Article

Application of the Learning Automaton Model for Ensuring Cyber Resiliency

Maxim Kalinin *, Tigran Ovasapyan and Maria Poltavtseva

Institute of Cybersecurity, Peter the Great St.Petersburg Polytechnic University, 195251 St. Petersburg, Russia
* Correspondence: max@ibks.spbstu.ru

Abstract: This work addresses the functional approach to ensuring cyber resiliency as a kind of adaptive security management. For this purpose, we propose a learning automaton model capable of self-learning and adapting to changes while interacting with the external environment. Each node in the under-controlled system has a set of probable actions with respect to neighboring nodes. The same actions are represented in the graph of the learning automaton, but the probabilities of actions in the graph model are permanently updated based on the received reinforcement signals. Due to the adaptive reconfiguration of the nodes, the system is able to counteract the cyberattacks, preserving resiliency. The experimental study results for the emulated wireless sensor network (WSN) are presented and discussed. The packets loss rate stays below 20% when the number of malicious nodes is 20% of the total number of nodes, while the common system loses more than 70% of packets. The network uptime with the proposed solution is 30% longer; the legitimate nodes detect malicious nodes and rebuild their interaction with them, thereby saving their energy. The proposed mechanism allows ensuring the security and functional sustainability of the protected system regardless of its complexity and mission.

Keywords: adaptability; cyber resiliency; functional approach; learning automaton; security

1. Introduction

Currently, there is a trend toward the use of devices capable of interacting with the external environment and exchanging information with each other via an internal network or the Internet. The number of such devices is constantly increasing, which indicates the transition to the next technological concept of a reconfigurable system-of-systems. A significant part of such a system are unattended computing nodes moving and distributed in space. Combining such devices into a self-organizing networks for collecting, processing and transmitting information, e.g., a wireless sensor network (WSN), the internet of things (IoT), vehicle ad hoc networks (VANET), flying ad hoc networks (FANET), and cyber–physical systems (CPS), expands the possibilities for presenting information about manufacturing processes, the environment, the automation, as well as improving ‘human-to-human’ or ‘human-to-machine’ interaction.

Ensuring security plays a crucial role in the use of the connected systems since they are used in critical areas that are directly related to the economy and life of society. This is evidenced by a number of security incidents targeted at the IoT-based formations [1] as well as regulatory acts [2] related to the security of critical infrastructure around the world. Many research efforts are already underway to develop security technologies concerning the security of the reconfigurable systems [3,4]. However, a crucial component of making ubiquitous security a reality is the ability to shift the balance that currently favors the attackers, in part by using cyber resiliency techniques.

Cyber resiliency is the ability of a system to anticipate, withstand, recover from, and adapt to adverse conditions and threats [3], and today it does matter for the critical infrastructure. From an engineering perspective, cyber resiliency is an aspect of emergent
quality—the trustworthiness of the system [6–8]. A cyber-resilient system is one that has security safeguards built into it as a fundamental element of its design and that displays a high level of withstanding cyber threats, security faults, and continues operating in a degraded or debilitated system to carry out the system’s mission-essential functions.

Today, cyber resiliency can be reached using trust-based and IDS-aided techniques that, in most cases, just allow us to identify the security issues in the systems. That approaches are eliminated by isolating the malicious node from the system or informing us how to counteract the cyber threat. Within our research, the objective of work is to observe the security resiliency technologies, discuss a functional adaptability method based on a learning automaton (LA) model and examine it. The LA model is capable of self-learning and adapting to changes while interacting with the external environment. Each node in the under-controlled system has a set of probable actions corresponding to neighboring nodes. The same actions are represented in the graph of the LA, but the probabilities of actions in the graph model are permanently updated based on the received reinforcement signals. Due to adaptive reconfiguration, the system is able to counteract the developing attacks. The preservation of system operability is ensured by the LA, which changes the node’s behavior with respect to malicious nodes, following the analysis of input signals. In this sense, since the benefit of the proposed method of defensive resiliency is an ability to provide an asymmetric advantage to defenders in order to maximize the effect applied toward winning cyber conflict between adversaries and defenders, the proposed approach is a part of the symmetry/asymmetry aspect meaningful in the more stable and longer functioning of the protected system.

The following sections of the paper present the functional approach to cyber resiliency based on adaptive control with a learning automaton (LA) model (Section 2), the experimental study of the proposed control mechanism of the LA (Section 3), the final discussion (Section 4), and conclusion (Section 5).

2. Materials and Methods

2.1. Approaches to Ensuring Cyber Resiliency

The response to security impacts should be comprehensive and of a purposeful nature to ensure preservation of the system in functional properties, and thus appeal to methods and means to hold the system’s dynamic development or reduce the degree of influence of security impacts on different system levels: components, subsystems, missions, and business functions. On every level, there are required approaches to ensuring resiliency. Such approaches can be based on principles following the biological analogy [8]. This similarity to biological systems can be applied to transfer the experience of millions of years of natural evolution to the safety of digital systems.

A digital system, as well as its biological prototype, can be represented as a complex topological structure forming a set of connected elementary units (nodes) through which complex functional or informational processes take place. Any threats or intrusions of the outer environment on such a system can cause the generation of additional signals and changes in node-to-node communications, system topology of the nodes, and reactions (functions) at each level of the system representation.

Summarizing the resiliency-providing principles in biological systems and transferring them to digital systems result in three main approaches to ensuring cyber resiliency (Figure 1).

- **Homeostatic approach** that preserves the system state under external influences [9]. Consideration of a digital system with a network structure as a homeostatic system implies the formation of some set of attributes, which should be satisfied by the system, forming a view of its state. In the case that, as a result of operation, one or more attributes cease to meet the required criteria, corrections are applied to the system [10–13];

- **Functional approach**, which is based on the theory of functional systems [7,14]. The main principle of the functional approach is the preservation of the system function...
under external influences. In its framework, a digital system is considered a system with one or more functions, and its performance under destructive influences is a priority. In this case, the goal of management is the preservation of this function or their set with the help of various methods and tools [15,16];

- **Ahead reflection (anticipation)** that prevents a destructive impact and its consequences before it is committed [17,18]. The essence of the ahead reflection is to predict possible security impacts and take measures to neutralize them by creating resource reserves, applying an anticipatory effect [19,20].

![Diagram of Approaches to Cyber Resiliency](image)

**Figure 1.** Theoretical approaches to ensuring cyber resiliency.

Each approach to cyber resiliency follows one of the dominant principles:

- **Expenses reducing**: choosing the way of reaction (out of acceptable ones) to a destructive impact (e.g., cyberattack) requires the minimization of costs—amount of resources or energy—for its implementation. For example, the number of operations on the graph of the system should be minimized to preserve the functional route or homeostatic equilibrium.

- **Maximization of the system’s freedom degrees**: This is to maximize information exchange with minimum entropy in the system. For resiliency, it causes maximization of communication links and interactions between the connected nodes of the system.

- **Cyber resistance preservation**: When responding to an external impact (e.g., cyberattack), the system has to ensure the preservation (if possible) of a sufficient stock of components for subsequent compensatory and anticipatory actions. For some systems, this principle can be formulated as the maintaining the margins of stability. The quantitative assessment of resiliency depends on the type of the system and approach to ensuring the system resiliency. For example, it can be expressed as a risk score or a number of reserved functional routes and a number of redundant nodes.

The dominance of one or another principle agrees with one of the above listed approaches and the goal of the system protection. Each approach has its own characteristics and key differences, respectively, to the point of view on cyber resiliency (Table 1).
Table 1. Comparative analysis of approaches to ensuring cyber resiliency.

| Characteristics          | Homeostasis                      | Functional Approach                      | Ahead Reflection                        |
|--------------------------|----------------------------------|------------------------------------------|------------------------------------------|
| Dominant principle       | Expenses reducing                | Maximum degrees of freedom               | Preservation of cyber resistance         |
| Feedback type            | Negative                         | Positive, negative                       | Positive                                 |
| Target                   | Homeostatic equilibrium          | Functionality preserving                 | Maintaining the local stability          |
| Mechanisms of implementation | Structural, parametric, and architectural homeostasis | Self-improvement, self-regulation         | Immunization, preventing threats to the system units |
| Technology               | Conflict analysis and finding an algorithm for its resolution at the level of object transformation | State-based control; generation and analysis of available states and transitions between them based on the system model | Adjusting communications; isolating nodes. Maintaining the functionally equivalent modules and redundancy |
| Methods and tools        | Heuristics, control of stability indicators; graph analysis; communication graph transformation | Intelligent control; methods for generating equivalent structures; self-regulation of system graph | Communication propagation and control modeling; redundant sets based on an intruder model |

In this work, we are inspired by the functional approach as a kind of adaptive control, the most promising technique for resiliency countering either natural (for bio-systems) or digital (for computer and cyber–physical systems) threats. Adaptive control solutions mainly allow us to identify the security threat and, as a counteraction, remove the malicious node from the system topology. At the same time, the functional approach is mainly aimed at providing protection against targeted attacks by malicious nodes without taking into account the occurrence of natural threats. Consequently, existing protection methods are not sufficiently effective for system nodes operating for a long period of time without maintenance on a non-monitored perimeter. The goal of our work is to add adaptive behavior whereby a node modifies the rules of interaction with its neighbors. The preservation of infrastructure operability is proposed to be ensured by changing the behavior of a node relative to a malicious node based on intelligent analysis of input signals.

The maintenance of functional stability has been proposed to be achieved by the application of a computing model of a learning automaton. The learning automaton (LA) is capable of self-learning while interacting with the external environment and adapting to changes. Each node in the under-controlled system has a set of probable actions with respect to neighboring nodes. Similar actions are represented in the LA, but the probabilities of actions in the LA are permanently updated based on the received reinforcement signals. The reinforcement signal is generated based on the received performance of neighboring nodes during network operation. In this model, each node changes the rules of interaction with its neighbors. Through the use of adaptive behavior, nodes are able to counteract both natural security threats and targeted attacks.
2.2. The Learning Automaton Model

Originally, the LA was specified by M. Tsetlin [21], and it is an optimization model required to determine an optimal action out of a set of actions. In this regard, learning for the automaton is effective if and only if the system in which the automaton works has a high level of fuzziness. In systems with a low level of fuzziness, the automaton learning may not be a correct measure for selection [22]. Therefore, this model is well suited for the application of security adaptability. For digital systems, the necessary characteristics of the LA are defined as follows:

- Type of automaton: stochastic.
- Structure: variable.
- Evaluation model: P-model (only two possible options: favorable or unfavorable).
- Learning model: combined, i.e., reward–\(\epsilon\)-penalty \((L_{\epsilon P}, a << b)\) and reward–inaction \((L_{RI}, b = 0)\), where \(a\)—reward feature, \(b\)—penalty parameter [23].

The probability vector is updated using the following systems of Equations (1) and (2):

\[
P_j(n + 1) = \begin{cases} 
P_j(n) + a(1 - P_j(n)), & j = i \\ P_j(n) - aP_j(n), & \forall j, j \neq i \end{cases}, \quad (1)
\]

\[
P_j(n + 1) = \begin{cases} 
(1 - b)P_j(n), & j = i \\
\frac{b}{1-1} + (1 - b)P_j(n), & \forall j, j \neq i \end{cases}, \quad (2)
\]

where \(P_j(n)\) is a probability of action at a point in time \(n\); \(a\) and \(b\) are coefficients, the values of which depend on the chosen learning model. The LA uses the learning models \(L_{\epsilon P}\) for actions \(\alpha_1\) and \(\alpha_2\), and \(L_{RI}\) for action \(\alpha_3\). Equation (1) is utilized in the case of winning, and Equation (2) in the case of losing the automaton.

Taking into account the given parameters, a graph representation for the LA is depicted in Figure 2. It marks the graph’s vertices and arcs by the labels: PSD/OSD—receiving/sending service data, PID/OID—receiving/sending information data, VID/VSD—verification of information/service data, OD—data processing, RST—reset of the connection, and \(p_{\alpha_m}^n\)—probability of the action. This graph is general and not bound to the routing protocol used in the concrete system. If a particular routing protocol has to be referred to, states of the PSD, OSD, PID and OID vertices should be specified depending on the specifics of the corresponding rules of the protocol.

![Figure 2. Graph for the learning automaton.](image-url)
Data transfer between the nodes is divided in information flow and service flow. Information messages include data required for the system to perform its functional task. For example, the wireless sensor network (WSN) is utilized for monitoring the surrounding manufacturing conditions, and, in this case, the information messages can be data about the pressure and temperature in the system’s surroundings. Service data messages contain information required for the routing protocol, and convey information about the state of the system’s communications and nodes (e.g., performance indicators, and behavior indicators).

The node function is based on the method of adaptive control of the node interaction rules. The system cyber resiliency is ensured by changing the probabilities of transitions between the states on the graph model. The transition on the graph occurs depending on the value of the complex indicator $Q$, which is calculated following the formula (3):

$$Q^{ij} = \frac{\sum_{k=1}^{m} g_k (1 - B^{ij}) B^{ij}_k}{\sum_{k=1}^{m} g_k (1 - B^{ij})}$$ (3)

where $g_k$—obsolescence rate ($g_k = \phi^{m-k}$, $\phi \in [0, 1]$), $m$—window size, and $B^{ij}_k$—complex behavioral indicator.

The complex behavioral indicator describes the node’s performance of the target function assigned to it. This indicator is calculated according to Formula (4) and consists of the direct behavioral indicator calculated by this node and the indirect behavioral indicator obtained from other nodes.

$$B^{ij} = C^{ij} \ast DI^{ij} + (1 - C^{ij}) \ast II^{ij}$$ (4)

where $DI^{ij}$—direct behavioral indicator, $II^{ij}$—indirect behavioral indicator, and $C^{ij}$—confidence coefficient.

The direct behavioral indicator is calculated by the node itself by analyzing the behavior of its neighbors. For example, the node monitors the fact that a neighboring node has transmitted a packet to it (verification of the correct re-transmission of the packet through the network).

The following indicators are distinguished, the use of which allows us to protect the system against cyber threats:

- **Packet re-transmission**: After transmitting a packet to a neighbor node, the sending node switches to a monitoring mode to track the re-transmission of its packet further through the network. It is used to counteract the nodes that re-transmit packets selectively or not at all.
- **Packet integrity**: In addition to checking for re-transmissions, the sending node also checks the checksum of the packet sent by its neighbor through the network.
- **Node data generation intensity**: The indicator is defined as the number of packets received from a node for a certain period of time and is designed to protect nodes from attacks of energy depletion and channel clogging.
- **Volume of sent data**: Similar to the previous one. Accounting the volume of data sent by neighboring nodes helps protect against resource exhaustion attacks.

The values of the indicators package re-transmission and package integrity are calculated by Formula (5) and represent the ratio of successful interaction events to all events:

$$I_m^{ij} = \frac{S_m^{ij}}{S_m^{ij} + F_m^{ij}}$$ (5)

where $S_m^{ij}$—the number of successful events between nodes $i$ and $j$ in the context of the corresponding indicator, and $F_m^{ij}$—the number of unsuccessful (failure) events.
The indicators are evaluated based on the thresholds. The thresholds depend on the application area of the system and type of the transmitted data.

To obtain a complex indicator of behavior $DI_{i,j}$, the value of each indicator is summed with the weight according to the formula (6). The weight of the indicator depends on the type and use case of the system.

$$DI_{i,j} = \sum_{m=1}^{N} (W_m \times I_{i,j}^m),$$  

(6)

where $N$—number of behavioral indicators, $W_m$—indicator’s weight, and $I_{i,j}^m$—the value of the indicator for a particular aspect of behavior relative to the corresponding node $j$.

The indirect behavioral indicator is calculated by Formula (7) on the basis of direct behavioral indicators, obtained from all neighbors relative to the node for which this indicator is calculated:

$$II_{i,j} = \frac{\sum_{l=1}^{n} (DI_{i,k_l} \times DI_{k,l,j})}{\sum_{l=1}^{n} DI_{i,k_l}},$$  

(7)

where $DI_{i,k_l}$—the value of the direct indicator relative to the node $k$, $DI_{k,l,j}$—the value of the indicator of node $k$ relative to node $j$, and $n$ is the number of nodes that provided their value. This indicator is introduced to compensate for insufficient data to calculate the correct value of the direct indicator. Over time, with an increase in the number of interactions, the weight in the value of the direct indicator becomes greater than the weight of the indirect indicator.

Let us take the sample of how this algorithm works in a single round of network node interactions. There are three nodes: $i, j, k$. The node $i$ needs to transmit data through the network to the base station. For a conventional routing algorithm, the nodes $j$ and $k$ are acceptable for further data transfer.

Based on the LA graph, the node $i$ is in the PSD state and needs to move to the OID state to send the packet. Let us assume that the probability of the node $j$ moving to the OID state is higher than that of the node $k$. Then, node $i$ will send a packet to node $j$ and then go into monitoring mode to monitor whether node $j$ has re-transmitted its packet further down the network. However, node $j$ did not re-transmit the packet through the network because of the cyberattack. Accordingly, node $i$ will recalculate indicators $I_{i,j}$ and $B_{i,j}$, and, based on the result of the complex indicator $Q_{i,j}$, determine the result of the action in the LA as the loss.

Using the system of Equation (2), the probabilities are recalculated; on the next iteration, node $i$ will send its data to node $k$ for further re-transmission when sending the packet again. If node $k$ re-transmits successfully, the probability for node $i$ grows.

Experiments with the use-case system were conducted, and their outputs are discussed in the following section.

3. Results

For the experimental study, a virtual ad hoc network was constructed in the NS-3 simulator [24]. The nodes are MICAz emulated devices [25] with Atmel ATmega128L micro-controller and 2.4 GHz IEEE 802.15.4 modules used to create a low-power wireless sensor network (WSN). The system topology on which the efficiency of the developed adaptive control method was evaluated includes 500 nodes located randomly in the area of 1000 to 500 m. The test bench consists of legitimate nodes, malicious nodes, and a base station governed by the AODV routing protocol. The number and behavior style of the compromised WSN nodes are varied.

The malicious nodes can perform packet modification attacks [26], black hole and grey hole attacks [27] with all or some packet ejection, and energy depletion [28,29]. When simulation starts, all nodes in the WSN consider each other a legitimate one.
Figure 3 shows the relationship between the number of lost packets and the number of malicious nodes in the system. In this experiment, the nodes performed the black hole and grey hole attacks with packet ejection as well as packet modification attacks. Only the correct packets arriving at the base station are counted. An incorrect packet is one that was generated by a legitimate node and did not reach the base station, or one that reached the base station but in some modified form differing from the original content.

The system with the LA-based control works better than conventional management in delivering the correct packets to the base station. Nodes successfully identify the malicious nodes and correct the rules of interaction with them. The loss rate stays below 20% when the number of malicious nodes is 20% of the total number of system nodes. Under the same conditions, the original system loses more than 70% of packets, which is too crucial for sensitive cyberspace.

Further experiments were carried out to evaluate the energy efficiency of the developed cyber resiliency method. A refined energy cost accounting model of the NS-3 simulator was utilized for the evaluation. Figure 4 depicts the dependence of the number of functioning nodes on the number of rounds passed. Round is defined as a certain period of time during which nodes transmit packets (in this sample: 100 s). In this experiment, the network worked in normal mode and there were no malicious nodes.

With the LA-based control, the nodes consume more power. In the following experiment, an additional 100 malicious nodes were deployed to conduct a resource exhaustion attack. The results are presented in Figure 5. The network uptime with active protection is 30% longer; the legitimate nodes successfully detect malicious nodes and rebuild the process of interaction with them, thereby not wasting their energy resources.
4. Discussion

To disrupt the stable functioning of the system, most cyber threats are targeted at breaking the work of the system. Cutting off the nodes of the system, breaking node-to-node communication via functional and control links connecting the system nodes, disturbing the routing protocol work and other impacts on resiliency inspire the researchers all over the world to design and develop various methods ensuring cyber resiliency.

The first group of the related works (e.g., [30–37]) proposes a technique of trust-based control for the distributed systems. The system nodes are grouped into unions (clusters), and each cluster allocates one node, the cluster head, which is responsible for the safety of the group. Data exchange in the cluster also takes place over the cluster head. Different studies (e.g., [38,39]) are focused on cluster head selection and voting mechanisms. The functional stability of the system is arranged as a reputation and trustworthiness model. It is based on the calculation of the score of the trust of nodes to each other while monitoring the activity of individual nodes and, consequentially, changing the nodes behavior to adapt to the varying circumstances [40]. Differences in approaches can arise due to the peculiarities of the environment in which nodes interact. There are different interpretations of reputation and trustworthiness considering various attributes, objects and subjects for trust measurement. For instance, Ref. [39] proposes swarm intelligence as an energy-

Figure 4. Number of functioning nodes as a function of network uptime (without attacking nodes).

Figure 5. Number of functioning nodes as a function of network uptime (exhaustion attacks).
efficient method. Additionally, Ref. [41] suggests an automaton-like model to select a trusted connection of the nodes within the re-configurable system.

The trust-based technique for the system control is promising because its application does not require the nodes to expend a large amount of system resources, while being able to protect against multiple cyber threats of different kinds. A weakness of this approach is the requirement of the computing resources for the head node and trustworthy calculations. Additionally, the introduction of a compromised node into a protected cluster can cause much more damage than the usual destructive impact of such a compromised node in a fully distributed system. Additional data transmission during trustworthy computing also affects the energy resources and lifetime of nodes. Data aggregation is used to optimize data transmission and thus preserve the functional stability of the network [42,43]. Aggregation techniques can, in some cases, prevent the targeted power depletion attacks [44]. For this purpose, special nodes, the aggregation points, are inserted into the structure for safe aggregation. However, the aggregation points can be susceptible to various types of attacks and hence require robust protection because false data can be inserted through the compromised nodes, which is guaranteed to lead to security faults [44].

The second group of competing works uses intrusion detection systems (IDS) operating to monitor the system nodes, identify the incidents and respond to security impacts. IDS functionality can be supplemented with additional operation to complete adaptability (e.g., [45–51]). IDS may be extended with an intelligent a posteriori security management subsystem, e.g., Ref. [52] suggests a smart advice system to improve the security maintenance, and Refs. [53,54] propose a finite state automaton to pave a secure data transmission route. The key weakness of this approach is the hard requirement for IDS agents running on the nodes and consuming vast computing and energy resources. A possible alternative as a centralized or cloud IDS, which requires a dedicated server, is not always feasible due to the nature of modern self-organizing cyberspaces of the IoT, WSN, VANET, and FANET.

Both trust-based and IDS-aided techniques mainly just allow us to identify the security impacts. In most cases, they are eliminated by isolating the malicious node from the system or informing us how to counteract the cyber threat. To preserve cyber resiliency, the proposed LA-based method adds adaptive behavior control whereby a node changes its behavior, continuing to interact with its neighbors. As in biological systems, in most cases, the hurt in some part of an organism does not force it to cut that part of it. The preservation of system operability is ensured by the LA, which changes the node’s behavior with respect to a malicious node, following the analysis of input signals.

The LA, as a control model, marshals adaptability for the under-controlled system. With respect to alternatives, the LA allows ensuring the security and functional sustainability for the protected system. The maintenance of cyber resiliency is achieved by adaptive behavior based on the system’s nodes dynamically changing the rules of interaction with their neighbors. Through the use of adaptive behavior, nodes are able to counteract both natural security threats and targeted attacks. It was experimentally demonstrated that the loss rate stays below 20% when the number of malicious nodes is 20% of the total number of nodes, while the common system loses more than 70% of packets. The network uptime with the LA-based solution is 30% longer.

The proposed mechanism of the LA-based control allows the security and functional resiliency to be ensured in the protected system regardless of its complexity and mission.

5. Conclusions

In this work, a novel method for the functional adaptation of the reconfigurable systems is composed on the basis of the LA model, which takes into account the current factors of the under-controlled system. The configuration of the LA model is built to describe dynamically changing the rules for the under-controlled interactions of the system nodes, and it allows nodes to self-adapt to the changes in the environment and thus preserve system resiliency. The flexible behavior of the system nodes is achieved by automatically changing the probabilities between machine states.
Experimental evaluation of the effectiveness of the proposed model for security control was carried out; it shows the superiority of the proposed approach over the traditional techniques. The developed solution supports the survivability of the supervised system, reducing the data loss rate and increasing the duration of faultless lifetime.

In further work, we are interested in focusing on modifying and adapting the developed method to expand applications, for example, cyber–physical technologies, such as VANET and FANET.

**Author Contributions:** Conceptualization, M.K.; methodology, software, T.O.; validation, M.K.; formal analysis, M.P. and T.O.; investigation, T.O.; resources, M.K.; writing—original draft preparation, M.K., T.O. and M.P.; writing—review and editing, M.K.; visualization, T.O.; supervision, M.K.; funding acquisition, M.K. All authors have read and agreed to the published version of the manuscript.

**Funding:** The research is funded by the Ministry of Science and Higher Education of the Russian Federation under the strategic academic leadership program “Priority 2030” (Agreement 075-15-2021-1333 dated 30 November 2021). Project results are achieved using the resources of supercomputer center of Peter the Great St. Petersburg Polytechnic University—SCC “Polytechnichesky” (www.spbstu.ru, accessed on 3 October 2022).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

**Abbreviations**

The following abbreviations are used in this manuscript:

- AODV: Ad hoc On-Demand Distance Vector
- FANET: Flying Ad hoc Network
- IoT: Internet of Things
- LA: Learning Automaton
- VANET: Vehicular Ad hoc Network
- WSN: Wireless Sensor Network

**References**

1. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* 2017, 88, 10–28.
2. Ross, R.; Pillitteri, V.; Graubart, R.; Bodeau, D.; Mcquaid, R. NIST SP 800-160. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021; Volume 2, Rev. 1, 294p. [CrossRef]
3. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* 2020, 77, 103201.
4. Djenna, A.; Harous, S.; Saidouni, D.E. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Appl. Sci.* 2021, 11, 4580. [CrossRef] [PubMed]
5. Online NIST Glossary. Available online: https://csrc.nist.gov/glossary (accessed on 3 October 2022). [CrossRef]
6. Malatji, M.; Marnewick, A.L.; von Solms, S. Cybersecurity capabilities for critical infrastructure resilience. *Inf. Comput. Secur.* 2022, 30, 255–279.
7. Ananiev, E.M. Intelligent biomechatronic systems. *Proc. IIF* 2016, 1, 98–100.
8. Zegzhda, P.; Pollatvtseva, M.; Lavrova, D. Systematization and security assessment of cyber-physical systems. *Autom. Control Comput. Sci.* 2017, 51, 835–843. [CrossRef]
9. Astafyev, V.I.; Gorsky, Y.M.; Pospelov, D.A. Homeostatics. In *Cybernetics and Applied Systems*; Marcel Decker: New York, NY, USA, 1992; pp. 7–22.
10. Teslinov, A.G. *Development of Control Systems: Methodology and Conceptual Structures*; Globus: Moscow, Russia, 1998; p. 229. [CrossRef]
11. Gerostathopoulos, I.; Bures, T.; Hnetyrka, P.; Keznikl, J.; Kit, M.; Plasil, F.; Plouzeau, N. Self-adaptation in software-intensive cyber–physical systems: From system goals to architecture configurations. *J. Syst. Softw.* 2016, 122, 378–397.
12. Gerostathopoulos, I.; Skoda, D.; Plasil, F.; Bures, T.; Knauss, A. Tuning self-adaptation in cyber-physical systems through architectural homeostasis. J. Syst. Softw. 2019, 148, 37–55.
13. Gerostathopoulos, I.; Skoda, D.; Plasil, F.; Bures, T.; Knauss, A. Architectural Homeostasis in Self-Adaptive Software-Intensive Cyber-Physical Systems; Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Cham, Switzerland, 2016; Volume 9839, pp. 113–128. [CrossRef]
14. Anokhin, P.K. Ideas and facts in developing the theory of functional systems. Psychol. J. 1994, 1, 107–108. [CrossRef]
15. Sudakov, K.V. General regularities of dynamic organization of functional systems. Man His Health. 2005, 2, 4–13.
16. Fradkov, A.L. Adaptive Control in Complex Systems; Nauka: Moscow, Russia, 1990.
17. Redko, V.G. Neuroinformatika-2002: Problems of Intellectual Control. In System-Wide, Evolutional and Neural Network Aspects; MIFI: Moscow, Russia, 2003; pp. 8–39.
18. Semyonov, R.D. Formation of high-organized organisms as a consequence of the anticipatory reflection of reality. In Proceedings of the Feozovsky Readings: Materials of All-Russian Scientific-Practical Conference, Cheboksary, Russia, 30 June 2020; pp. 54–59.
19. Skoptzov, O.P. An attempt to expand the theory of the functional system. In Proceedings of the International Congress “Neuroscience for Medicine and Psychology”, Crimea, Russia, 30 May–10 June 2018. Available online: http://brainres.ru/work/Sudak_2018_14_Congress_Proceeding.pdf (accessed on 3 October 2022).
20. Novikov, D.A. Methodology of Management; Librocom: Moscow, Russia, 2011; Volume 1, 128p.
21. Tsetlin, M.L. Automation Theory and Modeling of Biological Systems; Academic Press: New York, NY, USA, 1973; Volume 10, p. 102.
22. Narendra, K.S.; Thathachar, M.A.L. Learning Automata: An Introduction; Courier Corporation: New York, NY, USA, 2012.
23. Thathachar, M.A.L.; Sastry, P.S. Varieties of learning automata: an overview. IEEE Trans. Syst. Man Cybern. Part B (Cybern.) 2002, 32, 711–722.
24. NS-3 Model Library. Available online: https://www.nsnam.org/docs/release/3.30/models/ns-3-model-library.pdf (accessed on 3 October 2022).
25. Kramer, M.; Geraldy, A. Energy Measurements for Micaz Node; Technical Report KrGe06; University of Kaiserslautern: Kaiserslautern, Germany, 2006. [CrossRef] [PubMed]
26. Kannhavong, B.; Nakayama, H.; Nemoto, Y.; Kato, N.; Jamalipour, A. A survey of routing attacks in mobile ad hoc networks. IEEE Wirel. Commun. 2007, 14, 85–91.
27. Dixit, S.; Joshi, K.K.; Joshi, N. A review: Black hole and gray hole attack in MANET. Int. J. Future Gener. Commun. Netw. 2015, 8, 287–294.
28. Ghildiyal, S.; Semwal, A.; Rana, J.S. Analysis of Security Requirements, Attacks and Vulnerabilities at Transport Layer in Wireless Sensor Networks. Int. J. Comput. Appl. 2016, 137, 13–16. [CrossRef]
29. Jhaveri, R.H.; Patel, S.J.; Jinwala, D.C. DoS attacks in mobile ad hoc networks: A survey. In Proceedings of the Second International Conference on Advanced Computing and Communication Technologies, Rohtak, India, 7–8 January 2012; pp. 535–541. [CrossRef]
30. Manjeshwar, A.; Agrawal, D.P. TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks. IPDPS 2001, 1, 189. [CrossRef]
31. Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2000; Volume 2; p. 10.
32. Saqib, A. Cybersecurity Management for Distributed Control System: Systematic Approach. J. Ambient. Intell. Humaniz. Comput. 2021, 12, 10091–10103.
33. Kumar, A.; Mishra, S.; Kushwaha, D.S. A New Collaborative Trust Enhanced Security Model For Distributed System. Int. J. Comput. Appl. 2010, 1, 127–134.
34. Moreno, R.T.; Garcia-Rodriguez, J.; Bernabe, J.B.; Skarmeta, A. A Trusted Approach for Decentralised and Privacy-Preserving Identity Management. IEEE Access 2021, 9, 105788–105804.
35. Milne, A.J.M.; Beckmann, A.; Kumar, P. Cyber-Physical Trust Systems Driven by Blockchain. IEEE Access 2020, 8, 66423–66437. [CrossRef]
36. Ge, C.; Zhou, L.; Hancke, G.P.; Su, C. A Provenance-Aware Distributed Trust Model for Resilient Unmanned Aerial Vehicle Networks. IEEE Internet Things J. 2021, 8, 12481–12489. [CrossRef]
37. Ebrahimi, M.; Haghighi, M.S.; Jolfaei, A.; Shamaein, N.; Tadayon, M.H. A Secure and Decentralized Trust Management Scheme for Smart Health Systems. IEEE J. Biomed. Health Inform. 2022, 26, 1961–1968. [CrossRef]
38. Petrenko, A.S.; Petrenko, S.A.; Makoveichuk, K.A.; Chetyrbok, P.V. The IIoT/IoT device control model based on narrow-band IoT (NB-IoT). In Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, Russia, 29 January–1 February 2018; pp. 950–953. [CrossRef]
39. Juliana, R.; Maheswari, P.U. An energy efficient cluster head selection technique using network trust and swarm intelligence. Wirel. Pers. Commun. 2016, 2, 351–364 [CrossRef] [PubMed]
40. Ovasapyan, T.D.; Ivanov, D.V. Security provision in wireless sensor networks on the basis of the trust model. Autom. Control Comput. Sci. 2018, 8, 1042–1048.
41. Zhu, H.; Zhang, Z.; Du, J.; Luo, S.; Xin, Y. Detection of selective forwarding attacks based on adaptive learning automata and communication quality in wireless sensor networks. Int. J. Distrib. Sens. Netw. 2018, 14, 1550147718815046. [CrossRef]
42. Poltavtseva, M.A.; Lavrova, D.S.; Pechenkin, A.I. Scheduling Internet of Things data aggregation and normalization tasks for processing on a multiprocessor cluster. In Problems of Information Security. Computer Systems; Polytechnic University Press: St. Petersburg, Russia, 2016; Volume 1, pp. 37–46. [CrossRef]

43. Dhand, G.; Tyagi, S.S. Data aggregation techniques in WSN: Survey. Procedia Comput. Sci. 2016, 92, 378–384. [CrossRef]

44. Belenko, V.; Chernenko, V.; Krundyshev, V.; Kalinin, M. Data-driven failure analysis for the cyber physical infrastructures. In Proceedings of the IEEE International Conference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, 6–9 May 2019; pp. 1–5.

45. Corbò, G.; Foglietta, C.; Palazzo, C.; Panzieri, S. Smart Behavioural Filter for Industrial Internet of Things: A Security Extension for PLC. Mob. Netw. Appl. 2018, 23, 809–816. [CrossRef]

46. Steingartner, W.; Galinec, D.; Kozina, A. Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry 2021, 13, 597.

47. Quincozes, S.E.; Albuquerque, C.; Passos, D.; Mossé, D. A survey on intrusion detection and prevention systems in digital substations. Comput. Netw. 2021, 184, 107679. [CrossRef]

48. Annarelli, A.; Nonino, F.; Palombi, G. Understanding the management of cyber resilient systems. Comput. Ind. Eng. 2020, 149, 106829. [CrossRef]

49. Rajamäki, J. Resilience Management of Critical Cyber-Physical Systems: A Multiple Case Study Analysis. Des. Constr. Maint. 2021, 1, 86–92. [CrossRef]

50. Janakiraman, S.; Rajasoundaran, S.; Narayanasamy, P. A Dynamic Intrusion Detection on data flow at low data rate in Wireless Sensor Networks. Eur. J. Sci. Res. 2012, 73, 245–253. [CrossRef]

51. Nagarajan, A.; Sood, A. Realizing Cyber Resilience with Hybrid Intrusion Tolerance Architectures. Master’s Thesis, George Mason University, Fairfax, VA, USA, 2017. [CrossRef]

52. Anisimov, V.G.; Anisimov, E.G.; Zegzhda, P.D.; Saurenko, T.N.; Prisyazhnyuk, S.P. Indices of the effectiveness of information protection in an information interaction system for controlling complex distributed organizational objects. Autom. Control Comput. Sci. 2017, 8, 824–828.

53. Misra, S.; Krishna, P.V.; Abraham, K.I. A simple learning automata-based solution for intrusion detection in wireless sensor networks. Wirel. Commun. Mob. Comput. 2011, 11, 426–441.

54. Amir, H.; Navid, A.H.F.; Javadi, H.H.S. ICLEAR: Energy aware routing protocol for WSN using irregular cellular learning automata. In Proceedings of the 2009 IEEE Symposium on Industrial Electronics and Applications, Kuala Lumpur, Malaysia, 4–6 October 2009; Volume 1, pp. 463–468. [CrossRef]