sensors

MDPI

Article

Research about DoS Attack against ICPS

Jianlei Gao, Senchun Chai *, Baihai Zhang and Yuanqing Xia

School of Automation, Beijing Institute of Technology, Beijing 100081, China; jianleixinye@163.com (J.G.); smczhang@bit.edu.cn (B.Z.); xia_yuanqing@163.net (Y.X.)

* Correspondence: chaisc97@bit.edu.cn; Tel.: +86-1391-145-7765

Received: 13 February 2019; Accepted: 24 March 2019; Published: 29 March 2019

Abstract: This paper studies denial-of-services (DoS) attacks against industrial cyber-physical systems (ICPSs) for which we built a proper ICPS model and attack model. According to the impact of different attack rates on systems, instead of directly studying the time delay caused by the attacks some security zones are identified, which display how a DoS attack destroys the stable status of the ICPS. Research on security zone division is consistent with the fact that ICPSs' communication devices actually have some capacity for large network traffic. The research on DoS attacks' impacts on ICPSs by studying their operation conditions in different security zones is simplified further. Then, a detection method and a mimicry security switch strategy are proposed to defend against malicious DoS attacks and bring the ICPS under attack back to normal. Lastly, practical implementation experiments have been carried out to illustrate the effectiveness and efficiency of the method we propose.

Keywords: DoS attack; industrial cyber-physical system (ICPS); security zones; mimicry security switch strategy

1. Introduction

A cyber-physical system (CPS) is a physical system that combines physical plants with network systems for data transmission and control functions, which has attracted worldwide attention after it was put forward in 2006 by the U.S. National Natural Science Foundation [1]. The CPS usually integrates some physical processes, data communication capabilities, sensors, data calculation and process control. It utilizes computers and networks to monitor physical process and control production parameters. It realizes combined calculations with physical processes depending on the real-time data interaction. CPSs are ubiquitous in modern life, ranging from current sweeping robots to global energy power system networks, which include smart cities, medical systems, military command systems, etc.

There are a lot of different types of CPSs, whose most typical application is the industrial control system (ICS), also called industrial cyber-physical system (ICPS), such as a supervisory control and data acquisition (SCADA) system, or programmable logic controller (PLC) system. They are widely used in a variety of industries, especially those related to critical national infrastructures, such as smart grids, energy production and transmission, smart cities, municipal engineering, the petrochemical industry and so on [2].

In recent decades, the corresponding technology has been developed dramatically. In order to enhance the facilities, reduce the complexity and cut down costs, more and more ICPSs are being upgraded with the latest communication and control technology, such as network communication, wireless sensors networks, multi-agent systems and so on. Generally speaking, ICPSs with integration modern cyber-technologies, which include Internet technology, cloud technology, Internet of Things and so on, have been using those technologies to communicate with each part, monitor plants and control physical processes. However, network attacks and vulnerabilities that have produced great risks and a large number of information incidents have been triggered due to the open networks protocols, which have already resulted in serious damage.

In recent years, many ICPS incidents have happened around the world. In 2010, the Iranian nuclear incident where the country's nuclear energy program was attacked by the "Stunex Virus"and "Duqu Trojan" that was detected in many countries in 2011, was considered the first premeditated destruction aimed at critical ICPSs. In 2012 some security experts found that the "Flame virus" not only attacked Iran, but also affected the entire Middle East region. A German steelworks suffered from a cyber-attack, which resulted in the control systems and production systems being forced to stop in 2014, but the most striking example was the collapse of the Ukrainian electricity grid in December, 2016.

The report [3] published by ICS-CERT of China provides statistics of ICS information security incidents from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which shows that more and more ICPSs are being attacked by various malicious cyber actions as depicted in Figure 1. As is seen from the chart, obviously the incident occurrence is on the rise.

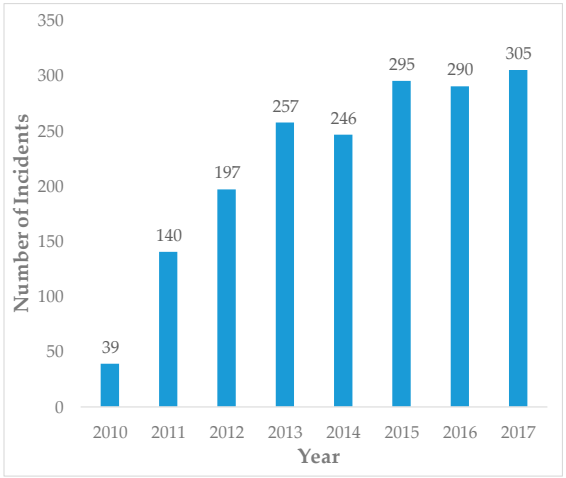


Figure 1. ICPS security incidents by year [3].

The ICPSs, especially the control systems of ICPSs, are connected to the public Internet, which raises greater security challenges than pure information systems when they are under cyberattack. As ICPSs are media to bridge physical process and virtual world of information, so the availability of data, including control data and communication data, is more important because of its effect on real-time performance. That is to say, once an ICPS is attacked by malicious attacks, it will cause more serious consequences than attacks on pure information systems.

The rest of paper is organized as follows: in Section 2, some related works are presented. Section 3 discusses some basic knowledge and mathematic models, which include an ICPS model, DoS attack model, DoS attack effect on ICPS model and so on. The detection model and defense strategy are designed in Section 4. We present some experimental results and analyses in the following Section 5. The last part presents the conclusions.

2. Related Work

As is known to all, unlike traditional information security where more attention is paid to the protection of data, cyber-attacks on CPSs' control networks usually wreck physical processes because of the existence of feedback networks, so the research and analysis on CPS must take both the cyber area and physical parts into consideration. Currently, there are various modes of attack against CPS, such as denial-of-service (DoS) attacks [4,5], bias injection attacks [6–8], zero dynamics attacks [9], convert attacks [10], zero response attacks [9], eavesdropping attacks [10] and so on. According to reference [10], the authors created a three-dimensional space, illustrated in Figure 2, to quantify them.

There have been a great deal of algorithms designed to analyze and solve these malicious attacks in CPSs [7,10–14]. They typically provide an explanation, system model and analysis, and control system experiments against different attack ways [10]. In [15], the authors do a lot of work about cyber-physical

systems, supply a mathematical framework of the systems' attacks and monitors, present some fundamental monitoring limitations from a system-theoretic and graph-theoretic perspective, and design a distributed attack detector and identification monitors. Reference [12] studies a general convex optimization method of estimation which demonstrates generic sufficient and necessary conditions instead of specific estimators. The current detection methods against cyber-attacks are based on statistical learning algorithms which could cause misleading alarms. Reference [13] adopts a mulit-order Markov chain framework based on supervised statistical learning to solve the above shortcoming. Besides, it designs an optimal attack strategy to destroy wireless sensor network control systems and worsens the cost function to maximum value and find a coping strategy in this way [14]. Among these efforts aimed at studying specific malicious attacks, the DoS attacks (including DDoS) has been widely studied because of their easiest implementation, most serious consequences and least system knowledge that is needed to destroy the communication channel between a system's parts.

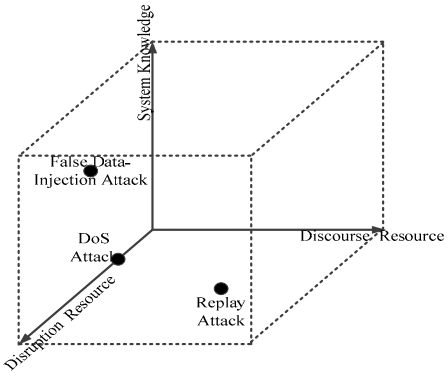


Figure 2. Three-dimensional attack space.

Many people have been devoted to studying DoS attacks against CPSs (including ICPSs), whose focus can mainly be divided into two parts: information security and control science. From the viewpoint of computer information security, people usually design an intrusion detection system (IDS) to protect targets from DoS attacks. The most typical methods are based on machine learning algorithms. For example: [16] proposes a new method based on support vector machine (SVM) which is motivated by the fact that the cloud environment is changeable/dynamic to detect DoS attacks. However, current IDS can't detect two specific hardware Trojans (HT)-assisted DoS attacks (sinkhole and blackhole attacks) which is explained by quantifying the effects of attacks as packet loss rates [17]. In order to deal with this problem in embedded systems designed with Multiprocessor-System-on-Chip (MPSoC) architectures, the utilization of pipelined MPSoC (PMPSoCs) is selected and improved to detect DoS attack-based hardware Trojan attacks [18]. Although all the studies provide some reasonable and useful methods to prevent, detect, defend and eliminate DoS attacks, they all have their limitations and deficiencies, especially in dealing with the carefully designed network DoS packets. What is worse is that they all don't consider the impact of attack on the physical part when they only fix their attention on the cyber layer. However, the physical part of ICPS is especially in need of strong real-time control data.

Many people study DoS attacks on ICPSs from the consideration of control theory. Some attack models and scenarios are given by reference [4] whose analyses are shown in Figure 2. Reference [5] uses the Tennessee Eastman challenge process to study the DoS attack through modeling the problem of DoS attacks as optimal stopping problems, which cause a change of the timing parameter in a physical process. The authors [14] analyze the problem of DoS attacks from the viewpoint of an attacker to study the optimal DoS attack strategy which can maximize the cost function of the linear quadratic regulator (LQR) controller. What' more, Yuan et al. [19] use a unified game theory to improve the robustness by designing a resilient control network system. Obviously, these algorithms can validly

address the influences of attacks against physical layer such as control systems, but most of them lack any study on the cyber layer, which cannot eliminate DoS attacks.

In this paper, we try our best to combine the two aspects of ICPS security research to detect and eliminate DoS attacks against networks, and effectively solve the impacts of the attacks in the physical area to maintain ICPSs' normal operation.

The main contribution of this work are: (1) we try to combine and information security method with a control theory method to study the DoS attacks against industrial cyber-physical systems (ICPSs), and propose a mathematical model of DoS attacks with a detailed explanation; (2) according to the influence of different attack rates against ICPSs, we study the time delay caused by attacks dividing the ICPS into security zones instead of studying it directly, which displays how a DoS attack destroys the stable status of the ICPS; (3) a detection method and a mimicry security switch strategy are proposed to defend against this malicious DoS attack and bring the abnormal operation of ICPS back to a normal status; (4) a practical implementation has been carried out to illustrate the effectiveness and efficiency of the proposed method, which gives us an inspiration to protect our critical ICPSs with multiple sets of redundant sub-control systems.

3. Preliminary Knowledge

3.1. ICPS Structure

With the improvement of information technology, more and more ICPSs adopt Ethernet technology based on the TCP/IP protocol, which makes the control system more integrated, improves information transfer rate and the compatibility between different systems and enhances the range of application. A typical ICPS structure is shown in Figure 3.

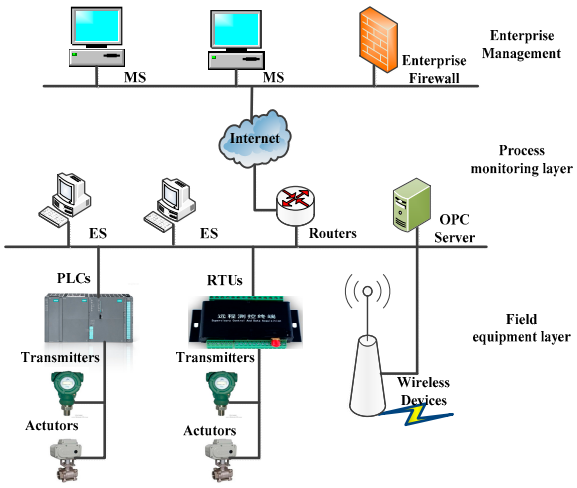


Figure 3. The structure of an ICPS.

3.2. ICPS Model

Consider the following ICPS with multi-subsystems:

$$\begin{cases} g = g(o_{i,}) \\ o_i = o_i(p_i, f_i) \end{cases} \quad (i = 1, 2, \cdots, N) \tag{1}$$

where i is the index of sub-control system, o_i is the i-th-sub-system, N is the sum of sub-control systems, p_i is the transfer function, f_i is the network characteristic function for which a detailed explanation

will be given below. Consider the following physical system which is assumed a continuous linear dynamic system:

$$p_i(x) = \begin{cases} \dot{x}(t) = A_s x(t) + B_s u(t) \\ y(t) = C_s x(t) + D_s u(t) \end{cases} \quad (2)$$

where $x(t) \in \mathbb{R}^n$ and $y(t) \in \mathbb{R}^m$ show the system states and system output, respectively, at time $t \in \mathbb{N}$. Besides, the matrix of A_s, B_s, C_s and D_s are constant matrixes with related ranks.

Assumption 1. *Only one sub-system o_i is running at one moment, and other sub-systems $o_j (j \neq i)$ are listening and in standby mode at the same time.*

3.3. DoS Attack Model

In this subsection, in order to build a DoS attack model, we need to provide some assumptions and a definition firstly:

Assumption 2. *The time delay caused by the network's background is not considerable.*

Assumption 3. *The ICPS has more than one sub-system $f = \{f_i | i = 1, 2 \cdots, m\}$ (m is the sum of sub-system), and each of them has different network parameters which include an IP address (l_1) and communication port (l_2).*

Definition 1. *There exists an attack function $a = \{a_i | i = 1, 2, \cdots, m\}$ (m is the sum of sub-system), an attack operator $\otimes$ and attack set $I_H = \{0, 1\}$.*

A Denial-of-Service (DoS) attack is defined as a means to send lots of network data packets to targets, which will shut down users' computers and make the paralyze the communication network. DoS attacks accomplish this by flooding the target with traffic, or sending malicious information that triggers a crash. However, explicit DoS attack models are not given in [20], which lacks real network information, so we will define an attack model to explain how a DoS attacks a system.

According to Assumption 3, the attack function $a = \{a_i | i = 1, 2, \cdots, m\}$ and the attack object (the ICPS with one running subject) have two parameters, we can get $a_i = a_i(l_1, l_2)$ and $f_i = f_i(l_1, l_2)$.

Applying Definition 1 and Equation (1), it can be obtained that:

$$I_H = a_i \otimes f_j = a_i \otimes o(f_i, *) \quad (3)$$

Theorem 1. *Consider a DoS attack against ICPS, the attack a_i is independent of each other and the attack object f_i is independent of each other. Therefore, the attack set $I_H = \{0, 1\}$ has:*

$$\begin{cases} I_H = a_i \otimes o(f_j, *) = a_i \otimes f_j = 1, i = j \\ I_H = a_i \otimes o(f_j, *) = a_i \otimes f_j = 0, i \neq j \end{cases} \quad (4)$$

3.4. DoS Attack Effect on ICPS

As we all know, a DoS attack will affect a system's normal operation. As for how it affects the system, modelling system service performance from an information security perspective is relatively plausible in traditional information systems but not reasonable in an ICPS without consideration of stability of its physical parts. Studies in control science suggest the DoS attacks can increase the delay of control processes, and thus this will degrade the performance of the control system which is lacking details. Therefore, we try our best to explain how a DoS attack affects an ICPS's performance with Definition 2.

Definition 2. *We define a packets rate function* fr:

$$fr = \frac{sum\,(packet)}{sum\,(time)} \tag{5}$$

Actually, the DoS attack destroys the system's performance by increasing the time delay and this undoubtedly reduces the real-time control performance when the DoS attack lasts for a certain period. According to the network's features and working principle, for a more intuitive explanation, we define a time delay τ, dangerous zone Ω and their relation with *fr* to explain the details here.

Definition 3: *The ICPS has running zones* $\Omega = \{\Omega_i | i = 1, 2, 3, 4\}$, *and* Ω_{ICPS} *represents the current running zone, which is shown in Figure 4.*

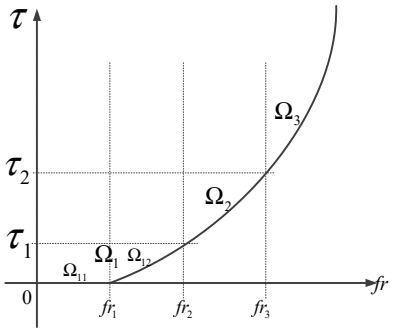


Figure 4. Relation between attack rate and time delay.

$$S = \begin{cases} \Omega_{11}, & 0 \le fr < fr_1 \\ \Omega_{12} & , \quad fr_1 \le fr < fr_2 \\ \Omega_2 & , \quad fr_2 \le fr < fr_3 \\ \Omega_3 & , \quad fr_3 \le fr \end{cases} \tag{6}$$

where Ω_{11} is an absolutely secure zone which indicates that no attack can affect the system's normal operation. That is to say no attack is launched. Ω_{12} is a related security zone which indicates the system can still operate normally under attack. Ω_2 is a hazardous zone which indicates the system runs abnormally under attack but does not crash. Ω_3 is an absolutely hazardous zone which indicates the system has collapsed under attack. τ_1 is the resilience time delay which means this time delay can be accommodated by the network under attack and does not have any negative effects. τ_2 is the maximum time delay that the system can sustain. τ_{num} is the sum of the delays in the current communication network.

Merging Ω_{11} and Ω_{12}, we can get:

$$\Omega = \begin{cases} \Omega_1 & , \quad 0 \le fr < fr_2 \\ \Omega_2 & , \quad fr_2 \le fr < fr_3 \\ \Omega_3 & , \quad fr_3 \le fr \end{cases} \tag{7}$$

From the above, it is known that Ω_1 is a security area; Ω_2 is a transient-normal area; Ω_3 is an abnormal operation area.

Explanation. *Nowadays, network devices are built with an inherent time delay, which does not affect the normal operation of the ICPS. Meanwhile, they also have an elasticity feature that has some capacity to bear a bit of large network traffic to maintain the normal operation of the ICPS. This is in conformity with the actual situation. Therefore, our assumption is reasonable and the experimental data provided later will prove it too.*

Remark 1. *When the ICPS was attacked, every zone has following property:*

$$\begin{cases} \bigcup_{i=1}^{3} \Omega_i = 1 \\ \bigcap_{i=1}^{3} \Omega_i = 0 \end{cases} \tag{8}$$

Remark 2. *When the ICPS was attacked, every zone had the following migration process as is shown in Figure 5:*

Figure 5. Attack zone migration process.

Theorem 2. *The necessary and sufficient conditions for the system to run normally are:*

(1) $\Omega_{ICPS} \notin \Omega_3$ *and* $\Omega_{ICPS} \notin \Omega_2$
(2) $\Omega_{ICPS} \in \Omega_2$ *but* $T_{ICPS} < \tau_2 - \tau_1$

Proof of Theorem 2.

Necessary condition:

About condition (1), if $\Omega_{ICPS} \notin \Omega_2$ and $\Omega_{ICPS} \notin \Omega_3 \rightarrow \Omega_{ICPS} \in \Omega_1$.

About condition (2), if $\Omega_{ICPS} \in \Omega_2$ but $T_{ICPS} \leq \tau_2 - \tau_1 \rightarrow \tau_{num} = 0 + \tau_1 + T_{ICPS} < \tau_2 \rightarrow$ runs normally.

Sufficient condition:

About the proof of sufficient condition, we can use opposite to prove it. Firstly we assume the system is abnormal, so the time delay $\tau_{num} \geq \tau_2$.

Obviously, there are only two conditions which can satisfy it: $\Omega_{ICPS} \in \Omega_3$ or $\Omega_{ICPS} \in \Omega_2$ and $T_{ICPS} + \tau_1 \geq \tau_2$

From the analysis of an attacker's perspective, it is intended to implement the DoS attack plan that transforms the running zone Ω_1 into Ω_2, or even Ω_3.

Problem 3.1 (Attackers' Purpose)

$$\begin{cases} \max \quad T_{ICPS} \\ s.t. \quad I_H = 1 \end{cases} \tag{9}$$

The Problem 3.1 means that this malicious DoS attack is launched ($I_H = 1$) to increase the maximum communication time delay of data packets (T_{ICPS}). According to the abovementioned Theorem 2, the increasing T_{ICPS} to deteriorate ICPS's normal running is equivalent to making the ICPS run in Ω_2 and Ω_3, so the Problem 3.1 can be equal to:

$$\begin{cases} \Omega_{ICPS} \in (\Omega_2 \cup \Omega_3) \\ \quad s.t. \quad I_H = 1 \end{cases} \tag{10}$$

3.5. Mimicry Security Policy

Assumption 4. *The time interval of switching between two different sub-systems is 0.*

In Nature a large number of creatures, the most typical example of which is the octopus, simulate other creatures through morphology, behavior and color, thus deceiving possible attackers and protecting themselves. This phenomenon is called mimicry, and it gives many living creatures a way to

survive. Inspired by this ability, a large number of scholars began to study this mimetic defense strategy in the field of information security, and they have achieved excellent results. What's more important is that this strategy is effective against many methods of network attack. Besides, the majority of important infrastructures have several sets of stand-by sub-systems, which provides good conditions for the application of this strategy, so we try to use a mimicry security policy to defend DoS attack against ICPS. First, we define a mimicry defense strategy $\sigma(\bullet)$, following modal transfer as is shown in Figure 6:

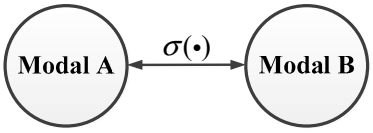


Figure 6. Mimicry policy.

That means the ICPS with multi-sub-systems will change its running-sub-system which is the modality of the current moment using a mimicry defense strategy $\sigma(\bullet)$ when it is attacked by a DoS attack.

Replace $\sigma(\bullet)$ into ICPS system's function:

$$\begin{cases} g = g(o_i) \\ \sigma(\bullet) \end{cases} = g_{\sigma(\bullet)}(o_i)$$

Applying Equation (1):

$$g_{\sigma(\bullet)}(o_i) = \begin{cases} f_{\sigma(\bullet)}(t) \\ p_{\sigma(\bullet)}(t) \end{cases} = \begin{cases} f_{\sigma(\bullet)}(t) \\ \begin{cases} \dot{x}(t) = A_{\sigma(\bullet)}x(t) + B_{\sigma(\bullet)}u(t) \\ z(t) = C_{\sigma(\bullet)}x(t) \end{cases} \end{cases}$$

Adding the constraint condition attack set I_H, we can get the following Equation (11):

$$\begin{cases} g_{\sigma(\bullet)}(o_i) \\ s.t \quad I_H = 1 \end{cases} = \begin{cases} \begin{cases} f_{\sigma(\bullet)}(t) \\ p_{\sigma(\bullet)}(t) \end{cases} \\ s.t \quad I_H \end{cases} = \begin{cases} \begin{cases} f_{\sigma(\bullet)}(t) \\ \begin{cases} \dot{x}(t) = A_{\sigma(\bullet)}x(t) + B_{\sigma(\bullet)}u(t) \\ y(t) = C_{\sigma(\bullet)}x(t) \end{cases} \end{cases} \\ s.t \quad I_H \end{cases} \tag{11}$$

Equation (11) shows that the function of mimicry switch strategy is to change the sub-system of the ICPS under DoS (I_H) to another sub-system to protect the ICPS. From the above analysis and assumption, we know that the cyber layer with a new network configuration has a natural immunity ability against DoS attacks after changing its sub-system using the mimicry defense strategy. These malicious attack packets cannot reach the ICPSS because of the new network configuration with a different IP address and port parameters. What's more, the physical layer with a new sub-system which has a new control system has the capability to keep the system stable and reduce the time delay to ensure the real-time character after the ICPS changes its old model.

In short, the role of these security tactics is that ICPS's running zone is transferred into a security zone from a transient-normal area as shown in Figure 7.

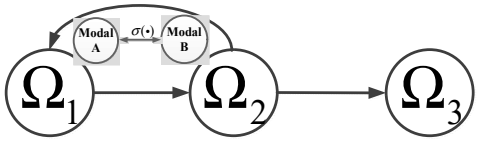


Figure 7. Zone transfer using mimicry strategy when under attack.

4. The Defense Strategy for DoS Attacks

In this section, some methods are developed to defend from DoS attacks, which contain a detection method and a mimicry security strategy to avoid the adverse effects of the attack.

4.1. The Detection of a DoS Attack

According to the physical system of ICPS shown in formula 2, we can get the model discretized by shift operator:

$$\begin{cases} x_{k+1} = Ax_k + Bu_k + w_k \\ y_k = C_k + v_k \end{cases} \tag{12}$$

where $x_k \in R^n$ is the n-dimensional vector of state variable at time k, $u(k) \in R^m$ is the m-dimensional system input vector at time k, y_k^T is an m-dimensional observation vector at time k, $w_k \in R^n$ and $v_k \in R^m$ are measurable white noises whose means are 0 at time k, respectively.

It is assumed that w_k and v_k are independent:

$$\begin{cases} w_k \sim \mathrm{N}(0, Q) \\ v_k \sim \mathrm{N}(0, R) \end{cases} \tag{13}$$

As we all know, the purpose of attacks against ICPS is to downgrade a stable operation state to a target state [21] and to evade detection, which could cause some indicators to deviate from the normal range. Different studies choose different standard indexes to identify anomalies, such as 2-normal, Chi-square, cost function, etc.

Although they are different methods, they are essentially all based on related errors. References [8,22,23] use a Chi-square detector to detect a CPS abnormity if the error between an estimated value and the real value exceeds a threshold. Although this method is unable to detect false data-injection attacks, it is applicable for other types of attack, for example: DoS attacks. The error covariance between the state value and estimated value, which we call minimum mean-square error (MMSE), is used in [24] to detect abnormal actions caused by network attacks because DoS attacks will break the system balance, which will increase system regulation cost. References [2,21] adopt a cost function to judge whether a system is under attack or not.

In many studies, a Kalman filter was utilized to perform state estimation, distinguish deviations and detect mistakes from observations under malicious attacks. In our research, we formulate a cost function that penalizes deviations from normal to abnormal states, and detects whether a DoS attack has happened. In this section, we model the physical part of an ICPS as a time-varying linear control system, which is equipped with a Kalman filter, LQR controller and failure detector:

$$\begin{cases} \widetilde{x}_{k+1|k} = A\widetilde{x}_k + Bu_k \\ P_{k+1|k} = AP_kA^T + Q \\ K_k = P_{k|k-1}C^T[CP_{k|k-1}C^T + R]^{-1} \\ P_k = P_{k|k-1} - K_kCP_{k|k-1} \\ \widetilde{x}_{k+1} = \widetilde{x}_{k+1|k} + K_k[y_k - C\widetilde{x}_{k+1|k}] \end{cases} \tag{14}$$

where $\widetilde{x}_k$ is the a posteriori state estimation value at time k, the error $(x_k - \widetilde{x}_{k+1|k})$ is between the estimation and real value, $P_k = \mathrm{cov}(x_k - \widetilde{x}_k)$ is the error covariance that shows the accuracy of the a priori estimation, A^T is the transposed matrix of A, and $X_{k=0} = X_0$, $P_{k=0} = P_0$.

According to [23,25], although the gain of Kalman filter K_k is time-varying, it always converges in a few steps to guarantee the system is detectable, so it can be defined as follows:

$$K \triangleq K_k = P_{k|k-1}C^T[CP_{k|k-1}C^T + R]^{-1} \tag{15}$$

At the same time, in order to simplify the analysis, it is usually assumed that the initial state of an ICPS with a linear state feedback controller is stable. Based on the LQR controller used in control systems, we assumed it is used in the ICPS to minimize the cost function, and the usefulness of the controller is to minimize the cost function J' as much as possible as follows:

$$J \triangleq \min \lim_{T\to\infty} E\frac{1}{T}\left[\sum_{k=0}^{T-1}(e_k^T W e_k + u_k^T U u_k)\right] \tag{16}$$

where $e_k = x_k - \widetilde{x}_k$ and the matrices of W and U are assumed as positive semi-definite matrices.

When an ICPS is attacked by a DoS attack, the attacker's intention is to transfer the running zone Ω_1 to other zones which will certainly increase the time delay. The increase of time delay means increasing the cost function, which also adds to the system's operation cost. Obviously, the communication time delay located in the network layer caused by a DoS attack will increase the cost function of the control system located in the physical layer. That is to say, the purpose of a malicious attacker is to degrade the stable running state of the control system of the physical layer by attacking the network layer, so Problem 3.1 can be rewritten as:

Problem 4.1 (Attacker's Purpose):

$$\begin{cases} \max \quad J \\ s.t. \quad I_H = 1 \end{cases} \tag{17}$$

It uses a Kalman filter to provide a system optimal state estimate of $\widetilde{x}_k$, so it can be obtained that:

$$\widetilde{x}_k = \widetilde{x}_{k|k-1} + K[y_k - C\widetilde{x}_{k|k-1}] \tag{18}$$

and we can get the optimal control law of LQR with fixed gain:

$$u_k = -(B^T S B + U)^{-1} B^T S A \widetilde{x}_k \tag{19}$$

where matrix S satisfies the Riccati equation:

$$S = A^T S A + W + A^T S B (B^T S B + U)^{-1} B^T S A \tag{20}$$

If we want to keep the ICPS running stably, we must make sure both J and the error are not unbounded. That is to say, it can be determined whether there is a DoS attack from whether the cost function J is bounded.

Simultaneously, it also defines a threshold function J_{th} J_{th}:

$$J_{th} \triangleq \max \lim_{T\to\infty} E\frac{1}{T}\left[\sum_{k=0}^{T-1}(e_k^T W e_k + u_k^T U u_k)\right] \tag{21}$$

so the detector works successfully with the following condition:

$$\begin{cases} J > J_{th} \quad , \quad alarm \\ J \leq J_{th} \quad , \quad no \quad alarm \end{cases} \tag{22}$$

This can trigger an attack alarm under DoS attack when the cost function exceeds the threshold.

4.2. Mimicry Security of Defense Policy

According to the DoS attack model, when an ICPS with one sub-system running is under attack, it could increase the time delay or even the rise of control cost as depicted in Problem 3.1 or Problem 4.1. In this sub-section, a mimicry security method is presented to solve this problem, which includes

a state management and a mimicry switch strategy. It requires every sub-system to be waiting for running in real time. The state management is listening to all sub-systems' running states, inputs, outputs, detection of DoS attacks and other running state variables. The mimicry switch strategy is responsible for switching the running sub-system equipped with different network configurations and same control algorithm on the basis of switch rules from the attack detection of state management, which is depicted in the following Figure 8.

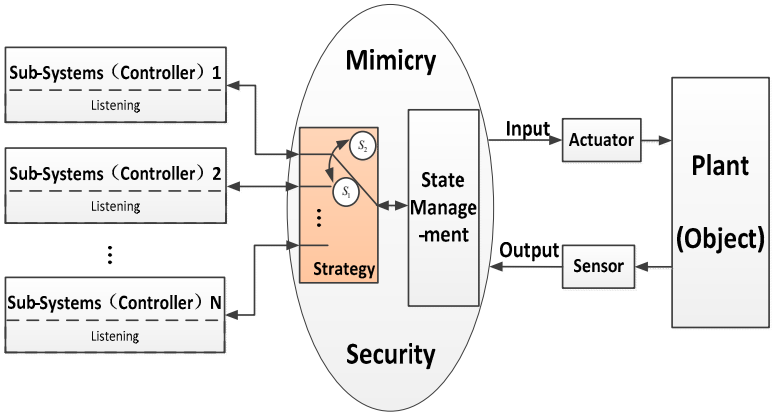


Figure 8. Mimicry security defense strategy.

From Subsection 3.3, it is known that the ICPS is secure when it is running in Ω_1. That means we can keep the ICPS running normally, whether the defense strategy is used or not. Only when the ICPS is running in the Ω_2 state under attack, we must adopt the mimicry defense strategy in time, keep the physical part stable, and ensure it is not operating in Ω_3, so the function of the defense strategy is to solve Problem 3.1 (or Problem 4.1) which can be rewritten as the following Problem 4.2 under the condition of the mimicry transformation time $T_{\sigma(\cdot)}$:

Problem 4.2

$$\begin{cases} g_{\sigma(\bullet)}(o_i) \\ s.t. \quad I_H = 1 \\ s.t. \quad T_{\sigma(\bullet)} \end{cases} \tag{23}$$

According to Equation (10), when $I_H = 1$*, which means* $\Omega_{ICPS} \in (\Omega_2 \cup \Omega_3)$ *Combined with Remark 2, we know* $\Omega_{ICPS} \in \Omega_2$*.* $\because P(\Omega_{ICPS} \in \Omega_2 | I_H = 1) = P(\Omega_{ICPS} \in \Omega_2)$*, so Equation (23) becomes:*

$$\begin{cases} g_{\sigma(\bullet)}(o_i) \\ s.t. \quad (\Omega_{ICPS} \in \Omega_2) \\ s.t. \quad T_{\sigma(\bullet)} \end{cases} \tag{24}$$

$\because \sup \quad T_{ICPS} = \tau_1 \therefore \inf \quad (\tau_2 - T_{ICPS}) = \tau_2 - \tau_1 = \tau$*. Combined with equations (1) and (2), Equation (24) becomes:*

$$\begin{cases} f_{\sigma(t)}(t) \\ \begin{cases} \dot{x}(t) = A_{\sigma(t)}x(t) + B_{\sigma(t)}u(t) \\ y(t) = C_{\sigma(t)}x(t) \end{cases} \\ s.t. \quad (\Omega_{ICPS} \in \Omega_2) \\ s.t. \quad T_{\sigma(\cdot)} \leq \tau \end{cases} \tag{25}$$

From the above analysis, we know a new sub-system with new network configuration is waiting to run. Based on Equation (4), once the ICPS adopted a mimicry security to defend a DoS attack,

the cyber part can work normally immediately, which will make the attack useless by transferring the ICPS to the Ω_1 from the Ω_2.

As is known to us, the sub-systems of ICPSs are changed after eliminating the impact of the cyber layer. However, if we want to protect the whole ICPS, we must keep the balance of the physical part. Hence, the problem that the mimicry security strategy needs to solve is changed from Problem 4.2 to Problem 4.3:

Problem 4.3

$$\begin{cases} \dot{x}(t) = A_{\sigma(t)}x(t) + B_{\sigma(t)}u(t) \\ y(t) = C_{\sigma(t)}x(t) \\ s.t. \quad T_{\sigma(\bullet)} \leq \tau \\ \sigma(\bullet) : J \geq J_{th} \end{cases} \tag{26}$$

If we want to make the ICPS free from paralysis, we should not only eliminate adverse effects from the network part, but also ensure the physical plant keeps running normally. When we adopt mimicry security strategy to switch sub-systems with different cyber parameters, it makes the system's cyber part be free from malicious actions instantly, so we need to design a switching controller to guarantee the every sub-system is running after switching.

Combined with equations (1), (2), (11) and (22), the switching signal $\sigma(\bullet) : J \geq J_{th}$ can be converted into $\sigma(\bullet) : \lim\limits_{T\to\infty} E\frac{1}{T}\left[\sum\limits_{k=0}^{T-1}(e_k^T W e_k + u_k^T U u_k)\right] \geq J_{th}$.

Define a switching sequence: $\{x_k; i_1, i_2, \cdots, i_k, \cdots | i_k \in N, k = 0, 1 \ldots.\}$. Therefore, the physical plant with feedback gain is:

$$\begin{cases} \dot{x}(t) = A_{\sigma(t)}x(t) + B_{\sigma(t)}u(t) \\ y(t) = C_{\sigma(t)}x(t) \\ s.t. \quad T_{\sigma(\cdot)} \leq \tau \\ \sigma(\bullet) : J \geq J_{th} \end{cases} \tag{27}$$

To keep the ICPS running normally, it is also needed to make $J \leq J_{th}$ after using the mimicry switch strategy, so the solution to Problem 4.3 becomes how to design a switching feedback gain $K = \{K_i \mid i = 0,1....,N\}$. If we want to keep the new sub-system stable after a mimicry switch, we need a positive definite matrix P [26,27]. At the same time, according to Theorem 1 in paper [28], the system must satisfy a bound to achieve a guaranteed cost function:

$$\begin{cases} A_i^T P A_i - P + Q + K_i^T R K_i < 0 \\ J \leq X_0^T P X_0 \end{cases} \tag{28}$$

Proof of Equation 28. Considering a known definite matrix P, and a Lyapunov function $V(x(k))$,

Make $V(x(k)) = x(k)^T P x(k) = \sum\limits_{i=1}^{N} V_i(x(k))$

Obviously: $V(x(k)) = 0$ only $x(k) = 0$; and $V(x(k)) > 0$ when $x(k) \neq 0$. Then:

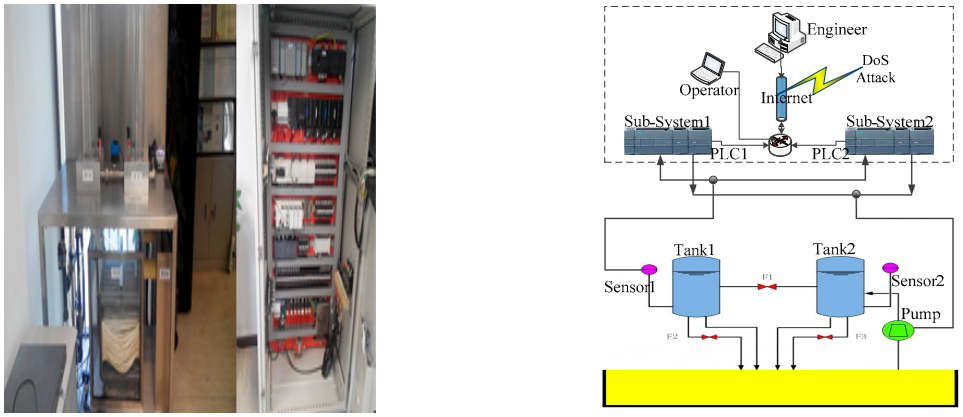
$$\begin{aligned}
\Delta V(x(k)) = \quad & x(k+1)^T P x(k+1) - x(k)^T P x(k) \\
= & \sum_{i=1}^{N} \Delta V_i(x(k)) = \sum_{i=1}^{N} (V_i(x(k+1)) - V_i(x(k))) \\
= & \sum_{i=1}^{N} [((A_i + B_i K_i)x(k))^T P((A_i + B_i K_i)x(k)) - x(k)^T P x(k)] \\
= & \sum_{i=1}^{N} [(\overline{A}_i x(k))^T P(\overline{A}_i x(k)) - x(k)^T P x(k)] \\
= & \sum_{i=1}^{N} [x(k)^T \overline{A}_i^T P \overline{A}_i x(k) - x(k)^T P x(k)] \\
= & \sum_{i=1}^{N} [x(k)^T (\overline{A}_i^T P \overline{A}_i - P) x(k)]
\end{aligned}$$

From (28): $\Delta V(x(k)) < 0$.

5. Experiments

In this section, we do some experiments to test our algorithms on a platform as depicted in Figure 8 which used a real industrial control system equipped with some industrial computers, sensors, electric motors, programmable logic controllers, a network server, cloud server and so on. Besides, this typical ICPS communicated by a network as shown in Figure 9.

On this experimental platform, we use two Siemens' programmable logic controllers (PLCs), which were set to two different IP addresses and two communication ports. The workflow of this platform is that the pump will pump some water into Tank 2 and keep a certain liquid level when the valve F_1 between Tank 1 and Tank 2 and the valve F_2 are opened. In our paper, we use the state of liquid level H that is the system response as an indicator to show whether the ICPS is being attacked by a DoS attack. The steady state of this liquid level H and sampling time are set as 400 mm and 0.2 s, respectively.



(**a**) (**b**)

Figure 9. This is the platform used in our experiments. (**a**) Test Platform Entity; (**b**) Test Platform Framework.

5.1. Related Network Feature

In this subsection, we analyze the effect on the ICPS's cyber part caused by DoS attacks with different attack rates. We repeat the DoS attacks against the PLC controller of ICPS 100 by the Monte Carlo method to get details of the network features used in the communication network. Firstly, we designed a probe to test the communication time delay between the PLC controller and the upper

computer located in the Alibaba cloud server. Secondly, we used the hping3 network tool to implement DoS attacks with different attack rates for at least 1 minute each time. Then, we made use of the probe to randomly test the time delay for 60 to 600 s. What's more, this experiment was repeated 100 times. Finally, it the statistical data was achieved and the relation between attack rate and time delay (TD) were obtained, as displayed in Table 1 and Figures 10–14.

Table 1. The time delay caused by different DoS attack rates.

Attack Rate	0	0.1	1	10	100	1000	10000	100000
Min TD (ms)	29.170	30.876	30.539	30.812	30.892	179.614	4850.917	5000
Max TD (ms)	157.017	156.437	130.180	327.192	232.517	369.547		
Average TD (ms)	42.224	43.352	42.251	42.139	42.430	196.638	∞	
Average Packet/s	23.647	22.552	23.081	23.162	22.962	20.807	0.691	0

Actually, the configuration software (for example: Intouch) used in industrial control systems always has a default time delay (5 s, 10 s, or 15 s and so on), which means once the time delay of data packets from the sender exceeds a default value, the system will trigger an alarm. In our paper, we set 5 s as a default value, which is the time delay threshold.

On this experimental platform, the PLC controllers send data to the upper computer and receive data from the upper computer. A 5 s socket timeout was designed, which means that if new data was not sent or new data was not accepted for more than five seconds, the communication connection was considered broken. In Table 1, ∞ indicates that the PLC controller's network has crashed due to a high attack DoS attack rate.

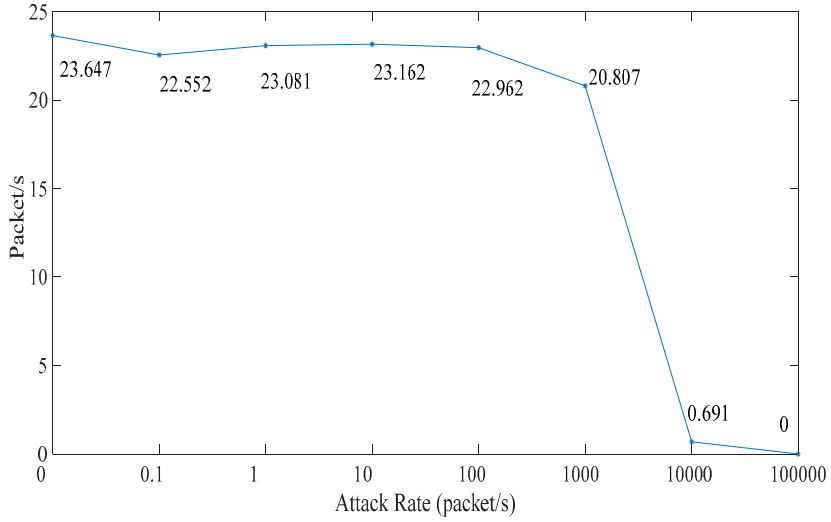


Figure 10. Test packet number per-second under different DoS attack rates.

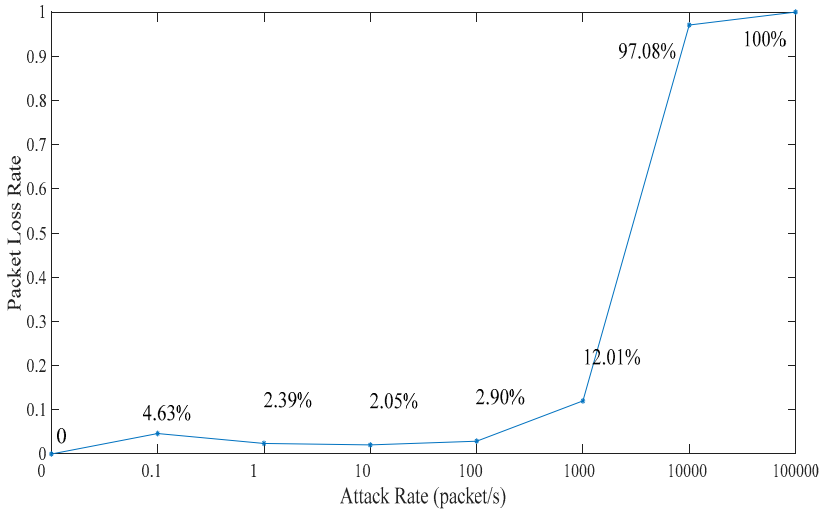


Figure 11. Test packet loss rate under different DoS attack rates.

The number of test packets from the probe is relatively stable when the attack rate is less than 1000. However, the change is sharply reduced when the attack rate is more than 1000 as seen in Figure 10. It can be seen that the packet loss rate is opposite to the above test packets numbers from the probe in Figure 11. When the attack rate is more than 1000, the packet loss rate will sharply increase until no packet data exists.

We can get that the maximum, minimum and average time delay of ICPS's network from Figures 12–14, respectively. No matter which the time delay it, its data trend is basically the same. They all reflect that the communication delay will increase with the rise of DoS attack rates until the network services has crashed undoubtedly, but every kind of time delay has only a little change when that attack rate is less than 1000.

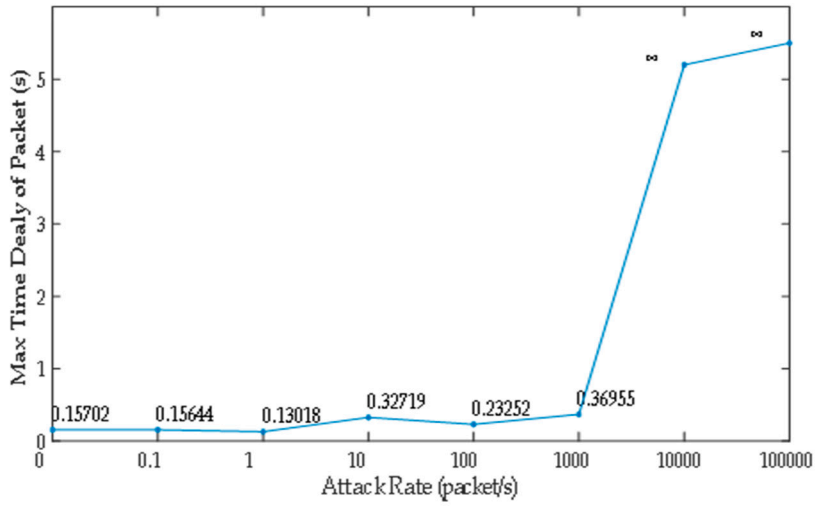


Figure 12. Max transmission time delay under different DoS attack rates.

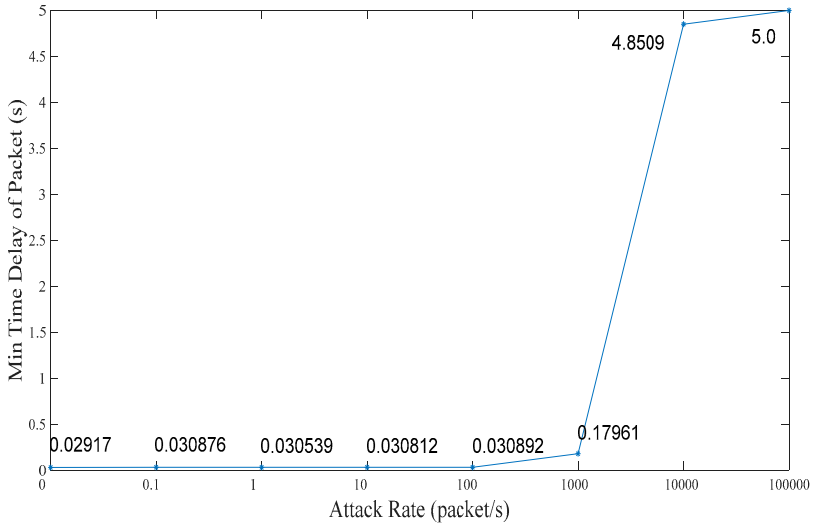


Figure 13. Min transmission time delay under different DoS attack rates.

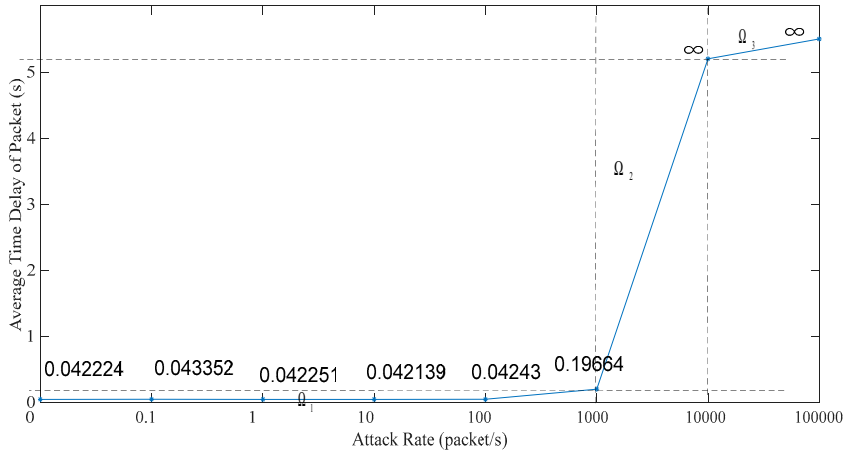


Figure 14. Average transmission time delay under different DoS attack rates.

The above table and charts show that the normal running of ICPS will not be affected by malicious attacks when the attack rate is less than a certain value. Usually, if the ICPS is not attacked by a DoS attack or the ICPS is under the DoS attack with an attack rate lower than fr_2, the time delay must be in the range Min TD to Max TD. Due to the performance limitations of network devices, the time delay can't be less than Min TD. Once the time delay exceeds Max TD, the performance of the ICPS will be destroyed. The randomness of time delay makes us select Average TD as an indicator to show the network performance. That is to say, we don't have to consider DoS attacks when the ICPS is running in the Ω_1 zone, which also demonstrates the correctness of Section 4.2.

5.2. Mimicry Security Strategy

In this subsection, we analyze the effect on an ICPS's physical part against DoS attack with different attack rates. The liquid level H (system response) and cost function of ICPS are illustrated in detail here, when it is in stable status.

Figure 15 depicts the system response without a DoS attack. We can see that no matter which sub-system was used, the ICPS whose sub-systems had different IP addresses and ports could stabilize the liquid level of platform at the same height H = 400 mm without a DoS attack.

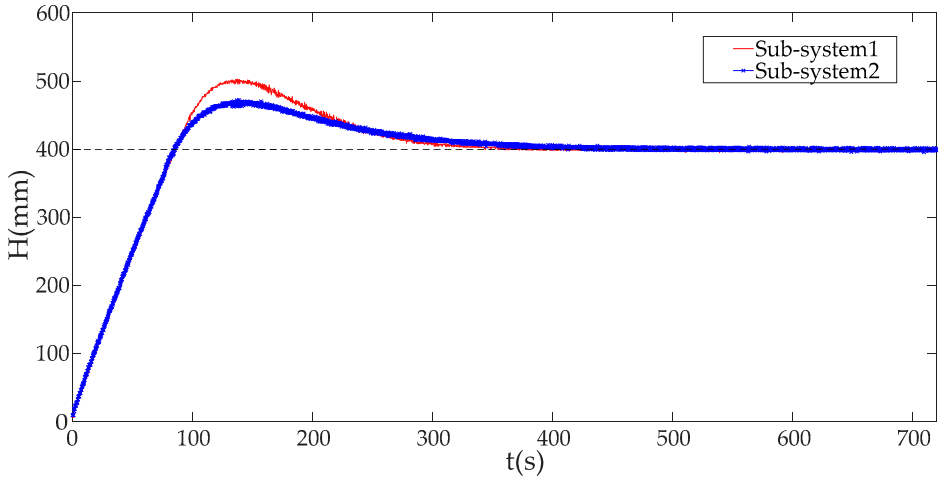


Figure 15. The system responses with different sub-system without DoS attack.

Figure 16 shows that system can keep running normally in the Ω_1 zone (including Ω_{11} and Ω_{12}) and Ω_2, but not in the Ω_3 zone. That is to say, the physical plant will not function well once that DoS attack rate exceeds a certain value. This has proved the validity of security zones.

Combining Figures 10–16, we can conclude that this ICPS is not affected by DoS attacks within a certain range of attack rates. However, once the DoS attack rate is more than a threshold, this malicious action will seriously damage the natural communication function of the cyber part, and will also affect the normal operation of the physical plant seriously in turn.

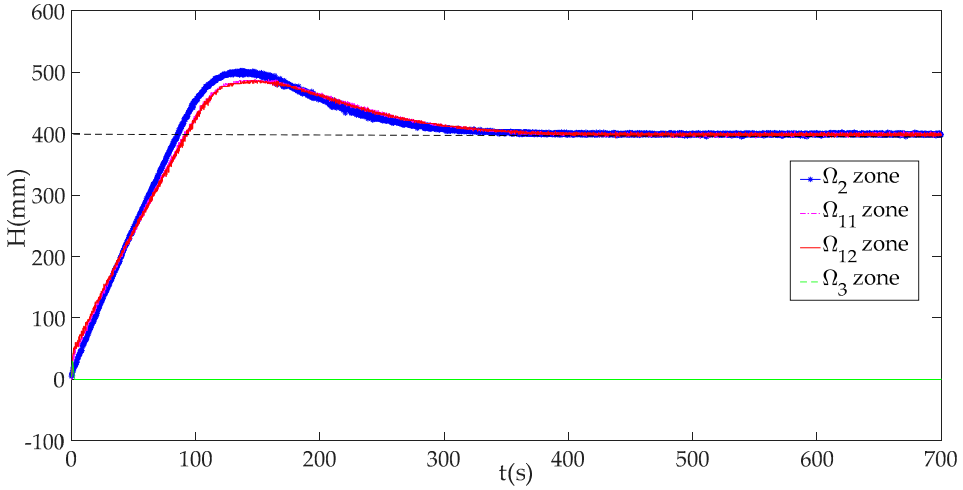


Figure 16. System responses in different zones.

We can see that the cost function value is very small and relatively stable in the stable running state of the control system in Figure 17, but, it will increase sharply under DoS attack with an attack rate of 1000 as shown in Figure 18.

Comparing Figure 17 with Figure 18, it can be seen that the cost function value J of ICPS will be enlarged more times. Obviously, once the DoS attack is launched by malicious attackers, we must have $J > J_{th}$, which will trigger an alarm.

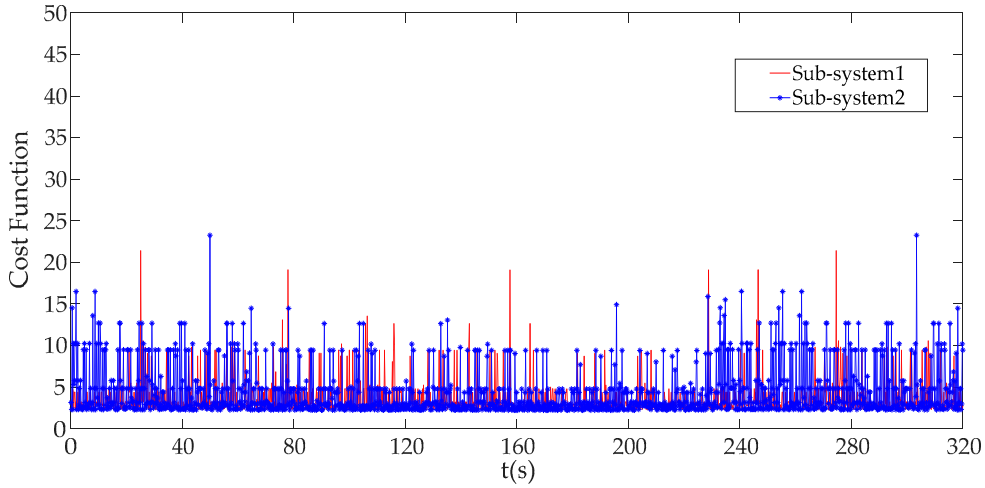


Figure 17. The cost function without DoS attack.

When an alarm is triggered, the mimicry security strategy will be used to protect the ICPS against the DoS attack. In our paper, we take sub-system 1 and sub-system 2 as an example. When the ICPS is under a DoS attack with an attack rate greater than 1000, the liquid tank level H controlled by the physical plant with sub-system1 begins to become unstable, and the same situation happens to sub-system2; However, when we use the mimicry security switch strategy to switch sub-system 2 with IP2 and port 2, the original ICPS equipped with sub-system 1 with IP1 and port1 become stable again, which is the same as switching ICPS's sub-system 2 to sub-system 1 as displayed in Figure 19.

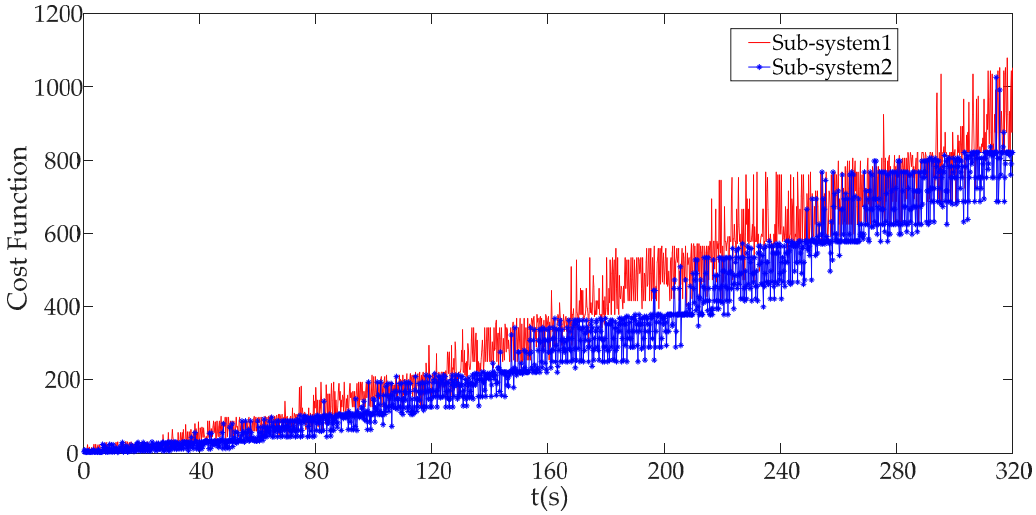


Figure 18. The cost function under DoS attack with an attack rate of 1000.

There is no doubt that the mimicry security strategy can solve the DoS attack against ICPS, which proves that this defense strategy is effective.

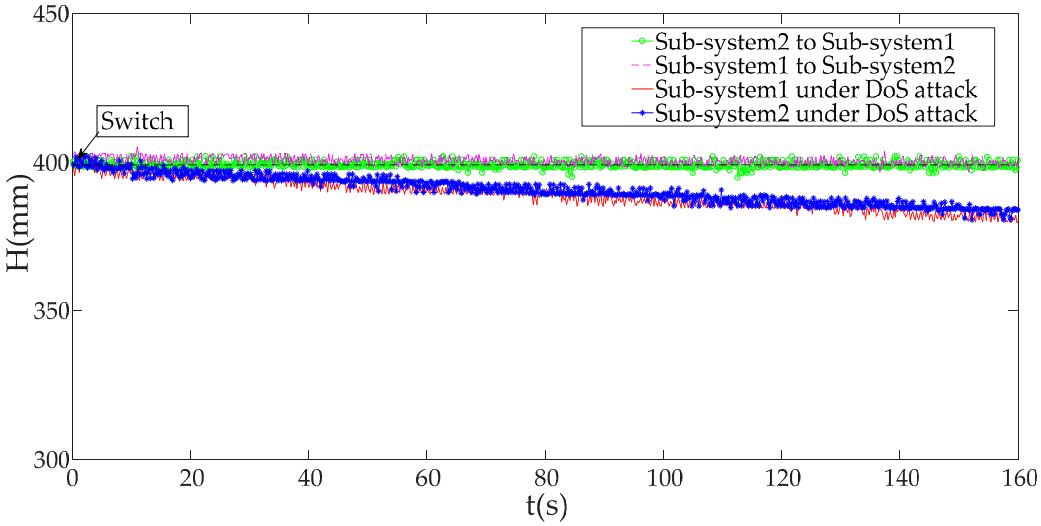


Figure 19. Different system responses before and after using the switch strategy.

5.3. Results Comparison

In this subsection, we compare with some experimental results using different methods to show details about the effectiveness of method proposed by us. In our paper, a predicted model-based algorithm [29,30] is selected as a contrast to show the usefulness of our proposed method. Figure 20 shows the comparisons of experimental results under different DoS attack rates. Obviously, both our method and the predicted method can eliminate the impacts on the physical plant caused by DoS attacks under the attack a rate of 1000 as is shown in Figure 20a. However, when the ICPS is under DoS attack with a rate of 10,000, our method can still work to keep the operation stable, while the method based on model prediction is invalid.

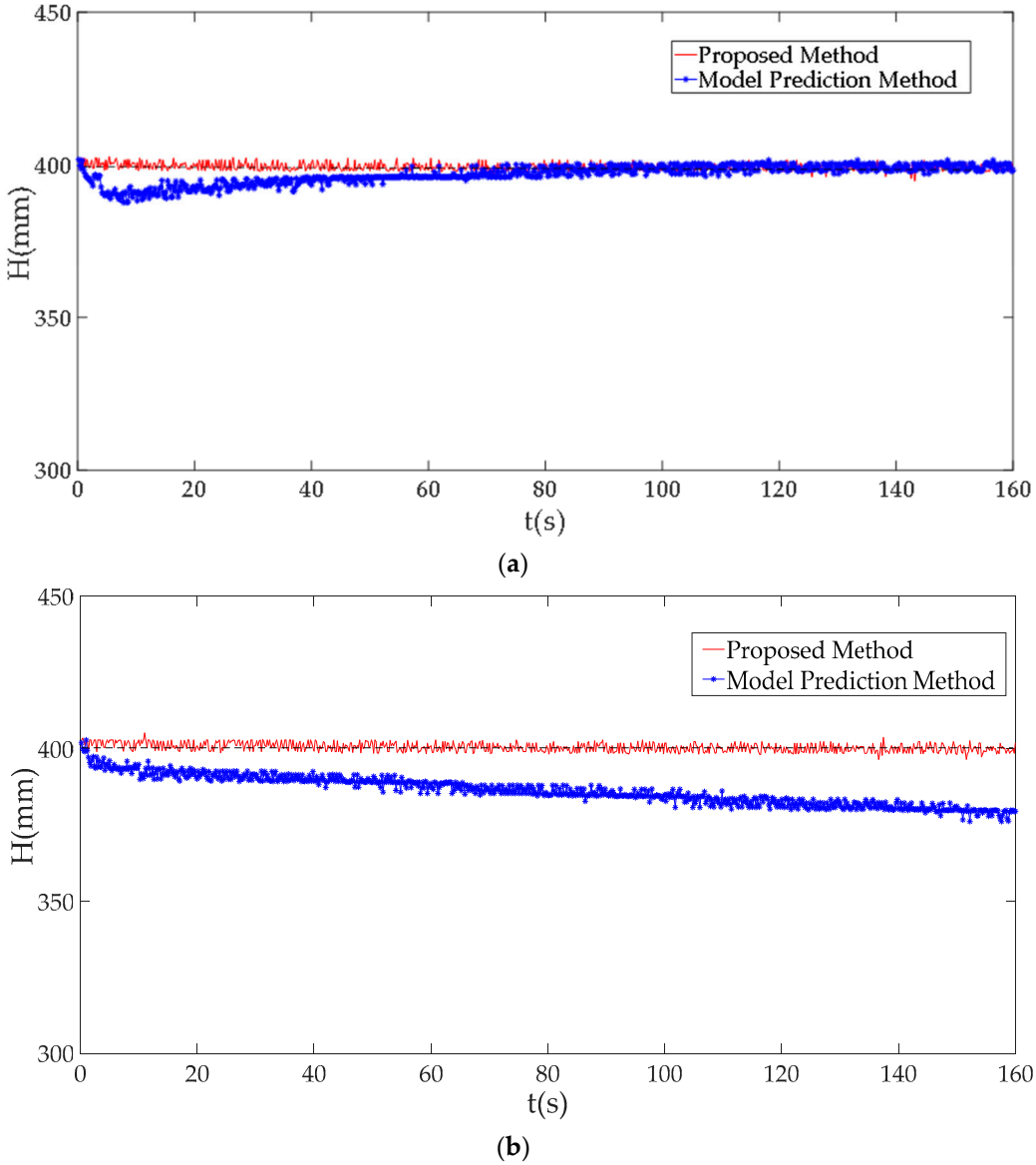


Figure 20. The comparison of results using different methods. (**a**) Experimental results under a DoS attack rate of 1000; (**b**) Experimental results under a DoS attack rate of 10,000.

Figure 21 shows that the comparisons of different packet loss of experimental results when we use different methods. It is obvious that this malicious attack can't affect the packet loss when the ICPS was under a DoS attack with an attack rate of less than 1000, which is equivalent to saying that that the ICPS is running in Ω_1. However, when the attack rate is more than 1000 ($\Omega_2 \cup \Omega_3$), and our method can solve this serious network problem through switching to a new sub-system equipped with a new IP address and communication port. The method based on model prediction does not have this function.

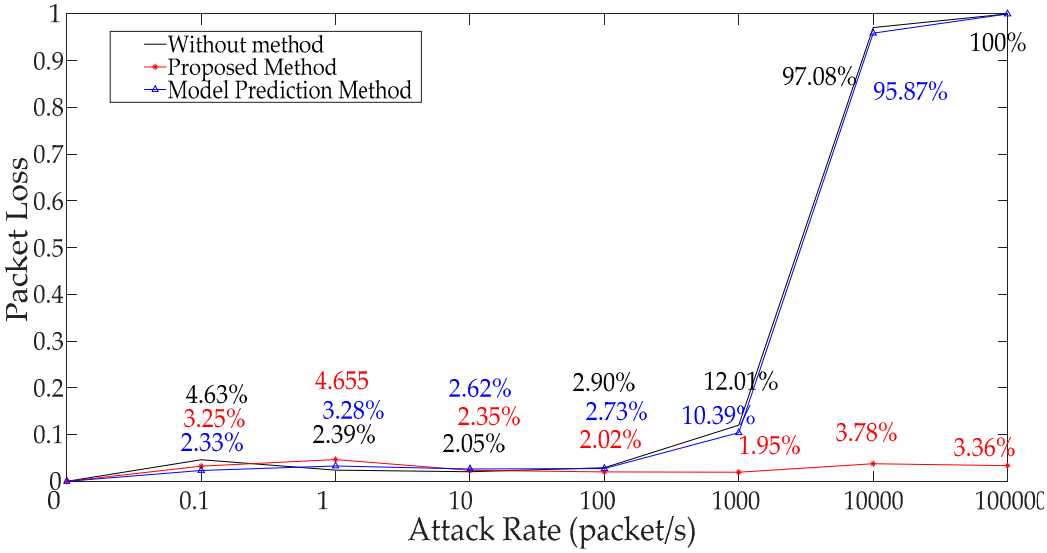


Figure 21. Different packet losses using different methods.

Figure 22 depicts the comparison of different average time delays of experimental results when we use the different methods. It can be obtained that our method can deal with the huge time delays caused by the DoS attack when the attack rate is more than 1000 and less than 10,000 (Ω_2), especially the controller crash problem when the attack rate is more than 10,000 (Ω_3), but, the predicted method based on the model cannot clear up it.

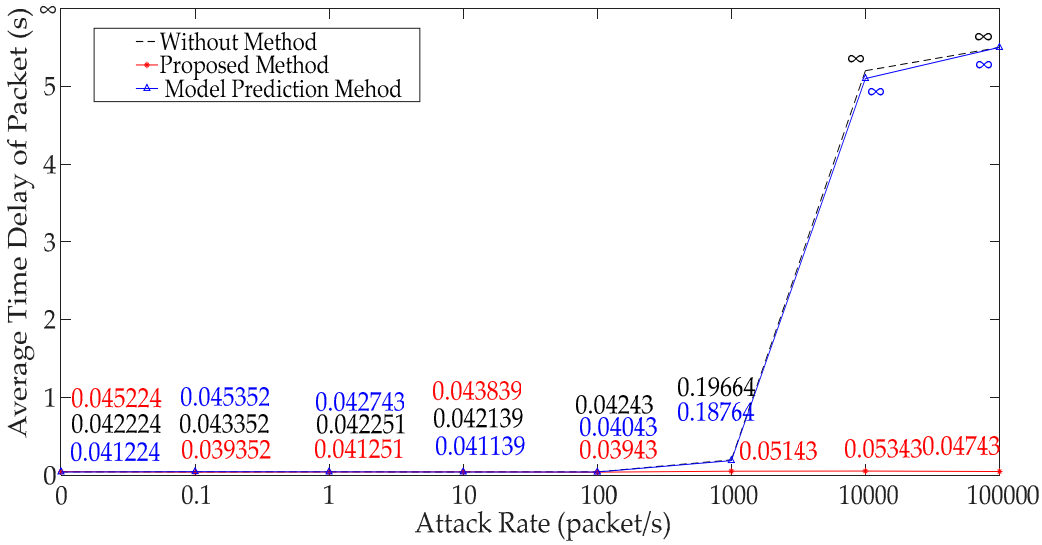


Figure 22. Different time delays using different methods.

From Figures 20–22, we know that the method proposed by us not only solves the network problems caused by DoS attacks, but also can maintain the normal operation of the ICPS. The algorithm based on model prediction is still unable to handle the cyber problem caused by this DoS attack with great attack rates. Even the physical process can't remain stable when the attack rate is too large ($\Omega_2 \cup \Omega_3$).

Obviously due to the resilient control ability of network devices, some DoS attacks with low attack rates cannot affect the normal operation of an ICPS. Previous works will produce some false alarms and reduce the detection accuracy, because of the existing resilient ability of network devices. Most models built by previous works don't consider specific DoS attacks, which is equivalent to studying the situation of ICPS running in zones Ω_1, Ω_2 and Ω_3. However, our paper takes this robustness of

network devices into consideration and it is simplified further by studying their operation conditions in different security zones. That is to say, we don't need the DoS attacks of Ω_1, so all we have to deal with is the DoS attacks of Ω_2 and Ω_3, which need to be detected no matter which method is used. When the DoS attacks which belong to zones of Ω_2 and Ω_3 are launched, our method not only detects this malicious action, but also maintains the physical process stable and eliminates the serious impact on the cyber layer, while the method based on model prediction cannot deal with the two aspects of the problem at the same time.

6. Conclusions

In this paper, we study DoS attack problems and build related mathematic models to explain how DoS attacks affect the stable operation of ICPSs with different attack rates, which are based on studying the impacts of attacks on the cyber part and physical plant, respectively.

According to different attack rates, we divide them into different running zones firstly, which is consistent with facts. Then, we build a DoS attack model and explain the effect on an ICPS against attack actions using the above zones instead of analyzing the time delay from ICPSs' control data directly, which also shows clearly that the ICPS has a defense ability against malicious DoS attacks. The time delays ought to be negligible and the impact is fatal once the DoS attack rate exceeds a threshold. What's more, we chose the cost function value as a norm to detect anomalous actions and propose a mimicry security switch strategy to defend against such malicious attacks. Finally, we modeled a lot of DoS attacks and used a mimicry switch strategy repeatedly. From the above table and charts we can obviously see the impacts on the ICPS's cyber part and physical plant caused by this malicious action. The comparisons with different experimental results also verify our model's correctness and our method's effectiveness.

Author Contributions: J.G. established experiment platform, provided experimental data after conducting numerous experiments and then composed the first draft of this paper; S.C. provided research methods for this paper and also improved it; B.Z. helped revise and finalize the paper; Y.X. revised the paper, and provided the research methods.

Funding: This work has been supported by National Natural Science Foundation of China (No.61573061).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lee, E.A. Cyber Physical Systems: Design Challenges. In Proceedings of the 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA, 5–7 May 2008.
2. Shang, W.; Zeng, P.; Wan, M.; Li, L.; An, P. Intrusion detection algorithm based on OCSVM in industrial control system. *Secur. Commun. Netw.* **2016**, *9*, 1040–1049. [CrossRef]
3. ICS-CERT Analysis on the Current Situation of Industrial Information Security in China in 2018. Available online: https://www.ics-cert.org.cn/portal/page/132/72be03492e944039a7a750bdb17bd42e.html (accessed on 28 July 2018).
4. Teixeira, A.; Perez, D.; Sandberg, H.; Johansson, K.H. Attack models and scenarios for networked control systems. In Proceedings of the 1st ACM International Conference on High Confidence Networked Systems, HiCoNS'12, Beijing, China, 17–19 April 2012; Association for Computing Machinery: Beijing, China, 2012; pp. 55–64.
5. Krotofil, M.; Manning, B.; Larsen, J. CPS: Driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals. In Proceedings of the Computer Security Applications Conference, New Orleans, LA, USA, 8–12 December 2014.
6. Bayou, L.; Espes, D.; Cuppens-Boulahia, N.; Cuppens, F. A Prediction-Based Method for False Data Injection Attacks Detection in Industrial Control Systems. In Proceedings of the International Conference on Risks and Security of Internet and Systems, Arcachon, France, 16–18 October 2018.
7. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter. *IEEE Trans. Control Netw. Syst.* **2014**, *1*, 370–379. [CrossRef]

8. Yang, Q.; Yang, J.; Yu, W.; An, D.; Zhang, N.; Zhao, W. On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 717–729. [CrossRef]
9. Yuan, C.; Kar, S.; Moura, J.M.F. Dynamic Attack Detection in Cyber-Physical Systems with Side Initial State Information. *IEEE Trans. Autom. Control* **2017**, *6*, 4618–4624.
10. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. A Secure Control Framework for Resource-Limited Adversaries. *Automatica* **2015**, *51*, 135–148. [CrossRef]
11. Pasqualetti, F.; Dorfler, F.; Bullo, F. Attack Detection and Identification in Cyber-Physical Systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
12. Han, D.; Mo, Y.; Xie, L. Convex Optimization Based State Estimation against Sparse Integrity Attacks. *arXiv*, 2015; arXiv:1511.07218.
13. Sha, W.; Zhu, Y.; Chen, M.; Huang, T. Statistical Learning for Anomaly Detection in Cloud Server Systems: A Multi-Order Markov Chain Framework. *IEEE Trans. Cloud Comput.* **2015**, *6*, 401–413. [CrossRef]
14. Zhang, H.; Cheng, P.; Shi, L.; Chen, J. Optimal DoS Attack Scheduling in Wireless Networked Control System. *IEEE Trans. Control Syst. Technol.* **2016**, *24*, 843–852. [CrossRef]
15. Pasqualetti, F.; Dorfler, F.; Bullo, F. Attack Detection and Identification in Cyber-Physical Systems—Part II: Centralized and Distributed Monitor Design. *arXiv*, 2012; arXiv:1202.6049.
16. Abusitta, A.; Bellaiche, M.; Dagenais, M. An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment. *J. Cloud Comput.* **2018**, *7*, 9. [CrossRef]
17. Zhang, L.; Wang, X.; Jiang, Y.; Yang, M.; Mak, T.; Singh, A. Effectiveness of HT-assisted Sinkhole and Blackhole Denial of Service Attacks Targeting Mesh Networks-on-chip. *J. Syst. Arch.* **2018**, *89*, 84–94. [CrossRef]
18. Malekpour, A.; Ragel, R.; Ignjatovic, A.; Parameswaran, S. DoSGuard: Protecting pipelined MPSoCs against hardware Trojan based DoS attacks. In Proceedings of the IEEE International Conference on Application-specific Systems, Seattle, WA, USA, 10–12 July 2017.
19. Yuan, Y.; Yuan, H.; Lei, G.; Yang, H.; Sun, S. Resilient Control of Networked Control System under DoS Attacks: A Unified Game Approach. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1786–1794. [CrossRef]
20. Zhou, W.; Jia, W.; Wen, S.; Xiang, Y.; Zhou, W. Detection and defense of application-layer DDoS attacks in backbone web traffic. *Future Gener. Comput. Syst.* **2014**, *38*, 36–46. [CrossRef]
21. Chen, Y.; Kar, S.; Moura, J.M.F. Optimal Attack Strategies Subject to Detection Constraints Against Cyber-Physical Systems. *IEEE Trans. Control. Netw. Syst.* **2017**, *5*, 1157–1168. [CrossRef]
22. Fawzi, H.; Tabuada, P.; Diggavi, S.N. Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks. *IEEE Trans. Autom. Control.* **2014**, *59*, 1454–1467. [CrossRef]
23. Mo, Y.; Garone, E.; Casavola, A.; Sinopoli, B. In False data injection attacks against state estimation in wireless sensor networks. In Proceedings of the Conference on Decision and Control, Atlanta, GA, USA, 15–17 December 2010; pp. 5967–5972.
24. Pang, Z.; Liu, G.; Zhou, D.; Hou, F.; Sun, D. Two-Channel False Data Injection Attacks Against Output Tracking Control of Networked Systems. *IEEE Trans. Ind. Electron.* **2016**, *63*, 3242–3251. [CrossRef]
25. Mo, Y.; Chabukswar, R.; Sinopoli, B. Detecting Integrity Attacks on SCADA Systems. *IEEE Trans. Control. Syst. Technol.* **2014**, *22*, 1396–1407.
26. Malmborg, J.; Bernhardsson, B.; Astrom, K.J. A Stabilizing Switching Scheme for Multi Controller Systems. *IFAC Proc. Vol.* **1996**, *29*, 2627–2632. [CrossRef]
27. Gao, H.; Liu, X.; Lam, J. Stability Analysis and Stabilization for Discrete-Time Fuzzy Systems with Time-Varying Delay. *Syst. Man Cybern.* **2009**, *39*, 306–317.
28. Wang, R.; Liu, G.; Wang, W.; Rees, D.; Zhao, Y.B. Guaranteed Cost Control for Networked Control Systems Based on an Improved Predictive Control Method. *IEEE Trans. Control. Syst. Technol.* **2010**, *18*, 1226–1232. [CrossRef]
29. Pang, Z.H.; Liu, G.P.; Dong, Z. Secure Networked Control Systems under Denial of Service Attacks. *IFAC Proc. Vol.* **2011**, *44*, 8908–8913. [CrossRef]
30. Pang, Z.H.; Liu, G.P. Design and Implementation of Secure Networked Predictive Control Systems under Deception Attacks. *IEEE Trans. Control. Syst. Technol.* **2012**, *20*, 1334–1342. [CrossRef]