ӘОЖ 004.056.5

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ОТ DDOS-АТАК В УСТРОЙСТВАХ ИНТЕРНЕТА ВЕЩЕЙ

Дауылбай А.А.
- магистрант 1-курса ОП «Программной инженерии»,
Ележанова Ш.К. - к.ф.-м.н., профессор кафедры «Программной инженерии»
Атырауский университет им. Х. Досмухамедова, г. Атырау,
anuarbekdauylbay@gmail.com, shinar1802@mail.ru

Аннотация. В статье представлен анализ способов защиты устройств Интернета вещей (IoT) от распределённых атак типа отказ в обслуживании (DDoS). Описаны актуальные угрозы, связанные с массовым внедрением IoT-устройств, и рассмотрены ключевые подходы к обеспечению их безопасности. Особый акцент сделан на фильтрации трафика, системах обнаружения вторжений, облачных технологиях и применении методов машинного обучения. Приведена оценка эффективности различных защитных методов и их пригодности для IoT-устройств с ограниченными ресурсами. Ключевые слова: Интернет вещей (IoT), DDoS-атака, кибербезопасность, ботнет, IDS, машинное обучение, защита сети.

Введение. Бурное развитие технологий Интернета вещей (IoT) вызвало резкий рост числа подключённых устройств, применяемых в самых разных областях — от интеллектуальных домашних систем до автоматизации производства. IoT — это сеть устройств, взаимодействующих и обменивающихся данными без непосредственного участия человека.

Тем не менее, вместе с быстрым распространением IoT увеличивается и количество киберугроз. Одной из самых серьёзных угроз считаются распределённые атаки типа отказ в обслуживании (DDoS), направленные на перегрузку систем и вывод их из строя.

Главная сложность заключается в том, что большинство IoT-устройств оснащены слабыми вычислительными ресурсами, имеют недостаточную систему защиты и редко получают обновления. Это делает их лёгкой добычей для злоумышленников, которые могут объединять такие устройства в ботнеты для организации крупных DDoS-атак.

В статье анализируются ключевые методы защиты IoT-устройств от DDoS-атак, их сильные и слабые стороны, а также направления дальнейшего развития этой сферы.

Обзор литературы. Актуальные научные работы по кибербезопасности уделяют значительное внимание проблеме DDoS-атак в среде IoT. Ярким примером служит ботнет Mirai, использовавший уязвимые IoT-устройства для проведения крупных атак на интернет-ресурсы.

K. Kolias и соавторы в своих работах анализируют структуру ботнетов и их воздействие на сетевую инфраструктуру. Исследования показывают, что причиной частых атак на IoT-устройства являются недостаточно надёжные механизмы аутентификации.

J. Mirkovic в исследовании, посвящённом атакам отказа в обслуживании, рассматривает различные виды DDoS-атак (SYN flood, UDP flood, HTTP flood) и способы их предотвращения.

Ряд исследований акцентирует внимание на использовании машинного обучения для выявления аномалий в сетевом трафике. Новейшие алгоритмы способны обнаруживать неизвестные ранее виды атак и значительно повышать уровень защиты.

Кроме того, исследуются облачные подходы, позволяющие вынести защитные функции на более производительные серверы и обеспечить масштабируемость всей системы.

Методы исследования. В этом исследовании был применён ряд взаимодополняющих методов. Системный анализ позволил рассмотреть Интернет вещей как единую систему, включающую устройства, сеть и серверную инфраструктуру. Для изучения научных работ и существующих защитных решений применялся аналитический подход. Сравнительный анализ использовался для оценки различных методов защиты по критериям эффективности, масштабируемости и стоимости внедрения. Также проводилось моделирование угроз, включая анализ распространённых сценариев DDoS-атак, таких как SYN flood, UDP flood и HTTP flood. Комплексное применение перечисленных методов позволило дать всестороннюю оценку современным способам защиты IoT-устройств от DDoS-атак.

Результаты исследования и обсуждение

В рамках исследования проведён анализ ключевых способов защиты устройств IoT от DDoS-атак.

Один из фундаментальных методов — фильтрация трафика. Этот подход ограничивает подозрительные запросы и уменьшает нагрузку на систему, однако при распределённых атаках его эффективность зачастую снижается.

Системы обнаружения и предотвращения вторжений (IDS/IPS) выявляют аномалии в сетевом трафике и оперативно реагируют на угрозы. Такие решения обеспечивают повышенную защиту, но требуют дополнительных вычислительных ресурсов.

Использование облачных решений обеспечивает масштабируемую защиту и позволяет эффективно обрабатывать значительные объёмы трафика, однако связано с дополнительными расходами и зависимостью от сторонних поставщиков услуг.

Применение методов машинного обучения показывает высокую результативность при обнаружении новых типов атак. Эти технологии анализируют поведенческие паттерны устройств и фиксируют отклонения от нормы.

Значительный вклад вносит защита непосредственно на устройствах — это применение надёжных методов аутентификации, регулярные обновления программного обеспечения и использование технологий шифрования.

Анализ показал, что наилучшие результаты достигаются при комплексном подходе, объединяющем различные способы защиты.

Заключение

Вопрос защиты устройств Интернета вещей от DDoS-атак составляет одну из центральных проблем кибербезопасности сегодня. Увеличение числа подключённых устройств способствует росту угроз и расширяет возможные точки для атак.

Анализ показал, что универсального метода защиты не существует. Наибольшую эффективность обеспечивает совмещение различных инструментов — фильтрации трафика, систем обнаружения вторжений, облачных решений и технологий машинного обучения.

В будущем важно разрабатывать простые и действенные методы защиты, подходящие для устройств с ограниченными возможностями, а также внедрять стандарты безопасности для IoT.

Таким образом, для надёжной защиты IoT-систем необходимы постоянное развитие технологий и проведение дальнейших исследований в этой сфере.

Список литературы

1. Kolias C., Kambourakis G., «DDoS in the IoT: Mirai and other botnets», 2017 жыл
2. Mirkovic J., Reiher P., «A taxonomy of DDoS attack and defense mechanisms», 2004 жыл
3. RFC 4732, «Internet Denial-of-Service Considerations», 2006 жыл

4. Sicari S., Rizzardi A., Grieco L., Coen-Porisini A., «Security, Privacy and Trust in Internet of Things», 2015 жыл

5. Zhang Y., «Machine Learning for Network Security: Detection of DDoS Attacks», 2020 жыл