UDC 004.51-74

Models of Denial of Service Attacks on Cyber-Physical Systems

Mykola Ovcharuk[1], Mykola Ilin[1]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», 37, Prosp. Beresteyskyi, Kyiv, 03056, Ukraine*

Abstract

Mathematical models of denial-of-service attacks are investigated in the paper. Threats of kinetic impact on systems in cyberspace are considered. Targeted computer systems and systems with low and high-security levels were studied. The simulation results demonstrate a successful resolution of the task.

Keywords: cyberspace, cyber-physical system, DDoS, epidemiological model

Introduction

Behind the alleged simplicity of a denial-of-service (DoS) attack, there is a rapidly growing threat. Google has reported an exponential growth in DDoS attacks and informed the IoT botnet-generated attack on their services peaked at 2.5 Tbit/s in 2017 [1]. Microsoft disclosed details of a 3.47 Tbit/s DDoS attack targeting an Azure customer [2]. APT groups use DDoS to increase pressure on victims during ransomware attacks [3]. Mitigation techniques such as traffic filtering, load balancing, and speed limiting are used to protect against DDoS attacks. Large commercial companies are protected against sophisticated attacks, but state-sponsored attackers can also target government and critical infrastructure systems. In addition, attackers are looking for new, more effective attack methods and attempting to adapt their tactics to circumvent the methods used for protection. For example, while classic amplifiers (DNS, SSDP, NTP, etc.) can amplify the attack tens or hundreds of times, exploiting the CVE-2022-26143 vulnerability in the Mitel MiCollab and MiVoice Business Express system driver can help an attacker to amplify the attack to 4 billion of times. It is actively used in attacks. In a year after the discovery of the vulnerability, the volume of attacks increased by more than 5 times [4]. A network of bots (botnet) is required to run such attacks successfully. Using a botnet, attackers generate initial traffic, manage attack flow, and attract new participants to the botnet [5].

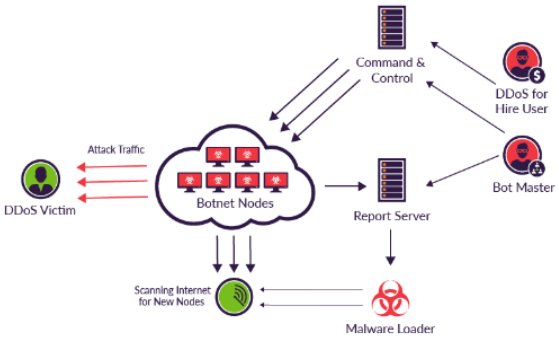

Figure 1: Botnet communication design

We will use appropriate mathematical models to analyze the dynamics of DDoS attacks spread and adaptive defense measures against them.

DDoS Attack Vectors

DDoS attacks impact a target system's quality, making it unreachable for legitimate customers. To achieve this goal, attackers can utilize various kinds of attack vectors [6].

Volumetric attack: traffic-flood to exhaust network or hardware resources using a large traffic volume. For volumetric reflection attacks with amplification, actors use forged small requests to generate massive traffic from several devices to the target (usually via vulnerable services – amplifiers).

Protocol exploitation: exploiting network protocol vulnerabilities and exhausting connection state tables.

Application layer attack: exploitation of vulnerable application layer protocols.

Furthermore, applications can be vulnerable to DoS attacks, and these attacks do not require generating vast amounts of traffic. Application layer attacks are challenging to detect because they are stealthy and concealed inside legitimate traffic.

Attack Models

Attack modeling is vital to understanding any threat in detail and considering the attack success factors [7]. Also, it can help assess the defense system's effectiveness [8] and test the network's sustainability.

Among attack models presented in the literature, only a few have used accurate mathematical models suitable for analyzing DDoS attacks.

The first approach is traffic-based modeling. The model considers the attack patterns and the network environment. J. Luo et al. [9] presented a model to estimate the attack effect of low-rate shrew DDoS by analyzing the behavior of the TCP congestion window. The attack exploits vulnerabilities in the retransmission timeout mechanism used in TCP. The authors proposed a formula to calculate the minimum cost to launch (MCL) a successful attack with the maximum effect. S. Ramanauskaite et al. [10] described the model as a multidimensional problem where the attack simultaneously targets three resources: RAM, CPU, and network bandwidth. Queuing theory, used in the model, allows the authors to evaluate various DDoS attacks. The queuing theory allowed the authors to evaluate the different types of DDoS attacks. S. Belamfedel et al. [11] also considered the TCP protocol behavior under DDoS attacks, and they proposed a mechanism to stabilize the routers' queuing process. Also, the authors executed models for different attack rates and explored the impact on the device's performance degradation.

The analytical modeling approach determines attack success probability according to specific conditions and parameters. Y. Xiang et al. [8] described the interaction model between the attack and defense sides, defining the defense system's efficacy and assessing optimal security funds. S. Ramanauskaite et al. [7] presented a model that makes it possible to calculate the attack success probability based on the botnet size and agent distribution strategies. The model can estimate the victim resistance probability under different attack types and defense strategies. A semantic DDoS attack model against wireless network protocols, proposed by M. Eian [12], can be used to find protocol vulnerabilities. Consequently, the model helps find protocol vulnerabilities and enhances protocol configuration and optimization.

The hierarchical modeling approach considers the availability of several components that can be affected by an attack. R. Maciel et al. [13] introduced a hierarchical model based on an attack tree analysis that assesses the effects of DDoS attacks by estimating implementability, probability of an attack, and attacker profit. The offered attack tree allows the evaluation of the impact of different simultaneous attacks on the system.

Let's consider mathematical models for studying in laboratory conditions the processes of botnet construction through the spread of malicious software in communication networks and/or the exploitation of common vulnerabilities. Such models have become widely used in epidemiology, but they have also become useful for cyber security specialists, as they allow modeling the formation of botnets and selecting appropriate attack parameters during stress testing of target systems.

Analogies with biological viruses are used here because the behavior of malware is similar to the behavior of viruses in the human population [14]. The accuracy of the mathematical model depends on the assumptions made during the modeling process. It is vital to take into account the limitations of the corresponding models. So, in models based on differential equations, you can get good results on a large scale (regarding global behavior), but for small local networks or individual hosts, they are not very applicable [15].

In conditions of active military, countering an attack in cyberspace can complement physical kinetic effect attacks. And vice versa – a kinetic impact during physical attacks can affect processes in cyberspace. As a result of missile attacks on critical infrastructure objects (telecom hubs, power substations, etc.), the availability of target systems may be disrupted: communication with them is temporarily lost, or they are disabled.

This work investigated the effect of initial conditions on the outcome of a denial-of-service attack. A simulation was performed based on the results of which the parameters of the obtained system were analyzed.

Problem statement

The paper aims to simulate denial-of-service attacks on cyber-physical systems. One of the essential phases of preparing for a distributed attack is creating a botnet (network of bots). Bots are malware-infected hosts or compromised IoT devices that can be used to generate DDoS attack traffic. A group of such bots is considered a botnet. The development and spread of botnets should be regarded as modeling a complete DDoS attack scenario, as this is an essential component in achieving successful distributed DDoS attacks.

The mathematical model created based on epidemiological modeling is used to analyze the dynamics of the spread of bots in communication systems. It is distinguished by considering kinetic attacks on network components, which consist of the physical disabling of nodes or their destruction.

Model description

A closed network with two subsets (attack and target) is studied. The number of participants (hosts) in the network is unchanged. Accordingly, $(t) + I(t) + R(t) = N$ for any moment of time t, where N is the total number of hosts in the network.

Susceptible hosts are vulnerable computers, servers, IoT devices in the network that can be infected;

Infected hosts are network elements that are infected with malicious software and are members of a botnet and through which further spread of malicious software occurs;

Restored hosts are network elements that were members of the botnet, but removed from it (quarantined, deleted, patched).

Consequently, we consider three variables depending on time (the number of iterations — if we consider discrete time intervals):

- allocation of receptive hosts $S(t)$,
- allocation of infected hosts $I(t)$,
- allocation of restored (remedied) hosts $R(t)$.

The allocation of susceptible hosts in the attacking population is denoted by Sa(t), infected hosts — $I_a(t)$.

Moreover

$S_a(t) + I_a(t) = 1$

The target population of network hosts is divided into two subgroups:

- weakly protected (security measures are not applied or incorrectly configured). Let's mark them accordingly $S_{low}(t)$, $I_{low}(t)$, $R_{low}(t)$
- well protected (security measures are implemented, but vulnerabilities are still present). Let's mark them accordingly $S_{high}(t)$, $I_{high}(t)$, $R_{high}(t)$

Moreover

$S_{low}(t) + I_{low}(t) + R_{low}(t) + S_{high}(t) + I_{high}(t) + R_{high}(t) = 1$

The dynamic of the model is described by a system of differential equations (1). Differential equations proposed by Ahmad, Ashraf & Abu Hour et. al [16] were supplemented by submitting the variable σ, which describes the system's response to physical influences in the cyber-physical space:

$$
\begin{aligned}
&\frac{dS_a}{dt} = \mu - \beta S_a - \mu S_a + \xi I_a \\
&\frac{dI_a}{dt} = \beta S_a I_a - (\xi + \mu) I_a \\
&\frac{dS_{low}}{dt} = -(\lambda + \sigma) S_{low} \\
&\frac{dI_{low}}{dt} = \lambda S_{low} - (\gamma_{low} + \sigma) I_{low} \\
&\frac{dR_{low}}{dt} = \gamma_{low} I_{low} - \xi_{low} R_{low} \\
&\frac{dS_{high}}{dt} = -\lambda(1 - \varepsilon) S_{high} + \xi_{high} R_{high} + \xi_{low} R_{low} - \sigma S_{high} \\
&\frac{dI_{high}}{dt} = \lambda(1 - \varepsilon) S_{high} - (\gamma_{high} + \sigma) I_{high} \\
&\frac{dR_{high}}{dt} = \gamma_{high} I_{high} - \xi_{high} R_{high} \\
&\frac{dD}{dt} = \sigma(S_{high} + S_{low} + I_{high} + I_{low})
\end{aligned}
\tag{1}
$$

where

I – infected hosts,

R – restored hosts,

μ – botnet recruitment rate (recruiting infected hosts),

β – rate of spread of malicious software (rate of botnet growth),

γ – recovery rate (withdrawal) of attacked hosts,

ξ – recovery of target network hosts that join a susceptible state,

ε – the security level of the target network kinetic physical effects on target systems,

σ – system's response to physical influences.

Threshold R = β/γ characterizes the conditions when the scale of the epidemic will increase (R>1) or decrease (R<1).

The system equations indicate:

- changes in the number of vulnerable hosts in the network over time depend on the intensity of contacts between vulnerable and infected network hosts (bots), as well as on the speed of the spread of malicious software;
- changes in the number of infected hosts (bots) – the difference between newly infected hosts and those that have been restored (where the incident was responded and mitigated);
- increasing of restored (removed from the botnet) hosts is proportional to the number of infected (recovery coefficient is a constant).

Security level of the target networks affects the peak values of the number of infected hosts and, accordingly, the peak power of the botnet. The dynamics of number of infected I changes accordingly hosts (Figure 3).

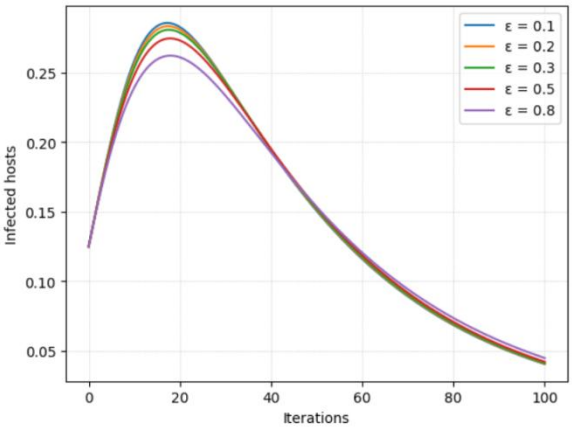

Figure 3: Population dynamic of infected hosts

Denial of service attack model research

Consider the system's behavior in standard conditions, with changes in the target system's protection level, and impacted by physical attacks.

With initial standard conditions, hosts enter a state of better protection (Figure 2).

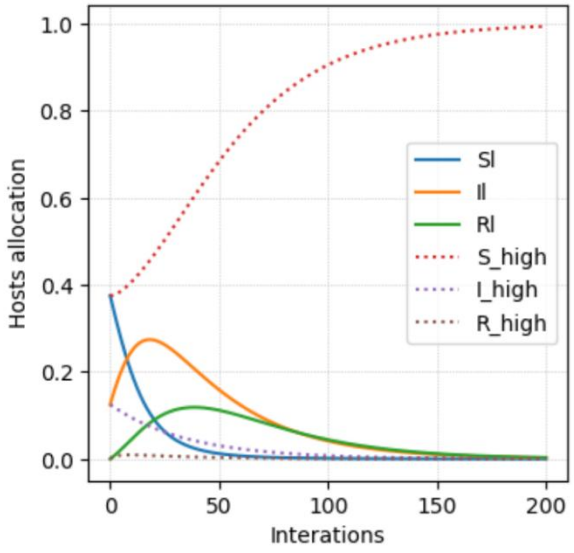

Figure 2: Population dynamics during the attack

Infection occurs faster in a scenario with less effective protection mechanisms. This is because infected hosts can infect more susceptible hosts before they are detected, respond to the incident, and mitigate the vulnerability.

In addition, the model considers physical attacks on systems in cyberspace, where the coefficient σ depicts the intensity of the kinetic impact on the attacked hosts. Physical attacks can destroy infrastructure and temporarily reduce the availability of target systems. The consequences of such a physical impact lead to the destruction of infrastructure facilities (telecommunication nodes, electrical substations) and a temporary decrease in availability or a long-term lack of communication with the target systems. It can lead to both helping achieve the goals of an attack in cyberspace (the target system is unavailable) and interfering with such plans (the attacker's network access is limited, but the target system services continue to work and serve clients).

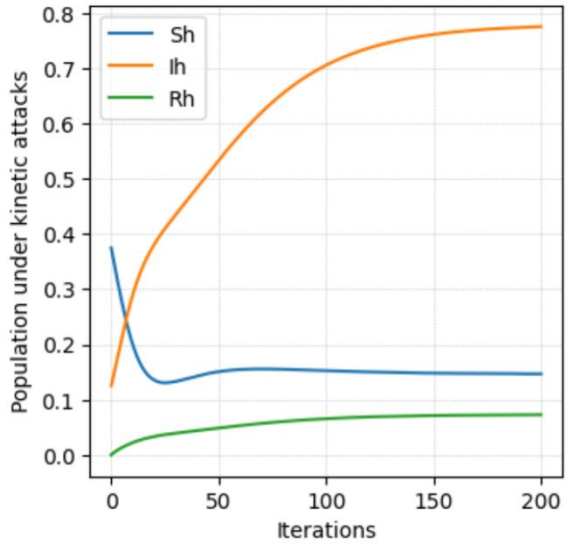

Figure 4: Population dynamic in normal conditions

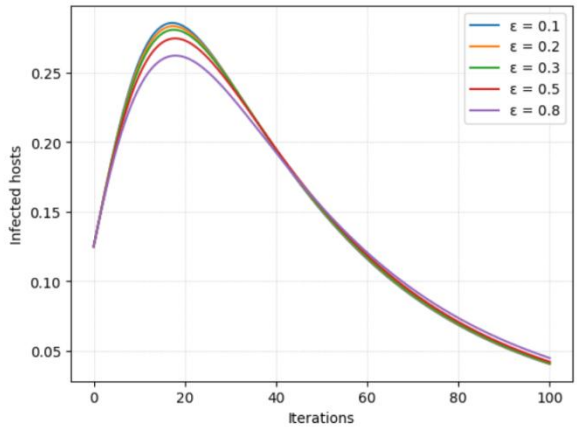

Figure 3: Population dynamic of infected hosts

Infection occurs faster in a scenario with less effective protection mechanisms. This is because infected hosts can infect more susceptible hosts before they are detected, respond to the incident, and mitigate the vulnerability.

In addition, the model considers physical attacks on systems in cyberspace, where the coefficient σ depicts the intensity of the kinetic impact on the attacked hosts. Physical attacks can destroy infrastructure and temporarily reduce the availability of target systems. The consequences of such a physical impact lead to the destruction of infrastructure facilities (telecommunication nodes, electrical substations) and a temporary decrease in availability or a long-term lack of communication with the target systems. It can lead to both helping achieve the goals of an attack in cyberspace (the target system is unavailable) and interfering with such plans (the attacker's network access is limited, but the target system services continue to work and serve clients).

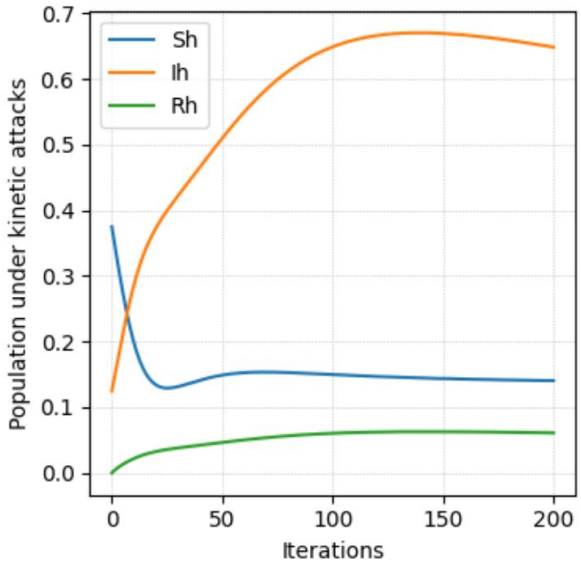

Figure 5: Population dynamic during physical attacks

The studied model demonstrates that physical kinetic attacks restrain the creation of a botnet (Figure. 5). On one hand, physical attacks can lead to irreversible loss of access to the target system (the attack is successful). Still, from another side, it negatively affects the power of a denial of service attack.

The model exhibits the expected behavior: with a rapid increase in the number of hosts in the botnet, followed by a slow decline as the hosts recover and become immune (response to the incident followed by remediation). Hosts with a low level of defense after infection and recovery move to a higher level of security (acquire immunity).

In general, the studied model provides a ground for understanding the process of botnet deployment and the impact of the defense mechanisms of target systems on it.

Conclusions

In the work, a study of models of denial-of-service attacks on cyber-physical systems was performed. The mathematical model for analyzing the spread of bots in communication networks considers the impact of kinetic attacks on network components. Further research can extend the model to consider the network topology and connections between hosts to

obtain a more detailed attack and defense dynamics map.

References

[1] Exponential growth in DDoS attack volumes, 2020. [Online]. Access: https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks

[2] [2] Alethea Toh, Azure DDoS Protection-2021 Q3 and Q4 DDoS attack trends, 2022. [Online]. Access: https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021- q3-and-q4-ddos-attack-trends/

[3] John Leyden, Ransom-related DDoS attacks rise from the dead as attack vectors diversify, 2021. [Онлайн]. Доступ: https://portswigger.net/daily-swig/ransom-related-ddos-attacks-rise-from-the-dead-as-attack-vectors-diversify

[4] Omer Yoachimik, Jorge Pacheco, “DDoS threat report for 2023 Q2”, 2023. [Online]. Access: https://blog.cloudflare.com/ddos-threat-report-2023-q2/

[5] How to Identify a Mirai-Style DDoS Attack, 2017. [Online]. Access: https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

[6] Matthew Prince, "Deep Inside a DNS Amplification DDoS Attack", 2012. [Online]. Access: https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/

[7] Simona Ramanauskaite, Nikolaj Goranin, Antanas Cenys, Jonas Juknius, "Modelling influence of Botnet features on the effectiveness of DDoS attacks", Security and Communication Networks 8 (12) pp. 2091-2100, 2015. DOI:10.1002/sec.1156

[8] Xiang Yang, Zhongwen Li, Wanlei Zhou, "An Analytical Model for DDoS Attacks and Defense", in: Conference on Computing in the Global Information Technology, 2006. DOI: 10.1109/ICCGI.2006.7

[9] Jingtang Luo, Xiaolong Yang, Jin Wang, Jie Xu, Jian Sun, Keping Long, "On a Mathematical Model for Low-Rate Shrew DDoS", IEEE Transactions on Information Forensics and Security 9(7), pp. 1069-1083, 2014. DOI: 10.1109/TIFS.2014.2321034

[10] Simona Ramanauskaite, Antanas Cenys, Nikolaj Goranin, Justinas Janulevicius, "Modeling of two-tier DDoS by combining different types of DDoS models", in: Open Conference of Electrical, Electronic and Information Sciences (eStream), 2017. DOI: 10.1109/eStream.2017.7950319

[11] Sadek Belamfedel Alaoui, Tissir El Houssaine, Chaibi Noreddinee, "Modelling, analysis, and design of active queue management to mitigate the effect of denial of service attack in wired/wireless network", in: Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, 2019. DOI: 10.1109/WINCOM47513.2019.8942547

[12] Martin Eian, Stig F. Mjolsnes, "The modeling and comparison of wireless network denial of service attacks", in: The 3rd ACM SOSP Workshop on Networking, Systems, and Applications on Mobile Handhelds, 2011, pp. 1-6. DOI: 10.1145/2043106.2043113

[13] Ronierison Maciel, Jean Araujo, Jamilson Dantas, Carlos Melo, Erico Guedes, Paulo Maciel, "Impact of a DDoS attack on computer systems: An approach based on an attack tree model", in: Annual IEEE International Systems Conference (SysCon), Vancouver, 2018. DOI: 10.1109/SYSCON.2018.8369611

[14] M.S. Dyakunenko, I. V. Styopochkina "Modeling the processes of spreading malicious software on the Internet" // Theoretical and applied problems of physics, mathematics and informatics: materials of the XIX All-Ukrainian scientific and practical conference of students, graduate students and young scientists (May 13-14, 2021, Kyiv, Ukraine). p. 212-215

[15] I.V. Styopochkina, M.V. Graivoronsky Modeling the distribution of computer viruses based on a probabilistic cellular automaton. //Protection of information. — 2015. — No. 4, p.1-9.

[16] Ahmad, Ashraf & Abu Hour, Yousef & Alghanim, Firas. (2021). A Novel Model for Distributed Denial of Service Attack Analysis and Interactivity. Symmetry. 13. 10.3390/sym13122443. D. Harel, First-Order Dynamic Logic, volume 68 of Lecture Notes in Computer Science, Springer-Verlag, New York, NY, 1979. doi:10.1007/3-540-09237-4.