ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

SECURITY OF CYBER-PHYSICAL SYSTEMS DESIGN OF A SECURITY SUPERVISOR TO THWART ATTACKS

[1]P. MOUNIKA, [2]Y. GANAPATHI

[1](Assistant Professor), MSC, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM, ANDHRA PRADESH**

[2]MSC, scholar, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM, ANDHRA PRADESH**

Abstract

Cyber-physical systems (CPSs) integrate computing and communication capabilities to monitor and control physical processes. In order to do so, communication networks are commonly used to connect sensors, actuators, and controllers in the feedback system. The use of communication networks increases the vulnerability of CPSs to cyber attacks that can drive the system to unsafe states. One of the most powerful Cyber attacks is the so-called man-in-the-middle attack, where the intruder can observe, hide, create, or change information in the attacked network channels. In this article, we propose a defense strategy that can thwart man-in-the-middle attacks in the sensor and/or control communication channels of CPSs modeled as discrete-event systems. We also introduce the definition of network attack security (NA-Security), which is related to the possibility of preventing the system from reaching unsafe states by using a security supervisor, whose online implementation has polynomial computational complexity, and we propose an algorithm to verify this property.

Machine learning is an important component of the growing field of data science. Through the use of statistical methods, different type of algorithms is trained to make classifications or predictions, and to uncover key insights in this project. These insights subsequently drive decision making within applications and businesses, ideally impacting key growth metrics.

Machine learning algorithms build a model based on this project data, known as training data, in order to make predictions or decisions without being explicitly programmed to do so. Machine learning

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

algorithms are used in a wide variety of datasets, where it is difficult or unfeasible to develop conventional algorithms to perform the needed tasks.

1. INTRODUCTION

CYBER-PHYSICAL systems (CPSs) form the basis for the fourth industrial revolution, called Industry 4.0These kinds of systems integrate computing and communication capabilities to monitor and control physical processes [1]. In order to do so, communication networks are commonly used to connect sensors, actuators, and controllers in the feedback system. The increase in the use of communication networks for the control of systems increases its vulnerability to attacks in the network. Thus, it is important to implement defense strategies against cyber attacks in CPSs. The use of conventional network defenses, such as firewalls, is not recommended in industrial systems (and in some cases is not sufficient [2]) since these defenses introduce communication delays that may interfere in the implemented control logic. Thus, new defense strategies must be developed to thwart attacks in industrial networked control systems.

CPSs can be modeled by using different levels of abstraction. In this article, we focus on the control of the logical behavior of the system described by the sequences of events that it can execute, and thus, the plant is modeled as a discrete event system (DES) [3]. In this case, the control of the system behavior is carried out by a supervisor that is capable of disabling events of the plant to satisfy a set of specifications. We assume that the supervisor has already been designed and is implemented in the system.

There are several types of network attacks, as shown in [4]. A well-known type of attack in communication networks is the so-called man-in-the-middle attack [5]. In this type of attack, the intruder can observe, hide, create, or even change information that transits from one device to another in a communication channel. Thus, once the intruder has attacked a sensor and/or a control communication channel in a supervisory control system, it can lead the plant to execute a sequence with the objective to reach an unsafe state, i.e., a state that represents a risk to the plant or its operators.

EXISTING SYSTEM:

There are several types of network attacks, as shown in [4]. A well-known type of attack in communication networks is the so-called man-in-the-middle attack [5]. In this type of attack, the intruder can observe, hide, create, or even change information that transits from one device to another in a communication channel. Thus, once the

intruder has attacked a sensor and/or a control communication channel in a supervisory control system, it can lead the plant to execute a sequence with the objective to reach an unsafe state, i.e., a state that represents a risk to the plant or its operators.

Several works in the literature propose strategies to cope with cyberattacks considering different approaches [6]–[21]. In the context of DES, methods for the detection and mitigation of cyberattacks has been proposed [8]–[14], as well as methods for misleading an outside observer in order to hide a secret system behavior, referred in the literature to as opacity [15]–[21].

There are some works in the literature that deal with attack detection in the context of DESs [11], [13], [14], [22], where in [13], [14], and [22], the system is modeled as an automaton. In [13], the problem of intrusion detection in supervisory control systems, where the attacker has the ability to enable vulnerable actuator events that are disabled by the supervisor and to change sensor readings, is addressed. A mathematical model for the system under such actuator and sensor attacks is obtained. A defense strategy, based on diagnosers, that detects attacks online and disables all controllable events of the system after the attack has been detected is proposed. In [14], a method to thwart man-in-the-middle attacks in both sensor and actuator channels is presented. Differently from [13], where all controllable events are disabled when the attack is detected, in [14], all controllable events are disabled only if the system may reach an unsafstate. This defense strategy does not restrict the system behavior if the attack cannot cause damages to the system.

Recently, in [23], two notions of network attack security (NA-Security) for DESs, called detectable NA-Security and undetectable NA-Security, associated with the capability of disabling some controllable events to prevent the system from reaching unsafe states, are presented. Based on these notions, a security module to prevent the reach of unsafe states, without altering the non attacked language of the system, is proposed.

PROPOSED SYSTEM:

The proposed security supervisor disables only those controllable events that lead the system to an imminent risk scenario. In addition, the proposed security supervisor, in some cases, can prevent the system from reaching unsafe states even without the attack detection, i.e., the method proposed in this article can also be used to protect the system against stealthy

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

attacks [10], [22]. This strategy is less restrictive than the one proposed in [14], in the sense that the system behavior may execute more sequences after an attack, without reaching unsafe states. Thus, the system may execute safe sequences while the threat is eliminated or, eventually, the system returns to its non attacked closed-loop behavior after the actuation of the security supervisor.

We also introduce in this article a class of systems, called NA-Secure Systems, for which a security supervisor, that thwarts attacks in the network without altering the non attacked closed-loop behavior, can be computed in polynomial time. A polynomial-time algorithm to verify the NA-Security property is proposed. It is important to remark that the security supervisor proposed in this article is an improvement of the module presented in [23] since, in this article, we propose a security supervisor that does not interfere with the non attacked closed-loop system and is also maximally permissive.

3. MODULES

service provider:

in this module, the service provider has to login by using valid user name and password. after login successful he can do some operations such aslogin, browse datasets and train & test data sets, view trained and tested accuracy in bar chart, view trained and tested accuracy results, view prediction of attack status, view attack status ratio, download predicted data sets, view attack detection ratio results, view all remote users.

view and authorize users:

in this module, the admin can view the list of users who all registered. in this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

remote user:

in this module, there are n numbers of users are present. user should register before doing any operations. once user registers, their details will be stored to the database. after registration successful, he has to login by using authorized user name and password. once login is successful user will do some operations like register and login, predict attack status, view your profile.

4. SCREEN SHOTS

Cyber security login

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

Cyber security register:

View all remote users:

View thwart attack detect prediction type ratio details:

View thwart attack detect prediction type details:

5. CONCLUSION

In this article, we propose a defense strategy to thwart man-in-the-middle attacks in CPSs, by using the framework of DESs. We present a model for systems subject to man in- the-middle attacks and formalize the class of ANSs that are NA-Secure, which is associated with the existence of a solution to the MPSP. If the system is NA-Secure, then the security supervisor proposed in this article disables the occurrence of events only on a possible

imminent risk scenario, and it does not affect the non attacked closed-loop system behavior. We also propose an algorithm to verify the NA-Security property.

In contrast to the approaches for MPRCP, which have exponential complexity with respect to the number of states and events of the system, the approach proposed in this article is polynomial with respect to the number of states and linear with respect to the number of events of the system.

An extension of this work would be to consider the case when the system is not NA-Secure. In this case, it may be necessary o restrict the closed-loop behavior to guarantee that the system does not reach unsafe states. By doing so, the closed-loop system may block. Thus, a future research topic is to design a security supervisor that prevents the system from reaching blocking states and unsafe states.

6. REFERENCES

[1] C. Hildebrandt *et al.*, "Ontology building for cyber–physical systems: Application in the manufacturing domain," *IEEE Trans. utomat. Sci. Eng.*, vol. 17, no. 3, pp. 1266–1282, Jul. 2020, doi: 10.1109/TASE.2020.2991777.

[2] F. Zhang, H. A. D. E. Kodituwakku, W. Hines, and J. B. Coble, "Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4362–4369, Jul. 2019.

[3] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. New York, NY, USA: Springer, 2008.

[4] V. Kumar, J. Srivastava, and A. Lazarevic, *Managing Cyber Threats: Issues, Approaches, and Challenges*. Boston, MA, USA: Springer, 2005.

[5] D. Comer, *Computer Networks and Internets*. Upper Saddle River, NJ, USA: Prentice-Hall, 2009.

[6] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.

[7] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[8] D. Thorsley and D. Teneketzis, "Intrusion detection in controlled discrete event systems," in *Proc. 45th IEEE Conf. Decis. Control*, San Diego, CA, USA, Dec. 2006, pp. 6047–6054.

[9] Q. Zhang, Z. Li, C. Seatzu, and A. Giua, "Stealthy attacks for partially-observed discrete event systems," in *Proc. IEEE 23rd Int. Conf. Emerg. Technol. Factory Autom.*

(ETFA), vol. 1, Turin, Italy, Sep. 2018, pp. 1161–1164.

[10] R. M. Goes, E. Kang, R. Kwong, and S. Lafortune, "Stealthy deception attacks for cyber-physical systems," in *Proc. IEEE 56th Annu. Conf. Decis. Control (CDC)*, Melbourne, VIC, Australia, Dec. 2017, pp. 4224–4230.

[11] R. Fritz and P. Zhang, "Modeling and detection of cyber attacks on discrete event systems," *IFAC-PapersOnLine*, vol. 51, no. 7, pp. 285–290, 2018.

[12] R. Su, "Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations," *Automatica*, vol. 94, pp. 35–44, Aug. 2018.

[13] L. K. Carvalho, Y.-C. Wu, R. Kwong, and S. Lafortune, "Detection and mitigation of classes of attacks in supervisory control systems," *Automatica*, vol. 97, pp. 121–133, Nov. 2018.

[14] P. M. Lima, M. V. S. Alves, L.K. Carvalho, andM. V. Moreira, "Security against communication network attacks of cyber-physical systems," *J. Control, Autom. Electr. Syst.*, vol. 30, no. 1, pp. 125–135, Feb. 2019.

[15] R. Jacob, J.-J. Lesage, and J.-M. Faure, "Overview of discrete event systems opacity: Models, validation, and quantification," *Annu. Rev. Control*, vol. 41, pp. 135–146, 2016.