김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제10호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 10 JUCHE105(2016).

이동모호추론에 기초한 DoS공격검출의 한가지 방법

허철만, 곽선일

모호추론에 대한 연구는 3개 부분(모호추론원리와 방법, 그것의 해석과 모호추론의 론리적기초, 모호추론방법의 응용)으로 진행되였으며 이에 따르는 여러가지 모호추론방법이 제기[1－3]되였다. 그런데 선행한 모호추론방법은 복잡하고 많은 계산량을 가진다.[3]

한편 콤퓨터망보안령역에서 중요한 부분인 침입검출체계는 실시간검출을 요구하며 여러가지 모호추론방법을 리용한 침입검출방법들과 체계들이 연구되였다.[1, 2]

론문에서는 계산량이 적고 속도가 빠른 모호추론방법 즉 이동모호추론방법을 적용한 DoS공격검출의 한가지 방법을 제안하였다.

1. 이동모호추론방법

표준모호체계에 대한 모호추론모형은 다음과 같다.[3]

$$\mathrm{R}_i:\ \text{if}\ \ x_1\ \text{is}\ P_{i1},\ \cdots,\ x_i\ \text{is}\ P_{ji},\ \cdots,\ x_s\ \text{is}\ P_{js}\ \ \text{then}\ \ z_j=Q_j \tag{1}$$

여기서

$$x_1\ \text{is}\ P_{i1},\ \cdots,\ x_i\ \text{is}\ P_{ji},\ \cdots,\ x_s\ \text{is}\ P_{js}$$

는 입력정보이고 $z_j=Q_j$ 는 결론으로서 $x_i\in X(i=\overline{1,\ s})$ 는 대상입력을 나타내는 변수, $z_j\in Z$ 는 대상출력을 나타내는 변수이다. 그리고 $P_{ji}\in U$, $Q_j\in V$ 는 각각 입력정보와 규칙기지의 전반부, 후반부모호모임이며 U, V는 대상체계가 정의되는 모임이다.

여기에 기초하여 이동모호추론방법을 다음과 같이 정의할수 있다.

① 식 (1)로 표시되는 표준모호모형에 대하여 입력정보모호모임

$$x_1\ \text{is}\ P_{i1},\ \cdots,\ x_i\ \text{is}\ P_{ji},\ \cdots,\ x_s\ \text{is}\ P_{js} \tag{2}$$

가 주어지면 j번째 규칙에 해당한 전반부모호모임들과 그것에 대응하는 입력정보들사이의 평균이동거리를 다음과 같이 구한다.

$$\delta x_j=\frac{1}{s}\sum_{i=1}^{s}\delta x_i^{(j)} \tag{3}$$

여기서

$$\delta x_i^{(j)}=\begin{cases}\dfrac{x_{P_i}-x_{P_{ji}}}{l_{ji}}, & x_{P_{ji}}\geq x_{P_i}\\[2ex] \dfrac{x_{P_j}-x_{P_{ji}}}{r_{ji}}, & x_{P_{ji}}<x_{P_i}\end{cases} \tag{4}$$

로서 l_{ji}, r_{ji}는 모호모임의 좌측폭, 우측폭이며 $x_{P_{ji}}$, x_{P_i}는 각각 P_{ji}, P_i의 중심점들이다.

② 전반부모임 P_{ji}들에서 구한 이동거리 δx_j들을 리용하여 후반부모임을 이동시켜 부분추론결과를 얻을 때 이동량 δz_j를 다음과 같이 구한다.

$$\delta z_j = F(\delta x_j),\ \ j=\overline{1,\ n} \tag{5}$$

③ 부분추론결과의 모호모임 Q_i'의 성원함수 $\mu_{Q_i'}(z)$를 다음과 같이 구한다.

$$\mu_{Q_i'}(z)=\begin{cases}\mu_{Q_i}(z), & \Delta Q_i=\phi\\ \mu_{Q_i'}(z+\delta z_i), & \Delta Q_i\neq\phi\end{cases} \tag{6}$$

④ 종합추론결과 Q'의 성원함수 $\mu_{Q'}(z)$를 식 (6)으로부터 다음과 같이 결정한다.

$$\mu_{Q'}(z)=\frac{1}{n'}\sum_{i}^{n'}\mu_{Q_i'}(z)_i \tag{7}$$

여기서 n'는 추론에 참가하는 규칙을 의미하며 일반적으로 $n'\le n$이다.

2. 이동모호추론에 기초한 DoS공격검출

론문에서는 DoS공격검출을 하기 위한 특징량으로서 시간차 DT와 IP주소의 통계적분포특성 DH를 선택하였다.

DoS공격의 대표적인 Synflood공격에서 공격자는 반드시 대량의 위조된 SYN자료파케트를 발송하여 체계자원이 랑비되게 함으로써 사용자의 봉사요구에 반응할수 없게 한다. 따라서 공격시 SYN파케트가 빈번히 발생하고 그 시간간격이 상대적으로 짧은 특징에 주목하여 DT를 첫번째 특징량으로 하였다.

한편 특정한 망범위에서 발생하는 통보문은 일정한 통계적특성을 가진다. 실례로 IP주소의 분포는 일정한 통계적특성을 만족시킨다. 그러나 공격이 발생하면 공격통보문의 IP주소는 일반적으로 우연적으로 위조된 IP주소이거나 유한개의 IP주소에 국한되므로 원래의 IP주소의 통계적분포특성이 파괴된다. 따라서 DH를 두번째 특징량으로 하였다.

일반적으로 DoS공격에서 공격통보문의 위조된 IP주소의 우연성이 매우 크므로 DH가 정상상태보다 커질수 있고 공격통보문의 IP주소가 위조되지 않으면 우연성이 감소하여 DH가 정상상태보다 작을수 있다. 그리고 DH가 너무 크고 DT가 작으면 공격가능성이 크다고 보며 역시 DH가 너무 작고 DT가 너무 작아도 공격가능성이 크다고 본다.

따라서 우리는 이동모호추론방법을 리용하여 DoS공격을 검출하기 위한 한가지 방법을 제안하였다. 그것은 이 방법이 침입검출의 실시간적인 요구를 만족시키고 계산량이 작기때문이다.[3] 만일 공격가능성이 큰 결과들이 련속 출현하고 그것들이 루적되여 어떤 턱값을 초과하면 공격행위로 판단한다.

DoS공격에서 대표적인 Synflood공격의 검출체계는 특징선택부분, 조건검출부분, 공격검출부분으로 이루어지는데 여기서 공격검출부분은 다음과 같은 4개의 부분으로 이루어진다.

모호발생부분: 여기서는 공격검출부분의 입력과 출력을 확정한 후에 Synflood공격검출의 주요한 인자인 DH와 DT의 성원함수를 정의한다. 이것들은 5개의 모호모임 즉 L+,

L, M, H, H+로 구분하며 매개의 의미는 더 작다, 작다, 중간, 크다, 더 크다이다.

모호규칙기지: 이것은 모호추론규칙으로 구성되며 규칙의 전제조건이 만족되여야 1개의 결론을 얻는다.

모호처리부분: 여기서는 모호추론규칙과 입력값에 따라서 공격가능성을 결정한다. 이때 모호모임 H+, H, M, L, L+가 대표하는 공격결정값의 초기값은 1, 0.8, 0.6, 0.4, 0.2로 설정한다.

공격결정부분: 이 부분은 공격가능성결정부분과 공격판단부분으로 나누어진다. 우선 공격가능성결정부분에서는 실험분석을 통하여 공격가능성을 결정하는데 턱값이 0.65이상인 파케트는 공격가능성이 크다고 본다. 한편 공격판단부분에서는 검출된 200개의 파케트에 대하여 판단을 진행한다. 만일 공격가능성이 큰 파케트수가 규정된 수의 개수를 초과하면 공격상태로 본다.

3. 실험결과분석

제안한 DoS공격검출체계에 대하여 실험에서 리용한 미끄럼창문의 크기는 100이다.

먼저 공격콤퓨터수의 증가에 따라서 실험을 진행하고 다음 공격자료기지 DARPA 98을 리용하여 실험을 진행하였다.

실험콤퓨터의 장치적조건은 CPU 3GHz, 주기판 915, 내부기억 512MB이다.

실험결과를 표에 주었다.

표. DoS공격도구와 DARPA 98자료기지를 리용한 공격검출시간의 비교결과

리용된 도구와 자료기지	턱값	제기한 방법에 의한 검출시간/s	선행한 방법에 의한 검출시간/s
DoS Tool	0.65	1.460 3	1.463 7
DoS Tool	0.7	1.461 1	1.462 8
DARPA 98자료기지	0.65	1.461 4	1.462 7
DARPA 98자료기지	0.7	1.436 7	1.437 1

표에서 보는바와 같이 제안한 방법의 평균검출시간이 선행한 방법보다 빠르다는것을 알수 있다.

맺 는 말

DT와 DH를 리용한 DoS공격검출방법을 제안하고 원천코드공개형침입검출체계 Snort 및 그것의 확장성을 리용하여 개발을 진행하였다. 그리고 망침입자료기지 DARPA 98을 리용하여 실험을 진행하였다.

제안한 방법은 다른 방법에 비하여 검출시간이 빠르고 계산량이 적으며 침입검출에 유효하므로 여러가지 응용분야에 적용할수 있다.

참 고 문 헌

[1] H. Mohamadi et al.; 2nd Asia International Conference on Industrial Electronics and Applications, 439, 2008.

[2] Zhao Bo et al.; 3rd IEEE Conference on Industrial Electronics and Applications, 36, 2008.

[3] L. Jingjiao et al.; IEEE Computer Society, 297, 2010.

주체105(2016)년 6월 5일 원고접수

A Method of DoS Attack Detection based on Removal Fuzzy Reasoning

Ho Chol Man, *Kwak Son Il*

This paper explains a kind of fuzzy reasoning method and its application on DoS attack detection. Test results explained that the proposed method is faster than others and it is effective on DoS attack detection.

Key words: fuzzy reasoning, synflood attack, DoS attack detection