2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

네트워크 기반의 침입을 탐지하기 위한 통계적 분석 기법

박찬이, 홍선호, 위규범
아주대학교 정보 및 컴퓨터 공학과
e-mail: (charn sunhong kbwee)@ajou.ac.kr

Statistical Analysis Methods For Network Based Intrusion Detection

Charny Park, Sun-Ho Hong, Kyu-Bum Wee
Dept. of Information and Communication, Ajou University

요 약

현재 네트워크 기반의 침입 탐지는 대부분 오용 탐지 기법을 사용한다. 하지만 이는 알려지지 않은 침입을 탐지하는 능력이 떨어지는 기법으로서 이를 보완할 수 있는 비정상행위 탐지 기법을 찾는 것이 필요하다. 따라서 수집된 감사 자료로부터 정상행위를 프로파일링하고 침입임을 판정하는데 통계적인 기법을 사용하였다. 수집된 로그로부터 통계적인 방법으로 정상행위를 프로파일링하기 위해 우선 패킷으로부터 수집되는 감사 자료의 통계적인 특성을 대변하는 분포와 파라미터를 추정하고 카이스퀘어 검정법을 사용하여, 감사 자료가 가설하는 이론적인 분포의 특성을 가지고 있다고 판정되면 이를 정상행위의 기준으로 삼는다. 이후에 수집되는 감사자료를 감시하기 위해 추정된 분포와 파라미터를 따르고 있는지의 여부를 Kolmogorov-Smirnov 적합도 검정을 이용하여 판별하고, 이를 벗어나는 경우 침입으로 판정할 수 있도록 한다.

1. 서론

침입탐지 시스템에는 오용 탐지 기법 (Misuse Detection)과 비정상행위 탐지 기법 (Anomaly Detection)이 있다. 알려지지 않은 침입 탐지의 효율성을 높이기 위해 현재 호스트에 기반 하여 시스템 콜을 사용하여 비정상행위를 탐지하려는 기법은 많이 연구되고 있다. 그러나 기존 상용 침입탐지 시스템 중에 네트워크 기반의 침입탐지 시스템의 대부분은 다량의 패킷을 실시간으로 탐지할 수 있도록 하기 위해 오용탐지 기법을 선택하고 있다. 그러므로 새로운 공격 기법에 대한 탐지율이 떨어질 수 밖에 없는 단점을 가지고 있다. 따라서 네트워크에 기반한 비정상행위 탐지를 위한 몇 가지 기법들이 제안되었다. 그러나 SRI 에서 제안하는 NIDES 의 기법과 데이터 마이닝을 사용한 기법[6]은 그 침입탐지 방법의 높은 복잡도와 룰을 추출하기 위한 효율성이 떨어지는 단점을 가지고 있다. 따라서 패킷으로부터 얻어지는 정보를 통해 효과적으로 정상 행위를 분석, 프로파일링하고 실시간으로 침입 탐지한 기법이 필요한 실정이다. 본 논문에서는 네트워크 기반의 침입 탐지 시스템을 위한 비정상행위 탐지 기법을 통계적인 방법으로 접근하고자 한다.

수집된 패킷 정보들 중에서 telnet 의 단위시간당 연결을 통해 침입을 탐지하기 위한 통계적인 방법론이 제한되어 있다[1]. 이 방법은 통계적인 방법을 사용하여 telnet 연결 요청에 대해서 가능한 몇 가지 공격, 서비스 거부 공격 및 이외의 공격들을 탐지할 수 있음을 제안하였다. 그러나 여러 가지 유형의 공격들을 통해 나타나게 되는 연결시간의 지연, 프래그멘테이션을 이용한 공격으로 인한 비정상적인 사이즈의 패킷 생성 등도 감시 대상이 되어야 한다.

감시 대상의 정상행위 모델링을 위해 보통은 포아송 분포를 전제하여 실험을 한다. 그러나 실제 네트워크에서 수집되는 다양한 로그들이 포아송 분포만을 따르는 것은 아니다. [3]에서는 TCP 에서 수집되는 다양한 정보들을 통계적인 방법으로 접근, 비모수적 표본들이 어떠한 분포를 따르고 있는가를 분석하고 결과를 제시하였다.

이후 Kolmogorov-Smirnov 적합도 검정 (Goodness-of-fit test)을 침입 판정에 사용하였다. 감시중인 데이터가 실험을 통해 얻어진 이론상의 CDF (Cumulative Distribution Function)를 따르는지의 여부를 적합도 검정을 통하여 판정하고 이를 침입으로 판단할 수 있는 기준으로 삼았다[1].

본 논문에서도 위와 같이 Kolmogorov-Smirnov 적합도 검

정을 통해서 침입을 판정하였다. [1]의 논문에서는 연결요청을 이용하여 일어날 수 있는 공격에 대해서만 감시하였지만 본 논문에서는 앞서 언급했듯이 공격에 의해 변화할 수 있는 다른 요소들, originator bytes, duration time 등도 감시 대상에 포함하였다.

2. 통계적 기법

앞서 언급했듯이 정상행위 결정 및 침입 탐지를 위해 통계적인 방법으로 수집된 TCP 데이터를 분석한 기존 연구를 소개한다. 뒤이어 침입 탐지를 위한 통계적인 기법을 제시한다.

2.1. 감사 데이터를 통한 정상 행위 프로파일링

[2]에서의 실험은 공개 제공되는 버클리 대학의 TCP 로그 데이터들을 통해서 정상적인 TCP 의 데이터를 분석하려는 시도를 하였다. 그리고 각 데이터가 보통 실험의 전제로 삼는 포아송 분포만을 따르지 않는다는 결론을 얻었으며 다음 표 1 과 같은 분석 결과를 제시하였다. 연구에서는 여러 개의 서비스 중 사용도가 높은 상위 4 개 서비스인 telnet, nntp, smtp, ftp 를 분석하였다. 그 결과 중에서 서비스의 연결요청은 포아송 분포를 따르지만 다른 데이터는 포아송 이외의 분포를 따른다는 결론을 얻었다. 큰 사이즈의 데이터가 교환되는 smtp, nntp 의 originator bytes 같은 경우에는 log-normal 같은 분포가 적합하다는 결론을 내렸다. 각 분석 모델을 위해 추출된 몇 개의 변수들은 공격이 일어날 경우 충분히 정상적인 분포를 벗어나 침입을 판정하는 기준을 제시하는 값들이다. 예를 들어 SYN-Flooding 을 이용한 서비스 거부 공격의 경우에 공격 연결 요청에 의해 arrival connection 과 duration time 등의 값이 변하게 된다. 프레그멘테이션을 이용한 공격의 경우 공격자로부터 오는 패킷의 사이즈가 비정상적으로 작아지는 경향이 있다.

분석 모델을 설정하기 위해서는 파라미터를 추출하고 제안한 모델을 따르고 있는지를 검정하기 위한 방법이 필요하다. [3]의 실험은 χ^2 검정법을 사용하였다.

표 1 에서 포아송 분포로 모델링 될 수 있는 arrival connection 의 추정치는 단위시간에 따라 변할 수 있으므로 표기하지 않았다. duration time 은 연결지연 시간을, originator bytes 는 소스 호스트로부터 전송되는 데이터의 사이즈를 의미한다. 기존 실험에서 ftp 는 이전 실험에서 수집된 대상이 타 서비스와 다르기 때문에 본 논문에서는 실험하지 않았다.

추정

수집된 데이터의 정상행위 프로파일링을 위해서 각 데이터는 제안된 이론상의 모델을 따른다는 가정 하에 파라미터를 추정해야 한다. 기본적인 정규분포부터 잘 사용되지 않은 extreme 분포까지의 추정식을 소개한다. 가장 널리 사용되는 정규 분포는 평균과 분산 두 파라미터를 가지는데 이를 위한 추정식은 다음과 같다.

$$\hat{\mu} = \sum_{i=1}^{n} \frac{x_i}{n}, \quad \hat{\sigma}_x = \sqrt{\sum_{i=1}^{n} \frac{(x_i - \bar{x})^2}{(n-1)}}$$

log-normal 분포는 $Y = \log_2 X$ 를 만족하는 Y 가 정규분포를 따르는 경우라고 할 수 있다. 위와 마찬가지로 log-extreme 분포는 $Y = \log_2 X$ 를 만족하는 Y 가 extreme 분포를 따르는 것을 의미한다. Extreme 분포를 위한 파라미터 α , β 의 추정치는 다음과 같다[5]. 이때 $\hat{\beta}$ 는 iteration 하여 풀어야 한다.

$$\hat{\beta} = \sum_{i=1}^{n} \frac{x_i}{n} - \frac{\sum_{i=1}^{n} x_i \exp(-x_i / \hat{\beta})}{\sum_{i=1}^{n} \exp(-x_i / \hat{\beta})}$$

$$\hat{\alpha} = -\hat{\beta} \log(\sum_{i=1}^{n} \exp(-x_i / \hat{\beta}) / n)$$

단위 시간당 연결 요청에 대해서 모델링하기 위해 사용되는 포아송 분포는 단위 시간 t 당 이벤트가 일어나는 기대값 λ 를 파라미터로 하는 포아송 분포의 경우 다음과 같은 추정값을 가진다.

$$\hat{\lambda} = \text{Total count of X / The length of T}$$

2.2. Kolmogorov-Smirnov 적합도 검정

Kolmogorov-Smirnov 적합도 검정법은 이론적으로 나올 수 있는 CDF 인 $F_T(z)$ 와 표본 데이터로부터 추출될 수 있는 CDF $F_n(z)$ 의 적합도를 측정하여 특정 이론적 분포와 수집된 데이터를 비교할 수 있는 척도이다[4]. 이 때 사용되는 통계량을 D_n 로 나타내는데 이는 $F_n(z)$ 와 $F_T(z)$ 의 최대 차이를 의미한다. 표본 데이터의 CDF $F_n(z)$ 는 다음과 같이 정의 된다.

경험적 분포 함수 (Empirical Distribution Function)

함수 $t(u)$ 는 만약 $u < 0$ 이면 $t(u) = 0$, $u \geq 0$ 이면

[표 1] TCP 로그 데이터 분석 모델의 특징

Protocol	Variable	Distribution	Estimates
telnet	Duration time Originator bytes Arrival Connection	log2-normal log2-extreme Poisson	$\bar{x} = \log_2 240 ; \sigma_x = \log_2 7.8$ $\alpha \approx \log_2 100 ; \beta \approx \log_2 3.5$
nntp	Originator bytes Arrival connection	log2-normal Poisson	$\bar{x} \approx 11.5; \sigma_x \approx 3$
smtp	Originator bytes Arrival connection	log2-normal 0-80% log2-normal 80-100% Poisson	$\bar{x} \approx 10 ; \sigma^x \approx \log_2 2.75$

$t(u)=1$로 정의 되는 함수이다. 만약 모집단으로부터 추출된 임의의 표본을 $z_1, z_2, \cdots, z_n$이라고 한다면 이때 표본의 경험적 CDF 는 아래와 같이 정의될 수 있다.

$$F_n(z) = \frac{1}{n}\sum_{k=1}^{n} t(z - z_k)$$

Kolmogorov-Smirnov 적합도 검정법

주어진 표본 $z_1, z_2, \cdots, z_n$ 로부터 Kolmogorov 통계량 $D_n(z_1, z_2, \cdots, z_n)$을 아래와 같이 정의할 수 있다.

$$D_n := \sup_{z \in Z} |F_n(z) - F(z)|$$

여기서 D_n은 비모수적 특성으로부터 아래와 같은 적합도 검정을 위한 통계적인 추론을 이끌어내기 위해 사용된다. 이론상의 CDF $F_T(z)$와 표본 $z_1, z_2, \ldots, z_n$가 주어졌을 때, 주어진 표본이 이론적인 분포를 따르고 있는가에 대해 귀무가설을 다음과 같이 세울 수 있다. 여기서 유의 수준 α에 대해 $\gamma = 1-\alpha$를 의미한다.

$$H_0 : F_n(z) = F_T(z)$$
$$H_1 : F_n(z) \neq F_T(z) \quad \text{for all } z \in Z$$
$$\text{Reject Region: } D_n := \sup_{z \in Z} |F_n(z) - F(z)| > D_{n,\gamma}$$

기각역의 조건을 만족한다면 귀무가설 H_0 를 기각, $F_n(z)$이 $F_T(z)$을 따르지 않는다고 할 수 있다. 이론상의 분포와 표본 데이터가 정확히 일치할 수 없기 때문에 채택역에 대한 오류를 허용하는 정도인 유의 수준 α 의 선택을 통해서 수치상으로 파악할 수 있다. α 가 작을수록 데이터들의 수치가 이론적인 CDF 를 더 정확히 따른다고 가정할 수 있다. 즉, 허용되는 오차의 범위가 작아짐을 의미한다.
실제 실험에서 설정하기 위한 각 유의 수준에 따른 실제 $D_{n,1-\alpha}$ 의 값은 다음과 같다.

$1-\alpha$	0.20	0.10	0.05	0.02	0.01
$D_{n,1-\alpha}$	$\frac{1.07}{\sqrt{n}}$	$\frac{1.22}{\sqrt{n}}$	$\frac{1.36}{\sqrt{n}}$	$\frac{1.52}{\sqrt{n}}$	$\frac{1.63}{\sqrt{n}}$

[표 2] Kolmogorov-Smirnov 검정법을 위한 임계값: $n > 40$

2.3. 추가된 침입 탐지 감시 대상

기존의 실험 [1]에서는 arrival connection, 즉 연결 요청에 대해서 감시하고 이를 비정상적으로 나타내는 각종 서비스 거부 공격에 대해서 탐지하였다. 그러나 여러 가지 다른 침입 유형들에 대해서도 통계적인 이론을 적용하여 침입 탐지를 할 수 있다.

따라서 [3]의 실험에서 사용된 버클리 대학의 패킷 로그를 이용하여 또 다른 요소들에 대해 침입 탐지를 해보기로 하였다. 우선 몇 가지 공격에 의해 비정상적인 패턴을 보일 수 있는 몇 가지 요소들을 추출하였다.

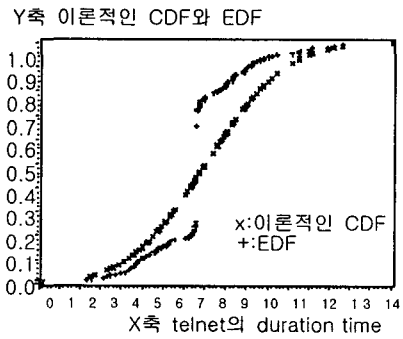
Duration time 은 상대방이 연결을 요청하고 서버에 의해 이루어지는 연결 요청 시간을 의미한다. 공격이 이루어 질 때에 공격자가 보내는 거짓된 연결 요청에 대해 서버는 연결을 확립할 수 없으므로 비정상적인 Duration time 을 가지게 된다. 따라서 침입 탐지에 고려해야 할 중요한 사항이다.

Originator bytes 는 상대방으로부터 받게 되는 패킷의 바이트 사이즈를 의미한다. 연결 요청을 위해 공격자로부터 받게 되는 패킷은 각종 해킹 툴에 의해 제작되어 그 사이즈가 일정한 특징이 있으며, smtp 에서 다량의 웜이 발생한다면 역시 같은 사이즈의 데이터 교환이 다량으로 이루어진다. 따라서 사용자로부터 전달 받는 패킷의 바이트 사이즈도 중요한 감시 대상이 될 수 있다.

본 논문에서는 위의 추가적인 감시 요소를 고려하였고 이들 또한 감시 대상이 될 수 있으며 다른 유형들의 공격도 탐지 가능하다는 것을 실험을 통하여 보였다. 침입 탐지를 위해서 기존에 사용된 Kolmogorov-Smirnov 적합도 검정법을 이용하였다. 이 방법을 통해서 얻어진 D_n 을 통해 수집된 데이터가 정상적인가 아닌가를 판정하였다.

3. 실험

Telnet 의 연결 요청 감시 및 침입 탐지는 기존 연구에서 검정된 방법이다[1]. 그 밖의 요소들에 대해서 침입 탐지가 가능한가의 여부를 실험을 통해 검정하였다. 이전 연구에서는 arrival connection 을 사용하여 탐지하였으나 duration time 과 originator bytes 두 가지 요소에 대해서는 고려하지 못한 상태였다. 따라서 본 실험에서는 duration time 과 originator bytes 에 대해서 각각 실험하였다.



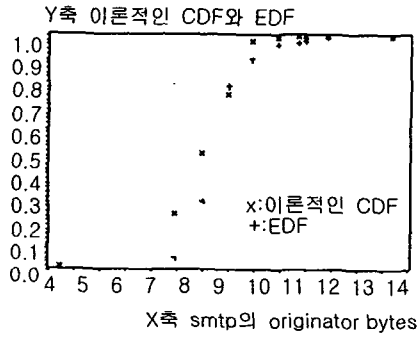
[그림 1] Telnet duration time 데이터의 EDF 와 이론적인 CDF

우선 telnet 에서 초단위 로그를 남긴 duration time 에 대해 실험하였다. $D_{n,1-\alpha}$ 의 경우 수집된 데이터가 많을수록 좋은 결과를 나타내게 되는데 침입을 탐지하기위한 감시 시간은 최소한의 기간에서 이루어져야 한다. 따라서 2 시간과 30 초 두 가지 경우에 대해서 침입 탐지에 타당한 시간 간격에 대해 실험을 하였다. 우선 정상행위에 대한 오진률을 측정하기 위해 앞서 말한 2 시간 단위와 30 초 단위의 정상적인 프로파일링 데이터에 대해 D_n 값을 측정하였다. 후자 30 초 동안의 로그의 경우 수집된 데이터가 소량이어서 D_n 수치가 커서 실제 가정하는 분포를 따른다고 말하기 어려웠다. 그러나 2 시간 동안 수집된 222 개 로그의 경우에는

D_{222} 값은 0.293 정도로 그림 1 에서 볼 수 있듯이 어느 정도 이론적인 분포를 따르고 있다. 표 2 를 참조하면 유의수준을 0.99 의 경우 $D_{222,1-0.99} = 0.12$ 이므로 유의 수준을 0.99 보다 작게 설정해야 하는 것이 적절함을 알 수 있다.

위의 telnet duration time 에 대해서 SYN 와 FIN 에 의해 정상적인 연결이 아닌 경우, 비정상적으로 연결이 이루어진 경우의 로그만을 수집하였다. Kolmogorov-Smirnov 검정법을 통해 실제로 비정상적인 이벤트의 로그들에 대해 탐지가 가능한가 살펴 보면, 비정상적인 환경에서 로그 데이터 100 개에 관한 $D_{100} = 0.658$ 이며 이는 정상적인 환경에서의 0.293 보다 훨씬 큰 값이다. 따라서 충분히 침입 탐지가 가능하다는 것을 알 수 있다.

2 시간 동안 수집된 정상적인 smtp 의 originator bytes 의 경우 로그 193 개에 대해 D_{193} 값은 0.239 로 telnet duration time 과 비슷한 유의 수준을 설정해야 함을 알 수 있다. 그림 2 는 실험 결과로써 수집된 데이터가 이론적인 분포를 따르고 있음을 보여주고 있다.



[그림 2] Smtp originator bytes 데이터의 EDF 와 이론적인 CDF

비정상적인 데이터는 웜이 발생할 경우 일정한 사이즈의 originator bytes 가 다량 발생한다는 사실을 이용하여 웜으로 추정할 수 있는 150 개의 데이터에 대해서 웜의 발생빈도를 달리하여 실험하였다.

실험 결과 D_{150} 에 대한 값은 다음과 같이 증가하여 웜의 빈도가 높을수록 D_n 값이 증가하여 탐지율이 높아진다는 결론을 얻을 수 있다.

$1-\alpha$	1%	5%	10%	15%	20%	25%
$D_{150,1-\alpha}$	0.2999	0.2969	0.2960	0.3036	0.3102	0.3210

[표 3] 가능한 발생 빈도로부터 얻어지는 $D_{n,1-\alpha}$

4. 결론 및 향후 연구과제

위의 실험을 통해서 연결 요청 뿐만이 아닌 다른 요소들도 침입 탐지의 대상이 될 수 있음을 알 수 있다. 그러나 telnet duration 데이터의 경우 Kolmogorov-Smirnov 검정법을 사용하기 위해서는 수집 감시될 데이터의 양이 일정수준 이상이어야 탐지율이 높음을 알 수 있다. 따라서 감시 측정될 데이터의 양을 고려하는 것도 중요한 과제라고 할 수 있겠다. 이와 같은 이유로 본 방법은 차후에 남겨진 다량의 로그에 대해 무결성을 검정하고 침입의 존재여부를 판별하기에 빠르고 적절한 방법이라고 할 수 있겠다. 하지만 아직 비정상행위 탐지의 중요한 요소인 긍정적 결함률, 즉 다양한 유의 수준에 대한 종합적인 실험이 아직은 미비한 상태이다.

본 논문은 널리 알려진 통계적 검정방법을 이용하여 이전 보다 확장된 감시 요소를 통해 침입을 탐지할 수 있음을 보였다. 또한 데이터 마이닝 기법이나 뉴럴 네트워크 등의 알고리즘처럼 높은 복잡도를 요구하지도 않기 때문에 타 비정상행위 탐지 기법보다 네트워크 기반의 침입 탐지에 적절한 방법이다. 또한 침입 탐지를 위해 네트워크 이외의 요소, 예를 들면 CPU 타임 감시를 통한 내부 서비스 거부 공격등에도 확장하여 사용하기 좋은 방법이다. 그리고 현재 결과는 [3]에서 제공된 telnet, smtp 등과 같은 대표적인 서비스에 대한 분석 결과로부터 얻어진 것이다. 최근 들어 http 의 사용이 증가하고 따라서 서비스 거부 공격 외에 다양한 공격 대상이 되고 있다. 본 논문에서는 분석되지 않았지만 http 또한 침입 탐지를 위한 필수적인 분석 대상이다.

이전의 실험 [3]은 모델 제안과 검정을 위해 χ^2 방법을 사용하였지만 좀 더 많은 데이터를 검정하는데 정확한 방법인 Kolmogorov-Smirnov 검정법을 통해서 http 의 모델을 제안하는 것도 좋은 결과를 얻을 수 있다[7].

본 논문은 패킷으로부터 수집된 감사자료를 통해 침입 탐지를 위한 통계적인 분석 기법을 제시했다. 향후 실제 네트워크 기반의 침입 탐지 시스템에 적용할 수 있도록 탐지 모듈로의 확장이 필요하다.

참고문헌

[1] Joao B. D. Cabrera, B. Ravichandran and Raman K. Mehra, "Statistical Traffic Modeling for Network Intrusion Detection," Proceedings of the 8th International symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems IEEE, pp. 446-476, August 2000.

[2] V. Paxson, and S. Floyd, "Wide-Area Traffic: The Failure of Poisson Modeling," IEEE/ACM Transactions on Networking, Vol. 3 No. 3, pp. 226-244, June 1995.

[3] V. Paxson, "Empirically-Derived Analytic Models of Wide-Area TCP Connections," IEEE/ACM Transactions on Networking, Vol. 2 No. 4, pp. 319-336, August 1994.

[4] G. E. Noether, "Elements of Nonparametric Statistics," John Wiley & Sons, pp 11-23, 1967.

[5] R. B. D'Agostino and M. A. Stephens, editors, "Goodness-of-Fit Techniques", Marcel Dekker Inc., pp 145-149, 1986.

[6] W. Lee, S. J. Stolfo, and K. W. Mok, "A Data Mining Frame Work for Building Intrusion Detection Models," Proceedings of the IEEE Symposium on Security and Privacy, 1999.

[7] W. W. Daniel, "Biostatistics: A Foundation for Analysis in the Health Sciences", Sixth Edition, John Wiley & Sons, pp 597,. 1929.