МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/itech.2025.5.3

DOS-АТАКИ КАК КАТАСТРОФА «ЗВЕЗДА»

Научная статья

Гуц А.К.[1, *]
[1] ORCID : 0000-0002-3752-476X;
[1] Сочинский государственный университет, Сочи, Российская Федерация

* Корреспондирующий автор (aguts[at]mail.ru)

Аннотация

В статье рассматривается описание DoS-атак с помощью теории дифференциальных уравнений потенциального вида с шестью управляющими параметрами. В правой части уравнения взят потенциал, который представляет катастрофу «звезда». Управляющие параметры отражают четыре наиболее эффективные способа защиты от DoS-атак, а также производительность системы и входящий трафик. Скачкообразные смены стационарных равновесий – это катастрофы, которые могут ожидать компьютерную систему. Прогнозирование нежелательных катастроф состоит в отслеживание значений изменяющихся управляющих параметров. Опасными являются пересечения параметрами бифуркационных множеств. Продемонстрированы три проекции множества особенностей, позволяющие видеть, как меняется потенциальная функция и тем самым предсказывать возможные удачные хакерские атаки.

Ключевые слова: DoS-атака, катастрофа «звезда», компьютерная система, атаки хакеров.

DOS-ATTACKS AS A "STAR" CATASTROPHE

Research article

Guts A.K.[1, *]
[1] ORCID : 0000-0002-3752-476X;
[1] Sochi State University, Sochi, Russian Federation

* Corresponding author (aguts[at]mail.ru)

Abstract

In the article, DoS-attacks using the theory of differential equations of a potential type with six control parameters are described. On the right side of the equation, the potential is taken, which represents the Star catastrophe. The control parameters reflect the four most effective ways to protect against DoS-attacks, as well as system performance and incoming traffic. Abrupt changes in stationary equilibria are catastrophes that can be expected by a computer system. Predicting undesirable catastrophe consists in tracking the values of changing control parameters. Intersections between the parameters of bifurcation sets are dangerous. Three projections of a variety of features are demonstrated, allowing you to see how the potential function is changing and thereby predict possible successful hacker attacks.

Keywords: DoS attack, "star" catastrophe, computer system, hacker attacks.

Введение

Атаки на сервер, известные под названием «отказ в обслуживании» (DoS-атака (от англ. Denial of Service)), доставляют много хлопот администраторам, и теоретически исследуются, как правило, в рамках понятий и терминологии теории компьютерной безопасности.

Когда осуществляется DoS-атака, то пользователи не смогут получить доступ к сайту или веб-сервису из-за их перегрузки. Происходит это в силу того, что для обслуживания запросов у сервера не хватает необходимой производительности, или в силу отсутствия соответствующей системы защиты установленной на сервере.

Напомним, что DoS-атаки на компьютерную систему осуществляются с другого компьютера, при которых происходят передачи данных. Как известно, для передачи данных используются семь уровней формирования данных для их передачи по физическому каналу связи, именуемых моделью OSI (Open System Interconnection model). Это прикладной, представительский, сеансовый, транспортный, сетевой, канальный и физический уровни. Каждый из них выполнят определенную функцию по передаче данных или по представлению их в том или ином виде для пользователя компьютера; каждому соответствует тот или иной набор протоколов передачи данных.

В статье [1] была предложена математическая теоретико-катастрофическая модель DoS-атак, учитывающая все семь уровней модели OSI:

$$\frac{dx}{dt} = \left[(p - p_0) - x^7(t)\right] x(t) + (\tau - \tau_0). \quad (1)$$

Здесь $x(t)$ – число откликов сервера на запросы в момент времени t, τ – трафик и p – производительность сервера, p_0 и τ_0 – «типичные» характерные для данного сервера величины.

Два управляющих параметра t u p явно не отражают в полной мере ситуацию с работой сервера, который подвергнут DoS-атаке. Действительно, в этом случае единственной защитой от DoS-атак у нас будет наращивание производительности компьютерной системы. А это фактически означает техническое обновление системы и дополнительные финансовые затраты. Очевидно, что руководство далеко не всегда с этим согласится, и предложит

решать проблему защиты за счет использования имеющейся квалификации персонала, обслуживающего сервер. В статье мы усложняем модель (1) за счет конкретизации способов защиты сервера от DoS-атак.

Переход к 6-параметрической модели

Физический уровень в модели OSI имеет дело с кабелями, модуляцией сигнала, кодированием и прочим. Проще говоря, физический уровень – это уровень проводов и физических способов передачи сигналов по проводам или с помощью беспроводной связи.

Поэтому более реалистичным кажется учет только шести уровней модели OSI, оставляющий без внимания физический уровень. В таком случае наша модель принимает вид

$$\frac{dx}{dt} = \left[(p - p_0) - x^6(t)\right] x(t) + (\tau - \tau_0),$$

или

$$\frac{dx}{dt} = -\frac{\partial}{\partial x} V(x, p, \tau), \tag{2}$$

где

$$V(x, p, \tau) = \frac{1}{8}x^8 - \frac{1}{2}(p - p_0)\, x^2 - (\tau - \tau_0)\, x. \tag{3}$$

Но эта модель по-прежнему ограничивается самым примитивным способом защиты как наращивание производительности системы, как было отмечено во введении, т.е. ее обновлением. Очевидно, что нужно добавить в нее дополнительные управляющие параметры, которые отражали бы другие известные специалистам по отражению DoS-атак способы организации защиты сервера и которые были бы приемлемыми для владельцев сервера.

Рассмотрим следующую модель

$$V(x, p, \tau, m, u, l) = \frac{1}{8}x^8 - fx^6 - mx^5 - ux^4 - lx^3 - px^2 - \tau x, \tag{4}$$

где

l – управляющий параметр, отвечающий за блокирование через firewall превышения и настройку лимитов по количеству SYN-пакетов в секунду, которые вы ожидаете для вашего сервиса (защита от **атак TCP SYN Flood**) [2];

u – управляющий параметр, отвечающий за отбрасывание пакетов, которые по ожиданиям будут слишком большого размера, чтобы не забивать оперативную память (защита от атак **UDP Flood**) [2];

f – управляющий параметр, отвечающий за настройку firewall сервера: в политиках ни в коем случае нельзя оставлять настройки по дефолту. Важно закрыть все, кроме доверенных адресов и сетей [2];

m – управляющий параметр, отвечающий за настройку мониторинга показателей сервиса: канал, загрузка CPU, траты памяти, работоспособности отдельных микросервисов и важных для бизнеса элементов сайта [2].

Эти параметры также учитывают не все способы защиты, но мы принимаем во внимание рекомендации специалистов, что «важно настроить мониторинг показателей сервиса: канал, загрузка CPU, траты памяти, работоспособности отдельных микросервисов и важных для бизнеса элементов сайта» [2].

Демонстрация 6-параметрической модели типа «звезда»

Предлагаемая модель (4) – это теоретико-катастрофическая модель типа «звезда» [4]. Как правило, она подробно не анализируется в книгах по математической теории катастроф из-за сложности ее графического представления, за исключением монографии Вудкока и Постона [4], где даны различные сечения бифуркационного множества (см. ниже). Но приводимыми в этой книге графическими данными трудно воспользоваться на практике – они хороши лишь при теоретическом неторопливом анализе тех ли иных ситуаций. Работа сервера при DoS-атаках – это смена стационарных состояний. Опишем это подробнее.

Нормальная рабочая обстановка функционирования сервера – это **стационарные состояния**, при которых величина $x(t)$ практически не меняется с течением времени t, т.е. имеем состояния, удовлетворяющие равенству

$$\frac{dx}{dt} = 0.$$

Смысл использования теории катастроф состоит в том, что при некоторых малых изменениях параметров l, u, m, p, τ могут происходить скачкообразные изменения числа откликов, т.е. возможны непредсказуемые резкие замены одного стационарного состояния на другое, что характерно для поведения компьютерных систем, подвергшихся DoS-атакам.

Для моделирования ситуаций на компьютере нам нужно визуализировать множество катастроф Σ_V и множество особенностей C_V функции $V(x,a)$ соответственно

$$\Sigma_V = \{(x, a) : d_x V(x, a) = 0\} \text{ и } C_V = \{(x, a) : d_x V(x, a) = 0 \text{ и } d_x^2 V(x, a) = 0\}$$

для рассматриваемой катастрофы «звезда» (4) и проекции $C(x)$ на различные плоскости управляющих параметров $a = (l, u, m, p, \tau)$, получив так называемые **бифуркационные множества**, пересекая которые потенциальная функция $V(x)$ будет изменяться: минимумы, соответствующие стационарным равновесиям, лежащим на Σ_V, будут исчезать и образоваться новые, т.е. новые ситуации, в которых вынужден будет функционировать сервер (см. рис. 1-3), выдавая при этом соответствующее значение числа откликов x. Резкое падение x – это успешно проведенная атака. Поэтому важно знать, по каким путям изменения параметров можно прийти к стационарным равновесиям, в которых резко падает величина откликов x.

Очевидно, что некоторые переходы, смены состояний, могут восприниматься как нежелательные, а компьютерные эксперименты подскажут, изменение каких параметров опасно и чего надо избегать. В идеале было бы неплохо иметь установленное на сервере теоретико-катастрофическое программное приложение, которое в автоматическом режиме отслеживает состояние сервера, информирует о нем администратора и бьет тревогу, если близка опасная бифуркационная граница. На сегодня нам неизвестно существование такого приложение, а как выглядит визуализация

проекций на плоскости (p, τ) (u, l) и (l, p) демонстрируется на рис. 1-3, полученных с помощью приложения, разработанного Е.О. Хлызовым в 2011 году [3].

На этих рисунках (в середине) даются проекции множества особенностей на ту или иную 2-мерную плоскость управляющих параметров, т.е. изображены бифуркационные множества. Цифрами помечены различные зоны на плоскости параметров, разделенные линиями бифуркационного множества, и приводятся графики функции $V(x)$ соответствующие этим зонам. Минимумы отвечают стационарным состояниям, т.е. нормальным рабочим режимам сервера. Мы видим, что при переходах линий бифуркационного множества происходит исчезновения одних минимумов и появление других. Иначе говоря, мы видим смену рабочих режимов функционирования сервера.

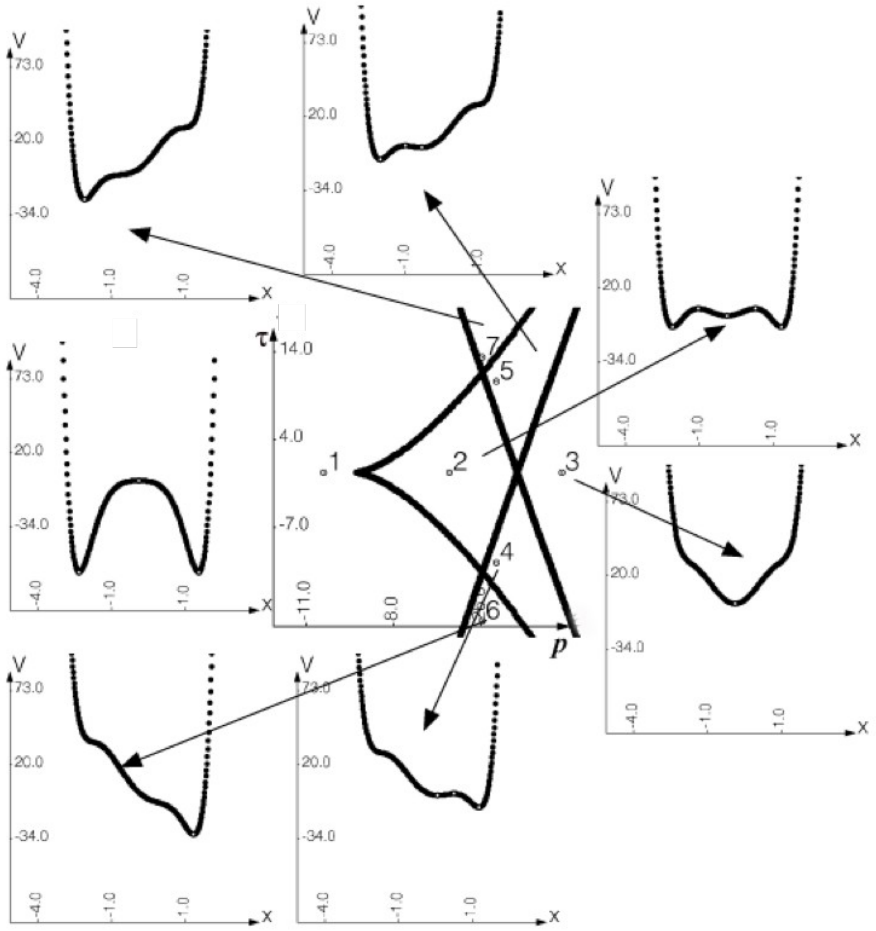

Рисунок 1 - Бифуркационное множество в проекции на (p, τ) и изменения функции $V(x)$

DOI: https://doi.org/10.60797/itech.2025.5.3.1

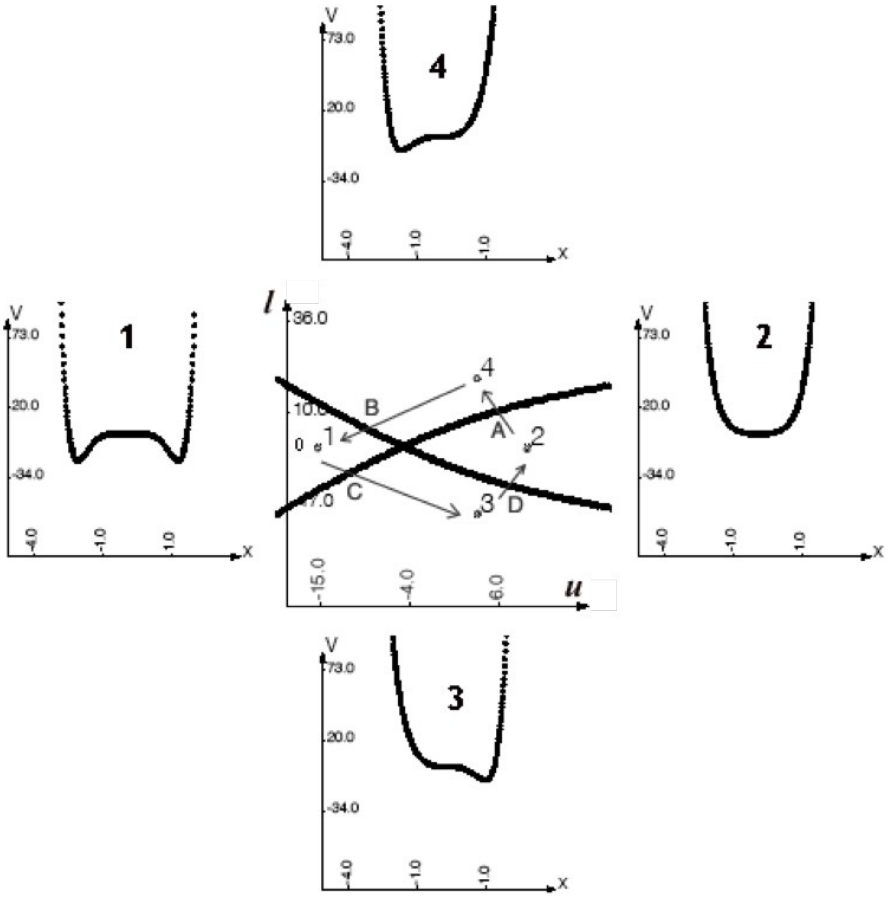

Рисунок 2 - Бифуркационное множество в проекции на (*u*, *l*) и изменения функции *V(x)*
DOI: https://doi.org/10.60797/itech.2025.5.3.2

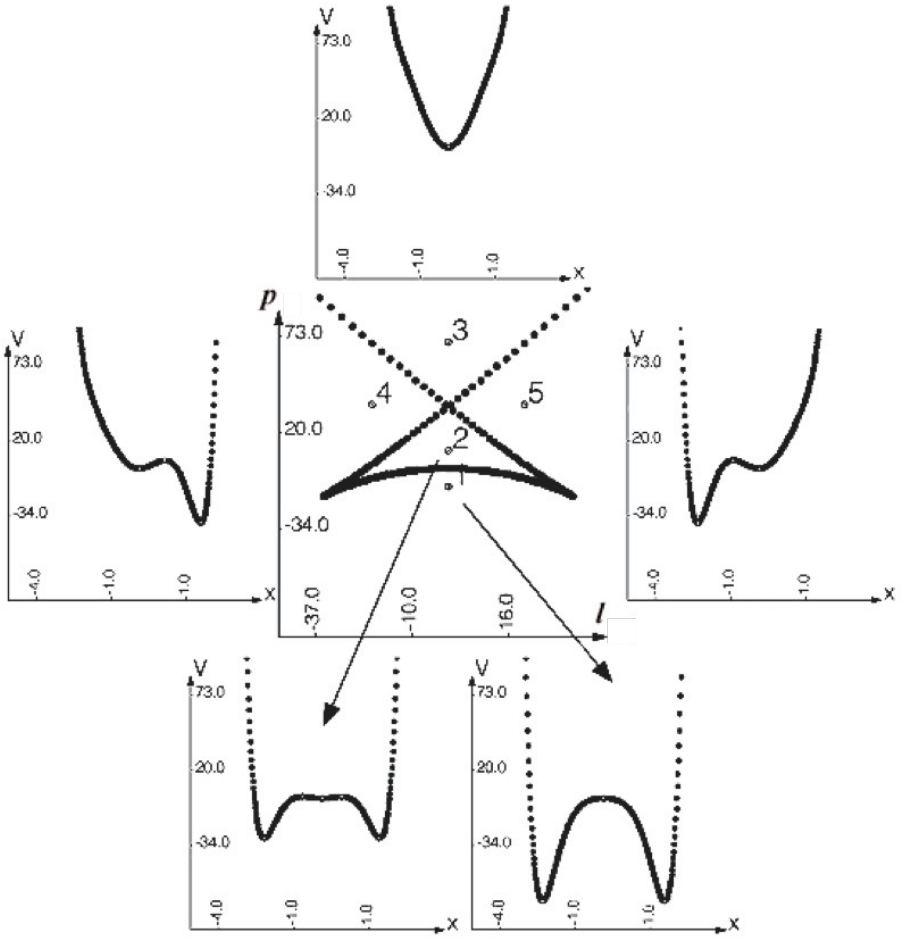

Рисунок 3 - Бифуркационное множество в проекции на (*l*, *p*) и изменения функции *V(x)*
DOI: https://doi.org/10.60797/itech.2025.5.3.3

Достаточно подробно бифуркационные множества для катастрофы «звезда» в различных проекциях приведены в книге [4]. Отметим еще одну важную особенность катастрофы «звезда». Она содержит шесть параметров, а как известно при числе параметров >5 функция *V(x)* скорее всего не обладает свойством структурной устойчивости [5], т.е. может меняться при определенных возмущениях, и это надо учитывать в случае использования катастрофы «звезда» при моделировании ситуаций отражения DoS-атак.

Заключение

В статье мы предложили теоретико-катастрофическое описание DoS-атак, учитывающее шесть уровней модели OSI. В принципе, вместо OSI сейчас имеется в виду модель DoD (Department of Defence), которая пришла на смену модели OSI и содержит четыре уровня. Соответствующее теоретико-катастрофическое описание сводится к катастрофе «бабочка», которая проще, чем «звезда», и для нее имеются различные программные приложения. Тем не менее, изощренность хакеров известна, и иметь возможность проводить эксперименты по DoS-атакам с учетов всех уровней взаимодействия компьютерных систем более чем желательно. И, следовательно, разработка программного приложения, описанного выше, весьма актуальна.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Гуц А.К. DDoS-атаки как катастрофа типа «бабочка» / А.К. Гуц // Омские научные чтения – 2020 : материалы четвертой Всероссийской научно-практической конференции. — Омск : Издательство Омского государственного университета им. Ф.М. Достоевского, 2020. — С. 383–386. — EDN QSXXKN.

2. Аверина П. DDoS-атаки в 2022 и методы защиты от них / П. Аверина. — 2022. — URL: https://habr.com/ru/companies/slurm/articles/674218/.

3. Гуц А.К. Компьютерный графический пакет для построения потенциальной функции в случае катастрофы «звезда» / А.К. Гуц, Е.О. Хлызов // Математические структуры и моделирование. — 2011. — № 22. — С. 69–73. — EDN PAIOKR.

4. Woodcock A.E.R. A Geometrical Study of the Elementary Catastrophes / A.E.R. Woodcock, T.A. Poston // Lecture Notes in Mathematics. — Vol. 373. — Heidelberg : Springer Berlin, 1974 — DOI: 10.1007/BFb0068967.

5. Постон Т. Теория катастроф и её приложения / Т. Постон, И. Стюарт. — Москва : Мир, 1982.

Список литературы на английском языке / References in English

1. Guts A.K. DDoS-ataki kak katastrofa tipa "babochka" [Ddos-atacks as catastrophes of butterfly type] / A.K. Guts // Omskie nauchnye chtenija – 2020 [Omsk Scientific Readings 2020] : Proceedings of the Fourth All-Russian Scientific and Practical Conference. — Omsk : Publishing House of Dostoevsky Omsk State University, 2020. — P. 383–386. — EDN QSXXKN. [in Russian]

2. Averina P. DDoS-ataki v 2022 i metody zashhity ot nih [DDoS attacks in 2022 and methods of protection against them] / P. Averina. — 2022. — URL: https://habr.com/ru/companies/slurm/articles/674218/. [in Russian]

3. Guts A.K. Komp'juternyj graficheskij paket dlja postroenija potencial'noj funkcii v sluchae katastrofy "zvezda" [The Computer Graphic Package for Creation of a Potential Function in Case of Accident "Star"] / A.K. Guts, E.O. Hlyzov // Matematicheskie struktury i modelirovanie [Mathematical Structures and Modeling]. — № 22. — P. 69–73. — EDN PAIOKR. [in Russian]

4. Woodcock A.E.R. A Geometrical Study of the Elementary Catastrophes / A.E.R. Woodcock, T.A. Poston // Lecture Notes in Mathematics. — Vol. 373. — Heidelberg : Springer Berlin, 1974 — DOI: 10.1007/BFb0068967.

5. Poston T. Teorija katastrof i ejo prilozhenija [Catastrophe Theory and Its Application] / T. Poston, I. Stewart. — Moscow : Mir, 1982. [in Russian]