aerospace

MDPI

Article

Research on Game Theory of Air Traffic Management Cyber Physical System Security

Zhijun Wu, Ruochen Dong and Peng Wang *

College of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China; zjwu@cauc.edu.cn (Z.W.); kfdongruochen@163.com (R.D.)
* Correspondence: pwang_cauc@163.com

Abstract: For the air traffic management cyber physical system, if an attacker successfully obtains authority or data through a cyber attack, combined with physical attacks, it will cause serious consequences. Game theory can be applied to the strategic interaction between two parties, especially if the two parties have different goals. The offensive and defensive game process of the air traffic management cyber physical system is a non-cooperative and incomplete information dynamic game. The attacker can choose to camouflage the type of attack launched. The attack detection device configured in the system has a certain probability that the attack type can be successfully detected. According to the type of attack detected, the defender updates the posterior belief of the attack type and selects the corresponding protective strategies. According to the game process of offense and defense, a dynamic Bayesian game model of the air traffic management cyber physical system is established, the possible perfect Bayesian Nash equilibrium and its existence conditions are solved, and a complete mathematical model is constructed. The analysis shows that the dynamic Bayesian game model of the air traffic management cyber physical system can help the system defender to quickly obtain an equilibrium strategy and reduce the loss of the system as much as possible.

Keywords: air traffic management system; cyber physical system; dynamic bayesian game; offensive and defensive strategy; bayesian nash equilibrium

Citation: Wu, Z.; Dong, R.; Wang, P. Research on Game Theory of Air Traffic Management Cyber Physical System Security. *Aerospace* **2022**, *9*, 397. https://doi.org/10.3390/aerospace9080397

Academic Editor: Álvaro Rodríguez-Sanz

Received: 9 June 2022
Accepted: 21 July 2022
Published: 23 July 2022

1. Introduction

Cyber Physical System (CPS) was proposed by the National Aeronautics and Space Administration (NASA) in 1992. It is a complex system that deeply integrates cyber systems and physical systems [1], and is an important support for the integration strategy of informatization and industrialization [2]. CPS was originally used in the aerospace field by the United States, and later in the military field by the US Department of Defense. It defines "3C (Computation, Communication, Control)" as the technical core [3] and is applied to the "5C (Connection, Conversion, Cyber, Cognition, Configuration)" architecture of manufacturing systems [4]. The control field mainly uses actuators for feedback, the communication field mainly uses sensors for interaction, and the computing field uses cloud platforms and distributed computing to make intelligent decisions. The CPS architecture is shown in Figure 1.

Traditional embedded systems emphasize the use of limited computing resources to improve the performance of physical equipment by embedding the computer system into physical equipment under the constraints of the physical equipment environment. Different from traditional embedded systems, CPSs deeply integrate computing, communication and control capabilities, emphasizing the high interaction and real-time nature of cyber systems and physical systems. By relying on the powerful computing resources of the cyber system to assist decision-making, the physical system can be sensed and controlled [5].

As a large and complex system, the air traffic management (ATM) system still needs to consume a lot of manpower and other resources to maintain its flight, communication,

navigation and scheduling. The vision of designing an air traffic management cyber-physical system (ATMCPS) is to make the operation and scheduling of civil aviation aircraft more efficient and intelligent, and further promote the application of CPS in the aviation field.

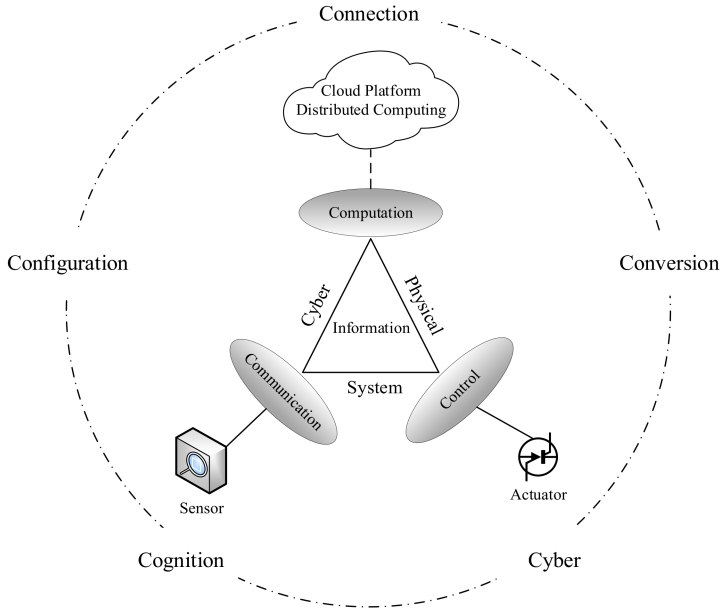

Figure 1. CPS Architecture.

The CPS also faces more serious security threats while using the powerful computing and decision-making capabilities of the cyber system to feedback and adjust the physical system. In 2010, the core control system of Iran's nuclear power plant was invaded by "Stuxnet" virus and issued false instructions to nuclear power plant equipment, causing the nuclear reactor to be paralyzed on a large scale. It is proved that attacking cyber systems can cause serious physical damage to critical infrastructure, and even endanger national security [6]. In 2012, the "Trojan.Milicenso" virus caused thousands of printers in the United States, India and other countries to lose control, and continued to print meaningless characters until the resources were exhausted [7]. In 2015, the "BlackEnergy" virus attacked Ukrainian substations, which led to large-scale blackouts [8]. Compared with the 9·11 incident, if the attackers successfully hijacked civil aviation airliners through cyber attacks, combined with physical attacks, it will cause more serious consequences.

Regarding the attack issued by the attacker, if the system defender can select the optimal protection strategy in the first time, the loss caused by the attack can be reduced to the greatest extent. Game theory can be applied to the strategic interaction between two parties, especially if the two parties have different goals.

In order to guarantee the safe operation of the system, this paper proposes a protection model of ATMCPS based on dynamic Bayesian game. The system defender has an initial belief in the attack type, and updates the belief according to the attack type detected by the attack detection device to generate a posterior belief, solve the expected income under different protection strategies, and select the optimal protection strategy. The system defender can make corresponding protection strategies according to the protection model proposed in this paper to reduce the loss of the system.

The major contributions of this paper are as follows:

(1) Focus on the application of the CPS in the ATM field, and design the architecture of the ATMCPS.
(2) Pay attention to the judgment of the system defender on the real attack intention when two attack types exist at the same time and the attacker will camouflage the attack type. The game model is established based on the dynamic Bayesian game, and the

system defender will update the belief according to the detected attack characteristics, which is more in line with the actual attack and defense scenarios.

The rest of this paper is organized as follows. Section 2 describes the related work. Section 3 designs the architecture of the ATMCPS. Section 4 defines the game model, analyzes the game process, and explains related parameters and model assumptions. By solving the income matrix under all combinations of attack and defense strategies, the equilibrium strategies existing in the game model are analyzed, and all possible equilibrium strategies and their existence conditions are solved. Section 5 analyzes the performance of the model and verifies the feasibility of the model. Section 6 concludes this paper and looks forward to the future work.

2. Related Work

The ATMCPS has a good prospect in the development of the next generation of civil aviation system. Krishna Sampigethaya, a technical researcher at Boeing, proposed the CPS architecture in the future aviation system. In the cabin, cyber and physical integration can be realized through advanced electronic equipment, sensors and other devices, and the cabin environment can be automatically controlled to create the most comfortable environment for passengers and crew members. At the same time, as the service life of the aircraft increases, it may degrade the performance of the aircraft and cause system failures. In the future, the inspection and maintenance process of aircraft must be automated, real-time and continuous. The physical state of cabin assets is assessed, corresponding lifecycle data is stored, and automatic maintenance is performed in the event of component failure. The entire ATM system achieves efficient management and automatic dispatch through the tight integration and coordinated control of communication, navigation, and surveillance between ground-to-ground, ground-to-air, and air-to-air [9]. Based on a multi-dimensional, multi-view, multi-paradigm and multi-tool comprehensive method, Lichen Zhang [10] used formal modeling to analyze and design the various subsystems of the aviation CPS. Cyber systems are modeled using Architecture Analysis and Design Language (AADL), and physical systems are modeled using Modelica. Faisal Alrefaei [11] described the layered architecture of the aviation CPS, and analyzed the new challenges and security issues faced by the aviation CPS. Xinglong Wang [12] et al. constructed an air traffic CPS model. By improving the K-shell algorithm, the nodes with greater influence in the air traffic network were identified and protected to avoid large-scale paralysis of the air traffic network caused by node failure.

Because the ATMCPS has the characteristics of high integration of physical space and cyber space, while providing powerful computing resources for the operation of the system, attackers can also affect physical facilities through cyber attacks. In 2008, Spanish Airline Flight 5022 crashed due to a malware attack that affected the onboard central computer [13]. On 5 December 2011, the Iranian military announced that its "electronic warfare unit" had hijacked the advanced U.S. RQ-170 UAV with a "hacker hijacking" method, and released a video showing the RQ-170 UAV on 9 December 2011. Therefore, how to ensure the safe and stable operation of the system has become a major challenge.

In recent years, there have been more and more researches using game theory methods to analyze CPS security. Long Li [14] established the Stackelberg game model of the network layer, and regarded the attacker and the defender as followers and leaders. When the actions taken by others are known, calculate the performance indicator under the Stackelberg game: the signal to interference noise ratio (SINR), and then analyze the stability and security of the system. Wei Tai [15] studied the cyber offensive and defensive game process of the CPS of the power grid, and established a two-layer offensive and defensive model of the power system. The two-person zero-sum game is used to solve the optimal offensive and defensive strategies of both parties, and the influence of information symmetry on the optimal offensive strategy is studied. Hamed Orojloo [16] et al. abstracted the operational status of the CPS as the transition between different states such as penetration, destruction, recovery, etc., and solved the Nash equilibrium under pure strategy and mixed strategy

by calculating the income matrix of both offensive and defensive strategies in different states. Quantitative evaluation of the system is carried out by defining two evaluation indicators of attack failure time and system availability. Based on the non-cooperative game model, Jithish J [17] captures the factors that affect the credibility of the sensor nodes of the CPS, and evaluates the credibility of the sensor nodes of the CPS. Using the Nash equilibrium solution, the trust threshold is obtained, and the sensor nodes below the trust threshold are regarded as potentially malicious nodes, and deleted or isolated to ensure the safe operation of the CPS. Based on incomplete information zero-sum game, Bingjing Yan [18] et al. constructed a dynamic network security defense strategy for power CPS. Through multi-dimensional analysis of the asset value of each node, the Markov belief is dynamically updated to ensure the rational allocation of resources when defense resources are limited. Jun Li [19] built a static Bayesian game model for both offense and defense to help system defenders judge the attacker's attack type. By solving the existing Nash equilibrium, determining the type of attacker, using the reverse analysis method to analyze the game tree, and finding the equilibrium path.

The above research on CPS security still needs improvement in two aspects:

(1) Most researches are based on cyber attacks or physical attacks. There is a lack of relevant research on how to choose a protection strategy when the two types of attacks exist at the same time.

(2) Most researches are based on complete information games or static games, and there is still a certain gap between offensive and defensive situations in real life.

Therefore, this paper will carry out a more detailed design of the ATMCPS, and based on the dynamic game of incomplete information, study the protection strategy of defenders when facing two kinds of attacks at the same time.

3. Design of Air Traffic Management Cyber Physical System

The ATMCPS is the development direction of the next-generation ATM system. It is a complex system that deeply integrates the cyber system and the physical system, and is the application of the CPS in the aviation field. For the ATM system, the cyber system is composed of decision-making units such as ground control stations and data fusion centers, and uses the network, cloud platform and various software to feedback and adjust the physical system; the physical system includes aircraft, airports, staff and environment, etc.

The ATMCPS can be divided into four components: application layer, network layer, transmission layer and physical layer. Coordination between layers to ensure the safe and stable operation of the ATM system. The layered architecture of the ATMCPS is shown in Figure 2.

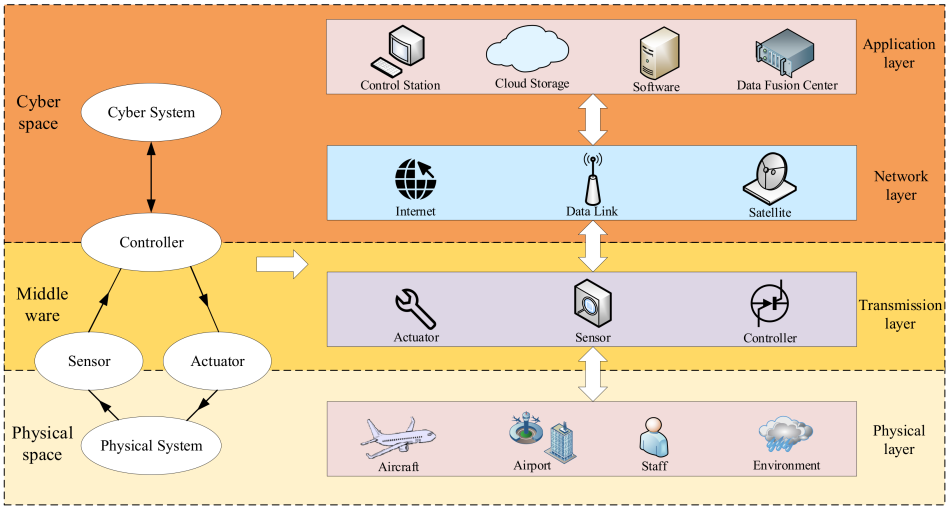

Figure 2. Layered Architecture of the ATMCPS.

(1) Physical Layer

The physical layer corresponds to the physical system in the ATMCPS, including physical elements in the ATM system, such as aircraft, airports, staff, and the environment. Sensors are used to perceive the information at the physical layer, fuse the data, and transmit it to the cyber system for calculation and analysis. According to the decision-making instructions fed back by the cyber system, the actuator is used for adjustment. For example, based on airborne data and satellite navigation information, the cyber system fuses and calculates the parameters and destinations of each aircraft in an airspace. Dynamically schedule flight routes, speeds and altitudes, reduce the workload of air traffic controllers, and realize self-awareness and self-management of air traffic situations. Similarly, as a kind of physical element, the aircraft is also a small CPS. Before and after a flight mission, the internal components of the aircraft are automatically scanned to find unsafe factors, and automated equipment is used for autonomous maintenance. For parts that cannot be repaired, the data is automatically reported to the relevant departments and the maintenance personnel are requested to maintain the equipment. During the flight, the environmental sensor can sense the environment in the cabin in real time, and combine with the meteorological environment of the airspace where the aircraft is located to calculate the most suitable temperature and humidity in the cabin, and adjust it to improve the comfort of passengers.

The physical layer is the starting point and end point of the closed-loop data flow of the CPS. Information collection and command feedback at the transmission layer, data distribution at the network layer, and intelligent decision-making at the application layer are all to enable the physical layer to adjust to a better state. For example, for the ATMCPS, when the aircraft is flying according to the original route, it suddenly encounters extreme bad weather or an accident ahead. For safety of flight, the cyber system can calculate the optimal solution based on multi-party data, such as environmental data, other flight routes data, etc. According to the decision-making instructions issued by the cyber system, the aircraft uses middleware such as controllers and actuators to adjust physical components such as engines and rudders to complete the route conversion. Through the self-organization, self-decision and self-adjustment of the whole system, it helps the aircraft to dynamically adjust the route in real time, ensures the efficiency and safety of the flight, and simplifies the communication and coordination process of the ground control personnel.

For the physical layer, attackers can destroy physical devices, affecting the stable operation of the system, or destroy sensor devices, network devices, etc., affecting data communication.

(2) Transmission Layer

The transmission layer is the link in the ATMCPS. The transmission layer collects the state information of the physical system, preprocesses the information, and transmits it to the cyber system for analysis. The cyber system issues corresponding decision-making instructions by analyzing the data of the physical system. The transmission layer converts the issued decision-making instructions, and adjusts the physical state of the physical system through the controller and the actuator. The cyber system and the physical system communicate and cooperate with each other through the transmission layer, forming a closed-loop circulation of data. The transmission layer mainly consists of three parts: sensors, controllers and actuators. The sensor senses the state of the physical layer and obtains raw data. The actuator performs feedback adjustment to the physical layer according to the decision-making instructions issued by the cyber system. The controller mainly plays the role of data fusion, data transmission, and instruction conversion.

For the transmission layer, the most important issue is to ensure the confidentiality, integrity and reliability of the transmitted data. As the link between the cyber system and the physical system, if the transmitted information is intercepted and tampered by an attacker, the calculation and analysis results of the cyber system may be different from the actual physical system operating conditions. The cyber system will issue wrong decision-

making instructions, which may even affect the normal scheduling of aircraft and the stable operation of the ATM system in severe cases.

(3) Network Layer

The network layer mainly involves the distribution and storage of data. Navigation satellites provide navigation data for calculations and decisions of cyber system. In terms of ground-to-air communication and air-to-air communication, multiple aircraft in the same airspace can exchange information through data link technology. By sensing the weather conditions and aircraft heading in the airspace, combined with the satellite-based navigation technology that may be developed in the future, the aircraft can dynamically plan and adjust the route. The ATM command center can use digital twin technology to conduct digital twin modeling based on the perception data of the aircraft's internal sensors and real-time data uploaded to the cloud to monitor the operation of the aircraft in real time. If the pilot gets out of control [20] or loses the ability to control in an unexpected situation, the ground control center can use the ground-air data link technology to take over and control the flight according to the digital twin model, and realize the control authority of the aircraft on the ground.

The characteristics of decentralization, non-tampering, non-forgery, and collective maintenance of blockchain have good application prospects in the data storage of the ATMCPS. As a type of blockchain, consortium chain is supported by national security standards. By participating in bookkeeping, industry alliance members reach consensus internally, simplifying the number of nodes, making the system run more efficiently, and speeding up data interaction on the basis of security and trustworthiness. The application of blockchain ensures the data security of the ATMCPS to a certain extent [21].

(4) Application Layer

As the top layer of the ATMCPS, the application layer is the intelligent decision-making center of the entire system. All data are collected here for calculation and analysis, and corresponding decision-making instructions are issued, which are transmitted to the physical layer for adjustment. Artificial intelligence algorithms have a good development prospect in massive data processing and analysis. It should be noted that the existing system often needs to be controlled and issued manually. The identity of the crew members in the next-generation ATMCPS will be converted from the operator to the supervisor. Communication, monitoring, navigation and other systems can independently adjust and make decisions according to the operating conditions of the physical layer, and can learn autonomously based on past experience to deal with emergencies.

At the same time, system defenders need to focus on security issues at the application layer, especially data tampering and unauthorized access by attackers. In the 9·11 incident, the attackers launched a terrorist attack by hijacking a plane and crashing into a building. While causing losses, they also paid a heavy price. But if attackers can invade cyber systems and issue fake instructions to manipulate physical systems, they can cause serious losses at a very small cost, which will be very serious.

The ATMCPS model is shown in Figure 3. In the ATMCPS, the cyber system and the physical system are closely integrated and frequently interact. The closed-loop flow of data within the system enables the system to be continuously optimized to achieve a spiral upward trend. At the same time, attackers can also use the cyber space as a springboard to attack the physical system, thereby affecting the operation of the entire system. Attackers can launch two different types of attacks, physical attacks and cyber attacks. Although attackers use cyber space as the entry point for attacks, it is different from the traditional concept. Cyber attacks are the theft of data, information, or interference with information transmission, while physical attacks are the acquisition of control authority or the destruction of critical infrastructure. Therefore, it is necessary to have a more accurate judgment on the type of attack, and take corresponding defensive strategies, which can reduce the loss of the system as much as possible.

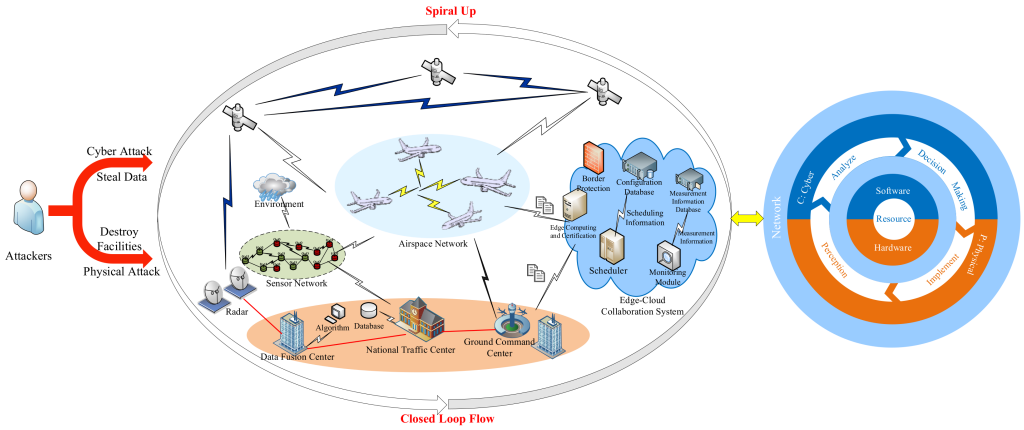

Figure 3. ATMCPS Model.

4. Dynamic Bayesian Game Model of ATMCPS

This paper focuses on the strategic interaction between the attacker and the defender. In the face of unknown attackers and attack methods, how should the system defender protect themselves to minimize the possible losses. This section will analyze the game process, construct a dynamic Bayesian game model, and solve all possible pure-strategy Nash equilibria.

4.1. Game Model Definition

The dynamic Bayesian game model of ATMCPS can be defined as a seven-tuple:

$$CPSG = \{P, S, U, T, R, D, F\} \tag{1}$$

(1) $P = \{P_A, P_S, P_N\}$ represents the set of participants. P_A stands for attacker, P_S stands for system defender, and P_N stands for "Nature" in the Harsanyi transformation.

(2) $S = \{S_A, S_S\}$ represents the set of strategy. $S_A = \{S_{A0}, S_{A1}\}$ is the attacker's strategy set, S_{A0} means that the attacker camouflage the attack type, S_{A1} means that the attacker does not camouflage the attack type. $S_S = \{S_{S0}, S_{S1}\}$ is the defender's strategy set, S_{S0} is physical protection, and S_{S1} is cyber protection.

(3) $U = \{U_A, U_S\}$ represents the set of income functions. U_A represents the income function of the attacker, and U_S represents the income function of the system.

(4) $T = \{T_0, T_1\}$ represents the set of attack types. T_0 means physical attack, T_1 means cyber attack.

(5) $R = \{R_0, R_1\}$ represents the set of attack types displayed by the attacker after the camouflage or non-camouflage strategy. R_0 represents that the attack feature displayed by the attacker is a physical attack, and R_1 represents the attack feature displayed by the attacker is a cyber attack. For example, if an attacker conducts a camouflage strategy for an attack of type T_0, the attack feature displayed is R_1, and if a non-camouflage strategy is performed, the displayed attack feature is R_0.

(6) $D = \{D_0, D_1\}$ represents the set of attack types detected by the system's attack detection device. D_0 indicates that the detection result is a physical attack, and D_1 indicates that the detection result is a cyber attack.

(7) $F = \{F_0, F_1\}$ represents a set of beliefs. F_0 represents the initial belief of the defender, and F_1 represents the updated posterior belief of the defender.

4.2. Symbol Description

The parameters required in the model are defined as follows. Among them, the value range of the relevant parameters of probability is (0, 1), and the value range of relevant parameters of cost, benefit and loss is (0, $+\infty$)

$\boldsymbol{\mu}$: The probability of a physical attack, that is, the defender's initial belief that the attacker will launch a physical attack.

$\boldsymbol{\alpha}$: The detection success rate of the attack detection device when the attack type is camouflaged.

$\boldsymbol{\beta}$: The detection success rate of the attack detection device when the attack type is not camouflaged.

$\boldsymbol{p(T_i)}$: The defender's initial belief about the type of attack. (i = 0, 1)

$\boldsymbol{p(T_i \mid D_k)}$: The defender's posterior belief about the type of attack. (i = 0, 1; k = 0, 1)

$\boldsymbol{C_P}$: All costs for the attacker to launch a physical attack.

$\boldsymbol{C_C}$: All costs for the attacker to launch a cyber attack.

$\boldsymbol{C_I}$: The cost for the attacker to camouflage the type of attack.

$\boldsymbol{E_{AP}}$: The benefit that the attacker can obtain after successfully launching a physical attack.

$\boldsymbol{E_{AC}}$: The benefit that the attacker can obtain after successfully launching a cyber attack.

$\boldsymbol{M_P}$: The cost for the defender to choose the strategy for physical protection.

$\boldsymbol{M_C}$: The cost for the defender to choose the strategy for cyber protection.

$\boldsymbol{L_{SP}}$: The loss of the system when the attacker successfully attacks the physical system.

$\boldsymbol{L_{SC}}$: The loss of the system when the attacker successfully attacks the cyber system.

4.3. Model Assumption

Assumption 1. *In the entire game process, all participants are in a rational state, that is, the goal of each participant is to protect their own maximum incomes.*

Assumption 2. *If the protection type selected by the defender does not match the attack type launched by the attacker, it is equivalent to no protection strategies.*

Assumption 3. *The benefit of the attacker's successful attack is greater than the cost of the attack (including the cost of camouflage), and the loss of the defender being attacked is greater than the cost of protection.*

Assumption 4. *The detection success rate of the attack detection device configured in the system under the attacker's non-camouflage attack is greater than the detection success rate under the camouflage attack, that is,* $\beta > \alpha$.

4.4. Offensive and Defensive Game Process

The complete offensive and defensive game process is shown in Figure 4. In 1967, Harsanyi proposed the method of the Harsanyi transformation [22], by introducing a virtual participant: "Nature", so that the game of incomplete information can be solved. The defender can know the probability of the attacker launching the two types of attacks and set it as the initial belief. The attacker has two strategies when launching an attack, camouflaging or not camouflaging the attack type. If the attack type is camouflaged, the attack characteristic displayed is the attack characteristic of another attack type. The ATMCPS is equipped with an attack detection device. When it is attacked, it can identify the type of attack based on the attack characteristics displayed. For the attacker's camouflage attack and non-camouflage attack, the attack detection devices have different detection success rates. The system defender updates the initial beliefs based on the attack type detected by the detection device and the detection success rate of the device to form a posterior belief, and judges the attacker type based on the posterior belief, and selects the corresponding protection strategy.

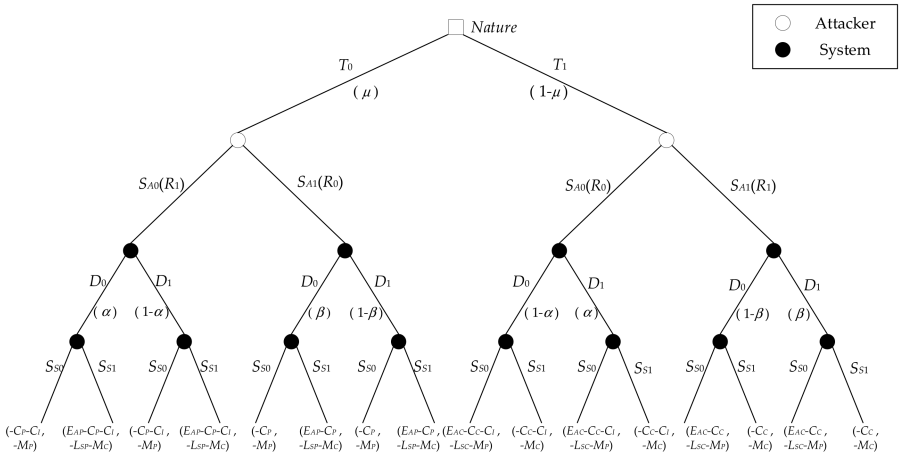

Figure 4. The Process of Offensive and Defensive Game.

Then, an example is used to show the process of dynamic game from the perspective of the defender:

(1) Before the attack occurs, the defender has an initial belief about the type of attack according to the existing information and historical data, that is, the defender has an initial judgment on the probability of the attacker launching a physical attack;
(2) The defender has a partial understanding of the attacker's behavior. For example, the defender can know that the attacker will camouflage the attack type when launching a physical attack, but will not camouflage the attack type when launching a cyber attack;
(3) When the system is attacked, the attack detection device detects and judges the attack type according to the attack characteristics;
(4) The defender updates the posterior belief according to the initial belief, the detection success rate of the attack detection device, and the detected attack type. For example, calculating the probability that the actual attack type is a physical attack when a physical attack is detected, and the probability that the actual attack type is a cyber attack when a cyber attack is detected;
(5) Calculate the expected income under the combination of strategies and determine the protection strategies according to the initial belief, the posterior belief, the cost of physical protection and cyber protection, and the loss of physical attack and cyber attack. For example, if the attacker's strategy is: when launching a physical attack, the attack type will be camouflaged, and when launching a cyber attack, the attack type will not be camouflaged. The defender selects physical protection when detecting a physical attack, and selects cyber protection when detecting a cyber attack. This combination of strategies can minimize the loss of the system. The defender will choose this set of strategies.

4.5. Belief Renewal

The initial beliefs of the system defenders regarding the types of attacks are:

$$p(T_0) = \mu \tag{2}$$

$$p(T_1) = 1 - \mu \tag{3}$$

When the system is under attack, the defender updates the posterior belief of the attack type according to the attack type detected by the attack detection device:

$$p(T_i|D_k) = \frac{p(T_i, D_k)}{p(D_k)},\ (i = 0, 1;\ k = 0, 1) \tag{4}$$

Expanding the above formula according to the total probability theorem, it can be concluded that the update formula of the posterior belief is shown in formula (5):

$$p(T_i|D_k) = \frac{\sum_{j=0}^{1} p(D_k|T_i,R_j)\cdot p(R_j|T_i)\cdot p(T_i)}{\sum_{i=0}^{1}\sum_{j=0}^{1} p(D_k|T_i,R_j)\cdot p(R_j|T_i)\cdot p(T_i)} \quad (5)$$

The value of $p(R_j \mid T_i)$ is 0 or 1. For example, if an attacker camouflages a T_0 type of attack, then $p(R_0 \mid T_0) = 0$, $p(R_1 \mid T_0) = 1$. The attack strategy of attacker has four groups:

$$[(T_0, S_{A0}), (T_1, S_{A0})]; [(T_0, S_{A0}), (T_1, S_{A1})]; [(T_0, S_{A1}), (T_1, S_{A0})]; [(T_0, S_{A1}), (T_1, S_{A1})]$$

According to the type of attack detected, the defender uses formula (5) to update the posterior beliefs under the four attack strategies. The updated posterior beliefs are shown in Table 1.

Table 1. The Posterior Beliefs of Defenders under Different Attack Strategies.

Attack Strategy	Posterior Belief	
$(T_0, S_{A0}), (T_1, S_{A0})$	$p(T_0\|D_0) = \frac{\alpha\cdot\mu}{\alpha\cdot\mu+(1-\alpha)\cdot(1-\mu)}$ $p(T_0\|D_1) = \frac{(1-\alpha)\cdot\mu}{(1-\alpha)\cdot\mu+\alpha\cdot(1-\mu)}$	$p(T_1\|D_0) = \frac{(1-\alpha)\cdot(1-\mu)}{\alpha\cdot\mu+(1-\alpha)\cdot(1-\mu)}$ $p(T_1\|D_1) = \frac{\alpha\cdot(1-\mu)}{(1-\alpha)\cdot\mu+\alpha\cdot(1-\mu)}$
$(T_0, S_{A0}), (T_1, S_{A1})$	$p(T_0\|D_0) = \frac{\alpha\cdot\mu}{\alpha\cdot\mu+(1-\beta)\cdot(1-\mu)}$ $p(T_0\|D_1) = \frac{(1-\alpha)\cdot\mu}{(1-\alpha)\cdot\mu+\beta\cdot(1-\mu)}$	$p(T_1\|D_0) = \frac{(1-\beta)\cdot(1-\mu)}{\alpha\cdot\mu+(1-\beta)\cdot(1-\mu)}$ $p(T_1\|D_1) = \frac{\beta\cdot(1-\mu)}{(1-\alpha)\cdot\mu+\beta\cdot(1-\mu)}$
$(T_0, S_{A1}), (T_1, S_{A0})$	$p(T_0\|D_0) = \frac{\beta\cdot\mu}{\beta\cdot\mu+(1-\alpha)\cdot(1-\mu)}$ $p(T_0\|D_1) = \frac{(1-\beta)\cdot\mu}{(1-\beta)\cdot\mu+\alpha\cdot(1-\mu)}$	$p(T_1\|D_0) = \frac{(1-\alpha)\cdot(1-\mu)}{\beta\cdot\mu+(1-\alpha)\cdot(1-\mu)}$ $p(T_1\|D_1) = \frac{\alpha\cdot(1-\mu)}{(1-\beta)\cdot\mu+\alpha\cdot(1-\mu)}$
$(T_0, S_{A1}), (T_1, S_{A1})$	$p(T_0\|D_0) = \frac{\beta\cdot\mu}{\beta\cdot\mu+(1-\beta)\cdot(1-\mu)}$ $p(T_0\|D_1) = \frac{(1-\beta)\cdot\mu}{(1-\beta)\cdot\mu+\beta\cdot(1-\mu)}$	$p(T_1\|D_0) = \frac{(1-\beta)\cdot(1-\mu)}{\beta\cdot\mu+(1-\beta)\cdot(1-\mu)}$ $p(T_1\|D_1) = \frac{\beta\cdot(1-\mu)}{(1-\beta)\cdot\mu+\beta\cdot(1-\mu)}$

There are four groups of protection strategies for system defenders:

$$[(D_0, S_{S0}), (D_1, S_{S0})]; [(D_0, S_{S0}), (D_1, S_{S1})]; [(D_0, S_{S1}), (D_1, S_{S0})]; [(D_0, S_{S1}), (D_1, S_{S1})]$$

The optimal protection strategy and optimal attack strategy can be calculated by Formulas (6) and (7) [23]:

$$S_S^* = arg\max_{S_S} \sum_{i=0}^{1} p(T_i|D_k)\cdot U_S(S_A^*, S_S) \quad (6)$$

$$S_A^* = arg\max_{S_A} \sum_{h=0}^{1} p(D_h|T_k, S_{Ai})\cdot U_A(S_A, S_S^*) \quad (7)$$

4.6. Income Matrix

There are 16 combinations of offensive and defensive strategies for attackers and system defenders. Under each combination of offensive and defensive strategies, both offense and defense have different income functions. The expected incomes of both parties under the 16 offensive and defensive strategy combinations are shown in Tables 2 and 3.

Table 2. Income Function of the Attacker.

	(T_0, S_{A0}), (T_1, S_{A0})	(T_0, S_{A1}), (T_1, S_{A0})
(D_0, S_{S0}), (D_1, S_{S0})	$E_{AC} - C_P - C_C - 2C_I$	$E_{AC} - C_P - C_C - C_I$
(D_0, S_{S0}), (D_1, S_{S1})	$(1-\alpha)\cdot(E_{AP} + E_{AC}) - C_P - C_C - 2C_I$	$(1-\beta)\cdot E_{AP} + (1-\alpha)\cdot E_{AC} - C_P - C_C - C_I$
(D_0, S_{S1}), (D_1, S_{S0})	$\alpha\cdot(E_{AP} + E_{AC}) - C_P - C_C - 2C_I$	$\beta\cdot E_{AP} + \alpha\cdot E_{AC} - C_P - C_C - C_I$
(D_0, S_{S1}), (D_1, S_{S1})	$E_{AP} - C_P - C_C - 2C_I$	$E_{AP} - C_P - C_C - C_I$
	(T_0, S_{A0}), (T_1, S_{A1})	(T_0, S_{A1}), (T_1, S_{A1})
(D_0, S_{S0}), (D_1, S_{S0})	$E_{AC} - C_P - C_C - C_I$	$E_{AC} - C_P - C_C$
(D_0, S_{S0}), (D_1, S_{S1})	$(1-\alpha)\cdot E_{AP} + (1-\beta)\cdot E_{AC} - C_P - C_C - C_I$	$(1-\beta)\cdot(E_{AP} + E_{AC}) - C_P - C_C$
(D_0, S_{S1}), (D_1, S_{S0})	$\alpha\cdot E_{AP} + \beta\cdot E_{AC} - C_P - C_C - C_I$	$\beta\cdot(E_{AP} + E_{AC}) - C_P - C_C$
(D_0, S_{S1}), (D_1, S_{S1})	$E_{AP} - C_P - C_C - C_I$	$E_{AP} - C_P - C_C$

Table 3. Income Function of the Defender.

(T_0, S_{A0}) (T_1, S_{A0})	$\frac{-\alpha\cdot\mu\cdot M_P-(1-\alpha)\cdot(1-\mu)\cdot(L_{SC}+M_P)}{\alpha\cdot\mu+(1-\alpha)\cdot(1-\mu)} + \frac{(\alpha-1)\cdot\mu\cdot M_P+(\mu-1)\cdot\alpha\cdot(L_{SC}+M_P)}{(1-\alpha)\cdot\mu+\alpha\cdot(1-\mu)}$	(D_0, S_{S0}) (D_1, S_{S0})
	$\frac{-\alpha\cdot\mu\cdot M_P-(1-\alpha)\cdot(1-\mu)\cdot(L_{SC}+M_P)}{\alpha\cdot\mu+(1-\alpha)\cdot(1-\mu)} + \frac{(\alpha-1)\cdot\mu\cdot(L_{SP}+M_C)+(\mu-1)\cdot\alpha\cdot M_C}{(1-\alpha)\cdot\mu+\alpha\cdot(1-\mu)}$	(D_0, S_{S0}) (D_1, S_{S1})
	$\frac{-\alpha\cdot\mu\cdot(L_{SP}+M_C)-(1-\alpha)\cdot(1-\mu)\cdot M_C}{\alpha\cdot\mu+(1-\alpha)\cdot(1-\mu)} + \frac{(\alpha-1)\cdot\mu\cdot M_P+(\mu-1)\cdot\alpha\cdot(L_{SC}+M_P)}{(1-\alpha)\cdot\mu+\alpha\cdot(1-\mu)}$	(D_0, S_{S1}) (D_1, S_{S0})
	$\frac{-\alpha\cdot\mu\cdot(L_{SP}+M_C)-(1-\alpha)\cdot(1-\mu)\cdot M_C}{\alpha\cdot\mu+(1-\alpha)\cdot(1-\mu)} + \frac{(\alpha-1)\cdot\mu\cdot(L_{SP}+M_C)+(\mu-1)\cdot\alpha\cdot M_C}{(1-\alpha)\cdot\mu+\alpha\cdot(1-\mu)}$	(D_0, S_{S1}) (D_1, S_{S1})
(T_0, S_{A0}) (T_1, S_{A1})	$\frac{-\alpha\cdot\mu\cdot M_P-(1-\beta)\cdot(1-\mu)\cdot(L_{SC}+M_P)}{\alpha\cdot\mu+(1-\beta)\cdot(1-\mu)} + \frac{(\alpha-1)\cdot\mu\cdot M_P+(\mu-1)\cdot\beta\cdot(L_{SC}+M_P)}{(1-\alpha)\cdot\mu+\beta\cdot(1-\mu)}$	(D_0, S_{S0}) (D_1, S_{S0})
	$\frac{-\alpha\cdot\mu\cdot M_P-(1-\beta)\cdot(1-\mu)\cdot(L_{SC}+M_P)}{\alpha\cdot\mu+(1-\beta)\cdot(1-\mu)} + \frac{(\alpha-1)\cdot\mu\cdot(L_{SP}+M_C)+(\mu-1)\cdot\beta\cdot M_C}{(1-\alpha)\cdot\mu+\beta\cdot(1-\mu)}$	(D_0, S_{S0}) (D_1, S_{S1})
	$\frac{-\alpha\cdot\mu\cdot(L_{SP}+M_C)-(1-\beta)\cdot(1-\mu)\cdot M_C}{\alpha\cdot\mu+(1-\beta)\cdot(1-\mu)} + \frac{(\alpha-1)\cdot\mu\cdot M_P+(\mu-1)\cdot\beta\cdot(L_{SC}+M_P)}{(1-\alpha)\cdot\mu+\beta\cdot(1-\mu)}$	(D_0, S_{S1}) (D_1, S_{S0})
	$\frac{-\alpha\cdot\mu\cdot(L_{SP}+M_C)-(1-\beta)\cdot(1-\mu)\cdot M_C}{\alpha\cdot\mu+(1-\beta)\cdot(1-\mu)} + \frac{(\alpha-1)\cdot\mu\cdot(L_{SP}+M_C)+(\mu-1)\cdot\beta\cdot M_C}{(1-\alpha)\cdot\mu+\beta\cdot(1-\mu)}$	(D_0, S_{S1}) (D_1, S_{S1})
(T_0, S_{A1}) (T_1, S_{A0})	$\frac{-\beta\cdot\mu\cdot M_P-(1-\alpha)\cdot(1-\mu)\cdot(L_{SC}+M_P)}{\beta\cdot\mu+(1-\alpha)\cdot(1-\mu)} + \frac{(\beta-1)\cdot\mu\cdot M_P+(\mu-1)\cdot\alpha\cdot(L_{SC}+M_P)}{(1-\beta)\cdot\mu+\alpha\cdot(1-\mu)}$	(D_0, S_{S0}) (D_1, S_{S0})
	$\frac{-\beta\cdot\mu\cdot M_P-(1-\alpha)\cdot(1-\mu)\cdot(L_{SC}+M_P)}{\beta\cdot\mu+(1-\alpha)\cdot(1-\mu)} + \frac{(\beta-1)\cdot\mu\cdot(L_{SP}+M_C)+(\mu-1)\cdot\alpha\cdot M_C}{(1-\beta)\cdot\mu+\alpha\cdot(1-\mu)}$	(D_0, S_{S0}) (D_1, S_{S1})
	$\frac{-\beta\cdot\mu\cdot(L_{SP}+M_C)-(1-\alpha)\cdot(1-\mu)\cdot M_C}{\beta\cdot\mu+(1-\alpha)\cdot(1-\mu)} + \frac{(\beta-1)\cdot\mu\cdot M_P+(\mu-1)\cdot\alpha\cdot(L_{SC}+M_P)}{(1-\beta)\cdot\mu+\alpha\cdot(1-\mu)}$	(D_0, S_{S1}) (D_1, S_{S0})
	$\frac{-\beta\cdot\mu\cdot(L_{SP}+M_C)-(1-\alpha)\cdot(1-\mu)\cdot M_C}{\beta\cdot\mu+(1-\alpha)\cdot(1-\mu)} + \frac{(\beta-1)\cdot\mu\cdot(L_{SP}+M_C)+(\mu-1)\cdot\alpha\cdot M_C}{(1-\beta)\cdot\mu+\alpha\cdot(1-\mu)}$	(D_0, S_{S1}) (D_1, S_{S1})
(T_0, S_{A1}) (T_1, S_{A1})	$\frac{-\beta\cdot\mu\cdot M_P-(1-\beta)\cdot(1-\mu)\cdot(L_{SC}+M_P)}{\beta\cdot\mu+(1-\beta)\cdot(1-\mu)} + \frac{(\beta-1)\cdot\mu\cdot M_P+(\mu-1)\cdot\beta\cdot(L_{SC}+M_P)}{(1-\beta)\cdot\mu+\beta\cdot(1-\mu)}$	(D_0, S_{S0}) (D_1, S_{S0})
	$\frac{-\beta\cdot\mu\cdot M_P-(1-\beta)\cdot(1-\mu)\cdot(L_{SC}+M_P)}{\beta\cdot\mu+(1-\beta)\cdot(1-\mu)} + \frac{(\beta-1)\cdot\mu\cdot(L_{SP}+M_C)+(\mu-1)\cdot\beta\cdot M_C}{(1-\beta)\cdot\mu+\beta\cdot(1-\mu)}$	(D_0, S_{S0}) (D_1, S_{S1})
	$\frac{-\beta\cdot\mu\cdot(L_{SP}+M_C)-(1-\beta)\cdot(1-\mu)\cdot M_C}{\beta\cdot\mu+(1-\beta)\cdot(1-\mu)} + \frac{(\beta-1)\cdot\mu\cdot M_P+(\mu-1)\cdot\beta\cdot(L_{SC}+M_P)}{(1-\beta)\cdot\mu+\beta\cdot(1-\mu)}$	(D_0, S_{S1}) (D_1, S_{S0})
	$\frac{-\beta\cdot\mu\cdot(L_{SP}+M_C)-(1-\beta)\cdot(1-\mu)\cdot M_C}{\beta\cdot\mu+(1-\beta)\cdot(1-\mu)} + \frac{(\beta-1)\cdot\mu\cdot(L_{SP}+M_C)+(\mu-1)\cdot\beta\cdot M_C}{(1-\beta)\cdot\mu+\beta\cdot(1-\mu)}$	(D_0, S_{S1}) (D_1, S_{S1})

4.7. Proof of Equilibrium Existence

The ATMCPS game model proposed in this paper involves a total of 16 combinations of offensive and defensive strategies. Under different parameter values, there may be different equilibrium strategies. This section analyzes all possible equilibrium strategies and solves the conditions that the parameter values should satisfy when each set of equilibrium exists. For each set of equilibrium strategies, the parameters must satisfy all the equilibrium existence conditions at the same time before the equilibrium can be established.

In the game model, the existence of an equilibrium strategy means that both the attacker and the defender cannot obtain more incomes by unilaterally changing the strategy,

and the two sides will be in a state of equilibrium. That is, under this group strategy, the incomes of both the attacker and the defender are the maximum. According to the income matrix derived in Section 4.6, it can be calculated that when a certain strategy combination belongs to an equilibrium strategy, the parameters such as cost, benefit and probability should satisfy the conditions.

When the defense strategy is $[(D_0, S_{S0}), (D_1, S_{S0})]$ or $[(D_0, S_{S1}), (D_1, S_{S1})]$, the attacker's maximum profit strategy is strictly $[(T_0, S_{A1}), (T_1, S_{A1})]$. Therefore, $[(T_0, S_{A1}), (T_1, S_{A1}), (D_0, S_{S0}), (D_1, S_{S0})]$ and $[(T_0, S_{A1}), (T_1, S_{A1}), (D_0, S_{S1}), (D_1, S_{S1})]$ are possible equilibrium strategies, and the conditions for equilibrium existence are as follows:

Equilibrium 1: $[(T_0, S_{A1}), (T_1, S_{A1}), (D_0, S_{S0}), (D_1, S_{S0})]$

Existence conditions:

$$L_{SP} \geq \frac{\beta(1-\mu)(L_{SC}+M_P-M_C)}{\mu(1-\beta)} + M_P - M_C \tag{8}$$

$$L_{SP} \geq \frac{(1-\beta)(1-\mu)(L_{SC}+M_P-M_C)}{\beta\mu} + M_P - M_C \tag{9}$$

$$L_{SP} \geq \left\{1 + \frac{2\beta(1-\beta)(1-2\mu)}{\mu[2\beta\mu(1-\beta)+(1-\mu)(1+2\beta^2-2\beta)]}\right\}\cdot(L_{SC}+M_P-M_C) + M_P - M_C \tag{10}$$

Equilibrium 2: $[(T_0, S_{A1}), (T_1, S_{A1}), (D_0, S_{S1}), (D_1, S_{S1})]$

Existence conditions:

$$L_{SP} \leq \frac{\beta(1-\mu)(L_{SC}+M_P-M_C)}{\mu(1-\beta)} + M_P - M_C \tag{11}$$

$$L_{SP} \leq \frac{(1-\beta)(1-\mu)(L_{SC}+M_P-M_C)}{\beta\mu} + M_P - M_C \tag{12}$$

$$L_{SP} \leq \left\{1 + \frac{2\beta(1-\beta)(1-2\mu)}{\mu[2\beta\mu(1-\beta)+(1-\mu)(1+2\beta^2-2\beta)]}\right\}\cdot(L_{SC}+M_P-M_C) + M_P - M_C \tag{13}$$

When the defense strategy is $[(D_0, S_{S0}), (D_1, S_{S1})]$, under different parameter values, each attack strategy may be combined with the defense strategy to become an equilibrium strategy. Through calculation, four different equilibrium strategies and their corresponding existence conditions are as follows:

Equilibrium 3: $[(T_0, S_{A0}), (T_1, S_{A0}), (D_0, S_{S0}), (D_1, S_{S1})]$

Existence conditions:

$$\alpha \geq \frac{1}{2} \tag{14}$$

$$C_I \leq (\beta-\alpha)E_{AP} \tag{15}$$

$$C_I \leq (\beta-\alpha)E_{AC} \tag{16}$$

$$L_{SP} \geq \frac{(1-\alpha)(1-\mu)(L_{SC}+M_P-M_C)}{\alpha\mu} + M_P - M_C \tag{17}$$

$$L_{SP} \leq \frac{\alpha(1-\mu)(L_{SC}+M_P-M_C)}{\mu(1-\alpha)} + M_P - M_C \tag{18}$$

Equilibrium 4: $[(T_0, S_{A0}), (T_1, S_{A1}), (D_0, S_{S0}), (D_1, S_{S1})]$

Existence conditions:

$$\alpha + \beta \geq 1 \tag{19}$$

$$(\beta-\alpha)E_{AC} \leq C_I \leq (\beta-\alpha)E_{AP} \tag{20}$$

$$L_{SP} \geq \frac{(1-\beta)(1-\mu)(L_{SC}+M_P-M_C)}{\alpha\mu} + M_P - M_C \tag{21}$$

$$L_{SP} \leq \frac{\beta(1-\mu)(L_{SC}+M_P-M_C)}{\mu(1-\alpha)} + M_P - M_C \tag{22}$$

Equilibrium 5: [(T_0, S_{A1}), (T_1, S_{A0}), (D_0, S_{S0}), (D_1, S_{S1})]
Existence conditions:

$$\alpha + \beta \geq 1 \tag{23}$$

$$(\beta-\alpha)E_{AP} \leq C_I \leq (\beta-\alpha)E_{AC} \tag{24}$$

$$L_{SP} \geq \frac{(1-\alpha)(1-\mu)(L_{SC}+M_P-M_C)}{\beta\mu} + M_P - M_C \tag{25}$$

$$L_{SP} \leq \frac{\alpha(1-\mu)(L_{SC}+M_P-M_C)}{\mu(1-\beta)} + M_P - M_C \tag{26}$$

Equilibrium 6: [(T_0, S_{A1}), (T_1, S_{A1}), (D_0, S_{S0}), (D_1, S_{S1})]
Existence conditions:

$$\beta \geq \frac{1}{2} \tag{27}$$

$$C_I \geq (\beta-\alpha)E_{AP} \tag{28}$$

$$C_I \geq (\beta-\alpha)E_{AC} \tag{29}$$

$$L_{SP} \geq \frac{(1-\beta)(1-\mu)(L_{SC}+M_P-M_C)}{\beta\mu} + M_P - M_C \tag{30}$$

$$L_{SP} \leq \frac{\beta(1-\mu)(L_{SC}+M_P-M_C)}{\mu(1-\beta)} + M_P - M_C \tag{31}$$

When the defense strategy is [(D_0, S_{S1}), (D_1, S_{S0})], under different parameter values, each attack strategy may become the optimal attack strategy. But combined with assumption 4 in the model assumptions, there is only one possible equilibrium strategy:

Equilibrium 7: [(T_0, S_{A1}), (T_1, S_{A1}), (D_0, S_{S1}), (D_1, S_{S0})]
Existence conditions:

$$\beta \leq \frac{1}{2} \tag{32}$$

$$L_{SP} \geq \frac{\beta(1-\mu)(L_{SC}+M_P-M_C)}{\mu(1-\beta)} + M_P - M_C \tag{33}$$

$$L_{SP} \leq \frac{(1-\beta)(1-\mu)(L_{SC}+M_P-M_C)}{\beta\mu} + M_P - M_C \tag{34}$$

In summary, among the 16 sets of offensive and defensive strategies involved in the model, there are a total of 7 possible equilibrium strategies under different parameter values. When the value of the relevant parameter satisfies the value condition of any one of the above seven groups of equilibrium, the group strategy is the equilibrium strategy that satisfies the current parameter value. In practical applications, by calculating the conditions met by the actual parameters, the equilibrium existing in the actual situation can be judged to help the system defender make the decision of the protection strategy.

5. Analysis of Performance

This section introduces the analysis process of the game model through an example, and analyzes the results to verify the feasibility of the model. The environment is shown in Figure 5. For the ATMCPS, the cyber system includes a database server that stores a large amount of user privacy data, and a control system that can dispatch aircraft. The attacker launches an attack on the system, and the attack detection device can detect the attack characteristics. The system defender determines whether the attacker's true intention is to attack the cyber system to obtain private information, or to attack the control system to affect the normal operation of the aircraft.

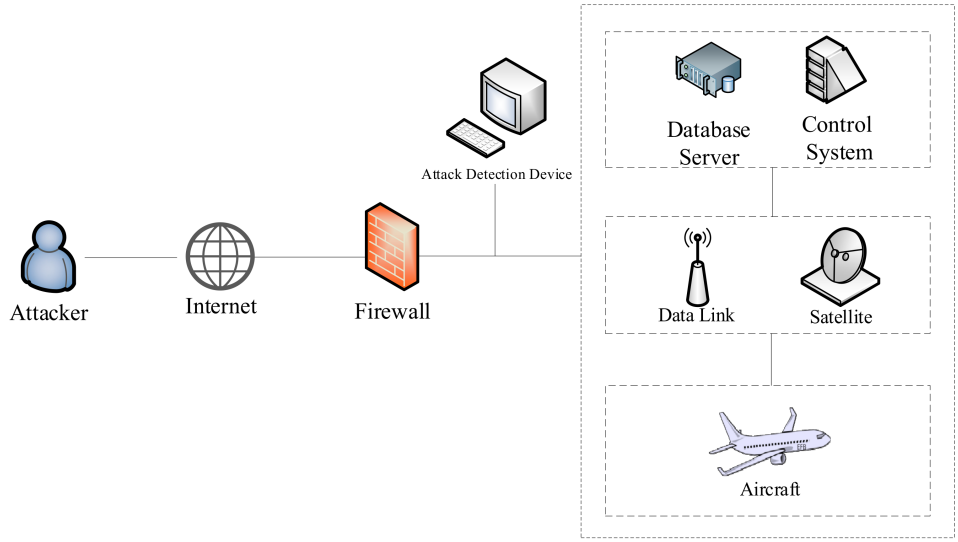

Figure 5. Experimental Topology.

(1) Parameter Definition

For the ATMCPS, if the attacker can obtain the control authority of the aircraft through the cyber system and launch a physical attack, the loss to the system will be higher than that of a cyber attack for the purpose of obtaining data. Likewise, attackers can get higher benefits. Different from the traditional attack methods, the attackers attack through the cyber system, and the required cost is low, and the camouflage of the attack also requires a certain cost. For defenders, it costs more to protect physical attacks. However, due to the difficulty of physical attack and the high cost of attack, the initial belief of the defender for the attacker to launch a physical attack is lower than the initial belief of the attacker to launch a cyber attack. For the attack detection device, if the attacker does not camouflage the attack type, the attack detection device should maintain a high detection success rate. If the attacker camouflages the attack type, the detection success rate will decrease, but it should be high 0.5, otherwise it is difficult to ensure the security of the system. Therefore, the relevant parameters are assumed to verify the model.

The cost and benefit parameters related to the attacker are shown in Table 4. The relevant cost and benefit parameters of the system defender, the initial belief of the attacker type, and the detection success rate of the attack detection device under the attacker's different strategies are shown in Table 5.

Table 4. Related Parameters of the Attacker.

Parameter	C_P	C_C	C_I	E_{AP}	E_{AC}
Value	18	12	9	50	40

Table 5. Related Parameters of the System and the Defender.

Parameter	μ	α	β	M_P	M_C	L_{SP}	L_{SC}
Value	0.4	0.6	0.8	40	25	70	60

(2) Posterior Belief

The system defender has an initial belief about the attacker's attack type, combined with the detection success rate of the attack detection device and the detected attack type, the system will update the initial belief to form a posterior belief. All the updated posterior beliefs are shown in Table 6.

Table 6. Posterior Belief of the Defender.

Posterior Belief	$p(T_0 \mid D_0)$	$p(T_1 \mid D_0)$	$p(T_0 \mid D_1)$	$p(T_1 \mid D_1)$
(T_0, S_{A0}), (T_1, S_{A0})	0.5	0.5	0.3	0.7
(T_0, S_{A0}), (T_1, S_{A1})	0.67	0.33	0.25	0.75
(T_0, S_{A1}), (T_1, S_{A0})	0.57	0.43	0.18	0.82
(T_0, S_{A1}), (T_1, S_{A1})	0.73	0.27	0.14	0.86

(3) Income and Equilibrium Analysis

Under different strategies, the incomes of both offense and defense are shown in Tables 7 and 8. The data in Tables 6–8 are solved by formula (6) and formula (7), and the expected incomes of the attacker and the system can be obtained. Table 9 shows the income matrix of under the 16 combinations of offensive and defensive strategies.

Table 7. Incomes of the Attacker.

Corresponding Type T	Attack Strategy S_A	$U_A(S_A, S_S)$			
		D_0		D_1	
		S_{S0}	S_{S1}	S_{S0}	S_{S1}
T_0	S_{A0}	−27	23	−27	23
	S_{A1}	−18	32	−18	32
T_1	S_{A0}	19	−21	19	−21
	S_{A1}	28	−12	28	−12

Table 8. Incomes of the Defender.

Corresponding Type D	Protection Strategy S_S	$U_S(S_A, S_S)$			
		T_0		T_1	
		S_{A0}	S_{A1}	S_{A0}	S_{A1}
D_0	S_{S0}	−40	−40	−100	−100
	S_{S1}	−95	−95	−25	−25
D_1	S_{S0}	−40	−40	−100	−100
	S_{S1}	−95	−95	−25	−25

Table 9. Income Matrix of Both Offense and Defense.

Income	(D_0, S_{S0}), (D_1, S_{S0})	(D_0, S_{S0}), (D_1, S_{S1})	(D_0, S_{S1}), (D_1, S_{S0})	(D_0, S_{S1}), (D_1, S_{S1})
(T_0, S_{A0}), (T_1, S_{A0})	(−8, −151.54)	(−12, −116.54)	(6, −141.54)	(2, −106.54)
(T_0, S_{A0}), (T_1, S_{A1})	(1, −145)	(−11, −102.5)	(23, −156.67)	(11, −114.17)
(T_0, S_{A1}), (T_1, S_{A0})	(1, −154.8)	(−13, −103.44)	(25, −154.09)	(11, −102.73)
(T_0, S_{A1}), (T_1, S_{A1})	(10, −147.79)	(−12, −91.36)	(42, −167.34)	(20, −110.91)

According to the income matrix shown in Table 9, it can be seen that both the attacker and the defender can obtain the maximum income when the strategy combination of the attacker and the defender is $[(T_0, S_{A0}), (T_1, S_{A1}), (D_0, S_{S0}), (D_1, S_{S1})]$. Neither side can get more incomes by unilaterally changing their strategies. That is to say, this group of strategies is the perfect Bayesian Nash equilibrium strategy that exists under the current value condition. For an attacker, if the attacker can successfully launch an attack on the physical system, the relative income after removing the cost is higher than that of a cyber attack. Therefore, the attacker adopts a camouflage strategy for physical attacks and a non-camouflage strategy for cyber attacks. That is, no matter what type of attack the attacker launches, the attack type displayed is a cyber attack. For system defenders, the detection success rate of detection devices is at a relatively high level, and if the physical system is successfully attacked, the losses suffered are more serious. Therefore, when the

attack type detected by the system's attack detection device is a physical attack, a physical protection strategy is adopted. Since the initial belief of the system, the probability of cyber attacks is high, and under the attacker's strategy, the displayed attack characteristics are all cyber attacks. Therefore, when the detected attack type is a cyber attack, cyber protection is adopted.

At the same time, substituting the parameter values into the conclusion obtained in Section 4.7, it can be concluded that only all the existence conditions of equilibrium 4 are met, which is consistent with the equilibrium strategy obtained by the actual calculation.

(4) Parametric Analysis

Most of the parameters involved in the model are based on certain objective facts, and only the initial belief "μ" will be greatly influenced by the defender's subjective ideas. Therefore, keeping other variables constant, consider the relationship between the defender's initial belief and the loss after the system is attacked.

Compared with when the system defender has a relatively neutral initial belief, when the system defender has a more biased initial belief about the type of attack launched by the attacker, the possible losses will be reduced. If the defender's initial belief about the attack type is neutral, it may lead to larger errors when updating the posterior belief and choosing a protection strategy. As shown in Figure 6, when the loss value of the system under physical attack increases, that is, when the "L_{SP}" increases, the lowest point of the system income is closer to $\mu = 0.5$.

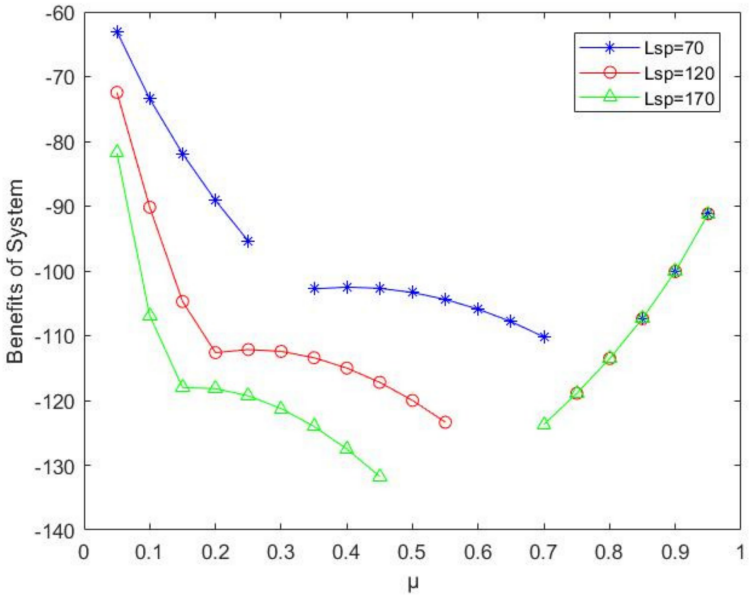

Figure 6. System Incomes under Changes in μ and $L_{SP.}$

On the other hand, it can be seen from Figures 6 and 7. When the loss value of the system under physical or cyber attack increases, for example, the loss of the system under physical attack is much higher than that under cyber attack. Even if defenders still believe that attackers may be launching a cyber attack for some reason, they should still focus on defending against physical attacks. In Figure 6, when the value of "μ" is in the range of 0.75–0.95, although the loss of the system under physical attack increases, that is, the value of the variable "L_{SP}" increases, the overall income of the system remains unchanged. Similarly, in Figure 7, when the value of "μ" is in the range of 0.05–0.35, although the loss of the system under cyber attack increases, that is, the value of the variable "L_{SC}" increases, the overall income of the system remains unchanged.

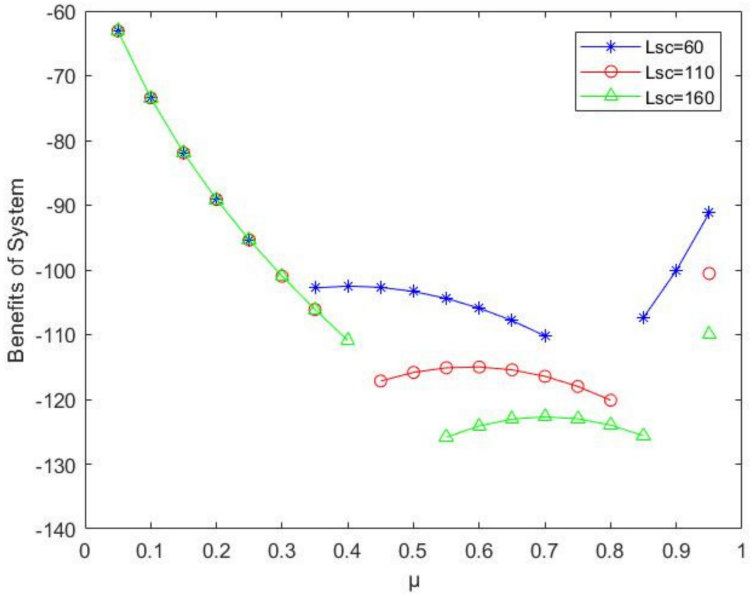

Figure 7. System Incomes under Changes in μ and $L_{SC.}$

Therefore, the defender's initial belief about the attack type should not choose a more neutral value. When the defender does not have a high degree of understanding of the attacker, he can provide a reference for the judgment of the initial belief according to the possible damage to the system, so as to prevent the system from suffering more serious losses as much as possible.

The model proposed in this paper calculates the expected income value under the combination of the two strategies when calculating the final income of the attacking and defending parties, and does not consider the Nash equilibrium solution under the mixed strategy. Therefore, there will be some breakpoints in the data in Figures 6 and 7. The reason is that there is no Nash equilibrium solution under the pure strategy under the value of this group of parameters. For example, when L_{SC} is 160 and μ is 0.9, the income matrix is shown in Table 10.

Table 10. The Income Matrix without a Pure-Strategy Nash Equilibrium.

Income	(D_0, S_{S0}), (D_1, S_{S0})	(D_0, S_{S0}), (D_1, S_{S1})	(D_0, S_{S1}), (D_1, S_{S0})	(D_0, S_{S1}), (D_1, S_{S1})
(T_0, S_{A0}), (T_1, S_{A0})	$(-8, -113.89)$	$(-12, -136.03)$	$(6, -153.03)$	$(2, -175.17)$
(T_0, S_{A0}), (T_1, S_{A1})	$(1, -114.81)$	$(\underline{-11}, -127.99)$	$(23, -161.59)$	$(11, -174.77)$
(T_0, S_{A1}), (T_1, S_{A0})	$(1, -128.42)$	$(-13, -125.92)$	$(25, -171.32)$	$(11, -168.82)$
(T_0, S_{A1}), (T_1, S_{A1})	$(10, -133.56)$	$(-12, -117.79)$	$(42, -182.34)$	$(20, -166.57)$

It can be seen from Table 10 that there is no set of strategies such that the incomes of both the attacker and the defender are maximized at the same time. Attackers or defenders can always make more incomes by unilaterally changing their strategies. Therefore, there is no Nash equilibrium under pure strategy. However, from the existence of Nash equilibrium [19], in a standard game, when both players and strategy sets are limited, there is at least one Nash equilibrium in the game, and the equilibrium may contain mixed strategies. Therefore, when there is no pure-strategy Nash equilibrium under some parameter values, there may be a mixed-strategy Nash equilibrium.

(5) Model Comparison

As shown in Table 11, compared with the existing research on the game model of CPS security, the model proposed in this paper comprehensively considers two types of attacks: physical attacks and cyber attacks. According to the incomes of both parties, a non-zero-sum game is constructed. According to the degree of mutual understanding

between the two parties, the incomplete information game is constructed. According to the sequence of the behaviors of the two parties, a dynamic game is constructed. The defender only has a partial understanding of the attacker, and can update the belief about the attacker based on the type of attack detected. Therefore, the model constructed in this paper is more suitable for the actual scene of attack and defense. Furthermore, for the game model proposed in this paper, the equilibrium strategies that exist under different parameter values are calculated, and a complete mathematical model is constructed. The system defender can quickly obtain the possible Bayesian Nash equilibrium according to its own relevant parameters.

Table 11. Model Comparison.

	Cyber Attack	Physical Attack	Static Game	Dynamic Game	Complete Information Game	Incomplete Information Game
[15]	√	√	√	×	√	×
[16]	×	√	√	×	√	×
[19]	√	√	√	×	×	√
[24]	√	√	×	√	√	×
Our Model	√	√	×	√	×	√

6. Conclusions

In this paper, the architecture of the ATMCPS is described, and based on the dynamic Bayesian game, the protection model of the ATMCPS is established. Through the results detected by the attack detection device of the system, the defender will update the initial belief of the attacker and determine the optimal protection strategy. The model provides all possible pure-strategy Nash equilibrium solutions and their corresponding existence conditions. By analyzing the performance of the model through an example, the system defender can quickly obtain the equilibrium strategy that meets the conditions according to the actual system parameter values, which verifies the validity of the model.

ATMCPS is highly complex, especially when cyber-attacks also hit physical system, and vice versa. Therefore, in the following research, the income function will be further optimized to better reflect the strong interaction and integration of the physical system and the cyber system. At the same time, the problem of solving the mixed strategy Nash equilibrium in the game model will be considered to further improve the model.

Author Contributions: Conceptualization, Z.W. and P.W.; methodology, Z.W. and R.D.; validation, R.D.; resources, Z.W.; writing—original draft preparation, R.D.; writing—review and editing, Z.W. and P.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the joint funds of National Natural Science Foundation of China and Civil Aviation Administration of China (U1933108 and U2133203), the National Natural Science Foundation of China (62172418), the Natural Science Foundation of Tianjin, China (21JCZDJZ00830), the Scientific Research Project of Tianjin Municipal Education Commission (2019KJ117), and the Fundamental Research Funds for the Central Universities of China (ZXH2012P004, 3122021026).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Jia, X.; Zheng, B.; Liu, X.; Jia, Z. Security control of cyber-physical systems with input quantization. *Sci. Technol. Eng.* **2020**, *20*, 12897–12903. [CrossRef]
2. Li, L. China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0". *Technol. Forecast. Soc. Chang.* **2018**, *135*, 66–74. [CrossRef]
3. Bouk, S.H.; Ahmed, S.H.; Eun, Y.; Park, K.-J. Multimodal Named Data Discovery with Interest Broadcast Suppression for Vehicular CPS. *IEEE Trans. Mob. Comput.* **2020**, *20*, 1877–1891. [CrossRef]
4. Lee, J.; Bagheri, B.; Kao, H.A. A Cyber-Physical Systems architecture for industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
5. Wang, L.; Huang, T. Application of Cyber-physical System in Aviation. *Aeronaut. Comput. Tech.* **2013**, *43*, 117–119. [CrossRef]
6. Nourian, A.; Madnick, S. A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet. *IEEE Trans. Dependable Secur. Comput.* **2015**, *15*, 2–13. [CrossRef]
7. Zhang, H. Research on Security Theory for Cyber-Physical Systems. Ph.D. Thesis, Zhejiang University, Hangzhou, China, 2015.
8. Wang, Y.; Wang, Y.; Zhang, L.; Zhang, L. Analysis and defense of the BlackEnergy malware in the Ukrainian electric power system. *Chin. J. Netw. Inf. Secur.* **2017**, *3*, 46–53. [CrossRef]
9. Sampigethaya, K.; Poovendran, R. Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport. *Proc. IEEE* **2013**, *101*, 1834–1855. [CrossRef]
10. Chen, W.; Zhang, L. Physical and cyber convergence approach to design future complex aviation cyber physical systems. In Proceedings of the 2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 23–25 September 2015. [CrossRef]
11. Alrefaei, F.; Alzahrani, A.; Song, H.; Zohdy, M.; Alrefaei, S. Cyber Physical Systems, a New Challenge and Security Issue for the Aviation. In Proceedings of the 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 21–24 April 2021. [CrossRef]
12. Wang, X.; Miao, S.; He, M.; Liu, M. Node ranking of air traffic information physical system based on improved K-shell algorithm. *China Sciencepaper* **2020**, *15*, 1144–1149. [CrossRef]
13. Shaikh, F.; Rahouti, M.; Ghani, N.; Xiong, K.; Bou-Harb, E.; Haque, J. A Review of Recent Advances and Security Challenges in Emerging E-Enabled Aircraft Systems. *IEEE Access* **2019**, *7*, 63164–63180. [CrossRef]
14. Li, L. The Research on Security Control of Cyber-Physical Systems under Denial-of-Service Attacks. Master's Thesis, Lanzhou University of Technology, Lanzhou, China, 2020.
15. Tai, W. Research on Game Theory Based Cyber Attack-Defense Strategies in Cyber Physical Power Systems. Master's Thesis, Southeast University, Nanjing, China, 2019.
16. Orojloo, H.; Azgomi, M.A. A game-theoretic approach to model and quantify the security of cyber-physical systems. *Comput. Ind.* **2017**, *88*, 44–57. [CrossRef]
17. Jithish, J.; Sankaran, S.; Achuthan, K. Towards Ensuring Trustworthiness in Cyber-Physical Systems: A Game-Theoretic Approach. In Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 7–11 January 2020. [CrossRef]
18. Yan, B.; Yao, P.; Wang, J.; Yang, T.; Ruan, W.; Yang, Q. Game Theoretical Dynamic Cybersecurity Defense Strategy for Electrical Cyber Physical Systems. In Proceedings of the 2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2), Taiyuan, China, 22–25 October 2021. [CrossRef]
19. Li, J.; Li, T. Cyber-physical Security Analysis of Smart Grids with Bayesian Sequential Game Models. *Acta Autom. Sin.* **2019**, *45*, 98–109. [CrossRef]
20. Kammuller, F.; Kerber, M. Investigating Airplane Safety and Security Against Insider Threats Using Logical Modeling. In Proceedings of the 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 22–26 May 2016. [CrossRef]
21. Lu, X.; Wu, Z.; Wu, Y.; Wang, Q.; Yin, Y. ATMChain: Blockchain-Based Solution to Security Problems in Air Traffic Management. In Proceedings of the 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, 3–7 October 2021. [CrossRef]
22. Tan, X.; Xu, L.; Ni, J.; Li, S.; Jiang, X.; Zheng, Q. Game Theory Based Dynamic Adaptive Video Streaming for Multi-Client Over NDN. *IEEE Trans. Multimed.* **2021**, *24*, 3491–3505. [CrossRef]
23. Geng, H.; Lu, H.; Huang, M.; Sun, S.; Zheng, C. Design Decision of Protection Engineering Based on Dynamic Bayesian Game. *J. Ordnance Equip. Eng.* **2020**, *41*, 209–215. [CrossRef]
24. Gao, B.; Shi, L. Modeling an Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in a Cyber-Physical Power System. *IEEE Access* **2020**, *8*, 30322–30331. [CrossRef]