

논문 2007-44TC-3-5

Low-rate TCP 공격 탐지를 위한 스케일링 기반 DTW 알고리즘의 성능 분석

(Performance Evaluation of Scaling based Dynamic Time Warping Algorithms for the Detection of Low-rate TCP Attacks)

소 원 호*, 심 상 현**, 유 경 민**, 김 영 천**

(Won-Ho So, Sang-Heon Shim, Kyoung-Min Yoo, and Young-Chon Kim)

요 약

본 논문에서는 최근 새롭게 발견된 low-rate TCP (LRT) 공격과 이 공격을 감지하기 위한 DTW (Dynamic Time Warping) 알고리즘을 분석하고 공격 검출에 대한 성능 향상을 위한 스케일링 기반 DTW (Scaling based DTW; S-DTW) 알고리즘을 소개한다. Low-rate TCP 공격은 대용량 트래픽을 사용한 기존 서비스 거부 공격과는 다르게 공격 트래픽의 평균 트래픽 양이 적어서 기존 DoS 공격에 대한 감지 방식으로는 검출되지 않는다. 그러나 LRT 공격은 주기적이고 짧은 버스트 트래픽으로 TCP 연결의 최소 재전송 타임아웃 (Retransmission Timeout: RTO)에 대한 취약성을 공격하기 때문에 패턴 매칭으로 공격 감지가 가능하다. 기존 메커니즘에 의한 감지 기법은 공격 패턴의 입력 샘플 템플릿을 기준으로 입력 트래픽이 정상 트래픽인지 또는 공격 트래픽인지를 판별한다. 이 과정에서 입력 트래픽의 특성에 따라서 DTW 알고리즘은 정상 트래픽을 공격 트래픽으로 오판하는 문제점을 갖는다. 따라서 본 논문에서는 이러한 오판을 줄이기 위하여 기존 DTW 알고리즘의 전처리 과정인 자기상관 (auto-correlation) 처리를 분석하여 오판을 규명한다. 또한 스케일링 기반으로 자기상관 처리 결과를 수정하여 공격 트래픽과 정상 트래픽의 특성의 차이를 증가시킴으로써 DTW 알고리즘에 의한 공격 감지 능력을 향상시킨다. 마지막으로 다양한 스케일링 방식과 표준편차에 의한 트래픽 분석 방법도 논의된다.

Abstract

In this paper, low-rate TCP attack as one of shrew attacks is considered and the scaling based dynamic time warping (S-DTW) algorithm is introduced. The low-rate TCP attack can not be detected by the detection method for the previous flooding DoS/DDoS (Denial of Service/Distributed Denial of Service) attacks due to its low average traffic rate. It, however, is a periodic short burst that exploits the homogeneity of the minimum retransmission timeout (RTO) of TCP flows and then some pattern matching mechanisms have been proposed to detect it among legitimate input flows. A DTW mechanism as one of detection approaches has proposed to detect attack input stream consisting of many legitimate or attack flows, and shown a depending method as well. This approach, however, has a problem that legitimate input stream may be caught as an attack one. In addition, it is difficult to decide a threshold for separation between the legitimate and the malicious. Thus, the causes of this problem are analyzed through simulation and the scaling by maximum auto-correlation value is executed before computing the DTW. We also discuss the results on applying various scaling approaches and using standard deviation of input streams monitored.

Keywords : Denial of Service, Shrew attack, Low-rate TCP attack, DTW algorithm, RTO

I. 서 론

* 정희원, 순천대학교 컴퓨터교육과
(Dept. of Computer Education, Sunchon National University, Korea)

** 정희원, 전북대학교 컴퓨터공학과
(Dept. of Computer Engineering, Chonbuk National University, Korea)

접수일자: 2007년2월22일, 수정완료일: 2007년3월14일

인터넷을 이용한 사이버 금융거래, e-교육, 그리고 행정처리와 같은 서비스의 증가는 개인 정보 보호와 QoS (Quality of Service) 보장, 그리고 공격으로부터 보호의 중요성을 증가시켜왔다. 하지만 빠른 속도로 새

로운 해킹 기술과 네트워크 공격 방법이 개발되고, 단순한 구조가 아닌 지능적인 해킹 기법이 지금의 보안 체계를 위협하고 있다. 특히 차세대통신망으로서 국내에서는 광대역통합망 (Broadband convergence Network; BcN)에 관한 연구가 활발히 진행되고 있는데 기존 단일망 네트워크 보안의 한계를 극복하는 것이 매우 중요하게 고려되고 있다^[1].

2000년 이후에는 DoS (Denial of Service)와 DDoS (Distributed Denial of Service) 같은 외부 공격이 주류를 이루고 있기 때문에 망 관점에서 이에 대한 대응 기법이 확보되고 운용되고 있으며 연구도 활발히 진행되고 있다. 특히 적은 공격 트래픽을 이용하여 TCP 기반 서비스의 질(quality)을 급격하게 저하시키는 LTA (Low-rate TCP Attack)은 기존의 DoS/DDoS 공격 감지 기법과는 다른 새로운 감지 및 대응 방법을 요구한다. 먼저 TCP 연결의 RTO (retransmission timeout) 값을 랜덤하게 설정하는 방식은 모든 TCP 송신측의 모듈이 이 방식으로 구현되어야 하는 현실적인 문제점을 갖고 있다^[2,3]. 예지 라우터 필터링 기법은 TCP 플로우별로 패킷의 도착 시간을 측정하여 공격 플로우를 구분하는 방법으로 많은 플로우 데이터를 관리해야 한다^[4]. 또한 플로우의 트래픽 양의 주파수 스펙트럼 분석을 이용한 감지 기법도 제시되었는데, 감지 능력이 탁월하지만 많은 정보의 관리와 처리에 대한 부담이 증가한다^[5]. 이상과 같은 플로우 기반 방식에 비하여 입력 링크^{**}에 대한 감지를 시도하고 DTW (Dynamic Time Warping)에 의해서 짧은 시간에 공격 링크를 감지하는 방식이 제시되었다^[6]. 이 방식은 상대적으로 고속으로 감지가 가능하지만 대응 방식은 DRR (deficit round-robin) 방식을 베퍼를 스케줄링함으로써 정상적인 트래픽의 QoS도 저하시킬 수 있다. 또한 단순히 음성 인식에 사용하던 접근 방법을 그대로 사용하기 때문에 정상적인 트래픽을 공격 트래픽으로 오판하는 경우가 발생한다.

본 논문은 BcN과 같은 광대역통합망에서 단계적 공격 감지와 협력적인 대응을 위한 메커니즘 제시를 위한 기초 단계로서 플로우가 아닌 입력 링크를 대상으로 LTA를 신속하게 감지하는 기법을 고려한다. 따라서 음

성 인식에 사용되는 DTW을 이용한 기존 LTA 탐지 기술의 단점을 분석한다. 또한 LTA 공격 탐지 능력을 향상시킬 수 있는 스케일링 기반 DTW를 제시하고 시뮬레이션을 통하여 평가한다.

II. 관련 연구

1. TCP 타임아웃 메커니즘

TCP/IP의 TCP 프로토콜 중에서 TCP Reno 방식은 망의 혼잡제어를 위하여 다음과 같은 방식으로 TCP 재전송 타이머를 운용하는데 이것이 DoS 공격의 취약성으로 이용된다. 즉, TCP 송신측은 패킷 전송 후 타이머가 타임아웃되거나 또는 동일한 ACK 신호를 3개 수신하면 패킷 손실로 가정한다. 만일 패킷이 손실되고 동일한 ACK 신호가 3개미만 전송되었다면 TCP 모듈은 재전송 타임아웃 (Retransmission TimeOut; RTO)동안 기다리며 혼잡 윈도우의 크기를 1로 설정하고 손실된 패킷을 다시 전송한다. 따라서 이 시간 동안 패킷의 처리율은 급격히 감속한다.

RTO의 하한값은 Allman과 Paxson의 실험에 의하여 제시되었는데 망의 모든 플로우의 RTO 값을 적어도 1초로 설정할 때 망의 혼잡이 제거되면서 성능이 가장 좋은 것으로 증명되었다. 일반적으로 TCP 송신측은 두 가지의 상태 변수를 갖고 있다. 하나는 SRTT (Smoothed Round-Trip Time)이고 다른 하나는 RTTVar (Round-Trip Time Variation)이다. SRTT와 RTTVar, 그리고 RTO의 관계는 다음과 같다.

첫 RTT의 측정값이 결정되기 전까지 RTO는 3초로 설정된다. 그리고 첫 RTT값이 R' 로 측정되면 $SRTT = R'$, $RTTVar = R'/2$, 그리고 $RTO = SRTT + \max(G, 4RTTVar)$ 로 결정되며 여기서 G 는 클럭 단위로서 일반적으로 100ms 이하이다. 만일 다음 RTT의 측정값이 R 이면, 송신측은 $RTTVar = (1 - \beta)RTTVar + \beta|SRTT - R'|$ 그리고 $SRTT = (1 - \alpha)SRTT + \alpha R$ 로 설정한다. 일반적으로 $\alpha = 1/8$ 그리고 $\beta = 1/4$ 가 권고된다. 그래서 TCP 송신측은 RTO를 다음 식과 같이 설정한다. $RTO =$

$$\max(\min RTO, SRTT + \max(G, 4RTTVar))$$

마지막으로 RTO의 운용을 그림 1로 설명한다. 시간 $t = 0$ 에 TCP 송신측이 n 번째 패킷을 전송했다고 가정하고 그때의 RTO는 1초로 설정되었다고 가정하다. 만일 n 이 손실되고 3개미만의 동일한 ACK를 받고, 1초인 RTO가 타임아웃 되었다고 가정하자. 그 순간 혼잡 윈

* 플로우 (flow)는 패킷의 근원지 IP 주소, 목적지 IP 주소, 근원지 포트 번호, 목적지 포트 번호, 프로토콜에 의해서 구분되는 패킷의 연속으로 정의된다.

** 입력 링크는 라우터에 입력되는 물리적인 포트를 의미하며 정상 트래픽과 공격 트래픽이 혼합되어 입력될 수 있음을 가정한다.

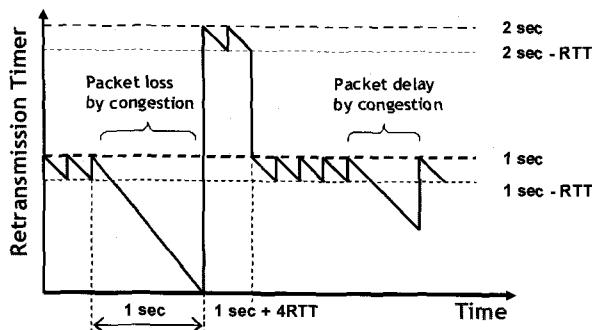


그림 1. TCP 재전송 타이머의 동작

Fig. 1. Behavior of TCP retransmission timer.

도우를 1로 하고 RTO 값을 2초로 설정하면서 ACK를 받지 않은 n 번째 패킷을 다시 전송한다. 그림에는 나타내지 않았지만 만일 또 손실이 발생한다면 $t = 3$ 초에 RTO 값이 4초로 설정되면서 위의 과정을 반복하게 된다. 하지만 아래 그림에서는 다시 보낸 패킷이 $t = 1+RTT$ 시간에 응답이 왔기 때문에 $n+1$ 과 $n+2$ 번째 패킷도 전송하여 정상적인 과정을 다시 수행하는 것을 보인다.

2. Low-rate TCP 공격

TCP 송신측의 RTO의 운용을 앞 절에서 확인했듯이 타임아웃에 의한 패킷의 손실은 혼잡 원도우의 크기를 1로 감소시킴으로써 TCP 플로우의 처리율을 급격하게 감소시킨다. 만일 그림 2와 같은 인터넷 모델의 에지 라우터에서 TCP 플로우들의 패킷 손실을 유발하는 트래픽이 그림 3과 같이 발생한다면 각 TCP 플로우들은 지수적인 backoff 상태에 접어들게 된다. 각 플로우의 RTO값이 감소될 수 있는 시간에 또 다른 공격이 감행된다면 RTO의 급격한 증가로 TCP의 처리율은 0에 근접한다. 예를 들면 최초의 공격이 0초에 시행되면 그때 TCP 송신측의 패킷이 손실된다. 1초 후에는 RTO의 타임아웃으로 다시 전송을 시도하지만 만일 다시 공격이 1과 $1 + 2RTT$ 시간동안 계속된다면 두 번째 패킷도

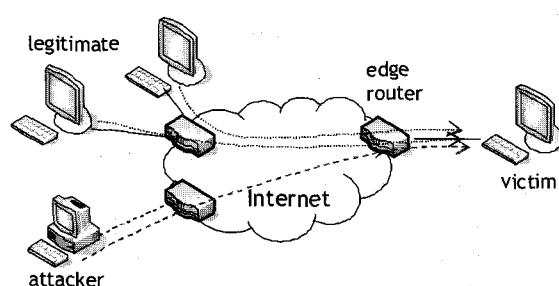


그림 2. Low-rate TCP 공격 모델

Fig. 2. Low-rate TCP attack model.

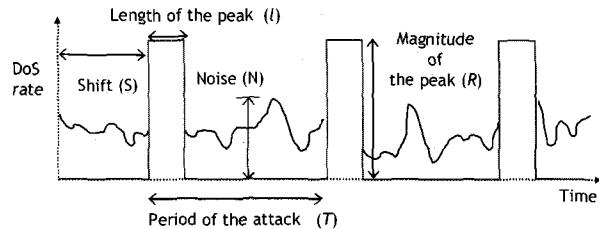


그림 3. 방형파 Low-rate TCP 공격 패턴

Fig. 3. Square-wave of low-rate TCP attack.

손실되어 TCP 송신측은 지수적 backoff 상태 ($RTO = 4$ 초)에 빠지게 된다.

이와 같은 일반적인 TCP 대상 low-rate 공격 패턴은 다음과 같은 파라미터에 의해서 정의된다. R 은 링크의 용량을 초과해야 하고, l 은 버퍼에서 패킷의 손실을 유발하지만 평균에 의한 공격 감지를 피할 수 있어야 한다. 마지막으로 T 는 추가적인 패킷의 손실을 유발시키는 RTO값으로 설정된다.

3. 공격 감지 및 대응 기법

가. 관련 대응 기법

기존 대응 방식으로 RTO 시간을 랜덤화하는 방식이 있다^[3]. 이 방식은 LRT 공격에 동기되지 않고 데이터를 전송할 수 있지만 제시된 기법의 구현과 TCP 연결의 성능이 낮은 문제점이 있다. [4]에서 제시한 방식은 패킷의 도착 시간을 관리하여 공격 플로우 도착 패턴과 정상 TCP 플로우의 패턴을 비교하는 방식이다. 이 방식은 단순하지만 중간 라우터에서 발생되는 공격에 의한 피해는 막지 못한다. 다음으로 공격 트래픽의 방형파 특성을 DFT (Discrete Fourier Transform)를 이용하여 주파수 영역에서 분석하는 방식으로 플로우 기반 감지가 가능하지만 플로우 단위로 관리를 해야 하기 때문에 오버헤드가 크다^[5].

마지막으로 자기상관 (이후부터 auto-correlation으로 표기함)과 DTW 알고리즘, 그리고 동적 프로그래밍을 이용한 감지기법으로 시간 영역에서의 패턴 매칭을 사용하는 방식이다^[6]. 이 방식은 입력링크의 전체 트래픽 양을 측정하여 공격의 감지하는 방식으로 위에서 소개한 플로우 기반의 방식보다 간단하여 에지 라우터뿐만 아니라 다른 라우터에서 쉽게 운용이 가능하다. 따라서 본 논문에서는 이 방식의 문제점과 해결 방안을 제시한다. 보다 자세한 내용은 다음 절에 설명한다.

나. DTW 기반 감지 기법

이 방식은 미리 정해진 공격패턴 (signature)과 입출력포트에서 트래픽을 모니터링 하여 얻은 입력 샘플을 DTW 알고리즘을 이용하여 비교하고 공격 트래픽과 정상 트래픽을 구분하는 방식이다. 감지 기법은 다음과 같다. 첫 번째 단계는 입출력 포트의 전송 용량을 통계적으로 검출하여 일반화 한다 (*statistical sampling*). 초당 100개의 샘플을 검출하며 검출 시간 (T_s)은 샘플링 이론이 근거하여 $T_s \geq 2T$ 를 만족하도록 결정한다. 본 연구에서는 $T_s = 3$ 초로 가정한다. 측정된 트래픽 용량은 일반화된 처리율 (normalized throughput)로 계산된다.

두 번째 단계는 샘플링과정에서 공격 패킷이 아닌 다른 패킷들도 처리율로 계산된다. 따라서 일정한 문턱값 β 를 설정하여 문턱값 보다 작은 값은 처리율을 0으로 결정한다 (*noise filtering*). 본 연구에서는 $\beta = 0.3$ 으로 가정한다.

세 번째 단계는 auto-correlation을 이용한 특성 추출 단계이다 (*feature extraction*). 이 방식은 입력 신호의 주기적인 특징(signature)을 추출한다. 만일 입력 신호가 n 개의 $(x_0, x_1, \dots, x_{n-1})$ 와 다른 경우는 $x_i = 0$ 으로 구성된 것으로 가정하자. Auto-correlation $A(k)$ 는 $A(k) = 1/(n-k) \sum_{i=0}^{n-k+1} x_{i+k} x_i$ 와 같이 계산된다.

네 번째 단계는 DTW 메커니즘을 이용한 패턴 매칭이다 (*signature comparison*). Auto-correlation에 의해서 특성이 추출되면 LRT 공격 패턴과 입력 신호의 유사도를 비교해야 하는데 이때 DTW 알고리즘을 사용한다. 이 방식은 두 개의 신호에 대한 유사도를 검사할 수 있는 강력한 방법이다.

두 개의 신호, 즉 템플릿 S 와 입력 신호 I 가 각각 $S = s_1, s_2, s_3, \dots, s_n$ 과 $I = i_1, i_2, i_3, \dots, i_m$ 같다고 가정 한다. DTW에 의해서 두 신호의 유사도를 비교하기 위하여 $n \times m$ 거리 행렬 D 를 구성할 수 있다. 이때 D 의 $d(x, y)$ 는 s_x 와 i_y 간의 Euclidean 거리를 의미하는 것으로 $d(x, y) = \|s_x - i_y\|$ 같이 계산된다. Warping 경로 W 는 행렬 D 의 인접한 원소들의 집합으로서 템플릿 S 와 입력신호 I 간의 사상(寫像 mapping)으로 정의된다. W 의 k 번째 요소는 $w_k = d(i_k, j_k)$ 로 정의 되며 $W = w_1, w_2, w_3, \dots, w_K$ 이고 $\max(m, n) \leq K \leq m + n + 1$ 이다. 구성되는Warping 경로는 몇 가지 제약을 따르며 많

은 Warping 경로가 이 조건을 만족한다^[6]. 그러나 신호의 유사도를 판별하기 위해서는 S 와 I 의 Warping 경로 비용이 최소인 것을 찾는데 관심을 갖는다. 즉, 식 (1)과 같은 $DTW^*(S, I)$ 값이 작을수록 두 신호는 유사하다. 이 최소값은 동적 프로그래밍 (Dynamic Programming; DP)방식으로 계산될 수 있는데 $\gamma(x, y) = d(x, y) + \min\{\gamma(x-1, y-1), \gamma(x-1, y), \gamma(x, y-1)\}$ 과 같다. 여기서 $1 \leq x \leq n$ 와 $1 \leq y \leq m$ 이다.

$$DTW^*(S, I) = \min \left(\sqrt{\sum_{k=1}^K w_k} \right) \quad (1)$$

III. DTW의 분석 및 문제점

DTW를 이용한 기존 방식을 분석하기 위하여 그림4와 같이 하나의 기준 공격 패턴(APT), 2가지의 공격 패턴(SPSB, RPGB), 그리고 하나의 정상 트래픽 패턴 (LEGI)을 생성한다. 기준이 되는 공격 패턴 APT는 LTA(T, l, R, S, N)으로 정의하며 본 논문에서는 각각 $T = 1.2$ 초, $l = 0.2$ 초, $R = 1$, $S = 0$, 그리고 $N = 0$ 으로 하나를 생성한다. 나머지 공격과 정상 트래픽은 각각 5000개의 서로 다른 샘플파일을 생성하였으며 실험에 적용한다. 입력 트래픽 신호들은 II장에서 설명한 것과 같이 auto-correlation을 먼저 적용한다. 그리고 이때 나온 결과 I 와 APT의 auto-correlation 결과 S 를

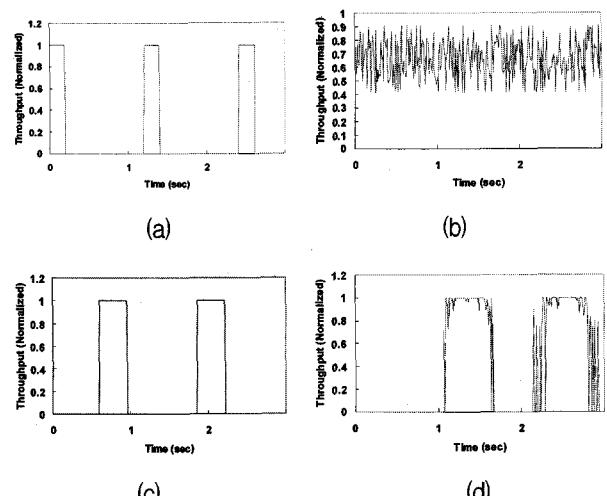


그림 4. DTW 분석을 위한 생성 트래픽 패턴: (a) Attack Pattern Template (APT), (b)Legitimate traffic (LEGI), (c) Strictly Periodic Square Burst (SPSB), (d) Random Periodic General Burst (RPGB)

Fig. 4. Generated traffic patterns for the analysis of DTW.

DTW 알고리즘으로 계산하고 마지막으로 동적 프로그램을 이용하여 식(1)을 만족하는 최소 Warping 비용을 계산한다.

그림 5는 분석에 의한 DTW값의 분포를 나타낸다. 각각 5000개인 공격과 정상 트래픽의 샘플 파일의 DTW 값의 분포를 알 수 있다. SPSB의 경우에는 대부분 50보다 작은 값에 분포되어 있는데 이것은 기준 공격 패턴인 APT와 유사성이 높은 것을 의미한다. 또한 RPGB의 경우도 많은 부분이 50이하에 분포되어 있다. 하지만 최대 112에 근접하는 경우도 발생한다. 정상 트래픽인 LEGI의 경우는 60부터 453까지 넓은 분포 특성을 보인다. 상대적으로 큰 값에 분포가 되기 때문에 공격 패턴과는 유사하지 않음을 나타낸다. 그러나 공격 패턴 SPSB, RPGB와 LEGI를 명확하게 구분할 수 있는 DTW값 (threshold)의 설정이 어렵다. DTW값이 50에서 120사이에서 발생되는 경우는 측정된 입력 트래픽이 공격인지 정상 트래픽인지 판단을 하기 어렵다. 물론 상대적으로 낮은 비율로 DTW값이 겹치지만 이 부분에서 공격과 정상 트래픽을 구분하기 위해서는 새로운 방법이 제시되어야 한다.

이 문제의 원인을 좀더 자세하기 분석하기 위하여 각 샘플의 auto-correlation값을 그림 6과 같이 APT와 각각 비교한다. SPSB의 경우는 DTW 값이 2로 최소값을 갖는 spsb23 파일과 최대값 61을 갖는 spsb1658를 보인다. 반면에 RPGB와 LEGI는 최소와 최대 DTW에 근접하는 2개의 파일을 각각 선택하여 비교한다. 여기서 주목할 부분은 rpgb4712(101)와 rpgb184(112), 그리고 legi42(60)와 legi2813(61)이다. RPGB의 경우는 입력 패턴만 보면 APT와 유사하지만 DTW 값이 높게 결정되며 LEGI의 경우는 유사하지 않지만 DTW 값이 낮거나 온다. 다시 말해서 패턴이 유사한 경우는 DTW 값이

낮게, 유사하지 않은 경우는 높게 결정되어야 한다. 따라서 기존 방식은 auto-correlation의 결과를 단순히 DTW 알고리즘으로 수행함으로써 공격과 정상 트래픽을 오판할 수 있는 확률이 증가한다.

IV. 스케일링 기반 DTW

1. 기본 알고리즘

이러한 문제를 해결하고 공격의 탐지력을 향상시키기 위하여 스케일링 기반 DTW를 제안한다. 주요 부분인 특성 추출부분은 다음과 같다.

- Auto-correlation 결과 중 최대값 A_{\max} 를 결정한다.
- Auto-correlation 결과 $X(x_0, \dots, x_{n-1})$ 를 A_{\max} 값을 기준으로 스케일링하여 X' 를 계산한다. 즉, $x'_i = x_i / A_{\max}$ 이다.
- 공격 템플릿(APT)도 스케일링 한다.
- 스케일링된 auto-correlation값으로 DTW 알고리즘을 수행하고 동적 프로그래밍으로 최소 경로를 결정한다.

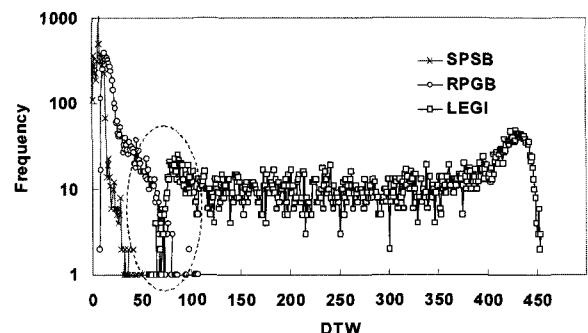
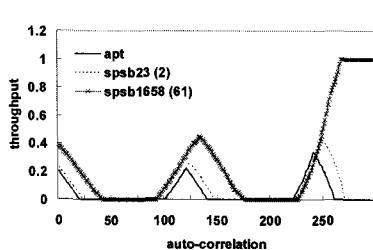
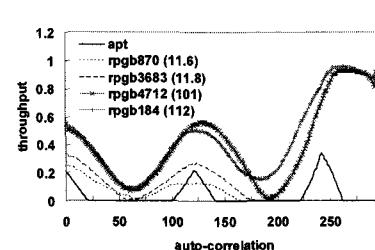


그림 5. DTW 결과의 확률 밀도 함수

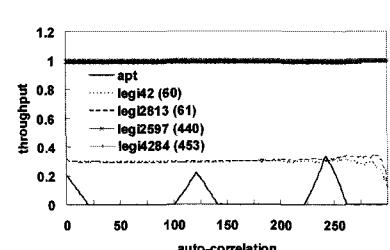
Fig. 5. Probability density functions of DTW values.



(a) APT vs. SPSB



(b) APT vs. RPGB



(c) APT vs. LEGI

그림 6. 입력 신호간의 자기 상관성 비교

Fig. 6. Comparison of auto-correlation values among different input signal.

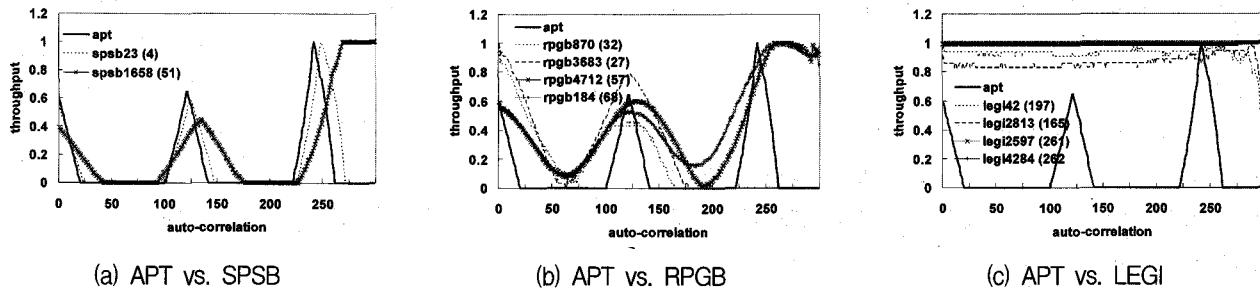


그림 7. 스케일링 기반에 의한 입력 신호간의 자기 상관성 비교

Fig. 7. Comparison of auto-correlation values among different input signals with simple scaling.

표 1. DTW값의 최소값과 최대값 비교

Table 1. Comparison of minimum and maximum values of DTW.

방식 패턴	기존 방식		제안된 방식	
	min	max	min	max
SPSB	0	61	2	51
RPGB	11	112	13	68
LEGI	60	453	104	262

제안된 방식으로 처리한 auto-correlation값이 그림 7에 보였다. APT에 대한 공격 샘플 (SPSB, RPGB)의 유사성은 높아졌으며 공격 샘플의 처리율의 평균값에 따른 auto-correlation값의 변화량도 줄일 수 있다. 예를 들면 spsb1658 샘플의 DTW값의 경우에 기존 방식에서는 61이였는데 제안된 방식에서는 51로 줄었으며 rpgb4712와 rpgb184는 각각 57과 68로 값이 크게 줄었다. 이것은 제안된 방식이 APT와 유사한 경우는 더욱 DTW값을 낮게 결정하며 정상 트래픽의 경우는 높게 결정함을 알 수 있다.

표 1은 제안된 방식과 기존 방식의 최소, 최대 DTW값을 보였으며 그림 8은 이때의 분포도이다. 기존 방식에서 DTW값이 낮게(높게) 결정된 경우가 높게(낮게) 나오는 경우가 SPSB, RPGB, 그리고 LEGI에서 발생된다. 하지만 DTW값이 70부터 100까지 분포되는 경우가 발생되지 않기 때문에 이 범위가 공격을 구분하는 문턱값으로 적용될 수 있다. 따라서 기존 방식의 문제점을 해결한다.

2. 관련 논의

제시된 스케일링 기반의 공격 감지 기법은 기준 패턴과 입력 신호의 auto-correlation 값을 단순히 비교하는 기존 방식의 문제점을 해결한다. 그러나 스케일링을 기준 패턴과 입력 신호에 모두 수행함으로써 전체적으로 공격과 정상 트래픽을 구분하는 능력은 향상되었으나

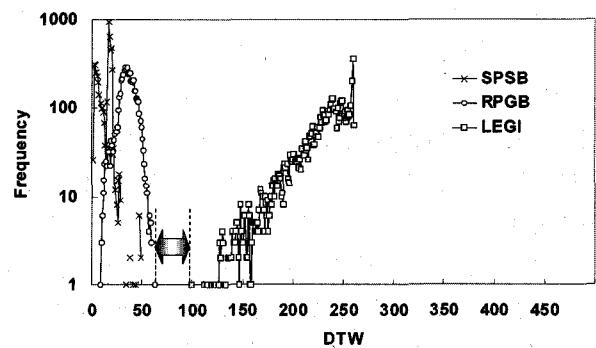


그림 8. 스케일링 기반 DTW 결과의 확률 밀도 함수

Fig. 8. Probability density functions of scaling based DTW.

해결해야 할 문제점이 존재한다. 첫째, 스케일링으로 낮은 DTW 값을 갖는 공격 신호가 DTW 값이 증가되는 현상이 발생된다. 둘째, 정상 신호의 경우도 스케일링으로 인하여 DTW 값이 낮게 나오는 경우가 있다.

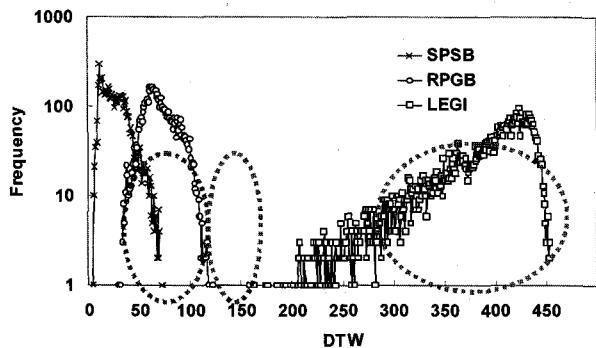
따라서 스케일링으로 인하여 DTW 값이 공격을 감지하는데 부정적으로 사용되는 경우를 최소화해야 한다. 즉, 공격 트래픽은 기준 패턴(APT)에 더 가깝게 DTW값이 결정되어야 하고 정상 트래픽은 기준 패턴과 유사성이 더욱 멀어지도록 해야 한다. 이를 위한 방안으로 본 논문에서는 두 가지 분석을 추가로 수행한다. 첫 번째는 스케일링 방식을 다양화하여 DTW 알고리즘을 수행하고 그 결과를 관찰한다. 두 번째는 입력 샘플의 특성을 SPSB, RPGB, 그리고 LEGI에 따른 표준 편차를 분석하여 새로운 특징을 검출하다.

가. 다양한 스케일링 방식의 적용

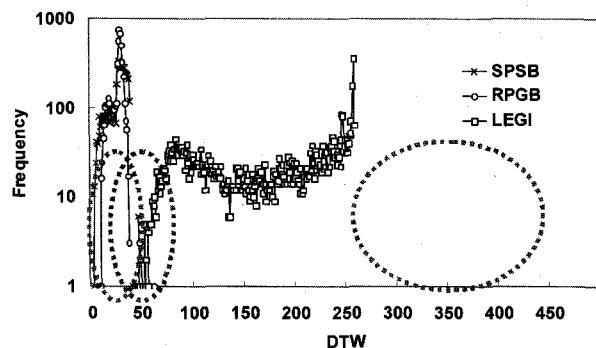
이를 위하여 본 논의에서는 제안된 스케일링을 표 2와 같이 분류한다. 먼저 입력 샘플과 기준 패턴을 그대로 사용한 SC0는 기준 DTW 알고리즘이고 SC1은 두 가지 모두 스케일링을 하는 제안된 방식이다. SC1과 SC2는 기준 패턴 또는 입력 샘플만을 스케일링하는 방

표 2. 스케일링 기법의 분류
Table 2. Classification of scaling.

종류	입력	APT	설명
SC0	0	0	기준 방식
SC1	0	1	APT만 스케일링
SC2	1	0	입력 샘플만 스케일링
SC3	1	1	제시된 방식



(a) SC1에 의한 DTW 값의 확률 밀도 함수



(b) SC2에 의한 DTW 값의 확률 밀도 함수

그림 9. 다양한 스케일링에 따른 결과 비교
Fig. 9. Comparison of results from various scaling types.

식으로 정의된다.

따라서 SC1과 SC2만 분석하여 개선 방향을 모색한다. 분석을 위한 실험 가정과 알고리즘은 앞에서 수행한 내용과 같다. 기준에 사용한 실험 가정과 알고리즘을 이용하여 분석한다.

그림 9는 SC1과 SC2에 의한 스케일링을 기반으로 수행된 DTW 값의 결과를 보인다. 그림 9a의 경우를 보면 입력 신호의 auto-correlation 결과만 스케일링한 경우로서 공격과 정상 트래픽을 쉽게 구분할 수 있다. 특히 정상 트래픽의 경우는 대부분 DTW 값이 200이상에 분포됨으로써 기준 패턴과 상이함을 나타낸다. 그러나 상대적으로 공격 신호의 DTW 값이 증가됨으로써 공격과 정상 트래픽을 구분하는 문턱값의 결정에 영향

을 준다. 반면에 그림 9b는 기준 패턴만 auto-correlation 후에 스케일링을 하고 DTW 알고리즘을 수행한 결과이다. SPSB와 RPGB의 DTW 값이 기준 패턴으로 근접하는 것을 알 수 있다. 하지만 정상 트래픽의 경우는 큰 효과를 기대할 수 있다. 따라서 두 방식 SC1과 SC2의 효과를 최대로 이용할 수 있는 방안이 모색되어야 한다.

나. 표준 편차에 의한 분석

본 논문에서 고려하고 있는 트래픽의 패턴을 보면 상대적으로 정상 트래픽은 평균값을 기준으로 처리율이 분포되고 공격 패턴은 최대 1과 최소 0사이에서 분포됨을 알 수 있다. 따라서 각 샘플에 대한 특성을 추출하기 위하여 샘플의 분포 범위를 측정할 수 있는 표준 편차 (standard deviation)를 이용한다. 표준 편차는 n 개의 입력 신호 x_0, x_1, \dots, x_{n-1} 이 있을 때 다음과 같이 계산된다.

$$\rho = \sqrt{\frac{1}{n-1} \sum_{i=0}^{n-1} (x_i - \mu)^2 / n}$$

여기서 μ 는 입력 신호의 평균이다. 입력 신호 LEGI, SPSB, 그리고 RPGB에 대하여 표준편차를 구하면 그림 10과 같은 표준편차 확률 밀도 함수를 구할 수 있다. 그림에서 알 수 있듯이 LEGI의 경우는 $\rho < 1.5$ 인 경우에 해당되며 공격 트래픽 RPGB의 경우는 $\rho > 0.4$ 에 분포된다. 또한 SPSB의 경우는 대부분 $\rho > 0.1$ 이상에 균등하게 분포됨을 알 수 있다. 따라서 입력 신호의 분포 특성은 정상 트래픽의 경우는 상대적으로 분포가 밀집되어 있고 공격 트래픽은 넓게 분포됨을 알 수 있다. 지금까지 논의된 내용을 정리하면 입력 신호의 표준편

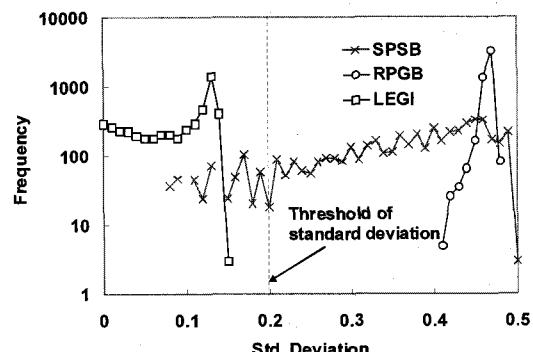


그림 10. 입력 신호의 종류에 따른 표준 편차
Fig. 10. Standard deviation of input samples.

차를 이용하여 신호의 분포 특성을 간단히 이해하고 이를 기준으로 스케일링 방식을 결정하면 정상 트래픽으로부터 공격 트래픽을 더욱 효과적으로 검출할 수 있다. 하지만 정상 트래픽의 특성과 공격 트래픽의 패턴이 일정하다는 가정으로 논의가 진해되었기 때문에 향후 추가적인 연구와 논의가 요구된다.

V. 결 론

본 논문에서는 auto-correlation에 의한 특성 추출 후에 스케일링을 사용으로써 LRT 공격 트래픽과 정상 트래픽을 더욱 명확하게 판별하는 메커니즘을 제안하였다. 단순히 DTW 알고리즘을 적용하는 기존 방식에 대한 문제점을 분석하여 입력 샘플의 패턴이 LRT 공격 또는 정상 트래픽인데도 이것에 대한 DTW 값이 서로 비슷하게 산출되는 원인을 규명한다. 공격과 정상 트래픽의 DTW 값이 유사하다는 것은 LRT 공격 검출의 기준을 정하기가 어렵다는 것을 의미한다. 따라서 스케일링 기법을 적용하는 스케일링 기반 DTW 방식을 제시하여 이러한 문제점을 줄일 수 있도록 하였다. 또한 패턴매칭의 기준이 되는 공격 트래픽과 정상 트래픽의 특성이 항상 일정하다고 가정하기 어렵기 때문에 다양한 스케일링 값 적용 방안과 표준편차를 이용한 분석 방법도 논의하였다. 향후에 기준 공격 패턴의 운용 방법과 다른 통계적 기법을 이용하여 보다 정확한 LRT 공격 탐지 기법에 대한 연구가 수행되어야 한다.

참 고 문 헌

- [1] 김영선, "BcN의 기술적 이슈와 전망," 한국정보통신기술협회, 2005.
- [2] A. Kuzmanovic and E. Knightly, "Low-rate TCP-targeted denial of service attacks," In Proc. ACM SIGCOMM, Karlsruhe, Germany, August 2003.
- [3] G. Yang, M. Gerla, and M. Y. Sanadidi, "Randomization: Defense against Low-Rate TCP-targeted Denial-of-Service Attacks," in Proc. IEEE Symposium on Computers and Communications, July 2004, pp. 345-350.
- [4] A. Shevtsekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Communications Letters, Vol. 9, No. 4, April 2005.
- [5] Y. Chen, K. Hwang, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis," J. Parallel Distributed Computing, Vol. 66, 2006, pp.1137-151.
- [6] H. Sun, J. C. S. Lui, and D. K. Y. Yau, "Defending Against Low-rate TCP Attacks: Dynamic Detection and Protection," in Proc IEEE Conference on Network Protocols (ICNP2004), Oct. 2004, pp. 196-205.
- [7] W. H. So, S. H. Shim, K. M. Yoo, B. J. Oh, Y. S. Kim, Y. C. Kim, "Scaling based Dynamic Time Warping Algorithm for the Detection of Low-rate TCP Attack," Proceedings of IEEK Fall Conf. 2006, Hanyang Univ., Korea, Nov. 2006 (in Korean)

저 자 소 개

소 원 호(정회원)
대한전자공학회 논문지
제43권 TC편 1-14 참고



심 상 현(학생회원)
2004년 전북대학교 컴퓨터공학과
학사 졸업.
2007년 현재 전북대학교 컴퓨터
공학과 석사 과정
<주관심분야 : 네트워크 보안, 네
트워크 운용, 시스템 관리>

유 경 민 (정회원)
대한전자공학회 논문지
제43권 TC편 5-11 참고
2007년 현재 전북대학교 컴퓨터공학과 박사과정

김 영 천(평생회원)- 교신전자
대한전자공학회 논문지
제29권 A편 제10호 참고
2007년 현재 전북대학교 전자정보공학부 교수