마코프 프로세스에 기반한 확률적 피해 파급 모델
(A Probabilistic Model of Damage Propagation based on the Markov Process)

김 영 갑 † 백 영 교 †† 인 호 ††† 백 두 권 †††
(Young-Gab Kim) (Youngkyo Baek) (Hoh Peter In) (Doo-Kwon Baik)

요 약 급속한 인터넷 기술의 발전으로 기업이나 기관에서의 업무 처리는 인터넷 기반 기술에 의존하고 있다. 또한 주요 정보통신 시설의 네트워크 의존도와 결합도가 증가함에 따라 시스템내의 취약성을 대상으로 하는 침해 행위와 같은 사이버 보안 사고의 수가 크게 증가하고 있다. 이에 따라 개인정보는 물론 컴퓨터 자원들의 침해와 관련된 피해 파급(damage propagation)에 관한 연구가 요구된다. 그러나 기존의 제안된 모델들은 위험 관리 측면의 방법론적인 접근이거나, 바이러스(virus)나 웜(worm) 같은 특정 위협(threats)에 대해서만 적용할 수 있는 연구가 진행되어 왔다. 따라서 본 논문에서는 과거의 위협 발생 데이타를 근거로 하여 전체 시스템이 가지고 있는 다양한 위협들에 대해 적용 가능한 마코프 프로세스(markov process)에 기반한 피해 파급 모델을 제시한다. 이를 통하여 각 위협별 발생 확률 및 발생 빈도를 예측할 수 있다.

키워드 : 마코프 프로세스(Markov Process), 위험 산정, 피해 파급, 사이버 공격

Abstract With rapid development of Internet technology, business management in an organization or an enterprise depends on Internet-based technology for the most part. Furthermore, as dependency and cohesiveness of network in the communication facilities are increasing, cyber attacks have been increased against vulnerable resource in the information system. Hence, to protect private information and computer resource, research for damage propagation is required in this situation. However the proposed traditional models present just mechanism for risk management, or are able to be applied to the specified threats such as virus or worm. Therefore, we propose the probabilistic model of damage propagation based on the Markov process, which can be applied to diverse threats in the information systems. Using the proposed model in this paper, we can predict the occurrence probability and occurrence frequency for each threats in the entire system.

Key words : Markov Process, Risk Estimation, Damage Propagation, Cyber Attack

1. 서 론

최근 급속한 인터넷 기술의 발전으로 기업이나 기관에서의 업무 처리는 인터넷 기반 기술에 의존하고 있다. 또한 주요정보통신 시설의 네트워크 의존도와 결합도가 증가함에 따라 시스템내의 취약성을 대상으로 침해 행위와 같은 사이버 보안 사고의 수가 크게 증가하고 있다. 이에 따라 개인정보는 물론 컴퓨터 자원들의 침해와 관련된 위험 분석(risk analysis) 및 피해 파급(damage propagation)에 관한 연구가 요구된다.

정확한 위험 분석은 적절한 보안 대응책 선정을 가능하게 하고 결과적으로 위험 발생 가능성을 크게 감소시켜 차후에 실제적으로 발생될 수 있는 보안 사고의 피해규모를 크게 감소시킨다. 이와 같은 위험 분석은 보안 사고를 사전에 예방하기 위해 의미가 크고, 실제적으로 많은 연구가 진행되어 왔다[1-3]. 이에 반해, 피해 파급에 대한 개념은 아직 정립되지 않았으며, 기존의 피해 파급 모델은 현재의 IT 환경에 대한 사고 유형들의 특성을 적절히 반영하기에 부적절하다. 즉, 기존의 제안된 피해 파급 모델들은 바이러스(virus)나 웜(worm)

· 이 논문은 2006년도 두뇌한국 21사업에 의하여 지원되었음
† 학생회원 : 고려대학교 컴퓨터학과
always@korea.ac.kr
†† 학생회원 : 고려대학교 수학과
ykbaek@korea.ac.kr
††† 종신회원 : 고려대학교 컴퓨터학과 교수
hoh_in@korea.ac.kr
baikdk@korea.ac.kr
(Corresponding author임)
논문접수 : 2005년 9월 13일
심사완료 : 2006년 5월 18일

같은 특정 위협(threats)에 대한 피해 파급 모델을 제시[4-7]하여 전체 시스템이 가지고 있는 다양한 위협에 대해 적용하기 힘들다. 또한 위협이 발생 하였을 때 생성되는 위협 영역에 대하여 위협들 사이의 관계 또는 시간적인 요소에 의한 분석이 힘들다. 피해 파급 영역(damage propagation area)은 위협의 종류나 위협들 사이의 연관 관계에 따라 달라지므로 피해 파급 모델은 이러한 요구사항을 만족해야 한다. 따라서 본 논문에서는 과거의 위협 발생 데이타를 근거로 하여 정보 시스템이 가지고 있는 위협들 사이의 상호 관계 및 시간의 흐름에 따라 피해 파급을 종합적으로 예측 및 분석할 수 있는 마코프 프로세스(markov porcess)[8,9] 기반의 확률적 피해 파급 모델을 제안한다. 본 논문에서 제안하는 피해 파급 모델을 통하여 주요 위협들에 대해 사전에 위협 발생 확률 및 위협 발생 빈도를 예측하고 피해 파급 정도에 따른 위협 대책 수립에 활용할 수 있다. 또한 각 위협간의 상관관계를 분석하는데도 적용 가능하다. 지난 연구[10,11]에서도 마코프 프로세스 기반의 피해 파급 모델을 제시하였지만, [10]에서는 모델의 구성 요소 및 개념적인 측면을 강조한 반면 세부 절차에 대해서는 언급하지 않았다. 또한 [11]에서는 피해 파급 모델을 위한 세부 절차를 정의하고 간단한 적용사례만을 보여주었다. 본 논문에서는 피해 파급 모델을 구축하기 위해 세부 절차를 명확히 정의하고 신뢰성 있는 데이타를 이용하여 다양한 적용 사례를 제시한다. 또한 위협간의 관계 정도(밀접성)를 분석하기 위한 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 마코프 프로세스와 피해 파급과 관련된 기존의 방법론들에 대해서 살펴보고, 3장에서는 확률적 피해 파급 모델 설계의 접근 방법에 대하여 기술한다. 4장에서는 마코프 프로세스에 기반한 확률적 피해 파급 모델을 제시하고 세부 절차에 대하여 설명한다. 5장에서는 제안된 모델을 이용하여 실제 적용되는 사례를 보여주고 6장에서는 결론 및 향후 연구에 대한 내용을 기술한다.

2. 연구 배경 및 관련 연구

2.1 마코프 프로세스(Markov process)

본 절에서는, 논문에서 제시하는 피해 파급 모델을 설계하기 위해 적용되는 마코프 프로세스에 대해 설명한다[8,9]. 마코프 프로세스는 상태간 전이가 오로지 이전 n개의 상태에 의존하여 이루어지는 프로세스를 말한다. 이 때 이 모델을 n차원 모델이라 하는데 n은 다음 상태를 결정하는데 영향을 미치는 상태의 개수를 말한다. 과거의 상태를 기억하지 않는다는 점에서 비기억 프로세스(memoryless process)라고도 한다. 마코프 프로세스를 $X(t)$라 하면 임의의 시간 $t_1 < t_2 < \cdots < t_k < t_{k+1}$에 대해 $X(t)$가 이산값이면

$$P[a < X(t_{k+1}) = x_{k+1} | X(t_k) = x_k, \cdots, X(t_1) = x_1]$$

$$= P[X(t_{k+1}) = x_{k+1} | X(t_k) = x_k]$$

이고 $X(t)$가 연속값이면

$$P[a < X(t_{k+1}) \le b | X(t_k) = x_k, \cdots, X(t_1) = x_1]$$

$$= P[a < X(t_{k+1}) \le b | X(t_k) = x_k]$$

로 마코프 성질이 기술된다. 위의 식에서 t_k는 현재, t_{k+1}은 미래, 그리고 $t_1, \cdots, t_{k-1}$은 과거의 시점이다. 마코프 프로세서의 값이 이산값이면 마코프 체인(markov chain)이라고 한다. 마코프 체인은 t가 이산적이냐 연속적이냐에 따라 이산시간 마코프 프로세스(discrete-time markov provess), 연속시간 마코프 프로세스(continuous-time markov chain)로 나뉜다.

마코프 프로세스는 다음의 세 가지로 설명될 수 있는 모든 시스템을 말한다.:

- 상태 집합(set of state) : 가능한 상태들의 집합 - 예, sunny, cloudy, rainy
- π 벡터(초기 확률) : 시스템의 초기화 확률 벡터
- 상태 전이 행렬(state transition matrix) : 각 상태간 전이 확률

본 논문에서는 마코프 프로세스의 세 가지 구성요소를 정의함으로써 피해 파급 모델을 설계하고 적용하였다.

2.2 웜 전파 모델

전파 모델(Epidemic Model)[12,13]은 특정 모집단 내에서 발병원이 발생 한다 가정하고 시간변화에 따라 감염된 개체와 감염에 노출된 개체, 치유되는 개체들 간의 개체수 관계를 설명하기 위한 모델이다. 이를 통하여 실제 네트워크상의 웜이 전파되는 확산력을 설명할 수 있다.

기본적으로 네트워크상에서 발생 가능한 전파 특성을 지니는 위협들의 피해 확산력을 설명하기 위하여 생물학적 고전모델인, 고전단순전파모델(Classical Simple Epidemic Model)을 사용하고 있다. 그 중에서 가장 범용적으로 사용되는 모델이 바로 Kermack-Mckendrick 모델(또는 전통적 SIR 전파모델)이다[12-14]. 이 모델에서는 웜에 의해 변화하는 호스트의 상태를 S(Susceptible), I(Infectious), R(Removed) 세 가지로 나누고 있어 SIR 모델이라고도 부른다. 웜에 노출된 호스트는 최초에 웜에 취약한 상태(S)를 띠고 웜에 걸리게 되면 감염된 상태(I)로 변한다. 그리고 마지막으로 감염된 호스트가 웜을 치료 하거나 웜의 기능을 완전 상실케 되는 상태(R)로 전환된다.

SIRS 모델은 기존의 SIR모델을 개량한 전파 모델이다[15]. 즉, 일반적인 경우는 시간에 따른 감염된 호스트

I(t), 감염에 노출된 호스트 S(t), 그리고 제거되는 호스트 R(t)를 생각하였는데, SIRS 모델에서는 S → I → R 단계 이후에 다시 해당 호스트가 감염될 수 있다는 사실을 가정하였다. 즉, 감염에 노출된 호스트에서 감염이 발생되면서 일정 시간 후 제거과정을 통해 완전 제거가 아닌, 다시 감염될 수 있는 호스트의 상태를 추가한 것이다.

마지막으로, 기존의 SIR, SIRS 모델에 포함되지 않았던 요소 2가지를 추가하여 TWO Factor Model을 제안하였다[13,16]. 이는 코드레드 사고 이후 새롭게 제안된 모델이다. 이 모델은 인간의 대응책과 감소되는 감염율을 고려하였다. 웜의 관점에서, 인간의 대응책은 어떤 호스트들을 웜 확산 유통으로부터 제거한다. 제거되는 호스트들은 감염된 호스트 및 여전히 취약한 호스트들을 모두 포함한다.

지금까지 살펴본 것과 같이 피해 파급 모델은 웜과 바이러스와 같은 특정 위협에 국한되어 연구되어져 왔기에 전체 시스템이 가질 수 있는 다양한 위협들에 적용 가능한 새로운 피해 파급 모델이 요구된다. 본 논문에서는 마코프 프로세스에 기반한 확률적 피해 파급 모델을 통하여 이러한 요구사항을 만족하고 있다.

3. 확률적 피해 파급 모델 설계의 접근 방법

마코프 프로세스 기반의 확률적 피해 파급 모델은, 독립 또는 단일 시스템의 피해로 인하여 그 시스템과 관련된 전체 시스템에 영향을 주는 정도를 확률적 접근방법으로 예측하는 것을 말한다. 전체 시스템이 가지고 있는 피해 파급 모형과 피해 파급 속도는 시간의 흐름, 또는 위협의 종류에 따라 달라질 수 있다. 마코프 프로세스에 기반한 피해 파급 모델은 전체 시스템에서 주요 위협들에 대한 위협 전이 확률 및 위협 발생확률을 마코프 프로세스를 이용하여 설명한다. 그림 1은 위협의 종류(T_1, T_2, T_3,...,T_8)에 따른 피해 파급 모형 나타낸다.

그림 1에서 볼 수 있듯이, 피해 파급 모형은 위협의 종류, 위협들 사이의 관계 및 위협 행위에 대한 대응책에 의해 다양한 형태를 이룰 수 있다. 본 논문에서 제안하는 마코프 프로세스에 기반한 피해 파급 모델은 다양한 위협들에 적용 가능할 뿐만 아니라 이들 사이의 상호 관계 정도(밀접도)를 바탕으로 그림 1과 같은 다양한 형태의 피해 파급 영역에 대하여 적용할 수 있다. 이를 위해서 확률적 피해 파급 모델은 몇 가지 요구 사항을 만족해야 한다. 첫째, 시간에 따른 피해 파급 영역을 고려해야 한다. 즉, 기관이나 사용자들은 시간의 흐름에 따라 위협에 대한 패치(patch) 또는 업그레이드(upgrade)를 취할 수 있기 때문에 이에 의하여 피해 파급 영역이 바뀔 수 있다. 둘째, 피해 파급 속도는 위협 및 취약점의 종류에 따라 달라질 수 있으므로, 피해 파급 모델은 다양한 종류의 위협에 적용될 수 있도록 설계해야 한다.

위에서 언급한 요구사항을 만족하는 마코프 프로세스에 기반한 피해 파급 모델을 설계하기 위해서는 몇 가지 가정이 필요하다. 첫째, 위협과 관련된 과거의 데이타가 충분하고 신뢰할 만하다. 마코프 프로세스를 이용하여 모델을 설계하기 위해서는 신뢰할 만한 과거 데이타이 수집이 무엇보다도 중요하다. 둘째, 정보 자산(asset)의 피해 파급은 이산 시간(discrete time)에 의해 확산된다. 즉, 생물체 바이러스의 확산과는 달리 이산 시간 또는 특정 이벤트에 의해 확산된다. 이것은 정보통신 시설의 자산이 완전히 피해를 받았을 경우에만 이것과 관련된 자산에게 피해를 전파한다는 것을 의미한다. 셋째, 전체 시스템은 하나 이상의 정의된 위협을 가지고 있다. 즉, 피해 파급 모델은 정의된 위협에 대한 전체 시스템의 피해 산정 및 피해 파급 효과를 구할 수 있어야 한다. 넷째, 기관이나 사용자들은 시간의 흐름에 따라 위협에 대한 대책을 수립, 적용할 수 있다. 이에 따라 피해 파급 영역은 증가 또는 감소 될 수 있다. 마지막으로, 마코프 프로세스 전이 확률은 전체 시스템의 위협 상태에 적용되는 확률이다. 따라서 하나 이상의 위협 상태에 대해 적용할 수 있다. 마코프 프로세스에 기반한 피해 파급 모델은 앞서 설명한 마코프 프로세스의

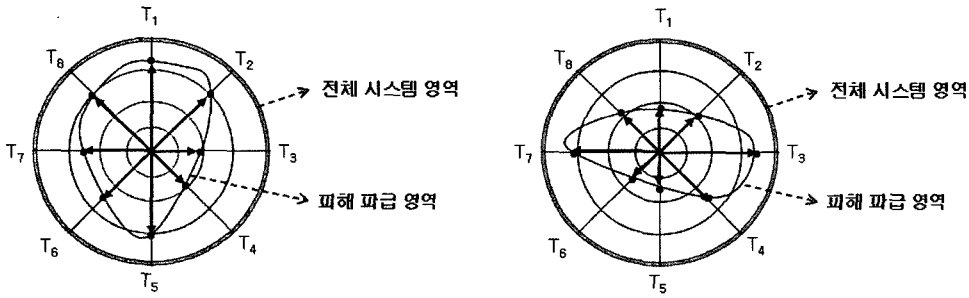

그림 1 피해 파급 모형의 다양성

요소, 즉, 상태 집합, π 벡터, 전이확률을 정의함으로써 이루어진다.

본 논문에서는 피해 파급에 대한 전체 시스템의 피해 손실을 정량적으로 표현하기 위해서 식 (1)을 이용한다.

$$RISK(s, t) = Loss(s, t) \times Prob.(s, t) \quad (1)$$

식 (1)에서 RISK는 자산의 취약한 부분에 위협 요소가 발생하여 자산의 손실, 손상이 일어났을 때의 손실액(피해 산정액)을 의미하고, 공간(s, scope)과 시간(t, time) 개념을 함께 고려하였다. 공간은 피해 파급 시스템의 크기 즉, 특정 이벤트 후의 피해 영역의 확산 및 감소를 계산해 주기 위한 영역 개념이다. 시간 t는 시간 경과에 따른 피해 파급의 정도를 고려하기 위한 요소로서 일정한 시간 또는 특정 이벤트에 의한 피해 영역의 모양 및 크기가 변경되는 것을 적용하기 위한 것이다. 즉, 피해 파급 손실액은 자산이 특정한 위협의 발생에 의해 자산의 하락하는 정도(Loss)와 위협이 발생할 확률(Prob.)에 의해 계산되며, 본 논문에서는 피해 파급 확률(Prob.)을 구하는 것에 중점을 두었다.

4. 마코프 프로세스에 기반한 확률적 피해 파급 제안 모델

본 장에서는 마코프 프로세스에 기반한 피해 파급 모델에 대하여 단계별 프로세스를 정의한다. 본 논문에서 제안한 마코프 프로세스에 기반한 확률적 피해 파급 모델은 그림 2와 같은 과정을 거쳐 생성되며, 크게 4 단계(상태집합의 정의, 위협상태 전이행렬, 초기 확률, 위협 예측)로 이루어진다.

'상태집합의 정의'단계에서는 조직이나 기관이 가지고 있는 위협들이 취할 수 있는 상태를 정의한다. 상태(state)란 주요 정보통신 기반 시설이 가지고 있는 위협의 상태를 말하며, 상태집합은 하나의 위협 상태가 가질 수 있는 값들의 범위를 나타내거나, 여러 위협 상태들의 쌍(조합)이 될 수 있다. '위협 상태 전이 행렬'에서는 상태집합에서 정의된 위협 상태와 위협 발생 빈도 데이타를 이용하여 위협 상태들 간의 전이 행렬을 구한다. '초기 확률(π 벡터)'에서는 정의된 각 위협 상태가 초기 상태에 발생할 수 있는 확률을 구한다. '위협 예측'단계에서는 전 단계에서 구한 위협 상태 전이행렬과 초기 확률 값을 통해 앞으로 발생할 위협 발생 확률이나 빈도수를 예측할 수 있다. 각 단계에 대한 세부 절차는 다음 절에서 설명한다.

4.1 상태 집합의 정의

'상태 집합의 정의' 단계에서는 주요 정보통신 기반 시설이 가지고 있는 위협의 종류를 조사하고 위협 발생 데이타를 수집, 분석하여 전체 시스템이 가질 수 있는 위협 상태 집합을 정의한다. 상태집합의 정의는 그림 3과 같은 세부 절차를 따른다.

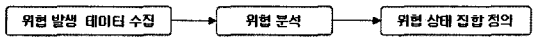

그림 3 상태 집합 정의 단계의 세부 절차

'위협 발생 데이타 수집' 절차에서는 조직이나 기관이 가지고 있는 과거의 위협 발생 데이타를 수집하는 단계이다. 마코프 프로세스 기반의 피해 파급 모델은 이러한 과거의 데이타가 다른 요소들보다 높은 비중을 차지하기 때문에 신뢰성 있고 대용량의 데이타 수집이 무엇보다 중요하다. 본 논문에서는 한국정보보호진흥원(Korea Information Security Agency, KISA)에서 2001년 1월부터 2005년 6월까지 보고된 해킹바이러스 통계 및 분석 월보[16]를 분석, 이용하여 데이타에 대한 신뢰를 얻으려 하였다.

'위협 분석' 절차는 자산의 가치에 악영향을 줄 수 있는 잠재적인 위협을 파악하고 발생 가능성 등을 파악하는 단계로 피해를 산출하는데 있어서 중요한 과정이다. 위협 분석은 크게 위협 파악과 위협 순위 산정으로 구성된다. 위협 파악은 위협을 유형별로 분류, 조사하고 각 위협의 주기를 산출한다. 본 논문에서의 위협 유형은 한국정보보호진흥원의 보고서를 토대로 하여, 크게 해킹, 바이러스, 스캔탐지로 구분하였다. 위협 순위는 파악된 위협 주기를 바탕으로 위협의 심각성에 따라 가장 고려해야 될 위협 순위를 결정한다. 이는 조직에 대해 가장 많은 영향을 줄 수 있는 위협의 중요도를 정하여 조직에 피해를 줄 수 있는 위협을 우선적으로 고려하여 보다 효과적인 대책을 마련하기 위해 필요하다. 이를 통해 마코프 프로세스 기반의 피해 파급 모델에 우선적으로 적용해야 할 위협을 결정한다. 위협 순위는 다음과 같은 기준에 의해 정할 수 있다.

• 위협 주기(위협 발생수)

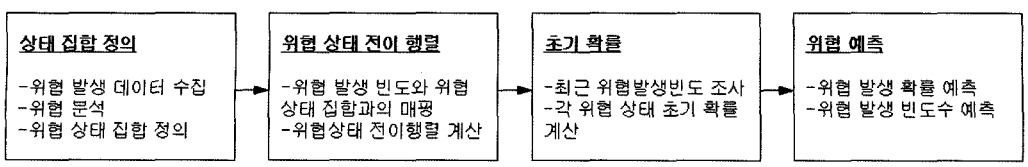

그림 2 확률적 피해 파급 모델 생성 절차

• 델파이에 의한 전문가 의견(위협의 중요도)

• 주요 자산에 의한 매핑된 위협(자산의 정성가치)

본 논문에서는 한국정보보호진흥원 보고된 해킹바이러스 통계 및 분석 월보를 이용하여 각 위협 유형별 위협 주기를 분석하여 대표적인 위협을 선택하였다.

'위협 상태 집합 정의'절차에서는 위협 주기를 분석하여 위협 발생수의 적절한 임계값(threshold)을 결정하여 위협 상태를 정의한다. 위협 상태 집합은 '위협이 독립적으로 발생하는가?' 또는 '위협이 위협들 사이에 서로 연관성을 가지고 발생하는가?'에 따라 정의하는 방법이 다르다. 전자의 경우, 위협 상태 집합은 하나의 위협이 가질 수 있는 임계값 범위가 집합이 된다. 반면, 후자의 경우에는 여러 위협들의 임계값 범위의 조합으로 상태 집합이 정의된다. 그래서 각 위협 주기의 임계값을 얼마나 세분화하여 설정하느냐에 따라 위협 상태의 수와 복잡도가 다르게 되며, 또한 전이 행렬이 가지는 요소(element)의 수 및 복잡도도 달라진다. 즉, 각 위협들의 임계값 범위를 세분화 할수록 생성되는 위협 상태집합이 커지며, 이에 따라 복잡도도 증가하게 된다.

4.2 위협 상태 전이 행렬

'위협 상태 전이 행렬'단계는 '상태 집합 정의' 단계에서 정의된 위협 상태들 간의 전이 확률을 구하는 단계이다. 분석된 각 위협별 발생 빈도수와 전 단계에서 정의된 상태 집합과의 매핑을 통해 위협 상태 전이 행렬을 구한다. 위협 상태 전이 행렬을 구하기 위해서는 그림 4와 같이 2가지의 세부 절차를 수행한다.

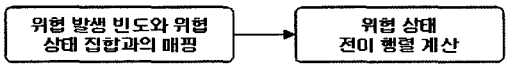

그림 4 위협 상태 전이 행렬 단계의 세부 절차

첫째, 각 위협별 발생 빈도 데이타를 위협 상태 집합과 매핑(mapping)하여 상태들을 열거한다. 둘째, 열거된 상태들을 분석하여 하나의 위협 상태에서 다른 상태로의 전이 횟수를 구하고 이를 이용하여 전이 행렬을 구한다.

'위협 상태 전이 행렬'단계는 '상태 집합 정의'단계와 마찬가지로, 위협들이 서로 독립적으로 발생하여 각 위협별 상태 전이 행렬을 구하는 경우와, 여러 위협들이 서로 연관되어 만들어지는 경우로 나눌 수 있다. 위협들이 서로 독립적으로 발생하여 만들어지는 위협 상태 전이 행렬은 복잡도가 작아 위협 발생 빈도와 정의된 상태 집합과의 매핑을 통해 쉽게 생성할 수 있다. 반면에 여러 위협들이 서로 연관되어 만들어지는 경우의 전이 행렬은 연관된 위협의 종류가 많을수록, 또한 각 위협별 정의된 상태의 개수에 따라 전이 행렬의 크기 및 복잡도가 커지게 된다. 복잡도를 적절하게 만들기 위해서는 상태 집합 정의 단계에서 각 위협별 적절한 임계값 범위를 설정하여 적당한 개수의 위협 상태를 정의해야 한다. 본 논문의 적용 사례에서는 두 가지의 경우로 나누어 설명하였다.

위협 상태 전이 행렬단계에서 생성되는 상태 전이 행렬 P를 나타내면 (2)과 같고 조건 (3)을 만족한다.

$$P=\begin{pmatrix} P_{11} & P_{12} & P_{13} & \cdots & \cdots & P_{1n} \\ P_{21} & P_{22} & P_{23} & \cdots & \cdots & P_{2n} \\ P_{31} & P_{32} & P_{33} & \cdots & \cdots & P_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & P_{ij} & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ P_{n1} & P_{n2} & P_{n3} & \cdots & \cdots & P_{nn} \end{pmatrix} \quad (2)$$

$$\sum_{j=1}^{n} P_{1j}=1,\ \sum_{j=1}^{n} P_{2j}=1,\ \sum_{j=1}^{n} P_{3j}=1,\ \cdots,\ \sum_{j=1}^{n} P_{nj}=1$$

$$\text{즉, } P_{ij}\geq 0,\ \sum_{j=1}^{n} P_{ij}=1,\ i=1,\ 2,\ \ldots,\ n \quad (3)$$

. 각 열(row)은 하나의 위협 상태에서 다른 위협 상태로의 확률을 나타내고, 각 행의 합은 1이 되어야 한다.

4.3 초기 확률(π 벡터)

'초기 확률(π 벡터)'단계는 전체 시스템에서 정의된 각 위협 상태가 초기 상태에 가질 수 있는 위협 발생 확률로써 그림 5와 같은 세부 절차를 따른다.

그림 5 초기 확률 단계의 세부 절차

위협 상태의 초기 확률값을 구하기 위해서, 우선 구하고자 하는 위협의 최근 발생 데이타를 조사한다. 초기 확률을 구하기 위한 최근의 위협 발생 데이타는 3개월, 6개월, 9개월, 1년 등의 시간 단위로 이용한다. 최근의 위협 발생 데이타를 분석하여 각 위협 상태별 발생 빈도 및 초기 확률을 (4)와 같이 계산하며 조건 (5)을 만족한다.

$$P(S_1\ \ S_2\ \ \cdots\ \ S_k\ \cdots\ \ S_n)=P\left(\frac{\alpha}{F}\ \ \frac{\beta}{F}\cdots\frac{\gamma}{F}\cdots\frac{\delta}{F}\right) \quad (4)$$

단, α, β, γ, δ 는 각 상태(S_1, S_2, S_k, S_n)에서의 발생 횟수

$$F=\sum_{i=1}^{n} f_i=\alpha+\beta+\ldots+\gamma+\ldots+\delta \quad (5)$$

또한 초기 위협 확률의 총 합은 1이 되어야 하므로 식 (6)을 만족한다.

$$\sum_{i=1}^{N} P(S_i)=1 \text{ (S는 위협 상태)} \quad (6)$$

4.4 위협 예측

'위협 예측' 단계는 전 단계에서 생성된 위협 상태 전이행렬과 초기 확률 값을 이용하여 앞으로 발생할 위협 발생 확률이나 빈도수를 예측한다. 크게 그림 6과 같은 세부 절차를 수행된다.

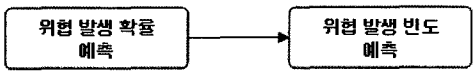

그림 6 위협 예측 단계의 세부 절차

위협 발생 빈도를 예측하기 위해서 임계값의 중간값(median)을 대표값으로 이용하게 되며 이에 대한 적용은 적용 사례에서 볼 수 있다. 그림 7은 위협 상태 전이 행렬 식 (2)와 초기 확률 식 (4)를 이용하여 위협 발생 확률을 구하는 것을 보여준다. 또한 식 (7)과 같이 여러 위협 상태 중 특정 위협 상태에 대한 발생 확률을 구할 수 있다.

$$P(S_k)' = \sum_{i=1}^{n} P(S_i) P_{ik} \qquad (7)$$

(S :위협 상태, k : 특정 위협 상태)

단, n = 위협 발생 상태집합이 개수, $P(S_i)$ = 각 위협 상태의 초기 발생 확률, $P(S_i)'$ = 각 위협 상태의 다음 발생 확률

위협 발생 확률과 각 상태의 중간값을 이용하여 (8)과 같은 예상 위협 발생 빈도를 구할 수 있다.

$$\text{예상 위협 발생 빈도} = \sum_{i=1}^{n} P(S_i)\, M(S_i) \qquad (8)$$

단, n = 위협 상태 집합의 개수, $P(S_i)$ = 각 위협 상태의 발생 확률, $M(S_i)$ = 각 위협 상태의 중간값

5. 적용 사례

앞서 언급하였듯이 본 논문의 적용 사례는 한국정보보호진흥원에서 2001년 1월부터 2005년 6월까지 보고된 해킹바이러스 통계 및 분석 월보에 보고된 데이타를 이용하였다. 우선 상태 집합의 정의 단계에서 위협 발생 데이타를 수집하고 수집된 데이타를 분석하여 위협 유형을 분류하고 위협 순위를 산정한다. 위협 유형은 크게, 해킹, 바이러스, 스캔탐지로 나누었고 각 유형별 대표적인 위협과 월별 발생수는 표 1, 2, 3과 같다.

- T_1 : 해킹 (악성 프로그램을 이용한 통신망에 대한 불법적인 침입)

해킹 위협 유형 중 T_1은 Netbus, Subseven처럼 악성 프로그램을 이용한 공격과 함께 시스템의 취약점을 자동으로 공격하는 프로그램을 이용한 '통신망에 대한 불법적인 침입' 위협이다. 이 위협은 사용자의 시스템에 설치되어 백도어를 오픈하여 정보를 유출하거나 시스템의 정상적인 동작을 방해하는 위협으로써 발생하기 쉬운 해킹 위협이다.

- T_2 : 바이러스 (인터넷 웜)

T_2는 '인터넷 웜'으로써 바이러스 위협 유형 중 하나로, 독립적으로 자기 복제를 실행하여 번식하는 빠른 전파력을 가진 컴퓨터 프로그램 또는 실행 가능한 프로그램으로 인한 위협이다. 최근 들어 이러한 인터넷 웜에 대한 위협 발생이 많이 발생하고 있으며, 이에 대한 피해 파급 정도도 많이 연구되고 있다.

- T_3 : 스캔탐지 (네트워크 도청 및 감청)

T_3는 스캔탐지 위협 유형의 한 종류로, 대상 시스템의 운영체제, 설정 등을 알아보기 위하여 스캔하는 등의 행위로 주로 해킹의 사전 단계로 이용되는 '네트워크 도

$$(P(S_1)\ P(S_2)...P(S_k)...\ P(S_n)) \begin{pmatrix} P_{11} & P_{12} & P_{13} & \cdots & \cdots & P_{1n} \\ P_{21} & P_{22} & P_{23} & \cdots & \cdots & P_{2n} \\ P_{31} & P_{32} & P_{33} & \cdots & \cdots & P_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & P_{ij} & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ P_{n1} & P_{n2} & P_{n3} & \cdots & \cdots & P_{nn} \end{pmatrix} = (P(S_1)'\ P(S_2)'..P(S_k)'\ ..P(S_n)')$$

그림 7 피해 파급 확률의 계산

표 1 T_1의 월별 발생수 및 통계

	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	총계
2001년	85	125	70	89	85	64	65	495	268	77	51	97	1,571
2002년	401	119	82	59	286	417	313	298	210	465	472	990	4,112
2003년	1148	557	1132	934	306	450	185	544	119	137	129	96	5,837
2004년	154	148	118	1066	493	181	72	22	16	24	125	90	2,509
2005년	29	20	15	3	15	36							118
평균	363.4	193.8	283.4	430.2	237.0	229.6	158.7	339.7	153.2	175.7	194.2	318.2	

표 2 T_2의 월별 발생수 및 통계

	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	총계
2001년	1	1529	2429	625	684	520	6106	5965	10772	4795	4068	3024	17,859
2002년	2005	1384	1306	3165	2760	1774	1706	1458	1610	3566	3028	1684	25,446
2003년	1361	1320	2537	2350	3704	1854	1185	9748	19682	3999	11658	8949	68,347
2004년	4824	5750	9820	4233	19728	22767	15228	8132	3153	2658	2319	2117	100,727
2005년	1832	1205	1049	648	1302	1040							7,076
평균	2,004	2,237	3,428	2,204	5,635	5,591	6,056	6,325	8,804	3,754	5,268	3,943	

표 3 T_3의 월별 발생수 및 통계

	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	총계
2002년	1665	1256	2080	2110	1776	1418	1177	1216	1601	2483	1596	1597	20335
2003년	648	593	656	402	345	1489	469	1168	3120	3560	2201	315	14966
2004년	2004	3389	10631	18546	11618	833	1591	1964	901	1794	2628	1381	57217
평균	1,439	1,746	4,455	7,019	4,579	1,246	1,079	1,449	1,874	2,612	2,141	1,097	

청 및 감청' 위협이다.

위의 위협들과 발생 빈도를 분석한 다음 적절한 임계값을 설정하여 위협 상태를 정의한다. 상태 집합을 정의하기 전에, 각 위협이 서로 독립적으로 발생하는 경우와 서로 연관성을 가지고 발생하는 경우로 나누어 설명한다.

5.1 각 위협이 독립적으로 발생하는 경우

본 절에서는 각 위협이 서로 독립적으로 발생하여 다른 위협들과 연관 관계가 없는 경우의 적용 사례를 보여준다. 따라서 주요 정보통신 기반 시스템이 가지고 있는 각 위협별 서로 다른 위협 상태 전이 행렬을 가지게 된다. 단, 위협이 발생할 때마다 각 위협은 동일한 조건에서 발생한다고 가정한다. 예를 들어, 위협에 대한 보안 대응책, 시스템 자원 및 동일한 환경을 가지고 있다.

우선, 위협 T_1(악성 프로그램을 이용한 통신망에 대한 불법적인 침입)에 대한 상태 집합을 정의한다. T_1에 대한 월별 발생 빈도수는 표 1과 같으며 (9)와 같은 임계값의 범위로 상태 집합(S) (10)을 정의한다. 본 논문에서 임계값은 위협의 단위 시간(월별) 발생 빈도를 몇 개의 구간으로 나누어 표현한다.

- S의 임계값의 범위:

S_1 : 0~300, S_2 : 301~600, S_3 : 601~900, S_4 : 901~1200 (9)

- $S = \{S_1, S_2, S_3, S_4\}$ (10)

(9),(10)에서 볼 수 있듯이, 위협이 독립적으로 발생하는 경우에는 상태집합이 단지 해당 위협의 임계값 범위에 의해 결정된다. 다음으로, 2001년 1월부터 2005년 6월까지 월별 위협 발생수를 정의된 상태집합(S)과 매핑하여 상태를 열거한다.

$S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_2, S_1, S_1, S_1, S_1, S_2, S_1, S_1, S_1, S_1, S_2, S_2, S_1, S_1, S_2, S_2, S_4, S_4, S_2, S_4, S_4, S_2, S_2, S_1, S_2, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_4, S_2, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1$

열거된 상태들로부터 각 상태(S_1, S_2, S_3, S_4)에서 다른 상태로의 전이 횟수를 구하고 이를 바탕으로 (2)와 같은 형태의 상태전이행렬 (11)을 구한다.

$$\begin{array}{c} \\ S_1 \\ S_2 \\ S_3 \\ S_4 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} S_1 & S_2 & S_3 & S_4 \end{array} \\ \begin{pmatrix} 31 & 5 & 0 & 1 \\ 6 & 3 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 2 \end{pmatrix} \end{array} \qquad \begin{array}{c} \\ S_1 \\ S_2 \\ S_3 \\ S_4 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} S_1 & S_2 & S_3 & S_4 \end{array} \\ \begin{pmatrix} 0.84 & 0.13 & 0 & 0.03 \\ 0.55 & 0.27 & 0 & 0.18 \\ 0 & 0 & 0 & 0 \\ 0 & 0.60 & 0 & 0.40 \end{pmatrix} \end{array} \tag{11}$$

상태 전이 행렬 (11)로부터, 각 위협에서 다른 위협으로의 전이 확률 값의 합이 1이 되어 식 (3)을 만족한다. 또한 위 위협 상태 전이 확률을 상태 다이어그램으로 나타내면 그림 8과 같다.

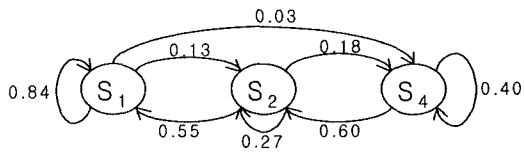

그림 8 위협 T_1에 대한 위협 상태 다이어그램

5.1절의 예에서는 T_1에 대한 전이 행렬을 구하는 과정을 보였으며, 다른 위협들도 위와 같은 과정을 거쳐 각 위협별 상태 전이 행렬을 구할 수 있다.

본 논문에서는 위협 T_1에 대한 초기 확률을 구하기 위해 최근 6개월(표 1의 2005년 1월~6월) 동안 발생한 빈도수를 이용한다. 앞서 제시한 식 (4)를 이용하여 최근 6개월 동안 발생한 빈도수와 이에 따른 초기 확률 값을 구하면 (12)와 같다.

- 빈도수 : 29, 20, 15, 3, 15, 36 = S_1, S_1, S_1, S_1, S_1, S_1
- 초기 확률 : $P(S_1\ S_2\ S_3\ S_4) = P(1\ 0\ 0\ 0)$ (12)

위협 상태 전이 행렬 (11)과 초기 확률 (12)를 이용하여 다음에 발생하게 될 위협 발생 확률을 예측하고 또한 위협 발생 빈도수를 예측할 수 있다. 즉, 위협 발생

확률은 (13)과 같이 계산할 수 있다.

$$(1\ 0\ 0\ 0)\begin{pmatrix}0.84 & 0.13 & 0 & 0.03\\ 0.55 & 0.27 & 0 & 0.18\\ 0 & 0 & 0 & 0\\ 0 & 0.60 & 0 & 0.40\end{pmatrix}=(0.84\ \ 0.13\ \ 0\ \ 0.03)\quad(13)$$

결과 (13)부터 T_1은 다음 달 S_1 상태로 0.84, S_2 상태로 0.13, S_4 상태로 0.03의 확률로 발생할 것이라고 예측할 수 있다. 즉, 0과 300 사이의 발생빈도를 가질 것이라는 것을 알 수 있다. 좀더 구체적인 다음 달의 위협 발생 빈도를 구하기 위해서 식 (8)을 이용한다. 이를 위해 위협 발생 확률 (13)과 각 임계값의 중간값을 이용한다. 본 적용사례에서는 중간값을 구하기 위해 전달의 위협 발생빈도를 이용하였다. 앞서 정의한 임계값의 범위에 따라 중간값을 구하면 다음과 같다.

• $M(S_1)=36$, $M(S_2)=0$, $M(S_3)=0$, $M(S_4)=0$

또한 각 위협상태에 대한 발생확률은 (13)으로부터 얻을 수 있다.

• $P(S_1)=0.84$, $P(S_2)=0.13$, $P(S_3)=0$, $P(S_4)=0.03$

따라서 위협 발생 빈도는 식 (8)에서 n=4 일 때, 즉 위협 상태의 개수가 4개일 때 이므로 아래와 같이 구한다.

• 예상 위협 발생 빈도 $= \sum_{i=1}^{4} P(S_i)\ M(S_i)$

$= 0.84 \times 36$

$\fallingdotseq 30$

위 결과로부터 다음 달 T_1이 발생할 빈도수는 약 30으로 예측할 수 있다. 또 다른 위협 T_2와 T_3의 경우도 위와 같은 방식으로 각각의 위협 발생 확률 및 빈도를 구할 수 있다.

5.2 위협들이 서로 연관되어 발생하는 경우

각각의 상태가 서로 독립적이지 않고 서로 연관되어 발생되는 경우에 이들 위협들 사이의 관계를 반영하기 위해서 위협 상태들의 쌍(조합)으로 처리한다. 본 절에서는 이에 대한 예를 들기 위해, T_1(악성 프로그램을 이용한 통신망에 대한 불법적인 침입)과 T_2(인터넷 웜)에 관련된 위협상태 전이행렬을 구한다. 5.1절의 예와 마찬가지로, 각 위협이 발생할 때마다, 전체 시스템은 모든 동일한 조건을 가진다고 가정한다. 즉, 동일한 시스템 자원 및 환경을 가지고 있다.

T_1, T_2에 대한 월별 발생 빈도수는 표 1, 2와 같으며 각 위협에 대하여 아래와 같은 임계값의 범위를 정의한다.

• T_1의 임계값:

H_1: 0~400, H_2: 401~800, H_3: 801~1200 (14)

• T_2의 임계값:

W_1: 0~4000, W_2: 4001~8000, W_3: 8001 이상 (15)

위협 상태 집합은 T_1과 T_2의 임계값의 쌍을 조합하여 총 9개의 상태가 정의된다. 즉, 위협 상태의 집합은 (16)과 같다.

• $S = \{ S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8, S_9\}$ (16)

단, $S_1 = (H_1, W_1)$, $S_2 = (H_1, W_2)$, $S_3 = (H_1, W_3)$, $S_4 = (H_2, W_1)$, $S_5 = (H_2, W_2)$, $S_6 = (H_2, W_3)$, $S_7 = (H_3, W_1)$, $S_8 = (H_3, W_2)$, $S_9 = (H_3, W_3)$

위협상태 전이행렬을 구하기 위해, 2001년 1월부터 2005년 6월까지 T_1, T_2의 월별 위협 발생 데이타를 이용하여 각 달의 T_1, T_2 의 위협 발생수 쌍 (T_1, T_2)을 정리한다.

(85, 1), (125, 1529), (70, 2429), (89, 625), (85, 684), (64, 520), (65, 6106), (495, 5965), (268, 10772), (77, 4795), (51, 4068), (97, 3024), ... 중간 생략 ..., (29, 1832), (20, 1205), (15, 1049), (3, 648), (15, 1302), (36, 1040)

위의 (T_1, T_2) 쌍을 각 위협의 임계값(T_1, T_2의 임계값) 범위에 맞추어 (H_i, W_j) 쌍을 구한다.

(H_1, W_1), (H_1, W_1), (H_1, W_1), (H_1, W_1), (H_1, W_1), (H_1, W_1), (H_1, W_2), (H_2, W_2), (H_1, W_3), (H_1, W_2), (H_1, W_2), (H_1, W_1), ... 중간 생략 ..., (H_1, W_1), (H_1, W_1), (H_1, W_1), (H_1, W_1), (H_1, W_1), (H_1, W_1)

각 (H_i, W_j) 쌍을 정의된 위협상태집합 (16)과 매핑하여 상태를 열거한다.

$S_1, S_1, S_1, S_1, S_1, S_1, S_2, S_5, S_3, S_2, S_2, S_1, S_4, S_1, S_1, S_1, S_1, S_4, S_1, S_1, S_1, S_4, S_4, S_7, S_7, S_4, S_7, S_7, S_1, S_4, S_1, S_6, S_3, S_1, S_3, S_3, S_2, S_2, S_4, S_2, S_6, S_3, S_3, S_3, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1$

열거된 위협 상태들로부터 각 상태(S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8, S_9)에서 다른 상태로의 전이 횟수를 구하고 이를 바탕으로 전이행렬을 구하면 (17)과 같다.

$$\begin{array}{c} \\ S_1\\ S_2\\ S_3\\ S_4\\ S_5\\ S_6\\ S_7\\ S_8\\ S_9\end{array}\begin{array}{c}\begin{array}{ccccccccc} S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_7 & S_8 & S_9\end{array}\\ \begin{pmatrix}19 & 1 & 1 & 4 & 0 & 1 & 0 & 0 & 0\\ 1 & 2 & 0 & 1 & 1 & 1 & 0 & 0 & 0\\ 2 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 0\\ 3 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix}\end{array}$$

$$\begin{array}{c} \\ S_1\\ S_2\\ S_3\\ S_4\\ S_5\\ S_6\\ S_7\\ S_8\\ S_9\end{array}\begin{array}{c}\begin{array}{ccccccccc} S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_7 & S_8 & S_9\end{array}\\ \begin{pmatrix}0.73 & 0.04 & 0.04 & 0.15 & 0 & 0.04 & 0 & 0 & 0\\ 0.17 & 0.32 & 0 & 0.17 & 0.17 & 0.17 & 0 & 0 & 0\\ 0.29 & 0.29 & 0.42 & 0 & 0 & 0 & 0 & 0 & 0\\ 0.50 & 0.17 & 0 & 0.17 & 0 & 0 & 0.16 & 0 & 0\\ 0 & 0 & 1.00 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1.00 & 0 & 0 & 0 & 0 & 0 & 0\\ 0.25 & 0 & 0 & 0.25 & 0 & 0 & 0.50 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix}\end{array} \quad (17)$$

상태 전이행렬 (17)로부터, 각 상태에서 다른 상태로의 전이 확률 값의 합이 1이 됨을 알 수 있다. 즉, 조건 (3)을 만족한다. 또한 위협상태 전이확률을 상태 다이어그램으로 나타내면 그림 9와 같다.

T_1,T_2에 대한 위협 상태의 초기 확률을 구하기 위해 최근 1년(표 1, 2의 2004년 7월~2005년 6월) 동안 발생한 빈도수를 이용한다. 최근 1년 동안 발생한 T_1, T_2의 빈도수 쌍과 이에 따른 초기 확률 값은 식 (4)에 의하여 (18)과 같이 계산한다.

- 빈도수: (72, 15228), (22, 8132), (16, 3153), (24, 2658), (125, 2319), (90, 2117), (29, 1832), (20, 1205), (15, 1049), (3, 648), (15, 1302), (36, 1040) = S_3, S_3, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1, S_1
- 초기 확률: $P(S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7\ S_8\ S_9)$

$$= P(0.83\ 0\ 0.17\ 0\ 0\ 0\ 0\ 0\ 0) \quad (18)$$

위협상태 전이행렬 (17)과 초기 확률 (18)을 이용하여 다음에 발생하게 될 위협 발생 확률을 예측하고 또한 위협 발생 빈도수를 예측할 수 있다.

$$(0.83\ 0\ 0.17\ 0\ 0\ 0\ 0\ 0\ 0) \begin{pmatrix} 0.73 & 0.04 & 0.04 & 0.15 & 0 & 0.04 & 0 & 0 & 0 \\ 0.17 & 0.32 & 0 & 0.17 & 0.17 & 0.17 & 0 & 0 & 0 \\ 0.29 & 0.29 & 0.42 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.50 & 0.17 & 0 & 0.17 & 0 & 0 & 0.16 & 0 & 0 \\ 0 & 0 & 1.00 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1.00 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.25 & 0 & 0 & 0.25 & 0 & 0 & 0.50 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= (0.66\ 0.08\ 0.10\ 0.13\ 0\ 0.03\ 0\ 0\ 0) \quad (19)$$

결과(19)로부터 다음 달 각 위협 상태(S_1~S_9)는 0.66, 0.08, 0.10, 0.13, 0, 0.03, 0, 0, 0의 확률로 발생할 것이라고 예측할 수 있다. 이는 S_1의 상태, 즉, (H_1, W_1)의 값이 갖는 발생빈도를 가질 확률이 가장 크다는 것을 말한다. 따라서 T_1은 0에서 400 사이의 값을, T_2는 0에서 4000 사이의 값이 발생할 것이라는 것을 예측할 수 있다. 다음 달의 T_1, T_2의 위협 발생 빈도를 예측하기 위해 앞서 구한 위협 발생 확률과 각 위협들의 임계값 중간값(M)을 이용한다. 본 적용사례에서도 5.1절의 예제와 마찬가지로 중간값을 구하기 위해 전달의 위협 발생 빈도를 이용한다. 우선 상태 정의 단계에서 구분한 T_1, T_2의 임계값 범위에 따라 중간값을 구하면 다음과 같다.

- T_1의 중간값($M(H_i)$)

  $M(H_1)=36$, $M(H_2)=0$, $M(H_3)=0$
- T_2의 중간값($M(W_i)$)

  $M(W_1)=1040$, $M(W_2)=0$, $M(W_3)=0$

각 위협의 발생 빈도를 구하기 전에, 각 위협별 임계값에 대한 발생 확률을 구해야 하는데, 위협 발생 확률 값을 이용하여 구할 수 있다. 위협 T_1, T_2의 각 임계값 발생 확률은 아래와 같다.

- T_1의 임계값 확률($P(H_i)$)

  H_1 : 0.66 + 0.08 + 0.10 = 0.84

  H_2 : 0.13 + 0 + 0.03 = 0.16

  H_3 : 0
- T_2의 임계값 확률($P(W_i)$)

  W_1 : 0.66 + 0.13 + 0 = 0.79

  W_2 : 0.08 + 0 + 0 = 0.08

  W_3 : 0.10 + 0.03 + 0 = 0.13

마지막으로, 각 위협별 예상 발생 빈도는 식 (8)을 이용하여 구할 수 있다.

- 예상 위협 발생 빈도 = $\sum_{i=1}^{n} P(S_i)\ M(S_i)$

  = 예상 위협 발생 확률(임계값 확률) × 임계값의 중간값
- T_1의 예상 발생 빈도 = $\sum_{i=1}^{3} P(H_i)\ M(H_i) = 0.84 \times 36 \fallingdotseq 30$
- T_2의 예상 발생 빈도 = $\sum_{i=1}^{3} P(W_i)\ M(W_i) = 0.79 \times 1040 \fallingdotseq 821$

위 결과로부터 다음 달 T_1이 발생할 빈도수는 약 30, T_2가 발생할 빈도는 821로 예측할 수 있다.

5.3 위협들 사이의 관계성 분석을 위한 시도

앞서 언급하였듯이 정보 기반 시스템에는 다양한 위협들이 존재하는데 이들 사이의 명확한 관계성 분석을 하기 위해, 먼저 위협들 사이에 어느 정도의 연관성이 있는지를 분석할 필요가 있다. 이러한 분석을 통해 서로 연관된 위협을 탐색할 수 있으며, 연관된 위협들 사이의 관계성 분석을 위한 기초가 된다. 본 논문에서는 이를 위해 공분산(covariance, Cov)[8,17]과 상관계수(corr-

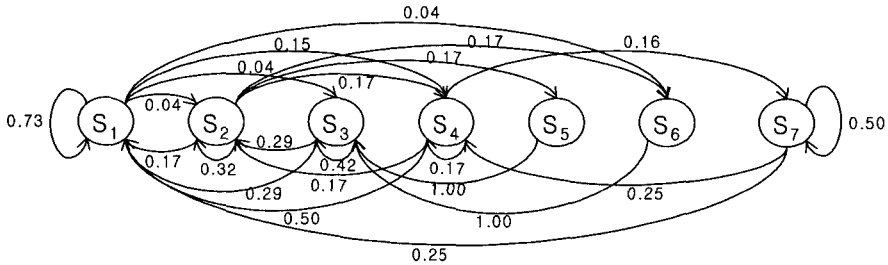

그림 9 위협 T_1, T_2에 대한 위협 상태 다이어그램

leation coefficient)[8,17]를 이용한 위협간의 연관 관계 정도를 분석한다.

공분산은 변수들 간의 상관관계 정도를 나타내며 (20)과 같이 정의된다.

$$Cov(X, Y) = E(XY) - E(X)E(Y) \quad (20)$$

단, E(X)는 변수 X의 기대값(expectation)이다.

Cov(X, Y)= 0 일 경우에는, 임의의 변수 X, Y 값이 아무런 관련이 없음을 나타낸다.

상관계수 ρ(X, Y)는 관련성의 밀접성을 평가하는 지표로 (21)와 같이 정의되고 조건 (22)를 만족한다.

$$\rho(X, Y) = \frac{Cov(X, Y)}{\sqrt{Var[X]\,Var[Y]}} = \frac{Cov(X, Y)}{\sigma_X \sigma_Y} \quad (21)$$

단, $Var(X) = E(X^2) - E(X)^2$,

$\sigma_X = \sqrt{Var[X]}$, $\sigma_Y = \sqrt{Var[Y]}$

$$-1 \le \rho(X, Y) \le 1 \quad (22)$$

$$\rho(X, Y) = \begin{cases} -1, \text{if } X = -aY (a > 0) \\ 0, \text{ if } X \text{ and } Y \textit{ are uncorrelated} \\ +1, \text{if } X = aY (a > 0) \end{cases} \quad (23)$$

(23)에서 볼 수 있듯이, 특히 상관계수의 값이 0일 경우에는 변수간의 관련성이 0인 경우이다. 상관계수의 값이 -1값에 가까울수록 X가 증가 할수록 Y는 감소하고, 1에 가까울수록 X가 증가 할수록 Y는 감소하는 관계를 가지고 있다.

적용사례의 세 가지 위협 T_1, T_2, T_3 의 상관관계 정도에 대하여 살펴보면 식 (21)에 의해 (24), (25), (26)과 같은 값을 얻었다.

$$\rho(T_1, T_2) = \frac{Cov(T_1, T_2)}{\sqrt{Var[T_1]\,Var[T_2]}} = \frac{Cov(T_1, T_2)}{\sigma_{T_1}\sigma_{T_2}} = -0.0401 \quad (24)$$

$$\rho(T_1, T_3) = \frac{Cov(T_1, T_3)}{\sqrt{Var[T_1]\,Var[T_3]}} = \frac{Cov(T_1, T_3)}{\sigma_{T_1}\sigma_{T_3}} = 0.19979 \quad (25)$$

$$\rho(T_2, T_3) = \frac{Cov(T_2, T_3)}{\sqrt{Var[T_2]\,Var[T_3]}} = \frac{Cov(T_2, T_3)}{\sigma_{T_2}\sigma_{T_3}} = 0.25718 \quad (26)$$

(24), (25), (26)의 결과로 두 위협 T_2, T_3는 관련성의 밀접성이 0.2571 값으로 세 위협 사이에 가장 밀접한 관련이 있는 것으로 분석할 수 있다. 즉, 위협 T_2(바이러스 : 인터넷 웜)의 발생이 위협 T_3(스캔탐지 : 네트워크 도청 및 감청)의 발생에 어느 정도의 영향을 미친다고 분석할 수 있다. 또한, 적용사례에 보인 두 위협 T_1, T_2는 관련성의 밀접성이 -0.040로 T_1, T_2 사이의 관련성이 거의 없다는 것을 알 수 있다. 즉, 위협 T_1(해킹: 악성 프로그램을 이용한 통신망에 대한 불법적인 침입)의 발생이 위협 T_2(바이러스 : 인터넷 웜)의 발생에 거의 영향을 주지 않는다고 분석할 수 있다. 본 논문에서는 세 가지 위협에 대해서만 연관 관계 정도를 보였지만, 이 위협 이외의 다양한 위협에도 공분산과 상관관계를 이용한 연관 관계 정도를 분석할 수 있다. 이를 이용하여 수많은 위협들 중에서 어떤 위협에 대해 적용할 것인지를 결정하여 피해 산정을 계산하기 위한 성능을 높일 수 있다. 또한 이를 바탕으로 각 위협들 사이의 명확한 연관 관계 분석에 이용할 수 있다.

본 논문에서 제안하는 모델을 통해 좀더 정확한 예측값을 얻기 위해서는 몇 가지 고려해야 할 사항이 있다. 첫째로, 위협 상태 집합을 정의하기 위해 적절한 범위의 임계값을 정해야 한다. 임계값의 범위를 어떻게 정의하느냐에 따라 예측값이 실제 발생하는 위협과 어느 정도 가깝게 예측할 수 있는지를 결정하게 되고 임계값을 세분화하면 할수록 실제 값과 가까운 값을 예측할 수 있다. 그렇지만 임계값의 범위를 세분화 할수록 위협 상태나, 전이 행렬 및 모든 요소들의 복잡도가 커진다는 제한점을 가지고 있다. 둘째로, 초기 확률 설정시 필요로 하는 최근 데이타의 범위 설정도 고려해 보아야 한다. 최근 데이타의 범위 설정도 마찬가지로 위협 발생 확률에 영향을 준다. 셋째, 마코프 체인에 기반한 확률적 피해 파급 모델에서는 위협 주기를 파악하는 것이 중요하다. 위협에 대한 정확한 통계 없이는 정량 분석을 할 수 없다. 따라서 위협에 관련된 관측된 데이타 값들에 대하여 통계화가 필수적이다. 본 논문에서는 관측된 월별 데이타를 이용하였는데, 일별, 또는 주별 데이타가 확보되고 이용한다면 좀더 정확한 예측값을 얻을 수 있다.

본 논문에서 제시하는 마코프 프로세스를 이용한 피해 파급 모델은 기존의 방법론과는 몇 가지 차이점이 있다. 첫째, 웜/바이러스 피해 파급 모델과 같이 피해 자산의 수, 특히 감염된 자산의 수를 구하는 것이 아니라, 위협이 발생할 확률 및 빈도수를 구한다. 이러한 확률적 접근 방식을 통하여 다양한 형태의 정보통신 기반 시설에 적용할 수 있을 뿐만 아니라 이를 근거로 하여 위협 대책 수립에 도움이 된다. 둘째, 웜/바이러스 피해 파급과는 달리 특정 위협에 국한되지 않고 다양한 위협에 대해 적용 가능하다. 따라서 위협들 사이의 관계를 파악하여 전체 시스템이 가지고 있는 위협에 대하여 종합적으로 예측 및 분석할 수 있다.

6. 결론 및 향후 연구

본 논문에서는 바이러스나 웜 뿐만 아니라 여러 가지 위협의 종류들로부터 공격을 받았을 때 그 피해 파급 정도를 예측할 수 있는 마코프 프로세스 기반의 확률적 피해 파급 모델을 제안하였다. 또한 과거의 관찰된 데이타를 이용하여 제안한 모델의 적용사례를 보였다. 제안된 모델은 전체 시스템에서 위협들의 발생 확률 및 발생 빈도를 마코프 프로세스를 이용하여 설명함으로써 하나의 특정 위협이 아니라 전체 시스템이 가지고 있는 여러 가지 위협들에 대해 적용할 수 있다. 더불어 공분산과 상관계수를 통해 위협들 사이의 상관관계 정도를 파악할 수 있었다. 그러나 좀더 정확한 피해 파급 예측을 위해 적절한 임계값 설정에 대한 연구가 필요하다. 또한 위협들 사이의 연관 관계 분석을 위한 연구가 필요하다. 마지막으로, 마코프 프로세스 기반의 모델을 사용하기 위해서는 위협이 발생 하였을 때 이에 대한 정확한 자료의 통계화가 요구된다.

참 고 문 헌

[1] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Mangement Guide for Information Technology Systems," NIST Special Publication 800-30, National Institute of Standards and Technology (NIST), 2002.

[2] 한국정보보호진흥원(KISA), "취약점 분석·평가 보델", 한국정보보호진흥원(KISA), 2002.

[3] 이동훈, 이현숙, 김영자, 변진욱, 김역, 이래, 박혜영, 최은영, "컴퓨터 해킹·바이러스 피해액 산출방법 연구", 한국정보보호진흥원(KISA), 2002.

[4] S. Staniford, V. Paxson, and N.Weaver, "How to Own the Internet in Your Spare Time," In Proc. of the 11th USENIX Security Symposium (Security02), 2002.

[5] Z. Chen, L. Gao, K. Kwiat, "Modeling the Spread of Active Worms," In Proc. of IEEE INFOCOM2003, 2003.

[6] T. Vogt, "Simulating and Optimising Worm Propagation Algorithms," http://web.lemuria.org/security/WormPropagation.pdf, 2003.

[7] C. C. Zou, W. Gong, and D. Towsley, "Code Red Worm Propagation Modeling and Analysis," In Proc. of the 9th ACM Conference on Computer and Communications Security, pp. 138-147, November 2002.

[8] Kishor S. Trivedi, "Probability and Statisics with Reliability, Queuing and Computer Science Applications," Second Edition, WILEY Interscience, 2002.

[9] Roy D. Yates, David J. Goodman, "Probability and Stochastic Process," Second Edition, WILEY International Edition. 2003.

[10] 김영갑, 이택, 인호, 정윤정, 김인중, 백두권, "정보 통신 기반 시설에 대한 피해 파급 모델", 제 17회 정보보호와 암호에 대한 학술대회(WISC2005), 국가 보안기술 연구소(NSRI), 2005년 9월.

[11] Y.-G. Kim, T. Lee, H. P. In, Y.-J. Chung, I. Kim, and D.-K. Baik, "A Probabilistic Approach to Estimate the Damage Propagation of Cyber Attacks," Lecture Notes in Computer Science, Vol. 3935, pp. 175-185, Springer-Verlag, Berlin Heidelberg, 2006.

[12] J. C. Frauenthal, "Mathematical Modeling in Epidemiology," Springer-Verlag, New York, 1980.

[13] C. C. Zou, W. Gong, and D. Towsley, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," In Proc. of ACM CCS Workshop on Rapid Malcode (WORM'03), October, 2003.

[14] D. J. Deley and J. Gani, "Epidemic Modeling :An Introduction," Cambridge university Press, 1999.

[15] L. Edelstein-Keshet, "Mathematical Models in Biology," Random House, New York, 1988.

[16] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, "Internet Quarantine: Requirements for Containing Self-Propagating Code," In Proc. of IEEE INFOCOM, 2003.

[17] 한국정보보호진흥원(KISA), "해킹바이러스 통계 및 분석 월보(2001년 1월 ~ 2005년 6월)", 한국정보보호진흥원(KISA), http://www.krcert.or.kr/

[18] Robert V. Hogg and Allen T. Craig, Introduction to Mathematical Statistics, Fifth Edition, Prentice-Hall, 1995.

김 영 갑

2001년 고려대학교 식량자원학과 학사(컴퓨터학과 부전공). 2003년 고려대학교 컴퓨터학과 석사. 2006년 고려대학교 컴퓨터학과 전산학박사. 2006년~현재 고려대학교 정보보호대학원. 관심분야는 보안정책, 위험분석, 보안공학, 임베디드 보안, 메타데이타

백 영 교

2000년 고려대학교 수학과 학사. 2002년 고려대학교 수학과 석사. 2002년~현재 고려대학교 수학과 박사과정. 관심분야는 확률론적모델링, 대기행렬이론, 통신망분석

인 호

1990년 고려대학교 전산학 학사. 1992년 고려대학교 대학원 전산학 석사. 1998년 University of Southern California 컴퓨터학 박사. 1999년~2003년 Texas A&M 대학 조교수. 2003년~현재 고려대학교 컴퓨터학과 조교수. 2004년~현재 한국시스템엔지니어링협회 이사. 2005년~2006년 한국정보과학회 학술지 편집위원. 2005년~현재 한국정보처리학회 학술지 편집위원. 관심분야는 요구공학, 임베디드 소프트웨어, 소프트웨어 보안, 정황인지 미들웨어 등

백 두 권

1974년 고려대학교 수학과 학사. 1977년 고려대학교 대학원 산업공학과 석사. 1983년 Wayne State Univ. 전산학 석사 1986년 Wayne State Univ. 전산학 박사. 1986년~현재 고려대학교 정보통신대학 교수. 1989년~현재 한국정보과학회 이사/학술위원장/편집위원장/평의원. 1991년~현재 한국시뮬레이션학회 이사/부회장/감사/회장/고문. 1992년~현재 ISO/IEC JTC1/SC32 국내위원회 위원장. 1996년~1997년 고려대학교 컴퓨터과학기술연구소 초대소장. 2001년~현재 도산아카데미 원장. 2002년~2004년 고려대학교 정보통신대학 초대학장. 2004년~2005년 한국정보처리학회 부회장. 2006년~현재 한국정보과학회 부회장. 관심분야는 메타데이타, 소프트웨어 모델링, 시뮬레이션, 정보기술표준 등