

# Security Monitoring and Network Management for the Power Control Network

Sugwon Hong, Jae-Myeong Lee, Mustafa Altaha

Department of Computer Engineering, Myongji University, Yongin, R. of Korea

Email: swhong@mju.ac.kr; ljm9317kr@gmail.com; mustafaraed@mju.ac.kr

Muhammad Aslam

Department of Electrical Engineering, Myongji University, Yongin, R. of Korea

Email: aslammju@gmail.com

**Abstract**—Security monitoring is a viable solution to enhance the security capability in the current power control SCADA network, since the intrusion detection system as a main tool for monitoring can be easily deployed without any change of SCADA configuration. We explain how to design the domain-specific network security monitoring system, reflecting semantics of the target SCADA network. However, considering the recent attacks to the SCADA/ICS systems, the attack vectors are the vulnerabilities of the software underlying the host systems. In this respect, we need security monitoring running on host systems which can provide process and memory protection. Furthermore, Network and system management which incorporates the IT network management into the power control system can not only help to manage and maintain the IT/OT system in a unified way, but also enhance the security capability of the SCADA system with collaboration with network and host security monitoring.

**Index Terms**—power control network, SCADA, cyber security, security monitoring, IDS, HIDS, network management

## I. INTRODUCTION

Realizing the importance of cyber security of the supervisory control and data acquisition (SCADA) network which lies in the core of the power control system, a plethora of works have been published to address this issue by international standard bodies, government organizations, utilities, vendors, and academic researchers. These cyber security-related documents published mainly by international standard bodies and government organizations are classified by two criteria. One is the degree of technological details by which the documents can fall under management-oriented or technology-oriented categories. The other is the target or domain to which the documents are intended. All the security measures adopted to the power control system eventually can come under one of three security

strategies: network separation, communication message security, and security monitoring [1].

Even though complete physical separation is not possible in the current SCADA network, logical network separation, which divides the network into different domains depending on criticality or functionality or any other purposes, is an effective strategy to prevent unwarranted entries into the network. Each domain constitutes a virtually separated network which is only connected to other domains via dedicated entry points only on which all information flows are exchanged and strict security policing is enforced. The primary goal is that when attackers try to penetrate deeper networks, it can reduce the probability of attack success, i.e., attacks are as isolated into a penetrated network domain as possible, mitigating attack impacts. The concept to separate one network into several segmented zones or domains is nothing new in the network design of the IT world. Firewall and intrusion prevention system (IPS) are common equipment used for this purpose, and virtual private LAN (VPN) is a common network design technique used for deploying virtual networks. The network separation, which is often called ‘Defense-in-Depth’, is the go-to strategy that is being implemented in the current SCADA/ICS system, and maybe it will continue to be so for a foreseeable future [2, 3].

Communication message security in the power control system targets providing the integrity, authentication, and/or confidentiality of messages exchanged between devices in the SCADA system, based on digital signature, hashed MAC(HMAC), crypto algorithms, and security protocols such as TLS. The document [4-7] addresses this issue, specifying security measures to provide the integrity, authentication, and/or confidentiality of messages in the IEC 61850 communication substation.

However, the major challenge of this strategy lies in implementation. Embedded devices in substations have limited computing resources and can devote only a part of their resources for security processing. In addition to implementation, migration is another daunting challenge since installing security functions into legacy devices overnight is not possible. Replacement or even retrofitting process will be difficult and time-consuming

---

Footnotes: 8-point Times New Roman font;

Manuscript received July 1, 2012; revised August 1, 2012; accepted September 1, 2012.

Copyright credit, project number, corresponding author, etc.

because SCADA systems should be in 24/7 operation. Considering implementation and migration challenges, it is hard to expect to adapt the communication message strategy to the SCADA system in the foreseeable future.

Security monitoring is also an integral part of security strategies in the traditional IT network. While network separation is aimed to prevent unauthorized access into the SCADA system, security monitoring intends to detect and reports any illegitimate behavior inside the SCADA system. In reality, network separation cannot guarantee complete prevention of illegal access, but only can decrease the possibility of unauthorized access and mitigate any disruptive incidents by illegal operations. For this reason, security monitoring is considered to be an indispensable part of security strategies. Compared to typical IT systems, the SCADA systems have predictable patterns of traffic flow between fixed network nodes. This simplicity renders monitoring solution more attractive in the SCADA system. Furthermore, the communication in the SCADA system mostly rely on the standard protocols such as IEC 61850, DNP3, and Modbus, which correspond to the application layer protocols above the TCP/IP stack. This uniformity makes easy to derive rules from the protocols which can be used to decide which behaviors are normal or not in the network. Moreover, security monitoring can be easily adapted to the current SCADA network without any significant change of system architecture and components. In this sense, security monitoring strategy can provide much room for enhancing security capability in the current system without any hassle.

In this paper we will explain how to design network security monitoring which is reflecting the semantics of the underlying SCADA systems based on the analysis of the current works. We also point out the limitation of the network security monitoring approach, considering the current cyber attacks against SCADA/ICS networks. And we explain the necessity of host-level security monitoring.

Network management is an essential tool to monitor and control a network system in a comprehensive way. However, the current network management system is only focused on network components, consequently causing IT and OT operation management to be separated. In this respect, network and system management will help to realize the integration of IT and OT operations. Another benefit of monitoring based on network management is that it can provide the possibility to upgrade the capability of security in SCADA systems.

## II. NETWORK SECURITY MONITORING

Network security monitoring is to do the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions. Security monitoring is a way of finding intruders on the network and do something about them before they damage the system [8]. In a nutshell, security monitoring is involved in detecting and reporting any illegal behaviors in the system, consequently providing the necessary high-level of security and reliability in the SCADA system.

The intrusion detection system (IDS) is a main tool to do security monitoring. The techniques of IDS in which we are interested for the SCADA system is the anomaly-based detection. The anomaly detection is the process to determine which observed events are to be identified as abnormal because it has significant deviation from normal behavior which is called ‘profile.’ As always, the difficult part is how to decide or derive profiles which reflect all semantics of the system. Thus, the main task to do security monitoring is to design domain-specific IDS which is aware of the target domain semantics. Here, we classify four kinds of information to derive profiles for SCADA-aware IDS: network flows, application protocols, process features, and data features for self-learning.

Fig. 1 shows the framework of the anomaly-base intrusion detection. In this framework, the learning box to derive profiles is part and parcel of the whole procedure. Analyzing inputs of the learning box, we derive profiles or normal behavior.

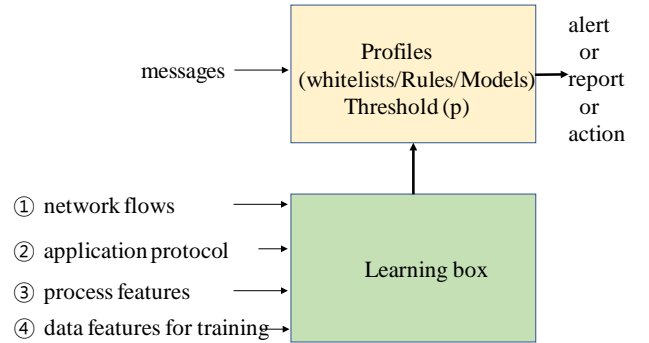


Figure 1. Framework of intrusion detection system(IDS)

### A. Flow-aware Monitoring

The first input to the learning box to be considered is the information about network traffic flows in the target system. As the paper [9] well pointed out, the SCADA networks have very predictable patterns compared to IT networks. In the IT network, it is not possible to completely predict a list of allowable communication paths. A large portion of the traffic occurring in the IT network is involved in human actions, leading to dynamic traffic patterns. On the contrary, the SCADA network configuration is stable and has the fixed IP addressing schemes. Unless there is any abrupt change in the system configuration, intentional or unintentional, communication paths are deterministic since data exchanges take place between fixed nodes such as control servers, IED, PLC, RTU, and other field devices, which are mostly machine-to-machine communication.

Considering the current substation automation system(SAS) is running on the TCP/IP stack and Ethernet-based LANs, the flow can be defined by the 3 address tuples of source and destination stations: (MAC address, IP address, TCP/UDP port). Then we can specify a list of allowable flows in the network, which is often called a whitelist. This list can be preconfigured based on the knowledge of legitimate nodes and communication in the network, and/or dynamically managed based on the

result of monitoring traffic by switches in the network. The papers [9-12] elaborate the network flow-aware anomaly detection approach.

### B. Protocol-aware Monitoring

These days, the SCADA networks in the power control system are operating based on the standard communication protocols such as IEC 61850, IEC 60870-5-104, DNP3.0, and Modbus. All the measured data, state information, and on/off command are delivered as the application protocol data unit (APDU) encapsulated in IP packets. The semantics of each fields in the APDU can be used to verify the validity of the incoming packets, and detect any anomalous communication. Furthermore, any correlated rules between different fields of the same packet or between the fields of subsequent packets are also utilized as effective criteria to decide whether incoming packets obey the logic of the application protocols. For example, if the sequence number field exists in the header, the sequence numbers of all packets should be in order, and the following packet's number should be incremented by one. Time stamp field is also useful to check the correctness of a series of arriving packets.

In this way, the extracted APDU information of incoming packets is compared with profiles by simple matching or sometimes checking rules of a single packet or between the sequence of packets.

The protocol-aware anomaly detection approach can be integrated with the flow-aware method insofar, since the SCADA-specific application protocols are running over the TCP/IP stacks. This approach is also called the rule-based, model-based, or specification-based anomaly detection in other literatures. The papers [13-20] derive the profile regarding IEC 61850 protocols, and the papers [21, 22] propose IDS based on IEC 60870-5-104 and DNP3.0 protocols. The paper [23] proposes IDS relating to Modbus protocol, and the paper [24] proposes the framework to generate dynamic rules for multi-protocols.

### C. Process-aware Monitoring

The effectiveness of anomaly detection can be increased as we can derive profiles which are more aware of semantics of the target SCADA system. If we can extract normal/abnormal features from the changes of process-level states and field devices, we can enhance the performance of anomaly detection capability. The papers [25-29] propose and explain the process-aware anomaly detection approaches. This deep process-level inspection method tries to capture useful features from data semantics of sensors, logics of commands, and dynamics of process operations. Its generalized framework can be depicted as in Fig. 2. The commands issued by control servers generate new state at the process. Then IDS compares new state with the predicted state. The detection system generates alert signals when suspicious and erroneous commands and sensor readings are detected, which cause the process to reach insecure or unsafe states.

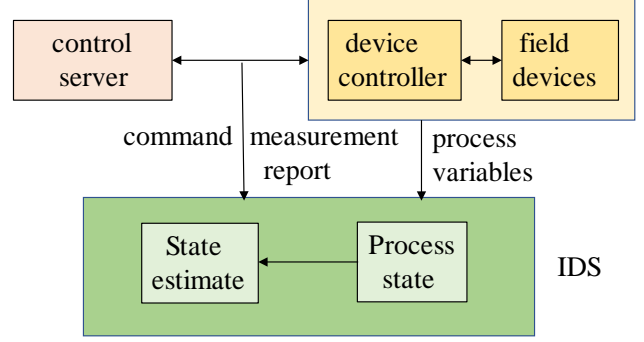


Figure 2. Process-aware IDS framework

### D. Self-learning based Monitoring

In recent years, many researchers have begun to focus on constructing SCADA-IDSs using machine learning and deep learning methods. Machine learning-based IDSs can achieve satisfactory detection levels when sufficient training data is available, and machine learning models have sufficient generalizability to detect attack variants and novel attacks. Compared with traditional machine learning methods, deep learning methods are better at dealing with a large volume of data. Moreover, deep learning methods can automatically learn feature representations from raw data and then output results.

While considerable works on machine learning-based SCADA-IDSs have been done so far, few works have been done for deep learning-based IDSs focusing on the SCADA systems [30-36]. Moreover, fewer works have been reported on the power SCADA systems [32, 34], while others are focusing on the different SCADA domains such as gas pipeline networks [30, 35], water treatment systems [33, 36], and heating control system [31].

The framework of the deep learning-based IDS is shown in Fig. 3. First and foremost, meaningful design of deep learning detection model requires significant understanding of domain knowledge and acquisition of proper datasets. In this sense, the data feature extraction is the most important step to develop successful detection models. From raw network traffic, we should derive the feature vector at time  $t$ ,  $X_t = (x_0, x_1, \dots, x_n, label)$  to train and test a deep learning model, consequently constructing the detection model which is corresponding to the profile of IDS. The *label* in the feature vector signifies the types of attacks, which might be a binary value or multi-class values. The input features,  $(x_0, x_1, \dots, x_n)$  should reflect the semantics of the SCADA domains. All the works are using the data field information of the application protocol data units (PDU) of the SCADA communication protocols such as Modbus [30, 31, 33] and DNP3.0 [32, 34], along with the TCP/IP header information. Together with the input data features, the deep learning models will affect the effective of the detection model. The deep learning models to be used in the papers are varied: LSTM[30,33, 36], ANN[31], CNN[32, 35], and RNN[34].

Ironically, automatic learning capability of the deep learning approaches is the merits, and also demerits at the same time. Contrary to the other monitoring methods, the

profiles of which we can understand and control, the deep learning detection model, i.e. the profiles, is opaque to us, which means we cannot understand and control the detection logics of the profiles.

Machine and deep learning provides significant benefits, since it is expected to offer capability of updating in defense quick to respond new variants of attacks. However, model construction requires significant understanding of the problem being addressed, which involves analyzing the data collected to extract ‘features’ that are used to learn detection logics. The challenge of deep learning-based IDS lies in proper usage of data features for training and testing to reflect as much of semantics of power SCADA systems as possible, and reasonable validation to verify its usefulness of defense against attack variants.

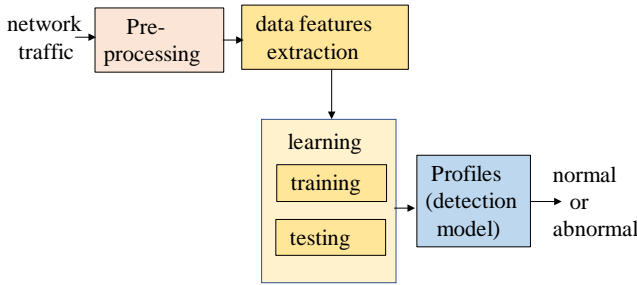


Figure 3. Deep Learning-based IDS framework

### III. EVALUATION

The attack model or scenario in the power system can be summarized into two steps: first, an attacker penetrates into any vulnerable stations in the SCADA network, and finally an attacker generates maliciously coded commands to the field devices and causes the power system into insecure or unsafe states. The possible attacks on which most anomaly detection systems set their sights are data injection, replay, and DoS attacks among others [37], because these attacks are directly related to compromise field devices, consequently causing malfunction in the power operation.

Then, the question is whether the network security monitoring explained in the previous section can detect these attacks. The answer, unfortunately, is not optimistic, considering the substance of the recent sophisticated attacks against SCADA/ICS systems [38-48].

One of main purposes of anomaly detection is to check the integrity and authenticity of data exchanged, i.e. whether they comply with the underlying SCADA protocols and accompanying rules in the system. In the real systems, however, there are other types of information or messages that are exchanged for configuration and operation related to various software, especially OS. The recent attacks, which shocked people in SCADA/ICS systems, hijack or take control of host stations, control servers and eventually device controllers, once they penetrate the networks in one way or another. Their attack vectors are vulnerabilities of the software underlying the host systems. In this respect, we need to pay attention to the supply chain management and

precaution for managing and/or outsourcing servers. But if we want to find any security solutions on top of vendor-independent platforms, we need to take special attention to the attack vectors which have been revealed in the recent incidents [48].

The network IDS, which is currently proposed in the context of the SCADA/ICS systems, intends to detect anomaly behavior based on traffic patterns or contextual mismatch of message contents which are specified in the standard protocols such as Modbus, DNP3.0 and IEC61850. However, the real attacks do not take place via the standardized and defined communication messages. Rather, the attacks were accomplished by way of taking over central servers and local device controllers. As shown in the Stuxnet, the attack was realized by injecting malicious codes -DLL files in this case- into legitimate process memory and executing the malicious codes in the context of a legitimate process. Once a code is injected into the target process, it has full access to the process memory and can manipulate code and data blocks of programmable logic controllers (PLC), and eventually cause malfunction of field devices. For this reason, the authenticity and integrity check of the messages which are exchanged between control servers and local device controllers cannot detect these kinds of attacks.

In this respect, the process-aware monitoring is considered to be more reasonable and realistic approach, reflecting the semantics of process-level operations. This monitoring can be used to support a central IDS, locating at the local process network. Furthermore, considering that the attacks are aiming at manipulating process and memory in the intelligent devices of the power system, we need to go deep into host-level monitoring along with network security monitoring [49].

### IV. HOST SECURITY MONITORING

In order to execute all the programs, all executable codes as well as external libraries such as DLL files which are referred to by the executable codes should be loaded into process memory. In the same way malicious codes can be loaded into the memory, which is often called the code injection technique. By way of the code injection, attackers can execute malicious codes in the name of legitimate processes, access the code memory and data memory of the main processes, and also hide themselves from monitoring imposed by the internal security policies of security solutions. The code injection, by which attackers inject their intended codes, can take a form of directly writing executable codes or shellcode into memory or of loading their DLL files into memory.

For the former case, they utilize the memory management system calls. First, they assign necessary memory space by the memory allocation system calls, and load the executable binary codes into memory space by the memory writing system calls. To execute these loaded codes, they often create new threads. In the case of loading DLL which is also called “DLL injection”, once the malicious DLL files are loaded into the target process, the process refers to these files on executing without any extra manipulation. Attackers utilize



invoking the loader system calls by thread generation, or windows hooks, or DLL swapping. In general, the DLL injection is more utilized for its convenience.

Once a code is injected onto the target process memory, it has full access to the process memory and can modify its components. Manipulating the process memory components enables attackers to modify system functions (executable codes) or to change the function addresses such as entries in the Import Address Table(IAT). This technique is called as “hooking”. In this way attackers can force their intended codes to be executed instead of original legitimate codes.

In order to detect and prevent such attacks, we need security measures to detect any process manipulation which is involved in memory range protection, file paths, and file handling. To prevent the attack of the executable code injection, we should inspect whether the process memory is assigned by legitimate executable codes or loading legal DLL files, or allocated by external system calls, which can be examined by referring to memory information enquiry functions provided by the OS. For the case of the DLL injection, we can utilize the method to find out where the codes to invoke the DLL load calls are located.

## V. NETWORK MANAGEMENT

### A. IT/OT convergence

Traditionally, network management is an indispensable tool to manage complex IT network systems. Network management enables a human manager to have a big picture of complex systems by monitoring the status and operation of all network components in real-time. So, this leads to obtain up-to-date information about system components at the right time.

Currently SCADA operation management and IT network management are separated. SCADA servers or EMS collect operation information from IED over the IT network. Then the SCADA operation manager takes necessary actions based on this operation information about the SCADA system. On the other hand, the IT network manager collects information about network component such switches, routers, and transmission equipment, which consists of the IT network overlaying the SCADA system. The SCADA operation manager is blind to the IT network, and at the same time the IT network manager is also unaware of the SCADA operating system components. For example, when the SCADA operation managers detect a problem, they could not decide whether it is caused by the IT network or an IED failure [50].

To expand the concept of network management to the SCADA system can enhance the capability of monitoring IT/OT system in an integrated way. The agent residing in the SCADA system component, mainly Intelligent Electronic Devices (IEDs), collects information regarding physical access, communication security, SCADA protocols, clock, and environment, so that the IT/OT network manager can have the integrated view of the SCADA operating components as well as IT

communication components. For this purpose, we need to expand the network and system management (NSM) data objects to reflect what information is needed to manage the SCADA system reliably. The abstract NSM data objects can then be mapped to any appropriate protocol. At present, some of SCADA system device vendors define private MIBs and try to utilize them for monitoring SCADA operations. In order to provide interoperability and approach to NSM in a unified way, IEC defines the standard MIBs for the substation automation devices [51].

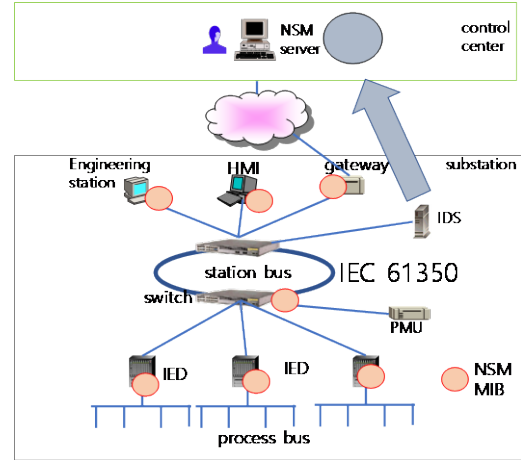


Figure 4. Substation automation system with NSM and IDS

### B. Integrated Security Monitoring

NSM typically have two functional aspects: management and monitoring. NSM provides the integrated view of the IT/OT system and resolve detected problems and facilitate maintenance. To acquire information that is related to the operational aspects of the SCADA infrastructure provides the capability of NSM monitoring. Not only can such information be utilized for system operation optimization, it can also be applied to security threat detection, which is the main role of IDS. The question is how an NSM manager interacts with IDS for this purpose. One possible interaction scenario and configuration is shown in Fig. 4. In this figure, IDS is placed as a standalone device and collect necessary information for its own purpose. And IDS will send results of its actions, so NSM share this report to make any critical security decision.

One advantage of NSM monitoring is that we can obtain deep-level data of field devices along with network traffic data. Utilization of this deep-level data can enhance the capability of security monitoring together with network-aware and host-aware IDSs. Fig. 5 shows the framework of a way of integrating security monitoring, combining all functions of three components: network-based IDS, host-based-IDS, and NSM monitoring.

The current IEC 62351-7 MIBs do not contain all the information that is necessary to implement the IDS functions explained in section II [51]. The detection functions based on NSM MIBs are limited to detect

physical access and resource exhaustion with respect to IED. Applying NSM to the SCADA system will take time, while the deployment of IDS can be deployed anytime when it is necessary and ready without any impact on the SCADA system configuration.

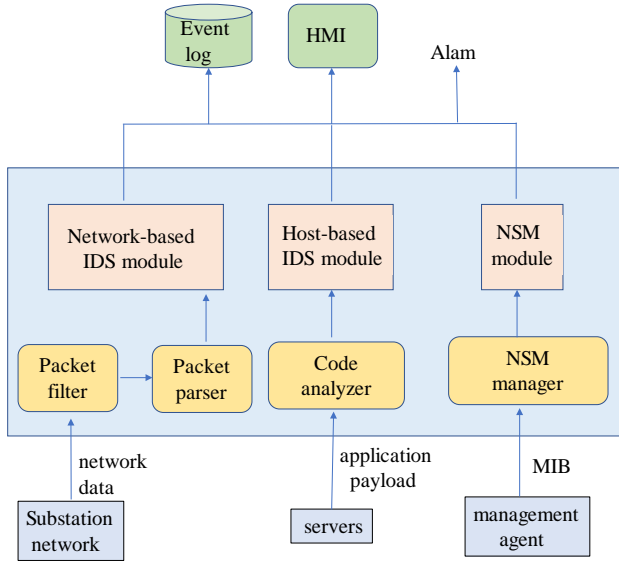


Figure 5. Framework of Integrated Security Monitoring

## VI. CONCLUSION AND FUTURE DIRECTION

Network separation is currently the dominant security strategy which the SCADA systems rely on. Security monitoring is a viable solution to enhance the security capability in the SCADA system, considering that the deployment of intrusion detection systems (IDS) is applied without any change of current SCADA system configuration. The main challenge is how to design domain-specific IDS which is aware of semantics of the SCADA system. The profiles of SCADA-friendly IDS can be derived based on network flows, application protocols, process-aware features, and deep learning techniques.

However, considering the recent attacks against SCADA/ICS systems, the network-based security monitoring does not provide sufficient measures to detect and prevent these sophisticated attacks. For this reason, we need to derive profiles which are more aware of semantics of the target SCADA system. In this sense, the process-aware IDS is more appropriate to defend sophisticated attacks which are eventually targeting field devices.

With the success of deep learning techniques in other areas, anomaly intrusion detection system is emerging as a promising application area of deep learning. However, deep learning-based IDS for the SCADA systems is still at a fledgling stage. Constructing deep learning models requires a significant understanding of the domain knowledge. Relating to SCADA security, the knowledge means to understand attack patterns, operating mechanisms, and process (or field) networks, which have different characteristic and semantics from the typical IT

systems. Creating successful models also requires deep expertise in SCADA data features which are used for learning. Learning requires to collect massive amounts of real-life information and engineer it into useful formats.

The nature of the recent sophisticated attacks against SCADA/ICS systems is to exploit software vulnerability, performing process manipulation by injecting malicious codes into legitimate process memory and executing the malicious codes in the context of a legitimate process. Thus, we need security monitoring running on host systems which can provide process and memory protection. These measures can provide a holistic security monitoring strategy for the power control system.

Recently, the IT network management technique is applied to the OT system, providing a way of IT/OT management integration. However, the current IT/OT management is focusing on only monitoring OT system components in order to facilitate maintenance functions. However, cooperating with network-based and host-based IDS, the network and system management (NSM) can enhance the capability of security monitoring.

## CONFLICT OF INTEREST

The authors declare no conflict of interest.

## AUTHOR CONTRIBUTIONS

Sugwon Hong researched, designed, and wrote the paper. Jae-Myeong Lee did the work on the part of host security monitoring, and Mustafa Altaha did literature survey and analysis on deep learning-based IDS. And Muhammad Aslam gave valuable advices and comments to improve the paper.

## ACKNOWLEDGMENT

This work was supported by “Human Resources Program in Energy Technology” of the Korea Institute of Energy Technology Evaluation and Planning (KETEP), granted financial resource from the Ministry of Trade, Industry & Energy, Republic of Korea. (No. 20174030201790) And this research was also supported by Korea Electric Power Corporation. (Grant number: R18XA01).

## REFERENCES

- [1] S. Hong, “Cyber Security Strategies and their Implications for Substation Automation Systems,” *Int’l J. of Smart Grid and Clean Energy*, vol. 8, no. 6, pp 747-756, November 2019.
- [2] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, DHS ICS-CERT. September 2016.
- [3] Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82 Rev.2, May 2015.
- [4] Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security – Profiles including TCP/IP, IEC TC57 WG15, IEC 62351-3, May 2018.
- [5] Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS, IEC TC57 WG15, IEC 62351-4, November 2018.
- [6] Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives, IEC TC57 WG15, IEC 61850-5, 2013.

- [7] Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850, IEC TC57 WG15, IEC 62351-6, 2007.
- [8] R. Bejtlich. *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press, 2013.
- [9] A. Lemay, J., Rochon, and J. Fernandez, "A Practical flow white list approach for SCADA systems," in *Proc. the 4th International Symposium for ICS & SCADA Cyber Security Research*, 2016.
- [10] G. K. Ndonga and R. Sadre, "A Two-level Intrusion Detection System for Industrial Control System Networks using P4," in *Proc. ICS & SCADA*, 2018.
- [11] R. Udd, M. Asplund, S. Nadjm-Tehrani, M. Kazemtabrizi, and M. Ekstedt, "Exploiting Bro for Intrusion Detection in a SCADA System," *CPSS'16*, June 2016.
- [12] R. Barbosa, "Anomaly Detection in SCADA Systems, A Network Based Approach," Ph.D. dissertation, University of Twente, April 2014.
- [13] M. Ko and M. Jenkner, "Cybersecurity Defense System for Distributed Communication Network in IEC-61850 Power Substations," *Cigre De Colloquium*, June 2019.
- [14] J. Hong and C-C. Liu, "Intelligent Electronic Devices with Collaborative Intrusion Detection Systems," *IEEE Tran. On Smart Grid*, Vol. 10, No.1, January 2019.
- [15] M. Kabir-Querrec, "Cyber security of the smart grid control systems: intrusion detection in IEC 61850 communication networks," Ph.D. dissertation, University Grenoble, 2017, Available: <https://hal.archives-ouvertes.fr/tel-01609230>
- [16] M. T. A. Rashid, S. Yusoff, and Y. Yusoff, "Trust System Architecture for Securing GOOSE Communication in IEC 61850 Substation Network," *International Journal of Security and its Applications*, vol. 10, no. 4, pp289-302, 2016.
- [17] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, and K. McLaughlin, "Multidimensional Intrusion Detection System for IEC 61850 based SCADA Networks," *IEEE Transactions On Power Delivery*, vol. 32, no. 2, April 2017.
- [18] J. Hong, C-C. Liu, "Integrated Anomaly Detection for cyber security of the substation," in *IEEE Tran. On Smart Grid*, vol. 5, no. 4, July 2014.
- [19] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiatribute SCADA-Specific Intrusion Detection System for Power Networks," *IEEE Tran. On Power Delivery*, vol. 29, no. 3, June 2014.
- [20] Y. Yang, K. McLaughlin, L. Gao, S. Sezer, Y. Yuan, and Y. Gong, "Intrusion detection system for IEC 61850 based Smart Substations," in *Proc. IEC Power and Energy Society General Meeting*, 2016.
- [21] H. Lin, A. Slagell, C. D. Martina, Z. Kalbarczyk, and R. K. Iyer, "Adapting Bro into SCADA: Building a Specification-based Intrusion Detection System for the DNP3 Protocol," in *Proc. CSIRW '12*, October 2012.
- [22] S. Cheung, R. Dutertre, M. Fong, U. Lindqvist, and K. Skinner, "Using Model-based Intrusion Detection for SCADA Networks," in *Proc. the SCADA Security Scientific Symposium*, January 2007.
- [23] J. Nivethan and M. Papa, "Dynamic Rule Generation for SCADA Intrusion Detection," in *Proc. IEEE Symposium on Technologies for Homeland Security*, May 2016.
- [24] J. J. Chromik, A. Memke, and B. Haverkort, "Bro in SCADA: dynamic intrusion detection policies based on a system model," in *Proc. ICS & SCADA*, 2018.
- [25] H. Lin, A. Slagell, Z. T. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Runtime Semantic Security Analysis to Detect and Mitigate Control-Related Attacks in Power Grids," *IEEE Tran. On Smart Grid*, vol. 9, no. 1, January 2018.
- [26] J. Nivethan and M. Papa, "A SCADA Intrusion Detection Framework that Incorporates Process Semantics," in *Proc. CISRC*, 2016.
- [27] J. J. Chromik, A. Remke, B. R. Haverkort, "What's under the hood? Improving SCADA security with process awareness," in *Proc. Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, 2016.
- [28] H. Janicke, A. Nicholson, S. Webber, and A. Cau, "Runtime-Monitoring for Industrial Control Systems," *Electronics* 2015, 4, pp 995-1017.
- [29] D. Hadziosmanovic, R. Sommer, and E. Zambon, "Through the Eye of the PLC: Towards Semantic Security Monitoring for Industrial Control Systems," in *Proc. ACSAC'14*, December 2014.
- [30] R. L. Perez, F. Adamsky, R. Soua, and T. Engel, "Forget the Myth of the Air Gap: Machine Learning for Reliable Intrusion Detection in SCADA Systems," *EAI Endorsed Transactions on Security and Safety*, 2019.
- [31] A. Hijazi and J-M. Flaus, "A Deep Learning Approach for Intrusion Detection System in Industry Network," *The 1st int'l conference on Big Data and Cybersecurity intelligence*, Beirut, Lebanon, 2019.
- [32] H. Yang, L. Cheng, and M. D. Chuah, "Deep-Learning-Based Network Intrusion Detection for SCADA Systems," *IEEE conf. on Communication and Network Security (CNS): Workshops: CPS Sec: Internation Workshop On Cyber-Physical Systems Security*, 2019.
- [33] J. Gao, L. Gan, F. Buschendorf, L. Zhang, H. Liu, P. Li, X. Dong, and T. Lu, "Omni SCADA Intrusion Detection Using Deep Learning Algorithms," *arXiv*, Aug. 2019.
- [34] S. Kwon, H. Yoo, and T. Shon, "RNN-based Anomaly Detection in DNP3 Transport Layer," *IEEE int'l Conf. on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019.
- [35] J. Liu, L. Yin, Y. Hu, S. Lv, and L. Sun, "A Novel Intrusion Detection Algorithm for Industrial Control Systems Based on CNN and Process State Transition," *IEEE 37th Int'l Performance, Computing and Communications*, 2018.
- [36] J. Goh, S. Adepu, M. Tan, and L. X. Shan, "Anomaly Detection in Cyber Physical Systems using Recurrent Neural Networks," *IEEE 18th Intl Symposium on High Assurance Systems Engineering*, 2017.
- [37] A. Elgargouri and M. Elmusrati, "Analysis of Cyber-Attacks on IEC 61850 Networks," in *Proc. IEEE 11th Int'l Conf. on Application of Information and Communication Technologies*, Sept 2017.
- [38] Threat Research: Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure, FIREEYE, June 2019.
- [39] J. Weiss, "Control system cyberattacks have become more stealthy and dangerous – and less detectable," April 2019, <https://www.controlglobal.com/blogs/unfettered>.
- [40] J. Slowik, "Evolution of ICS Attacks and Prospects for Future Disruptive Events," 2019.
- [41] J. Slowik, "Anatomy of an Attack: Detecting and Defeating Crashoverride," VB2018, October, 2018.
- [42] CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations, DRAGOS, 13 June 2017.
- [43] SANS ICS, "ICS Defense Use Case No.6: Modular ICS Malware," E-ISAC, E-ISAC, August 2017.
- [44] A. Cherepanov, "Win32/Industroyer: a new threat for industrial control systems," ESET, June 2017.
- [45] TRISIS Malware: Analysis of Safety System Targeted Malware, DRAGOS, December 2017.
- [46] Security Report: Black Energy, ThreatSTOP, February 2016.
- [47] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier version 1.4," Symantec, February 2011.
- [48] E. Byres, A. Ginter, and J. Langill, "How Stuxnet spreads – A Study of Infection Paths in Best Practice Systems," Tofino Security, February 2011.
- [49] S. Hong and J.-M. Lee, "Direction of Security Monitoring for Substation Automation Systems," in *Proc. The 5th EECSS*, August 2019.
- [50] Network System Management: Implementations and Applications of the IEC 62351-7 Standard, EPRI, 2014.
- [51] Power systems management and associated information exchange - Data and communications security - Part 7: Network and System Management (NSM) data object models, IEC TC57 WG15, IEC 62351-7. July 2017.

Copyright © 2020 by the authors. This is an open access article distributed under the Creative Commons Attribution License ([CC BY-NC-ND 4.0](#)), which permits use, distribution and reproduction in any medium, provided that the article is properly cited, the use is non-commercial and no modifications or adaptations are made.



**Sugwon Hong** was born in Incheon, S. Korea. He received the B.S. degree in physics from Seoul National University, Seoul, Korea, in 1979, and the M.S. and Ph.D. degrees in computer science from North Carolina State University, Raleigh, USA, in 1988 and 1992, respectively.

His employment experience includes Korea Institute of Science and Technology (KIST), Software Development Center; Korea Energy Economics Institute (KEEI); SK Innovation Co., Ltd. (formerly Korea Oil Company); Electronic and Telecommunication Research Institute (ETRI). Currently he is a professor in the department of computer engineering, Myongji University, Yongin, S. Korea, where he has been since 1995. His current research interest are cyber security and smart grid.

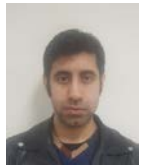
**Jae-Myeong Lee** was born in Seoul, S. Korea on September 28, 1992.



He received a Bachelor's degree in computer engineering from Myongji University, Korea, in 2018. Then he started his Master's degree program in computer engineering at Myongji University, Korea, from 2018. He is now researching about Machine Learning, Deep Learning, Computer Security, Smart Grid, and SCADA Security, under supervision of Prof. Sugwon Hong.

He was enthusiastic about computer programming from a very young age. In 2009, He was awarded Microsoft Most Valuable Professional (MVP) for Visual Basic by Microsoft, which was the youngest record in Korea.

**Mustafa Altaha** born on February 7, 1992. He completed his bachelor degree in computer communication at Al Mansour University Colleague, Iraq, in 2014. Then he starts his Master program at Myongji University, Korea, from 2015-2017 at department of information and communication engineering. He is currently in his second year of his PhD in computer engineering department at Myongji University.



He worked as network operated engineer in Earthlink-Co (biggest Internet service provider in Iraq) from 2014-2015. During his master degree program, he published on OFDM systems, and during his first year as Ph.D. he published an articles on fault tolerance in PTP systems. His current research, is about implementing intrusion detection in SCADA system by using deep learning algorithms.

MSc. Altaha was awarded the first in Iraq in cisco national net-riders competition in network skills in 2014 and, awarded the fifth in Middle East in cisco international net-riders competition in 2014.

**Muhammad Aslam** born on December 12, 1991. He completed his bachelor degree in electrical engineering at University of Engineering and Technology, Peshawar, Pakistan, in 2013. He completed his Master program at Myongji University, Korea, from 2015-2017 at department of electrical engineering. He is currently in his 3<sup>rd</sup> year of PhD in electrical engineering department at Myongji University.



During his Masters, he worked with Next-Generation Power Technology (NPTC) research center in Myongji University, where he worked on power system protection, power system load flow calculation and Artificial Intelligence (AI). Currently, he is working to apply AI into power system and network security.