Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.5, October 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.5.939

IEC 61850 변전소 네트워크에서의 이상 징후 탐지 연구

임 용 훈,[1†] 유 형 욱,[2] 손 태 식[2‡]
[1]한전 전력연구원, [2]아주대학교

Anomaly Detection for IEC 61850 Substation Network

Yong-hun Lim,[1†] Hyunguk Yoo,[2] Taeshik Shon[2‡]
[1]Korea Electric Power Corporation Research Institute, [2]Ajou University

요 약

본 논문에서는 IEC 61850 기반 자동화 변전소 네트워크에서의 이상 징후 탐지를 위한 MMS/GOOSE 패킷 정상행위 프로파일링 방법을 제안한다. 기존에 주로 사용되고 있는 시그니처(signature) 기반의 보안 솔루션은 제로데이(zero-day) 취약점을 이용한 APT 공격에 취약에 취약할 수밖에 없다. 최근 제어시스템 환경에서의 이상 탐지(anomaly detection) 연구가 이뤄지고 있지만, 아직까지 IEC 61850 변전소 환경에서의 이상 탐지에 대한 연구는 잘 알려져 있지 않다. 제안하는 기법은 MMS/GOOSE 패킷에 대한 3가지 전처리(3-phase preprocessing) 방법과 one-class SVM 알고리즘을 이용한 정상 행위 모델링 방법을 포함한다. 본 논문에서 제시하는 방법은 IEC 61850 변전소 네트워크에 대한 APT 공격 대응 솔루션으로 활용될 것을 기대한다.

ABSTRACT

This paper proposes normal behavior profiling methods for anomaly detection in IEC 61850 based substation network. Signature based security solutions, currently used primarily, are inadequate for APT attack using zero-day vulnerabilities. Recently, some researches about anomaly detection in control network are ongoing. However, there are no published result for IEC 61850 substation network. Our proposed methods includes 3-phase preprocessing for MMS/GOOSE packets and normal behavior profiling using one-class SVM algorithm. These approaches are beneficial to detect APT attacks on IEC 61850 substation network.

Keywords: Anomaly Detection, IEC 61850 Substation, MMS/GOOSE, Normal Behavior Profiling, One-class SVM

I. 서 론

일반적인 IT 환경에서의 보안 솔루션에는 anti-virus program, 방화벽(fire wall), 침입 탐지 시스템(Intrusion Detection System, IDS) 등이 존재한다. 그러나 IEC 61850 기반 디지털변전소에서 종래의 보안 기술들을 그대로 적용하기에는 많은 어려움이 따른다. 일례로 종래의 기술로는 디지털 변전소에서만 사용되는 통신 트래픽에 대한 검사가 불가능하며, 트래픽 허용 용량의 차이를 고려하지 않은 임계값 사용 등으로 인해 서비스거부(denial of service) 공격 종류를 적절히 탐지할 수 없게 된다. 또한 기존 침입 탐지 관련 보안 솔루션들은 대체로 공격 패킷에 대한 시그니처 정보가 있는 blacklist DB를 참조하여 공격을 탐지하고 있다. 하지만 이러한 방법의 경우 알려지지 않은 취약점을 이용한 제로데이

접수일(2013년 8월 6일), 수정일(2013년 9월 23일), 게재확정일(2013년 9월 30일)
† 주저자, adsac@kepco.co.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

(zero-day) 공격을 탐지할 수 없으며, 새로운 공격 패턴이 발생할 때마다 DB를 업데이트해줘야 하는 오버헤드가 존재하게 된다. 전력망과 같이 가용성(availability)이 중시되는 환경에서는 잦은 DB 업데이트로 인한 서비스 지연 문제는 사소하지 않다.

최근에는 이러한 일반 IT환경에서 사용되던 보안 솔루션의 문제점을 해결하기 위해 제어시스템에 특화된 보안 솔루션 연구도 많이 진행되고 있다. 대표적으로 Torfino社의 "Tofino Modbus TCP Enforcer"는 방화벽에 탑재되어 Modbus 프로토콜 패킷에 대한 검사를 수행할 수 있으며, McAfee社의 "Application Control" 솔루션은 어플리케이션 화이트리스트 기법으로 제어 장비에서 동작하는 어플리케이션들을 제어한다.

한편 제어시스템 환경은 IT 환경과 달리 네트워크 트래픽 발생이 규칙적이며, 제한된 프로토콜만 사용되기 때문에 정상 행위 프로파일링을 통한 이상 징후 탐지가 용이하다. 이러한 기법은 정상 행위를 기준으로 비정상 행위를 탐지하기 때문에 APT 공격과 같이 알려지지 않은 공격에 대해서도 효과적으로 대응할 수 있다.

본 논문에서는 IEC 61850 변전소 네트워크에서 주로 사용되는 MMS, GOOSE 패킷들에 대해 정상 행위 프로파일링을 수행함으로써 MMS, GOOSE 패킷에 대한 이상 징후 탐지 시스템을 모델링하였다. 본 논문에서 제안하는 정상 행위 기반 침입 탐지 시스템을 다른 제어시스템 방화벽, 화이트리스트 기법, Anti Virus 솔루션 등과 함께 다중 방호(Defense in Depth)를 형성한다면, APT 공격과 같이 고도화된 공격에 대해서도 효과적으로 대응할 수 있을 것이라 기대한다. 2장에서는 제어시스템에서의 이상 징후 탐지 관련 기존 연구들에 대해 소개하고, 3장에서 IEC 61850 변전소 네트워크 구성과 트래픽 특성에 대해 기술한다. 4장에서 제안하는 정상 행위 기반의 이상 징후 탐지 시스템을 소개하고, 5장에서 제안 시스템에 대한 성능을 평가한다. 마지막으로 6장에서는 논문의 결론을 도출하고, 향후 연구 방향을 제시한다.

II. 관련 연구

2.1 기존 제어시스템 대상 이상 탐지 연구

이상 탐지 기법은 정상 행위를 기반으로 하기 때문에 제로데이 공격과 같은 새로운 형태의 공격도 탐지할 수 있으며, 제어 시스템과 같이 정상 행위 범위가 한정적이고 변화가 적은 도메인에서는 한 번 정상 행위를 규정하면 자주 업데이트 할 필요가 없다는 장점이 있다. 이상 탐지 기법의 단점은 일반적으로 오경보 비율(false positive rate)이 높고, 처음 정상 행위 모델을 만들 때 어떤 정해진 법칙이 없기 때문에 최적화된 모델을 찾기 위해 많은 시간과 노력이 필요하다는 것이다. 그럼에도 불구하고 제어시스템 환경은 일반 IT 환경에 비해 사용하는 서비스 종류가 매우 한정적이며, 행위 패턴 또한 규칙적이기 때문에 이상 탐지 기법의 적용이 용이하다.

Steven Cheung 등[4]은 Modbus TCP 네트워크를 대상으로, 정상 행위 기반의 3가지 모델(Protocol Level, Communication Pattern, Learning-Based)을 이용해 이상 징후를 탐지하였다. Protocol Level 모델은 Modbus 프로토콜 명세서를 기반으로 지원 가능한 기능 코드(function code)들을 규정하고 이를 위반하는 패킷을 이상 패킷으로 추정하는 모델이다. Communication Pattern 기반 모델은 IP 주소, TCP Port 등을 기반으로 허용 가능한 통신 연결 집합을 규정하고 이에 속하지 않는 패킷을 비정상으로 판단한다. Learning-Based Model은 Modbus 기능 코드를 이용해 Bayesian Network를 구성하고, 조건 확률 관계를 이용해 이상 징후를 탐지해 낸다. Partrick Dussel 등[5]은 payload 기반의 실시간 이상 징후 탐지 시스템을 제안하였다. 이 시스템은 TCP payload 데이터를 n 바이트(n-gram)씩 나누어 feature space를 나타내고, 정상 byte sequence와 유사도(similarity)를 비교하여 비정상 패킷을 탐지한다. 이 기법은 TCP payload 부분을 n-gram으로 일괄적으로 자르기 때문에 상위 프로토콜 종류에 대해 독립적으로 적용할 수 있다.

앞서 언급한 기존 연구들은 제어시스템에서의 이상 징후 탐지 방법들을 다루고 있지만, IEC 61850 변전소 네트워크에 그대로 적용하기에는 무리가 있다. [4]의 경우 오로지 Modbus 프로토콜을 대상으로 한 이상 탐지를 다루고 있으며, [5]는 TCP payload를 대상으로 하기 때문에 TCP/IP 레이어가 없는 GOOSE에서는 사용할 수 없다.

2.2 IEC 61850 변전소 네트워크 프로토콜

과거 변전소 데이터 교환 프로토콜로 사용된 시리

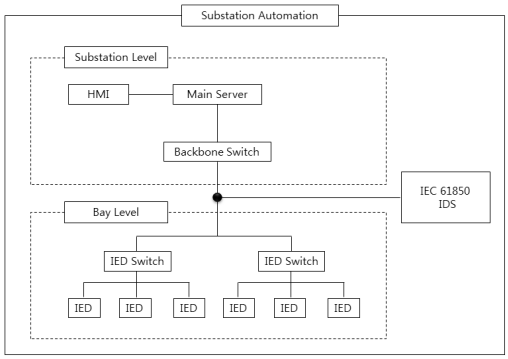
얼 기반의 IEC 60870-5 시리즈 및 DNP3는 1980년대에 개발되어 오래기간 사용되어져 왔다. 하지만 IEC 60870-5 등은 하드웨어 의존성으로 인해 여러 벤더들 간의 호환성이 떨어지며, 해당 포인트 정보 및 상태정보를 가지는 단순한 기능만을 하고 있어 차세대 자동화 변전소 환경의 다양한 운영 데이터를 표현함에 있어 부족한 부분이 많았다. 이에 따라 IEC TC57 WG10에서는 이러한 기존 변전소 통신 프로토콜의 확장성 및 유연성 부족 문제를 극복하고자 차세대 자동화 변전소 환경에 적합한 새로운 통신 규격으로 IEC 61850을 개발하였다. IEC 61850에서 사용되는 대표적인 프로토콜에는 MMS와 GOOSE가 있다. MMS는 TCP/IP 기반 프로토콜로 서버/클라이언트 간의 정보 전달 및 평상시 제어 명령 전송 등에 사용된다. 반면 GOOSE는 이더넷 위에서 바로 동작하는 프로토콜로써 IED 상태 정보 전송을 위한 peer-to-peer 통신에서 사용된다. 아직까지 MMS나 GOOSE 프로토콜을 이용한 공격 사례나 방법이 공개된 바는 없다. 하지만 MMS 프로토콜 스택의 TPKT 레이어 취약점(US-CERT Vulnerability Note VU#468798, VU#372878)이 발견된 바 있으며, IEC 62351이 적용되지 않은 기본 MMS나 GOOSE는 암호화 및 인증 메커니즘을 제공하지 않기 때문에 공격자가 악용할 여지가 충분하다.

III. 이상 징후 탐지 기법

본 논문에서는 IEC 61850 변전소 네트워크에서의 이상 징후를 탐지하기 위해 MMS 및 GOOSE 패킷에 대한 정상행위 프로파일링 방법을 제안한다. 앞서 관련 연구에서 살펴보았듯이, 기존 제어시스템에서의 이상 징후 탐지 연구는 대부분 Modbus 또는 DNP3 프로토콜을 대상으로 하거나 또는 TCP 상위 프로토콜을 고려하지 않기 때문에 IEC 61850 환경에 적용하기에 부적합하다.

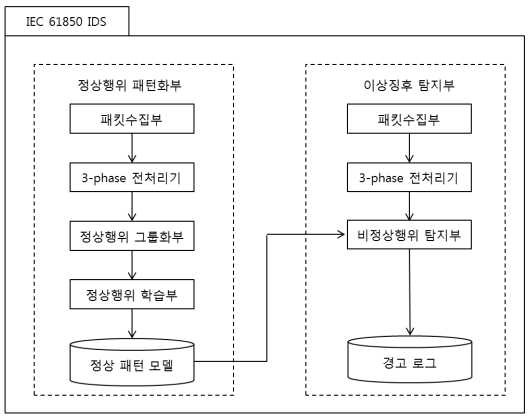
본 연구에서는 GOOSE/MMS 패킷에 대한 3가지 전처리(3-phase preprocessing) 기법을 새롭게 제시하였으며, 비교사 학습(unsupervised learning) 기반의 EM 알고리즘을 적용한 정상행위 그룹화 방법과, one-class SVM을 이용한 정상 행위 학습 및 비정상 행위 탐지 방법을 제시한다.

제시하는 IEC 61850 이상 징후 탐지 시스템은 네트워크 레벨의 탐지 시스템으로 IEC 61850 네트워크 Substation Level 및 Bay Level 기기들의 통신 패킷을 수집하고, 이를 대상으로 이상 징후를 탐지한다. 〔그림 1〕은 IEC 61850 변전소 네트워크에서의 패킷 수집 및 탐지 위치를 나타낸다.



〔그림 1〕 IEC 61850 변전소 네트워크

IEC 61850 이상 징후 시스템은 크게 정상행위 패턴화부와 이상 징후 탐지부로 나누어지며, 핵심 모듈은 3-phase 전처리기, 정상행위 그룹화부, 정상행위 학습부, 비정상행위 탐지부이다〔그림 2〕.



〔그림 2〕 이상 징후 탐지 시스템 세부 구조

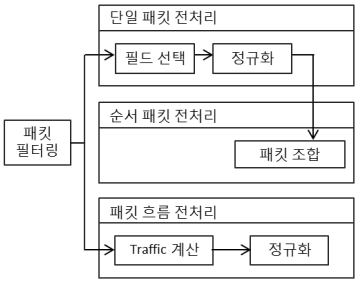
정상행위 패턴화부의 3-phase 전처리기 모듈에서는 패킷 수집부에서 수집한 변전소 네트워크 전체 패킷에서 MMS 및 GOOSE 패킷만을 추출하고, 이후 3가지 전처리 방법(단일 패킷 전처리, 순서 패킷 전처리, 패킷 흐름 전처리)에 따라 서로 다른 데이터 집합으로 변형된다. 단일 패킷 전처리에서는 개별 패킷 단위로 학습 데이터를 만들며, 순서 패킷 전처리에서는 같은 플로우(flow) 내의 연속적인 패킷들을 하나의 데이터로 묶는다. 패킷 흐름 전처리에서는 단위 시간당 전송 바이트 및 단위 시간당 패킷 수를 계산하여

데이터를 만든다. 정상행위 그룹화부에서는 3가지 전처리 프로세스를 거쳐서 만들어진 데이터 집합들에서 아웃라이어(outlier)를 제거하기 위해 잘 알려진 클러스터링 기법인 EM(Expectation Maximization) 알고리즘을 적용한다. 본 연구에서는 EM 알고리즘을 통해 그룹화 된 결과에서 하위 20%의 소규모 그룹에 대해서는 아웃라이어로 간주하고 학습 데이터에서 제외하였다. 정상행위 학습부에서는 정상행위 그룹화부에서 상위 80%로 그룹에 속하는 데이터들에 대해 one-class SVM 알고리즘을 적용하여 학습시킴으로써 정상 패턴 모델을 생성한다.

이상 징후 탐지부에서는 실시간으로 수집되는 패킷들에 대해 3-phase 전처리 모듈을 통해 처리 가능한 형태로 변형한 후, one-class SVM 알고리즘을 이용해 기존 정상행위 패턴화부에서 만들어진 정상 패턴 모델과 비교함으로써 이상 여부를 판단하고 로그 기록을 남긴다.

3.1 3-phase preprocessing

3-phase 전처리기는 단일 패킷 전처리, 순서 패킷 전처리, 패킷 흐름 전처리로 구성된다〔그림 3〕.



〔그림 3〕 3-phase Pre-processing

단일 패킷 전처리에서는 각각 하나의 패킷 단위로 학습 데이터를 만들며, 순서 패킷 전처리에서는 같은 플로우 내의 연속적인 패킷들을 하나의 데이터로 묶는다. 패킷 흐름 전처리에서는 단위 시간당 전송량 등을 계산하여 데이터를 만든다.

○ 패킷 필터링

패킷 필터링 부분에서는 MMS와 GOOSE 패킷의 fingerprint를 이용하여 전체 패킷 집합에서 MMS와 GOOSE 패킷만을 추출한다.

○ 단일 패킷 전처리

단일 패킷 전처리부에서는 데이터 집합을 만들기 위해 개별 패킷에서의 주요 헤더 필드(MAC 주소, IP 주소, TCP 포트 등)를 선택한다. 필드 선택에서 주요하게 고려된 것은 패킷 간에 값의 변화로써, 패킷 간의 값의 변화가 없을 것이라 예상되는 필드들을 제외하였다. GOOSE 패킷의 경우, MAC 주소를 포함한 GOOSE 메시지 간에 변화가 존재하는 11개 필드(APPID, Length, gocbRef 등)를 선택하였다〔표 1〕. MMS 패킷에서는 Ethernet 헤더, TCP/IP 헤더에서의 주요 필드를 선택하고, MMS 메시지 부분은 20바이트까지만 1바이트씩 잘라서 20개 필드를 추출하였다〔표 2〕.

〔표 1〕 GOOSE 단일 패킷 데이터 필드

필드		설명
Ethernet	Destination MAC	목적지 MAC 주소
	Source MAC	송신지 MAC 주소
IP	Total Length	IP 패킷 전체 길이
	Identification	Datagram 일련 번호
	IP Flags	Fragment 여부 표시
	TTL	패킷 라우팅 회수 제한
	Source IP	송신지 IP 주소
	Destination IP	목적지 IP 주소
TCP	Source Port	송신지 Port 번호
	Destination Port	목적지 Port 번호
	Sequence Number	Segment의 일련번호
	Ack Number	Acknowledgement 번호
	TCP Flags	TCP 회선 및 데이터 관리, 제어
	Window	TCP 흐름제어를 위한 버퍼 사이즈
TPKT	Length	TPKT 헤더를 포함한 길이
COTP	EOT	마지막 데이터 여부
MMS	1-20 Bytes	MMS Message 부분

〔표 2〕 MMS 단일 패킷 데이터 필드

필드		설명
Ethernet	Destination MAC	목적지 MAC 주소
	Source MAC	송신지 MAC 주소
GOOSE	APPID	Application Identification
	Length	Ethernet header 크기(14 byte)를 제외한 GOOSE message 길이
	gocbRef	GOOSE 메시지 제어 GoCB 지시
	timeAllowedtoLive	메시지 최대 대기 시간
	datset	Control Block의 ObjectReference
	goID	GOOSE 메시지 식별 ID
	time	stNum이 증가한 시각
	stNum	data-set 값 변화 발생 시 증가
	sqNum	메시지가 전송 시마다 증가
	confRev	simulation 여부를 표시 (T/F)
	numDatSetEntries	메시지에 포함된 데이터 개수

○ 순서 패킷 전처리

순서 패킷 전처리부에서는 단일 패킷 전처리부의 결과를 바탕으로 같은 통신 노드 간의 통신에 있어서 연속적인 2~5개 사이의 패킷을 하나로 묶어서 데이터 집합을 만든다. 이 때 MAC/IP 주소, Port 번호 등 중복되는 필드들은 첫 번째 패킷에서만 선택하고 두 번째 이후 패킷에서는 값이 중복되지 않는 필드들만 선택한다. 연속적인 패킷들을 하나로 묶는 이유는 공격 정보를 포함하고 있는 메시지가 IP Datagram 단위로 잘릴 수도 있으며, 또한 연속적인 패킷 순서들을 하나의 데이터로 묶어서 정상 행위를 학습할 때 개별 패킷 단위의 학습에서 고려되지 못했던 부분이 포함될 수 있기 때문이다.

○ 패킷 흐름 전처리

패킷 흐름 전처리부에서는 두 노드 간의 단위 시간 당 패킷 전송량, 단위 시간 당 전송 바이트 크기를 계산하여 데이터 집합을 만든다〔표 3〕〔표 4〕. 트래픽 기반 데이터 집합을 통해 학습된 정상 행위 모델은 서비스 거부 공격 종류를 탐지할 수 있다.

〔표 3〕 GOOSE 패킷 흐름 데이터 필드

필드		설명
Ethernet	Destination MAC	목적지 MAC 주소
	Source MAC	송신지 MAC 주소
Traffic	PPS	1초당 GOOSE 패킷 전송 수
	BPS	1초당 전송된 GOOSE 패킷의 전체 바이트

〔표 4〕 MMS 패킷 흐름 데이터 필드

필드		설명
IP	Destination IP	목적지 IP 주소
	Source IP	송신지 IP 주소
Traffic	PPS	1초당 MMS 패킷 전송 수
	BPS	1초당 전송된 MMS 패킷의 전체 바이트

○ 정규화

패킷 전처리 시 선택된 데이터 필드들 각각이 가지는 값의 범위가 상이하기 때문에 정규화 작업이 반드시 필요하다. 본 논문에서는 각 필드의 평균과 표준편차를 이용하여, 아래의 식으로 정규화 하였다.

$$x = \frac{x_i - \bar{x}}{\sigma}$$

x_i : 정규화 대상 값
x : 정규화 처리된 값
$\bar{x}$: 데이터 필드 값의 평균
σ : 데이터 필드 값의 표준 편차

3.2 정상행위 그룹화

정규화까지 처리된 데이터 집합들은 아웃라이어 처리가 필요하다. 정상 행위 모델을 만들기 위해서는 데이터 수집 시 수집 데이터가 모두 정상일 것이라는 가

정이 필요하다. 하지만, 실제 필드에서 패킷을 수집할 때 정상 가동 중인 변전소 네트워크라고 해도 관리자의 실수, 기기 결함, 노이즈(noise) 등으로 인해 비정상 데이터가 포함될 여지가 충분하다. 따라서 정상 모델을 만들기 이전에 데이터 집합에 대한 아웃라이어 처리가 반드시 필요하다. 본 논문에서는 아웃라이어 처리를 위해 EM 클러스터링 기법을 이용해 정상행위를 그룹화 하였다. EM 기법은 반복 과정을 통해 각 데이터들이 혼합 클러스터(mixture cluster)에 속할 가능성을 조적하여 최적의 클러스터 모델을 생성하는 알고리즘이다. 데이터 집합에 EM 알고리즘을 적용하여 도출되는 클러스터들 중에서 매우 작은 클러스터들은 아웃라이어로 간주하고 정상 행위 학습 시 제외한다. 본 연구에서는 전체 데이터 집합에서 하위 20% 속하는 클러스터들을 아웃라이어로 처리하였다.

3.3 정상행위 학습

본 논문에서 정상 행위 모델을 만들기 위해 사용한 방법은 one-class SVM 알고리즘이다. SVM은 성능이 우수한 binary classification 알고리즘으로 잘 알려져 있다. 하지만 정상행위만을 이용한 학습 기법으로는 binary class SVM 사용이 부적합하며 이에 따라 본 논문에서는 정상 데이터 클래스만을 가지고 학습 모델을 도출할 수 있는 one-class SVM을 사용하였다. One-class SVM에서는 커널 함수를 사용해 투사된 feature space에서 모든 데이터들을 하나의 클래스로 간주하고, 원점과의 거리가 최대가 되는 hyper-plane을 계산한다. One-class SVM에서 사용할 수 있는 커널함수에는 Linear, Polynomial, Sigmoid, RBF(Radial Basis Function) 등이 있지만, 본 연구에서는 다수의 실험결과 Sigmoid 커널의 성능이 가장 우수하였기 때문에 Sigmoid 커널을 이용하여 학습하였다.

3.4 이상 탐지

정상 행위 학습 모듈에서 one-class SVM 알고리즘을 이용해 만든 정상 행위 모델들은 이상 탐지 엔진에 탑재된다. 이후 실시간 패킷들이 들어올 때 이상 탐지부에서는 패킷들에 대한 전처리(3-phase pre-processing)를 수행하고, 기 탑재된 정상 모델들을 이용 패킷들의 정상/비정상 여부를 판단한다. 패킷에 대한 정상/비정상 여부는 로그 기록으로 남겨서 차후 분석을 위해 사용한다.

IV. 실험 결과

본 논문에서는 제안하는 기법의 유효성을 검증하기 위해 실제 운영되고 있는 IEC 61850 변전소에 수집한 패킷을 이용해 실험하였다. 개발한 IEC 61850 이상 징후 탐지 시스템은 리눅스(우분투 12.04)에서 동작하며, one-class SVM 적용을 위해 libsvm v3.14 라이브러리를 일부 이용하였다. 한편, EM을 통한 정상행위 그룹화 부분은 윈도우 환경에서 WEKA v3.6.8을 이용해 오프라인에서 수행하였다.

순서 패킷 기반 모델 및 패킷 흐름 기반 모델의 경우 전처리에서 메모리 공간과 시간이 소모되기 때문에 우선적으로 현장 적용 적합성 평가를 위해 단일 패킷 기반 모델에 대해서만 성능 평가를 수행하였다. 또한, 현재 알려진 IEC 61850 프로토콜 기반 공격 기법이나 패킷이 존재하지 않기 때문에 우선적으로 정상 패킷에 대한 FPR(False Positive Rate)을 평가하였다. 실험에서 one-class SVM 알고리즘에서 사용되는 error tolerance 값은 0.01로 고정하였으며, 학습 패킷 데이터를 이용한 10-fold cross validation 방법과 새로운 테스트 패킷을 이용한 방법을 통해 FPR을 평가하였다〔표 5〕.

〔표 5〕 단일 패킷 탐지 비율

프로토콜	MMS	GOOSE
Error Tolerance	0.01	
학습 패킷 수	25,357	22,570
10-fold cross validation (잘못 분류된 패킷/전체 패킷)	1.0175% (258/25357)	1.4222% (321/22570)
테스트 패킷 검증 (잘못 분류된 패킷/전체 패킷)	2.1706% (1416/65235)	5.8761% (770/13104)

위 실험 결과를 통해 확인한 FPR 값은 처음으로 시도된 IEC 61850 변전소 네트워크에서 MMS 및 GOOSE를 이용한 이상 징후 탐지 시스템임을 고려할 때 나쁘지 않은 수치라고 판단하였다. 하지만 실제 변전소에 적용되기 위해서는 FPR 값을 더 낮출 필요가 있으며, 공격 시뮬레이션을 통해 FNR(False

Negative Rate)에 대해서도 평가할 필요가 있다.

V. 결 론

본 논문에서는 IEC 61850 표준의 대표적 프로토콜인 MMS/GOOSE 패킷의 정상 행위 프로파일링을 통한 이상 징후 탐지 모델을 제시하였다. 제안한 기법은 정상 패턴 정보를 이용하기 때문에 제로데이 공격과 같이 알려지지 않은 취약점을 이용한 사이버 공격에 대응할 수 있을 것으로 기대한다. 향후 연구에서는 순서 패킷 기반 모델 및 패킷 흐름 기반 모델에 대한 성능 평가가 수행되어야 할 것이며, 탐지 정확도를 높이기 위해 노드 간 플로우(Flow) 별로 각각 다른 정상 행위 모델을 만들어 적용하는 방법 또한 고려해 볼 수 있다. 그리고 IEC 61850 공격 패킷에 대한 탐지율을 검사하기 위해서는 공격 패킷을 만들 수 있는 방법이 연구되어야 할 것이다. IEC 61850에 대한 공격 기법들이 정형화되어 도출된다면 공격 패킷들에 대해서도 모델링을 수행할 수 있을 것이며, 이를 통해 탐지 정확도 향상 및 맞춤형 공격 대응이 가능할 것이다.

참고문헌

〔1〕 E.J. Markey and H.A. Waxman, "Electric Grid Vulnerability: Industry Responses Reveal Security Gps," U.S. House of Representatives, May 2013.

〔2〕 Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, and Alfonso Valdes, "Using Model-based Intrusion Detection for SCADA Networks," SCADA Security Scientific Symposium, pp. 186-199, Jan. 2007.

〔3〕 Partrick Dussel, Christian Gehl, Pavel Laskov, Jens-Uwe Buber, Christof Stormann, and Jan Kastner, "Cyber-Critical Infrastructure Protection Using Real-time Payload-based Anomaly Detection," Critical Information Infrastructures Security, vol. 6027, pp. 85-97, 2010.

〔4〕 Dayu Yang, Alexander Usynin, and J.W. Hines, "Anomaly-Based Intrusion Detection for SCADA Systems," 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies, pp. 12-16, 2006.

〔5〕 Upeka Premaratne, Jagath Samarabandu, Tarlochan Sidhu, Bob Beresh, and Jian-Cheng Tan, " Evidence Theory based Decision Fusion for Masquerade Detection in IEC 61850 Automated Substations," 4th International Conference on Information and Automation for Sustainability, pp 194-199, 2008.

〔6〕 Alfonso Valdes and Steven Cheung, "Communication Pattern Anomaly Detection in Process Control Systems," IEEE Conference on Technologies for Homeland Security, pp 22-29, 2009.

〔7〕 Chee-Wooi Ten, Junho Hong, and Chen-Ching Liu, "Anomaly Detection for Cybersecurity of the Substations," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp 865-873, 2011.

〔8〕 Alfonso Valdes and Steven Cheung, "Intrusion Monitoring in Process Control Systems," 42nd Hawaii International Conference on System Sciences, pp 1-7, 2009.

〔9〕 Erik Pleijsier, "Towards Anomaly Detection in SCADA Networks using Connection Patterns," 18th Twente Student Conference on IT, pp 1-6, 2013.

〔10〕 Rafael Ramos Regis Barbosa, Ramin Sadre, and Aiko Pras, "Towards Periodicity Based Anomaly Detection in SCADA Networks," 2012 IEEE 17th Conference on Emerging Technologies & Factory Automation, pp 1-4, 2012.

〔11〕 M.P. Coutinho, G. Lambert-Torres, L.E.B. da Silva, H.G. Martins, H. Lazarek, and J.C. Neto, "Anomaly detection in power system control center critical infrastructures using rough classification algorithm," 3rd IEEE International Conference on Digital Eco-

systems and Technologies, pp. 733-738, 2009.
〔12〕 Ondrej Linda, Todd Vollmer, and Milos Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures", International Joint Conference on Neural Networks, 2009.
〔13〕 Jordi Cucurull, Simin Nadjm-Tehrani, and Mikael Asplund, "Anomaly Detection and Mitigation for Disaster Area Network," Recent Advances in Intrusion Detection, vol. 6307, pp 339-359, 2010.
〔14〕 Rafael Ramos Regis Barbosa and Aiko Pras, "Intrusion Detection in SCADA Networks," Mechanisms for Autonomous Management of Networks and Services, vol. 6155, pp 163-166, 2010.
〔15〕 Taeshik Shon and Jongsub Moon, "A Hybrid Machine Learning Approach to Network Anomaly Detection," Information Sciences, vol. 177, no. 18, pp 3799-3821, 2007.
〔16〕 Inaki Garitano, Roberto Uribeetxeberria, and Urko Zurutuza, "A Review of SCADA Anomaly Detection Systems," Advances in Intelligent and Soft Computing, vol. 87, pp 357-366, 2011.
〔17〕 Bonnie Zhu and Shankar Sastry, "SCADA-Specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy," Proceedings of the 1st Workshop on Secure Control Systems, pp 1-16, 2010.
〔18〕 고폴린, 최화재, 김세령, 권혁민, 김휘강, "트래픽 자기 유사성(Self-similarity)에 기반한 SCADA 시스템 환경에서의 침임탐지방법론," 정보보호학회논문지, 22(2), pp. 267-281, 2012년 4월.

〈저자소개〉

임 용 훈 (Yong-hum Lim) 정회원
1996년 2월: 건국대학교 전자공학과 졸업
1998년 2월: 건국대학교 전자공학과 석사
1996년 2월~현재: 한국전력공사 근무
〈관심분야〉 정보보호, 스마트그리드, 보안관제

유 형 욱 (Hyunguk Yoo) 학생회원
2011년 8월: 아주대학교 정보 및 컴퓨터공학부 졸업
2011년 9월~현재: 아주대학교 컴퓨터공학과 통합과정
〈관심분야〉 스마트그리드 보안, 디지털 포렌식, 이상탐지, 리눅스 및 안드로이드 보안

손 태 식 (Taeshik Shon) 종신회원
2000년 2월: 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월: 아주대학교 정보통신전문대학원 공학석사
2005년 8월: 고려대학교 정보보호대학원 공학박사
2004년 2월~2005년 2월: Research Scholar, University of Minnesota
2005년 8월~2011년 2월: 삼성전자 DMC 연구소 책임연구원
2011년 3월~현재: 아주대학교 정보통신대학 정보컴퓨터공학과 조교수
〈관심분야〉 전력제어시스템 보안, 디지털 포렌식, 비정상행위탐지, ICT융합보안