프로파일 모니터링을 이용한 네트워크 침입 탐지

김다은, 이성임

단국대학교 응용통계학과

연구배경

통계적 공정관리(SPC)에서는 일정한 시점마다 하나의 품질 특성치 또는 다수의 품질 특성치에 관한 관리도를 통해 품질 이상 유무를 모니터링한다. 한편 문제에 따라 특성치간의 관계로 설명하는 것이 더 적절한 경우가 있는데, 이러한 특성치간의 관계를 profile이라고 한다. profile은 선형 또는 비선형으로 나타날 수 있으며 프로파일 모니터링이란 profile이 시간에 따라 일정하게 나타나는지 모니터링하는 것을 말한다.

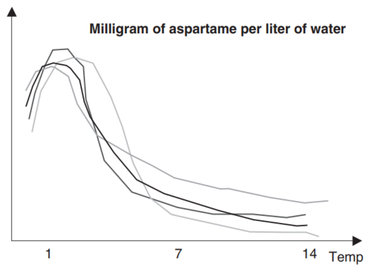

그림 1. 물 온도에 따른 용해되는 아스타팜의 양[1]

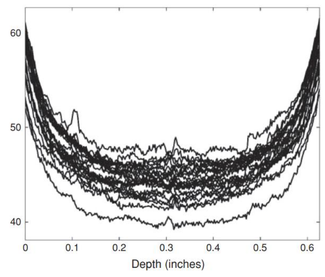

그림 2. 목재 깊이에 따른 밀도[2]

▶ 본 연구에서는 R2L 네트워크 공격 시 그림 3 으로부터 네트워크 패킷정보에 있는 2가지 주요 특성치가 선형함수관계가 나타남에 주목하여 프로파일 모니터링을 적용하고자 한다

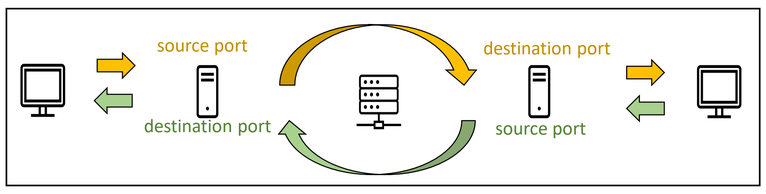

그림 3. 네트워크 패킷 정보

▶ 기존 연구는 설명변수가 고정된 경우를 주로 다루지만, 위 데이터에 적용하기 위해 설명변수가 고정되지 않은 경우로 확장 연구하고자 한다.

연구방법

profile 1	profile 2	…	profile m
(x_{11}, y_{11})	(x_{12}, y_{12})		(x_{1m}, y_{1m})
(x_{21}, y_{21})	(x_{22}, y_{22})		(x_{2m}, y_{2m})
⋮	⋮		⋮
(x_{n1}, y_{n1})	(x_{n2}, y_{n2})		(x_{nm}, y_{nm})

표 1. 프로파일 데이터

본 연구에서는 simple linear profile을 가정하고 표 1의 m개의 profile을 모니터링한다. Profile은 다음의 관계를 가정한다.

▶ 선형 프로파일

$$y_{ij} = \alpha_j + \beta_j x_{ij} + \epsilon_{ij}\ ,\ \ \epsilon_{ij} \sim N(0, \sigma^2)$$
$$i = 1,2,\dots,n,\ \ j = 1,2,\dots,m$$

profile마다 기울기와 절편이 일정하다는 것은 두 변수의 관계가 일정하며 관리상태 하에 있는 것을 의미한다. 따라서 기울기와 절편을 모니터링하는 관리도를 작성하여 다음의 두 가설을 동시에 검정한다.

$$H_{0A}: \alpha_1 = \alpha_2 = \cdots = \alpha_m (= \alpha)$$
$$H_{0B}: \beta_1 = \beta_2 = \cdots = \beta_m (= \beta)$$

다중비교로 인한 제1종 오류를 보정하기 위해 Bonferroni 수정을 한다.

Phase I 관리도

각 profile의 기울기와 절편은 최소제곱추정법으로 다음과 같이 추정한다.

$$\hat{\beta}_j = b_j = \frac{\sum_{i=1}^{n}(x_{ij} - \bar{x}_{\cdot j})(y_{ij} - \bar{y}_{\cdot j})}{\sum_{i=1}^{n}(x_{ij} - \bar{x}_{\cdot j})^2} = \frac{S_{xy(j)}}{S_{xx(j)}}$$

$$\hat{\alpha}_j = a_j = \bar{y}_{\cdot j} - b_j \bar{x}_{\cdot j}\ ,\ \ \bar{x}_{\cdot j} = \frac{1}{n}\sum_{i=1}^{n} x_{ij}\ ,\ \ \bar{y}_{\cdot j} = \frac{1}{n}\sum_{i=1}^{n} y_{ij}$$

불편 추정량	분산
$\hat{\alpha} = \bar{a} = \frac{1}{m}\sum_{j=1}^{m} a_j$	$Var[\bar{a}] = \frac{\sigma^2}{m^2}\sum_{j=1}^{m}\left(\frac{1}{n} + \frac{\bar{x}_{\cdot j}^2}{S_{xx(j)}}\right)$
$\hat{\beta} = \bar{b} = \frac{1}{m}\sum_{j=1}^{m} b_j$	$Var[\bar{b}] = \frac{\sigma^2}{m^2}\sum_{j=1}^{m}\frac{1}{S_{xx(j)}}$

표 2. 귀무가설하에 모수 α, β에 대한 불편 추정량과 분산

설명변수가 고정이 아닌 경우 새로운 방법의 신뢰구간으로 추정한 기울기와 절편의 관리한계선은 다음과 같다.

A1: $S_{xx(j)}$대신 $\bar{S}_{xx}$ 를 사용한 경우

기울기에 대한 관리한계선

$$(UCL_{\beta}^{*}, LCL_{\beta}^{*}) = \bar{b} \pm t\left(m(n-2); \frac{\alpha}{4}\right)\sqrt{\frac{\hat{\sigma}^2}{m^2}\left(\frac{(m-1)^2}{S_{xx(j)}} + \sum_{l\neq j}\frac{1}{S_{xx(l)}}\right)}$$

절편에 대한 관리한계선

$$(UCL_{\alpha}^{*}, LCL_{\alpha}^{*}) = \bar{a} \pm t\left(m(n-2); \frac{\alpha}{4}\right)\sqrt{\frac{\hat{\sigma}^2}{m^2}\left\{(m-1)^2\left(\frac{1}{n} + \frac{\bar{x}_{\cdot j}^2}{S_{xx(j)}}\right) + \sum_{l\neq j}\left(\frac{1}{n} + \frac{\bar{x}_{\cdot l}^2}{S_{xx(j)}}\right)\right\}}$$

A2: $S_{xx(j)}$를 사용한 경우

기울기에 대한 관리한계선

$$(UCL_{\beta}, LCL_{\beta}) = \bar{b} \pm t\left(m(n-2); \frac{\alpha}{4}\right)\sqrt{\frac{(m-1)\hat{\sigma}^2}{m\bar{S}_{xx}}}\ ,\ \ \bar{S}_{xx} = \frac{1}{m}\sum_{j=1}^{m} S_{xx(j)}$$

절편에 대한 관리한계선

$$(UCL_{\alpha}, LCL_{\alpha}) = \bar{a} \pm t\left(m(n-2); \frac{\alpha}{4}\right)\sqrt{\frac{\hat{\sigma}^2(m-1)}{m}\left(\frac{1}{n} + \frac{\bar{x}^2}{\bar{S}_{xx}}\right)}\ ,\ \bar{x} = \frac{1}{nm}\sum_{j=1}^{m}\sum_{i=1}^{n} x_{ij}$$

표 3. 기울기 b과 절편 a의 관리한계선

Phase II 관리도

A1: $S_{xx(j)}$대신 $\bar{S}_{xx}$ 를 사용한 경우

기울기에 대한 관리한계선

$$(UCL_{\beta}^{*}, LCL_{\beta}^{*}) = \bar{b} \pm t\left(m(n-2); \frac{\alpha}{4}\right)\sqrt{\hat{\sigma}^2\left(\frac{1}{S_{xx(k)}} + \frac{1}{m^2}\sum_{j=1}^{m}\frac{1}{S_{xx(j)}}\right)}$$

절편에 대한 관리한계선

$$(UCL_{\alpha}^{*}, LCL_{\alpha}^{*}) = \bar{a} \pm t\left(m(n-2); \frac{\alpha}{4}\right)\sqrt{\hat{\sigma}^2\left\{\left(\frac{1}{n} + \frac{\bar{x}_{k}^2}{S_{xx(k)}}\right) + \frac{1}{m^2}\sum_{l\neq j}\left(\frac{1}{n} + \frac{\bar{x}_{\cdot l}^2}{S_{xx(j)}}\right)\right\}}$$

표 4. 기울기 b과 절편 a의 관리한계선

▶ 이때 $\hat{\sigma}^2 = MSE = \frac{1}{m}\sum_{j=1}^{m} MSE_j$

사이버 공격탐지 판정 기준 : 새로운 자료로 $k\ (= m+1, m+2, \cdots)$번째 프로파일에서 추정한 절편과 기울기 $(a_k\ , b_k)$에 대하여 $(a_k < LCL_{\alpha}$ 또는 $a_k > UCL_{\alpha})$이거나 $(b_k < LCL_{\beta}$ 또는 $b_k > UCL_{\beta})$인 경우 새로운 프로파일 의 형태가 기존과 다르다고 판단하고, 이 경우 사이버 공격이 탐지된다고 판정한다

실제 자료 분석

R2L 공격은 Dos 등 다른 공격에 비해 상대적으로 탐지성능이 낮다고 알려진 공격으로 source bytes와 destination bytes의 linear 관계로 R2L 공격을 탐지했다.

▶ 데이터는 NSL-KDD를 사용해 n=8개씩 하나의 프로파일로 지정하고 α=0.01로 설정하였으며 profile 내 하나 이상의 공격이 존재할 경우 이상상태라 판단했다.

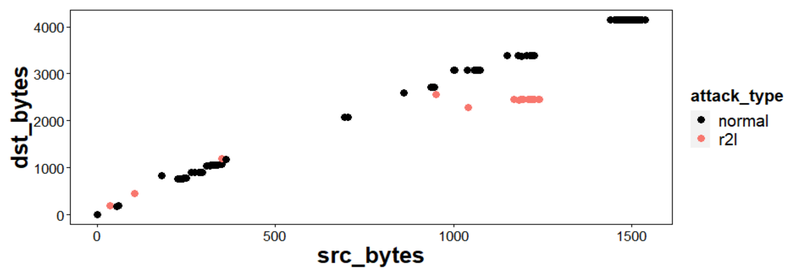

그림 4. NSL-KDD train dataset profile

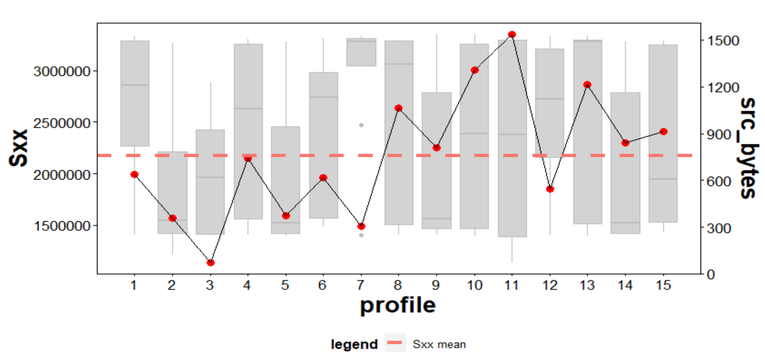

그림 5. profile별 설명변수(src_bytes)의 분포& $S_{xx(j)}$ 그래프

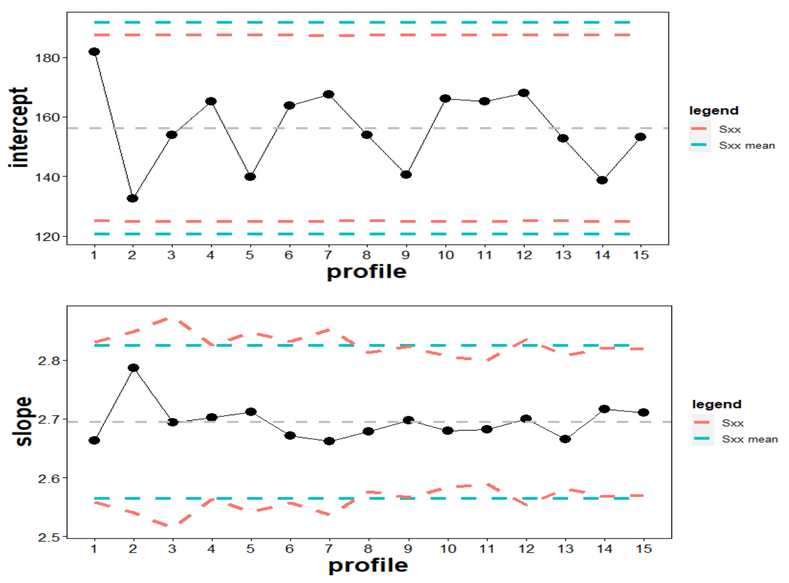

그림 6. Phase I 관리도의 결과

▶ 정확히 계산한 관리한계선과 $S_{xx(j)}$ 대신 $\bar{S}_{xx}$ 를 대입한 관리한계선은 큰 차이가 나지 않는다는 것을 확인할 수 있으므로 표 3의 A1 방법으로 적용할 수 있다.

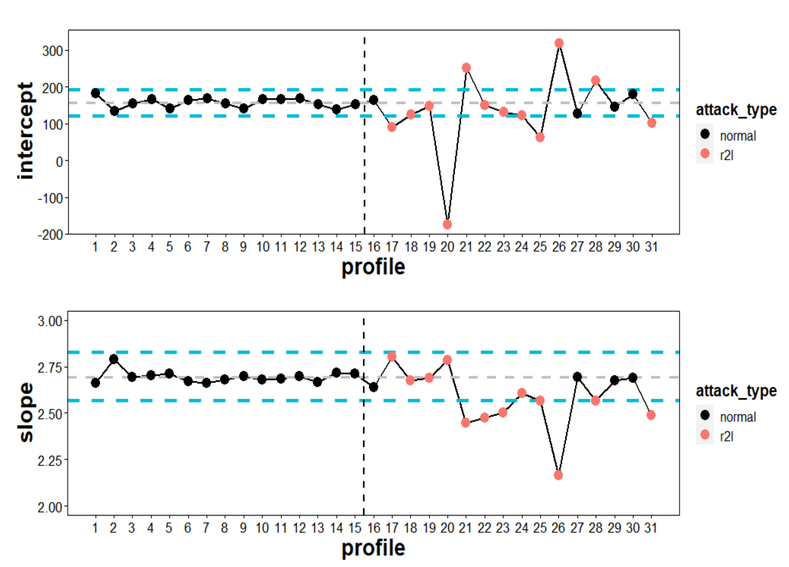

그림 7. 검증데이터의 Phase II 관리도의 결과

실제 / 예측	공격	정상	계	
공격	10	0	10	정확도: 87.5% 민감도: 83.33% 특이도: 100%
정상	2	4	6	
계	12	4	16	

표 5. 탐지 성능에 관한 정오 분류표

▶ 공격을 포함하는 새로운 12개의 profile 중 10개를 올바르게 잡았으며 정상상태만을 포함하는 4개의 profile은 모두 정상이라고 판단했다.

▶ NSL-KDD가 제공하는 각 네트워크 연결의 공격탐지 횟수와 비교하면 공격은 평균 42.2% 의 탐지능력을 보이고 있는 반면 profile monitoring은 83.3%의 높은 민감도를 보인다.

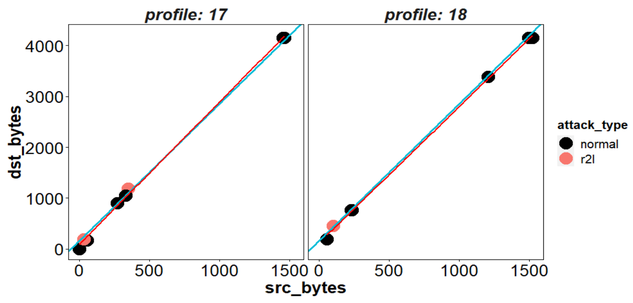

그림 8. 공격을 포함하는 profile이 탐지되지 못한 경우

▶ 관리상태 하의 파란선과 추정된 profile의 빨간 선이 거의 일치한다.

▶ 탐지횟수 변수와 비교해보면 각각 공격은 평균적으로 33%, 1%의 낮은 탐지율로 잡기가 어려웠다.

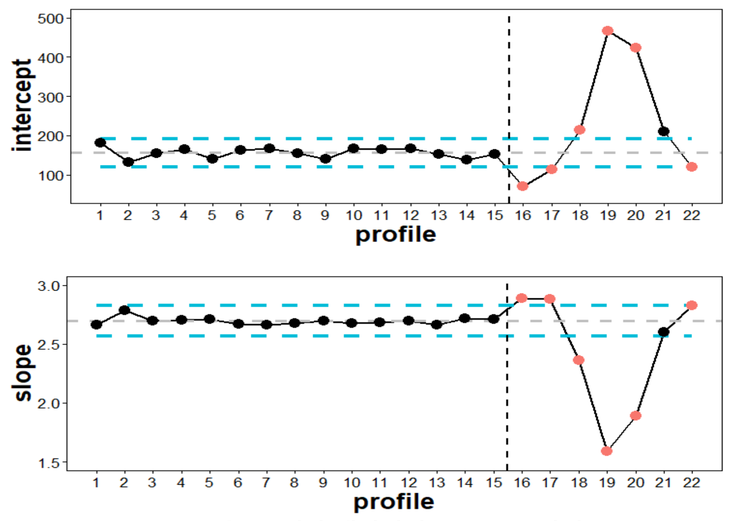

그림 9 . 평가 데이터의 Phase II 관리도

실제 / 예측	공격	정상	계	
공격	6	1	7	정확도: 85.7% 민감도: 100% 특이도: 0%
정상	0	0	0	
계	6	1	7	

표 6. 탐지 성능에 관한 정오 분류표

▶ 공격을 포함하는 6개의 profile과 정상상태만을 포함하는 하나의 profile을 전부 공격이라 판단했다.

▶ 탐지횟수 변수에서 공격은 평균 42.2%의 탐지능력을 보이고 있는 반면 profile monitorin은 100%의 민감도를 보인다.

결론 및 토의

▶ Phase II 선형 프로파일 모니터링 시 프로파일마다 설명변수가 고정되지 않은 경우에도 설명변수의 분포가 크게 다르지 않다면, 과거 프로파일로부터 Sxx(j)를 평균하여 사용하는 것으로 확장 가능하다는 것을 알 수 있다.

▶ NSL-KDD 자료는 21번의 적합모형으로부터 각 공격을 탐지한 횟수를 제공하는데, 본 연구의 검증자료와 평가자료에서 사용한 R2L 공격은 평균 42.2%의 탐지능력을 보인 것으로, 공격 탐지가 낮았던 자료임을 알 수 있다. 본 논문에서 선형 프로파일을 구성하여 공격을 탐지한 경우 민감도가 평균 91.7%로 매우 높게 나타남을 알 수 있다.

▶ 다만 기존 모형은 개별적인 네트워크 패킷을 사용하고, 본 연구에서는 n개의 패킷을 한 단위로 사용하여 공격 탐지에 대한 시차가 늦어질 수 있지만, 탐지성능 면에서 매우 효과적임을 알 수 있다.

▶ 또한 Sklavounos 등.(2019)[3] 이 제안한 한 개의 특성치만 사용한 EWMA 관리도 성능과 비교했을 때 특성치에 대한 제약 조건도 없이 훨씬 뛰어난 탐지성능을 보이는 것을 알 수 있었다.

▶ 본 연구는 사이버 공격이 없는 경우 네트워크 패킷 특성치 간 프로파일 관계가 일정하다는 가정하에 진행한 것으로, 특성치 간 프로파일 관계에 대해 확장 연구할 필요가 있다.

참고문헌

[1] Kang, L., and Albin, S. L. (2000). "On-Line Monitoring When the Process Yields a Linear Profile" Journal of Quality Technology, 32, 418-426

[2] Walker, E. and Wright, S. P. (2002). Comparing curves using additive models. Journal of Quality Technology, 34, 118–129.

[3] Dimitris Sklavounos, Aloysius Edoh and Markos Plytas. (2019). "Statistical Process Control Method for Cyber Intrusion Detection(DDoS, U2R, R2L, Probe)"

[4] Rassoul Noorossana, Abbas Saghaei and Amirhossein Amiri. (2011). *Statistical Analysis of Profile Monitoring.* John Wiley & Sons, Inc.

[5] Douglas C.Montgomery. (2013). *Introduction to statistical quality control.* John Wiley & Sons, Inc.

[6] Keunpyo Kim, Mahmoud A. Mahmoud, and William H. Woodall. (2003). "On The Monitoring of Linear Profiles"