Analiza QoS în baza GSPN Fuzzy a Apărării prin Mutarea Ţintelor de Atac a Reţelelor de Calculatoare

Guţuleac Emilian, Zaporojan Sergiu, Sclifos Alexei, Ţurcanu Iurie
Departament "Informatică și Ingineria Sistemelor"
Universitatea Tehnică a Moldovei
Chişinău, Republica Moldova
emilian.gutuleac@calc.utm.md

Abstract — Moving target defense (MTD) is a novel way to alter the asymmetric situation of attacks of computer networks (CN), and a lot of MTD studies have been carried out recently. However, relevant performance modeling and analysis for the defense mechanism of CN with the MTD technology is still absent. In this paper, we introduced a model of fuzzy generalized stochastic Petri (FGSPN), under which it is carried out QoS analysis of Web server defense process with uncertain parameters due to uncontrollable factors using typical kinds of MTD techniques. We also take a case study to describe the usage of the FGSPN model to show how it can be applied to the proposed approach, which better represents both dimensions of uncertainty, stochastic variability and inaccuracy in the shaping of CN with MTD.

***Key Words* — Fuzzy, moving target defense, network security, modeling, performance analysis, stochastic Petri net.**

I. INTRODUCERE

Odată cu creșterea rapidă a tehnologiilor informaționale, rețelele de calculatoare (RC) au devenit o infrastructura cheie în diferite domenii cu aplicații, unde securitatea informațională se confruntă permanent cu o gravitate severă de provocări. Unele dintre cauzele majore ale acestor situații constau în faptul că configurațiile actuale ale sistemelor de securitate RC sunt în mod tipic deterministe, statice și omogene [3, 6, 13]. Aceste caracteristici reduc dificultățile atacatorilor cibernetici pentru a identifica ținte specifice, prin scanarea vulnerabilităților RC, pentru a accesa informații esențiale, care oferă atacatorilor avantaje asimetrice la elaborarea, lansarea și răspândirea unor atacuri, iar apărătorii sunt întotdeauna dezavantajați prin faptul că ei deseori proactiv reacționează.

Pentru a modifica situația asimetrică dintre atacuri și apărare, recent au fost propuse modalități de apărare prin mutarea țintei de atac (AMŢ), ca fiind unele din tehnici "schimbătoare a jocului" în securitatea cibernetică [5, 12]. Acestă abordare permite de a crea, evalua și a implementa mecanisme și diverse sisteme de strategii de apărare ce se schimbă în mod dinamic, crescând astfel complexitatea și costurile atacurilor, limitează exploatarea vulnerabilităților și duce la mărirea rezilienții sistemului de securitate al RC [6].

Principale tehnici tipice AMŢ folosite sunt: 1) Transformări software (ST); 2) Tehnici cu platforme dinamice (TPD) și 3) Amestecarea adreselor în rețea (NAS) [12]) care pot fi implementate aparte sau simultan, de exemplu, pe un server Web (SW). Mai exact, metoda ADŢ bazată pe ST poate fi utilizată pe aplicații SW pentru a îmbunătăți capacitatea apărării RC. Abordarea DPT poate fi folosită pe platforma de rulare a SW pentru a complica atacurile, iar cea NAS cu scopul de a încurca atacatorul.

De obicei, evaluarea indicatorilor QoS (Quality of Service) ai RC cu tehnici AMŢ este efectuată în mod empiric, însă nu sunt aplicate modele formale. Până în prezent, doar câteva lucrări aferente au introdus modele probabilistice în domeniul folosirii tehnicilor ADŢ pentru apărare RC [3, 6, 10].

La modelarea și analiza indicatorilor QoS (Quality of Service) ai RC una dintre cele mai importante subiecte care trebuie luate în considerare este *incertitudinea*, legată de motivul pentru care parametrii modelului sunt, de obicei, sub forma unor parametri fuzzy. Deși 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 ce nu are o natură statistică și deci, ea nu poate fi descrisă numai prin utilizarea modelelor probabi-listice [1]. De asemenea, atacurile intruşilor nu întotdeauna pot fi bine caracterizate prin modele de natură pur aleatorie, ceea ce reduce cunoştinţele sistemului de securitate al RC despre riscul reuşitei unui atac. Cu toate acestea, pentru a modela corect atacurile intenționate asupra unei RC, orice model probabilistic trebuie să includă și incertitudinile epistemice ale comportamentului atacatorului.

Argumentăm că acest comportament trebuie să fie reprezentat ca o distribuție de probabilitate asupra posibilelor acțiuni de atac în fiecare stare a modelului și, de asemenea, pe o abordare bazată pe utilizarea numerelor fuzzy [2].

Unul dintre cele mai răspândite formalisme avansate, folosite pentru modelarea , verificarea şi analiza sistemelor cu evenimente discrete sunt reţelele Petri stocastice generalizate (GSPN) [4, 7], care permit de a descrie analitic și în mod graphic procesul de atac și apărare al RC [3].

În această lucrare este dezvoltat și analizat un model GSPN fuzzy (GSPNF) pentru evaluarea indicatorilor QoS ai

sistemului de apărare RC al unui SW cu tehnici ADȚ în care parametrii cantitativi sunt considerați ca fiind numere fuzzy.

II. Elemente ale teoriei Credibilității

Lanțurile markoviene în timp continuu (LMTC) [7] și GSPN [4, 7] sunt formalisme importante ce permit de a descrie fenomene dinamice sub incertitudine aleatorie. Totuși, în lumea reală deseori întâlnim probleme dificile care nu pot fi tratate prin utilizarea doar a teoriei proceselor stocastice.

Pentru a face față unor astfel de probleme complexe, Liu în [9] a propus teoria credibilității (TC), care este o ramură a matematicii pentru studierea comportamentului fenomenelor fuzzy. Teoria mulțimilor fuzzy şi conceptele cu numere fuzzy [2, 9] au apărut din necesitatea de a exprima cantitativ mai nunțat mărimi imprecise, in care domeniul de valori pe care il ia funcția de apartenență nu mai este limitata la doua valori, ci se extinde la intreg intervalul [0, 1].

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

O mulțime fuzzy $\tilde{A}$ este definită astfel [2]:

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

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

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

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

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

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

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

Un NFTz este un NFT pentru cazul special cu $a_2 = a_3$.

Credibilitatea măsoară gradul de încredere, acordat unei mulțimi anumite de date, apariției unor evenimente, a unor variabile fuzzy, etc. Scopul teoriei credibilității este de a combina eficient informațiile din diverse surse: date istorice și actuale, date privind riscul individual și riscul colectiv, rate ale apariției atacurilor și a măsurilor de apărare, etc. [9].

În continuare, introducem noțiunile de bază ale teoriei credibilității, cum ar fi: măsura de credibilitate; spațiul de credibilitate; variabilă fuzzy aleatorie; funcția de apartenență; distribuția credibilității și valoarea ei medie. Fie Θ o mulțime nu este vidă, iar $Bag(\Theta)$ este puterea de descriere a acesteia, adică mulțimea tuturor submulțimilor lui Θ. Pentru fiecare element $A \in Bag(\Theta)$, numit eveniment, este definită o măsură de credibilitate, fiind redată de un număr $Cr\{A\}$, care exprimă șansa apariției acestuia. În [9] este demonstrat că mulțimea de funcții $Cr\{\Theta\}$ este o măsură de credibilitate dacă și numai dacă aceasta satisface condițiile de:

normalitate: $Cr\{\Theta\} = 1$; *monotonie:* $Cr\{A\} \le Cr\{B\}$, $\forall A \subset B$; *autodualitate:* $Cr\{A\} + Cr\{A^c\} = 1$, $\forall A \in Bag(\Theta)$; *maximalitate:* $\forall A_i : Cr\{\sum_i \cup_i A_i\} \wedge 0.5 = \sup_i Cr\{A_i\}, Cr\{A_i\} \le 0.5$.

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

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

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

iar pentru orice mulțime de numere reale $B \in IR_+$, avem:

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

Valoarea medie $\bar{\xi} = E[\xi]$ a lui ξ este determinată de următoarea relație (3) [9]:

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

În continuare, vom folosi funcții de apartenență $\mu(x)$ ale câtorva tipuri de variabile fuzzy și anume: *echiposibile, triunchiulare* și *trapezoidale* [2, 9] pentru a descrie parametrii cantitativi ai GSPNF ce descrie comportarea atacatorului care folosește informații fuzzy despre vulnerabilitățile RC date.

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

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

Calculul valorilor medii ale unei variabile fuzzy. Fie ξ este o variabilă fuzzy echiposibilă pe $[a,b]$ cu $a \ge 0$. În conformitate cu relațiile (2) și (4) obținem (5):

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

În mod asemănător pentru o variabilă *fuzzy triunghiulară* η pe $[a,b,c]$ cu $0 \le a < b < c$, obținem relația (6):

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

Pentru o variabilă fuzzy trapezoidală ς pe $[a,b,c,d]$ cu $0 \le a < b < c < d$, obținem relația (7):

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

La modelarea și analiza QoS ai RC cunoştinţele despre valorile ratelor de atac, a riscurilor de vulnerabilitate etc. sunt, în general, imperfecte [1, 7] , incertitudinea cărora provine din caracterul aleatoriu de informaţii și cea epistemică legată de caracterul imprecis şi incomplet al informaţiilor din cauza lipsei de cunoştinţe despre valorile reale ale parametrilor RC ce își schimbă în mod dinamic stările sale. Deci, pentru a modela într-un mod mai realist incertitudinea comportamentului atacatorului și reacţia de apărare a RC, este necesar de a lua în considerare, de asemenea, atât aspectele probabilistice, cât şi cele fuzzy [1]. Acest fapt poate fi realizat prin definirea GSPNF în care unele atribute cantitative pot avea mărimi fuzzy. Ea se bazează pe fuzzificarea ratelor de declanşare ale tranziţiilor, în baza cărora sunt determinate probabilităţile fuzzy de stare GSPNF și indicatorii QoS [7].

III. GSPN cu Rate Fuzzy ale Tranziţiilor

În continuare, prezentăm unele definiții și notații, în conformitate cu [4, 7], care sunt necesare pentru a introduce GSPN cu rate fuzzy ale tranziţiilor, numite GSPNF.

O reţea GSPNF, este o structură de obiecte Γ, redată de următorul 13-tuplu: Γ = < *P, T, Pre, Post, Test, Inh,* K_p *, Pri, G,* $\tilde{\omega}$, $\tilde{\Lambda}$, $\mu_\omega, \mu_\lambda, M_0$ >, unde: *P* este mulţimea de *locaţii*, |*P*| = *k*. Locaţiile pot să conţină un număr întreg pozitiv de jetoane. În reprezentarea grafică locaţiile sunt redate prin cerculeţe; *T* este mulţimea de *tranziţii*, declanşarea cărora modifică marcajul curent. |*T*| = *n* şi $P \cap T = \varnothing$. În reprezentarea grafică tranziţiile sunt redate prin bare subţiri sau dreptunghiuri negre; *Pre, Test* şi *Inh* sunt funcţii de incidenţă *înainte*, *test* şi *inhibiţie,* iar *Post* este funcţii de incidenţă *înapoi*. Ponderile arcelor sunt funcţii marcaj-dependente ce au valori din mulţimea numerelor întregi nenegative IN_+. Prin arce normale se consumă jetoane din *pre-locaţii* sau se produc jetoane în *post-locaţiile* respective. Aceste arce sunt reprezentate prin săgeţi. Prin arcele inhibitoare şi/sau test nu se consumă jetoane. Un arc inhibitor este reprezentat printr-o linie cu un cerculeţ mic la sfârşit, iar un arc test este reprezentat printr-o săgeată cu o linie întreruptă. Implicit ponderea unui arc este egală cu 1 și ea nu se menţionează; K_p este funcţia de capacitate a locaţiilor ce redă numărul maxim de jetoane în locaţii . Implicit, ea este nelimitată; *Pri* este funcţia ce redă priorităţile dinamice ale declanşării tranziţiilor validate de către marcajul curent. Implicit, ele sunt sunt considerate nule; G este funcţia de gardă (eng. *Guard-function*) a tranziţiilor, care determină o funcţie Booleană $g(t,M)$ în marcajul curent M. Dacă tranziţia t este validată de marcajul curent M şi $g(t,M)$ are valoarea '*true*', atunci t rămâne validată şi eventual ea poate fi declanşată, iar dacă ea are valoarea '*false*' - ea nu este validată. Implicit $g(t,M)$ ='*true*'; *T* este partiționată în $T = T_\tau \cup T_0$, $T_\tau \cap T_0 = \varnothing$ cu $\Pr i(T_0) > \Pr i(T_\tau)$, unde T_τ este mulţimea tranziţiilor temporizate cu o durată aleatorie fuzzy de declanşare ce are o distribuţie exponenţial–negativă, iar T_0 este mulţimea tranziţiilor imediate cu o durată de declanşare nulă. În reprezentarea grafică tranziţiile imediate sunt redate prin bare subţiri, iar cele temporizate prin dreptunghiuri negre; $\tilde{\omega}: T_0 \times IN_+^{|P|} \to IR_+$ este funcţia de pondere fuzzy cu $0 \le \tilde{\omega}(t,M) < +\infty$ ce determină probabilitatea de declanşare a tranziţiei imediate în marcajul curent *M* care descrie un selector probabilistic. $\tilde{\Lambda}: T_\tau \times IN_+^{|P|} \to IR_+$ este funcţia ce determină rata fuzzy $0 < \tilde{\lambda}(t,M) < +\infty$ de declanşare a tranziţiei temporizate validate $t \in T_\tau(M)$ în marcajul curent *M*, adică parametrul legii exponenţial-negative. $\mu_\lambda: \tilde{\Lambda} \to [0,1]$ (resp. $\mu_\omega: \tilde{\omega} \to [0,1]$) este funcţia gradului de apartenenţă al lui $\tilde{\lambda}(t,M)$ (resp. $\tilde{\omega}(t,M)$) la mulţimea fuzzy $\tilde{\Lambda}$ (resp. $\tilde{\omega}$) care determină valorile numerice fuzzy ale ratelor (resp. ponderilor) de declanşare ale tranziţiilor temporizate (resp. imediate). IR_+ este mulţimea numerilor reale nenegative; M este un vector coloană ce reprezintă o funcţie de marcare a locaţiilor $p \in P$ în care $M(p) \in IN_+$ este numărul de jetoane în locația p. M_0 este marcajul inițial.

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

Regulile de funcţionare ale modelelor Γ de reţele GSPNF şi metoda de analiză a proprietăţilor lor comportamentale sunt aceleași ca și ale modelelor de GSPN, descrise în [4, 7]. Deosebirea se referă numai prin identificarea ratelor medii de declanşare a tranziţiilor validate ale GSPNF. Astfel, mai întâi identificăm ratele de declanşare ale tranziţiilor care sunt reprezentate ca NFT și/sau NFTz. Apoi în baza relațiilor (5), (6) și (7) din secțiunea 2 determinăm mărimile medii credibile ale ratelor $\bar{\lambda}_j$ (resp. ale ponderilor $\bar{\omega}_l$) de declanşare ale fiecărei tranziţii temporizate t_j (resp. imediate t_l) din Γ. Folosind mărimile respective ale acestor rate (resp. ponderi) medii, modelul Γ de reţea GSPNF este analizat în mod similar unui model GSPN. Însă, în această lucrare vom considera numai modele GSPNF în care toate atributele structurale (ponderile arcelor, funcția de gardă și prioritățile tranzițiilor) au mărimi implicite, iar capacitatea tuturor locaţiilor este egală cu 1.

IV. Analiza QoS în Baza GSPNF prin Tehnici ADŢ a RC

În această lucrare vom considera, ca scenariu de evaluare, un SW al unei RC ce utilizează tehnici AMŢ de apărare. Pentru a descrie prin GSPNF procesul de servire și apărare al SW vom presupune că:

1) Tehnicile AMŢ pot fi aplicate, conform regulilor periodice specificate de deplasare a ariei de atac, numai în procesul de servire a cererilor şi apariţiei evenimentului de expirare a duratei time-out sau la apariția unei alerte de securitate;

2) SW este gata să furnizeze servicii numai după completarea funcționalităților sale și a configurației sistemului de apărare;

3) Utilizatorul trimite o cerere de sincronizare pentru a obține adresa curentă a serverului rețelei. Dacă SW imple-

mentează tehnici de apărare AMŢ, sincronizarea este realizată prin actualizarea procesului de rutare și solicitare/răspuns. Dacă SW deplasează NAS în șablonul de salt, sincronizarea este realizată prin schema de sincronizare în timp sau printr-un schimb de informații ale șablonului de salt sau presetarea aceleiași funcții și a valorii inițiale [3, 6].

4) După obținerea adresei serviciului, utilizatorul poate stabili conexiunea cu SW. Apoi, acesta va trimite cererea de serviciu și va aștepta furnizarea serviciului solicitat;

5) În timpul procesului de servire, folosirea metodei AMŢ va schimba aria de atac a SW în conformitate cu schema de pre-setare (time-out expiră) sau la apariția unui eveniment anormal. Dacă este flosită metoda ST sau DPT, trebuie păstrată sau să fie migrată starea curentă a serviciului cu atributele sale (cum ar fi conexiunile, datele actuale etc.) pentru ca pe o nouă variantă software sau platformă să fie continuată procesarea sarcina anterioarei variante.

Dacă este folosită metoda NAS, există două cazuri:

a) Dacă este prevăzut un mecanism ce va asigura că conexiunile în curs să nu fie deconectate, sistemul ar continua să ofere servicii;

b) În caz contrar, sunt considerate următoarele două subcazuri: *i*) în cazul în care NAS este un șablon de salturi, cele două părți sunt pe deplin conștiente de acest fapt (inclusiv secvența de salturi) ambele sau o parte (de exemplu, clienții) sunt pe deplin conștienți de informațiile despre șablonul de salturi al celeilalte părți (de exemplu, serverul). Apoi utilizatorul poate primi în timp util adresa de serviciu și poate stabili direct conexiunea cu serverul; *ii*) Dacă NAS este un șablon AMŢ, utilizatorul nu va cunoaște informațiile despre starea curentă a serverului, prin urmare trebuie să trimită cererea de sincronizare și așteptare a conexiunii.

În cele mai multe din tehnicile AMŢ existente, de obicei, se trece la o nouă variantă/platformă/adresă după un interval de timp controlat de un mecanism time-out. Mai mult, unele dintre ele sunt schimbate în conformitate cu detectarea unei alerte de securitate [3, 6].

Schimbarea curentă a aplicării uneia din tehnici AMŢ, bazată pe un interval de timp fixat sau reglabil, este descrisă în modelul GSPNF de tranziții temporizate, pe când cea condusă de o alertă de securitate este descrisă de tranziții imediate.

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

- Colectarea informațiilor despre vulnerabilitatea componentelor RC, inclusiv și cea privind informațiile calculatoarelor gazdă, celor de servire și, de asemenea, colectarea relațiilor conexe ale echipamentelor;
- Construirea modelului comportamentului de atac și apărare atomic și compozit, apoi determinarea condițiilor în care apar tranziții de stări;
- Verificarea și validarea modelului prin metoda construirii lanțului Markov timp continuu (LMTC) al GSPN, subiacent GSPNF cu ratele medii credibile respectiv identificate [7, 9]. În cazul în care modelul nu este corect, ce vor efectua modificările necesare în GSPNF astfel construit.

Modelul $\Gamma 1$ în formă de GSPNF ce descrie procesul de servire și de apărare prin metode AMŢ este prezentat în Fig.1. În acest model locațiile (resp. tranzițiile) corespund stărilor (resp. acțiunilor, activităților) sistemului de securitate al RC.

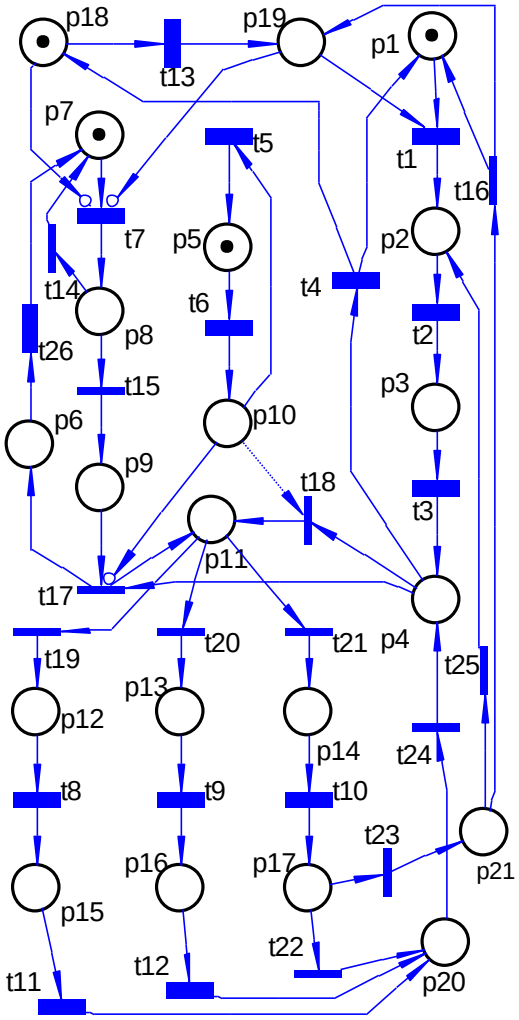

Fig. 1. Modelul $\Gamma 1$ de rețea GSPNF al apărării RC prin tehnici AMŢ.

Semnificația locațiilor și ale tranzițiilor modelului $\Gamma 1$:

- *locații*: p_1 - SW este gata să ofere servicii; p_2 - SW este în stare de sincronizare cu cererea de conectare; p_3 - SW este în stare de conectare; p_4 - SW servește cererea; p_5 - Timer-ul contorizează durata time-out; p_6 - Alerta de atac persistă; p_7 - Nu există nici-o alertă de securitate; p_8 - Alertă de securitate; p_9 - Alertă anormală de atac; p_6 - Alerta de atac persistă; p_7 - SW funcționează correct, nu există nici-o alertă de securitate; p_8 - Alertă de securitate; p_9 - Alertă anormală de securitate; p_{10} - Durata time-out a expirat; p_{11} - SW este în stare de apărare; p_{12} - SW își schimbă varianta software pentru a oferi servicii; p_{13} - SW își schimbă proprietățile platformei sale; p_{14} - SW își schimbă adresa de rețea; p_{15} -

SW utilizează o nouă variantă software de servire; p_{16} - SW are noi proprietăți de platformă; p_{17} - SW are o nouă adresă; p_{18} - utilizator sau atacator RC; p_{19} - accesare RC; p_{20} - setare comutare deservire după aplicarea unei metode AMȚ; p_{21} - Utilizatorul se reconectează la SW.

- *tranziții temporizate*: t_1 -Trimiterea cererii de sincronizare pentru a obține adresa de serviciu; t_2 - Stabilirea conexiunii cu SW; t_3 -Trimiterea unei solicitări de serviciu; t_4 - Utilizatorul obține serviciul solicitat ce se termină în mod normal; t_5 - Resetarea duratei time-out; t_6 - Durata time-out expiră în timpul procesului de servire; t_7 - Alertă de securitate apare în timpul procesului de servire; t_8 -Comutarea variantei software; t_9 - Comutarea schimbării proprietăților platformei de rulare; t_{10} - Comutarea schimbării adresei de rețea a serverului; t_{11} - Păstrarea stării serviciului; t_{12} - Migrarea stării de serviciu; t_{13} - Formarea cererii de servire (atac) ; t_{26} - atacul este cantracarat.
- *tranzițiilor imediate*: t_{14} - Eliminarea alertei false; t_{15} - Detectare alertă de atac RC; t_{16} - Utilizatorul inițiază reaccesarea SW în șablonul de schimbare a adresei; t_{17} - Sistemul de securitate răspunde la alerta de atac; t_{18} - Sistemul de securitate răspunde la expirarea duratei time-out; t_{19}, t_{20} și t_{21} - Sistemul de securitate alege metoda de apărare bazată respectiv: pe transformări software, pe *DPT* și pe schimbarea adreselor serverelor RC; t_{22} - Terminarea chimbării adreselor serverelor RC; t_{23} - Utilizatorul începe să se reconecteze la server; t_{24} - Terminarea comutării în starea de servire după aplicarea unei metode AMȚ; t_{25} - Utilizatorul inițiază reconectarea în șablonul de salt.

În acest model, folosim un arc inhibitor de la p_{10} la t_{17}, ceea ce înseamnă că atunci când există jetoane în locațiile p_9 și p_{10}, numai tranziția t_{18} poate fi declanșată, iar tranziția t_{17} este dezactivată. În starea de servire, dacă durata time-out expiră sau există o alertă de securitate, sistemul va răspunde celor două evenimente pentru a declanșa apărarea. Mai mult, acțiunile alternative pentru răspunsul la cele două evenimente (adică t_{17} și t_{18}) aparțin aceluiași set de acțiuni, care constă din cele trei acțiuni AMȚ respective și anume: transformări software; schimbarea proprietăților platformei de rulare și amestecarea adresei de rețea a sistemului. Ca urmare, atunci când SW procesează cererea și durata time-out expiră și între timp există o alertă de atac, sistemul de securitate trebuie doar să răspundă numai la un singur eveniment. În acest caz numai una din tranziții, t_{17} sau t_{18}, trebuie să fie declanșată.

În modelul $\Gamma 1$, sunt definite patru selectoare aleatoare. Primul este redat de tranzițiile imediate t_{14} și t_{15}. Probabilitatea ca tranziția t_{14} să fie declanșată este q_{14}, iar cea ca tranziția t_{15} să fie declanșată este q_{15}, care descrie probabilitatea existenței unei alerte de atac sau nu. Valorile lor satisfac condițiilor:

$$q_{14} = 1 - q_{15},\ q_{14}, q_{15} \in [0,1], \text{ unde}$$
$$q_{15} = (1 + M(p_8))/(1 + M(p_8) + M(p_{10}) + \gamma),$$

iar γ este un parametru ce caracterizează sistemul de securitate, care este determinat la etapa de proiectare.

Al doilea selector aleator este redat de tranzițiile imediate t_{17} și t_{18}, conditionat de $M(p_4) = 1$. Al treilea este redat de tranzițiile imediate t_{19}, t_{20} și t_{21}, care sunt declanșate cu probabilitatea respectivă q_{19}, q_{20} și q_{21}. Valorile lor satisfac următoarele relații: $q_{19} + q_{20} + q_{21} = 1, 0 \le q_{19}, q_{20}, q_{21} \le 1$.

Numim o arie de atac cea care schimbă o rundă de servire.

În diferite runde de servire pot fi alese diferite tipuri de tehnici AMȚ, dar numai o singură tehnică AMȚ poate fi folosită în fiecare rundă. Al patrulea selector este redat de tranzițiile imediate t_{22} și t_{23}, care sunt declanșate cu probabilitățile respective q_{22} și $q_{23}, q_{22} + q_{23} = 1,\ q_{22}, q_{23} \in [0,1]$. Acestea reprezintă probabilitatea ca apărarea să fie însoțită de un mecanism pentru a menține active conexiunile în curs sau nu. Valorile q_{22} și q_{23} sunt determinate de proiec-tant. Al cincilea selector este redat de tranzițiile imediate t_{16} și t_{25}, care sunt declanșate cu probabilitățile respective q_{16} și q_{25}, $q_{16} + q_{25} = 1, q_{16}, q_{25} \in [0,1]$. Valorile q_{16} și q_{25} se referă la politica de apărare selectată de către apărător.

Analiza numerică. Rețeaua GSPN subiacentă lui $\Gamma 1$ este mărginită, viabilă și reinițializabilă, deci LMTC fuzzy (LMTCF1) ce descrie funcționarea acestui model este ergodic [4, 7]. Acest LMTCF1 are 54 stări stabile.

Studiu de caz. Vom prezenta un studiu de caz de analiză numerică a unor indicatori QoS de securitate ai RC în baza utilizării modelului $\Gamma 1$ de rețea GSPNF descris anterior.

Folosind cunoștințele experților din domeniu [1, 2, 9, 13], pentru ratele fuzzy $\tilde{\lambda}_j$ de declanșare ale tranzițiilor temporizate, stabilim următoarele mărimi numerice:

$$\tilde{\lambda}_1 = (25, 36, 45),\ \tilde{\lambda}_2 = (65, 75, 85),\ \tilde{\lambda}_3 = (100, 150, 180),$$
$$\tilde{\lambda}_4 = (0.5, 1.0, 1.75),\ \lambda_5 = 30,\ \lambda_6 = 2.0,$$
$$\tilde{\lambda}_7 = (0.15, 0.35, 0.75),\ \tilde{\lambda}_{10} = (3.5, 5.5, 7.0), \quad (7)$$
$$\tilde{\lambda}_8 = \tilde{\lambda}_{11} = (2.0, 2.5, 3.5),\ \tilde{\lambda}_9 = \tilde{\lambda}_{12} = (1.5, 2.0, 3.5, 5.0),$$
$$\tilde{\lambda}_{13} = (2.75, 3.25, 4.75),\ \tilde{\lambda}_{26} = (10.75, 17.25, 19.5).$$

În mod similar stabilim $\gamma = 1$ și ponderile w_k asociate cu tranzițiile imediate, în baza cărora sunt determinate probabilitățile q_k de declanșare ale acestora:

$$w_k = 100 \cdot q_k,\ k = 14, 15, 19, 20, 21, 22, 23,$$
unde $q_{16} = 0.40, q_{25} = 0.40, q_{19} = 0.35,\ q_{20} = 0.25,$
$$q_{21} = 0.40,\ q_{22} = 0.70,\ q_{23} = 0.30; \quad (8)$$
$$w_l = 100,\ l = 16, 17, 18, 24, 25.$$

În baza relațiilor (6) și (7) din secțiunea 2 obținem următoarele mărimi ale ratelor medii credibile de declanșare ale tranzițiilor temporizate:

$$\bar{\lambda}_1 = 35.50,\ \bar{\lambda}_2 = 75.00,\ \bar{\lambda}_3 = 145.00,\ \bar{\lambda}_4 = 1.06,\ \bar{\lambda}_5 = 30.00,$$
$$\bar{\lambda}_6 = 2.00,\ \bar{\lambda}_7 = 0.40,\ \bar{\lambda}_{10} = 5.38,\ \bar{\lambda}_8 = \bar{\lambda}_{11} = 2.625,$$
$$\bar{\lambda}_9 = \bar{\lambda}_{12} = 3.00,\ \bar{\lambda}_{13} = 3.50,\ \bar{\lambda}_{26} = 16.31. \quad (9)$$

Pentru evaluarea indicatorilor QoS ai RC în baza modelului $\Gamma 1$, cu mărimile numerice specificate conform relațiilor (7), (8) și (9), au fost folosite platformele software instrumentale VPNP [8] și PIPE 2.5 [11].

În baza parametrilor numerici, redate de relațiile (8) și (9), ai modelului $\Gamma 1$, putem determina diferiți indicatori QoS, cum ar fi: durata medie a serviciului; productivitatea medie a sistemului; eficiența operațională pentru fiecare legătură de sistem etc. De exemplu, probabilitatea că sistemul de securitate al SW a contracarat cu succes atacurile intrușilor este determinată de probabilitatea $\pi_{sec} = \Pr(M(p_7) = 1)$ că $\Gamma 1$ de LMTCF1 se află în starea $M_k(p_7) = 1$, $M_k \in Acc(\Gamma 1)$, unde $Acc(\Gamma 1)$ este mulțimea de marcaje accesibile din M_0 ale $\Gamma 1$.

În Fig. 2 sunt prezentate graficele evoluției $\pi_{sec} = \Pr(M(p_7) = 1)$ funcție de $\bar{\lambda}_{13}$ și $\bar{\lambda}_7$.

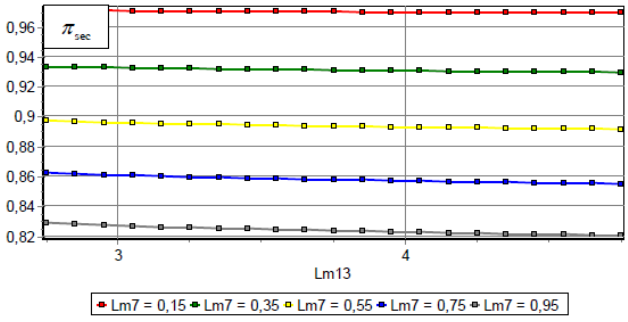

Fig. 2. $\pi_{sec} = \Pr(M(p_7) = 1)$ funcție de $\bar{\lambda}_{13}$ și $\bar{\lambda}_7$.

De asemenea, durata medie a serviciului unei cereri este determinată în baza legii lui Little [4, 7]: $\bar{\tau}_{serv.} = \bar{M}_{serv.} / \bar{\theta}_{serv.}$, unde $\bar{M}_{serv.}$ este numărul mediu de jetoane în locațiile fazelor de servire a cererii: $\bar{M}_{serv.} = (\sum_{i=1}^{4} \bar{M}(p_i)) = 0.5038$, iar $\bar{\theta}_{serv.}$ este rata medie a fluxului de jetoane ale tranzițiilor ce procesează serviciul dat: $\bar{\theta}_{serv.} = (\sum_{i=1}^{4} \bar{\theta}_i)) = 1.8454$. Prin urmare, obținem $\bar{\tau}_{serv.} = 0.27297$ (unităţi de timp).

CONCLUZII

În lucrarea dată este propusă o metodă de modelare și analiză a indicatorilor QoS ai RC cu modalități de apărare prin mutarea țintei de atac (AMȚ), ca fiind unele din tehnici "schimbătoare a jocului" în securitatea cibernetică, în baza rețelelor Petri stochastice generalizate (GSPN) cu rate fuzzy (GSPNF). Acest tip de modele permite de a descrie mai nuanțat comportamentul așteptat al atacatorilor și al apărării sistemului de securitate RC cu parametri fuzzy. În acest context, este prezentat şi analizat numeric un model GSPNF1 concret , cu parametri fuzzy, ce descrie funcţionarea apărării sistemului de securitate al unui server Web (SW) care folosește tehnici AMȚ cu atribute cantitativ nuanțate.

Abordarea propusă poate fi folosită la analiza eficienței implementării tehnicilor AMȚ la etapa de proiectare și dezvoltare a sistemelor de securitate ale RC.

Pe viitor, vom considera modele GSPNF colorate în care vom lua în considerație aspectul stocastic fuzzy intuiționist [2] de funcţionare al RC cu aplicații reconfigurabile și vom prezenta mai detaliat aplicabilitatea acestui demers.

Lucrarea dată a fost efectuată în cadrul proiectului naţional de cercetări ştiinţifice aplicative 14.820.18.02.03/U.

REFERINȚE

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

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

[3] G. Cai, B.Wang, Y. Luo, W. Hu,"A Model for Evaluating and Comparing Moving Target Defense Techniques Based on Generalized Stochastic Petri Net, Springer Science+Business Media Singapore J. Wu and L. Li (Eds.): ACA 2016, CCIS 626, pp. 184–197, 2016. DOI: 10.1007/978-981-10-2209-816.

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

[5] W. Connell, M, Albanese, S. Venkatesan,"A Framework for Moving Target Defense Quantification,"S. De Capitani di Vimercati and F. Martinelli (Eds.): SEC 2017, IFIP AICT 502, Springer International Publishing AG, pp. 124–138, 2017. DOI: 10.1007/978-3-319-58469-0 9.

[6] M. Crouse, B. Prosser, E.W. Fulp," Probabilistic performance analysis of moving target and deception reconnaissance defenses," In: Proceedings of the Second ACM Workshop on Moving Target Defense, AMȚ 2015, ACM, New York, pp. 21–29, 2015.

[7] E. Guţuleac, Evaluarea performanţelor sistemelor de calcul prin reţele Petri stochastice. Ed. „Tehnica-Info", Chişinău, 2004, - 276 p.

[8] E. Guţuleac E., C. Boşneaga, A. Reilean," VPNP-Software tool for modeling and performance evaluation using generalized stochastic Petri nets," In: Proceedings of the 6-th International Conference on D&AS2002, 23-25 May 2002, Suceava, România, pp. 243-248, 2002.

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

[10] I. El Mir, A. Chowdhary et al. , " Software Defined Stochastic Model for Moving Target Defense, " Proceedings of the Third International Afro-European Conference for Industrial Advancement—AECIA 2016, Advances in Intelligent Systems and Computing 565, pp. 188-197, 2016. DOI 10.1007/978-3-319-60834-1 20.

[11] Petri nets world - Petri nets tools database. *http://www.informatik.uni-hamburg.de/TGI/ PetriNets/tools/quick.html*

[12] H. Tan, C. Tang, C. Zhang, S. Wang,"Area-Dividing Route Mutation in Moving Target Defense Based on SDN. Z. Yan et al. (Eds.): NSS 2017, LNCS 10394, Springer International Publishing AG, pp. 565–574, 2017. DOI: 10.1007/978-3-319-64701-2_43.

[13] H. Xiao, R. Peng," Trade-Off Between Redundancy, Protection, and Imperfect False Targets in Defending Parallel Systems," A. Lisnianski et al. (eds.), Recent Advances in Multi-state Systems Reliability, Springer Series in Reliability Engineering, pp. 227-239, 2018. DOI 10.1007/978-3-319-63423-4_12.