Сиражудинов С.М. Сравнительный анализ способов защиты от DDoS атак в распределённых информационных системах // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 1(27) с. 66–74

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СПОСОБОВ ЗАЩИТЫ ОТ DDOS АТАК В РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Сиражудинов С.М.
Дагестанский Государственный Университет, Махачкала, Россия (367000, Республика Дагестан г. Махачкала, ул. Дзержинского, 12/1), email: the.r0.onneee@gmail.com

Статья посвящена вопросу сравнительного анализа способов защиты от DDOS атак в распределенных информационных системах. В статье рассмотрены теоретико-методологические основы DDoS-атак в распределённых информационных системах, способов защиты от DDoS-атак в распределённых информационных системах, методы противодействия распределенных сетевых атак, а также проведена сравнительная характеристика способов защиты (статистический, сигнатурный метод, метод на основе поиска аномалий) от DDOS атак в распределенных информационных системах. Был сделан вывод относительно того, что каждый метод имеет свои недостатки. Каждый из данных методов используется и применяется на основе объективного анализа специфики объекта защиты. Поэтому, можно сделать вывод, что нет универсального метода защиты информации и данных от DDoS-атак.

Ключевые слова: DDoS-атаки, методы защиты, связь, сеть, системы класса, трафик.

COMPARATIVE ANALYSIS OF WAYS TO PROTECT AGAINST DDOS ATTACKS IN DISTRIBUTED INFORMATION SYSTEMS

Sirazhudinov S.M.
Dagestan State University, Makhachkala, *Russia (*367000, Republic of Dagestan, Makhachkala Dzerzhinsky Str., 12/1*) e-mail: the.r0.onneee@gmail.com*

The article is devoted to the comparative analysis of methods of protection against DDoS attacks in distributed information systems. The article examines the theoretical and methodological foundations of DDoS attacks in distributed information systems, methods of protection against DDoS attacks in distributed information systems, methods of countering distributed network attacks, and provides a comparative characteristic of methods of protection (classical and modern) from DDoS attacks in distributed information systems. While each of these methods is used and applied on the basis of an objective analysis of the specifics of the object of protection. Therefore, we can conclude that there is no universal method of protecting information and data from Ddos attacks.

Keywords: DDoS attacks, protection methods, communication, network, class systems, traffic.

Атаки с распределенным отказом в обслуживании (DDoS) — это атаки на компьютерные системы (сетевые ресурсы или каналы связи), направленные на то, чтобы сделать их недоступными для пользователей, заблокировав их работу.[2]

Следует ввести понятие “защищённость” — невосприимчивость ресурса к воздействию DDoS-атак: чем она выше, тем эффективнее может быть его защита. И наоборот, если стойкость низкая, защита не сможет спасти этот ресурс - он наверняка будет недоступен какое-то время.[3]

Данные задачи выполняют статистический, сигнатурный и аномальный методы.

По данным Corero Network Security, ежемесячно от «атак с отказом в доступе» страдают больше 10 миллионов компаний в год и объём имеет постоянную тенденцию к росту.[7]

Отклонение, которое является стандартным, позволяет нам рассчитывать предел, выступающий в качестве недопустимого, чтобы определить то, какими параметрами обладает сетевая активность. Предположим, при нарушении границы – начинается падение, это связано с изменением нагрузки в соответствии с ресурсами сети. Для того, чтобы обнаружить атаку ранним доступом, нужно постоянно проводить мониторинг ограничений для каждого шага относительно времени.

К наиболее популярным методам защиты относятся методы, основанные на статистическом анализе.

Далее выделим основные параметры, с помощью которых проводится анализ:

- запросы за единицу времени;
- получение запросов, а также их скорость;
- запросы, определяемые конкретным источником;
- запросы в соответствии с местом назначения (если это веб-сервис, то для такого пункта характерно выступать в качестве отдельного скрипта);
- показатель временного интервала по каждому запросу;
- прочая сетевая активность.

Таким образом, рассмотрим пример расчёта среднего отклонения. Допустим, что x_i является числом запросов к серверу в течение одного часа. Для сервера характерна постоянная суточная нагрузка. n является показателем того, в каком количестве действуют суточные периоды. В результате этого матрица с запросами к серверу примет следующий вид:

$$x_{11}, x_{12}, x_{13} \dots x_{124}$$
$$x_{21}, x_{22}, x_{23} \dots x_{224}$$
$$x_{n1}, x_{n2}, x_{n3} \dots x_{n24}$$

Обычным способом с учетом определенного числа последних значений, например, так:

$$x_{21}, x_{22}, x_{23} \dots x_{224}, x_{11}, x_{12}, x_{13}, x_{14}$$

Получение значений осуществляется через строки матрицы, учитывая сезонность, для расчета берем столбцы:

$$x_{n1} \dots x_{21}, x_{11}$$

Следовательно, стоит отметить, что структура каждой строки матрицы характеризуется суточными данными по числу запросов к серверу. На основе первой строки осуществляется представление данных по текущим сутками, в результате чего допускается неполное

заполнение. Для того, чтобы рассчитать стандартное отклонение, могут быть использованы прочие методы.

Структура обычных специфических действий, подлежащих перехвату, характеризуется следующим:

- системные соглашения применяются не в рамках установленных норм и правил, скрывается интервал IP-адресов, стандартное соглашение выполняется в соответствии со скрытым портом;
- наличие уникальных паттернов трафика – больших UDP-пакетов, если приводить в сравнение TCP;
- наличие подозрительных примеров в соответствии с полезными данным приложения. На сегодняшний день достаточно сложно определить типичное поведение системы, выбрать предел, чтобы предупредить и предотвратить ложные предупреждения, этом и заключаются сложности, когда применяется метод обнаружения, включающий аномалии[4].

Специфика систем обнаружения DDOS-атак на основе сигнатур заключается в том, что для каждой подписи требуется раздел в базе данных, поэтому вся база данных может содержать сотни или даже тысячи подписей. Сигнатура каждого пакета должна быть сопоставлена с идентичной в базе данных. Этот процесс может быть очень ресурсоемким, может использовать всю пропускную способность и может сделать этот тип обнаружения уязвимым для DoS-атак.

Так как массив сетевого трафика является совокупностью составляющих его потоков, каждый из которых встречается в нем с определенной вероятностью, то данный массив M может быть описан в рамках рассматриваемой модели выражением, где $F_c(i)$ - функция распределения вероятности появления i-го потока в массиве тестового трафика:

$$M = ((C_i)_{i=1,}^{n} F_C(i)$$

Число потоков критических приложений можно использовать для обнаружения атак прикладного уровня, когда, например, к базе данных или системе инженерных вычислений.

Так же следует сказать, что для измерения значимых характеристик трафика реальной сети выделяют методы обнаружения вторжений.[6]

Несмотря на большое разнообразие методов обнаружения DDoS-атак, растущая обработка данных сварки требует разработки новых методов и алгоритмов обнаружения DDoS-атак с использованием высокоскоростных интерфейсов, машинного обучения и нейронных сетей.

Реалистичным в контексте данной работы будем называть синтезированный трафик, отражающий следующие свойства реальной сети:

- количество взаимодействующих узлов и топологию;
- статистическое распределение логических соединений между взаимодействующими сетевыми узлами;
- статистические характеристики трафика, связанные с размером и временным распределением сетевых пакетов внутри каждого из логических соединений.

Структура сигнатурных и аномальных методов различаются по применению подходов, чтобы проанализировать атаки:

1. Применение статического подхода со статическим анализом атаки, когда сама программа не запускается.

2. Применение динамического подхода. В соответствии с таким подходом анализ подозрительной программы осуществляется в динамике, когда она выполняется.

3. Применение гибридного подхода. Здесь статический и динамический методы объединены для того, чтобы проанализировать атаки с разных сторон.[5]

Сравнение статистического, сигнатурного и аномального метода по обозначенным критериям относительно статистического метода представлено в таб. 1.

Так же следует обозначить, что данные были рассчитаны относительно эффективности статистического метода по таким критериям как: дополнительный процент загрузки общего CPU ИС при применении защиты от DDOS без активной атаки; дополнительный процент пакетов, пересылаемых по сети при применении метода защиты от DDOS без активной атаки; дополнительный процент загрузки общего CPU ИС при применении защиты от DDOS при нахождении системы под атакой типа DDOS; частота ложных срабатываний системы защиты. Где 50% было взято как основа сравнения относительно классического (статистического) метода. Величина в процентах взята как показатель эффективности или неэффективности каждого метода, сравниваемом на основе характеристик каждого метода относительно критериев сравнения, приведенных в Таблице 1.

Поэтому, если 50% - среднестатистическое значение работы статистического метода относительно представленным критериям, то эффективность работы сигнатурного и метода на основе поиска аномалий была определена относительно классического метода.

Таким образом, если критерий соответственных методов, наведенных в Таблице 1 относительно статистического (как метод, который сравнивают с другими) меньше 50% - метод относительно представленного критерия считается более эффективным при сравнении данных методов с классическим.

Для сигнатурного метода затраты CPU выше, чем у статистического метода потому, что сигнатурный метод использует машинную синестезию, в связи с этим оценим эффективность этого параметра как 67%.[1]

В то же время для аномального метода дополнительный процент пакетов, пересылаемых по сети при применении метода защиты от DDOS без активной атаки выше сигнатурного и статистического метода в процентном соотношении потому, что аномальный метод использует машинную синестезию, в связи с этим оценим эффективность этого параметра как 75,43%.

Далее, статистический метод использует алгоритмы классификации изображений, потому возьмет критерии дополнительного процента загрузки общего CPU ИС при применении защиты от DDOS без активной атаки; дополнительного процента пакетов, пересылаемых по сети при применении метода защиты от DDOS без активной атаки; дополнительного процента загрузки общего CPU ИС при применении защиты от DDOS при нахождении системы под атакой типа DDOS; дополнительного процента пакетов, пересылаемых по сети при применении метода защиты от DDOS при нахождении системы под атакой типа DDOS; частоты ложных срабатываний системы защиты по 50%.

Таблица 1 – Сравнение методов защиты от DDoS относительно статистического метода (в процентах)

Критерий	%		
	Статистический	Сигнатурный метод	Метод на основе поиска аномалий
дополнительный процент загрузки общего CPU ИС при применении защиты от DDOS без активной атаки	50%	67%	23%
дополнительный процент пакетов, пересылаемых по сети при применении метода защиты от DDOS без активной атаки	50%	29,12%	75,43%
дополнительный процент загрузки общего CPU ИС при применении защиты от DDOS при нахождении системы под атакой типа DDOS	50%	15,21%	54%
дополнительный процент пакетов, пересылаемых по сети при применении метода защиты от DDOS при нахождении системы под атакой типа DDOS	50%	45,23%	36%
частоты ложных срабатываний системы защиты	50%	23%	23%

Поэтому, можем высчитать итоговый обобщённый показатель:

1. *Статистический метод* (как основной, с котором сравнивают сигнатурный и аномальный) (1): (средний коэффициент)

$$50\% * 0.25 + 50\% * 0.25 + 50\% * 0.15 + 50\% * 0.15 + 50\% * 0.2 = 0.125 + 0.125 + 0.750 + 0.750 + 0.10 = 1.85 \quad (1)$$

2. *Сигнатурный метод (*2): (средний коэффициент)

$$67\% * 0.25 + 29.12\% * 0.25 + 15.21\% * 0.15 + 45.23\% * 0.15 + 23\% * 0.2 = 0.1675 + 0.0728 + 0.0228 + 0.0345 + 0.0460 = 0.3436 \quad (2)$$

3. *Аномальный метод* (3): (средний коэффициент)

$$23\% * 0.25 + 75{,}43\% * 0.25 + 54\% * 0.15 + 36\% * 0.15 + 23\% * 0.2 = 0.0460 + 0.1885 + 0.0810 + 0.0540 + 0.0460 = 0.3615 \quad (3)$$

Основываясь на данных коэффициентах эффективности относительно статистического метода по обозначенным критериям в таблице, следует сказать, что статистический метод, при сравнении, является менее эффективным на фоне сигнатурного и аномального. При этом сигнатурный является эффективнее всего при защите от DDoS-атак.

Таким образом, можно сделать общий вывод об эффективности использования статистического метода при DDOS-атаках. Данный метод является эффективнее остальных по таким критериям как:

- дополнительный процент загрузки общего CPU ИС при применении защиты от DDOS без активной атаки;
- дополнительный процент пакетов, пересылаемых по сети при применении метода защиты от DDOS без активной атаки;
- дополнительный процент загрузки общего CPU ИС при применении защиты от DDOS при нахождении системы под атакой типа DDOS;
- дополнительный процент пакетов, пересылаемых по сети при применении метода защиты от DDOS при нахождении системы под атакой типа DDOS;
- частота ложных срабатываний системы защиты.

Говоря про использование статистического метода в защите от DDOS атак, следует сказать, что довольно самая большая трудность, которая встречается, когда применяется указанный выше подход, заключается в том, чтобы правильно выбрать периоды.

При проведении апробации необходимо провести выбор данных по таким серверам, в которых отмечается достоверность и надежность периодов работы.

Также следует отметить, что на сегодняшний день достаточно трудно определить периоды, по которым работаем крупный магистерский маршрутизатор.

Это связано с неправильным подчинением периодами его активности в соответствии с суточными периодами, при наличии собственных сложных периодов, получаемых тогда, когда складываются некоторые активности разных пользователей, когда они, например, находятся в разных часовых поясах.

Также следует сказать, что сезонные периоды, которые существуют, могут изменяться. К ним могут добавляться новые периоды, поэтому, при мониторинге трафика нужно проводить кластеризацию, и выявлять новые сезонные периоды в работе.

Таким образом, следует сказать, что каждый метод имеет свои недостатки. Сигнатурный, аномальный, статистический методы защиты применяются в защите информационных технологий, при этом каждый из данных методов используется и применяется на основе объективного анализа специфики объекта защиты. Поэтому, можно сделать вывод, что нет универсального метода защиты информации и данных от DDoS-атак.

Список литературы

1. Антонов, А.В. Системный анализ. 3-е изд., стер. / А. В. Антонов. — М.: Высшая школа, 2017. — 454 с.
2. Баринов, В.А. Теория систем и системный анализ в управлении организациями: Справочник: Учебное пособие / В. А. Баринов, Л. С. Болотова; под ред. В. Н. Волкова, А. А. Емельянов. — М.: ФиС, ИНФРА-М, 2016. — 848 с.
3. Баринов, В.А. Теория систем и системный анализ в управлении организациями: Справочник / В. А. Баринов, Л. С. Болотова. — М.: Финансы и статистика, 2017. — 848 с.
4. Вдовин, В.М. Теория систем и системный анализ: Учебник для бакалавров / В. М. Вдовин, Л. Е. Суркова, В. А. Валентинов. — М.: Дашков и К, 2016. — 644 с.
5. Волкова, В.Н. Теория систем и системный анализ: Учебник для бакалавров / В. Н. Волкова, А. А. Денисов. — М.: Юрайт, 2018. — 616 с.
6. Дрогобыцкий, И.Н. Системный анализ в экономике / И.Н. Дрогобыцкий. — М.: Финансы и статистика, 2016. — 512 с.
7. Батоврина Е.В. Информационные технологии в управлении предприятием // Теория и практика управления: новые подходы. - М.: Университетский гуманитарный лицей, 2016.- 217 с.
8. Методы защиты от DDOS нападений [Электронный ресурс] – Режим доступа: http://www.securitylab.ru/analytics/216251.php, свободный (дата обращения: 24.11.2022).
9. Терновой О.С. Раннее обнаружение DDOS-атак методами статистического анализа / Перспективы развития информационных технологий. – Новосибирск: Сибпринт, 2012. – С. 201–212.
10. Tripathi S., Gupta B., Almomani A., et al. Hadoop based defense solution to handle distributed denial of service DDoS attacks. J. Inf. Secur., 2013 [Электронный ресурс] - Режим доступа: https://www.scirp.org/journal/paperinformation.aspx?paperid=34629, свободный (дата обращения: 22.11.2022).
11. Mahajan D., Sachdeva M. DDoS attack prevention and mitigation techniques - a review. Int. J. Comput. Appl., 2013, vol. 67, no. 19, pp. 21–24. [Электронный ресурс] – Режим доступа: https://research.ijcaonline.org/volume67/number19/pxc3887221.pdf, свободный (дата обращения: 22.11.2022).
12. Ahamad T., Aljumah A. Detection and defense mechanism against DDoS in MANET. Indian J. Sci. Technol., 2015, vol. 8, no. 33. [Электронный ресурс] – Режим доступа: http://www.indjst.org/index.php/indjst/article/view/80152, свободный (дата обращения: 17.11.2022).
13. Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: a classification. Proc. 3rd IEEE Int. Symp. on Signal Processing and Information Technology, 2003. [Электронный ресурс] – Режим доступа: https://ieeexplore.ieee.org/document/1341092, свободный (дата обращения: 15.11.2022).
14. Munivara Prasad K., Rama Mohan Reddy A., Venugopal Rao K. DoS and DDoS attacks: defense, detection and traceback mechanisms–a survey. GJCST, 2014, no. 7-E. [Электронный ресурс] – Режим доступа: https://globaljournals.org/GJCST_Volume14/3-DoS-and-DDoS-Attacks-DefenseDetection.pdf, свободный (дата обращения: 15.11.2022).

15. Hachem N., Ben Mustapha Y., Granadillo G.G., et al. Botnets: lifecycle and taxonomy. Conf. on Network and Information Systems Security, 2011. [Электронный ресурс] – Режим доступа: https://ieeexplore.ieee.org/document/5931395, свободный (дата обращения: 15.11.2022).

References

1. Antonov, A.V. System analysis. 3rd ed., ster. / A.V. Antonov. — M.: Higher School, 2017. — p.454
2. Barinov, V.A. Theory of systems and system analysis in the management of organizations: Handbook: Textbook / V. A. Barinov, L. S. Bolotova; edited by V. N. Volkov, A. A. Emelyanov. — M.: FiS, INFRA-M, 2016. — p.848
3. Barinov, V.A. Theory of systems and system analysis in the management of organizations: Handbook / V. A. Barinov, L. S. Bolotova. — M.: Finance and Statistics, 2017. — p.848
4. Vdovin, V.M. Theory of systems and system analysis: Textbook for bachelors / V. M. Vdovin, L. E. Surkova, V. A. Valentinov. — M.: Dashkov and K, 2016. — p.644
5. Volkova, V.N. Theory of systems and system analysis: Textbook for bachelors / V. N. Volkova, A. A. Denisov. — M.: Yurayt, 2018. — p.616
6. Drohobytsky, I.N. System analysis in economics / I.N. Drohobytsky. — M.: Finance and Statistics, 2016. — p.512
7. Batovrina E.V. Information technologies in enterprise management // Theory and practice of management: new approaches. - M.: University Humanities Lyceum, 2016.- p.217
8. Methods of protection against DDOS attacks [Electronic resource] – Access mode: http://www.securitylab.ru/analytics/216251.php , free (accessed: 11/24/2022).
9. Ternovoy O.S. Early detection of DDOS attacks by statistical analysis methods / Prospects for the development of information technologies. – Novosibirsk: Sibprint, 2012. – pp. 201-212.
10. Tripathi S., Gupta B., Almomani A., et al. Hadoop based defense solution to handle distributed denial of service DDoS attacks. J. Inf. Secur., 2013 [Electronic resource] - Access mode: https://www.scirp.org/journal/paperinformation.aspx?paperid=34629 , free (accessed: 11/22/2022).
11. Mahajan D., Sachdeva M. DDoS attack prevention and mitigation techniques - a review. Int. J. Comput. Appl., 2013, vol. 67, no. 19, pp. 21–24. [Electronic resource] – Access mode: https://research.ijcaonline.org/volume67/number19/pxc3887221.pdf , free (accessed: 11/22/2022).
12. Ahamad T., Aljumah A. Detection and defense mechanism against DDoS in MANET. Indian J. Sci. Technol., 2015, vol. 8, No. 33. [Electronic resource] – Access mode: http://www.indjst.org/index.php/indjst/article/view/80152 , free (date of application: 17.11.2022).
13. Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: a classification. Proc. 3rd IEEE Int. Symp. on Signal Processing and Information Technology, 2003. [Electronic resource] – Access mode: https://ieeexplore.ieee.org/document/1341092 , free (accessed: 11/15/2022).
14. Munivara Prasad K., Rama Mohan Reddy A., Venugopal Rao K. DoS and DDoS attacks: defense, detection and traceback mechanisms–a survey. GJCST, 2014, no. 7-E. [Electronic resource] – Access mode: https://globaljournals.org/GJCST_Volume14/3-DoS-and-DDoS-Attacks-DefenseDetection.pdf , free (accessed: 11/15/2022).

15. Hachem N., Ben Mustapha Y., Granadillo G.G., et al. Botnets: lifecycle and taxonomy. Conf. on Network and Information Systems Security, 2011. [Electronic resource] – Access mode: https://ieeexplore.ieee.org/document/5931395 , free (accessed: 11/15/2022).