http://doi.org/10.24867/JPE-2019-02-035

Journal of Production Engineering

Vol.22 No.2

JPE (2019) Vol.22 (2) Preliminary Note

Mitrovic, S., Dimic, Z., Jakovljevic, Z.

DISTRIBUTED CONTROL OF MANUFACTURING RESOURCES – SECURITY RELATED ISSUES

Received: 11 December 2018 / Accepted: 22 March 2019

Abstract: *Industry 4.0 paradigm dictates highly efficient and flexible production through introduction of reconfigurable manufacturing systems and resources characterized by modularity, interoperability, scalability and communication capabilities. Various approaches are currently researched worldwide in an effort to achieve the next level of production technologies without compromising the production itself. Considered approaches imply implementation of Cyber Physical Systems, Internet of Things and generation of manufacturing systems Digital Twins. Complex industrial control systems, which were traditionally wired and considered safe, are now becoming distributed, internet-connected, usually based on wireless communication and wide open for all kinds of malicious exploits with potentially fatal consequences. This paper presents a review of security related issues that are crucial in developing safer wireless distributed control of manufacturing resources, adept for challenges in coming times.*
Key words: *Industry 4.0, distributed control systems, manufacturing cyber security, Internet of Things.*

Distribuirana kontrola proizvodnjih sredstava - pitanja vezana za sigurnost. *Paradigma industrije 4.0 diktira visoko efikasnu i fleksibilnu proizvodnju uvođenjem konfigurabilnih proizvodnih sistema i resursa koji odlikuju modularnost, interoperabilnost, skalabilnost i mogućnosti komunikacije. Trenutno se širom sveta istražuju različiti pristupi u nastojanju da se dostigne sledeći nivo proizvodnih tehnologija bez ugrožavanja same proizvodnje. Razmatrani pristupi podrazumevaju implementaciju Ciber Phisical Sistem-a, Interneta stvari i generacije proizvodnih sistema Digital Tvins. Složeni industrijski upravljački sistemi, koji su tradicionalno ožičeni i smatraju se sigurnim, sada postaju distribuirani, povezani na internet, obično se zasnivaju na bežičnoj komunikaciji i širom su otvoreni za sve vrste zlonamjernih podviga s potencijalno fatalnim posledicama. U ovom radu predstavljen je pregled bezbednosnih pitanja koja su ključna za razvoj sigurnije bežične distribucije kontrole proizvodnih resursa, pogodnih za izazove u narednim vremenima.*
Ključne reči: *Industrija 4.0, distribuirani kontrolni sistemi, proizvodnja ciber sigurnosti, Internet of Things.*

1. INTRODUCTION

Rapid advancement and broad deployment of information and communication technologies (ICT) is radically changing the world of today. Miniaturized, multipurpose, high performance electronic networked devices are becoming ubiquitous and indispensable in all segments of modern society, including the industry. Under the influence of ever growing market demands, in an attempt to further boost quality of the goods and shorten response time, production companies are evolving, maintaining competitiveness by steadily embracing new production paradigms based on coming technologies – Internet of Things (IoT) [1] and Cyber-Physical Systems (CPS) [2].

Introduction of the IoT and services into the manufacturing environment represents a base for fourth industrial revolution – Industry 4.0 [3]. It is expected that smart factories will be able to meet requirements of each individual customer, including one-off items. IoT and, consequently, CPS are perceived as innovative, disruptive technologies, with horizontal and vertical digital integration possibilities based on pervasive deployment and networking of smart objects [4]. Such a vast and complex network poses many challenges, among which security and reliability are of the highest priority. Cyber threats are already formidable for every mission-critical system (power and water distribution, production, waste management etc.).

This paper aims to review several security related issues, in particular cyberattacks whose modeling is of high priority for generation of secure wireless distributed control of manufacturing resources. Due to the difference in system's control and modeling approaches, we will consider possible attacks in continuous time and discrete event systems separately. The remainder of the paper is structured as follows. In Section 2, distributed control systems and potential attack variants are discussed. Section 3 presents deception attacks in continuous time systems while Section 4 deals with attacks in discrete event systems. Finally, in Section 5, we give some concluding remarks along with guidelines regarding future work.

2. DISTRIBUTED CONTROL SYSTEMS AND ATTACKS

IoT and CPS implementation, through utilization of smart devices with integrated computation and communication capabilities, bring about significant changes in manufacturing systems and resources control. Although all functional elements of five-level automation hierarchy will remain, strict automation pyramid gives the way to distributed control systems. In

Note: The manuscript was presented at the 13. International Scientific Conference MMA held in Novi Sad, Serbia, 28.-29. September, 2018.

distributed control, instead of controlling manufacturing system or resources centrally, the control is carried out through communication and interoperation of different smart devices (Fig. 1). As CPS based and communication intensive, distributed control systems are inherently prone to different kinds of cyberattacks. In addition, since, as expected [3], a significant part of communication will be wireless, security issues become even more severe.

Although all components of the system (sensors, actuators, etc.) may be subject of an attack in a cyber or physical domain, targeting them individually or in a combined manner, in this paper we will focus on the attacks carried out through communication channels.

During communication between different agents in distributed control system, confidentiality, integrity and availability of the data must be preserved at all times.

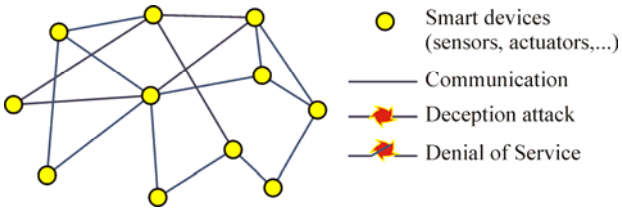

Fig. 1. Distributed control system and types of attack.

Confidentiality allows only the party with proper access rights to read the data, while integrity guarantees that the received data is genuine and no unauthorized changes were made. Availability enables access to data and system resources within the required time frame. Depending on the type of attack, adversaries aim to change some or all of the listed data properties.

In general, malicious cyberattacks can be split into two basic groups – Denial of Service (DoS) and deception attacks. DoS attacks compromise the availability of data, making the data or the requested resource permanently of temporarily inaccessible causing data loss or data delay. DoS attacks are disruptive, do not require knowledge about the attacked system and are not stealthy, but can be misdiagnosed, typically as network connection issues [5].

Deception attacks compromise data integrity and send corrupted data to the system components, thus altering behavior of the system. Deception attacks are more sophisticated than DoS attacks, require more resources and can be carried out in a number of ways.

Depending on the attack scenario, resources required for the successful attack vary. In order to compromise a control system, the adversary may need *a priori* system model, disclosure resources and/or disruption resources [6]. *A priori* system model represents an indispensable weapon for generation of stealthy attack; once the adversary gets the correct *a priori* system model, it is able to generate sophisticated attacks that security system cannot easily recognize. Nevertheless, if *a priori* system model is not available, disclosure resources can be utilized to violate data confidentiality and enable the adversary to obtain sensitive information about the targeted system, e.g. sensor readings and control signals. Data gathering and unauthorized system identification represents an attack *per se*, called Cyber Physical Intelligence attack [7]. Identified system model alone or in combination with *a priori* model represents a basis for generation of attacks. Finally, disruption resources work online, affect the communication operation and carry out active component of the attack.

3. DECEPTION ATTACKS IN CONTINUOUS TIME SYSTEMS

Application of smart sensors and actuators in continuous time systems can be regarded as networked control system (NCS) in which the loop between physical plant and controller is closed over communication network (Fig. 2) [7]. Physical plant can be described using linear stationary continuous time system [8]:

$$\begin{aligned} \dot{x}(t) &= \mathbf{A}x(t) + \mathbf{B}u(t) \\ y(t) &= \mathbf{C}x(t) + \mathbf{D}u(t) \end{aligned} \tag{1}$$

where $\mathbf{x} \in \mathbf{R}^n$ represents the state vector, $\mathbf{u} \in \mathbf{R}^m$ the control input vector, $\mathbf{y} \in \mathbf{R}^p$ the vector of measured output signal (Fig. 2) and **A**, **B**, **C**, and **D** are matrices with appropriate dimensions. In NCS, using feedback and forward communication lines, $\mathbf{y}(t)$ and $\mathbf{u}(t)$ are transmitted between plant and controller as complete time series. In deception attack, adversaries change $\mathbf{y}(t)$ and $\mathbf{u}(t)$ by injecting false data $\mathbf{y}^*(t)$ and $\mathbf{u}^*(t)$ based on available Cyber Physical Intelligence. Depending on the applied procedures for ensuring the stealthiness of $\mathbf{y}^*(t)$ and $\mathbf{u}^*(t)$ injection, there exist different types of deception attacks, and some of them will be shortly explained in the sequel.

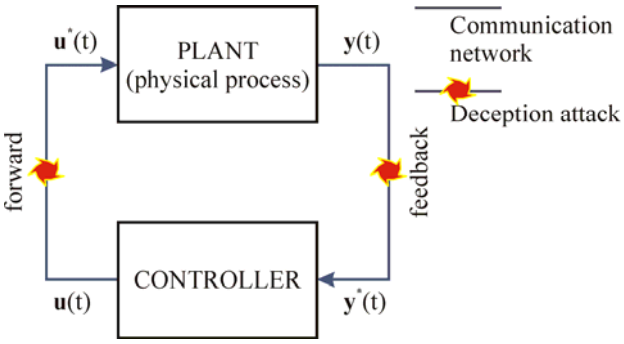

Fig. 2. Model of a continuous time system.

Replay attack [9] is a type of deception attack that records $\mathbf{y}(t)$ and $\mathbf{u}(t)$ time series for a certain time period and replays them in another period as $\mathbf{y}^*(t)$ and $\mathbf{u}^*(t)$ to attack the system. Evidently, preceding the actual replay attack, there is a Cyber Physical Intelligence attack, which is used to record as much relevant data from the system as possible. After some time, recorded data is replayed and presented to the system.

Attacks that are even more malicious eavesdrop data on communication lines and change them online according to the desired effect. For example, bias attack [6] adds the following signal to the communicated data

$$a_{k+1} = \beta a_k + (1-\beta)a_\infty \tag{2}$$

where a_0=0, a_∞ and β are coefficients that can be optimized [6] to get the desired effect and ensure stealthiness. An example of the effect of bias attack on

insertion force signal during Peg-in-Hole part making is presented in Fig. 3.

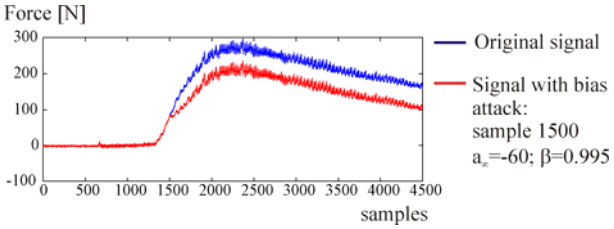

Fig. 3. Bias attack on insertion force signal during Peg-in-Hole part making.

Zero-dynamics attack [6, 10] is a very sophisticated deception attack requiring perfect knowledge of the plant dynamics represented through its *a priori* model. It is based on the open-loop predictions of the output changes due to the attack and it does not necessitate system identification through Cyber Physical Intelligence attack. Zero-dynamics attack targets global or local unstable zeros of control system transfer functions, aiming to shift the system into unsafe state, causing geometrical growth of the attack and great damage to the physical process. However, if the zeros of the system are stable, the attack will asymptotically decay to zero with little effect on the physical process.

Covert attacks [7, 11] are one of the most complex and sophisticated deception attacks that can covertly appropriate the control of the physical process to the adversary, while remaining undetected by the original controller and the security system. Complete knowledge of the system model is necessary and it is assumed that the adversary can eavesdrop and modify both, the sensing and actuation signals [11]. The adversary, in this case covert agent, connects between forward and feedback lines in parallel with the controller. Based on eavesdropped $\mathbf{y}(t)$ and $\mathbf{u}(t)$ signals, and utilizing plant model, it generates $\mathbf{y}^*(t)$ and $\mathbf{u}^*(t)$ in such a way to get desired performance of the plant.

4. ATTACKS IN DISCRETE EVENT SYSTEMS

Discrete event systems (DES) represent dynamic systems that change their state in discrete time instants, with typically irregular intervals according to the occurrence of instantaneous events. In DES, instead of communicating sensory signals change in time, the nodes in control network communicate the information about certain events represented by symbols defined by upper levels of communication protocols.

Supervisory control theory (SCT) [12, 13], that is based on logical DES model generated using formal languages and its formalisms, can be readily employed for modeling cyberattacks in DES [14]. Within SCT [12], the finite set of events' labels that cause state transitions in DES, represents an alphabet Σ, while Σ^* (where * denotes Kleene star) represents a set of all strings on Σ including empty string ε. Within Σ^*, a language L ($L \subseteq \Sigma^*$) that contains all admissible, i.e., physically possible, event strings in DES can be identified. The behavior of DES is modeled as a prefix closed language $L=\overline{L}$ where [12]:

$$\overline{L} = \left\{ u \in \Sigma^* \middle| u \le v \text{ for some } v \in L \right\} \tag{3}$$

and $u \le v$ denotes that u represents a prefix of v, i.e., $v=uw$ for some $w \in \Sigma^*$. The events alphabet Σ can be partitioned into two subsets ($\Sigma=\Sigma_c \cup \Sigma_u$) representing (i) Σ_c – set of controllable events that can be disabled at any time, and (ii) Σ_u – set of uncontrollable events that the agent cannot influence.

In the case of distributed control systems, each node in control network can observe only a part of events that occur within the system as a whole; these events represent an observation alphabet Σ_o, defined by [12]:

$$P(\sigma) = \begin{cases} \sigma, \text{if } \sigma \in \Sigma_o \\ \varepsilon, \text{if } \sigma \notin \Sigma_o \end{cases} \tag{4}$$

Projection from (4) represents a natural projection (mask) that can be extended to the strings as follows:

$$P(s\sigma) = P(s)P(\sigma), \text{for } s \in \Sigma^*, \sigma \in \Sigma \tag{5}$$

In DES, attacks can be introduced by removing, inserting or replacing symbols in observation strings. As shown in [14], the attack can be modeled as $A : \Sigma_o^* \to 2^{\Sigma_o^*}$ that maps original string $w \in \Sigma_o{}^*$ into a set of corrupted strings. Since, in general, attack is neither unique nor deterministic, the mapping A represents a set valued function, i.e., $A(w)$ is a set of corrupted strings [14]; eventually, the node will receive only one string $y \in A(w)$, for which it also holds that $y \in \Sigma_o{}^*$. Note that $y \notin \Sigma_o{}^*$ represents an attack that can be easily detected and it is not covered by mapping A.

It should be emphasized that the attack that represents a removal of a symbol represents a natural projection given in (4) and (5). The masks that model symbol insertion and replacement do not represent natural projection, but in these cases, relation (5) holds.

Example: In this example, we will consider 2 DoF pneumatic "pick and place" manipulator that is made of three intelligent pneumatic cylinders (C1, C2 and C3); C1 and C2 realize linear DoF while C3 represents a gripper. Each cylinder represents a CPS by itself and it has integrated microcontroller with computation and communication capabilities, employed for cylinder control. In addition, each cylinder is equipped with 5/2 monostable dual control valve and two limit switches for detection of final advanced and retracted position. Cylinder microcontrollers represent network nodes and manipulator control system is distributed over them [14]. Manipulator moves a part between two positions, (Fig. 4) performing the following sequence:

$$C2+C3+C2-C1+C2+C3-C2-C1- \tag{6}$$

During manipulator's regular operation, the events presented in Table 1 occur and can be detected by cylinder nodes as rising and falling edges of corresponding limit switches' signals; controllable events are denoted by capital, and uncontrollable by lower letters. The sequence from relation (6) can be represented as the following sequence of events:

$$CdEfDcAbCdFeDcBa \tag{7}$$

For proper functioning of the manipulator, in addition to the events locally detected by nodes (Table

1), it is necessary to communicate certain events between them [14]. In this way, each node i, i = 1, 2, 3 has its own observation alphabet Σ_{oi}: $\Sigma_{o1} = \{a, A, b, B, c\}$, $\Sigma_{o2} = \{c, C, d, D, a, b, e, f\}$, $\Sigma_{o3} = \{e, E, f, F, d\}$ obtained from the whole system observation alphabet $\Sigma_o = \{a, A, b, B, c, C, d, D, e, E, f, F\}$ by applying natural projections P_i as defined in relation (4).

Note that the events communicated between nodes are obtained during control system generation, considering that C1 changes position always after C2 reaches retracted position, C3 changes position after C2 reaches advanced position, while the control of C2 is more complex and requires signals from both, C1 and C3 [15], as can be observed from (6).

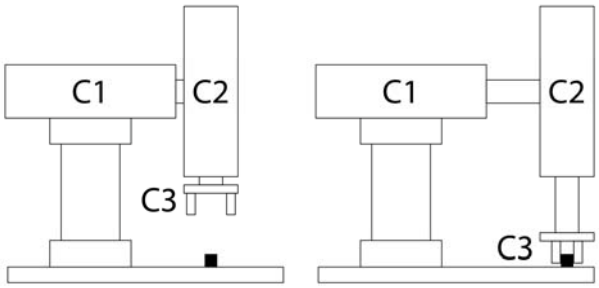

Fig. 4. Pneumatic manipulator – left: position I, right: position II.

Description of event per cylinder	C1 symbol	C2 symbol	C3 symbol
Reaches retracted position	a	c	e
Starts advancing	A	C	E
Reaches advanced position	b	d	f
Starts retracting	B	D	F

Table 1. Events during manipulator's regular operation.

As an example, we will consider two attacks on communication between C2 and C3. Attack A_1 represents an occasional removal of symbol d from the sequence of symbols observed by C3, represented by the following mask:

$$A_1(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \Sigma_{o3} / \{d\} \\ \{\varepsilon, d\}, & \text{if } \sigma = d \end{cases} \quad (8)$$

Attack A_2, on the other hand, represents insertion of symbols $\{e, f\}$ in communication of events from C3 to C2 and it affects symbols observed by C2 as follows:

$$A_2(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \Sigma_{o3} / \{d\} \\ \{e, f\}, & \text{if } \sigma = \varepsilon \end{cases} \quad (9)$$

Attack A_1 would affect the functioning of gripper as the occurrence of this attack would prevent start of gripping or releasing operation. Nevertheless, the consequences of this attack alone would not be catastrophic since, after this attack, the system would stop functioning, waiting for the events e or f from C3. However, the consequences of attack A_2 can be far more serious. If this attack occurs after cylinder C2 reaches advanced position and before C3 performs gripping/releasing, it can lead: (i) to an inappropriate gripping of the part; (ii) to the movement of manipulator from position I to position II without part in the gripper; (iii) to the release of part in an arbitrary position during motion of manipulator from position II to position I. Which of the considered scenarios would emerge depends on the moment of attack occurrence and the time necessary for gripping/releasing and retracting of C2. The combination of attacks A_1 and A_2 can give even worse consequences represented through completely stochastic motion of cylinders.

5. CONCLUSION

Implementation of IoT and CPS in manufacturing systems leads to the distribution of control tasks and high level reliance on communication network. This inevitably brings about increased vulnerability of the control systems to cyberattacks. In this paper, we have reviewed several attack scenarios and potential hazards that they pose against distributed control systems in continuous time and discrete event control. In an attempt to illustrate negative effects that a real attack can have unless properly neutralized, an example was given, where a combination of DoS and deception attacks were targeting discrete event system. Future work will consider methods that are suitable for securing CPS-based distributed discrete event systems.

6. REFERENCES

[1] Atzori, L., Iera, A., Morabito, G.: *The Internet of Things: A survey,* Computer Networks, vol. 54, no. 15, pp. 2787-2805, 2010.

[2] Lee, G. M., Crespi, N., Choi, J. K., Boussard, M.: *Internet of Things*, Evolution of Telecommunication Services, pp. 257-282, Springer, Berlin, Heidelberg, 2013.

[3] ACATECH: *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*, April 2013.

[4] Kopetz, H.: *Internet of Things*, Real-Time Systems, Springer, Boston, MA, pp. 307-323, 2011. DOI: 10.1007/978-1-4419-8237-7_13

[5] Amin S., Cárdenas A.A., Sastry S.S.: *Safe and Secure Networked Control Systems under Denial-of-Service Attacks, Hybrid Systems: Computation and Control, Lecture* Notes in Computer Science, vol. 5469, pp. 31-45, Springer, Berlin, 2009.

[6] Teixeira, A., Shames, I., Sandberg, H., Johansson, K.H.: *A Secure Control Framework for Resource-Limited Adversaries,* Automatica, vol. 51, pp. 135-148, 2015.

[7] De Sá, A.O., Carmo, L.F.R.d.C., Machado, R.C.S.: *Covert Attacks in Cyber-Physical Control Systems*, IEEE Transactions on Industrial Informatics, vol. 13, no. 4, pp. 1641-1651, Aug. 2017.

[8] Pasqualetti, F., Dorfler, F., Bullo, F.: *Attack detection and identification in cyber-physical systems*, IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715-2729, Nov. 2013.

[9] Mo, Y., Sinopoli, B.: *Secure control against replay attacks*, 47th Annual Allerton Conference on Communication, Control, and Computing, pp. 911-918, 2009.

[10] Hoehn, A., Zhang, P.: *Detection of Covert Attacks and Zero Dynamics Attacks in Cyber-Physical Systems*, Proceedings of the American Control Conference, pp. 302-307, 2016.
[11] Smith, R.S.: *Covert Misappropriation of Networked Control Systems: Presenting a Feedback Structure*, IEEE Control Systems, vol. 35, no. 1, pp. 82-92, Feb. 2015.
[12] Ramadge, P.J.G., Wonham, W.M.: *The Control of Discrete Event Systems*, Proceedings of the IEEE, vol. 77, no. 1, pp. 81-98, Jan. 1989.
[13] Thistle, J.G.: *Supervisory control of discrete event systems*, Mathematical and Computer Modelling, vol. 23 (11-12), pp. 25-53, 1996.
[14] Wakaiki, M., Tabuada, P., Hespanha, J. P.: *Supervisory Control of Discrete-event Systems under Attacks*, arXiv:1701.00881v1, 2017.
[15] Mitrović, S., Jakovljević, Ž.: *The application of distributed control system based on IEC 61499 and 802.15.4 standards*, Proceedings of ETIKUM Conference, pp. 37-40, Dec. 2017. (In Serbian)

Authors: **Research Assistant Stefan Mitrovic, Research Associate Dr. Zoran Dimic,** Lola Institute, Kneza Viseslava 70a, 11000 Belgrade, Serbia;
Dr. Zivana Jakovljevic, associate professor, University of Belgrade, Faculty of Mechanical Engineering, Kraljice Marije 16, 11000 Belgrade, Serbia.
E-mail: stefan.mitrovic@li.rs,
zoran.dimic@li.rs,
zjakovljevic@mas.bg.ac.rs

ACKNOWLEDGMENTS: This paper is supported by Ministry of Education, Science and Technological Development of the Republic of Serbia under grants TR35004, TR35020 and TR35023.