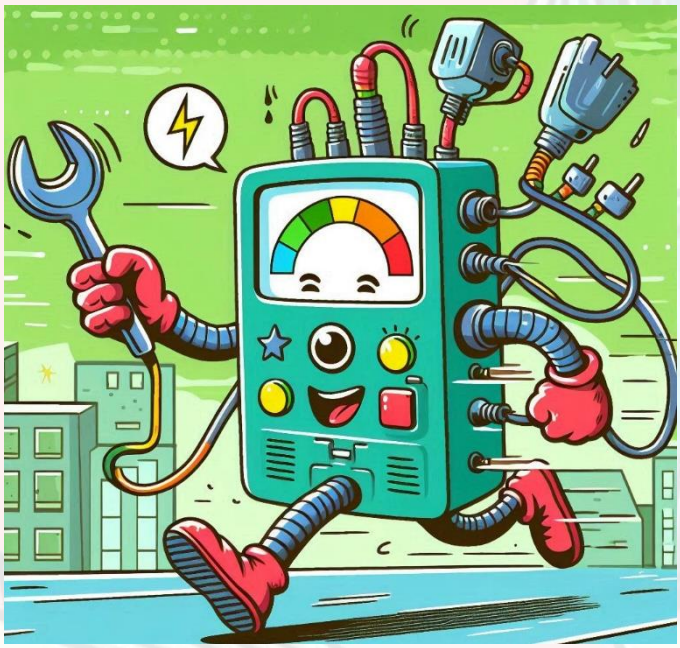

Аннотация – В научной статье "Detection of Energy Consumption Cyber Attacks on Smart Devices" подчёркивается растущая интеграция технологий Интернета вещей в умные дома и связанные с этим проблемы безопасности из-за нехватки ресурсов и ненадёжности сетей. Статья предлагает упрощённый метод обнаружения атак с использованием энергопотребления путём анализа принятых пакетов с учётом протоколов TCP, UDP и MQTT и оперативного оповещения при обнаружении аномального поведения, эффективно идентифицируя с помощью измерений скорости приёма пакетов.

I. Введение

В научной статье "Detection of Energy Consumption Cyber Attacks on Smart Devices" подчёркивается влияние интеграции технологии Интернета вещей в умные дома и связанные с этим проблемы безопасности.

- **Энергоэффективность**: подчёркивается важность энергоэффективности в системах Интернета вещей, особенно в средах "умного дома" для комфорта, уюта и безопасности.
- **Уязвимости**: уязвимость устройств Интернета вещей к кибератакам и физическим атакам из-за ограниченности их ресурсов подчёркивает необходимость защиты этих устройств для обеспечения их эффективного использования в реальных сценариях.
- **Предлагаемая система обнаружения**: Авторы предлагают систему обнаружения, основанную на анализе энергопотребления интеллектуальных устройств. Цель этой платформы – классифицировать состояние атак отслеживаемых устройств путём изучения структуры их энергопотребления.
- **Двухэтапный подход**: Методология предполагает двухэтапный подход. На первом этапе используется короткий промежуток времени для грубого обнаружения атаки, в то время как второй этап включает в себя более детальный анализ.
- **Облегчённый алгоритм**: представлен облегчённый алгоритм, который адаптирован к ограниченным ресурсам устройств Интернета вещей и учитывает три различных протокола: TCP, UDP и MQTT.
- **Анализ скорости приёма пакетов**: Метод обнаружения основан на анализе скорости приёма пакетов интеллектуальными устройствами для выявления аномального поведения, указывающего на атаки с использованием энергопотребления.

II. Преимущества и недостатки

Преимущества и недостатки дают сбалансированное представление о возможностях и ограничениях предлагаемой системы обнаружения, подчёркивая её потенциал для повышения безопасности "умного дома".

A. Преимущества

- **Облегчённый алгоритм обнаружения**: Предлагаемый алгоритм разработан таким образом, чтобы быть облегчённым, что делает его подходящим для устройств Интернета вещей с ограниченными ресурсами. Это гарантирует, что механизм обнаружения не будет чрезмерно нагружать устройства, которые он призван защищать.
- **Универсальность протокола**: Алгоритм учитывает множество протоколов связи (TCP, UDP, MQTT), что повышает его применимость к различным типам интеллектуальных устройств и конфигурациям сетей.
- **Двухэтапное обнаружение подход**: использование двухэтапного обнаружения подход позволяет повысить точность определения потребления энергии ударов при минимальном количестве ложных срабатываний. Этот метод позволяет как быстро провести первоначальное обнаружение, так и детальный анализ.
- **Оповещения в режиме реального времени**: Платформа оперативно оповещает администраторов об обнаружении атаки, обеспечивая быстрое реагирование и смягчение потенциальных угроз.
- **Эффективное обнаружение аномалий**: измеряя скорость приёма пакетов и анализируя структуру энергопотребления, алгоритм эффективно выявляет отклонения от нормального поведения, которые указывают на кибератаки.

B. Недостатки

- **Ограниченные сценарии атак**: Экспериментальная установка ориентирована только на определённые типы атак, что ограничивает возможность обобщения результатов на другие потенциальные векторы атак, не охваченные в исследовании.
- **Проблемы с масштабируемостью**: хотя алгоритм разработан таким образом, чтобы быть лёгким, его

масштабируемость в более крупных и сложных средах "умного дома" с большим количеством устройств и различными условиями сети может потребовать дальнейшей проверки.

- **Зависимость от исходных данных**: Эффективность механизма обнаружения зависит от точных базовых измерений скорости приёма пакетов и энергопотребления. Любые изменения в нормальных условиях эксплуатации устройств могут повлиять на исходные данные, потенциально приводя к ложноположительным или отрицательным результатам.
- **Ограничения ресурсов**: несмотря на легковесность, алгоритм по-прежнему требует вычислительных ресурсов, что может стать проблемой для устройств с крайне ограниченными ресурсами. Постоянный мониторинг и анализ также могут повлиять на срок службы батареи и производительность этих устройств.

III. Предлагаемый алгоритм

В работе подчёркивается роль алгоритмов машинного обучения (ML) в системах обнаружения вторжений (IDS) и проблемы, связанные с их развёртыванием на устройствах Интернета вещей с ограниченными ресурсами.

A. Пакетные измерения

- **Скорость приёма пакетов (PRR)**: обсуждается использование скорости приёма пакетов (PRR) в качестве ключевого показателя для обнаружения атак с энергопотреблением. PRR определяется как отношение успешно принятых пакетов к общему количеству пакетов, отправленных по сети.
- **Учёт протокола**: Алгоритм учитывает различные протоколы связи, включая TCP, UDP и MQTT, для измерения PRR. Каждый протокол обладает уникальными характеристиками, влияющими на передачу и приём пакетов.
- **Обнаружение аномального поведения**: Отслеживая PRR, алгоритм может выявлять отклонения от нормального поведения, которые могут указывать на наличие атаки. Значительное снижение PRR может быть признаком продолжающейся атаки на потребление энергии.

B. Измерения энергии

- **Анализ энергопотребления**: основное внимание уделяется анализу моделей энергопотребления интеллектуальных устройств для обнаружения аномалий. Алгоритм измеряет энергию, потребляемую устройствами, с течением времени и сравнивает её с ожидаемыми уровнями потребления.
- **Краткосрочные и долгосрочные измерения**: Предлагаемый метод использует двухэтапный подход с короткими и долгосрочными интервалами. В первом случае используется для первоначального, приблизительного обнаружения потенциальных атак, в то время как во втором – обеспечивается более подробный анализ для подтверждения наличия атаки.
- **Обнаружение конкретных атак**: Измерения энергопотребления помогают идентифицировать конкретные типы атак, такие как атаки типа "Отказ в обслуживании" (DoS) или распределённые атаки типа "Отказ в обслуживании" (DDoS), путём обнаружения необычных скачков или падений энергопотребления.

IV. Эксперименты

Эксперименты проводились в моделируемой среде "умного дома" с различными устройствами Интернета вещей, и для оценки предлагаемой системы обнаружения были смоделированы различные типы атак с энергопотреблением. Результаты показывают, что алгоритм дерева решений (DT), развёрнутый на устройстве, обеспечивает лучшую производительность с точки зрения времени вывода и энергопотребления по сравнению с другими моделями ML.

A. Экспериментальная установка

- **Испытательный стенд для умного дома**: Эксперименты проводились в моделируемой среде "умного дома", состоящей из различных устройств Интернета вещей, таких как интеллектуальные светильники, камеры видеонаблюдения и интеллектуальные колонки, взаимодействующие по различным протоколам (TCP, UDP, MQTT).
- **Сценарии атак**: Авторы смоделировали различные типы атак с энергопотреблением, такие как атаки типа "Отказ в обслуживании" (DoS), распределённый отказ в обслуживании (DDoS) и DDoS-атаки на основе энергопотребления (EC-DDoS), чтобы оценить эффективность предлагаемой системы обнаружения.
- **Базовые измерения**: Базовые скорости приёма пакетов (PRR) и уровни энергопотребления были установлены для интеллектуальных устройств в нормальных условиях эксплуатации, чтобы служить ориентиром для обнаружения аномалий.
- **Показатели производительности**: определение показателей производительности: точность обнаружения, частота ложноположительных срабатываний и вычислительные издержки, для оценки эффективности алгоритма.

B. Результаты и анализ

- **Анализ скорости приёма пакетов**: анализируется изменения скорости приёма пакетов (PRR), наблюдаемые во время моделируемых атак, демонстрируя способность алгоритма обнаруживать отклонения от нормального поведения.
- **Анализ энергопотребления**: анализ моделей энергопотребления интеллектуальных устройств подчёркивает способность алгоритма выявлять аномальное энергопотребление, указывающее на атаки.

- **Оценка двухэтапного подхода**: оценка эффективности предлагаемого подхода в рамках использования короткого промежутка времени для первоначального грубого обнаружения и более длительного промежутка времени для детального анализа, с точки зрения повышения точности обнаружения и уменьшения количества ложных срабатываний.
- **Наблюдения, относящиеся к конкретному протоколу**: Результаты могут включать наблюдения, относящиеся к различным протоколам связи (TCP, UDP, MQTT), использованным в экспериментах, и обсуждение их влияния на скорость приёма пакетов и структуру энергопотребления во время атак.
- **Оценка производительности**: оценка производительности алгоритма на основе определённых показателей, таких как точность обнаружения, частота ложноположительных срабатываний и вычислительные издержки, сравнивая её с существующими методами или базовыми показателями.

V. Заключение

В нем подчёркивается эффективность предлагаемой облегчённой системы обнаружения при выявлении кибератак на интеллектуальные устройства, связанных с потреблением энергии, подчёркивается её высокая точность обнаружения и низкий уровень ложноположительных результатов.

- **Краткое изложение выводов**: подчёркивается успешное использование скорости приёма пакетов (PRR) и моделей энергопотребления для обнаружения аномалий.
- **Производительность алгоритма**: подчёркивается высокая точность обнаружения и низкая частота ложных срабатываний, достигаемые двухэтапным подходом к обнаружению.
- **Масштабируемость и эффективность**: обсуждаются масштабируемость и эффективность фреймворка в реальных средах "умного дома", отмечается его пригодность для устройств Интернета вещей с ограниченными ресурсами.
- **Направления будущих исследований**: предлагаются направления будущих исследований:
  - Расширение фреймворка для охвата широкого спектра типов атак и умных устройств.
  - Усовершенствование алгоритма для повышения скорости обнаружения и снижения вычислительных затрат.
  - Интеграция дополнительных источников данных: сетевой трафик и журналы поведения устройств, для расширения возможностей обнаружения.
  - Использование передовых методов машинного обучения для дальнейшего повышения точности и надёжности системы обнаружения.
- **Сравнение с существующими методами**: сравнивается подход с существующими методами обнаружения аномалий, подчёркивая преимущества своего лёгкого двухэтапного метода с точки зрения точности, эффективности и пригодности для устройств с ограниченными ресурсами.
- **Практическое применение**: рассматриваются потенциальные практические применения платформы обнаружения, включая её внедрение в коммерческие системы "умного дома" и интеграцию с существующими решениями безопасности для обеспечения комплексной защиты от кибератак.

ХРОНИКИ КИБЕР-БЕЗОПАСНИКА