MODELAREA ŞI ANALIZA SECURITĂŢII REŢELELOR DE CALCULATOARE PRIN REŢELE PETRI MARKOVIENE FUZZY INTUIŢIONISTE CU JOCURI STOCASTICE

Emilian Guţuleac, dr. hab, prof.univ., Igor Calmîcov, drd, Sergiu Zaporojan, dr.,conf.univ., Ion Gîrleanu, drd
Universitatea Tehnică a Moldovei

INTRODUCERE

Actualmente, sistemele de calcul (SC) şi reţelele de calculatoare (RC) cu arhitecturi orientate pe servicii în timp real cunosc o dezvoltare rapidă, atât sub aspectul complexităţii şi/sau al calităţii aplicaţiilor serviciilor caracterizate de indicatori QoS (Qualty of Service), cât şi al ariei de răspândire [6, 11, 17]. Acest tip de SC şi RC trebuie să aibă o flexibilitate, disponibilitate şi siguranţă în funcţionare (SF) deosebită.

RC prezintă vulnerabilităţi în ceea ce priveşte securitatea datelor şi creează dificultăţi în asigurarea serviciilor de securitate în faţa multor tipuri de atacuri cum ar fi: interceptarea pasivă, interferenţa activă, personificarea, blackhole (gaura neagră), manipularea datelor şi refuzul serviciului [7, 11, 17]. În acest context, apare necesitatea de a modela comportamentul atacatorilor şi a evalua unii indicatori SF ai RC, care este capacitatea acestora de aşi indeplini misiunea, într-un interval de timp stabilit, în prezenţa atacurilor intruşilor.

Analiza cantitativă a SF a diferitor SC şi RC a avut o mare atenţie timp de mai multe decenii. Cu toate acestea cuantificarea securităţii informationnale a RC şi a riscurilor de atac au atras doar recent mai multă atenţie. Lucrări conceptuale bazate pe modele matematice serioase de evaluare a atucurilor şi a mecanismelor de securitate au fost publicate doar recent [10, 11, 16, 19]. Metodele uzuale de modelare ale comportării atacatorilor şi a evaluării riscului compromiterii SF al RC sunt arborii de defectare şi de atac [17], teoria jocurilor matematice [19], lanţurile Markov timp continuu (LMTC) [16].

Abordarea prin LMTC poate fi folosită doar pentru modelarea unei clase restrânse a astfel de procese ce au un spaţiu mic de stări, deoarece el poate fi construit numai în mod manual şi deci, apar probleme cu validarea acestor tipuri de modele. În acest context, apare necesitatea de a automatiza procesul de construire al LMTC, luând în consideraţie astfel de fenomene cum ar fi: competiţia, sincronizarea, situaţii de conflict, excludere mutuală, aşteptare etc. [6, 7].

Modelarea şi simularea vizuală prin reţele Petri geralizate stocastice (RPGS) markoviene [6, 12] şi prin RPGS cu jocuri stocastice [7, 10] au devenit recent instrumente tot mai des utilizate în procesul decisional, atunci când este vorba de rezolvarea problemelor complexe de verificare funcţională şi evaluare a SF a sistemelor informationale, SC şi a RC care implică factori de incertitudine şi risc.

În cazul în care sunt utilizate RPGS, modelul de sistem va fi mult mai compact faţă de cel în formă de LMTC şi acest fapt facilitează procesul de modelare concisă şi analiză al acestuia. Un beneficiu suplimentar al abordării prin RPGS este faptul că putem folosi şi alte tipuri de distribuţii, decât cea exponential-negativă. Totodată, modelele RPGS pot fi uşor analizate, verificate şi evaluate prin intermediul unor instrumente software, cum ar fi GreatSPN, TimeNET, PIPE, VPNP etc. [5, 15].

Metodele tradiţionale de modelare şi analiză a indicatorilor QoS la atac [11, 16] folosesc date referitoare la parametrii componentelor (ratele de defectare şi de restabilire ale componentelor, ratele de atac şi apărare etc.) care se presupune că sunt cunoscute cu 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 defectare, vulnerabilitate şi atac. 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 incerţi. 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 prin utilizarea modelelor probabilistice [7, 8, 9]. 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 unui SC sau a unei RC, orice model probabilistic trebuie să includă şi comportamentul atacatorului. Acest aspect este unul dintre principalele provocări atunci când sunt utilizate tehnicile de modelare stocastică la cuantificarea 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 şi, de asemenea, pe o abordare bazată pe utilizarea numerelor fuzzy [2, 14, 18], pentru a reprezenta incertitudinea probabilităților de aflare în stările respective de atac ale RC.

În acest context, îmbinarea modelelor RPGS markoviene cu elemente ale teoriei *mulțimilor fuzzy intuționiste* (MFI) [1] şi ale teoriei jocurilor stocastice [10, 19], pentru a determina şi estima unele strategii aşteptate ale atacatorului, sunt mai bine potrivite la modelarea şi analiza indicatorilor QoS ai RC, care includ astfel de aspecte probabilistice, incertitudini şi imprecizii.

În această lucrare este prezentată o abordare de modelare şi evaluare a riscului de atac SF care imbină utilizarea metodelor logicii fuzzy intuționiste [1, 3, 13, 14] şi a jocurilor matriceale stocastice cu modele RPGS. În baza îmbinării acestor paradigme este definită o nouă clasă de RPGS fuzzy intuționiste cu jocuri stocastice, numite reţele RPJSFI, în baza cărora este efectuată modelarea comportamentului atacatorilor şi analiza unor indicatori cantitativi QoS ai acestor tip de RC.

Avantajul îmbinării unor astfel de paradigme constă în faptul că modelele RPJSFI descriu mai nuanţat comportamentul aşteptat al atacătorilor şi al apărării sistemului de securitate al RC. De asemenea, acest tip de modele permit de a evalua indicatorii cantitativi QoS ai RC atacate, a estima riscul de pierderi aşteptate, asociate cu diferite strategii de atac şi apărare.

Abordarea propusă permite să fie luate în consideraţie parametrii fuzzy în aplicarea metodologiei SF la modelarea şi evaluarea securității RC. Pentru a demonstra utilitatea acestei abordări în continuare este considerat un exemplu ilustrativ de modelare şi analiză securității unei RC.

1. RPGS FUZZY INTUIȚIONISTE CU JOCURI STOCASTICE

1.1. Elemente de numere fuzzy intuiționiste

Teoria mulţimilor fuzzy şi conceptele cu numere fuzzy [1, 3, 4, 13, 14, 18] au apărut din necesitatea de a exprima cantitativ mărimi imprecise, in care domeniul de valori pe care il ia funcția de apartenenţă nu mai este limitata la doua valori, ci se extinde la intreg intervalul [0, 1]. Însă, în lumea reală, există multe situații în care este necesar de a considera şi gradul de ezitare la luarea deciziilor. Astfel de situații pot fi tratate prin MFI şi numere fuzzy intuiționiste (NFI), introduse de Atanassov în [1] ca o generalizare a teoriei mulțimilor fuzzy în ceea ce priveşte gradul de *apartenență*, gradul de *non-apartenență* şi gradul de *ezitare*. Acest grad de ezitare nu este altceva decât incertitudinea la luarea unei decizii de către un factor decizional. Teoria MFI are aplicații practice în diferite domenii unde apar fenomene de incertitudine [3, 13, 14].

În teoria MFI elementul x din universul X, mulțime nevidă, este asociat cu gradul de apartenenţă (numit *acceptare*) precum şi gradul de non-apartenenţă (numit *respingere*), astfel încât suma lor aparține întotdeauna intervalului unitate [0;1]. Mulțimea fuzzy intuiționistă $\widetilde{A} \subseteq X$ este expresia $\widetilde{A} = \{< x, \mu_A(x), \nu_A(x) >: x \in X\}$, caracterizată prin funcțiile:

$\mu_{\widetilde{A}} : X \to [0, 1];\ x \in X \to \mu_{\widetilde{A}}(x) \in [0, 1]\}$ şi

$\nu_{\widetilde{A}} : X \to [0, 1];\ x \in X \to \nu_{\widetilde{A}}(x) \in [0, 1]\}$,

unde valorile $\mu_{\widetilde{A}}(x)$ şi $\nu_{\widetilde{A}}(x)$ sunt respectiv gradul de apartenenţă (*acceptare*), $x \in \widetilde{A}$, şi gradul de non-apartenenţă (*respingere*) al elementului x la $\widetilde{A}$, $x \notin X$, astfel încât aceştea, pentru $\forall x \in \widetilde{A}$, satisfac condiția: $0 \le \mu_{\widetilde{A}}(x) + \nu_{\widetilde{A}}(x) \le 1$. Gradul de indeterminare (*ezitare*, *şovăire*) al apartenenței elementului x la $\widetilde{A}$ este redat de funcția:

$$\eta_{\widetilde{A}}(x) = 1 - \mu_{\widetilde{A}}(x) - \nu_{\widetilde{A}}(x).$$

Cu cât valoarea lui $\mu_{\widetilde{A}}(x)$ este mai apropiata de 1, cu atât x este mai puternică apartenenţa la $\widetilde{A}$.

O submulțime $\widetilde{A}$ continuă a mulțimii numerelor reale IR este convexă dacă funcția $\mu_{\widetilde{A}}(x)$ este fuzzy intuiționistă convexă, iar funcția $\nu_{\widetilde{A}}(x)$ este fuzzy intuiționistă concavă, adică:

$\mu_{\widetilde{A}}(\iota \cdot x_1 + (1 - \iota \cdot)x_2)) \ge \min(\mu_{\widetilde{A}}(x_1), \mu_{\widetilde{A}}(x_2))$ şi

$\nu_{\widetilde{A}}(\iota \cdot x_1 + (1 - \iota \cdot)x_2)) \ge \max(\nu_{\widetilde{A}}(x_1), \nu_{\widetilde{A}}(x_2))$,

$\forall x_1, x_2 \in X, \quad 0 \le \iota \le 1$.

O submulțime fuzzy intuționistă $\widetilde{A}$ a mulțimii numerelor reale IR este un NFI dacă sunt satisfăcute următoarele proprietăți:

(i) $\widetilde{A}$ este normală, adică există cel puţin un punct $x_0 \in X$ astfel încât $\mu_{\widetilde{A}}(x_0) = 1$;

(ii) $\widetilde{A}$ este fuzzy intuiţionistă convexă;

(iii) $\mu_{\widetilde{A}}(x)$ (resp. $\nu_{\widetilde{A}}(x)$) este superior (inferior) semicontinuu pe IR;

(iv) $A = \{x \in IR : \nu_{\widetilde{A}}(x) < 1$ este mărginită.

Două tipuri de NFI sunt cel mai des întâlnite în aplicaţii [3, 13, 18]: NFI trapezoidale si cele triunghiulare. Utilizarea NFI triunghiulare (NFIT) este mai indicată, un motiv fiind şi acela al volumului de calcul. Astfel, un NFIT al $\widetilde{A}$ cu parametrii $a_1' \le a_1 \le a_2 \le a_3 \le a_3'$ este o submulţime a MFI în mulţimea numerelor reale IR pentru care:

$$\mu_{\widetilde{A}}(x) = \begin{cases} (x-a_1)/(a_2-a_1), & a_1 \le x \le a_2 \\ (a_3-x)/(a_3-a_2), & a_2 \le x \le a_3 \\ 0, \quad altfel \end{cases},$$

$$\nu_{\widetilde{A}}(x) = \begin{cases} (a_2-x)/(a_2-a_1'), & a_1' \le x \le a_2 \\ (x-a_2)/(a_3'-a_2), & a_2 \le x \le a_3' \\ 1, \quad altfel \end{cases}.$$

În literatura cu aplicaţii NFIT ale $\widetilde{A}$, acestea sunt reprezentate ca: $\widetilde{A} = [a_2; (a_1, a_3); (a_1', a_3')]$ sau prin aşa numite $(\alpha, \beta)-$ *tăieturi* (eng. (α, β)-*cuts*), notate $[\widetilde{A}^{\alpha}; \widetilde{A}^{\beta}]$, cu $\widetilde{A}^{\alpha} \cap \widetilde{A}^{\beta} = \varnothing$, unde $\widetilde{A}^{\alpha} = \{x \in X : \mu_{\widetilde{A}}(x) \ge \alpha\}$ şi $\widetilde{A}^{\beta} = \{x \in X : \nu_{\widetilde{A}}(x) \le \beta\}$ pentru orice $\alpha \in (0, 1]$ şi $\beta \in (0, 1]$, astfel încât este verificată relaţia: $0 \le \alpha + \beta \le 1$. Pentru reda un NFIT deseori sunt folosite următoarele expresii:

$$\widetilde{A}^{\alpha} = [a_1 + \alpha(a_2 - a_1), a_3 - \alpha(a_3 - a_2)] \text{ şi}$$

$$\widetilde{A}^{\beta} = [a_2 - \beta(a_2 - a_1'), a_2 + \beta(a_3' - a_2)].$$

În Fig. 1 este dat un exemplu de prezentare grafică a unor NFIT cu $\alpha = \beta = 0.5$.

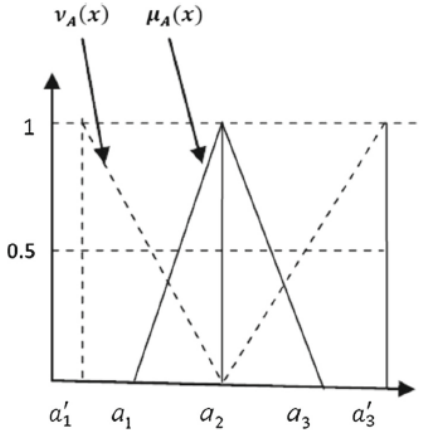

Figura 1. Reprezentarea grafică a NFIT cu o tăietură $\alpha = \beta = 0.5$.

De exemplu, fie $\widetilde{\lambda}_1 = [5; (3, 7); (1.5, 8)]$ este un NFIT. Redarea acestuia prin $(\alpha, \beta)-$ tăieturi este: $\widetilde{\lambda}_1 = [\widetilde{\lambda}_1^{\alpha}; \widetilde{\lambda}_1^{\beta}] = [(3 + 2\alpha, 7 - 2\alpha); (5 - 3.5\beta, 5 + 3\beta)]$.

În această lucrare vom folosi NFIT care vor fi redate şi prelucrate prin $(\alpha + \beta)-$ tăieturi, deoarece ele permit de a descrie într-un cadru unificator evaluarea şi analiza indicatorilor cantitativi QoS ai RC studiată.

1.2. Elemente de teoria jocurilor

Teoria jocurilor matematice (JM) oferă o gamă de instrumente care pot fi utilizate eficient la modelarea interacţiunii dintre nodurile independente ale RC şi atacatorii acesteia [7, 10 16, 19]. Metoda JM se bazează conceptul de recompensă, care are în vedere efectul de succes al atacurilor, precum şi costul posibil de detectare, atunci când se calculează strategia aşteptată a atacatorului. Într-un JM, jucătorii sunt factorii de decizii interdependente ale căror câştig depinde de acţiunile altor jucători cum ar fi atacatorii şi sistemul de securitate al RC. Îndată ce asupra unei RC a fost iniţiat un atac, atacatorul, în urma analizei vulnerabilităţii acesteia, are adesea posibilitatea de a alege între mai multe acţiuni atomice de atac. De asemenea, el poate decide de a întrerupe un atac în curs de desfăşurare într-o anumită stare sau să îl continue. O acţiune de atac poate fi considerată de succes, în cazul în care această acţiune produce o transformare nedorită a stării curente a RC.

Pentru a include aceste aspecte în probabilităţile de tranziţie între stările posibile ale modelului RPGS al atacatorului RC, este necesar să fie analizate toate opţiunile pe care un atacator le are în fiecare alte stări. Vom presupune că în fiecare stare $s_k, k = 1,...,n_s$ un atacator poate lua n_{sk} acţiuni de atac prin alegerea uneia dintre posibile acţiuni atomice de atac $a_i^k, i = 1,...,n_{sk} - 1$. Dacă prin acţiunea a_i^k atacatorul reuşeşte, el va primi o recompensă $\rho(a_i^k)$ asociată cu acest atac particular. În cazul în care el va eşua recompensa nu va fi obţinută, însă dacă această acţiune este detectată, atacatorul va fi penalizat de costurile asociate cu ea. Atacatorul poate întrerupe atacul în curs de desfăşurare prin acţiunea $a_{n_{sk}}^k$. Prin această opţiune el va fi penalizat de un cost, mărimea căruia depinde de faptul cât de departe a decurs atacul şi de probabilitatea că atacul ar fi rămas nedetectat, dacă el ar fi ales să continue.

Fie că în starea s_k jucătorul *A* (*atacătorul*) aplică acţiunile a_i^k, iar jucătorul *D* (*apărarea*)

aplică acţiunile d_j^k, iar matricea de plăţi al jocului este $\hat{\rho}^k = (\rho_{i,j}^k)$, $i, j = 1,...,n_{sk}$, $k = 1,...,n_s$, unde elementul $\rho_{i,j}$ reprezintă câştigul jucătorului A în cazul în care el foloseşte acţiunea a_i^k, iar jucătorul D modul de acţiune d_j^k. În acest joc J_A^k jucătorii A şi D au ca strategie mixtă vectorii de probabilitate respectivi:

$$\vec{q}_A^k = (q_A(a_1^k),...,q_A(a_{n_{sk}}^k)),$$
$$\vec{q}_D^k = (q_D(d_1^k),...,q_D(d_{n_{sk}}^k)).$$

Scopul atacatorului este de a maximiza câştigurile sale prin adoptarea anumitor strategii de atac $q_A(a_i^k)$, pe când sistemul va adopta strategia de apărare respectivă $q_D(a_i^k)$ pentru a minimiza pagubele sale în urma acestui atac. Astfel, câştigul mediu aşteptat de către atacator este exprimat de următoarea expresie [18] :

$$U^1 = \max_{a_j^k} \min_{d_j^k} \sum_{\forall a_i^k \in A} \sum_{\forall d_j^k \in D} q_A(a_i^k) \cdot q_D(d_j^k) \cdot \rho_{i,j}.$$

În această lucrare, pentru a descrie strategiile de atacuri, vom introduce jocuri stocastice în modele RPGS cu parametri NFIT.

1.3. Definirea şi regulile funcţionării RPJSFI

La studierea SF a diferitor tipuri de SC şi RC, cunoştinţele despre valorile parametrilor de defectare ale componentelor, ale ratelor de atac, ale riscurile de vulnerabilitate, etc. sunt, în general, mărimi imperfecte [2, 5, 7, 9, 13, 14]. Incertitudinea mărimilor reale ale parametrilor specificaţi poate avea două origini. Prima sursă de incertitudine provine din caracterul aleatoriu de informaţii care are o variabilitate naturală stocastică. A doua sursă de incertitudine, de evaluare epistemică a riscului de atac este legată de caracterul imprecis şi incomplet al informaţiilor din cauza lipsei de cunoştinţe despre mărimile reale ale parametrilor vulnerabilităţii RC şi ai atacatorilor ce îşi schimbă în mod dinamic stările lor. Deci, pentru a modela în mod mai realist incertudinea comportamentului atacatorilor şi reacţia de apărare a sistemului de securitate RC, este necesar de a lua în considerare atât aspectele probabilistice, cât şi cele fuzzy [1, 3]. Cum s-a menţionat, acest fapt poate fi realizat prin definirea unei noi extensii de RPGS în care unele atribute cantitative pot avea mărimi fuzzy intiuţioniste cu jocuri matriceale stocastice, în baza cărora sunt determinate probabilităţile fuzzy intiuţioniste de aflare în stările respective ale acestui tip de model şi a efectua analiza indicatorilor QoS aplicaţiilor de calcul orientate pe servicii.

În acest context, vom prezenta unele definiţii de bază necesare pentru înţelegerea abordării date.

Definiţia 1. O reţea Petri generalizată (RPG) [6], notată Γ, este o structură redată de un 10-tuplu de obiecte: $\Gamma = < P, T, Pre, Post, Test, Inh, K_p, Pri, G, M_0 >$, unde: P este mulţimea nevidă de *locaţii*, $|P| = k$. Locaţiile pot să conţină un număr întreg nenegativ de jetoane; T este mulţimea nevidă de *tranziţii*, $|T| = n$ şi $P \cap T = \varnothing$; *Pre*, *Test* şi $Inh : P \times T \times IN^{|P|} \to IN$ sunt, respectiv, funcţii de incidenţă înainte ale arcelor cu o cardinalitate marcaj-dependentă: *Pre* este funcţia de incidenţă înainte la tranziţii, *Test* este funcţia *promotor*, iar *Inh* este funcţia de *inhibiţie* a tranziţiilor; $Post : T \times P \times IN^{|P|} \to IN$ este funcţia de incidenţă înapoi la tranziţii; $K_p : P \times IN^{|P|} \to IN$ este funcţia de capacitate a locaţiilor; $\Pr i : T \times IN^{|P|} \to IN$ este funcţia de prioritate dinamică a declanşării tranziţiilor validate de marcajul curent; $G : T \times IN^{|P|} \to \{true, false\}$ este o funcţie de gardă a tranziţiilor; M_0 este marcajul iniţial; IN este mulţimea numerelor întregi nenegative.

Regulile de funcţionare ale reţelelor RPG tip Γ şi metodele de analiză ale proprietăţilor comportamentale ale acestora sunt descrise detaliat în [6].

Definiţia 2. O reţea RPG markoviană fuzzy intuiţionistă cu jocuri stacastice, denumită RPJSFI, este sistemul redat de 9-tuplul de obiecte $\widetilde{\Gamma} =< \Gamma, w, \hat{N}, \hat{q}, \hat{\rho}, \widetilde{\Lambda}, \mu_\lambda, \nu_\lambda, U >$, unde: Γ este o RPG temporizată stocastic în care mulţimea finită de tranziţii este partiţionată astfel încât: $T = T^0 \cup T^\tau$, $T^0 \cap T^\tau = \varnothing$, iar $\Pr i(T^0) > \Pr i(T^\tau)$ este prioritatea de declanşare a tranziţiilor validate. Aici T^0 este mulţimea tranziţiilor imediate (grafic sunt reprezentate prin bare subţiri) cu o durată de declanşare nulă, iar T^τ este mulţimea tranziţiilor temporizate (grafic sunt reprezentate prin dreptunghiuri negre) cu o durată aleatorie de declanşare ce are o distribuţie exponenţial–negativă; Funcţia de pondere $w(t, M)$ ce determină probabilitatea de declanşare $q(t, M)$ a tranziţiei imediate validate $t \in T_0(M)$ de către marcajul curent M, care descrie un selector probabilistic este $w : T_0 \times IN_+^{|P|} \to IR^+$; IR^+ este mulţimea mărimilor reale nenegative; $\hat{N} = \{1, 2, ..., \hat{n}\}$ denotă mulţimea de jucători; La rândul său mulţimea T^0 este partiţionată astfel încât $T^0 = (\bigcup_{l=1}^{\hat{n}} T_l^0) \bigcup T_{\hat{n}+1}^0$, $(\bigcap_{l=1}^{\hat{n}} T_l^0) \bigcap T_{\hat{n}+1}^0 = \varnothing$. Fiecare submulţime T_l^0, $l = 1,...,\hat{n}$ este asociată cu jucătorul l şi $T_{\hat{n}+1}^0$ este restul tranziţiilor imediate;

$\hat{q}: T^0 \to [0,1]$ este politica de decizie a unui jucător, reprezentată prin probabilitatea de a alege o tranziţie imediată particulară; $\hat{\rho}: T^0 \to (\hat{\rho}_1, \hat{\rho}_2, ..., \hat{\rho}_{\hat{n}})$ este funcţia de *recompensă* (eng. *reward*) a jucătorilor, unde $\hat{\rho}_l \in (-\infty, +\infty)$ primeşte valori din reale IR; $\widetilde{\Lambda}: T^\tau \times IN_+^{|P|} \to IR^+$ este funcţia ce determină rata fuzzy intuiţionistă $0 < \widetilde{\lambda}(t, M) < +\infty$ de declanşare a tranziţiei temporizate validate $t \in T^\tau(M)$ în marcajul curent M, adică parametrul legii exponenţial-negative; $\mu_\lambda : \widetilde{\Lambda} \to [0,1]$ şi $\nu_\lambda : \widetilde{\Lambda} \to [0,1]$ respectiv sunt funcţiile gradului de *apartenenţă* şi non *apartenenţă* al lui $\widetilde{\lambda}(t, M)$ la mulţimea fuzzy $\widetilde{\Lambda}$ care determină valorile NFI ale ratelor de declanşare ale tranziţiilor temporizate. ***U*** este funcţia de *câştig* a jucătorilor.

Analiza modelelor RPJSFI prin abordarea propusă în această lucrare este efectuată în două etape. Prima etapă este aceeaşi ca şi cea convenţională de modelare prin RPGS şi analiza acestora [6, 7]. Unica diferenţă este acea că distribuţia probabilităţilor staţionare de stare ale RPGS este obţinută parametric utilizând LMTC generat de RPGS. Cu alte cuvinte, fiecare probabilitate staţionară de stare π_i este descrisă în termenii ratelor nefuzificate de declanşare ale tranziţiilor, adică în funcţie de λ_i ca mărimi certe, care reflectă numai natura stocastică a proceselor sistemului modelat. În a doua etapă ratele de declanşare ale tranziţiilor sunt reprezentate prin mărimi ce sunt NFIT $\widetilde{\lambda}_i = (\widetilde{\lambda}_i^\alpha; \widetilde{\lambda}_i^\beta)$ care depind de contextul de identificare, de exemplu, cel prezentat de experţi.

După înlocuirea mărimilor numerice fuzzy ale $\widetilde{\lambda}_i$, folosind teoria de calcul fuzzy, obţinem (α, β) - tăieturi [18] ale probabilităţilor staţionare de stare fuzzy $\widetilde{\pi}_i(\alpha, \beta)$ ale LMTC subiacent RPJSFI. În conformitate cu lucrările [7, 8, 18] vom folosi aritmetica intervalelor cu (α, β) - tăieturi pentru a calcula funcţiile variabilelor fuzzy intuiţioniste, în baza cărora putem obţine mai multe informaţii decât prin utilizarea principiului de prelungire [1]. Pentru a putea găsi (α, β)- tăieturi fezabile ale $\widetilde{\pi}_i(\alpha, \beta)$ poate apărea necesitatea de a rezolva şi o problemă de optimizare, care face ca soluţia să fie fezabilă [8].

În continuare, cu scopul de a arăta utilitatea utilizeării abordării prezentate în această lucrare, vom considera un exemplu simplu (similar cu cel din [16]). Din cauza limitărilor de spaţiu, acest exemplu este extrem de abstract, însă el ilustrează elocvent abordarea propusă.

2. STUDIU DE CAZ PRIN RPJSFI

În acest context, vom considera o mică reţea de calculatoare (RC1), ilustrată în Fig. 2, care constă dintr-o staţie de lucru (*workstation*), un *webserver* public şi un *fileserver* privat.

Vom presupune că pe parcursul funcţionării sale sistemul de securitate al RC dispune de mecanisme suficiente de detectare ale intruziunilor cu un comportament suspicios şi de restabilire a componentelor compromise. De asemenea, vom presupune că, odată ce un atacator a luat controlul asupra oricărei dintre posibilele obiective, probabilităţile atacurilor reuşite împotriva ţintelor rămase vor creşte.

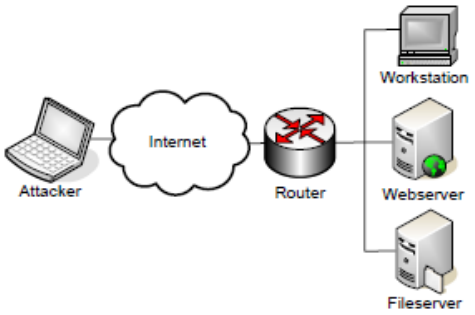

***Figura** 2.* Topologia reţelei de calculatoare RC1 atacată, similară cu cea din [16] .

Acţiunile a_i ale atacatorului acestei RC sunt: $A = \{a_1, a_2, a_3, \varnothing\}$, unde $a_1 =$"*atac workstation*", $a_2 =$"*atac webserver*", $a_3 =$"*atac fileserver*" şi $a_4 =$" *nu atacă*". De asemenea, vom presupune că priorităţile atacatorului, recompensele şi costurile acţiunilor sale sunt în prealabil determinate. Odată ce atacul a reuşit printr-una dintre ţintele sale, atacatorul se va concentra doar pe obiective cu o prioritate mai mare.

În Fig. 3 este prezentat modelul RPGS1, subiacentă RPJSFI1, care descrie comportamentul atacatorului. În acest model ratele de atac, de compromitere a RC1 şi a remedierii ei sunt NFIT, iar acţiunile de atac sunt redate de tranziţii imediate.

Semnificaţia locaţiilor şi a tranziţiilor RPGS1 din Fig. 3 pentru partea modelului atacator este:

- *locaţii*: p_1 - starea în care RC funcţionează în mod corect, intrusul nu atacă; p_2 - intrusul alege acţiunea de atac; p_3, p_4 şi p_5 - intrusul atacă RC1 prin acţiunea respectivă a_1, a_2 şi a_3; p_6 - workstation atacată este compromisă; p_7 - fileserver-ul

fiind compromis, intrusul continue atacul prin acțiunile a_2 și a_3; p_8 - webserver-ul fiind compromis, intrusul continue atacul prin acțiunea a_3; p_9 - atacul webserver-ului este depistat, administratorul RC începe restabilirea lui;

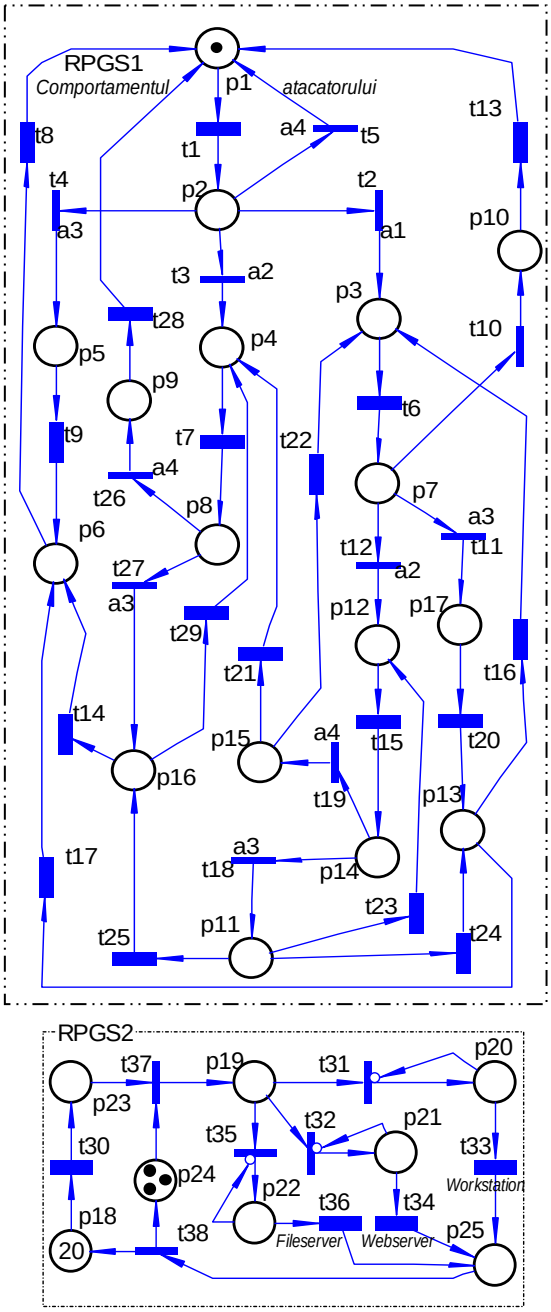

Figura 3. Modelul de rețea RPGS1 și RPGS2 subiacente RPJSFI1 al RC1 atacată.

p_{10} - atacul workstation este depistat, administratorul RC1 începe restabilirea acesteia; p_{11} - starea în care workstation, webserver-ul și fileserver-ul sunt toate compromise; p_{12} - workstation și webserver-ul sunt compromise; p_{13} - workstation și fileserver-ul sunt compromise; p_{14} - alegerea acțiunii de atac a_3, deja fiind com-promise *workstation* și *webserver*-ul; p_{15} - intrusul nu atacă, este declanșată restabilirea *workstation* și a *webserver*-ului; p_{16} - este declanșată restabilirea *fileserver*-ului și a *webserver*-ului. p_{17} - *workstation* și *fileserver*-ul sunt compromise.

- *tranziții temporizate*: t_1 - atacul RC1 de către intrus; t_6 - atacul reușit al *workstation*; t_7 - atacul reușit al *webserver*-ului; t_8 - restabilirea *fileserver*-ului compromis; t_9 - atacul reușit al *fileserver*-ului; t_{13} - restabilirea *workstation* compromisă din starea p_{10}; t_{14} - restabilirea *webserver*-ului compromis; t_{15} - atacul și compromiterea *webserver*-ului; t_{16} - restabilirea *fileserver* compromis din starea p_{13}; t_{17} - restabilirea *workstation* compromisă în starea p_{13}; t_{20} - atacul și compromiterea *fileserver* din starea p_{17}; t_{21} și t_{22} - restabilirea respectivă a *workstation* și *webserver*, compromise în starea p_{15}; t_{23}, t_{24} și t_{25} - restabilirea respectivă a *webserver, fileserver* și *workstation* , compromise în starea p_{11}; t_{28} - restabilirea *workstation* compromisă în starea p_9; t_{29} - t_{28} - restabilirea *workstation* compromisă în starea p_{16}.

- *tranziții imediate*: t_2, t_3, t_4 și t_5 - acțiunile respective de atac a_1, a_2, a_3 și a_4; t_{10}, t_{11} și t_{12} - acțiunile respective de atac a_2, a_3 și a_4 după compromiterea *workstation* din starea p_3; t_{18} și t_{19} - acțiunile respective de atac a_3 și a_4 după compromiterea *webserver*-ului din starea p_{14}; t_{26} și t_{27} - acțiunile respective de atac a_4 și a_3 după compromiterea *workstation* din starea p_{16}.

Semnificația locațiilor și a tranzițiilor RPGS2 din Fig. 3 pentru partea modelului RC1 atacată este:

- *locații:* p_{18} - pachete ce trebuie procesate; p_{18} - selectarea tipului de procesare; p_{20} - pachet în curs de procesare de către *workstation*; p_{21} - pachet în curs de procesare de către *webserver*; p_{22} - pachet în curs de procesare de către *fileserver*; p_{23} - fir de așteptare a pachetelor; p_{24} - număr de servere libere; p_{25} - pachet deja procesat.

- *tranziţii imediate*: t_{31}, t_{32} şi t_{35} - selectarea modului de procesare a unui pachet; t_{37} - alocarea unui server liber; t_{38} - eliberarea serverelor.

- *tranziţii temporizate*: t_{30} - sosirea pachetelor în reţea; t_{33}, t_{34} şi t_{36} - procesarea pachetelor de către serverele respective. Aceste tranziţii au funcţii de gardă, care depind de stările respective ale RPGS1:

$g(t_{33}) = (m_3 = 0) \& (m_{11} = 0) \& (m_{12} = 0) \& (m_{13} = 0),$

$g(t_{34}) = (m_4 = 0) \& (m_{11} = 0) \& (m_{12} = 0) \& (m_{16} = 0),$

$g(t_{36}) = (m_5 = 0) \& (m_{11} = 0) \& (m_{16} = 0) \& (m_{13} = 0),$

unde $m_i = M(p_i)$ este marcajul curent al lui p_i. Apariţia unui jeton în aceste locaţii indică la faptul că serverul respectiv este compromis, atacul a reuşit, pachetele nu pot fi procesate şi se va declanşa procedura de restabilire a acestui server.

Modelul RPJSFI1 a fost validat, folosind produsul program instrumental VPNP [5] de simulare vizuală, verificare şi evaluare a indicatorilor QoS ale modelelor tip RPSG.

Graful redus de marcaje accesibile, în formă de listă simbolică, al modelului RPGS1 care descrie comportamentul părţii atacatorului RC1 este:

M0 = [p1] [t1t2>M1, t1t3>M2, t1t4>M3;
M1 = [p3] [t6t10>M5, t6,t11>M6, t6t12>M7;
M2 = [p4] [t7t26>M8, t7t27>M9; **M3** = [p5] [t9>M4;
M4 = [p6] [t8>M0; **M5** = [p10] [t13>M0;
M6 = [p17] [t20>M10;
M7 = [p12] [t15t18>M11, t15t19>M12;
M8 = [p9] [t28>M0; **M9** = [p16] [t14>M4, t29>M2;
M10 = [p13] [t16>M1, t17>M4;
M11 = [p11] [t23>M7, t24>M10, t25>M9;
M12 = [p15] [t21>M2, t22>M1;

Analiza proprietăţilor comportamentale ale RPGS1 arată că ea este *mărginită*, *viabilă* şi *reiniţializabilă* [6, 12]. Deci, LMTC1 care descrie funcţionarea ei este ergodic [12], iar sistemul de ecuaţii ce descrie funcţionarea modelului RPGS1 în regim staţionar este:

$$\begin{gathered}
\lambda_1\pi_0 = \lambda_8\pi_4 + \lambda_{13}\pi_5 + \lambda_{28}\pi_8, \ \lambda_9\pi_3 = \lambda_1 q_4\pi_0 \\
\lambda_6\pi_1 = \lambda_1 q_2\pi_0 + \lambda_{16}\pi_{10} + \lambda_{22}\pi_{12}, \\
\lambda_7\pi_2 = \lambda_1 q_3\pi_0 + \lambda_{29}\pi_9 + \lambda_{21}\pi_{12}, \\
\lambda_8\pi_4 = \lambda_9\pi_3 + \lambda_{14}\pi_9 + \lambda_{17}\pi_{10}, \\
\lambda_{13}\pi_5 = \lambda_6 q_{10}\pi_1, \ \lambda_{20}\pi_6 = \lambda_6 q_{11}\pi_1, \quad (1) \\
\lambda_{15}\pi_7 = \lambda_6 q_{12}\pi_1 + \lambda_{23}\pi_{11}, \ \lambda_{28}\pi_8 = \lambda_7 q_{26}\pi_2, \\
(\lambda_{14} + \lambda_{29})\pi_9 = \lambda_7 q_{27}\pi_2 + \lambda_{25}\pi_{11}, \\
(\lambda_{16} + \lambda_{17})\pi_{10} = \lambda_{20}\pi_6 + \lambda_{24}\pi_{11}, \\
(\lambda_{23} + \lambda_{24} + \lambda_{25})\pi_{11} = \lambda_{15} q_{18}\pi_7, \\
(\lambda_{21} + \lambda_{22})\pi_{12} = \lambda_{15} q_{19}\pi_2, \ \ 1 = \sum_{i=0}^{12}\pi_i,
\end{gathered}$$

unde λ_j sunt ratele de declanşare cu valori certe ale tranziţiilor temporizate, iar q_l sunt probabilităţile de declanşare cu valori certe ale tranziţiilor imediate care redau alegerea acţiunilor de atac ale jocurilor stocastice respective.

După obţinerea probabilităţilor staţionare de stare π_i, exprimate parametric în termeni ai ratelor de declanşare ale tranziţiilor, acestea apoi sunt reprezentate ca NFIT. Intervalele aritmetice al acestor NFIT sunt redate prin metoda de (α, β)-tăieturi, bazată pe folosirea operatorilor *max* şi *min* care pot produce intervale mai mari. Menţionăm că $\alpha = 0$ şi $\beta = 1$ reprezintă cel mai mare interval de probabilitate pe când pentru $\alpha = 1$ şi $\beta = 0$ obţinem probabilităţile de stare certe ale LMTC1. Teoretic, (α^*, β^*) - tăietură a unui NFI oferă cel mai mare interval posibil de valori. Din moment ce ne dorim să fie calculate probabilităţile $\tilde{\pi}_i = [\pi_i^\alpha, \pi_i^\beta]$, cel mai mare interval posibil al acestora este limitat la intervalul $\tilde{\pi}_i \in [0, 1]$, $i = 0, 1, 2, ..., N$, unde $N+1$ este numărul de stări al LMTC1. Problema este de a găsi o astfel de (α^*, β^*) - tăietură optimală, care va satisface această condiţie şi ea poate fi găsită rezolvând următoarea problema de optimizare $\alpha = \alpha^*$ şi $\beta = \beta^*$ [8] pentru ca soluţia sistemului de ecuaţii (1) să fie fezabilă şi pentru NFIT $\tilde{\pi}_i$:

$$Min(Z) = \alpha$$

cu restricţiile: $\pi_i^+(\alpha) \le 1; \ \pi_i^-(\alpha) \ge 0;$

$0 \le \alpha \le 1; \ \pi_i^-(\alpha) \le \pi_i^+(\alpha),$

şi $Max(Z) = \beta$

cu restricţiile: $\pi_i^-(\beta) \le 1; \ \pi_i^+(\beta) \ge 0;$

$0 \le \beta \le 1; \ \pi_i^-(\beta) \ge \pi_i^+(\beta).$

3. ANALIZA NUMERICĂ A QoS

În această secţiune, vom evalua indicatorii de securitate şi de performanţă ai RC1 atacată, definiţi în continuare prin calcularea probabilităţilor $\tilde{\pi}_i(\alpha, \beta)$ ale LMTC1, subiacent RPGS1 şi ale LMTC2 al RPGS2.

3.1. Analiza confidenţialităţii

În mod similar cu [7], unii indicatori SF de securitate sunt consideraţi ca fiind *confidenţialitatea costurile de securitate* şi *productivitatea* ale RC, care sunt funcţii de probabilităţile NFI $\tilde{\pi}_i(\alpha, \beta)$, $i = 0, 1, ..., n_s$. Aceste probabilităţi NFI pot fi interp-

retate ca proporţia duratei de timp în care LMTC1 se află în starea M_i. În cazul în care atacul are succes, atacatorul poate naviga în mod neautorizat prin fişierele RC1. Astfel, în modelul RPGS1 marcajul M_0 denotă starea de aflare a RC1 în bună funcţionare, adică componentele ei nu sunt atacate. Celelalte marcaje indică la faptul că RC1 este atacată şi unele componente ale acesteia sunt compromise. Prin urmare, indicatorul QoS de confidenţialitate al RC1 în regim staţionar, funcţie de α şi β, este calculat în baza expresiei:

$$\widetilde{\pi}_{Conf.}(\alpha,\beta)=\widetilde{\pi}_0(\alpha,\beta). \qquad (2)$$

În acest context, vom considera un exemplu numeric de evaluare şi analiză a acestui indicator pentru următoarele valori NFI $\hat{\lambda}_i=\widetilde{\lambda}_i\cdot 10^4$ sec^{-1} ale ratelor de declanşare ale tranziţiilor temporizate respective cu $\widetilde{\lambda}_i=[\widetilde{\lambda}_i^{\alpha};\widetilde{\lambda}_i^{\beta}]$:

$$\widetilde{\lambda}_1=[(0.1+0.9\alpha),(1.1-0.1\alpha);\ (1-0.95\beta),(1+0.2\beta)],$$
$$\widetilde{\lambda}_6=\widetilde{\lambda}_9=\widetilde{\lambda}_{15}=[(3+\alpha,5-\alpha);(4-2\beta,4+2\beta)],$$
$$\widetilde{\lambda}_7=\widetilde{\lambda}_{20}=[(2+\alpha,4-\alpha);(3-2\beta,3+2\beta)], \qquad (3)$$
$$\widetilde{\lambda}_8=\widetilde{\lambda}_{16}=\widetilde{\lambda}_{23}=\widetilde{\lambda}_{29}=[(3+\alpha,5-\alpha);(4-2\beta,4+2\beta)],$$
$$\widetilde{\lambda}_{13}=\widetilde{\lambda}_{17}=\widetilde{\lambda}_{21}=\widetilde{\lambda}_{25}=[(7+\alpha,9-\alpha);(8-2\beta,8+2\beta)],$$
$$\widetilde{\lambda}_{14}=\widetilde{\lambda}_{22}=\widetilde{\lambda}_{24}=\widetilde{\lambda}_{28}=[(5+\alpha,7-\alpha);(6-2\beta,6+2\beta)].$$

În modelul RPSFI1 avem patru jocuri stocastice $J_A^1(p_l)$, redate de locaţiile p_l cu tranziţiile imediate respective, incidente înapoi la p_l, $t_j\in p_l^{\bullet}$ şi anume: $J_A^1(p_2)$, $J_A^2(p_7)$ $J_A^3(p_8)$ şi $J_A^4(p_{14})$.

Matricea de plăţi $\hat{\rho}_A^{J1}(p_2)$ a jocului $J_A^1(p_2)$ este:

$$\hat{\rho}_A^{J1}(p_2)=\begin{array}{c} \\ a_1\\ a_2\\ a_3\\ a_4\end{array}\begin{array}{c}\begin{array}{cccc} d_1 & d_2 & d_3 & d_4\end{array}\\ \begin{bmatrix}20 & 30 & 50 & 20\\ 40 & 10 & 20 & 50\\ 30 & 50 & 40 & 20\\ 10 & 30 & 30 & 40\end{bmatrix}\end{array},$$

Pentru jocul $J_A^1(p_2)$ obţinem strategiile:

$$\vec{q}_{J_1}^{\,1}(a_i)=(0.061,\ 0.388,\ 0.510,\ 0.041),$$
$$\vec{q}_{J_1}^{\,2}(d_j)=(0.082,\ 0.143,\ 0.367,\ 0.408).$$

Câştigul acestui joc este: $U_{J_1}=32.45$.

Pentru jocul $J_A^2(p_7)$ cu matricea de plăţi:

$$\hat{\rho}_{A_{J2}}(p_7)=\begin{array}{c} \\ a_2\\ a_3\\ a_4\end{array}\begin{array}{c}\begin{array}{ccc} d_2 & d_3 & d_4\end{array}\\ \begin{bmatrix}40 & 20 & 50\\ 35 & 40 & 20\\ 25 & 30 & 40\end{bmatrix}\end{array}$$

obţinem strategiile:

$$\vec{q}_{J2}^{\,1}(a_i)=(0.200,\ 0.467,\ 0.333),$$
$$\vec{q}_{J_1}^{\,2}(d_j)=(0.133,\ 0.533,\ 0.333),$$

câştigul cărora este: $U_{J2}=32.67$.

În acelaşi mod pentru jocurile $J_A^3(p_8)$ şi $J_A^4(p_{14})$ cu matricea de plăţi $\hat{\rho}_{A_{J3}}(p_7)=\hat{\rho}_{A_{J4}}(p_{14})$, elementele cărora sunt :

$$\rho_{3,3}=40,\ \rho_{3,4}=20,\ \rho_{4,3}=30,\ \rho_{4,4}=40,$$

obţinem strategiile:

$$\vec{q}_{J3}^{\,1}(a_i)=\vec{q}_{J4}^{\,1}(a_i)=(0.333,\ 0.667),$$
$$\vec{q}_{J_3}^{\,2}(d_j)=\vec{q}_{J_4}^{\,2}(d_j)=(0.667,\ 0.333)$$

cu câştigul: $U_{J3}=U_{J4}=33.33$.

Substituind în sistemul de ecuaţii (1) mărimile numerice redate de expresiile (3) şi a strategiilor jocurilor astfel definite, obţinem soluţiile acestui sistem de ecuaţii pentru intervalele respective stânga şi dreapta:

$$\widetilde{\lambda}_i^{\alpha}=(\widetilde{\lambda}_i^{\alpha-},\widetilde{\lambda}_i^{\alpha+}),\ \widetilde{\lambda}_i^{\beta}=(\widetilde{\lambda}_i^{\beta-},\widetilde{\lambda}_i^{\beta+}).$$

Analiza detaliată a acestor soluţii pentru valorile NFIT prezentate de expresiile (2) ale acestui exemplu arată că sunt verificate relaţiile:

$$\forall\alpha\in[0,\ 1],\ 0<\pi_i^-(\alpha)\le\pi_i^+(\alpha)<1 \text{ şi } \forall\beta\in[0,\ 1],$$
$$0<\pi_i^+(\beta)\le\pi_i^-(\beta)<1,\ i=0,\ 1,...,12.$$

De asemenea, această analiză arată că nivelul de confidenţialitate al RC1 este sub formă de NFIT şi valorile lui (pentru datele considerate de expresiile (3)) se află, cu un anumit grad de certitudine, în intervalul $[0.526317,\ 0.661832]$, adică $\widetilde{\pi}_{Conf.}(\alpha,\beta)=[\widetilde{\pi}_0(\alpha);\widetilde{\pi}_0(\beta)]$, unde:

$$\widetilde{\pi}_0(\alpha)=(0.526317+0.073083\ \alpha,$$
$$0.661832-0.062432\ \alpha);$$
$$\pi_0(\beta)=(0.5994-0.184248\beta,\ 0.5994+0.091008\beta).$$

Pentru aceste valori NFIT, gradul de *apartenenţă* (*certitudine*) $\mu_{\widetilde{\pi}_0}(x)$ la $\widetilde{\pi}_{Conf.}(\alpha,\beta)$ al RC1 este:

- $\mu_{\widetilde{\pi}_0}(x)=(x-0.526317)/0.073083$ pentru $0.52637\le x\le 0.599400$,
- $\mu_{\widetilde{\pi}_0}(x)=(0.661832-x)/0.062432$ pentru $0.599400\le x\le 0.661832$,
- altfel $\mu_{\widetilde{\pi}_0}(x)=0$.

De asemenea, gradul de *non-apartenenţă* (*incertitudine*) $\nu_{\widetilde{\pi}_0}(x)$ la $\widetilde{\pi}_{Conf.}(\alpha,\beta)$ al RC1 este:

- $\nu_{\widetilde{\pi}_0}(x)=(0.599400-x)/0.184248$ pentru $0.415152\le x\le 0.599400$,
- $\nu_{\widetilde{\pi}_0}(x)=(x-0.599400)/0.091008$ pentru $0.599400\le x\le 0.690408$,
- altfel $\nu_{\widetilde{\pi}_0}(x)=0$.

Gradul de *ezitare* $\eta_{\tilde{\pi}_0}(x)$ la intervalul respectiv al confidenţilităţii RC1 este calculat în conformitate cu expresia:

$$\eta_{\tilde{\pi}_0}(x) = 1 - \mu_{\tilde{\pi}_0}(x) - \nu_{\tilde{\pi}_0}(x).$$

În Fig. 4 sunt prezentate graficele respective ale gradului de *certitudine, incertitudine* şi *ezitare,* notate respectiv $\mu\pi 0, \nu\pi 0$ şi $\eta\pi 0$, ale confidentiallităţii RC1 funcţie de $\tilde{\pi}_0(\alpha, \beta)$.

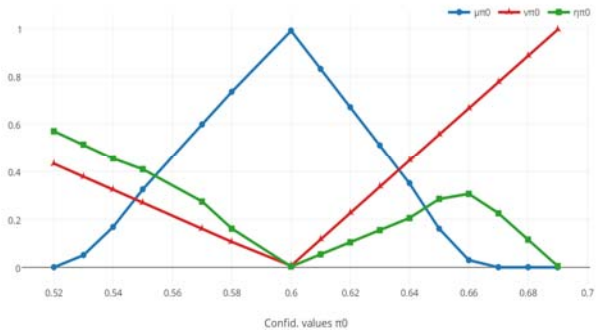

Figura 4. Graficele gradelor de *certitudine, incertitudine* şi *ezitare* ale confidenţialităţii RC1.

2.3. Evaluarea productivităţii serverelor

Pentru a evalua influenţa coruperii sistemului de securitate, ca rezultat reuşit al atacului, asupra productivităţii serverelor RC1 vom presupune că durata totală de viaţă a acestuia este $\bar{\tau}$. Deoarece firul de aşteptare în p_{23} este stabil limitat, numărul mediu de pachete $E[\tilde{\lambda}_{RC1}^{z_i}]$ deservite de către serverul respectiv al RC1 trebuie să fie:

$$E[\tilde{\lambda}_{RC1}^{z_1}] = \lambda_{33} \cdot \tilde{\pi}_x \cdot \bar{\tau},\ E[\tilde{\lambda}_{RC1}^{z_2}] = \lambda_{34} \cdot \tilde{\pi}_y \cdot \bar{\tau},$$

$E[\tilde{\lambda}_{RC1}^{z_3}] = \lambda_{36} \cdot \tilde{\pi}_z \cdot \bar{\tau}$, unde:

$$\tilde{\pi}_x = 1 - (\tilde{\pi}_1 + \tilde{\pi}_7 + \tilde{\pi}_{10} + \tilde{\pi}_{11}),$$
$$\tilde{\pi}_y = 1 - (\tilde{\pi}_2 + \tilde{\pi}_7 + \tilde{\pi}_9 + \tilde{\pi}_{11}),$$
$$\tilde{\pi}_z = 1 - (\tilde{\pi}_3 + \tilde{\pi}_9 + \tilde{\pi}_{10} + \tilde{\pi}_{11}).$$

Aici $\tilde{\pi}_x$, $\tilde{\pi}_y$ şi $\tilde{\pi}_z$ denotă respectiv probabilităţile că *workstation*, *webserver*-ul şi *fileserver*-ul nu sunt compromise, iar λ_{33}, λ_{34} şi λ_{35} sunt ratele respective de prelucrare a pachetelor de către aceste servere.

Pentru $\lambda_{30} < (\lambda_{33} + \lambda_{34} + \lambda_{36})$, numărul total de lucrări deservite în acest mod este $E[\tilde{\lambda}_{RC}]$. În stările nesecurizate toate pachetele expediate la servere nu mai sunt sigure şi deci ele vor fi anulate, deoarece acestea nu contribuie la evaluarea productivităţii sistemului. Astfel, în această stare, productivitatea sistemului este determinată doar de lucrările executate de RC1 la nivel local. Prin urmare, conform *legii Little* relativ la sistemele de aşteptare [6, 12] obţinem următoarea relaţie care determină *productivitatea* (engl. *Throughput*) RC1:

$$\tilde{\lambda}_{Thr.}^{z_1} = E[\tilde{\lambda}_{RC1}^{z_1}]/\bar{\tau} = \lambda_{33} \cdot \tilde{\pi}_x,$$
$$\tilde{\lambda}_{Thr.}^{z_2} = E[\tilde{\lambda}_{RC1}^{z_2}]/\bar{\tau} = \lambda_{34} \cdot \tilde{\pi}_y,$$
$$\tilde{\lambda}_{Thr.}^{z_3} = E[\tilde{\lambda}_{RC1}^{z_3}]/\bar{\tau} = \lambda_{36} \cdot \tilde{\pi}_z.$$

Analiza acestor indicatori QoS arată că productivitţile serverelor RC1 sunt mărimi ce au forma reprezentată de NFIT, iar valorile lor concrete (pentru datele considerate de expresiile (3)) sunt determinate de intervale respective de *certitudine* şi *incertitudine*, funcţie de (α, β)-tăieturi:

$$\tilde{\pi}_x(\alpha) = (0.87915 + 0.02537\alpha, 0.91097 - 0.00645\alpha),$$
$$\tilde{\pi}_y(\alpha) = (0.89159 + 0.03015\alpha, 0.93294 - 0.0112\alpha),$$
$$\tilde{\pi}_z(\alpha) = (0.90933 + 0.03461\alpha, 0.96776 - 0.02382\alpha),$$
$$\tilde{\pi}_x(\beta) = (0.90452 - 0.08761\beta, 0.90452 + 0.07814\beta),$$
$$\tilde{\pi}_y(\beta) = (0.92174 - 0.14028\beta, 0.92174 + 0.04376\beta),$$
$$\tilde{\pi}_z(\beta) = (0.94394 - 0.17465\beta, 0.94394 + 0.03654\beta).$$

Pentru aceste valori NFIT putem determina în mod respectiv: gradul de *apartenenţă*, gradul de *non-apartenenţă* şi gradul de *ezitare* la aceste intervale redate prin NFIT.

În Fig. 5 sunt prezentate graficele respective de *apartenenţă* şi *non-apartenenţă* la $\tilde{\pi}_x$ care indică probabilitatea că atacul *workstation* RC1 nu a reuşit.

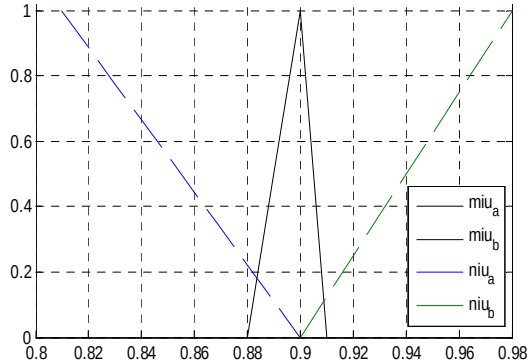

Figura 5. Graficele gradelor de *apartenenţă* şi *non-apartenenţă* la intervalul de probabilitate $\tilde{\pi}_x$.

În mod similar pot fi determinaţi aceşti indicatori ai $\tilde{\pi}_y$ şi $\tilde{\pi}_z$ pentru a evalua productivităţile serverelor RC1 respectivi.

3. CONCLUZII

În lucrare este propusă o abordare unificatoare de modelare, evaluare şi analiză a indicatorilor

cantitativi QoS la riscul de atac al intruşilor reţelelor de calculatoare (RC), bazată pe îmbinarea metodelor RPGS cu rate de declanşare ale tranziţiilor care sunt numere fuzzy intuiţioniste şi a jocurilor matriceale stocastice. În baza acestor paradigme este definită o nouă clasă de RPGS fuzzy intuiţioniste cu jocuri stocastice, numite RPJSFI. Acest tip de modele permit de a descrie mai nuanţat comportamentul aşteptat al atacatorilor şi al sistemului de securitate RC cu parametri fuzzy intuiţionişti care permit de a obţine rezultate mai realiste ale indicatorilor QoS specificaţi. În acest context, este prezentat şi analizat numeric un model concret de RPJSFI care descrie comportarea atacatorului şi a reacţiei sistemului de securitate al unei RC1 cu specificarea jocurilor stocastice şi a ratelor de declanşare a tranziţiilor ce sunt NFIT nuanţate intuiţionist.

Extinderea analizei prin includerea în acest tip de modele a unui protocol reconfigurabil de restabilire a serverelor atacate va fi efectuată pe viitor. Un alt obiectiv este de a dezvolta şi a integra în mediul de simulare vizuală VPNP un subsistem ce va automatiza procesul de verificare şi analiză a indicatorilor QoS ai modelelor de tipul RPJSFI.

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

Bibliografie

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

2. Augustin T., Miranda E., Vejnarova J. *Imprecise probability models and their applications. International Journal of Approximate Reasoning, 50(4), pp. 581 – 582,2009.*

3. Costa C. G., Benjamin Bedregal C., Doria Neto A. D. *Intuitionistic Fuzzy Probability. A.C. da Rocha Costa, R.M. Vicari, F. Tonidandel (Eds.): SBIA 2010, LNAI 6404, 2010. Springer-Verlag Heidelberg, pp. 273–282, 2010.*

4. Ding Z., Shen H. *Applying Fuzzy Differential Equations to the Performance Analysis of Service Composition. D.-S. Huang et al. (Eds.): ICIC 2010, LNCS 6215, Springer-Verlag, pp. 118–125, 2010.*

5. Guţuleac E. Boşneaga C., Reilean A. *VPNP-Software tool for modeling and performance evaluation using generalized stochastic Petri nets. In Proc. of the 6-th International Conference on D&AS-2002, Suceava, România, pp. 243-248, 2002.*

6. Guţuleac E. *Evaluarea performanţelor sistemelor de calcul prin reţele Petri stochastice. Editura „Tehnica-Info", Chişinău, 2004, - 276 p.*

7. Guţuleac E., Zaporojan S., Ţurcanu Iu., Gîrleanu I. *Analiza QoS a sistemelor Ad-hoc cu dispozitive de calcul orientate pe servicii prin reţele Petri stocastice fuzzy. Meridian Ingineresc. 3, pp. 36-45, 2016.*

8. Kahraman C., Tüysüz F. *Manufacturing System Modeling Using Petri Nets. In: C. Kahraman & M. Yavuz (Eds.): Prod. Engr. & Manage., STUD-FUZZ 252, Springer-Verlag, pp. 95–124, 2010.*

9. Liu F., Heiner M., Yang M. *Fuzzy Stochastic Petri Nets for Modeling Biological Systems with Uncertain Kinetic Parameters. PLoS ONE 11(2): e0149674, pp. 1-19, 2016. DOI:10.1371/ journal. pone.0149674.*

10. 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, pp.21-33, 2008.*

11. Murata T. *Petri Nets: Properties, Analysis and Applications. Proceedings of the IEEE, vol.77, no.4, pp.541-580, 1989.*

12. Nagoorganil A., Ponnalagu K. *An approach to solve intuitionistic fuzzy linear programming problem using single step algorithm. International Journal of Pure and Applied Mathematics, Volume 86 No. 5, pp. 819-832, 2013.*

13. Nayagam V. L. G., Sivaraman G. *Modified ranking of intuitionistic fuzzy numbers. Notes on intuitionistic fuzzy Sets, vol.17, pp. 5-22, 2011.*

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

15. Sallhammar K., Helvik B. E., Knapskog S. J. *On stochastic modelling for integrated security and dependability evaluation. The Journal of Networks, Vol. 1, Issue 5, 2006, p. 31 – 42.*

16. Tao M., Shan H. *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.*

17. Thamotharan S. *A Study on Multi Server Fuzzy Queuing Model in Triangular and Trapezoidal Fuzzy Numbers Using $\alpha-$Cuts. International Journal of Science and Research (IJSR), Volume 5 Issue 1, pp. 226-230, 2016.*

18. Zhuo W., Lin C., Chen X. *Quantitative analysis method of network attack and defense based on stochastic game model. Journal of Computers, Vol. 9, pp. 1748 – 1762, 2010.*

Recomandat spre publicare: 19.01.2017.