논문 17-42-06-10 The Journal of Korean Institute of Communications and Information Sciences '17-06 Vol.42 No.06
https://doi.org/10.7840/kics.2017.42.6.1167

SCADA 네트워크 다양성을 반영한 플로우 화이트 리스트 생성

정 우 석[◆], 윤 정 한[*], 김 신 규[**], 심 규 석[***], 김 성 민[****], 김 명 섭[°]

Flow Whitelists Creation Reflecting the Diversity of Scada Networks

Woo-Suk Jung[◆], Jeong-Han Yun[*], Sin-Kyu Kim[**], Kyu-seok Shim[***],
Sung-Min Kim[****], Myung-Sup Kim[°]

요 약

SCADA 시스템은 최근 비즈니스 시스템과의 통합으로 인해 개방형 시스템으로 전환됨에 따라 보안상 취약점들이 증가하고, SCADA 시스템을 대상으로 한 사이버 공격이 고도화·지능화 되고 있다. SCADA 시스템의 보안 문제 해결을 위해 화이트리스트를 기반으로 한 제어시스템의 보안기법이 각광받고 있다. 화이트리스트 보안 기법의 기본은 ACL을 생성하는 것이다. 기존에 트래픽의 지역성을 활용하여 ACL을 자동으로 생성하는 연구가 있었지만, ACL 생성을 위해 사용하는 threshold가 고정되어 있어 적용 사이트마다 다른 트래픽의 특성을 반영하지 못한다는 단점이 존재한다. 본 논문에서는 SCADA 네트워크 다양성을 반영하기 위하여 기존 시스템에 threshold를 가변적으로 적용하고, 동적 서버에 의한 통신관계도 도출하는 방안을 추가하였다. 제안하는 시스템은 실제 SCADA 네트워크 트래픽에 적용을 통하여 타당성을 증명하였다.

Key Words : Industrial Control System, SCADA, Whitelist, Traffic Locality

ABSTRACT

Due to recent integration of SCADA systems with business systems, SCADA systems became open(unprotected), leading to not only security vulnerabilities increase but also sophisticated and intelligent cyber-attacks specifically targeting SCADA systems. A whitelist based security control technique that has attracted a lot of attention, is an emerging systems control, currently can be applied to solve security problems of the SCADA system. The basics of whitelist security techniques are to create ACLs. Although tere have been studies to automatically generate ACLs based on the locality of traffic, there is a disadvantage in that the threshold used for ACL creation are fixed and thus can not reflect the characteristics of different traffic for each applicable site.

※ 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터(No. 2017-0-00513-001)의 지원을 받아 수행된 연구임
◆ First Author : Korea University Department of Computer and Information Science, hary5832@korea.ac.kr, 학생회원
° Corresponding Author : Korea University Department of Computer and Information Science, tmskim@korea.ac.kr, 종신회원
* National Security Research Institute, dolgam@nsr.re.kr
** National Security Research Institute, skkim@nsr.re.kr
*** Korea University Department of Computer and Information Science, kusuk007@korea.ac.kr, 학생회원
**** Korea University Department of Computer and Information Science, gogumiking@korea.ac.kr, 학생회원
논문번호 : KICS2017-02-045, Received February 16, 2017; Revised May 11, 2017; Accepted June 5, 2017

In this paper, we apply variable threshold to existing system to reflect diversity of SCADA network, and also we added a method to derive communication relation by dynamic server. We demonstrate the feasibility of the proposed system in this paper by applying the real SCADA network traffic.

Ⅰ. 서 론

스마트 미터와 같은 새로운 유틸리티가 도입될 뿐만 아니라 통합이 강화됨에 따라 사이버 공격에 대한 새로운 취약성이 드러날 수 있으므로 SCADA 시스템은 네트워크 보호를 위한 네트워크 침입 탐지 시스템(IDS)이 필요하다[6]. 최근 연구를 통해 access control 화이트리스트, 프로토콜기반 화이트리스트, 행위기반 규칙을 계층화 시킨 IDS 시스템을 SCADA에 특화된 차세대 IDS가 제안되었다[9]. 본 논문에서는 새로운 IDS 프레임워크의 제안이 아닌 IDS에 사용되는 화이트리스트를 대상 SCADA 네트워크의 지역성을 반영하여 생성하는 방법에 대해 제안한다.

제어시스템의 보안에 대한 연구는 크게 호스트 기반 접근 방법과 네트워크 기반 접근 방법으로 나누어진다. 해당 호스트에 보안 Agent를 설치해야하는 호스트 기반 접근 방법의 경우 SCADA 시스템에 설치 및 적용하기 힘들다는 한계점을 가지고 있다.

네트워크 기반 접근 방식은 다시 악의성이 입증된 것들을 차단하는 블랙리스트 보안 기법과 안전이 증명된 것만을 허용하는 화이트리스트 보안 기법으로 나누어진다.

SCADA 시스템의 경우 외부와 물리적으로 완전히 단절되어 있어 블랙리스트를 업데이트 하는데 어려움이 있다. 또한 블랙리스트를 업데이트하기 위해 사용하는 access point가 오히려 외부에 취약점으로 변할 수 있다는 단점을 가지고 있다. 높은 안정성과 신뢰성을 필요로 하는 제어시스템에서 새로운 공격에 대하여 해당 시그니처가 생성 되어야만 공격을 차단할 수 있는 블랙리스트 기법은 적절하지 않다. 블랙리스트 보안 기법이 가지는 이러한 단점과 제어시스템이 가지는 안정적인 구조 그리고 특정 응용만 동작하는 환경이라는 특수성 때문에 화이트 리스트 기반 기법의 적용이 많이 논의되고 있다.

화이트 리스트 보안 기법은 안전이 증명된 것만을 허용하는 것으로 악의성이 입증된 것들을 차단하는 블랙리스트(blackllist) 보안 기법과 상반되는 보안 방식이다. 화이트리스트는 보안성은 높지만 편의성을 심각하게 저해할 수 있어 제한적인 영역에서만 사용되었지만, 특히 리소스가 적고 시스템 동작 패턴 또는 네트워크 통신 트래픽이 규칙적인 제어시스템 환경에서 보안을 담보할 수 있는 효율적 방안으로 주목 받고 있다[8].

이에 따라 SCADA 네트워크에 적용하기 위한 화이트리스트 생성 방법에 대한 다양한 연구가 진행되고 있다[1,2]. 버스트 이전과 이후의 패킷들의 arriving time보다 짧은 inter-arriving 시간을 가지는 연속된 패킷들의 집합인 버스트를 사용하여 화이트리스트를 생성하는 연구[1]와 기존의 방법으로 표현하기 어려웠던 SCADA 시스템 내에서 발생하는 FTP 서비스를 화이트리스트로 표현하는 방법에 대한 연구[7] 등이 제안되었다.

제어망 내부 전체를 감시함에 있어서 트래픽 모니터링 capacity의 한계와 미러링 드랍 등으로 인해 핸드쉐이킹을 확인 수 없는 경우가 발생한다. 그리고 한 번 세션을 맺고 수주-수달을 사용하는 경우 역시 핸드쉐이킹을 확인 할 수 없는 경우가 발생한다. 기존 플로우 화이트리스트 추출 알고리즘[2]은 이런 문제를 해결하기 위하여 트래픽의 지역성을 기반으로 한 플로우 화이트리스트를 생성하는 방법을 제안했다.

기존 알고리즘[2]은 지역성을 활용하여 플로우 화이트리스트를 추출하는 과정에서 고정된 threshold를 사용한다. 하지만 고정된 threshold를 사용하게 되면 적용하는 사이트마다 달라지는 트래픽의 특성을 반영할 수 없다는 한계점을 가진다. 본 논문에서는 적용 사이트마다 달라지는 트래픽 특성을 반영할 수 있도록 기존 연구[2]에 variable threshold를 적용하여 플로우 화이트리스트를 추출하는 방법을 추가, 확장한 시스템을 제안한다.

2장에서는 본 논문에서 개선하고자 하는 기존 플로우 화이트리스트 추출 알고리즘을 소개하고, 3장에서는 기존 플로우 화이트리스트 생성 방법[2]이 가지는 문제점을 살펴본다. 4장에서는 본 논문에서 제안하는 기존 알고리즘 개선안을 서술하고, 5장에서는 실험을 통해 기존 알고리즘과 본 논문의 개선안을 분석하고, 6장에서는 결론 및 향후 연구에 대해 차례로 서술한다.

Ⅱ. Background : 트래픽 지역성을 반영한 플로우 화이트리스트 생성

본 장에서는 본 논문에서 개선하고자 하는 기존 플로우 화이트리스트 추출 알고리즘을 소개한다. 기존 알고리즘이 사용하는 트래픽의 지역성인 DC(Degree Centrality)와 LFP(Locally Frequently-Used Ports)에 대하여 간단히 소개한 후 알고리즘을 설명한다.

2.1 Degree Centrality

통신대상의 IP-port를 하나의 노드로 나타내고 플로우를 노드 간의 링크로 나타내었을 때 그림 1은 사이트 A에서 다섯 시간 동안 발생한 TCP와 UDP 플로우를 나타낸 것이다. 클라이언트 포트를 랜덤하게 할당하여 사용하거나 하나의 서버가 여러 개의 클라이언트와 통신하는 특성에 따라 서버 노드가 다수의 클라이언트가 연결되어 수많은 연결을 발생함을 알 수 있다.

DC는 노드와 연관되어 있는 링크의 수를 의미하는 트래픽의 지역성이다. DC는 incoming 링크들의 개수인 in-degree flow와 outcoming 링크들의 개수인 out-degree flow로 나누어진다. 기존 알고리즘에서는 DC가 큰 노드를 서버 노드, 서버 노드의 port가 고정으로 사용되고 있다고 가정하여 플로우 화이트리스트를 도출한다.

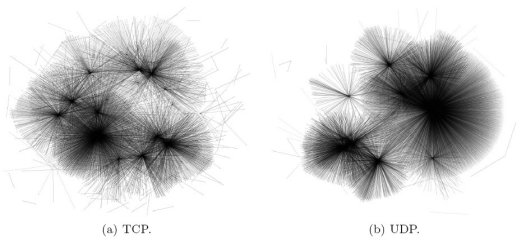

그림 1. 사이트 A에서 다섯 시간동안 발생한 플로우[2]
Fig. 1. Graphs of flows during a five-hour period at Site A[2]

2.2 Locally Frequently-Used Ports

DC만을 적용하여 플로우 화이트리스트를 생성할 경우 하나의 클라이언트와 다수의 서버가 통신을 하거나 클라이언트 포트를 고정하여 사용하는 통신의 경우 잘못된 규칙이 생성되는 문제점이 있다. 이를 해결하기 위하여 DC를 적용하기 전에 사용 되는 것이 LFP 개념이다.

LFP(Locally frequently port)는 빈번히 사용되는 포트를 의미한다. 이는 대상 트래픽에서 빈번하게 사용되고 있는 포트는 해당 사이트에서 고정으로 사용하는 port일 것이라는 가정이다. 이는 well-known port와 유사한 개념으로, 제어망마다 well-known port를 보안 등을 위해 변경하여 사용할 수 있으며 특정 제어프로토콜이나 제어서비스가 사용하는 고정port를 찾기 위한 것이다. 일정 threshold 이상 발생하는 번호를 LFP 리스트로 추가하고, 이 리스트를 플로우 화이트리스트 생성 시 사용한다.

그림 2는 LFP가 적용되는 과정을 도식화 한 것이다. LFP는 Unit threshold와 Final threshold의 두 개의 threshold 값을 가진다. 매 시간의 트래픽에 적용되는 Unit threshold는 매 시간마다 모든 플로우를 읽어 해당 파일에 존재하는 모든 포트번호들에 대해 각각 몇 번 등장했는지를 계산하여, 계산된 값이 Unit threshold를 넘지 않는 경우 해당 값을 버린다. 만약 계산된 값이 Unit threshold를 넘는 경우 전체 시간에 해당 port가 등장하는 횟수를 더하여 다시 최종적으로 더해진 값이 Final threshold를 넘는지 비교하여, Final threshold를 넘는 경우 해당 포트 번호는 LFP 리스트에 저장한다.

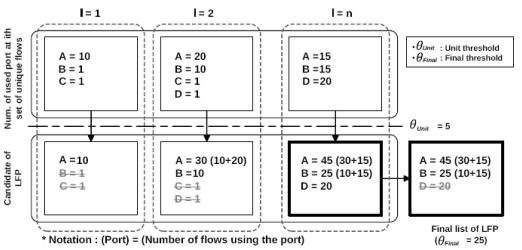

그림 2. Locally frequently-used port 추출[2]
Fig. 2. Locally frequently-used port extraction[2]

2.3 알고리즘

기존 플로우 화이트리스트 생성 과정은 알고리즘 1과 같다. 플로우를 입력으로 LFP를 먼저 추출하고, LFP를 사용하는 IP-port를 고정으로 가정하여 플로우 화이트리스트를 추출한다. 그 다음 DC를 계산하여 플로우 화이트리스트를 추출한다.

기존 연구[2]에서는 특정 SCADA 네트워크를 대상으로 하였기 때문에 고정된 threshold 값을 사용하였다. 따라서 호스트의 수, 트래픽 발생 빈도수 그리고 종류 등이 다른 다양한 SCADA 네트워크에 적용 시 그 특징을 잘 반영할 수 있다고 볼 수 없다. 따라서 본 논문에서는 다양한 SCADA 네트워크에 유연하게 대처하여 그 특징을 반영할 수 있는 시스템을 제안한다.

```
Input  : Flows
Output : whitelist
For each flow in flows do
    If IsInrule() == True then return
    End if
    If sPort or dPort ∈LFP then
        Addrules()
    End if
    If In-degree or Out-degree > θ_Port then
        Addrules()
    End if
End for
```

알고리즘 1. 플로우 화이트리스트 생성
Alg. 1. Flow whitelist generation

Ⅲ. 기존 알고리즘 문제점

본 장에서는 기존 알고리즘이 DC, LFP 결정하기 위해 threshold를 고정으로 사용하고 있는 문제점을 분석한다.

3.1 Overview

LFP와 DC에는 LFP unit threshold, LFP final threshold 그리고 DC threshold의 세 개의 threshold가 존재한다. LFP와 DC에서 threshold 값의 선정은 매우 중요하며, 그 이유는 threshold 값이 바로 화이트리스트를 생성할 타겟 SCADA 네트워크의 특징을 반영하기 때문이다. LFP의 unit threshold는 각 입력 트래픽 데이터에서 빈번한 포트를 결정하고, final threshold는 전체 입력 트래픽에서의 빈번 포트를 최종적으로 결정한다. 또한 DC threshold 역시 IP와 포트쌍이 총 몇 번 이상 발생할 경우 빈번한지를 결정하는 기준이기 때문이다.

3.2 실험

그림 3의 그래프는 Threshold의 변화에 따른 규칙의 개수 변화를 나타낸 것이다. 1시간을 기준으로 기존 플로우 화이트리스트 추출에 사용되는 고정 threshold인 LFP_UNIT_THRESHOLD 25, LFP_FINAL_THRESHOLD 100 그리고 DEGREE_THRESHOLD 10을 기준으로 작게는 0.05배, 크게는 25배까지 Threshold를 바꾸어 가며 실험하였다. 실험의 결과 현재 Threshold를 0.5배 하였을 때 생성되는

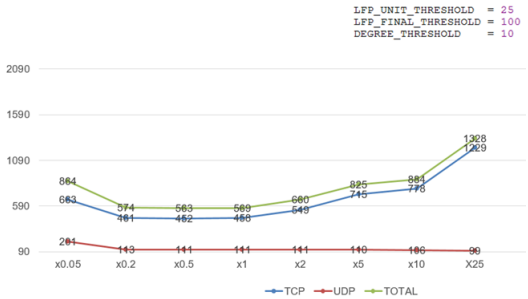

그림 3. Threshold의 변화에 따른 TCP, UDP 규칙 개수 변화
Fig. 3. Changes in the number of TCP and UDP as the threshold value changes

규칙의 개수가 가장 적으며, 0.5배를 기준으로 작아지거나 커질 경우 규칙의 개수가 증가하는 것을 확인 할 수 있다. 실험 결과를 분석해 보면 threshold가 너무 작아질 경우에는 트래픽 내에서 발생하는 모든 포트의 번호가 LFP list에 포함되게 되어 규칙의 개수가 증가하고, Threshold가 너무 커질 경우에는 LFP와 DC를 통해 규칙들이 생성되지 못하고, left flow로 5-tuple이 바로 규칙으로 생성되어 규칙의 개수가 증가함을 알 수 있다.

실험 결과를 통해 threshold 값이 달라질 경우 생성되는 화이트리스트의 결과가 달라지는 것을 확인 할 수 있었다.

Ⅳ. SCADA 네트워크 다양성을 반영한 플로우 화이트리스트 생성 알고리즘 개선

본 장에서는 본 논문에서 제안하는 SCADA 네트워크의 다양성을 반영한 플로우 화이트리스트 생성 시스템에 대해 설명한다.

4.1 Overview

그림 4는 본 논문에서 제안하는 시스템을 도식화

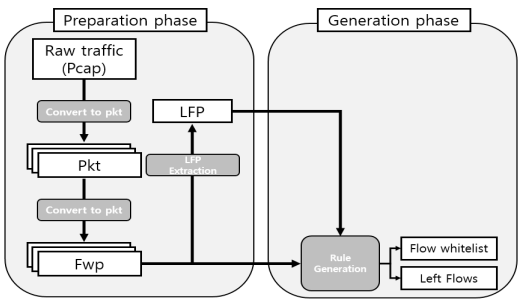

그림 4. 플로우 화이트리스트 생성 시스템
Fig. 4. Flow whitelist creation system

한 것으로 크게 두 부분으로 나누어진다. 첫 번째는 플로우 화이트리스트 생성을 위해 Pcap 포멧의 Raw traffic을 pkt 포멧으로, 다시 pkt 포맷의 트래픽 파일을 fwp 포멧의 입력 파일로 변환하는 Preparation 단계이고, 두 번째는 fwp 포멧의 입력 파일을 사용하여 실제로 플로우 화이트리스트를 추출하는 Generation 단계이다.

4.2 Generation

본 절에서는 호스트의 수, 트래픽의 발생 빈도수 그리고 종류가 다양한 SCADA 네트워크에 따라 LFP Unit threshold와 LFP Final threshold 그리고 DC threshold를 유동적으로 적용하기 위한 방법에 대하여 설명한다.

4.2.1 Variable LFP Unit threshold

LFP Unit threshold는 LFP Final threshold와 함께 플로우 화이트리스트 생성 방법 중 threshold의 입력으로 사용되는 여러 flow 파일들 각각을 읽어 Unit LFP list를 생성하는데 적용되는 threshold이다. 고정된 LFP Unit threshold를 사용할 경우 입력 데이터의 크기와 종류에 따라 생성되는 플로우 화이트리스트는 차이가 발생하게 된다. 본 논문에서는 이러한 문제를 해결하기 위하여 통계학에서 사용되는 68-95-99.7 규칙을 적용한다. 68-95-99.7 규칙은 정규 분포를 나타내는 규칙으로, 세 가지 경험적 규칙을 포함한다. 각각의 세 가지 규칙은 “약 68%의 값들이 평균에서 양쪽으로 1 표준편차 범위(μ±σ)에 존재한다.”, “약 95%의 값들이 평균에서 양쪽으로 2 표준편차 범위(μ±2σ)에 존재한다.” 그리고 “거의 모든 값들(실제로는 99.7%)이 평균에서 양쪽으로 3표준편차 범위(μ±3σ)에 존재한다.”이다.

본 논문에서는 68-95-99.7 규칙을 Variable LFP Unit threshold를 추출하는데 적용하기 위하여 포트별 매칭횟수 분석, 모든 포트번호와 각 포트별 매칭횟수 데이터를 사용하여 평균, 분산 그리고 표준편차를 구하였다.

기존 연구[2]에서 25로 고정하여 사용한 LFP unit threshold를 여러 SCADA 네트워크 트래픽에 적용을 통해 25의 threshold는 전체 포트번호 중 대략적으로 0.1%의 포트번호를 Locally Frequently하다고 판단함을 확인하였다. 실험 결과를 바탕으로 “약 99.9%의 값들이 평균에서 양의 방향으로 n표준편차 범위(μ±nσ)에 존재한다.”라는 공식에 대입하여, ‘n ≒ 0.2‘의 값을 도출할 수 있었다.

그림 5는 실험을 통하여 도출한 Variable LFP Unit threshold를 추출하는 식이다. 그림 5의 식을 통해 타겟 SCADA 네트워크의 포트 매칭 횟수가 상위 0.1%인 포트를 LFP로 추출할 수 있다.

추출된 식을 검증하기 위하여 각각 B, D, E 사이트에 식을 적용하였다. 그림 6은 그림 5의 Variable LFP Unit threshold 계산식을 각각 B, D, E 사이트에 적용하여 포트 매칭 횟수별 포트의 개수를 그래프로 나타낸 것이다. 그래프의 x축은 포트의 매칭 횟수이고, y축은 해당 매칭 횟수를 가지는 포트의 수이다. x값이 5이고, y값이 10인 지점은 5번 매칭된 포트의 번호가 총 10개란 뜻을 내포한다. B, D, E 사이트의 Variable LFP Unit threshold는 각각 13.5, 9.5 그리고 51.2가 추출되었고, 각 사이트의 Variable LFP Unit threshold를 기준으로 왼쪽 그래프의 넓이는 99.6%, 96.2% 그리고 99.9%로 나타났다. 실험을 통해 도출한 (μ+0.2σ)의 식을 이용한 Variable LFP Unit threshold 적용을 통해, 호스트의 수, 트래픽 발생 빈도수 그리고 종류가 다른 SCADA 네트워크에 적용해

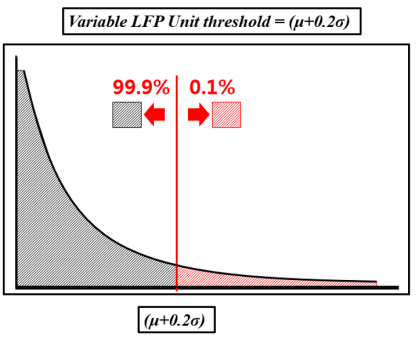

그림 5. Variable LFP Unit threshold
Fig. 5. Variable LFP Unit threshold

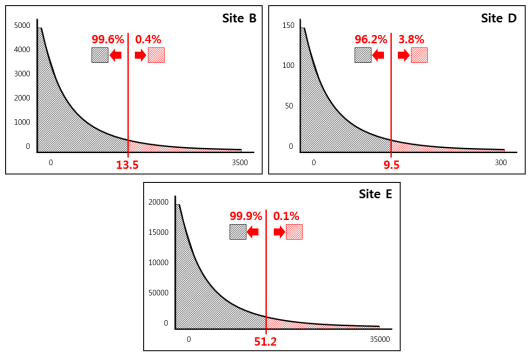

그림 6. 사이트 B, D, E의 포트 매칭 횟수별 포트 개수
Fig. 6. Number of ports followed by matching count at site B, D, E

도 의미 있는 LFP 리스트를 추출 할 수 있음을 증명하였다.

4.2.2 Variable LFP Final threshold

LFP Final threshold는 LFP Unit threshold와 다르게 입력 데이터의 단위에 종속적이지 않고, 총 입력 데이터 시간에 종속적이다. 총 6시간의 fwp 파일을 1시간 단위로 6개로 나누거나, 30분 단위 파일로 12개로 나누어도 전체 fwp 파일 내에 매칭된 각 포트별 매칭 횟수는 동일하기 때문이다. 예를 들어 6시간을 1시간 단위로 나눈 모든 fwp 파일에서 포트번호 2046번이 180번 매칭 되었다면, 30분 단위로 나눈 모든 fwp 파일에서도 포트번호 2046번이 매칭된 횟수는 180번으로 동일하다는 것이다. 본 논문에서 제안한 시스템의 Preparation 과정을 통해 생성된 fwp 파일은 flow를 시작 시간을 기준으로 생성하므로 총 입력 데이터 시간이 동일하다면 어떤 시간 단위로 나누어도 매칭된 각 포트별 매칭 횟수는 동일하다.

LFP Final threshold가 총 입력 데이터 시간에 종속성을 가지므로 전체 입력 파일에서 Variable LFP Unit threshold를 만족하는 비율인 Unit threshold Frequency는 기존 연구[2]에서 25와 100으로 고정하여 사용하는 LFP unit threshold와 LFP final threshold를 적용하여 생성한 LFP 리스트와 Variable LFP unit threshold를 만족하는 포트 리스트를 비교하여 95%로 정하였다.

실험을 통해 정한 Unit threshold Frequency에 시간 단위로 환산한 총 입력 시간을 곱하여 Variable LFP Final threshold를 구하는 계산식을 그림 7과 같이 도출하였다.

Variable LFP Final Threshold
= Total Input Time(hour) X Unit Threshold Frequency

그림 7. Variable LFP Final threshold
Fig. 7. Variable LFP Final threshold

4.2.3 Variable DC threshold

DC threshold는 LFP final threshold와 같이 총 입력 데이터 시간에 종속적인 threshold이다. DC threshold를 호스트 수, 트래픽 빈도수 그리고 종류가 다양한 SCADA 네트워크에 따라 variable하게 적용하기 위하여 기존 연구[2]에서 10으로 고정하여 사용한 DC threshold를 SCADA 네트워크에 적용하여 추출한 IP와 포트의 쌍 리스트와 총 입력시간이 다른 SCADA 네트워크 트래픽에서 추출한 모든 IP와 포트의 쌍의 DC 값을 비교하여 실험했다. 실험을 통해 DC를 만족하는 IP와 포트의 쌍은 시간당 2.5회 이상 발생하는 플로우로 정의하고, 그림 8의 Variable DC threshold 계산식을 도출하였다.

Variable DC Threshold = 2.5 X Total Input Time(hour)

그림 8. Variable DC threshold
Fig. 8. Variable DC threshold

V. 실 험

본 장에서는 본 논문에서 제안한 시스템의 타당성을 증명하기 위해 실제 SCADA 네트워크 트래픽에 적용 실험한다. 표 1은 실험에 사용된 SCADA 네트워크 트래픽으로 A 사이트를 제외한 나머지 6개의 사이트 들은 모두 각 사이트에서 12시간씩 수집한 트래픽이다.

표 2는 각 사이트별로 본 논문에서 제안한 시스템을 적용한 결과를 정리한 표이다. B 사이트의 경우 Variable LFP Unit threshold, Variable LFP Final threshold 그리고 Variable DC threshold가 각각 21, 239 그리고 30이 적용되었으며, 기존 시스템과 확장된 시스템을 통해 추출된 TCP LFP 리스트는 각각 81개와 15개, UDP LFP 리스트는 13개와 7개이다. 또한 기존 시스템과 확장된 시스템을 통해 추출된 TCP 화이트리스트는 각각 247개와 312개, 그리고 UDP 화이트리스트는 각각 65개와 343개이다.

표 1. 실험에 사용된 트래픽
Table 1. Test set spec

Site	Size of Traffic	No. of Flows
A	492 GB	9,198,938
B	14.6 GB	234,259
C	3.14 GB	13,729
D	10.4 GB	94,072
E	19.0 GB	1,709,279
F	2.79 GB	68,624
G	2.50 GB	637,199

VI. 결론 및 향후 연구

본 논문에서는 기존 트래픽의 지역성을 기반으로

표 2. 실험 결과
Table 2. Experiment result

Site	B	C	D	E	F	G
LFP Unit	21	13	189	90	13	63
LFP Final	239	148	2155	1026	148	718
DC	30	30	30	30	30	30
TCP LFP (origin)	81	12	25	34	45	180
TCP LFP (proposed)	15	6	2	11	8	42
UDP LFP (origin)	13	1	10	3	77	13
UDP LFP (proposed)	7	2	0	4	16	4
TCP Rule (origin)	247	16	36	68	74	254
TCP Rule (proposed)	312	24	48	86	99	337
UDP Rule (origin)	65	6	28	17	296	89
UDP Rule (proposed)	343	14	42	101	361	103

플로우 화이트리스트를 자동을 생성하는 방법을 확장하여 호스트 수, 트래픽 빈도수 그리고 종류 등의 SCADA 네트워크 다양성의 차이에도 유연하게 대처 가능한 시스템을 제안하였다. 제안한 시스템은 기존 연구의 플로우 화이트리스트 생성과정에 variable Threshold 적용을 통해 SCADA 네트워크의 다양성을 반영할 수 있었다. 또한 SCADA 네트워크의 호스트 수, 트래픽의 빈도수 그리고 종류에 상관없이 일정한 수준의 화이트리스트를 생성하고, 플로우의 서버/클라이언트 정보 및 플로우 duration 정보 등 다양한 플로우 정보를 추출하였다.

향후 연구로는 플로우 화이트리스트를 자동으로 유지 및 보수하여, 플로우 화이트리스트를 항상 최신의 것으로 유지할 수 있는 방법에 대해 연구 할 계획이다.

References

[1] J.-H. Yun, et al., “Burst-based anomaly detection on the DNP3 protocol,” *Int. J. Control and Automation,* vol. 6, no. 2, pp. 313-324, 2013.

[2] S. Choi, et al., *Traffic-locality-based creation of flow whitelists for SCADA networks*, pp. 87-102, Critical Infrastructure Protection IX, Springer International Publishing, 2015.

[3] H. Yoo, J.-H. Yun, and T. Shon, “Whitelist-based anomaly detection for industrial control system security,” *J. KICS*, vol. 38, no. 8, pp. 641-653, 2013.

[4] Y. H. Lim, H. Yoo, and T. Shon, “Anomaly detection for IEC 61850 substation network,” *JKIISC*, vol. 23, no. 5, pp. 939-946, Oct. 2013.

[5] J. Schneider, S. Obermeier, and R. Schlegel, “Cyber security maintenance for SCADA systems,” *ICS-CSR ’15*, pp. 89-94, Sept. 2015.

[6] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks,” *Computers & Security*, vol. 25, no. 7, pp. 498-506, 2006.

[7] W. Jung, et al., “Whitelist representation for FTP service in SCADA system by using structured ACL model,” *IEEE APNOMS*, Oct. 2016.

[8] R. R. R. Barbosa, R. Sadre, and A. Pras, “Flow whitelisting in SCADA networks,” *Int. J. Critical Infrastructure Protection*, vol. 6, no. 3, pp. 150-158, 2013.

[9] Y. Yang, et al., “Multiattribute SCADA-specific intrusion detection system for power networks,” *IEEE Trans. Power Delivery*, vol. 29, no. 3, pp. 1092-1102, Jun. 2014.

정 우 석 (Woo-Suk Jung)

2015년 : 고려대학교 컴퓨터정보학과 졸업
2015년~현재 : 고려대학교 컴퓨터정보학과 석사과정
<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석

윤 정 한 (Jeong-Han Yun)

2001년 2월 : KAIST 전산학과 졸업
2003년 2월 : KAIST 전산학과 석사
2011년 2월 : KAIST 전산학과 박사
2010년 12월~현재 : ETRI부설국가보안기술연구소 선임연구원
<관심분야> 프로그램 분석, 제어시스템 네트워크 침입탐지

김 신 규 (Sin-Kyu Kim)

2000년 2월 : 연세대학교 기계전자공학부 졸업
2002년 2월 : 연세대학교 컴퓨터과학과 석사
2014년 2월 : 연세대학교 컴퓨터과학과 박사
2003년 12월~현재 : ETRI부설국가보안기술연구소 선임연구원/실장
<관심분야> 스마트그리드 보안, 국가기반시설 보안, 취약점 분석

심 규 석 (Kyu-Seok Shim)

2014년 : 고려대학교 컴퓨터 정보학과 졸업
2016년 : 고려대학교 컴퓨터정보학과 석사
2016년~현재 : 고려대학교 컴퓨터정보학과 박사과정
<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석

김 성 민 (Sung-Min Kim)

2014년 : 고려대학교 컴퓨터 정보학과 졸업
2014년~현재 : 고려대학교 컴퓨터정보학과 석사과정
<관심분야> 네트워크 과니 및 보안, 트래픽 모니터링 및 분석

김 명 섭 (Myung-Sup Kim)

1998년 : 포항공과대학교 전자계산학과 학사
2000년 : 포항공과대학교 전자계산학과 석사
2004년 : 포항공과대학교 전자계산학과 박사
2006년 : Dept. of ECS, Univ of Toronto Canada
2006년~현재 : 고려대학교 컴퓨터정보학과 교수
<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석, 멀티미디어 네트워크