VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Simona RAMANAUSKAITĖ

SRAUTINIŲ ATAKŲ ĮTAKOS INTERNĖTINĖS PASLAUGOS SUTRIKDYMUI MODELIAVIMAS IR TYRIMAS

DAKTARO DISERTACIJOS SANTRAUKA

TECHNOLOGIJOS MOKSLAI,
INFORMATIKOS INŽINERIJA (07T)

VGTU
LEIDYKLA
Vilnius TECHNIKA 2012

Disertacija rengta 2008–2012 metais Vilniaus Gedimino technikos universitete.
Mokslinis vadovas
prof. habil. dr. Antanas ČENYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T).
Disertacija ginama Vilniaus Gedimino technikos universiteto Informatikos inžinerijos mokslo krypties taryboje:
Pirmininkas
doc. dr. Arnas KAČENIAUSKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T).
Nariai:
prof. habil. dr. Romualdas BAUŠYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),
doc. dr. Olga KURASOVA (Vilniaus universitetas, technologijos mokslai, informatikos inžinerija – 07T),
prof. habil. dr. Rimantas ŠEINAUSKAS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T),
prof. dr. Olegas VASILECAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T).
Oponentai:
prof. habil. dr. Vincas LAURUTIS (Šiaulių universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T),
prof. dr. Dalius NAVAKAUSKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Disertacija bus ginama viešame Informatikos inžinerijos mokslo krypties tarybos posėdyje 2012 m. birželio 7 d. 14 val. Vilniaus Gedimino technikos universiteto senato posėdžių salėje.
Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.
Tel.: (8 5) 274 4952, (8 5) 274 4956; faksas (8 5) 270 0112;
el. paštas doktor@vgtu.lt
Disertacijos santrauka išsiuntinėta 2012 m. gegužės 4 d.
Disertaciją galima peržiūrėti Vilniaus Gedimino technikos universiteto (Saulėtekio al. 14, LT-10223 Vilnius, Lietuva) ir Vilniaus universiteto Matematikos ir informatikos instituto (Akademijos g. 4, LT-08663 Vilnius, Lietuva) bibliotekose.
VGTU leidyklos „Technika“ 1998-M mokslo literatūros knyga.

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Simona RAMANAUSKAITĖ

MODELLING AND RESEARCH OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

SUMMARY OF DOCTORAL DISSERTATION

TECHNOLOGICAL SCIENCES,
INFORMATICS ENGINEERING (07T)

VGTU
LEIDYKLA
Vilnius TECHNIKA 2012

Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2008–2012.
Scientific Supervisor
Prof Dr Habil Antanas ČENYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).
The dissertation is being defended at the Council of Scientific Field of Informatics Engineering at Vilnius Gediminas Technical University:
Chairman
Assoc Prof Dr Arnas KAČENIAUSKAS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).
Members:
Prof Dr Habil Romualdas BAUŠYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).
Assoc Prof Dr Olga KURASOVA (Vilnius University, Technological Sciences, Informatics Engineering – 07T).
Prof Dr Habil Rimantas ŠEINAUSKAS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).
Prof Dr Olegas VASILECAS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).
Opponents:
Prof Dr Habil Vincas LAURUTIS (Šiauliai University, Technological Sciences, Electrical and Electronics Engineering – 01T).
Prof Dr Dalius NAVAKAUSKAS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).

The dissertation will be defended at the public meeting of the Council of Scientific Field of Informatics Engineering in the Senate Hall of Vilnius Gediminas Technical University at 2 p. m. on 7 June 2012.
Address: Saulėtekio al. 11, LT-10223 Vilnius, Lithuania.
Tel.: +370 5 274 4952, +370 5 274 4956; fax +370 5 270 0112;
e-mail: doktor@vgtu.lt
The summary of the doctoral dissertation was distributed on 4 May 2012.
A copy of the doctoral dissertation is available for review at the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, LT-10223 Vilnius, Lithuania) and at the Library of Vilnius University Institute of Mathematics and Informatics (Akademijos g. 4, LT-08663 Vilnius, Lithuania).

Įvadas

Mokslo problemos aktualumas. Verslo perėjimas į internetinę erdvę įtakoja kenksmingo programinio kodo kūrėjų siekius. Anksčiau vyraves pripažinimo siekis, dabar dažnai keičiamas ekonominės naudos siekimu. Vis dažniau pasitaiko kibernetinių atakų, siekiančių sutrikdyti internetinių paslaugų kokybę ar padaryti ją neprieinamą teisėtiems vartotojams. Tokių veiksmų ekonominė nauda pasiekiama reikalaujant išpirkos iš sistemos savininko už veiksmų nutraukimą, atakos nerengimą arba teikiant konkurentų internetinių sistemų eliminavimo numatytam laikotarpiui paslaugas.

Prieinamumo užtikrinimo poreikį rodo ir internete platinamos programinės įrangos ir nuomojamų Botnet tinklų kiekiai. Tai leidžia net ir nepatyrusiems programišiams vykdyti pakankamai sėkmingas srautines internetinės paslaugos sutrikdymo (angl. Distributed Denial of Service – DDoS) atakas.

Nors informacijos prieinamumo užtikrinimo problema yra žinoma daugeliui sistemų administratorių, tačiau griežtų rodiklių ir metodų, leidžiančių įvertinti turimų apsaugos priemonių efektyvumą, beveik nėra. Kiekvienas serverio administratorius pats vertina sistemos atsparumo lygį, pasitelkdamas turimas žinias ar eksperimentinę veiklą. Todėl vartotojas, ieškodamas serverio savo paslaugos diegimui, turi pasitikėti tiekėjo nurodytu sistemos patikimumo vertinimu arba vadovautis prieš tai vykusių atakų prieš tą serverį statistika.

Turint detalų tinklinių paslaugų trikdymo modelį, būtų galima kiekybiškai įvertinti potencialių grėsmių pavojų, modeliuoti įvairių apsaugos priemonių efektyvumą.

Tyrimo objektas. Tyrimo objektas – srautinė internetinės paslaugos sutrikdymo ataka ir jos efektyvumo vertinimo modelis.

Darbo tikslas ir uždaviniai. Pagrindinis darbo tikslas – sukurti srautinės internetinės paslaugos sutrikdymo atakos modelį atakos efektyvumui nustatyti. Darbo tikslui pasiekti reikia išspręsti šiuos uždavinius:

1. Išanalizuoti egzistuojančius DDoS atakų tipus ir kovai su jomis naudojamas kontrpriemones.
2. Išnagrinėti egzistuojančius šio tipo atakų modelius.
3. Sukurti tris skirtingo tipo resursų išnaudojimo DDoS atakų modelius.
4. Apjungti sukurtus DDoS atakų modelius bendrai atakos sėkmės tikimybei įvertinti.
5. Atlikti sukurtų modelių tinkamumo įvertinimą.
6. Sukurti modelio prototipą ir jį taikant atlikti eksperimentus su skirtingo tipo DDoS atakomis.

Tyrimų metodika. Norint pasiekti tikslą, buvo taikomi šie tyrimų metodai:

1. Lyginamoji ir literatūros analizė – DoS atakų ir jų kontrpriemonių savybių, taksonomijų, modelių tipų, egzistuojančių modelių palyginimui ir įvertinimui;
2. Apibendrinimas – analizės ir tyrimų rezultatų susisteminimui ir reikšmingumo nustatymui;
3. Matematinis modeliavimas – DDoS atakų savybių nustatymui ir situacijų parinkimui.

Mokslinis naujumas. Rengiant disertaciją, gauti šie informatikos inžinerijos mokslui nauji teoriniai ir praktiniai rezultatai:

1. Pasiūlytos naujos DoS atakų ir jų kontrpriemonių taksonomijos, leidžiančios išsamiau aprašyti tam tikrą DoS ataką ir jos kontrpriemones.
2. Sukurtas centrinio procesoriaus darbo išnaudojimo modelis, kuris dar nebuvo aprašytas kaip atskiras DoS atakų tipas, o priskiriamas prie resursų išnaudojimo atakų;
3. Pasiūlytas naujas jungtinis DDoS atakos modelis, leidžiantis tiksliau įvertinti skirtingo tipo DDoS atakų dedamąsias bendrai atakos sėkmės tikimybei įvertinti.

Praktinė vertė. Tinklinių sistemų prieinamumo vertinimas iki šio buvo grindžiamas tik ekspertų vertinimu, kuris pasižymi subjektyvumu. Todėl reikalinga metodika, leidžianti vienareikšmiškai vertinti skirtingų sistemų prieinamumą.

Rengiant disertaciją atlikti darbai leidžia, remiantis nauja klasifikacija, paprasčiau atlikti naujo tipo DoS atakų ir/ar jų kontrpriemonių priskyrimą atitinkamoms kategorijoms.

Pasiūlytas jungtinis DDoS atakų modelis, kurį taikant galimas skirtingo tipo DDoS atakų tikimybės įvertinimas. Jis leidžia iš anksto įvertinti sistemos patikimumą, neatliekant realių bandymų su sistema. Todėl, naudojant jį visuotinai prieglobos, paslaugų tiekėjų, galėtų padėti nustatyti jų serverių prieinamumo kiekybiniam vertinimui.

Disertacijoje atliktų eksperimentų rezultatai leidžia daryti išvadas apie DDoS atakos dedamąsias bei parametrus turinčius didžiausią įtaką atakos sėkmės tikimybei ir agentų skaičiaus Botnet tinkle kaitos įtaką atakos eigai.

Ginamieji teiginiai. Formuojami šie ginamieji teiginiai:

1. Tikimybinis skirtingo tipo DDoS atakų modeliavimas įgalina sukurti jungtinį DDoS atakų modelį, apibendrinantį atakos sėkmės tikimybę.

2. Netinkami sistemos nustatymai ar neįvertinta potenciali sistemos apkrova gali sukelti DoS atakos efektą. Dėl šios priežasties DDoS atakos sėkmės tikimybė turėtų būti naudojama, kuriant prevencijos priemones bet kokio tipo internetinių sistemų prieinamumui gerinti, neatsižvelgiant į joms gresiančių DDoS atakų tikimybę.
3. DDoS atakos metu skirtingos sistemos dalys įtakoja viena kitą, todėl, norint gauti tikslesnį DDoS atakos sėkmės tikimybės įvertinimą, turi būti naudojamas jungtinis DDoS atakų modelis.
4. Jungtinė DDoS atakos sėkmės tikimybė nėra tiesiškai priklausoma nuo atakos parametrų, todėl negali būti aprašoma tiesine lygtimi.

Darbo apimtis. Darbą sudaro įvadas, penkti pagrindiniai skyriai ir bendrosios išvados. Darbo apimtis yra 109 puslapiai, tekste panaudotos 42 numeruotos formulės, 55 paveikslai ir 8 lentelės. Rašant disertaciją buvo panaudota 120 literatūros šaltinių. Darbas buvo pristatytas 5 konferencijose. Disertacijos tema publikuoti 7 straipsniai.

1. Srautinės internetinės paslaugos sutrikdymo atakos, jų kontrpriemonės ir modelių analizė

Pirmame skyriuje pateikiami internetinės paslaugos sutrikdymo (DoS – Denial of Service) (dar žinomų kaip atkirtimo nuo paslaugos arba atsisakymo aptarnauti) ir srautinių internetinės paslaugos sutrukdymo (DDoS – Distributed Denial of Service) atakų apibrėžimai ir skirtingų autorių požiūriai į jas. Ypatingas dėmesys skiriamas Botnet principams, naudojamoms naujų agentų paieškos technologijoms, kenksmingo programinio kodo platinimo ir valdymo schemoms, nes Botnet panaudojimas yra pagrindas sėkmingoms DDoS atakoms rengti.

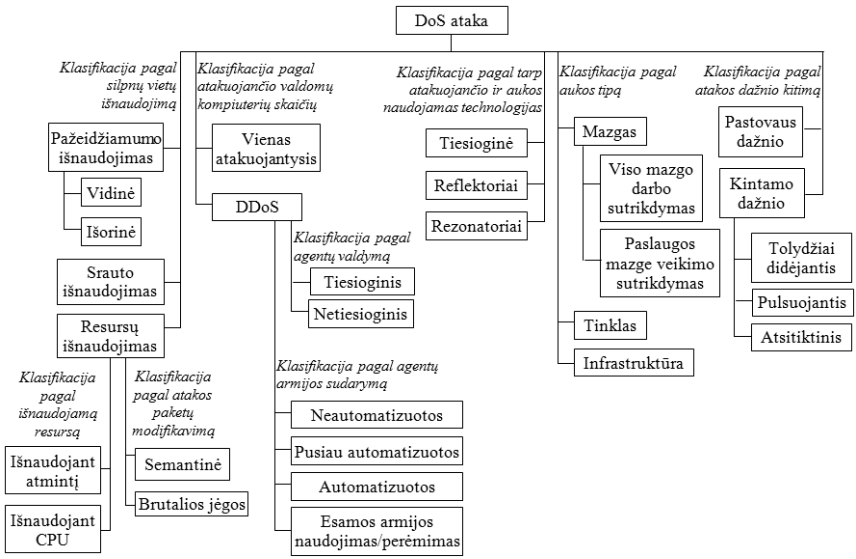
Šiame skyriuje taip pat gilinamasi į kompiuterių tinklų ir DoS, DDoS atakų modeliavimo specifiką. Jame analizuojamos internetinio srauto savybės ir siūlomi modeliai realiam internetinio srauto generavimui ar atspindėjimui. Taip pat pateikiami argumentai, kodėl Erlang modelis yra tinkamas ar netinkamas internetinio srauto modeliavimui.

Taip pat šiame skyriuje analizuojami modelių tipai ir jų realizavimo technologijos, bei aprašomi keturi pagrindiniai modelių tipai DoS ir DDoS atakų modeliavimui: kaina paremti modeliai; žaidimu paremti modeliai; perrašymo teorijos modeliai; matematiniai modeliai. Analizuojant šiuos modelių tipus ir jų taikymo atvejus, pastebima, kad naujausios idėjos daugelyje šių modelių tipų pradeda taikyti stochastinius elementus interneto srauto nenuspėjamumui atspindėti. Iš 21 analizuoto DoS ir DDoS atakų modelio tik 7

modeliai nenaudojo tikimybinių išraiškų atakos ar aukos savybėms nusakyti ir visi šie modeliai buvo publikuoti anksčiau nei 2007 metais.

2. Naujos internetinės paslaugos sutrikdymo atakų ir jų kontrpriemonių taksonomijos

Išanalizavus egzistuojančias DoS ir DDoS atakų taksonomijas pastebėta, kad analizuotos taksonomijos nepilnai atspindi šiuo metu egzistuojančių DoS atakų ir jų kontrpriemonių savybes arba yra palyginti sunkiai suvokiamos. Įvertinant, kad moksle ir praktikoje yra svarbi bendra terminologija ir galimų DoS atakų ir jų kontrpriemonių įvairovės suvokimas, antrame skyriuje aprašyta siūloma nauja DoS atakų taksonomija (1 pav.).

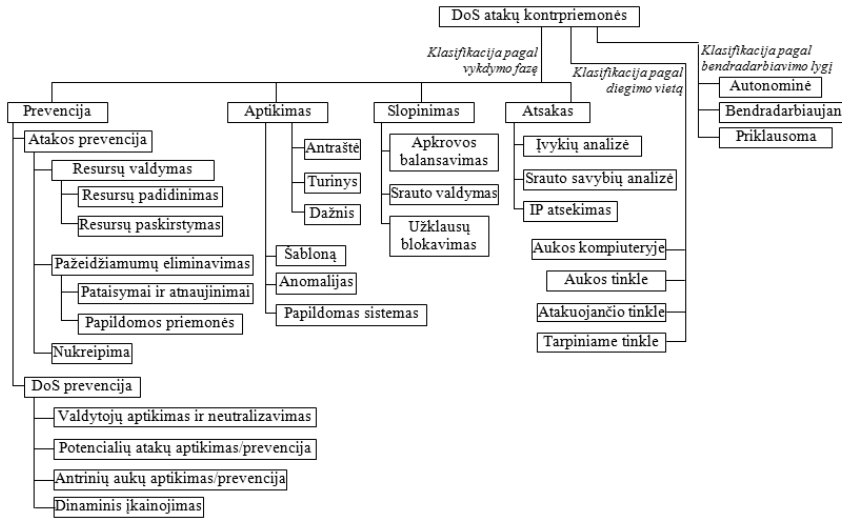


1 pav. Siūloma DoS atakų taksonomija

Lyginant su kitomis DoS ir DDoS atakų taksonomijomis, ji papildyta procesoriaus darbo išnaudojimo kategorija, išskirta nauja dimensija, apibendrinanti DoS efekto sukėlimo metodą. Atakos automatizavimo lygyje išskiriami keturi skirtingi atvejai (neautomatizuotas agentų armijos formavimas; pusiau automatizuotas agentų armijos formavimas; automatizuotas agentų armijos formavimas; egzistuojančios agentų armijos perėmimas ar nuoma), pakeista atakos aukos tipų taksonomija (tinklas, infrastruktūra, mazgas, kuris

gali būti sutrikdomas visas, arba tik tam tikra paslauga jame). Šie patobulinimai ir kitoks kitose DoS ir DDoS atakų taksonomijose naudojamų kategorijų išdėstymas turėtų aiškiau atspindėti DoS atakų savybes ir jų priklausomybę, nes dalis kategorijų taip pat gali būti detalizuojama pagal kelis skirtingus kriterijus.

Taip pat šiame skyriuje, remiantis apžvelgtomis DoS ir DDoS atakų kontrpriemonių taksonomijomis, pasiūlyta nauja DoS kontrpriemonių taksonomija (2 pav.).



2 pav. Siūloma DoS atakų kontrpriemonių taksonomija

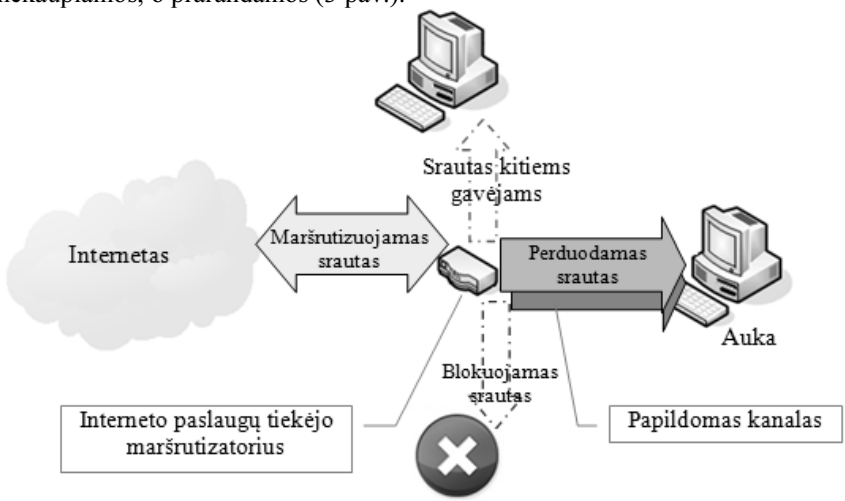
Joje naudojamos kitokios nei kitų autorių išskiriamos dimensijos (fazė, diegimo vieta ir bendradarbiavimo su kitomis sistemomis lygis), prevenciją patariame skirstyti į dvi kategorijas, nusakančias, kaip pasiruošti gresiančiai atakai ir kaip iš esmės išvengti DoS efekto internete. Taip pat šioje taksonomijoje sujungiamos kelių kitų taksonomijų savybės į vieną, kas leidžia plačiau atspindėti visas DoS atakų kontrpriemonių savybes.

Siūlomos naujos taksonomijos, skirtos esminiams DoS atakų ir jų kontrpriemonių tipams nusakyti ir atvaizduoti jų tarpusavio ryšius. Todėl, vadovaujantis pateiktomis taksonomijų diagramomis ir kategorijų aprašais, turėtų būti nesunku aprašyti egzistuojančių ar naujų DoS atakų ir jų kontrpriemonių savybes.

3. Jungtinis srautinės internetinės paslaugos sutrikdymo atakos modelis

Srauto išnaudojimo DDoS atakos modelis

Srauto išnaudojimo DDoS atakos modelyje naudojama atviroji daugiakanalė masinio aptarnavimo sistema su ribota eile (M/G/K/K). Joje yra K atvirų kanalų. Jei visi kanalai yra užimti, negalimos aptarnauti užklausos yra nekaupiamos, o prarandamos (3 pav.).



3 pav. Srauto išnaudojimo DDoS atakos konceptualusis modelis

Srauto išnaudojimo DDoS atakos sėkmės tikimybei P_B įvertinti, pagal (1) formulę randamas vidutinis užklausų blokavimo procentas P_{ub} ir įvertinamos sistemos filtravimo savybės (2).

$$P_{ub} = \frac{\frac{\rho^K}{K!}}{\sum_{j=0}^{K} \frac{\rho^j}{j!}} \tag{1}$$

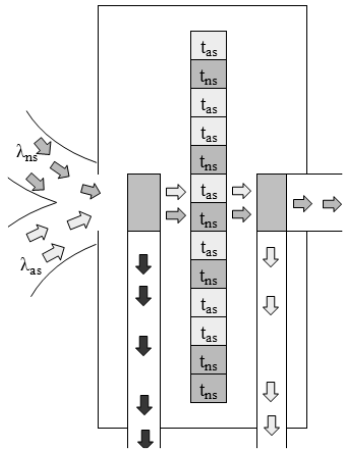
čia ρ – atvykstančių ir aptarnaujamų užklausų greičio santykis.

$$P_B = P_{fpr} + P_{ub} \cdot (1 - P_{fpr}) \tag{2}$$

čia P_{fpr} – tikimybė, kad teisėto vartotojo užklausa bus įvardinta kaip atakos srautas.

Atminties išnaudojimo DDoS atakos modelis

Atminties išnaudojimo DDoS atakos modeliui siūloma naudoti atvirąją daugiakanalę masinio aptarnavimo sistemą su ribota eile (M/M/N/N). Jos atminties buferyje telpa *N* sujungimų informacija. Jei visas atminties buferis yra užimtas – naujai atvykstančios užklausos yra prarandamos (4 pav.).



4 pav. Atminties išnaudojimo DDoS atakos konceptualusis modelis

Sistemoje teisėtų ir atakos užklausų sujungimų informacijos saugojimo terminai yra skirtingi. Todėl, skaičiuojant dėl nepakankamos vietos atminties buferyje blokuojamų užklausų dalį (3), prieš tai reikia įvertinti vidutinį atvykstančių užklausų greitį ir vidutinį vienos užklausos laikymo atminties buferyje laiką.

$$P_{im} = \frac{\frac{\rho^N}{N!}}{\Sigma_{j=0}^{K} \frac{\rho^j}{j!}} \tag{3}$$

čia ρ – atvykstančių užklausų greičio ir vidutinio vienos užklausos laikymo atminties buferyje sandauga.

Atminties išnaudojimo DDoS atakos sėkmės tikimybė taip pat priklauso nuo sistemą pasiekiančių užklausų filtravimo savybių (4).

$$P_M = P_{fpr} + P_{im} \cdot (1 - P_{fpr}) \tag{4}$$

čia P_{fpr} – tikimybė, kad teisėto vartotojo užklausa bus įvardinta kaip atakos srautas.

Centrinio procesoriaus darbo išnaudojimo DDoS atakos modelis

Centrinio procesoriaus darbo išnaudojimo DDoS atakos modelyje naudojama atviroji vienkanalė masinio aptarnavimo sistema (M/M/1), nes centriniame procesoriuje vienu laiko momentu gali būti vykdomas tik vienas uždavinys. Kadangi užklausos centriniame procesoriuje nėra blokuojamos dėl trūkstamos vietos, tai pagrindinė šio modelio charakteristika yra vienos užklausos vidutinis vykdymo laikas L (5), tačiau ji gali būti taikoma tik kuomet tenkinama (6) lygybė. Kitu atveju atvykstančių užduočių skaičius būtų didesnis, nei sistema gali aptarnauti.

$$L = \frac{1}{\mu_{cc} \cdot S - \lambda_{gc}} \tag{5}$$

$$\frac{\lambda_{gc}}{\mu_{cc} \cdot S} < 1 \tag{6}$$

čia λ_{gc} – vidutinis atvykstančių užklausų greitis; μ_{cc} – vidutinis vienos užklausos vykdymo greitis; S – užklausas aptarnaujančių procesorių skaičius sistemoje.

Centrinio procesoriaus darbo išnaudojimo DDoS atakos sėkmės tikimybei įvertinti naudojamas ribinis laukimo laikas t_w, kuris nusako kiek laiko vartotojas yra pasiryžęs laukti užklausos aptarnavimo. Todėl, apibendrinant visus galimus atvejus, centrinio procesoriaus darbo išnaudojimo DDoS atakos sėkmės tikimybė P_C gali būti apskaičiuojama pagal (7) formulę.

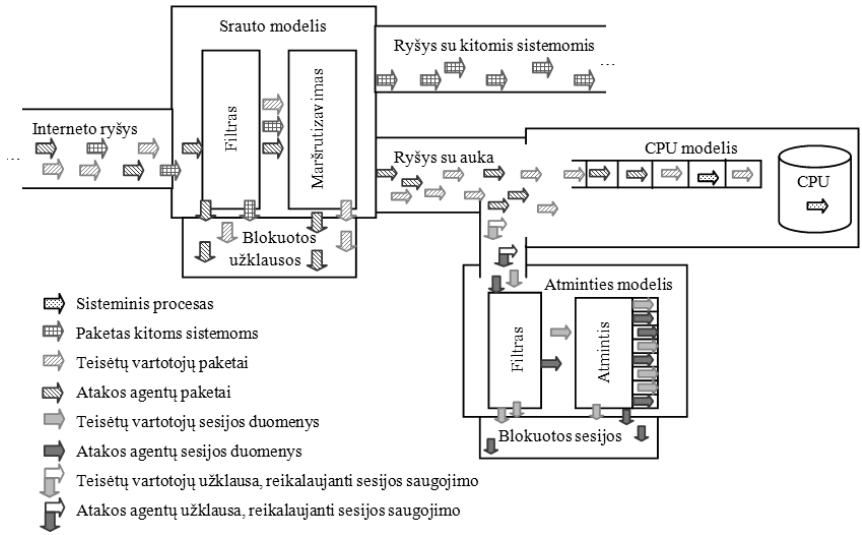
$$P_C = \begin{cases} 1, & \frac{\lambda_{gc}}{\mu_{cc} \cdot S} \geq 1 \quad arba \quad L \geq t_w \\ \frac{L}{t_w}, & \frac{\lambda_{gc}}{\mu_{cc} \cdot S} < 1 \quad ir \quad L < t_w \end{cases} \tag{7}$$

Šis modelis nėra visiškai universalus, nes skirtas neprioritetinių užklausų aptarnavimui ir neįvertina laiko, reikalingo užduočių vykdymo eigos planavimui.

Jungtinis DDoS atakos modelis

Jungtinis DDoS atakų modelis suprantamas kaip srauto, atminties ir procesoriaus darbo sistemų visuma, t.y. jame yra trys skirtingo tipo DDoS atakų modeliai. Todėl sistemoje, kurioje gali būti naudojami visi trys resursų tipai, galima visų trijų DDoS atakų tipų grėsmė (5 pav.). Bendra DDoS atakos sėkmės tikimybė turėtų būti vertinama kaip tikimybė, kad bent vieno iš sistemoje naudojamų resursų išnaudojimo tikimybė bus pakankamai didelė (8).

$$P = 1 - \overline{P_B} \cdot \overline{P_M} \cdot \overline{P_C} \tag{8}$$



5 pav. Jungtinės DDoS atakos konceptualusis modelis

Ši formulė nusako tikimybę, kad teisėto vartotojo užklausa bus prarandama bent vienoje iš sistemos dalių, todėl gali būti lengvai papildoma naujo tipo resursų išnaudojimo modeliais ar pritaikoma naudoti tik reikiamiems DDoS atakų tipams atspindėti.

4. Pasiūlytų klasifikatorių ir modelių tinkamumo vertinimo rezultatai

DoS atakų ir jų kontrpriemonių klasifikacijų savybių palyginimas

Ketvirtajame skyriuje eksperimentiškai lyginamos analizuotų DoS, DDoS atakų ir jų kontrpriemonių taksonomijų savybės. Kiekvienai taksonomijai skaičiuojamas unikalių kategorijų, nedalomų kategorijų ir kriterijų kiekiai bei įvertinamas vidutinis taksonomijos kategorijos detalumo lygis (iš kiek subkategorijų sudaryta kategorija). Jų metu gauta, kad siūlomos naujos taksonomijos yra vidutinio detalumo. Detaliausios ir turinčios daugiausiai kategorijų yra pasiūlytos J. Mirkovich,

Taip pat aprašyti analizuotų taksonomijų taikymo eksperimentų rezultatai. Vieno jų metu respondentai turėjo nusakyti Nuke, SQL wildcard ir internetinio kirmino savybes visose analizuotose DoS, DDoS klasifikacijose. Antrojo tyrimo metu kiekvienai iš šių atakų DoS, DDoS atakų kontrpriemonių taksonomijose nurodytos galimos naudoti priemones.

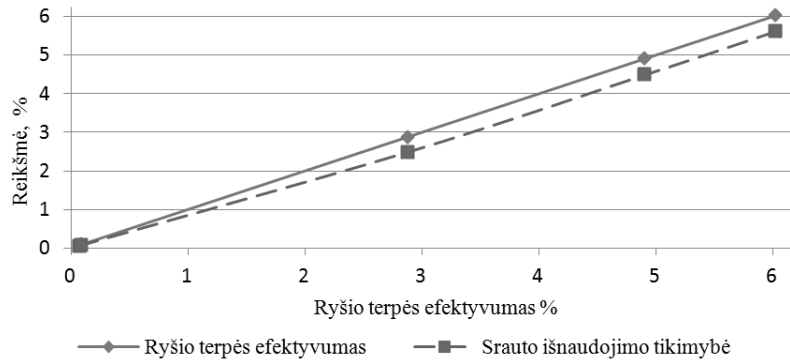
Praktiniai taksonomijų taikymo eksperimentai atskleidė, kad naujai pasiūlytos taksonomijos leidžia detaliau nusakyti šiuo metu vykstančias DoS atakas ar siūlomas prieš jas taikyti kontrpriemones (Nuke atakai nusakyti J. Mirkovich taksonomijoje buvo pažymėta daugiau kategorijų, o SQL wildcard ir internetinio kirmino atvejais daugiausiai kategorijų buvo pažymėta naujai pasiūlytoje DoS atakų taksonomijoje. Galimų naudoti kontrpriemonių nurodymui, visoms trims stebėtoms atakoms daugiausiai kontrpriemonių savybių buvo nurodyta pasiūlytoje DoS atakų kontrpriemonių taksonomijoje).

DDoS atakų modelių tinkamumo vertinimo eksperimentai

Pasiūlytų DDoS modelių tinkamumo vertinimui pasirinktas OPNET modeliavimo įrankis. Šiuo modeliavimo įrankiu sukurtų modelių rezultatai lyginami su darbe pasiūlytų srauto, atminties ir procesoriaus darbo išnaudojimo DDoS modelių rezultatais.

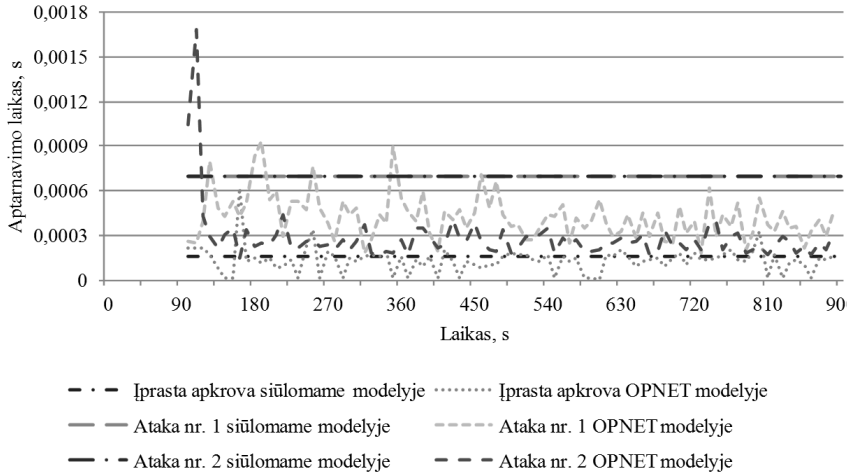
Srauto ir centrinio procesoriaus darbo išnaudojimo DDoS atakų modelių tinkamumui įvertinti išbandyta po 3 situacijas – normalus sistemos darbas ir dvi situacijos su skirtingais parametrais. Atminties išnaudojimo DDoS atakos modelio rezultatų palyginimui naudojamos keturios skirtingos situacijos.

Eksperimentų metu paaiškėjo, kad srauto išnaudojimo DDoS atakos sėkmės tikimybė yra panaši į ryšio terpės efektyvumą (6 pav.) – ji vidutiniškai 0,25 procento mažesnė nei ryšio terpės efektyvumas.



6 pav. Srauto išnaudojimo DDoS atakos sėkmės tikimybės ir srauto išnaudojimo palyginimas

Palyginus OPNET modeliavimo įrankiu gautus užklausų aptarnavimo laikus ir centrinio procesoriaus darbo išnaudojimo modeliu gautą vidutinį aptarnavimo laiką, šios reikšmės vidutiniškai skiriasi 0,238 milisekundės (7 pav.).



7 pav. Centrinio procesoriasu darbo DDoS atakos vidutinis užklausos aptarnavimo laiko ir OPNET modeliavimo įrankių gauto vidutinio užklausų aptarnavimo laiko palyginimas

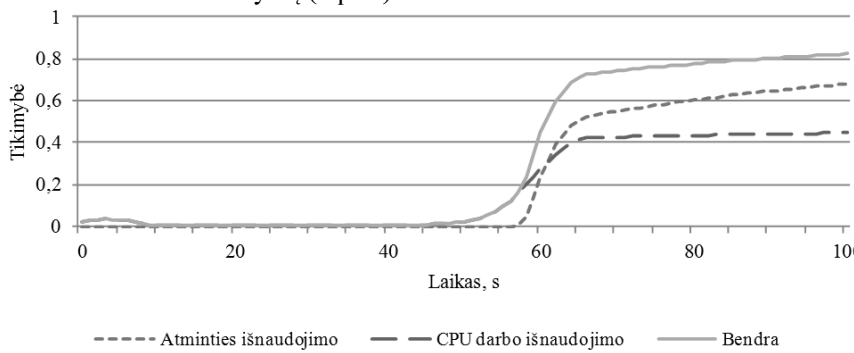
Atminties išnaudojimo DDoS atakos modelio rezultatų palyginti su OPNET modeliavimo įrankio rezultatais tiesiogiai nepavyko, nes pasirinktas modeliavimo įrankis nepateikia visos tam būtinos informacijos (papildomo atminties buferio išnaudojimo). Atminties išnaudojimo modelis buvo palygintas su teorine lyginimo reikšme, siekiant nustatyti atminties išnaudojimo DDoS atakos sėkmės tikimybės kaitos charakteristikas.

5. Jungtinio DDoS atakų modelio taikymas

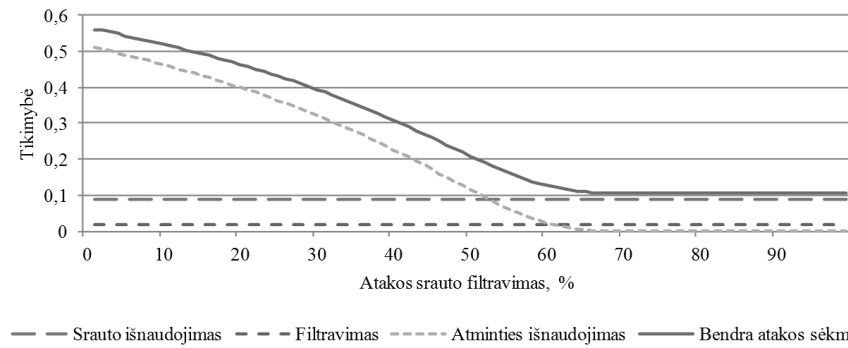
Penktame skyriuje aprašomi atlikti eksperimentai su pasiūlytais modeliais. Jų metu išbandytas atminties ir procesoriaus darbo jungtinis modelis, kuris atskleidė, kad tiesiškai didėjant atvykstančių užklausų kiekiui sistemoje, bendra atakos ir jos dedamųjų įtaka nėra tiesinė (8 pav.). Analizuotoje situacijoje atakos metu didėjant sistemą pasiekiančių užklausų kiekiui, centrinio procesoriaus darbo išnaudojimo tikimybė pradeda didėti greičiau, nei atminties išnaudojimo tikimybė. Tačiau pradėjus augti atminties išnaudojimo tikimybei, jos pokyčiai yra spartesni ir nuo 60 atakos sekundės ši tikimybė turi didesnę įtaką bendrai atakos sėkmės tikimybei, nei centrinio procesoriaus išnaudojimo sėkmės tikimybė.

Apjungus srauto ir atminties išnaudojimo DDoS atakų modelius, rezultatai patvirtino netiesinę atakos sėkmės tikimybę didėjant užklausų kiekiui. Taip pat

eksperimentais buvo tiriama atakos sėkmės tikimybės priklausomybė nuo sistemos filtravimo savybių (9 pav.).



8 pav. Jungtinio atminties ir centrinio procesoriaus darbo išnaudojimo DDoS atakos modelio sėkmės tikimybės kaita laiko bėgyje



9 pav. Jungtinio atminties ir srauto išnaudojimo DDoS atakos modelio sėkmės tikimybės priklausomybė nuo atakos srauto greičio

Gerinant atakos užklausų filtravimo rodiklį, atakos sėkmės tikimybė sparčiai mažėja, nes į atminties modulį nebepatenka netinkamos užklausos. Kadangi filtravimo sistema buvo įdiegta pačioje sistemoje, srautą išnaudojančios užklausos nėra filtruojamos ir srauto išnaudojimo sėkmės tikimybė nepriklauso nuo filtravimo savybių.

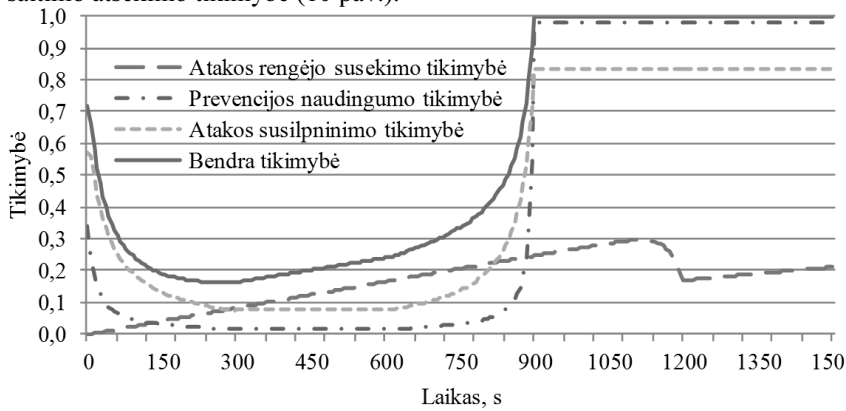
Šiame skyriuje aprašytas dar vienas pasiūlyto modelio atvejis, kuomet išplečiamos pasiūlyto modelio ribos ir įtraukiamos trys dedamosios: atakos prevencija, atakos sušvelninimo ir atakos atsekimo dedamosios. Šis modelis naudojamas atakos atlaikymo tikimybei nustatyti ir ištirti kaip ji priklauso nuo naudojamų agentų skaičiaus atakoje strategijos.

Eksperimento metu buvo tiriamos keturios agentų papildymo strategijos (nenaudojami papildomi agentai, ataka papildoma pastoviu agentų kiekiu, ataka papildoma vis didėjančiu ir vis mažėjančiu agentų skaičiumi). Paaiškėjo, kad jų efektyvumas skiriasi priklausomai nuo vertinamo laikotarpio (1 lentelė).

1 lentelė. DDoS efektyvumo palyginimas skirtingais atakos momentais ir naudojant skirtingas agentų papildymo strategijas

Agentų papildymo strategija	Atakos sėkmės tikimybė, %			
	Atakos vidurys	Agentų papildymo pabaiga	Atakos srauto generavimo pabaiga	Pasibaigus atakai
Nepildoma	91,2	45,7	30,6	18,5
Pastovus kiekis	75,2	77,5	72,0	43,3
Didėjantis kiekis	54,7	67,0	67,0	40,3
Mažėjantis kiekis	80,2	79,9	70,2	42,2

Šie eksperimentai taip pat parodė kaip atakos metu kinta DDoS atakos šaltinio atsekimo tikimybė (10 pav.).



10 pav. DDoS atakos atlaikymo tikimybės kaita laike, kuomet naudojamas pastovus agentų papildymas

Atakos metu didėjant atakuojančių agentų kiekiui, atakos rengėjo atsekimo tikimybė tiesiškai didėja. Pasibaigus atakai ir atakoje dalyvavusiems agentams dingus dėl trumpo gyvavimo laiko, jų atsekimo tikimybė krenta ir toliau vykstantis jos kitimas nėra toks augantis, kaip prieš tai.

Atakos šaltinio atsekimo tikimybė taip pat priklauso nuo atakoje esančių agentų skaičiaus ir jų valdymo būdo. Todėl, siekiant kuo mažesnės susekimo tikimybės, atakuojantysis turėtų rinktis didelius Botnet tinklus, kuriuose

kiekvieno agento vidutinis gyvavimo laikas yra pakankamai trumpas, o jų valdymo schema yra netiesioginė ir reikalaujanti daug laiko susekimui.

Bendrosios išvados

1. J.Mirkovich pasiūlyta DoS atakų taksonomija turi beveik 2 kartus daugiau kategorijų ir pasižymi didesniu kategorijų detalumu nei siūloma nauja DoS atakų taksonomija. Tačiau, atlikus praktinius analizuotų DoS taksonomijų panaudojimo eksperimentus šiuo metu vykstančių atakų aprašymui, pastebėta, kad pasiūlytoje taksonomijoje respondentai pažymėjo vidutiniškai 8,6% daugiau DoS atakos savybių, nei J.Mirkovich pasiūlytoje taksonomijoje. Tai parodo, kad taksonomijos aiškumas ir panaudojimo patogumas labiau priklauso nuo savybių išdėstymo ir aprašymo, nei nuo jų kiekio taksonomijoje.
2. Išanalizavus egzistuojančius DoS ir DDoS atakų modelius pastebėta, kad daugiau nei 65% modelių taiko tikimybines išraiškas atakos savybėms nusakyti (iš nagrinėtų 21 modelio, 7 modeliai nenaudojo stochastinių elementų, bet jie visi buvo publikuoti anksčiau nei 2007 metais). Tai parodo, kad agentų modeliai dėl pernelyg didelių atakos elementų kiekio DDoS atakose tampa nebeefektyvūs, o stochastiniai elementai leidžia modelį padaryti paprasčiau realizuojamą ir atspindėti atakai būdingas savybes.
3. Jungtinis DDoS atakų modelis įvertina sėkmės tikimybę, kad teisėto vartotojo užklausa bus prarandama bent vienoje iš modelį sudarančių dedamųjų. Tai leidžia padidinti jungtinio DDoS atakos modelio lankstumą ir plečiamumą, todėl jį nesunku pritaikyti naujo tipo DDoS atakų modeliavimui.
4. Sukurtų modelių tinkamumo įvertinimui darbe taikomas OPNET modeliavimo įrankis, nes šiuo metu nėra patikimų ir išsamių DDoS atakų duomenų šaltinių, o, atlikus eksperimentą vietiniame tinkle, neatsispindėtų visos DDoS srauto savybės. Atliktas tyrimas atskleidė modelių rezultatų panašumus. Sukurtas modelis negali būti laikomas tiksliu vertinant realias situacijas, nes jo nebuvo galima palyginti su realia atakos sėkmės tikimybe. Tačiau tai leidžia nustatyti DDoS atakos sėkmės tikimybės priklausomybę nuo atakos ir aukos savybių.
5. Skaitinių eksperimentų metu nustatyta, kad bendros atakos sėkmės tikimybės lemiama (turinti didžiausią įtaką) dedamoji priklauso nuo daugiau nei 5 atakų ir aukos savybių. Todėl, norint panaudoti sukurtą jungtinį DDoS modelį objektyviam prieglobos paslaugų vertinimui, turėtų būti naudojamos bent kelios skirtingos modeliuojamos situacijos.

Autoriaus publikacijų disertacijos tema sąrašas
Recenzuojamuose periodiniuose mokslo žurnaluose

Ramanauskaitė, S.; Čenys, A. 2009. DoS atakų modeliavimas stochastiniais metodais. Jaunųjų mokslininkų darbai 3 (24):. 97–101. ISSN 1648-8776.

Ramanauskaitė, S. 2010. Modeling of SYN Flooding Attacks. Jaunųjų mokslininkų darbai 1 (26): 331–335. ISSN 1648-8776.

Ramanauskaitė, S.; Juknius, J. 2010. BOTNET agentų naudojimo DDoS atakose strategijų modeliavimas. Jaunųjų mokslininkų darbai 3 (28): 114–119. ISSN 1648-8776.

Ramanauskaitė, S.; Čenys, A. 2011. Stochastinis TCP SYN atakų modelis. Science – Future of Lithuania 3 (1): 20–24. ISSN 2029-2341/ISSN 2029-2252.

Ramanauskaitė, S.; Čenys, A. 2011. Taxonomy of DoS Attacks and Their Countermeasures. Central European Journal of Computer Science 1 (3): 355–366. ISSN: 1896-1532/ ISSN: 2081-9935.

Ramanauskaitė, S.; Čenys, A. 2012. Composite DoS Attack Model. Science – Future of Lithuania 4 (1): 20–26. ISSN 2029-2341/ISSN 2029-2252.

Kituose leidiniuose

Ramanauskaitė, S.; Čenys, A. 2011. Modelling of Central Processing Unit Work Denial of Service Attacks, in *Proc. of the 17th International Conference on Information and Software Technologies*, Kaunas, 99–104. ISSN 2029-0063/ISSN 2029-0020.

Trumpos žinios apie autorių

Simona Ramanauskaitė gimė 1983 m. gruodžio 18 d. Šiauliuose. 2006 m. ji įgijo informatikos inžinerijos bakalauro laipsnį Šiaulių universiteto Technologijos fakultete. 2006 metų rugsėjį Simona Ramanauskaitė pradėjo dirbti Šiaulių universiteto Informacinių technologijų katedroje asistente. 2008 m. įgijo informatikos magistro laipsnį Šiaulių universiteto Matematikos ir informatikos fakultete. 2008–2012 m. – Vilniaus Gedimino technikos universiteto doktorantė. Šiuo metu dirba lektore Šiaulių universitete Informacinių technologijų katedroje.

MODELLING AND RESEARCH OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

Topicality of the problem. A saying “If You are not in online, You are not at all” becomes very popular in society and business field. Computer networks allow proliferation of information, as well as using and providing different

services for other computer systems. Such distributed systems or services supply fast and convenient way to access information, remotely manage processes or objects. Therefore business marketing becomes more oriented to internet users and services.

The other tendency can also be noticed. The main goal of hackers is not just recognition, cyber attacks become a way of making money. One of ways to make money from cyber attack is DDoS attack. During it a certain service is made unavailable for its legitimate users. Promising to cancel (sometimes even not starting at all) the attack, a hacker requires certain amount of money from the victim or competitors of a certain internet service, and it agrees to pay money for elimination of the competitor for a certain time of moment. There are many ways to make money from the cyber attack. However, accessibility can be one of the most expensive properties to ensure.

The other accessibility assurance problem is the opportunity to execute DDoS attacks easily. It is so because of variety of DDoS attack tools, Botnet existence and borrowing opportunity etc. The DDoS attack nature and popularity of its execution tools allows execution of such a type of cyber attacks even by amateurs. This is why system administrators should prepare carefully to ensure the systems accessibility on different levels.

However there are no unified measures to show systems resistance to DDoS attack. System administrators should rely on its experience and own knowledge to decide the effectiveness of different countermeasures and DDoS attack sizes. When client wants to check what the service accessibility rate is, the client must rely on service provider's opinion which sometimes can be subjective and not reliable.

Having model for network system DDoS attack success measurement there would be possible to estimate potential threads, looses, countermeasure effectiveness. It would allow modelling different situations before the attack appears and optimize the systems accessibility.

The object of research. Object of this dissertation is estimation of the probability of denial of service attack success.

Main objective and tasks of the work. The main objective is creation of the model for composite DDoS attack success estimation.. In order to achieve the objective, it is necessary to deal with the following issues:

1. To analyze existing DoS attacks and their countermeasure taxonomies.
2. To analyze existing DoS and DDoS attack models.
3. To derive models for different type DDoS attacks.

4. To combine the created models in order to represent composite DDoS attack success probability.
5. To validate the proposed model.
6. To develop the prototype and perform experiments on several DDoS attacks.

Research methodology. In order to achieve the objective, the following research methods were used:

1. Comparative research and literature research for DoS attacks and their countermeasure properties, taxonomies, model types, comparison of existing models and judgement;
2. The analysis results were summarized and the approach was expounded using the research generalization and logical induction methods.
3. Mathematical modelling methods were used for DDoS attack property estimation.
4. Proposed DDoS attack models relay on queuing theory and probability theory was used to derive the composite DDoS attack probability too.

Importance of scientific novelty. In preparation of this thesis these aspects of scientific novelty appeared:

1. New DoS attack and their countermeasure taxonomies where proposed;
2. Central processing unit (CPU) performance depletion model was proposed;
3. Composite DDoS attack model was proposed to estimate different type DDoS attack success probability and/or victim capacity to resist a certain size of DDoS attack.

Practical significance of achieved results. Network system accessibility assessment is usually based on the expert opinion. There is no complete methodology to estimate the resistance to different type of DoS attacks. In this work, new DoS attack and their countermeasure taxonomies are presented for classifying the new type of DoS attacks or their countermeasure.

Proposed composite DDoS model can be used to analyse and predict DDoS attack success probability for different attack and victim properties. It can be as well used to find the optimal system configuration to ensure its accessibility. In case of wide acceptance of this model defined additional certification procedures the proposed model could serve as a tool for unified service accessibility rate estimation.

The research presented in the thesis leads to some practical recommendations. It describes which DDoS attack properties can pose the biggest threat, and which Botnet agent allocation strategies can cause the biggest effectiveness in different attack stages, etc.

The defended statements. The following statements based on the results of present investigation may serve as the official hypotheses to be defended:

1. Probabilistic modelling of DDoS attacks belonging to different types gives the basis to create the consolidated DDoS attack model generalizing the probability of the success attack.
2. Incorrect system configuration or unpredicted system usage by legitimate users of the system can result as DoS attack. Therefore DDoS attack success probability can be used creating prevention measures to improve internet service availability, despite the probability of real DDoS attack threat.
3. Multiple types of resources are exhausted during DDoS attack. Therefore, to achieve more precise DDoS attack probability, composite DDoS attack model should be used.
4. Composite DDoS attack success probability does not depend linearly on attack parameters and cannot be modelled by linear equations.

The scope of the scientific work. The dissertation is composed of Introduction, five main chapters and general conclusions. The total dissertation scope is 109 pages, 42 equations, 55 pictures and 8 tables.

Chapter 1 – revision of DoS attacks, analysis of existing DoS attack and their countermeasure taxonomies. In this chapter, review of the specificities of the computer network modelling and analysis of the existing DoS and DDoS attack models is made as well.

Chapter 2 – introduction and description of the new taxonomies for DoS attack and their countermeasure.

Chapter 3 – description of proposed models for different types of DDoS attacks as well as composite DDoS attack model.

Chapter 4 and 5 – investigation of the results of proposed models. They are compared to OPNET modelling tool results, and different situations are also analysed to represent DDoS attack characteristics.

General conclusions

1. DoS attack taxonomy proposed by J. Mirkovich encompasses the biggest number of categories and the number of its taxonomy has the highest category minuteness level. However, our DoS attack taxonomy usage

experiments demonstrated that proposed taxonomy is more suitable for ongoing DoS attacks. On average 8.6% more categories were marked in our taxonomy than the in taxonomy proposed by J. Mirkovich. Our results confirm that the most important DoS attack taxonomy characteristics are its structure and clearness, and not the number of properties.

2. Analysis of existing DoS and DDoS attacks taxonomies demonstrated tendency to use stochastic elements for representation of the internet traffic randomness. From 21 analysed models only seven did not use probabilistic expressions, all introduced before 2007. This allows to suggest that agent models are not able accurately represent huge amount of DDoS attack data and stochastic models should be used instead.

3. Composite DDoS attack success probability represents a probability that legitimate user request will be lost at least in one of model components (will be blocked in bandwidth, memory or CPU work exhaustion models). It inflicts model flexibility and extensibility. Therefore it can be adopted to represent new type of DDoS attacks as well.

4. There are no reliable and detailed historical data of DDoS attacks while experiments in LAN cannot represent all characteristics of DDoS attack. Therefore we use OPNET modelling tool to validate our proposed DDoS attack models. Validation results proved that there exist model data similarities to OPNET modelling results. Therefore DDoS attack models that we propose can be used for estimation of theoretical attack success probability. However proposed models do not guarantee the precision of real DDoS attacks success probability.

5. Numerous experiments with composite DDoS attack model showed that the main component of composite DDoS attack success probability can vary depending on more than 5 parameters. Therefore using the composite DDoS attack model for hosting ranking purposes at least in a few standard situations should be analysed.

About the author

Simona Ramanauskaitė was born in Šiauliai, on 18 of December 1983.

First degree in Informatics Engineering, from Faculty of Technology, Šiauliai University (ŠU), 2006. Master of Science in Informatics, from Faculty of Informatics and Mathematics, ŠU, 2008. In 2008–2012 – PhD student of Vilnius Gediminas Technical University (VGTU). At present – lecturer at Department of Information Technology of ŠU.

Simona RAMANAUSKAITĖ

SRAUTINIŲ ATAKŲ ĮTAKOS INTERNĖTINĖS PASLAUGOS SUTRIKDYMUI MODELIAVIMAS IR TYRIMAS

Daktaro disertacijos santrauka
Technologijos mokslai, informatikos inžinerija (07T)

Simona RAMANAUSKAITĖ

MODELLING AND RESEARCH OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

Summary of Doctoral Dissertation
Technological Sciences, Informatics Engineering (07T)

2012 04 23. 1,5 sp. l. Tiražas 70 egz.
Vilniaus Gedimino technikos universiteto
leidykla „Technika“,
Saulėtekio al. 11, 10223 Vilnius,
http://leidykla.vgtu.lt
Spausdino UAB „Ciklonas“
J. Jasinskio g. 15, 01111 Vilnius