Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 1992429, 9 pages
https://doi.org/10.1155/2022/1992429

Research Article

Preschool Cyber Security Management System Based on Intelligent Agents

Jing Song

Zhengzhou Preschool Education College, Zhengzhou 450000, China

Correspondence should be addressed to Jing Song; songjing@zzpec.edu.cn

Received 29 August 2022; Revised 21 September 2022; Accepted 23 September 2022; Published 7 October 2022

Academic Editor: Konstantinos Demertzis

As information and communication technologies create an ever-increasing complexity in interconnected systems and devices, cybersecurity and privacy issues are constantly at the fore, highlighting the need to strengthen the protection and resilience of these systems against the ever-evolving threats of modern cyberspace. This particular work, taking into account that preschool children now have significant needs to ensure their digital identity and, in general, their protection from their contacts with the internet, aspires to provide an understandable and practical guide to strengthen the security of information systems and information from both public and private school agencies. Specifically, a preschool cybersecurity management system based on intelligent agents is proposed. Using sophisticated, intelligent techniques, it aims to improve the ability of preschools to resist modern threats adequately, respond to cyber-attack incidents with the least possible impact, and protect their critical systems, services offered, and the personal data they hold and process. The system intends to link and control distributed systems that currently exist, as well as to solve issues that are beyond the knowledge and skills of a single agent. This novel research idea has never been offered in the relevant literature, and we think it has the potential to advance the state of the art in cybersecurity significantly.

1. Introduction

Today's typical structure of the information systems of an educational institution such as preschools has reached an exceptionally high degree of complexity [1]. Their essential characteristics include at least a central building infrastructure with servers that have public IP (web, mail, DNS, etc.) and with various internal networks that host employees' office computers or other infrastructures used in education [2]. Sometimes, employees bring their own portable devices (laptops, tablets, and smartphones) connected to the carrier's network to the workplace and their mobile storage media (USB, external hard drives, etc.) [3].

The remote offices of the same organization in other regions with their own corresponding internal network infrastructure should be added to the infrastructures in question. The operator's applications assist the specific computing systems, usually web, hosted in the data centers of one or more cloud service providers [4]. Recently, due to the pandemic, the institution's employees, as well as the teachers, work from home (teleworking), connect remotely to the institution's internal network and handle critical data using a home network and computers that have not been tested and certified in terms of their safety [5, 6]. Also, third-party providers and suppliers who have undertaken the development of applications and the technical support of the organization's systems connect remotely to its internal network through their infrastructure or have assigned the work to their subcontractor [7].

As is logical, the sensitive data of educational institutions, especially those related to preschool children, should be supported by information systems that are at least aligned with in-depth defense architecture. In this model, security measures and mechanisms are applied in successive layers

across the entire scope of an operator's network and data to protect them from threats [8]. Each layer individually does not deal with all threats, while they deal with a wide variety of offensive techniques. If a threat manages to bypass a layer, it must deal with the defense mechanisms of the next layer.

An effective defense-in-depth strategy includes mechanisms at the purely technical level, as well as organizational or administrative measures, such as policies and procedures (risk analysis, user training, personal data management, etc.), access restrictions (least privilege, need-to-know, etc.), network security (network segmentation, firewalls, intrusion detection systems, VPNs, etc.), device protection (antivirus, application whitelisting, etc.), and application and data protection (patching, data backup, encryption, etc.) [9]. Figure 1 graphically illustrates an example of the sequential layering of defense-in-depth architecture.

We observe a broad and difficult-to-control dispersion in an operator's data processing, storage, and circulation. At the same time, the traditional network perimeter is no longer demarcated. The above is happening in an interconnected world becoming increasingly vulnerable to malicious activity as connectivity, device richness, distributed applications and services, and complexity in cloud and multicloud environments increase [4, 10, 11]. It is clear that such complexity dramatically increases the security requirements to protect the carrier's critical data from leakage, intentional alteration, or even disruption of availability. Various architecture models have been proposed for the effective defense against constantly evolving threats, which are found in the relevant research literature. But this novel research idea has never been offered in the relevant literature, and we think it has the potential to advance the state of the art in cyber security significantly.

The rest of this paper is structured as follows: Section 2 presents the relevant research studies. Section 3 is allocated to the presentation of the proposed system. Section 4 presents the protocol of the agreement, and finally, section 5 concludes the research.

2. Relevant Research Studies

The literature on the utilization of intelligent agents keeps expanding and covers not only the security aspect of research but also the safety or other perspectives.

Kasereka et al. [12] suggested in 2018 a smart agent-based model to model and simulate the removal of individuals from a burning building. Their concept has been founded on four criteria that allow for her realistic evaluation. In a simulated case study conducted in a building with the general layout of a supermarket, it was determined that the presence of multiple individuals to be removed, the consideration of fire propagation speed, and other aspects significantly impacted the model. This concept is sufficiently broad to be applied in multiple kinds of business buildings without significant modification. We seek to integrate these perspectives into the framework by incorporating a fuzzy approach into the system.

Kotenko et al. [13] presented a strategy for implementing intelligent agents for internet and vulnerability risk assessments in cyber-physical systems. The proposed method has a much smaller sliding window size than the sliding window technique with the same accuracy of assessing traffic characteristics, runs in real-time, and uses fuzzy logical inference to regulate parameters. The experimental evaluation supports the method's fast speed and appropriate precision for analyzing network data. Simultaneously with time, it offers evaluation accuracy equivalent to that of established algorithms. Methods of dynamic supervision of intelligent agents in cyber-physical security systems are the subject of more study.

Kushal et al. [14] developed a two-pronged technique to minimize the consequences of an unusual false data injection attempt, in which an attacker uses batteries to actively lower load curtailment to introduce updates to the central control system. An intelligent agent system examines directives from the primary energy administration system. A bilevel technique is constructed to describe the relationship between the cell and the hacked shipboard power system to discover symptoms of fraudulent data. They developed a heuristic defensive parameter to enhance the detection of tainted instructions. A danger assessment model is used to assess the advantages of the proposed strategy. The findings of the case studies demonstrate that a mixture of an autonomous battery and a heuristic strategy helps reduce the impacts of a cyberattack.

Manbachi and Ordonez [15] suggested an advanced agent-based method for the power management of AC-DC microgrids on isolated islands. This strategy supplied islanded ac-dc microgrids with three major operations interacting at each functioning time interval to improve system performance, efficiency, and dependability. Between the agents, bidirectional communication enabled data gathering and command flow control. They employed an innovative multiobjective particle optimization engine to successfully address each agent's issue for the goal of optimization. A microgrid with various ac-dc producing assets and loads was analyzed to evaluate the accuracy and practical efficiency of the proposed solution.

Biregani and Fotohi [16] presented a countermeasure against malicious UAV assaults. In the first stage, numerous criteria and principles were implemented to identify malicious UAVs. In phase two, a mobile agent was employed to destroy malicious UAVs by alerting regular neighbor UAVs not to listen to the data produced by malicious UAVs. The conjunction of these two steps resulted in secure interactions between the UAVs, allowing packets to exchange data safely. The simulation results demonstrated that the suggested strategy is superior to previous approaches. To detect hostile UAVs in future work, they propose integrating two or more innovative and optimum algorithms, such as earthworm efficiency algorithm, moth search method, monarch butterfly optimum, and elephant herding utilization.

Alhayani et al. [17] investigated the efficacy of artificial intelligence solutions against cyber security threats. They mostly used quantitative research methods and collected primary data from IT sector personnel. Using confirmatory pattern evaluation, discriminant validity, fundamental model analysis, and hypothesis testing, they determined that

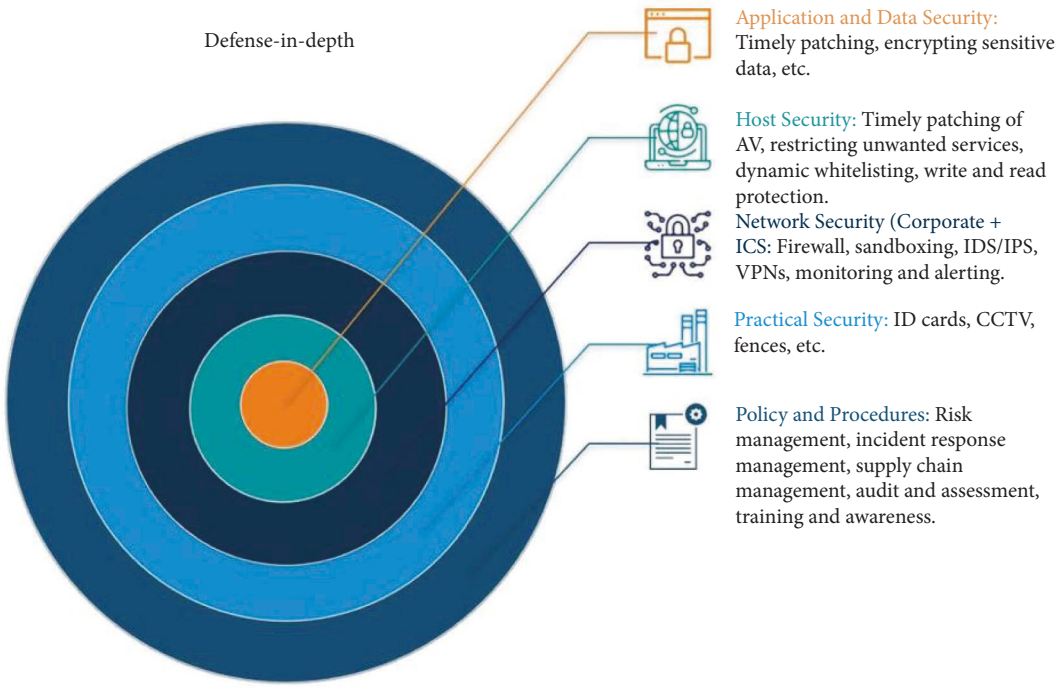

Figure 1: Defense in depth (https://modernciso.com/).

intelligence agents, and artificial neural networks strongly influenced synthetic intelligence approaches. The development of technology has expanded data storage, necessitating better data security.

3. Proposed System

Education agencies increasingly depend on information and communication technologies to carry out their day-to-day operations and mission [1, 2]. These technologies are subject to threats, which exploit known and unknown system vulnerabilities with possible severe effects on business operations, persons, infrastructures, and the safeguarding of sensitive personal data, due to the violation of the confidentiality, integrity, and availability of the information that these systems process, store, or transmit. Threats to IT include cyber-attacks, human errors, and structural failures [8, 18, 19].

For the above reasons, it is imperative for educational institutions, especially preschool education institutions, to realize their responsibility and establish a comprehensive organizational approach to risk management related to the operation and use of information systems.

A vital component of a risk management framework is risk assessment, which consists of the following series of actions [3]:

(1) The sources of threats related to the operator are identified (malicious groups, competitors, natural threats, errors, etc.)

(2) Actions/events (threat events) that could occur from the above sources (cyber-attacks, hardware failures, etc.) are identified

(3) The vulnerabilities of the organization that a source could exploit through specific actions/events are identified

(4) The probability that the identified sources will initiate specific actions and the probability of successful realization of the events are estimated

(5) The adverse effects (on the operations and systems of the entity, on persons, or other organizations) if the actions/events take place are assessed

(6) The risk to the operator's security is determined as a combination of the probability of the events and the adverse effects if the events occur

Based on the calculated risk, the operator should choose the corresponding protection measures to address the risks adequately. Also, the organization should develop a security policy [20, 21], which will define at a high level the security goals and the organization's approach to achieving them while referring to more specific thematic policies and procedures that will specify the implementation and application of the selected protection measures.

Risk management is always the starting point for a practical approach to cyber security. Thus, the agencies must establish an information security management system, which is as follows:

(1) Will be implemented by implementing technical and organizational security measures that will be based on risk management

(2) Will have the full financial and organizational support of the administrative leadership

(3) Will be inspected and renewed at regular intervals and

(4) Will shape a cyber security culture for all involved (from senior management to all involved staff)

An appropriate organizational structure with responsibility for the security of information systems should be created for an information security management system to be implemented effectively [22]. In this structure, it should

(1) Define the appropriate roles and responsibilities

(2) Be adequately staffed with persons possessing technical and legal expertise in cyber security issues and

(3) Allocate the required resources for the implementation of the goals set for cyber security

To automate the above functions and make them independent of human experience and knowledge, this work is proposed to develop a preschool cyber security management system based on intelligent agents [13]. Intelligent agents are modern artificial Intelligence systems that can be used selectively and combined with knowledge representation and problem-solving methods with advanced modern computing technologies [17]. Intelligent agents are computational systems that operate in a complex environment and perceive and act autonomously. In this way, they achieve a set of goals and perform tasks for which they are designed. Intelligent agents continuously perform three functions: they perceive the dynamic conditions of the environment, they act on the background to change it, and they reason to interpret what they perceive, solve problems, and draw conclusions to determine their actions [23].

The proposed system is a multiagent intelligent system that consists of a set of agents that act together to solve the given problem of cyber security management [24, 25]. The system aims to interconnect and operate already existing systems that are distributed, as well as to solve problems that are beyond the capabilities and knowledge of a single agent. Multiagent systems are a vital domain of distributed AI from a loosely considered view of agents, where relevant knowledge is distributed across discrete sources, such as existing experience in individual agent systems.

The proposed multiagent network is a set of agents with dynamic behavior interacting to achieve a common goal. The system in question includes any type of network or system consisting of spatially distributed autonomous devices that collectively record conditions and communicate with each other with wireless or wired devices, exchanging information to achieve an accurate estimate for the desired variable [15]. The system proposes to connect and control existing dispersed systems, as well as to solve problems that are beyond the knowledge and talents of a single person.

An essential element of networked systems, which separates them from the systems that have traditionally been considered in systems theory, is the existence of the network and its effect on the whole system's behavior. The geometry of the network imposes constraints on its behavior, as well as the interactions between agents, described by the graph theory translation of agents as nodes and interactions as branches of a graph representing the network. In such a graph, the existence of a branch indicates that the connected nodes interact with each other.

The agreement is one of the fundamental problems of multiagent coordination, in which a collection of agents must agree on a common state value [24, 26]. In this work, the dynamics of the agreement protocol for undirected static networks are studied to implement the multiagent network of cyber security management.

4. The Protocol of the Agreement

Let there be a multiagent network in which the agents must perform some measurement [27]. Although each measurement made by the individual agents will differ due to its location, it is necessary to reach an agreement on a specific value, which will be achieved by sharing the agents' information. For this purpose, the agents need some communication protocol that will act on the network and allow it to achieve the agreement. The agreement protocol includes n dynamic units, denoted as $1, 2, ..., n$ and are connected by a communication bus between them. Let the state of unit i be $x_i \in R$. Then, the protocol has the form [28]:

$$\dot{x}_i = -\sum_{j \in N(i)} \left(x_i(t) - x_j(t)\right), i = 1, \cdots, n, \tag{1}$$

where $N(i)$ is the set of neighbors of i in the network [29]. The overall network then has momentum

$$\dot{x}(t) = -L(G)x(t), \tag{2}$$

where the positive semidefinite matrix $L(G)$ is the Laplacian of the interaction network of agents G and $x(t) = (x_1(t), \ldots, x_n(t))^T \in \mathbb{R}^n$. The above equation will be referred to as agreement dynamics. With this protocol in action, node potentials are drawn toward the states of neighboring nodes [30]. The value they finally arrive at, i.e., the agreement state, is defined by the agreement set $A \subseteq \mathbb{R}^n$ which is the subset span {1} which is

$$A = \left\{x \in \mathbb{R}^n \,\middle|\, x_i = x_j, \forall i, j\right\}, \tag{3}$$

To clarify the mechanism by which dynamic agreement in an undirected graph drives network nodes to the agreement state, one should consider the eigenvalues of the Laplacian of a connected and undirected graph, which take the form [31]

$$0 = \lambda_0(G) \leq \lambda_1(G) \leq \ldots \leq \lambda_{n-1}(G), \tag{4}$$

where 1, the vector with all elements equal to unity, is the eigenvector corresponding to the zero eigenvalue $\lambda_0(G)$. Recall that the Laplacian is symmetric and $L(G)1 = 0$ for undirected G. Let $U = [u_0 u_1 \ldots u_{n-1}]$ be the matrix consisting of normalized and mutually orthogonal eigenvectors of $L(G)$ which are assigned to the ordered eigenvalues. In addition, let [32, 33]

$$\Lambda(G) = \mathrm{Diag}\left(\left[\lambda_0(G), \ldots, \lambda_{n-1}(G)\right]^T\right). \tag{5}$$

Applying the spectral theorem to the Laplacian, it yields

$$e^{-L(G)t} = e^{-\left(U\Lambda(G)U^T\right)t} = Ue^{-\Lambda(G)t}U^T = e^{-\lambda_0(G)t_0}u_0^T + e^{-\lambda_1(G)t_1}u_1u_1^T + \ldots + e^{-\lambda_{n-1}(G)t}u_{n-1}u_{n-1}^T. \tag{6}$$

Therefore, the solution of $\dot{x}(t) \in F[X](x(t))$, with initial value $x(0) = x_0$ is

$$x(t) = e^{-L(G)t}x_0, \tag{7}$$

which can be decomposed along each eigen-axis as [34]:

$$x(t) = e^{-\lambda_0(G)t}\left(u_0^Tx_0\right)u_0 + e^{-\lambda_1(G)t}\left(u_1^Tx_0\right)u_1 + \ldots + e^{-\lambda_n(G)t} \cdot \left(u_{n-1}^Tx_0\right)u_{n-1}. \tag{8}$$

The problem to be solved is to achieve agreement in a multiagent network with unknown disturbances for a stable network topology. Agents follow simple integrator dynamics. With blocked and continuous second-order derivatives, perturbations are considered blocked. The undirected network description graph is connected. The following solution employs discontinuous systems theory and distributed continuous control [28, 35].

The input of the individual agents is first filtered using the variables T and β as well as the sign of the error ξ. Then, using the filtered information, the final one is generated, which has an additional summation term using ξ. This control is fully distributed, that is, individual agents operate autonomously using information only from their neighbors. It is shown to asymptotically achieve agreement on a stable graph topology [36]. In practice, achieving convergence means that the input learns the perturbation and copes with it.

Specifically, the agent network topology is described using an undirected, connected graph where $G = (V, E)$, where$V = \{u_1, u_2, \ldots, u_n\}$ is the set of its nodes and $E \subseteq V \times V$ all its branches [37, 38]. The set of neighbors of agent i is $N(i) = \left\{u_j \in V \mid u_iu_j \in E\right\}$.

The dynamics of the agents are given by the equation [39]:

$$\dot{x}_i = u_i + d_i, i \in V, \tag{9}$$

where $\dot{x}_i$ are the one-dimensional state variables of the agents, and d_i are unknown blocked perturbations with continuous blocked derivatives up to the second degree and

$$u_i = -K_p\xi_i + u_{fi}, i \in V, \tag{10}$$

u_{fi} is the filtered input

$$T\dot{u}_{fi} + u_{fi} = -\beta\mathrm{sgn}(\xi_i), i \in V, \tag{11}$$

where sgn is the sign function and T, β, Kp are control gains. ξ_i contain the information of agent i about its neighbors and are given by the equation [40]

$$\xi_i = \sum_{j \in N(i)} \alpha_{ij}\left(x_i - x_j\right), i \in V, \tag{12}$$

The problem is to show that agreement is reached, i.e., that $x_i - x_j \longrightarrow 0, \forall i, j \in V$ for fixed graph topology [41].

For the existence of solutions of the system, a Lyapunov function will be used as follows [24, 31, 42, 43]:

$$V\left(x_{ag}, t\right) = \frac{1}{2}\left(\dot{x} + \frac{1}{T}x\right)^T\mathscr{L}\left(\dot{x} + \frac{1}{T}x\right) + \frac{\beta}{T}\sum_{i \in V}|\xi_i| - \sum_{i \in V}\left(\dot{d}_i + \frac{1}{T}d_i\right)\xi_i, \tag{13}$$

where $x_{ag} = (x, \dot{x}, d, \dot{d})$ the augmented state vector with $x, \dot{x}, d, \dot{d} \in \mathbb{R}^n$ and $\mathscr{L}$ the Laplacian of the network graph. All terms of the function are continuously differentiable and therefore normal, except for the term containing the absolute value of ξ_i. By the original hypothesis theorem, this term is also normal, so the Lyapunov function is also normal [44–46].

Using the eigenvalue decomposition of the Laplacian and since the Laplacian has a unique zero eigenvalue, we get [27, 45]

$$\mathscr{L} = \begin{bmatrix} U & \frac{1_n}{\sqrt{n}} \end{bmatrix}\begin{bmatrix} \sum & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} U^T \\ \frac{1_n^T}{\sqrt{n}} \end{bmatrix}, \tag{14}$$

where $U \in \mathbb{R}^{n \times (n-1)}$ with property $U^TU = \mathbb{I}_{(n-1)\times(n-1)}$ and $\Sigma \in \mathbb{R}^{(n-1)\times(n-1)}$ has in positions $(i, i), i = 1, \ldots, n-1$ the values $\sigma_i(L) = \sqrt{\lambda_i(L^TL)}$.

In the form presented, the matrix Σ has all nonzero eigenvalues of the Laplacian on its diagonal since the unique zero eigenvalue of the Laplacian has been removed. So, the Laplacian is written in the form [47, 48]

$$\mathscr{L} = U\Sigma U^T = U\Sigma\Sigma^{-1}\Sigma U^T = U\Sigma U^TU\Sigma^{-1}U^TU\Sigma U^T = \mathscr{L}U\Sigma^{-1}U^T\mathscr{L}. \tag{15}$$

Since the Laplacian has an eigenvector of 1, it also holds that

$$\mathscr{L} = \mathscr{L}\left(U\Sigma^{-1}U^T + r\frac{1^T}{N}\right)\mathscr{L}, \tag{16}$$

where r is a positive constant, which is chosen so that $\lambda_1(\mathscr{L}) < r < \lambda_{\max}(\mathscr{L})$. If set

$$\mathscr{L}_0 = \begin{bmatrix} U & \frac{1_n}{\sqrt{n}} \end{bmatrix}\begin{bmatrix} \sum^{-1} & 0 \\ 0 & r \end{bmatrix}\begin{bmatrix} U^T \\ \frac{1_n^T}{\sqrt{n}} \end{bmatrix} = U\sum^{-1}U^T + r\frac{11^T}{N}. \tag{17}$$

The request is satisfied.

Therefore, from the property $\xi = \mathscr{L}x$, the function V_0 can be written in the form [49, 50]

$$V_0 = \frac{1}{2}\left(\dot{\xi} + \frac{1}{T}\xi\right)^T\mathscr{L}_0\left(\dot{\xi} + \frac{1}{T}\xi\right). \tag{18}$$

So the function V_0 is [49, 51] continuous on its set of values as a quadratic function and so holds

$$\frac{d}{dt}\left(\dot{x}_i + \frac{1}{T}x_i\right) = \dot{d}_i + \frac{1}{T}d_i - K_p\left(\dot{\xi}_i + \frac{1}{T}\xi_i\right) + \frac{1}{T}\beta\mathrm{sgn}\ (\xi_i), \forall i \in V, \tag{19}$$

and so

$$\frac{dV_0}{dt} = -K_p \sum_{i\in V}\left(\dot{\xi}_i + \frac{1}{T}\xi_i\right)^2 + \sum_{i\in V}\left(\dot{d}_i + \frac{1}{T}d_i\right)\left(\dot{\xi}_i + \frac{1}{T}\xi_i\right) - \sum_{i\in V}\frac{\beta}{T}\operatorname{sgn}(\xi_i)\left(\dot{\xi}_i + \frac{1}{T}\xi_i\right). \tag{20}$$

Therefore V_0 is blocked and so

$$V_0 = \frac{1}{2}\left(\dot{x} + \frac{1}{T}x\right)^T \mathscr{L}\left(\dot{x} + \frac{1}{T}x\right) \geq \frac{\lambda_{\min}(\mathscr{L}_0)}{2}\left\|\dot{\xi} + \frac{1}{T}\xi\right\|^2. \tag{21}$$

So since V_0 is closed and locally Lipschitz, it is Lipschitz continuous on the set of values of x_{ag}.

So the Lyapunov function is [52, 53]

$$V\left(x_{ag}, t\right) = \frac{1}{2}\left(\dot{x} + \frac{1}{T}x\right)^T \mathscr{L}\left(\dot{x} + \frac{1}{T}x\right) + \frac{\beta}{T}\sum_{i\in V}|\xi_i| - \sum_{i\in V}\left(\dot{d}_i + 1/Td_i\right)\xi_i. \tag{22}$$

and is absolutely continuous, over the set of values of x_{ag}. Therefore, it is derivable almost everywhere, and its derivative is

$$\dot{V}\left(x_{ag}, t\right) = -K_p \sum_{i\in V}\left(\dot{\xi}_i + 1/T\xi_i\right)^2 - \beta/T^2 \cdot \sum_{i\in V}\operatorname{sgn}(\xi_i)\xi_i + 1/T^2\sum_{i\in V}\xi_i d_i - \sum_{i\in V}\xi_i\ddot{d}_i. \tag{23}$$

So, the system with a fixed network topology for connected and undirected graphs ensures that $\lim_{t\longrightarrow\infty}\xi(t) = 0$ using distributed continuous control for appropriate control gain β. Thus, it is true that [54]

$$W_1\left(\xi_{ag}\right) \leq V\left(x_{ag}, t\right) \leq W_2\left(\xi_{ag}\right), \tag{24}$$

where

$$W_1\left(\xi_{ag}\right) = \frac{1}{2}\lambda_{\min}(\mathscr{L}_0)\left\|\dot{\xi} + \frac{1}{T}\xi\right\|^2 + \sum_{i\in V}|\xi_i|\left(\frac{\beta}{T} + \max_{i\in V}\left|\dot{d}_i + \frac{1}{T}d_i\right|\right), \tag{25}$$

and

$$W_2\left(\xi_{ag}\right) = \frac{1}{2}\lambda_{\max}(\mathscr{L}_0)\left\|\dot{\xi} + \frac{1}{T}\xi\right\|^2 + \sum_{i\in V}|\xi_i|\left(\frac{\beta}{T} + \max_{i\in V}\left|\dot{d}_i + \frac{1}{T}d_i\right|\right), \tag{26}$$

W_1 and W_2 are positive definite and continuous, for $\xi_{ag} = (\xi, \dot{\xi})$ for suitable β which exceeds the term $\max|T\dot{d}_i + \ddot{d}_i|$. Moreover, it is true that [38, 43, 49]

$$\dot{V}\left(x_{ag}, t\right) \leq^{a.e.} -W\left(\xi_{ag}(t)\right). \tag{27}$$

where

$$W\left(\xi_{ag}\right) = K_p\sum_{i\in V}\left(\dot{\xi}_i + 1/T\xi_i\right)^2 + \sum_{i\in V}|\xi_i|\left(\beta/T^2 - \max_{i\in V}\left|d_i/T^2 - \ddot{d}_i\right|\right). \tag{28}$$

Eigenvalue decomposition of the Laplacian $\mathscr{L}$ of the network graph yields

$$\mathscr{L} = U\Sigma U^T, \tag{29}$$

and using the equation $\xi = \mathscr{L}x$ holds

$$U\Sigma^{-1}U^T\xi = UU^Tx = \left(\mathbb{I}_n - \frac{1_n 1_n^T}{n}\right)x = x - \frac{\sum_{i=1}^n x_i}{n}1_n, \tag{30}$$

and consequently

$$x = U\Sigma^{-1}U^T\xi + \frac{\sum_{i=1}^n x_i}{n}1_n. \tag{31}$$

Multiplying the above equality by $(e_i - e_j)^T$ results

$$x_i - x_j = \left(e_i - e_j\right)^T U\Sigma^{-1}U^T\xi, \tag{32}$$

and taking the limit at $t \longrightarrow \infty$ implies that $\lim_{t\longrightarrow\infty}(x_i(t) - x_j(t)) = 0$ for every $i, j \in V$.

So, the collective price of the agents converges to the average price of their situations (average consensus).

Unfortunately, no other comparable model exists to serve as a benchmark. As a result, to prevent prejudice or false perceptions, we report the performance of the suggested model without comparing it to any other potential models.

5. Conclusion

In this paper, we suggested a preschool cyber security management system based on intelligent agents. We used cutting edge, intelligent techniques, and it aims to improve the ability of preschools to resist modern threats adequately, respond to cyber-attack incidents with the least possible impact, and protect their critical systems, services offered, and the personal data they hold and process.

The suggested system is a multiagent intelligent system comprising a group of agents that collaborate to solve the cyber security management challenge. The system intends to link and control distributed systems that currently exist, as well as to solve issues that are beyond the knowledge and skills of a single agent. Multiagent systems are a crucial area of distributed AI, where information is dispersed among distinct sources, such as previous experience in individual agent systems. The suggested multiagent network consists of a collection of agents with dynamic behavior collaborating to accomplish a common objective. The system in issue encompasses any network or system composed of geographically dispersed autonomous devices that collectively record circumstances and interact with each other through wireless or wired devices, exchanging data to provide an accurate estimate of the desired variable.

One of the core issues of multiagent coordination is the agreement, in which a group of agents must agree on a shared state value. The dynamics of the agreement protocol for undirected static networks are investigated in this work to implement the multiagent network of cyber security management.

Intelligent applications, such as the ones presented here, offer network defenders command over their environment, enabling them to turn the tables on even the most sophisticated attackers and stop them before they damage them. The need for interdisciplinary knowledge and deep experience in foundational cyber science skills such as understanding crypto analysis methods, building out

security pipelines, and statistics, as well as computer science fundamentals and software engineering skills such as understanding computer architecture, proficiency with programming languages, and the ability to program software solutions is a significant disadvantage of multiagent applications.

Further research will be related to mechanisms of distributed control of intelligent agents in secure communications for other sector specific implementations. Also, I will be studying the multiagent reinforcement learning method that focuses on studying the behaviour of multiple learning agents that coexist in a shared environment.

Data Availability

The data used in this study are available from the author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This study was supported by the Key Project of Comprehensive Education Reform in Henan Province and reform of quality evaluation of kindergarten care and education in Henan province (No. 2022CG0265).

References

[1] L. Tetzlaff, F. Schmiedek, and G. Brod, "Developing personalized education: a dynamic framework," *Educational Psychology Review*, vol. 33, no. 3, pp. 863–882, 2020.

[2] A. Klašnja-Milićević and M. Ivanović, "E-Learning personalization systems and sustainable education," *Sustainability*, vol. 13, no. 12, p. 6713, Jan. 2021.

[3] Z. Amin, "A practical road map for assessing cyber risk," *Journal of Risk Research*, vol. 22, no. 1, pp. 32–43, Jan. 2019.

[4] A. S. Al-Ahmad and H. Kahtan, "Cloud computing review: features and issues," in *Proceedings of the 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, pp. 1–5, Shah Alam, Malaysia, July 2018.

[5] Z. Lassoued, M. Alhendawi, and R. Bashitialshaaer, "An exploratory study of the obstacles for achieving quality in distance learning during the COVID-19 pandemic," *Education Sciences*, vol. 10, no. 9, p. 232, Sep. 2020.

[6] D. Turnbull, R. Chugh, and J. Luck, "Transitioning to E-learning during the COVID-19 pandemic: how have higher education institutions responded to the challenge?" *Education and Information Technologies*, vol. 26, no. 5, pp. 6401–6419, 2021.

[7] H. Alamleh and A. A. S. AlQahtani, "Analysis of the design requirements for remote internet-based E-voting systems," in *Proceedings of the 2021 IEEE World AI IoT Congress (AIIoT)*, pp. 0386–0390, Seattle, WA, USA, May 2021.

[8] P. Ganguly, M. Nasipuri, and S. Dutta, "Challenges of the existing security measures deployed in the smart grid framework," in *Proceedings of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, pp. 1–5, Oshawa, ON, Canada, August 2019.

[9] M. N. Dazahra, F. Elmariami, A. Belfqih, and J. Boukherouaa, "A defense-in-depth cybersecurity for smart substations," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 6, p. 4423, 2018.

[10] M. T. Amron, R. Ibrahim, and S. Chuprat, "A review on cloud computing acceptance factors," *Procedia Computer Science*, vol. 124, pp. 639–646, Jan. 2017.

[11] S. Srivastava, A. Bisht, and N. Narayan, "Safety and security in smart cities using artificial intelligence — a review," in *Proceedings of the 2017 7th International Conference on Cloud Computing, Data Science Engineering - Confluence*, pp. 130–133, Noida, India, January 2017.

[12] S. Kasereka, N. Kasoro, K. Kyamakya, E.-F. Doungmo Goufo, A. P. Chokki, and M. V. Yengo, "Agent-Based Modelling and Simulation for evacuation of people from a building in case of fire," *Procedia Computer Science*, vol. 130, pp. 10–17, 2018.

[13] I. Kotenko, S. Ageev, and I. Saenko, "Implementation of intelligent agents for network traffic and security risk analysis in cyber-physical systems," in *Proceedings of the 11th International Conference on Security of Information and Networks*, pp. 1–4, Cardiff, UK, September 2018.

[14] T. R. B. Kushal, K. Lai, and M. S. Illindala, "Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4741–4750, 2019.

[15] M. Manbachi and M. Ordonez, "Intelligent agent-based energy management system for islanded AC–DC microgrids," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4603–4614, 2020.

[16] M. F. Biregani and R. Fotohi, "Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles," *The Journal of Supercomputing*, vol. 77, no. 5, pp. 5076–5103, May 2021.

[17] B. Alhayani, H. Jasim Mohammed, I. Zeghaiton Chaloob, and J. Saleh Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry," *Materials Today Proceedings*, Article ID S2214785321016722, 2021.

[18] S. Alromaihi, W. Elmedany, and C. Balakrishna, "Cyber security challenges of deploying IoT in smart cities for healthcare applications," in *Proceedings of the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 140–145, Barcelona, Spain, December 2018.

[19] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan, and A. Alsayat, "Cyber Security Issues and Challenges for Smart Cities: A Survey," in *Proceedings of the 2019 13th International Conference On Mathematics, Actuarial Science, Computer Science And Statistics (MACS)*, pp. 1–7, Karachi, Pakistan, December 2019.

[20] L. Schaefer and D. Millner, "Flight delay propagation analysis with the detailed policy assessment tool," in *Proceedings of the 2001 IEEE International Conference on Systems, Man and Cybernetics. e-Systems and e-Man for Cybernetics in Cyberspace (Cat.No.01CH37236)*, vol. 2, pp. 1299–1303, Tucson, AZ, USA, Jul. 2001.

[21] R. Telang, "Policy framework for data breaches," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 77–79, 2015.

[22] Z. Tang, "Analysis of information security problems and countermeasures in big data management of colleges and universities under smart campus environment," in *Proceedings of the 2021 2nd International Conference on Information Science and Education (ICISE-IE)*, pp. 912–915, Chongqing, China, November 2021.

[23] M. Dhingra, M. Jain, and R. S. Jadon, "Role of artificial intelligence in enterprise information security: a review," in *Proceedings of the 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 188–191, Waknaghat, India, December 2016.

[24] D. Zhang and X. Wang, "Opinion dynamics based on game theory in multi-agent network," in *Proceedings of the 2021 3rd International Symposium on Robotics Intelligent Manufacturing Technology (ISRIMT)*, pp. 282–286, Chongqing, China, September 2021.

[25] J. C. Bansal, H. Sharma, K. Deep, K. N. Das, and A. Nagar, "Special issue on swarm intelligence and its applications to engineering," *Int. J. Syst. Assur. Eng. Manag.*, vol. 9, no. 4, pp. 739-740, 2018.

[26] Y.-L. Wang, Z.-Z. Li, and H.-P. Zhu, "Mobile-agent-based distributed and incremental techniques for association rules," in *Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.03EX693)*, vol. 1, pp. 266–271, Xi'an, China, November 2003.

[27] Z. Cheng, T. Wang, and Y. Xin, "High-order distributed consensus in multi-agent networks," in *Proceedings of the 2018 IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS)*, pp. 965–969, Enshi, China, May 2018.

[28] S. T. Arzo, R. Bassoli, F. Granelli, and F. H. P. Fitzek, "Multi-agent based autonomic network management architecture," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3595–3618, 2021.

[29] H. Ye, H. Lv, and Q. Sun, "An improved clustering algorithm based on density and shared nearest neighbor," in *Proceedings of the 2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, pp. 37–40, Chongqing, China, May 2016.

[30] X. Wang, M. Dai, Y. Chen, and Y. Zong, "Laplacian spectra for a family of treelike networks," in *Proceedings of the IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, pp. 5855–5858, Beijing, China, July 2017.

[31] S. Feng, L. Wang, S. Sun, and C. Xia, "Effect of network structure to the convergence rate of agents in multi-agent systems," in *Proceedings of the 2017 36th Chinese Control Conference (CCC)*, pp. 1408–1412, Dalian, China, July 2017.

[32] L. Zhiwei, Z. Chonghu, S. Jie, L. Juan, and Z. Songhao, "A multi-agent task allocation strategy based on artificial immune system," in *Proceedings of the 2013 25th Chinese Control and Decision Conference (CCDC)*, pp. 3486–3491, Guiyang, China, Feb 2013.

[33] S. Ouiazzane, M. Addou, and F. Barramou, "A multi-agent model for network intrusion detection," in *Proceedings of the 2019 1st International Conference on Smart Systems and Data Science (ICSSD)*, pp. 1–5, Rabat, Morocco, October 2019.

[34] S. M. Amrr and M. Nabi, "Attitude regulation of spacecraft using large angle eigen-axis rotations," in *Proceedings of the 2020 International Conference on Decision Aid Sciences and Application (DASA)*, pp. 783–787, Bahrain, November 2020.

[35] C. Ma, W. Wu, H. Fu, and C. Wang, "Distributed leader-follower consensus of multi-agent systems with unreliable networks," in *Proceedings of the 2020 7th International Conference on Information, Cybernetics, and Computational Social Systems (ICCSS)*, pp. 581–584, Guangzhou, China, November 2020.

[36] C. Ma and Y. Gao, "Study on mesh segmentation of topology optimization results using Reeb graph," in *Proceedings of the 2021 International Conference on Artificial Intelligence and Electromechanical Automation (AIEA)*, pp. 277–280, Guangzhou, China, Feb 2021.

[37] M. Mohammadian, "Network security risk assessment using intelligent agents," in *Proceedings of the 2018 International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR)*, pp. 1–6, Putrajaya, Malaysia, December 2018.

[38] H. Liu, R. Gu, Z. Li, and Y. Ji, "Multi-agent federated reinforcement learning for privacy-enhanced service provision in multi-domain optical network," in *Proceedings of the 2021 Asia Communications and Photonics Conference (ACP)*, pp. 1–3, Shanghai, China, July 2021.

[39] N. A. Musa, M. Z. M. Yusoff, R. Ismail, and Y. Yusoff, "Issues and challenges of forensics analysis of agents' behavior in multi-agent systems: a critical review," in *Proceedings of the 2015 International Symposium on Agents, Multi-Agent Systems and Robotics (ISAMSR)*, pp. 122–125, Putrajaya, Malaysia, December 2015.

[40] C. C. Aggarwal, "Neighborhood-based collaborative filtering," in *Recommender Systems: The Textbook*, C. C. Aggarwal, Ed., Springer International Publishing, New York, NY, USA, 2016.

[41] V. Alieksieiev and B. Andrii, "Information analysis and knowledge gain within graph data model," in *Proceedings of the 2019 IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT)*, vol. 3, pp. 268–271, Lviv, Ukraine, September 2019.

[42] H. K. Dambanemuya and E. -Á. Horvát, "Network-aware multi-agent simulations of herder-farmer conflicts," in *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 721-722, Vancouver, BC, Canada, December 2019.

[43] S. E. Benton, E. Rogers, and D. H. Owens, "Lyapunov stability theory for linear repetitive processes — the 2D equation approach," in *Proceedings of the 1999 European Control Conference (ECC)*, pp. 4768–4773, Karlsruhe, Germany, December 1999.

[44] S. Chen, M. Fazlyab, M. Morari, G. J. Pappas, and V. M. Preciado, "Learning Lyapunov Functions for Hybrid Systems," in *Proceedings of the 2021 55th Annual Conference On Information Sciences And Systems (CISS)*, p. 1, Nashville, Tennessee, March 2021.

[45] Y. Ji, J. Huang, and J. Hu, "Optimal Lyapunov-based states transfer for superconducting qubits," in *Proceedings of the 2016 IEEE International Conference on Information and Automation (ICIA)*, pp. 849–852, Ningbo, China, December 2016.

[46] N. Wang, H. Liu, and W. Chen, "Lyapunov-based excitation control for the synchronous generator unit," in *Proceedings of the 32nd Chinese Control Conference*, pp. 899–903, Xi'an, China, July 2013.

[47] S. Gao, I. W.-H. Tsang, and L.-T. Chia, "Laplacian sparse coding, hypergraph laplacian sparse coding, and applications," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 1, pp. 92–104, 2013.

[48] Y. Liu and S. Liao, "An error bound for eigenvalues of graph laplacian with bounded kernel function," in *Proceedings of the 2011 Seventh International Conference on Computational Intelligence and Security*, pp. 436–440, Sanya, China, September 2011.

[49] G. Alessandrini, M. V. de Hoop, R. Gaburro, and E. Sincich, "Lipschitz stability for a piecewise linear Schrödinger potential from local Cauchy data," *Asymptotic Analysis*, vol. 108, no. 3, pp. 115–149, 2018.

[50] V. Sokolov, "Adaptive suboptimal tracking under bounded lipshitz uncertainty and disturbance in discrete-time minimum-phase plant," in *Proceedings of the 2016 International Conference Stability and Oscillations of Nonlinear Control*

Systems (Pyatnitskiy's Conference), pp. 1–4, Moscow, Russia, June 2016.

[51] C. Freer, B. r. Kjos-Hanssen, A. Nies, and F. Stephan, "Algorithmic aspects of Lipschitz functions," *Computability*, vol. 3, no. 1, pp. 45–61, Jan. 2014.

[52] L. Hu and L. Wang, "H Fuzzy filtering design via membership function dependent Lyapunov function," in *Proceedings of the 2016 3rd International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS)*, pp. 348–353, Jinzhou, China, December 2016.

[53] W. Junqiang and X. Meiqing, "Stochastic stability analysis of the power systems based on Lyapunov function," in *Proceedings of the 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1–9, Beijing, China, July 2018.

[54] Y. Gao and L. Jia, "Stability in measure for uncertain delay differential equations based on new Lipschitz conditions," *Journal of Intelligent and Fuzzy Systems*, vol. 41, no. 2, p. 2997, 2021.