ANALIZA QoS A SISTEMELOR AD-HOC CU DISPOZITIVE DE CALCUL ORIENTATE PE SERVICII PRIN REŢELE PETRI STOCASTICE FUZZY

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

INTRODUCERE

Actualmente, sistemele de calcul cu arhitecturi orientate pe servicii (SCOS) în timp real cunosc o dezvoltare rapidă, atât sub aspectul complexităţii şi/sau performanţelor, cât şi al ariei de răspândire [2, 5, 9]. Acest tip de sisteme trebuie să aibă o flexibilitate, disponibilitate şi siguranţă în funcţionare (SF) deosebită. Diferite configuraţii pot fi folosite pentru alocarea şi procesarea diferitor servicii sau condiţii de operare ale aplicaţiilor caracterizate de indicatori QoS (Qualty of Service) specificaţi. Astfel, reţelele Ad-hoc (MANET) cu dispositive de calcul mobile fără fir, utilizate în diferite domenii, au o arhitectură distribuită, topologie dinamică cu auto-organizare [10]. O reţea MANET 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. În acest context, apare necesitatea de a descrie comportamentul dispozitivelor de calcul mobile (DCM) la atac şi a evalua uni indicatori ai SF, care este capacitatea acestora de aşi indeplini misiunea, într-un interval de timp stabilit, în prezenţa defectărilor şi a atacurilor intruşilor.

Actualmente DCM sunt folosite nu doar pentru servicii de comunicaţii ale convorbirilor şi a mesajelor scurte, dar şi pentru vizionarea clipurilor video, navigarea pe WEB şi a multor altor aplicaţii complexe. Deşi în ultimele decenii s-au efectuat mari progrese în tehnologia hardware, DCM încă se confruntă cu restricţii de resurse folosite, cum ar fi durata de viaţă a bateriei, lăţimea de bandă a comunicaţiilor radio, capacitatea de stocare a datelor şi performanţa procesorului. Folosirea metodei de prelucrare prin migrarea (engl. Offloading) aplicaţiilor de calcul (MPC) către servere, cum ar fi cloud servere, cu resurse de calcul performante permite de a spori capabilităţile de prelucrare ale DCM [8]. Chiar dacă tehnologia bateriilor de alimentare cu energie este îmbunătăţită în mod constant, aceasta nu a este în măsură să ţină pasul cu creşterea rapidă a consumului de energie de către DCM. Abordarea MPC poate prelungi durata de viaţă a bateriei prin migrarea părţii aplicaţiilor de calculul cu consum intensiv de energie la cloud servere de calcul [8].

Decizia de a folosi aplicaţii MPO depinde de prformanţa DCM în MANET cu o conexiune stabilă, care garantează o comunicarea fiabilă. În cazul folosirii unei reţele nefiabile finalizarea aplicaţiei în curs de prelucrare poate fi amânată sau întreruptă la apariţia unor congestii sau a pierderii pachetelor. Un număr vast de cercetări există privind luarea deciziilor de a folosi MPC pentru a îmbunătăţi performanţele DCM şi a economisi energia cosumată [8, 10]. În timp ce abordarea MPC devine o soluţie atractivă pentru DCM performante şi de perspectivă energetică, aplicaţiile procesate devin tot mai complexe, ele prezintă noi provocări în ceea ce priveşte SF mai ales securitatea, din cauza creşterii intensităţii traficului transmisiei datelor prin reţele de calcul cu ameninţări potenţial necunoscute. Indicatorii cantitativi QoS, în baza cărora se vor lua deciziile de folosire a MPC, trebuie să includă în plus şi aspecte de securitate faţă de performanţa de calcul şi a eficienţei energetice. Într-adevăr, securitatea informaţională este o astfel arie ce acoperă un număr vast de probleme ce trebuie cercetate .

Analiza cantitativă a SF a sistemelor de calcul a avut o mare atenţie timp de mai multe decenii. Cu toate acestea cuantificarea securităţii informaţionale a atras doar recent mai multă atenţie, iar unele lucrări conceptuale iniţiale au fost publicate deja acum zeci de ani, însă cele bazate pe modele serioase de evaluare ale mecanismelor de securitate au fost publicate recent .

Astfel, autorii din [10] au arătat modul în care poate fi modelat şi analizat un centru de distribuţie al cheilor secrete şi cum de găsit rată optimă de reînoire a acestor chei pentru un astfel de sistem.

Metodele uzuale de modelare a atacurilor şi evaluare a riscului SF ale DCM, cum ar fi, arborii de defectare şi de atac, lanţuri Markov, sau reţele Petri (RP) fuzzy (RPF) şi RP generalizate stocastice (RPGS) care sunt metode probabilistice [8, 9, 12].

În [8] este efectuată analiza compromisului dintre performanţa şi securitatea sistemului MPC cu ameninţări specifice de atacuri temporale în baza modelului hibrid al unui lanţ Markov timp continuu

(LMTC) şi al unui sistem de aşteptare. Însă abordarea LMTC poate fi folosită doar pentru modelarea unei clase restrânse de procese de calcul cu un spaţiu mic de stări, deoarece el poate fi construit numai în mod manual şi apar probleme cu validarea acestor tipuri de modele. Totodată, este adoptată şi ipoteza distribuţiei duratelor de schimbare a stărilor conform legii exponenţiale, coeficientul de variaţie, K^v, al căreia este egal cu 1, ceia ce în realitate deseori acest fapt nu se confirmă. Astfel, apare necesitatea de a folosi un alt tip de distribuţii pentru care $K^v \neq 1$, adică $0 < K^v < +\infty$ şi 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. [4, 7].

Cu toate că aceste metode tradiţionale de analiză a SF la atac folosesc date referitoare la parametrii componentelor (ratele de defectare şi de reparaţii 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 QoS a DCM ce folosesc MPC 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 sistemului 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 [1, 2, 6]. Teoria mulţimilor fuzzy este mai bine potrivită pentru modelarea şi analiza sistemelor care includ şi astfel de incertitudini şi imprecizii. În plus, schimbarea dinamică a structurii MANET pot reduce cunoştinţele noastre despre riscul reuşitei unui atac. Prin urmare, pentru a elabora mecanisme de securitate adecvate, este necesar de a dezvolta noi abordări pentru a înţelege şi a descrie funcţionarea DCM wireless, a analiza vulnerabilităţile lor şi a estima cantitativ SF la atac a acestora.

În această lucrare este prezentată o abordare de modelare şi evaluare a riscului de atac SF care imbină utilizarea metodelor logicii fuzzy şi a RPG stocastice. În baza îmbinării acestor paradigme este definită o nouă clasă de RPG fuzzy, numite reţele RPGSF, în baza cărora este efectuată modelarea şi analiza indicatori rilor QoS ai acestor tip de sisteme.

Lucrarea de faţă are ca scop cuantificarea atributelor de securitate şi impactul acestora asupra performanţei sistemelor DCM cu MPO. Acest tip de sistem este modelat printr-o reţea RPGSF cu rate fuzzy de declanşare ale tranziţiilor respective.

Avantajul îmbinării unor astfel de paradigme constă în faptul că modelele RPGSF descriu mai nuanţat comportamentul aşteptat al atacătorilor şi al sistemului de securitate. De asemenea, aceste modele permit de a evalua SF şi pot ajuta la evaluarea indicatorilor QoS, estimarea riscului de pierderi aşteptate, asociate cu diferite strategii de atac şi apărare.

1. REŢELE PETRI STOCASTICE FUZZY

1.1. Elemente ale teoriei logicii fuzzy

Teoria mulţimilor fuzzy şi conceptele cu numere fuzzy [1, 2, 6, 11] au apărut din necesitatea de a exprima cantitativ mărimi imprecise, in care domeniul de valori pe care il ia funcţia de apartenenţă nu mai este limitata la doua valori, ci se extinde la întreg intervalul [0, 1]. Mulţimea fuzzy λ se defineşte astfel:

$$\lambda = \{(x, \mu_\lambda(x)) / x \in Z, \mu_\lambda(x) \in [0,1]\},$$

unde funcţia de apartenenţa $\mu_\lambda(x)$, asociată mulţimii fuzzy, arată gradul în care fiecare element din mulţimea Z aparţine mulţimii fuzzy λ. Cu cât valoarea $\mu_\lambda(x)$ este mai apropiata de 1, cu atât este mai puternică apartenenţa la mulţimea dată.

Două tipuri de numere fuzzy sunt cel mai des întâlnite în aplicaţii: numerele triunghiulare si numerele trapezoidale. Utilizarea numerelor fuzzy triunghiularizate este mai indicată, un motiv fiind şi acela al volumului de calcul .

Un număr fuzzy al λ este un număr fuzzy triunghiular, notat $\widetilde{\lambda}(a,b,c)$, numai în cazul în care există trei numere reale $a \le b \le c$ astfel încât funcţia de apartenenţa $\mu_\lambda(x)$ este:

$$\mu_\lambda = \begin{cases} (x-a)/(b-a), & a \le x \le b \\ 1, & x = b \\ (c-x)/(c-b), & b \le x \le c \\ 0, & altfel \end{cases}$$

De asemenea, în literatura de domeniu numerele fuzzy $\widetilde{\lambda}$ sunt reprezentate şi prin aşa numite α – *tăieturi* (eng. α - *cut*): $\widetilde{\lambda}_\alpha = \{x : \mu_\lambda(x) \ge \alpha \in [0,1]\}$

cu următoarele *intervale de incredere* posibile la nivel α [11]: $\widetilde{\lambda}_\alpha = [a + \alpha(b-a), c - \alpha(c-b)]$.

1.2. Definirea şi regulile de funcţionare RPGSF

La studierea SF a sistemelor, cunoştinţele despre valorile parametrilor de defectare ale componentelor, ratelor de atac, riscurile de vulnerabilitate, etc. sunt, în general, imperfecte [12]. Incertitudinea valorilor reale ale parametrilor specificate 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 valorile reale ale parametrilor DCM şi ai atacatorilor ce îşi schimbă în mod dinamic stările lor. Deci, pentru a modela în un mod mai realist incertudinea comportamentului atacatorilor 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, 2, 6]. 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, în baza cărora sunt determinate probabilităţile fuzzy de stare [7] şi a efectua analiza QoS aplicaţiilor de calcul orientate pe servicii.

Definiţia 1. O reţea Petri generalizată (RPG), 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 de declanşare a tranziţiilor validate de marcajul curent; $G: T \times IN^{|P|} \to \{true, false\}$ este o funcţie de gardă; M_0 este marcajul iniţial; IN este mulţimea numerilor întregi nenegative.

Regulile de funcţionare ale reţelelor Γ şi metoda de analiză a proprietăţilor comportamentale sunt descrise în [3].

Definiţia 2. O reţea Petri stocastică fuzzy, numită RPGSF, este o structură de obiecte, redată de următorul 7-tuplu: $\widetilde{\Gamma} =< \Gamma, w, \widetilde{\Lambda}, \mu_\lambda >$, 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; $w: T_0 \times IN_+^{|P|} \to IR^+$ este 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; IR^+ este mulţimea mărimilor reale nenegative; $\widetilde{\Lambda}: T^\tau \times IN_+^{|P|} \to IR^+$ 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. Aici IR^+ este mulţimea mărimilor reale nenegative; $\mu_\lambda: \widetilde{\Lambda} \to [0,1]$ 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.

Abordarea noastră de modelare şi analiză este efectuată în două etape. Prima etapă este aceeaşi ca şi cea convenţională de modelare prin RPGS. Unica diferenţă este aceia că distribuţia probabilită-ţilor 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 care reflectă natura stocastică a sistemului modelat. În a doua etapă ratele de declanşare ale tranziţiilor sunt reprezentate ca numere fuzzy triunghiulare, $\widetilde{\lambda}_i = (\widetilde{\lambda}_i^-, \widetilde{\lambda}_i^+)$, care pot depinde de opiniile experţilor. După înlocuirea mărimilor numerice fuzzy ale $\widetilde{\lambda}_i$, folosind teoria de calcul fuzzy, obţinem α-tăieturi ale probabilităţilor staţionare de stare fuzzy $\widetilde{\pi}_i$ ale LMTC subiacent RPGSF [4]. În conformitate cu [7, 11] vom folosi aritmetica intervalelor cu α-tăieturi pentru a calcula funcţiile varia-bilelor fuzzy, în baza cărora putem obţine mai multe informaţii decât prin utilizarea principiului de prelungire [11]. Pentru a putea găsi α-tăieturile ale

$\tilde{\pi}_i(\alpha)$ este necesar de a rezolva şi o problemă de optimizare , care face ca soluţia să fie fezabilă [7].

În cazul în care legea de distribuţie a activităţilor considerate nu este cunoscută, însă dispunem de primele cele două momente ale acesteia, adică de media matematică $\overline{u}$ şi variaţia $Var.$, atunci ea poate fi aproximată prin legea Cox-2 de ordinul 2 sau Erlang generalizat de ordinul l. Se poate de demonstrat [3] că pentru orice $\overline{u}$ şi coeficient de variaţie $K^v = Var/(\overline{u})^2$, $0.5 \le K^v < +\infty$ este posibil de a determina o lege Cox-2, parametrii căreia sunt identificaţi astfel: 1) dacă $K^v < 1$, atunci $\lambda' = 1/(\overline{u} \cdot K^v)$, $\lambda'' = 2/\overline{u}$ şi $q = 2(1-K^v)$; 2) dacă $1 < K^v$, atunci $\lambda' = 2/\overline{u}$, $\lambda'' = 1/(\overline{u} \cdot K^v)$ şi $q = 1/(2 \cdot K^v)$. Aici λ' $(resp. \lambda'')$ este rata de prelucrare la prima (*resp.* la a doua) fază, iar q (*resp.* $1-q$) este probabilitatea că după terminarea primei faze (*resp.* nu) se va efectua a doua fază.

În Fig. 1 este prezentat modelul RPG1 stocastică (RPGS1) subiacentă RPGSF1 care descrie funcţionarea unui DCM ce foloseşte metoda de prelucrare MPC a aplicaţiilor în care duratele de atac, de compromitere a sistemului de securitate şi a reînnoirii cheii din stările nesecurizate sunt distribuite conform legii Cox-2.

Semnificaţia locaţiilor şi a tranziţiilor RPSG1 din Fig. 1 este:

- *locaţii:* p_1 - stare în care sistemul funcţionează în mod corect; p_2 - sistemul este atacat; p_3 - sistemul reînnoieşte cheia secretă; p_4 - stare nesecurizată, atacatorul cunoaşte secretele acestuia; p_5, p_8, p_{11} - iniţierea selectării fazei 2 a legii Cox-2 respective; p_6, p_9, p_{12} - faza 2 de prelucrare a legii Cox-2 respective; p_7, p_{10}, p_{13} - semafor al legii Cox-2 respective; p_{14}, p_{15}, p_{16} - terminarea activităţilor conform legii Cox-2 respective; p_{17} - iniţierea selectării prelucrării aplicaţiilor în mod local sau pe server; p_{18} - aplicaţiile MPC sunt prelucrate de server; p_{19} - aplicaţiile sunt prelucrate în mod local de către dispozitivul mobil; p_{20} - populaţia potenţială de cereri prelucrare aplicaţii.

- *tranziţii*: t_1, (t_{10}) - schimbarea (reînnoirea) cheii secrete; t_2, (t_8) - prima (a doua) fază în care un atacator declanşează un atac temporal al sistemului; t_3, (t_{13}) - prima (a doua) fază în care atacatorul sparge sistemul de securitate; t_4 - sistemul este readus starea bună funcţionare după reînnoirea cheii secrete; t_5, (t_{16}) - prima (a doua) fază de reînnoire a cheii secrete din starea nesecurizată; t_6 - intrusul nu reuşeşte să efectueze atacul şi îl abandonează;

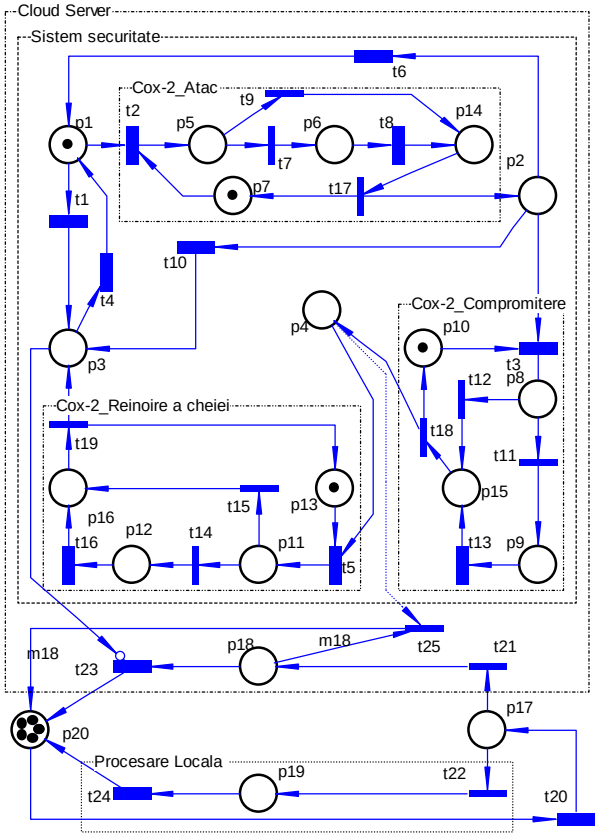

Figura 1. Modelul de reţea RPGS1 subiacentă RPGSF1 ce descrie funcţionarea sistemului MPO.

t_7, (t_9), t_{11}, (t_{12}), t_{14}, (t_{15}) – selectarea (sau nu) fazei 2 a legii Cox-2 respective; t_{17}, t_{18}, t_{19} - terminarea activităţii conform legii Cox-2 respective; t_{19} - sosirea cererilor în sistem pentru prelucrarea aplicaţiilor mobile; t_{21}, (t_{22}) - selectării prelucrării aplicaţiilor în mod local (sau pe server); t_{23}, (t_{24}) - prelucrării aplicaţiilor pe server (sau în mod local) ; t_{25} - aplicaţiile nesecurizate (în p_{18}) sunt anulate, acest fapt este redat de ponderile arcelor (p_{18}, t_{25}) şi (t_{25}, p_{18}) care sunt egale cu marcajul curent m_{18} al locaţiei p_{18}.

Reînnoind cheia de criptare serverul poate preveni sau să întrerupă un atac temporal. În stările nesecurizate toate lucrările expediate către server, nu mai sunt sigure, prin urmare, ele sunt pierdute şi prelucrarea acestora trebuie să fie repetată deoarece ele nu contribuie la *productivitatea* totală a siste-

mului. În RPGS1 faptul că lucrările sunt pierdute este redat de declanşarea tranziţiei t_{25}.

Graful de accesibilitate în formă de listă simbolică [4] al părţii sistemului de securitate al modelului RPGS1 este:

$$M_0 = (p_1 p_7 p_{10} p_{13})[t_1 > M_1, t_2 t_7 > M_2, t_2 t_9 t_{17} > M_3;$$
$$M_1 = (p_3 p_7 p_{10} p_{13})[t_4 > M_0;$$
$$M_2 = (p_1 p_7 p_{10} p_{13})[t_8 t_{17} > M_3;$$
$$M_3 = (p_2 p_7 p_{10} p_{13})[t_6 > M_0, t_{10} > M_1,$$
$$t_3 t_{11} > M_4, t_3 t_{12} t_{18} > M_5;$$
$$M_4 = (p_7 p_9 p_{13})[t_{13} t_{18} > M_5;$$
$$M_5 = (p_4 p_7 p_{10} p_{13})[t_5 t_{14} > M_6, t_5 t_{15} t_{19} > M_1;$$
$$M_6 = (p_7 p_{10} p_{12})[t_{16} t_{19} > M_1.$$

Analiza proprietăţile comportamentale ale RPGS1 arată că aceasta este mărginită, viabilă şi reiniţializabilă. Deci, LMTC1 ce descrie funcţionarea ei este ergodic [4], iar sistemul de ecuaţii ce descrie funcţionarea RPGS1 în regim staţionar este:

$$(\lambda_1 + \lambda_2)\pi_0 = \lambda_4 \pi_1 + \lambda_6 \pi_3,\ \lambda_8 \pi_2 = q_7 \lambda_2 \pi_0,$$
$$(\lambda_3 + \lambda_6 + \lambda_{10})\pi_3 = \lambda_8 \pi_2 + q_9 \lambda_2 \pi_0, \qquad (1)$$
$$\lambda_{13}\pi_4 = q_{11}\lambda_3 \pi_3,\ \lambda_5 \pi_5 = q_{12}\lambda_3 \pi_3 + \lambda_{13}\pi_4,$$
$$\lambda_{16}\pi_6 = q_{14}\lambda_5 \pi_5,\ 1 = \sum_{i=0}^{6} \pi_i, \text{ unde:}$$
$$q_7 = w_7/(w_7 + w_9),\ q_9 = 1 - q_7,$$
$$q_{11} = w_{11}/(w_{11} + w_{12}),\ q_{12} = 1 - q_{11},$$
$$q_{14} = w_{14}/(w_{14} + w_{15}),\ q_{15} = 1 - q_{14}.$$

După obţinerea probabilităţilor staţionare de stare $\pi_i(\alpha)$, exprimate parametric în termini ai ratelor de declanşare ale tranziţiilor, acestea apoi sunt reprezentate ca numere fuzzy triunghiulare, reprezentate prin α -tăieturi. Intervalul aritmetic al acestora, redat prin metoda de α -tăieturi, este bazat pe folosirea operatorilor *max* şi *min* care pot produce intervale mai mari. Menţionăm că $\alpha = 0$ reprezintă cel mai mare interval de probabilitate pe când pentru $\alpha = 1$ obţinem probabilităţile de stare certe ale LMTC1. Teoretic, $\alpha = \alpha^*$ - tăietura unui număr fuzzy oferă cel mai mare interval posibil de valori. Din moment ce ne dorim să fie calculate probabilităţile fuzzy $\tilde{\pi}_i = [\pi_i^-, \pi_i^+]$, cel mai mare interval posibil al acestora este limitat la intervalul $\tilde{\pi}_i \in [0,\ 1]$, $i = 0, 1, 2, ..., N$, unde N este numărul de stări al LMTC. Problema este de a găsi o astfel de α -tăietură minimală, care va satisface această condiţie şi ea poate fi găsită rezolvând următoarea problema de optimizare $\alpha = \hat{\alpha}$:

$$Min(Z) = \alpha$$

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

2. ANALIZA NUMERICĂ A QoS

Indicatorii SF de securitate şi de performanţă definiţi în continuare vor fi folosiţi pentru a evalua unele atribute QoS ale sistemului în restul lucrării de faţă. În următoarea secţiune, vom evalua aceşti indicatori prin calcularea probabilităţilor $\pi_i(\alpha)$ ale CTMC1, subiacent modelului RPGS1, şi de rezolvare a modelului de aşteptare respectiv.

Vom presupune că pe parcursul funcţionării sale sistemul dispune de mecanisme de detectare ale intruziunilor cu un comportament suspicios, caz în care sistemul va declanşa mai frecvent procesul de reînnoire a cheii secrete. Deci, vom presupune că în starea nesecurizată M_5 procesul de reînnoire a cheii secrete este declanşat la o rată diferită, $\tilde{\lambda}_5 = n \cdot \tilde{\lambda}_1$. Parametrul *n* este coeficientul de reînnoire a cheii în starea nesecurizată, deoarece aceasta reprezintă relaţia dintre rata de reînnoire a cheii în starea bună funcţionare şi dintre cea nesecurizată.

Analiza unor indicatori ai SF va fi efectuată pentru cazul în care coeficienţii de variaţie $K_j^v > 1$, ai funcţiilor de distribuţie Cox-2 ale duratelor de declanşare ale tranziţiilor, sunt mai mari ca 1. În acest context, analiza va fi efectuată considerând, ca exemplu de evaluare şi analiză a unor indicatori QoS, pentru următoarele valori numerice fuzzy ale ratelor de declanşare ale tranziţiilor respective:

$$\tilde{\lambda}_1 = (0.1 + \alpha,\ 2.1 - \alpha),\ \tilde{\lambda}_2 = (0.5 + \alpha,\ 2.5 - \alpha),$$
$$\tilde{\lambda}_3 = (0.1 + 0.2\alpha,\ 0.5 - 0.2\alpha),\ \tilde{\lambda}_4 = (1 + \alpha,\ 3 - \alpha),$$
$$\tilde{\lambda}_5 = n \cdot \tilde{\lambda}_1,\ \tilde{\lambda}_6 = \tilde{\lambda}_2,\ \tilde{\lambda}_8 = 0.2,\ \tilde{\lambda}_{10} = \tilde{\lambda}_1, \qquad (2)$$
$$\tilde{\lambda}_{13} = \tilde{\lambda}_{16} = 0.05,\ \tilde{q}_7 = 1/(4 \cdot \tilde{\lambda}_2),$$
$$\tilde{q}_{11} = 1/(20 \cdot \tilde{\lambda}_3),\ \tilde{q}_{14} = 1/(20 \cdot \tilde{\lambda}_1).$$

Substituind mărimile numerice fuzzy redate de relaţiile (2) în sistemul de ecuaţii (1), obţinem următoarele soluţii ale sistemului de ecuaţii (1) pentru intervalele stânga $\lambda_i^- = [a_i + \alpha \cdot (b_i - a_i)]$ şi dreapta $\lambda_i^+ = [c_i + \alpha \cdot (c_i - b_i)]$:

$$\pi_0^- = \pi_2^- = 0.1n(0.1 + \alpha)(1 + \alpha)(0.7 + 2.2\alpha)/\gamma_1^-,$$
$$\pi_1^- = n(34\alpha^3 + 20.6\alpha^2 + 3.42\alpha + 0.17)/\gamma_1^-,$$
$$\pi_3^- = \pi_4^- = 0.5n(2\alpha^2 + 3\alpha + 1)(1 + 10\alpha)/\gamma_1^-, \qquad (3)$$
$$\pi_5^- = \pi_6^- = 0.5(4\alpha^3 + 8\alpha^2 + 5\alpha + 1)/\gamma_1^-,$$

unde $\gamma_1^- = (98n + 4)\alpha^3 + (115n + 8)\alpha^2 +$

$$(36.22n+5)\alpha+2.57n+1.$$

$$\pi_0^+=\pi_2^+=n(\alpha-2.1)(\alpha-0.3)(2.2\alpha-5.1)/\gamma_1^+,$$
$$\pi_1^+=n(34\alpha^3-224.6\alpha^2+493.82\alpha-361.41)/\gamma_1^+,$$
$$\pi_3^+=\pi_4^+=0.5n(2\alpha^2-11\alpha+15)(10\alpha-21)/\gamma_1^+, \quad (4)$$
$$\pi_5^+=\pi_6^+=0.5(4\alpha^3-32\alpha^2+85\alpha-75)/\gamma_1^+,$$

unde $\gamma_1^+=(98n+4)\alpha^3-(703n+32)\alpha^2+(1672.22n+85)\alpha-1319.01n-75$.

Analiza detaliată a acestor soluţii (4) arată că $\forall\alpha\in[0,\,1]$ şi $\forall n>0$ sunt verificate relaţiile:

$$0<\pi_i^-(\alpha)\le\pi_i^+(\alpha)<1,\ i=0,\,1,\,2,...,N.$$

2.1. Analiza confidenţialităţii

În mod similar cu [8], indicatorii SF de securitate sunt consideraţi ca fiind confidenţialitatea şi costurile sistemului (de securitate), care sunt funcţii de $\widetilde{\pi}_i(\alpha,n)$, $i=0,\,1,\,2,...,N$. Aceste probabilităţi fuzzy pot fi interpretate ca proporţia duratei de timp în care LMTC1 se află în starea M_i. În cazul în care un atac temporal într-un sistem ce foloseşte MPO are succes, atacatorul obţine cheia secretă şi ulterior, el poate naviga în mod neautorizat prin fişierele sistemului. Astfel în RPGSF1 marcajul M_5 denotă pierderea confidenţialităţii. Prin urmare, indicatorul de confidenţialitate $\widetilde{\pi}_{Conf.}(\alpha,n)$ în regim staţionar, funcţie de α şi n, este calculat ca:

$$\widetilde{\pi}_{Conf.}(\alpha,n)=1-\widetilde{\pi}_5(\alpha,n). \quad (5)$$

Pentru ratele $\lambda_j^-(\alpha)\in[a_j+\alpha\cdot(b_j-a_j)]$ de declanşare ale tranziţiilor respective, redate de valorile numerice din (2), graficele $\pi_{Conf.}^-(\alpha,n)$ şi $\pi_{Conf.}^+(\alpha,n)$ pentru $\lambda_j^+(\alpha)\in[c_j+\alpha\cdot(c_j-b_j)]$ sunt prezentate respectiv în Fig. 2.

Din Fig. 2 observăm că $\forall n\ge 0.5$ valoarea maximă a $\pi_{Conf.}^-(\alpha,n)$ (resp. $\pi_{Conf.}^+(\alpha,n)$) este obţinută în cazul în care $\alpha=1$, (resp. $\alpha=0$). Analiza mai nuanţată a rezultatelor numerice ale $\pi_{Conf.}^-(\alpha,n)$, redate de relaţia (5), arată că acest indicator creşte monoton odată cu creşterea ratei $\widetilde{\lambda}_1(\alpha)\in[\lambda_j^-(\alpha),\lambda_j^+(\alpha)]$. Totodată, el creşte şi atunci când n, multiplul ratei de reînnoire a cheii în starea nesecurizată, este mai mare. Aceasta se datorează faptului că securitatea se îmbunătăţeşte atunci când sistemul lansează mai frecvent procesul de reînnoire a cheii, deoarece este mult mai probabil ca sistemul să fie adus înapoi în starea bună funcţionare din starea de atac şi cea nesecurizată.

Astfel, pentru mărimile numerice analizate determinăm că cel mai mare indicator de confidenţialitate este acel pentru care ratele de declanşare ale tranziţiilor primesc valori din intervalul drept $\lambda_j^+(\alpha)\in[c_j+\alpha\cdot(c_j-b_j)]$. De exemplu, pentru n=10 avem următoarele relaţii:

$$Max(\widetilde{\pi}_{Conf.}^-(\alpha=1,n=10))=0.9964=$$
$$Min(\widetilde{\pi}_{Conf.}^+(\alpha=1,n=10))<$$
$$Max(\widetilde{\pi}_{Conf.}^+(\alpha=0,n=10))=0.9972.$$

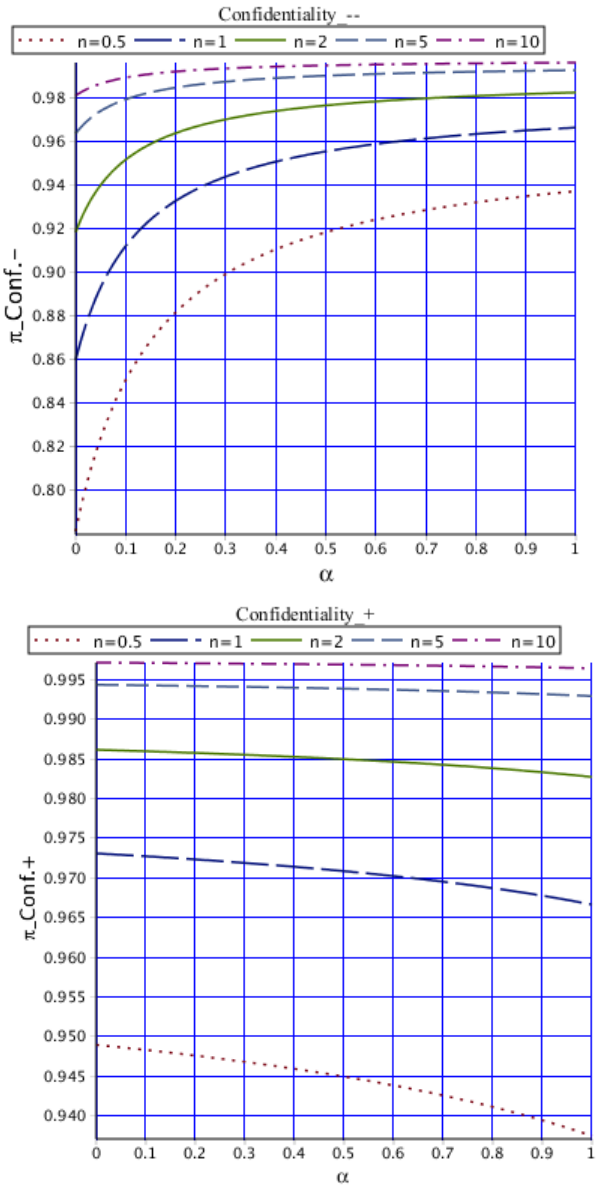

Figura 2. Indicatorii de confidenţialitate $\pi_{Conf.}^-(\alpha,n)$ şi $\pi_{Conf.}^+(\alpha,n)$ funcţie de α şi n.

2.2. Costul confidenţialităţii

Un alt indicator al SF este costul sistemului de securitate $\pi_{Conf.}^-(\alpha,n)$, deoarece acesta suferă pierderi în două stări: în starea nesecurizată M_5 şi în

cea de reînnoire a cheii M_1. Sistemul suportă un cost sensibil la pierderea informaţiilor în starea nesecurizată şi, de asemenea, un alt cost este suportat atunci când sistemul lansează un proces de reînnoire a cheii. Aceste costuri sunt interpretate ca proporţia timpului de viaţă al sistemului, adică, probabilitatea de aflare în starea de echilibru a CTMC1 în stările respective. Pentru a evidenţia importanţa relativă între pierderea informaţiilor sensibile în starea nesecurizată şi a efortului necesar pentru reînnoirea cheii în mod regulat folosim o pondere normalizată $0 \le \omega \le 1$ prin care acest cost este determinat de următoarea relaţie:

$$\tilde{\pi}_{Cost}(\alpha, n) = \omega \cdot \tilde{\pi}_1(\alpha, n) + (1-\omega) \cdot \tilde{\pi}_5(\alpha, n). \quad (6)$$

În Fig. 3 sunt prezentate graficele costurilor de securitate $\pi^-_{Cost}(\alpha, n)$ şi $\pi^+_{Cost}(\alpha, n)$ pentru $\omega = 0.5$ şi respectiv ale ratelor de declanşare $\lambda_i^-(\alpha)$ şi $\lambda_i^+(\alpha)$, redate de valorile numerice (2).

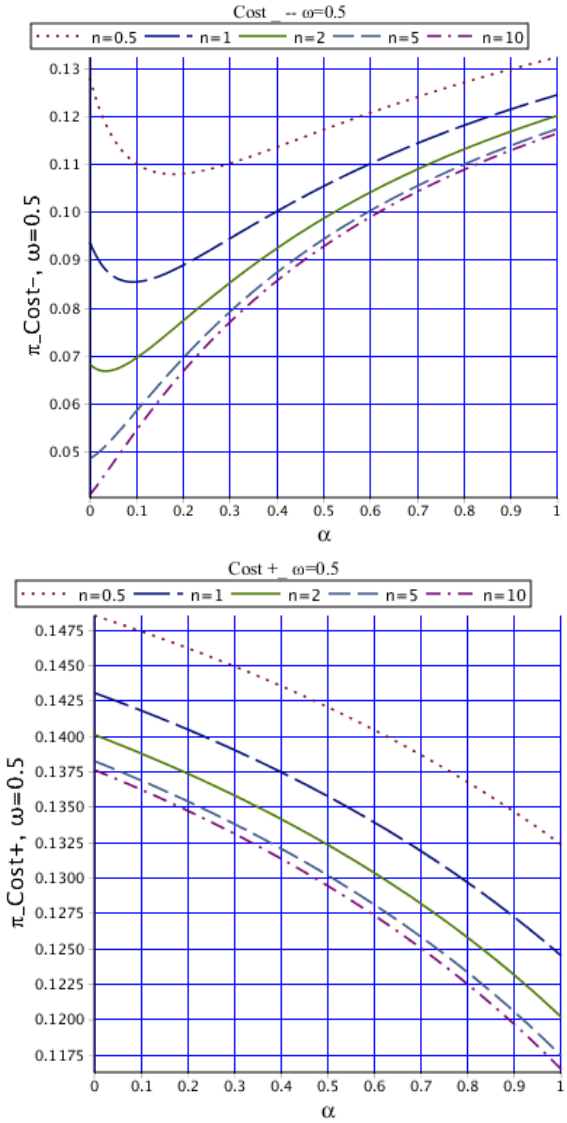

Figura 3. Indicatorii de cost $\tilde{\pi}^-_{Cost}(\alpha, n)$ şi $\tilde{\pi}^+_{Cost}(\alpha, n)$ funcţie de α şi n.

Analiza numerică detaliată a acestor grafice arată că $\forall n > 0$ *costul confidenţialităţii* (CC) minimal este obţinut în intervalul $\lambda_j^-(\alpha)$. De exemplu, pentru n=1 avem:

$$\pi^-_{Cost}(\alpha^* = 0.0922, n = 1) = 0.0855 <$$
$$\pi^+_{Cost}(\alpha^* = 1, n = 1) = 0.1245,$$

iar pentru n=10 avem:

$$\pi^-_{Cost}(\alpha^* = 0, n = 10) = 0.0412 <$$
$$\pi^+_{Cost}(\alpha^* = 1, n = 10) = 0.1165,$$

ceia ce înseamnă că CC minimum este obţinut $\forall n > 0$ atunci când $\lambda_j^* \in \lambda_j^-(\alpha)$, de exemplu, pentru n=1 costul minim va fi obţinut pentru $\lambda_j^* = 0.1922$.

În cazul în care rata de reînnoire a cheii λ_1 este mică, costul sistemului este mic, din cauza probabilităţii mici de a se afla în starea de reînnoire a cheii. Pentru aceşti parametri stabiliţi, atunci când n = 10, a fost determinat că cel mai mic CC al sistemului este obţinut în cazul în care rata optimă de reînnoire a cheii este $\lambda_1^* = 0.1$. La o valoare λ_1 mai mare decât λ_1^*, CC creşte din cauza creşterii efortului al procesului de reînnoire a cheii. De asemenea, vedem că în continuare costul sistemului scade odată cu creşterea coeficientului n de reînnoire a cheii. Acest lucru se datorează faptului că pentru toate ratele de reînnoire a cheii, durata medie de aflare în stările nesecurizate scade pe măsură ce în această situaţie reînnoirea cheii se va efectua mai frecvent. Practic, acesta înseamnă că este mai util de a declanşa mai des procesul de reînnoire a cheii doar când mecanismul de detectare găseşte unii indici de intruziune.

În acelaşi context a fost analizat şi efectul parametrului de ponderare ω şi al α asupra CC sistemului $\tilde{\pi}_{Cost}(\alpha, n)$ care este prezentat în Fig. 4 pentru n=10. Din această figură se poate observa că CC scade monoton cu creşterea ratei de reînnoire a cheii $\tilde{\lambda}_1(\alpha)$ când ω = 0, unde se vor lua în considerare numai costurile pierderii informaţiilor sensibile în cazul când sistemul este nesecurizat. Intuitiv, în acest caz, atunci când este declanşat procesul de reînnoire a cheii mai des, CC va scădea. Însă, când se pune toată ponderea pe efortul de reînnoire a cheii (ω = 1) cu creşterea ratei $\tilde{\lambda}_1(\alpha)$ va creşte şi costul acestui efort. Pentru valorile medii ale parametrului de ponderare ω, rata de reînnoire a cheii optimă pentru cel mai mic cost scade atunci când s-a pus o mai mare pondere pe costul efortului de reînnoire a cheii. Din figura 4, pentru parametrii specificaţi, constatăm că cel mai mare cost al

efortului de reînnoire a cheii şi cel mai mic cost de securitate este când $\alpha = 0$, adică $\lambda_1^* = 0.1$.

2.3. Analiza productivităţii

Pentru a analiza influenţa coruperii sistemului de securitate, ca rezultat reuşit al atacului, asupra productivităţii sistemului MPO vom presupune că durata totală de viaţă a acestuia este $\bar{\tau}$. În starea bună funcţionare M_0 şi în starea de atac M_3, numărul de lucrări deservite de către sistem trebuie să fie $E[X_1] = \tilde{\lambda}_{20}(\tilde{\pi}_0 + \tilde{\pi}_3)\bar{\tau}$, dat fiind că cozile de aşteptare în p_{18} şi p_{19} sunt stabil limitate. În starea M_1 de reînnoire a cheii, serverul refuză toate solicitările utilizatorilor şi în acest caz toate lucrările trebuie să fie executate la nivel local.

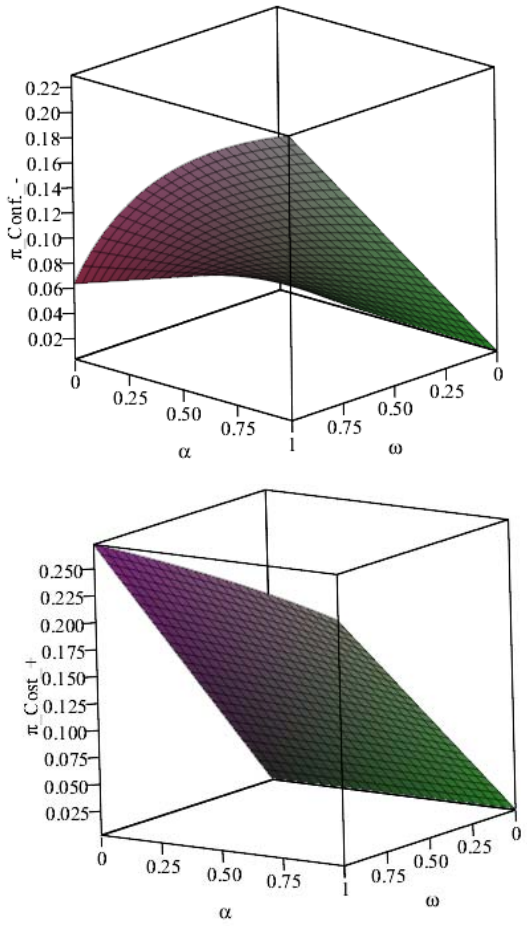

Figura 4. Indicatorii de cost $\pi^-_{Cost}(\alpha,\omega)$ şi $\pi^+_{Cost}(\alpha,\omega)$ funcţie de α şi ω cu n=10.

Pentru $\tilde{\lambda}_{20} < \tilde{\lambda}_{24}$, numărul total de lucrări deservite în acest mod este $E[X_2] = \tilde{\lambda}_{24}\tilde{\pi}_1\bar{\tau}$. În starea nesecurizată M_5, toate lucrările expediate la server 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 sistem la nivel local $E[X_3] = q_{22}\tilde{\lambda}_{20}\tilde{\pi}_5\bar{\tau}$. Prin urmare, conform legii Little relativ la sistemele de aşteptare [4, 11] obţinem următoarea relaţie care determină *productivitatea* (engl. *Throughput*) sistemului:

$$\tilde{\lambda}_{Thr.} = (E[X_1] + E[X_2] + E[X_3])/\bar{\tau} = \tilde{\lambda}_{20}(\tilde{\pi}_0 + \tilde{\pi}_3) + \tilde{\lambda}_{24}\tilde{\pi}_1 + q_{22}\tilde{\lambda}_{20}\tilde{\pi}_5.$$

Analiza acestui indicator QoS este efectuată pentru următoarele valori numerice fuzzy ale ratelor de declanşare a tranziţiilor respective:

$$\tilde{\lambda}_{20} = (2+\alpha, 4-\alpha),\ q_{21} == 1 - q_{22},$$
$$\tilde{\lambda}_{24} = (5+2\alpha, 8-3\alpha),$$
$$q_{22} = (0.3+0.1\alpha, 0.6-0.2\alpha),$$
$$q_{22} = (0.3+0.1\alpha, 0.6-0.2\alpha).$$

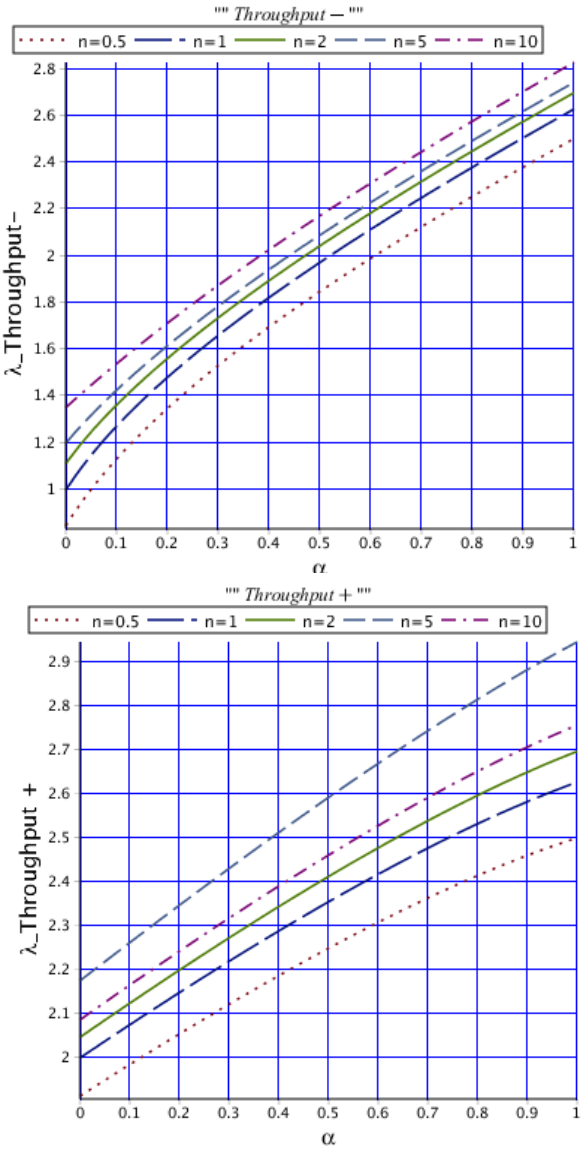

Figura 5. Indicatorii QoS de *productivitate* $\lambda^-_{Thr.}(\alpha,n)$ şi $\lambda^+_{Thr.}(\alpha,n)$ funcţie de α şi n.

În Fig. 5 sunt prezentate graficele indicatorilor de performanţă ale sistemului, şi anume productivitatea lui, funcţie de parametrii α şi n. Din ele observăm că indicatorul de productivitate creşte monoton odată cu creşterea lui α şi a lui $\lambda_j^-(\alpha)$. De asemenea, el creşte şi atunci când n, multiplul ratei de reînnoire a cheii în starea nesigură, este mai mare. Acest lucru se datorează faptului că securitatea se îmbunătăţeşte atunci când sistemul lansează procesul de reînnoire a cheii mai frecvent, deoarece este mult mai probabil ca sistemul să fie adus înapoi în stare bună funcţionare din starea de atac şi cea nesigură. Productivitatea maximă, pentru un n dat, este obţinută atunci când $\alpha = 1$. Însă pentru $\lambda_j^+(\alpha)$ acest fapt este valabil numai când $n < 10$.

2.4. Analiza indicatorului tradeoff

Pentru a analiza modul în care securitatea sistemului MPO influenţează performanţa acestuia, este definit, de asemenea, indicatorul *tradeoff*, $\widetilde{\eta}_{Thr.}(\alpha, n)$, care este o funcţie obiectiv formată din produsul *confidenţialităţii*, atribut al securităţii acestuia, cu *productivitatea* lui [8]:

$$\widetilde{\eta}_{Thr.}(\alpha, n) = \widetilde{\pi}_{Conf.}(\alpha, n) \cdot \widetilde{\lambda}_{Thr.}(\alpha, n). \qquad (7)$$

În Fig. 6 sunt prezentate graficele indicatorului $\widetilde{\eta}_{Thr.}(\alpha, n)$ ce redă compromisul posibil între securitatea şi productivitatea sistemului MPC. Acest indicator creşte cu creşterea lui α şi a lui n, deoarece securitatea sistemului se îmbunătăţeşte rapid. Trendul acestora este similar cu cel al graficelor productivităţii sistemului MPC. Însă ele diferă de cele obţinute pentru cel mai mic indicator de cost al securităţii, deoarece ele sunt considerate la diferite aspecte de evaluare ale sistemului. În cazul în care rata de reînnoire a cheii are o valoare mare, parametrul multiplu n puţin afectează indicatorul $\widetilde{\eta}_{Thr.}(\alpha, n)$ când procesul de reînnoire a cheii este declanşat destul de frecvent. Acest indicator scade la rate mari de reînnoire a cheii, deoarece în acest caz productivitatea sistemului degradează. Acest indicator creşte rapid la mărimi medii ale lui $\lambda_1(\alpha)$, deoarece securitatea sistemului se îmbunătăţeşte rapid. Rata optimă λ_1^* de reînnoire a cheii pentru un $\widetilde{\eta}_{Thr.}^*$ maximum, cea mai bună securitate şi performanţă, este $\lambda_1^* = 1.10$ pentru $\alpha_1^* = 1$, când $n = 5$, unde n este multiplul ratei de ieşire din starea compromisă, $\widetilde{\lambda}_5 = n\widetilde{\lambda}_1$. Această rată optimă de reînnoire a cheii este diferită de cele obţinute pentru cel mai mic indicator de *Cost*, deoarece acestea sunt considerate la diferite aspecte de evaluare ale sistemului. Indicatorul $\widetilde{\eta}_{Thr}$ scade mai lent când rata de reînoire a cheii λ_1 devine mai mare decât λ_1^*. În cazul în care rata de reînoire a cheii are o valoare mare, parametrul multiplu $n > 5$ nu afectează indicatorul $\widetilde{\eta}_{Thr}$ mult când procesul de reînnoire a cheii este declanşat destul de frecvent. Acesta scade la rate mari de reînnoire a cheii, deoarece în acest caz productivitatea sistemului degradează.

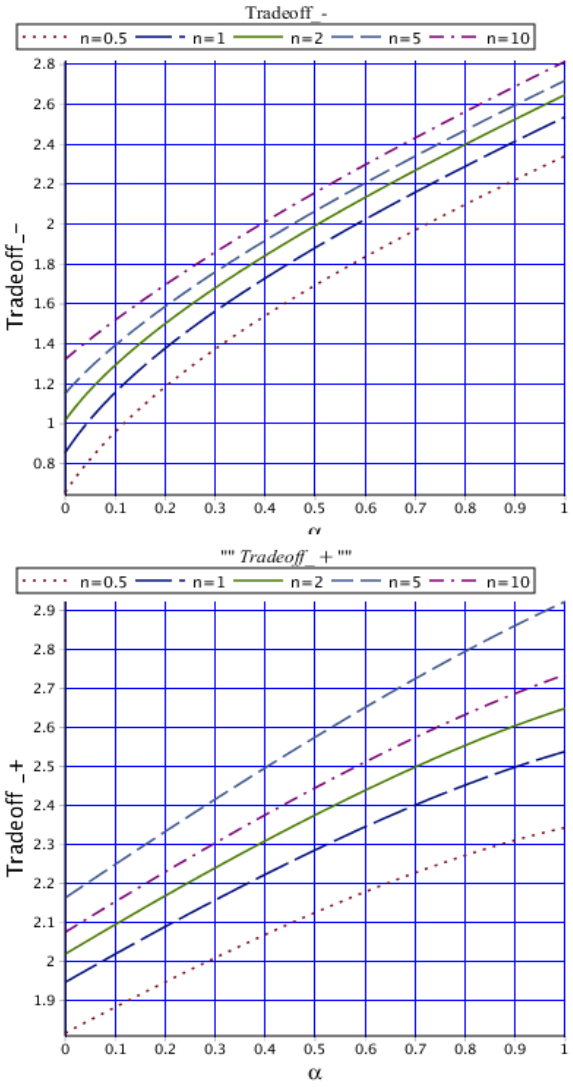

Figura 6. Indicatorii QoS *tradeoff* $\eta_{Thr.}^-(\alpha, n)$ şi $\eta_{Thr.}^+(\alpha, n)$ funcţie de α şi n.

De asemenea, pentru intervalul stâng al schimbării ratelor $\lambda_j^-(\alpha)$ de schimbare a stărilor sistemului MPC pentru $\forall n > 0$ este totdeauna relaţia $\widetilde{\eta}_{Thr.}^-(\alpha = 1, n) > \widetilde{\eta}_{Thr.}^-(\alpha = 1, n+1)$ este verificată, însă pentru $\forall \lambda_j^+(\alpha)$ al intervalului drept $\exists n$ astfel încât această relaţie nu totdeauna are loc. De exemplu, din Fig. 6 observăm că:

$\widetilde{\eta}^{-}_{Thr.}(\alpha = 1, n = 5) > \widetilde{\eta}^{-}_{Thr.}(\alpha = 1, n = 10)$.

Astfel, în această lucrare este propusă o metodă care poate fi utilizată de către administratorul de sistem pentru a găsi cum să fie controlat mecanismul de securitate (reînnoirea cheii) al sistemului. Costul de sistem este un indicator ce poate fi folosit ca un criteriu pentru furnizorii de servicii pentru a taxa utilizatorii lor. Dacă utilizatorii au nevoie de un nivel de securitate mai ridicat, ei trebuie să plătească mai mult pentru serviciile MPC. De asemenea, administratorul de sistem poate utiliza acest rezultat pentru a obţine un cost minim sau un maxim *tradeoff* de productivitate - securitate pentru sistemul dat.

Menţionăm că această abordare poate fi generalizată prin îmbinarea utilizarea metodelor RPGSF cu *jocuri teoretice* pentru a modela şi evalua riscurile pierderilor aşteptate, asociate cu diferite strategii de atac şi apărare.

Soluţiile parametrice ale sistemului de ecuaţii (1), toate calculele numerice şi construirea graficelor respective în această lucrare au fost efectuate folosind pachetul de programe ştiinţifice Maple Toolbox 2015 WindowsX86

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

3. CONCLUZII

În lucrare este prezentat un cadru unificator de modelare, evaluare şi analiză a indicatorilor QoS la riscul de atac al intruşilor reţelelor MANET cu dispozitive de calcul mobile (DCM), care îmbină utilizarea metodelor RPG stocastice cu durate de declanşare ale tranziţiilor conform legii Cox-2 şi a logicii fuzzy. În baza acestor paradigme este definită o nouă clasă de RPG stocastice fuzzy, reţele RPGSF. Acest tip de modele permite de a descrie mai nuanţat comportamentul aşteptat al atacatorilor şi al sistemului de securitate MANET cu parametri fuzzy. În acest context, este prezentat şi analizat numeric un model concret de RPSF1 ce descrie funcţionarea sistemului de securitate a DCM care folosesc migrarea aplicaţiilor de calcul (MPC) către servere performante cu specificarea locaţiilor, tranziţiilor şi a atributele cantitative nuanţate.

Extinderea analizei prin includerea unui protocol reconfigurabil de reînnoire a cheilor şi validarea lui înainte de a fi aplicat va fi efectuată în viitor. Un alt obiectiv pe viitor este de a dezvolta şi a integra în mediul de simulare vizuală VHPN un subsistem ce va automatiza procesul de verificare şi analiză a indicatorilor QoS a acestor tipuri de reţele.

Bibliografie

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

***2. 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.*

***3. Gelenbe, E. et all.** Réseaux de files d'attente : modélisation et traitement numérique. Ed. Hommes et Techniques. Monographies d'Informatique de L'AFCET, 1980. - 160 p.*

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

***5. Li, B., Xu, Y., Wu, J., Zhu, J.** A Petri net and QoS Based Model for Automatic Web Service Composition. Journal of Software, Vol. 7, No. 1, pp. 149-155, 2012.*

***6. 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.*

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

***8. Meng, T., Wolter, K., Wang, Q.** Security and Performance Tradeoff Analysis of Mobile Offloading Systems Under Timing Attacks. In M. Beltran et al. (Eds.): Computer Performance Engineering 12th European Workshop, LNCS 9272, pp. 32–46, 2015. DOI:10.1007/978-3-319-23267-6 3.*

***9. 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.*

***10. 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.*

***11. 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.*

***12. Zhou, K. Q., Zain, A. M.** Fuzzy Petri nets and industrial applications: a review. Artif. Intell. Rev. 45, pp. 405–446, 2016. DOI 10.1007/s10462-015-9451-9.*

Recomandat spre publicare: 10.09.2016.