Journal of Engineering Science *Vol. XXVI, no. 3 (2019), pp. 38 - 53*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

DOI: 10.5281/zenodo.3444051
CZU 004.056.53:519.711

PERFORMANCE MODELING OF NETWORK DEFENSE IN BREADTH SYSTEMS BY MATRIX REWRITING SRN WITH FUZZY PARAMETERS

Emilian Guțuleac*, ORCID ID: 0000-0001-6839-514X
Sergiu Zaporojan, ORCID ID: 0000-0001-5928-4229
Victor Moraru, ORCID ID: 0000-0002-5454-8341
Alexei Sclifos

Technical University of Moldova, 168 Stefan cel Mare bvd., MD-2004 Chisinau, Republic of Moldova
*Corresponding author: Emilian Guțuleac: *emilian.guțuleac@calc.utm.md*

Received: July, 04, 2019
Accepted: September, 22, 2019

Abstract. We have defined in this paper, a new kind of stochastic reward network (SRN) by introducing matrix attributes and fuzzy parameters of timed transitions and of rewriting rules, called MFRSRN, allowing the dynamic marking-dependent reconfiguration of these models. Moreover, this formalism offers a descriptive language that allows managing the compact representations the model's size through the introduction of matrix structuring and rewriting mechanisms of the compositional model's behavior. As an example of application, we show how the proposed formalism can be applied to performance modeling of network "Defense in Breadth" system which includes the combination of firewall, IDS, honeypot and moving target defense (MTD) techniques, taking into account the probabilistic and epistemic uncertainty aspects.

Keywords: *attack, cyber-security, evaluation, fuzzy number, honeypot, moving target defense, reconfiguration, stochastic reward net.*

1. Introduction

Currently computer networks (CNs), embedded computing systems, information systems and control systems with interconnecting components and increasing interconnection have become a key infrastructure in different fields of applications, where the information security of CNs is constantly confronted with seriousness severity of challenges. Some of the major causes of these situations are that the current configurations of CN security systems are typically deterministic, static and homogeneous [1]. These features reduce attackers' difficulties in identifying specific targets by scanning CN vulnerabilities, in accessing essential information, which gives attackers asymmetrical advantages in developing, launching and spreading attacks, and defenders are always disadvantaged by their late reaction.

In order to ensure the better security and availability of the CN, a variety of defense techniques have been proposed and developed, among which the most common are: firewalls [2]; the intrusion detection systems (IDS) [3]; honeypots [4] and Moving Target Defense (MTD) [5 - 7]. As a first line of defense, the firewall protects CN against intruders. However, the firewall very rarely can identify the attacks of the allowed services [2]. Therefore, it is easy for attackers to bypass the firewall and to penetrate into the CN. IDS is a well-known technique of security analysts in order to detect intrusions and misuse of CNs. However, it is well known that IDS-based defense has the following limitations [3]: (1) it activates a lot of false alarms; (2) it has a minor effect on the prevention or on the protection against intrusions; (3) it has a limited capacity to detect the malicious traffic in real time, thus gives to many false negative alarms.

While IDS has played a key role in cyber security, new proactive defense techniques, known as intrusion prevention techniques, have recently emerged that target the shortcomings of using IDS. To this end, intrusion prevention techniques (honeypot deceptive and MTD) have been introduced to control the actions of the attackers, as a proactive defense that can be implemented independently or combined with other defense techniques. Although deception techniques are used to mitigate the attacks success, they also have some limitations [6], including: they incur additional costs; it increases the likelihood that they will be detected by the attacker as he experiences them more over time, thus enhancing the knowledge of the deception detected as part of a "fraud" attack against a defender.

In order to create difficulties and increase the uncertainty of launching a successful CN attack, innovative proactive MTD defense techniques have been proposed and used which continuously change the area of the attack, resulting in increased effort (i.e. cost and time) [6] when carrying out the attack. For example, SW - a new server software variant, DPT - new properties of its processing platform, NAS - the system changed its network address [7]. The key features of MTD have been described in several existing papers [5-7]. Thus, frequent changes of the attack surface increase the attacker's uncertainty about the behavioral characteristics of the attack target and, thus, make it difficult to identify and exploit system vulnerabilities and greatly reduce the probability of an attack being successful.

Not oblivious to the fact that the MTD approach offers a wide range of techniques to mitigate a wide range of cyber-attacks of CN, some limits on their use have been mentioned and discussed in the literature [6]. Some MTD techniques are better at dislocating the attack compared to others, depending on the target of the attacker, which is often unknown. Also, the use of MTD leads to new costs associated with maintaining the performance of CN systems and may affect the availability of services or computing performance and / or network connectivity [6].

Designing a CN security system based on the above-mentioned defense techniques is a complex task, in which a large number of parameters must be taken into account. The influence of these parameters is often mutually opposite, often uncertain and weakly predictable. This situation is explained by the fact that it is necessary to organize the protection not of the network as such, but of the network with all the computer systems that work into and which contain many components. And because all of these factors affect the ability to perform certain attacks, building a CN protection system with a specified level of security and performance that fully takes them into account is a very daunting task. It should also be mentioned that, at present, the cyber security of the CN cannot be ensured or maintained through the use of only one defense technique [8-9]. Therefore, a combined collection of defense techniques is needed that can collaborate and complement each other to cope with sophisticated attacks. This type of defense, called “Defense in Breadth” [8], refers to defense based on several techniques and mechanisms to counter more sophisticated attack classes.

In this context, we need to model the behavior of the attackers; the defense strategies and we need also to evaluate some quantitative QoS (Quality of Service) characteristics of the CN security system and their ability to fulfill the mission within a set time frame and in the presence of intruder attacks [10]. When designing a model that describes the operation of a security system, it is necessary to select specific formalisms, methods and tools according to the specific requirements to this system, i.e. the objectives, risks, quality indicators of services, etc., as well as the incompleteness and uncertainty of the information regarding the behavior of the attackers.

Modeling and simulating the interaction of attackers and CN defense have been a great topic for several decades. However, the modeling, evaluation and quantitative analysis of CN information security have only recently attracted more attention of reseachers. We mention here only some relevant bibliographic sources recently published, based on mathematical models that use different formalisms and approaches to evaluate the security mechanisms [11 - 22]. They can be grouped according to the similarity of the used approaches, being created based on different mathematical formalisms: continuous time Markov chains (CTMC) [17, 18]; attack tree [20]; theory of mathematical games [14, 22]; Petri net (PN) extensions [12, 15, 16, 19, 21], such as stochastic reward nets (SRN) [23] and generalized stochastic PN (GSPN) [24], which reflect their different behavioral aspects. The differences between these models consist in the parameters used as input and in which performance characteristics of the modeled system are evaluated. CTMC and mathematical games can be used only for modeling a small class of random attack and defense interaction processes with a small state space, because these kind of models can only be built manually and there are some problems with their validation.

SRN and GSPN allow describing the dynamics of the change of system states, to automate the process of building the underlying LMTC with a very large state space and to evaluate some QoS indicators.

However, in this type of models, the reconfigurability and the fuzzy epistemic uncertainties of the attacker's and defense's behavior are not taken into account. It is also easy to confirm from experience that ordinary SRNs (or GSPNs) [23, 24] are often difficult to use in practice due to the problem of rapidly increasing the graphical size of the model to describe the behavior of a real system. In this context, it is necessary to improve the SRN formalism in order to fully represent more compactly and flexibly the models that describe complex stochastic processes.

At the same time, the activities of the attackers and the defenses have to be represented by probability distributions of the possible actions and activities of attack in each state of the model based on the use of fuzzy numbers.

The uncertainty of epistemic evaluation of the attack risk is related to the imprecise and incomplete character of the information due to the lack of knowledge about the real values of the parameters of the defense mechanisms and of the attackers who dynamically change their states.

This can be achieved by defining a new fuzzy SRN extension (FSRN), based on which you can build compact graphical models with reconfigurability issues and some quantitative parameters may be fuzzy numbers.

In this paper a SRN matrix rewriting model (MFRSRN) with fuzzy parameters is developed and analyzed for the evaluation of the QoS indicators of a security system, “Defense in Breadth” [8] type, of the CN integrated with firewall, IDS and intrusions prevention techniques (i.e., honeypot and MTD), where quantitative parameters are considered fuzzy numbers.

2. Matrix rewriting SRN with fuzzy parameters

2.1. Elements of fuzzy sets , fuzzy numbers and credibility theory

SRNs are an important formalism that describe the dynamic phenomena under random uncertainty. However, in the real world we often encounter difficult problems that cannot be addressed by using only the theory of stochastic processes. To deal with such complex problems, Liu in [25] have proposed the credibility theory (CT), which is a branch of mathematics for studying the behavior of systems with fuzzy phenomena. The measure of credibility is the degree of trust given to a certain data set, to an occurrence of events, to some fuzzy variables, etc. The purpose of the credibility theory is to efficiently combine information from various sources: previous and current data, data on individual and collective risk, rates of attacks and defenses, etc. [25].

The theory of fuzzy sets and concepts with fuzzy numbers [26 - 28] appears from the need to express quantitatively the imprecise quantities, in which range of values taken by the function of belonging is no longer limited to two values, but it is extended to the whole interval [0, 1].

To facilitate the exposition of the proposed approach, in this subsection we present some basic elements of fuzzy sets, trapezoidal fuzzy numbers (TrFN) [26] and some elements of CT required defining SRNs with fuzzy parameters.

Let X be the set of discourse. Then a fuzzy subset of X is a function $\mu : X \to [0, 1]$ and it is denoted by $\mu_{\widetilde{X}}$. A fuzzy subset $\mu_{\widetilde{A}}$ is called a fuzzy number if A is a subset of the set of real numbers and there exists at least one real number *x* such that $\mu_{\widetilde{A}}(x) = 1$.

Two types of fuzzy numbers are most commonly found in real applications: trapezoidal numbers and triangular numbers. The use of these types of fuzzy numbers is more appropriate, one reason being the computing complexity.

Definition 2.1. A fuzzy number is said to be a TrFN if its membership function is given by the expression (2.1):

$$\mu_{\widetilde{A}}(x) = \begin{cases} 0 & if\ -\infty < x \le a \\ (x-a)/(b-a) & if\ a \le x < b \\ 1 & if\ b \le x \le c \\ (x-d)/(c-d) & if\ c < x < d \\ 0 & if\ d \le x < \infty \end{cases}$$

Definition 2.2. A TrFN $\widetilde{A} = (a, b, c, d)$ is said to be zero (respectively non-negative) iff $a = 0, b = 0, c = 0, d = 0$ (iff $a \ge 0$). Also, two TrFNs $\widetilde{A} = (a_1, b_1, c_1, d_1)$ and $\widetilde{B} = (a_2, b_2, c_2, d_2)$ are said to be equal i.e., $\widetilde{A} = \widetilde{B}$ iff $a_1 = a_2, b_1 = b_2,\ c_1 = c_2, d_1 = d_2$.

Note that the triangular fuzzy number (TFN) $\widetilde{A} = (a, b, d)$ is a particular case of TrFN $\widetilde{A} = (a, b, c, d)$ if $b = c$.

Let Θ be a nonempty set, and $Bag(\Theta)$ is its description power that is the set of all subsets of Θ. Each element of $Bag(\Theta)$ is called an event. For each element $A \in Bag(\Theta)$, a credibility measure $Cr\{A\}$ is defined that expresses the chance of occurrence a fuzzy event

A [25]. The triplet (Θ, Bag, Cr) is called the credibility space, and a fuzzy variable ξ is defined as a function (measurable) at this space on the set of real numbers IR. According to [25], the membership function $\mu_{\xi}(x)$ of a measurable fuzzy variable ξ at space (Θ, Bag, Cr), is derived from the credibility measure as follows:

$$\mu_{\xi}(x) = (2Cr\{\xi = x\}) \wedge 1,\ x \in IR,$$

and for any set $B \in IR$ of real numbers we have:

$$Cr\{\xi \in B\} = (\sup_{x\in B} \mu_{\xi}(x) + 1 - \sup_{x\in B^c} \mu_{\xi}(x))/2 .$$

The average value $\bar{\xi} = E[\xi]$ of ξ is determined by the following relation [25]:

$$E[\xi] = \int_0^{+\infty} Cr\{\xi \ge x\}dx - \int_{-\infty}^{0} Cr\{\xi \le x\}dx .$$

According to [25], based on this expression and the membership function $\mu_{\xi}(x)$ of a trapezoidal fuzzy variable ξ at $[a,b,c,d]$ on $0 \le a < b < c < d$ which determines a fuzzy number $\widetilde{A} = (a, b, c, d)$, we obtain the relation: $\bar{\xi} = E[\xi] = (a+b+c+d)/4$.

This expression will further to be used to determine the parameters of the credible parameters of an FSRN or MFRSRN model.

2.2. Definition and behavior of matrix rewriting SRN with fuzzy parameters

In order to model more realistically the uncertainty of the attackers' behavior and the defense reaction of the security system, it is necessary to consider both probabilistic and fuzzy aspects [28]. As already mentioned, this fact can be achieved by defining a new extension of SRN in which some quantitative attributes may have fuzzy values. This enhancement allows the compact modeling of high complexity discrete event systems (SED) through MFRSRN, without the risk of having a very complicated graphical FRSRN model, too difficult to represent and difficult to understand.

Let IN_{+} and IR_{+} are sets of nonnegative natural and nonnegative real numbers, respectively. The definition of an MFRSRN is derived according to [29 -31] and inherits most of the SRN [23] and GSPN [24] characteristics. In a MFRSRN model, the matrix attributes of objects (arcs, places capacities, guard functions and transition priorities, rewriting rules, firing rates of transitions etc.) of the specified type z, depending on the current state of the network, are defined by a set of matrix $A^z = [a^z_{ij}(s)]_{k\times n} \in \mathbf{A}$. The values of the network attributes may be constant, variable, or functions of the specified type and may depend on the current state of the MFRSRN networks.

The size $k\times n$ and location of the current element $a^z_{ij}(s)$ of the matrix A^z is specified by a set $P^z_A \subset P$ of net control places. For example, for the matrix specifications A^z and the current location of its elements, two control locations should be set. Therefore, the current number of tokens $i = m_l = M(p_l)$ and $j = m_v = M(p_v)$ in control places p_l and p_v shows the position of the respective element of matrix A^z, and its values must be imported and taken into account when executing and analyzing the model. Furthermore, the capacity of the control places $p_l \in P^z_A$ and place $p_v \in P^z_A$ should be specified respectively.

Definition 2.3. The MFRSRN, denoted$MR\Gamma$, is specified as a 13-tuple system such that $MR\Gamma$= < P, T ,R, ϕ ,A_{rcs}, *Pri*, G^E, G^R, M_0, $\widetilde{\Lambda}$, $\widetilde{W}$, $\widetilde{\rho}$, Lsp >, where:

- P is the finite set of places, $|P|= n \neq 0$. A place $p_i \in P$ is drawn with a circle and can contain a number of tokens $m_i = M(p_i) \in IN_+$ (*local state*). The current *marking* (*global state*) M of the $MR\Gamma$ is a vector-column, describing the contents value of each place, respectively;
- T is a finite set of transitions, $|T|= k \neq 0$,$P \cap T = \varnothing$, which is partitioned into $T = T_0 \cup T_\tau$, $T_0 \cap T_\tau = \varnothing$ so that: T_τ is a set of timed transitions (drawn as black rectangles) and T_0 is a set of immediate transitions (drawn as tin bar);
- R is a finite set of rewriting rules, $|R|= k_R \neq 0$ which is partitioned into $R = R_0 \cup R_\tau$, $R_0 \cap R_\tau = \varnothing$ so that: R_τ is a set of timed rewriting rules (drawn as embedded empty rectangles) and R_0 is a set of immediate rewriting rules (drawn as embedded empty tin rectangles) about the runtime structural change (reconfiguration) of net, so that $P \cap T \cap R = \varnothing$. We let $E = T \cup R$ denote the set of *events* of the net; $\phi : E \to \{T, R\}$ is the function that indicates for every rewriting rule the type of event can occur;
- A_{rcs}= < *Pre*, *Post*, *Test*, *Inh* > is a set of forward, backward, test and inhibition functions, that describes the respectively arcs with matrix marking-dependent weight cardinalities;
- *Pri* defines the dynamic matrix marking-dependent priority function for the firing of each event$e \in E$. The firing of an event with higher priority potentially disables all event $e \in E$ with the lower priority. By default, the *Pri*(E_0)>*Pri*(E_τ);
- $G^E : E \times IN_+^{|P|} \to$ {*True*, *False*} is the set of matrix *guard function* associated with all event$e \in E$ and $G^R : R \times IN_+^{|P|} \to$ {*True*, *False*} is the set of matrix *guard function* associated with all *rewriting rule* $r \in R$. For$\forall r \in R$, the $g^E(M) \in G^E$ and$g^r(M) \in G^R$ will be evaluated in each current marking and if they are evaluated to *True*, the rewriting rule *r* is *enabled*, otherwise it is *disabled*. Default value of $g^E(M)$ is *True* and for $g_r(M)$ it is *False*;
- $M_0$is the initial marking of net. Graphically, the initial marking is represented by writing the value of $m_i^0 = M(p_i)$inside the corresponding placep_i . If the number m_i^0 is small it is common to draw m_i^0 tokens inside the placep_i , represented by black dots. A missing value indicates zero tokens;
- $K^p : P_D \times IN_+^{|P|} \to IN_+ \cup \{\infty\}$ is the matrix capacity bound $0 < K_i^p < +\infty$ of each place $p_i \in P$, which can contain an *integer* finite number of *tokens*. By default and K_i^p it is unlimited;
- $\widetilde{\Lambda} : E_\tau \times IN_+^{|P|} \to IR^+$ is the function that determines the matrix fuzzy firing rate $0 < \widetilde{\lambda}(e,M) < +\infty$ (the parameters of exponential-negative law) of timed event $e \in E_\tau$, that is enabled by current marking M ;
- $W : E_0 \times IN_+^{|P|} \to IR^+$ is the matrix fuzzy weight function $0 \leq w(e,M) < +\infty$ which deter-mines the firing probability $q(t,M)$ of immediate event $e \in E_0$, enabled by current marking M , therein describes an probabilistic selector;
- $\widetilde{\rho} : P \cup E \to IR^+$ is a matrix reward rates (real numbers) assigned to each current marking M and to each firing event $e \in E$;

- Lsp is the set of $MR\Gamma_v$, $v = 1, 2 \cdots, n_v$ subnet pattern class library involved in structural reconfiguration of the current $MR\Gamma$configuration by firing of an enabled rewriting rule$r \in R$.

Figure 1 summarizes the graphical representation of all $MR\Gamma$ primitives.

Let be $RN = < R\Gamma, M >$ is the current configuration of $MR\Gamma$, where $R\Gamma = <$ P, T ,R, A_{rcs}, *Pri*, G^E, G^R, $\widetilde{\Lambda}$, $\widetilde{W}$, $\widetilde{\rho}$> and M is the current marking of $MR\Gamma$.

A dynamic reconfiguration of *RN* by the firing of enabled rewriting rule $r \in R$ is a map$r$: $RN_L \triangleright RN_W$, where $RN_L \in Lsp$ subnet and $RN_W \in Lsp$ subnet are the left-hand side and the right-hand side of the rewriting operator$\triangleright$ assigned to rewriting rule$r$, respectively. The rewriting operator, $\triangleright$, represents a binary operation which produces a *structure change* in *RN* by replacing (rewriting) the fixed current subnet $RN_L \subseteq RN$ ($RN_L$are dissolved with $P_L \subseteq P$, $E_L \subseteq E$ and subset of arcs $A_L \subseteq A$) and a new $RN_W \in Lsp$ subnet (with$P_w \subseteq P$,$E_w \subseteq E$ and set of arcs A_W) belongs to the new modified resulting underlying net $RN' = (RN \setminus RN_L) \cup RN_W$ with $P' = (P \setminus P_L) \cup P_W$ and $E' = (E \setminus E_L) \cup E_W$, $A' = (A - A_L) + A_W$ where the meaning of \ (and $\cup$) is operation of removing (adding) RN_L from (RN_W to) *RN.*

In this new RN' net, obtained by the execution of the enabled$r \in R$, the places and the events with the same attributes which belong to$RN'$are fused. By default, the rewriting rules $r : RN_L \triangleright \varnothing$ or $r : \varnothing \triangleright RN_W$ describe the rewriting rule which maintains $RN' = (RN \setminus RN_L)$ or $RN' = (RN \cup RN_W)$. So, a current state configuration of a *RN* net is the pair ($R\Gamma, M$), i.e. the current structure configuration $R\Gamma$ of the net together with a current marking *M.* Also, the pair $(R\Gamma_0, M_0)$ with$P_0 \subseteq P$,$E_0 \subseteq E$ is the initial configuration. *Enabling and firing of events* and *rewriting rules* are the same as for reconfigurable GSPN presented in [31].

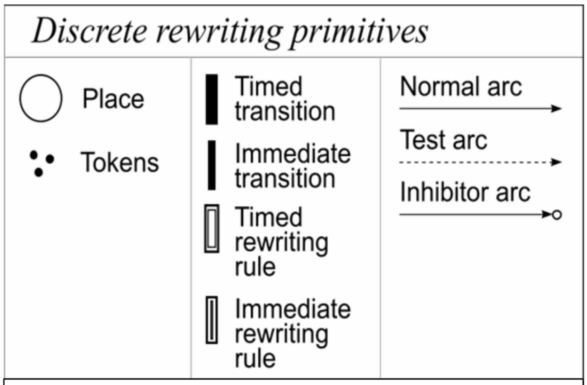

Figure 1. Graphical representation of all $MR\Gamma$ primitives.

Let the $T(M)$ and $R(M)$, $T(M) \cap R(M) = \varnothing$, be the set of enabled transitions and rewriting rules in current marking *M*, respectively. Let the$E(M) = T(M) \cup R(M)$, be the set of enabled events in a current marking *M.* The event $e_j \in E(M)$fires if no other event $e_k \in E(M)$ with higher priority has been enabled. Hence, for e_j event ***if*** $((\phi_j = t_j) \vee (\phi_j = r_j) \wedge (g^R(r_j, M) = False))$ $(g^R(r_j, M) = False))$ ***then*** the firing of $t_j \in T(M)$ or of $r_j \in R(M)$ changes only the current marking: $(R\Gamma, M) \xrightarrow{e_j} (R\Gamma, M') \Leftrightarrow (R\Gamma = R\Gamma$and $M[e_j > M'$ in$R\Gamma$)).

Also, for the every event $e_j \in E$ *if* $((\phi_j = r_j) \wedge (g^R(r_j, M) = True))$ *then* the event e_j occurs at firing of the rewriting rule r_j and it changes the configuration and marking of the current net, such that: $(R\Gamma, M) \xrightarrow{r_j} (R\Gamma', M')$, $M[r_j > M'$).

The accessible state graph configuration of a net $RN=<R\Gamma,M>$ is the labeled directed graph whose nodes are states and whose arcs, which are labeled with events or rewriting rules of RN , are of two kinds:

a) *firing* of an enabled event $e_j \in E(M)$: arcs from state $(R\Gamma,M)$ to state $(R\varGamma,M')$ labeled with event e_j, so that this event can fire in the configuration $R\varGamma$ at marking M and leads to a new marking:

$$M':(R\varGamma,M)\xrightarrow{e_j}(R\varGamma',M')\Leftrightarrow(R\varGamma=R\varGamma' \text{ and } [M[e_j>M' \text{ in } R\varGamma);$$

b) *change configuration*: arcs from state $(R\Gamma,M)$ to state$(R\varGamma,M')$ labeled with the rewriting rule $r_j \in R$, $r_j:(R\Gamma_L,M_L)\triangleright R\Gamma_W,M_W$ which represent the change configuration of current *RN* net: $(R\varGamma,\ M)\xrightarrow{r_j}(R\varGamma',\ M')$ with $M[r_j>M'$.

The operating rules of the network models and the method of analyzing their behavioral properties are similar to those of the GSPN or SRN models, described in [23, 24]. The difference refers to identifying the firing rates of enabled events.

Thus, we first identify the firing rates (resp. weights) of the enabled timed (resp. immediate) events, which are represented as TrFN and / or TFN. Using the respective fuzzy values of these rates (resp. weights), the model is analyzed by running it in a flat SRN model, for which the Markov chain is equivalent to the fuzzy Markov chain of the original model. In this paper we will consider only models in which all the structural attributes have implicit sizes, and the capacity of all places is equal to 1.

3. MR*Γ*-based performance modeling of network defense in breadth systems

In this paper, we assume that if a single CN node is compromised and exploited by an attacker, the entire security system fails. This harsh security condition is used to evaluate the level of integrated defense of the security system equipped with honeypot, IDS and MTD techniques. To model through **MR*Γ*** the process of serving the packets, the attacks and the defense of a CN node we will adopt the following assumptions [4, 8, 12]:

- The attacker has a finite set of exploits of the vulnerabilities depending on the interaction between the attacker and the software stack of the security system of the CN target nodes;
- An attacker can detect with imperfect knowledge whether a CN node of interest has a vulnerability or not. That is, he knows with some degree of certainty whether the accessed node can be exploited to affect the security system, which can lead to system compromise. He may also, with a certain probability, detect the frauds committed;
- An attacker can learn from his past experience, including from his failure experiences. Thus, the attacker becomes more intelligent on the basis of this learning, which reduces the time to compromise the security system;
- RC has a firewall, honeypot and IDS mechanisms, used by a distributed security system in which each node must detect malicious intruder activities. The IDS is triggered adaptively at a certain time in proportion of the detected attacks, the IDS also learn from past attacks;
- The MTD mechanisms are applied according to periodic rules of modification and displacement of the attack area only in the process of serving the requests and the occurrence of the time-out expiry event or when a security alert appears. Different types of MTD mechanisms can be chosen in different rounds of service, but only one can be used in each round.

The construction of $MR\Gamma$ model, which describes the behavior of the attacker interaction, exploiting the vulnerabilities of a given CN and the defense of this network through "Defense in Breadth" mechanisms, based on the integrated combination of the techniques presented above, is performed using the method described in [8].

In order to show the advantage of using the approach described in this paper, we will first present a FSRN1 model, built in the traditional form [23], which describes the behavior of the attacker interaction exploiting the vulnerabilities of a given CN node and of the defense of this node through "Defense in Breadth" mechanisms [8], based on the integrated combination of firewall, honeypot, IDS and MTD techniques. Then we will show how to build a $MR\Gamma$model based on FSRN1.

Figure 2 shows such a FSRN1 model in which, in order to give graphic visibility to this type of model, only 3 firewall rules and 3 MTD techniques are considered, namely: SW, DPT and NAS. In order to describe in the GSPN1 model the on-line switching of the MTD security mechanisms, 2 timed transitions t_{18}, t_{19} are used to reproduce the time-out times of change (modification) and use of the proactive MTD security techniques.

In this model the places (resp. transitions) correspond to the locale states (resp. events, actions, activities) of the attacker and of the CN security system.

The meanings of the places, transitions and rewriting rules of the model FRSN1*are*:

• **Places**: p_1 - normal state of the CN, it is not attacked; p_2 - an CN node is attacked, the firewall is activated; p_3 - IDS has triggered a security alert; p_4 - the arrived packet is malicious; p_5, p_6, p_7 - the intruder packet bypass the firewall (with k_{r1} specified rules); p_8 - IDS activates the verification of the legitimacy of the packet data; p_9 - IDS did not trigger a security alert, the honeypot trap is activated; p_{10} - the intruder is trapped in the honeypot trap; p_{11} - the intruder bypassed the honeypot trap; p_{12} - CN is available to provide services; p_{13} - the user accesses the node resources; p_{14} - activation of the timer that measures the time-out; p_{15} - the time-out period has expired (control place for the application of the MTD mechanisms); p_{16} - the CN node server is free; p_{17} - selecting the activation of one of the type of TMD defense mechanisms; p_{18}, p_{19}, p_{20} - the respective MTD mechanism is selected, changed and activated: SW - a new variant of server software, DPT - new dynamic properties of its processing platform, NAS - the system has changed its network address; p_{21}, p_{22} - processing end of the node request in which the respective SW, DPT and NAS mechanism is used; p_{23} - requesting to be served normally; p_{24} - initiating the release of computing resources and testing the server; p_{25} - reconnecting the user to the server; p_{26} - initiation of isolation of the intruder when switching TMD; p_{27} - the intruder packet is removed when changing a current TMD mechanism.

• **Timed transitions**: t_1 - the occurrence of an attack; t_4 - the intruder bypasses the honeypot trap; t_6 - restoring the normal operating regime; t_7 - the activity of processing and rejecting the malicious package by the firewall; t_8, t_9, t_{10} - the respective activities for executing firewall rules as a result of which the intruder bypasses the firewall; t_{11} - detection of the intruder by the IDS; t_{12} - the intruder bypasses the IDS; t_{13} - the intruder falls into the trap of honeypot; t_{14} - recovery of the normal CN regime as a result of the intruder falling into the honeypot trap; t_{15} - the intruder bypasses the honeypot trap; t_{16} - access of users by RC; t_{18}, t_{19} - the time-out of change (modification) and use of proactive MTD security mechanisms; t_{23}, t_{24}, t_{25} - the time delay of the respective MTD mechanisms established in the RC: SW - a new variant of server software, DPT - new dynamic properties of its processing platform, NAS - the system has changed its network address; t_{29} - processing of the current application; t_{30} - CN provides the requested service; t_{34} - removing the intruder from the network.

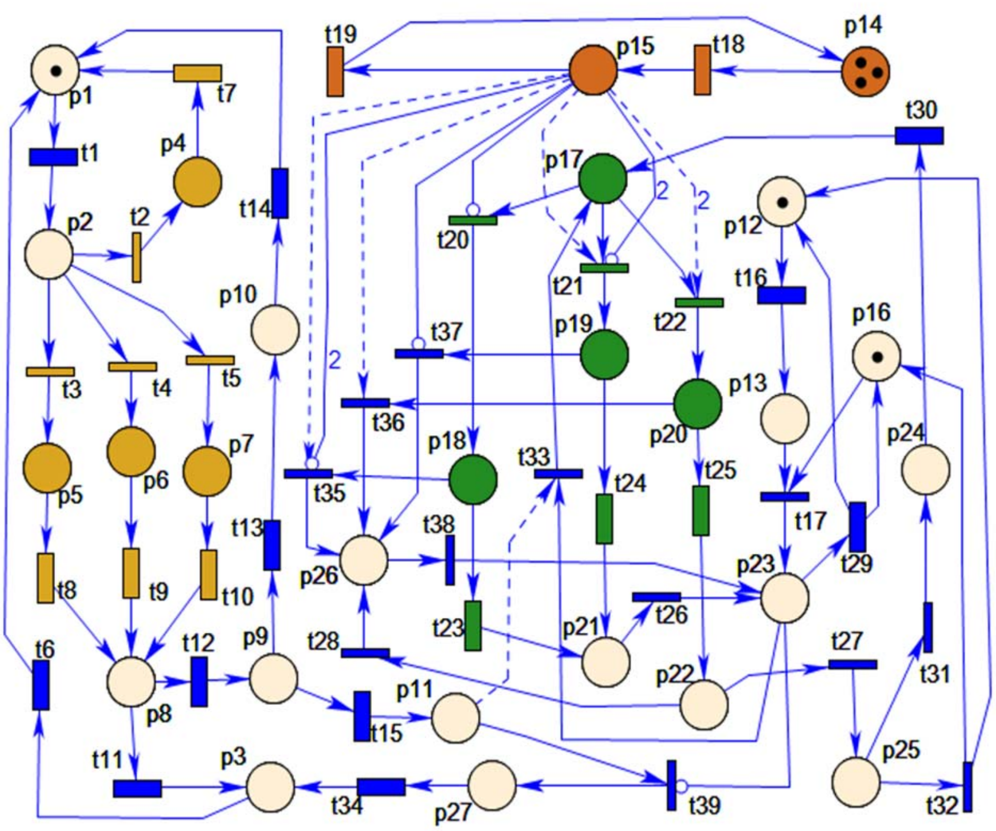

Figure 2. SRN1 model with 3 security firewall rules, honeypot, IDS and 3 MTD techniques.

- **Immediate transitions**:t_2 - determines the probability that the malicious package was detected by the firewall; t_3, t_4, t_5 - probabilistic selector that determines the probability that the malicious package will bypass the respective firewall rule; t_{20}, t_{21}, t_{22} - selecting and activating the respective MTD security mechanism: SW - a new variant of server software, DPT - new dynamic properties of its processing platform, NAS - the system changes its network address; t_{26}, t_{27}, t_{31} - reactivating the processing of the user's request by the server;t_{32} - reset the server release; t_{33} - initialization of the MTD defense activation and triggering the elimination of the intruder; t_{34} - reset the selection and change of a MTD mechanism; t_{35}, t_{36}, t_{37} - elimination of the intruder when changing the current MTD mechanism;t_{38} - switching demand service normally with the current MTD mechanism; t_{39} - eliminating the intruder when switching MTD.

It can be demonstrated that any FSRN or FGSPN model can be folded in a $MR\Gamma$ model type with the same attributes and behavioral properties. Figure 3 shows the $MR\Gamma 1$ model obtained by the respective folding of the model FSRN1. It can also be demonstrated that any model or GSPN can be wrapped in a model of the type with the same attributes and behavioral properties. Figure 3 shows the model obtained by the respective folding of the FSRN1 model.

The timed rewriting rules of $MR\Gamma1$ are: $\mathbf{r}1 = [r1_i]$, $i = 0, 1, \cdots, k_r - 1$ ($\mathbf{r}3 = [r3_j], j = 0, 1, \cdots, k_{r3} - 1$ and $\mathbf{r}4 = [r4_l], l = 1, 2, \cdots, k_{r4} - 1$, respectively)) are timed matrix rules for rewriting subnets that describe the activation of firewall rules (time-out changing of MTD mechanisms, respectively) for which the control place is p_{28} (p_{15} and p_{14}, respectively).

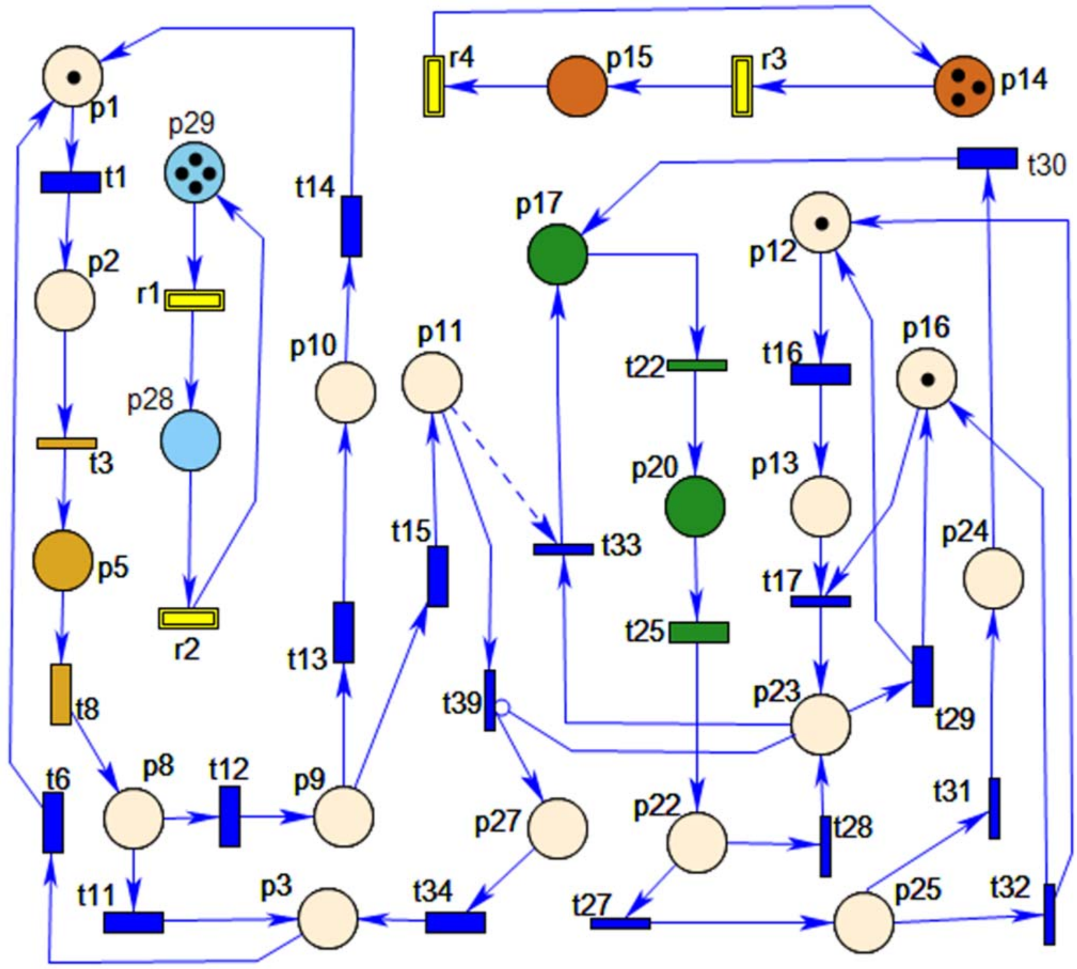

Figure 3. The $MR\Gamma1$ model obtained by folding the SRN1 model **RN1.**

$r2$ is a rewriting rule for which it guard function is $g_l^{r2}(m_{28}) = "False"$ and *thus it is enabled and fired as an ordinary timed transition*. The selection of a $r1_i$ (respectively $r3_j$ or $r4_j$) is made by the current marking of the place p_{28} (p_{15} and p_{14}, respectively), that $i = m_{28} = M(p_{28})$ ($j = m_{15} = M(p_{15})$ and $l = m_{15} = M(p_{15})$, respectively).

The libraries Lsp^{r1}, Lsp^{r3} and Lsp^{r4} contain subnets FSRN templates of the RN type with respective attributes, associated respectively with $\mathbf{r}1$, $\mathbf{r}3$ and $\mathbf{r}4$ of the $MR\Gamma1$ model:

$$Lsp^{r1} = \{RN1_i, RN1_i^*, i = 0, 1, \cdots, k_{r1} - 1\}, \; Lsp^{r3} = \{RN3_j, RN3_j^*, \; j = 0, 1, \cdots, k_{r3} - 1\} \text{ and}$$

$$Lsp^{r4} = \{RN4_l, RN4_l^*, l = 1, 2, \cdots, k_{r4} - 1\}.$$

The guard function of the application $r1_i$ is $g_i^{r1}(M) = \vee_{i=0}^{k_{r1}-1}(m_{i+4} = 0)$, and of the application $r3_i$ and $r4_i$ are respectively: $g_j^{r3}(M) = \vee_{i=0}^{k_{r3}-1}(m_{j+18} = 0)$ and $g_l^{r4}(M) = \vee_{l=0}^{k_{r3}-1}(m_{l+18} = 1)$.

When a rule $r1_i$ or $r3_i$ or $r4_l$ is fired the changing of current structure $MR\Gamma 1$ model, with the respective attributes, is performed as follows:

$$r1_i : RN1_i \triangleright RN1^*_{i+1},\ r1_v : RN1_v \triangleright RN1^*_0, \quad i = 0, 1, \cdots, k_{r1} - 1, v = k_{r1};$$

$$r3_j : RN3_j \triangleright RN3^*_{j+1}, r3_s : RN3_s \triangleright RN3^*_0 \quad j = 0, 1, \cdots, k_{r3} - 1,\ s = k_{r3};$$

$$r4_l : RN4_l \triangleright RN4^*_{l+1}, r4_e : RN_e \triangleright RN4^*_0 \quad l = 0, 1, \cdots, k_{r4} - 1,\ e = k_{r4},$$

descriptive expressions whose [29] are:

$$RN1_i = |_{t_{i+3}}\ p_{i+5}\ |_{t_{i+8}},\ RN1_v = |_{t_2}\ p_4\ |_{t_7},\ RN1^*_{i+1} = p_2\ |_{t_{l+3}}\ p_{i+5}\ |_{t_{i+8}}\ p_8,\ RN1^*_v = p_2\ |_{t_2}\ p_4\ |_{t_7}\ p_8,$$

$$i = 0, 1, \cdots, k_{r1} - 1, \quad v = k_{r1} = 3; RN3_j = |_{t_{j+20}}\ p_{j+18}\ |_{t_{j+23}}\ p_{21}\ |_{t_{26}},\ \ RN3^*_j = p_{17}\ |_{t_{j+20}}\ p_{j+18}\ |_{t_{j+23}}\ p_{21}\ |_{t_{26}}\ p_{23},$$

$$RN3_s = |_{t_{s+20}}\ p_{s+18}\ |_{t_{s+23}}\ p_{22}\ |_{t_{27}}\ p_{25}\ |_{t_{31}}\ p_{24}\ |_{t_{30}}\ \overset{\leftrightarrow}{\triangledown} p_{22}\ |_{t_{28}}\ \overset{\leftrightarrow}{\triangledown} p_{25}\ |_{t_{32}};$$

$$RN3^*_s = p_{17}\ |_{t_{s+20}}\ p_{s+18}\ |_{t_{s+23}}\ p_{22}\ |_{t_{27}}\ p_{25}\ |_{t_{31}}\ p_{24}\ |_{t_{30}}\ p_{17} \overset{\leftrightarrow}{\triangledown} p_{22}\ |_{t_{28}}\ p_{23} \overset{\leftrightarrow}{\triangledown} p_{25}\ |_{t_{32}}\ (p_{12} \Diamond p_{16});$$

$$RN4_j = |_{t_{j+20}}\ 1p_{j+18}\ |_{t_{j+23}}\ p_{21}\ |_{t_{26}},\quad RN4^*_j = p_{17}\ |_{t_{j+20}}\ p_{j+18}\ |_{t_{j+23}}\ p_{21}\ |_{t_{26}}\ 1p_{23},$$

$$RN4_s = |_{t_{s+20}}\ 1p_{s+18}\ |_{t_{s+23}}\ p_{22}\ |_{t_{27}}\ p_{25}\ |_{t_{31}}\ p_{24}\ |_{t_{30}}\ \overset{\leftrightarrow}{\triangledown} p_{22}\ |_{t_{28}}\ \overset{\leftrightarrow}{\triangledown} p_{25}\ |_{t_{32}};$$

$$RN4^*_s = p_{17}\ |_{t_{s+20}}\ p_{s+18}\ |_{t_{s+23}}\ p_{22}\ |_{t_{27}}\ p_{25}\ |_{t_{31}}\ p_{24}\ |_{t_{30}}\ p_{17} \overset{\leftrightarrow}{\triangledown} 1p_{22}\ |_{t_{28}}\ p_{23} \overset{\leftrightarrow}{\triangledown} p_{25}\ |_{t_{32}}\ (p_{12} \Diamond p_{16}),$$

$$j = 0, 1, \cdots, k_{r3} - 1, \quad s = k_{r3} = k_{r4} = 2.$$

The meaning of a descriptive expression (DE) of the structure of a Petri net is [29, 31]: $DE ::= DE_i \otimes DE_j \mid \circ DE$, where $\otimes$ represents the operator of a *binary compositional operation*, and $\circ$ is the operator of a unary operation. By default, when applying these operations, the locations, transitions and rewriting rules that have the same name are merged, respectively. In a DE, any symbol-place, symbol-transition or symbol- rewriting rule can be used in any order multiple times. When one of these symbols is removed, all of its incident arcs will also be removed.

In [29, 31] it is shown how one can perform the mapping of a DE in graphical representation of RP and vice versa, the graphical representation of this RP mapped in DE.

We briefly explain only the significance of the compositional operations used in this work. For more details the reader can consult the works [29, 31]: The binary *Fork operation*, rendered by the operator "$\Diamond$", describes the fact that at the occurrence of a specified event e_j two or more post-conditions will occur simultaneously. This operation is commutative, associative and reflective; The *Sequential operation*, rendered by the operator " $|_{e_j}$ ", is a binary operation that determines the "cause-consequence" logic of the relationship between two local states p_i (pre-condition) and p_k (post-condition), determined by the event. This operation is associative, reflexive and transitive, but non-commutative;

The operation *Competitive Parallelism*, rendered by the operator "$\overset{\leftrightarrow}{\triangledown}$", describes the logical relations of the competitive parallelism of the conditions and events between two or more competing processes. It is applied to perform the model composition of several sub-modules of the PN subnets, which describe the functioning of the respective subsystems in a resulting model of the considered system.

Let two subnets RN_A and RN_B. They are rendered by the $DE_A = A$ and $DE_B = B$ expressions, respectively then composing them by applying the "$\overset{\leftrightarrow}{\triangledown}$" operator, relative to these two DE, we obtain the resultant RN_R net, rendered by $DE_R = C = A \overset{\leftrightarrow}{\triangledown} B$ where the places and transitions having the same name will be merged respectively. The merged nodes will retain the attributes and incidence of the arcs in each subnet. This operation is commutative, associative and reflexive.

When evaluating DE, the following priorities for the use of compositional operations will be taken into consideration: a unary operation links more strongly than the binary ones; " $\Diamond$" is superior to the operation "$|_{t_j}$", which, in turn, is superior to the operation $\overset{\leftrightarrow}{\nabla}$.

In turn, the $MR\Gamma1$ model can be unfolded in a FSRN1 model with the same attributes and behavioral properties, which allows using some of the specialized PetriNetTool [32] instrumental platforms to simulate and analyze these types of models, for example, VPNP [33], PIPE 4.3 [32].

In the case of a large number of firewall rules and / or MTD techniques, the size of the graphical presentation of a model similar to FSRN1 increases considerably. Thus, we can see the advantage of compact representation of $MR\Gamma$ type models.

The FSRN1 model, underlying to$MR\Gamma1$, has BLR behavioral properties, so the fuzzy CTMC1 (FCTMC1) describing the functioning of this model is ergodic [18, 23, 24] and it has 211 vanishing markings and 140 tangible markings.

Case Study. Next we will present a case study to show the use of the approach presented in this paper. The numerical analysis of some QoS characteristics of CN security system is based on the FSRN1 model, using the knowledge of the experts in the field [1, 4, 8, 18]. As an example for the fuzzy rates of fired transitions and timed rewriting rules, we establish the following TrNFs values: $\tilde{\lambda}_1 = (0.005, 0.0075, 0.01, 0.0125)$, $\tilde{\lambda}_6 = (0.5, 1.0, 1.5, 2.0)$, $\tilde{\lambda}_7 = (2.0, 2.5, 3.0, 3.5)$,

$\tilde{\lambda}_8 = (1.75, 2.0, 2.25, 3.0)$, $\tilde{\lambda}_1 = (0.005, 0.0075, 0.01, 0.0125)$, $\tilde{\lambda}_6 = (0.5, 1.0, 1.5, 2.0)$, $\tilde{\lambda}_7 = (2.0, 2.5, 3.0, 3.5)$,

$$\tilde{\lambda}_8 = (1.75, 2.0, 2.25, 3.0),\ \tilde{\lambda}_9 = (2.5, 2.75, 3.25, 3.50),\ \tilde{\lambda}_{10} = (2.25, 3.0, 3.25, 3.75),$$

$$\tilde{\lambda}_{11} = \tilde{\lambda}_{12} = (1.5, 2.0, 2.25, 2.75),\ \tilde{\lambda}_{13} = (2.0, 2.5, 3.0, 3.5),\ \tilde{\lambda}_{14} = (5.0, 5.5, 6.0, 6.5),\ \tilde{\lambda}_{15} = (2.0, 2.5, 3.0, 3.5),$$

$$\tilde{\lambda}_{16} = (0.5, 1.0, 1.5, 2.0),\ \lambda_{18} = \lambda_{19} = r3 = r4 = 0.5,\ \tilde{r}1 = \tilde{r}2 = 2.0,$$

$$\tilde{\lambda}_{23} = (3.5, 4.0, 4.5, 5.0),\ \tilde{\lambda}_{24} = (4.5, 5.0, 5.5, 6.0),\ \tilde{\lambda}_{25} = (3.5, 4.0, 4.5\ 5.0),$$

$$\tilde{\lambda}_{29} = (3.0, 4.0, 4.25, 4.5),\ \tilde{\lambda}_{30} = (10, 18, 22, 25),\ \tilde{\lambda}_{34} = (2.0, 2.75, 3.0, 3.25).$$

Similarly, we determine the weights$w_k = 100$,associated with all the immediate transitions, based on which their firing probabilitiesq_k are determined [24].

The credible values of the fuzzy firing rates $\tilde{\lambda}_j = (a_j, b_j, c_j, d_j)$ of the timed transitions are calculated according to the expression:

$$\bar{\xi} = E[\xi] = (a_j + b_j + c_j + d_j)/4 \text{ [25].}$$

In order to evaluate the QoS characteristics of the CN based on the FSRN1 model, with the credible fuzzy parameters of this case study, the VPNP instrumental software platform was used [33]. For example, the probability that the security system successfully countered the intruder attacks is the probability$\pi_{\sec} = \Pr(M(p_1) = 1)$ that FSRN1 is in the state $M_k(p_1) = 1$, $M_k \in Acc(\text{FSRN1})$, where$Acc(\text{FSRN1})$ is the set of accessible markings of FSRN1 from M_0. Figure 4 shows the graphs evolution of the state-steady probability $\pi_{\sec} = \Pr(M(p_1) = 1)$ and the $\pi_{sva} = \Pr(M(p_{23}) = 1)$, respectively that the server processes the user request, function on$\bar{\lambda}_{18} \in [0.5, 1.5]$, $\Delta\bar{\lambda}_{18} = 0.1$ and $\bar{\lambda}_{13} \in [1, 4]$, $\Delta\bar{\lambda}_{13} = 1$.

Thus, each evaluator can build his own type $MR\Gamma1$ and/or GSPN1 model, using various combinations of CN security techniques and respective fuzzy parameters to evaluate the specified performance characteristics. In other words, it can assign a weight for each chosen performance feature based on the specified requirements. For each security technique (firewall, honeypot, MTD, etc.), the evaluator can specify the values of each fuzzy parameter and then obtain based on this type of model final results of quantitative values of performance characteristics with different combinations of types of security techniques and their associated weight to perform a comparative analysis of their efficiency.

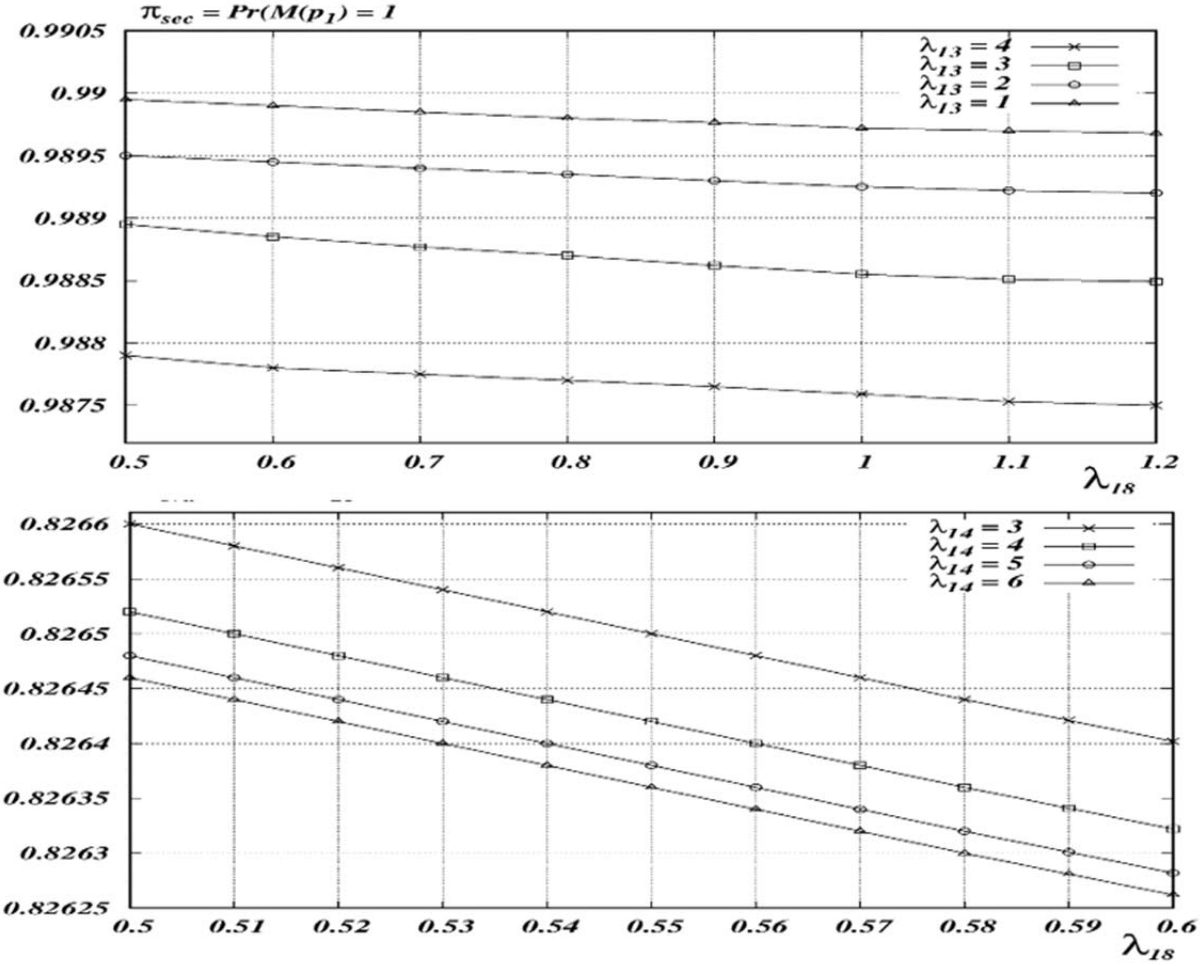

Figure 4. The graphs evolution of the state-steady probability $\pi_{\sec}$ and π_{sva}.

Conclusion

In this paper a new type of reward stochastic network (FSRN) is defined by introducing matrix attributes and dynamically rewriting them and its structure, called MFRSRN, which allows the dynamic reconfiguration, dependent on the current marking, of these types of models. Moreover, this formalism offers a descriptive language that allows the management of the compact representation of the model size by introducing the matrix structuring and rewriting mechanisms of the compositional behavior of the model.

As an example of an application, we show how the proposed formalism can be applied to the performance modeling of a CN "Defense in Breadth" security system, which incorporates a combination of firewall, IDS, honeypot and MTD techniques, taking into account the probabilistic uncertainty issues and the epistemic one.

In the future we intend to carry out the following researchs: (1) to validate the proposed model based on different scenarios through a comprehensive analysis taking into account the fact that the timing distributions of the transitions and the timed rewriting rules are random variables with phase distributions [10] (for example, Elang, Cox, Hyperexponential etc.), and their parameters are intuitionistic fuzzy numbers [34]; (2) to integrate in the VPNP tool a software subsystem that will allow to solve by means of the Mehar method [35] the Chapman-Kolmogorov differential equations of the fuzzy CTMC, generated by a model type FGSPN; (3) to elaborate and develop a similar software product VPNP tool for visual simulation and analysis of models of the type that describe the evolution of discrete event systems with reconfigurable matrix applications.

This work was carried out within the national project of applied scientific research 14.820.18.02.03 / U.

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

References

1. Kumar, U.et al. Analysis of Network Security Issue and Its Attack and Defence. [online]. In: *International Journal of Computer Science and Information Technologies*, Vol. 7 (3), 2016, pp. 1029-1031. [accesat 14.03.2019]. available at: https://www.researchgate.net/publication/301802858
2. Kashefi, I., Kassiri, M., Shahidinejad, A. *A Survey on security issues in firewalls: a new approach for classifying firewall vulnerabilities*. [ONLINE]. In: International Journal Of Engineering Research And Applications, VOL. 3, ISSUE 2, MARCH -APRIL 2013, PP.585-591. [ACCESS DATE 16.02.2019]. Available at: https://www.researchgate.net/publication/262116695
3. Harale, N., Meshram, B.B. *Network Based Intrusion Detection and Prevention Systems: Attack Classification , Methodologies and Tools*. [online]. In: International Journal of Engineering And Science Vol.6, Issue 5, 2016, pp. 1-12. [access date 14.03.2019]. available at: http://www.researchinventy.com/papers/v6i5/A60501012.pdf
4. Shi, L., Li, Y., Feng, H. *Performance Analysis of Honeypot with Petri Nets*. [online]. In.: Information, 9, 245, 2018, pp. 2-19. [access date 25.01.2019]. available at: https://www.mdpi.com/2078-2489/9/10/245
5. Carvalho, M., Ford, R. Moving-target defenses for computer networks. In: *IEEE Security & Privacy*, 12(2), Mar.-Apr. 2014, pp. 73-76.
6. Cai, G., Wang, B., Hu, W., Wang. T. *Moving target defense: state of the art and characteristics* [online]. Frontiers of Information Technology & Electronic Engineering, November 2016, 17(11), pp.1122-1153 [access date 17.01.2019]. available at: https://link.springer.com/article/10.1631/FITEE.1601321
7. Zheng. J, Namin A.S. A survey on the moving target defense strategies: An architectural perspective. In: *Journal of Computer Science and Technology*, 34(1), 2019, pp. 207–233.
8. Cho, J.H., Ben-Asher, N. Cyber defense in breadth: Modeling and analysis of integrated defense systems. In: *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, Vol. 15(2), 2018, pp. 147–160.
9. Kure, H. I, Islam, S., Razzaque, M. A. *An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System*. [online]. In: Applied Sciences. 8, 898, 2018, pp. 1-29. [access date 11.05.2019]. available at: https://www.mdpi.com/2076-3417/8/6/898/pdf
10. Trivedi, K. S., Kim, D.S., Roy A., Medhi D. Dependability and security models. In: *Proceedings of 7th International Workshop on the Design of Reliable Communication Networks*, Oct. 2009. pp. 11-20.
11. Cherdantseva, Y. *A review of cyber security risk assessment methods for SCADA systems*. [online]. In: Computers & Security, 56, 2016, pp.1–27. [access date 18.03.2019]. available at: https://www.sciencedirect.com/science/article/pii/S0167404815001388
12. Cai G., Wang B., Luo Y., Hu W. A Model for Evaluating and Comparing Moving Target Defense Techniques Based on Generalized Stochastic Petri Net. In: *Wu J., Li L. (eds) Advanced Computer Architecture. ACA 2016. Communications in Computer and Information Science*, vol 626. Springer, Singapore, 2016, pp. 184–197.
13. Connell, W., Menasce, D. A., Albanese M. *Performance Modeling of Moving Target Defenses* [online]. In: MTD Models and Evaluation, MTD'17, October 30, 2017, pp. 53-63, Dallas, TX, USA. [access date 16.01.2015]. available at: https://www.academia.edu/36284557

14. Ibidunmoye, E. O., Alese, B. K., Ogundele, O.S. A Game-theoretic Scenario for Modeling the Attacker-Defender Interaction. In: J. Comput. Eng. Inf. Technol.,Vol.2, No.1, 2013, pp1-8.
15. Lin, C., Wang, Y Z., Wang, Y. A Stochastic Game Nets Based Approach for Network Security Analysis. In: *Proceedings of the 29th International Conference on Application and Theory of Petri Nets and other Models of Concurrency, Concurrency Methods*: *Issues and Applications Workshop*, 2008, pp.21-33.
16. Li, Y., Sun, J., Cao, Q. *Analysis for Ad Hoc Network Attack-Defense Based on Stochastic Game Model*. [online]. In: Sensors & Transducers, Vol. 173, Issue 6, June 2014, pp. 256-262. [access date 14.03.2019]. available at: https://www.researchgate.net/publication/289241903
17. Maleki, H. ET.AL. *Markov modeling of moving target defense games* [online]. In: proceedings of the 3rd ACM workshop on moving target defense (MTD 2016). ACM, VIENNA, 2016. AUSTRIA, 81−92. [Access date 21.01.2019]. Available at: HTTPS://www.researchgate.net/publication/310821430.
18. Sallhammar, K., Helvik, B. E., Knapskog, S. J. On stochastic modelling for integrated security and dependability evaluation. In: *Journal of Networks*, Vol. 1, Issue 5, 2006, pp. 31 – 42.
19. Shi, L., Li, Y., Feng, H. *Performance Analysis of Honeypot with Petri Nets*. [online]. In: Information 9, 245, 2018, pp. 1-19. [access date 11.05.2019]. available at: https://www.mdpi.com/2078-2489/9/10/245/pdf
20. Tao, M., Shan, H. An improved method of the attack tree model for mobile Ad Hoc networks. In: *Computer Applications and Software*, Vol. 26, Issue 4, 2009, pp. 271 – 273.
21. Zhang, G. et.al. *Attack Simulation based Software Protection Assessment Method with Petri Net*. [online]. In: Intl. Journal on Cyber Situational Awareness, Vol. 1, No. 1, 2016, pp. 152-181. [access date 11.05.2019]. available at: https://www.c-mric.com/wp-content/uploads/2017/10/article8.pdf
22. Zhuo, W., Lin, C., Chen, X. Quantitative analysis method of network attack and defense based on stochastic game model. In: *Journal of Computers*, Vol. 9, 2010, pp. 1748 – 1762.
23. Han K, Nguyen T.A, Min D, Choi E.M. An evaluation of availability, reliability and power consumption for a SDN infrastructure using stochastic reward net. In: *Advances in Computer Science and Ubiquitous Computing: CSACUTE 2016*, Singapore: Springer Singapore, 2017, pp. 637-648.
24. Chiola, G., Ajmone- Marsan, M., Balbo, G., Conte, G. Generalized stochastic Petri nets: A definition at the net level and its implications. In: *IEEE Transactions on Software Engineering*, 1993, 19 (2), pp. 89-107.
25. Li, X., Liu, B. Foundation of credibilistic logic. In: *Fuzzy Optimization and Decision Making*, vol.8, no.1, 2009, pp. 91-102.
26. Abbasbandy, S., Viranloo, T. *Numerical solution of fuzzy differential equation*. [online]. Mathematical & Computational Applications, 7, 2002, pp. 41−52. [access date 11.12.2018]. available at: http://dx.doi.org/10.3390/mca7010041
27. Ding, Z., Shen, H. Applying Fuzzy Differential Equations to the Performance Analysis of Service Composition. In: *Advanced Intelligent Computing Theories and Applications*, *ICIC 2010,* D.-S. Huang et al. (Eds.): LNCS 6215, Springer-Verlag, pp. 2010, pp. 118−125.
28. Tüysüz, F., Kahraman, C. *Modeling a flexible manufacturing cell using stochastic petri nets with fuzzy parameters*. [ONLINE]. IN: EXPERT SYSTEMS WITH APPLICATIONS 37, 2010, PP. 3910−3920. [Access date 11.05.2018]. Available at: HTTPS://www.researchgate.net/publication/287993951
29. Guţuleac, E. Descriptive compositional HSPN modeling of computer systems. In: *Annals of the Craiova University*, *România*, 2006, Vol. 3 (30), no.2, pp.82-87.
30. Guţuleac, E; Zaporojan, S.; Gîrleanu, I.; Cărbune, V. Hybrid stochastic Petri nets with matrix attributes for modelling of discrete-continuous process. In: *Meridian Ingineresc*, 2, 2016, pp.34-40.
31. Guţuleac, E., Mocanu M. L. Descriptive Dynamic Rewriting GSPN-based Performance Modeling of Computer Systems. In: *Proceedings of the 15th International Conference on Control Systems and Computer Science*, 25-27 May 2005, Bucureşti, România, 2005, pp. 62-66.
32. Petri Nets Tools Database Quick Overview. [online]. [access date 11.01.2019]. available at:
https: // *www.informatik.uni-hamburg.de/TGI/PetriNets/ tools/quick.html.*
33. Guţuleac, E., Boşneaga, C., Reilean A. VPNP-Software tool for modeling and performance evaluation using generalized stochastic Petri nets. In: *Proceedings of 6-th International Conference on D&AS-2002*, Suceava, România, 2002, pp. 243-248.
34. Atanassov, K. T. Intuitionistic fuzzy sets. In: *Fuzzy Sets and Systems*, vol. 20, 1986, pp. 87-96.
35. Lata, S., Kumar, A. *Mehar's method for analyzing the fuzzy reliability of piston manufacturing system*. [Online]. In: Eksploatacja niezawodnosc – maintenance and reliability, *51*, NR. 3, 2011, PP. 26−39. [Access Date 11.01.2019]. Available at: http://www.Ein.Org.Pl/Sites/Default/Files/2011-03-04.Pdf