DEVELOPMENT OF MODELS FOR DESCRIBING THE PROCESSING OF ENVIRONMENTAL INFORMATION IN SECURITY PROBLEMS OF CONTROLLING A PROTECTION SYSTEM BASED ON PETRI NETS

Ibrokhimali Normatov, Inomjon Yarashov, Bekzod Boboqulov
National university of Uzbekistan named after Mirzo Ulugbek

Abstract
The study is devoted to the description of the protection system as a set of applications based on the Petri net. The main difficulty in managing the safety of such systems lies in the processing of a large amount of environmental information about the state of the object, possible threats and the formation of management actions. This article proposes the use of Petri nets to describe the processes of processing environmental information during the functioning of the elements of the protection system. The structural-logical model of the system is presented as a hypergraph. The elements of the structural-logical model of the protection system are presented in the form of control points (CP). Which are divided according to their functions: detection point (DP), access point (AP), observation point (OP), delay point (DeP) and controls represented by authorization and authentication managers (AzM, AcM). Models for environmental information processing of the following elements of the protection system have been developed: abnormal motion analyzer, logical manager, general manager, universal control unit.

© 2019 Hosting by Central Asian Studies. All rights reserved.

Introduction
The protection system (PS) is a set of organizational, legal and regulatory solutions aimed at detecting, repelling and eliminating various kinds of threats to the system [1-8]. Modern protection systems are complex systems of environmental information, including subsystems for monitoring and audit, access control and management, cyber security alerts, etc. The environmental information interconnection of individual elements of the PS is carried out by building such systems based on Petri nets. Managing such an environmental information system[9-14] is an extremely difficult task, due to the need to process a large amount of information about the state of the system and emerging threats, the necessary actions to manage security. Considering the degree of importance and ubiquity of protection systems for various objects (from
an environmental information system to objects of increased danger of information attacks[15-18]: protection systems, systems for preventing data loss, data identification, etc.); It is necessary to build such an environmental information system that will provide the fastest and most effective protection of the object. To solve the problems of security management[19-22], it is necessary to develop models for processing information about the environment, based on the logical connections of the elements of the system that arise when a particular threat occurs. Currently, there is no mathematical model of the protection system that takes into account and optimally uses resources in the process of functioning of the protection system. To describe the processes of interaction of elements, it is proposed to use models based on Petri nets.

**Main part**

The protection system is a set of programs that includes:

- security and control subsystem;
- access control subsystem;
- subsystem of monitoring and audit;
- subsystem of temporal integration and dynamic events;
- auxiliary subsystems (granting privileges, emergency protection, etc.) [3,4].

Modern complex protection systems are built on the basis of Petri nets of various levels of complexity [5].

As a rule, a typical complex of integrated protection includes:

1. Central security control point, server with a common security control panel and identifiers or automatic protection.
2. Security managers connected to the Petri net.
3. API connected to security managers.
4. API for various purposes.
5. Connection managers, authentication manager, etc. [6,7].

The complexity of managing the security of such a system lies in the processing of a large amount of input information about the environment and the need to form security management actions that are optimal for the current situation. To organize effective system security management, a detailed mathematical description of the processes of the elements functioning is necessary.

To build a mathematical model, it is necessary to abstract from the physical nature of the elements that make up the protection system. The elements of the lower level in the structural-logical model of the protection system can be represented as control points (CP), which may include several protection tools that perform one common function. Security control points are divided by functions: detection point (DP), access point (AP), observation point (OP), delay point (DeP) [8]. System security controls are represented by authentication and authorization managers (AzM,AcM).

The developed models of environmental information processing in the protection system should take into account the logic of interaction between elements of various subsystems. Such models can be most fully described using the hypergraph apparatus, which has the following advantages:

- Displays many-to-many relationships;
- each vertex of the hypergraph can be expanded into an independent graph or hypergraph as the model is refined and complicated;
- the hypergraph model allows you to build optimization procedures;
- a hypergraph can be considered as an arbitrary set of subsets, applying to them further the possibilities of graph theory [6,9].
Let's imagine the protection system as a hypergraph (Fig. 1):

\[ H = \{V, E\} \]  \hspace{1cm} (1)

where \( V \) is a set of vertices, which are separate structural and logical elements of the protection system 
\[ V = \{V_1, V_2, ..., V_n\}. \]

\( E \) - a set of edges representing information relationships between individual elements of the protection system
\[ E = \{E_1, E_2, ..., E_n\} \]

Each edge \( E \) of graph \( H \) can be described as a subset of vertices:
\[ V_j = \{1, 2, ..., D\} \]

Where, \[ E_1 \in V \]

When representing the security system of an ecological information system as a hypergraph, each edge \( E \) of the hypergraph \( H \) corresponds to some nested scheme of inter-network processes as an element of the sub-network architecture.

A route in a hypergraph will be a sequence of \( vH = \{V, E\} \)s of the form:
\[ V_1, E_1, V_2, E_2, ..., E_n, V_n, V_i \in V, i \in [0, n] \]

where \[ E_i \in E, (V_i, E_i) \in l, i \in [1, n] \]  \hspace{1cm} (3)

As a result of decomposition, the hypergraph model of the protection system can be represented as subprocesses of the functioning of individual elements. For the description of which it is proposed to use Petri nets, the peculiarity of which is the possibility of displaying parallelism, asynchrony of processes in the system and the hierarchy of its elements [6,10-13].

At the initial stage, models were developed for processing environmental information in the process of functioning of such elements of the protection system as: analyzer, authentication manager, general manager, universal control unit.

Fig 1. Fragment of the hypergraph of the security system[23]
Below is a description of the Petri net of the analyzer operation process (Fig. 2) with the possibility of independent decision-making on notification; and the corresponding transmission of actuation data to the control panel at the session level of the ISO/OSI model. The analyzer is working properly.

The conditions for the existence of the connection will be:
1. connect the analyzer to the network;
2. authorization of the analyzer at the security control;
3. work of the analyzer in standby mode;
4. hacker found;
5. hacker notification;
6. return to normal analyzer operation;
7. exclusion of the analyzer from the protection system (shutdown of the system).

Events for the network:
1. receiving and sending initialization packets;
2. received information about the hacker;
3. notice;
4. warning information;
5. the analyzer returns to work;
6. termination of the connection.

**Fig 2. Description of the analyzer operation process in the form of a Petri net[24]**

Position p1 means that the analyzer is enabled.

Position p2 will mean that the analyzer is processing the session setup packet. A small manager in position p3 means that the analyzer is working, that is, receiving data, and in position p4 it processes the received data.

The small manager in position p5 means that the unit is in an alarm state.

The p6 position will be summed up. Here the amount of incoming information will be accumulated. And the position itself is characterized by a security control panel.

And the last little manager in p7 means that the analyzer is done.

t1 - receiving a packet from the authentication and authorization manager;
t2 - sending the packet back;
t3 - the analyzer sends data to the authentication and authorization manager, which, in turn, passes them through the main manager to the security control unit;

t4 - hacker not found and switched to normal operation;

t5 - a hacker has been found and information is being transferred;

t6 - the notification stops and switches to normal operation;

t7 - receiving a packet about the end of the session level and turning off the analyzer.

Extended input function I and output function O are defined.

\[ C = (P, T, I, O), \]

\[ P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}, \]

\[ T = \{t_1, t_2, t_3, t_4, t_5, t_6, t_7\}, \]

\[ I(p_1) = \{0\} I(p_2) = \{t_1\} \]

\[ I(p_3) = \{t_2, t_6, t_4\} I(p_4) = \{t_5\} \]

\[ I(p_5) = \{t_5\} I(p_6) = \{t_5\} I(p_7) = \{t_7\} \]

\[ O(p_1) = \{t_1\} O(p_2) = \{t_2\} O(p_3) = \{t_3\} \]

\[ O(p_4) = \{t_4, t_5, t_7\} O(p_5) = \{t_6\} O(p_6) = \{0\} \]

\[ O(p_7) = \{0\} \]

\[ I(t_1) = \{p_1\} I(t_2) = \{p_2\} I(t_3) = \{p_3\} \]

\[ I(t_4) = \{p_4\} I(t_5) = \{p_4\} \]

\[ O(t_1) = \{p_2\} O(t_2) = \{p_3\} \]

\[ O(t_3) = \{p_4\} O(t_4) = \{p_3\} \]

\[ O(t_5) = \{p_5, p_6\} O(t_6) = \{p_3\} O(t_7) = \{p_7\} \]

Let’s analyze the Petri net on the basis of matrix equations. An alternative to the definition of the Petri net in the form \((P, T, I, O)\) is the definition of two matrices \(D^+\) and \(D^-\), where \(D = D^+ - D^-\) is a composite matrix of changes. Each matrix has \(m\) rows (one per transition) and \(n\) columns (one per position). \(D^- [j, i] = (pj, I(tj))\), and \(D^+[j, i] = (pj, O(tj))\) are defined. \(D^-\) defines transition inputs, \(D^+\) - outputs.

\[
D^- = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 
\end{bmatrix}
\]

\[
D^+ = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 
\end{bmatrix}
\]

\[
D = \begin{bmatrix}
-1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & +1 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & +1 & 0 & 0 & 0 \\
0 & 0 & +1 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & +1 & +1 & 0 \\
0 & 0 & +1 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & +1 
\end{bmatrix}
\]
In the initial marking $\mu = (1,0,0,0,0,0)$ the transition $t_1$ is allowed and leads to the marking $\mu'$, where

$$\mu' = (1,0,0,0,0,0) + (0,1,0,0,0,0) \cdot 
\begin{bmatrix} 
-1 & +1 & 0 & 0 & 0 & 0 \\
0 & -1 & +1 & 0 & 0 & 0 \\
0 & 0 & -1 & +1 & 0 & 0 \\
0 & 0 & +1 & -1 & 0 & 0 \\
0 & 0 & 0 & -1 & +1 & 0 \\
0 & 0 & +1 & 0 & 0 & +1 \\
\end{bmatrix} = 
\begin{bmatrix} 
0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}$$

Next (Fig. 3) is a fragment of the reachability tree of the imitation model of the analyzer.

![Fig 3. Fragment of the reachability tree of the imitation model of the analyzer][25]

The triggering of transition $t_6$ leads to the accumulation of tokens of position $p_6$. This model describes how the analyzer works under normal conditions, when a message about a hacker may appear. The analyzer accumulates information about the number of operations in the cycle of its work.

Further (Fig. 4) the model of the Petri net of the functioning of the authentication and authorization manager at the session level of the OSI/ISO model is presented.

The conditions for the existence of the network will be:

1. the presence of a security control unit;
2. the presence of one or more analyzers connected according to the structures;
3. the presence of a hacker;
4. correct connection of the working authentication and authorization manager to the protection system;
5. the same developer (eliminates the problem of unit incompatibility at the program level).

The events for such a system would be:
1. connecting the unit to the system;
2. establishing a connection session and maintaining it;
3. receiving a information about the analyzer operation;
4. connection interruption information.

The above conditions and events are required to simulate the operation of authentication and authorization manager. In this model, did not rule out a malfunction of the security control unit. All connection for the security control unit is via the default security manager.

Position p1 will mean that the authentication and authorization manager is in the off state, but connected to the system. Position p2, respectively, will be the state of waiting for receiving packets about the establishment of a connection session.

Position p3 will characterize the state of the analyzer as the state of the formation of a packet about the notification of the absence of a connection session with the analyzer and its subsequent sending to the security control unit.

Position p4 will be characterized by the fact that the authentication and authorization manager makes a decision and attempts to establish a connection session (initialization) with the security control unit.

A small manager in position p5 will mean that the authentication and authorization manager has established a connection session with both the analyzer and the security control unit.

Position p6 is characterized by the fact that the analyzer has switched to normal operation and is ready to receive packets from the analyzer.

A small manager in position p7 means that the authentication and authorization manager is waiting for an acknowledgment response packet, and after the specified waiting period has elapsed.

Position p8 will characterize the state of the authentication and authorization manager as waiting for a response from the analyzer and security control unit.

The small manager at position p9 will mean that the security block is framing a packet to the security control block about the operation of the analyzer(s).

Position p10 is characterized by the fact that the authentication and authorization manager processes the received packet from the security control unit.

The small manager at position p11 means that the authentication and authorization manager is disabled.

Fig. 4. Description of the process of operation of the authentication manager in the form of a Petri net[24]
t1 - sending a packet to establish a communication session of the analyzer and initialization on the security control unit and the main dispatcher.

t2 - reception of packets from the successful establishment of a communication session with the control unit and analyzers.

t3 - receiving a packet from the analyzer about the successful establishment of a connection session, but not receiving a packet from the security control unit about confirming the connection establishment (initialization of the authentication and authorization manager).

t4 - receiving a successful connection packet from the security control unit, but not receiving a packet from the analyzer.

t5 - successful establishment of a communication session with the security control unit.

t6 - the authentication and authorization manager is included in the operator for its main work.

t7 - Send a retry session setup packet to the security control unit.

t8 - the authentication and authorization manager maintains a connection session with the analyzer by sending it an empty packet, and receives an empty packet from the main manager.

t9 - receives an empty packet from the analyzer and sends its packet to the manager.

t10 - receiving a packet from the analyzer about its work.

t11 - the authentication and authorization manager sends data to the security control unit and returns to its work.

t12 - receiving a packet from the security control unit about the end of the communication session with it.

t13 - the authentication and authorization manager sends a message about the end of the communication session with the analyzer.

The definition of input and output functions, network analysis based on matrix equations were carried out similarly to the analyzer model.

Also, models of the main security manager and the universal security control unit were obtained, as well as the process diagrams of the blocks in the form of Petri nets (Fig. 5 and Fig. 6).

---

**Fig 5. Description of the process of operation of the main security manager in the form of a Petri net[24]**
Fig 6. Description of the process of operation of the universal security control unit in the form of a Petri net[24]

Conclusion

The undoubted advantage of Petri nets is the mathematically rigorous description of the model. This makes it possible to analyze them with the help of modern information technologies and use complex environmental information systems in safety management. For this, models of information processing have been developed in the process of functioning of such elements of the protection system as: action analyzer, authentication and authorization manager, general manager, universal unit manager. In the future, it is planned to develop a general hypergraph model for the interaction of elements of the protection system, taking into account possible threats. The resulting models provide the possibility of automated analysis, allow you to move from one level of detail of the system description to another (by opening / closing transitions) and can be used in the future to organize an intelligent system for protecting environmental information.

The use of models based on Petri nets in the security system will improve the quality of security management. For example, it is possible to more clearly coordinate the interaction of elements in the attacked zone, identifying, taking into account possible relationships between them, highlighting the most important tasks of the system depending on the current situation.

References


