MOKSLAS – LIETUVOS ATEITIS
SCIENCE – FUTURE OF LITHUANIA

ISSN 2029-2341 print / ISSN 2029-2252 online
2012 4(1): 20–26 doi:10.3846/mla.2011.05

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

Elektronika ir elektrotechnika
Electronics and Electrical Engineering

COMPOSITE DoS ATTACK MODEL

Simona Ramanauskaitė[1], Antanas Čenys[2]
[1]Šiauliai University
[2]Vilnius Gediminas Technical University
E-mails: [1]simram@it.su.lt; [2]antanas.cenys@vgtu.lt

Abstract. Preparation for potential threats is one of the most important phases ensuring system security. It allows evaluating possible losses, changes in the attack process, the effectiveness of used countermeasures, optimal system settings, etc. In cyber-attack cases, executing real experiments can be difficult for many reasons. However, mathematical or programming models can be used instead of conducting experiments in a real environment. This work proposes a composite denial of service attack model that combines bandwidth exhaustion, filtering and memory depletion models for a more real representation of similar cyber-attacks. On the basis of the introduced model, different experiments were done. They showed the main dependencies of the influence of attacker and victim's properties on the success probability of denial of service attack. In the future, this model can be used for the denial of service attack or countermeasure optimization.

Keywords: denial of service, modelling, DoS, DDoS.

Introduction

The Internet becomes a quite important part of daily life and gives us an opportunity to easily and quickly get the newest and necessary information. However, an increase in the need of particular Internet services makes its quality and availability very important and sometimes even a critical factor for proper company's operation.

Denial of Service (DoS) attacks is a type of cyber-attacks aimed at disturbing or denying the Internet services, thus making difficult usage of it by its legitimate users. According to CERT-LT, in 2010, Denial of Service attacks were in the 4th place considering the frequency of occurrence in Lithuania. The office of the State Chief Information Security Officer (State of Texas) in the United States of America accepted that DDoS attacks as a way to make ransom attacks would also be one of the most popular attacks in the future.

Depending on a situation, DoS attacks can cause huge damage and loses. It can be quite difficult to prepare for similar attacks, because of insufficient ways or methods for estimating attack success. The aim of this work is to suggest a composite DoS attack model and use it for the analysis of how different properties of the attack and victim influence the overall attack success probability.

The coming sections of this paper describe why modelling DDoS attacks is a better solution than real experiments. Most common model types used for DoS attack modelling are mentioned to show why we suggest using mathematical models and what models have already been proposed to be used for modelling different types of DoS attacks.

The following sections represent the ideas and calculations of the above proposed composite DoS attack model used for modelling different DDoS attack situations and for distinguishing the impact of attack and victim properties on the success probability of composite attack. The results of the performed experiments and imposed conditions are also represented.

Denial of Service Attacks and Models

In the denial-of-service attack, the attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection or the computers and network of the sites you are trying to use, the attacker may be able to prevent you from an accessing email, websites, online accounts or other services that rely on the affected computer (McDowell 2004). In order to increase the attack power, many controlled computers can be used. This kind of attack is also known as a Distributed Denial of Service (DDoS) attack.

Practical experiments with DoS and DDoS attacks are difficult because of the following reasons:

- the area of attack sources spreads in a wide geographical area and experiments in the local network can be insufficient to illustrate the real situation;
- DDoS attacks require plenty of controlled computers, and therefore make difficulties in getting a sufficient amount of infected and ready to attack computers;
- execution of the DoS attack on the Internet can be illegal;

- real experiments on the Internet can cause problems for the third parties, disturb the work of innocent Internet users or even services.

The examination of attack properties without the real execution of DoS attacks can be done using different modelling methods and tools. Modelling allows making the estimation of the influence of different attack properties with less time and resource supplies.

For DoS and DDoS attack modelling different methods is used. C. Meadows (1999) proposed a cost-based framework useful to analyse protocol resistance to DoS attacks. The framework was used for researching different protocols (Meadows 2011; Diffie *et al.* 1992; Gong, Syverson 1995; Lafrance, Mullins 2003; Smith *et al.* 2006; Aiello *et al.* 2004; Cao *et al.* 2007). While this type of the model did not represent two confronting sides (attacked and victim), the other type of the multi-agent based DoS attack model - game-based model - was proposed by B. Bencsath *et al.* (2003). This type of models was used for computer science (Shenker 1994; Altman 1994; Maheswaran, Basar 1998; Hespanha, Bohacek 2001; Lye, Wing 2002) while B. Bencsath started using it for DoS attack modelling. The idea of game-based models in DoS attack modelling was developed by M. Fallah (2010) and I. Kotenko (2005). However, game-based models were not meant to represent the dynamics of object changes. Thus, rewrite theory models found a place in agent based DoS attack modelling and some researches were done using it (Agha *et al.* 2005; AlTurki *et al.* 2009; Kim *et al.* 2007).

These models relay on programming approaches (simulation, multi agent, rule-based models). However, the existing mathematical DoS and DDoS models can be used separately or combined with programming to produce model results without long lasting simulation or model execution. Those models are more dependent on a type of the DoS attack and use an appropriate queuing theory system for a certain situation. Q. Huang (Huang *et al.* 2003a, 2003b) and R. K. Chang (2002) applied general arrival rate to model DoS attacks. S. Khan, I. Traore (2005), A. Aissani (2008), G. Macia-Fernandez (Macia-Fernandez *et al.* 2006, 2009) and N. Chaturvedi, H. Mohant (2011) employed exponential distribution (Poisson process) to represent a certain level of traffic randomness in incoming traffic.

According to many different researches (Puigjaner 2006; Jain, Routhier 1986; Leland *et al.* 1994; Vandalore *et al.* 1999; Paxson, Floyd 1995), the present Erlang models do not represent the Internet traffic precisely and can be used only at a session level. Meanwhile, for model composition, burst and packet levels require more detailed traffic activity states and their intrinsic characteristics analysis. Therefore, Y. Wang *et al.* (2007) and K. Salah (2010) propose to model DoS attacks in a more general form and use Markov chains. It allows representing transitions from one state to another in a more detailed way. However, to describe a DoS attack in detail using Markov chain sometimes can be challenging and bring more complexity to model execution.

We believe that usually DoS and DDoS attacks can be modelled at the session rather than at the package level. Therefore, mathematical models of Poisson process with arrival rate is one of the most appropriate solutions taking into account both a model adequate to a certain situation and computation resources. However, as mentioned before, these models can vary depending on DoS type.

Mathematical Models of Bandwidth Exhaustion DoS Attack

A bandwidth exhaustion DoS attack happens when an intruder consumes all available bandwidth on a certain network by generating a large number of packets directed to your network. Typically, these packets are ICMP ECHO packets but in principle they may be anything (CERT 2001).

Q. Huang, H. Kobayashi and B. Liu suggested two models for modelling bandwidth exhaustion DoS attacks: one is for the attacks in the global network (Huang 2003a), and the other is for wireless networks (Huang 2003b). These two models offer the methods allowing finding a minimal number of agents necessary to execute successful DDoS attacks; however, the models do not pay enough attention to the properties of all attacks. More attack properties are taken into account in the paper focusing on modelling DoS attacks using stochastic methods (Ramanauskaitė, Čenys 2009). Also, this paper represents a mathematical expression of calculating the success of DoS attack using the known data on the attacks, normal flow and other properties of the victim.

Mathematical Models of Memory Exhaustion DoS Attack

DoS resource depletion attacks involve the attacker sending packets that misuse network protocol communications or sending malformed packets that tie up network resources so that none are left for legitimate users (Specht, Lee 2004). Memory is usually exhausted, and thus no new queries can be stored and served.

Memory depletion DoS attacks are the most common because of noticeable effect and quite low attack expenses. This is why there is a quite big range of the proposed models for memory depletion DoS attacks:

- Q. Huang *et al.* (2003a) apply the simplified Engest loss model G(N)/G/m(0) that enables to estimate the success of the SYN flooding attack when average attack flow, the average storage time of open-state connections and buffer size are known. However, these authors do not consider legitimate users, so there are no characteristics of legitimate users in this model and only the attack itself is characterised;

- R. K. C. Chang (2002) uses G/D/∞/N model to calculate minimal attack flow necessary to make a successful TCP SYN attack. However, in this work, the model is not described in detail, and only the results of the conducted experiment are given. Therefore, no possibility of making a conclusion concerning the comprehensiveness of this model exists.
- Y. Wang *et al.* (2007) use the model of two-dimensional embedded Markov chain taking into account legitimate and attack flow characteristics and buffer size. Nevertheless, this model is difficult to use in practice because of complex calculations.
- S. Ramanauskaitė (2010) suggests the SYN flooding attack model that can be used for any kind of memory depletion DoS attacks and allows estimating the success probability of the attack considering both victim and attacker properties.

Composite DoS Attack Model

Bandwidth exhaustion and memory depletion models allow analysing only certain parts of the overall DoS or DDoS attack. The real situation usually involves the interaction between different types of attacks. Therefore, the relations of DoS attacks should be taken into account and DoS attack models should be represented using a combined model involving at least a few types of the DoS attack.

When analyzing the DoS attack, we allow for accounts both bandwidth and memory depletion DoS models as well as for the filtering properties of the system. The concept of this composite model is explained in Fig. 1 or this way: incoming traffic can be blocked because of insufficient bandwidth. The rest part of traffic can be blocked by the filtering system. Finally, everything left after filtering can be blocked by an insufficient place in the buffer devoted to store open connections.

We denote bandwidth exhaustion probability as P_{B}, the probability of filtering legitimate traffic as P_{Fn} and memory depletion probability as $\mathrm{P_M}$. Composite attack probability P can be calculated as the probability of blocking legitimate traffic at least in one of these three subsystems (bandwidth exhaustion, filtering or memory depletion):

$$P = 1-(1-P_{\mathrm{B}})\cdot(1-P_{\mathrm{Fn}})\cdot(1-P_{\mathrm{M}})\,. \tag{1}$$

For estimating bandwidth exhaustion probability P_{B} we use the model of stochastic bandwidth exhaustion (Specht, Lee 2004):

$$P_{\mathrm{B}} = \left(\frac{\rho^k}{k!}\right) \Bigg/ \sum_{i=0}^{k} \frac{\rho^i}{i!}. \tag{2}$$

where $\rho = (s_{\mathrm{Ba}} + s_{\mathrm{Bn}})/T = (l_{\mathrm{a}}\cdot\lambda_{\mathrm{Ba}} + l_{\mathrm{n}}\cdot\lambda_{\mathrm{Bn}})/T$; k – the number of open channels; s_{Ba} – attack traffic (bps); s_{Bn} – normal traffic (bps); T – channel bandwidth (bps); l_{a} – the average query size of the attack (b); l_{n} – the average query size of legitimate users (b); λ_{Ba} – an arrival rate

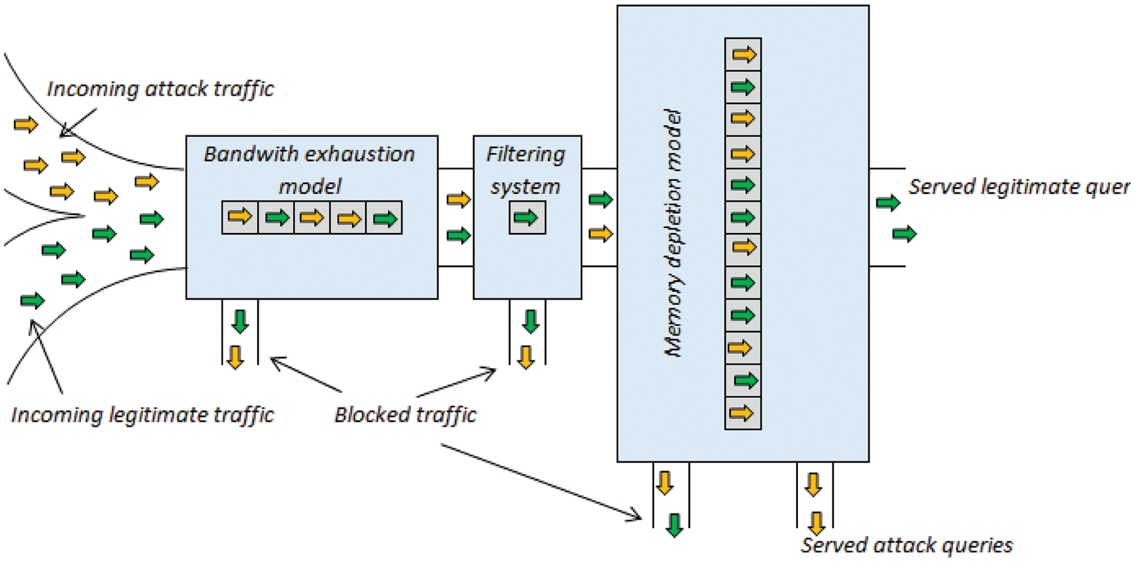

Fig. 1. A model of a conceptual composite DoS attack

of attack queries (qps); λ_{Bn} – an arrival rate of legitimate user queries (qps).

We assume that the filtering system has two properties: the probability of filtering legitimate traffic P_{Fn} and the probability of filtering attack traffic P_{Fa}. These properties show the part of legitimate and attack traffics that are blocked on average using filters.

To estimate incoming traffic, these properties are important both to composite attack probability and a subsystem of memory depletion. Considering the bandwidth exhaustion model, we assume that both legitimate and attack traffic has the same distribution in time as the overall incoming data. After passing the bandwidth exhaustion model, the rate of incoming traffic will be reduced to λ_{Fa} and λ_{Fn}:

$$\lambda_{\text{Fa}} = \lambda_{\text{Ba}} \cdot (1 - P_{\text{B}}) \, , \tag{3}$$

$$\lambda_{\text{Fn}} = \lambda_{\text{Bn}} \cdot (1 - P_{\text{B}}) \, . \tag{4}$$

The filtering system should block traffic equally considering time; thus, incoming legitimate traffic λ_{Ma} and attack traffic λ_{Mn} should change in size but not in its distribution. The extent to which traffic size will be reduced depends on filtering properties P_{Fa} and P_{Fn}:

$$\lambda_{\text{Ma}} = \lambda_{\text{Fa}} \cdot (1 - P_{\text{Fa}}) \, , \tag{5}$$

$$\lambda_{\text{Mn}} = \lambda_{\text{Fn}} \cdot (1 - P_{\text{Fn}}) \, . \tag{6}$$

The third subsystem of this composite DoS attack model is the memory depletion model. To represent this kind of the DoS attack, we use the SYN flooding attack model (Ramanauskaitė 2010) that might be also used for more general DoS attack types (for all DoS attacks based on extended information storage time to disturb the normal work of systems):

$$P_M = \left(\frac{\sigma^M}{M!} \right) \Bigg/ \sum_{i=0}^{M} \frac{\sigma^i}{i!} \, , \tag{7}$$

where $\sigma = \lambda_{\text{Ma}} \cdot t_{\text{a}} + \lambda_{\text{Mn}} \cdot t_{\text{n}}$; M – buffer size; t_{a} – the average processing time of the attack query (s); t_{n} – the average processing time of the legitimate query (s).

Modelling Results

Using the proposed model of the composite DoS attack, different situations were examined. The purpose of these experiments was to distinguish the influence of different attack properties on the success of the DoS attack.

For the analysis of these experiments, standard situation parameters may be chosen:

- regular 20 Mbps traffic (100 queries per second by 200 bits in each);
- 10 Mbps attack traffic (50000 queries per second by 200 bits in each);
- 1 channel with 100 Mbps bandwidth;
- victim uses filters that filter 20% of the attack and 2% of legitimate users queries;
- legitimate query takes 200 ms to execute;
- attack query execution takes 2 000 ms;
- buffer can hold information of 50 connections.

These attack and victim parameters lead to 8.7% of bandwidth exhaustion. 2% of legitimate queries are blocked by filtering system and memory depletion probability is 39.3%. The success probability of the composite DoS attack is 45.7%.

Changing filtering properties brings clarity that the blocking probability of legitimate queries is very important and linearly increases the success probability of the composite DoS attack. Meanwhile, the percentage of filtering attack traffic influences the memory and probability of the composite DoS attack to change in a not linear way (Fig. 2a).

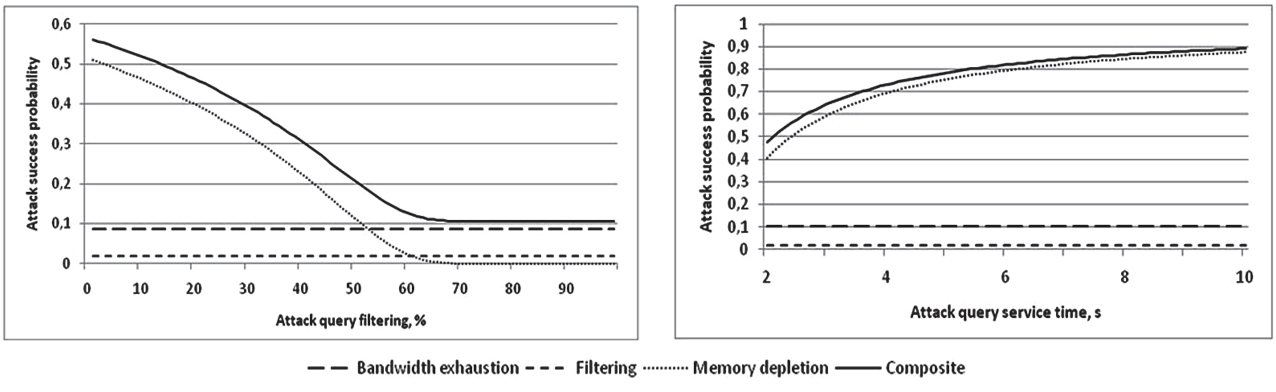

Fig. 2. The dependency of attack success on the percentage of filtering the attack query (a); attack query service time (b)

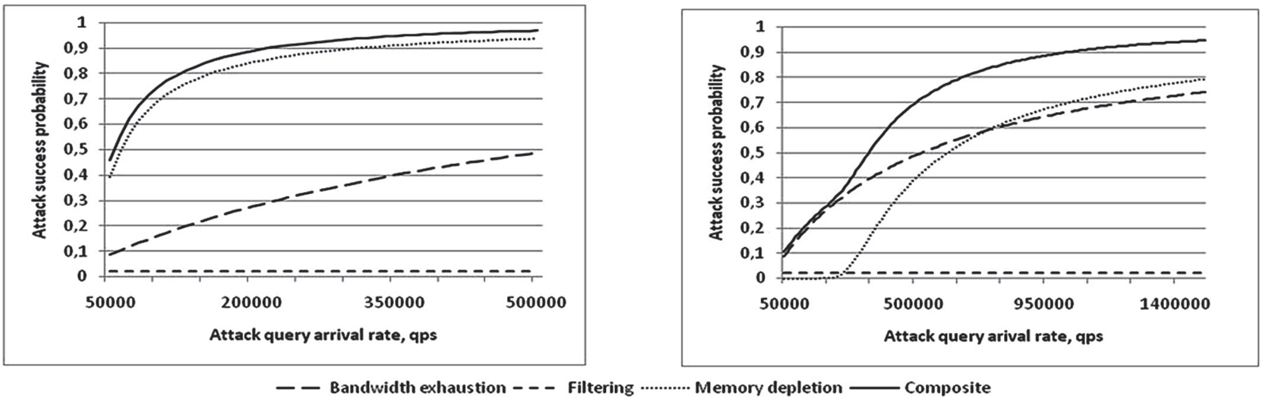

Fig. 3. The dependency of attack success probability on query arrival rate: a) with average service time; b) with very small service time

Similar tendencies also apply to the influence of service time on attack success. When increasing average service time (both legitimate and attack queries), the probability of memory depletion increases, although its influence on the success of the composite attack is not proportional (Fig. 2b).

The previous experiments had influence only on memory depletion and composite attack probabilities. Meanwhile, changes in incoming traffic properties also have influence on bandwidth exhaustion probability.

An increase in legitimate and attack traffic leads to an increase in attack success. However, in our experimental environment, an increase in memory depletion is higher than bandwidth exhaustion probability. Even if we decreased service time 10 times, the impact of bandwidth exhaustion on the success probability of the composite attack would be stronger only until the attack rate is quite low. While using heavier attack traffic, memory depletion probability has a more significant influence and is more sensitive to the attack size (Fig. 3).

Conclusions

The article shows the need for the composite DoS attack model due to the fact that though there are models for the exact DoS attack type they do not reveal the overall DoS success. Therefore, the composite DoS attack model was proposed for a more accurate estimation of attack success probability. When using this model, experimental modelling was done and revealed some facts concerning the success probability of the DoS attack:

- incorrect configurations of the filtering system can make more damage than the DoS attack itself;
- memory depletion attacks are more sensitive to changes in incoming traffic and can be the main reason for the high success probability of the composite attack;
- changes in the DoS attack and victim property values has not a linear influence on different parts of attack success probability not mentioning the success probability of the composite DoS attack.

The proposed composite DoS attack model can be improved adding additional components to a successful DoS attack such as computer processing power depletion subsystem or global filtering options. However, the suggested model can be used for evaluating the basic success probability of the DoS attack or different attack properties having influence on it.

References

Agha, G.; Gunter, C. A.; Greenwald, M.; Khanna, S.; Meseguer, J.; Sen, K.; Thati, P. 2005. Formal modeling and analysis of DoS using probabilistic rewrite theories, *International Workshop on Foundations of Computer Security* (FCS'05).

Aiello, W.; Bellovin, S. M.; Blaze, M.; Canetti, R.; Ioannidis, J.; Keromytis, A. D.; Reingold, O. 2004. Just fast keying: key agreement in a hostile internet, *ACM Transactions on Information and System Security* (TISSEC) 7(2): 242–273. http://dx.doi.org/10.1145/996943.996946

Aissani, A. 2008. Queueing analysis for networks under DoS attack, *International Conference on Computational Science and Its Applications* (ICCSA) 2: 500–513.

Altman, A. 1994. Flow control using the theory of zero-sum markov games, *IEEE Transaction on Automatic Control* 39: 814–818. http://dx.doi.org/10.1109/9.286259

AlTurki, M.; Meseguer, J.; Gunter, C. A. 2009. Probabilistic modeling and analysis of DoS protection for the ASV protocol, *Electronic Notes in Theoretical Computer Science* 234: 3–18. http://dx.doi.org/10.1016/j.entcs.2009.02.069

Bencsath, B.; Vajda, I.; Buttyan, L. 2003. A game based analysis of the client puzzle approach to defend against DoS attacks, in *International Conference on Software, Telecommunications and Computer Networks*, 763–767.

Cao, Z.; Guan, Z.; Chen, Z.; Hu, J.; Tang, L. 2007. An economical model for the risk evaluation of DoS vulnerabilities in cryptography protocols, in *International Conference on Information Security Practice and Experience*. Hong Kong, 7–9.

CERT-LT apibendrina 2010 metų veiklą [online]. CERT-LT, 2010 [cited 2011.10.31]. Available from Internet: https://www.cert.lt/doc/2010.pdf

Chang, R. K. C. 2002. Defending against flooding-based distributed denial-of-service attacks: a tutorial, *IEEE Communications Magazine* 40(10): 42–51. http://dx.doi.org/10.1109/MCOM.2002.1039856

Chaturvedi, N.; Mohant, H. 2011. A mathematical model for randomly-occurring low-rate denial of service attack, *International Journal of Computer & Communication Technology* 2(5): 13–17.

Cyber Security Trends for 2010 [online]. *State of Texas Cyber Security Tips Monthly Newsletter* 4(2) [cited 2011.10.08]. Available from Internet: http://www2.dir.state.tx.us/SiteCollectionDocuments/Security/Reading Room/201002cybersec.pdf

Denial of Service Attacks [online]. *CERT*, 2001 [cited 2011.10.10]. Available from Internet: http://www.cert.org/tech_tips/denial_of_service.html

Diffie, W.; Oorschot, P. C.; Wiener, M. J. 1992. Authentication and authenticated key exchanges, *Designs, Codes, and Cryptography* 2: 107–125. http://dx.doi.org/10.1007/BF00124891

Fallah, M. 2010. A puzzle-based defense strategy against flooding attacks using game theory, *IEEE Transactions on Dependable and Secure Computing* 7(1). http://dx.doi.org/10.1109/TDSC.2008.13

Gong, L.; Syverson, P. 1995. Fail-stop protocols: an approach to designing secure protocols, in *Int. Working Conference on Dependable Computing for Critical Applications*, 44–55.

Hespanha, J. P.; Bohacek, S. 2001. Preliminary results in routing games, *Proceedings of the American Control Conference* 3: 1904–1909.

Huang, Q.; Kobayashi, H.; Liu, B. 2003a. Analysis of a new form of distributed denial of service attack, in *Conference of Information Science and Systems*. The Johns Hopkins University, 2003, March 12–14.

Huang, Q.; Kobayashi, H.; Liu, B. 2003b. Modeling of distributed denial of service attacks in wireless networks, *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing* 1: 41–44.

Jain, R.; Routhier, S. A. 1986. Packet trains – measurements and a new model for computer network traffic, *IEEE Journal on Selected Areas in Communications* 4(6): 986–995. http://dx.doi.org/10.1109/JSAC.1986.1146410

Khan, S.; Traore, I. 2005. Queue-based analysis of DoS attacks, in *Proceedings IEEE Workshop on Information Assurance and Security*, 266–273. http://dx.doi.org/10.1109/IAW.2005.1495962

Kim, M.; Stehr, M. O.; Talcott, C. L.; Dutt, N. D.; Venkatasubramanian, N. 2007. A probabilistic formal analysis approach to cross layer optimization in distributed embedded systems, in *Formal Methods for Open Object-Based Distributed Systems*, 44–68.

Kotenko, I. 2005. Agent-based modeling and simulation of cyberwarfare between malefactors and security agents in internet, in *19th European Simulation Multiconference "Simulation in wider Europe"*.

Lafrance, S.; Mullins, J. 2003. An information flow method to detect denial of service vulnerabilities, *Formal Specifications of Computer-Based Systems* 9: 1259–1260.

Leland, W. E.; Taqqu, M. S.; Wilinger, W.; Wilson, D. V. 1994. On the self-similar nature of ethernet traffic, *IEEE/ACM Transactions on Networking* 2(1): 1–15. http://dx.doi.org/10.1109/90.282603

Lye, K.; Wing, J. M. 2002. Game strategies in network security, in *Proceedings of the Workshop on Foundations of Computer Security*. Copenhagen.

Macia-Fernandez, G.; Diaz-Verdejo, J. E.; Garcia-Teodoro, P. 2006. Mathematical foundations for the design of a low-rate DoS attack to iterative servers, *Lecture Notes in Computer Science* 4307: 282–291. http://dx.doi.org/10.1007/11935308_20

Macia-Fernandez, G.; Diaz-Verdejo, J. E.; Garcia-Teodoro, P. 2009. Mathematical model for low-rate dos attacks against application servers, *IEEE Transactions on Information Forensics and Security* 4(3): 519–529. http://dx.doi.org/10.1109/TIFS.2009.2024719

Maheswaran, R.; Basar, T. 1998. Multi-user flow control as a nash game: performance of various algorithms, in *IEEE Conference on Decision and Control*, 1090–1095.

McDowell, M. 2004. *Understanding Denial-of-Service Attacks* [online]. National Cyber Alert System, Cyber Security Tip ST04-015 [cited 2011.10.19]. Available from Internet: http://www.us-cert.gov/cas/tips/ST04-015.html

Meadows, C. A. 1999. A formal framework and evaluation method for network denial of service, in *IEEE Workshop on Computer Security Foundations*, *June 28–30*. Italy, 4. http://dx.doi.org/10.1109/CSFW.1999.779758

Meadows, C. A. 2001. A cost-based framework for analysis of denial of service in networks, *Journal of Computer Security* 9(1–2): 143–164.

Paxson, V.; Floyd, S. 1995. Wide-area traffic: the failure of poisson modeling, *IEEE/ACM Transactions on Networking* 3(3): 226–244. http://dx.doi.org/10.1109/90.392383

Puigjaner, R. 2006. Performance modelling of computer networks, in *Ifip/Acm Latin America Conference on Towards a Latin American Agenda for Network Research*, 106–123.

Ramanauskaitė, S. 2010. Modeling of SYN flooding attacks, *Jaunųjų mokslininkų darbai* 26(1): 331–335.

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

Salah, K. 2010. Queuing analysis of network firewalls, in *IEEE Global Telecommunications Conference*, 1–5.

Shenker, S. 1994. Making greed work in networks: a game-theoretic analysis of switch service disciplines, in *Symposium on Communications Architectures and Protocols*, 47–57.

Smith, J.; Gonzalez, N. J.; Boyd, C. 2006. Modelling denial of service attacks on JFK with meadows's cost-based framework, *Australasian Workshops on Grid Computing and e-Research* 54: 125–134.

Specht, S. M.; Lee, R. B. 2004. Distributed denial of service: taxonomies of attacks, tools and countermeasures, in *International Conference Parallel and Distributed Computing Dydtems*. San Francisco, 15–17.

Vandalore, B.; Babic, G.; Jain, R. 1999. Analysis and modeling in modern data communications networks, in *Applied Telecommunications Symposium*.

Wang, Y.; Lin, C.; Li, Q.; Fang, Y. 2007. A queueing analysis for the denial of service (DoS) attacks in computer networks, *Computer Networks* 54: 3564–3573. http://dx.doi.org/10.1016/j.comnet.2007.02.011

JUNGTINIS *DoS* ATAKŲ MODELIS

S. Ramanauskaitė, A. Čenys

Santrauka

Siekiant užkirsti kelią bet kokioms sistemų saugumo grėsmėms, vienas iš svarbiausių uždavinių yra prevencija. Tai leidžia numatyti galimus pavojus ir kovos su jais būdus, nustatyti jų efektyvumą ir pan. Tačiau realiai eksperimentuoti su turima sistema dažnai gali būti pernelyg sudėtinga, todėl daug lengviau šią problemą spręsti padeda matematiniai / programiniai modeliai. Straipsnyje siūlomas naujas *DoS* atakų modelis, sujungiantis kelių tipų *DoS* atakas (srauto ir atminties išnaudojimo, netinkamo filtrų nustatymo) ir jų įtaką viena kitai. Remiantis šiuo naujai sukurtu modeliu atlikti eksperimentai, kurių metu vertinama skirtingų atakos ir aukos savybių reikšmių įtaka bendrai atakos sėkmės tikimybei.

Reikšminiai žodžiai: elektroninės paslaugos trikdymo ataka, modelis, *DoS*, *DDoS*.