MOKSLAS – LIETUVOS ATEITIS
SCIENCE – FUTURE OF LITHUANIA

ISSN 2029-2341 print / ISSN 2029-2252 online
2012 4(1): 27–30 doi:10.3846/mla.2012.06

Sistemų inžinerija, kompiuterių technologija T 120
System Engineering, Computer Technology T 120

Elektronika ir elektrotechnika
Electronics and Electrical Engineering

KOMPIUTERIŲ SISTEMŲ SAUGUMO MODELIAVIMAS

Lech Gulbinovič

Vilniaus Gedimino technikos universitetas
El. paštas lech.gulbinovic@vgtu.lt

Santrauka. Nagrinėjami šiuo metu žinomi kompiuterių sistemų saugumo modeliavimo metodai: tikimybių teorijos, Markovo procesų, Petri tinklų ir stochastinių veiklos tinklų. Šie metodai leidžia modeliuoti dinamines sistemas, kurioms kombinatoriniai metodai yra netinkami. Kadangi kompiuterių tinkluose įvykiai gali būti pasiskirstę ne tik pagal eksponentinį dėsnį, todėl jiems modeliuoti netinka Markovo procesų ir Petri tinklų modeliai. Realiuose tinkluose įvykiai gali būti pasiskirstę pagal eksponentinį, gama, Veibulo ir kt. dėsnius. Parodyta, kad iš aptartų šiuo metu žinomų modeliavimo metodų pagrindiniams saugumo veiksniams įvertinti tinkamiausias yra stochastinės veiklos tinklų metodas.

Reikšminiai žodžiai: modeliavimas, tikimybių teorija, Markovo procesai, Petri tinklai, stochastinės veiklos tinklai.

Įvadas

Sparti technologijų plėtra daro įtaką kompiuterių tinklo ir kompiuterių sistemų projektavimo procesui. Kompiuterių sistemos kuriamos keliant didelius reikalavimus sistemos spartai ir patikimumui. Suprojektuota ir įgyvendinta sistema turi atitikti jai iškeltus saugumo reikalavimus. Saugumo modeliavimas yra svarbus tokių sistemų projektavimo etapas. Jis gali gerokai sumažinti kompiuterių sistemos projektavimo sąnaudas ir trukmę, kadangi leidžia analizuoti sistemos elgseną pradedant nuo projektavimo pradžios iki sistemos galutinio įgyvendinimo (Paulauskas *et al.* 2009).

Kompiuterių sistemos saugumas apibūdinamas keliais parametrais. Pagrindiniai iš jų yra: konfidencialumas, vientisumas ir pasiekiamumas. Šiuo metu žinoma daug kompiuterių sistemų saugumo modeliavimo metodų, kurie taikomi projektuojant naujas sistemas ir vertinant jau naudojamų sistemų saugumą, tai: tikimybiniai, Markovo procesų, Petri tinklų ir kiti metodai (Nicol *et al.* 2004). Šio darbo tikslas yra išnagrinėti žinomus modeliavimo metodus, aptarti jų galimybes, privalumus bei trūkumus ir pasirinkti metodą, tinkamiausią pagrindiniams saugumo veiksniams įvertinti.

Tikimybiniai metodai

Tikimybių teorija gali būti taikoma patikimumui ir pasiekiamumui modeliuoti priimant tam tikras prielaidas, kad sistemos komponentų įvykių tikimybės yra nepriklausomos.

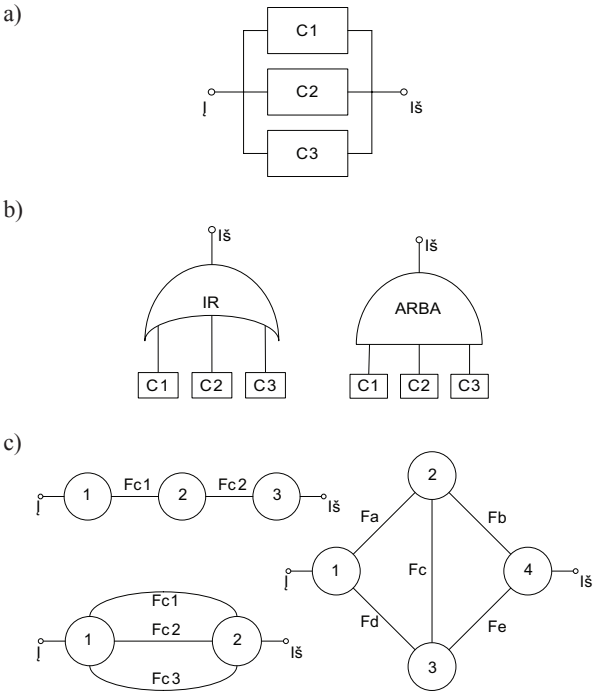
Universali charakteristika, tinkanti diskretiesiems, ir tolydiesiems dydžiams aprašyti, yra pasiskirstymo funkcija. Pasiskirstymo funkcija (arba integraliniu tikimybių skirstiniu) vadinama funkcija $F(X)$, atitinkanti tikimybę P, kad atsitiktinis dydis X įgis vertes, mažesnes negu x, t. y. intervale nuo $(0; \infty)$ iki x:

$$F\left(X\right) = P\left(X < x\right). \qquad (1)$$

Kai kuriais atvejais atsitiktinis dydis aprašomas nesinaudojant pasiskirstymo funkcija ar tikimybės tankiu, o imant tam tikras jo skaitines charakteristikas. Paprasčiausios ir svarbiausios atsitiktinio dydžio skaitinės charakteristikos yra teorinis vidurkis ir dispersija.

Sistemos pasiekiamumas yra apskaičiuojamas analogiškai, tik vietoj negendamumo tikimybės $P(t)$ taikoma $A(t)$ pasiekiamumo tikimybė. Pasiekiamumas – tai tikimybė, kad sistema atliks savo funkcijas numatytame laiko intervale.

Tinklo sistemos paprastai susideda iš kelių komponentų, tai gali būti maršrutų parinkikliai, komutatoriai, serveriai. Šiuos komponentus sudaro smulkesni komponentai, pvz.: atmintis, procesoriai, valdikliai ir kaupikliai. Taigi, visos sistemos negendamumas priklauso nuo visų komponentų negendamumo tikimybių. Sistema gali sugesti, kai vienas, keli arba visi komponentai sugenda. Modeliuojant tokią sistemą tikimybiniais metodais priimama prielaida, kad komponentų gedimų tikimybės yra nepriklausomos ir nedaro įtakos kitų komponentų gedimo tikimybei. Kompiuterių sistemos gali būti atvaizduojamos grafiškai (1 pav.). Yra keli populiarūs grafinio atvaizdavimo metodai, pvz., gedimų medis, patikimumo diagramos ar patikimumo grafai. Šie grafinio atvaizdavimo metodai labai mažai skiriasi tarpusavyje, yra tiktai daugiau ar mažiau populiarūs.



1 pav. Sistemos komponentų patikimumo grafinis atvaizdavimas: a) patikimumo diagramos; b) patikimumo medis; c) patikimumo grafai

Fig. 1. Graphical representation of the components of system components: a) reliability diagram; b) reliability tree; c) reliability graph

Grafiškai atvaizduota sistema leidžia įvertinti komponentų gedimų tikimybes ir jų išsidėstymą sistemoje. Sistema yra veikianti, kol yra bent vienas kelias tarp įėjimo ir išėjimo.

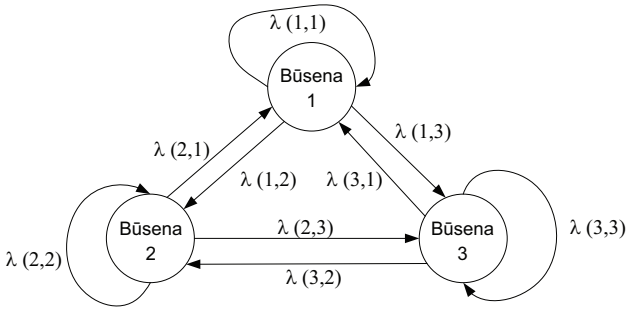
Tikimybių teorijos metodus tinka taikyti statinėms sistemoms, bet netinka – dinaminėms sistemoms modeliuoti. Realybėje dažniausiai sutinkamos dinaminės sistemos. Taip pat tikimybių teorijos prielaidos dažniausiai netinka realioms sistemoms, nes realios sistemos komponenčių gedimų tikimybės gali būti priklausomos. Vienas įvykis gali daryti įtaką kito įvykio tikimybei.

Markovo procesai

Dinaminėms sistemoms modeliuoti taikomi Markovo procesai (Pukite, J., Pukite, P. 1998). Sistema padalijama į būsenas, perėjimas tarp būsenų priklauso tik nuo esamos būsenos ir nepriklauso nuo praeities įvykių. Siekiant taikyti Markovo procesus turi būti priimtos tam tikros prielaidos, t. y. kad perėjimas tarp sistemos būsenų tūri būti pasiskirstęs pagal eksponentinį dėsnį. Eksponentinio pasiskirstymo funkcija yra be atminties, tai reiškia, kad vidutinis įvykių atsiradimo dažnis laiko intervale yra pastovus ir nepriklauso nuo jo padėties laiko ašyje, o priklauso tiktai nuo intervalo ilgio. Norint aprašyti Markovo procesą reikia:

− nurodyti visas būsenas, kuriose gali būti sistema,
− sudaryti sistemos būsenų grafą ir jame nurodyti visus galimus perėjimus iš vienos būsenos į kitą,
− kiekvienam perėjimui nurodyti atitinkamą įvykių srauto intensyvumą $\lambda_{ij}(t)$, kuris sistemos vieną būseną S_i pakeičia kita būsena S_j,
− nurodyti pradinę sistemos būseną, kai $t = 0$.

Sistemoje vykstantį nenutrūkstamą Markovo procesą galima aprašyti paprastomis diferencialinėmis lygtimis, kuriose nežinomos funkcijos yra būsenų tikimybės. Kaip atvaizduoti sistemos būsenų grafą, esant 3 būsenoms, parodyta 2 pav.



2 pav. Sistemos, sudarytos iš trijų būsenų, grafas

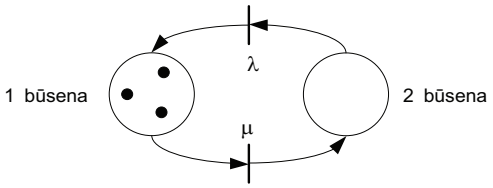
Fig. 2. Graph of a three-state system

Markovo grandines galima taikyti sistemos patikimumui, pasiekiamumui, našumui ir išliekamumui modeliuoti. Vienas iš Markovo grandinių trūkumų yra tas, kad sudarant grandinę tūri būti apibrėžtos visos galimos sistemos būsenos. Realių sistemų būsenų aibė gali būti labai didelė, dėl to Markovo grandinė tampa labai sudėtinga. Kai sistema turi daug (šimtus ar tūkstančius) būsenų, tai be kompiuterio sudaryti būsenų grafą ir atitinkamą algebrinių lygčių sistemą faktiškai neįmanoma. Jei lygčių sistemą ir turėtume, tai gauti analizinį sprendinį taip pat retai pavyksta. Antrasis trūkumas yra modelio nelankstumas, dėl to realios sistemos elgsenos atkūrimas dažniausiai yra komplikuotas.

Petri tinklai

Alternatyva Markovo grandinėms yra Petri tinklai. Petri tinklai buvo sukurti dinaminėms sistemoms modeliuoti. Jais galima modeliuoti tiek programinės įrangos, tiek tinklų sistemų patikimumą (Gulbinovič 2011; Nianhua *et al.* 2011). Petri tinklų naudojimas leidžia išvengti minėtų Markovo grandinių trūkumų. Šiuo atveju modelio dydis nepadidėja dėl komponentų skaičiaus, kadangi yra naudojamos ne globalios, o lokalios sistemos būsenos. Be to, Markovo grandinėse perėjimas tarp būsenų turi būti pasiskirstęs pagal eksponentinį dėsnį, o tai ne visada tinka realioms sistemoms.

Petri tinklai sudaromi naudojantis tokiais elementais, kaip pozicijos, veiklos, žetonai ir lankai. Pozicijos atvaizduoja sistemos būseną. Veiklos parodo įvykių prigimtį, tai gali būti momentiniai įvykiai, įvykiai esant vėlinimui ir įvykiai, pasiskirstę laike pagal pasirinktą pasiskirstymo dėsnį. Žetonai modelyje atvaizduoja sąlyginius objektus, kurie realioje sistemoje gali būti sistemos komponentai. Lankai – tai keliai, kuriais žetonai gali judėti modelyje. 3 pav. parodytas sistemos, sudarytos iš trijų komponentų Petri tinklo. Kiekvienas iš komponentų gali sugesti esant tai pačiai tikimybei λ, komponentas atstatomas esant μ tikimybei. Petri tinkle sistemos būsena nuskaitoma iš pozicijų, kurios aprašomos lokaliai. Dėl to nuo komponentų skaičiaus modelis nedidėja (Nianhua *et al.* 2011).



3 pav. Sistemos, sudarytos iš trijų komponentų Petri tinklo, modelio pavyzdys

Fig. 3. Example of the Petri network model for a three-component system

Petri tinklus lengviau sudaryti, modifikuoti ir analizuoti negu Markovo grandines. Petri tinklai – tai patogi grafinė aukšto lygio kalba, nusakanti sistemos elgseną. Yra keli Petri tinklų tipai, pasižymintys įvairiais funkcijų plėtiniais, kurie taikomi sprendžiant specifinius uždavinius. Laiką įvertinantis Petri tinklas (angl. *Petri Net with Time*). Laikas buvo įvestas norint modeliuoti sąveikas tarp kelių procesų atsižvelgiant į jų pradžią ir pabaigą. Stochastiniai Petri tinklai SPN (angl. *Stochastic Petri Nets*) yra tokie laiką įvertinantys tinklai, kurių būsenos keičiasi nepriklausomai, perėjimų vėlinimai yra atsitiktinai pasiskirstę pagal eksponentinį dėsnį. Apibendrintas stochastinis Petri tinklas (angl. *Generalized Stochastic Petri Net,* GSPN) įvertina dviejų rūšių sistemos būsenų kaitą: nepriklausančią nuo laiko ir priklausančią nuo laiko (pasiskirsčiusią eksponentiniu dėsniu). Neuždelsti perėjimai turi pirmenybę prieš priklausančius nuo laiko perėjimus. Taip pat neuždelsti perėjimai gali turėti prioritetus vienas kito atžvilgiu. Egzistuoja ir daugiau Petri tinklų rūšių. Šio formalaus metodo paplitimas rodo jo paprastumą ir universalumą.

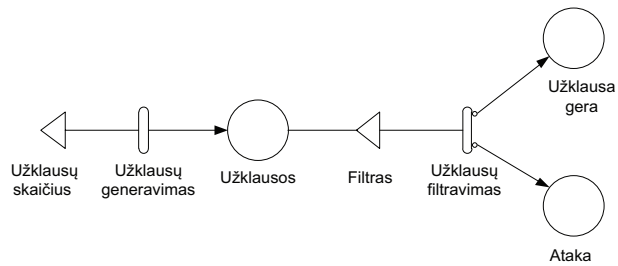
Stochastinės veiklos tinklai

Kompiuterių ir tinklo sistemų patikimumo, pasiekiamumo, našumo ir išliekamumo įvertinimo modeliavimo metodai plėtojosi tiek pat ilgai, kiek ir pačios sistemos. Vieni metodai, turėję trūkumų arba apribojimų, buvo pakeisti kitais metodais. Vienas iš tobuliausių ir lanksčiausių modeliavimo metodų yra stochastinės veiklos tinklai, tai yra patobulintas Petri tinklų metodas. Stochastiniai veiklos tinklai (angl. *Stochastic Activity Network*) yra lanksti ir lengvai taikoma stochastinių Petri tinklų atmaina (Beaudet *et al.* 2006; Pinsky, Karlin 2001).

Stochastinės veiklos tinkluose yra galimi papildomi tinklo modeliavimo objektai – įėjimo ir išėjimo vartai – leidžiantys kontroliuoti įvykių pradžią ir pabaigą, priklausomai nuo aprašytų sąlygų. Stochastiniai veiklos tinklai apima stochastinį veiklos tinklų AN (angl. *Activity Network*) išplėtimą, panašiai kaip stochastiniai Petri tinklai – klasikinių Petri tinklų išplėtimą. Stochastinės veiklos tinkluose galimas matematinis sąlygų aprašymas naudojant tokius veiksmus, kaip sudėtis, atimtis, palyginimas – daugiau, mažiau, prilyginimas nuliui. Naudojantis stochastinės veiklos tinklais galima kurti sudėtingus ir kompleksinius įvairių sistemų modelius. Veikla gali turėti kelis baigties atvejus. Įėjimo vartai turi įjungimo sąlygą ir funkciją, kuri kontroliuoja veiklų vykdymą. Išėjimo vartai turi tik funkciją, kuri nusako, kaip keičiasi žyma įvykdžius veiklą. Vartų naudojimas suteikia daugiau lankstumo ir todėl SAN yra funkcionalesni už Petri tinklus (Garšva *et al.* 2011; Garšva 2006).

Stochastinės veiklos tinklo pavyzdys pateiktas 4 pav. Tai yra tinklo sistemos vartotojo modelis, kuris realizuotas kaip vartotojo užklausų generatorius. Modelyje apibrėžtos tokios modelio sąlygos, kaip sugeneruotų užklausų kiekis, užklausų pasiskirstymo dėsnis, užklausų filtravimas pagal tam tikrus kriterijus modeliuojant ugniasiene, užklausų pasiskirstymas pagal prigimtį – ataka ar užklausa.

Taikant 4 pav. pateiktą modelį galima įvertinti pagrindines saugumo charakteristikas: konfidencialumą, vientisumą ir pasiekiamumą. Kiekviena užklausa gali vienaip ar kitaip daryti įtaką sistemai, ar tai bus visos sistemos arba jos dalies gedimas, sistemos duomenų atskleidimas, veikiantis konfidencialumą, arba kito pobūdžio ataka. Patikimumas



4 pav. Stochastinės veiklos tinklų pavyzdys

Fig. 4. Example of the stochastic activity network

$P_{(s=1)}$ – tai tikimybė, kad kompiuterių sistema bus normalaus būvio (s = 1); vientisumas – tai tikimybė, kad visą sistemos naudojimo laiką T_{eks} sistema nepereis iš normalaus pradinio būvio (s = 1) į kokį nors kitą. Modelis pagrįstas įvairiausių įvykių tikimybėmis, kurios yra pasiskirsčiusios laike.

Išvados

1. Tikimybių teorijos metodai tinka tik statinių sistemų charakteristikoms modeliuoti.
2. Markovo procesai tinka dinaminėms sistemoms modeliuoti. Tačiau taikant Markovo procesus sistemos modelis greitai išauga dėl komponenčių skaičiaus padidėjimo, nes yra modeliuojamos globalios būsenos.
3. Petri tinklai yra alternatyva Markovo grandinėms. Jų privalumas tas, kad modelis neišauga dėl komponenčių skaičiaus padidėjimo, nes modeliuojamos lokalios būsenos vietoj globalių. Petri tinklus lengviau sudaryti, modifikuoti ir analizuoti negu Markovo grandines. Petri tinklai yra apriboti tokiomis sąlygomis, kaip +, –, > ir prilyginimas nuliui. Sudėtinga modeliuoti sudėtingas sistemas.
4. Stochastinės veiklos tinklai yra išplėstas galimybėmis Petri tinklas. Yra galimybė aprašyti įvykių pradžios ir pabaigos sąlygas bei pasirinkti laikines ir akimirkos veiklas, jų pasiskirstymo dėsnį. Būsenų keitimo galimybė priklausoma nuo įvykių. Galimi papildomi tinklo aprašymo objektai: perėjimo sąlygos, įėjimo ir išėjimo vartai.
5. Atliktas tyrimas parodė, kad iš aptartų modeliavimo metodų labiausiai dinaminių sistemų saugumo charakteristikoms modeliuoti tinka stochastinės veiklos tinklų metodas. Stochastinės veiklos tinklai leidžia įvertinti skirtingus įvykių pasiskirstymo dėsnius. Stochastinių veiklos tinklų modeliai yra funkcionalesni už Petri tinklų modelius. Be to, jie gali būti lengvai tobulinami ir redaguojami.

Literatūra

Beaudet, S. T.; Courtney, T.; Sanders, W. H. 2006. A behavior-based process for evaluating availability achievement risk using stochastic activity networks, in *Reliability and Maintainability Symposium*, 21–28.

Garšva, E. 2006. Computer system survivability modelling by using stochastic activity network, in *Safecomp Conference Proceedings*, 71–84.

Garšva, E.; Paulauskas, N.; Gulbinovič, L.; Stankevičius, A. 2011. Computer system survivability evaluation based on risk analysis, in *Information Systems Architecture and Technology. Web Information Systems Engineering, Knowledge Discovery and Hybrid Computing Networks*. Wroclaw, 291–301. ISBN 978-83-7493-630-9.

Gulbinovič, L. 2011. Aštuonių skilčių mikrovaldiklių galimybių tyrimas panaudojimo Ethernet tinklo įrenginiuose, *Mokslas – Lietuvos ateitis* [Science Future – of Lithuania] 3(1): 82–86. http://dx.doi.org/10.3846/mla.2011.017

Nianhua, Y.; Huiqun, Y.; Zhilin, Q.; Hua, S. 2011. Modeling and quantitatively predicting software security based on stochastic Petri nets, *Mathematical and Computer Modelling*. ISSN 0895-7177.

Nicol, D. M.; Sanders, W. H.; Trivedi, K. S. 2004. Model-based evaluation: from dependability to security, in *IEEE Transaction on Dependable and Secure Computing*, 48–65.

Paulauskas, N.; Garsva, E.; Skudutis, J. 2009. Network scan detection simulation, *Elektronika ir elektrotechnika* 2(90): 43–46.

Pinsky, M.; Karlin, S. 2001. *An Introduction to Stochastic Modeling*. 4th edition. ISBN 978-0-12-381416-6.

Pukite, J.; Pukite, P. 1998. *Markov Modeling for Reliability Analysis*. IEEE Press Series. ISBN 0-7803-3482-5. http://dx.doi.org/10.1109/9780470545317

TECHNIQUES FOR MODELLING NETWORK SECURITY

L. Gulbinovič

Abstract

The article compares modelling techniques for network security, including the theory of probability, Markov processes, Petri networks and application of stochastic activity networks. The paper introduces the advantages and disadvantages of the above proposed methods and accepts the method of modelling the network of stochastic activity as one of the most relevant. The stochastic activity network allows modelling the behaviour of the dynamic system where the theory of probability is inappropriate. A real network distributes incidents referring to various distribution methods (exponential, gama, Veibul, etc.). A real system should evaluate time value when the stochastic activity network allows such activity.

Keywords: modelling, probability, Markov processes, Petri network, stochastic activity network.