symmetry

MDPI

Article

Modelling Artificial Immunization Processes to Counter Cyberthreats

Dmitry Zegzhda, Evgeny Pavlenko * and Elena Aleksandrova

Institute for Cyber Security and Information Protection, Peter the Great St. Petersburg Polytechnic University, 195251 Saint Petersburg, Russia; dmitry@ibks.spbstu.ru (D.Z.); helen@ibks.spbstu.ru (E.A.)
* Correspondence: pavlenko@ibks.spbstu.ru; Tel.: +7-921-958-79-09

Abstract: This paper looks at the problem of cybersecurity in modern cyber-physical and information systems and proposes an immune-like approach to the information security of modern complex systems. This approach is based on the mathematical modeling in information security—in particular, the use of immune methods to protect several critical system nodes from a predetermined range of attacks, and to minimize the success of an attack on the system. The methodological approach is to systematize the tasks, means and modes of immunization to describe how modern systems can counter the spread of computer attacks. The main conclusions and recommendations are that using an immunization approach will not only improve the security of systems, but also define principles for building systems that are resistant to cyber attacks. The immunization approach enables a symmetrical response to an intruder in a protected system to be produced rapidly. This symmetry provides a step-by-step neutralization of all stages of a cyber attack, which, combined with the accumulation of knowledge of the attacker's actions, allows a base of defensive responses to be generated for various cyber attack scenarios. The theoretical conclusions are supported by practical experiments describing real-world scenarios for the use of immunization tools to protect against cyber threats.

Keywords: cybersecurity; immunization; targeted immunization; cyber threat; honeypot

Citation: Zegzhda, D.; Pavlenko, E.; Aleksandrova, E. Modelling Artificial Immunization Processes to Counter Cyberthreats. *Symmetry* **2021**, *13*, 2453. https://doi.org/10.3390/sym13122453

Academic Editor: Tomohiro Inagaki

Received: 25 November 2021
Accepted: 14 December 2021
Published: 20 December 2021

1. Introduction

Considering the digitalization developments, information systems are constantly consolidating in the interests of business and industry. These systems function as a whole, representing conglomerates of databases and data warehouses, information processing systems, supervisory control and data acquisition (SCADA) systems, etc. They also interact with other similar systems and with endpoint protection [1,2]. Examples of such large-scale systems are airport management, manufacturing, e-government and banking systems. Such objects are susceptible to constant targeted attacks, and therefore, there is a need to develop an approach that could create a methodology for repelling the corresponding cyber threats and targeted attacks, which leads to the topic of this article.

The listed systems have the following signature features considering information security:

1. Complex heterogeneous composition of components, duplicated links and high formalization difficulty.
2. These systems are multifunctional, which means that a constant operator cannot express the general functionality. Superposition of functional units of the structure shows dynamically changes.
3. A lack of redundancy and the interchangeability of nodes, determined by the inability to stop the system or the violation of permanent data transmission systems.
4. The targeted nature of the threats, which means that the target of the attack are individual nodes or segments of the system. Concurrently, the attack itself is on a distributed mode.

5. The critical nodes' persistence and the possibility of information security violations of secondary nodes.

The authors have experience in creating methodology for preventing cyber threats and mitigating the consequences of attacks with dynamically reconfiguring systems using the properties of redundancy and interchangeability, which are used to restore the functionality of the system, represented as a route on a connected graph structure. Based on the peculiarities of this object, the application of this approach is directly difficult; therefore, the authors propose the development an immuno-like approach aimed at protecting critical nodes of such systems by developing a set of temporarily applied structures and functional nodes to reduce the risk of an attack.

Unlike the previously described self-regulating approach, immunization is not restoring all possible functions of the system. It is aimed at developing symmetrical measures that protect the system from a given set of threats and reducing the risk of affecting critical nodes from new threats. The main feature of the approach, and at the same time its advantage, is its focus on a given list of attacks, since it allows one to protect critical nodes from complex targeted attacks typical for these types of systems.

The aim was to search for such a set of operators that, by analogy with the immune approach, prevent threats to a number of components from computer attacks, by generating the necessary protective action frames. Each of these frames implements a symmetric response to an attacker's actions on the system, eliminating or minimizing their malicious impacts. The proposed immune approach also reduces the risk of a pandemic of highly dangerous viruses and represents a set of structural measures to reserve additional components to protect critical catches from targeted attacks.

2. Backround

Reference [3] presents the simulation study results of viruses' spread characteristics. There, the study results of immunization as a potential defense mechanism are presented, and it is shown that in certain topologies, a relatively small number of strategically located immune nodes can have significant impact on the spread of a virus.

A method was proposed in [4] of targeted immunization based on self-similarity. It has been shown experimentally that immunization based on the self-similarity method is the most effective in comparison with other types of immunization. The method based on self-similarity is much more convenient in practical settings. Unlike existing methods, which do not take into account the time delay between virus infection and vaccine development, in this study, such a delay is modeled on the assumption that the vaccine will be available only when the virus reaches a critical point.

In [5], the immunization of a small fraction of adjacent nodes was proposed instead of the immunization of selected nodes. This approach does not require network knowledge. It selects a random fraction of the total number of nodes and searches a random node adjacent to it. This approach is probabilistic in nature.

A new model for computer virus epidemics was proposed in [6]. Its novelty lies in the fact that the overall nonlinear rate of infection is taken into account. The authors showed that, under moderate conditions, the proposed model admits a (viral) globally asymptotically stable equilibrium, fully demonstrating equilibrium robustness to the details of infections.

The authors of [7] presented the susceptible–vaccinated–exposed–infectious–recovered (SVEIR) model for the treatment of infectious nodules, taking into account the development of acquired immunity in recovered nodules. The authors noted that the existence of a unique internal equilibrium depends on the basic multiplication number and the speed of treatment.

A model of an electronic epidemic of malicious code in a computer network through vertical transmission is presented in [8]. The authors note that if the basic reproduction number is less than unity, then the infected fraction of computer nodes disappears and ma-

licious code dies out, and the equilibrium without malicious code is globally asymptotically stable, leading to the code's eradication.

In [9], a model with two different structures—attacking class and target class—is presented to study the mobility of viruses when attacking a target network. The concept of optimal control is introduced to regulate the spread of the virus, and the use of a firewall is also suggested.

The authors of [10] aimed to investigate the effect of vaccination on the spread of computer viruses. For this purpose, the authors proposed a new model of computer virus propagation which includes a non-linear probability of vaccination. The results obtained by the authors show that, depending on the value of the underlying multiplication number, either an equilibrium without viruses or an equilibrium with viruses is globally asymptotically stable.

The authors of [11] proposed a simulation of virus behavior in a network and developed an immunization algorithm for it. The approach to immunization considered in this work is also probabilistic, since the process of restoring the graph (transition from an infected state to a susceptible one) also has a given probability. The data focus only on countering computer viruses and do not take into account the peculiarities of cyber threats in complex systems. It should be noted that this approach from paper [11] can be used, but it should be complemented by proposals for an immunization strategy that would take into account the type of attack which is being carried out.

The source [12] focuses on an approach based on the immunization of centralized nodes in large-scale networks and argues that it is not always possible to determine the optimal nodes for immunization. The approach they propose is based on the estimation of node centrality metrics of the network and immunization of nodes with the highest centrality scores. Their results demonstrate that the spread of the epidemic with such immunization is significantly slower.

The paper [13] highlights the security problem of IoT systems; in particular, the authors note that the attack surface increases due to the large number of connected devices. In the paper, the authors propose an approach, which seeks to account for the intrinsic properties of nodes in an IoT system, to building a multi-layered network that can help develop more realistic propagation models. From this, the authors then derive a compact representation that facilitates decision-making processes and security analysis.

The authors of the source [14] focused on the problem of malware infecting the network. They argued that attackers decide whether to attempt to infect a host depending on the security mechanisms detected in it. The authors suggested keeping track of such checks carried out by attackers and "vaccinating the system"—creating special points that attackers will spend time examining. Experimental studies have shown a reduction in the rate of malware infections on the network.

3. Basic Provisions of the Immune Approach

The reason for choosing an approach based on immunization is that immunization is another approach to solving the problem of countering cyber threats—the development of the ideas of P.K. Anokhin about the transfer of the biological properties of life preservation to information security [15,16]. Immunization is one of the mechanisms of self-regulation for systems, which, unlike homeostasis, protects the system from a certain spectrum of cyber threats and reduces the risk of damage to critical nodes from new cyber threats.

The key idea of the immune approach consists of two stages: protecting critical nodes and building immunity. Node immunity is the complexity (algorithmic, computational, organizational) required for an attacker to implement an attack on said node.

An attack on a system is viewed as a specific action frame, independent of what happened in the system. Actions are assessed in terms of danger to critical nodes in the system, and protection is to limit the spread of these actions throughout the system (similarly to how limiting communications is a protective measure in a pandemic) by generating and activating symmetrical frames of defensive actions. Protection of critical

nodes is real instead of the protection of all nodes in a multicomponent complex system, and the implementation of such protection includes performing a certain frame-action to change the parameters of the nodes' connections. A scientific task closely related to this practical task is the correlation of the infection spread with the time of the frame-action (reaction) [17].

An action frame is a structure consisting of a set of slots with different types and values. Some of the information in the frame remains unchanged, while other information changes. Mathematically, a frame is expressed as an operator Δ, which is applied to a set of parameters P that characterize the system and its current state. In this case, the part of the information in the frame describing the system will be constant, since the system has a certain functionality that is predefined. The changing part of the information corresponds to the conditions in which the system is located, including the values of important parameters by which a destructive effect can be detected. The result of applying the frame to the system parameters is a set of actions and parameters of the system P_{out}, with which it is in a secure state: $\Delta(P) \rightarrow P_{out}$.

Mathematically, a frame can be conveniently represented as a set of matrices describing the parameters of the system in the current time period—directly, the time of observation of the system and the structure:

$$\Delta(P) \rightarrow TIME \left| \begin{array}{ll} hour & \{1, \ldots, 24\} \\ minute & \{0, \ldots, 60\} \\ second & \{0, \ldots, 60\} \end{array} \right| \times STRUCTURE \left| \begin{array}{lll} nodes & current\ value & MAX \\ connections & current\ value & MAX \\ reserve & [nodes\ number] & [connections\ list] \end{array} \right| \times PARAMETERS \left| \begin{array}{lll} p_1 value & MIN\ p_1 value & MAX\ p_1\ value \\ \ldots & \ldots & \ldots \\ p_N\ value & MIN\ p_N value & MAX\ p_N\ value \end{array} \right| \quad (1)$$

A separate knowledge base is used to automatically generate frames for defensive actions, storing the frame templates according to the structure described in Equation (1). The frame pattern according to which the automatic generation of a symmetrical response to an attack is carried out includes:

1. The time parameter: For defensive actions it corresponds to the time necessary for activation of actions counteracting an attack (time for redistribution of functions between nodes, time for activation of reserve nodes, etc.).
2. The structure in the form of a graph, corresponding to the structure with which the attack realized on the system is eliminated. In this structure the changes are made compared to the current structure: links with reserve nodes are added (reserve (connections list) field), graph nodes corresponding to compromised nodes are removed (nodes field), reserve nodes are added (reserve field) and interactions between nodes are redistributed (connections field). For each protection frame, according to the structure, the maximum numbers of nodes and connections that can be changed when responding to an attack are defined.
3. Structure in the form of a set of triplets: "graph node–node parameter–parameter value." The need for such a structure is due to the fact that modern systems often perform some technological processes in which the parameters of some components must remain within specified limits (for example, the temperature value in the industrial shop of digital factory must be maintained within the specified interval). For each parameter there is a minimum value and maximum value. The data stored in this frame structure are needed to adjust key parameters for system operation. Such parameters may include both the operational parameters of industrial devices, and for example, the performance metrics of network devices.

The practical implementation of the frame consists in the matching of software commands to graphical operations. These mappings are stored in a separate database in the form of lists. For example, for an action frame in which a compromised node is deactivated (vertex deletion) and a standby node is activated (vertex and its incident arcs are added),

software commands "switch off," "switch on" and "establish connection with . . . " are sent to the control controller, where identifiers of nodes with which the activated standby node should exchange data are specified instead of dots.

For example, an attack involving nodes v_1 and v_2 produces an action frame that replaces node v_1 with node v_3 and redistributes the functions of node v_2 between nodes v_4 and v_5. The pattern of such a frame is as follows (Table 1):

Table 1. Pattern of a security frame.

Frame Field	Field Parameter	Parameter Value	
Time	Hour	0	
	Minute	0	
	Second	0	
Structure	$nodes: \{$ $v_1 =$ "*delete*", $v_2 =$ "*delete*", $v_3 =$ "*activate*", $v_4,\ v_5 =$ "*add_fn*" $\}$	$current\ value: \{$ $v_1, v_2 =$ "*infected*", $v_3 =$ off, $v_4,\ v_5 =$ "*on*" $\}$	$MAX: 10$
	$connections: \{$ $v_1 =$ "*delete*", $v_2 =$ "*delete*" $v_3 =$ "*add incidental to* (v_1)" $v_4, v_5 =$ "*distribute from* (v_2)" $\}$	$current\ value: \{$ $v_1 =$ "*incidental to* (v_6, v_7)" $v_2 =$ "*incidental to* $(v_8, v_9,\ v_{10})$", $v_4 =$ "*incidental to* (v_{11}, v_{12})" $v_5 =$ "*incidental to* (v_{13})" $\}$	MAX: 30
	reserve	$[v_3]\ [v_6, v_7]$	$[v_3, v_6;\ v_3, v_7]$
Parameters	$v_1:$ p_1 p_2	$MIN\ p_1 value:\ 5$ $MIN\ p_2\ value:\ 11$	$MAX\ p_1 value:\ 15$ $MAX\ p_1 value:\ 30$

Using a graphical representation of the system, the generation of frames is not a complex operation and is conveniently reduced to templates, within which the vertices and arcs on the graph characterizing the system components and the connections between them are specified. The graphical representation also allows adjusting the parameters of the system components as well. Thus, an important part of the frame generation mechanism is the setting of unary operations on the graph that models the systems. Frame template generation requires some preliminary work and effort from cyber security specialists, but can be automated quite easily thereafter.

The problem statement is as follows: There is a protected system modeled by a directed graph G with a set of vertices V and arcs E: $G: \langle V, E \rangle$. Each vertex $v_i \in V$ corresponds to a set of parameters $P_i: \left\{P_i^1, P_i^2, \ldots, P_i^N\right\}$. The problem of countering attacks consists in finding such symmetrical transformation operators Op of system G so that the values of all parameters for each vertex are within the admissible limits: $p: \forall v_i \in V,\ \forall P_i^j \in P_i\ P_i^j \in \left[P_{i\,min}^j; P_{i\,max}^j\right]$.

We introduce the following three groups of operators Op for transforming the system, aimed at countering attacks:

1. The operator for transferring the structure of the system into a functionally equivalent one: The structure changes relative to the protected node $p_1: G \to G',\ G': \langle V', E' \rangle, V = V',\ E = E'$. Here, the functional symmetry of the system itself is preserved by replacing some equivalent nodes.
2. Operator for limiting the spread of massive attacks within the system: It minimizes the number of infected V_Z nodes. $Op_2: V_Z \to min$. A symmetrical response to an attacker infecting nodes is to exclude them from any important functionality.

3. Operator for complication of access to the protected node: Increases the time t_Z, and computational res_Z and organizational org_Z costs, for the attacker when trying to attack the node. $Op_3 : t_Z$, $res_Z, org_Z \rightarrow max$. The symmetrical response here is to increase the resilience of the components of the system: the more valuable it is for the attacker to gain access to a component, the harder it will be for him to carry out destructive actions.

The task of increasing the immunity of nodes (later on—the immunity of an entire network segment) is associated with countering a certain set of attacks by creating for each of them a symmetrical frame-action to protect critical nodes.

Regarding building up the immunity of nodes, it should be clarified that by the immune resistance of a system node or network segment, we mean an estimate of the number and complexity of operators that aim to have a destructive effect along the access route from the entry point to the system while attacking a protected node. For example if the system is presented as a graph, then the immune resistance is the path length weighted by the complexity of the movement from the entry point to the node.

3.1. Immunization Goals

1. Prevention of cyber attacks' spread.
2. Strengthening the existing protection or adding new protective elements to the system, implemented by making parametric changes or adding properties.
3. Countering attacks' mechanisms of action for specific nodes.
4. Elimination of attacks' consequences.
5. Protection of critical nodes. It is important to note that critical nodes may not be the same, and different methods should be used to protect them.

3.2. Means, Modes and Mechanisms of Immunization

The system is exposed to cyber attack Z, the intensity of which is expressed as $Z \rightarrow G(V, E, R) \rightarrow G\prime(V\prime, E\prime, R\prime)$. For the automated generation of a corrective symmetrical action, a set of structures is generated that are equivalent to a structure that ensures the execution of the function F on the graph G. Since the current structure requires changes in this scenario, in [18], the transition was made to a new graph G', with another set of structures R', including into themselves both those structures that had not been touched by the destructive influence of the attacker, and new structures that made it possible to respond symmetrically such an influence by preventing it or eliminating it.

The main emphasis usually is placed on the description of the functioning of the system, and the scheme of functioning is set using a directed connected graph, which simultaneously determines the physical and functional structure of the system.

Let us distinguish two types of system components: a functional component capable of performing a certain function, semantically indivisible in terms of the operation of the system under consideration, and a structural component, which is a certain subgraph of the system with certain characteristics (connectivity, redundancy, etc.).

Figure 1 shows the systematization of immunization means [7,19–21].

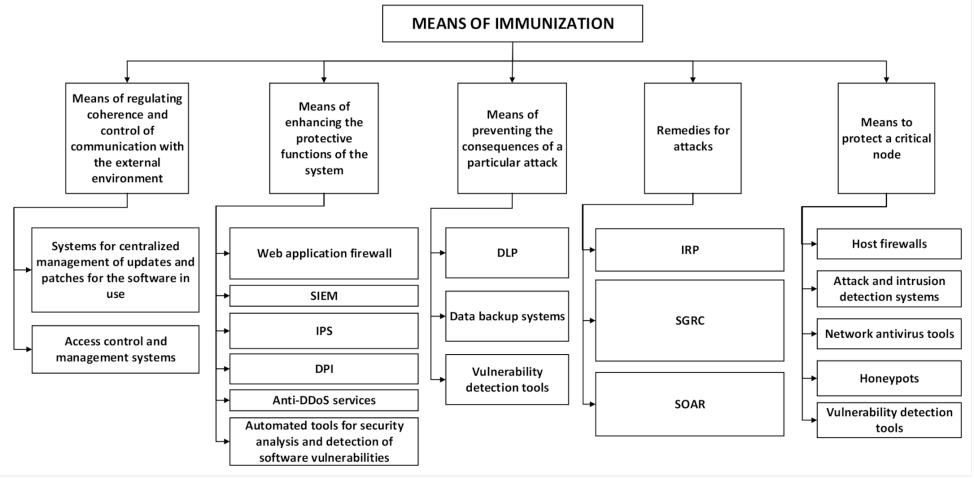

Figure 1. Systematization of immunization means.

There are two modes of immunization: prophylactic and probabilistic.

Preventive mode is based on the fact that when any new cyber threats appear (for example, new types of virus programs), the system must immediately learn to recognize and block them, even before attackers try to use them when attacking the system. To block cyber threats, symmetrical immune templates should be created, separate for each cyber threat. Preventive mode is aimed at countering specific attacks or types of security breaches; it does not matter if it concerns individual nodes of the system or the entire system as a whole.

The probabilistic mode is a set of measures used to protect critical nodes by creating additional lines of defense. These can include honeypot systems that create false targets for an attacker and pass them off as components of a real infrastructure, and additional security systems.

Honeypots should be mentioned separately: their functionality is very broad due to the fact that there are several types of them [22]. There are:

1. Low-interactive ones emulate services, applications and operating systems. They are quite easy to integrate into the protected system. The risk of compromise is also fairly low, but the set of available information about the attacker's behavior is limited.
2. Highly interactive ones represent real, not emulated, services, applications and operating systems. They allow you to obtain a significant amount of information about the behavior of an attacker in the system, but their risk of being compromised is significantly higher, and it is also quite difficult to develop and implement them secretly from an attacker.
3. Servers listen to network connections, analyzing attacks on users, services and host systems.
4. Clients are capable of communicating and remotely interacting with potentially malicious resources to obtain information. However, to do this, they need specially prepared "instructions" for connecting to untrusted sources. Additionally, such honeypots are capable of analyzing attacks aimed at clients and users.

4. Experimental Studies on Real Scenarios

Consider specific examples of immunization mechanisms.

Example 1. *Preventing the Spread of Attacks to Critical Systems.*

A redundant distributed network is given which consists of a finite number of computers that make up a population. At the first moment in time, the population size is N_0. Each population member has a certain set of useful functions that it supports. The more unique the set of functions supported by the node, the more important it is for the popula-

tion. According to this principle, critical individuals carrying a rare, critically important functional, and secondary nodes, are distinguished in the population.

Figure 2 shows the lifecycle of a node. The processes of population replenishment at the expense of reserve nodes and extinction due to infection at each moment in time of the population part are included.

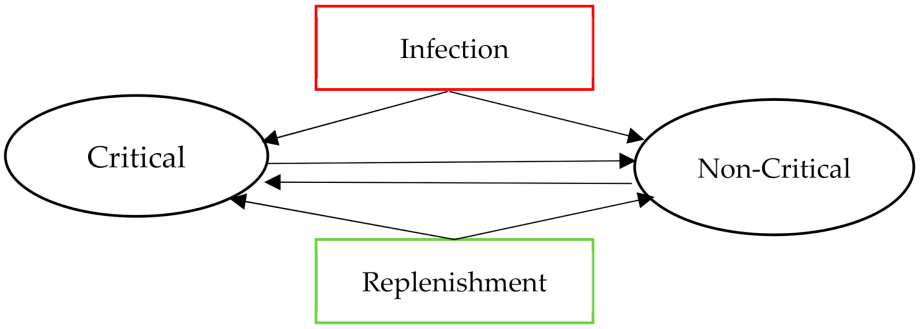

Figure 2. A node's lifecycle.

Infection is understood as the process of infection of nodes, which is tantamount to the process of extinction. With a decrease in the breeding potential of the system, the rate of extinction increases. Moreover, each node can arrive in the "critical" or "secondary" state and change its state an arbitrary number of times during its life; this is due to the constant extinction of individuals in both states. At each moment in time, the selection of critical nodes occurs anew, and the number of critical nodes should be C_0.

For a mathematical description, sets of redundant and infected nodes are highlighted; arrows indicate all possible transitions from one state to another (Figure 3).

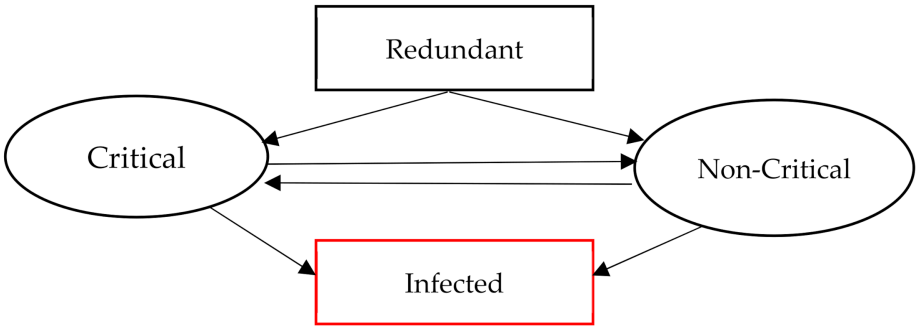

Figure 3. Transitions cycle.

All nodes can be divided into four types:

1. C—Critical nodes.
2. O—Non-critical/minor nodes.
3. R—Redundant nodes, representing nodes equivalent to the failed ones. A redundant node or chain of nodes is built into the network and becomes critical or non-critical.
4. I—Infected nodes. The total number of dead nodes since the beginning of the life of the system.

Initial conditions:

$$C = C_0,\ C_0 > 0,\ O = O_0,\ O_0 \geq 0,\ R = R_0,\ I \geq 0 \tag{2}$$

$$\begin{cases} C(t) = O(t)\beta + C(t)(1-\eta_1) + \vartheta t k_1 - C(t)\gamma \\ O(t) = \vartheta t k_2 + O(t)(1-\eta_2) - O(t)\beta + C(t)\gamma \\ I(t) = C(t)\eta_1 + O(t)\eta_2 \\ R(t) = R - \vartheta t \end{cases} \tag{3}$$

where

1. η_1, η_2, γ, β—Coefficients lying in the range [0, 1] reflect the shares of nodes at a certain moment in time that have passed from one state to another.
2. η_1—The infection rate of critical nodes is the proportion of nodes that have passed from state C to state I at a given time. It sets the mortality rate of critical nodes. It changes over time—it grows as the number of non-infected nodes decreases. η_1 increases as O and C decrease.
3. η_2—The infection rate of non-critical nodes O specifies the fraction of nodes that have passed from state O to state I at a given time. It specifies the mortality rate of secondary nodes. η_2 increases as redundant nodes decrease.
4. γ—The coefficient of transition of a critical node C to a non-critical state O. (The share of critical nodes in the network is fixed; in this case, the critical status of a node can be changed to non-critical.)
5. β—The coefficient of a non-critical site transition from O to critical C.
6. ϑ—The speed of population reproduction. Measured as a fraction of knots per second. It sets the rate of transition from state R to O or C.
7. k_1, k_2—Coefficients of transition of the reserve node to critical or secondary, $k_1 + k_2 = 1$.
8. d_1—The fraction of critical nodes among all nodes in the system.
9. d_2—The fraction of non-critical nodes among all nodes in the system.

As can be seen from system (3), calculations are performed on the number of nodes (individuals). The coefficients reflecting mortality at each time point of critical and secondary nodes change in accordance with the following ratios:

$$\begin{array}{c} \eta_1 \propto 1 - \frac{O}{N_0} \\ \eta_2 \propto 1 - \frac{R}{R_0}. \end{array} \quad (4)$$

This means that the fewer secondary nodes in the population, the faster the "critical" individuals die out, and the lesser the population's reproducibility, the higher the mortality of the secondary nodes.

After performing a number of mathematical transformations to estimate the fraction of critical nodes d_1, we get:

$$\begin{array}{c} d_1 < \frac{\beta - \beta d_2}{d_2 - \gamma} \\ \beta < \frac{d_1 d_2 - d_1 \gamma}{1 - d_2} \end{array} \quad (5)$$

This means that the lower boundary of the critical site's fraction d1 and the coefficient of transition from secondary to critical sites must satisfy conditions (5). In other words, the fraction of critical nodes from all of the population at the initial selection should not exceed the product of the coefficient of transition from critical nodes to secondary nodes and the proportion attributable to critical and infected nodes at the initial moment of time with a known proportion of secondary nodes. Moreover, the fraction of secondary nodes at the initial moment of time should not coincide with the coefficient of transition from secondary nodes to critical ones, but it can be less than it. Then, d_1, the fraction of critical nodes at the initial moment in time within the entire population, should exceed the ratio described above.

The automatic generation of frames here was done both with and without node type (critical or non-critical). In the simulated attack, the goal was to render the system inoperable by disabling the critical nodes as quickly as possible. However, due to their higher security, non-critical nodes were infected faster.

The immunization of critical nodes was done by generating frames that activated redundant nodes: removing a node and creating a new one that incurred all the arcs of the deleted one (replacing the compromised node with a redundant one, including all its network communications).

Immunization of non-critical nodes was mainly performed by simple frames, which were modeled by unary operations on the graph inverse to destructive actions:

1. Vertex deletion (disconnection of a compromised node).
2. Deletion of links (termination of network communications with the compromised node).

The following parameters were used in the simulation: the network consisted of 600 nodes, of which 200 were critical, 350 were non-critical and 50 were redundant. In non-infected mode, 100 nodes were already infected in the first 5 virtual strokes, and in 32 strokes all nodes were infected and the system failed. When immunizing non-critical nodes, the 100 infected node mark was reached in 15 virtual clock cycles, the system was almost completely inoperable after 40 clock cycles and full system infection occurred at 55 clock cycles. When critical nodes were immunized, the system was able to function for up to 55 cycles, and it is important to note that not all 600 nodes were disabled.

Three lines are shown in Figure 4: the first is for when no immunization was implemented in the system, the second is for when immunization was performed against non-critical nodes whose importance to system operation is low and the third is for when immunization was implemented against critical nodes. Figure 4 shows that the best result in terms of cybersecurity was achieved when immunizing critical nodes.

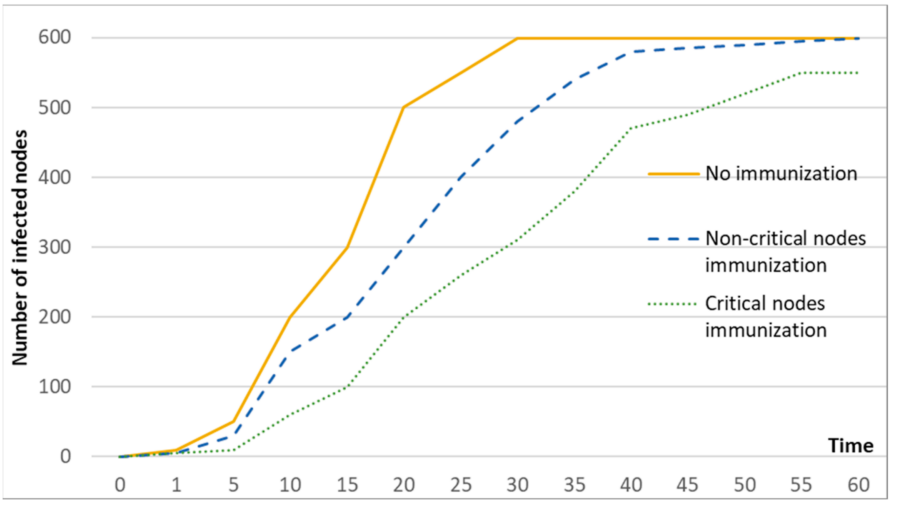

Figure 4. Experiments for different immunization types.

Thus, when developing a symmetrical response to an attacker's actions, the specifics and structure of the system must be taken into account. The protection and replacement of critical nodes must be carried out first; only then can one speak of successful immunization.

Example 2. *Protection against a specific attack.*

The response to an attack being implemented must be related to the type of attack. If the purpose of a malicious attack is to disable one or more components of the system, the symmetrical response to such an attack involves the search for a system component that, in addition to its functions, is capable of performing the functions of the component under attack. The reaction to such an event can also involve activating a backup system component that did not perform any functions before, but is capable of replacing one or more compromised or disabled components in the event of an attack.

Attacking influences can relate not only to the disabling of a part of the system, but also to aspects of its components' functions. The functioning of a part of the system in an improper way will lead to changes in the values of the key indicators of the quality of the system. For example, such attacks can negatively affect the performance of the system or cause incorrect operation of a part.

Responding to malicious influences requires a more complex transformation in the system. It is already required not only to redistribute the functions of a compromised

component (or a set of components), but also to change the processes within the system while maintaining the logic of their implementation. This will require the creation of new network connections functionally symmetrical to those previously in the system (and the destruction of a number of existing ones in order to prevent the spread of malicious impact throughout the entire network infrastructure of the system). Please note that the creation of new network connections will also have performance and quality requirements, and therefore, not all network reconfiguration options will be suitable.

Thus, when receiving a signal about an ongoing attack, it is necessary to have a set of compensatory actions. At the same time, instead of creating an excessive set of options for countering each type of attack, it is more expedient to have at least one option of compensatory action for each type of attack.

Consider an example. Let a distributed attack be carried out on a certain component of the system, in which an attacker sends a large number of specially generated requests to a victim host from different IP addresses, thereby reducing its performance. In terms of operators, the initial graph of the correctly functioning system $G = \langle V, E \rangle$ is transformed; the graph G is mapped to the graph $G\prime$: $G' = \langle V', E' \rangle$. The functionality of the system's component has decreased: $\theta(v_i) > \theta(v_i')$. The task of the immunization mechanism is to preserve the functionality and performance of the system; for this, an appropriate immunization tool should be selected and launched in a certain mode which will ensure the addition of a data conversion node and initiate its communication links with the data parsing node. In terms of the graph model, it looks like this: $V'' \subseteq V \cup \{v_k\}$, $v_k = v_i$, $\theta(v_k) \subseteq \theta(v_i)$.

Here, the generation of defensive action frames was aimed primarily at maintaining the functionality of the component under attack, i.e., the PARAMETERS field of the frame template was of key importance. At first, the functionality of the component was reduced during the attack, and frames were generated to partially redistribute that component's functions among others as it approached its minimum value.

Figure 5 illustrates the state of the component of the system being attacked—before, during and after immunization.

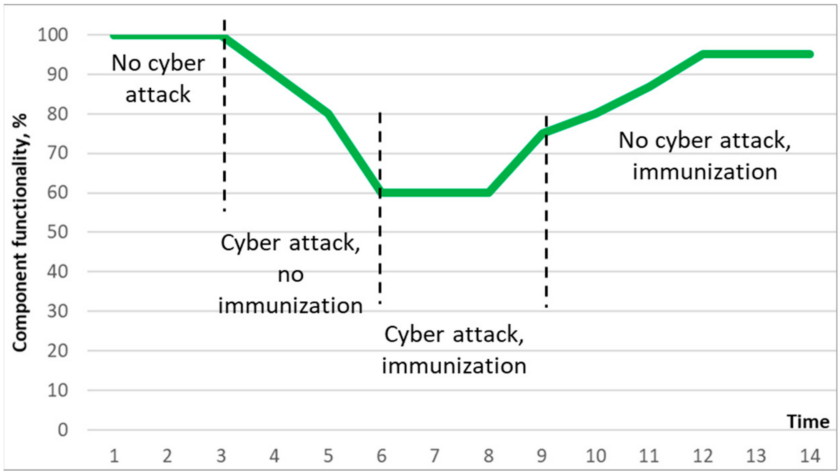

Figure 5. System component state during immunization process.

The evaluation of the experimental results showed that when the attack was implemented and before the immunization process was initiated, the component's performance fell from 100% to 60%, whereas the immunization mode allowed it to contain the destructive impact of the attack and keep the performance at the same level. The 60% uptime lasted for two virtual time stamps, after which there was a jump in performance to 74%—this was because a set of protection frames neutralized the attack and stopped it from spreading through the system. Thereafter, starting at the ninth tact, the system's functionality returned to its previous level and almost reached 95%. This had almost no effect on system

performance, and the 5% decrease was due to a redistribution of functionality between other nodes, resulting in a slight decrease in the data rate to the component.

In practice, such an immunization mechanism can be implemented in the following way: By sending the appropriate command, the virtually available backup node is programmatically activated, and its communication with the victim node and the data conversion node is also programmatically activated. Thus, part of the load is removed from the victim node alongside the gradual transfer of all its functions to the backup node—in case the victim node stops responding to requests.

5. Conclusions

The immuno-like approach presented in this paper is aimed at protecting critical nodes of modern complex systems; it is based on the idea of creating a set of structures and nodes that can be applied to the system for its reconfiguration in order to ensure information security.

The proposed approach is distinguished by the focus on protecting only a certain set of critical system nodes, which is carried out through the use of various immunization techniques, including the use of the mechanism of deceptive systems—honeypots. The approach provides for the generation of defensive action frames, each of which creates a symmetrical response to an attacker's destructive influence when he is attempting to execute a cyber attack. The focus of the approach on a given list of attacks is its distinctive advantage, since it allows critical nodes to be protected from complex targeted attacks.

The novelty of the proposed approach also lies in immunization, by generating a symmetrical response to the attacker based on protective action frames. The convenience of frames is that they rely on a graphical model of the system, and attacks for them are a set of unary operations on the graph modeling the system. Therefore, finding a symmetric response—an inverse unary operation—is quick and can be accomplished by a priori specifying frame patterns. This paper presented a detailed example of completing a frame template for an attack which resulted in two nodes in the system being knocked out.

Experimental results for different types of disruptive attacks showed the effectiveness of immunization, with the primary focus being on "curing" critical nodes in the system. By generating frames, it was possible not only to neutralize the attack quickly, but also to bring the attacked component back to a working state. The results of another simulation are also interesting, showing that even with a mass system node shutdown attack, immunization of critical nodes prevented all components from failing. Thus, the approach proposed in this paper can improve the level of security of today's complex heterogeneous networks.

Author Contributions: Conceptualization, E.P. and D.Z.; methodology, E.P.; software, E.P.; validation, E.P., D.Z. and E.A.; formal analysis, E.A.; investigation, E.A.; resources, E.P.; data curation, E.A.; writing—original draft preparation, E.P.; writing—review and editing, E.P.; visualization, E.A.; supervision, E.P.; project administration, D.Z.; funding acquisition, D.Z. 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 as part of World-class Research Center program: Advanced Digital Technologies (contract number 075-15-2020-934, dated 17 November 2020).

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

References

1. Choraś, M.; Kozik, R.; Flizikowski, A.; Hołubowicz, W.; Renk, R. Cyber threats impacting critical infrastructures. In *Managing the Complexity of Critical Infrastructures*; Springer: Cham, Switzerland, 2016; pp. 139–161.
2. Bécue, A.; Praça, I.; Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artif. Intell. Rev.* **2021**, *54*, 3849–3886. [CrossRef]
3. Wang, C.; Knight, J.C.; Elder, M.C. On computer viral infection and the effect of immunization. In Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC'00), New Orleans, LA, USA, 11–15 December 2000; pp. 246–256.

4. Bahashwan, W.S.; Al-Tuwairqi, S.M. Modeling the Effect of External Computers and Removable Devices on a Computer Network with Heterogeneous Immunity. *Int. J. Differ. Equ.* **2021**, *2021*, 6694098. [CrossRef]
5. Cohen, R.; Havlin, S.; Ben-Avraham, D. Efficient immunization strategies for computer networks and populations. *Phys. Rev. Lett.* **2003**, *91*, 247901. [CrossRef] [PubMed]
6. Yang, L.X.; Yang, X. The impact of nonlinear infection rate on the spread of computer virus. *Nonlinear Dyn.* **2015**, *82*, 85–95. [CrossRef]
7. Upadhyay, R.K.; Kumari, S.; Misra, A.K. Modeling the virus dynamics in computer network with SVEIR model and nonlinear incident rate. *J. Appl. Math. Comput.* **2017**, *54*, 485–509. [CrossRef]
8. Mishra, B.K.; Pandey, S.K. Effect of anti-virus soft-ware on infectious nodes in computer network: A mathematical model. *Phys. Lett. A* **2012**, *376*, 2389–2393. [CrossRef]
9. Upadhyay, R.K.; Singh, P. Modeling and control of computer virus attack on a targeted network. *Phys. A Stat. Mech. Appl.* **2020**, *538*, 122617. [CrossRef]
10. Gan, G.; Yang, X.; Liu, W.; Zhu, Q. A propagation model of computer virus with nonlinear vaccination probability. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 92–100. [CrossRef]
11. Fagan, B. On the Immunization of Small Computer Networks. 2016. Available online: https://www.siam.org/Portals/0/Publications/SIURO/Volume%2010/1.%20ON%20THE%20IMMUNIZATION%20OF%20SMALL%20COMPUTER%20NETWORKS.pdf?ver=2018-01-19-101500-827 (accessed on 7 November 2021).
12. Liu, Y.; Sanhedrai, H.; Dong, G.; Shekhtman, L.M.; Wang, F.; Buldyrev, S.V.; Havlin, S. Efficient network immunization under limited knowledge. *Natl. Sci. Rev.* **2021**, *8*, nwaa229. [CrossRef] [PubMed]
13. Folly, F. Modelling IoT for Immunisation. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, 7–8 October 2021; pp. 1–6.
14. Ädel, L.; Eliasson, O. The Development and Effectiveness of Malware Vaccination: An Experiment. 2020. Available online: http://www.diva-portal.org/smash/get/diva2:1440225/FULLTEXT01.pdf (accessed on 23 November 2021).
15. Anokhin, P.K. Philosophical aspects of the theory of a functional system. *Sov. Stud. Philos.* **1971**, *10*, 269–276. [CrossRef]
16. Anokhin, P.K. Systemogenesis as a general regulator of brain development. *Prog. Brain Res.* **1964**, *9*, 54–86.
17. del Rey, A.M. Mathematical modeling of the propagation of malware: A review. *Secur. Commun. Netw.* **2015**, *8*, 2561–2579. [CrossRef]
18. Zegzhda, D.; Lavrova, D.; Pavlenko, E.; Shtyrkina, A. Cyber attack prevention based on evolutionary cybernetics approach. *Symmetry* **2020**, *12*, 1931. [CrossRef]
19. Fomichev, M.; Álvarez, F.; Steinmetzer, D.; Gardner-Stephen, P.; Hollick, M. Survey and systematization of secure device pairing. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 517–550. [CrossRef]
20. Mandal, N.; Jadhav, S. A survey on network security tools for open source. In Proceedings of the 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), Bangalore, India, 10–11 March 2016; pp. 1–6.
21. Wang, Z.; Zhu, H.; Sun, L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access* **2021**, *9*, 11895–11910. [CrossRef]
22. Mokube, I.; Adams, M. Honeypots: Concepts, approaches, and challenges. In Proceedings of the 45th Annual Southeast Regional Conference, Winston-Salem, NC, USA, 23–24 March 2007; pp. 321–326.