Abstract − Cyber-physical systems are a crucial part of modern automation applications. Cyber security gains more and more relevance due to recent attacks on such systems. This work investigates possible defense mechanisms against attacks on cyber-physical systems modeled by networked discrete event systems. Based on a threat assessment, attack prevention, attack detection and localization, and attack recovery methods are proposed. The attacks under consideration stealthy attacks that actively hide their influence and are not detectable by conventional anomaly detection schemes. An attack prevention method based on homomorphic encryption of the controller is proposed. The controller encryption does not only allow to encrypt the communication between the plant and the controller but also the controller logic itself. Based on the weakpoints of the attacks under consideration, two attack detection schemes are proposed. The first scheme introduces unexpected behavior into the transmitted signals by the integration of permutation matrices into the sensor and actuator channels to disrupt the stealthiness of an attacker. The second scheme exploits the change in timing behavior to detect the attacks. Moreover, an attack localization scheme is proposed, which allows to determine which signals are attacked in case that the attacker only attacks a subset of communication channels. The information gained from the attack detection and localization is used in the proposed attack recovery approach to reconfigure the controller. Monte-Carlo Tree Search is applied to efficiently solve the reconfiguration problem.

Zusammenfassung − Cyber-physische Systeme sind ein wichtiger Bestandteil moderner Automatisierungsanwendungen. Durch die jüngsten Angriffe auf solche Systeme gewinnt die Cybersicherheit immer mehr an Bedeutung. In dieser Arbeit werden mögliche Verteidigungsmechanismen gegen Angriffe auf cyber-physische Systeme, die durch vernetzte diskrete Ereignissysteme modelliert werden, untersucht. Basierend auf einer Bedrohungsanalyse werden Angriffsprävention, Angriffserkennung und -lokalisierung sowie Methoden zur Wiederherstellung entwickelt. Bei den untersuchten Angriffen handelt es sich um heimliche Angriffe, die ihren Einfluss aktiv verbergen und mit konventionellen Anomalieerkennungsmethoden nicht erkennbar sind. Es wird eine Methode zur Angriffsprävention vorgstellt, die auf der homomorphen Verschlüsselung des Steuerung basiert. Die Steuerungsverschlüsselung ermöglicht nicht nur die Verschlüsselung der Kommunikation zwischen Anlage und Steuerung, sondern auch der Steuerungslogik selbst. Basierend auf den Schwachstellen der untersuchten Angriffe werden zwei Methoden der Angriffserkennung vorgeschlagen. Die erste Methode injiziert unerwartetes Verhaltes in die übertragenen Signale durch die Integration von Permutationsmatrizen in den Sensor und Aktuatorkanäle und stört die Heimlichkeit des Angriffs. Die zweite Methode analysiert die Änderung des Zeitverhaltens zur Erkennung der Angriffe. Darüber hinaus wird eine Methode zur Angriffslokalisierung entwickelt, die es ermöglicht die angegriffenen Signale zu identifizieren. Es wird eine Methode zur Wiederherstellung entiwickelt, die die aus aus der Angriffserkennung und -lokalisierung gewonnenen Informationen nutzt, um die Steuerung zu Rekonfigurieren. Dabei wird Monte-Carlo Baumsuche verwendet, um das Rekonfigurationsproblem effizient zu lösen.

1 Introduction

1.1 Motivation

Cyber-physical systems (CPS) are a crucial part of modern automation applications ranging from advanced manufacturing plants, communication, smart power grids and transportation networks (Teixeira et al., 2015). CPS take into account both physical and information aspects of an automation system. The physical side of CPS includes the physical process, the controller, the actuators, the sensors and the communication infrastructure. The information side of CPS includes the software components, the controller logic and the communication protocols.

CPS are used in the manufacturing industry and in critical infrastructures, such as energy, water and traffic and thus a high degree of security, reliability and availability is required for the operation of CPS. Since CPS not only influence information but also physical processes, these systems have to be secured against outside interference.

In comparison to classic control systems where the controller, the sensors and the actuators are hard-wired, CPS often handle the communication over a network or the internet to take advantage of cloud computing and distributed control architectures. Such networked CPS are vulnerable to cyber attacks. An attacker can compromise one of the components of the CPS or the communication itself, which can lead to real physical consequences.

The Aurora generator experiment in 2007 illustrated the susceptibility of CPS against an attacker with the goal to destroy physical equipment (Zeller, 2011). The experiment demonstrated the potential consequences that an attack on CPS may have. Due to several real-world examples of cyber attacks on CPS, such as Stuxnet attacking an Iranian uranium enrichment facility (Langner, 2013), the attack on the Ukrainian power grid (Lee et al., 2016) and the Triton attack on safety systems (CISA, 2017), the interest in the security of CPS is growing. This is shown in the standards for security such as the ”Information Security Management System” standard ISO 27001 (2022), the ”Security for Industrial Automation and Control Systems” standard IEC 62443-2-1 (2009). Globally, regulatory authorities are enforcing stricter regulation on CPS, such as the German IT-security Act 2.0 (BSIG,

2021), the European Network and Information Security Directive (NIS-Directive, 2022) or the American Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, 2022). Thus effective approaches securing CPS are required.

In the scientific community, security of control systems has gained much attention in recent years. The considered aspects of security range from the modeling of attacks and the prevention of attacks to the detection of attacks and the recovery following the attack (Teixeira et al. (2015), Rashidinejad et al. (2019), Dibaji et al. (2019), Cao et al. (2020)).

The measures against cyber attacks on CPS can be categorized into four mechanisms as shown in Fig. 1.1. Prevention algorithms postpone the onset of the attack, resilience algorithms reduce the maximum impact of the attack to allow the CPS to operate as close as possible to the normal operation, detection and localization algorithms identify the attack source and isolate the attacked subsystems. The information gained by the detection and localization algorithms is then used by the recovery algorithms to restore the normal operation (Dibaji et al., 2019). The basis for the design of these algorithms is a threat assessment to analyze the vulnerabilities of the CPS. It is advised to combine multiple defense mechanism since only a single defense mechanisms is often not enough. For example, prevention algorithms postpone the start of the attack but may not prevent it indefinitely. Thus a defense-in-depth strategy combining multiple defense mechanisms is required for a reasonable protection of CPS. In a defense-in-depth strategy the attacker has to overcome multiple security measures that expend the attacker's resources before the real attack goal can be reached (Cleghorn, 2013).

1.2 Objectives

In this thesis, the focus is on systems that can be modeled by discrete event systems (DES) and the cyber security of networked discrete event systems is investigated. Such systems are widely used, for example, in automated manufacturing systems or traffic control systems (Cassandras and Lafortune, 2008).

For this purpose, a threat assessment of automation systems controlled by DES-based controllers is carried out. Based on the threat assessment, models for the attacks are derived and methods to increase cyber security are presented. In line with a defense-in-depth strategy, prevention, detection and localization, and attack recovery methods are presented.

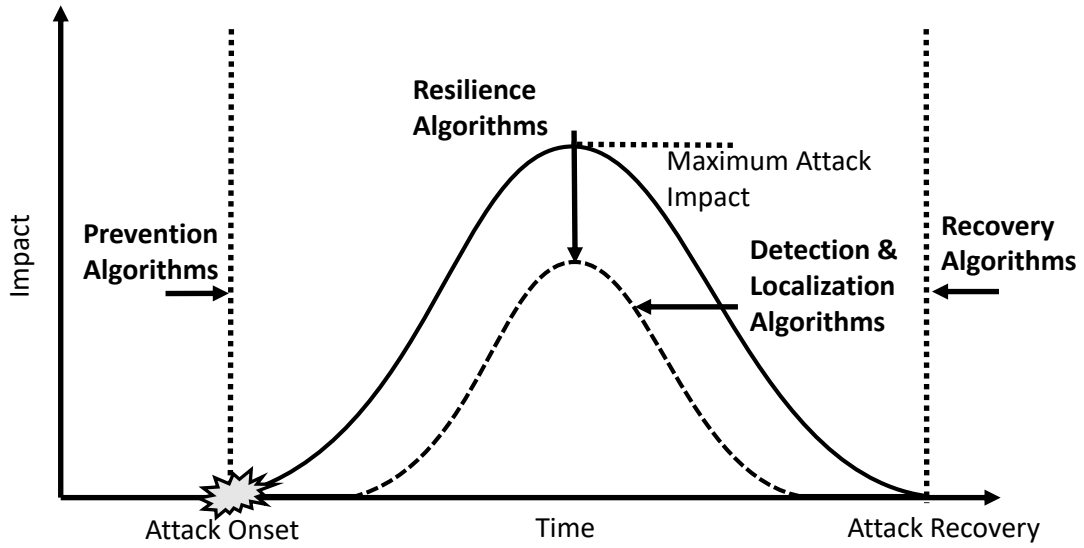

Figure 1.1: Overview of defense mechanisms against attacks on CPS (Dibaji et al., 2019)

The main contributions of this thesis are:

- Threat assessment: In the literature, often only simple attacks are considered. In this thesis, the attack possibilities of an intelligent attacker are analyzed. Such an attacker can use information about the automation system to develop highly sophisticated attack strategies. Four stealthy attacks are presented which are difficult to detect by conventional anomaly detection schemes.
- Attack prevention: An effective method to prevent attacks on CPS is encryption. By exploiting homomorphic encryption schemes allowing arithmetic operation on encrypted data, a controller encryption scheme is proposed in this thesis. The proposed scheme not only encrypts the communication between the plant and the controller but also the controller logic itself. This makes it more difficult for an attacker to gain information about the controller and the plant. It is shown that a DES-based controller can be transformed into an arithmetic form to allow the use of homomorphic encryption. Moreover, an extension for timed DES is presented, allowing the use of encrypted timers and encrypted counters in the controller logic.
- Attack detection and localization: Based on the threat assessment, a detection and localization approach against stealthy cyber attack is proposed in this thesis. The weak points of the stealthy attacks are analyzed and two detection schemes are presented. The first scheme introduces unexpected behavior into the transmitted signals by the integration of permutation matrices into the sensor and actuator channels. The permutation disrupts the stealthiness of an

attacker and allows the detection of cyber attacks. The second scheme exploits the change in timing behavior to detect the attacks. Moreover, an attack localization scheme is proposed, which allows to determine which signals are attacked in case that the attacker only attacks a subset of communication channels.

- Attack recovery: Similar to fault-tolerant control, the attack recovery methods can be differentiated into active and passive attack recovery. The focus of passive attack recovery are resilient controllers (Su (2018),Wakaiki et al. (2019)). In this thesis, an active attack recovery scheme is proposed. The attack recovery reconfigures the controller based on the information gained by the attack detection and localization. For the reconfiguration, a tracking control approach based on Monte-Carlo Tree Search (MCTS) is developed. It is shown how the MCTS is adapted to different types of Petri nets, allowing a wide range applications apart from the attack recovery, such as scheduling or reachability analysis.

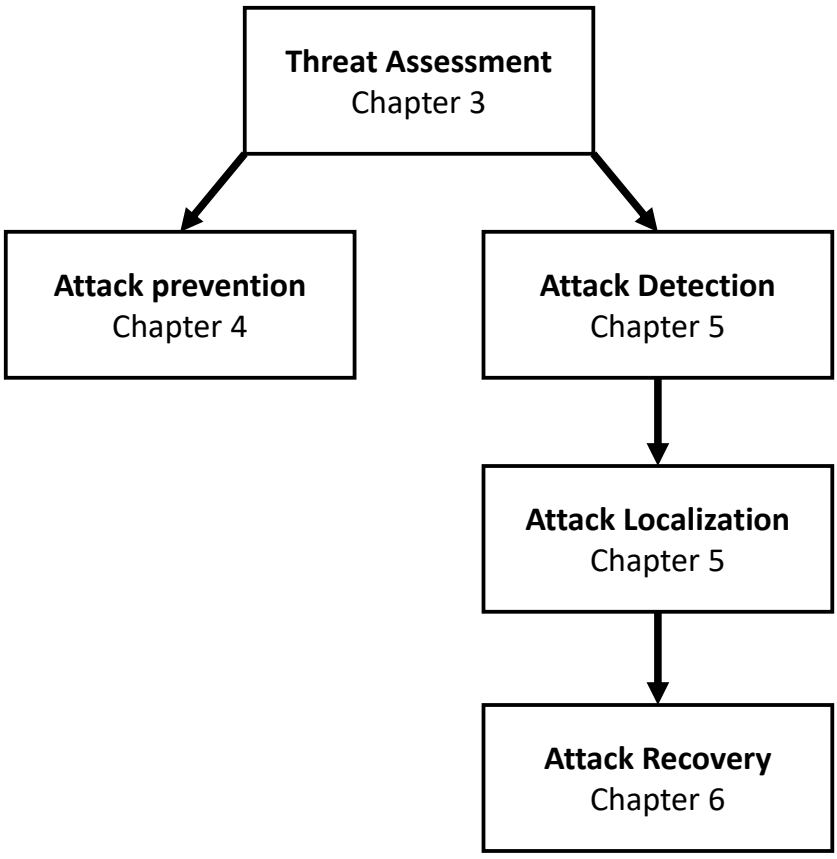

Figure 1.2: Overview of dependencies and connections between the chapters