EvaluareaVulnerabilității la Atac a Rețelelor de Calculatoare prin GSPN Credibil Agregate

Emilian GUȚULEAC, Sergiu ZAPOROJAN, Ion GÎRLEANU, Alexei SCLIFOS, Inga IAVORSCHI
Technical University of Moldova
Emilian.Gutuleac@calc.utm.md,

***Abstract* — Cu dezvoltarea cercetărilor securității rețelelor de calculatoare (RC), modelarea atacurilor în rețea și tehnicile de analiză ale vulnerabilității acestora au atras din ce în ce mai multă atenție. În lucrarea dată este propusă o metodă de modelare a atacurilor și analiză a vulnerabilității RC prin rețele Petri stochastice generalizate (GSPN) cu rate fuzzy (GSPNF) credibil aggregate. Pentru fiecare tip de atac, este construit un model GSPNF pentru a descrie în mod grafic relația dintre componentele acestora. Este prezentată o metodă de construire a modelului GSPNF ce redă mai nuanțat atacurile combinate concurente și colaborative ale atacatorului și o metodă de analiză a costului de exploatare a vulnerabilității RC. Metoda propusă, fiind relativ simplă, diferă de cea tradițională. În acest context, este prezentat un exemplu ce validează metoda propusă de analiză a vulnerabilității unei RC.**

***Index Terms* — Agregare, calculatoare, credibilitate, fuzzy, rețele Petri, securitate, vulnerabilitate.**

I. INTRODUCERE

Odată cu dezvoltarea rapidă a rețelelor de calculatoare (RC) problema securității informațiilor acestora devine deosebit de proeminentă. Virușii și atacurile hackerilor provoacă pierderi incomensurabile utilizatorilor și întreprinderilor, deci trebuie să fie luate măsuri eficiente pentru a asigura funcționarea în siguranță a RC [12,13,15]. Metodele și tehnicile tradiționale de apărare pasivă a RC, cum ar fi detectarea intruziunilor și firewall-urile, deja nu mai satisfac cerințele actuale de securitate ale utilizatorilor. Mulți cerce-tători au studiat activ problema analizei vulnerabilității securității RC, precum și au dezvoltat metode și tehnologii de modelare, evaluare și analiză a atacurile ce sunt la baza evaluării securității RC. Recent, în ceea ce privește modelarea atacurilor RC, au fost obținute unele rezultate. Metodele cunoscute includ modele cu arbori de atac [12], grafuri de atac [1 4], diagrame de stări ale vulnerabilității [2], modele de propagare a amenințărilor [3], modele cu jocuri teoretice [6, 13, 15], grafuri de exploatare a vulne-rabilității [2] și modele de lanțuri Markov ascunse [11]. Ele reflectă schimbarea de stare a atacatorului și a sistemului de securitate al RC din diferite puncte de vedere, dar acestor tipuri de modele le lipsesc capacitatea de a descrie procesul de atac colaborativ și concurent în atacurile combinate ale RC. În contrast, rețelele Petri stocastice (eng. SPN) [3, 7] și SPN generalizate (GSPN) [4] sunt un formalism grafic de modelare matematică care au mai multe avantaje, cum ar fi normalizarea semantică și capacitatea lor puternică de exprimare. Acest fapt, permite de a descrie în mod graphic mai compact procesul de atac al RC prin SPN sau GSPN. În plus, recent cele mai multe evaluări ale securității bazate pe un model matematic utilizează metoda de analiză a probabilității de success a secvenței de atac [11, 12]. Dezavantajul este acela că se calculează probabilitatea maximă de succes a atacului ceia ce generează rezultate extreme de analiză. Dacă există o situație de a determina o probabilitate nejustificată, ar face ca rezultatele să fie cu mari devieri. Deci, cercetătorii încearcă de a analiza securitatea RC și a evalua costul optimist de apărare.

Metodele tradiţionale de modelare şi analiză a indicatorilor QoS la atac [6, 13, 15] folosesc date referitoare la parametrii componentelor (ratele de atac şi apărare, de reconfigurare, etc.) care se presupune că sunt cunoscute cu o anumită precizie şi apoi validate prin experienţe reale. Însă, deseori, revenirea la experienţe, cu regret, este insuficientă pentru a valida cu precizia specificată a parametrilor de vulnerabilitate, atac şi apărare. De asemenea, la modelarea şi analiza indicatorilor QoS ai RC una dintre cele mai importante subiecte care trebuie luată în considerare este *incertitudinea,* legată de motivul pentru care parametrii modelului sunt, de obicei, sub forma unor parametri fuzzy. Deşi abordarea cea mai frecvent folosită pentru reprezentarea incertitudinii la modelarea acestor tip de procese este efectuată prin modele markoviene, care se bazează pe procese stocastice, acest tip de modele nu totdeauna sunt bine potrivite pentru a descrie toate dimensiunile de incertitudine. Mai ales, imprecizia datelor, care este, de exemplu, rezultatul preciziei limitate de măsurare care nu are o natură statistică şi deci, ea nu poate fi descrisă numai prin utilizarea modelelor probabilistice [6, 15]. De asemenea, spre deosebire de defecţiuni, atacurile intruşilor nu întotdeauna pot fi bine caracterizate prin modele de natură pur aleatorie, ceia ce reduce cunoştinţele sistemului de securitate al RC despre riscul reuşitei unui atac. De cele mai multe ori atacatorii acţionează intenţionat luând în considerare posibilele consecinţe: satisfacţie, profit sau statutul său faţă de efortul şi riscul acţiunilor sale înainte de a acţiona. Cu toate acestea, pentru a modela corect atacurile intenționate asupra unei RC, orice model probabilistic trebuie să includă şi incertitudinile epistemice ale comportamentului atacatorilor. Acest aspect este unul dintre principalele provocări atunci când sunt utilizate tehnicile de modelare stocastică la cuantificarea vulnerabilității securității RC. Argumentăm că comportamentul atacatorului trebuie să fie reprezentat ca o distribuție de probabilitate asupra posibilelor acțiuni de atac în fiecare stare a modelului și, de asemenea, pe o abordare bazată pe utilizarea numerelor fuzzy [1, 6, 9], pentru a reprezenta incertitudinea probabilităților de aflare în stările respective de atac ale RC.

În conformitate cu problemele menționate mai sus, în această lucrare este prezentată o abordare de modelare și analiză credibilă a indicatorilor cantitativi QoS ai vulnerabilității securității RC prin îmbinarea modelelor GSPN [4] cu rate fuzzy de declanșare ale tranzțiilor temporizate (GSPNF) și a teoriei credibilității [9]. Acest tip de mode-le sunt deosebit de potrivite pentru a descrie atacuri combinate concurente și colaborative, a efectua evaluarea cantitativă a vulnerabilității și a performanțelor sistemului de securitate RC, evitând problema de analiză a probabilităților de succes ale secvențelor de atac.

Avantajul acestei metode constă în capacitatea sa de a explica atât incertitudinea obiectivă, cât și cea subiectivă prin integrarea abordărilor stochastice și a a celor fuzzy. Atacurile și măsurile de apărare sunt modelate ca evenimente aleatorii, în timp ce incertitudinea în ratele de apariții ale acestor evenimente este modelată folosind teoria mulțimilor fuzzy și a teoriei credibilității [9]. În acest mod, distribuția interapariției atacurilor, duratele acestora sunt evaluate luând în considerare simultan incertitudinea obiectivă și cea subiectivă.

Avantajul îmbinării unor astfel de paradigme constă în faptul că modelele GSPNF descriu mai real și mai nuanțat comportamentul așteptat al atacatorilor RC. Metoda propusă, fiind relativ simplă, diferă de cea tradițională și ea este validată printr-un exemplu de analiză cantitativă a costului la atac a vulnerabilității unei RC.

II. ELEMENTE ALE TEORIEI CREDIBILITĂȚII

Lanțurile markoviene și cele semimarkoviene în timp continuu (LMTC) sunt un instrument important ce descriu fenomene dinamice sub incertitudine aleatorie. Totuși, în lumea reală deseori întâlnim probleme dificile care nu pot fi tratate prin utilizarea doar a teoriei proceselor stocastice.

Pentru a face față unor astfel de probleme complexe, Liu în [9] a propus teoria credibilității (TC), care este o ra-mură a matematicii pentru studierea comportamentului fenomenelor fuzzy. Teoria mulțimilor fuzzy și conceptele cu numere fuzzy [1, 6] au apărut din necesitatea de a exprima cantitativ mai nunțat mărimi imprecise, in care domeniul de valori pe care il ia funcția de apartenență nu mai este limitata la doua valori, ci se extinde la intreg intervalul [0, 1].

Pentru a facilita expunera metodei propuse în această lucrare, prezentăm unele elemente de bază ale TC.

O mulțime fuzzy $\widetilde{A}$ este definită astfel:

$$\widetilde{A} = \{(x, \mu_A(x)) / x \in X, \mu_A(x) \in [0,1]\},$$

unde funcția de apartenența $\mu_A(x)$, asociată mulțimii fuzzy, arată gradul în care fiecare element din mulțimea X aparține mulțimii fuzzy $\widetilde{A}$. Cu cât valoarea $\mu_A(x)$ este mai apropiata de 1, cu atât este mai puternică apartenența la mulțimea dată.

Două tipuri de numere fuzzy sunt cel mai des întâlnite în aplicații: numerele triunghiulare și cele trapezoidale. Utilizarea acestor tip de numere fuzzy este mai indicată, un motiv fiind și acela al volumului de calcul .

Un număr fuzzy al A este un număr fuzzy triunghiular (NFT), notat $\widetilde{A}(a_1, a_2, a_3)$, numai în cazul în care există trei numere reale $a_1 \le a_2 \le a_3$ astfel încât funcția de apartenență $\mu_A(x)$ a căruia este redată de următoarea relație:

$$\mu_A = \begin{cases} (x-a_1)/(a_2-a_1), & a_1 \le x \le a_2 \\ 1, & x = a_2 \\ (a_3-x)/(a_3-a_2), & a_2 \le x \le a_3 \\ 0, & altfel \end{cases}$$

De asemenea, în literatura de domeniu NFT $\widetilde{A}$ sunt reprezentate și prin așa numite α – *tăieturi* (eng. α - *cut*): $\widetilde{A}_\alpha = \{x : \mu_\lambda(x) \ge \alpha \in [0,1]\}$ cu următoarele *intervale de incredere* posibile la nivel α [11]:

$$\widetilde{A}_\alpha = [a_1 + \alpha(a_2 - a_1),\ a_3 - \alpha(a_3 - a_2)].$$

În Fig.1 este prezentată funcția de apartenență a unui NFT $\widetilde{A}$.

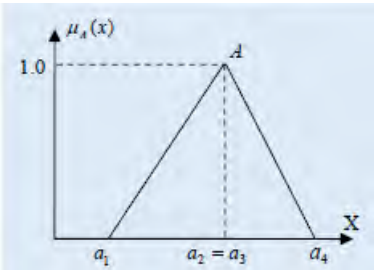

Fig. 1. Funcția de apartenență a unui NFT $\widetilde{A}$.

Un număr fuzzy al A este un număr fuzzy trapezoidal (NFTz), notat $\widetilde{A}(a_1, a_2, a_3, a_4)$, numai în cazul în care există patru numere reale $a_1 \le a_2 \le a_3 \le a_4$ astfel încât funcția de apartenență $\mu_A(x)$ a căruia este:

$$\mu_A = \begin{cases} (x-a_1)/(a_2-a_1), & a_1 \le x \le a_2 \\ 1, & a_2 \le x \le a_3 \\ (a_4-x)/(a_4-a_3), & a_3 \le x \le a_4 \\ 0, & altfel \end{cases}$$

Este evident că un NFTz este un NFT pentru cazul special cu $a_2 = a_3$.

În Fig.2 este prezentată funcția $\mu_A(x)$ a unui NFTz.

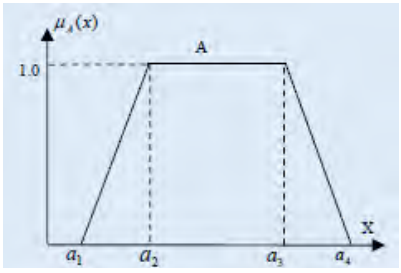

Fig. 2. Funcția de apartenență a unui NFTz $\widetilde{A}$.

Credibilitatea măsoară gradul de încredere, acordat unei mulțimi anumite de date, apariției unor evenimente, a unor variabile fuzzy, etc. Scopul teoriei credibilității este de a combina eficient informațiile din diverse surse: date precedente și actuale, date privind riscul individual și riscul colectiv, rate ale apariției atacurilor și a măsurilor de apărare, etc. [9]. În contnuare, introducem noțiunile de bază ale teoriei credibilității, cum ar fi: măsura de credibili-tate; spațiul de credibilitate; variabilă fuzzy aleatorie; funcția de apartenență; distribuția credibilității și valoarea ei medie.

Fie Θ o mulțime nevidă, iar $Bag(\Theta)$ este puterea de descriere a acesteia, adică mulțimea tuturor submulțimilor lui Θ. Fiecare element al lui $Bag(\Theta)$ este numit un eveniment. Pentru fiecare element $A \in Bag(\Theta)$ este definită o măsură de credibilitate $Cr\{A\}$ care exprimă șansa apariției unui eveniment fuzzy A [9]. La definirea axiomatică a credibilității, este necesar să atribuim fiecărui eveniment fuzzy $A \in Bag(\Theta)$ un număr $Cr\{A\}$ care indică credibilitatea de apariție a acestuia. În [9] este demonstrat că mulțimea de funcții $Cr\{\Theta\}$ este o măsură de credibilitate dacă și numai dacă aceasta satisface condițiile de:
1) normalitate: $Cr\{\Theta\} = 1$*; 2) monotonie:* $Cr\{A\} \le Cr\{B\}$ *oricând* $A \subset B$*; 3) autodualitate:* $Cr\{A\} + Cr\{A^c\} = 1$ *pentru orice* $A \in Bag(\Theta)$*; 4) maximalitate:* $Cr\{\sum_i \cup_i A_i\} \wedge 0.5 = \sup_i Cr\{A_i\}$ *pentru orice* A_i *cu* $Cr\{A_i\} \le 0.5$.

Tripletul (Θ, Bag, Cr) este numit spațiu de credibilitate, iar o variabilă fuzzy este definită ca o funcție (măsurabilă) din acest spațiu pe mulțimea numerelor reale *IR* [9].

Fie variabila fuzzy ξ este o funcție măsurabilă din spațiul (Θ, Bag, Cr) pe IR. Conform [9], funcția de apartenență $\mu(x)$ a lui ξ este derivată din măsura de credibilitate în modulul următor:

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

iar pentru orice mulțime $B \in IR$ de numere reale avem:

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

Valoarea medie $\overline{\xi} = E[\xi]$ a lui ξ este determinată de relația (3) [??]:

$$E[\xi] = \int_0^{+\infty} Cr\{\xi \ge x\} dx - \int_{-\infty}^0 Cr\{\xi \le x\} dx \quad (3)$$

În continuare, vom folosi funcții de apartenență $\mu(x)$ ale câtorva tipuri de variabile fuzzy și anume: *echiposibile*, *triunchiulare* și *trapezoidale* pentru a descrie parametrii modelului GSPNF ce descrie comportamentul atacatorului care folosește informațiile fuzzy despre vulnerabilitățile RC date.

O variabilă fuzzy *echiposibilă* este redată de părechea (a, b) de valori certe cu $a < b$, funcția de apartenență $\mu(x)$ a căreia este:

$$\mu(x) = \begin{cases} 1, & dacă\ a \le x \le b \\ 0, & altfel \end{cases} . \quad (4)$$

Calculul valorilor medii $\overline{\xi} = E[\xi]$ *ale unei variabile fuzzy echiposibile, triunchiulare și trapezoidale.* Fie ξ este o variabilă fuzzy echiposibilă pe $[a,b]$ cu $a \ge 0$. În conformitate cu relațiile (2) și (4) avem:

$$Cr\{\xi \ge x\} = \begin{cases} 1, & x \le a \\ 0.5, & a < x < b \\ 0, & x \ge b \end{cases} .$$

Folosind relația (4) obținem:

$$\overline{\xi} = \int_0^a 1 \cdot dx + \int_a^b 0.5 \cdot dx + \int_b^{+\infty} 0 \cdot dx \int_{-\infty}^0 0 \cdot dx = (a+b)/2 . \quad (5)$$

În mod asemănător pentru o variabilă *fuzzy triunghiulară* η pe $[a,b,c]$ cu $0 \le a < b < c$, obținem relația:

$$\overline{\eta} = E[\eta] = (a + 2b + c)/4 . \quad (6)$$

Pentru o variabilă fuzzy trapezoidală ς pe $[a,b,c,d]$ cu $0 \le a < b < c < d$, obținem relația:

$$\overline{\varsigma} = E[\varsigma] = (a + b + c + d)/4 . \quad (7)$$

La modelarea și analiza vulnerabilității RC cunoștințele despre valorile ratelor de atac, riscurile de vulnerabilitate, etc. sunt, în general, imperfecte [1] şi ea poate avea două origini. Prima sursa de incertitudine provine din caracterul aleatoriu de informaţii, care are o variabilitate naturală stocastică. A doua sursă de incertitudine epistemică este legată de caracterul imprecis şi incomplet al informaţiilor din cauza lipsei de cunoştinţe despre valorile reale ale parametrilor RC ce îşi schimbă în mod dinamic stările sale. Deci, pentru a modela într-un mod mai realist incertudinea comportamentului atacatorului şi reacţia de apărare a sistemului de securitate, este necesar de a lua în considerare, de asemenea, atât aspectele probabilistice, cât şi cele fuzzy [1, 6]. Acest fapt poate fi realizat prin definerea unei noi extensii a GSPN în care unele atribute cantitative pot avea mărimi fuzzy. Ea se bazează pe fuzzificarea ratelor de declanşare ale tranziţiilor, în baza cărora sunt determinate probabilităţile fuzzy de stare [6].

III. GSPN CU RATE FUZZY ALE TRANZIŢIILOR

În continuare, prezentăm unele definiţii şi notaţii, în conformitate cu [4, 7], care sunt necesare pentru a introduce GSPN cu rate fuzzy ale tranziţiilor, GSPNF.

Definiţia 1. O reţea GSPNF, este o structură de obiecte Γ, redată de următorul 13-tuplu: $\Gamma = < P, T, Pre, Post, Test, Inh, K_p, Pri, G, \omega, \tilde{\Lambda}, \mu_\lambda, M_0 >$, unde: *P* este mulţimea nevidă de *locaţii*, $|P| = k$. Locaţiile pot să conţină un număr întreg pozitiv de jetoane. În reprezentarea grafică locaţiile sunt redate prin cerculeţe; *T* este mulţimea nevidă de *tranziţii*, declanşarea cărora modifică marcajul curent. $|T| = n$ şi $P \cap T = \varnothing$. În reprezentarea grafică tranziţiile sunt redate prin bare subţiri sau dreptunghiuri negre; *Pre, Test* şi *Inh*: $P \times T \times IN_+^{|P|} \to IN_+$ sunt funcţii de incidenţă *înainte*, *test* şi *inhibiţie,* iar $Post: P \times T \times IN_+^{|P|} \to IN_+$ este funcţii de incidenţă *înapoi*. IN_+ este mulţimea numerilor întregi nenegative. Prin arce normale se consumă jetoane din *pre-locaţii* sau se produc jetoane în *post-locaţii* respective (relaţie *consumator-producător*). Aceste arce sunt reprezentate prin săgeţi. Prin arcele inhibitoare şi/sau test nu se consumă jetoane. Un arc inhibitor este reprezentat printr-o linie cu un cerculeţ mic la sfârşit, iar un arc test este reprezentat printr-o săgeată cu o linie întreruptă. Ponderea unui arc ce este egală cu 1 nu se menţionează explicit; Funcţia de capacitate a locaţiilor este $K_p: P \times IN_+^{|P|} \to (IN_+ \cup +\infty)$ şi ea redă capacitatea maximă de jetoane în $\forall p_i \in P$, $0 < K_p(p_i) < +\infty$. Implicit, $K_p(p_i)$ este nelimitată; $Pri: T \times IN_+^{|P|} \to IN_+$ este funcţia de priorităţi dinamice ale declanşării tranziţiilor validate de către marcajul curent. Implicit, priorităţile ce nu sunt menţionate ale unor tranziţii sunt considerate nule; $G: T \times IN_+^{|P|} \to \{true, false\}$ este funcţia de gardă (eng. *Guard-function*). Ea determină pentru orice t o funcţie

Booleană $g(t,M)$ în marcajul curent M. Dacă tranziţia t este validată de marcajul curent M şi $g(t,M)$ are valoarea '*true*', atunci tranziţia t rămâne validată şi eventual ea poate fi declanşată, iar dacă ea are valoarea '*false*' - această tranziţie nu este validată. Implicit $g(t,M)$='*true*'; T este partiţionată în $T=T_\tau \cup T_0$, $T_\tau \cap T_0 = \varnothing$ cu $\Pr i(T_0) > \Pr i(T_\tau)$, unde T_τ este mulţimea tranziţiilor temporizate cu o durată aleatorie fuzzy de declanşare ce are o distribuţie exponenţial–negativă, iar T_0 este mulţimea tranziţiilor imediate cu o durată de declanşare nulă; $\omega : T_0 \times IN_+^{|P|} \to IR_+$ este funcţia de ponere cu $0 \le \omega(t,M) < \infty$ ce determină probabilitatea de declanşare a tranziţiei imediate în marcajul curent M care descrie un selector probabilistic. $\widetilde{\Lambda} : T^\tau \times IN_+^{|P|} \to IR^+$ este funcţia ce determină rata fuzzy $0 < \widetilde{\lambda}(t,M) < +\infty$ de declanşare a tranziţiei temporizate validate $t \in T_\tau(M)$ în marcajul curent M, adică parametrul legii exponenţial-negative. $\mu_\lambda : \widetilde{\Lambda} \to [0,1]$ este funcţia gradului de apartenenţă al lui $\widetilde{\lambda}(t,M)$ la mulţimea fuzzy $\widetilde{\Lambda}$ care determină valorile numerice fuzzy ale ratelor de declanşare ale tranziţiilor temporizate. IR_+ este mulţimea numerilor reale nenegative; $M : P \to Bag(P)$ este un vector coloană ce reprezintă o funcţie de marcare a locaţiilor $p \in P$ în care $M(p) \in IN_+$ este numărul de jetoane în locaţia p. M_0 este marcajul iniţial. ■

Mulţimea tranziţiilor validate de marcajul curent M al reţelei Γ este notată $T(M) = T_0(M) \cup T_\tau(M)$.

Regulile de funcţionare ale modelelor Γ de reţele GSPNF şi metoda de analiză a proprietăţilor lor comportamentale sunt aceleaşi ca şi ale modelelor de GSPN, descrise în [??]. Deosebirea se referă numai prin identificarea ratelor medii de declanşare a tranziţiilor validate ale GSPNF. Astfel, mai întâi identificăm ratele de declanşare ale tranziţiilor care sunt reprezentate ca NFT şi/sau NFTz. Apoi în baza relaţiilor (5), (6) şi (7) din secţiunea 2 determinăm mărimile medii credibile ale ratelor $\overline{\lambda}_j$ de declanşare ale fiecărei tranziţii t_j a GSPNF din Γ. Folosind mărimile respective ale acestor rate medii, modelul Γ de reţea GSPNF este analizat în mod similar unui model GSPN. Însă, în această lucrare vom considera numai modele GSPNF în care toate atributele structural (ponderile arcelor, funcţia de gardă şi priorităţile tranziţiilor) au mărimi implicite, iar capacitatea tuturor locaţiilor este egală cu 1.

IV. ANALIZA VULNERABILITĂŢII RC

Pentru a reda proprietaţi compoziţionale analitice modelelor de reţele GSPN în [7] este introdusă *noţiunea* de *dexel* (***d**escriptive **ex**pression **el**ement*) şi un set de operatori compoziţionali, cu atribute respective, care permit de a construi expresii descriptive (*DE*) ce apoi sunt mapate direct în GSPN. În acest context, pentru a facilita expunerea lucrării date, prezentăm succint doar unii operatori compoziţionali. Mai detaliat cititorul poate consulta lucrările [6, 7]. Implicit, la aplicarea acestor operatori, locaţiile şi tranziţiile ce au acelaşi nume se vor contopi în mod respectiv. Într-o *DE*, orice simbol-locaţie sau simbol-tranziţie poate fi folosit în orice ordine de mai multe ori. Astfel, se va subînţelege că în reţele Γ respective, redate de o *DE* , aceleaşi locaţii (tranziţii), cu acelaşi simbol vor fi *contopite* într-un singur *simbol-locaţie* (*simbol-* tranziţie).

Pentru a descrie organizarea ierarhică modulară a sistemului dat şi funcţionarea lui prin compunerea submodelelor Γ_i ale atacurilor A_i, vom folosi, în mod similar cu [7], paradigma de reţele Γ membranale (ΓM) [7] . Un submodel de reţea Γ_i este structurat într-o membrană $[_i \ ]_i$, redat de o expresie descriptivă Z_i, adică $\Gamma M_i = [_i \ Z_i \ ]_i$ sau $\Gamma M_i = [_i \ \Gamma_i \ ]_i$. În Z_i sau Γ_i vom folosi două *indexuri* pentru a codifica simbolurile-locaţii $p_{i,k}$ şi cele ale tranziţiilor $t_{i,j}$, unde primul index i arată numărul de ordine al ΓM_i, adică al membranei $[_i \Gamma_i]_i$, iar al doilea index j arată numărul de ordine al simbolului-nod respectiv în acest model. La construirea modulară (membranală) a modelului ΓM ce descrie comportamentul unui atacator al RC, acest model este partiţionat în atacuri atomice şi/sau atacuri combinate (*compozite*) folosind operaţii compoziţionale respective.

Înainte de a prezenta unele submodele ΓM_i de GSPNF ale comportamentul unui atacator vom folosi notaţiile: ${}^\bullet p = \{t \mid Post(t,p) > 0\}$ (resp. $p^\bullet = \{t \mid \Pr e(t,p) > 0\}$) este mulţimea de tranziţii incidente *înainte* (resp. *înapoi*) la locaţia p ; ${}^\bullet t = \{p \mid \Pr e(t,p) > 0\}$ (resp. $t^\bullet = \{p \mid Post(t,p) > 0\}$) este mulţimea de locaţii incidente *înainte* (resp. *înapoi*) la tranziţia t .

Un atac atomic A_i este redat de un submodel $\Gamma M_i = [_i \ \Gamma_i \ ]_i$ în care Γ_i conţine: $T_i = \{t_{i,1}\}$, $P_i = \{p_{i,1}, p_{i,2}\}$, $p_{i,1} \in {}^\bullet t_{i,1}$, $p_{i,2} \in t_{i,1}^\bullet$, ${}^\bullet p_{i,1} = \varnothing$, $p_{i,2}^\bullet = \varnothing$, iar activitatea de atac atomic este redată de tranziţia temporizată $t_{i,1}$. Locaţia $p_{i,1}$ denotă echipamentele pe care atacatorul le alocă, precum şi statutul acestuia atunci când atacul este lansat, iar $p_{i,2}$ denotă echipamentele pe care atacatorul deja le-a alocat, precum şi statutul său după terminarea atacului.

Vom estima costul aşteptat al atacatorului ce exploatează cu succes vulnerabilitatea sistemului de securitate al RC la atingerea obiectivului său prin durata medie de atac (*DMA*) $\overline{\tau}_{Atac}$. Cu cât este mai mare mărimea aşteptată $\overline{\tau}_{Atac}$, cu atât este mai mare şi efortul depus, deci şi costul atacatorului pentru a finaliza obiectivul său. Putem evalua costul succesului prin estimarea $\overline{\tau}_{Atac} = 1/\overline{\lambda}_{Atac}$, unde $\overline{\lambda}_{Atac}$ este rata medie credibilă a activităţii de *Atac*.

În cazul în care atacatorul poate continua să realizeze atacul A_j cu noi resurse de atac după ce deja el a realizat atacul A_i, atunci considerăm că există o relaţie dintre A_i şi A_j. Atacul combinat cu un comportament A_i şi A_j poate fi direcţionat către acelaşi calculator gazdă sau pe diferite calculatoare gazde. Vom considera că cea mai bună cale de atac este cea care are cea mai mică *DMA*.

Operaţii combinate ale comportamentului atacatorului. Comportamentele unui atacator ce ralizează atacuri multi-

ple pot fi combinate într-un atac compozit cu relații dintre comportamente de atac atomic prin operații compoziționale binare [5, 7]: operații secvențiale "|", operații concurente "$\vec{\vee}$" sau operații de selecție"$\oplus$". Combinațiile dintre comportamentele de atac pot fi definite formal astfel:

$$A_k ::= (A_i \mid A_j)/(A_i \vec{\vee} A_j)/(A_i \oplus A_j),$$

unde A_i, A_j și A_k denotă comportamentele respective ale atacatorului. Atacuri combinate din două atacuri atomice A_1 și A_2, cu atribute respective, sunt prezentate în Fig. 3.

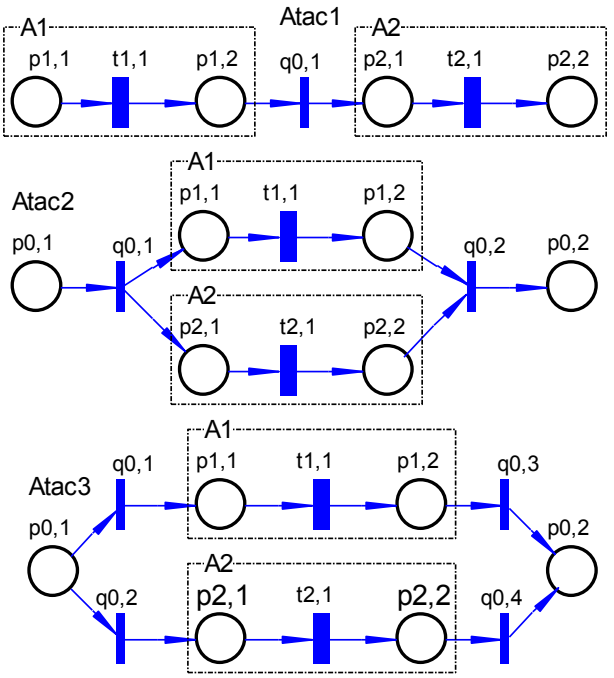

Fig. 3. Combinaţii ale comportamentului atacatorului: Atac1-secvenţial; Atac2-concurent; Atac3-selecţie.

Atacul *Atac1* din figura 3a este compus din comportamente atacator A_1 și A_2 prin *operație secvențială*. Rolul tranziției imediate $q_{0,1}$ este de a conecta cele două comportamente ale atacatorului. Ratele medii de declanșare ale tranzițiilor temporizate $t_{1,1}$ și $t_{2,1}$ sunt, respectiv $\overline{\lambda}_{1,1}$ și $\overline{\lambda}_{2,1}$. În acest caz *DMA* este: $\overline{\tau}_{Atac1} = 1/\overline{\lambda}_{1,1} + 1/\overline{\lambda}_{2,1}$.

Dacă atacul este compus prin *operații secvențiale* din mai multe comportamente atacator $A_1, A_2, ..., A_n$, redate de tranzițiilor temporizate $t_{1,1}, t_{2,1}, ..., t_{n,1}$ cu ratele medii respective $\overline{\lambda}_{1,1}, \overline{\lambda}_{2,1}, ..., \overline{\lambda}_{n,1}$, atunci *DMA* este [3]:

$$\overline{\tau}_{Atac1} = \sum_{i=1}^{n} (1/\overline{\lambda}_{i,1}) . \quad (8)$$

Atacul *Atac2* din Fig. 3 este compus din comportamente atacator A_1 și A_2 prin *operație concurentă*. Locațiile $p_{0,1}$ și $p_{0,2}$ sunt respectiv locație de intrare și locație de ieșire ale atacului combinat. Rolul tranziției imediate $q_{0,1}$ este de a genera condițiile inițiale ale comportamen-telor A_1 și A_2 ale atacatorului în funcție de datele de intrare, iar rolul tranziției imediate $q_{0,2}$ este de a genera rezultatul total de ieșire. Ratele medii de declanșare ale tranzițiilor temporizate $t_{1,1}$ și $t_{2,1}$ sunt, respectiv, $\overline{\lambda}_{1,1}$ și $\overline{\lambda}_{2,1}$. *DMA* este[16]: $\overline{\tau}_{Atac2} = 1/\overline{\lambda}_1 + 1/\overline{\lambda}_2 - 1/(\overline{\lambda}_1 + \overline{\lambda}_2)$.

Dacă atacul este compus din comportamente atacator $A_1, A_2, ..., A_n$ prin operații *concurente, în care* ratele medii de declanșare ale tranzițiilor temporizate $t_{1,1}, t_{2,1}, ..., t_{n,1}$ sunt respectiv $\overline{\lambda}_{1,1}, \overline{\lambda}_{2,1}, ..., \overline{\lambda}_{n,1}$, atunci *DMA* este [3]:

$$\overline{\tau}_{Atac2} = \sum_{i=1}^{n} (1/\overline{\lambda}_{i,1}) - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} (1/(\overline{\lambda}_{i,1} + \overline{\lambda}_{j,1}) + \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} (1/(\overline{\lambda}_{i,1} + \overline{\lambda}_{j,1} + \overline{\lambda}_{k,1}) + \cdots + (-1)^{n-1} / (\sum_{i=1}^{n} \overline{\lambda}_{i,1}) . \quad (9)$$

Atacul *Atac3* din Fig. 3 este compus din comportamente atacator A_1 și A_2 prin operație de selecție. $p_{0,1}$ și $p_{0,2}$ sunt respectiv locație de intrare și cea de ieșire ale atacului combinat. Rolul tranzițiilor immediate $q_{0,1}, q_{0,2}, q_{0,3}, q_{0,4}$ este de a transmite jetonul de la locația de intrare $p_{0,1}$ către locația de ieșire $p_{0,2}$, iar probabilitățile de declanșare ale $q_{0,1}$ și $q_{0,2}$ sunt respectiv α și $1-\alpha$. Ratele medii de declanșare ale tranzițiilor temporizate $t_{1,1}$ și $t_{2,1}$ sunt, respectiv $\overline{\lambda}_{1,1}$ și $\overline{\lambda}_{2,1}$, iar *DMA* este:

$$\overline{\tau}_{Atac3} = \alpha/\overline{\lambda}_{1,1} + (1-\alpha)/\overline{\lambda}_{2,1} .$$

În cazul în care atacul este compus din comportamente atacator $A_1, A_2, ..., A_n$ prin operații de selecție cu rate medii de declanșare respective, atunci *DMA* este [3]:

$$\overline{\tau}_{Atac3} = \sum_{i=1}^{n} (\alpha_i / \overline{\lambda}_{i,1}) . \quad (10)$$

Construirea modelului GSPNF. Pentru a construi modelul GSPNF al comportamentului atacatorului ce exploatează vulnerabilitatea unei RC date este necesar de a efectua următoarele activități [5, 7]:

- Colectarea informațiilor în ce privește vulnerabilitatea echipamentelor RC, inclusiv și cea privind informațiile calculatoarelor gazdă, celor de servire și, de asemenea, colectarea relațiilor conexe ale echipamentelor;
- Construirea modelului fiecărui comportament de atac atomic și determinarea condițiilor în care apar tranziții;
- Definirea stării inițiale a rețelei și a atacurilor combinate prin operații compoziționale în conformitate cu relațiile comportamentale dintre atacurilor atomice;
- Simplificarea modelului pentru a reduce complexitatea acestuia. Atacurile atomice sau atacurile combinate sunt reprezentate prin tranziții compozite cu rate echivalente conform expresiilor prezentate mai sus[7];
- În baza ratelor echivalente astfel determinate este identificată cale de atac care are cea mai mică DMA;
- Verificarea și validarea modelului prin metoda construirii LMTC al GSPN, subiacent GSPNF cu ratele medii credibile respectiv identificate [4, 6]. În cazul în care modelul nu este corect, ce vor efectua modificările necesare în GSPNF astfel construit.

Reducerea modelului. Dacă există prea multe stări în modelul GSPNF astfel construit, putem simplifica acest model prin metoda prezentată mai sus, folosind relațiile (8), (9) și (10) [3]. Astfel, pentru modelul GSPNF $\Gamma M1$ din Fig. 5 comportamentele atacurilor combinate pot fi reprezentate mai simplu așa cum este arătat în Fig. 6. Rata

medie de declanşare a tranziţiilor temporizate compozite, astfel agregată, este $1/\overline{\tau}_{DMA\_j}$.

III. ESTIMAREA CELEI MAI BUNE CĂI DE ATAC

Vom considera cazul în care atacatorul lansează atacuri, de exemplu un atac DDOS, către nodul RC vizat ca stare finală [5, 6]. În timpul procesului de atac pot exista mai multe căi şi scopul principal al atacatorului constă în a obţine cea mai bună cale de atac. Fie γ^* este marimea pragului de cost al atacului, marimea maxtimă a căreia este determinată de cel mai mare cost stabilit. Tipul de atac, condiţionat de vulnerabililtatea nodurilor RC, determină rezultatele comportamentale ale atacatorilor. În modelul GSPNF astfel construit $p_{0,1}$ este locaţia de unde este lansat atacul, iar $p_{0,n0}$ este locaţia ţintă a atacului.

Ipoteza 1: Atacatorii sunt conştienţi de vulnerabilităţile care există în sistemul de securitate al RC (SRC) şi au capacitatea de a exploata aceste vulnerabilităţi şi cele ale aplicaţiilor curente pentru a aduce pagube acestei RC.

Ipoteza 2: Orice tranziţie $t_{i,1}$ ce se află în calea de atac este declanşată doar o singură dată. De asemenea, este presupusă o monotonie a comportamentelor de atac.

Algoritmul determinării celei mai bune căi de atac.

Pasul 1. Determinăm $p_{0,2}$, $p_{0,no}$ şi setăm iniţial valoarea *DMA* egală cu zero. Atribuim $\overline{\lambda}_{1,1}, \overline{\lambda}_{2,1}, ..., \overline{\lambda}_{n,1}$ tranziţiilor temporizate respective $t_{1,1}, t_{2,1}, ..., t_{n,1}$;

Pasul 2. Pornind de la locaţia iniţială, traversăm în modelul GSPNF toate căile posibile de atac prin algoritmul de căutare în adâncime şi de determinare a T-invarianţilor ale GSPN, subiacentă acestui model;

Pasul 3. Calculăm mărimea *DMA* a fiecărei combinaţii de atac folosind formulele de calcul respective ale operaţiilor secvenţiale, concurente şi de selecţie menţionate mai sus.

Pasul 4. Acumulăm mărimile *DMA* $\overline{\tau}_{Atac\_A_i}$ a fiecărui atac combinat pe calea de atac $Atac\_j$ considerată. Dacă mărimea *DMA* $\overline{\tau}_{DMA\_j}$ acumulată a căii de atac considerată este mai mare decât cea maxtimă de prag γ^*, atunci se va renunţa la această cale. În cele din urmă, sunt obţinute mărimile *DMA* ale fiecărei căi de atac posibil.

Pasul 5. Comparăm mărimile *DMA* ale fiecărei căi de atac $\overline{\tau}_{DMA\_j}$. Calea care are mărimea *DMA* minimă este cea mai bună cale de atac.

Pasul 6. Sfârşit.

Pentru a reduce complexitatea algoritmului, stabilim unele condiţii de limitare la luarea deciziilor. De exemplu, în al doilea pas, este considerată monotonicitatea căii de atac. În al patrulea pas, decidem dacă marimea *DMA* a căii explorate este mai mare decât cea de a pragului γ^*. Aceste restricţii vor reduce cu mult complexitatea algoritmului şi va spori caracterul practic al acestuia. În cazul în care modelul construit conţine m vârfuri şi n muchii, complexitatea calculului duratei necesare pentru a traversa toate locaţiile şi tranziţiile este de ordinul $O(m+n)$. Deci, acest tip de model satisface cerinţele de evaluare rapidă la atac a vulnerabilităţii securităţii RC.

Regulile de funcţionare ale unei reţele GSPN, subiacente GSPNF, şi cele de construire a lanţului Markov timp continuu (LMTC) inclus sunt descrise mai detaliat în [4].

V. STUDIU DE CAZ

Pentru a demonstra capabilitatea acestei abordări vom considera o reţea RC1 , structura căreia este prezentată în Fig. 4 [6]. RC1 este constituită din IP1 gazdă ce oferă servicii telnet, IP2 gazdă ce oferă servicii FTP, IP3 gazdă ce furnizează servicii cu baza de date şi IP4 gazdă ce oferă servicii HTTP. Fie că scopul atacatorului RC1 este de a controla trei IP gazdă pentru a lansa un atac de refuz al serviciului asupra IP4 gazdă. Informaţiile, privind vulnerabilitatea RC1, sunt prezentate în continuare.

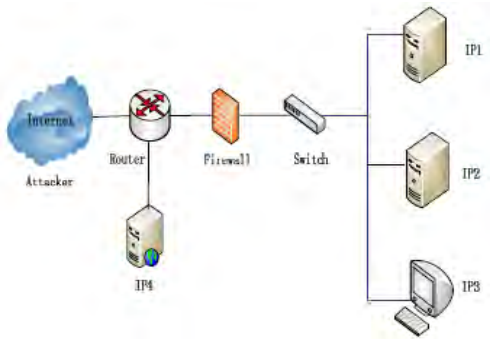

Fig. 4. Topologia RC1[6].

Modelul $\Gamma M1$ de GSPNF, construit prin activităţile descrise mai sus şi mai detaliat în [7], este prezentat în Fig. 5.

Valabilitatea şi eficacitatea modelului pot fi dovedite prin metoda construirii arborelui de accesibilitate şi a LMTC care este analizat folosind produsul program instrumental de analiză a modelelor GSPN: VPNP şi PIPE 2.5 [10]. Comportamentul atacului atomic A_m este compus din locaţia de intrare $p_{m,1}$ şi cea de ieşire $p_{m,2}$ a tranziţiei temporizate $t_{m,1}$, $m = 1,...,12$.

În modelul $\Gamma M1$ din Fig. 5, $p_{0,1}$ indică faptul că atacatorul doreşte să atace, iar $p_{0,2}$ faptul că atcul este lansat; $p_{0,3}$ indică faptul că scopul atacului este atins; $p_{i,1}$ şi $p_{i,2}$, $i = 1, 2, 3$ reprezintă respectiv starea atcatorului înainte şi după atacul respectiv a lui IP1, IP2, IP3; $p_{4,1}$ şi $p_{4,2}$ denotă starea atacatorului înainte şi după atacul IP2, când atacatorul este deja în IP1; $p_{5,1}$ şi $p_{5,2}$ denotă starea atacatorului înainte şi după atacul IP3, când atacatorul este deja în IP1; $p_{6,1}$ şi $p_{6,2}$ denotă starea atacatorului înainte şi după atacarea lui IP1, când atacatorul este deja în IP2; $p_{7,1}$ şi $p_{7,2}$ denotă starea atacatorului înainte şi după atacul IP3, când atacatorul este deja în IP2; $p_{8,1}$ şi $p_{8,2}$ denota starea atacatorului înainte şi după atacul IP1, când atacatorul este deja în IP3; $p_{9,1}$ şi $p_{9,2}$ denotă starea atacatorului înainte şi după atacul IP2, când

atacatorul este deja în IP3; $p_{j,1}$ și $p_{j,2}$, $j=10,11,12$ reprezintă respectiv starea atacatorului înainte și după realizarea atacului DDoS.

Din Fig. 5 determinăm că există trei căi de atac:

$$Atac\_1=[_1 A1\,|\,(A4 \veebar A5)\,|\,A10]_1,$$
$$Atac\_2=[_2 A2|\,(A6 \veebar A7)\,|\,A11]_2,$$
$$Atac\_3=[_3 A3\,|\,(A8 \veebar A9)\,|\,A12]_3.$$

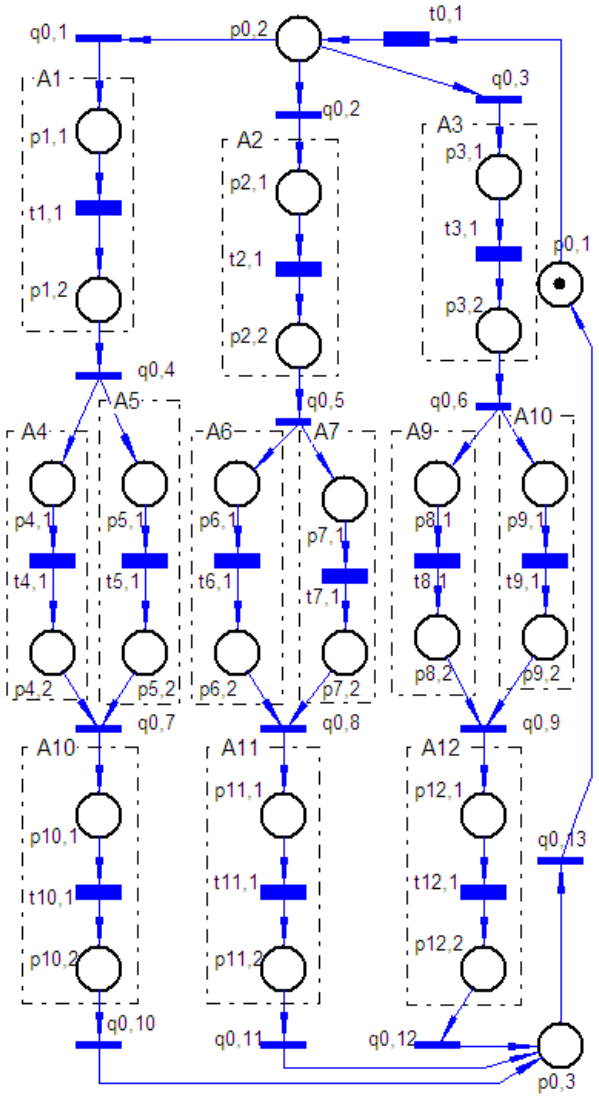

Figura 5. Modelul $\Gamma M1$ de rețea GSPNF al RC1.

Rolul tranzițiilor imediate $q_{0,k}$, $k=1,2,\cdots,12$ este de a conecta comportamentele combinate de atac respective, iar tranziția imediată $q_{0,13}$ denotă revenirea la starea inițială; $q_{0,1}$, $q_{0,2}$ și $q_{0,3}$ au aceeași probabilitate de declanșare. Ratele fuzzy de declanșare ale tranzițiilor temporizate $t_{0,1}$ și $t_{1,1},t_{2,1},...,t_{12,1}$ sunt respectiv $\widetilde{\lambda}_{0,1}$ $\widetilde{\lambda}_{1,1},\widetilde{\lambda}_{2,1},...,\widetilde{\lambda}_{12,1}$ în care, $t_{1,1},t_{6,1},t_{8,1}$ denotă atac de *revărsare trafic* (*overflow*) *Linux7.0-telnet* și de instalare a software-uli *troian*; $t_{2,1},t_{4,1},t_{9,1}$ denotă atac *revărsare trafic ServU5.0* și instalarea software-ului *troian*; $t_{3,1},t_{5,1},t_{7,1}$ denotă atac *Sql-no-password* și instalarea software-ului *troian*; $t_{10,1},t_{11,1},t_{12,1}$ reprezintă atac *DDoS*.

Analiza numerică. Folosind cunoștințele experților din domeniu [3], pentru ratele $\widetilde{\lambda}_j$ ale atacurilor, ce sunt variabile fuzzy, stabilim următoarele mărimi numerice:

$\widetilde{\lambda}_{0,1}=(0.005,0.008,0.03)$ (u.t.) sunt NFT;

$\widetilde{\lambda}_{1,1}=\widetilde{\lambda}_{6,1}=\widetilde{\lambda}_{8,1}=(0.1,0.2,0.4)$ (u.t.) sunt NFT;

$\widetilde{\lambda}_{2,1}=\widetilde{\lambda}_{4,1}=\widetilde{\lambda}_{9,1}=(0.05,0.15,0.2,0.4)$ (u.t.) sunt NFTz;

$\widetilde{\lambda}_{3,1}=\widetilde{\lambda}_{5,1}=\widetilde{\lambda}_{7,1}=(0.3,0.5,0.6)$ (u.t.) sunt NFT;

$\widetilde{\lambda}_{10,1}=\widetilde{\lambda}_{11,1}=\widetilde{\lambda}_{12,1}=(0.06,0.1,0.25,0.35)$ (u.t.) sunt NFTz.

În baza relațiilor (6) și (7) din secțiune 2 obținem următoarele mărimi ale ratelor medii credibile de atac:

$\overline{\lambda}_{0,1}=0{,}051$ (u.t.); $\overline{\lambda}_{1,1}=\overline{\lambda}_{6,1}=\overline{\lambda}_{8,1}=0.225$ (u.t.);

$\overline{\lambda}_{2,1}=\overline{\lambda}_{4,1}=\overline{\lambda}_{9,1}=0.200$ (u.t.); $\overline{\lambda}_{3,1}=\overline{\lambda}_{5,1}=\overline{\lambda}_{7,1}=0.475$ (u.t.); $\overline{\lambda}_{10,1}=\overline{\lambda}_{11,1}=\overline{\lambda}_{12,1}=0.19$ (u.t.).

Pentru aceste mărimi ale $\overline{\lambda}_{j,1}$ în baza relațiilor (8), (9) și (10) calculăm *DMA* $\overline{\tau}_{DMA\_j}$ pe calea respective de atac $Atac\_j$, j=1, 2, 3. În rezultat obținem:

$$\overline{\tau}_{DMA\_1}=1/\overline{\lambda}_{1,1}+(1/\overline{\lambda}_{4,1}+1/\overline{\lambda}_{5,1}-1/(\overline{\lambda}_{4,1}+\overline{\lambda}_{5,1}))+1/\overline{\lambda}_{10,1}=15.331 \text{ (u.t.)};$$

$$\overline{\tau}_{DMA\_2}=1/\overline{\lambda}_{2,1}+(1/\overline{\lambda}_{6,1}+1/\overline{\lambda}_{7,1}-1/(\overline{\lambda}_{6,1}+\overline{\lambda}_{7,1}))+1/\overline{\lambda}_{11,1}=15.382 \text{ (u.t.)};$$

$$\overline{\tau}_{DMA\_3}=1/\overline{\lambda}_{3,1}+(1/\overline{\lambda}_{8,1}+1/\overline{\lambda}_{9,1}-1/(\overline{\lambda}_{8,1}+\overline{\lambda}_{9,1}))+1/\overline{\lambda}_{12,1}=14.459 \text{ (u.t.)}.$$

Stabilim $\gamma^*=18{,}00$ (u.t.). În rezultat, constatăm că atacul pe calea $Atac\_3$ are *cea mai mică durată medie*, deci ea este *cea mai bună pentru a ataca*. Astfel, ar trebui să acordăm prioritate consolidării măsuri securității RC1în acest sens.

Modelul GSPN $\Gamma M2$ al GSPNF $\Gamma M1$ care este redus prin agregarea credibilă a ratelor medii este prezentat în figura 6. În acest model tranzițiile temporizate aggregate $t_{13,1}$, $t_{14,1}$ și $t_{15,1}$ reprezintă căile respective de atac $Atac\_j$, j=1, 2, 3.

Ratele de declanșare ale tranzițiilor din $\Gamma M2$ sunt:

$\overline{\lambda}_{13,1}=1/\overline{\tau}_{DMA\_1}=0.0653$, $\overline{\lambda}_{14,1}=1/\overline{\tau}_{DMA\_2}=0.0650$ și $\overline{\lambda}_{15,1}=1/\overline{\tau}_{DMA\_3}=0.0692$.

Pentru validarea acestor rezultate a fost efectuată simularea modelului $\Gamma M1$ prin metoda tradițională, folosind platformele software instrumentale VHPN și PIPE 2.5 [10]. Rezultatele acestei simulări sunt după cum urmează:

$\overline{\tau}'_{DMA\_1}=15.296$, $\overline{\tau}'_{DMA\_2}=15.397$ și $\overline{\tau}'_{DMA\_3}=14.418$.

Diferența dintre cele două abordări este foarte mică. Metoda tradițională de analiză a modelelor GSPNF, bazată LMTC inclus [4], are o complexitate de calcul în timp care, în caz general, este exponențială, pe când metoda de analiză prin reducerea modelului GSPNF prezentată în această lucrare are o complexitate liniară. Deci, metoda de

calcul prezentată în această lucrare este simplă şi mai practică.

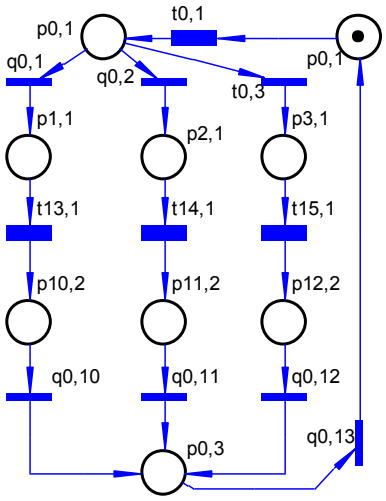

Fig.6. Modelul GSPN $\Gamma M2$ al GSPNF $\Gamma M1$ redus.

O generalizare a acestei abordări pe viitor poate fi efectuată în baza GSPN colorate (GSPNC) [8] cu rate fuzzy intuiționiste (GSPNFC) [1, 6] care oferă posibilitatea de a modela vulnerabilitățile RC și comportamentele atacatorilor într-un mod mult mai compact și mai nuanțat decât prin modele GSPNF, deoarece ele folosesc mecanisme de nivel înalt, similare cu cele ale limbajelor de programare: cu fiecare jeton este asociat o valoare a unui anumit tip de date (set de culori). Astfel, pentru un marcaj inițial dat numărul de comportamente ce pot fi exprimate de un model GSPNFC este cu mult mai mare decât cel prin GSPNF considerate în această lucrare.

Cu toate acestea GSPNF nu pot fi folosite pentru a descrie funcţionarea sistemelor ce trebuie reconfigurate în mod dinamic sau mobilitatea lor. Pe viitor vom considera și aceste aspect.

VI. CONCLUZII

Pentru a deveni mai nuanțate, cuprinzătoare și comprehensive, în lucrarea dată este propusă o metodă de modelare a atacurilor și analiză a vulnerabilității RC la atacuri prin rețele Petri stochastice generalizate (GSPN) cu rate fuzzy (GSPNF) credibil aggregate. Pentru fiecare tip de atac, este construit un model GSPNF care descrie intuitive în mod grafic relația dintre componentele acestora. Este prezentată o metodă de construire a modelului GSPNF, ce descrie mai nuanțat atacurile combinate concurente și colaborative ale atacatorului și o metodă de analiză a costului de exploatare a vulnerabilității RC. În același context, este prezentat un exemplu ce validează metoda propusă de analiză a vulnerabilității unei RC. Metoda propusă de evaluare a vulnerabilității RC este simplă și este ușor de efectuat prin manipulări automate. Ea poate ajuta administratorii de securitate de a elimina în mod eficient dezavantajele de securitate și pericolele ascunse în RC.

Pe viitor, vom considera modele GSPNF colorate în care vom lua în considerație aspectul stochastic fuzzy intuiționist de funcționare al RC cu aplicații orientat pe servicii reconfigurabile și vom prezenta mai detaliat aplicabilitatea acestui demers.

Lucrarea dată a fost efectuată în cadrul Proiectului Naţional de Cercetări Ştiinţifice Aplicative 15.817.02.28A din Republica Moldova.

REFERINȚE

[1] K. T. Atanassov,"Intuitionistic fuzzy sets," Fuzzy Sets and Systems, vol. 20, pp. 87-96, 1986.

[2] P. Ammann, D. Wijesekera, S. Kaushik, "Scalable graph-based network vulnerability analysis," Proceedings of the 9th ACM Conf. on Computer and Communications Security, pp. 217-224, 2002.

[3] L. Chuang, Q. Yang, Z.Bo, T. Li-qin," An Approach to Performance Equivalent Simplification and Analysis of Stochastic Petri Nets," *Acta Electronica SINICA*, vol. 30, pp. 1620-1623, 2002.

[4] G. Chiola, M. A. Marsan, G. Balbo, et al.," Generalized stochastic Petri nets: A definition at the net level and its implications," IEEE Transactions on Software Engineering, vol. 19, pp. 89-107, 1993.

[5] X. Gao, Y. Zhu, J. Fei, T. Han,"Method Based on GSCPN for Network Vulnerability Analysis," Journal of Software, vol. 8, no. 8, pp. 2032-2038, 2013.

[6] Gîrleanu, E. Guţuleac, Modelarea şi evaluarea riscului la atac al reţelelor Ad-hoc mobile prin reţele Petri cu jocuri stocastice fuzzy. Materialele Conf. Intern. ,"Modelare Matematică, Optimizare şi Tehnologii Informaţionale", vol. 1, Chişinău, 22-25 martie, pp.154-163, 2016.

[7] E. Guţuleac," Descriptive compositional HSPN modeling of computer systems,"Annals of the University of Craiova, Series: Atomation, Computers, Electronics and Mechatronics, Vol. 3(30), No.2, Ed.: Universitaria, Craiova, România, pp. 82-87, 2006.

[8] K. Jensen, Coloured Petri nets: Basic concepts analysis methods and practical use. Volume 1, Basic concepts. Berlin: Springer-Verlag, 1997.

[9] X. Li, B. Liu,"Foundation of credibilistic logic," Fuzzy Optimization and Decision Making, vol.8, no.1, pp. 91-102, 2009.

[10] Petri Nets Tools Database Quick Overview. https://www.informatik.uni-hamburg.de/TGI/PetriNets/tools/quick.html.

[11] A. Sh. Sendi, M. Dagenais, et al. ," Real Time Intrusion Prediction based on Optimized Alerts with Hidden Markov Mode,"*J. of Networks*, vol. 7, pp. 311-321, 2012.

[12] M. Tao, H. Shan,"An improved method of the attack tree model for mobile Ad -Hoc networks," Research. Computer Applications and Software, Vol. 26, Issue 4, pp. 271 – 273, 2009.

[13] Y. Wang, C. Lin, et al.," Analysis of Attack Actions for E-Commerce Based on Stochastic Game Nets Model,"J. of Computers, vol. 4, pp. 461-468, 2009.

[14] W.Yong-jie, et al.," Study of network security evaluation based on attack graph model,"Journal on Communications, vol. 28, pp. 29-34, 2007.

W. Zhuo, C. Lin, X. Chen, " Quantitative analysis method of network attack and defense based on stoc-hastic game model," J. of Computers, Vol. 9, p. 1748 – 1762, 2010.