63	571	11:0.44,13:0.20,14:0.36	-571
2*2	V:0.65,B:0.35	695	13:0.31,14:0.69	-695

의 실험데이터 1번에 서 찾아볼 수 있다. 이러한 접근방법은 [그림 1]을 통해 살펴볼 수 있다.

공격방법에 따른 공격자와 운영자의 이윤 및 비용을 전부 같은 1천만 원을 주고 보수행렬을 구한 후 거짓경보 상한 6과 탐색속도하한 15로 실험한 결과는 [표 3]과 같다.

운영자는 2번, 13번 및 14번 백신을 단위시간당 각각 44%, 16%, 40%의 비율로 조합하여 구성하는 방법이 사용 가능한 구성임을 살펴 볼 수 있다. 단위 시간당 44%의 비율로 2번 백신을, 16%의 비율로 13번 백신을, 마지막으로 40%의 확률로 14번 백신을 실행하는 방법으로 위 균형점을 시스템에 적용할 수 있다. 이 방법은 판교 신도시 인터넷청약이 시행될 때 한국정보보호진흥원에서 웹사이트를 2분 단위로 모니터링하고 악성코드 탐색을 1시간 단위로 하였다는 기록이 있기에[1], 이 문헌을 바탕으로 단위 시간당 시행 횟수의 비율로 해석할 수 있다.

Ⅴ. 시나리오별 결과 분석

첫 번째 시나리오는 홍보 및 광고용 시스템을 운영하는 상황을 다룬다. 이 시스템의 운영자는 접속자의 접속을 힘들게 하여 광고효과를 감소시키는 네트워크 지연과 제품 및 광고 내용의 신뢰성을 손상시키는 사이트 변조의 위험을 가진다. 운영자는 다른 공격방법보다 웜에 의한 네트워크 지연과 윈도우 바이러스에 의한 사이트 변조 피해를 중시한다고 생각할 수 있다. 따라서 운영자는 윈도우 바이러스와 웜에 대한 비용 5천만 원, 백도어 및 트로이얀 방식에 의한 비용 1천만 원의 기대비용을 부여한다. 반면 공격자는 윈도우 바이러스를 통한 사이트 변조에 3천만 원, 네트워크 지연에 2천만 원, 나머지 공격방법에는 1천만 원의 기대이익을 부여한다. 거짓 경보 상한 12, 탐색속도 하한 6의 제약조건하에서 이 연구에서 제안한 균형점 탐색절차를 이용한 결과는 [표 4]와 같다.

[표 4] 부록 실험 3의 예제 10번 전체 결과

해의 크기	공격자 전략선택 및 비율(%)	공격자 보수	운영자 전략선택 및 비율(%)	운영자 보수
2*2	V:0.75 W:0.25	1358	1:0.68 14:0.32	-2550*
2*2	V:0.77 W:0.23	1400	2:0.71 14:0.29	-2606

이 시나리오에서는 ‘GriSoft’ 제품군과 ‘SYMANTEC’ 제품군을 68%와 32%의 비율로 조합하여 사용하는 백신조합을 제안한다.

하지만 운영자가 임의의 백신을 사용한다면 다음과 같은 결과도 발생할 수 있다. 운영자가 위의 상황에서 임의로 백신 7번, 8번으로 시스템을 구성한다고 하자. 이 상황은 [표 5]의 게임 보수행렬로 구성됨을 알 수 있다. 이 경우 균형점은 (V, 8)로 나타나게 된다. 운영자가 7과 8의 백신을 조합하는 방법은 공격자가 바이러스 공격방법만 사용하게 유도하므로, 이 백신조합을 사용하는 의미가 없어진다. 동시에 운영자는 여기서 제시한 백신조합의 보수보다 낮은 -3400의 보수를 받게 됨을 알 수 있다. 따라서 임의의 백신조합이 아닌, 이 연구에서 제안하는 방법을 이용하여 보안시스템을 구성하는 방법이 효율적임을 살펴볼 수 있다.

[표 5] - 7,8번 백신 조합에 따른 보수행렬

	7	8
V	2.94,-4.90	2.04,-3.40
W	1.98,-4.95	1.82,-4.55
B	0.94,-0.94	0.48,-0.48
T	0.97,-0.97	0.65,-0.65

두 번째 시나리오는 정부관련 웹 시스템을 운영하는 상황을 다룬다. 운영자는 자료유출을 가장 중요시하며 네트워크 지연과 시스템 통제권 상실도 중요하게 생각한다. 이와 달리 공격자는 정보 유출과 네트워크 지연을 통해 국가 신뢰도를 낮추려는 목적을 가지고 있다고 생각할 수 있다. 따라서 운영자는 네트워크 지연 피해 4천만 원, 시스템 통제권 상실 4천만 원, 자료유출 5천만 원,

[표 6] 부록 실험 3의 예제 10번 전체 결과

해의 크기	공격자 전략선택 및 비율(%)	공격자 보수	운영자 전략선택 및 비율(%)	운영자 보수
2*2	V:0.92,W:0.08	2150	1:0.39,14:0.61	-630*
2*2	V:0.93,W:0.07	2187	2:0.40,14:0.60	-632
2*2	V:0.94,B:0.06	2250	10:0.44,14:0.56	-635
2*2	V:0.93,W:0.07	2188	11:0.41,12:0.59	-632
2*2	W:0.30,B:0.70	758	11:0.06,14:0.94	-2306
2*2	W:0.10,T:0.90	2222	11:0.42,14:0.58	-3517
3*3	V:0.79,W:0.07,T:0.14	2205	4:0.03,11:0.39,14:0.58	-1064
3*3	V:0.80,W:0.07,T:0.13	2204	5:0.07,11:0.34,14:0.59	-1036
3*3	V:0.44,W:0.08,T:0.48	2217	8:0.03,11:0.39,14:0.58	-2157
3*3	V:0.87,W:0.07,T:0.06	2198	10:0.07,11:0.35,14:0.58	-832
3*3	V:0.64,W:0.08,T:0.28	2212	11:0.40,12:0.03,14:0.57	-1535
3*3	V:0.14,W:0.09,T:0.77	2221	11:0.40,13:0.03,14:0.57	-3067

사이트 변조 1천만 원의 기대비용을 부여하고, 공격자는 네트워크 지연에 5천만 원, 자료 유출 4천만 원, 사이트 변조 3천만 원, 시스템 통제 1천만 원의 기대이익을 부여한다. 거짓경보상한 6, 탐색속도 하한 12의 제약조건 하에서 이 연구에서 제안한 균형점 탐색절차를 이용한 결과는 [표 6]과 같다. 이 시나리오에서는 'G-DATA' 제품군과 'SYMANTEC' 제품군을 39%와 61%의 비율로 조합하여 사용하는 백신조합을 제안한다.

마지막으로 시나리오로 해석할 수 있는 공격방법별 보수를 무작위 발생시켜 실험을 진행하였다. 공격방법별 보수를 무작위 발생시킨 이유는 현실에서 발생할 수 있는 다양한 상황을 편향되지 않게 입력하여 실험 결과를 살펴보기 위함이다. 이렇게 무작위로 발생시킨 40개의 공격방법 별 보수를 이 연구에서 제안한 균형점 탐색절차를 이용해 백신조합을 계산하였다. 실험은 제약조건이 없는 상태(거짓경보 상한: ∞, 탐색속도 하한: 0)부터 시작하여 거짓경보상한 12, 탐색속도하한 6인 상태와 거짓경보상한 6, 탐색속도하한 12인 상태로 진행하였다.(공격방법별 보수는 공격자와 운영자별로 엑셀 랜덤함수를 사용하여 발생시켰음) 실험결과는 부록의 실험 1, 2, 3에 제시하고 있으며, 무작위 발생시킨 보수 중 10개씩 표현하고 있다.

Ⅵ. 결론 및 향후 연구 방향

이 논문은 슈타켈버그 상황에 기반한 Anti-virus 백신 선택 게임모형과 제안된 모형의 균형점 탐색절차를 다루고 있다. 또한, 제시된 모형과 절차를 사용하여 운영자가 자신의 상황에 적용 가능한 맞춤형 백신조합 운영전략을 제안하고, 모형에 사용된 모수의 변화에 따른 두 가지 가능한 시나리오 분석을 제공하였다.

추후 진행될 수 있는 후속 연구주제로는 주요 가정이 완화된 모형의 개발을 생각할 수 있다. 예를 들면, 제안한 모형은 게임모형 문헌에서 통상 사용되는 완전정보를 가정하고 있으나, 이러한 가정이 적용될 수 없는 현실 경우도 다수 존재한다. 공격자와 운영자가 각자의 기대이익과 자신의 전략에 대한 상대의 대응전략을 서로 알고 있다고 가정할 수 없는 경우에는 보수행렬이 확률적으로 변하는 확률게임모형을 고려할 필요가 있다. 다음으로 운영자가 백신만이 아닌 여러 종류의 보안 제품을 조합하여 사용하는 보안문제를 구성할 수 있다. 여러 종류의 보안 제품을 이용한 보안 모형은 백신만이 아니라 스파이웨어, 방화벽 등 다양한 종류의 보안 제품의 조합을 가리킨다. 향후 이러한 방향으로 연구를 확장하기 위해, 알고리즘의 개발과 다양한 보안 제품에 대한 관련 자료의 수집이 필요하다. 더불어, 다양한 수준의 공격자를 다룰 수 있는 게임 상황의 방법론 등에 대한 연구가 추가적으로 필요하다.

참고문헌

[1] 김우한, 심원태, 노명선, 최중섭, 허창열, "정보시스템 해킹, 바이러스 현황 및 대응," 한국정보보

호진홍원, 2006년 12월.

[2] A. Clementi, “Anti-Virus comparative, No.11,” AV comparatives, Aug. 2006.

[3] R. Aumann and S. Hart, Handbook of Game Theory with Economic Application, ELSEVIER, vol. 3, pp. 1723-1797, Jan. 2002.

[4] T. Alpcan and T. Basar, “A game theoretic approach to decision and analysis in network intrusion detection,” Decision and Control, vol. 42, no. 3, pp. 2595-2600, Dec. 2003.

[5] M. Kodialam and V. Lakshman, “Detecting Network Intrusions via Sampling: A Game Theoretic Approach,” IEEE INFOCOM 2003, vol. 3, pp. 1880-1889, Mar. 2003.

[6] D. Fudenberg and J. Tirole, Game Theory, MIT Press, pp. 1-63, Feb. 1991.

[7] R. Myerson, Game Theory: Analysis of Conflict, Harvard Press, Nov. 1991.

[8] X. You and Z. Shiyong, “A Kind of network security behavior model Based on game theory,” Parallel and Distributed Computing, Applications and Technologies, pp. 950-954, Aug. 2003.

[9] M. Mavronicolas, V. Papadopoulou, A. Philippou and P. Spirakis, “A Graph -Theoretic Network Security Game,” International Journal of Autonomous and Adaptive Communications Systems, vol. 1, no. 4, pp. 390-410, May 2008.

[10] K. Lye and J. Wing, “Game strategies in network security,” International Journal of Information Security, vol. 4, no. 1-2, pp. 71-86. Feb. 2005.

[11] J. Oberheide, E. Cooke and F. Jahanian, “Rethinking Antivirus: Executable Analysis in the Network Cloud,” Proceedings of the 2nd USENIX Work shop on Hot Topics in Security, pp. 1-11, Aug. 2007.

[실험 1] 거짓경보 상한: ∞, 탐색속도 하한: 0

예제 번호	공격자 전략선택 및 비율(%)	공격자 보수 (단위:만원)	운영자 전략선택 및 비율(%)	운영자 보수 (단위:만원)	균형점 갯수	공격자의 공격방법별 가치 (단위: 천만 원)				운영자의 공격방법별 가치 (단위: 천만 원)			
						V	W	B	T	V	W	B	T
1	W:0.09,B:0.91	2299	4:0.87,14:0.13	-755	12	1	3	5	5	2	5	1	5
2	V:0.55,W:0.47,B:0.02	1370	1:0.32,14:0.12,15:0.55	-1845	56	3	2	4	1	5	2	5	1
3	V:0.34,T:0.66	1199	1:0.83,4:0.17	-1593	16	3	1	2	2	3	2	1	3
4	V:0.11,W:0.11,T:0.85	2409	10:0.85,12:0.03,14:0.11	-1471	70	5	3	1	4	5	4	4	2
5	W:0.38,T:0.62	2584	14:0.26,15:0.74	-2068	18	4	5	2	5	3	4	3	4
6	W:0.55,T:0.45	2361	14:0.12,15:0.88	-750	18	1	4	1	5	2	1	1	2
7	T:1.00	1200	16:1.00	-720	1	4	1	1	5	3	2	4	3
8	V:0.14,W:0.06,T:0.90	1837	1:0.36,5:0.50,12:0.14	-1302	59	4	2	3	3	5	2	4	2
9	W:0.03,T:0.97	2915	11:0.59,14:0.41	-1506	11	1	5	3	4	1	5	3	2
10	V:0.92,W:0.08	2150	1:0.39,14:0.61	-630	15	4	5	1	3	1	4	4	5

[실험 2] 거짓경보 상한: 12, 탐색속도 하한: 6

예제 번호	공격자 전략선택 및 비율(%)	공격자 보수 (단위:만원)	운영자 전략선택 및 비율(%)	운영자 보수 (단위:만원)	균형점 갯수	공격자의 공격방법별 가치 (단위: 천만 원)				운영자의 공격방법별 가치 (단위: 천만 원)			
						V	W	B	T	V	W	B	T
1	B:0.24,T:0.76	3021	1:0.21,12:0.79	-2445	5	1	3	5	5	2	5	1	5
2	V:0.19,W:0.53,B:0.46	1689	4:0.33,10:0.48,13:0.19	-1898	19	3	2	4	1	5	2	5	1
3	V:0.41,T:0.59	1245	2:0.88,4:0.13	-1611	6	3	1	2	2	3	2	1	3
4	V:0.11,W:0.11,T:0.85	2409	10:0.85,12:0.03,14:0.11	-1471	39	5	3	1	4	5	4	4	2
5	W:0.22,T:0.78	3129	12:0.85,14:0.15	-2503	14	4	5	2	5	3	4	3	4
6	W:0.57,T:0.43	2945	4:0.11,12:0.89	-926	11	1	4	1	5	2	1	1	2
7	.	.	.	.	.	4	1	1	5	3	2	4	3
8	V:0.05,W:0.24,T:0.60	1772	1:0.65,4:0.30,14:0.05	-1488	19	4	2	3	3	5	2	4	2
9	W:0.12,T:0.88	2515	4:0.52,14:0.48	-1412	8	1	5	3	4	1	5	3	2
10	V:0.92,W:0.08	2150	1:0.39,14:0.61	-630	13	4	5	1	3	1	4	4	5

[실험 3] 거짓경보 상한: 6, 탐색속도 하한: 12

예제 번호	공격자 전략선택 및 비율(%)	공격자 보수 (단위:만원)	운영자 전략선택 및 비율(%)	운영자 보수 (단위:만원)	균형점 갯수	공격자의 공격방법별 가치 (단위: 천만 원)				운영자의 공격방법 가치 (단위: 천만원)			
						V	W	B	T	V	W	B	T
1	.	.	.	.	.	1	3	5	5	2	5	1	5
2	V:0.65,B:0.35	2285	13:0.75,14:0.25	-3477	1	3	2	4	1	5	2	5	1
3	.	.	.	.	.	3	1	2	2	3	2	1	3
4	W:0.34,B:0.66	711	1:0.16,14:0.84	-2206	3	5	3	1	4	5	4	4	2
5	W:0.04,T:0.96	3701	3:0.74,14:0.26	-2961	2	4	5	2	5	3	4	3	4
6	.	.	.	.	.	1	4	1	5	2	1	1	2
7	.	.	.	.	.	4	1	1	5	3	2	4	3
8	.	.	.	.	.	4	2	3	3	5	2	4	2
9	W:0.10,T:0.90	2616	12:0.68,14:0.32	-1437	6	1	5	3	4	1	5	3	2
10	V:0.92,W:0.08	2150	1:0.39,14:0.61	-630	12	4	5	1	3	1	4	4	5

공격자와 운영자의 확률 및 이득은 소수점 셋째 자리에서 반올림한 값.
N: 윈도우 바이러스, W: 웜, B: 백도어, T: 트로이얀.

<著者紹介>

사 진

최 인 찬 (In-Chan Choi) 정회원
1990년 10월: 컬럼비아대학 IE/OR Ph.D
1996년 3월~현재: 고려대학교 정보경영공학부 교수
<관심분야> 시스템 최적화 이론 및 응용

성 시 일 (Si-il Sung) 학생회원
2007년 2월: 고려대학교 산업시스템정보공학과 학사
2007년 3월~현재: 고려대학교 정보경영공학과 석사과정
<관심분야> 최적화 이론, 게임이론, 정보보안