Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.037257

ARTICLE

Honeypot Game Theory against DoS Attack in UAV Cyber

Shangting Miao[1], Yang Li[2,*] and Quan Pan[2]

[1]School of Cybersecurity, Northwestern Polytechnical University, Xi'an, 710129, China

[2]School of Automation, Northwestern Polytechnical University, Xi'an, 710129, China

*Corresponding Author: Yang Li. Email: liyangnpu@nwpu.edu.cn

Received: 28 October 2022 Accepted: 22 February 2023 Published: 08 October 2023

ABSTRACT

A space called Unmanned Aerial Vehicle (UAV) cyber is a new environment where UAV, Ground Control Station (GCS) and business processes are integrated. Denial of service (DoS) attack is a standard network attack method, especially suitable for attacking the UAV cyber. It is a robust security risk for UAV cyber and has recently become an active research area. Game theory is typically used to simulate the existing offensive and defensive mechanisms for DoS attacks in a traditional network. In addition, the honeypot, an effective security vulnerability defense mechanism, has not been widely adopted or modeled for defense against DoS attack UAV cyber. With this motivation, the current research paper presents a honeypot game theory model that considers GCS and DoS attacks, which is used to study the interaction between attack and defense to optimize defense strategies. The GCS and honeypot act as defenses against DoS attacks in this model, and both players select their appropriate methods and build their benefit function models. On this basis, a hierarchical honeypot and G2A network delay reward strategy are introduced so that the defender and the attacker can adjust their respective strategies dynamically. Finally, by adjusting the degree of camouflage of the honeypot for UAV network services, the overall revenue of the defender can be effectively improved. The proposed method proves the existence of a mixed strategy Nash equilibrium and compares it with the existing research on no delay rewards and no honeypot defense scheme. In addition, this method realizes that the UAV cyber still guarantees a network delay of about ten milliseconds in the presence of a DoS attack. The results demonstrate that our methodology is superior to that of previous studies.

KEYWORDS

UAV cyber security; honeypot game-theoretical model; DoS attack

1 Introduction

UAVs differ from conventional information infrastructure because they have more application scenarios and can be used for military and civil purposes. Among them, military applications are primarily shown as decoy and fire guidance, as well as reconnaissance and surveillance. Civil use, notably for the creation of movies and television programs, navigation, traffic monitoring, protection of agricultural plants, mobile communications, fire detection, and human search and rescue. UAVs are also utilized in the fight against the new crown epidemic. UAVs are given more critical tasks, playing a bigger and bigger role as their use increases [1]. With the production scale application of modern

information technology in manufacturing UAVs, UAV cyber security has emerged as a crucial area for research and development.

Cyber security is constantly evolving in response to increasingly sophisticated cyber attacks, so it is necessary to develop new ways to enhance the protection of UAVs. DoS attacks are now the leading cyber security issue for UAVs, gradually providing ineffective passive defense methods like firewalls, virus protection, and security scans. Their distinctive features are as follows. First, malicious code could be hidden in installed software, waiting for an opportunity to launch an attack. Second, because UAVs are not connected to public cyberspace, they can still be attacked. Third, it is tenacious and covert to avoid being discovered. The DoS attack is complicated to defend against because it can be launched to interfere with UAV service by inserting specific false information.

As an active defense technology [2], honeypot is suitable for solving UAV cyber security issues such as various communication protocols, seriously lacking or conveying security authentication mechanisms, and other related problems. Therefore, the honeypot effectively complements UAV cyber security against DoS attacks [3]. Unlike traditional security tools like firewalls and intrusion detection, honeypots could use GCS, UAV network services, or information as bait to detect and analyze the attacks. As we all know, there is almost no research on the use of honeypots in the UAV DoS attack and defense game. This study is motivated by the fact that the honeypot has not yet been applied to UAV cyber security.

This paper introduces a honeypot game theory to lessen the possibility of maliciously stopping UAVs for DoS attacks. The attack-defense game theory is implemented to study the information security transmission problem of GCS in UAV cyber, specifically for DoS attacks, to reduce the risk of malicious interference in the information transmission process between UAV and GCS. Therefore, this paper proposes a honeypot game model against DoS attacks in UAV cyber. The GCS and honeypot are regarded as the defense. By employing a deception strategy, the honeypot could confuse the attackers and increases the attack's cost. This paper uses the UAV network transmission delay as a reward evaluation to dynamically adjust the deception strategy of the honeypot. Concerning the UAV communication network, we also want to maintain low transmission delay while enhancing the payoff of GCS. The main contributions are summarized below.

1. In this article, it incorporates an attack-defense game model into the UAV cyber to study the respective benefit functions of the defender and the attacker, and it utilizes mixed Nash equilibrium strategy analysis to show that Nash equilibrium may be obtained when the predicted benefits of the attacker and the defender are equal.
2. This article also proposes using honeypots in the attack-defense game model to bait attackers, decrease the security impact of UAVs on cyberspace, and improve the security of data transmission in the G2A network.
3. This article uses the network delay generated after GCS or honeypot, is attacked by DoS as a reward evaluation value to adjust the deception strategy of the hierarchical honeypot dynamically and comprehensively consider the network delay and the security of UAV information transmission. Under the condition of ensuring lower network delay, the security performance of information transmission in UAV cyber is improved.

The rest of this paper is organized as follows: Section 2 provides a summary of the related work. Section 3 describes the network model of the UAV range, the model of the UAV network data link, and

the reward model based on a DoS attack are all described. Section 4 describes the honeypot offense-defense game problem and proves the existence of the Nash equilibrium solution. Section 5, this paper conducts extensive numerical simulations using an OPNET-based UAV network co-simulation with MATLAB to evaluate the proposed approach. Finally, Section 6 concludes the paper.

2 Related Work

In this section, this paper briefly summarizes related work on UAV cyber security issues, a honeypot for DoS attacks, and modeling attack and defense processes using game theory.

2.1 Security Issues in UAV Cyber

This study is related to the recent global increase in malicious UAV activities, including the filming of the White House in the United States by an illegally controlled DJI UAV [4], the filming of Kuala Lumpur Airport in Malaysia by an illegally controlled UAV [5], and the illegal intrusion of the Japanese Prime Minister's residence by a UAV carrying radioactive materials [6].

Existing studies focus on UAV penetration. For example, Watkins et al. [7] discussed vulnerabilities in UAV components, including vulnerabilities in wireless cyber, GPS, embedded systems, and navigation systems. In their study of three typical UAVs attacks, Liu et al. [8] examined wireless signal spoofing, GPS spoofing, and an assault on wireless sensor hacking. Trust in the GCS is key to the attack's success.

This paper compares UAVs with traditional infrastructure in terms of security threat, security protection, and security management, as shown in Table 1. Several possible security threats related to UAV cyber security are summarized as follows: (i) The variety of UAV software may lead to unknown vulnerabilities; (ii) UAV communication protocols lack encryption, and attackers capture control data and commands sent from the GCS to the UAV for replay or data forgery attack; (iii) As the wireless environment is open, a malicious attacker can send a false wireless control command to take over the UAV illegally.

Table 1: Comparison between UAV and traditional infrastructure

Term of comparison		UAV	Traditional infrastructure
Security threats	Source of threats	An individual, group, organization	An individual, group, organization
	Attack methods	WIFI password cracking attack, MITM attack, Bluetooth Pineapple logic vulnerability	Normal attack
Safety protection	System Security	Vulnerabilities and configuration problems in the proprietary operating system of the UAV	It focuses on vulnerabilities, security configurations, virus protection, and unauthorized access to system resources for standard operating systems.
	Network security	UAV proprietary communication protocol secure transmission capability	It focuses on the secure transmission, denial of service, and application layer security of TCP/IP clusters. Generally, it does not have high requirements for the security of data transmission

(Continued)

Table 1 (continued)

Term of comparison		UAV	Traditional infrastructure
	Data security	It focuses on the security of UAV status and control information in transmission, processing, and storage	Secure storage and authorized use of data stored on a server
Security management	Identity management	No authentication	User identity authentication and authorization mechanism
	Patch management	It is challenging to manage UAV system patches and deal with vulnerabilities in time	Vulnerability and patch management systems or tools are mature, and vulnerabilities can generally be dealt with promptly manner
	Behavior management	Lack of security log auditing and configuration change management for UAVs	It has a relatively complete IT system and network behavior audit mechanism
	Emergency response	Focus on emergency response plans to ensure continuity of UAV missions, with emphasis on rapid response	Emergency response plan optional

2.2 Honeypot for Denial of Service Attack

Existing studies focus on the discovery of security threats and attacks in UAV cyber, as well as the use of different security protection mechanisms for tampering with physical layer DoS attacks and the resource consumption of link layer DoS attack. Anti-UAV security research schemes include Wi-Fi jamming and cracking [9–11], replay [12,13], buffer overflow [14,15], ARP cache poisoning [16,17], injection and modification [18], and civilian GPS spoofing [19–22]. In addition, honeypot solutions for DoS attacks have been studied in [23]. The study suggests a method for simulating a product network in order to set up a honeypot, record an attack, and capture it. Although the honeypot can detect the attack early, the honeypot is not set according to the essential characteristics of the system, resulting in a low imitation degree. Therefore, the honeypot may effectively defend against DoS attacks in UAV cyber as an active defense technology.

The developer tool kit (DTK) [24], launched on UNIX platforms by Cohen in 1997, was the most influential early honeypot software tool. It records the behavior of tool vulnerabilities by simulating many vulnerabilities on the system. Up to now, various honeypots have appeared in the fields of industrial control systems, IP voice and other fields in terms of simulation level and captured data quality, such as MiniCPS [25], IoTPOT [26], Iotcandyjar [27], Artemisa [28] and many innovative honeypot products. In addition, the creation technique of the deception simulation environment determines the veracity of the honeypot. It should be mentioned that the honeypot study of UAVs has not received enough attention.

To the best of our knowledge, most research on DoS attacks is based on the energy-sensitive and resource-constrained characteristics of UAV networks. Wood et al. [29] studied various DoS attacks that may occur at various layers in sensor networks. Simple DoS attack attempts to deplete the available resources of the victim node by sending many unnecessary packets, thereby preventing legitimate network users from accessing services or resources to which they are entitled. Therefore, methods to protect local devices from DoS attacks at the source include source-based DWARD [30], traceback [31], path identification [32], etc. Raymond et al. [33] also explored defense mechanisms in wireless

networks. However, the traditional method of defending against DoS attacks requires constant system traffic monitoring, which consumes resources and is unsuitable for UAVs. It should be mentioned that as an effective security vulnerability defense tool, it seems that there is no honeypot supports UAV-specific protocols. The use of honeypot as defense against UVA-based DoS attacks may have gone unnoticed in earlier research.

2.3 Game Theory for Modeling

The application of game theory in DoS modeling is studied in [34] and [35]. In [36], La et al. introduced a two-player zero-sum game to deal with DoS traffic injection. In [37], Liu et al. proposed a dynamic attack-based game model to compute Nash equilibrium to solve the attack detection problem. Neither study could balance the energy consumption rate and attack detection rate. Therefore, the honeypot can consume fewer resources while protecting the UAV network. The attacker's choice can be influenced or interfered with by it, and the intent also can be detected by it. However, the current study on the honeypot attack and defense game focuses on smart grids, intelligent transportation, and cloud computing. Ashok et al. [38] discussed cyber-physical security from the perspective of coordinated cyber attacks. They introduced a game-theoretic approach to improving the cyber defense performance of intelligent grids, aiming at the problem that the national grid and other critical infrastructures face the threat of cyber attack. Koutsoukos et al. [39] proposed a traffic signal detection model based on game theory to protect the traffic network from cyber threats. The model obtains the optimal defense strategy under high computational load through a heuristic algorithm. Xiao et al. [40] proposed a bounded rational game model based on prospect theory, which uses prospect theory to describe the bounded rational game process between the defender and the attacker of the cloud storage system. The simulation results show that exploiting the attacker's bounded rational behavior can improve the defender's profit. Compared with the above studies, this study is oriented towards the field of UAV and introduces honeypot technology as an active defense mechanism to trap DoS attacks.

There is currently little research on the implementation of a honeypot to enhance the security of UAV cyber, and the majority of studies in the field of UAV cyber security mainly address the issue of attack detection. Then this paper considers applying the honeypot to the game model to deceive the attacker and increase the cost.

3 Game Model for UAV Range

In this section, the UAV range is a virtual simulation environment for simulating UAV cyber. Next, this paper describes its network model, and network data link model, and finally introduces the reward model for the DoS attack. This paper places the relevant symbol definitions in Table 2.

Table 2: List of symbols

Symbols	Description
q	GCS
u	UAV
a	Malicious GCS or attacker
h	Honeypot
$\beta_{a,u}(t)$	Channel gain between UAV and malicious GCS

(Continued)

Table 2 (continued)

Symbols	Description
$\gamma_{h,u}(t)$	Channel gain between UAV and honeypot
$\omega_u^q(t)$	Represents the signal-to-noise ratio between GCS and UAV when the UAV network communication is under DoS attack
$\xi_u^q(t)$	Represents the signal-to-noise ratio between GCS and UAV when the UAV network communication is not under a DoS attack

3.1 Network Model

Fig. 1 depicts the four components of this game model: GCS, honeypot, malicious GCS, and UAV. Among them, the GCS is deployed by the service provider within the operating range of the UAV to provide efficient computing caching services for the UAV, such as UAV navigation and route conditions information sharing, which is essential for flight. This paper defines GCS in the same area as $Q = \{1, 2, 3, \ldots, \mathrm{Q}\}$. Each GCS in the network is equipped with a cache server to provide cache services for the UAV network.

This paper considers that the attacker can gain control of GCS through vulnerabilities and implement a DoS attack. At the same time, the UAV receives a large amount of garbage data, causing network interruption and security incidents. This paper defines the malicious GCS as $A = \{1, 2, 3, \ldots, \mathrm{A}\}$. It affects the network transmission quality by interfering with the downlink.

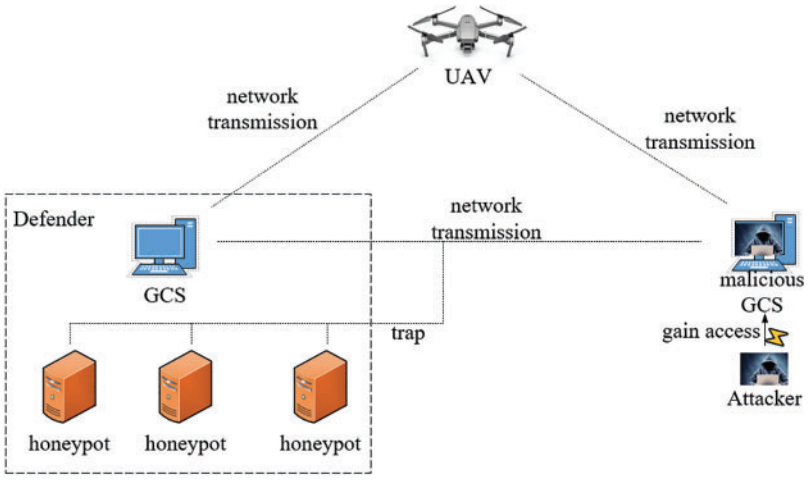

Figure 1: Game model of UAV range

Generally speaking, UAVs need to obtain some services in real-time during the navigation process, such as map navigation, airborne missions, collision warning, etc. Then, this paper defines UAV as $U = \{1, 2, 3, \ldots, \mathrm{U}\}$, assuming that each UAV can obtain cache services from multiple GCS, and attackers may have hacked some. Then, this paper feeds back the network delay of the UAV to the GCS, and it judges whether it is under DoS attack according to the network delay.

This paper deploys the honeypot near the GCS to hide the identity and define the honeypot as $\mathrm{H} = \{1, 2, 3, \ldots, \mathrm{H}\}$. When the UAV sends a request to the GCS, the honeypot and the GCS respond to

the network request of the UAV at the same time, and the honeypot can transmit some information that hackers are interested in, such as the location information of the UAV user, or the UAV management background. Once the honeypot is successfully trapped, then this paper considers it to increase the attack cost.

3.2 UAV Network Data Link Model

In this section, this paper assumes that the UAV is waiting to take off, and the network data transmission model is the line of sight (LOS) wireless transmission model. This paper applies it to network communication between UAV and GCS [41]. First of all, this paper makes a relevant definition of the defender. At a particular time, the position of UAV is defined as (x_u, y_u, z_u), where $z_u = 0$, q is a fixed position, which is defined as (x_q, y_q), and the distance between GCS and UAV is $d_{q,u}(t) = \sqrt{\left(x_q - x_u(t)\right)^2 + \left(y_q - y_u(t)\right)^2}$. The honeypot is also a fixed location, and its location is defined as (x_h, y_h). This paper defines the confounding deception quality of a hierarchical honeypot as $\eta_h \in [0, 10]$ and believes that η_h, between 7 and 10, represents the selection of a highly interactive honeypot. It makes the attacker easy to believe honeypot and attack.

Then this paper defines the attacker. Attack is assumed to be (x_a, y_a), the initial position at the time. The hacker obtains permission to control the GCS by attacking. Thereby they can send a large amount of junk information to UAV, causing it to failure to receive average data. The distance between a and u is $d_{a,u}(t) = \sqrt{(x_a - x_u(t))^2 + (y_a - y_u(t))^2}$.

This paper defines the channel gain between q and u as $\alpha_{q,u}(t)$, and the calculation formula is shown in (3-1).

$$\alpha_{q,u}(t) = \frac{\lambda}{d_{q,u}(t)^{\varepsilon}} = \frac{\lambda}{\left(\sqrt{\left(x_q - x_u(t)\right)^2 + \left(y_q - y_u(t)\right)^2}\right)^{\varepsilon}} \tag{3-1}$$

where λ represents the channel power gain, ε is the path loss exponent, and $\varepsilon > 1$.

Similarly, this paper defines the channel gain between a and u as $\beta_{a,u}(t)$, and the calculation formula is shown in (3-2). The channel gain between h and u is defined as $\gamma_{h,u}(t)$, and the calculation formula is shown in (3-3).

$$\beta_{a,u}(t) = \frac{\lambda m_a}{d_{a,u}(t)^{\varepsilon}} = \frac{\lambda m_a}{\left(\sqrt{(x_a - x_u(t))^2 + (y_a - y_u(t))^2}\right)^{\varepsilon}} \tag{3-2}$$

$$\gamma_{h,u}(t) = \frac{\lambda}{d_{h,u}(t)^{\varepsilon}} = \frac{\lambda}{\left(\sqrt{(x_h - x_u(t))^2 + (y_h - y_u(t))^2}\right)^{\varepsilon}} \tag{3-3}$$

where $m_a = \{0, 1\}$, 0 means no DoS attack, and 1 means DoS attack. This paper defines the power of network transmission between q and u as p_q, $q \in (1, 2, 3, \ldots, Q)$, the power of network transmission between h and u as p_h, $h \in (1, 2, 3, \ldots, H)$, and the power of network transmission between a and u as p_a, $a \in (1, 2, 3, \ldots, A)$. From the point of view of the signal noise ratio (SNR), this paper defines the background noise as N, assuming that the DoS attack will occur between 1 q and 1 a, affecting the data link layer of the wireless network. This paper defines the SNR of u at the time as $\omega_u^q(t)$. Then its calculation formula is as follows:

$$\omega_u^q(t) = \frac{p_q \alpha_{q,u}(t)}{N + p_a \beta_{a,u}(t) + p_h \gamma_{h,u}(t) + \psi\{-q, u\}(t)} \tag{3-4}$$

The attacker has attacked h with a DoS without interfering with regular network communication if the data connection layer of the interaction between q and u is standard. Then, this paper defines q and SNR as $\xi_u^q(t)$, and its calculation formula is as follows:

$$\xi_u^q(t) = \frac{p_q \alpha_{q,u}(t)}{N + p_h \gamma_{\mathrm{h},u}(t) + \psi\{-q,u\}(t)} \tag{3-5}$$

where $\psi\{-q,u\}(t)$ represents the channel interference generated by other q except the current q, since there is no other redundant q interference at present, here is $\psi\{-q,u\}(t) = 0$.

In addition, from the point of view of the transmission rate of the data link layer, if the data link layer of q interacting with u is abnormal, it means that q may be DoS attacked. That is, there is real noise. According to Shannon's theorem, this paper can define the transmission rate of the data link layer between q and u as $C_{\omega_u^q(t)}(B)$, and its calculation formula is as follows:

$$C_{\omega_u^q(t)}(B) = Blb\left(1 + \frac{S}{N}\right) = Blb\left(1 + \frac{p_q \alpha_{q,u}(t)}{N + p_a \beta_{a,u}(t) + p_h \gamma_{\mathrm{h},u}(t)}\right) \tag{3-6}$$

Analogously, if the network data link layer of q is normal, this paper defines the data transmission rate of interaction between q and u as $C_{\xi_u^q(t)}(B)$, and its calculation formula is as follows:

$$C_{\xi_u^q(t)}(B) = Blb\left(1 + \frac{S}{N}\right) = Blb\left(1 + \frac{p_q \alpha_{q,u}(t)}{N + p_h \gamma_{\mathrm{h},u}(t)}\right) \tag{3-7}$$

3.3 Reward Strategy Based on Network Delay

This paper also needs to consider the delay of the communication network after the DoS attack q as a reward signal. When initiates a DoS attack and affects data transmission, q and h need to consider how to adjust the transmission strategy to obtain adequate data transmission. This paper wants q to transmit as much information as possible to u in a time period, but a can affect the quality of network information transmission. Therefore, this paper defines the computational data sent by q to u request as $V = \{1, 2, 3, \ldots, V\}$, and the data size as K_v.

When this paper assumes the first case, q is under DoS attack, the network transmission delay is $t_{\omega_u^q(t)}$, and its calculation formula is as follows:

$$t_{\omega_u^q(t)} = \frac{K_v}{C_{\omega_u^q(t)}(B)} \tag{3-8}$$

This paper also assumes the second case, when q is not under DoS attack, the network transmission delay is $t_{\xi_u^q(t)}$, and its calculation formula is as follows:

$$t_{\xi_u^q(t)} = \frac{K_v}{C_{\xi_u^q(t)}(B)} \tag{3-9}$$

In addition, this paper uses the network transmission delay value as a reward. When the network transmission delay value is significant, the reward value is small, indicating that the trapping effect of h is not good. At this time, the defense parameters of h are evaluated. When the network transmission delay is slight, the reward value is enormous, indicating that the trapping effect of h is good. Then, this paper defines the reward value as τ, and its calculation formula is as follows:

$$\tau = \frac{\sigma}{t_0} \tag{3-10}$$

where σ represents the parameters of h to adjust the defense, $\sigma = t_u - t_0$, $t_0 = \left\{t_{\omega_u^q}, t_{\xi_u^q}\right\}$, and t_u represents the actual transmission delay of the UAV receiving the requested network data. The following table provides the honeypot deception quality update calculation formula: (3-11) [41].

$$\begin{aligned} \triangle\eta &= 1 - e^{\tau}, \\ \eta_{new} &= \eta_h + \triangle\eta \end{aligned} \tag{3-11}$$

This paper analyzes the above formula. If the actual network transmission delay of the environment is much smaller than the specified, then the possibility of a DoS attack on the network communication is less. It means that the h adjustment parameter is more extensive now, indicating that the reward value is higher, $\triangle\eta < 0$ and the updated η_h is lower. Vice versa, this paper needs to go through multiple rounds of iterations, and both the offensive and defensive sides constantly adjust their strategies to achieve a more stable balance.

4 Optimal Defensive Strategy of Honeypot in UAV Cyber

This section describes how to model the network interaction problem between q, h and a in the UAV range as an attack and defense game model and build a benefit function model for both parties. This section also sets up the rules of network delay reward evaluation. The defender and attacker can dynamically adjust their strategies and use the mixed strategy Nash equilibrium theory to obtain the optimal solution. The specific analysis is as follows. At the same time, this paper puts the definitions of symbols in Table 3 for easy reading.

Table 3: List of symbols

Symbols	Description
π_q	Data connection layer transmission costs for defense
ϕ_q	Total transmission cost of defender
ϕ_a	Total transmission cost of the attacker
g_q	Whether GCS is a network communication
g_a	Whether a malicious GCS does a DoS attack on a UAV
$\left\{R_q\right\}_{q\in Q}$	Payoff function of GCS
Ω	Attack and defense game model of UAV range
η_h	Hierarchical honeypot
x_h	The parameter of interaction degree between honeypot and drone
y_h	Parameters for the degree of IP address emulation in the honeypot for GCS

4.1 Problem Description of Honeypot Game for UAV Cyber

Above all, this paper takes a as the attacker, q and h as the defender. At the same time, it introduces a honeypot trapping strategy. Hence, this paper wants to find their optimal Nash equilibrium through the benefit function of the offense and defense and the reward strategy of network delay.

Then this paper establishes the game model. As far as the defender is concerned, this paper defines the transmission cost per unit of data link layer as π_q, $\pi_q = \pi_h$. Therefore, when the transmission power of each unit network is p_q, the total transmission cost of q is $\phi_q = p_q\pi_q$, and the total transmission cost of the attacker can also be calculated as $\phi_a = p_a\pi_a$. Similarly, this paper uses $g_q = \{0, 1\}$ to indicate

whether q communicates with the network. When $g_q = 1$, it means that q transmits data to u. When $g_q = 0$, it means that no data is transmitted. At the same time, $g_a = \{0, 1\}$ is used to indicate whether a DoS attack is performed. When $g_a = 1$, it means that a conducts a DoS attack on the UAV. When $g_a = 0$, it means there is no DoS attack.

Specifically, this paper treats the game model as a zero-sum game model, defined as $\Omega = \left\{\{Q, H, \mathrm{A}\}, \ \left\{p_q, p_h\right\}_{q\in Q, h\in H}, \ \{p_a\}_{a\in A}, \ \left\{R_q\right\}_{q\in Q}, \ \{R_a\}_{a\in A}\right\}$, in which the attacker and the defender obtain more excellent benefits through mutual restriction. Therefore, the benefits of q are not only related to their benefits and costs but also related to the cost of a. This paper defines the benefit function of q as $\left\{R_q\right\}_{q\in Q}$, and its calculation formula is as follows:

$$\left\{R_q\right\}_{q\in Q} = Blb\left(1 + \frac{p_q \alpha_{q,u}(t)\, g_q}{N + p_a \beta_{a,u}(t) + p_h \gamma_{\mathrm{h},u}(t)}\right) + g_q \kappa \eta_h - g_q \phi_h - g_q \phi_q + g_a \phi_a \tag{4-1}$$

where this paper defines κ as the adjustment parameter of the honeypot trapping rate, $\eta_h \in [1, 100]$ represents the decoy quality of the honeypot, and its calculation formula is as follows:

$$\eta_h = \theta x_h + (1 - \theta)\, y_h \ (0 \le \theta \le 1) \tag{4-2}$$

Specifically, when the network data transmission delay is high, h appropriately improves the interactivity and IP address emulation, and increases the attack cost by deceiving the DoS attacker. In addition, this paper also defines the benefit function of a as $\{R_a\}_{a\in A}$, and its calculation formula is as follows:

$$\{R_a\}_{a\in A} = \phi_q g_q - \kappa \eta_h g_q - \phi_h g_q - \phi_a g_a - Blb\left(1 + \frac{p_q \alpha_{q,u}(t)\, g_q}{N + p_a \beta_{a,u}(t) + p_h \gamma_{\mathrm{h},u}(t)}\right) \tag{4-3}$$

In summary, Since the two sides are antagonistic, any one of them changing its strategy will change the benefits of both parties involved in the game. The advantage of using a zero-sum game to model this attack-defense interaction is that one party's gain is the other's loss, which better reflects the degree of opposition. Therefore, the zero-sum game can better reflect the confrontation between q and a so that both parties can maximize their utility.

4.2 Offensive and Defensive Utility Function Matrix

In the process of analyzing the offensive and defensive game of the UAV range, q and a have their strategies. Since both sides have two strategies to choose from, there are four strategies after the combination. The details of these four strategies are as follows.

In the first strategy S_1, q transmits network data to u, and a initiates a DoS attack. This paper defines the benefit function of q as $R_{q,q\in Q}$, and its calculation formula is shown in (4-4). The benefit function of a is defined as $R_{\mathrm{a},\mathrm{a}\in A}$, and its calculation formula is shown in (4-5).

$$R_{q,q\in Q} = C_{\omega_u^q(t)}(B) - \phi_q + \phi_a + \phi_h \tag{4-4}$$

$$R_{\mathrm{a},\mathrm{a}\in A} = \phi_q - C_{\omega_u^q(t)}(B) - \phi_a - \phi_h \tag{4-5}$$

In the second strategy S_2, q does not transmit network data to u, and a initiates a DoS attack. This paper defines the benefit function of q as $R_{q,q\in Q}$, its calculation formula is shown in (4-6). The benefit function of a is defined as $R_{\mathrm{a,a}\in A}$, and its calculation formula is shown in (4-7).

$$R_{\mathrm{q,q}\in Q} = \phi_a \tag{4-6}$$

$$R_{\mathrm{a,a}\in A} = -\phi_a \tag{4-7}$$

In the third strategy S_3, q transmits network data to u, and a does not initiate a DoS attack. This paper defines the benefit function of q as $R_{q,q\in Q}$, and its calculation formula is shown in (4-8). The benefit function of a is defined as $R_{\mathrm{a,a}\in A}$, and its calculation formula is shown in (4-9).

$$R_{q,q\in Q} = C_{\xi_{u(t)}^{q}}(B) - \phi_q + \phi_h \tag{4-8}$$

$$R_{\mathrm{a,a}\in A} = \phi_q - C_{\xi_{u(t)}^{q}}(B) - \phi_h \tag{4-9}$$

In the fourth strategy S_4, q does not transmit network data to u, and a does not initiate a DoS attack. This paper defines the benefit function of q as $R_{q,q\in Q} = 0$, and the benefit function of a is defined as $R_{\mathrm{a,a}\in A} = 0$.

Then, this paper assumes that in one case, the transmission benefits of GCS and honeypot outweigh the cost of maintaining security, and GCS has reason to have network interactions with UAV. Finally, this paper shows the payoff function matrix of the offensive and defensive sides under different strategies in Table 4.

Table 4: Attack and defense payoff function matrix

	Benefits	
	q	a
S_1	$R_{q,q\in Q}$	$R_{\mathrm{a,a}\in A}$
S_2	ϕ_a	$-\phi_a$
S_3	$C_{\xi_{u(t)}^{q}}(B) - \phi_q + \phi_h$	$\phi_q - C_{\xi_{u(t)}^{q}}(B) - \phi_h$
S_4	0	0

4.3 Mixed Strategy Nash Equilibrium Analysis

In the last subsection, this paper regards UAV cyber's offensive and defensive game as a zero-sum game. Both offensive and defensive sides have their strategies combined into four situations. Meanwhile, this paper assumes that the hackers and honeypot deployers in the game are rational, and they have to consider the cost. With the same benefits, participants need to consider lower-cost attack and defense methods. As a result, both players in the game must select an effective tactic to maximize their gains. Because both sides have their optimal strategies, this paper needs to use mixed strategy Nash equilibrium analysis to solve the problem.

To evaluate the UAV range honeypot game, this paper defines the probability distribution of the participants on χ as $f, f = (f_1, f_2, f_3, \ldots f_r) \in R \geq 0$, where $\sum_{t=1}^{R} f_t = 1$. Then, this paper defines the probability of safe network transmission as F_T and the probability of unsafe transmission as F_{NT}.

Analogously, we define the probability of a launching a DoS attack as F_A and the probability of not launching a DoS attack as F_{NA}, as shown in Table 5.

Table 5: Benefit function matrix of offensive and defensive strategies

		F_T	F_{NT}
F_A	$R_{q,q\in Q}$	$C_{\omega_u^q(t)}(B) - \phi_q + \phi_a + \phi_h$	ϕ_a
	$R_{\mathrm{a,a}\in A}$	$\phi_q - C_{\omega_u^q(t)}(B) - \phi_a - \phi_h$	$-\phi_a$
F_{NA}	$R_{q,q\in Q}$	$C_{\xi_u^q(t)}(B) - \phi_q + \phi_h$	0
	$R_{\mathrm{a,a}\in A}$	$\phi_q - C_{\xi_u^q(t)}(B) - \phi_h$	0

Specifically, according to the definition of mixed Nash equilibrium, when the expected benefits of the defender and the attacker are equal, the players no longer care about the choice of strategy. Therefore, in the honeypot game model of the UAV range, the mixed strategy gives the attacker the same expected benefit when generating a DoS attack or not generating a DoS attack.

When this paper sets $E(F_A) - E(F_{NA}) = 0$ and $E(F_T) - E(F_{NT}) = 0$, the mixed Nash equilibrium strategies of both sides of the game are obtained, and their calculation formulas are as follows:

$$\begin{cases} F_T = \dfrac{\phi_a}{C_{\xi_u^q(t)}(B) - C_{\omega_u^q(t)}(B)} \\ F_{NT} = 1 - \dfrac{\phi_a}{C_{\xi_u^q(t)}(B) - C_{\omega_u^q(t)}(B)} \end{cases} \tag{4-10}$$

$$\begin{cases} F_A = \dfrac{\phi_q - C_{\xi_u^q(t)}(B) - \phi_h}{C_{\omega_u^q(t)}(B) - C_{\xi_u^q(t)}(B)} \\ F_{NA} = 1 - \dfrac{\phi_q - C_{\xi_u^q(t)}(B) - \phi_h}{C_{\omega_u^q(t)}(B) - C_{\xi_u^q(t)}(B)} \end{cases} \tag{4-11}$$

In summary, this paper obtains the probability of each strategy by calculating and getting the mixed Nash equilibrium, that is, the obtained probability set, in the process of the offensive and defensive game of the UAV range. In this probability set, the benefits of both parties can reach the optimal situation simultaneously. Assuming that both parties abide by the regulations, neither party will change the strategy to break the balance, that is, to achieve the mixed Nash equilibrium of the honeypot attack and defense game in the UAV range.

5 Numerical Results

In this section, this paper mainly introduces the experimental simulation environment and the result analysis. This paper uses Matlab R2016a to conduct the simulation environment of the UAV cyber evolutionary game experiment. The test running environment is Intel(R) Xeon(R) CPU E5-1603 @ 2.80 GHz processor, the running memory is 8 GB, and the operating system is Windows 10 64-bit. In addition, the scene of the UAV range consists of GCS, honeypot, malicious ground station and UAV. Where GCS provides network data transmission services for UAV, the honeypot is responsible for disguising as GCS to trick attackers into conducting DoS attacks. Expressly, the number of GCSs, UAVs, and malicious GCSs is set to 1, whereas the number of honeypots is set to 3.

To investigate the advantages of GCS during a DoS assault, this paper adopted the honeypot defense strategy (UDRH) proposed in this paper and compared it with the no honeypot defense scheme (NHDS) in [42]. As shown in Fig. 2. This paper can see that the change range is relatively gentle in the early stage of the iteration, and the attacker and defender continue to interact and play the game. In the case of a DoS attack, the benefits of GCS tend to be those without a DoS attack, indicating that the honeypot defense strategy can resist to a certain extent. DoS attacks improve the defense's effectiveness. In the absence of DoS attacks, the benefits of GCS are higher overall. By contrast, the overall benefit of GCS in the UDRH strategy was higher than that of the NHDS strategy.

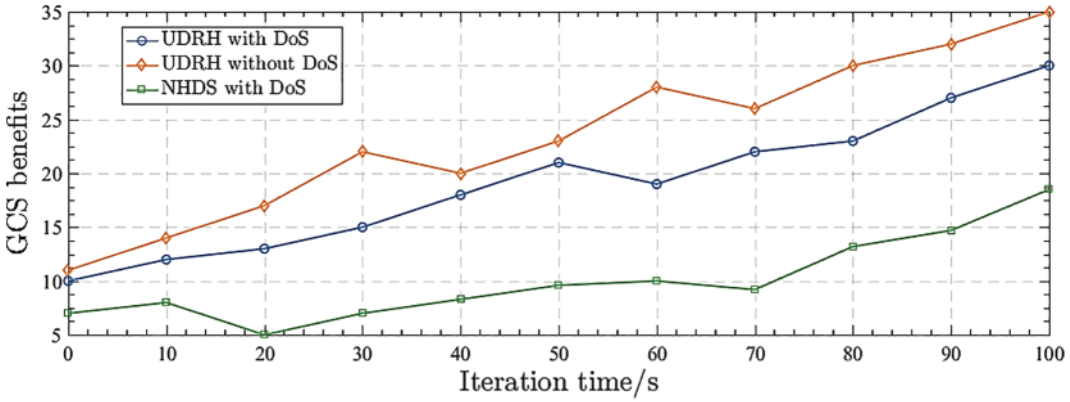

Figure 2: GCS benefit in the case of a DoS attack

In particular, this paper divides the hierarchical honeypot into three types: high, middle and low, and their deception quality is 1–10. To this end, this paper can analyze the cyber security probability and DoS attack probability from Fig. 3. In general, this paper equates the degree of emulation of a honeypot with its trapping quality, which is mainly determined by its interactivity. When the deception quality is between 7–10, it is a highly interactive honeypot, and the probability of the UAV communication network being attacked by DoS is reduced. In addition, as the degree of honeypot camouflage has increased, network transmission security has improved, significantly reducing the probability of a DoS attack. The honeypot protects the security of UAV cyber, making it difficult for the attacker to conduct a DoS attack effectively.

In Fig. 4, this paper analyzes the network security probability under the UDRH strategy. With the change of iteration time, it is higher when there is no DoS attack than when there is a DoS attack. It shows that the attacker floods the communication channel between the UAV and the GCS with garbage data. As a result, the UAV cannot usually receive messages, reducing the cyber security rate. Meanwhile, in the presence or absence of a DoS attack, the UDRH strategy has a higher network security rate than the NHDS, which shows that honeypot defense is of great significance for improving UAV cyber security performance. In addition, after a period of iteration, the cyber security probability of the UDRH strategy under the presence or absence of a DoS attack is equal, reaching the final balance.

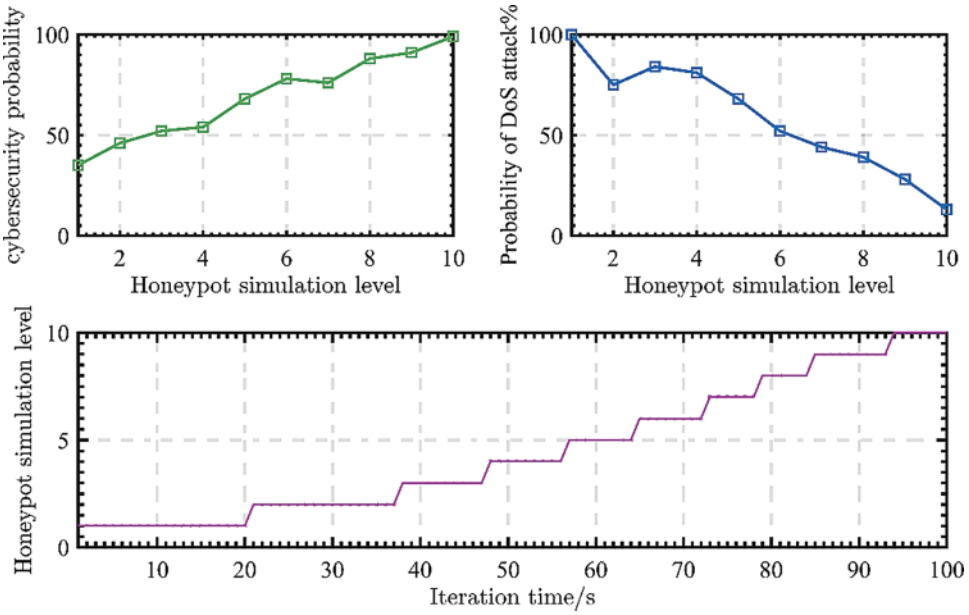

Figure 3: The deceptive quality of hierarchical honeypot

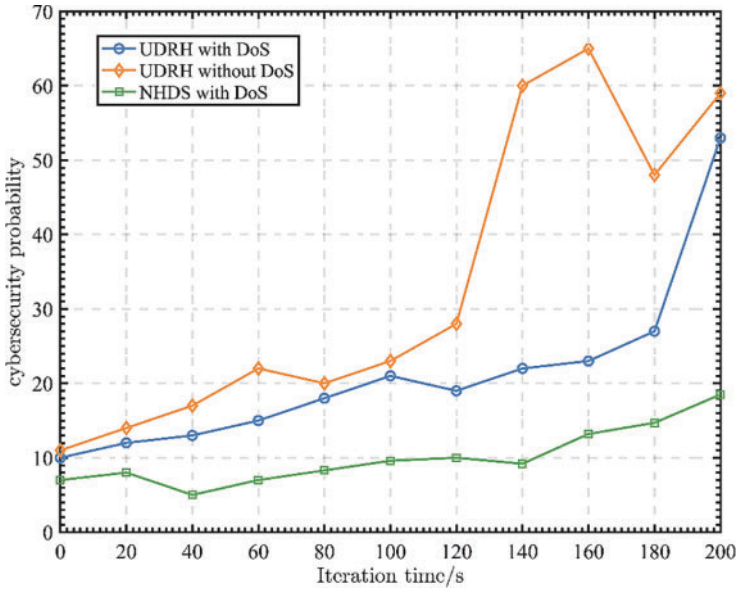

Figure 4: Variation of cyber security rate with iteration time

Analogously, this paper can analyze from Fig. 5 that the network transmission delay changes with the iteration time. In the presence of a DoS attack, the network transmission delay is higher than when there is no DoS attack. It shows that the DoS attack intensity is high. However, this paper adopts a reward adjustment strategy. After a period of iteration, the network transmission delay continues to approach the situation without a DoS attack. The honeypot defense strategy can resist the DoS attack. If the honeypot is absent compared to the NHDS scheme, there is a higher chance that the UAV network transmission may be interrupted.

In this paper, Fig. 6 compares the expected benefits of the defender with the degree of honeypot camouflage under different schemes. The honeypot strategy based on the zero-sum game proposed in this paper has apparent advantages over the other two schemes. It can improve the expected benefits of the defense more efficiently. The NHDS is that in the case of no honeypot defense, the mixed Nash equilibrium strategy selects its actions, resulting in lower expected returns. While adopting the honeypot defensive technique, the drone reward scheme (DRS) [43] lacks the time-delay feedback evaluation to dynamically change attack and defense strategies. In addition, when the degree of camouflage of the honeypot is low, the expected benefits of the UDRH and the DRS are similar. However, as the degree of honeypot camouflage increases, the expected benefit value of UDRH and DRS gradually increases. Simultaneously, the advantages of UDRH are steadily reflected.

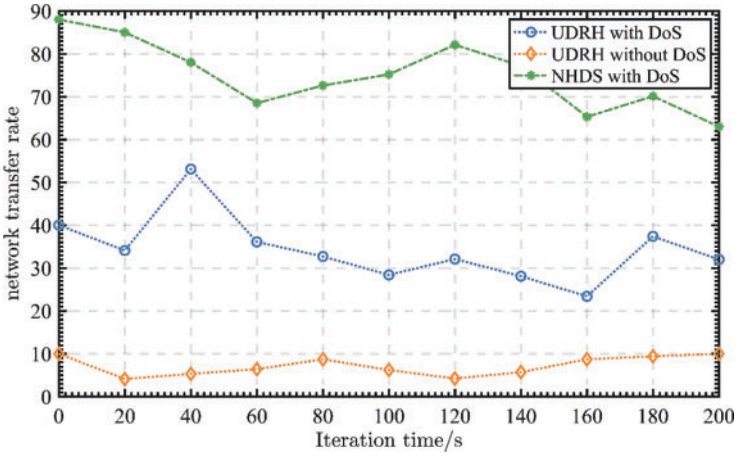

Figure 5: Variation of network transmission delay with iteration time

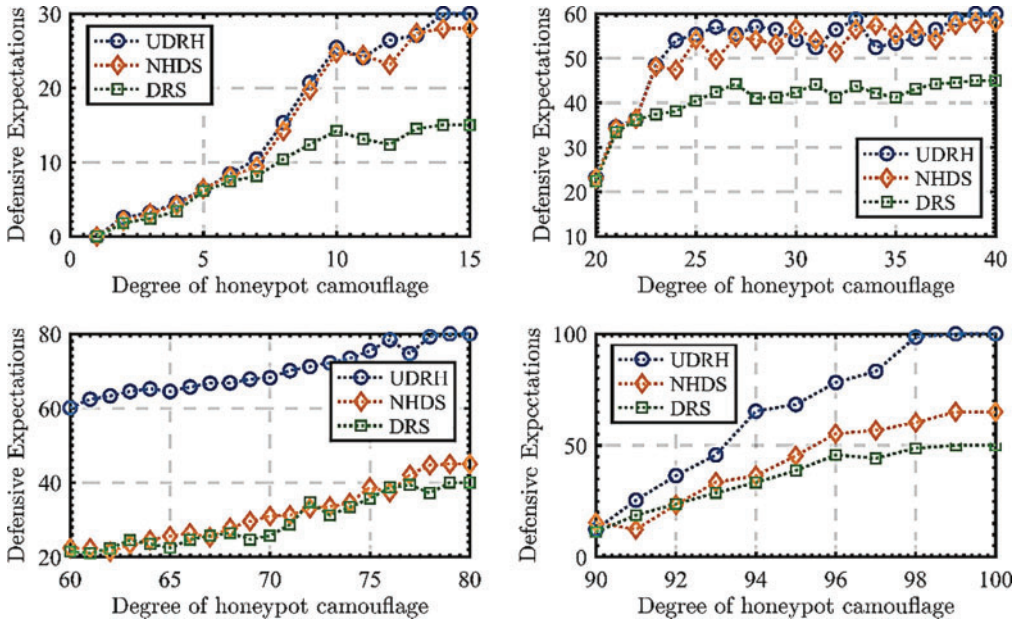

Figure 6: Comparison of benefits under different schemes

6 Conclusion

UAV gives a promising future to brilliant intelligent cities. With the advances in UAV technology, UAVs will become a part of the human environment. However, due to the openness of the G2A network, the transmission of UAV security information has become a challenging issue. UAV is vulnerable to cyber attacks, causing harm such as loss of confidential data and productivity. Given the vulnerability of UAVs to DoS attacks, a method to reduce the impact of UAV network delay in the environment of cyber attacks is proposed. This paper uses hierarchical honeypots and delayed rewards to establish a honeypot game model. The experimental results show that this method is suitable for effectively mitigating the impact of G2A network communication by DoS attack. In the offensive and defensive game model we use, the ground station's strategy is choosing network transmission, and the strategy of the malicious ground station is choosing a DoS attack. It is regarded as a zero-sum game model. Among them, the behavior of defender is to improve its confusion, while the attacker mainly provides prerequisites for the network delay. Finally, we give a detailed analysis of the experiment. In the presence of a DoS attack, the UDRH strategy can guarantee that the G2A network delay is about 10.2 milliseconds, while the G2A network delay under the NHDS strategy is about 58.6 milliseconds. For the future, it is intended to improve the security of UAV cyber through the analysis of honeypot data.

Acknowledgement: Previous UAV data link security is the basis of our research. We are grateful to all the researchers and applications that have guided us in developing the honeypot system for UAVs.

Funding Statement: Basic Scientific Research program of China JCKY2020203C025 funding is involved in this study.

Author Contributions: All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Shangting Miao, Yang Li and Quan Pan. The first draft of the manuscript was written by Shangting Miao and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Availability of Data and Materials: Part of the data comes from the DroneWars website.

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

References

[1] M. R. Asghar, Q. Hu and S. Zeadally, "Cybersecurity in industrial control systems: Issues, technologies and challenges," *Computer Networks*, vol. 165, no. 1, pp. 106–146, 2019.

[2] K. Wang, "Game-theory-based active defense for intrusion detection in cyber-physical embedded systems," *ACM Transactions on Embedded Computing Systems*, vol. 16, no. 1, pp. 1–18, 2016.

[3] A. Md, Q. Agrawal, D. Mehta, M. Sivaraman, A. Tee *et al.,* "Time optimization of unmanned aerial vehicles using an augmented path," *Future Internet*, vol. 12, no. 3, pp. 298–308, 2021.

[4] R. Priyadarshini, M. Qadir, A. Rajendran, N. Neelanarayanan, V. Sabireen *et al.,* "An enhanced encryption-based security framework in the CPS Cloud," *Journal of Cloud Computing*, vol. 11, no. 1, pp. 1–13, 2022.

[5] Q. Jaiswal, D. Daftari, J. Haneef, S. Iwendi, C. Jain *et al.,* "Efficient dynamic phishing safeguard system using neural boost phishing protection," *Electronics*, vol. 11, no. 19, pp. 31–33, 2022.

[6] W. Ripley, *UAV with Radioactive Material Found on Japanese Prime Minister Roof.* Cable News Network, 2015. [Online]. Available: https://edition.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone/index.html
[7] L. Watkins, J. Ramos and G. Snow, "Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems," *ACM MobiHoc Workshop on Mobile IoT Sensing, Security and Privacy*, vol. 2, no. 1, pp. 1–6, 2018.
[8] W. Liu, M. Bingwen and J. Weng, "Review of small UAV security research," *Journal of Network and Information Security*, vol. 2, no. 3, pp. 39–45, 2016.
[9] Z. Birnbaum, A. Dolgikh, V. Skorimin, E. O. Brien, D. Muller *et al.,* "Unmanned aerial vehicle security using recursive parameter estimation," *Journal of Intelligent & Robotic Systems*, vol. 84, no. 4, pp. 107–120, 2016.
[10] A. Abbaspour, K. Yen, P. Forouzannezhad and A. Sargolzaei, "A neural adaptive approach for active fault-tolerant control design in UAV," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 50, no. 9, pp. 3401–3411, 2018.
[11] H. Sedjelmaci and S. M. Senouci, "Cyber security methods for aerial vehicle cyber: Taxonomy, challenges and solution," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4928–4944, 2018.
[12] D. He, S. Chan and M. Cuizani, "UAV-assisted public safety cyber: The security aspect," *IEEE Communication Magazine*, vol. 55, no. 8, pp. 218–223, 2017.
[13] C. A. T. Bonilla, O. J. S. Parra and J. H. D. Forero, "Unmanned aircraft systems in logistics legal regulation and worldwide examples toward use in Groatia," *International Journal of Applied Engineering Research*, vol. 13, no. 7, pp. 4982–4988, 2018.
[14] J. Lindley and P. Coulton, "Game of UAVs," in *Proc. of the 2015 Annual Symp. on Computer-Human Interaction in Play*, New York, NY, USA, pp. 35–45, 2015.
[15] F. Trujano, B. Chan, G. Beams and R. Rivera, "Security analysis of DJI phantom 3 standard," *Massachusetts Institute of Technology*, vol. 13, no. 8, pp. 911–934, 2016.
[16] R. French and P. Ranganathan, "Cyber attack and defense framework for unmanned aerial systems (UAS) environment," *Jounal of Unmanned Aerial Systems*, vol. 3, no. 11, pp. 37–58, 2017.
[17] M. Booker, "Effects of hacking an unmanned aerial vehicle connected to the cloud," Ph.D. Dissertation, The Ohio State University, USA, 2018.
[18] H. Sedjelmaci, S. M. Senouci and N. Ansari, "A hierarchical detection and response system to enhance securlty against lethal cyber-attack in UAV cyber," *IEEE Transactions Systems, Man, and Cybenetics: Systems*, vol. 48, no. 9, pp. 1594–1606, 2017.
[19] N. O. Tippenhauer, C. Popper, K. B. Rasmussen and S. Capku, "On the requirements for successful GPS spoofing attack," in *Proc. of the 18th ACM Conf. on Computer and Communications Security*, Chicago, Illinois, USA, pp. 75–86, 2011.
[20] K. Hartmann and K. Giles, "UAV exploitation: A new domain for cyber power," in *Proc. of the 8th Int. Conf. on Cyber Conflict*, Tallinn, Estonia, pp. 205–221, 2016.
[21] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attack-an approach to the risk assessment," in *Proc. of the 5th Int. Conf. on Cyber Conflict*, Tallinn, Estonia, pp. 1–23, 2013.
[22] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," *The University of Texas at Austin*, vol. 3, no. 9, pp. 1–16, 2012.
[23] W. Nathalie, "Honeypot for distributed denial of service attack," in *Proc. of the Eleventh IEEE Int. Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, Pittsburgh, PA, USA, pp. 1080–1382, 2002.
[24] F. Cohen, "The deception toolkit," *Risks Digest*, vol. 2, no. 1, pp. 19–28, 1998.
[25] D. Antonioli and N. O. Tippenhauer, "MiniCPS: A toolkit for security research on CPS networks," in *Proc. of the First ACM Workshop on Cyber-Physical Systems-Security and Privacy*, Denver, Colorado, pp. 91–100, 2015.
[26] Y. M. Pa, S. Suzuki and K. Yoshioka, "Analysing the rise of IoT ComPromises," in *9th USENIX Workshop on Offensive Technologies*, Washington, 2015.

[27] T. Luo, Z. Xu and X. Jin, "Iotcandyjar: Towards an intelligent-interaction honeypot for iot devices," *Black Hat*, vol. 2, no. 1, pp. 131–142, 2017.
[28] R. Carmo, M. Nassar and O. Festor, "Artemisa: An open-source honeypot back-end to support security in voip domains," in *12th IFIP/EEE Int. Symp. on Integrated Network Management and Workshops*, Bern, Switzerland, pp. 361–368, 2011.
[29] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.
[30] J. Mirkovic, G. Prier and P. Reiher, "Attacking DDoS at the source," in *Proc. of 10th IEEE Int. Conf. on Network Protocols*, Paris, France, pp. 312–321, 2002.
[31] B. T. Wang and H. Schulzrinne, "An IP traceback mechanism for refiective DoS attacks," in *Proc. of Canadian Conf. on Electrical and Computer Engineering*, Halifax, NS, Canada, pp. 901–904, 2004.
[32] A. Yaar, A. Perrig and D. Song, "Pi: A path identification mechanism to defend against DDoS attacks," in *Proc. of 2003 Symp. on Security and Privacy*, Berkeley, California, UAS, pp. 93–107, 2003.
[33] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Computing*, vol. 1, no. 1, pp. 74–81, 2008.
[34] C. F. Tsai, Y. F. Hsu and C. Y. Lin, "Review: Intrusion detection by machine learning: A review," *Expert Systems with Applications*, vol. 36, no. 10, pp. 1194–1200, 2009.
[35] M. Panda, A. Abraham and S. Das, "Network intrusion dection system: A machine learning approach," *Intelligent Decision Technologies*, vol. 5, no. 4, pp. 347–356, 2011.
[36] Q. D. La, T. D. Quek and J. Lee, "Deceptive attack and defense game in honeypot-enabled networks for the Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1025–1035, 2016.
[37] B. Liu, Z. Su and Q. Xi, "Game theoretical secure wireless communication for UAV-assisted vehicular Internet of Things," *China Communications*, vol. 18, no. 7, pp. 147–157, 2021.
[38] A. Ashok, A. Hahn and M. Govindarasu, "Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment," *Journal of Advanced Research*, vol. 5, no. 4, pp. 481–489, 2014.
[39] X. Koutsoukos, G. Karsai and A. Laszka, "SURE: A modeling and simulation integration platform for evaluation of Secure and Resilient cyber-physical systems," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 93–112, 2018.
[40] L. Xiao, N. B. Mandayam and H. Vincent Poor, "Prospect theoretic analysis of energy exchange among microgrids," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 63–72, 2015.
[41] Q. Xi, Z. Su and S. Yu, "Trust based incentive scheme to allocate big data tasks with mobile social cloud," *IEEE Transactions on Big Data*, vol. 8, no. 1, pp. 113–124, 2022.
[42] Z. Fanzi, "Resource allocation and trajectory optimization for QoE provisioning in energy-efficient UAV-enabled wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 9, no. 9, pp. 1, 2020.
[43] S. Hichem and S. Mohamed, "Cyber security methods for aerial vehicle networks: Taxonomy, challenges and solution," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4928–4944, 2018.