Impact Factor: 9.9 ISSN-L: 2544-980X

Проблемы, Связанные С Аномалиями В Сетевом Трафике

Хусанова Мохирахон Курбоналиевна [1], Абдулхамидова Нилуфар Кахрамоновна [2]

Аннотация: Статья посвящена проблемам, связанным с аномалиями в сетевом трафике, которые представляют собой значительную угрозу для информационной безопасности. Рассматриваются сложности, связанные с разнообразием аномалий, шумом в данных и изменчивостью сетевого трафика. Описаны современные методы обнаружения аномалий, включая машинное обучение и гибридные подходы, которые помогают повысить точность и адаптивность систем безопасности. Обсуждаются основные вызовы, такие как вычислительная сложность и необходимость адаптации к изменяющимся условиям сети, а также роль облачных технологий и AutoML в решении этих проблем.

Ключевые слова: Аномалии, сетевой трафик, обнаружение, машинное обучение, кибератаки, гибридные подходы.

Введение. В настоящее время одной из ключевых и быстро развивающихся областей в сфере информационной безопасности является обнаружение атак и предотвращение вторжений в компьютерные системы и корпоративные сети злоумышленниками. Для этой цели используется ряд специализированных алгоритмов и средств, основанных на поведенческих и сигнатурных методах для обнаружения известных и неизвестных атак, а также методах обнаружения аномальной активности, которые особенно полезны для выявления атак со стороны инсайдеров и нулевых дней.

Аномалия - отступление или уклонение от правила, поэтому аномальным называют все отступающее или уклоняющееся от правильного или нормального [1]. По своей сути анализ аномалий позволяет выявлять существенные отклонения трафика сетевых устройств от «нормального» профиля трафика для данного устройства или группы устройств. Как правило, шаблон «нормального» трафика сети составляется в течение определенного промежутка времени на основе статистических данных и обучающей выборки. Анализ [2] показывает, что для выявления плохого поведения и аномалий в большинстве случаев достаточно анализировать основные параметры трафика (телеметрию) и нет необходимости изучать содержимое каждого пакета. Примерами аномалий, обнаруженных на основе анализа телеметрии трафика, являются внезапное увеличение интенсивности трафика от рабочей станции или изменение структуры трафика в сравнении с обычными ежедневными показателями для данной сети или устройства. При обнаружении сетевой аномалии, с целью принятия решения о дальнейших действиях, необходимо тщательно изучить ее природу, потенциальную опасность и возможные последствия, т.е. решить задачу классификации.

Эта статья сосредоточена на проблемах, возникающих при использовании и анализе аномалий, и представляет современные способы их решения. Другой причиной беспокойства при работе с аномалиями в сетевом трафике будет:

- Разнообразие аномалий.
- Фоновый шум в сигнале.

[1] Старший преподаватель кафедры «Информационная безопасность» Ферганского филиала Ташкентского университета информационных технологий имени Мухаммад ал-Хорезми Фергана, Узбекистан
[2] Магистрант кафедры «Информационная безопасность» Ферганского филиала Ташкентского университета информационных технологий имени Мухаммад ал-Хорезми Фергана, Узбекистан

- Изменчивость сетевого трафика.

Разнообразие аномалий в контексте сетевого трафика относится к различным типам отклонений от нормального поведения или шаблонов данных, которые могут быть вызваны как вредоносными, так и незначительными событиями. Аномалии в сетевом трафике могут принимать различные формы, такие как резкие всплески трафика, задержки, абоминирующе подозрительные запросы или атаки типа DDoS. Каждая из них определяется определенными характеристиками. Например, всплески трафика могут быть вызваны резким увеличением интереса со стороны пользователей к предложениям, размещенным на сайте.

Попытки вторжения сочетаются с изменчивостью структур шаблонов, что может включать SQL-инъекции, атаки методом грубой силы и другие.

Атака с распределенной отказом в обслуживании (DDoS) использует экстремальный объем трафика, поступающего от множества распределенных источников, чтобы взломать сетевой ресурс цели.

Обнаружение аномалий классифицируется по ряду стратегий, которые могут обрабатываться с адаптивной способностью к множеству ситуаций. Общие методы — это машинное обучение, например, модели, которые были обучены с различными аномалиями, и гибридные методы, которые применяют методы статистического анализа и алгоритмы искусственного интеллекта.

Фоновый шум в сигнале — это случайные и непредсказуемые колебания, которые добавляются к основному сигналу в процессе его передачи или обработки. Он может быть вызван различными источниками, такими как атмосферные явления, электрические устройства, механические колебания и другие помехи, которые нарушают чистоту сигнала. В зависимости от частоты и интенсивности, фоновый шум может затруднять или искажать восприятие и анализ передаваемой информации. В телекоммуникациях, например, это может привести к снижению качества связи или ухудшению точности распознавания данных.

Фоновый шум в сетевом трафике включает:

- нагрузки, которые можно ожидать в организации в любой момент (например, во время праздников).
- нерелевантные оповещения из-за неполных или неполных источников информации.
- Фоновый шум, способный скрывать законные проблемы безопасности, такие как.

Изменчивость сетевого трафика: Сетевой трафик изменяется из-за: • Новых приложений или технологий, которые влияют на структуру данных. • Сезонных изменений, таких как пиковая нагрузка в праздники. • Разных моделей использования сети, которые меняются в зависимости от времени суток или региона. Такая изменчивость делает традиционные подходы, основанные на жестко заданных правилах, менее эффективными. Современные методы решают эту проблему за счет:

- Онлайн-обучения моделей машинного обучения, которые обновляются в реальном времени.
- Адаптивных алгоритмов, способных учитывать изменения в данных.
- Использования облачных решений, которые обеспечивают масштабируемость и возможность обработки изменчивого трафика. Эти подходы помогают эффективно выявлять аномалии, даже в условиях постоянного изменения сетевого окружения.

При этом для выявления потенциальных сетевых атак, наибольшее значение будут иметь такие признаки как источник возникновение, область проявления и характер изменения трафика. В таблице 1 представлено описание связи аномалий, классифицированных по причине возникновения и характеру изменений сетевого трафика.

Таблица 1

Тип и причина сетевой аномалии	***Описание***	***Характеристики изменений трафика***
Альфа-аномалия	Необычно высокий уровень трафика типа точка-точка	Выброс в представлении трафика байты/с, пакеты/с по одному доминирующему потоку источник-назначение. Небольшая продолжительность (до 10 минут)
DoS-атака, DDoS-атака	Распределённая атака типа отказ в обслуживании на одну жертву	Выброс в представлении трафика пакеты/с, потоки/с, от множества источников к одному адресу назначения.
Перегрузка	Необычно высокий спрос на один сетевой ресурс или сервис	Скачок в трафике по потокам/с к одному доминирующему IP-адресу и доминирующему порту. Обычно кратковременная аномалия.
Сканирование сети/портов	Сканирование сети по определённым открытым портам или сканирование одного хоста по всем портам с целью поиска уязвимости ОС	Скачок в трафике по потокам/с, с несколькими пакетами в потоках от одного доминирующего IP-адреса.
Деятельность червей	Вредоносная программа, которая самостоятельно распространяется по сети и использует уязвимости ОС	Выброс в трафике без доминирующего адреса назначения, но всегда с одним или несколькими доминирующими портами назначения
Точка-мультиточка	Распространение контента от одного сервера многим пользователям	Выброс в пакетах, байтах от доминирующего источника к нескольким назначениям, все к одному хорошо известному порту.
Отключения	Сетевые неполадки, которые вызывают падение в трафике между одной парой источник-назначение	Падение трафика по пакетам, потокам и байтам обычно до нуля. Может быть долговременным и включать все потоки источник-назначение от или к одному маршрутизатору.
Переключения потока	Необычное переключение потоков трафика с одного входящего маршрутизатора на другой	Падение в байтах или пакетах в одном потоке трафика и выброс в другом. Может затрагивать несколько потоков трафика.

Предложенный подход к классификации может использоваться при проведении исследований сетевых аномалий, а также процессе разработки моделей и алгоритмов обнаружения аномалий и атак.

Обсуждение. Аномалии в сетевом трафике остаются одной из главных угроз для сетевой безопасности. Традиционные методы обнаружения не способны справляться с эволюцией угроз, особенно с учётом увеличения сложности атак. Методы машинного обучения, хотя и обладают высоким потенциалом, требуют значительных вычислительных ресурсов. Гибридные подходы, которые комбинируют лучшие черты статистических и интеллектуальных систем, предлагают наиболее перспективные решения, но остаются сложными в реализации. Также аномалии сетевого трафика являются серьёзной угрозой для кибербезопасности, и их выявление требует современных подходов. Основные проблемы включают разнообразие типов аномалий, шум в данных и изменчивость сетевого поведения. Современные методы, такие как

машинное обучение, гибридные системы и адаптивные алгоритмы, обеспечивают более точное и быстрое обнаружение отклонений.

Классификация аномалий, предложенная в статье, способствует разработке эффективных систем, адаптированных к различным сценариям. Основной вызов остаётся в сложности реализации этих систем и высоких вычислительных затратах. Будущее за облачными технологиями, AutoML и гибридными подходами, которые объединяют точность, адаптивность и масштабируемость.

Выводы. Выявление аномалий в сетевом трафике — ключевая задача для обеспечения сетевой безопасности. Традиционные методы обеспечивают базовый уровень защиты, но современные угрозы требуют применения более сложных решений, таких как алгоритмы машинного обучения и гибридные системы. Для дальнейшего прогресса в этой области необходимо развивать методы, способные обрабатывать большие объёмы данных в реальном времени и минимизировать число ложных срабатываний.

Будущее технологий обнаружения аномалий лежит в облачных решениях и автоматизированных инструментах машинного обучения, которые обеспечивают точность, масштабируемость и способность к самонастройке для защиты современных сетей от сложных угроз.

Список литературы

1. Хусанова, М. К. (2022). Сетевая безопасность и мониторинг. *Research Focus*, *1*(4), 177-183.
2. Абдулхамидова, Н. (2024). ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ СЕТЕВОГО ТРАФИКА: ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ. Research and implementation, 2(2), 35-37.
3. Khusanova, M. K., & Muminova, M. M. (2023). SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)-MONITORING. *Horizon: Journal of Humanity and Artificial Intelligence*, *2*(5), 682-688.
4. Хусанова, М., Ганиева, Ш, Н., Садирова, Х. (2023, October). ПРОТОКОЛЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ОБЕСПЕЧЕНИИ СЕТЕВОЙ БЕЗОПАСНОСТИ: АНАЛИЗ И ЭФФЕКТИВНОСТЬ. In Conference on Digital Innovation:" Modern Problems and Solutions".
5. Хусанова, М., Ганиева, Ш, Н., Садирова, Х. (2023, October). ПРОТОКОЛЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ОБЕСПЕЧЕНИИ СЕТЕВОЙ БЕЗОПАСНОСТИ: АНАЛИЗ И ЭФФЕКТИВНОСТЬ. In Conference on Digital Innovation:" Modern Problems and Solutions".
6. Хусанова, М., Ганиева, Ш., & Садирова, Х. (2023, October). ТЕХНОЛОГИЧЕСКИЕ ИННОВАЦИИ И РАЗВИТИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. In Conference on Digital Innovation:" Modern Problems and Solutions".
7. Sadirova, X., & Ganiyeva, S. (2023, October). Cloud-Based Security Solutions: Protecting Networks in the Era of Digital Transformation. In Conference on Digital Innovation:" Modern Problems and Solutions".
8. Mamadaliyeva, L., Xusanova, M., & Sadirova, X. (2023, October). Endpoint Protection in the Modern Network Landscape: Securing Devices Beyond the Perimeter. In Conference on Digital Innovation:" Modern Problems and Solutions".
9. Садирова, Х., & Набижонов, Р. (2023). Методы создания корпоративной системы безопасности для обеспечения информационной безопасности. Journal of technical research and development, 1(2), 170-174.
10. Sadirova, X., Qadamova, Z., & Tojidinov, A. (2023). Qisman tarmoqli shovqin siqilish muhitida shifrlangan tarqalish kodlari bilan chastota sakrashining tarqalishi spektrining xavfsizligi. Journal of technical research and development, 1(2), 69-74.

11. Sadirova, X., & Ergasheva, A. (2023). TA’LIMDA INNOVATSION O ‘QITISH TEXNOLOGIYALARI. Engineering problems and innovations.
12. Sadirova, X., & Ergasheva, A. (2023). AXBOROTNING MAXFIYLIGINI, YAXLITLIGINI VA FOYDALANUVCHANLIGINI BUZISH USULLARI. Engineering problems and innovations.
13. Mamadaliyeva, L., Xusanova, M., & Sadirova, X. (2023, October). Endpoint Protection in the Modern Network Landscape: Securing Devices Beyond the Perimeter. In Conference on Digital Innovation:" Modern Problems and Solutions".