정 보 보 호 학 회 지
제24권 제5호, 2014. 10

제어시스템 침입탐지 시스템 기술 연구 동향

최 승 오*, 김 우 년**

요 약

국가기반시설 제어시스템은 독립망 운영 정책 적용과 독자적 제어시스템 통신 프로토콜 사용으로 안전하다고 여겨져 왔다. 하지만 최근 국가기반시설 제어시스템을 대상으로 한 최초의 사이버 무기인 스턱스넷(Stuxnet) 악성코드의 발견 이래로 현재까지도 지속적인 사이버 위협 및 사고사례가 보고되고 있다. 이에 따라 사회경제적으로 큰 혼란을 야기할 수 있는 제어시스템 대상 사이버공격에 대응하기 위해 일반 IT 환경과는 다른 제어시스템만의 특성이 반영된 보안기술이 요구되고 있다. 본 논문에서는 제어시스템 보안기술 중 침입탐지 시스템 기술 연구 동향을 분석하고 해당 기술이 적용되는 제어시스템 영역과 제어시스템 통신 프로토콜별 특성에 따른 기술들의 특징을 분석한다. 또한, 탐지 기법에 따른 제어시스템 공격 탐지 성능을 비교 및 분석한다.

Ⅰ. 서 론

국가기반시설인 제어시스템은 계측 및 제어, 상태 감시 및 관리를 위해 다양한 산업분야에 걸쳐 폭 넓게 사용되고 있다. 이러한 제어시스템은 일반 IT환경의 시스템과는 달리 인터넷망과 분리되어 운영되고 제어시스템 네트워크 통신을 위한 전용 프로토콜이 사용되고 있다. 따라서 제어시스템을 대상으로 한 사이버 위협의 가능성이 없다고 인식되어 왔다. 하지만, 이러한 인식은 제어시스템을 겨냥한 정밀 사이버 미사일로 불리는 스턱스넷(Stuxnet) 악성코드가 발견됨에 따라 급격한 전환을 맞게 된다. 또한, 스턱스넷 발견 이후에도 제어시스템을 대상으로 한 듀크(Duqu), 플레임(Flame), 가우스(Gauss), 마흐디(Mahdi), 샤문(Shamoon), 스카이와이퍼(SkyWiper) 등 새로운 악성코드가 지속적으로 발견되고 있는 상황이다.

이와 더불어, 최근 업무의 효율성을 위해 제어망과 내부 업무망이 연결되고, 제어시스템을 통해 물리적 거리가 먼 제어기기 관리를 위해 제어망과 인터넷망까지 연계된 개방적 운영이 이뤄지고 있다[1,2]. 이러한 개방적 운영 환경에 대한 위험성은 제어시스템 보안위협의 지속적인 증가 추세가 방증하고 있다. 실제로 미국 ICS-CERT에 따르면 2013년 제어시스템 사이버사고 발생건수는 2012년 대비 30%이상 급증한 것으로 나타났다[3,4]. 따라서 공격에 대한 막대한 피해가 발생할 수 있는 제어시스템의 안전한 운영 및 관리를 위해서 제어시스템을 대상으로 한 사이버공격 탐지기술이 절실하다. 하지만 일반 IT 환경과는 달리 제어시스템에서 요구되는 매우 높은 실시간 응답성 및 가용성과 운영환경의 차이점으로 인해 제어시스템에 특화된 침입탐지 기술이 요구된다.

본 논문에서는 제어시스템의 환경적 특성을 고려한 제어시스템 특화 침입탐지 시스템(IDS, Intrusion Detection System)의 연구 동향에 대해 소개한다. 또한, 제어시스템 운영영역(Domain-specific)과 침입탐지에 사용되는 정보의 출처(Information source)와 탐지 기법(IDS Analysis)에 따라 기술 분류를 제시한다. 또한, 제어시스템 통신 프로토콜 관점에서 탐지 활용 정보 및 단위와 탐지 기법 및 성능을 비교하고 분석한다.

본 논문은 총 5장으로 구성되어 있다. Ⅱ장에서는 일반적인 침입탐지 시스템에 대한 정의와 기술 분류에 따른 기능상의 특징을 설명한다. Ⅲ장에서는 제어시스템의 일반적인 네트워크의 구조에 대해 설명하고 제어시스템의 보안위협과 제어시스템 네트워크 특성을 기술한다. Ⅳ장에서는 제어시스템 침입 탐기 기술 연구 동향에 대해 기술하고 침입탐지 기법에 따른 분류, 제어시스템

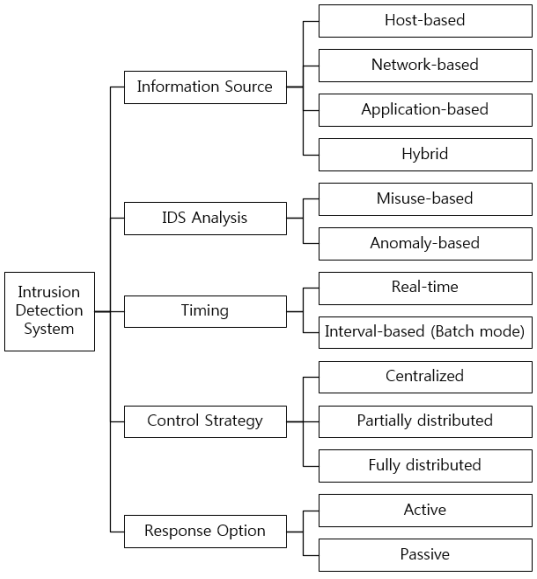
* ETRI 부설연구소 (sochoi@ensec.re.kr)
** ETRI 부설연구소 (wnkim@ensec.re.kr)

통신 프로토콜에 따른 분류, 탐지 성능 분석 결과 비교를 통해 제시한다. 마지막으로 Ⅴ장에서는 이 논문의 결론을 맺는다.

Ⅱ. 침입탐지 시스템

침입탐지 시스템(IDS, Intrusion Detection System)은 컴퓨터 또는 네트워크의 감시를 통해 침입 발생 시이를 적시에 탐지하고 대응하는 기능을 제공한다. 침입탐지 시스템은 [그림 1]과 같이 다양한 분류기준이 존재한다. 침입탐지 시스템을 분류할 때 침입탐지에 사용되는 정보의 출처(Information source)와 탐지 기법(IDS Analysis)이 주로 사용된다[5].

우선, 침입 감시에 사용되는 정보에 따라 호스트 기반, 네트워크 기반, 응용프로그램 기반, 호스트와 네트워크 특징을 결합한 혼합 기반 침입탐지 시스템으로 구분된다. 호스트 기반 침입탐지 시스템은 해당 호스트에서 생성된 이벤트 및 로그를 분석하여 네트워크 기반에서 탐지할 수 없는 침입도 탐지 가능하지만 모든 호스트에 설치되어 관리에 어려움이 있다. 네트워크 기반 침입탐지 시스템은 네트워크 트래픽 감시를 통해 호스트 기반에서 탐지할 수 없는 전반적인 네트워크 침입에 대한 탐지가 가능하다. 하지만 네트워크 트래픽에 기밀성을 보장하기 위한 암호화 기법이 적용된 경우 내용



〔그림 1〕 침입탐지 시스템(IDS)의 분류

(context)을 이해할 수 없기 때문에 탐지에 한계가 있다. 이처럼, 호스트 기반 및 네트워크 기반 침입탐지 시스템의 상호간 단점을 보완하고 장점을 결합한 혼합형 침입탐지 시스템이 있으며, 그 예로 Prelude가 있다.

침입탐지 시스템은 탐지 기법에 따라 오용(Misuse) 기반 탐지와 비정상(Anomaly)기반 탐지로 구분된다. 오용 탐지 기법의 경우, 알려진 악의적인 공격 또는 의도치 않은 동작에 대한 정보(일반적으로 Signature)를 기반으로 공격을 탐지하여 제로데이 공격 탐지에는 부적합한 것으로 알려져 있다. 비정상 기반 탐지 기법은 말 그대로 정상적인 동작 및 행위로 정의된 상태를 벗어난 모든 상황을 비정상으로 간주하여 탐지하게 된다. 따라서 오용 탐지 기법과는 달리 제로데이 공격에 대한 탐지에 적합하지만 정상 동작 및 행위를 판단할 수 있는 근거로써 방대한 데이터가 요구되거나 학습을 통한 모델 수립에 어려움이 있다.

Ⅲ. 제어시스템 네트워크 구조 및 특성

제어시스템 네트워크는 망 분리 정책을 적용하는 것이 일반적이지만 업무 및 운영의 효율성을 위해 제어망과 내부 업무망이 연결된 운영 방식으로 확대되는 추세이다. 본 장은 제어시스템 네트워크의 구조와 네트워크 보안위협에 대응하기 위한 제어시스템 네트워크 침입탐지 시스템에 대해 설명하고자 한다.

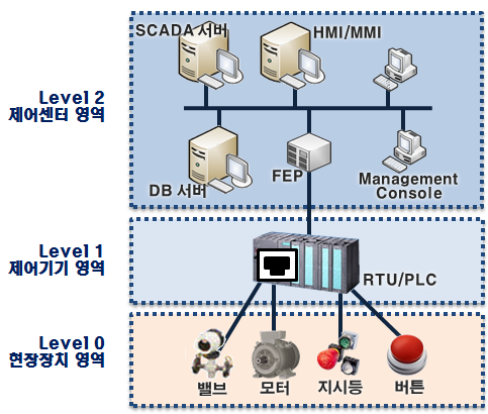
3.1. 제어시스템 네트워크 구조

제어시스템 구성요소들이 연결된 일반적인 제어시스템 네트워크의 기본적인 구조는 [그림 2]와 같다. 제어시스템 네트워크는 수준별로 현장장치 영역, 제어기기 영역, 제어센터 영역으로 구분된다. 현장장치 영역에서는 각종 상태 측정을 담당하는 센서와 동작을 수행하게 하는 구동기가 설치된 영역으로 센서 측정값의 전달과 밸브 및 모터 등의 구동이 이루어진다. 제어기기 영역은 현장장치 영역에서 전달되는 정보를 수집하고 제어센터 영역에 전송한다. 또한 제어센터 영역에서 전달되는 제어명령을 현장장치에 전송하여 해당 제어명령을 반영토록 한다. 마지막으로, 제어센터 영역은 제어시스템의 운영을 총괄적으로 관리하는 영역으로써 현장장치의 상태값을 주기적으로 수집하고 제어명령을 내리는

〔표 1〕 제어시스템 네트워크 침입탐지 기술 분류

Related work	Pub. year	Domain-specific	IDS Analysis	Information source	Extended from
[6]	2006	SCADA	Hybrid	N/A	
[7]	2009	SCADA	Anomaly-based	Network-based	
[8]	2010	SCADA	State-based	Network-based	
[9]	2010	SCADA	Anomaly-based	Network-based	
[10]	2010	SCADA	Anomaly-based	Network-based	
[11]	2010	SCADA	State-based	Network-based	[8]
[12]	2010	IEC61850	Rule-based	Network-based	
[13]	2010	SCADA	State-based	N/A	[11]
[14]	2011	Power plant	N/A	N/A	[11]
[15]	2011	Power-grid	Anomaly-based	Host-based	
[16]	2012	Smart-grid	Anomaly-based	Network-based	
[17]	2012	Power-grid	Anomaly-based	Host-based	[15]
[18]	2013	SCADA	N/A	N/A	
[19]	2013	SCADA	Anomaly-based	Network-based	
[20]	2013	SCADA	Anomaly-based	N/A	
[21]	2013	SCADA	Hybrid	Host-based	
[22]	2014	SCADA	Hybrid	N/A	[6]
[23]	2014	Smart-grid	Hybrid	N/A	
[24]	2014	SCADA	Anomaly-based	N/A	
[25]	2014	Power plant	Anomaly-based	N/A	

SCADA(Supervisory Control And Data Acquisition) 서버가 설치된 영역이다.



〔그림 2〕 일반적인 제어시스템 네트워크 구조

3.2. 제어시스템 네트워크 특성

일반적으로 제어시스템은 물리적 망 분리를 통한 폐쇄망 운영방식을 채택하고 있다. 하지만, 최근 제어시스템을 겨냥한 특화된 악성코드의 지속적인 발견과 더불어 제어시스템 침투의 교두보적인 역할을 제공하는 제어시스템-인터넷 연계 구간의 증가로 인해 제어시스템 네트워크에 대한 보안 위협이 증가하고 있다.

이러한 보안위협에 대응하기 위해 제어시스템 특성을 고려한 침입탐지 시스템에 대한 연구가 활발히 진행 중에 있다. 특히, 미국 Tofino社에서 제어시스템 통신 프로토콜(Modbus, Ethernet/IP 등)을 대상으로 한 DPI(Deep Packet Inspection) 기반 침입탐지 시스템 제품을 출시한 바 있다.

제어시스템 네트워크 토폴로지는 일반 IT 네트워크

〔표 2〕 제어시스템 통신 프로토콜별 침입탐지 기술 비교

Related work	Protocol-specific				Source	Analysis unit	Analysis method
	Modbus TCP	DNP3	Ethernet/ IP	Others			
[6]	●				N/A	Packet	Bayesian analysis and Snort
[7]			●		Data recorded from an existing critical infrastructure	Packet	Neural Network
[8]	●	●			Testbed of gas power plant	Traffic flow	Industrial Critical State Modeling Language
[10]	●	●	●		Water tank control system	Packet	Neural Network
[12]				●	Real IEC61850 network	Traffic flow	Blacklist rule
[13]	●	●			Power company,	Packet	Knowledge base and System state
[14]	●				ENEL SPA, European Commission.	Traffic flow	Critical State Analysis and State Proximity
[16]	●				Controller for the Power Supplies in ALS BTS Beam Line	Packet	Bloom-filter, N-gram, and Physical state
[18]	●				Campus power grid	Traffic flow	DFA(Deterministic Finite Automaton)
[19]		●			DNP3 network traffic in a real-world SCADA system	Packet	Burst-based whitelist Model
[21]				●	Internet Traffic and Content Analysis (ITACA) tool.	Packet	Rule-based DPI
[23]		●		●	Real grid-connected photovoltaic(PV)SCADA system	Packet	Whitelist and Behavior-based rules
[24]				●	Real SCADA data collected from Beirut power plant.	Traffic flow	Analysis for temporal behavior of frequent patterns
[25]				●	Real-world power plant simulator	Variables in App.	State relational graphs

에 비해 비교적 정적이고 소규모로 구성되어 있다. 또한, 제어명령에 대한 응답의 실시간성과 매우 높은 가용성을 요구한다. 이에 반해, 운영 중인 현장장치 및 제어기기 영역에 설치된 기기의 형태는 일반적으로 임베디드 장치이기 때문에 자원 사용의 제약이 존재한다.

다음 장에서는 이러한 특성을 지닌 제어시스템에 적용 가능한 침입탐지 기술 연구에 대해 상세히 살펴본다.

Ⅳ. 제어시스템 침입탐지 기술 연구 동향

본 장에서는 제어시스템을 대상으로 한 침입탐지 기술 연구 동향을 침입탐지 특성을 기반으로 분석하였다. 제어시스템 특성과 통신 프로토콜 특성을 기반으로 관련연구의 특징을 분류하고, 각 연구의 기술별 성능을 분석·비교한다.

〔표 3〕 제어시스템 네트워크 침입탐지 기술 공격별 성능 비교

Related work	Attack-specific	FPR(%)	TPR(%)	Accuracy(%)
[7]	Various Intrusion	0~0.378	66.063~100	N/A
[10]	MITM-based Response Injection	0~6.2	N/A	84.9~100
	DoS-based Response Injection	0~8.2	N/A	90.9~100
	Replay-based Response Injection	45.1	N/A	12.1
[13]	Complex	N/A	65.89~100	N/A
[14]	Random malicious State	0.094~0.352	N/A	99
[16]	MITM(Man in the Middle)	0	N/A	N/A
[20]	DoS(Denial of Service)	N/A	N/A	5~65
	R2L(Remote to Local)	N/A	N/A	25~100
	U2R(User to Root)	N/A	N/A	27~80
[21]	Malicious Packet Injection	0	100	N/A
[23]	MITM(Man in the Middle)	N/A	N/A	100
[24]	Injection	1.3 (Max. N/A)	89.9 (Min. N/A)	N/A
[25]	False Data Injection	0.0125	95.83	N/A

4.1. 제어시스템 네트워크 침입탐지 기술 분류

본 절에서는 2장에 언급한 일반적인 침입탐지 시스템의 분류 기준에 따라 제어시스템 네트워크 침입탐지 기술 연구를 적용 분야, 탐지 기법, 탐지에 사용되는 정보의 출처로 분류하였다.

[표 1]과 같이, Power-grid, Smart-grid, IEC61850의 전력 분야와 SCADA 시스템 분야를 대상으로 침입탐지 기술 연구가 진행되었다. 탐지 기법은 제어시스템 특성을 반영하여 제어시스템 동작 상태 정보를 활용하는 상태기반(State-based) 탐지 기법이 연구되었다. 또한, 오용 기반 탐지와 비정상 기반 탐지를 모두 사용한 혼합형(Hybrid) 기반 탐지 기술 연구가 있다. 탐지 활용 정보 출처의 경우, 센서로 부터 수집된 정보를 이용한 호스트 기반 침입탐지 기술과 제어시스템 네트워크 트래픽 분석을 통한 탐지 기술 모두 연구가 진행되었다.

4.2. 제어시스템 통신 프로토콜별 침입탐지 기술

침입탐지 기술에서 제어시스템을 대상으로 한 통신 프로토콜과 침입탐지를 위한 정보 및 분석 단위, 탐지 기법은 [표 2]와 같다. 관련 연구들은 주로 Modbus over TCP와 DNP3를 대상으로 한 탐지 기술을 제안 하였으며, 일부 연구들은 Ethernet/IP, BACnet(빌딩 제어 시스템), IEC 60870-5-104(전력 제어시스템), IEC 61850(지능형 전력 제어시스템)을 대상으로 하고 있어 제어시스템의 다양한 통신 프로토콜과 관련된 연구가 진행되고 있음을 알 수 있다.

특히, 제어시스템 네트워크 트래픽 수집의 한계점에도 불구하고 트래픽 특성을 반영하기 위해 대부분의 연구에서 실제 해당 분야의 트래픽을 수집하여 분석 데이터로 사용하였으며, 인위적인 데이터를 생성하여 탐지 기술에 적용한 경우는 극히 드물었다.

탐지 분석 단위는 대부분 네트워크 트래픽을 대상으로 한 단일 패킷 또는 트래픽 흐름(복수개 이상의 패킷) 단위로 분석하였다. 예외적으로 상태 관계형 그래프 모델을 이용한 침입탐지 기술의 경우, 시스템에서 사용되는 변수를 단위로 한다[25].

탐지 기법에 사용된 기술은 기계학습(Machine learning) 알고리즘인 인공 신경망(Artificial neural network)과 베이지안 네트워크(Bayesian network) 분석법이 사용되고 있다. 또한, 규칙 기반 기술로 흔히 쓰

이는 Snort나 Whitelist를 활용하여 트래픽의 패턴이나 행위(Behavior) 기반 개념을 적용한 혼합된 기술이 사용되었다.

4.3. 제어시스템 침입탐지 기술 성능 분석

제어시스템 네트워크 침입탐지 기술의 탐지 대상이 되는 공격과 해당 공격의 탐지 성능은 [표 3]과 같다. 우리는 관련 연구 간 성능 비교의 지표로 활용될 수 있는 요소를 FPR(False Positive Rate), TPR(True Postive Rate), 정확도(Accuracy)로 구분하였다.

제어시스템이 도입되어 운영하는 기관이 대부분 기반시설임을 감안하면, FPR이 0을 초과할 때 미치는 영향 및 파급효과를 고려한다면 대부분의 침입탐지 기술의 경우 0에 가까운 완벽한 탐지 성능을 보이고 있다.

대표적인 공격 유형인 인젝션(Injection) 공격 탐지 시 호스트 기반 혼합형 탐지 기술을 적용한 연구[21]에서 가장 뛰어난 성능을 보여줬다. 또한, 중간자 공격(MITM, Man in the Middle attack)의 경우 해당 기술 모두 완벽한 탐지가 가능함을 확인했다[16].

Ⅴ. 결 론

본 논문에서는 제어시스템의 특성을 고려한 제어시스템 특화 침입탐지 시스템의 탐지 기술 연구 동향에 대해 분석하고 제어시스템 운영영역, 침입탐지 활용 정보, 탐지 기법에 따른 기술의 분류를 제시했다. 더불어, 제어시스템의 특성을 고려한 탐지 기법의 공격 탐지 성능을 비교하여 현재 탐지 가능한 제어시스템 공격과 공격별 최적 탐지 기법에 대해 기술했다.

본 논문을 통해 제안된 제어시스템 침입탐지에 적용된 탐지기법 및 모델의 분류를 참조하고, 제어시스템 특성을 반영한 침입탐지 기술 개발에 필요한 객관적인 자료로써 활용될 수 있을 것이라 기대한다.

참 고 문 헌

[1] ICS-CERT, “ICS-CERT Monitor: October/Novbember/December,” 2013.

[2] ICS-CERT, “Alert (ICS-ALERT-10-301-01): Control System Internet Accessibility,” Oct. 2010.

[3] ICS-CERT, “Year in Rreview 2012,” Mar. 2013.

[4] ICS-CERT, “Year in Review 2013,” Feb. 2014.

[5] R. Bace, P. Mell, “NIST Special Publication on Intrusion Detection Systems,” September 2001.

[6] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, “Using Model-based Intrusion Detection for SCADA Networks,” *In Proceedings of the SCADA Security Scientific Symposium*, 2006.

[7] O. Linda, T. Vollmer, M. Manic, “Neural Network Based Intrusion Detection System for Critical Infrastructures,” *Neural Networks*, *International Joint Conference on*, pp.1827-1834, June 2009.

[8] I. N. Fovino, M. Masera, M. Guglielmi, A. Carcano, A. Trombetta, “Distributed Intrusion Detection System For SCADA Protocols,” *Critical Infrastructure Protection IV*, *IFIP Advances in Information and Communication Technology*, vol.342, pp.95-110, 2010.

[9] R. Ramos, R. Barbosa, A. Pras, “Intrusion Detection in SCADA Networks,” *Mechanisms for Autonomous Management of Networks and Services*, *Lecture Notes in Computer Science*, vol.6155, pp.163-166, 2010.

[10] W. Gao, T. Morris, B. Reaves, D. Richey, “On SCADA Control System Command and Response Injection and Intrusion Detection,“ *eCrime Researchers Summit (eCrime)*, pp.1-9, Oct. 2010.

[11] A. Carcano, I. N. Fovino1, M. Masera1, A. Trombetta, “State-Based Network Intrusion Detection Systems for SCADA Protocols A Proof of Concept,“ *Critical Information Infrastructures Security*, *Lecture Notes in Computer Science*, vol.6027, pp.138-150, 2010.

[12] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, J. Tan, “An Intrusion Detection System for IEC61850 Automated Substations,” *Power Delivery*, *IEEE Transactions on*, vol.25, no.4, pp.2376-2383, Oct. 2010.

[13] I. N. Fovino, A. Carcano, T. D. L. Murel, A. Trombetta, M. Masera, “Modbus/DNP3

State-based Intrusion Detection System," *Advanced Information Networking and Applications (AINA)*, *24th IEEE International Conference on*, pp.729-736, April 2010.

[14] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino, A. Trombetta, "A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems," *Industrial Informatics*, *IEEE Transactions on*, vol.7, no.2, pp.179-186, May 2011.

[15] J. Reeves, A. Ramaswamy, M. Locasto, S. Bratus, S. Smith, "Lightweight Intrusion Detection for Resource-Constrained Embedded Control Systems," *Critical Infrastructure Protection V*, *IFIP Advances in Information and Communication Technology*, vol.367, pp.31-46, 2011.

[16] S. Parthasarathy, D. Kundur, "Bloom Filter based Intrusion Detection for Smart Grid SCADA," *Electrical & Computer Engineering (CCECE)*, *25th IEEE Canadian Conference on*, pp.1-6, April 2012.

[17] J. Reeves, A. Ramaswamy, M. Locasto, S. Bratus, S. Smith, "Intrusion Detection for Resource-constrained Embedded Control Systems in the Power Grid," *International Journal of Critical Infrastructure Protection*, vol.5, Issue 2, pp.74–83, July 2012.

[18] N. Goldenberg, A. Wool, "Accurate Modeling of Modbus/TCP for Intrusion Detection in SCADA Systems," *International Journal of Critical Infrastructure Protection*, vol.6, Issue 2, pp.63–75, June 2013.

[19] J. Yun, S. Jeon, K. Kim, W. Kim, "Burst-based Anomaly Detection on the DNP3 Protocol," *International Journal of Control and Automation*, vol.6, no.2, pp.313-324 April 2013.

[20] A. Anoop, M. S. Sreeja, "New Genetic Algorithm Based Intrusion Detection," *International Journal of Engineering Innovation & Research*, vol.2, Issue 2, pp.171-175, 2013.

[21] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, H. F. Wang, "Rule-based intrusion detection system for SCADA networks," *Renewable Power Generation Conference (RPG)*, pp.1-4, September 2013.

[22] Q. Chen, S. Abdelwahed, "A Model-based Approach to Self-Protection in SCADA Systems," *9th International Workshop on Feedback Computing*, June 2014.

[23] Y. Yang, K. McLaughlin, S. Sezer, B. Pranggono, T. Littler, B. Pranggono, H. F. Wang, E. G. Im, "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks," *Power Delivery*, *IEEE Transactions on*, vol.29, no.3, pp.1092-1102, June 2014.

[24] N. Sayegh, I. H. Elhajj, A. Kayssi, A. Chehab, "SCADA Intrusion Detection System Based on Temporal Behavior of Frequent Patterns," *17th IEEE Mediterranean Electrotechnical Conference (MELECON)*, pp.432-438, April 2014.

[25] Y. Wang, Z. Xu1, J. Zhang, L. Xu, H. Wang, G. Gu, "SRID: State Relation Based Intrusion Detection for False Data Injection Attacks in SCADA," *Computer Security - ESORICS*, *Lecture Notes in Computer Science*, vol.8713, pp.401-418, 2014.

〈저자소개〉

사 진

최 승 오 (Seungoh Choi)
비회원

2012년 2월 : 아주대학교 정보및컴퓨터공학과 졸업
2014년 2월 : 아주대학교 컴퓨터공학과 공학석사
2013년 12월~현재 : ETRI 부설연구소 연구원

관심분야 : SCADA 보안, 제어시스템 보안, 제어 프로토콜 퍼징, 네트워크 보안

사 진

김 우 년 (Woo-Nyon Kim)
정회원

1996년 2월 : 안동대학교 컴퓨터공학과 졸업
1998년 2월 : 경북대학교 컴퓨터과학과 이학석사
2000년 2월 : 경북대학교 컴퓨터과학과 박사수료
2000년 3월~2003년 12월 : ㈜니츠 선임연구원
2003년 12월~현재 : ETRI 부설연구소 책임연구원/실장
관심분야 : 기반시설보안, SCADA 보안, 제어시스템 보안, 취약점 분석, 네트워크 보안