DOS ATAKŲ MODELIAVIMAS STOCHASTINIAIS METODAIS

Simona Ramanauskaitė, Antanas Čenys
Šiaulių universitetas,
Vilniaus Gedimino technikos universitetas

Įvadas

Atkirtimo nuo paslaugos ataka – tai ataka, kurios pagrindinis tikslas yra „paveikti kompiuterinę sistemą arba tinklą taip, kad kompiuterinės paslaugos taptų neprieinamos vartotojams“ [5].

Kuomet atkirtimo nuo paslaugos ataka atliekama pasinaudojant Botnet tinklu, ji tampa paskirstyta (*angl.* Distributed Denial of Service, toliau tiesiog DoS), t. y. numatyta auka vieningai atakuojama daugybės tam darbui sutelktų, bet jiems patiems nežinomų užkrėstų ir valdomų kompiuterių. Visuomenėje labiausiai iki šiol nušviestas tokių atakų pavyzdys yra 2009 metų liepos 4–10 dienomis vykusios DoS atakos prieš JAV ir Pietų Korėjos žiniatinklius [8], tačiau vien 2008 metais įvairaus masto DoS atakų būta apie 193000 [7], nors jos ir nesusilaukė tokio visuomenės atgarsio.

Potenciali DoS atakų galia ir sukelta žala gali būti itin didelė, tačiau sudėtinga ją realiai įvertinti ir jai pasiruošti, todėl tam vartojami įvairūs modeliai ar simuliacijos, leidžiančios bent apytikriai prognozuoti ar įvertinti tam tikras galimos atakos savybes.

Darbo tikslas – sudaryti stochastinius srauto išnaudojimo DoS atakų statinį ir dinaminį modelius.

Tyrimo metodai: mokslinės ir techninės literatūros analizė, modeliavimas, eksperimentas.

Egzistuojantys stochastiniai DoS atakų modeliai

Yra nemažai pavyzdžių, kur stochastiniai modeliai padeda įvertinti gana sudėtingų objektų veikimo savybes ar nuspėti jų elgseną konkrečiais atvejais. Jie taikomi ir kompiuterių tinklų saugumui, pvz., DoS atakai modeliuoti.

1 lentelė. ***Egzistuojančių stochastinių DoS atakų modelių palyginimas***

Nr.	Autoriai	Modelio situacija	Naudojama sistema	Privalumai	Trūkumai
1.	D. Boteanu, J. M. Fernandez, J. McHugh, J. Mullins. [1]	SYN užtvindymo DoS atakos	Markovo grandinės	Rezultatai vertinami tik pagal teisėtų vartotojų paketų praradimą	Neįvertinamos galimos kontrpriemonės
2.	Y. Wang, C. Lin, Q.-L. Li, Y. Fang. [9]	SYN užtvindymo DoS atakos	Dvimatės Markovo grandinės	Aiškiai atskirti teisėtų vartotojų ir atakos sugeneruoti srautai	Neįvertinamos galimos kontrpriemonės
3.	Q. Huang, H. Kobayashi, B. Liu. [3]	SYN užtvindymo DoS atakos	Erlag ir Engset mišrus praradimo modelis	Aiškiai išreikšta paketų praradimo tikimybės formulė	Naudojama neribota laukimo eilė. Neįvertinamos galimos kontrpriemonės
		Srauto išnaudojimo DoS atakos	Markovo moduliuoto greičio procesai	Aiškiai išreikšta minimali agentų skaičiaus sėkmingai atakai radimo formulė	Nenustatoma konkreti sėkmės tikimybė Neįvertinamos galimos kontrpriemonės
4.	Q. Huang, H. Kobayashi, B. Liu. [4]	SYN užtvindymo DoS atakos bevieliuose tinkluose	Erlag ir Engset mišrus praradimo modelis	Aiškiai išreikšta paketų praradimo tikimybės formulė	Naudojama neribota laukimo eilė Neįvertinamos galimos kontrpriemonės
		Srauto išnaudojimo DoS atakos bevieliuose tinkluose	Paslėpta Markovo grandinė	Aiškiai išreikšta minimali agentų skaičiaus sėkmingai atakai radimo formulė	Nenustatoma konkreti sėkmės tikimybė Neįvertinamos galimos kontrpriemonės

Apibendrinant 1 lentelę, galima teigti, kad minėtų autorių sukurti modeliai atspindi tik situacijas, kuomet nesiimama jokių (kad ir minimalių) kontrpriemonių prieš DoS atakas, ir labiau skirti resursų, o ne srauto išnaudojimo DoS atakoms modeliuoti.

Srauto išnaudojimo DoS atakos

C. Douligeris ir A. Mitrokotsa [2] srauto išnaudojimo atakas įvardija kaip užtvindymo duomenimis atakas (data flooding attacks) ir apibūdina kaip atakuojančiojo siunčiamą kiek įmanoma didesnį kiekį duomenų numatytai aukai, kad ši nebepajėgtų priimti visų duomenų, todėl dalis būtų blokuojama.

Jei būtų blokuojami tik atakos srauto paketai – DoS efektas būtų nejuntamas tikriesiems sistemos vartotojams, tačiau atakuojančiosios pusės siunčiami duomenys būna itin panašūs į realių vartotojų užklausas, todėl sunkiai atskiriami. Taigi, dėl per didelio bendro srauto, blokuojamos tiek teisėtų, tiek ir atakuojančių kompiuterių užklausos.

Siūlomas srauto išnaudojimo DoS atakų konceptualus modelis

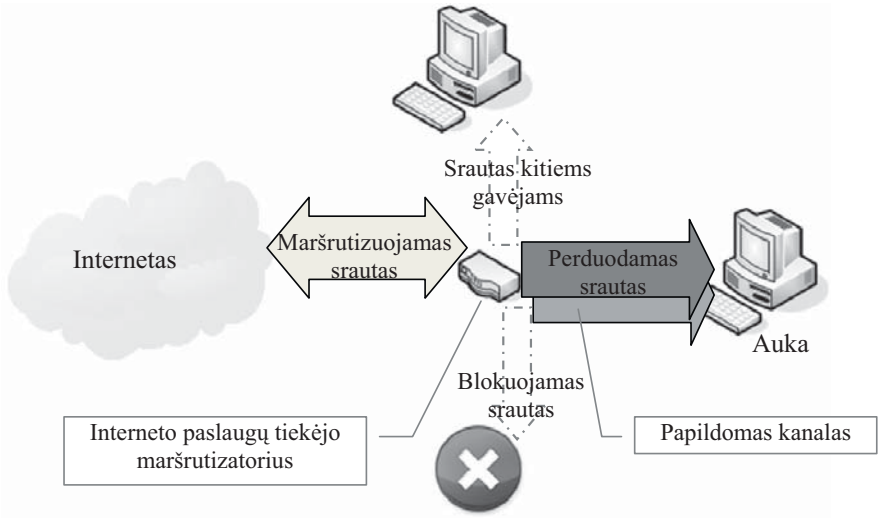
Visos auką pasiekiančios užklausos eina per jos interneto paslaugų tiekėjo maršrutizatorių, kuris yra pirmasis taškas, siejantis auką su internetu. Likęs kelias nuo šio maršrutizatoriaus iki atakos šaltinio mūsų nedomina.

Sakykime, kad interneto paslaugų tiekėjo maršrutizatorius yra pajėgus aptarnauti begalinį kiekį užklausų ir jas tinkamai maršrutizuoti. Be to, linija, jungianti šį maršrutizatorių su auka, yra riboto pralaidumo, o sujungimai su kitais tinklais – neriboto pralaidumo.

Interneto paslaugų tiekėjo maršrutizatorius aukai skirtą srautą perduoda jo linija kiek tai yra įmanoma, o jei ši linija yra perpildoma – „netilpusių“ paketų nekaupia, o tiesiog numeta, blokuoja ir jie aukos nebepasiekia.

Kaip kontrpriemone prieš DoS ataką, auka gali naudoti papildomus kanalus. Sakykime, kad interneto paslaugų tiekėją ir auką jungia kelios ryšio linijos, nors realiai yra dubliuojama visa aukos sistema.

Kreipiamas dėmesys tik į aukos turimą gauti srautą, jos pačios siunčiami duomenys šiame modelyje (1 pav.) neaktualūs.



1 pav. Srauto išnaudojimo DoS atakos formalaus modelio iliustracija

Pristatytasis modelis atspindi pagrindinius šio tipo atakos principus: per daug nesigilinama, kokiu būdu atliekamas maršrutizavimas, kokiu būdu rengiama ir vykdoma pati DoS ataka ir pan. Tai leidžia aiškiau suvokti srauto išnaudojimo DoS atakos pagrindinius elementus ir esmę.

Siūlomas formalus srauto išnaudojimo DoS atakų modelis

M. Zukerman teigimu [10], interneto srautams modeliuoti, kuomet juose vaizduojamas ganėtinai trumpas laiko tarpas ir didelė paketų gausa, labiausiai tinkamas yra Puasono, arba eksponentinis, paketų pasiskirstymas.

Tai įvertindami, srauto išnaudojimo DoS atakos formaliam modeliui sudaryti siūlome M/G/k/k aptarnavimo sistemų atvejį. Jame aukos turimas gauti srautas atitinka Pareto pasiskirstymą su parametru λ, aptarnavimo greitis pasiskirstęs visiškai atsitiktinai, su parametru μ (vidutiniu aptarnavimo vidutiniu užklausų atvykimo), sistemoje yra k kanalų ir joje vienu metu gali būti tik tiek užklausų, kiek tuo metu aptarnaujama, t. y. nėra laukimo eilės.

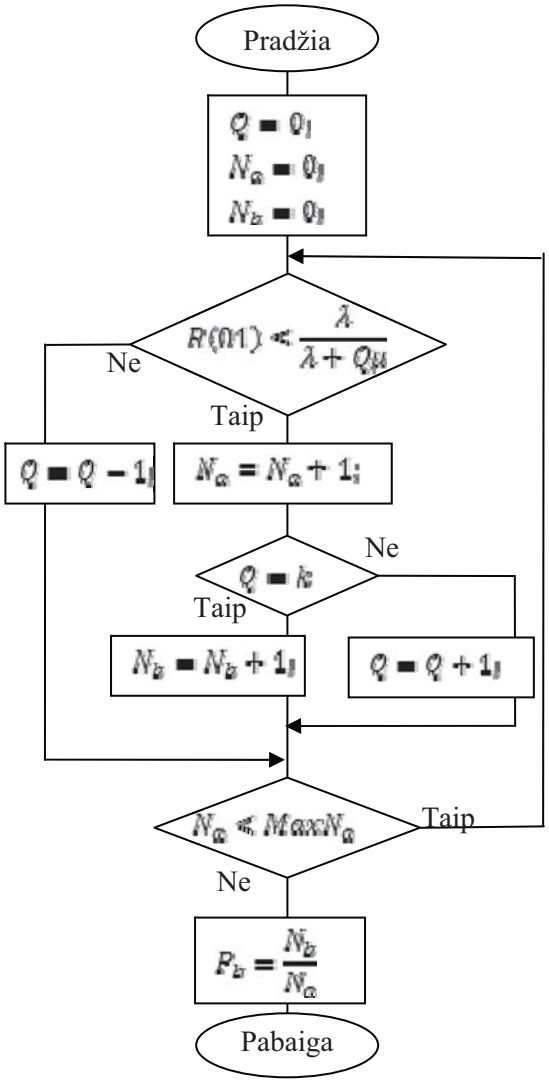
Kadangi DoS sėkmės tikimybė labai glaudžiai susijusi su blokuojamų paketų dalimi, tuo remdamiesi siūlome formalų srauto išnaudojimo DoS atakų modelį šios tipo atakos sėkmės tikimybei vertinti.

Simuliavimo algoritmas

Šis modelis (2 pav.) padeda nustatyti, kokia procentinė viso srauto dalis blokuojama ir nepasiekia aukos, kad ji galėtų atsakyti reikalaujamais duome-

nimis. Norint nustatyti srautą išnaudojančios DoS atakos sėkmės tikimybę, vartotojas turi pasirinkti, kuri teisėtų užklausų praradimo procentinė dalis jam jau nebepriimtina.

Atitinkamai įvedus paketų blokavimo ribą r (reikšmė nuo 0 iki 1), šio tipo atakos sėkmės tikimybė būtų išreiškiama formule $P_a = \frac{P_b}{r}$.



2 pav. Srauto išnaudojimo DoS atakos formalus modelis

Žymėjimai:

Q – šiuo metu sistemoje jau aptarnaujamų (siunčiamų) paketų skaičius; N_a – iš viso maršrutizatorių pasiekęs aukai skirtas paketų skaičius; N_b – blokuotų paketų skaičius; $MaxN_a$ – stebimas paketų skaičius (skirta simuliacijos pabaigai nustatyti); k – atvirų kanalų skaičius (galima kontrpriemonė); D – vidutinis aukai siunčiamo paketo dydis, matuojamas baitais; T – aukos kanalo vidutinis pralaidumas, matuojamas bitais per sekundę; μ – vidutinis aptarnavimo greitis paketais per sekundę ir randamas pagal formulę $\mu = \frac{T}{D}$;

S_n – normalus (įprastai pasitaikantis) aukai tenkantis srautas, matuojamas baitais per sekundę;

S_z – vieno atakos kompiuterio (zombio, agento) sugeneruojamas vidutinis atakos srautas, matuojamas baitais per sekundę;

n – atakoje dalyvaujančių kompiuterių (zombių, agentų) skaičius;

S_a – visas atakos generuojamas srautas aukai, matuojamas baitais per sekundę ir apskaičiuojamas pagal formulę $S_a = S_z n$;

λ – vidutinis paketų atvykimo greitis, matuojamas paketais per sekundę ir paskaičiuojamas pagal formulę $\lambda = \frac{S_n + S_a}{D}$;

R(01) – atsitiktinių skaičių generatorius, generuojantis skaičius nuo 0 iki 1.

Šis modelis yra dinaminis ir kiekvieno paketo sistemoje reikalauja inicijuoti pasirodymą ir aptarnavimą (atsitiktinio skaičiaus generavimą), tačiau gali būti vartojamas kartu su kitais dinaminiais modeliais, platesnės ir detalesnės srities analizei.

Statinį šio stochastinio modelio analogą galima pateikti remiantis Sanjay Kumar Bose medžiaga [6], kurioje jis nusako M/G/k/k tipo aptarnavimo sistemos blokavimo tikimybės išraišką.

$$P_b = \frac{\frac{\rho^k}{k!}}{\sum_{j=0}^{k} \frac{\rho^j}{j!}}, \text{ kur } \rho = \frac{\lambda}{\mu}. \quad (2)$$

Remiantis ja, mūsų aprašomą srauto išnaudojimo DoS atakos sėkmės tikimybę galima išreikšti taip:

$$P_a = \frac{\frac{\rho^k}{k!}}{r\sum_{j=0}^{k} \frac{\rho^j}{j!}}, \text{ kur } \rho = \frac{S_z n + S_a}{T}. \quad (3)$$

Modeliavimo rezultatai ir jų analizė

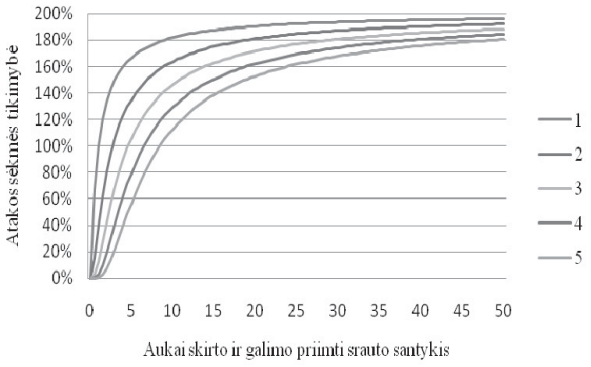
Remiantis siūlomais dinaminiu ir statiniu srauto išnaudojimo DoS atakų modeliais, realizuota programinė įranga. Ji leidžia vartotojui dinaminiu ir statiniu būdais modeliuoti pageidaujamas situacijas ir stebėti paketų blokavimo ir / arba atakos sėkmės tikimybės priklausomybes nuo įvairių tam įtaką darančių faktorių.

Dinaminis ir statinis modeliai skiriasi tik savo veikimo principu, o rezultatai tapatūs: dinaminio modelio rezultatai nuo statinio skiriasi ~1% esant 1000 ir daugiau stebimų paketų.

Atliekant įvairius srauto išnaudojimo DoS atakų modeliavimus, nustatyta, kad:

- paketų skaičius turi įtakos tik rezultatų tikslumui, todėl modeliavimui patariama nenaudoti mažiau nei 1000 paketų, kad nenukentėtų rezultatų tikslumas;

- paketų blokavimo ir atakos sėkmės tikimybės labiausiai priklauso nuo aukai siunčiamo ir galimo priimti duomenų srauto santykio bei kanalų skaičiaus;
- papildomų kanalų atvėrimas labiausiai jaučiamas esant nedideliam siunčiamo ir galimo priimti srauto santykiui; šiam santykiui smarkiai išaugus nebėra toks veiksmingas (3 pav.).



3 pav. Atakos sėkmės priklausomybė nuo siunčiamo ir galimo priimti srauto santykio, esant skirtingam kiekiui atvirų kanalų (blokuojamų paketų riba DoS atakai nustatyti lygi 50%)

Išvados

1. Šiuo metu egzistuojantys stochastiniai DoS atakų modeliai labiau skirti resursų išnaudojimo atakoms modeliuoti; eliminuotos galimos kontrpriemonės.
2. Mūsų pasiūlytas stochastinis srauto išnaudojimo DoS atakų modelis turėtų leisti realiau įvertinti šio tipo atakos sėkmės tikimybę, atakai dar neįvykus; analizuoti šio tipo atakas, jų realiai nevykdant; sėkmingiau pasiruošti galimoms tokio tipo atakoms;
3. Aprašytųjų dinaminio ir statinio modelio variantų rezultatai praktiškai yra tapatūs, skirtingas tik veikimo principas. Tai leidžia šį modelį taikyti skirtingose aplinkose ir taip jį lengviau integruoti į kitus modelius.

Literatūra

1. Boteanu D., Fernandez J. M., McHugh J., Mullins J. Queue Management as a DoS counter-measure? Interaktyvus. Prieiga per internetą: <http://secsi.polymtl.ca/gondwana/papers/QueueManagementDoS-1.pdf>.
2. Douligeris C., Mitrokotsa A., 2004, DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks* 44 643-666. Interaktyvus. Prieiga per internetą: <http://ict.ewi.tudelft.nl/pub/amitrokotsa/comnet.pdf>.
3. Huang Q., Kobayashi H., Liu B. Analysis of a New Form of Distributed Denial of Service Attack. Conference on Information Science and Systems, The John Hopkins University, 2003. Interaktyvus. Prieiga per internetą: <http://www.princeton.edu/kobayashi/papers/Network%20Security%20Protocols/Analysis%20of%20a%20New%20Form%20of%20Distributed%20Denial%20of%20Service%20Attack.pdf>.
4. Huang Q., Kobayashi H., Liu B. Modeling of Distributed Denial of Service Attacks in Wireless Networks. IEEE 2003. Interaktyvus Prieiga per internetą <http://www.princeton.edu/kobayashi/papers/Network%20Security%20Protocols/Modeling%20of%20distributed%20denial%20of%20service%20attacks%20in%20wireless%20networks.pdf>.
5. LITNET CERT. Interaktyvus. Prieiga per internetą: <http://cert.litnet.lt/faq.html>.
6. M/G/m/m Loss System. Interaktyvus Prieiga per internetą: <http://www3.ntu.edu.sg/home/eskbose/qbook/MGmm_Queue.PDF>.
7. ShadowServer, DDoS Historical. Interaktyvus Prieiga per internetą <http://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSHistorical>.
8. ShadowServer, Korean/U.S. DDoS Attacks - Perplexing, Disruptive, and Destructive. Interaktyvus. Prieiga per internetą: <http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20090710>.
9. Wang Y., Lin C., Li Q.-L., Fang Y. A queueing anglysis for the denial of service (DoS) attacks in computer networks. *Computer Networks* 51 (2007) 3564-3573. Interaktyvus. Prieiga per internetą: <http://www.fang.ece.ufl.edu/mypaper/comnet07wang.pdf>.
10. Zukerman M., 2008, Introduction to Queueing Theory and Stochastic Teletraffic Models, 14, 156 psl.. Interaktyvus. Prieiga per internetą: <http://www.ee.cityu.edu.hk/~zukerman/classnotes.pdf>.

STOCHASTIC MODELING METHODS OF DOS ATTACKS

Simona Ramanauskaitė, Antanas Čenys

Summary

In this paper we describe a DoS attack and need too predict the success of attacks of various strengths. Analysis of existing stochastic models of DoS attack revealed that not enough attention is paid to the exploitation of attack traffic, and there is a lack of models where countermeasures are presented. We propose new dynamic and static stochastic flow exploitation DoS attack models. These models differ in their operating principle and it allows applying them in different situations, but the results are identical. The proposed models enable to model attack success by changing various parameters of attackers and victims. The proposed models can help evaluate the effectiveness of opening up additional channels of traffic exploitation during DoS attacks to reduce the DoS effect.

Keywords: DoS, stochastic modeling, computer network, security.

DOS ATAKŲ MODELIAVIMAS STOCHASTINIAIS METODAIS

Simona Ramanauskaitė, Antanas Čenys

Santrauka

Šiame darbe aprašytos DoS atakos, jų pasekmė bei poreikis prognozuoti tam tikro galingumo atakų sėkmės tikimybę. Atliktas egzistuojančių stochastinių DoS atakų modelių apibendrinimas, kuris atskleidžia, kad skiriama nepakankamai dėmesio srauto išnaudojimo atakoms bei trūksta modelių, DoS atakų kontrpriemonių naudojimui atskleisti. Atsižvelgiant į tai, siūlomi nauji stochastiniai srauto išnaudojimo DoS atakos modeliai – dinaminis ir statinis. Šie modeliai skiriasi savo veikimo principu ir leidžia juos taikyti skirtingose situacijose, o rezultatai yra tapatūs. Siūlomi modeliai leidžia aiškiai įvertinti atakos sėkmės tikimybę, keičiant įvairius atakos ir aukos parametrus. Taip pat siūlomais modeliais galima įvertinti papildomų kanalų atvėrimo efektyvumą srauto išnaudojimo DoS atakų efektui sumažinti.

Prasminiai žodžiai: DoS, stochastinis, kompiuterių tinklai, saugumas, modeliavimas.

Įteikta 2009-09-17