Cyber-Physical Vulnerability Analysis of Communication-Based Train Control

Sangjun Kim, Yuchang Won, In-Hee Park, Yongsoon Eun, *Member, IEEE*, and Kyung-Joon Park, *Member, IEEE*

***Abstract*—A cyber-physical system (CPS) is an entanglement of physical and computing systems by real-time information exchange through networking, which can be considered as real-time IoT because of end-to-end real-time performance guarantee. Most societal infrastructures, such as transportation systems, smart power grid, smart factory, and smart buildings, are key application domains of CPS. Though there have been extensive studies on infrastructures from the perspective of cyber security, insufficient research has been conducted from a practical viewpoint of *cyber-physical security*. In this paper, we focus on train control systems as one of the critical infrastructures. We fully investigate the emerging de facto standard of train control systems, communication-based train control (CBTC). We analyze the cyber-physical vulnerability of CBTC and discover that a man-in-the-middle attack combined with knowledge on train signaling can cause train collisions in CBTC. To resolve the issue, we propose a countermeasure for resiliency of CBTC. By implementing a realistic CBTC testbed, we validate our analysis. To the best of our knowledge, this is the first in-depth empirical study on cyber-physical vulnerability of CBTC systems.**

***Index Terms*—Communication-based train control, cyber-physical security, cyber-physical systems, real-time IoT, vulnerability analysis.**

I. Introduction

CYBER-PHYSICAL systems (CPSs) tightly integrate physical and computing systems, and interact between them by information exchange through communication networks [1]–[5]. As the interaction between physical and computing systems increases, CPS is more susceptible to various attacks [6]–[9]. For instance, in 2010, Stuxnet malware caused serious damage to the control systems of an Iranian uranium enrichment facility [10]. In 2015, malware incurred damage to the Ukraine power grid and resulted in a massive power outage [11].

Manuscript received September 4, 2018; revised April 4, 2019; accepted May 15, 2019. Date of publication May 27, 2019; date of current version July 31, 2019. This work was supported in part by the National Research Foundation of Korea (NRF) funded by the Korea Government (MSIT) under Grant NRF-2016R1C1B2007899 and in part by the Institute for Information and Communications Technology Promotion (IITP) funded by the Korea Government (MSIP) (Resilient Cyber-Physical Systems Research) under Grant 2014-0-00065. *(Corresponding author: Kyung-Joon Park.)*

S. Kim, Y. Won, Y. Eun, and K.-J. Park are with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu 42988, South Korea (e-mail: sjkim@dgist.ac.kr; yuchang@dgist.ac.kr; yeun@dgist.ac.kr; kjp@dgist.ac.kr).

I.-H. Park is with the Agency for Defense Development, Daejeon 34186, South Korea (e-mail: inhee@add.re.kr).

Digital Object Identifier 10.1109/JIOT.2019.2919066

Traditional cyber security research mainly focuses on the cyber aspect of information protection without paying much attention to cyber-physical interaction [6], [12]. Recently, there has been a line of research on security of CPS, called *cyber-physical security* [3], [9], [13], which extends the dimension of traditional cyber security with an additional axis of knowledge on physical dynamics. Consequently, cyber-physical security considers cyber-physical attacks that further exploit the physical aspect of CPS on top of conventional cyber attacks. It should be noted that cyber-physical attacks are critical in that they can directly cause unexpected operations of physical systems, which are often disasters.

From the perspective of application domains, the concept of CPS is essential in societal infrastructures because of their critical impact [1], [5]. In particular, a high level of resiliency against malicious attacks should be ensured. However, there have been insufficient studies on cyber-physical security of societal infrastructures from a practical point of view.

In this paper, as one of the critical infrastructures, we focus on train control systems. Currently, the traditional train control systems are being transformed into communication-based train control (CBTC) systems for enhancing key functionality as well as efficiency [14]. Hence, we study cyber-physical vulnerability of CBTC from a realistic viewpoint. More specifically, our main contributions can be summarized as follows.

1) We fully investigate the CBTC architecture, and discover that a man-in-the-middle (MITM) attack combined with detailed knowledge on train signaling can cause train collisions. Then, to resolve the issue, we propose a countermeasure for resiliency of CBTC.
2) In order to validate our analysis, we implement a realistic CBTC testbed by considering all the key components in CBTC systems on top of a commercial train control and supervision software. Our empirical results confirm the validity of the analysis.

The rest of this paper is organized as follows. Section II provides an introduction on CBTC. In Section III, we analyze the cyber-physical attacks on CBTC, especially MITM attack based on ARP spoofing, and present the impact of the attack on train operation. Section IV presents an SDN architecture for implementing various attack scenarios. Section V presents our testbed, which captures all the key components in CBTC, and then, we present our performance evaluation. Our conclusions follow in Section VI.

TABLE I
LIST OF ACRONYMS USED IN THIS PAPER

Acronyms	Elaboration
ATS	Automatic Train Supervision
CBTC	Communication Based Train control
DSP	Dynamic Speed Profile
MA	Movement Authority
MRSP	Most Restrictive Speed Profile
OATO	Onboard Automatic Train Operation
OATP	Onboard Automatic Train Protection
WATP	Wayside Automatic Train Protection

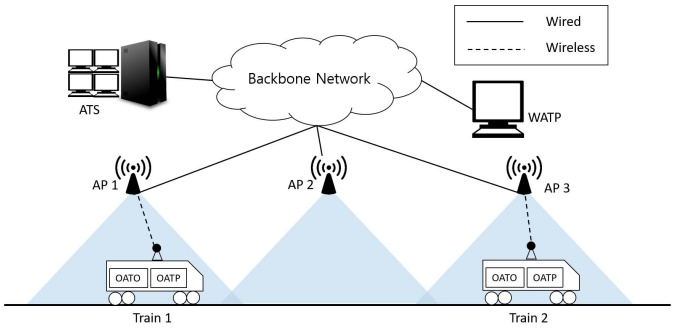


Fig. 1. CBTC network architecture.

II. COMMUNICATION-BASED TRAIN CONTROL

A. CBTC Architecture

CBTC is the next-generation train control system adopting wireless communication, which has recently been introduced worldwide [15]. CBTC uses both in-vehicle and ground signal control equipment. A computer installed in the central control center on the ground continuously checks the position and velocity of each train to determine the distance to the preceding train and the train speed limit point. Also, the computer in the train uses wireless communication for data transmission between the ground facility and the train by optimally controlling the speed according to the situation of the train, which will greatly improve the transport efficiency [15].

These systems not only provide the communication links for information transmission but also measure the position of moving trains. Then, the real-time position of moving trains can be detected much more accurately than the conventional positioning system, which has a very limited position accuracy of a so-called block due to the fixed block system. Thus, the train can transmit detailed status information to the control center, and the control center can transmit detailed command information to the trains. Moreover, it is possible to keep the intervals between the trains to a minimum and to improve the transport efficiency of operation. In Table I, we list the acronyms used for the CBTC systems.

As shown in Fig. 1, the CBTC systems consist of several components for railway operation, such as automatic train supervision (ATS), wayside/onboard automatic train protection (ATP), and onboard automatic train operation (OATO). ATS monitors operation of trains, specifies the routes of the trains and sends command messages for safe train operation to wayside ATP (WATP). WATP units are installed at certain intervals on the track. WATP determines maximum velocity and movement authority (MA) of the train and creates the most restrictive speed profile (MRSP) using information of the train and infrastructures. WATP notifies the train MA and MRSP. Then onboard ATP (OATP) on the train receives operation data that WATP transmits. OATP generates dynamic speed profile (DSP) to the destination point using the MRSP information received from WATP and determines the speed and position of the train. Also, OATP transmits the details of its states of the motion (i.e., position and velocity) of the train to WATP. The OATO compares the speed of the train with the DSP and performs the train operation. WATP and OATP exchange the messages using railway-specific radio communication, such as GSM-R and LTE-R, or IEEE 802.11-based wireless communication technology. The type of wireless communications can be selected according to some constraints, such as frequency band allocation, cost of the system configuration, operating distance, and speed of the trains. IEEE 802.11-based communication has a coverage of several hundreds of meters for one access point (AP), while a railway-specific radio communication has the range of several kilometers for one cell [16], [17].

The units on the ground facility and the onboard facility communicate with each other by wire. The communication between WATP and OATP use standardized wireless communication and periodically exchange the control messages and sensing messages. Since CBTC uses wireless networks, the attack surface is broader than the conventional train control systems. There is a possibility of air-gap attacks, with which malicious hackers can access the computer management systems that control trains and signals through the network. This attack can cause severe damage to CBTC systems such as train collisions.

B. Information Exchange for Train Operation

In CBTC systems, a train receives data for operation through control messages from WATP, which periodically sends control messages to OATP. Then, OATP determines the operation based on the data received from WATP. Consequently, if operation data is manipulated by an attacker, it will seriously affect train operation. Hence, we thoroughly investigate the details of operation data and how it operates the trains for vulnerability analysis of CBTC. In particular, we study the KRS-SG-0069 standard [18], which is the Korean version of the CBTC standard for the communication protocol between WATP and OATP. It should be noted that all the CBTC standards basically share the same protocol while some implementation details are different. In the CBTC protocol, MA and MRSP data are essential for train operation.

MA indicates the allowable travel distance of a train. MA is calculated considering the safety margin to prevent collision with the preceding train and the location of the train station. If the MA of a train is longer than the distance to the preceding train, train collision may occur.

MRSP means the speed limit profile in a certain section of the railway. Trains must operate at a speed below the

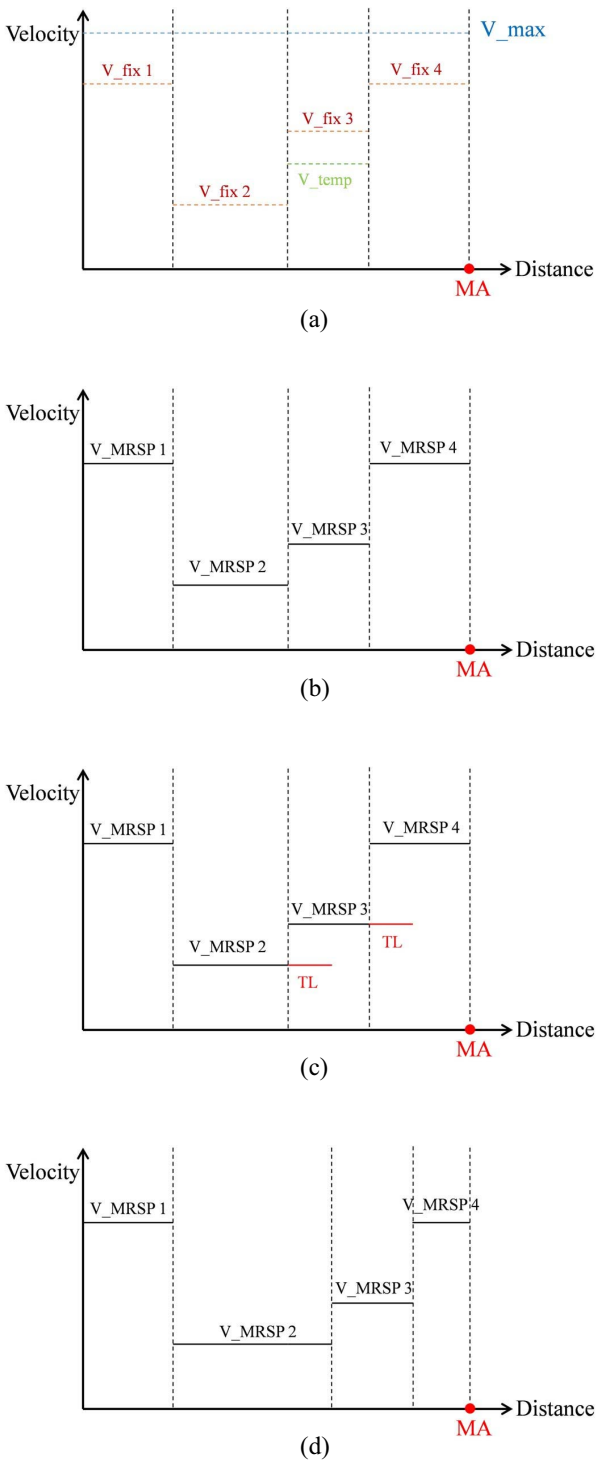


Fig. 2. MRSP calculation process. (a) Initial stage. (b) Speed limit by section. (c) Extend speed limit as train length. (d) Final MRSP.

speed limit indicated by MRSP. Basically, MRSP considers the length of a train, MA, and geographic information of a specific section. WATP calculates MRSP and then transmits it to OATP. MRSP can be calculated by

$$V_{\mathrm{MRSP}}(X) = \min\big(V_{\max}, V_{\mathrm{fix}}(X), V_{\mathrm{temp}}(X)\big). \tag{1}$$

There are three speed limit criteria, $V_{\max}$, $V_{\mathrm{fix}}(X)$, and $V_{\mathrm{temp}}(X)$. Here, $V_{\max}$ corresponds to the maximum speed the train can reach. $V_{\mathrm{fix}}(X)$ is the prescribed speed in section X of the railway. $V_{\mathrm{temp}}(X)$ is the temporary speed limit set by the temporary traffic policy in section X. Fig. 2 shows the MRSP decision process. There are $V_{\max}$, $V_{\mathrm{fix}}(X)$, and $V_{\mathrm{temp}}(X)$ as shown in Fig. 2(a). Then, WATP adopts the lowest speed limit in each section according to (1) as shown in Fig. 2(b). In the section where the speed limit of the next section is lower than the current speed limit, the head portion of the train reduces speed before entering the next section, so there is no need to adjust the length of MRSP section. However, in the section where the speed limit of the next section is higher than the current speed limit, the train must accelerate after the tail portion of the train enters the next section. Therefore, if the speed limit of the next section is higher than the current speed limit, the end of the current section must be extended by the length of the train as shown in Fig. 2(c). At the same time, the starting point of the next section is moved to the end point of the adjusted current section as shown in Fig. 2(d). The overall process of deciding MRSP is given in Algorithm 1 [19]–[21]. In the actual development of a train operation simulator, Algorithm 1 is typically adopted for generation of the speed profile required for train operation, and the MRSP generation algorithm considering the train length is also used in the real CBTC system [22].

Algorithm 1 MRSP Generation [19]–[21]

Require: $S(X) = [\mathrm{Pos}(X), \mathrm{Pos}(X+1)]$: MRSP section X, TL: train length
  if $V_{\mathrm{MRSP}}(X) < V_{\mathrm{MRSP}}(X+1)$ **then**
    $S(X) \Leftarrow [\mathrm{Pos}(X), \mathrm{Pos}(X+1) + TL]$
    $S(X+1) \Leftarrow [\mathrm{Pos}(X+1) + TL, \mathrm{Pos}(X+2)]$
  else
    Search next section
  end if

Once the calculated MRSP is transmitted to OATP on the train, OATP creates the DSP actually needed to control the train. There are multiple methods to calculate the DSP [23], [24]. In this paper, we assume that the train takes uniformly accelerated motion and DSP is calculated by the formula of uniformly accelerated motion. In order to calculate DSP, we divide DSP into the accelerating section, the decelerating section, and the constant velocity section according to the current velocity and the target velocity. That is, if the current velocity is smaller than the target velocity, it corresponds to the accelerating section. In a similar manner, when the target speed is smaller than the current velocity, it is the decelerating section, and in the case that they are the same, it is the constant velocity section. Therefore, DSP is generated by using the current position d_n, current time t_n, uniform acceleration constant acc, uniform deceleration constant dec, current velocity V_n, and target velocity V_{n+1} received from MRSP. The time interval of each section in DSP can be derived from

$$t_{n+1} - t_n = \begin{cases} \frac{V_{n+1}-V_n}{acc}, & \text{if } V_{n+1} > V_n \\ \frac{d_n}{V_n}, & \text{if } V_{n+1} = V_n \\ \frac{V_n-V_{n+1}}{dec}, & \text{if } V_{n+1} < V_n. \end{cases} \tag{2}$$

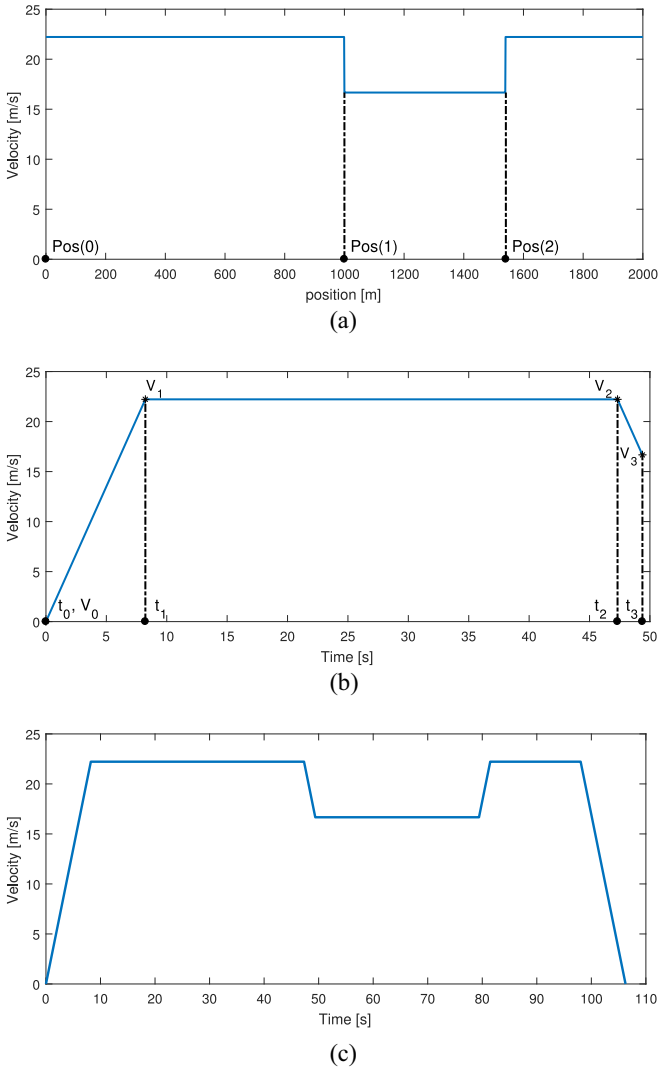


Fig. 3. DSP calculation process. (a) Received MRSP from WATP. (b) DSP for the first section. (c) Final DSP.

Now, DSP can be represented by the velocity–time graph. Fig. 3 shows the process of creating DSP when MRSP is given. Fig. 3(a) shows the OATP's MRSP data received from WATP. In Fig. 3(b), DSP of the time interval t_0 to t_3 is calculated from the section between Pos(0) and Pos(1) in Fig. 3(a). The moving distance d_n, from the specific instant t_n to the next time instant t_{n+1}, is calculated from (3). The final DSP for all MRSP data given in Fig. 3(a) can be calculated as shown in Fig. 3(c). In the given DSP time intervals, the sum of d_i's is equal to MA

$$d_n = \int_{t_n}^{t_{n+1}} \mathrm{DSP}(t)\, dt$$
$$\sum_i d_i = \mathrm{MA}. \tag{3}$$

III. Cyber-Physical Attack Vulnerability of CBTC

A. Attacks for Wireless Networks

By adopting wireless communication, the attack surface of CBTC systems is broader than the traditional one. Especially, as the network structure becomes more complex, there will be more vulnerability points for cyber-physical attacks. When the wireless communication systems transmit data, it generates electromagnetic signals into the air. The issue in terms of security is that there is a possibility that attackers near the AP can receive the signal. Even when the signal is encrypted, it may still be a vulnerable point for a malicious attacker.

Thus, while adopting CBTC, network security has become the most critical issue, and there exist analysis results of the network security of CBTC [25], [26]. The collective opinion of the results is that three types of attack are possible for CBTC. The first type is disturbing the transmission of data between a train and WATP physically. The second is to exhaust network resources for delaying the communication. The last one is to manipulate the operation data between a train and WATP, which is the most critical one.

By using a jamming signal, a malicious attacker can disconnect the wireless link between a train and WATP. In order to generate jamming signals, an attacker needs to understand the physical characteristics of wireless communication and the attacker emits a high-power electromagnetic wave to the air-gap between WATP and OATP [27], [28]. If the attacker generates a jamming signal, the train receives a mixed signal and cannot distinguish perfectly between the jamming signal and the data signal from WATP. For the train, the high-power electromagnetic wave emitted by the attacker corresponds to noise. Then, the signal-to-noise ratio (SNR) for the WATP signal is drastically lowered, which may cause communication failure. However, if the communication is continuously disconnected by this jamming attack, the train stops for safety.

Another kind of attack is to send a large number of packets to the victim. The host that receives a lot of packets consumes extensive computation resources to process the received packets [29]. In addition, network bandwidth is consumed. As a result, the network delay significantly increases. In this case, the train control performance can be degraded due to the large network delay [25].

The most significant attack is as follows. The MITM attack intercepts a packet destined for the end user and forwards the wrong data [30]. When the attacker is already connected to the wireless network and attempts an MITM attack between the train and the supervision system, the attacker manipulates the operation data from WATP to OATP and injects wrong control messages to OATP. Then, malfunction of the train may occur, such as derailment or collision with a preceding train. So, this type of attack is classified as the most dangerous one in CBTC [25].

Unlike the jamming attack and the flooding attack, the MITM attack is difficult to detect because it does not make significant traffic changes or physical changes. This cyber-physical attack takes the control authority of the train and may cause serious malfunction of the train.

B. ARP Spoofing-Based Man-in-the-Middle Attack

The MITM attack is for a malicious user to take control of the communication channels between two or more hosts. Among the hosts, the attacker can intercept and manipulate

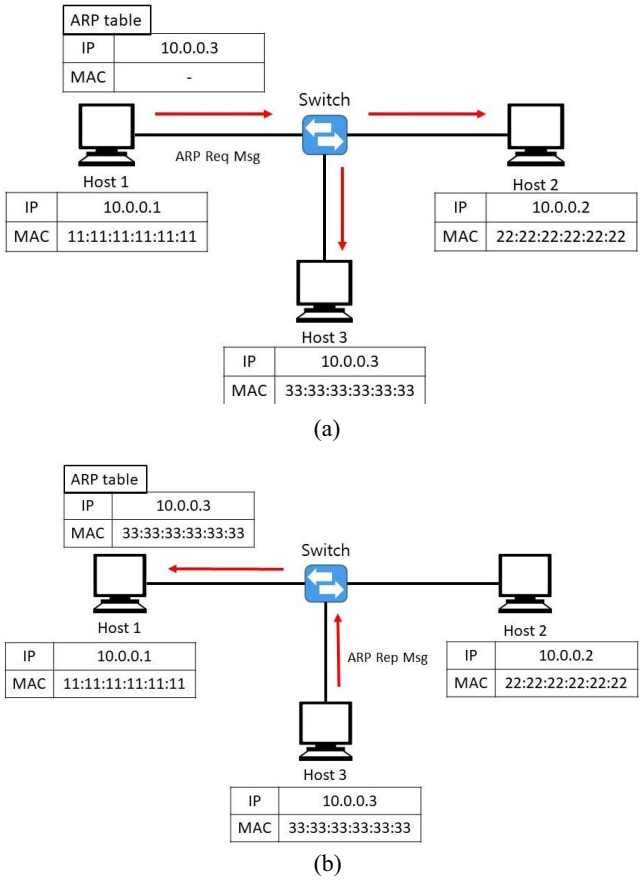


Fig. 4. ARP cache updating process. (a) ARP request message broadcasting. (b) ARP reply message unicasting.

messages on the network. MITM attacks are performed not only on wired but also in wireless environments such as GSM, LTE, Wi-Fi, and Bluetooth. In addition, MITM attacks can be conducted at various layers of the OSI model and in various methods [30]. Here, we focus on a MITM attack based on address resolution protocol (ARP) spoofing in the data-link layer via wireless networks.

In order for two hosts to communicate on the network, they need to know both the MAC address and the IP address of the other. The hosts use ARP to map the IP address and MAC address of each other as shown in Fig. 4. Through the following process, two hosts can communicate with each other.

1) If host 1 wants to communicate with host 3, the MAC address of host 3 is required to host 1. Then, to obtain the MAC address of host 3, host 1 broadcasts ARP request messages to all hosts on the network.
2) When host 3 receives an ARP request message from host 1, host 3 directly sends an ARP reply message containing its MAC address to host 1.
3) When host 1 receives the ARP reply message of host 3, host 1 registers destination hosts IP address-MAC address pair to its ARP cache. Then two hosts can communicate since they know each others' MAC address.

When ARP messages are exchanged, there is no authentication process because ARP is designed without consideration of

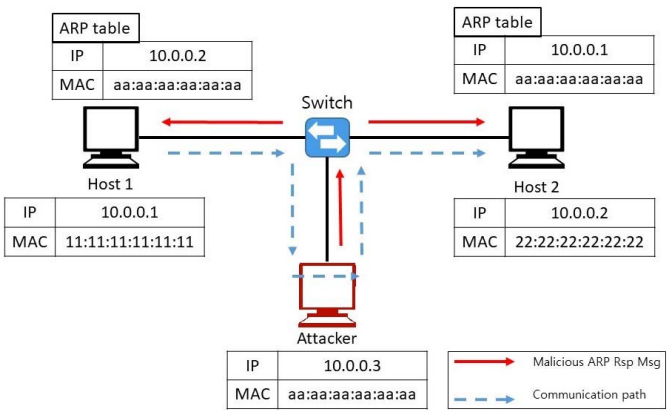


Fig. 5. ARP spoofing.

security. If the host receives the ARP reply message, the host registers the information of the ARP reply message to the ARP cache regardless of the request, as shown in Fig 5. Although the MAC address in the attacker's message and the MAC address already registered in the ARP cache are different for the same IP, the host overwrites information of the attacker's ARP reply message to the ARP cache. This vulnerability is called the stateless nature of ARP [31].

When victims that have a poisoned ARP cache send the packets to another host, these packets are sent to the attacker. Thus, a malicious host can intercept the communication path and exploit sensitive information. Even worse, the intercepted packets can be manipulated and forwarded to the original destination by the attacker. In the CBTC systems, MITM attacks that modify operation data can result in train collisions.

If the MA and MRSP are manipulated by an MITM attack, OATP generates the wrong DSP. Fig. 6(a) shows an example of MRSP under normal operation and under attack, respectively. The DSPs are calculated from the received MRSP as shown in Fig. 6(b). In Fig. 6, the blue and red lines represent data under normal operation and under attack, respectively. By manipulating the MA and MRSP data, the attacker can take the control authority of the train. If the attacker has sufficient knowledge on train signaling and DSP generation, the attacker can cause train collisions, which corresponds to the case of cyber-physical attacks that exploit the dynamics of physical systems through cyber systems.

IV. SDN-Based ARP Spoofing Countermeasure for CBTC

In Section III, we confirmed that malfunction of a train can occur in CBTC systems under a MITM attack through the wireless network. In this section, to resolve the situation of the MITM attack, we propose a software-defined networking (SDN)-based countermeasure for ARP spoofing in CBTC systems.

The attacker that enters the network can scan all the hosts. In other words, hosts that are scanned by the attacker can be victims. Thus, a host that cannot be detected by the attacker is needed to notify OATP of the attack. The main idea of this countermeasure architecture is to have a subsystem with a host

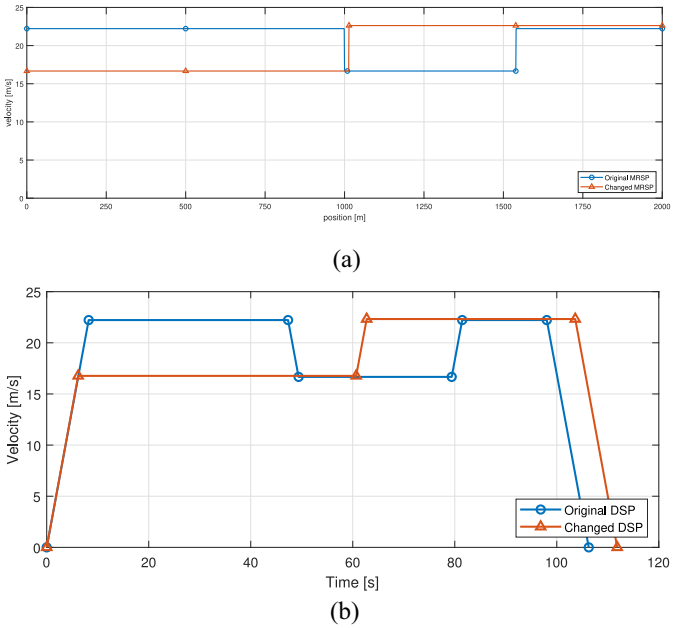


Fig. 6. Manipulated MRSP and DSP under normal and attack scenario. (a) Normal and manipulated MRSP. (b) Normal and manipulated DSP.

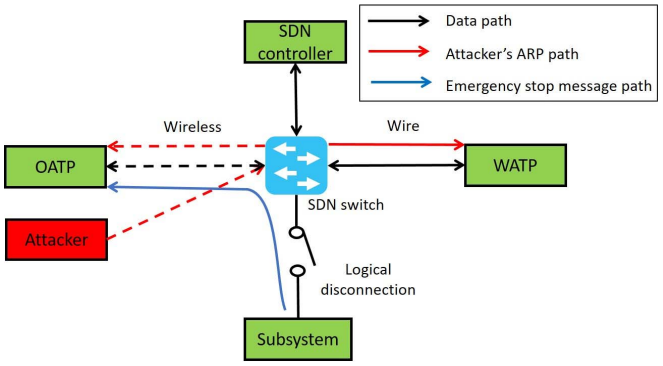


Fig. 7. SDN-based ARP spoofing countermeasure structure.

unexposed to the attacker. Fig. 7 shows the countermeasure structure against ARP spoofing and how the network structure works. The subsystem is physically connected to the SDN switch by wire. However, the link between the SDN switch and the subsystem is logically disconnected by the SDN controller. When the attacker scans the victims, the subsystem is undetected because of the logical disconnection. Thus, the subsystem can remain undetected under the MITM attack.

In order for the subsystem to notify OATP of the attack situation, the SDN switch should detect ARP spoofing. In the structure, the SDN switch continuously monitors ARP messages and creates an IP-MAC list for ARP messages across the SDN switch. Then, ARP spoofing can be detected by Algorithm 2.

Under ARP spoofing, the countermeasure architecture operates by the following process.

1) The attacker sends unsolicited ARP reply messages to WATP and OATP.
2) The SDN switch inspects the ARP reply messages from the attacker and determines ARP spoofing by Algorithm 2. After detecting the attack, the SDN switch notifies the SDN controller of the attack.
3) Then, the SDN controller commands the SDN switch to connect the link between the isolated subsystem and the SDN switch.
4) The SDN switch connects the link and subsystem sends the emergency stop message to OATP.
5) Finally, the train stops as soon as the emergency stop message is received.

The subsystem is connected to the network under ARP spoofing. Since the victims are scanned and targeted by the attacker before ARP spoofing, the ARP cache of the subsystem is not poisoned. So, the subsystem remains intact under ARP spoofing.

Algorithm 2 ARP Spoofing Detection

Input: *ARP*, *list*
  if *ARP.type* = *request* **then**
    if *ARP.sourceIP* $\notin$ *list* **then**
      add (*ARP.sourceIP*, *ARP.sourceMAC*) to *list*
    end if
  end if
  if *ARP.type* = *reply* **then**
    if *ARP.sourceIP* $\notin$ *list* **then**
      add (*ARP.sourceIP*, *ARP.sourceMAC*) to *list*
    else if *ARP.sourceIP* $\in$ *list* **then**
      if (*ARP.sourceIP*, *ARP.sourceMAC*) $\notin$ *list* **then**
        Determine ARP spoofing attack.
      else
        Already registered (*IP*, *MAC*)
      end if
    end if
  end if

V. Empirical Study

A. Testbed Environment

For validation of our vulnerability analysis and countermeasure architecture, we implement a realistic CBTC testbed as shown in Fig. 8. For information exchanges between WATP and OATPs, we consider the KRS-SG-0069 standard [18]. The testbed consists of all the core parts of the CBTC systems, which are ATS, WATP, OATO, OATP, track information, and a network. We use commercial software for implementation of ATS, WATP, OATO, and OATP. In addition, track information is taken from an actual line with four stations in a certain country. Based on the track information, we revise the ATS, WATP, OATO, and OATP software. The WATP and OATP transmit train data and track information data through the network. The train dynamics are simulated on a desktop using a simulator, which receives motor and brake commands from OATO and returns the signals from the encoders.

We build four bridges using Raspberry Pi 3 to construct the network. Since the CBTC network is a mixed environment of wired and wireless networks, we consider that one of the bridges in the network operates as a Wi-Fi AP as shown in Fig. 9. There are two paths from OATP to WATP in the

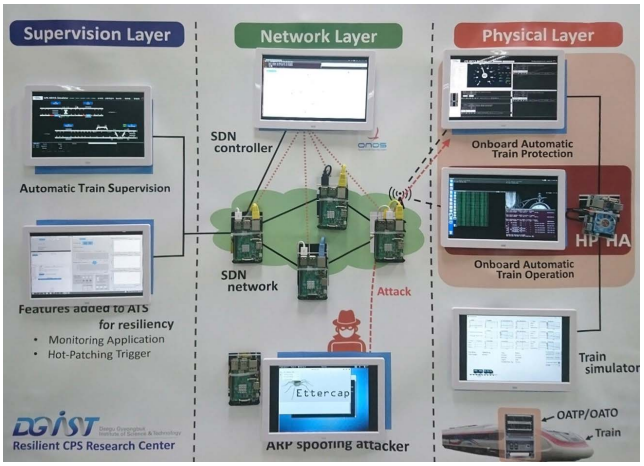


Fig. 8. CBTC testbed.

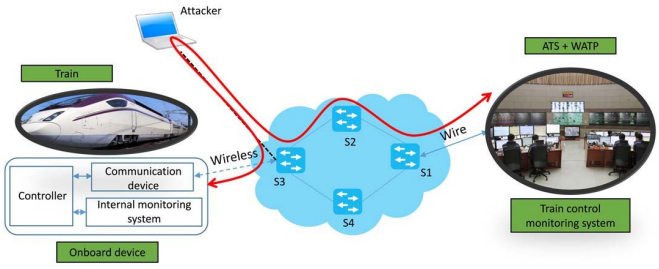


Fig. 9. MITM attack scenario in CBTC.

network. OATP is connected with the Wi-Fi AP bridge using a wireless connection. WATP is connected with one of the bridges using a wired connection.

The attack device consists of a Raspberry Pi 3 and Ettercap software, which is a suite of software tools for the MITM attack [32]. The attack device can access the network and "sniff" the exchanged information between WATP and OATP via the Wi-Fi AP. Based on the sniffed information, the attack device specifies the target train and modifies the data related to its MA information.

To evaluate the SDN-based countermeasure for ARP spoofing in Section IV, we build a network as shown in Fig. 10. Raspberry Pi 3 with Open vSwitch software functions as the SDN switch interacting with the SDN controller, and the ONOS SDN controller manages four SDN switches [33], [34]. Additional software, which continuously inspects ARP messages and detects ARP spoofing, is installed on the SDN switch S1 connected to WATP, as shown in Fig. 10. Since one of the ARP spoofing targets is WATP, a malicious ARP reply message is delivered to WATP through S1, and it is sufficient to monitor ARP messages on S1.

B. MITM Attack Implementation

There are two steps for attacking CBTC from the viewpoint of the attacker. The first step is to specify IP of WATP and trains, and the second step is to perform the MITM attack. To implement the MITM attack, we consider the following scenario.

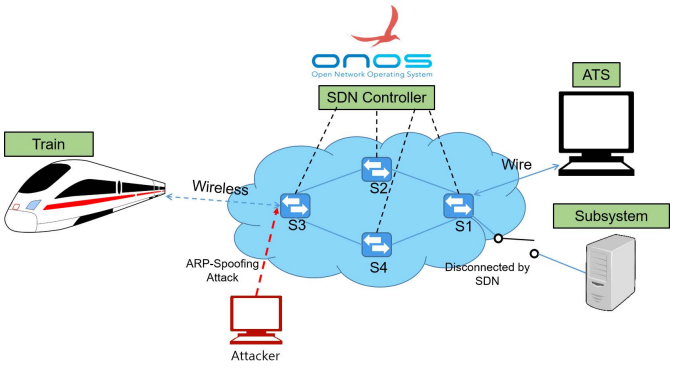


Fig. 10. Structure of the ARP spoofing countermeasure for CBTC.

1) There are two trains on the railway line and the preceding train is in a stationary position for some reasons. The following train is stopped at the previous station and ready for departure.
2) Trains operate unmanned and rely on communication with WATP and the maximum velocity of trains is 80 km/h (22.2 m/s).
3) The attacker is already connected to the AP and knows the protocol for communication between WATP and OATPs.
4) The attacker can scan the hosts. However, the attacker cannot specify the preceding train and the following train.
5) The attacker specifies two victims, WATP and the following train, before the MITM attack. If the attacker sets all hosts on the network as victims, ARP spoofing is easily detected due to the excessive traffic changes.

The attacker who accesses AP can sniff and filter the messages between WATP and OATPs in real time. The attacker can specify WATP through the source IP address and source MAC address of the sniffed control messages. Once this is done, the attacker specifies the following train as the target to make the train malfunction. To distinguish between the preceding train and following train, the attacker constantly inspects the position data in the sensing message of the trains by Algorithm 3. If there is no position change in θ consecutive sensing messages of a train, the attacker determines this train as the preceding one. If the movement of the train is detected in the sensing messages, the attacker regards this train as the target.

The second step for attacking CBTC is to generate the MITM attack using ARP spoofing. To implement ARP spoofing on the network, we use the Ettercap tool, in which we use a filter to eavesdrop and manipulate MA and MRSP of control messages from WATP to the following train. Through the MITM attack, we can manipulate the MA of the following train, and then the following train runs over the original MA to the preceding train and collides with the preceding train.

C. Verification of Train Collision by the MITM Attack

In order to check whether train collisions can actually happen due to the MITM attack, we carry out experiments with

Algorithm 3 Identification of WATP and Target Train

Input: *pkt* : control and sensing messages, *pos* : position of train, θ : threshold for preceding train

```
if pkt.type = control then
    WATP.IP ⇐ pkt.sourceIP
    WATP.MAC ⇐ pkt.sourceMAC
end if
for all train do
  if pkt.train = X then
    if pkt.type = sensing and pkt.seq = n then
      counter ⇐ 0
      k ⇐ n
      while n > k + θ do
        if pkt(n + 1).pos = pkt(n).pos then
          counter ⇐ counter + 1
        end if
        n ⇐ n + 1
      end while
    end if
    if counter = θ then
      train X is preceding train
    end if
  else if counter < θ then
    train X is following train
    Target.IP ⇐ pkt.sourceIP
    Target.MAC ⇐ pkt.sourceMAC
  end if
end for
```

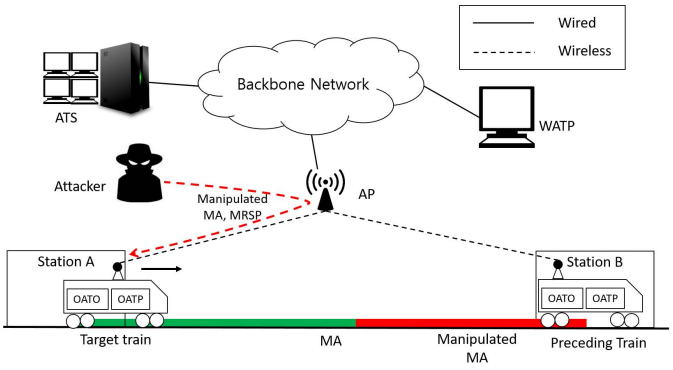


Fig. 11. Experimental scenario.

our testbed. Fig. 11 shows the MITM attack on the target train. When the target train is under the normal operation, it follows the MA and MRSP information received from the WATP and travels to the end of the green separation where the safety margin to the preceding train is considered. However, under the MITM attack, due to the manipulated MA and MRSP, the train travels to the end of the red separation as shown in Fig. 11. Then, the target train cannot recognize the preceding train and crashes into the preceding train.

Fig. 12 shows the movement of the target train when it is under MITM attack and normal operation, respectively. Under normal operation, the target train travels 566 m because of the safety margin to the preceding train. However, under the

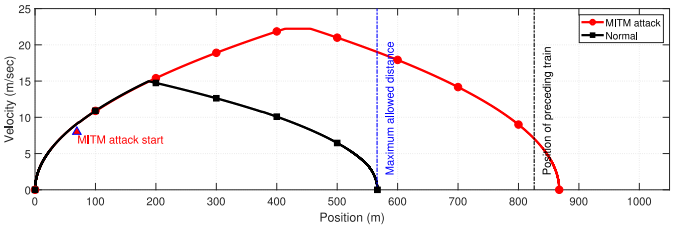


Fig. 12. Train speed profile under MITM attack.

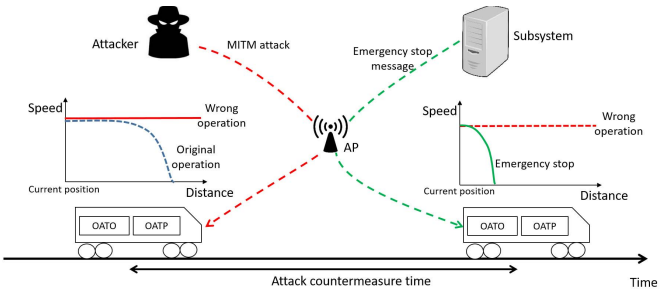


Fig. 13. Diagram of the countermeasure time for ARP spoofing.

MITM attack, the target train receives MA data that exceeds the distance to the preceding train. Then, the target train does not take into account the preceding train, and travels beyond the position of the preceding train. As a result, the target train collides with the preceding train.

From our experiment, we can confirm that manipulation of control messages through the MITM attack can cause train collision in CBTC. Train collisions are the most damaging accidents in the CBTC systems. So, the MITM attack is the most dangerous cyber-physical attack that can damage the CBTC systems.

D. Evaluation of the Proposed Countermeasure Structure

In order to evaluate the proposed countermeasure architecture for the ARP spoofing attack, we carried out experiments. To evaluate how fast the target train recovers from the MITM attack, we define the attack countermeasure time t_c as the total time period that the train malfunctions by the MITM attack. The attack countermeasure time is calculated as the time interval from the instant the first manipulated packet arrives at OATP until the arrival of the train emergency stop packet, as shown in Fig. 13.

Here, we conduct experiments when the transmission period of the control message from WATP to OATP is 500 ms. In the case of more than half, as shown in Fig. 14(a), countermeasure time is zero. This result indicates that our countermeasure structure detects ARP spoofing before any manipulated control message is delivered to the train, so the target train is not manipulated at all by the attacker. In 500 ms, our structure handles about 74% of the MITM attacks. In the worst case, the proposed structure can handle the MITM attacks in 2.25 s. In order to verify the safety of our countermeasure structure, we assume the worst-case attack scenario in which the train travels beyond the original MA.

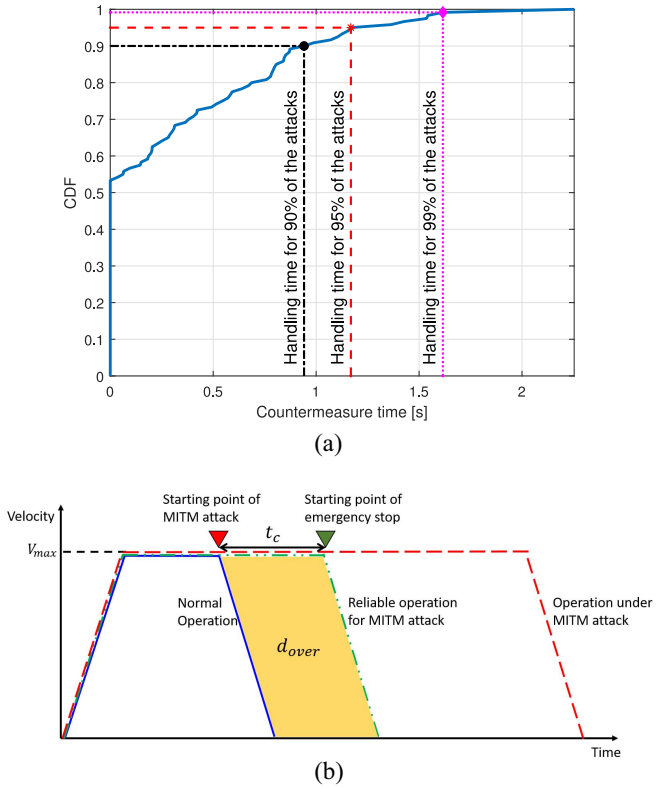


Fig. 14. Attack countermeasure time for ARP spoofing and mitigation of influence on train operation under MITM attack. (a) ARP spoofing countermeasure time. (b) DSPs of target train.

1) The travel separation should be far enough to allow the train to run at the maximum speed, and the point of the MITM attack is when the train starts to decelerate at the maximum speed. Then, the train does not decelerate but runs at the maximum speed.
2) The safety margin between the trains is 260 m as shown in Fig. 12, and the maximum velocity of the train $V_{\max}$ is 80 km/h (22.2 m/s).
3) Other emergency braking systems do not exist on the train. When the train receives emergency stop messages, the train just attempts to brake.

In our scenario, the target train which has received the manipulated control message travels farther than the original MA during the attack countermeasure time with the maximum speed. We define the distance d_{over} that is the exceeded distance over the original MA. As shown in Fig. 14(b), d_{over} can be represented by the yellow area. When t_c increases, d_{over} also increases by

$$d_{\text{over}} = V_{\max} \times t_c. \tag{4}$$

If d_{over} is larger than the safety margin, the target train collides with the preceding train. In the measured t_c as shown in Fig. 14(a), despite the worst case, our proposed structure can handle the MITM attack in 2.25 s, and d_{over} does not exceed 50 m. This result shows that the trains do not collide because d_{over} is smaller than the safety margin.

We show that the proposed SDN countermeasure structure properly handles the MITM attack based on ARP spoofing in real time and guarantees the reliable operation of CBTC systems.

VI. Conclusion

In this paper, we have shown the possibility of cyber-physical attacks to the CBTC systems. By introducing wireless communication, the surface has become broader in the CBTC systems. We have carried out vulnerability analysis of the CBTC systems. Our analysis has shown that the MITM attack combined with knowledge of train signaling can cause train collisions. In order to detect the attack, we have also proposed a countermeasure structure for improving resiliency of the CBTC systems. The purpose of this structure is to have a host that is not exposed to the attacker using SDN. The unexposed host can issue an emergency stop command to OATP under the ARP spoofing attack. In order to validate our analysis, we have implemented a realistic CBTC testbed on top of a commercial train control and supervision software. Our empirical results have shown that the proposed countermeasure structure can effectively detect the attacks in real time.

References

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," *Comput. Commun.*, vol. 36, no. 1, pp. 1–7, 2012.
[2] K.-J. Park, J. Kim, H. Lim, and Y. Eun, "Robust path diversity for network quality of service in cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2204–2215, Nov. 2014.
[3] E. Bou-Harb, W. Lucia, N. Forti, S. Weerakkody, N. Ghani, and B. Sinopoli, "Cyber meets control: A novel federated approach for resilient CPS leveraging real cyber threat intelligence," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 198–204, May 2017.
[4] K.-D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, pp. 1287–1308, May 2012. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6176187
[5] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th Design Autom. Conf. (DAC)*, Anaheim, CA, USA, 2010, pp. 731–736.
[6] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.
[7] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Proc. Workshop Future Directions Cyber Phys. Syst. Security*, vol. 5, 2009. [Online]. Available: https://ptolemy.berkeley.edu/projects/chess/pubs/601.html
[8] A. Burg, A. Chattopadhyay, and K.-Y. Lam, "Wireless communication and security issues for cyber-physical systems and the Internet-of-Things," *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, 2018.
[9] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
[10] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.
[11] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid," in *Proc. 4th Int. Symp. ICS SCADA Cyber Security Res.*, 2016, pp. 53–63.
[12] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.
[13] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 20–23, Feb. 2015.
[14] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

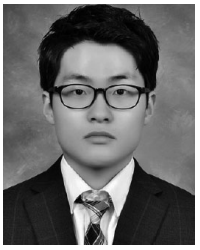
[15] R. D. Pascoe and T. N. Eichorn, "What is communication-based train control?" *IEEE Veh. Technol. Mag.*, vol. 4, no. 4, pp. 16–21, Dec. 2009.
[16] J. Farooq and J. Soler, "Radio communication for communications-based train control (CBTC): A tutorial and survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1377–1402, 3rd Quart., 2017.
[17] R. He *et al.*, "High-speed railway communications: From GSM-R to LTE-R," *IEEE Veh. Technol. Mag.*, vol. 11, no. 3, pp. 49–58, Sep. 2016.
[18] "Korean radio based train control system for urban rapid transit," Korea Railroad Res. Inst., Gyeonggi-do, South Korea, Rep. KRS SG 0069, 2015. [Online]. Available: https://krs.krri.re.kr/MultiViewer/ViewStartFrame.aspx?cid=72548&gubun=K&xSize=1890&ySize=930
[19] Y. Zhou and C. Mi, "Modeling train movement for moving-block railway network using cellular automata," *Comput. Model. Eng. Sci.*, vol. 83, no. 1, pp. 1–21, 2012.
[20] J.-C. Jong and S. Chang, "Algorithms for generating train speed profiles," *J. Eastern Asia Soc. Transport. Stud.*, vol. 6, pp. 356–371, Mar. 2005. [Online]. Available: http://easts.info/online/journal-of-easts/
[21] S. Oh, Y. Yoon, and Y. Kim, "Automatic train protection simulation for radio-based train control system," in *Proc. Int. Conf. Inf. Sci. Appl.*, 2012, pp. 1–4.
[22] "Operational concept for ERTMS," Rail Safety Stand. Board, London, U.K., Rep. RSSB-ERTMS-OC, 2014.
[23] W. Shangguan, X.-H. Yan, B.-G. Cai, and J. Wang, "Multiobjective optimization for train speed trajectory in CTCS high-speed railway with hybrid evolutionary algorithm," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 2215–2225, Aug. 2015.
[24] A. Fernández-Rodríguez, A. Fernández-Cardador, A. P. Cucala, M. Domínguez, and T. Gonsalves, "Design of robust and energy-efficient ATO speed profiles of metropolitan lines considering train load variations and delays," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 2061–2071, Aug. 2015.
[25] I. Lopez and M. Aguado, "Cyber security analysis of the European train control system," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 110–116, Oct. 2015.
[26] B. Chen *et al.*, "Security analysis of urban railway systems: The need for a cyber-physical perspective," in *Proc. Int. Conf. Comput. Safety Rel. Security*, 2014, pp. 277–290.
[27] Y. Wu, J. Weng, Z. Tang, X. Li, and R. H. Deng, "Vulnerabilities, attacks, and countermeasures in balise-based train control systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 4, pp. 814–823, Apr. 2017.
[28] S. Lakshminarayana *et al.*, "Signal jamming attacks against communication-based train control: Attack impact and countermeasure," in *Proc. 11th ACM Conf. Security Privacy Wireless Mobile Netw.*, Stockholm, Sweden, 2018, pp. 160–171.
[29] A. D. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*. Boca Raton, FL, USA: CRC Press, 2004, pp. 739–763.
[30] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016.
[31] N. Hubballi, S. Biswas, S. Roopa, R. Ratti, and S. Nandi, "LAN attack detection using discrete event systems," *ISA Trans.*, vol. 50, no. 1, pp. 119–130, 2011.
[32] NF Ettercap Dev Team, ALoR. (Jan. 2001). *Ettercap*. [Online]. Available: https://ettercap.github.io/ettercap/index.html
[33] Open Network Laboratory. (Dec. 2014). *ONOS*. [Online]. Available: https://wiki.onosproject.org/
[34] Linux Foundation. (Jul. 2009). *Open vSwitch*. [Online]. Available: http://openvswitch.org/

Sangjun Kim received the B.S. degree in electronics engineering from Pukyong National University, Busan, South Korea, in 2017. He is currently pursuing the Ph.D. degree with the Department of information and communication engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea.

His current research interests include cyber-physical systems and software-defined networking.

Yuchang Won received the B.E. degree in computer engineering from Gachon University, Seongnam, South Korea, in 2014 and the M.S. degree in information and communication engineering from Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea, in 2016.

His current research interests include cyber-physical-systems, railway control systems, networked control systems, smart production systems, and QoS or long-tail controls with control algorithms.



In-Hee Park received the B.S. degree in information and communication engineering from Chungbuk National University, Cheongju, South Korea, in 2016 and the M.S. degree in information and communication engineering from Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea, in 2018.

He is currently an Engineer with the Agency for Defense Development, Daejeon, South Korea. His current research interests include software-defined networking and resilient networks.

Yongsoon Eun (M'03) received the B.A. degree in mathematics, the B.S. and M.S.E. degrees in control and instrumentation engineering from Seoul National University, Seoul, South Korea, in 1992, 1994, and 1997, respectively, and the Ph.D. degree in electrical engineering and computer science from the University of Michigan, Ann Arbor, MI, USA, in 2003.

From 2003 to 2012, he was a Research Scientist with Xerox Innovation Group, Webster, NY, USA, where he researched several subsystem technologies in the xerographic marking process and image registration method in production inkjet printers. Since 2012, he has been an Associate Professor with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea. His current research interests include control systems with nonlinear sensors and actuators, geometric control of quadrotors, communication network, and resilient cyber-physical systems.

Kyung-Joon Park (M'05) received the B.S. and M.S. degrees in electrical engineering from the School of Electrical Engineering, Seoul National University, Seoul, South Korea, in 1998 and 2000, respectively, and the Ph.D. degree in electrical engineering and computer science from Seoul National University in 2005.

From 2005 to 2006, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. From 2006 to 2010, he was a Post-Doctoral Research Associate with the Department of Computer Science, University of Illinois at Urbana-Champaign, Champaign, IL, USA. He is currently an Associate Professor with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea. His current research interests include resilient cyber-physical systems and smart production systems.