applied sciences

MDPI

Article

Features of the Practical Implementation of the Method for Managing Observations of the State of Monitored Objects in Intrusion Detection Systems

Nikolay V. Boldyrikhin, Olga A. Safaryan *, Denis A. Korochentsev, Irina V. Reshetnikova, Irina A. Alferova and Anastasia N. Manakova

Department of Cyber Security of Information Systems, Don State Technical University,
344000 Rostov-on-Don, Russia
* Correspondence: safari_2006@mail.ru; Tel.: +7-(863)-238-15-18

Abstract: This article discusses the possibility of generalizing the existing methods of optimization of observations to the problems of resource management of intrusion detection systems. The aim of this work is to study the applied aspects of the application of the surveillance optimization method, which increases the efficiency of using the resources of intrusion detection systems. The set goal of the work was achieved through the following tasks: (1) on the basis of experimental data, the development of a dynamic model of the controlled object and the observation model was carried out; and (2) numerical modeling of the solution to the problem of optimizing observations of the state of monitored objects in the intrusion detection system was carried out. As a result of this research, modern approaches to the management of resources of intrusion detection systems have been analyzed. A practical study of the possibility of using the mathematical apparatus for optimizing observations in relation to the problems of resource management of intrusion detection systems has been carried out. The most important scientific findings are as follows: (1) model of the dynamics of the controlled object; (2) model for monitoring the state of controlled objects; and (3) procedure for optimizing the plan for monitoring the state of monitored objects in intrusion detection systems. The significance of the results obtained is confirmed by a numerical experiment, within the framework of which a relative gain in the accuracy of assessing the state of controlled objects of 99.9% was obtained in comparison with a uniform observation plan.

Keywords: intrusion detection system; observation management; observation optimization; filtering; controlled object; dynamic model

check for updates

Citation: Boldyrikhin, N.V.; Safaryan, O.A.; Korochentsev, D.A.; Reshetnikova, I.V.; Alferova, I.A.; Manakova, A.N. Features of the Practical Implementation of the Method for Managing Observations of the State of Monitored Objects in Intrusion Detection Systems. *Appl. Sci.* **2023**, *13*, 1831. https://doi.org/10.3390/app13031831

Academic Editors: Howon Kim and Thi-Thu-Huong Le

Received: 29 December 2022
Revised: 16 January 2023
Accepted: 18 January 2023
Published: 31 January 2023

1. Introduction

In modern society, the role of information technology is constantly growing, as it makes our lives more convenient. These technologies have become firmly established not only in our everyday life but also in almost all spheres of human activity: economic, managerial, social, industrial, scientific, etc. However, along with undeniable advantages, these technologies bring new problems locally and globally. The number of crimes in the field of information technology is growing rapidly [1–25]. Cyberattacks carry a wide range of malicious impacts from the most harmless, such as displaying a banner or playing a sound signal on a local machine, to stealing the confidential data of millions of people. This makes the problem of ensuring information security extremely important [1–25]. There are many software and hardware tools for ensuring the cybersecurity of information systems, an important place among which is occupied by intrusion detection systems (IDS) [2–25]. In modern literature, much attention is paid to the principles of functioning of such systems. In the most general form, intrusion detection systems can be divided into two classes: signature-based intrusion detection systems (SIDS) and anomaly-based intrusion detection systems (AIDS).

The operation of SIDS is based on comparing the current state of a controlled object, for example, a local computer or a network segment, with some sample (signature) of a previously known attack [2,6–9]. Such signatures are sequences of commands, actions that were previously identified as an intrusion. Traditional SIDS inspect network packets and attempt to match them against a signature database that is generated by the IDS developer based on analysis of known intrusions into information systems. Of course, such databases are constantly updated with new signatures, but their major drawback is the ability to detect only known intrusions. They are immune to new, unknown types of attacks.

AIDS have become very popular due to their ability to detect so-called zero-day attacks, i.e., attacks for which signatures cannot be extracted [2,10–23]. These are new types of attacks or attacks using polymorphic technologies, encryption, etc. In AIDS, a "normal" model of information system behavior is formed. Any unacceptable deviation between the behavior of the controlled object and the "normal" model is regarded as an anomaly, which can be interpreted as an intrusion.

Intrusion detection methods in AIDS can be divided into three main groups: methods based on statistics, knowledge-based methods, and machine learning-based methods.

Methods based on statistics include the collection of statistical data and the construction of a model of the "normal" behavior of the information system [2,15,16].

Knowledge-based methods use information about installed software, current protocols, allowed TCP ports, and so on [2,17,18].

Machine learning methods involve the use of complex neural network algorithms, clustering, genetic algorithms, etc. [2,4,19–23].

In AIDS, the Kalman filter can be used to detect anomalies [24,25]. The article [24] states that new types of attacks have been appearing recently, and traditional approaches of detecting them using methods based on statistics are not always effective. The same article presents a method for detecting anomalies based on the use of the Kalman filter. This method proved to be much more effective than traditional methods. The article [25] provides an effective method for using Kalman filtering in hierarchically distributed intrusion detection systems. Thus, the use of the Kalman filter in intrusion detection systems is relevant and promising, since this approach corresponds well to the logic of the problem being solved. The Kalman filtering algorithm shows good results in the presence of a large amount of a priori data about the filtered process. Based on these data, the so-called "reference trajectory" is constructed, which is already used in the a posteriori block. This is consistent with the principles of intrusion detection systems based on statistics, for which a model of "normal" behavior is built based on statistical observations, which is later used to identify abnormal behavior. However, it is much easier to identify anomalies after filtering the information process, since this eliminates the influence of random factors.

A significant reserve for improving the quality indicators of filtering the dynamic trajectory of controlled objects is the optimization of the control of observation processes. At present, there is a well-developed mathematical apparatus for the optimal control of observations, which is used in practice in navigation systems, radar, and information-measuring systems [26–28]. However, at present, there are many technical problems for which this mathematical apparatus could also be successfully used, for example, in communication network monitoring systems, intrusion detection systems, etc. Therefore, within the framework of this article, we will consider the features of applying the classical theory of observation management in AIDS.

There are currently two main directions in the theory of observation management [28]. The first of them is related to the use of static and regression models of the processes being evaluated. The second direction is related to the optimization of observation management in dynamic systems. Dynamic optimization problems of measuring processes are interpreted as problems of controlling the accuracy of Kalman filtration. This interpretation is the most general, since it includes simpler cases corresponding to the theory of planning regression experiments. The noted generality lies in the possibility of including in the dynamic model of the experiment such factors as: the stochastic nature of the information process, the correlation of observation errors, restrictions on the intensity of measurements, as well as a number of other factors, which are either impossible or difficult to account for within the regression model. The more general nature of the planning tasks determines the complexity of their solution in the initial statements. This is explained by the complexity of the model of the observed process described in the case of continuous time by a system of stochastic differential equations. There are several approaches to solving such problems.

The first of them treats the initial optimization problem as a problem of controlling directly the accuracy of the Kalman filter. The accuracy characteristics of the Kalman filter are determined by the a posteriori covariance matrix of estimation errors and described by a nonlinear matrix differential equation (the Riccati equation). This equation defines a "fictitious" dynamic system for which various optimization problems can be formulated [28]. The terminal-type quality criteria are used here. This approach is based on the application of the Pontryagin maximum principle, which provides, according to [28], necessary and sufficient optimality conditions. However, the application of this approach to the synthesis of optimal laws for controlling observations encounters a number of difficulties. This is due to the fact that in order to determine the optimal control functions, it is necessary to solve a matrix nonlinear two-point boundary value problem [28]. Due to the nonlinearity of the Riccati equation, as well as the large dimension of the covariance matrix of estimation errors, the solution of this problem is problematic and requires the use of rather complex numerical methods that do not always have a sufficient degree of convergence.

The second approach [28] is based on the analytical properties of the Riccati equation, the use of which allows for an equivalent transition from the initial nonlinear optimization problems to control problems of a linear dynamic system in phase variables, which is a projection of the so-called Hamiltonian system onto a vector space [28]. For each specific problem and the terminal optimality criterion, the type of projection is determined, that is, the number of Hamiltonian variables sufficient to form the initial criterion. This approach is also based on the application of the Pontryagin maximum principle. It makes it possible to obtain numerical algorithms for constructing optimal observation control laws that have monotonic convergence and allow to build consistently improving measurement strategies.

Of great practical interest is the second approach, which allows us to obtain constructive results when solving problems of optimizing observations. It is this approach that is used in the framework of the studies described in this article.

As part of this research, it is assumed that the intrusion detection system monitors the state of several controlled objects included in the telecommunications network. It is assumed that the Kalman filter is used in the system to improve the quality of the assessment of the state of objects. It should be noted that this article does not consider the issues of filtering and searching for anomalies in the behavior of objects, since they have been researched quite extensively to date. It seems relevant to study the possibility of using the mathematical apparatus for optimizing observations in relation to the tasks of resource management of IDS.

The mathematical formulation of the problem described above is provided in the second section. The general algorithm for solving this problem is also considered there. Later in the article, in the third section, the results of mathematical modeling are presented, confirming the effectiveness of the proposed method of optimizing AIDS resources. The fourth section contains a discussion of the results obtained in the framework of this work. The fifth section summarizes the results and makes a general conclusion.

2. Materials and Methods

2.1. Formulation of the Problem

To develop an AIDS resource management algorithm, it is necessary to complete the following tasks: to develop a model of the dynamics (state) of the set of observed objects; set the observation model; and set the conditions of the optimization problem, i.e., determine the constraints and select the quality criterion.

When solving this problem, it is necessary to synthesize an adequate dynamic model of the information process.

The coordinates of the state vector can be various parameters of the controlled object, such as processor load, RAM usage, file system access, traffic intensity, energy consumption, etc. [25,29].

It is obvious that these and many other parameters of controlled objects are random variables. The random nature of these values may be due to both internal factors related to the processes occurring inside the object of observation, and external. For example, the random response time to an echo request (RTT delay) may be related to both server load (internal factor) and connection speed and channel load throughout from the client to the server. Within the framework of the model, it is advisable to associate internal random factors with formative noise. External random influences affecting the result of measuring the parameters of the controlled object are taken into account in the observation model in the form of observation noise. It should be noted that within the framework of this ap-proach, the formative and noise observations should be Gaussian, which does not corre-spond to the real characteristics of information processes, therefore it is necessary to apply the Gaussian approximation method. This stage should be preceded by a full-scale ex-periment that allows you to identify the real statistical characteristics of the information random process and the observation process.

After constructing state and observation models, the classical apparatus for managing observations can be used to solve the problem. The optimization problem is based on the terminal quality criterion and involves the implementation of an iterative procedure for synthesizing the observation plan [27,28].

In the theory of control of observations, a differential equation of the following form is used as a dynamic model describing the state of a controlled object [27,28]:

$$x_i{}' = S_i x_i + G_i q_i,\ i = 1, 2, \ldots,\ x_i(t_{0i}) = x_{i0}, \tag{1}$$

$x_i = x_i(t) \in R^{n_i}$—the state vector of the i-th object; here and below entry $\bullet'$ means the operation of differentiation with respect to time t, i.e., applied to (1)—$x_i{}' = \frac{dx_i(t)}{dt}$; x_{i0}—Gaussian vector, for which $M[x_{i0}] = x^*{}_{i0}$, ($M[\bullet]$ means the mathematical expectation operation), $M[(x_{i0} - x^*{}_{i0})(x_{i0} - x^*{}_{i0})^T] = D_{i0}$ (operator $(\bullet)^T$ means transpose); t_{0i}—monitoring start time i-th object; $G_i = G_i(t) \in R^{n_i \times v_i}$; $q_i = q_i(t) \in R^{v_i}$—white noise for which $M[q_i(t)] = 0$, $M[q_i(t) q_i{}^T(t - \mu)] = N_{iq}\delta(\mu)$, $\delta(\mu)$—delta function; $N_{iq} \in R^{v_i \times v_i}$—diagonal matrix.

The observation model is described by the following relationship:

$$u = \sum_{i=1}^{I} \gamma_i (C_i x_i + g_i),\ t \in [0, t_f], \tag{2}$$

$u = u(t) \in R^z$; $\gamma_i = \gamma_i(t)$—control function for i-th controlled object; $C_i = C_i(t) \in R^{z \times n_i}$—matrix that specifies the composition of controlled parameters i-th object; $g_i = g_i(t) \in R^{z_i}$—is white Gaussian noise, $M[g_i(t)] = 0$, $M[g_i(t) g_i(t - \mu)^T] = N_{ig}\delta(\mu)$; $N_{ig} \in R^{z_i \times z_i}$—diagonal matrix; I—number of monitored objects in a time interval $[0, t_f]$.

Control functions $\gamma_i(t)$ and matrices C_i satisfy the following restrictions:

$$\begin{aligned} &\gamma_i(t) \in L = \{0, 1\},\ \sum_{i=1}^{I} \gamma_i(t) \in L, \\ &\int_0^{t_0} \sum_{i=1}^{I} \gamma_i(t) dt = t_s \le t_f,\ C_i(t) \in \overline{C}_i(t). \end{aligned} \tag{3}$$

Constraints (3) determine the range of tasks to be solved, i.e., the following calculations correspond to the conditions for the operation of AIDS with a time division of computing resources: at the same time, it can control only one object.

The observation plan is described by the following expression:

$$\{\mathrm{P}_i, i = \overline{1, I}\} = P, \tag{4}$$

$$P_i = \{\gamma_i \in L, C_i \in \overline{C_i}\}.$$

Models (1) and (2) correspond to the Kalman filtering algorithm, which is described by the following analytical relations:

$$\begin{aligned} &{x^*}_i{}' = S_i {x^*}_i + \gamma_i D_i {C_i}^T {N_{ig}}^{-1}[u - C_i {x^*}_i], \\ &x^*(t_{0i}) = {x^*}_{i0}, \end{aligned} \tag{5}$$

$$\begin{aligned} &D_i{}' = S_i D_i + D_i {S_i}^T + Q_i - \gamma_i D_i K_i D_i, \\ &i = \overline{1, I},\ t \in [t_{0i}, t_f],\ t_{0i} \in [0, t_f], \\ &D_i(t_{0i}) = D_{i0}, \end{aligned} \tag{6}$$

$$Q_i = G_i N_{iq} G^T;\ K_i = {C_i}^T {N_{ig}}^{-1} C_i.$$

The statement of the problem of optimization of observation processes in the framework of these studies is based on the use of the *l*-optimality criterion [23]:

$$l = \sum_{i=1}^{I} {m_i}^T D_i(t_f) m_i \to \min_P,\ m_i \in R^{n_i}. \tag{7}$$

Criterion (7) minimizes the sum of errors in estimating the state of controlled objects at the final moment of time.

The optimization problem is to determine the optimal observation plan in terms of the *l*-optimality criterion (7). The use of the terminal criterion (7) within the framework of this problem is quite justified, given that the decision will be made on local time intervals.

Thus, the conditions of the optimization problem are formalized as follows: a generalized model of the dynamics of a set of controlled objects is described by Equation (1); the observation model for a set of controlled objects is described by the Formula (2); the observation plan (4) is determined by control functions that obey the constraints (3); and the quality criterion (7) minimizes the error in estimating the state vector at the final moment of the observation interval.

2.2. Method for Optimizing Resource Management Aids

When solving practical problems, the use of the Riccati Equation (6) is associated with a high computational costs due to nonlinearity and high dimensionality.

In [28], a method was proposed that allows us to proceed to the projection of the Hamiltonian system corresponding to (6) on the space of variables, which has the following form:

$$\begin{aligned} &\alpha_i{}' = -{S_i}^T \alpha_i + \gamma_i K_i \beta_i, \\ &\beta_i{}' = Q_i \alpha_i + A_i \beta_i, \end{aligned} \tag{8}$$

$$\beta_i = \beta_i(t) \in R^{n_i},\ \alpha_i = \alpha_i(t) \in R^{n_i}, D_i \alpha_i = \beta_i, \forall t, t \in [t_{0i}, t_f].$$

In particular,

$$D_{i0} \alpha_{i0} = \beta_{i0},\ i = \overline{1, I}, \tag{9}$$

$$\alpha_{i0} = \alpha_i(t_{0i}),\ \beta_{i0} = \beta_i(t_{0i}).$$

Let us represent criterion (7) in terms of (8) as

$$\hat{l} = \sum_{i=1}^{I} {m_i}^T \beta_i(t_f) \to \min_P, \tag{10}$$

provided that

$$\alpha_i(t_f) = m_i. \tag{11}$$

Thus, the conditions of the optimization problem include a set of fictitious dynamical systems described by two-point boundary value problems (TPBVP) (8), (9), (11), and a quality criterion (10). The algorithm for solving such problems is considered in detail in [28] and includes an iterative procedure of successive approximations. This procedure involves setting an initial observation plan, and its gradual refinement from one iteration to another until the change in value of the optimality criterion becomes insignificant. The observation plan synthesized in this way is considered to be approximately optimal (hereinafter optimal). The iterative procedure itself is not presented in this article; it can be found in detail in [28].

Observation planning is based on the following relations describing program functions $\Lambda_i(t)$ and matrices that determine the optimal composition of the measured parameters $C_i^{opt}(t)$:

$$\Lambda_i(t) = \beta_i^T(t) K_i^{opt} \beta_i(t), \tag{12}$$

$$K_i^{opt}(t) = \left(C_i^{opt}(t)\right)^T N_{ig}^{-1}(t) C_i^{opt}(t), \tag{13}$$

$$C_i^{opt}(t) = \arg \max_{C_i \in \overline{C_i}} \beta_i^T(t) K_i(t) \beta_i(t). \tag{14}$$

The decision rule for constructing an observation plan is described by the formula

$$\begin{array}{l} \gamma_i{}^{opt}(t) = \begin{cases} 1, \ \Lambda_i(t) \geq \varepsilon, \ \Lambda_i(t) \geq \Lambda_j(t), \\ 0, \ \Lambda_i(t) < \varepsilon, \ \Lambda_i(t) < \Lambda_j(t), \end{cases} \\ j = \overline{1, I}, \ j \neq i, \end{array} \tag{15}$$

ε—Lagrange multiplier associated with the limit on the total observation time for all objects $t_s \leq t_f$.

The observation planning algorithm presented above makes it possible to carry out most of the calculations a priori, i.e., it is possible to calculate in advance the observation plan. To do this, it is necessary to obtain statistical data on the parameters of controlled objects, which are assumed to be unchanged. The result of security monitoring will be the determination of the real state in which the controlled object is located at the current time and the determination of the deviation from the "reference" trajectory: whether it is within acceptable limits or not. If not, then AIDS issues a message about a possible invasion.

3. Results

In order to implement the approach to AIDS resource management described above, it is first necessary to collect statistics on the "normal" behavior of each controlled object. Based on these statistics, the so-called "reference" trajectory of the "movement" of the observed object in time is built, while it is assumed that the object is not attacked during the study period. Then, based on the "reference" trajectory as well as data on the intensity of noise, an optimal observation plan is built.

Within the framework of this article, to simplify the computational experiment, only one parameter was used as the trajectory of the observed object: the intensity of network traffic, which changes over time.

To illustrate the process of collecting and evaluating the statistical characteristics of the observed objects, we will use the results of a full-scale experiment, which are shown in Figure 1.

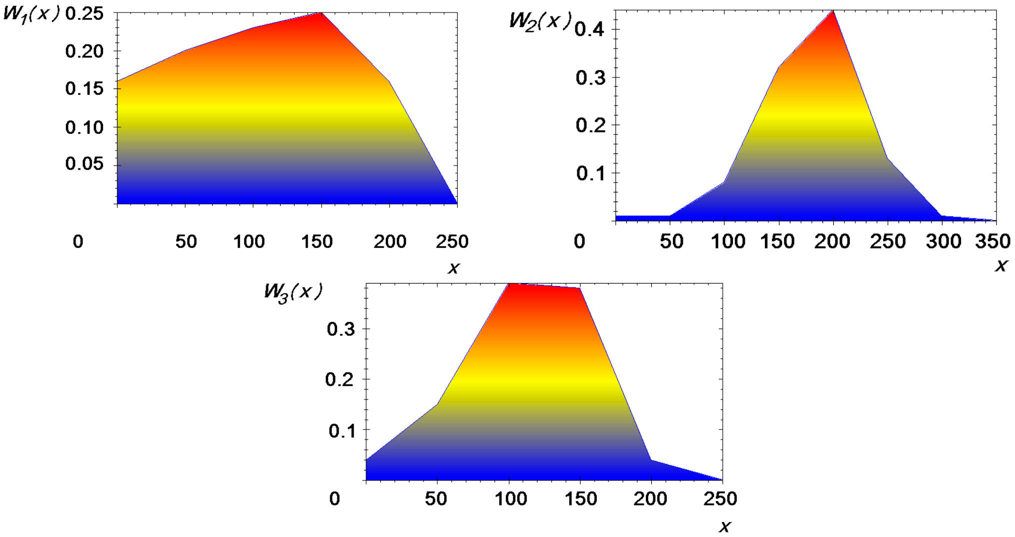

Figure 1. Graphs of the experimental probability density of traffic intensity at fixed times t_1, t_2, t_3.

During the experiment, software developed within the framework of these studies was used. The software tool makes it possible to determine the intensity of traffic passing through the network port of the observed object, calculate the experimental density of the distribution of traffic intensity at fixed points in time, and display them on the screen, as shown in Figure 1. These probability densities may be approximated by a Gaussian distribution.

To obtain an analytical expression describing the dynamics of the observed object within the framework of this work, it is proposed to divide the entire observation interval into local sections and solve the optimization problem separately for each section. In small areas, the instantaneous values of traffic intensity are well approximated by an exponential curve.

In Figure 2, $u_1(t), u_2(t), u_3(t)$—instantaneous values of traffic intensity for the first, second, and third objects, respectively, $x_1(t), x_2(t), x_3(t)$—estimated parameters, show examples of such an approximation obtained using the expfit function of the Mathcad application package. Knowing the exponent parameters $x(t) = be^{S\,t} + c$, the dynamics model of the observed object obtained using expfit can be written in the form

$$x_i{}' = S_i x_i. \tag{16}$$

To simplify calculations, Model (16) does not contain shaping noise, since it has no physical meaning, and the entire random component is taken into account in the observation model. However, in the general case, shaping noise may be present, for example, when observing RTT (round-trip time) delays. Forming noise in this case will be due to data processing processes inside the monitored object, and observation noise will be due to processes occurring in network paths.

The observation model can be written as

$$u = \sum_{i=1}^{I} \quad \gamma_i (x_i + g_i). \tag{17}$$

When simulating the operation of the algorithm, the following restrictions were introduced:

$$\begin{gathered} n_i = 1, C_i(t) \equiv 1, G_i(t) \equiv 1, \\ m_i \equiv m, D_{i0} \equiv D_0. \end{gathered} \tag{18}$$

These restrictions were introduced in order to minimize the computational complexity of the problem, while maintaining the logic of its solution using the example of scalar models of state and observation.

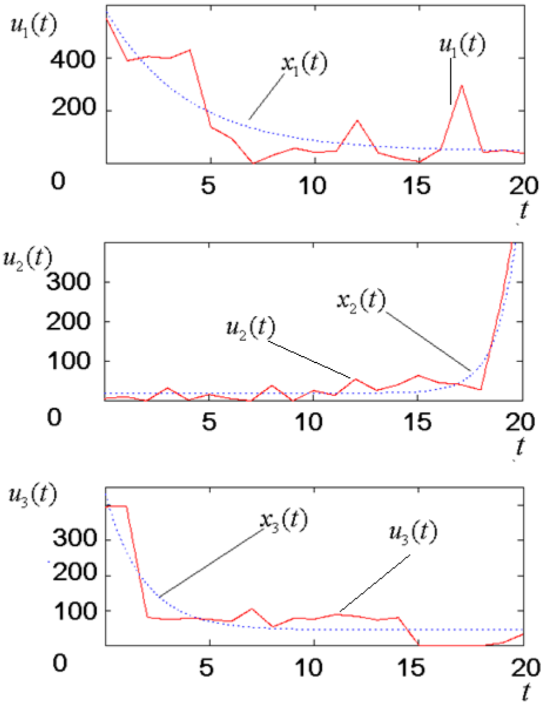

Figure 2. Models of observation of controlled objects.

All quantities given in the example are taken to be dimensionless for simplicity. Equations (6) and (8), taking into account restrictions (18), respectively, take the form

$$D_i{}' = 2S_iD_i - 2\gamma_iD_i^2/N_{ig},\ i = \overline{1, I}, \tag{19}$$

$$\begin{aligned} \alpha_i{}' &= -S_i\alpha_i + 2\gamma_i\beta_i/N_{ig}, \\ \beta_i{}' &= S_i\beta_i, \quad i = \overline{1, I},\ \ t \in [t_{0i}, t_f]. \end{aligned} \tag{20}$$

The quality criterion in the conditions of the example is described by the relation

$$\hat{I} = \sum_{i=1}^{I} m\beta_i(t_f) \to \min_{P}. \tag{21}$$

Relation (12), taking into account (20), takes the form

$$\Lambda_i(t) = [\beta_i]^2/N_{ig}(t). \tag{22}$$

The simulation was carried out with the following initial data:

$$\begin{gathered} S_1 = 1.003, S_2 = -0.258,\ S_3 = -0.55, \\ N_{1g} = 73.896\ ,\ N_{2g} = 139.197,\ N_{3g} = 91.7, \\ \mathrm{D}_0 = 1, m = 0.1, t_f = 20, t_s = 20. \end{gathered} \tag{23}$$

The values of the parameters S_1, S_2, S_3, N_{1g}, N_{2g}, and N_{3g} were determined on the basis of experimental data using the Mathcad program, and the remaining parameters were selected manually to ensure rapid convergence of the iterative procedure for synthesizing the observation plan.

In Figure 3, $\gamma_1(\mathrm{t}), \gamma_2(\mathrm{t}), \gamma_3(\mathrm{t})$—control functions for the first, second, and third objects, respectively—show the initial plan used at the first step of the iterative procedure for finding the optimal plan, which is considered in detail in [23].

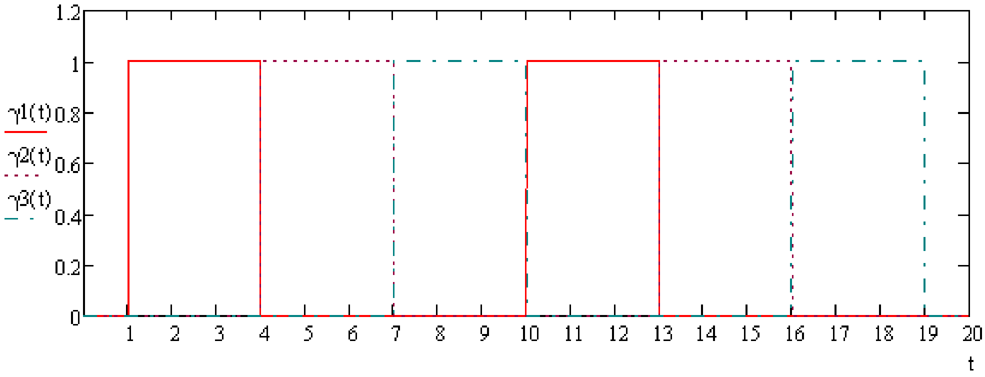

Figure 3. Initial observation plan.

Starting from the third step of the iterative procedure, there are practically no changes in program functions and, as a result, in the laws of control of observations. Therefore, the observation plan obtained at the third iteration can be considered optimal.

The structure of program functions at the third iteration is shown in Figure 4, $\Lambda_1(t), \Lambda_2(t), \Lambda_3(t)$—program functions for the first, second, and third objects, respectively.

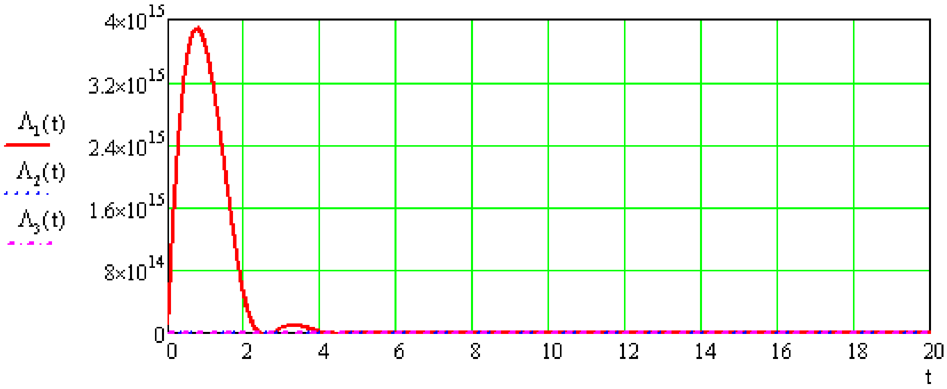

Figure 4. Program functions in the third iteration.

In Figure 5, $\gamma_1(t), \gamma_2(t), \gamma_3(t)$ —control functions for the first, second, and third objects, respectively—show the optimal observation plan. It can be seen from the figure that in this area it is most important to observe the first and second objects from the point of view of the quality criterion. This is since during the iterative procedure, the program function for the second object did not affect the process of forming the observation plan. Observation of the second object can be provided in the next local interval. In the general case, it may happen that too little observation time is provided for an object on the global interval, which is undesirable. This can be avoided by forcibly including the minimum observation time interval for the object, the observation of which is not provided for by the plan synthesized because of the implementation of the iterative procedure for optimizing observations. It is obvious that such "inserts" will reduce the quality of filtration in terms of the accuracy of estimating the state of controlled objects; however, these studies were not carried out within the framework of this work. The accuracy gain was estimated exclusively based on the results of a comparison of the synthesized plan shown in Figure 5 and the uniform plan shown in Figure 3.

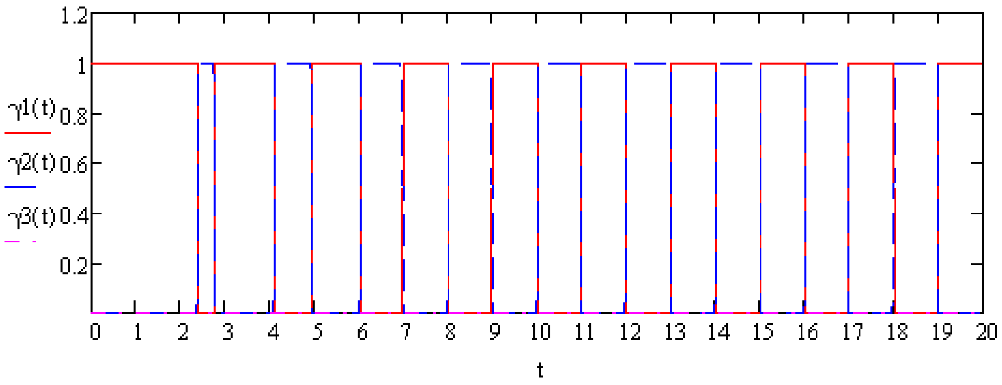

Figure 5. Optimal observation plan.

The absolute value of the quality criterion for the initial plan and for the optimal plan were obtained, respectively, $l^0 = 734.414$ and $l^3 = 9.915 \times 10^{-4}$.

The relative gain is exactly equal to

$$\Delta = \frac{l^0 - l^3}{l^0} \times 100\% \approx 99.9\%. \tag{24}$$

4. Discussion

The authors discussed the results of their research with the involvement of leading experts in the field of observation control theory, monitoring systems, and computer security.

At present, the mathematical apparatus of random processes is used in the description and solution of a large number of theoretical and practical problems in various fields of science and technology. An important place in this series is occupied by tasks described by dynamic models, which are used both in the humanities and in the natural and technical sciences. In technical sciences, such tasks include those related to estimating the motion parameters of moving objects by location and navigation systems, monitoring information systems, describing communication networks, controlling traffic flows, and many other applied tasks. Despite the fact that the mathematical apparatus for solving such problems has been researched quite extensively, the potential for its further development remains very high. New technical problems appear, in which classical approaches can be successfully applied. These tasks include optimization of IDS computing resources.

The scientific novelty of this research lies in the generalization of existing methods for optimizing observations and filtering for a class of practically important problems of optimal resource management of an intrusion detection system, in which these approaches have not been previously employed.

The practical implementation of the research results will help to significantly optimize the distribution of computing resources of the IDS information system, which uses the Kalman filter to filter data. Today, such systems are gradually gaining popularity [24,25]. The approach given in this article for the organization of observations in IDS using the Kalman filter is also of scientific interest.

The results of studies by other scientific groups confirm the effectiveness of using this approach to solving measurement control problems in systems for estimating motion parameters [26–28]. However, the use of the considered mathematical apparatus in optimizing IDS resources also made it possible to obtain high results, which confirmed the effectiveness of this approach.

At the same time, information security experts recommended a more in-depth study of the possibilities of using this approach. Real intrusion detection systems can monitor a large number of parameters: traffic intensity, RTT delays, CPU-cores load, CPU temperature, disk access intensity, number of running processes, RAM consumption, power consumption, etc. Many of them can be approximated by Gaussian processes and can be included in the state vector of the controlled object, and accordingly considered when planning AIDS resources.

5. Conclusions

Thus, the above example made it possible to illustrate the implementation of the proposed iterative procedure for the synthesis of the observation control law in intrusion detection systems, which allows selection of the optimal plan for monitoring the state of controlled objects based on a priori information about them.

The research presented in this article aimed to consider the most general applied aspects of the application of the surveillance optimization method, which increases the efficiency of using the resources of intrusion detection systems. The data and models provided in this article are intended to illustrate the applicability of the method to the simplest example. Even in this case, the task proved to be nontrivial. To implement this method in a real intrusion detection system, a full-scale field experiment is required, involving long-term statistical observation of the intrusion detection system, building a dynamic model of the "normal" behavior of the system based on many parameters, and modeling an abnormal situation. This is planned within the framework of subsequent studies.

It should also be noted that the method discussed in the article allows you to obtain only an a priori or reference observation plan, which needs to be adjusted in real time. The article [30] provides an example of the adaptation of the reference observation plan to the real conditions of the functioning of the network monitoring information system with dy-namic topology. In part, this approach may be applicable to intrusion detection infor-mation systems. However, the peculiarities of the functioning of AIDS require the devel-opment of a new method for adapting the reference plan of observations to the conditions of functioning in real time. This is also planned as part of further research.

Author Contributions: Conceptualization, N.V.B., O.A.S., D.A.K., I.V.R., I.A.A. and A.N.M.; methodology, N.V.B., O.A.S., I.A.A. and A.N.M.; software, N.V.B., I.A.A. and A.N.M.; validation, N.V.B., O.A.S. and D.A.K.; formal analysis, N.V.B.; investigation, N.V.B., O.A.S. and I.A.A.; resources, D.A.K., I.V.R. and A.N.M.; data curation, N.V.B., O.A.S., I.A.A. and A.N.M.; writing—original draft preparation, N.V.B., O.A.S. and D.A.K.; writing—review and editing, N.V.B., O.A.S. and D.A.K.; visualization, I.V.R. and A.N.M.; supervision, N.V.B. and O.A.S.; project administration, N.V.B. and O.A.S.; funding acquisition, O.A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The study did not report any data.

Acknowledgments: Beskopylny Alexey Nikolaevich.

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

References

1. Stallings, W. *Computer Security: Principles and Practice*; Pearson: Boston, MA, USA, 2012; 182p.
2. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 20. [CrossRef]
3. Alazab, A.; Hobbs, M.; Abawajy, J.; Khraisat, A.; Alazab, M. Using response action with intelligent intrusion detection and prevention system against web application malware. *Inf. Manag. Comput. Secur.* **2014**, *22*, 431–449. [CrossRef]
4. Agrawal, S.; Agrawal, J. Survey on Anomaly Detection using Data Mining Techniques. *Procedia Comput. Sci.* **2015**, *60*, 708–713. [CrossRef]
5. Abbasi, A.; Wetzels, J.; Bokslag, W.; Zambon, E.; Etalle, S. On Emulation-Based Network Intrusion Detection Systems. In *RAID 2014: Research in Attacks, Intrusions and Defenses*; Lecture Notes in Computer Science; Stavrou, A., Bos, H., Portokalidis, G., Eds.; Springer: Cham, Switzerland, 2014; Volume 8688, pp. 384–404. [CrossRef]
6. Khraisat, A.; Gondal, I.; Vamplew, P. An Anomaly Intrusion Detection System Using C5 Decision Tree Classifier. In *PAKDD 2018: Trends and Applications in Knowledge Discovery and Data Mining*; Lecture Notes in Computer Science; Ganji, M., Rashidi, L., Fung, B., Wang, C., Eds.; Springer: Cham, Switzerland, 2018; Volume 11154. [CrossRef]
7. Modi, C.; Patel, D.; Borisaniya, B.; Patel, H.; Patel, A.; Rajarajan, M. A survey of intrusion detection techniques in Cloud. *J. Netw. Comput. Appl.* **2013**, *36*, 42–57. [CrossRef]

8. Lin, P.; Lin, Y.; Lai, Y. A Hybrid Algorithm of Backward Hashing and Automaton Tracking for Virus Scanning. *IEEE Trans. Comput.* **2011**, *60*, 594–601. [CrossRef]
9. Díaz-Verdejo, J.; Muñoz-Calle, J.; Estepa Alonso, A.; Estepa Alonso, R.; Madinabeitia, G. On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks. *Appl. Sci.* **2022**, *12*, 852. [CrossRef]
10. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. *ACM Comput. Surv.* **2009**, *41*, 1–58. [CrossRef]
11. Patcha, A.; Park, J.M. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Comput. Netw.* **2007**, *51*, 3448–3470. [CrossRef]
12. Agarwal, B.; Mittal, N. Hybrid Approach for Detection of Anomaly Network Traffic using Data Mining Techniques. *Procedia Technol.* **2012**, *6*, 996–1003. [CrossRef]
13. Padhy, N.; Mishra, P.; Panigrahi, R. The Survey of Data Mining Applications and Feature Scope. *Int. J. Comput. Sci. Eng. Inf. Technol. (IJCSEIT)* **2012**, *2*, 43–58. [CrossRef]
14. Garcia-Teodoro, P.; Diaz-Verdejo, J.; Maciá-Fernández, G.; Vázquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Comput. Secur.* **2009**, *28*, 18–28. [CrossRef]
15. Ye, N.; Emran, S.M.; Chen, Q.; Vilbert, S. Multivariate statistical analysis of audit trails for host-based intrusion detection. *IEEE Trans. Comput.* **2002**, *51*, 810–820. [CrossRef]
16. Viinikka, J.; Debar, H.; Mé, L.; Lehikoinen, A.; Tarvainen, M. Processing Intrusion Detection Alert Aggregates with Time Series Modeling. *Inf. Fusion* **2009**, *10*, 312–324. [CrossRef]
17. Walkinshaw, N.; Taylor, R.; Derrick, J. Inferring extended finite state machine models from software executions. *Empir. Softw.* **2016**, *21*, 811–853. [CrossRef]
18. Studnia, I.; Alata, E.; Nicomette, V.; Kaâniche, M.; Laarouchi, Y. A language-based intrusion detection approach for automotive embedded networks. *Int. J. Embed. Syst.* **2018**, *10*, 1. [CrossRef]
19. Tang, D.H.; Cao, Z. Machine Learning-based Intrusion Detection Algorithms. *J. Comput. Inf. Syst.* **2009**, *5*, 1825–1831.
20. Yoshimura, N.; Kuzuno, H.; Shiraishi, Y.; Morii, M. A Deep Learning-Based Method for Feature Extraction and Anomaly Detection in Network Traffic. *Sensors* **2022**, *22*, 4405. [CrossRef]
21. Elejla, O.E.; Anbar, M.; Hamouda, S.; Faisal, S.; Bahashwan, A.A.; Hasbullah, I.H. Deep-Learning-Based Approach to Detect ICMPv6 Flooding DDoS Attacks on IPv6 Networks. *Appl. Sci.* **2022**, *12*, 6150. [CrossRef]
22. Antunes, M.; Oliveira, L.; Seguro, A.; Veríssimo, J.; Salgado, R.; Murteira, T. Benchmarking Deep Learning Methods for Behaviour-Based Network Intrusion Detection. *Informatics* **2022**, *9*, 29. [CrossRef]
23. Saridou, B.; Rose, J.R.; Shiaeles, S.; Papadopoulos, B. SAGMAD—A Signature Agnostic Malware Detection System Based on Binary Visualisation and Fuzzy Sets. *Electronics* **2022**, *11*, 1044. [CrossRef]
24. Meng, A.; Wang, H.; Aziz, S.; Peng, J.; Jiang, H. Kalman Filtering Based Interval State Estimation For Attack Detection. *Energy Procedia* **2019**, *158*, 6589–6594. [CrossRef]
25. Liu, J.; Wuxia, Z.; Ma, T.; Tang, Z.; Xie, Y.; Gui, W.; Niyoyita, J.P. Toward Security Monitoring of Industrial Cyber-Physical Systems via Hierarchically Distributed Intrusion Detection. *Expert Syst. Appl.* **2020**, *158*, 113578. [CrossRef]
26. Khutortsev, V. Local optimization of trajectory control of observations for mobile digital direction-finder in the location of discrete sources of radiation system. *Autom. Control Comput. Sci.* **2016**, *50*, 211–219. [CrossRef]
27. Khutortsev, V.V.; Svizhenko, A.A. Lokal'no optimal'noye upravleniye nablyudeniyami za puassonovskimi potokami fil'truyemykh protsessov [Locally optimal control of observations of Poisson flows of filtered processes]. Izvestiya RAN: Teoriya i sistemy upravleniya. *J. Comput. Syst. Sci. Int.* **2010**, *3*, 33–39. (In Russian)
28. Malyshev, V.V.; Krasil'shchikov, M.M.; Karlov, V.I. *Optimizatsiya Nablyudeniya i Upravleniya Letatel'nykh Apparatov. [Optimization of Observation and Control of Aircraft]*; Mashinostroenie: Moscow, Russia, 1989; 312p.
29. Liu, T.; Sun, Y.; Liu, Y.; Gui, Y.; Zhao, Y.; Wang, D.; Shen, C. Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for Smart Grid attack detection. *Future Gener. Comput. Syst.* **2015**, *49*, 94–103. [CrossRef]
30. Razumov, P.; Boldyrikhin, N.; Cherckesova, L.; Safaryan, O.; Reshetnikova, I.; Beryoza, A. Specific features of the practical implementation of observation planning in systems for monitoring networks with dynamic topology. *E3S Web Conf.* **2020**, *224*, 01033. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.