지능형 화이트리스트를 이용한 SCADA/DAS망의 이상행위 탐지 기법 연구

장민해*, 이주현*, 이상염*, 김명수*
한국전력공사 전력연구원*

A Study on the Detection Method of Abnormal Behavior of SCADA/DAS Network Using Intelligent White List

Min-Hae Jang*, Joo-Hyun Lee*, Sang-Yum Lee*, Myong-Soo Kim*
Kepco Research Institute*

Abstract - 매년 개인과 산업체 내/외부에서 보안사고가 발생하고 있으며, 해커들의 다양한 공격 시도로 공격의 지능화가 이루어져 이에 대한 대응이 점점 어려워지고 있다. 이러한 환경에서 SCADA/DAS망은 국가 주요기반 시설로 보안의 중요성이 강조된다. 그런데, 하루에 무수히 많이 발생하는 데이터를 수동으로 모두 관제하기에는 인프라적 한계가 있다. 이러한 한계점을 극복하고 공격을 탐지하기 위한 여러 시그니쳐 기반 관제 기법이 연구되었으나, 운영환경의 변화 등 보안 트렌드를 즉각 반영하기 어려운 문제점이 존재한다. 이를 해결하기 위해, 본 연구에서는 등록된 White List 데이터에 TTL(Time To Live) 기법을 적용해, 데이터의 생명주기에 따라 자동으로 List를 관리하여 실시간으로 보안 트렌드를 반영할 수 있는 지능형 White List 기반 이상행위 탐지 기법을 제안하고자 한다.

1. 서 론

모든 것이 유기적으로 연결된 현대사회에서 보안 문제는 점점 더 중요한 이슈가 되고있다. 매년 수천만 건의 개인정보 유출사건이 발생하고 있으며, 산업체의 내/외부 위협에 따른 무수히 많은 사이버 공격들이 행해지고 있다. 공격자는 악의적인 목적을 달성하기 위해 다양한 공격들을 시도하여, 공격의 지능화를 이루고 있기에 점점 더 모든 공격에 대한 대응이 어려워지고 있다. 이러한 환경에서 SCADA와 DAS망은 국가 주요기반 시설로 보안의 중요성이 강조된다. 따라서, 각종 위협에 대응하기 위해 SCADA/DAS망은 물리적으로 완전히 분리하여 관리하고 있기에, 주로 서버와 단말간의 통신이 발생되고 있다. 하지만, 1일 기준 SCADA와 DAS망에서 수천만, 수억 건의 대규모 통신이 방화벽 기준으로 발생하기 때문에, 관제 시 비정상 통신에 대한 탐지가 쉽지 않다. 이를 극복하기 위해 수집된 악의적 공격들을 분석하여 시그니쳐(signature)를 생성하고, 이에 대해 조치 및 대응이 가능한 여러 시그니쳐 기반 악성 공격 탐지 기법이 연구되고 있다. 그 예로, Black List 기법과 White List 기법이 있다. 그러나 해당 기법들은 수많은 트래픽에 대해 사람이 직접 기준과 범위를 판단하고 정의하여, 고정된 List로 차단 및 허용을 하는 방식이다. 이는 정확성이나 편의성이 떨어지는 문제점을 야기하고, 계속해서 바뀌는 보안 트렌드를 반영하지 못한다는 한계점이 있다. 이를 해결하기 위해, 본 연구에서는 정상적인 데이터는 주기적으로 통신함을 가정하고, 등록된 White List 데이터에 TTL(Time To Live) 기법을 활용하여 일정 기간 List 안의 데이터가 발생하지 않으면, 자동으로 리스트에서 삭제시켜, 현재 보안 트렌드를 실시간으로 자동 반영하는 지능형 White List 기반 이상행위 탐지 기법을 제안하고자 한다.

2. 본 론

2.1 SCADA

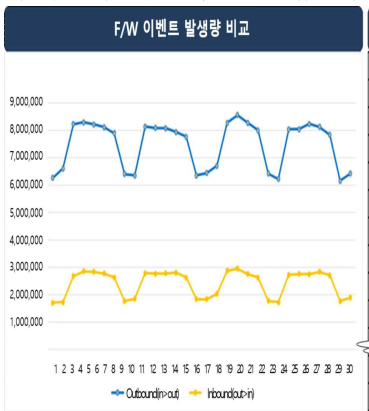
SCADA(Supervisory Control And Data Acquisition)는 원격감시 제어설비로 설비의 작업공정을 감시 및 제어하는 시스템이다. 한전에서는 송변전 계통 관리용으로 사용한다. 송전 및 배전의 원활한 흐름을 위해, 중앙에서 효율적으로 원격 감시 및 제어가 가능하나, 그만큼 주요 설비들에 대한 제어가 가능하기 때문에 사이버공격의 타겟이 될 수 있어 보안관리에 유의해야 한다.

2.2 DAS

DAS(Distribution Automation System)는 배전자동화 시스템으로 배전 설비에 대해 실시간으로 원격 감시 및 제어하여 배전계통의 모든 상황을 효율적으로 파악하고, 정전피해를 최소화하는 시스템이다. DAS도 SCADA와 마찬가지로 한전의 주요 산업망이기에 사이버공격으로부터 대응 방안이 필요하다.

2.3 F/W 데이터 분석

정상적인 통신은 Inbound가 있으면 Outbound가 존재한다고 가정하였을 때, 아래 그림과 같이 F/W 이벤트 발생량을 비교해보니 Inbound 대비 Outbound 트래픽이 많은 것을 확인할 수 있었고, Request 요청이 없는 Outbound에 대한 이상 트래픽을 확인할 수 있었다. 따라서, 비정상 트래픽 발생을 확인하여 F/W 데이터와 지능형 White List 기술을 활용한 이상행위 탐지모델의 개발 가능성을 확인할 수 있었다.



F/W 이벤트 분석 데이터

발생일	Outbound(in>out)	Inbound(out>in)	in, out 비교
8.1	6,269,706	1,700,462	4,569,244
8.2	6,614,840	1,725,626	4,889,214
8.3	8,224,111	2,680,007	5,544,104
8.4	8,295,034	2,855,323	5,439,711
8.5	8,222,978	2,837,006	5,385,972
8.6	8,124,800	2,776,106	5,348,694
8.7	7,898,966	2,624,688	5,274,278
8.8	6,403,370	1,765,187	4,638,183
8.9	6,356,365	1,852,159	4,504,206
⋮			
8.29	6,155,758	1,762,756	4,393,002
8.30	6,420,144	1,886,916	4,533,228

<그림 1> F/W 이벤트 발생량 비교 및 이벤트 분석 데이터

현재 F/W에서 발생하는 일일 트래픽은 약 43억 건이다. 그중 한전의 SCADA는 약 6천만 건, DAS는 약 25억 건의 통신이 발생하고 있기에, 관제 시 비정상 통신에 대한 탐지가 쉽지 않다.

2.4 Black List 기반 이상탐지 기법

다양한 시그니쳐 기반의 이상탐지 기법 중 하나인 Black List는 개인 정보 유출을 위한 금융, 결제 회사를 사칭한 사이트가 많아지면서, 악성 코드를 유포하는 IP 정보 등의 악의적인 목적을 지닌 트래픽을 차단하기 위해 사용되는 것으로, 사람이 차단할 범위 및 기준을 정해 해당 조건을 Black List화 하고, Black List에 해당되는 트래픽을 필터링하여 선제적으로 차단시키는 악성 공격 탐지기법이다.

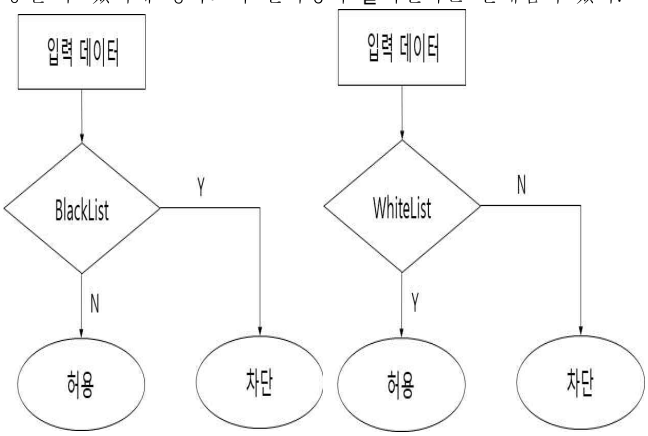
이 Black List 기법은 리스트 생성자가 위협을 미리 수동으로 지정한 것에 대해서만 차단하는 것으로, 고정성을 지닌 Black

List 기법만으로 다양한 공격패턴과 새롭게 생성되는 공격에 대해 모든 차단 기준을 List화 하는 것이 어려워, 새로운 환경에서 발생하는 신규 위협에 대응하기가 힘든 한계점이 있다.

2.5 White List 기반 이상탐지 기법

White List 기법은 Black List보다 넓은 범위의 공격을 차단할 수 있는 기법으로, 생성자가 안전하다고 보장되는 범위 및 기준을 White List화 하여 해당되는 트래픽은 언제나 허용하고, 그 외의 트래픽은 차단시키는 기법이다.

이 기법은 한번 안전하다고 판단된 것에 대해서는 이후 트렌드에 따라 공격 위험이 있어도 바로 반영하기가 어려워 공격을 놓칠 수 있기에 정확도와 편의성이 떨어진다는 한계점이 있다.

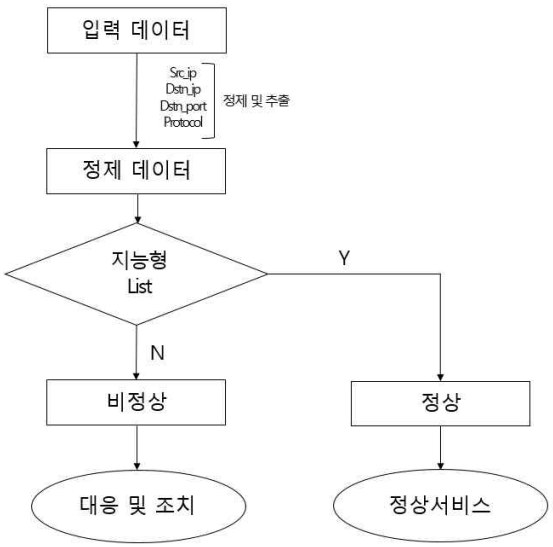


〈그림 2〉 Black List(좌) / White List(우)의 동작원리

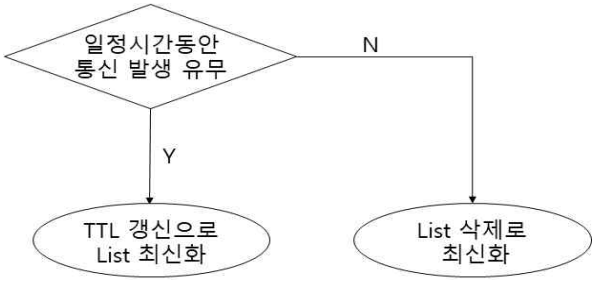
2.6 지능형 White List 기반 이상탐지 기법

따라서, 본 연구에서는 많은 양의 데이터를 효율적으로 처리할 수 있으며, 보안 트렌드를 실시간으로 반영할 수 있는 지능형 White List 기반 이상 탐지 기법을 제안한다.

해당 기법은 정상적인 데이터는 주기적으로 통신함을 가정하고, SCADA/DAS망의 실시간 장비 통신 중 기존 관제 환경에서 정상 조건을 White List에 등록한다. 등록된 White List의 데이터에 TTL(Time To Live) 기법을 활용하여 일정 기간 List 안의 데이터가 발생하면, TTL값을 갱신시켜 데이터의 생명주기를 늘려 List에 보존하고, 발생하지 않을 때엔, 자체적으로 메모리에서 TTL값이 감소되어 0이 되면, 자동으로 White List에서 해당 데이터를 삭제시켜, 현재 환경에 맞게끔 보안 트렌드를 자동 반영하는 원리이다. 아래는 지능형 White List 기반 이상행위 탐지 기법의 동작 원리다.

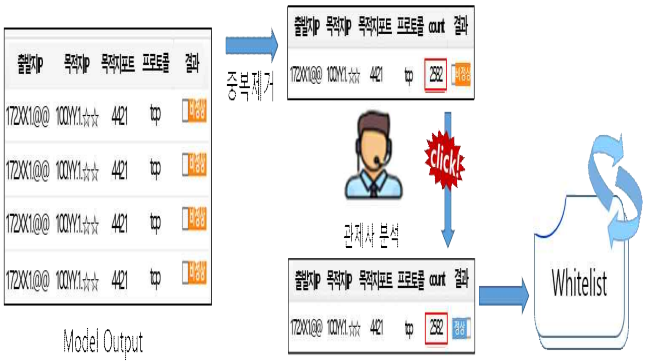


〈그림 3〉 지능형 White List 기반 이상행위 탐지 전체 프로세스



〈그림 4〉 지능형 White List 내부 동작 원리(TTL)

최종적으로 정상, 비정상으로 판단된 데이터는 <그림 5>와 같이 Group by된 최종 산출물만 보여주기 때문에, 직관적으로 관제사가 판단할 수 있게 하여, GUI를 활용한 원클릭 방식으로 정상이 비정상으로 나왔을 시 TTL값을 0으로 초기화 시켜 리스트에서 삭제를 해주거나, 비정상이 정상으로 나왔을 시 해당 데이터를 리스트에 새로 추가하며 TTL 값을 설정 기간만큼 주기 때문에 새로운 리스트를 생성할 수 있어, White List를 관제사가 편리하게 관리 및 최적화 할 수 있다.



〈그림 5〉 지능형 White List 업데이트 과정(Group by)

3. 결 론

본 연구는 SCADA/DAS망의 F/W 데이터와 지능형 White List를 이용하여 이상행위를 탐지하는 기법이다. 기존 Black List, White List와 같이 고정된 List 방식이 아닌 TTL을 이용하여 보안 트렌드를 자동으로 반영하는 기법으로, 변화가 많은 실제 운영환경에서 효율적인 관제가 가능하다. 또한, Group by로 중복된 통신에 대한 정보를 제거하여 방대한 방화벽 로그를 적은 양의 데이터로 재표현하여 직관적 판단이 가능하게 하고, 이를 원클릭 방식으로 판단 및 처리하여 White List를 쉽고 빠르게 업데이트할 수 있다.

해당 연구는 SCADA와 DAS망 외에 외부 연결구간에서도 정해진 규약 이외의 통신을 쉽게 찾아내고 관리할 수 있어, 확장 적용 및 개발이 가능할 것으로 기대된다.

[참 고 문 헌]

[1] 한전 용어사전 :(https:// home.kepco.co.kr/kepco/KO/KOEAPP001.po)
[2] 김종관 et al, “머신러닝을 이용한 검색량 기반 악성 URL 탐지기법 연구”, 전기학회논문지, vol.70, no.1, pp. 114-120, 2021
[3] 김명수 et al, "인공지능기술기반 보안관제시스템 개발 연구과제 최종보고서", 한국전력공사 전력연구원, 2021