Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Sensor attack detection using history based pairwise inconsistency

Kang Yang [a,b], Rui Wang [a,b,*], Yu Jiang [d], Houbing Song [c], Chenxia Luo [a,b], Yong Guan [a,b,*], Xiaojuan Li [a,b], Zhiping Shi [a,b]

[a] College of Information Engineering, Capital Normal University, Beijing, 100048, China
[b] Beijing Advanced Innovation Center for Imaging Technology, China
[c] Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, United States
[d] School of Software, Tsinghua University, Beijing, 100084, China

HIGHLIGHTS

- This paper focus on the security issues of Cyber-Physical Systems with multiple sensors measuring the same physical variables.
- We present a novel sensor attack detection method based on fusion interval and historical measurements.
- This Method can enhance the performance of attack detection and recognition.
- The core idea is to add a virtual sensor that takes the fusion intervals or past measurements as its value and it uses the inconsistencies between the two sensors to detect and identify the attack.
- Experiments show that our approach is very effective for a variety of attacks and can first detect stealth attacks comparing with the existing methods.

ARTICLE INFO

Article history:
Received 30 September 2017
Received in revised form 15 March 2018
Accepted 26 March 2018
Available online xxxx

Keywords:
Cyber-physical system
Security
Sensor attack detection and identification

ABSTRACT

This paper focuses on the security issues of Cyber-Physical Systems with multiple sensors measuring the same physical variables. We use an abstract sensor model, and each sensor provides the controller with an interval that contains the true value. Some of the sensors may be subject to malicious attacks and provide the wrong measurements, thereby misleading the controller into performing an unsafe action. Although there are several existing methods for detecting sensor attacks in the presence of transient sensor faults, they treat all sensors' faults and attacks in the same way, and may not work well when an attacker has sufficient ability to cover up for different sensors at different times, e.g., stealth attacks. To address this problem, we propose a pairwise inconsistency based algorithm to enhance attack detection capability. The main idea is to build different fault models for different sensors, add a virtual sensor to utilize the fusion intervals and historical measurements, and use pairwise inconsistencies between real and virtual sensors to identify attacks. Finally, we validate the performance of the algorithm on real measurement data obtained from the LEGO EV3 ground vehicle, the results show that the proposed method outperforms state-of-the-art algorithms.

1. Introduction

Along with the widespread use of Cyber-Physical Systems (CPS), more and more people are beginning to focus on CPS security issues. The interaction between information technology and the physical world makes CPS vulnerable to various malicious attacks, which undermines its security [1–5]. For example, several methods are proposed to interrupt the operation of the vehicle, disable the vehicle or hijack the car [6,7]. In addition, because the CPS system introduces the network characteristics in the control system, the malicious attacker can delay or distort the control command by means of sensor spoofing, DoS (Denial of Service) attack and DDoS (Distributed Denial of Service) attack, etc. [8–12]. These means of sensor attack can cause the CPS system to fail to perform the task in time and then lead to disastrous consequences [13].

As sensor technology develops rapidly, modern CPS typically has multiple sensors that can measure the same physical variables [14,15]. For example, encoder, ultrasound, GPS and IMU can provide speed measurements. Even if the precision of each sensor may be different, fusing measurements of multiple sensors not only produces an estimate that is more precise than any single sensor's [16], but also increases the robustness of the system to external interferences (e.g., the car runs on an uneven ground) [17].

In this work, we deal with the problem of CPS security which usually considers the worst-case system operation. Therefore, we

* Corresponding authors at: College of Information Engineering, Capital Normal University, Beijing, 100048, China.
E-mail address: rwang04@cnu.edu.cn (R. Wang).

https://doi.org/10.1016/j.future.2018.03.050
0167-739X/

use the abstract sensor model, an interval is constructed around the measurement of each sensor. The interval's size can be obtained based on the relevant parameters which are provided by the manufacturer [18], such as measurement error, the precision and sampling jitter. These parameters can also be obtained through a large number of actual data training. For example, an automatic method is proposed, which uses the characteristic of knee point to find the parameters of the transient fault model (described in Section 2.4) [19]. In [20], Marzullo develops a fusion algorithm that utilizes the measurements of multiple sensors to produce a fusion interval that contains the true value. Based on the fusion algorithm of Marzullo, a precise and resilient sensor fusion algorithm is proposed by introducing the sensor transmission schedules [21] and using the historical measurements [22].

In general, the system does not know the true value, so it is difficult to determine which sensor is attacked. In [20], Marzullo proposes a sensor fault detection method based on the fusion interval. The disadvantage of this approach is to treat faults and attacks in the same way. Thus, this may lead to a system does not trust sensors that are only transient faults. The transient faults refer that provide the wrong measurements in the short period of time and usually soon disappear. For example, GPS often temporarily loses connection with the satellite in the tunnel. So we should not regard transient faults as sensor attacks.

In order to eliminate this limitation, in [23], a transient fault model is provided for each sensor to distinguish transient faults and attacks. The sensor is attacked maliciously if the acquired sensor data does not match this model. In addition, [23] also proposes an attack detection algorithm that uses the relationship between the two sensor measurements to generate redundant information for attack detection. On the basis of this method, the attack detection performance of multiple operating mode systems is improved by finding the appropriate transient fault model parameters [19]. The limitation of these two methods is that they only consider the situation that the two sensors do not intersect with each other. They ignore the fact that they may also provide faulty measurements when they intersect, so that some attacks cannot be detected. For example, stealth attack, that is, the attacker has enough ability to maximize the fusion interval and make the interval of any two sensors intersect as much as possible while keeping undetected. Other related works include those of [24–29].

To solve this problem, we propose an improved sensor attack detection method. The idea of this algorithm is to consider the sensor's measurements from different ways, and to use the generated redundant information to detect and identify the attack. Therefore, we propose a weak inconsistency detection method, which takes into account the following three aspects: (1) Compare the relationship between any two sensors' measurements in the current round. (2) The fusion interval is calculated after receiving all measurements of the current round, then compare the relationship between the measurement of each sensor and the fusion interval. (3) Fusing past and current measurements. For each sensor, compare the difference between the current round and the previous round of measurements.

Finally, we provide a case study with an autonomous vehicle, called the EV3 robot, to illustrate the effectiveness of the method. We present the detection and recognition rate of the algorithm for three different types of attacks, and illustrate the advantages of the algorithm over the existing methods. In addition, we also compare the number of weak inconsistencies detected by the two algorithms under bias attack. This further illustrates the effectiveness and robustness of our algorithm.

The contribution of this Paper. This paper presents a novel sensor attack detection method based on fusion interval and historical measurements, and can enhance the performance of attack detection and recognition. The core idea is to add a virtual sensor that takes the fusion intervals or past measurements as its value (see Section 3 for details), and it uses the inconsistencies between the two sensors to detect and identify the attack. Experiments show that our approach is very effective for a variety of attacks, especially for stealth attacks. The proposed method can well detect stealth attacks in the system, but the existing method cannot detect such attacks.

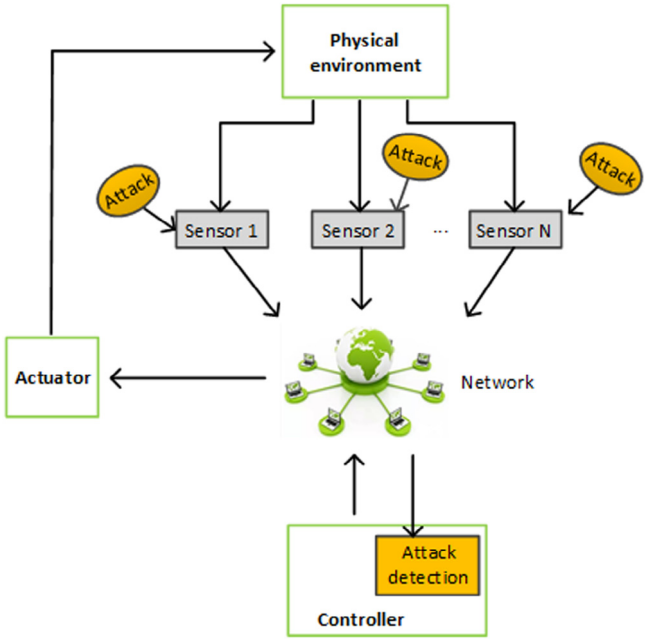

Fig. 1. General architecture of CPS.

The rest of the paper is organized as follows. The subsequent section provides the problem formulation. In Section 3, we introduce our method for sensor attack detection and identification. In Section 4, we use an example to illustrate the characteristics of the two methods. Section 5 evaluates our algorithm by obtaining real measurement data from the EV3 robot. Finally, conclusions are presented in Section 6.

2. Problem formulation

2.1. System model

We consider a system which consists of N sensors that measure the same physical variables (e.g., velocity). The redundant information of multiple sensors is used to provide more precise estimates for the controller.

As shown in Fig. 1, sensors in the system communicate over the shared bus such that all measurements are broadcast to all nodes in the network. Attackers can tamper with the sensor measurements, so as to achieve the purpose of attacking the entire system. We assume that the system periodically obtains the measurements of the sensor. Once the controller receives all measurements in a given round, it performs the sensor attack detection and identification algorithm.

2.2. Abstract sensor model

The sensor models are mainly divided into two categories: probability and abstract. Probability model means that each sensor provides a numeric measurement that is damaged by noise with a known probability distribution, Such as Gaussian distribution and uniform distribution [30,31]. Unlike the probability model [32,33],

Please cite this article in press as: K. Yang, et al., Sensor attack detection using history based pairwise inconsistency, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.03.050.