An Attack-Resilient CPS Architecture for Hierarchical Control: A Case Study on Train Control Systems

Yuchang Won, Buyeon Yu, Jaegeun Park, and In-Hee Park, DGIST
Haegeon Jeong, Jeanseong Baik, and Kyungtae Kang, Hanyang University
Insup Lee, University of Pennsylvania
Sang Hyuk Son, Kyung-Joon Park, and Yongsoon Eun, DGIST

This article presents an attack-resilient architecture for cyber-physical systems (CPSs). As a case study, the authors build a radio-based train control testbed and validate the proposed resilient design architecture. The target CPS application is a hierarchical control system.

Cyber-physical systems (CPSs) are next-generation engineered systems that require tight integration of computing, communication, and control technologies to achieve the required performance level while satisfying such characteristics as stability, reliability, robustness, and resilience.[1–5] In particular, because many societal infrastructures are built in the framework of CPSs, resilience becomes critical in CPS design.[6,7] The term *resilience* implies systems that can tolerate a certain level of malicious external attacks or internal faults, secure core functions if full operation is not possible, and fail gracefully when inevitable.

In this article, we introduce an attack-resilient CPS architecture. Then, as a case study, we implement a train control testbed and empirically validate the proposed resilient architecture under various safety-critical scenarios. Attacks on passenger trains have occurred[8,9] and hence received attention.[10–12]

Digital Object Identifier 10.1109/MC.2018.2876054
Date of publication: 15 January 2019

0018-9162/18©2018IEEE

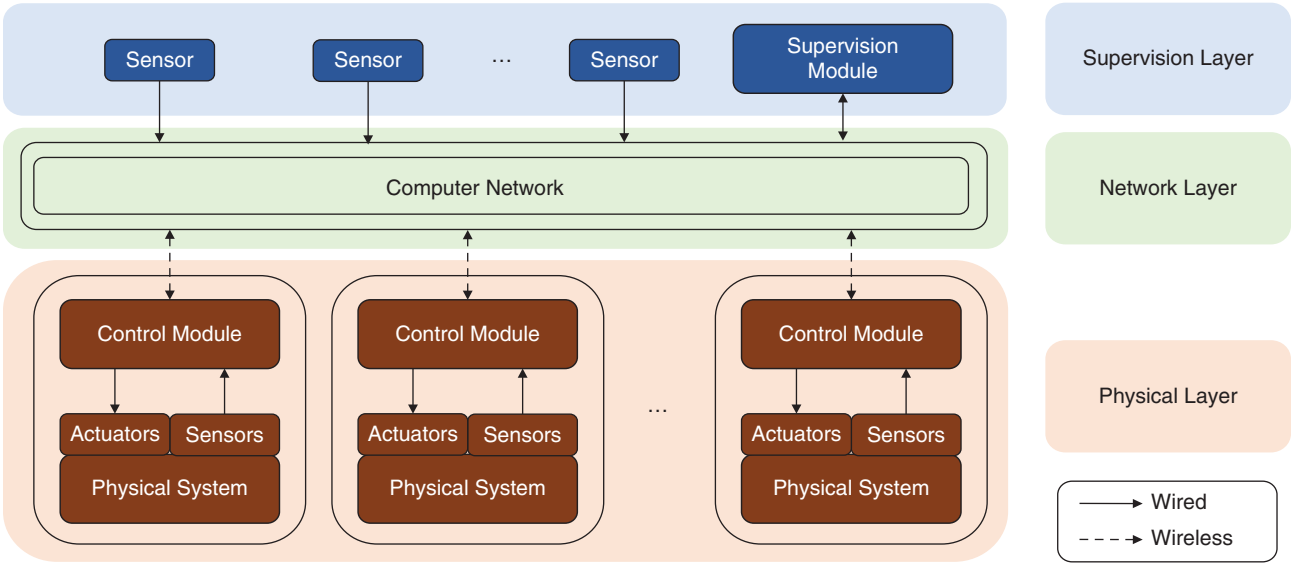


FIGURE 1. The conventional architecture for hierarchical control systems.

Our target CPS application is a hierarchical control system as shown in Figure 1, which consists of physical systems equipped with local embedded controllers, a supervision module that manages high-level operation of physical systems, and a computer network connecting physical systems to the supervision module. The hierarchical control architecture is prevalent in many CPS applications, including autonomous ground and aerial vehicles.

In particular, we design a resilient architecture for attacks on each component—that is, physical systems, embedded controllers, and network. For physical systems, we introduce an attack-detection algorithm that can tolerate sensor failure as long as one sensor remains intact. For embedded controllers, we propose a switching mechanism between high-performance (HP) and high-assurance (HA) modules upon detection of failure. For networks, we consider a software-defined networking (SDN) method for real-time recovery of networks.

We build a train control testbed to validate the proposed architecture under various safety-critical scenarios. Our testbed is based on a commercial train control and supervision software. In addition, the railway-installed sensors and other related mechanisms are implemented reflecting the actual train control and supervision system, whereas the train dynamics are computer simulated. Our empirical case study with the testbed validates the resilience of the proposed architecture under various attacks on sensors, embedded controllers, and networks.

RESILIENT CPS ARCHITECTURE

An attack-resilient architecture is proposed in this article for the purpose of increasing resiliency of the target CPS systems. The proposed architecture is illustrated in Figure 2, where several architectural changes are introduced to the basic architecture of the target CPS system in Figure 1. The changes introduced in the physical layer include software-based functional isolation capability with the use of hypervisors. This allows multiple operating systems (OSs) to be run in isolation from each other so that a level of resiliency is ensured in case of failure. Specifically, live migration of critical control algorithms from one OS to another may be enabled. Also included is a simplex structure[13] with an HA computing module to ensure graceful failure.

Multiple sensors are introduced in the physical systems and support algorithms for sensor attack detection and countermeasures. We also introduce SDN technology[14] in the network layer so that the layer has a level of intelligence and the means to detect and

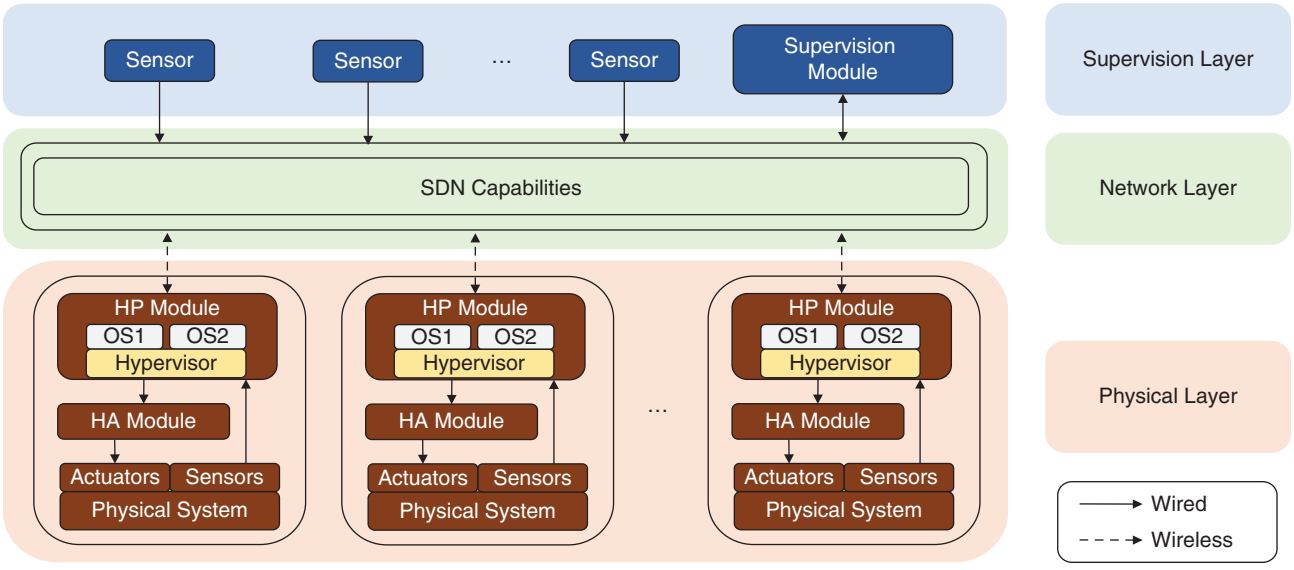


FIGURE 2. The resilient CPS architecture for hierarchical control systems.

recover from attacks or faults on the network.

Finally, although not explicitly shown in Figure 2, we can further implement a method in the supervision layer that monitors the operations of the entire system and provides online corrections to the SDN controller in the network layer and the embedded systems in the physical layer.

Software isolation in a CPS

A hypervisor provides multiple isolated virtual machines (VMs) and enables a VM to back up the functions of another VM that fails due to attacks or faults. The machine that hosts the hypervisor monitors the other VMs and initiates prepared countermeasures when it detects abnormal situations. A primary VM runs processes that operate each physical system, and a backup VM is prepared to receive primary processes, resuming when the primary VM is not available to proceed.[15]

Supporting graceful failure

Figure 2 shows that each embedded system controlling a physical plant includes separate HP and HA hardware modules. The HP module fulfills the task allotted to that system, and the HA module monitors the HP module. Normally, the HA module simply passes control-related data from the HP module to the physical system. If abnormal behavior is detected, the HA module isolates the HP module from the physical plant and directly controls that system to maintain a set of critical core tasks or fails safe.

Sensor-attack-resilient algorithms

Multiple sensors provide resilience against sensor attacks.[16,17] Existing methods to detect attacked sensors and algorithms to assess the state of the physical system in the presence of a sensor attack can be implemented in the HP module.

Most existing algorithms rely on principles similar to triple modular redundancy.[18,19] This implies that the number of attacked sensors the system can tolerate is, strictly, lower than the number of intact sensors. One notable distinction is found in Yu and Eun,[20] where a method is proposed for the system to correctly function as long as there is one sensor that is intact. The condition for the method to be applicable is that a dominant disturbance to the system is known a priori. Examples of such cases include a train control system where a dominant disturbance comes from the slope and curvature of the tracks and is known in advance. This algorithm is adopted in our radio-based train control testbed and will be explained later.

CPS with SDN capability

For network resiliency, we use SDN technology. SDN enables network anomaly detection by periodically collecting network statistics. In addition, SDN is capable of rerouting network traffic

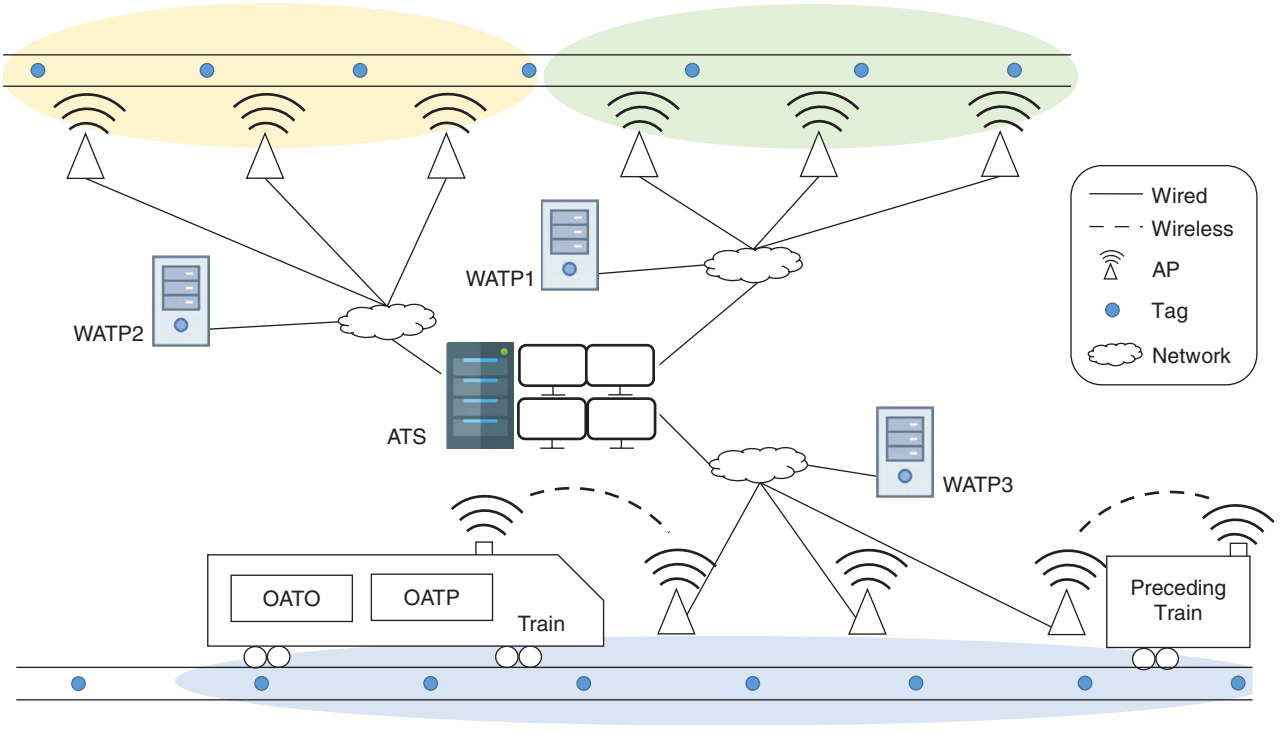


FIGURE 3. A communication-based train control system. AP: access point; WATP: wayside automatic train protection; OATO: onboard automatic train operation; OATP: onboard automatic train protection; ATS: automatic train supervision.

upon failure detection. Based on these SDN functions, we can implement real-time recovery of networks, which is critical for resilient CPSs.

Resiliency in the supervision layer

Detection of some malfunctions may be more straightforward if it takes place in the supervision layer rather than other layers. Examples include the case where messages from the supervision layer are corrupted while being delivered to modules in another layer. In this case, abnormal behaviors can be detected only at the supervision layer. The hot-patching technique can modify the functionality of processes without shutting down the system.[21] Upon detection of abnormal behavior, the supervision layer with the hot-patching technique can initiate patching of the algorithms being executed in the SDN controller, HP module, or HA module.

RADIO-BASED TRAIN CONTROL TESTBED

Train control and supervision

A metro nicely fits with the target CPS architecture of hierarchical control systems. Each train is equipped with an embedded feedback controller and operates by command of the central operation unit. Messages containing the locations of each train and commands from the central unit to each train are sent and received through a communication network.

Communication-based train control systems

Communication-based train control (CBTC) systems[22] use wireless communication technology to enable a real-time observation of train locations and improve the efficiency of transport by allowing shorter intertrain distances than conventional systems. For this reason, CBTC systems have recently been adopted in many countries.

However, CBTC systems are exposed to malicious threats more than conventional systems because of wireless communication. Therefore, we demonstrated the effect of malicious attacks and the resiliency of the proposed CPS architecture on our testbed of CBTC systems.

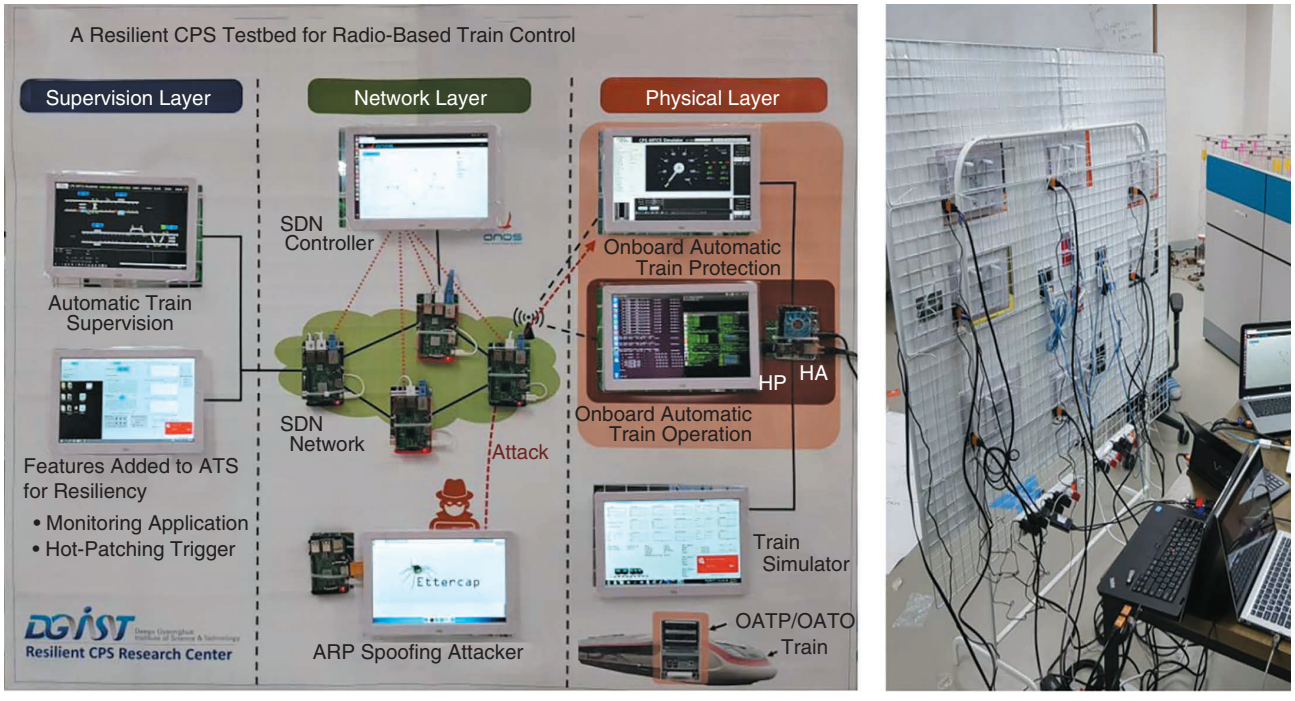
The operation of the CBTC system is illustrated in Figure 3, where system

components and interconnections are shown. Automatic train supervision (ATS) monitors the entire operation of the trains and, when safety protocols are violated, manually sends commands to wayside automatic train protection (WATP). There are many WATP units on the track. Each WATP oversees the train operation within a specified segment of the track (the shaded portion in Figure 3) and notifies the trains in the segment of the maximum velocity and distance they are allowed to travel. This information is received by the onboard automatic train protection (OATP) unit on each train. Then OATP calculates the velocity profile the train has to follow and sends it to onboard automatic train operation (OATO). Finally, OATO feedback controls the train using encoders and tag sensors. OATP also monitors whether the train operation respects the maximum velocity and allowed distance given by WATP. If not, OATP applies the emergency brake and stops the train. In addition, Figure 3 shows rails, trains, tags on the rail, and access points (APs) along the track. Wired and wireless communication between modules is also shown with solid and dotted lines, respectively.

Radio-based train control testbed implementation

The testbed implements most of the components in CBTC systems realistically. The ATS is implemented on a desktop PC with a Windows OS and commercial ATS software. Track information is taken from an actual line, which contains four stations. The WATP is also implemented on the same desktop computer, following closely the operation of actual systems. Communication between the two is emulated based on the Korean CBTC standard KRS-SG-0069.[23] In the testbed, only one WATP is included because a single WATP is enough to cover the track segment of four stations.

As shown in Figure 3, the hierarchical control system of a metro includes many trains. Each train is equipped with OATP and OATO. However, for the sake of simplicity, only one train in the testbed is implemented with the actual OATP and OATO following the proposed structure; the rest are implemented virtually.



(a) (b)

FIGURE 4. The radio-based train control system testbed. (a) The front view of the testbed. (b) Each monitor is connected with a laptop on the table behind. SDN: software-defined networking; ARP: Address Resolution Protocol.

The detailed train is constructed as follows. A single desktop implements both OATP and OATO. Some functions of OATO, for example, door control, are removed for simplification, and the motion control module is implemented on a separate laptop computer and an Odroid XU4. The laptop is installed with the Linux operating system, and it implements the HP module with a host machine running two kernel-based VMs. The Odroid XU4 takes the role of an HA module for graceful degradation. For the detailed train, the dynamics are simulated on another Windows-based desktop using a simulator, which receives motor and brake commands from OATO and returns the signals from the encoders and tag sensors. Three onboard encoders are included in the simulator, and attacks can be generated and applied to each of them. For the virtual trains, OATP and OATO are combined and simplified so that the train information is reported to ATS.

The network consists of a laptop with SDN controller and four Raspberry Pis with OpenvSwitch. OpenFlow 1.3 is used as an SDN protocol. One Raspberry Pi operates as a router and an AP, and the other three operate as routers to provide multiple paths between WATP and OATP.

The HP module contains sensor attack detection algorithms,[20] a live migration algorithm, and a hot-patching platform.[21] The SDN contains a countermeasure against link failovers. Figure 4 shows the whole testbed.

ATTACK RESILIENCY UNDER VARIOUS SAFETY-CRITICAL SCENARIOS

In this section, we validate the resiliency of the proposed architecture under various attacks that can result in the collision of two trains with the conventional architecture. Our evaluation scenario sufficiently captures all of the key operational aspects of the train control system. Performance evaluation with a full-scale scenario is a subject of future work. In our experimental study with the testbed, the train operation scenario shown in Figure 5 is as follows:

1) Train 0002 stops at Station B; the passengers enter and exit the train.
2) Train 0001 at Station A departs to Station B.
3) Due to a certain issue, Train 0002 is unable to depart from Station B.
4) After receiving the information on Station B from the WATP, Train 0001 lowers its speed to maintain the safety distance to Train 0002.

In this setting, we show the resiliency of the proposed architecture under various safety-critical attack scenarios.

Resiliency against encoder attack

Here, we consider the attack scenario where two of the three encoders are compromised. Specifically,

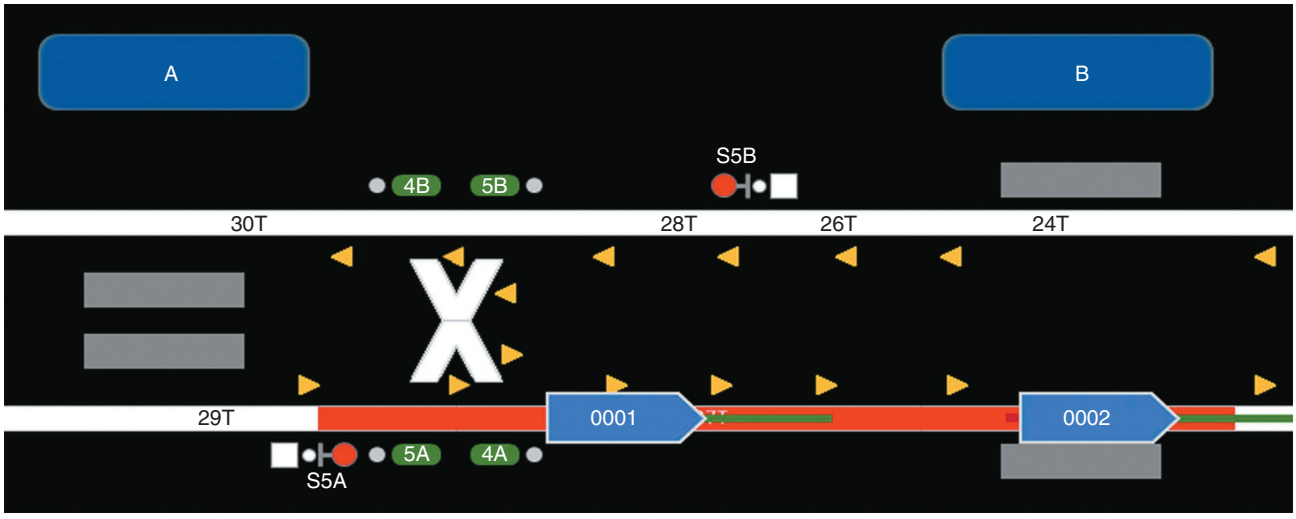


FIGURE 5. Station A, Station B, Train 0001, and Train 0002 displayed on the ATS screen.

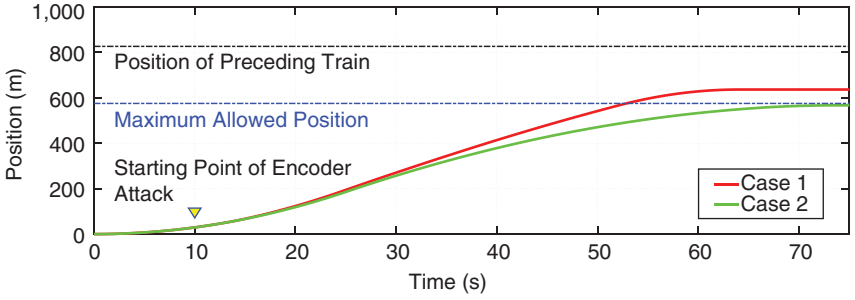


FIGURE 6. The positions of Train 0001 under encoder attack.

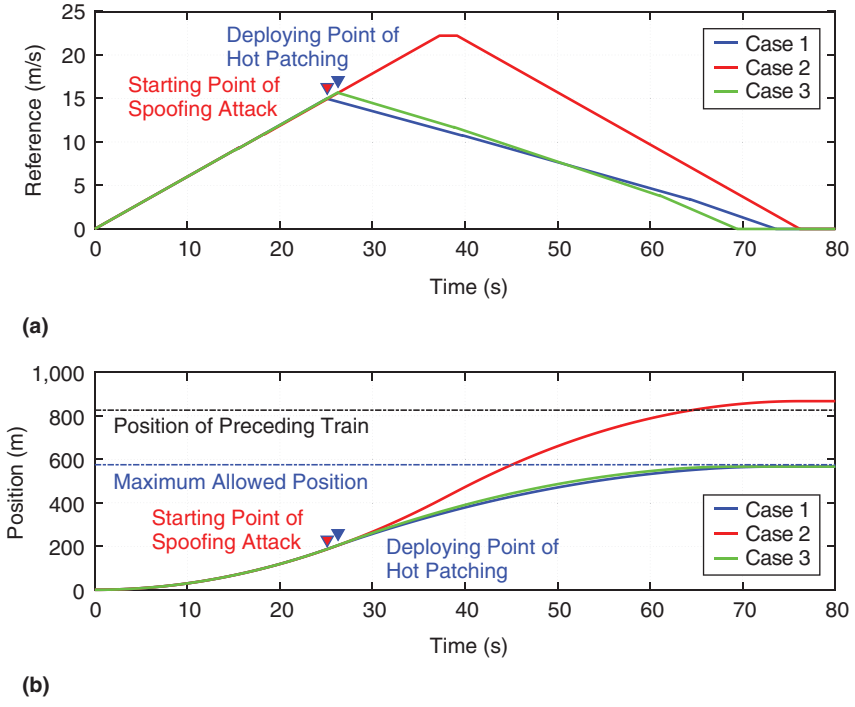


FIGURE 7. (a) The OATP velocity profiles and (b) the positions of Train 0001.

two encoders are attacked so that the velocity measurements from them are lower than actual train speed by 6 m/s. Figure 6 shows the movement of Train 0001 in two cases. First, the resiliency algorithm[16] that can tolerate a single sensor failure is included in the HP module. Second, the algorithm that can tolerate the failure of up to two sensors[20] is in the HP module. In the first case (solid red), Train 0001 violates the maximum allowed position set by WATP (shown by the blue dotted line). Nevertheless, no collision occurs because OATP applies an emergency brake. In the second case (solid green), Train 0001 does not violate the limit.

Resiliency against Address Resolution Protocol spoofing attack

We consider the scenario where the maximum allowed position sent from WATP to OATP is increased from 566 m to 866 m by an Address Resolution Protocol (ARP) spoofing attack.

We can provide resiliency against the ARP spoofing attack by two methods. First, we use hot patching of the communication protocol so that the altered packet is invalidated. In case of abnormal behavior, the ATS triggers the hot patching to change the communication protocol to the maximum allowed position sent from WATP to OATP. The other method is, upon detection, to reroute network traffic around the compromised node using SDN capability. SDN captures a suspicious connection, removes the compromised node from the network, and reroutes the data from WATP to OATP.

Figure 7(a) shows the velocity profile computed by OATP in the following three cases: Case 1 (blue) has no attack, Case 2 (red) is not under the ARP spoofing attack, and Case 3 (green) is under attack, but hot patching is deployed immediately. Clearly, the profile in Case 3 is similar to the one in Case 1, whereas Case 2 exhibits great deviation. Figure 7(b) shows the positions of Train 0001 in the three cases, respectively. Cases 1 and 3 operate normally, whereas Case 2 results in collision of the two trains. Unlike the encoder attack case, OATP cannot prevent the collision because the attack has introduced a deceptive maximum allowed travel position.

Resiliency against OATO failure

OATO may show abnormal behaviors due to system software errors or

hardware malfunctions. In this situation, the conventional CBTC system stops the train. However, in the proposed architecture, the HP module recovers from the software error by migrating the train control process to back up the VM.

Resiliency against network link failure

We implement a link failover algorithm that is based on the switch state information and changes the original path to the alternative one. Our experiment shows that the link can be restored within 30 ms, which is sufficient to deliver control information to the train control system in a resilient architecture.

In this article, we introduced a design method for resilient CPSs. In particular, we focused on the hierarchical control architecture that is prevalent in many CPS applications. To validate the proposed scheme, we built a radio-based train control testbed. Then, we verified the resiliency of the testbed under various safety-critical attack scenarios. For further validation, we are currently working on other applications, such as autonomous cars and drones.

ACKNOWLEDGMENTS

The three leading authors contributed equally on this article. Yongsoon Eun and Kyung-Joon Park are the corresponding authors. This work was partly supported by an Institute for Information and Communications Technology Promotion grant funded by the Korea government (Ministry of Science, Information and Communications Technology and Future Planning) (2014-0-00065, Resilient Cyber-Physical Systems Research) and partially supported by the Global Research Laboratory Program through the National Research Foundation of Korea (NRF-2013K1A1A2A02078326).

REFERENCES

1. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th Design Automation Conf. (DAC)*, 2010, pp. 731–736.
2. K.-D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, pp. 1287–1308, May 2012.
3. 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.
4. T. Sanislav, S. Zeadally, and G. D. Mois, "A cloud-integrated, multilayered, agent-based cyber-physical system architecture," *Computer*, vol. 50, no. 4, pp. 27–37, 2017.
5. H. A. Müller, "The rise of intelligent cyber-physical systems," *Computer*, vol. 50, no. 12, pp. 7–9, 2017.
6. 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, 2017.
7. 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, 2015.
8. G. Baker. (2008, Jan. 11). Schoolboy hacks into city's tram system. *Telegraph*. [Online]. Available: https://www.telegraph. co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html
9. E. Boyle. (2016, July 13). U.K. rail network attacked by hackers four times in a year. Independent. [Online]. Available: http://www.independent.co.uk/life-style/gadgets-and-tech/uk-rail-network-railways-hacked-four-times-hackers-trains-a7135026.html
10. Y. Wu, Z. Wei, J. Weng, and R. H. Deng, "Position manipulation attacks to balise-based train automatic stop control," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5287–5301, 2018.
11. P. Darlington. (2017, May 30). Hacking the railway. [Online]. Available: https://www.railengineer.uk/2017/05/30/hacking-the-railway/
12. B. Chen, C. Schmittner, Z. Ma, W. G. Temple, X. Dong, D. L. Jones, and W. H. Sanders, "Security analysis of urban railway systems: The need for a cyber-physical perspective," in *Proc. Int. Conf. Computer Safety, Reliability, and Security*, 2014, pp. 277–290.
13. L. Sha, "Using simplicity to control complexity," *IEEE Softw.*, vol. 18, no. 4, pp. 20–28, 2001.
14. B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *Commun. Surveys Tuts.*, vol. 99, no. 3, pp. 1–18, 2014.
15. S. Kashyap, C. Min, B. Lee, T. Kim, and P. Emelyanov, "Instant OS updates via userspace checkpoint-and-restart," in *Proc. 2016 USENIX Annu. Technical Conf. (USENIX ATC)*, pp. 605–619.
16. H. Jeon, S. Aum, H. Shim, and Y. Eun, "Resilient state estimation for control systems using multiple observers and median operation," *Math. Probl. Eng.*, vol. 2016. doi: http://dx.doi.org/10.1155/2016/3750264.
17. M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, "Design and implementation of

ABOUT THE AUTHORS

YUCHANG WON is a PhD candidate with the Department of Information and Communication Engineering, DGIST, Korea. His research interests include resilient cyber-physical systems, smart production systems, networked control systems, and quality-of-service or long-tail controls with control algorithms. Contact him at yuchang@dgist.ac.kr.

BUYEON YU is a PhD candidate with the Department of Information and Communication Engineering, DGIST, Korea. His research interests include control theory, resilient cyber-physical systems, and railway systems. Contact him at yubuyeon@dgist.ac.kr.

JAEGEUN PARK is a PhD candidate with the Department of Information and Communication Engineering, DGIST, Korea. His research interests include resilient control systems and metropolitan train systems. Contact him at jaegeun2@dgist.ac.kr.

IN-HEE PARK is an engineer with the Agency for Defense Development, Korea. His research interests include software-defined networking and resilient networks. Park received an MS in information and communication engineering from DGIST, Korea. Contact him at inhee@dgist.ac.kr.

HAEGEON JEONG is a unified master's and doctor's course student in the Division of Computer Science and Engineering, Hanyang University, Korea. His research interests include high reliability and resilient systems, memory management, and hot-patching technique. Contact him at haegeonj@hanyang.ac.kr.

JEANSEONG BAIK is a unified master's and doctor's course student in the Division of Computer Science and Engineering, Hanyang University, Korea. His research interests include fault tolerance in critical systems, process migration techniques, embedded operating systems, and resilient cyber-physical systems. Contact him at jsbaik@hanyang.ac.kr.

KYUNGTAE KANG is an associate professor with the Department of Computer Science and Engineering, Hanyang University, Korea. His research interests lie primarily in systems, such as operating, wireless, distributed, and real-time embedded systems, as well as interdisciplinary areas of cyber-physical systems. Kang received a PhD in electrical engineering and computer science from Seoul National University. He is a Member of the IEEE and ACM. Contact him at ktkang@hanyang.ac.kr.

INSUP LEE is the Cecilia Fitler Moore professor of computer and information science, codirector of Penn Health Tech, and director of the PRECISE Center at the University of Pennsylvania. His research interests include cyber-physical systems, real-time and embedded systems, runtime assurance, assurance cases, and connected health. Lee received a PhD from the University of Wisconsin–Madison. He is an ACM fellow and is a Fellow of the IEEE. Contact him at lee@cis.upenn.edu.

SANG HYUK SON is the president of DGIST, Korea. He received a PhD in computer science from the University of Maryland, College Park. He is a member of both the Korean Academy of Science and Technology and the National Academy of Engineering of Korea. He is a Fellow of the IEEE. Contact him at son@dgist.ac.kr.

KYUNG-JOON PARK is an associate professor in the Department of Information and Communication Engineering, DGIST, Korea. His research interests include resilient cyber-physical systems and smart production systems. Park received a PhD in electrical engineering and computer science from Seoul National University. He is a Member of the IEEE. Contact him at kjp@dgist.ac.kr.

YONGSOON EUN is a professor with the Department of Information and Communication Engineering, DGIST, Korea. His research interests include control systems with nonlinear sensors and actuators, geometric control of quadrotors, communication network, smart production systems, and resilient cyber-physical systems. Eun received a PhD in electrical engineering and computer science from the University of Michigan. He is a Member of IEEE. Contact him at yeun@dgist.ac.kr.

attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators," *IEEE Control Syst. Mag.*, vol. 37, no. 2, pp. 66–81, 2017.

18. R. E. Lyons and W. Vanderkulk, "The use of triple-modular redundancy to improve computer reliability," *IBM J. Res. Develop.*, vol. 6, no. 2, pp. 200–209, 1962.
19. P. M. Frank and X. Ding, "Survey of robust residual generation and evaluation methods in observer-based fault detection systems," *J. Process Control*, vol. 7, no. 6, pp. 403–424, 1997.
20. B. Yu and Y. Eun, "Sensor attack detection for railway vehicles using topographic information," in *Proc. 17th Int. Conf. Control, Automation and Systems (ICCAS)*, 2017, pp. 149–154.
21. H. Jeong, J. Baik, and K. Kang, "Functional level hot-patching platform for executable and linkable format binaries," in *Proc. IEEE Int. Conf. Systems, Man, and Cybernetics (SMC)*, 2017, pp. 489–494.
22. *IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements*, IEEE Standard 1474.1-2004.
23. Korean Radio Based Train Control System for Urban Rapid Transit. (2018). KRS-SG-0069 (in Korean). [Online]. Available: http://krs.krri.re.kr/MultiViewer/ViewStartFrame.aspx?cid=72548&gubun=K&xSize=1890&ySize=930