Immunity-empowered Collaboration Security Protection for Mega Smart Cities

Kun Lan *, Jianhua Li *, Wenkai Huang *, Gaolei Li *

Posted Date: 6 May 2024

doi: 10.20944/preprints202405.0190.v1

Keywords: Cyber Security; Cyber physical systems; Mega Smart Cities; Public Safety; Human Immune Mechanism

Article

Immunity-Empowered Collaboration Security Protection for Mega Smart Cities

Kun Lan [1,2], Jianhua Li [1,*], Wenkai Huang [1] and Gaolei Li [1]

[1] School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University
[2] China Electronics Technology Cyber Security Co., Ltd
* Correspondence: lijh888@sjtu.edu.cn

Abstract: The cyber physical systems of smart cities are facing increasingly severe attack situations, and traditional separate protection methods are difficult to effectively respond to. It is urgent to coordinate public security and network security protection. However, the integration of the two faces many challenges and is a very promising research field. The aim of this study is to investigate technical approaches for the synergy between public safety and cyber security. This paper proposes a smart city safety protection model inspired by the human immune mechanism. It was found that through a three line defense architecture similar to the human immune mechanism, and with the help of certain algorithms and functional middleware modules, public security and network security protection components can be dynamically combined to achieve collaboration. This work has verified through experiments a promising path to effectively resist complicated attack threats intertwined with public safety and cyber security factors.

Keywords: cyber security; cyber physical systems; mega smart cities; public safety; human immune mechanism

1. Introduction

The critical infrastructure network of smart cities faces frequent complex attacks and intrusion events intertwined with network and physical space, and traditional separation protection methods are difficult to effectively cope with. Public safety and cyber security belong to two different fields of smart cities, which aim to solve different problems for different objects. For example, public safety mainly deals with video surveillance in physical space, monitoring and early warning of natural disasters, medical infectious diseases, and environmental ecology, while cyber security mainly solves the problems of attacks and protection in virtual space of the network. With the development of smart city information physical systems and the widespread application of big data technology, the attack behaviors of public security and network security are mutually penetrating and intertwined. For example, hackers control natural disaster sensors through attacks, illegally stealing geographic basic data information from opponent countries. Traditional methods of separating public security and network security make it difficult to locate and locate attack sources, as well as cross domain data flow behavior. The 2023 National Security Strategy of the United States emphasizes, "One of the strategic objectives is to develop cyber security requirements that support national and public security" [1]. The research on combining the information domain with the physical domain as a defense method is currently a hot topic, but there is a lack of feasible basic structures and methods for integrating the two. Public safety and cyber security correspond to the physical and information security of smart cities, involving different technological fields and implemented by different technologies. Devices with different technological systems are difficult to directly interconnect. This essay aims to delve into the multifaceted dimensions of collaborative defense in the realm of public security and cyber security, exploring the challenges, strategies, and implications of this imperative endeavor. This essay aims to conduct in-depth research on the infrastructure, technology, and methods of collaborative defense in the fields of public safety and network security in smart cities, as well as the experiments conducted.

The collaborative integration of public security and cybersecurity faces new technological challenges, they target different protection objects and require different technologies. The usual network security protection mainly relies on methods based on communication protocol processing, software

 doi:10.20944/preprints202405.0190.v1

development, and cryptographic calculations, while public safety protection involves more signal (video, audio, electromagnetic, sensor, etc.) processing technologies in addition to communication network processing mechanisms. There is no connection between them, For example, it is difficult to directly connect public video cameras to firewalls. This isolation is shown in Figure 1.

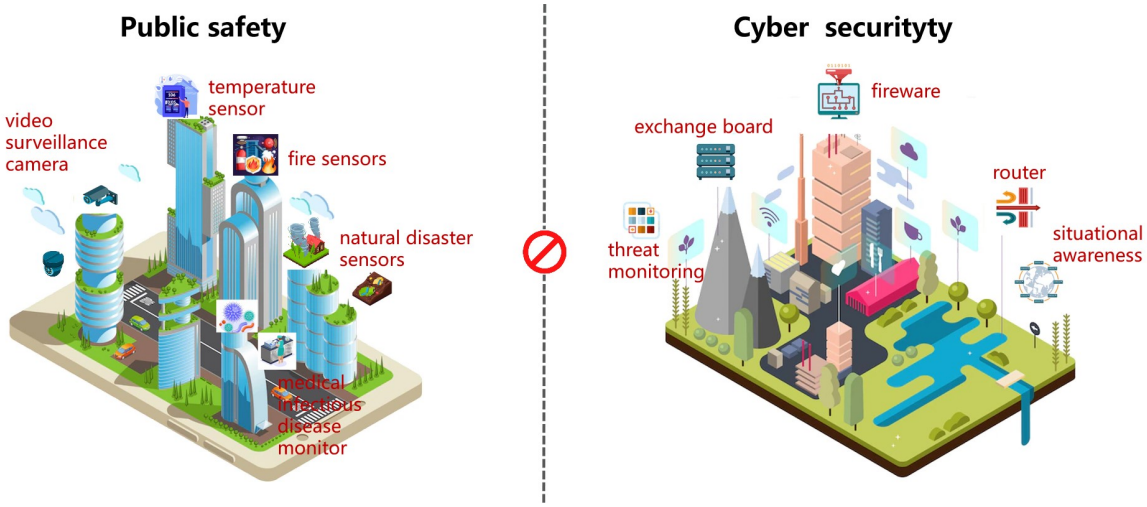

Figure 1. Public safety & cyber security.

Therefore, it is difficult to synergistically integrate different technological systems using traditional methods. Lisova et al. (2019) pointed out that safety and security co-analysis is still a developing domain [2]. Network security and public safety protection technologies are independently developed, and in recent years, researchers have made some research progress in the integration of the two technologies. Suciu et al. (2021) present a protective system, S4AllCities, that proposes advanced technological concepts and methodologies for implementing city digital intelligence and makes it accessible in real-time to authorized and authenticated security practitioners (from public & private) and city executives for advancing their situation awareness on cyber and physical threats [3]. Liu et al. (2021) proposed a collaborative modeling framework that enables co-analysis of safety and security requirements for network protocols [4]. Fan et al. (2022) proposed a simple collaborative protection system for public safety and network security based on cloud computing and big data technology [5]. Dimitrov et al. (2022) proposed a three-dimensional analysis method for smart city network security, emphasizing the unified consideration of public safety and network security factors [6]. Sengan et al. (2020) proposed a method called Hybrid Smart City Network Security Architecture (HSCCA) to address security issues related to the implementation of smart city technology. This approach not only protects data security but also analyzes risks [7]. Fang et al. (2020) designed a trust model that uses binomial distribution to calculate node trust values and proposed a trust management scheme to prevent switch attacks, ensuring that the data collection phase of smart cities can identify attack behavior from environmental interference and establish a secure data transmission path for resource-limited terminals [8]. Paul et al. (2021) [9] proposed a smart city architecture based on the Internet of Things, which protects all encryption security and privacy issues by adopting public and private chains. However, preliminary research did not focus on the specific methods and functional modules required for the collaboration of public security and network security technology mechanisms.

On the other hand, in the application of human immune theory and its network security field, Farzadnia et al. (2021) have developed a novel sophisticated hybrid method for intrusion detection using the artificial immune system [10]. Damai et al. (2021) have proposed the use of artifcial immune systems to alleviate DDoS attacks in cloud computing by identifying the most potential features of the attack [11]. Grigorieva et al. (2023) have defined the concept of cyber immunity systems, which have some common points with the theory of biological immunity [12]. Jim et al. (2022) designed a mobile self-organizing network (MANET) security method based on an artificial immune system by

 doi:10.20944/preprints202405.0190.v1

simulating the mechanisms of the human immune system. This method has better packet delivery and detection rates, even in the presence of malicious nodes [13]. He et al. (2021) designed an immune-based digital virtual asset risk assessment method by simulating the mechanism of synchronized dynamic evolution between antibody concentration and invading viruses in the human immune system. This method can effectively generate high-performance immune detectors to identify attack risks and evaluate the risk of different users being attacked in real time [14]. Fotohi(2019) proposed in his research to use the human immune system to protect unmanned aerial systems from security threats [15]. Yang(2020) proposed a network layer security detection model of Internet of Things based on immune system [16]. He et al. (2021) proposed an immune system-based defence system of robot network security [17]. Kodati et al. (2023) described an ensemble framework of artificial immune system (AIS) based on network intrusion detection system [18]. Melo et al. (2022) inspired by the human immune system and proposed an immune security model, ISM-AC, which based on alert correlation and software-defined networking [19]. Sanders et al. (2019) mentioned in their research that traditional methods treat network security and public safety protection methods as independent of each other, managed by different departments, and responded to by different technical means [20]. The above literature mainly focuses on applications in the field of cyber security and does not involve applications in public security. However, these studies did not involve the application of human immunity in the synergy of public safety and cyber security. Furthermore, these studies have not addressed the application of human immunity in the synergy of public and cybersecurity.

This paper proposes a comprehensive immune system for smart city network information security, CPCSIS, which mainly focuses on the integration of smart city network security and public safety. Based on the complex environment of the Internet of Things in a smart city, which has network heterogeneity, device heterogeneity, data heterogeneity, and cross-domain sharing, combined with the operating mechanism of the human immune system, CPCSIS has realized the perception of network information security threats and public security risk factors throughout the entire process, all domains, and all times of the smart city. On the basis of data fusion, it has carried out risk anomaly detection and completed the identification of “self" and “non-self." And timely and effective response and disposal of identified security threats are carried out to achieve the goal of disrupting and repelling unwanted intrusion activities in the system, forming a fully aware, adaptive, and self- feedback immune system. Naveed et al. (2020) present a dynamic framework, Celosia, which is inspired by the immune system offering good accuracy and high performance with minimal human intervention [21]. The Internet and cloud computing are equivalent to the human nervous system, transmitting and exchanging information to achieve precise operations in commanding and scheduling various aspects of the city. Multi-modal big data is equivalent to blood and nutrients, used to support the normal operation of the entire ecosystem. Smart city users, managers, decision-makers, and other entities are like individual cells that exist and operate continuously, completing the normal operation and metabolism of the entire system. This article proposes a smart city security protection model inspired by the human immune mechanism, CPCSIS, which is a protection system that ensures the healthy operation of the entire ecosystem. CPCSIS uses sensors, the Internet, cloud computing, big data, and user behavior information to identify and clean up harmful substances (attack threats, etc.), helping the smart city ecosystem resist external interference and maintain its own structure and function in its original state.

2. Models and Methods

2.1. The Basic Principles of CPCSIS

The proposal of CPCSIS has a solid theoretical foundation. Research in the biomedical field indicates that the human immune system is generally composed of three lines of defense. CPCSIS draws on the hierarchical structure of the three lines of defense of human immunity, focusing on the elements of citizens, enterprises, and government affairs, and constructs three lines of defense that are similar to human immunity in terms of immune methods, immune functions, and immune components, as shown in Table 1. CPCSIS combines cybersecurity with biomedical research for interdisciplinary

 doi:10.20944/preprints202405.0190.v1

innovation, which is a fundamental research method for solving complex technical problems. Its scientificity is as pointed out by Tache et al. (2023) in his research paper, through transdisciplinarity, the aim of which is to highlight the nature and characteristics of the flow of information that circulates between the different branches of knowledge [22].

The basic principle of CPCSIS is shown in Figure 2.

Table 1. Comparison of similarities between CPCSIS and human immunity.

The basic properties of immunity	Human immunity	CPCSIS
Immune mode	The immune system of the human body includes a series of processes such as the exclusion or elimination of foreign objects (such as allergic reactions, rejection reactions), as well as intervention measures such as planned immunity (vaccination).	The comprehensive prevention and control of network security in smart cities can also be divided into the process of discovering or disposing of network and public security threats (cross domain denial of security threats, dynamic adjustment of security strategies), as well as monitoring and warning of unknown threats through behavior learning and other methods.
Immunity	The human immune function includes three main tasks: immune monitoring, immune response, and immune memory. Immune surveillance identifies pathogens such as bacteria, viruses, fungi, etc; The immune response extensively clears invading pathogens and implements precise strikes against them; Immune memory exerts a stronger immune response, enabling complete elimination of pathogens.	The comprehensive immunity of smart city network information security has achieved security functions such as anomaly detection, threat identification, asset protection, emergency response, state recovery, and attack blocking through network security components and prevention and control measures, maintaining the smooth operation of the network environment.
Immune components	There are three immune defense lines in the human body:The first line of defense includes skin, mucous membranes, etc; The second line of defense includes phagocytosis, bactericidal substances, neutrophils, etc. The first two lines of defense are natural defense functions gradually established by humans in the process of evolution. They do not target a specific pathogen and have defensive effects against multiple pathogens; The third line of defense is lymphocytes, a type of white blood cell that is responsible for combating external infections and monitoring cellular mutations in the body.	Based on the principle of human immune components, the immune components of smart cities are also composed of three lines of defense: The first line of defense emphasizes environmental awareness, scene awareness, and access control capabilities; The second line of defense completes functions such as information fusion, threat detection, and element rights confirmation; The third line of defense is equipped with safety isolation, coordinated disposal, and learning modeling.

CPCSIS has a three line defense architecture. HWolf-Ostermann (2021) mentioned in his paper the basic concepts of three lines of defense structure of the human immune system [23]. In the corresponding CPCSIS, firstly, it is able to achieve network and public environment perception and scene cognition, and secondly, it has basic access control capabilities, which can defend against attacks of moderate intensity in the network environment. In the paper by Robert et al. (2023), it was mentioned that bactericidal substances and phagocytic cells form the second line of defense, which has the functions of phagocytosis and digestion. They phagocytose, process antigens, and transmit antigen-specific transmission to T lymphocytes and B lymphocytes [24]. Analogous to the information fusion, threat discovery, and factor authentication mechanisms in the CPCSIS system,

 doi:10.20944/preprints202405.0190.v1

the fusion of public safety and cyber security information is similar to the phagocytic and digestive functions of phagocytic cells. Antigen specificity is similar to identifying “self" and “non-self" abnormal behaviors that already exist, identifying and blocking illegal access, illegal acquisition, and illegal leakage behaviors, and presenting the identified information to higher-level analysis, response, and processing systems, confirming the ownership of key data and its circulation, for risk fusion analysis and response strategy generation across the entire network. In the paper by Chiara et al. (2023), it was mentioned that the third line of defense is composed of immune organs and immune cells, which is an acquired defense function gradually established by the human body after birth and only works against a specific pathogen or foreign object [25]. The characteristic of specific immunity is immune memory, which is the ability of the human body to resist infections acquired through acquired infections or artificial vaccination and can acquire memory against the antigen.

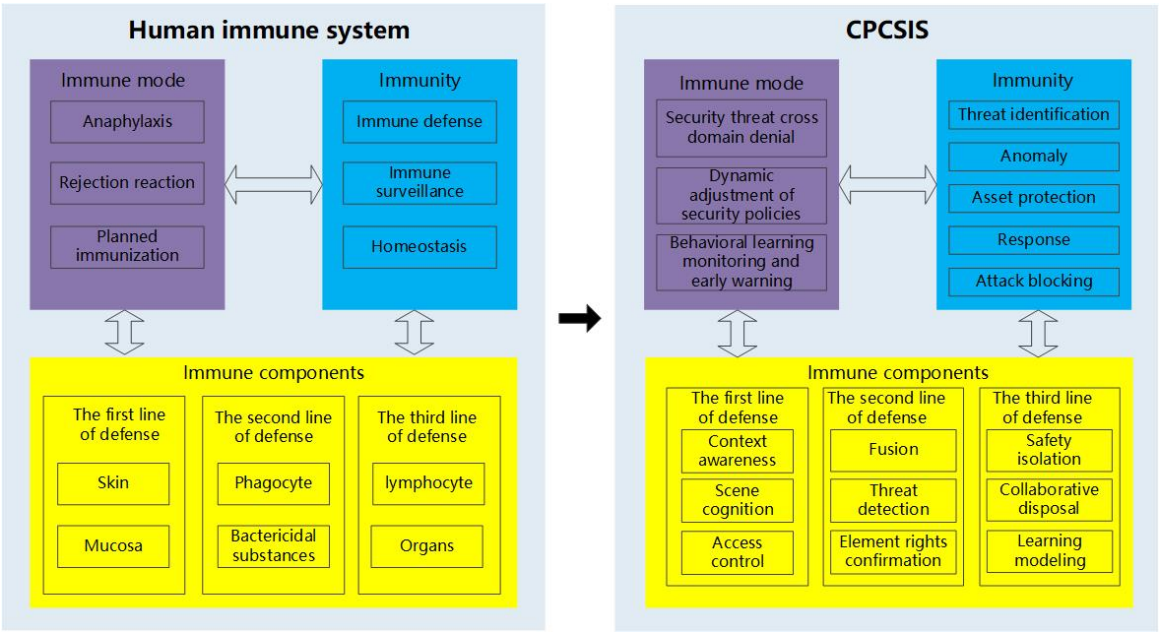

Figure 2. Schematic diagram of CPCSIS principle

In the field of network security, protective systems constructed based on algorithms such as artificial intelligence and machine learning can also achieve similar learning, recognition, memory, and feature extraction capabilities. When facing specific types of risks (such as abnormal behavior) and new threats (APT), these protective measures can establish highly specialized detection strategies, defense strategies, and isolation mechanisms, making the entire immune system exhibit typical self-learning habits. Adaptability to achieve specific immunity for network security.

2.2. The Basic Components of CPCSIS

The three lines of defense of the CPCSIS system will include network and public security protection functional components in multiple key information infrastructure areas of smart cities, such as the Internet of Things, IP Internet, and Industrial Internet, as shown in Figure 3.

Among them, the public security monitoring platform module based on video surveillance, the public security and network security strategy visualization module, the network security monitoring data collection module, the intelligent public security gateway module, the multi-source heterogeneous data collection module, the network asset mapping module, the network security vulnerability scanning module, and the public security multi-risk linkage analysis and accurate warning module (including network public opinion monitoring and content security monitoring) are included. They form the first line of defense with environmental awareness, scene awareness, and access control capabilities.

 doi:10.20944/preprints202405.0190.v1

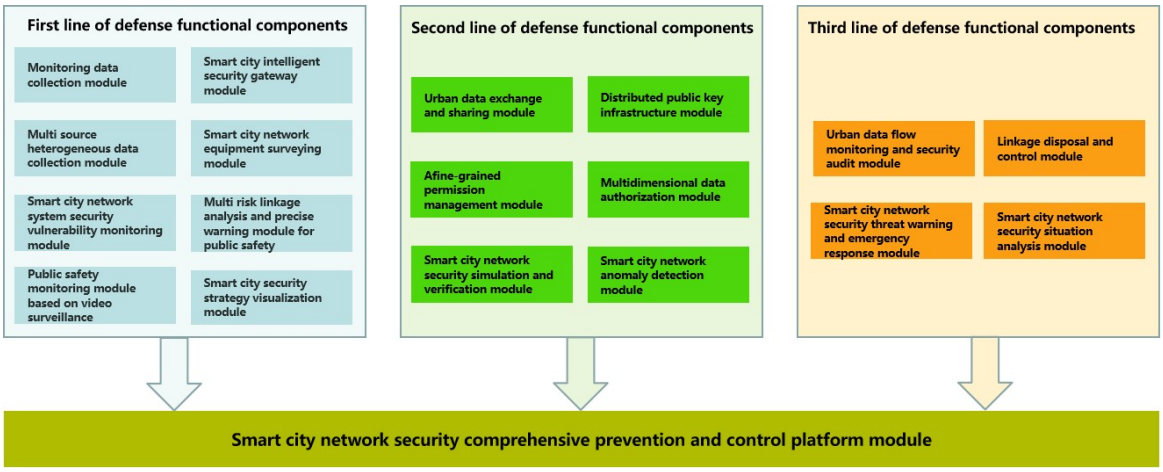

Figure 3. CPCSIS Functional Components.

The second line of defense consists of a distributed public key infrastructure module, a fine-grained permission management module, an urban data sharing and exchange module, a multi-dimensional data authorization module, a multi-dimensional simulation module for virtual and real integration of smart cities, and a comprehensive threat detection module for smart cities. It will provide information fusion, threat discovery, and element authorization mechanisms for public and network security in smart cities at the level of virtual and real space.

On the third line of defense, the smart city network security and public security situation analysis module, the smart city ultra-large capacity data flow monitoring module, the network security and public security linkage disposal and control module, the network security and public security threat warning and disposal module, and the smart city network information security comprehensive immune prevention and control platform module are combined to output security isolation, linkage disposal, and learning modeling mechanisms.

The smart city network information security comprehensive immune prevention and control platform module is the fusion processing center unit of CPCSIS. The first line of defense is displayed in the smart city network security comprehensive prevention and control platform, which includes the perception and detection of the smart city network environment, including the distribution of smart city network assets, asset attributes, and asset risk vulnerabilities; Understanding the operational status of smart city business systems and application scenarios; Display the execution results of network control operations triggered by public safety incidents, etc. The first line of defense is achieved through the combination of middleware - public security and network security strategy visualization module, intelligent public security gateway module, and public security monitoring platform module for video surveillance, to handle public security events under collaborative control conditions. The second line of defense displays the protection status of important business data in the smart city network security comprehensive prevention and control platform module, including the operation status of element authorization, threat detection of data flow, and dynamic operation process information of multimodal data information fusion. Among them, based on blockchain technology, element rights are mainly achieved. The third line of defense in the smart city network security comprehensive prevention and control platform module mainly displays monitoring and early warning information of unknown attack threats in smart city government information networks, multi-sensor networks, and the Internet of Things, corresponding network security control strategies, as well as security isolation measures and their results against high-level attack threats. In terms of interfaces for collaborative disposal, in the first line of defense, the Smart city intelligent security gateway module collects data from smart city IoT sensors, reports the detected environmental data to Smart city security strategy visualization module, and disposes of IoT sensors based on the disposal actions issued by Smart city security strategy visualization module. The Public safety monitoring module based on video surveillance monitors

 doi:10.20944/preprints202405.0190.v1

public safety event information through video capture and reports real-time information on possible personnel intrusion. The multi risk linkage analysis and precise warning module for public safety issue real-time alarm information based on the reported public safety event information, and report it to the smart city security strategy visualization module, then it receives and integrates alarm event data from the public safety multi risk linkage analysis and accurate warning system, as well as the smart city intelligent security gateway. The smart city security strategy visualization module reports the execution results of the security response strategy to the smart city network security comprehensive prevention and control platform module, this module processes the received alarm information and issues disposal commands and actions layer by layer. The communication interfaces between various devices in the first line of defense and the interface with the smart city network security comprehensive prevention and control platform are shown in Figure 4:

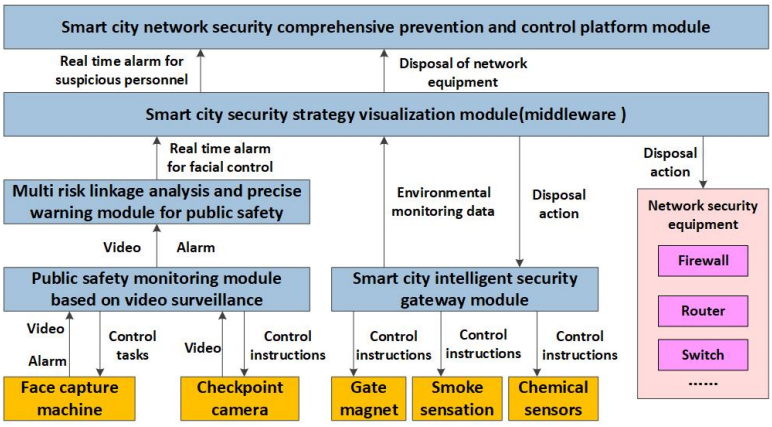

Figure 4. Interface relationship of the first line of defense.

The second line of defense mainly completes the dynamic display of the protection process in the smart city network security comprehensive prevention and control platform. Therefore, the system interaction design in the second line of defense is implemented in the form of web page URL redirection.

The third line of defense is mainly aimed at protecting against high-level sustained attacks and other high-energy level attack activities. Through the ability to learn and model unknown attacks, it intelligently executes security isolation and linkage disposal measures. The interface and communication relationships of the various components of the third line of defense are shown Figure 5:

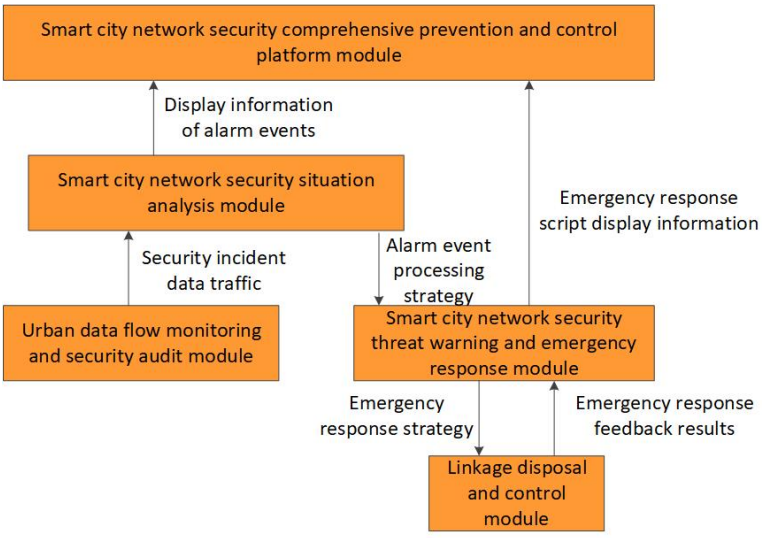

Figure 5. Interface relationship of the third line of defense.

 doi:10.20944/preprints202405.0190.v1

2.3. The Collaborative Protection Method of CPCSIS

The human immune system has an adaptive regulatory mechanism to maintain immune balance. CPCSIS will adopt an elastic protection mechanism for attacks and invasions of different intensities, which can be adjusted through changes in the operating status of the three lines of defense to achieve this elastic protection. The defense of the human immune system is a limited defense, and the immune process of the three lines of defense of the human immune system is a hierarchical and evolutionary process rather than a simultaneous initiation process. Therefore, in the context of a wide variety and distribution of smart city Internet and IoT devices, as well as complex and diverse attack and intrusion pathways, in order to prevent situations where the three lines of defense are "under protected" or "over reinforced," CPCSIS needs to design an elastic adjustment algorithm to dynamically control the operation process of the three lines of defense. About the Dynamic Arrangement of Security Resources, Shao et al. (2020) proposed a resource optimization allocation strategy based on particle swarm optimization [26]. Mahfouzi et al. (2019) proposed a security-aware methodology for routing and scheduling for control applications in Ethernet networks [27]. The protection control process based on the CPCSIS elastic adjustment defense algorithm is divided into four steps:

Step 1: Calculation of Smart City Network Security Threat Index Based on Information Entropy

Jing et al. (2024) proposed a resilience-oriented planning strategy for thecyber-physical active distribution network (ADN) under the malicious attacks [28]. Ibrahim et al. (2022) proposd an efficient protection mechanism against entropy deception, which is based on the analysis of changes in different entropy types, namely Shannon, Renyi, and Tsallis entropies, and monitoring the number of distinct elements in a feature distribution as a new detection metric [29]. Yang et al. (2021) proposed a dynamic spatio-temporal causality modeling approach to analyze traffic causal relationships for the large-scale road network [30]. Numerous studies have shown that Shannon entropy can be used to discover changes in the normal distribution of network traffic, thereby identifying security anomalies. By monitoring the flow entropy of the smart city network through the functional modules of the first and second lines of defense of CPCSIS, the network status and security status of the smart city can be detected. For traffic samples in cyberspace, the probability distribution of public safety and network security attributes of traffic packets can reflect the characteristics of traffic, and information entropy can measure any variable, which is a feature quantification method.

Algorithm 1 Part of the Smart City Network Space Security Threat Level

Input: Probability of IP address segment distribution $\{P = p_1, p_2, \ldots, p_n\}$
Output: The degree of attack threat R_s
$\{Q = q_1, q_2, \ldots, q_n\} \leftarrow$ Average probability distribution $\{X = x_1, x_2, \ldots, x_n\}$
for $i = 1, 2, \ldots, n$ **do**
    Relative entropy $A \leftarrow$ Relative entropy$D(P||Q)$
end for
for $i = 1, 2, \ldots, n$ **do**
    Scan traffic entropy $B \leftarrow$ Scan entropy$D(P, Q)$
end for
if `checkentropyverity(A,B)` **then**
    $R_s \leftarrow$`calculatethreatlevel()`
else
    return Unreasonable scanning flow entropy
end if

Implement real-time detection of malicious attack threats based on the smart city network security situation awareness method of scanning traffic entropy, with specific methods: Assuming that the cyberspace of smart cities is represented by a random variable s, we define its set of values as:$\{s = s_1, s_2, \ldots, s_n\}$. The probability distribution of values is defined as: $\{p = p_1, p_2, \ldots, p_n\}$. Wherein

 doi:10.20944/preprints202405.0190.v1

$\sum_{i=1}^{n} p_i = 1$, p_i indicate the probability of 1 to n network anomalies occurring, $0 < p_i < 1$. The information entropy of variable can be expressed as:

$$H = -\sum_{i=1}^{n} p_i \log p_i. \tag{1}$$

The H value determines the degree of attack on the system network. The lower the value, the more stable the system is; the higher the value, the more chaotic the system is. Chen et al. (2022) proposed an improved Technique for Order Preference by Similarity to Ideal Solution , called CPR-TOPSIS, which is based on information Communication Probability and Relative entropy (CPR) and presented for identifying influential nodes in complex networks from the view of global, local and location information dimensions [31]. In the CPCSIS, Relative entropy is equivalent to the information entropy of two probability distributions, which can characterize the similarity between the two probability distributions. For the distribution of two discrete probabilities $\{P = p_1, p_2, \ldots, p_n\}$ and $\{Q = q_1, q_2, \ldots, q_n\}$, where:

$$\sum_{i=1}^{n} p_i = \sum_{i=1}^{n} q_i = 1. \tag{2}$$

Overall, the formula for calculating relative entropy for P and Q is:

$$D(P||Q) = -\sum_{i=1}^{n} p_i \log \frac{p_i}{q_i}. \tag{3}$$

Where D represents the difference in probability distribution between P and Q; When D is 0, Indicates that P and Q belong to the same distribution, because $D(P||Q) \neq D(Q||P)$. In order to accurately and stably depict the distribution of P and Q , Expanding relative entropy to scan flow entropy:

$$D(P,Q) = -\sum_{i=1}^{n} p_i\{p_i - q_i\} \log \frac{p_i}{q_i}. \tag{4}$$

Based on the above, it can be concluded that When the cyberspace domain of the smart city that needs to be protected is divided into n_s blocks, Within the t time cycle, The summary of failed application messages is N_{fail}, The number of failed network space application messages in the i block is N_i^{fail}. Use Equation (5) to obtain $P_i^{src}(\pi)$ which is the probability distribution of failed application source addresses within a time cycle. Wherein, the probability distribution of destinations can be expressed as $P_i^{Dst}(\pi)$, setting $j\epsilon\{Src, Dst\}$.

$$p_i^j(\pi) = \pi \cdot \left(\sum_{i=1}^{N_{fail}} \pi_i \right). \tag{5}$$

The above methods can better grasp the current operation status and environment of protected networks in smart cities and perceive various attackers and their attack activities, such as zombie networks, malicious websites, and denial of service.

From a mathematical perspective, based on the completion of information entropy calculation, the average number of scans of each partitioned address space in a specified time period is $\frac{N_{fail}}{n_s}$. But in reality, Within a divided time period, the likelihood of completing a random scan is relatively low. In a failed application message within a time period, it is easier to directly calculate the probability distribution of the obtained IP address and $\frac{N_{fail}}{n_s}$ scan traffic entropy in engineering. Therefore, this situation can be adjusted through the criterion of Formula (6).

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 May 2024 doi:10.20944/preprints202405.0190.v1

$$\frac{N_{fail} - \frac{N_{fail}}{n_s}}{\frac{(n_s)^2}{12}} < -\delta. \tag{6}$$

Step 2: Classification of Cyber security threats in smart cities based on the threat level, Formula (7) is used to calculate the probability distribution of IP addresses in failed application packets within the time period and the corrected average probability distribution scan traffic entropy. By comparing it with the set threshold, the degree of attack threat can be determined.

$$R_s = D_{KL}(P_t^{Src}(\pi) \parallel \frac{N_{fail}}{n_s}) = -\sum_{t=1}^{n}(P_t^{Src}(\pi) - \frac{N_{fail}}{n_s}) \log \frac{P_t^{Src}(\pi)}{\frac{N_{fail}}{n_s}}. \tag{7}$$

R_s represents the cyberspace security threat index. The overall algorithm process can be found in Algorithm 1.

Step 3: The classification of security threat levels for smart cities by CPCSIS should include both public safety and cybersecurity factors. In the third step, the cyber security threat level index is calculated using information entropy. According to the research of Guo et al. (2020), The level of public safety threat is generally divided according to the regulations of government management departments for various types of public threats [32]. For the convenience of research, this article only focuses on threats related to smart city video surveillance and network public opinion content security and divides them into four levels: R_p representing the Public Security Threat Index, $R_{pe(1,2,3,4)}$. Calculate the threat level of smart cities using weighted processing algorithms as shown in Formula (8):

$$I_s(t) = \alpha R_p + \beta R_s. \tag{8}$$

In the formula, α is the public safety factor, β is the Cyber security factor, $\alpha + \beta = 1$. According to the requirements of CPCSIS application scenarios, it can be divided into three situations:

a) $\alpha > \beta$: Public safety disposal or scenarios with high attention, such as natural disasters;

b) $\alpha = \beta$: Scenarios where public safety factors are of equal concern to cybersecurity factors, such as handling public health incidents, etc;

c) $\alpha < \beta$: Scenarios with high cyber security disposal or attention, such as being subjected to organized large-scale network attacks, etc.

In theory, the values of relative entropy and flow entropy can be infinitely large, and the value of R_s is infinite. However, the actual situation is not like this. According to the research of Imanbayeva et al. (2020), When the system becomes chaotic to a certain extent, it will become unusable as a whole [33]. As a result, the value of R_s will never be infinite, there always exists an upper limit value γ. The range of values for $I_s(t)$ is : $0 \leq I_s(t) < 3 + \gamma$. By dividing the interval of $[0, 3 + \gamma)$ into 5 segments, 5 threat levels can be formed. The classification of attack threat levels can be calculated, as shown in Table 2.

Table 2. Threat Level Classification.

Grade	R_sValue range	Threat level
1	$[0, \frac{3+\gamma}{5})$	Normal
2	$\left[\frac{3+\gamma}{5}, \frac{2\times(3+\gamma)}{5}\right)$	Low
3	$\left[\frac{2\times(3+\gamma)}{5}, \frac{3\times(3+\gamma)}{5}\right)$	Medium
4	$\left[\frac{3\times(3+\gamma)}{5}, \frac{4\times(3+\gamma)}{5}\right)$	High
5	$\left[\frac{4\times(3+\gamma)}{5}, (3+\gamma)\right)$	Extremely high

 doi:10.20944/preprints202405.0190.v1

Step 4: Three lines of defense operation control based on threat level classification According to the attack threat level of protected objects in smart cities, the activation status design of the functional components of the three lines of defense of CPCSIS is shown in Tables 3–5, respectively.

Table 3. The activation status of the first line of defense functional components.

Functional module	Grade 1	Grade 2	Grade 3	Grade 4	Grade 5
Monitoring data collection module	●	●	●	●	●
Smart city intelligent security gateway module				●	●
Multi source heterogeneous data collection module			●	●	●
Smart city network equipment surveying module					●
Smart city network system security vulnerability monitoring module			●	●	●
Multi risk linkage analysis and precise warning module for public safety		●	●	●	●
Public safety monitoring module based on video surveillance		●	●	●	●
Smart city security strategy visualization module	●	●	●	●	●

Table 4. The activation status of the second line of defense functional components.

Functional module	Grade 1	Grade 2	Grade 3	Grade 4	Grade 5
Urban data exchange and sharing module		●	●	●	●
Distributed public key infrastructure module					●
Afine-grained permission management module			●	●	●
Multidimensional data authorization module				●	●
Smart city network security simulation and verification module					●
Smart city network anomaly detection module		●	●	●	●

 doi:10.20944/preprints202405.0190.v1

Table 5. The activation status of the third line of defense functional components.

Functional module	Grade 1	Grade 2	Grade 3	Grade 4	Grade 5
Urban data flow monitoring and security audit module				●	●
Linkage disposal and control module					●
Smart city network security threat warning and emergency			●	●	●
Smart city network security situation analysis module		●	●	●	●
Smart city network comprehensive prevention and control platform module	●	●	●	●	●

The collaborative protection principle of CPCSIS proposed by this innovative research work is in line with the current trend of smart city information infrastructure development and the common research practice of researchers in this field. Kaššaj et al. (2024) highlights the importance of cooperation between city authorities, local communities and European institutions to achieve successful digital urban development [34]. CPCSIS will promote cooperation between public safety management departments and cybersecurity management departments in smart cities.

3. Experiment and Analysis of Models

3.1. Experimental Purpose

By using different network attack methods and public video surveillance images with different levels of danger, experiments were conducted to test the ability of CPCSIS to synergistically protect public security and network security. The effectiveness of collaborative protection is evaluated in two dimensions: detection and disposal rates. Meanwhile, compare the disposal efficiency of traditional methods and CPCSIS under different threat levels.

3.2. Experimentation

1) Implement the functional module structure of CPCSIS through open source software and programming development. Use four common public safety protection devices: video cameras, temperature sensors, position sensors, access control sensors, and gas sensors to build a public safety experimental environment. Build a network security experimental environment using firewalls, routers, switches, and intrusion detection systems.

2) Public safety dataset: Use the CIFAR-10 dataset and label the images in the dataset with different labels, representing different levels of threat to public safety: 1, 2, 3and 4. Then send the image data to CPCSIS for testing.

3) Network security dataset: Using the IoT-23 dataset to simulate DDoS attacks, IoT botnet attacks, and other attack methods.

4) Based on testing the information entropy of the experimental environment, the γ value in Table 2 is 135.

3.3. Experimental Result

310 experiments were conducted on CPCSIS using public safety and cyber security datasets. The detection and disposal rates of CPCSIS under five different threat levels are shown in Figure 6. Detection rate refers to the proportion of successful detection of attack threats, while the disposal rate refers to the proportion of successful disposal (including network isolation and IoT device control)

 doi:10.20944/preprints202405.0190.v1

using network security protection equipment and public security equipment after discovering attack threats.

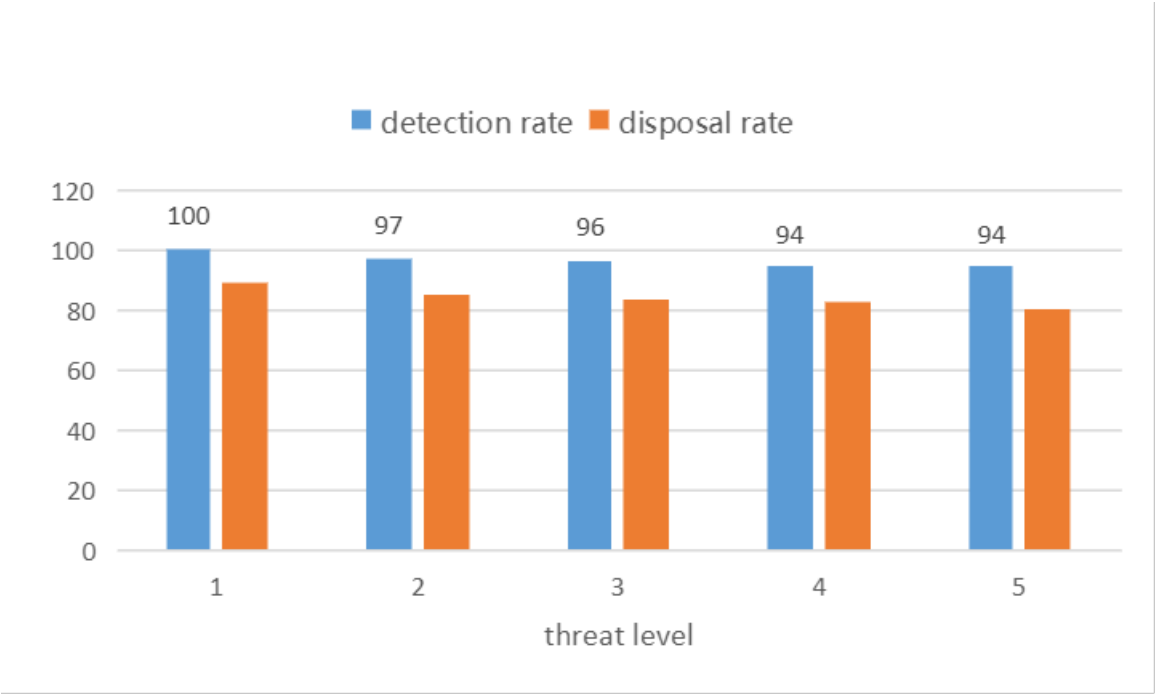

Figure 6. detection and disposal rates of CPCSIS.

During the experiment, a comparison was made between CPCSIS and traditional defense methods. The traditional method refers to using public security and network security methods separately to deal with attack threats, without any cooperative relationship between them, but with different processing orders. When public security and network security threats arise, the traditional defense method is to use independent mechanisms for defense, and record the control operation time of operating the four sensors as T_p, And the time for operating firewalls, routers, switches, and intrusion detection systems separately is recorded as T_c, The time for traditional operations is recorded as $T_1 = T_p + T_c$, The response time of CPCSIS is recorded asT_2. Comparison betweenT_1 and T_2, Reflect the difference in processing efficiency between traditional methods and CPCSIS. Also, compared the defense success rates of CPCSIS and traditional methods in 310 attack tests as shown in Figure 7.

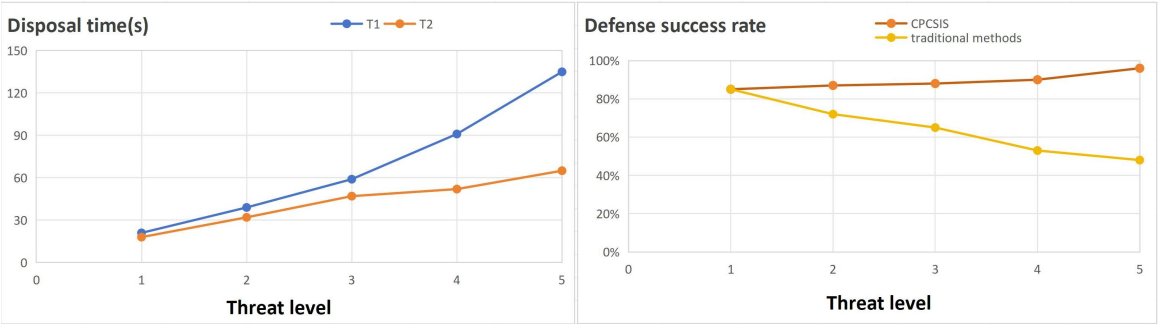

Figure 7. Comparison between CPCSIS and traditional methods.

During the experiment, the processing orders for the four types of sensors, as well as the processing orders for operating firewalls, routers, switches, and intrusion detection systems, were exchanged, and the resulting differences in processing efficiency showed the same trend.

 doi:10.20944/preprints202405.0190.v1

4. Discussion and Conclusions

Prior work has documented the research of overall safety of smart cities, S4AllCities, for example. Compared with the S4AllCities project proposed by Suciu et al. (2021), the similarity is that both papers propose the architecture of smart city security protection. The previous paper proposed a smart city defense architecture, called SoS, which consisting of a three-layer digital twin structure (DecIoT, MAIDS and ACMS). This article proposes an architecture inspired by human immune mechanisms-CPCSIS. The difference is that the focus of the SoS architecture is focused on: risk-based open smart spaces security management; cyber security shielding; and behavior tracking; real-time estimation of cyber-physical risks in multiple locations and measures activation for effective crisis management. While CPCSIS combines public safety and network security technology mechanisms more targeted, and has stronger defense capabilities against complex and unknown security risks. The above experiment confirms the collaborative protection capability provided by CPCSIS. Figure 4 reflects the relatively stable and balanced response ability of CPCSIS when facing different threat levels from the dimensions of detection rate and disposal rate. Figure 5 shows that as the threat level increases, the average disposal time of the traditional method of separating public security and network security will gradually increase, while CPCSIS shows better protection capabilities. Meanwhile, Figure 5 also demonstrates that, With the changing intensity of public and cybersecurity attack threats, the defense capability of CPCSIS is significantly stronger than traditional methods. Therefore, when dealing with complex threat scenarios, such as unknown attack threats, the superiority of CPCSIS will be more prominent. At the same time, this study reveals that when it is necessary to consider a mixed protection scenario of network security and public safety factors in smart cities, by referring to the inherent logic of environmental perception, anomaly detection, and antibody learning in the three lines of human immunity, and by designing certain middleware and orchestration algorithms, the two can be organically combined. On the other hand, the research practice of this article has demonstrated the cross application of biomedical concepts in the field of cybersecurity in smart cities. Collaborating on public safety and network security protection resources is the development trend of future smart city security defense, and CPCSIS is an effective method. However, alongside these promising results, challenges arose. The research experiment in the paper only involves four types of public security devices and four types of network security devices. In the next stage, more devices need to be added for experiments to verify the correctness of the research conclusions. Furthermore, the value γ in formula 8 above will exhibit different values with different network scenario conditions. In the future, it is necessary to study the γ values under various different network entropy conditions and establish corresponding relationship tables. The CPCSIS must be tested using as many attack datasets as possible in various complex smart city network environments to ensure its wide applicability and effectiveness.

Acknowledgments: This work is supported by National Key R&D Program of China (no. 2019YFB2101700) and National Nature and Science Grant (no. U20B2048).

References

1. National Cybersecurity Strategy 2023. White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf(February 21, 2024).
2. Elena Lisova, Irfan Sljivo, and Aida Čaušević. Safety and Security Co-Analyses: A Systematic Literature Review. *IEEE Systems Journal* **2019**, *1*, 2189–2200.
3. G.Suciu, I. Hussain, G. Iordache, C. Beceanu, R. A. Kecs and M. Safety and Security of Citizens in Smart Cities. 2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet), Iasi, Romania, November 4, 2021.
4. Z. Liu, Q. Wang, Y. Li, and Y. Zhao. "CMSS: Collaborative Modeling of Safety and Security Requirements for Network Protocols," IEEE Intl Conf on Parallel and Distributed Processing with Applications, Big Data and Cloud Computing, Sustainable Computing and Communications, Social Computing and Networking (ISPA/BDCloud/SocialCom/SustainCom), 2021.

5. J. Fan, K. Hu, Z. Chen, and J. Li. Research on Information Sharing and Fusion of Public Security Information Under Big Data Environment. *Fresenius Environmental Building* **2022**, *31*, 6115-6123.
6. W. Dimitrov, K. Spasov, I. Trenchev, S. Syarova, "Complexity Assessment of Research Space for Smart City Cybersecurity, " IFAC Workshop on Control for Smart Cities (CSC), 2022.
7. S. Sengan, V. Subramaniyaswamy, S.K. Nair, et al., "Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network,"*Future generation computer systems* **2020**, *112*, 724-737.
8. W. Fang, N. Cui, W. Chen, et al., "A trust-based security system for data collection in smart city, " *IEEE Transactions on Industrial Informatics*, **2020**, *17*, 4131-4140.
9. R. Paul, N. Ghosh, S. Sau, et al. "Blockchain based secure smart city architecture using low resource IoTs," *Computer Networks* **2021**, *196*, 198-207.
10. E. Farzadnia, H. Shirazi, and A. Nowroozi, "A novel sophisticated hybrid method for intrusion detection using the artificial immune system, " *Journal of Information Security and Applications*, **2021**, *58*, 199-223.
11. D.J. Prathyusha, G. Kannayaram, "A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment, " *Evoluationary Intelligence*, **2021**, *14*, 607-618.
12. N.M. Grigorieva, S.A. Petrenko, "Biological Metaphor for Cyber Immunity. 2023 XXVI International Conference on Soft Computing and Measurements (SCM)," 2023.
13. L.E. Jim, N. Islam, M.A. Gregory, "Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes, " *Computers & Security* **2022**, *113*, 67-69.
14. J. He, T. Li, B. Li, X. Lan, Z. Li and Y. Wang, "An immune-based risk assessment method for digital virtual assets, " *Computers & Security* **2021**, *102*, 102-134.
15. R. Fotohi, "Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system," *Reliability Engineering & Sysstem Safety* **2019**, *193*, 237-253.
16. B. Yang, "Network Layer Security Detection Model of Internet of Things Based on Immune System, " Annual International Conference on Information System and Artificial Intelligence (ISAI), 2020.
17. H. He, Z. Zhu and J. Zhang, "An immune system-based defence system of robot network security, " *Journal of Physics: Conference Series* **2021**, *1873*, 012082.
18. S. Kodati, N Sreekanth, K.S.R.K. Sarma, P. Chandra Sekhar Reddy, Archana Saxena and B. Palajonna Narasaiah. Ensemble Framework of Artificial immune system based on Network Intrusion Detection System for Network Security Sustainability, International Conference on Materials Processing and Characterization (ICMPC 2023), Newcastle upon Tyne, UK, FEB 15 2024.
19. R. V. Melo, D.J.M., Douglas, K. Diego, D.B. Alessandra, M.F. Mauricio, "ISM-AC: an immune security model based on alert correlation and software-defined networking," *International Journal of Information Security* **2022**, *21*, 191-205.
20. B.S. Carrie, L. Debra, "New public management and the extension of police control: community safety and security networks in Canada, " *POLICING & SOCIETY* **2019**, *29*, 566-578.
21. K. Naveed, H. Wu. Celosia, "An Immune-Inspired Anomaly Detection Framework for IoT Devices, "IEEE Conference on Local Computer Networks (LCN), 2020.
22. (ADD-12) Popa Tache, C.E., & Săraru, C.-S. (2023). Lawfare, Between its (Un)Limits and Transdisciplinarity. Precedente Revista Jurídica, 23, 37-66. https://doi.org/10.18046/prec.v23.5889.
23. HWolf-Ostermann, "The role of collagen in immune health. *NutraCos* **2021**, *20*, 8-10.
24. S. Robert, K. Jolanta, C. Maciej, "Mechanisms of evasion of the innate immune system response by human coronaviruses, " *Alergia Astma Immunologic* **2023**, *28*, 85–94.
25. M. Chiara, T. Mauro, M. Fernanda, T.E. Rotondo, J. Charles, "Probiotics Mechanism of Action on Immune Cells and Beneficial Effects on Human Health, " *Cells* **2023**, *12*, 231- 242.
26. Z. Shao, L. Chen and T. Zhang, "Dynamic Deployment of Power IoT Security Components with Unified Resource Scheduling, " IEEE Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2020.
27. R. Mahfouzi, A. Aminifar, S. Samii, P. Eles, & Z. Peng, "Security-aware Routing and Scheduling for Control Applications on Ethernet TSN Networks, "*ACM Transactions on Design Automation of Electronic Systems*, **2020**,*25* , 1–26.
28. X. Jing, W. Qin, H. Yao, X. Han and P. Wang, " Resilience-oriented planning strategy for the cyber-physical ADN under malicious attacks, " *Applied Energy*,**2024**,*353* ,1510-1524.

 doi:10.20944/preprints202405.0190.v1

29. J. Ibrahim, S. Gajin, "Entropy-based Network Traffic Anomaly Classification Method Resilient to Deception.*Computer Science and Information Sysstems*,**2022**,*19*,87-116.
30. S. Yang, L. Ning, X. Cai and M. Liu, "Dynamic Spatiotemporal Causality Analysis for Network TrafficFlow Based on Transfer Entropy and Sliding Window Approach, " *Journal of Advanced Transaction*, **2021**,*2021*, 234-251.
31. D. Chen, G. Xu, L. Meng, and P. Yang, "CPR-TOPSIS: A novel algorithm for finding influential nodes in complex networks based on communication probability and relative entropy, " *Physica-Asia Statistic Mechanics and ITS Applications*,**2022**,*603*,435-448.
32. H. Guo, L. Cheng, S. Li, and H. Lin, "Regional risk assessment methods in relation to urban public safety, " *Process Safety and Environmental Protection*,**2020**,*143*,361-366.
33. A. Imanbayeva, Y. Tursynbek, R. Syzdykova, and A. Mukhamedova, "Evaluating the effectiveness of information security based on the calculation of information entropy, " Annual Conference on Science and Technology Research (ACOSTER), 2020.
34. (ADD-13) Kaššaj M, & Peráček T. 2024. Sustainable Connectivity—Integration of Mobile Roaming, WiFi4EU and Smart City Concept in the European Union. Sustainability, 16 (2):788. https://doi.org/10.3390/su16020788.