IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received March 19, 2020, accepted April 19, 2020, date of publication April 23, 2020, date of current version May 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989770

IEEE 1815.1-Based Power System Security With Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical System

SUNGMOON KWON[1], (Graduate Student Member, IEEE), HYUNGUK YOO[2], (Member, IEEE), AND TAESHIK SHON[1,3], (Senior Member, IEEE)

[1]Department of Computer Engineering, Ajou University, Suwon 16499, South Korea
[2]Department of Computer Science, University of New Orleans, New Orleans, LA 70148, USA
[3]Department of Cyber Security, Ajou University, Suwon 16499, South Korea

Corresponding author: Taeshik Shon (tsshon@ajou.ac.kr)

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and Future Planning under Grant NRF-2018R1D1A1B07043349.

ABSTRACT The introduction of the cyber-physical system (CPS) into power systems has created a variety of communication requirements and functions that existing legacy systems do not support. To this end, the IEEE 1815.1 standard defines the mapping between existing distributed network protocol networks and IEC 61850 networks that reflect new requirements. However, advanced CPS cyberattacks have been reported, and in order to address cyberattacks, security research on new power systems that use network devices and heterogeneous communication is necessary. In this study, we propose an intrusion detection system for an IEEE 1815.1-based power system using CPS. We 1) analyze an IEEE 1815.1-based power system network and propose a suitable application method for an intrusion detection system, 2) suggest a bidirectional recurrent neural network-based anomaly detection system for an IEEE 1815.1-based network, and 3) demonstrate the verification of the proposed technique using various power system-specific attack data, including real power system using CPS network traffic, CPS malware behavior (CMB), false data injection (FDI), and disabling reassembly (DR) attacks. Proposed technique successfully detected five types of CMB attacks, three types of FDI and DR attacks.

INDEX TERMS Anomaly detection, cyberattack, cyber-physical system (CPS), network security, smart grid communications, supervisory control and data acquisition (SCADA).

I. INTRODUCTION

The Distributed network protocol (DNP3) [1] is the de facto communication protocol used at the distribution and transmission level and it is widely used in the North American and Asian power systems. With the introduction of the cyber-physical system (CPS), various power systems are connected, resulting in communication functions and requirements that the existing DNP3 systems cannot support. However, the "IEC 61850-Communication networks and systems for power utility automation [2]" standard is the standard for communication networks and systems in substations. Since 2007, IEC 61850 has expanded to communications networks and systems for power utility automation and includes a variety of interconnected systems related to power systems, including hydropower systems and wind power systems. In particular, IEC 61850 defines a systematic data structure and communication functions, considering the interoperability and requirements of various interconnected systems for power systems using CPS. Therefore, for the power system using CPS, the existing DNP3 system adopts the IEC 61850 system; the standard for mapping DNP3 and IEC 61850 for this is IEEE 1815.1 [3].

Fig. 1 shows the supervisory control and data acquisition (SCADA) system of CPS. The intelligent electronic device (IED) is connected to wireless/wired sensors, actuators and physical devices to perform monitoring, metering, protection, and control. The human machine interface (HMI) connected to the IED allows an operator to check the system status and interact with it. The remote terminal unit (RTU)

The associate editor coordinating the review of this manuscript and approving it for publication was Hong-Ning Dai.

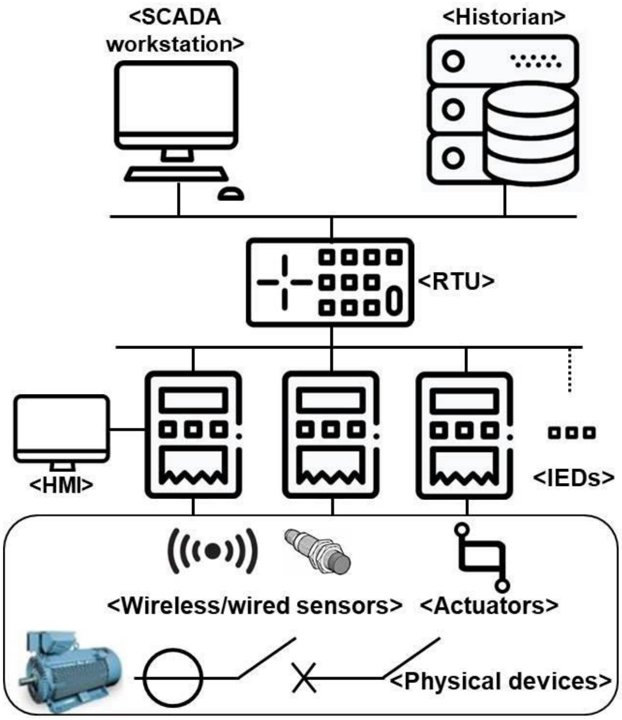


FIGURE 1. SCADA system of CPS.

collects the field digital and analog signals monitored by the IEDs, transmits them to the SCADA workstation, interprets the control commands of the SCADA workstation, and transmits the control commands to the corresponding IED. Historian stores sensor data and performs logging. Fig. 2 shows the IEEE 1815.1 use cases. IEEE 1815.1 use case (a) is when the IEC 61850 IED is connected to a DNP3 master. An example of using IEEE 1815.1 use case (a) is when an IEC 61850 substation is connected to a network control center using DNP3 communication. IEEE 1815.1 use case (b) is when the DNP3 IED is connected to an IEC 61850 Client. An example of using IEEE 1815.1 use case (b) is when an IEC 61850 substation should be connected to DNP3 legacy IEDs. Thus, power systems are more connected with network and complicated due to the use of CPS and heterogeneous communication.

Cyberattacks targeting CPS are becoming more advanced. BlackEnergy3 (2015) and Crashoverride (2016), which caused blackouts in Ukraine, and TRITON (2017), a highly advanced malware that installs backdoors in a safety instrumented system (SIS), have been recently reported. In addition, in June 2019, the Xenotime hacking group, behind TRITON, was believed to be acquiring data from the power industry in the US and Asia-Pacific, creating a crisis in cyber security in the power system. In particular, Crashoverride and TRITON have the function of attacking the control system by generating a packet complying with the CPS communication protocol. Therefore, security based on network traffic behavior is required rather than a simple whitelist-based security. However, the application of IEEE 1815.1 is being considered when opening a new substation in a network control center using the existing DNP3 communication. But the current research on IEEE 1815.1-based network security is limited to the work of Yoo *et al.* [4], a security analysis study for heterogeneous networks, and no cyber security system has been proposed. Therefore, this study proposes an intrusion detection system in environment IEEE 1815.1-based system to address cyber threats targeting CPS. To this end, we 1) analyze the IEEE 1815.1-based network and propose a suitable application method of an intrusion detection system, 2) propose a bidirectional recurrent neural network (BRNN)-based anomaly detection system and a method for improving false detection for IEEE 1815.1-based network. The proposed method is validated through actual power system using CPS network traffic and various CPS-specific attack data including CPS malware behavior (CMB), false data injection (FDI) [5], and disabling reassembly (DR) [6] attacks. The main contributions of this study are as follows.

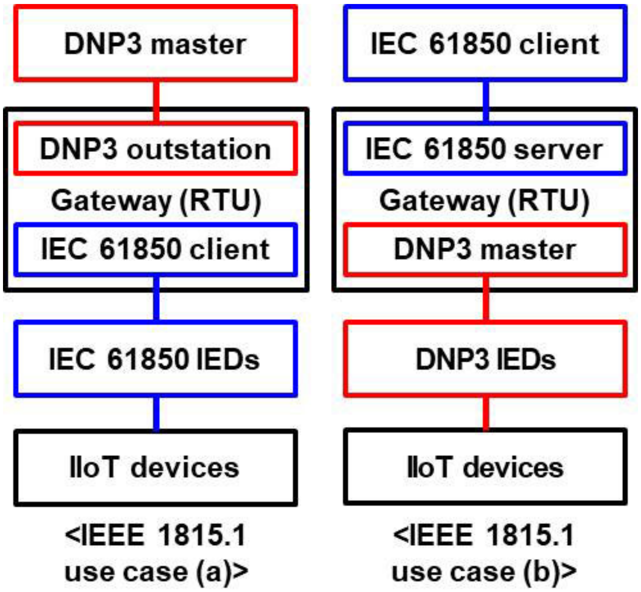


FIGURE 2. IEEE 1815.1 use cases.

1) The IEEE 1815.1-based power system was analyzed and an application method of the network security solution such as intrusion detection system was proposed.

2) Bidirectional RNN based anomaly detection system is proposed considering the network characteristics of power system using CPS in the heterogeneous system with DNP3 and IEC 61850.

3) Test methods for abnormal behavior were presented through various CPS-specific attack data including power system using CPS network traffic, CMB, FDI, and DR attacks.

This paper is organized as follows. In Section II, related research is described. In Section III, the application scope of the proposed technique and the target protocol are presented. Section IV describes the proposed technique and Section V describes the normal and attack data sets used to verify the proposed technique. Section VI describes the verification of the proposed technique and discussion about the proposed technique. Finally, we provide conclusions in Section VII.

II. RELATED WORKS

The CPS intrusion detection system can be divided into anomaly detection based on a network packet header or network traffic flow and that based on a network packet payload or measurement value. Yun *et al.* [7] proposed a method of whitelisting traffic patterns based on the main header information of the packet by each command. The proposed technique can identify the abnormality of the use of a disused abnormal command and network transmission of a single command. However, this technique does not detect the abuse or absence of existing used commands. Zolanvari *et al.* [8] detected abnormal behavior through various features of network traffic flow and machine learning algorithms. Because statistical information is regarding network traffic flow of the existing transmission control protocol (TCP) port, it has a disadvantage in that an advanced attack executed through the existing port is difficult to detect. As an anomaly detection study based on the network packet payload and measurement values, Agrawal *et al.* [9] proposed a support vector machine (SVM) model to discriminate abnormal behavior using the variation in the measurement data as a feature. Wu *et al.* [10] proposed a neural network model for discriminating abnormal behavior using the measurement data as a feature. These studies are typical black-box-level machine learning-based techniques. In this case, it is difficult to analyze the detection result and improve the false detection. Goh *et al.* [11] proposed a model to learn a recurrent neural network (RNN) using the measurement data as a feature and analyze the results through cumulative sum (CUSUM). Goh *et al.* did not determine normal or abnormal characteristics through the RNN but generated the next measurement data that is predicted and abnormal behavior was determined through CUSUM, a technique for analyzing continuous data. Therefore, it has the advantage that it is easy to analyze the learning results. Lin *et al.* [12] proposed a model to learn normal behavior through timed automata (TA) and Bayesian networks after simplifying changes in measurement data to quick/slow and up/down. Compared to the existing SVM and the cyclic neural network, it shows a faster processing speed but has a disadvantage of low accuracy in learning normal behavior. Feng *et al.* [13] proposed a normal behavior learning technique for changes in measurement data and control events and showed a high normal behavior learning rate. However, it has a disadvantage that in expressing the change in measurement data, it is difficult to intuitively interpret the detection result because it maps each change in the measurement data to one of several Gaussian mixture models (GMMs) generated based on the expectation-maximization (EM) algorithm.

Existing studies have investigated network anomaly detection using network packet header and traffic flow features and payload anomaly detection using network packet payload and measurement values. Network anomaly detection does not detect advanced attacks using manipulation of payloads. However, payload anomaly detection does not detect various attacks that prevent data acquisition through a network such as denial of service (DoS). In our prior work [14], we proposed an anomaly detection model that learned header-based whitelist and payload through one-class support vector machine (OCSVM) and verified it using testbed data. However, the model did not detect advanced attacks such as FDI and DR and it is difficult to improve because it generates anomaly detection results through OCSVM.

Research regarding the security of an IEEE 1815.1-based network is limited to the work of Yoo *et al.* [4], which is a security analysis study for heterogeneous networks, and no cyber security system has been proposed. Therefore, this study analyzes the network of a heterogeneous system with DNP3 and IEC 61850 and proposes a suitable application method of an intrusion detection system. In addition, to utilize the advantages of related research and compensate for the disadvantages, we include both header and payload in the feature use. In addition, we selected RNN as anomaly detection algorithm. The RNN can predict patterns over a set of network input data and also using RNN as a data generation model, rather than for abnormal behavior discrimination, RNN results can be interpreted intuitively. Model verification is performed through actual IEEE 1815.1-based power system data using CPS and advanced CPS-specific attack data such as CMB, FDI, and DR attacks.

III. APPLICATION SCOPE AND PROTOCOL OF THE PROPOSED TECHNIQUE

“NISTIR 8219 – Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection” [15] describes the definition and function of anomaly detection in industrial control systems. There are three types of anomaly detection systems described in NISTIR 8219: network-based, agent-based, and historian- and sensor-based systems. A network-based system aggregates the overall network traffic and performs anomaly detection. An agent base installed in specific systems performs abnormal behavior detection based on collected information. A historian- and sensor-based system performs abnormal behavior detection through sensor data stored in the historian. The technique proposed in this study aims to detect network attacks such as Crashoverride and TRITON using CPS protocols. Therefore, based on the classifier of the recent national institute of standards and technology (NIST) work, it belongs to the category of a network-based system and performs abnormal behavior detection for the entire network traffic of the power system. Network traffic may be collected by performing mirroring on the network switch, such as NISTIR 8219, or by performing mirroring on an RTU that communicates with both SCADA and IEDs. However, commercial products are already available for a variety of general information technology (IT) network traffic except the protocol of the power system.

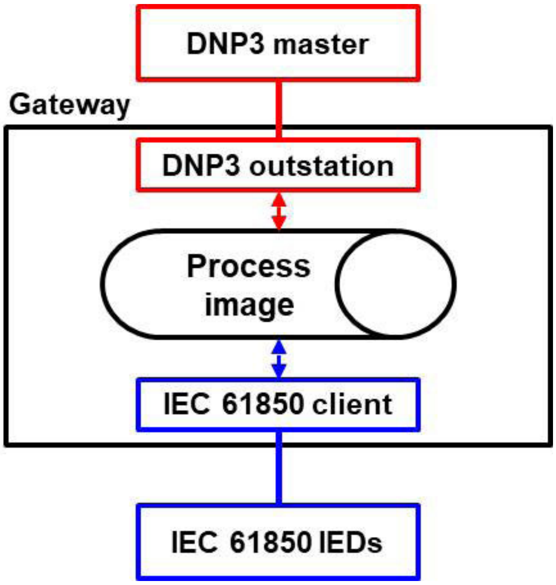


FIGURE 3. IEEE 1815.1 use cases (a) communication flow.

Therefore, the proposed technique only covers the network traffic of the power system using CPS such as DNP3 and IEC 61850.

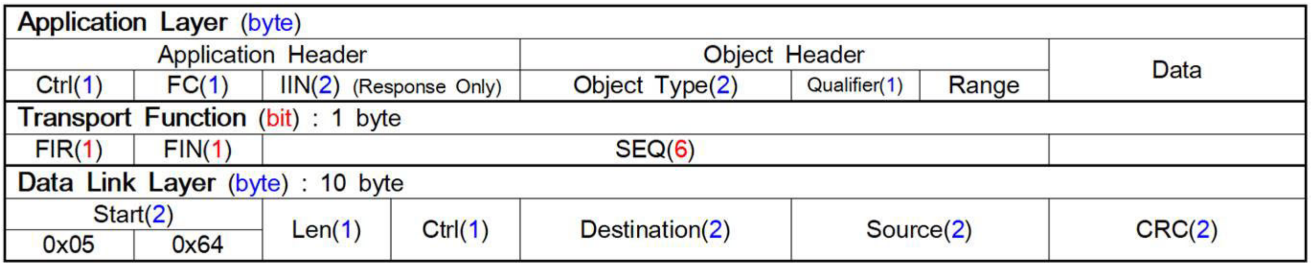
The proposed technique is applicable to both IEEE 1815.1 use case (a) and (b). However, use case (b) is a case where DNP3 legacy IEDs are connected to an IEC 61850 substation, and its practical applications are limited. However, use case (a) is a dominant case in which a new IEC 61850-based digital substation is connected to a control center of an existing power grid and some actual application cases exist. The IEEE 1815.1-based power system data used in this paper are also data collected in the field of use case (a); thus, the subsequent description is with regard to IEEE 1815.1 use case (a). Fig. 3 shows the communication flow of the IEEE 1815.1 use case (a). A key feature of the IEEE 1815.1-based networks is the use of process images. The process image, which is a database that stores the current data values of all IEDs, is updated through communication between the gateway and the IEDs. When acquiring data from SCADA, a command is not directly sent to an IED and necessary data are acquired from the process image of the gateway. There are as many as dozens of IEDs, depending on the site, and there may be delays in directly communicating with the IEDs in real time. Therefore, using the process image has the advantage of not having to perform real-time pass through with a large number of IEDs. However, in the case of a control command message, protocol conversion is performed through the gateway and directly transmitted to the relevant IED. Because of these characteristics, the SCADA and IED communication sections have different communication characteristics with the gateway as the boundary; messages in the gateway-IED section are not detected in the SCADA-gateway section. Therefore, to collect all network traffic in an IEEE 1815.1-based network, network traffic collection for two sections, the SCADA-gateway and gateway-IED, is required. In this environment in which substations are transformed into IEC 61850-based automated substations through the application of the IEEE 1815.1 standard structure, the proposed technique of this study is applied and verified for the DNP3 communication section which is known for cyber-security threats as described in [16] and can be attacked using Internet communication protocols such as TCP/internet protocol (IP).

The DNP3 protocol is one of the data transmission protocols widely used in SCADA systems for power and water in North America and Asia and is defined in IEEE 1815-2012 [1]. DNP3 is more reliable than IEC 60870-5 [17], a data transmission protocol of the SCADA system which is mainly used in Europe, because a fragmented message can be transmitted according to message length. The data acquisition side is defined as the DNP3 master and the data transmission side as the DNP3 outstation. There are two types of communication: request response and unsolicited response. The request response type is that in which an outstation responds after the master sends a request. The unsolicited response type allows the outstation to send a message without the master's request to more quickly report important events. The transmitted data do not include detailed information such as the name of the data other than the type. Therefore, when communication is first established, the master requests the entire data of the outstation to perform synchronization. As a function of security, IEEE 1815-2012 specifies secure authentication version 5, which uses digital-signature-based authentication and encryption. However, the majority of SCADA systems using DNP3 do not use authentication and encryption functions because of the availability of legacy devices depending on its capability and the necessity of installing public key infrastructure (PKI). The DNP3 protocol operates at the application layer and internally consists of a data link layer, a transport function, and an application layer. Fig. 4 shows a field of a DNP3 message for each layer. The data link layer is a layer for station addressing and error detection and performs DNP3 communication link management. The transport function segments the message up to 249 bytes for reliable communication and manages the segment message. The transport function field consists of a 1-bit FIR, FIN, and 6-bit sequence number, indicating whether it is the first or last segment message. Even in the application layer, messages can be divided according to the performance of the application. Thus, the application header has control fields similar to transport functions. The object header contains object information required by each function code and consists of object type information such as a binary/analog signal and integer/float and address range information of the object.

IV. PROPOSED TECHNIQUE

A. ALGORITHM SELECTION

Despite the existence of advanced cyber threats targeting CPS such as Crashoverride and TRITON, few network intrusion detection systems have been applied to



Application Layer (byte)							
Application Header				Object Header			Data
Ctrl(1)	FC(1)	IIN(2) (Response Only)		Object Type(2)	Qualifier(1)	Range	
Transport Function (bit) : 1 byte							
FIR(1)	FIN(1)	SEQ(6)					
Data Link Layer (byte) : 10 byte							
Start(2)		Len(1)	Ctrl(1)	Destination(2)	Source(2)		CRC(2)
0x05	0x64						

FIGURE 4. Structure of the DNP3 protocol message.

CPS environments. As a result of analyzing the opinions of CPS managers of several smart factories and smart grids in collaboration with Korea power exchange (KPX), Korea energy technology evaluation and planning (KETEP) and Korea electric power corporation (KEPCO) when conducting the research [14], [18], the main reasons why the intrusion detection system is not actually used for CPS are the frequent false positives and the difficulty in interpreting the detection results. For example, a false positive rate of 0.1% means very high accuracy. However, at least 100,000 packets in a general-sized CPS network and millions of packets in a big-sized CPS network can be sent per day. Therefore, even if 100,000 packets are transmitted per day, a false detection rate of 0.1% means that 100 false detections occur per day. Frequent false positives can mitigate security awareness of security managers. In the case of TRITON, forensic analysis has reported that two or more intrusion detection alerts were ignored, allowing hackers to successfully install malware.

Therefore, a measure for improving the accuracy by analyzing the cause of false positives is needed. However, the difficulty in interpreting detection results hinders improvement of false positives. The algorithms of detection techniques of previous studies such as Zolanvari *et al.* [8], Agrawal *et al.* [9], Wu *et al.* [10], and Feng *et al.* [13] generate their detection results at a black box level and there is no suggestion to interpret the detection results. Therefore, it is difficult to analyze whether an abnormal behavior detected as a detection result is a false detection for normal behavior or a true detection for an abnormal behavior. This leads to difficulty in using and improving detection results. To solve this problem, there is a technique that can easily visually analyze the result value instead of at the black box level, such as a graph-based automata creation as in Lin *et al.* [12]. However, as a result of practical application, it was found that detection is performed only one time in the automata-based detection technique which is a problem. For example, when there is an automata represented by (1234)*, if a packet of a type representing 5 after 123 has been transmitted and determined to be abnormal, a ground is needed to determine whether the next abnormality determination would continue to be performed again as a 4 state after a 3 state which has been normal or as a 1 state again after a 4 state. In particular, the data used for the verification of the proposed technique have a normal network flow pattern length of greater than 100. From analysis, it has been noted that the time to return to normal network flow after abnormal behavior is inconsistent. Therefore, we selected the RNN algorithm that can determine the next abnormality by learning the pattern of the data input after the occurrence of abnormal behavior. The RNN stack is a useful model for predicting patterns over a set of input data [19]. In this study, RNN is used as a model to predict the data of the next expected packet by learning the pattern through a series of network packet data rather than directly determining abnormal behavior. The general "many to many" RNN model is not suitable because it performs an accuracy calculation by generating all the next predictive data for each input over a series of inputs. Therefore, we use a "many to one" RNN model that predicts only one next prediction data for a series of inputs. However, in our priori research [18], it was found that the unidirectional RNN model did not predict rare data. For example, suppose there are commands with a 5-s cycle and a command with a 5-min cycle. In this case, the unidirectional RNN model tends to predict only 5-s periodic commands, ignoring 5-min periodic commands for better accuracy. Therefore, this study uses a "many to one" bidirectional RNN structure. However as shown in Fig. 5, traditional "many to one" bidirectional RNN uses N series input as forward layer and (N+1)th to (N+m)th input as backward layer to predict the (N+1)th input. Because backward layer already has (N+1)th input, the backward layer's weight became so high and appropriate training cannot be done. Therefore we propose new type of many to one bidirectional RNN as shown in Fig. 6. This structure receives N traffic patterns as input and generates (N+1)th prediction data and further receives M data from (N+2)th data to correct (N+1)th prediction data. As M data are additionally used for correction delay abnormal behavior determination, a model with a smaller M is advantageous for real-time detection.

B. BRNN-BASED ANOMALY DETECTION SYSTEM

The BRNN-based anomaly detection system is shown in Fig. 7. It is largely divided into training, and test phases. The training phase is the step of creating a BRNN model that generates the next prediction value by learning with the training data and threshold. The test phase is the step of

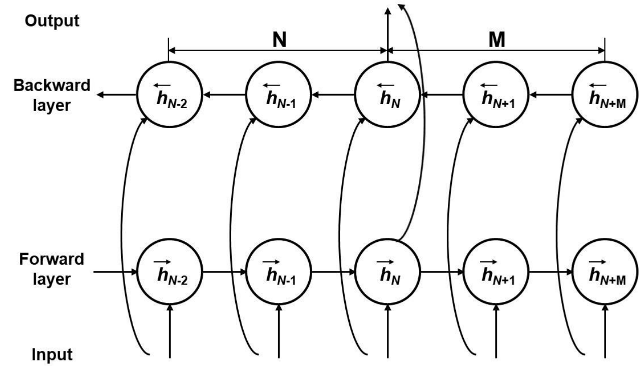

Output
Backward layer
Forward layer
Input
N
M
$\overleftarrow{h}_{N-2}$
$\overleftarrow{h}_{N-1}$
$\overleftarrow{h}_{N}$
$\overleftarrow{h}_{N+1}$
$\overleftarrow{h}_{N+M}$
$\overrightarrow{h}_{N-2}$
$\overrightarrow{h}_{N-1}$
$\overrightarrow{h}_{N}$
$\overrightarrow{h}_{N+1}$
$\overrightarrow{h}_{N+M}$

FIGURE 5. **Traditional many to one bidirectional RNN.**

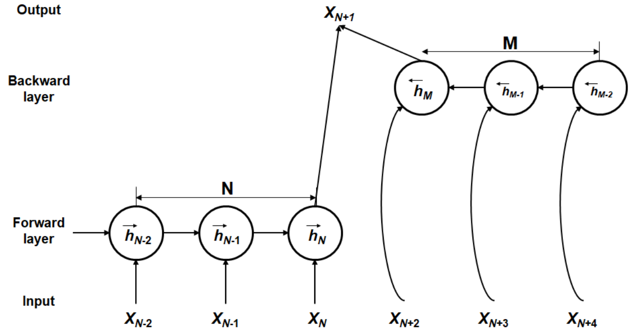


FIGURE 6. **Proposed many to one bidirectional RNN.**

generating a predicted value of the BRNN model through test data including normal and attack data and providing a detection result by comparing the predicted value to a threshold. Even within each step, learning and detection are performed by separating the header and payload of the packet. Anomaly detection for the header of a packet aims to ensure normal data acquisition through the network by learning the pattern of the communication flow of the network and determining anomalies on the network. The detection of abnormal behavior of the payload portion of the packet ensures the validity of power system data by determining abnormal behavior in payload data acquired through the network.

1) TRAINING PHASE OF THE BRNN-based ANOMALY DETECTION SYSTEM

a: HEADER TRAINING PHASE

Training phase of BRNN-based anomaly detection system is shown Fig. 8. The BRNN model is trained by extracting the header part from the packet and using the extracted header as a series of inputs. The function code for determining the type of a command and FIN, FIR and SEQ for packet reassembly and detecting packet duplication and loss were selected as the main features of the header. In the case of SEQ, we didn't use integer value of SEQ, but it is generally represented by 1 using a changed value from the previous packet. The red-colored part of Fig. 9 shows the header feature. The application layer fragmentation fields were excluded from the feature because fragmentation was not used in our data. Because the number of header types is finite, 1-hot vectors are constructed for each finite header type without generating prediction values as real values for each field. Therefore, a higher accuracy BRNN model can be expected without considering the types of headers that cannot be generated. In addition, the header information corresponding to a 1-hot vector can be used as a whitelist. In general, even normal network communication includes abnormal communication flow because of network instability. Therefore, the anomaly frequency detected through normal training data learning is used to set the threshold during the test phase.

b: PAYLOAD TRAINING PHASE

Training a BRNN model with an entire set of payloads as input is less than optimal in terms of learning time and accuracy. To improve the learning time, it is possible to shorten it by removing unnecessary fields in advance, such as a value that is always constant. To improve accuracy, it is advantageous to extract the fields related to pattern learning. Ideally, fields that are not related to pattern learning, such as fields with random values, are expected to have their weights related to the corresponding fields all set to zero during the training process. Otherwise, fields that are not related to pattern training will act as variables that reduce accuracy in loss calculation during the training phase. Therefore, via constructing a separate BRNN by removing unrelated fields and tying related fields, a BRNN model of higher accuracy can be constructed. Payload training phase consists of preprocessing, association rule mining, rule revision and BRNN model training steps.

Preprocessing: During the preprocessing step, the field always used as a constant value is removed and the change in the variable field value is expressed as increased, decreased, or unchanged. Removing constant value fields shortens the BRNN model training and association rule mining time. In addition, the main reason for removing constant value fields is that in BRNN model training, the data is meaningless, and for association rule mining, a set of constant value fields is always generated as the highest frequency of association rules. Changing field values to increased, decreased, and unchanged is because association rule mining is not optimized for numeric values such as integer and float.

Association rule: During the association rule mining step, we used the Apriori algorithm to find patterns in which the increase and decrease in each value always matches and generate the association rule. Algorithm I shows pseudo code of Apriori algorithm. Let $\mathcal{P} = \{\boldsymbol{\mathscr{P}}_1, \boldsymbol{\mathscr{P}}_2, \cdots, \boldsymbol{\mathscr{P}}_k\}$ be a set of k payload data and $\boldsymbol{\mathscr{P}} = \{\boldsymbol{\mathscr{f}}_1, \boldsymbol{\mathscr{f}}_2, \cdots, \boldsymbol{\mathscr{f}}_l\}$ be a set of l fields in the payload in which each field $\boldsymbol{\mathscr{f}}\ in\ \left[\text{increased, decreased, unchanged}\right]$. Metrics used in the Apriori algorithm include support, trust, lift, and conviction. Among them, we used confidence, which means the accuracy of the rule, and under the assumption that the data change in

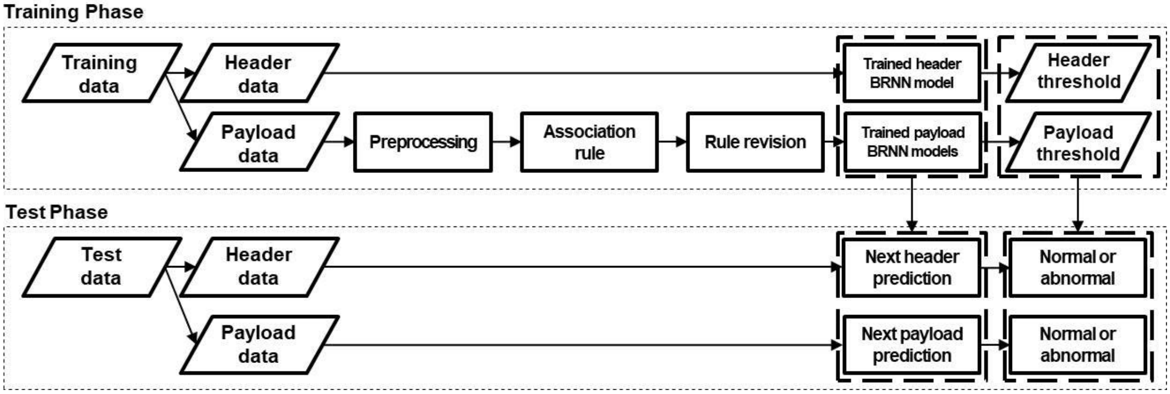


FIGURE 7. BRNN-based anomaly detection system.

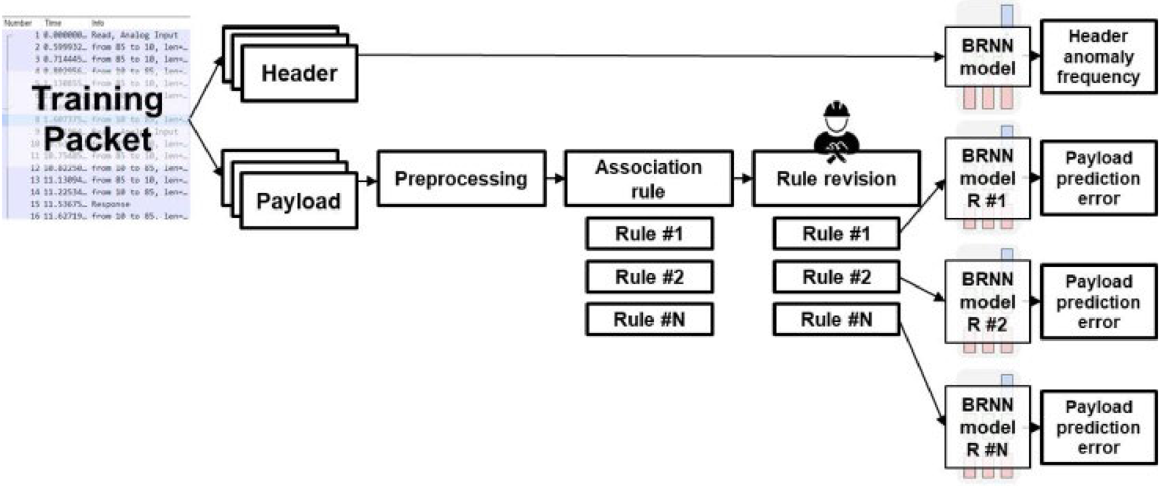
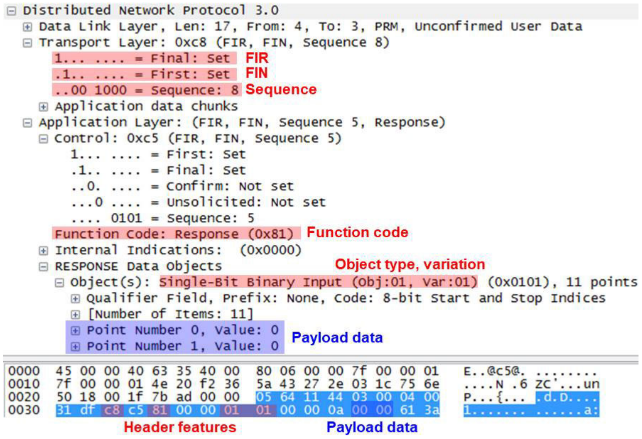


FIGURE 8. Training phase of the BRNN-based anomaly detection system.



```
⊟ Distributed Network Protocol 3.0
  ⊞ Data Link Layer, Len: 17, From: 4, To: 3, PRM, Unconfirmed User Data
  ⊟ Transport Layer: 0xc8 (FIR, FIN, Sequence 8)
      1... .... = Final: Set
      .1.. .... = First: Set
      ..00 1000 = Sequence: 8
    ⊞ Application data chunks
  ⊟ Application Layer: (FIR, FIN, Sequence 5, Response)
    ⊟ Control: 0xc5 (FIR, FIN, Sequence 5)
        1... .... = First: Set
        .1.. .... = Final: Set
        ..0. .... = Confirm: Not set
        ...0 .... = Unsolicited: Not set
        .... 0101 = Sequence: 5
      Function Code: Response (0x81)
    ⊞ Internal Indications:  (0x0000)
    ⊟ RESPONSE Data Objects
      ⊟ Object(s): Single-Bit Binary Input (Obj:01, Var:01) (0x0101), 11 points
        ⊞ Qualifier Field, Prefix: None, Code: 8-bit Start and Stop Indices
        ⊞ [Number of Items: 11]
        ⊞ Point Number 0, Value: 0
        ⊞ Point Number 1, Value: 0

0000  45 00 00 40 63 35 40 00  80 06 00 00 7f 00 00 01   E..@c5@. ........
0010  7f 00 00 01 4e 20 f2 36  5a 43 27 2e 03 1c 75 6e   ....N .6 ZC'...un
0020  50 18 00 1f 7b ad 00 00  05 64 11 44 03 00 04 00   P...{... .d.D....
0030  31 df c8 c5 81 00 00 01  01 00 00 0a 00 00 61 3a   1....... ......a:
```

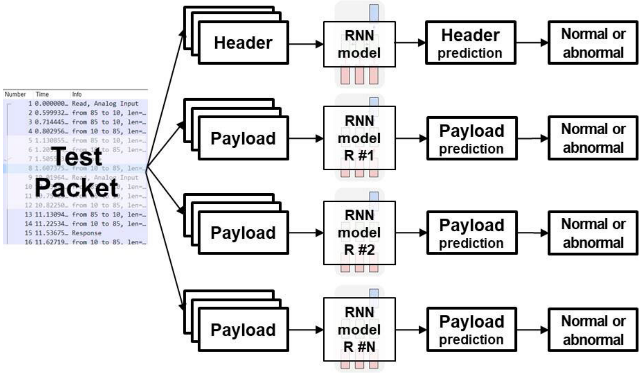
FIGURE 9. DNP3 example packet and header/payload features.

the CPS is made under certain conditions, min_conf is set to 1. Example of association rule is field A increases when field B increases for proportional relations field A and B.

Rule Revision: The generated association rule goes through a rule revision step. During the rule revision step, the field engineer analyzes the generated rule to 1) remove the nonsensical rules, 2) supplement the generated rule by adding a field among the fields used as constant values if it is associated with the generated rule, and 3) add a rule that consists only of constant values. The rule revision step has the advantage of not only including the characteristic of the field

Algorithm 1 Apriori Algorithm

```
INPUT :$\mathcal{P}$, $conf$ WHERE $\mathcal{P} = payloadset$, $min\_conf = 1$
OUTPUT : S$etofFields$
procedure GetConfidentFields
  $freqFields[] \leftarrow null$
  for all $payload$ $\mathscr{P}$ in $\mathcal{P}$ do
    for all $Fields$ $\mathscr{f}$ in $\mathscr{P}$ do
      if $conf \geq min\_conf$ then
        $freqFields[] \leftarrow \mathscr{f}$
      end if
    end for
  end for
end procedure
```



```
Number  Time        Info
     1 0.000000… Read, Analog Input
     2 0.599932… from 85 to 10, len=…
     3 0.714445… from 85 to 10, len=…
     4 0.802956… from 10 to 85, len=…
     5 1.130855… from 85 to 10, len=…
     6 1.20[illegible] from 10 to 85, len=…
     7 1.5855[illegible]
     8 1.607375… from 10 to 85, len=…
     9 10.01964… Read, Analog Input
    10 [illegible], len=…
    11 10.75[illegible], len=…
    12 10.82250… from 10 to 85, len=…
    13 11.13094… from 85 to 10, len=…
    14 11.22534… from 10 to 85, len=…
    15 11.53675… Response
    16 11.62719… from 10 to 85, len=…
```

FIGURE 10. Test phase of the BRNN-based anomaly detection system.

TABLE 1. IEEE 1815.1 based power system network traffic characteristic.

Data Object (Code)	Request Function (Code)	Response Function (Code)
Binary Input (1)	Read (1)	Response (129)/ Unsolicited Response (130)
Binary Output (10)	Read (1)	Response (129)/ Unsolicited Response (130)
Analog Input (30)	Read (1)	Response (129)/ Unsolicited Response (130)
Time and Date (50)	Write (2)	Response (129)
Internal Indications (80)	Read (1)	Response (129)

that is not included in the test data or missed by the algorithm but also including the monitoring rule for safety in use.

BRNN Models Training: BRNN models are created by training the real values for each rule as input rather than a series of incremental and decrement values for each field. The number of BRNN models is same as number of field set of association rules. However, if all data are not included through association rule mining, additional BRNN can be configured using the remaining fields after eliminating unnecessary fields at the discretion of the engineer. The maximum error rates of each field after training each BRNN model are used to set the thresholds during the test phase.

2) TEST PHASE OF BRNN-BASED ANOMALY DETECTION SYSTEM

a: HEADER TEST PHASE

Fig. 10 shows test phase of the BRNN-based anomaly detection system. A predictive header value is generated from a series of header information and compared to the actual header value. Because the header information is expressed as a 1-hot vector, the result of the comparison is divided into right and wrong. Abnormal data flow, such as packet loss, occurs even in a normal operating control system. Therefore, alarming with only one wrong prediction can be a cause of frequent false positives. To solve this problem, we set the Z score suitable for use as the threshold through the anomaly frequency calculated during the training phase. If the current anomaly frequency per unit time exceeds the threshold, it is determined as an anomaly. If an input value that cannot be represented as a 1-hot vector occurs, it is considered as an anomaly because it is regarded as abnormal behavior resulting from an inappropriate command or packet type use.

b: PAYLOAD TEST PHASE

BRNN learned by each association rule uses different input fields and requires different input lengths. Therefore, the predictive payload value is generated by inputting the appropriate series of payload information for each BRNN and comparing it to the actual payload value. Unlike the header information, because it is not a 1-hot vector, the actual output payload generally has a real value. The initial threshold is set as the maximum prediction error rate of the payload calculated during the training phase. When the threshold is exceeded by comparing the error between the predicted and actual values, it is determined as anomalous.

V. DATASET

A. IEEE 1815.1-BASED POWER SYSTEM DATA USING CPS

A total of three days of network packets were collected from an operating IEEE 1815.1-based Korean substation. The SCADA gateway has approximately 320,000 DNP3 packets. The collected packet was confirmed by the engineer as normal data without a cyberattack and abnormal behavior.

However, it was found that 2% abnormal network traffic was included because of network burst and session reestablishment. The DNP3 master equipment acquires five types of data as shown in Table 1 according to the power market operation rule [20] and the observed normal network traffic pattern length is 137.

Because the actual payload data are private information, the entire contents cannot be publicly shared. Therefore, with the aid of engineers, four IEDs and 127 data were selected to express substations out of dozens of IEDs. DNP3 has no data naming rules. Therefore, IEEE 1815.1 maps the data points of DNP3 according to the data and naming rules standardized in IEC 61850. The data name of IEC 61850 largely consists of LDName, LNName, DataObjectName, and DataAttributeName, as shown in Fig. 11. LDName is a logical device (LD) name that is the name of a corresponding device and it is application specific. LNName is a logical node (LN) name that consists of an application-specific prefix, a class name of four alpha characters as defined in IEC 61850-7-4 [21], and an instance ID that is a number for distinguishing the same class name. DataObjectName is a data object belonging to each LN class and is also defined in IEC 61850-7-4. Each DataObjectName belongs to the common data class (CDC) defined in IEC 61850-7-3 [22] and each DataAttributeName and attributes type are defined in the CDC. The example in Fig. 11 shows the ctlVal attribute of Pos which means switch position in XCBR which is a circuit

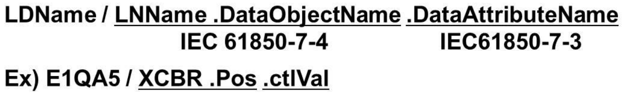

LDName / LNName .DataObjectName .DataAttributeName
IEC 61850-7-4
IEC61850-7-3
Ex) E1QA5 / XCBR .Pos .ctlVal

FIGURE 11. IEC 61850 naming architecture.

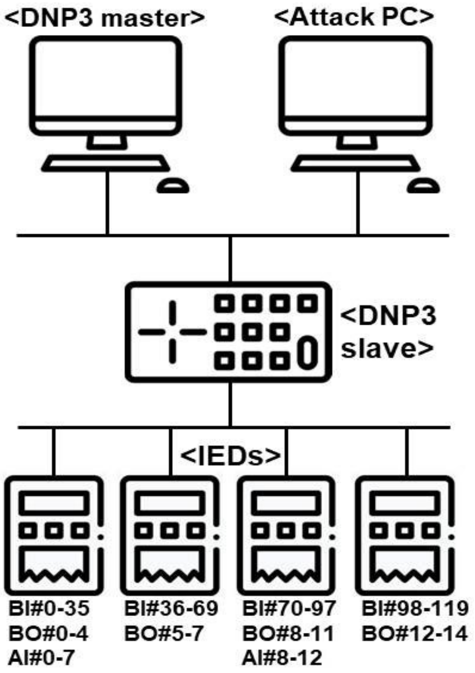


FIGURE 12. Simulation testbed.

breaker of E1QA5 LD. CtlVal is a BOOLEAN value with on and off. The selected 127 data with 4 IEDs were organized into data names mapped in IEC 61850 according to the standard of IEEE 1815.1, as shown in the Appendix. The IEDs of Fig. 12 shows data point composition of each IED. However, application-specific information, which is private, was removed or replaced with meaningless information when it was necessary to distinguish between data. A total of 50% of the collected data was used for training and the remaining 50% for testing.

B. ATTACK DATASET

Attacks cannot be performed against an actually operating substation. Therefore, using a commercial product of Triangle Microworks' distributed test manager (DTM) [23], a DNP3 network with four IEDs was constructed to configure the same experimental environment as a substation as shown Fig. 12. When an attack packet itself could be generated in the DTM, it was generated through the DNP3 master of the DTM. Otherwise, the packet was directly generated using Ostinato [24], which is an open source traffic generator in Attack PC. To construct the attack dataset, the packet was generated by a CMB attack, an FDI attack, and a DR attack and it included in the test packet. A description of each type of attack is as follows.

TABLE 2. CMB attack.

CMB type	Function type	Function code
Reconnaissance	Integrity data polling	0x01
DoS #1	Operate	0x04
DoS #2	Cold restart	0x0D
DoS #3	Warm restart	0x0E
File transfer	OPEN_FILE	0x19

1) CMB ATTACK

The main types of attacks of Crashoverride [25] and TRITON [26] are reconnaissance and DoS attacks and file transfer commands. Table 2 shows 3 type of CMB attack. The reconnaissance attack is an attack for collecting network information. In the case of DNP3, the integrity data polling command that requests the entire data of the device belongs to this attack. When the session is re-established, integrity data polling commands may be transmitted depending on the DNP3 device configuration. In this case, the integrity data polling, which is unrelated to the session re-establishment, should be detected as abnormal. A DoS attack refers to device operation through abnormal control commands, such as operate and cold/warm restart of DNP3. The file transfer command is an attack for transferring malicious firmware and files and file writing is initiated through the OPEN_FILE command of DNP3. Because all commands were standard DNP3 commands supported by DTM, DTM sent commands of the IBM attack type through the DNP3 master and a total of five commands were sent 10 times.

2) FDI ATTACK

An FDI attack [5] is an attack that is not easily detected by generating false data that maintains the linear characteristics during data manipulation after identifying the linear characteristics in the data. An FDI attack was performed by selecting data with linear characteristics for the fields included in each association rule. Fig. 13 shows a graph of an FDI attack performed against active and apparent power in a proportional relationship with each other. The red line represents the point in time of the attack. FDI (a) is the case in which one data has been changed to an abnormal value. The abnormal value is the original value plus 10% to 100% of the original value. FDI (b) is the case in which the data has been changed in the decreasing direction, and in the case of FDI (c), the original value has been changed to 1.5 times. Because an FDI attack is an attack performed on data values, FDI attack data is directly injected into existing payload data without network packet transmission. Ten types of FDI attacks were performed 10 times on 10 analog input data included in the association rule.

3) DR ATTACK

A DR attack is an attack that interrupts reassembly by transmitting a packet having an abnormal reassembly header

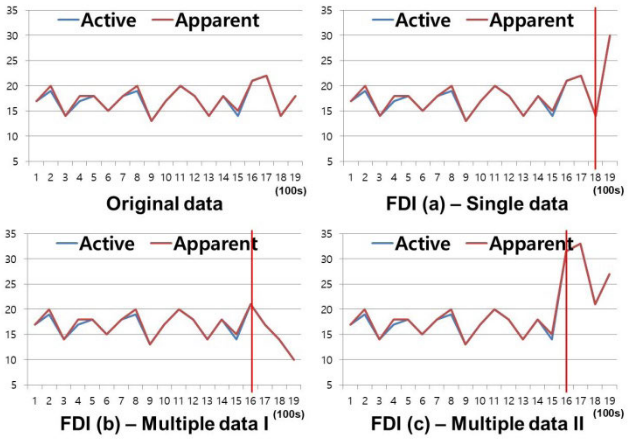


FIGURE 13. Example of FDI attack.

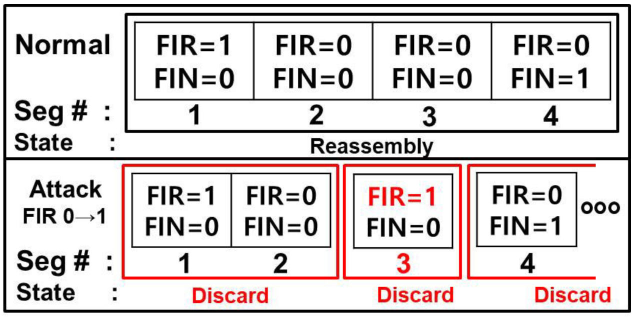


FIGURE 14. Example of DR attack.

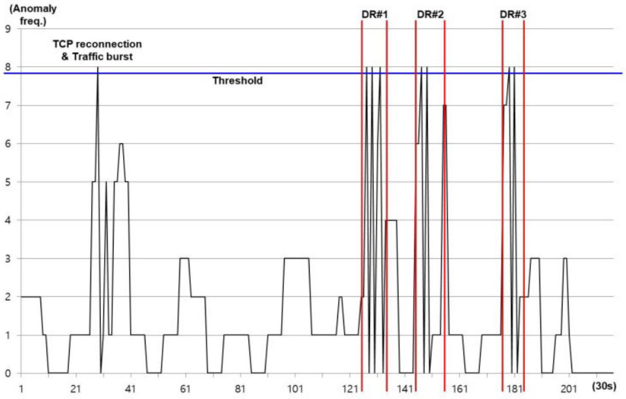


FIGURE 15. Header-based anomaly detection result – DR attack.

TABLE 3. Development environment and training model parameters.

Parameters	Header model	Payload models
Number of the models	1	5
RNN cell type	GRU	GRU
RNN stack	3	3
Input Length N	45	10–15
Input Length M	2	2–3
Epoch	300	200–300
Training time	1 h	5–15 min

between normal packets when the DNP3 message is fragmented because of its long length. The segment message processing method of DNP3 is to drop all segment messages that were previously transmitted at the moment of receiving packets of abnormal FIR, FIN, and sequence fields. Thus, continuous DR attacks can lead to DoS [16], and depending on the configuration of the DNP3 device, a single DR attack can cause tens of seconds of DoS [18]. Fig. 14 is an example of a DR attack. When data is transmitted in four segment messages, FIR means the first is set in the first segment message and no flag is set in the middle segment messages. In the fourth segment message, FIN, which means the last packet, is set. However, because of the DR attack, the segmentation field of the third packet is manipulated and changed to abnormal such that segment messages 1 and 2 are dropped and the corresponding command cannot be processed. Because such an abnormal DR attack message could not be generated through DTM, the DR attack was generated through Ostinato on the attack PC. Three types of DR attacks including FIR, FIN, and FIR + FIN were performed 10 times each and each attack made data acquisition impossible for more than 30 s.

VI. VERIFICATION OF THE PROPOSED TECHNIQUE

A. DEVELOPMENT ENVIRONMENT AND MODEL GENERATION RESULTS

The development environment is an Intel Core i7-8700 central processing unit (CPU) with 16 GB of memory, a GeForce GTX 1070 Ti, and TensorFlow library. The parameters of each learning model were optimized by repeated experiments. The RNN cell type was selected as a gated recurrent unit (GRU) [27] for faster learning. Table 3 summarizes the parameters of the generated header-based anomaly and payload-based anomaly detection models.

There was considerable trial and error in the creation of the association rule. Finally, five data point groups were created as listed in Table 4. To create an association rule, we first removed the constant value field. Binary values are not likely to change in a normal operating substation environment. In practice, the binary values also had a small number of data points that changed but selected data points were not changed. For analog input, AI #8 and AI #12 are excluded because of constant values. The constant value fields can be configured as whitelists for monitoring. Therefore, the Apriori algorithm is performed on 11 analog inputs and the min_conf is set to 1 under the assumption that data change occurs under specific conditions in the CPS. The first problem encountered is the generation of meaningless rules based on data imbalance. As a result of analyzing the created association rule, approximately 70–95% of the analog data were expressed as unchanged according to data points. The analysis result from the engineering information is a result of the power data changing in a cycle of approximately 100 s. Therefore, to focus on the data change, unchanged data is treated as

TABLE 4. Association rules.

Data Points	Rule	Confidence
AI # 0, 1, 2, 3, 5	0, 1, 2, 3, 5 increase	0.99
	0, 1, 2, 3, 5 decrease	0.97
AI # 4 + 3, 5	Manually added	-
AI # 6 + 3, 5	Manually added	-
AI # 7	None	-
AI # 9, 10, 11	9, 10, 11 increase	0.72
	9, 10, 11 decrease	0.71

TABLE 5. Header-based anomaly detection results.

Category	Result
Normal pattern learning rate	1.000
CMB – reconnaissance	10/10
CMB – DoS	30/30
CMB – File upload	10/10
DR	30/30
	FPR 0.0003
	F-measure 0.909

missing data such that it does not affect the association rule calculation. The second problem we faced was the lower confidence resulting from data errors. As a result of analysis through engineering information, the analog input value is transmitted by rounding off the measured float value to an integer. This results in data errors because of measurement and rounding down, creating certain patterns of variation that are not always consistent. Therefore, we set min_conf to a lower value of 0.7, not 1. As a result, four association rules and two data point groups were generated by the Apriori algorithm. Analyzing the data point group of the created association rule, AI #0, 1, and 2 are the A/B/C current and AI #3 and 5 are power points that are proportional to each other. Therefore, it can be seen that a reasonable association rule has been created in which all five points are increased and decreased. AI #9, 10, and 11 can also confirm that a reasonable association rule has been created with data points that are proportional to each other with A/B/C phase currents. However, AI #9, 10, and 11 have a lower confidence level of 0.7 than that of AI #0, 1, and 2 because the analysis information shows that AI #9, 10, and 11 have a small amount of change, which causes a greater error from rounding down. For AI #4, 6, 7, 8, and 12, the rules were written based on engineering information. AI #4 and 6 are cases in which the Apriori algorithm could not extract the associated field because of data error of rounding down. AI #4 is a reactive power, AI #3 is an active power, and AI #5 is an apparent power.

$$AI\#3^2 + AI\#4^2 = AI\#5^2 \tag{1}$$

$$AI\#3/AI\#5 = AI\#6 \tag{2}$$

AI# 3, 4, and 5 have an Eq. (1) relationship. Therefore, we added AI #3 and 5 to AI #4. AI #6 is a power factor that has an Eq. (2) relationship. Therefore, we added AI #3 and 5 to AI #6. AI #7 is a frequency and was independently added because there is no analog input related to frequency. AI #8 is a reclosing operation and AI #12 is a power factor of IED #3. AI #8 and 12 are constant value and there is no other analog input related to these analog inputs. Therefore, learning with AI #8 and 12 is impossible and AI #8 and 12 were excluded.

B. NORMAL DATA LEARNING RATE AND ANOMALY DETECTION RESULTS

The threshold value used in the header-based anomaly detection model is a Z score of 1.65 (95%) for the 5-min frequency of anomaly detection in the training data. The detection results are listed in Table 5. The normal behavior pattern of 137 lengths was well learned and all three types of CMB attacks were detected. All three types of attacks were detected as abnormal because they were not mapped to the 1-hot vector because they were types of instructions not found in the training dataset. However, if integrity data polling of the reconnaissance attack was a commonly used environment, it would not be possible to perfectly detect it. Fig. 15 shows the result of the DR attack detection. If the frequency of the anomaly detection exceeds a threshold, the anomaly detection system alerts and sets the frequency to 0. In the case of DR attacks, attack detection was performed well but some abnormal network traffic on normal operation CPS was classified as abnormal behavior. We analyzed and found that this was the case in which network traffic congestion occurred during the process of reestablishing the session and the TCP reconnection was not normally performed for a long time. Therefore, the proposed technique also identifies communication problems on the network of the control system under normal operation, which can be utilized in terms of network state management.

The initial threshold used in the payload-based anomaly detection model is the maximum prediction error rate of the actual value and the predicted value during the training phase. Table 6 shows the results of payload anomaly detection. The total is the result of anomaly detection when anomaly is detected on any AI prediction result. Higher thresholds do not detect precise FDI (a) attacks. In the case of FDI (b), an attack can be immediately detected according to an analog point. However, even if an attack cannot be immediately detected, all attacks are detected because of the continuous change in the value. In the case of FDI (c), it was immediately detected because of the great change in value. Because AI #6, a power factor of Rule group #3, has only values of 0 and 1, and the value does not frequently change, all values were predicted well with threshold 0 for normal data. However, the FDI attacks on AI #6 were not detected at all and the FDI attacks on rule group 3 were detected by AI #3 and 4 which were

TABLE 6. Payload-based anomaly detection results.

Rule Group Number	Data point	Threshold (%)	FDI (a)	FDI (b)	FDI (c)	Threshold 10% Normal	Threshold 15% Normal
1	AI #0	18.36	7/10	10/10	10/10	86.21	96.04
	AI #1	20.34	6/10	10/10	10/10	83.64	94.02
	AI #2	18.59	7/10	10/10	10/10	85.76	95.83
	AI #3	17.91	9/10	10/10	10/10	85.99	95.93
	AI #5	17.39	8/10	10/10	10/10	86.65	96.45
	TOTAL		9/10	10/10	10/10		
2	AI #3	17.01	8/10	10/10	10/10	88.30	97.52
	AI #4	40.31	6/10	10/10	10/10	68.79	79.07
	AI #5	16.52	9/10	10/10	10/10	89.06	98.01
	TOTAL		9/10	10/10	10/10		
3	AI #3	17.01	8/10	10/10	10/10	88.30	97.52
	AI #5	16.52	9/10	10/10	10/10	89.06	98.01
	AI #6	0.00	0/10	0/10	0/10	-	-
	TOTAL		9/10	10/10	10/10	86.62	
4	AI #7	0.02	10/10	10/10	10/10	-	-
5	AI #9	14.90	9/10	10/10	10/10	90.98	-
	AI #10	15.89	9/10	10/10	10/10	89.43	98.62
	AI #11	15.53	9/10	10/10	10/10	89.97	98.82
	TOTAL		9/10	10/10	10/10		

added through rule revision. It was found that fraction information is needed for effective learning of the power factor, AI #3. The threshold can be lowered for higher immunity to attacks such as those FDI (a). To detect a 10% level of an FDI (a) attack, the threshold also requires a level of 10%. The last column of Table 6 lists the normal behavior accuracy when the threshold is set at 10% and 15%, respectively. It is difficult to detect 10% FDI (a) attacks due to the low accuracy of normal behavior, and it was found that a 15–20% level of FDI (a) attacks can be detected.

C. DISCUSSION

We analyze the proposed technique in terms of 1) SCADA system function, 2) CPS network traffic characteristic, 3) result analysis and management and 4) CPS-specific attack detection result.

1) SCADA SYSTEM FUNCTION

Function of a SCADA system can be seen as data acquisition and control through a network. Therefore, the main requirement of an intrusion detection system is the detection of an anomaly from the network packet flow and payload. Anomaly detection from the network packet flow ensures normal data transmission through the network by detecting abnormal behavior such as missing data transmission and abnormal packets preventing reassembly of segment packets. Anomaly detection on the payload detects an FDI attack that transmits an abnormal value and abnormal behavior, ensuring the validity of the received data. The proposed technique detects abnormal behavior of network traffic flow patterns using a header-based technique to ensure normal data transmission through the network. In addition, by verifying the validity of the data transmitted through the network using the BRNN model via each associated payload field, the proposed technique was found to satisfy the functional considerations of the SCADA system.

2) CPS NETWORK TRAFFIC CHARACTERISTICS

Depending on each CPS environment, various abnormal traffic exists in the CPS network traffic itself under normal operation. Older legacy systems often contain slower communication lines. In this case, packets are easily dropped when instantly crowded. For security reasons, there are cases in which the port is changed through aperiodic session reconnection. In addition, commands such as the unsolicited response of DNP3 are aperiodic and the number of commands can be low such that they may not be considered in learning or may be determined abnormal data. It is difficult to separately process various abnormal traffics for each type according to the CPS environment. Therefore, an abnormal behavior detection technique should be able to address abnormal traffic in this normal operating environment. When an anomaly detection engine is applied to an actual CPS, its processing speed should not be slower than the CPS network packet transmission rate such that packets to be analyzed will not accumulate and normal operation will be possible. The proposed technique generates prediction data using the BRNN technique and the determination of abnormal behavior is performed using a threshold value based on the number of abnormal network traffic per unit time in the normal control system traffic. Therefore, it has partial immunity to abnormal traffic occurring in the normal control system traffic. In terms of real-time processing capability, the deep learning technique has an advantage of taking a long time for learning but a short time for determining; it will be applied to and validated in a real power system through port mirroring.

3) RESULT ANAYLSIS AND MANAGEMENT

To utilize the actual intrusion detection system, the interpretation of the detection result should be easy. For this purpose, it should be possible to distinguish whether a behavior actually analyzed as abnormal is a falsely detected normal behavior or a truly detected abnormal behavior by presenting the reason why it is deemed abnormal behavior. In addition, when a false detection occurs, there should be a tuning method for reducing the false detection and improving accuracy. The proposed technique facilitates analysis of the result of the learning engine because the predicted value of the BRNN does not indicate abnormal or normal but generates the field value of the actual packet. For the false detection management, in the CPS environment in which the network communication pattern does not mainly change, false detection of abnormal behavior detection on headers is infrequent. If the unusual commands used for rare events such as maintenance do not belong to the 1-hot vector of the trained model, it will be determined as abnormal. If this frequently occurs, it needs

TABLE 7. IED #1's Data points.

IED	IEC 61850 Name	DNP3 Data Point
IED #1	IED_1/CALH.GrAlm.stVal	BI #0
	IED_1/LLN0.Loc.stVal	BI #1
	IED_1/XCBR.Pos.stVal	BI #2,3
	IED_1/AXSWI.Pos.stVal	BI #4,5
	IED_1/BXSWI.Pos.stVal	BI #6,7
	IED_1/CXSWI.Pos.stVal	BI #8,9
	IED_1/DXSWI.Pos.stVal	BI #10,11
	IED_1/EXSWI.Pos.stVal	BI #12,13
	IED_1/FXSWI.Pos.stVal	BI #14,15
	IED_1/AGGIO.Ind1.stVal	BI #16
	IED_1/ASIMG1.PresAlm.stVal	BI #17
	IED_1/ASIMG2.PresAlm.stVal	BI #18
	IED_1/BSIMG1.PresAlm.stVal	BI #19
	IED_1/BSIMG2.PresAlm.stVal	BI #20
	IED_1/CSIMG1.PresAlm.stVal	BI #21
	IED_1/CSIMG2.PresAlm.stVal	BI #22
	IED_1/DSIMG1.PresAlm.stVal	BI #23
	IED_1/DSIMG2.PresAlm.stVal	BI #24
	IED_1/BGGIO.Ind1.stVal	BI #25
	IED_1/BGGIO.Ind2.stVal	BI #26
	IED_1/AGGIO.Ind2.stVal	BI #27
	IED_1/AGGIO.Ind3.stVal	BI #28
	IED_1/AGGIO.Ind4.stVal	BI #29
	IED_1/BGGIO.Ind3.stVal	BI #30
	IED_1/AGGIO.Ind5.stVal	BI #31
	IED_1/AGGIO.Ind6.stVal	BI #32
	IED_1/AGGIO.Ind7.stVal	BI #33
	IED_1/AGGIO.Ind8.stVal	BI #34
	IED_1/AGGIO.Ind9.stVal	BI #35
	IED_1/ACSWI.Pos.Oper.ctlVal	BO #0
	IED_1/BCSWI.Pos.Oper.ctlVal	BO #1
	IED_1/CCSWI.Pos.Oper.ctlVal	BO #2
	IED_1/DCSWI.Pos.Oper.ctlVal	BO #3
	IED_1/ECSWI.Pos.Oper.ctlVal	BO #4
	IED_1/MMXU.A.phsA.cVal.mag.f	AI #0
	IED_1/MMXU.A.phsB.cVal.mag.f	AI #1
	IED_1/MMXU.A.phsC.cVal.mag.f	AI #2
	IED_1/MMXU.TotW.mag.f	AI #3
	IED_1/MMXU.TotVAr.mag.f	AI #4
	IED_1/MMXU.TotVA.mag.f	AI #5
	IED_1/MMXU.TotPF.mag.f	AI #6
	IED_1/MMXU.Hz.mag.f	AI #7

TABLE 8. IED #2's Data points.

IED	IEC 61850 Name	DNP3 Data Point
IED #2	IED_2/CALH.GrAlm.stVal	BI #36
	IED_2/LLN0.Loc.stVal	BI #37
	IED_2/XCBR.Pos.stVal	BI #38,39
	IED_2/AXSWI.Pos.stVal	BI #40,41
	IED_2/BXSWI.Pos.stVal	BI #42,43
	IED_2/CXSWI.Pos.stVal	BI #44,45
	IED_2/DXSWI.Pos.stVal	BI #46,47
	IED_2/AGGIO.Ind1.stVal	BI #48
	IED_2/ASIMG1.PresAlm.stVal	BI #49
	IED_2/ASIMG2.PresAlm.stVal	BI #50
	IED_2/BSIMG1.PresAlm.stVal	BI #51
	IED_2/BSIMG2.PresAlm.stVal	BI #52
	IED_2/CSIMG1.PresAlm.stVal	BI #53
	IED_2/CSIMG2.PresAlm.stVal	BI #54
	IED_2/DSIMG1.PresAlm.stVal	BI #55
	IED_2/DSIMG2.PresAlm.stVal	BI #56
	IED_2/BGGIO.Ind1.stVal	BI #57
	IED_2/BGGIO.Ind2.stVal	BI #58
	IED_2/AGGIO.Ind2.stVal	BI #59
	IED_2/AGGIO.Ind3.stVal	BI #60
	IED_2/AGGIO.Ind4.stVal	BI #61
	IED_2/BIGGIO.Ind3.stVal	BI #62
	IED_2/AGGIO.Ind5.stVal	BI #63
	IED_2/APIOC.Op.general	BI #64
	IED_2/BPTOC.Op.general	BI #65
	IED_2/CPTOC.Op.general	BI #66
	IED_2/AGGIO.Ind6.stVal	BI #67
	IED_2/AGGIO.Ind7.stVal	BI #68
	IED_2/AGGIO.Ind8.stVal	BI #69
	IED_2/ACSWI.Pos.Oper.ctlVal	BO #5
	IED_2/BCSWI.Pos.Oper.ctlVal	BO #6
	IED_2/CCSWI.Pos.Oper.ctlVal	BO #7

to re-learn from the learning dataset containing the command or make an exception rule. In addition, if the communication periodicity is changed, re-learning is required because the pattern of communication flow itself has changed. If the pattern of communication flow is frequently disturbed by network instability, the threshold needs to be set higher to reduce false positives. In the case of an actual DR attack, because the attack must be continuously executed for its effectiveness, even if the threshold is set high, a DR attack can be detected. In the case of payload anomaly detection, because field values which are predicted as real values are compared, the more uncertain the change pattern, the higher the prediction error rate. In this case, the threshold will be set higher but FDI attacks that manipulate field values may not be detected. Therefore, for data points that require more sensitive countermeasures against FDI attacks, it is better to create an exception rule that eliminates false positives of the same type by analyzing false positives rather than setting the thresholds higher; however, it is necessary to verify the validity of the proposed technique by applying a real field for a long time.

4) RESULT ANAYLSIS AND MANAGEMENT

The verification of proposed technique was performed using various power system-specific attack data, including real power system using CPS network traffic, CMB, FDI, and DR. Five types of CMB attacks including reconnaissance, DoS and abnormal firmware upload were detected by header-based anomaly detection using 1-hot vector as header whitelist. Three types of FDI attacks were performed and multiple data FDI attacks were detected through payload-based BRNNs. In case of single data FDI, only attack with large changes in values exceeding 20% were detected. But a

TABLE 9. IED #3's Data points.

IED	IEC 61850 Name	DNP3 Data Point
IED #3	IED_3/LPHD.PhyHealth.stVal	BI #70
	IED_3/LLN0.Loc.stVal	BI #71
	IED_3/XCBR.Pos.stVal	BI #72,73
	IED_3/AXSWI.Pos.stVal	BI #74,75
	IED_3/BXSWI.Pos.stVal	BI #76,77
	IED_3/CXSWI.Pos.stVal	BI #78,79
	IED_3/AGGIO.SPCSO32.stVal	BI #80
	IED_3/BGGIO.Ind1.stVal	BI #81
	IED_3/ASIMG.DenAlm.stVal	BI #82
	IED_3/BSIMG.DenAlm.stVal	BI #83
	IED_3/CSIMG.DenAlm.stVal	BI #84
	IED_3/BGGIO.Ind2.stVal	BI #85
	IED_3/BGGIO.Ind3.stVal	BI #86
	IED_3/PIOC.Op.general	BI #87
	IED_3/PTOC1.Op.general	BI #88
	IED_3/PIOC2.Op.general	BI #89
	IED_3/PTOC3.Op.general	BI #90
	IED_3/BGGIO.Ind4.stVal	BI #91
	IED_3/BGGIO.Ind5.stVal	BI #92
	IED_3/BGGIO.Ind6.stVal	BI #93
	IED_3/BGGIO.Ind7.stVal	BI #94
	IED_3/BGGIO.Ind8.stVal	BI #95
	IED_3/BGGIO.Ind9.stVal	BI #96
	IED_3/BGGIO.Ind10.stVal	BI #97
	IED_3/ACSWI.Pos.Oper.ctlVal	BO #8
	IED_3/BCSWI.Pos.Oper.ctlVal	BO #9
	IED_3/CCSWI.Pos.Oper.ctlVal	BO #10
	IED_3/AGGIO.SPCSO32.Oper.ctlVal	BO #11
	IED_3/RREC.AutoRecSt.stVal	AI #8
	IED_3/MMXU.A.phsA.cVal.mag.f	AI #9
	IED_3/MMXU.A.phsB.cVal.mag.f	AI #10
	IED_3/MMXU.A.phsC.cVal.mag.f	AI #11
	IED_3/MMXU.TotPF.mag.f	AI #12

TABLE 10. IED #4's Data points.

IED	IEC 61850 Name	DNP3 Data Point
IED #4	IED_4/LPHD.PhyHealth.stVal	BI #98
	IED_4/LLN0.Loc.stVal	BI #99
	IED_4/XCBR.Pos.stVal	BI #100,101
	IED_4/AXSWI.Pos.stVal	BI #102,103
	IED_4/BXSWI.Pos.stVal	BI #104,105
	IED_4/CXSWI.Pos.stVal	BI #106,107
	IED_4/DXSWI.Pos.stVal	BI #108,109
	IED_4/AGGIO.Ind1.stVal	BI #110
	IED_4/ASIMG.DenAlm.stVal	BI #111
	IED_4/BSIMG.DenAlm.stVal	BI #112
	IED_4/CSIMG.DenAlm.stVal	BI #113
	IED_4/AGGIO.Ind2.stVal	BI #114
	IED_4/AGGIO.Ind3.stVal	BI #115
	IED_4/AGGIO.Ind4.stVal	BI #116
	IED_4/AGGIO.Ind5.stVal	BI #117
	IED_4/AGGIO.Ind6.stVal	BI #118
	IED_4/AGGIO.Ind7.stVal	BI #119
	IED_4/ACSWI.Pos.Oper.ctlVal	BO #12
	IED_4/BCSWI.Pos.Oper.ctlVal	BO #13
	IED_4/CCSWI.Pos.Oper.ctlVal	BO #14

single FDI attack that manipulates a small change in value is not worth it as an attack and even if the attacker performs continuous attacks with small change, proposed technique can eventually detect it, as with FDI (c), (d). Three types of DR attacks manipulating FIN, FIR, SEQ were performed and it is detected by header-based anomaly detection using anomaly frequency based threshold. Few false detection were analyzed as network congestion, therefore proposed technique also identifies communication problems on the network of the control system under normal operation.

VII. CONCLUSION

The recent cyberattacks targeting the CPS are advanced attacks that use CPS protocol packets. Therefore, the CPS requires an abnormal behavior detection system at a network-traffic level. In this study, we propose an IEEE 1815.1-based network intrusion detection system to address CPS cyberattacks in an IEEE 1815.1-based network, a new network structure of the power system using CPS. The proposed technique performs header- and payload-based abnormal behavior detection to guarantee the main functions of the CPS of SCADA system and improves accuracy by using a BRNN. This facilitates the interpretation of results. In addition, we validate the proposed technique using IEEE 1815.1-based Korea power system network data and CPS-specific attack data such as an CMB attack that performs reconnaissance, DoS and abnormal firmware upload, an FDI attack that falsifies acquisition data, and a DR attack that prevents data acquisition. Five types of CMB attacks, three types of FDI and DR attacks were successfully detected. By using the proposed technique, we can detect not only attacks using various unauthorized commands, but also advanced attacks such as FDI through existing commands, so that we can measure advanced CPS cyberattacks. In future research, we will verify the suitability of the tuning scheme and test the real-time processing capability by applying the proposed technique to the actual field using port mirroring.

APPENDIX

See Table 7–10.

REFERENCES

[1] *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*, IEEE Standard 1815, 2012.

[2] *Communication Networks and Systems for Power Utility Automation*, IEC Standard 61850, 2019.

[3] *IEEE Standard for Exchanging Information Between Networks Implementing IEC 61850 and IEEE Std 1815(TM) [Distributed Network Protocol (DNP3)]*, IEEE Standard 1815.1, 2015.

[4] H. Yoo and T. Shon, "Challenges and research directions for heterogeneous cyber-physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture," *Future Gener. Comput. Syst.*, vol. 61, pp. 128–136, Aug. 2016.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 21–32.

[6] S. Kwon, H. Yoo, and T. Shon, "Recovery measure against disabling reassembly attack to DNP3 communication," *IEICE Trans. Inf. Syst.*, vol. E100.D, no. 8, pp. 1790–1797, 2017.

[7] J.-H. Yun, "Burst-based anomaly detection on the DNP3 protocol," *Int. J. Control Automat.*, vol. 6, no. 2, pp. 313–324, 2013.

[8] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019.

[9] A. Agrawal, C. M. Ahmed, and E.-C. Chang, "Poster: Physics-based attack detection for an insider threat model in a cyber-physical system," in *Proc. Asia Conf. Comput. Commun. Secur. (ASIACCS)*. New York, NY, USA: ACM, 2018, pp. 821–823.

[10] D. Wu, H. Shi, H. Wang, R. Wang, and H. Fang, "A feature-based learning system for Internet of Things applications," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1928–1937, Apr. 2019.

[11] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, Jan. 2017, pp. 140–145.

[12] Q. Lin, S. Adepu, S. Verwer, and A. Mathur, "TABOR: A graphical model-based approach for anomaly detection in industrial control systems," in *Proc. Asia Conf. Comput. Commun. Secur. (ASIACCS)*. New York, NY, USA: ACM, 2018, pp. 525–536.

[13] C. Feng, V. R. Palleti, A. Mathur, and D. Chana, "A systematic framework to generate invariants for anomaly detection in industrial control systems," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019, pp. 1–22.

[14] S. Lee, S. Lee, H. Yoo, S. Kwon, and T. Shon, "Design and implementation of cybersecurity testbed for industrial IoT systems," *J. Supercomput.*, vol. 74, no. 9, pp. 4506–4520, Sep. 2018.

[15] *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*, NIST Standard 8219, 2018.

[16] S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the DNP3 protocol," in *Critical Infrastructure Protection III*, vol. 31. Berlin, Germany: Springer, 2009, pp. 67–81.

[17] *Telecontrol Equipment and Systems—Part 5: Transmission Rotocols*, IEC Standard 60870-5, 2018.

[18] S. Kwon, H. Yoo, and T. Shon, "RNN-based anomaly detection in DNP3 transport layer," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–7.

[19] X. Li and X. Wu, "Constructing long short-term memory based deep recurrent neural networks for large vocabulary speech recognition," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 4520–4524.

[20] *Power Market Operating Rules*, Korea Power Exchange, Naju, South Korea, 2019.

[21] *Communication Networks and Systems for Power Utility Automation—Part 7-4: Basic Communication Structure—Compatible Logical Node Classes and Data Object Classes*, IEC Standard 61850-7-4, 2010.

[22] *Communication Networks and Systems for Power Utility Automation—Part 7-3: Basic Communication Structure—Common Data Classes*, IEC Standard 61850-7-3, 2010.

[23] *Triangle Microworks Product [Internet]*. Accessed: Mar. 19, 2020. [Online]. Available: http://www.trianglemicroworks.com/products/

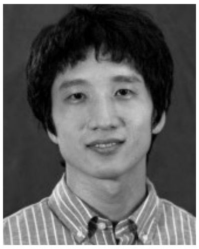
[24] *Ostinato Packet Generator [Internet]*. Accessed: Mar. 19, 2020. [Online]. Available: http://ostinato.org

[25] *CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations*, Dragos, Washington, DC, USA, Jun. 2017.

[26] *Malware Analysis Report, MAR-17-352-01 HatMan—Safety System Targeted Malware*, Nat. Cybersecur. Commun. Integr. Center, New Delhi, India, Dec. 2018.

[27] K. Cho, B. van Merrienboer, C. Gulcehre, D. Bahdanau, F. Bougares, H. Schwenk, and Y. Bengio, "Learning phrase representations using RNN encoder-decoder for statistical machine translation," 2014, *arXiv:1406.1078*. [Online]. Available: http://arxiv.org/abs/1406.1078

SUNGMOON KWON (Graduate Student Member, IEEE) received the B.S. degree in information and computer engineering from Ajou University, Suwon, South Korea, in 2013, where he is currently pursuing the Ph.D. degree in computer engineering. He is with the Information and Communication Security Laboratory. His current research interests include smart grid security and industrial control system security.



HYUNGUK YOO (Member, IEEE) received the B.S. degree in information and computer engineering and the Ph.D. degree in computer science and engineering from Ajou University, South Korea, in 2011 and 2017, respectively. He is currently an Assistant Professor with the Department of Computer Science, University of New Orleans, Louisiana, USA. His research interests include systems security, malware analysis, digital forensics, cyber-physical systems security, and applied machine learning.

TAESHIK SHON (Senior Member, IEEE) received the B.S. and M.S. degrees in computer engineering from Ajou University, Suwon, South Korea, in 2000 and 2002, respectively, and the Ph.D. degree in information security from Korea University, Seoul, South Korea, in 2005. While he was working toward his Ph.D. degree, he was awarded the KOSEF Scholarship to be a Research Scholar with the Digital Technology Center, University of Minnesota, Minneapolis, USA, from February 2004 to February 2005. From August 2005 to February 2011, he was a Senior Engineer with the Convergence S/W Laboratory, DMC Research and Development Center, Samsung Electronics Company, Ltd. He was a Visiting Professor with the Electrical Computer Engineering Department, Illinois Institute of Technology, Chicago, USA, in 2017. He is currently a Professor with the Division of Cyber Security, College of Information Technology, Ajou University. His research interests include industrial control systems, anomaly detection algorithms, and digital forensics. He was awarded the Gold Prize for the Sixth Information Security Best Paper Award from the Korea Information Security Agency, in 2003, the Honorable Prize for the 24th Student Best Paper Award from Microsoft-KISS, in 2005, the Bronze Prize for the Samsung Best Paper Award, in 2006, the Second Level of TRIZ Specialist Certification in Compliance with the International TRIZ Association requirements, in 2008, and the Silver, Bronze, Excellent Publication Prize for Ajou University Award, in 2013, 2014, and 2016. He is serving as a Guest Editor, an Editorial Staff, and a Review Committee Member of *Computers and Electrical Engineering* (Elsevier), *Mobile Network and Applications* (Springer), *Security and Communication Networks* (Wiley InterScience), *Wireless Personal Communications* (Springer), the *Journal of the Korea Institute of Information Security and Cryptology*, the *IAENG International Journal of Computer Science*, and other journals.