Telecommunications and Radio Engineering, 68(3):269-275 (2009)

On a Model of Shielding of Mutually Correlated Corporate Information Spaces Using Petri Nets

R. G. Shykhaliev

Institute of Information Technologies, National Academy of Sciences, Azerbaijan, Baku, Azerbaijan

ABSTRACT: A model of shielding of mutually correlated corporate information spaces (MCCISs) is proposed. Modeling is based on Petri nets (PNs). PNs are well suited for modeling MCCIS shielding systems which prescribe the policy of access control based on filtration rules. The constructed model can be used to simulate and test an MCCIS shielding system and check the correctness of the security policy of the latter. The model can also be used as the basis for designing MCCIS shielding system analysis means.

The development of a uniform state-controlled corporate information space and its integration into the global information space is a precondition for organization of information society in any country. Therefore, the development of mutually correlated corporate information spaces (MCCISs) is very significant.

MCCIS means a territorially distributed filtration structure representing an integrity of mutually correlated and interacting corporate information spaces (CISs) based on uniform corporate standards which ensures access to user information through their authorities, irrespective of their CIS. In the context of information security, every CIS has its own security policy.

The defining factor in the development of MCCISs which deserves special attention is the ensuring of information security. To solve this problem, it is necessary to create an environment within the MCCIS that would ensure protection of the corporate information space and information resources and enable users to safely operate information resources, irrespective of their CIS. The means enabling such an environment is a firewall (FW). Usually, a

ISSN 0040-2508

FW is located between two nets with different security policies, monitoring all information streams passing through it.

The main task of the FW is to suppress attempts of unauthorized access (UA) to the protected net and perform the following functions:

- access control;
- keeping records of information stream;
- concealing the protected net topology; and
- responding to UA.

These tasks are described in [1–3] in detail. Taken together, the fulfillment of these tasks makes the FW complete.

Shielding of MCCISs is achieved by installing FWs in points of connection of the given CIS to public information spaces (such as Internet) and other CISs. Shielding is the FW function which enables maintaining safety of the inside information space facilities, ignoring unauthorized requests from the outside information space.

The main elements for describing MCCIS shielding are:

- information packages (information traffic);
- information interaction subjects;
- information interaction objects;
- filtration rules (the list of conditions which are used, together with the set filtration criteria, to allow or disallow further transmission of packages and the list of actions performed by FWs to register and/or perform additional protection functions); and
- filtration criteria (parameters, attributes and characteristics which are the basis for allowing or disallowing further transmission of the package according to the specified access differentiation rules (filtration rules)).

Despite the fact that FWs are widely used to ensure CIS information security, it must be emphasized that many issues related to the organization and design of the system for shielding such distributed information spaces as MCCISs remain unresolved, since MCCISs require a shielding strategy that should substantially differ from strategies used in individual CISs. Based on the above, shielding of MCCISs presupposes the solution of a series of basic problems, including analysis of correctness of the security policy implemented by FWs, description of FW functionalities, formalization of the shielding process, etc.

The article is devoted to the issue of formalization of the MCCIS shielding process. In formalizing the MCCIS shielding process, it is appropriate to use Petri net (PN) properties, which enables the solution of the shielding process modeling and analysis problem.

STATEMENT OF THE PROBLEM

Irrespective of the FWs used for shielding MCCISs, shielding is defined, primarily, by the set of packages U and the set of filtration rules R (CIS security policies).

Assuming that $R = \{r_1, r_2, ..., r_n\}$ is the set of filtration rules and $\underline{U} = \{u_1, u_2, ..., u_m\}$ is the set of packages. For every filtration rule $r_i \in R$, $i = \overline{1, n}$ the set of input and output packages, processed by this rule, was specified, i.e., the matrix of filtration rules and packages interconnections was set. It is required to represent the MCCIS shielding process by means of the PN, specified by the set $N = \{P, T, F, W, M_0\}$.

THE MCCIS SHIELDING MODEL

Petri nets is the set

$$N = \{P,\ T,\ F,\ W,\ M_0\},$$

where

P is the nonvacuous finite set of states;

T is the nonvacuous finite set of transitions;

$F : P \times T \to \{0, 1\}$, $W : T \times P \to \{0, 1\}$ are incidence functions;

$M_0 : P \to \{0, 1, 2, ...\}$ is the PN initial marking [4].

Graphically, the PN is presented in the form of an oriented graph. The set of the graph apexes forms the set $P \cup T$. The state apex p and the transition apex t are connected by the arc (p, t), if $F(p, t) = 1$, and the arch (t, p), if $W(t, p) = 1$. The state apexes are marked by non-negative integers and in case of a graphical PN imaging by the respective number of marking points.

If all states of the net are designated sequentially by symbols $p_1, p_2, ..., p_n$, then the marking is represented by an n-dimensional vector M whose coordinates are equal to the number of marking points in respective states.

Functioning of the PN represents transition from one marking to another. Change of markings occurs as a result of operation of one of the transitions. The transition t can operate for the marking M, if

$$M(p) - F(p, t) \geq \forall p \in P. \qquad (1)$$

This means that every input state of transition t is marked by, at least, one marking point.

After operation of some transition t, meeting condition (1), the marking M is replaced:

$$M: \forall p \in P, \; M'(p) = M(p) - F(p, t) + W(t, p),$$

i.e., when a transition operates, one marking point is removed from each of its input state and one marking point is added to each of its input state. In this case, it is stated that the marking M precedes M' and the designation $M \xrightarrow{t} M'$ is used.

Functioning of the PN can be presented in the form of a reachability graph whose apexes are individual net markings. Two apexes M and M' of the reachability graph are connected by the arc marked by the symbol t, if $M \xrightarrow{t} M'$.

To represent the MCCIS shielding process by means of a PN, we shall, firstly, assign to each package $u_j \in U$, $j = \overline{1, m}$ the apex of the state p_j of the PN N. Let us designate the set of the states p_j as P, $P = \{p_j, j = \overline{1, m}\}$.

Each filtration rule $r_i \in R$, $i = \overline{1, n}$ shall be assigned the transition t_i of the net. Let us designate the set of transitions as T, $T = \{t_i, i = \overline{1, n}\}$. Meeting the conditions of the filtration rule r_i corresponds to the operation of the transition t_i.

According to the matrix of interconnections between rules and packages, we shall connect by arcs the elements of the sets P and T, i.e., establish interconnections between elements of these sets. The element $p_j \in P$, $j = \overline{1, m}$ is connected with the element $t_i \in T$, $i = = \overline{1, n}$ by the arch (p_j, t_i), if the package $u_j \in U$, $j = \overline{1, m}$ is the input package of the rule $r_i \in R$, $i = 1, n$, and by the arch (t_i, p_j), if it is the output package for the rule $r_i \in R$, $i = \overline{1, n}$. Since the MCCIS package can be the input package for several filtration rules, then to restore the marking points of the state $p_j \in P$, $j = \overline{1, m}$ following the operation of the transition $t_i \in T$, $i = \overline{1, n}$ it is also required to build arcs (t_i, p_j) for such t_i and p_j for which the arc (p_j, t_i) exists.

Functioning of the PN is determined at every time instant by the location of the marking points in the state apexes. The transition $t_i \in T$, $i = \overline{1, n}$. can operate, if all of its input states $p_j \in P$, $j = \overline{1, m}$ for which the arc (p_j, t_i) exists, has, at least, one marker.

Let us define the initial marking of the constructed PN. The packages that are not output packages for any of the filtration rules are called input packages of the MCCIS shielding system. Each state of the PN, correspon-

dent to the input package of the MCCIS shielding system, is marked by a marking point. The thus obtained vector M_0 is the initial marking of the net.

Thus, the model for MCCIS shielding can be formalized by means of a PN specified by the set $N = \{P, T, F, W, M_0\}$, where $P = \{p_j, j = \overline{1, m}\}$ is the set of the net states (MCCIS packages), and $T = \{t_i, i = \overline{1, n}\}$ is the set of the net transitions (package filtration rules);

$$F(p, t) = \begin{cases} 1, \text{ if the state } p \in P \text{ is connected} \\ \text{with the transition } t \in T \text{ by the arc } (p, t); \\ 0, \text{ otherwise;} \end{cases}$$

$$W(t, p) = \begin{cases} 1, \text{ if the transition } t \in T \text{ is connected} \\ \text{with the state } p \in P \text{ by the arc } (p, t); \\ 0, \text{ otherwise;} \end{cases}$$

$M_0(p) = \{0/1\}$, $\forall p$ is the initial marking of the net.

When PN transitions operate, the initial marking changes. Assuming that the marking M_l can be achieved from the marking M_k. Then $M_k \le M_l(p)$, i.e., $\forall p \in P$, $M_k(p) \le M_l(p)$. This follows from the fact that for any transition $t_i \in T$, $i = \overline{1, n}$ the condition $\forall p \in w(t_i) : F_k(p, t_i) = W_l(t_i, p) = 1$ is fulfilled.

The finite marking M_z shall be such PN marking for which $M_z(p) > 0$, $\forall p \in P$. Such marking corresponds to the end of operation of the PN or the end of the package filtration.

Any path in the reachability graph, leading from the initial marking to the end marking, is called a possible path. The possible path meeting all restrictions on the operation of the shielding system and, hence, on the operation of the PN is called a permissible path.

Now we shall define the type of the PN constructed for modeling the MCCIS shielding system. In shielding MCCIS, each filtration rule operates once; therefore, PN transitions operate once. Each package (state) is the result of operation of one filtration (transition) rule. For the initial marking of the net, each of its input state is marked by only one marker, i.e., $\forall p \in P$: $M_0(p) \le 1$.

Let us analyze a random state of the PN p. As is known, the number of marking points in the state p, when the transition t operates, changes according to the following rule:

$$M'(p) = M(p) + W(t, p) - F(p, t).$$

If change of the marking occurs during operation of transition t for which the state p is the input state (i.e., $F(p, t) = 1$), then the number of marking points in the state p does not change, since in this case $W(t, p) = 1$ according to the PN structure. However, if the state p is the output state for the transition t, then the number of marking points increases by one. Since such transition is the only one for the state p and it operates once, then $M'(p) = 1$. If the state p is not connected with the transition t, then $W(t, p) = 0$ and $F(p, t) = 0$ and, hence, $M'(p) = M(p)$. Thus, the constructed PN, simulating operation of the MCCIS shielding system, is safe.

The problem of recognition of PN vitality and safety is rather complicated, since this solution is related to great computational difficulties caused by construction and viewing of the reachability graph.

In order to verify that the PN simulating operation of the MCCIS shielding system is operable, we suggest the following algorithm.

1. To define the initial network marking, i.e., to build the vector M_0, $i = 0$.

2. If all coordinates of the vector M_i are equal to one, go to item 6; otherwise go to item 3.

3. To define the set of net transitions T_i, such that $t \in T_i$, if $\forall p \in w(t)$: $M_i(p) > 0$.

4. If $T_i = \varnothing$, go to item 7; otherwise go to item 5.

5. $M_{i+1} = M_i$. Change the marking of the net M_{i+1} as follows:

$$\forall p \in \bigcup_{t \in T_i} f(t) : M_{i+1}(p) = 1, \quad i = i + 1.$$

Go to item 2.

6. The Petri net is defined as operable. Shutdown.

7. The Petri net is not operable. Shutdown.

Thus, if the required set of filtration rules and packages is selected correctly at the stage of preliminary analysis, the PN simulating this MCCIS shielding system is correct.

CONCLUSIONS

In formalizing the MCCIS shielding process, we used PN properties that enable the solution of the problem of modeling and analysis of such process. Petri nets used as the theoretical basis provide the developers means for description, construction, simulation and analysis of MCCIS shielding systems.

The model based on PN can be the principal instrument to prove the MCCIS shielding system compliance with the given security policy. Besides, this model can be used to simulate and test MCCIS shielding systems and verify the correctness of the security policy implemented by the system. This model can also be used as the basis for designing means for analysis of MCCIS shielding systems.

REFERENCES

1. Alguliev, R. M. and Shykhaliev, R. G. *Metody i tekhnologicheskie aspekty ekranirovaniya vzaimouvyazannykh korporativnykh informatsionnykh prostranstv* (Methods and Technological Aspects of Shielding of Mutually Correlated Corporate Information Spaces). Elm Press, Baku, 2003.
2. Ogltree, T. *Prakticheskoe primenenie setevykh ekranov* (Firewalls. Practical Application), DMK Press, Moscow, 2001.
3. Pallman, N. and Crathers, T. *Arkhitektura brandmauerov dlya setei predpriyatii* (Architecture of Firewalls for Corporate Nets), Williams Publishing House, Moscow, 2003.
4. Kotov, V. E. *Seti Petri* (Petri Nets), Nauka Press, Moscow, 1984.