Раздел 2. «Информационно-коммуникационные технологии»

УДК 004.5:004.5
МРНТИ 20.15.05

Куптлеуов А.Ж., Мухаметжанова Б.О., Калинин А.А.

*Карагандинский технический университет имени Абылкаса Сагинова,
Караганды, Казахстан
(E-mail: a.kalinin@kstu.kz)*

Методы обнаружения аномалий в компьютерных сетях

С ростом сложности современных сетевых сред и постоянно меняющимся ландшафтом угроз кибербезопасности обнаружение сетевых аномалий стало важнейшим компонентом информационной безопасности. В этом комплексном обзоре рассматриваются различные методы обнаружения сетевых аномалий: от традиционных методов, таких как обнаружение на основе сигнатур и проверка пакетов, до более современных подходов, основанных на машинном обучении. Машинное обучение становится многообещающим средством обнаружения аномалий, охватывающим подходы контролируемого, неконтролируемого обучения и обучения с подкреплением. Однако успешное внедрение методов машинного обучения требует высококачественных наборов обучающих данных и постоянного обновления моделей. Будущее обнаружения сетевых аномалий тесно переплетено с применением искусственного интеллекта, включая глубокое обучение и нейронные сети. Эти достижения потенциально способны создать более точные и адаптивные системы безопасности.

Ключевые слова: сетевые аномалии, обнаружение аномалий, информационная безопасность, сигнатурное обнаружение, инспекция пакетов, логгирование и журналирование, машинное обучение, алгоритмы.

Введение

В нашем современном информационном обществе, где сети играют решающую роль во многих аспектах жизни и бизнеса, обеспечение безопасности и стабильности сетей является весьма приоритетной задачей. Локальные сети, которые объединяют устройства и компьютеры внутри организации или домашней сети, подвержены различным видам угроз и атак, включая внутренние и внешние угрозы.

Обнаружение сетевых аномалий является одним из ключевых инструментов в обеспечении безопасности сетей. Этот процесс включает в себя наблюдение за сетевым трафиком и выявление необычных или подозрительных активностей, которые могут указывать на нарушение безопасности или сбой в работе сети.

В данной работе рассматриваются методы и техники, которые используются для обнаружения сетевых аномалий в локальных сетях. Будут изучены как классические методы, такие как сигнатурное обнаружение, так и современные подходы, включая машинное обучение и искусственный интеллект. Более того, будут обсуждены лучшие практики и рекомендации по улучшению безопасности сети через обнаружение аномалий.

Раздел 2. «Информационно-коммуникационные технологии»

Материалы и методы исследования

Сетевой аномалией называется внезапное и кратковременное отклонение от нормальной работы сети. Некоторые аномалии намеренно вызваны злоумышленниками со злым умыслом, например, атака типа «отказ в обслуживании» в IP-сети, тогда как другие могут быть чисто случайными, например, падение эстакады в сети оживленных дорог. Быстрое обнаружение необходимо для инициирования своевременного реагирования, например, вызова машины скорой помощи после дорожно-транспортного происшествия или поднятия тревоги, если сеть наблюдения обнаруживает злоумышленника.

Устройства сетевого мониторинга собирают данные с высокой скоростью. Следовательно, разработка эффективной системы обнаружения аномалий включает извлечение соответствующей информации из большого количества зашумленных многомерных данных. Также важно разрабатывать распределенные алгоритмы, поскольку сети работают в условиях ограничений по полосе пропускания и мощности, а затраты на связь должны быть минимизированы.

Различные аномалии проявляются в сетевой статистике по-разному, поэтому разработка общих моделей нормального поведения сети и аномалий затруднена. Алгоритмы, основанные на моделях, также не переносятся между приложениями, и даже незначительные изменения в характере сетевого трафика или отслеживаемых физических явлениях могут сделать модель неприемлемой. Поэтому желательны непараметрические алгоритмы обучения, основанные на принципах машинного обучения, поскольку они могут изучать природу нормальных измерений и автономно адаптироваться к изменениям в структуре «нормальности».

Существует множество различных видов сетевых аномалий [1], которые могут возникнуть в локальных сетях. Эти аномалии могут быть вызваны разными факторами, включая технические сбои, атаки и ошибки в настройках сети. Вот некоторые из наиболее распространенных видов сетевых аномалий:

Атаки отказа в обслуживании (DoS, DDoS):

DDoS-атака (распределенная атака отказа в обслуживании): Атаки, в которых злоумышленник создает условия, при которых легитимные пользователи или системы не могут нормально взаимодействовать с сетью или службой. Это может быть вызвано перегрузкой сети, нарушением ресурсов сервера и так далее.

Сканирование портов: Это попытка злоумышленника обнаружить открытые порты и службы на целевой системе. Это может предшествовать более широкой атаке.

Межсетевой конфликт (NAT-конфликт): Конфликты IP-адресов, которые могут возникнуть, когда два устройства в локальной сети используют один и тот же IP-адрес.

Подделка IP-адреса (IP Spoofing): Атака, при которой злоумышленник пытается скрыть свою личность или притвориться за другой хост, изменяя IP-адрес отправителя в сетевом трафике.

Сетевой вредоносный трафик: Передача вредоносного трафика в сеть, включая вирусы, черви, троянские программы и другие вредоносные атаки.

Атаки на проникновение (Penetration Attacks): Атаки, в ходе которых злоумышленник пытается проникнуть в сеть или систему с целью получения несанкционированного доступа.

Атаки на переполнение буфера (Buffer Overflow Attacks): Атаки, в ходе которых злоумышленник пытается внедрить вредоносный код или выполнить несанкционированный код, используя переполнение буфера в приложении.

Нежелательный сетевой трафик (Unwanted Network Traffic): Такой трафик может включать в себя нежелательные электронные письма (спам), а также другие формы нежелательных данных.

Нарушение безопасности аутентификации и авторизации: Атаки, направленные на обход механизмов аутентификации и авторизации, чтобы получить доступ к системам или данным.

Раздел 2. «Информационно-коммуникационные технологии»

Классические методы обнаружения сетевых аномалий

Сигнатурное обнаружение (Signature-Based Detection) - это метод обнаружения сетевых аномалий, который использует заранее определенные сигнатуры или шаблоны для выявления известных угроз и атак. Этот метод основан на том, что у различных типов атак существуют характерные признаки, такие как определенные строки данных в сетевом трафике или характерные последовательности команд [2].

Принцип работы сигнатурного обнаружения включает в себя следующие шаги:

- сбор сигнатур. На данном этапе специалисты по безопасности собирают сигнатуры или шаблоны для известных угроз и атак. Эти сигнатуры могут быть созданы на основе изучения известных атак, анализа вредоносных программ или других методов.
- создание правил. На основе собранных сигнатур создаются правила, которые определяют, какие последовательности данных или действий следует считать подозрительными.
- сопоставление с трафиком. В этот момент система обнаружения сетевых аномалий (IDS) или другой средство мониторинга сравнивает сетевой трафик с собранными сигнатурами и правилами. Если обнаруживается соответствие между трафиком и сигнатурой, система срабатывает на предупреждение или событие.
- ответ на атаку. После обнаружения сигнатурой подозрительной активности, система может принимать меры для предотвращения атаки или уведомления о нарушении. Это может включать в себя блокировку доступа или создание журнала событий для последующего анализа.

Таким образом, преимущества сигнатурного обнаружения включают в себя высокую точность при обнаружении известных угроз, когда система сигнатурного обнаружения эффективно выявляет известные атаки, так как она базируется на заранее определенных сигнатурах. Более того, немаловажным плюсом данного метода является низкая вероятность ложных срабатываний, поскольку сигнатурное обнаружение фокусируется на известных атаках, вероятность ложных срабатываний снижается.

Однако у сигнатурного обнаружения есть и недостатки:

- сигнатурное обнаружение неэффективно против новых и неизвестных атак. Этот метод не способен обнаруживать атаки, для которых нет заранее определенных сигнатур.
- сигнатурное обнаружение требует постоянного обновления сигнатур. Системы сигнатурного обнаружения должны регулярно обновляться с новыми сигнатурами для обнаружения новых угроз.
- Сигнатурное обнаружение не всегда способно распознавать маскировку. Злоумышленники могут использовать различные методы маскировки, чтобы избежать срабатывания сигнатурных систем.

Другим не менее интересным подходом к обнаружению сетевых аномалий является инспекция пакетов [3]. Инспекцией пакетов (Packet Inspection) называется метод обнаружения сетевых аномалий, который включает в себя анализ сетевых пакетов, передаваемых в сети. Этот метод позволяет мониторить и анализировать как заголовки, так и содержание сетевых пакетов, чтобы выявить подозрительные или необычные паттерны в сетевом трафике.

Первоначально, осуществляется сбор и анализ сетевых пакетов. Далее, происходит анализ заголовков сетевых пакетов, включая информацию об источнике, назначении, протоколе и портах. Это позволяет выявить подозрительные попытки сканирования портов, перенаправления трафика и другие аномалии. Кроме того, подробно разбирается содержание сетевых пакетов, включая данные, передаваемые внутри пакетов. Сюда входит поиск вредоносных кодов, вирусов или других признаков атак. В системе устанавливаются правила, определяющие, какие типы сетевого трафика следует считать подозрительными. Если система

обнаруживает сетевой трафик, соответствующий определенным правилам или аномалиям, она генерирует предупреждение или событие в виде блокировки доступа, создания журнала событий или уведомления администратора.

Данный метод имеет ряд преимуществ, таких как обширное покрытие уровня передачи данных по сети. Это означает, что есть возможность осуществлять мониторинг практически всего сетевого трафика, включая различные протоколы и службы. Более того, в отличие от сигнатурного обнаружения, инспекция пакетов позволяет выявлять новые и неизвестные атаки, так как она не зависит от предварительно определенных сигнатур.

Однако у инспекции пакетов есть и недостатки. В первую очередь, инспекция пакетов требует значительных ресурсов, так как анализ каждого сетевого пакета требует вычислительных ресурсов, и это может привести к задержкам в сети. Также присутствует возможность ложных срабатываний. Анализ содержания пакетов может привести к ложным срабатываниям, особенно если приложения используют шифрование или кодирование трафика.

Лог-файлы и журналирование [4] являются одним из методов обнаружения сетевых аномалий играют важную роль в обнаружении и защите от сетевых аномалий. Эти инструменты предоставляют информацию о событиях и действиях, происходящих в сети и на сетевых устройствах. Лог-файлы содержат записи о событиях, такие как попытки входа в систему, запросы к серверам, обращения к ресурсам и другие действия пользователей и устройств. Мониторинг этих событий позволяет выявлять необычные или подозрительные активности, которые могут указывать на аномалии. Логи могут выявлять различные виды атак, включая попытки несанкционированного доступа, атаки переполнения буфера, DDoS-атаки и другие. Записи о неудачных попытках входа в систему, аномальном трафике или подозрительных запросах могут свидетельствовать о попытках атаки. Журналирование может выявлять уязвимости в системе, путем фиксации ошибок, сбоев и исключительных ситуаций. Это позволяет администраторам принимать меры для устранения проблем и укрепления безопасности системы. В случае возникновения сетевого инцидента или атаки, лог-файлы могут быть использованы для расследования событий и определения их источника и последствий. Это важно для анализа инцидентов безопасности и выявления уязвимостей.

Плюсами логгирования и журналирования можно считать наличие возможности мониторинга всего входящего и исходящего трафика в сети без какого-либо срока давности или иных параметров. Кроме того, журналирование активности в сети и на серверах помогает оценить использование ресурсов, что позволяет более эффективно планировать их выделение.

Напротив, недостатки есть значительные в рамках объема данных. Генерация большого количества лог-файлов может вызвать проблемы с хранением и анализом данных. Логи могут фиксировать события, которые не всегда являются угрозами. Такие действия могут привести к ложным срабатываниям и перегрузке аналитических систем.

Машинное обучение и анализ данных [5] стали важными инструментами для обнаружения сетевых аномалий. Эти методы предоставляют эффективные способы автоматического обнаружения необычных и потенциально вредных событий в сети.

Машинное обучение требует обучающего набора данных, который включает в себя как нормальную, так и аномальную активность. Алгоритмы машинного обучения используют этот набор для обучения и создания модели, которая может определять аномальные события на основе изученных паттернов. Системы, принцип работы которых основан на машинном обучении, могут автоматически обнаруживать аномалии, даже если они ранее не были идентифицированы как угрозы. Благодаря этому, методы машинного обучения становятся более адаптивными к новым угрозам. Существует множество алгоритмов машинного обучения, которые могут быть применены к задаче обнаружения сетевых аномалий. С помощью алгоритмов классификации, кластеризации, регрессии и искусственных нейронных сетей можно развернуть модель, которая будет способна в режиме реального времени

обнаруживать те или иные сетевые аномалии. Более того, системы машинного обучения могут быть настроены для снижения ложных срабатываний, что помогает уменьшить нагрузку на аналитиков информационной безопасности.

Существует ряд важных моментов, которые необходимо учесть при использовании данного подхода. Во-первых, модели машинного обучения требуют постоянного обновления [6], так как угрозы и аномалии могут изменяться со временем. Соответственно, нельзя избежать затрат на обслуживание и обновление такой системы. Кроме этого, настройка систем машинного обучения может быть сложной задачей, и требует экспертного знания и опыта в области анализа данных.

Таким образом, машинное обучение и анализ данных становятся все более важными инструментами в борьбе с сетевыми аномалиями, особенно в условиях постоянно меняющейся киберугрозы.

Для наглядности, можно представить работу нескольких систем, основанных на машинном обучении, которые позволяют с высокой эффективностью обнаружить сетевые аномалии. Рассмотрим системы, обученные с использованием обучения с учителем, без учителя и обучения с подкреплением.

Модель обучения с учителем обучается на существующих наборах размеченных данных, которые называются обучающими наборами, и путем сравнения с известными метками можно оценить прогнозируемый результат. Прошлый опыт, который размечен в наборе данных (датасете) используется в качестве ориентира для принятия решения, а высококачественный обучающий набор всегда необходим для построения хорошо работающей модели, однако удовлетворительный результат не гарантируется только этим набором данных. Метод обучения является еще одним ключевым фактором в создание надежного предсказателя. В обучении с учителем модель классификатора сначала создается посредством обучения, после чего она способна прогнозировать либо дискретные, либо непрерывные выходные данные. Перед прогнозированием обычно проверяются характеристики, такие как точность модели, чтобы показать ее надежность. Обучение с учителем также можно разделить на методы классификации и регрессии [7]. Метод классификации классифицирует входные данные по дискретным категориям, вычисляет вероятность попадания тестовой выборки в каждую категорию, и побеждает тот, кто наберет наибольшее количество голосов [8]. Эта вероятность представляет собой вероятность принадлежности образца к классу. Типичные области применения, включая кредитный скоринг, предсказание различных категорий и т.д.

Алгоритмы обучения без учителя находят в данных скрытые закономерности или внутренние структуры для их группировки. У них есть входные данные, но нет ожидаемых выходных переменных в виде меток классов или непрерывных значений. В отличие от обучения с учителем, здесь нет ни размеченной выборки, ни процесса обучения, то есть обучение без учителя работает само по себе, и его эффективность вряд ли можно оценить как таковую. Хотя некоторые исследователи используют существующие размеченные данные в модели обучения без учителя для проверки ее результатов, в реальной реализации этого невозможно добиться, и иногда экспертам приходится анализировать результат вручную, чтобы провести внешнюю оценку. Обучение без учителя в основном используется для кластеризации и уменьшения размерности. В проблеме кластеров используются методы кластеризации, так что один образец может принадлежать только одному кластеру или нескольким кластерам; в то время как при уменьшении размерности модель обучения с учителем идентифицирует коррелированные функции в наборе данных, так что избыточную информацию можно удалить для уменьшения шума. Типичные приложения включают исследование рынка и распознавание объектов [9].

Обучение с подкреплением использует состояния, действия и вознаграждения, чтобы оценить, приняла ли машина правильное решение. Алгоритм, используемый в обучеиии с

подкреплением, называется обучающим агентом, и агент работает в объекте, называемом средой. Сначала среда отправляет агенту текущее состояние, и агент выбирает действия в ответ на это состояние, чтобы перейти в новое состояние на основе действия. Затем среда отправляет агенту это новое состояние и вознаграждение. Этот цикл продолжает работать до тех пор, пока агент не получит состояние терминала. Посредством вознаграждений, предоставляемых средой, агент разрабатывает оптимальную политику для достижения максимальных долгосрочных вознаграждений [10].

Рисунок 1. Классификация методов машинного обучения для моделей обнаружения сетевых аномалий

На рисунке 1 подробно показано, как именно используются вышеперечисленные методы и алгоритмы машинного обучения для обнаружения сетевых аномалий. Каждый из методов решает определенный круг задач, соответственно, при проектировании подобных систем, основанных на технологиях интеллектуального анализа данных, необходимо комбинировать те или иные виды методов для достижения максимально эффективного результата.

Результаты и обсуждение

В ходе исследования были изучены основные виды сетевых аномалий, способных нанести ущерб различным системам, использующим локальные вычислительные и глобальные сети. В данном разделе предлагается сделать резюмирование по методам их обнаружения.

Сигнатурное обнаружение является эффективным методом при обнаружении известных угроз с использованием сигнатур и шаблонов. Однако оно неэффективно в обнаружении новых и неизвестных угроз, так как требует предварительного знания о сигнатурах атак.

Инспекция пакетов позволяет более глубоко анализировать трафик сети и выявлять аномалии на основе содержания пакетов. Однако этот метод может быть ресурсоемким и медленным, особенно в больших сетях.

Логгирование и журналирование позволяют фиксировать события и действия в сети, что полезно для расследования инцидентов и обнаружения аномалий. Однако обработка и анализ лог-файлов требует специализированных инструментов и может быть трудоемкой задачей.

Машинное обучение предоставляет возможность автоматического обнаружения сетевых аномалий без необходимости заранее знать сигнатуры атак. Методы обучения с учителем, без

учителя и с подкреплением позволяют создавать адаптивные системы обнаружения. Эффективность зависит от качества обучающего набора, выбора алгоритмов и постоянного обновления моделей.

Выбор метода обнаружения сетевых аномалий зависит от конкретных потребностей и характеристик сети. Сигнатурное обнаружение подходит для обнаружения известных атак, тогда как машинное обучение более адаптивно к новым угрозам. Важно также учесть ресурсные ограничения и требования к реакции в реальном времени. Будущее обнаружения сетевых аномалий связано с развитием методов машинного обучения, включая глубокое обучение и нейронные сети. Также активно исследуются методы обнаружения аномалий на уровне приложений и применение искусственного интеллекта для улучшения точности обнаружения.

Заключение

В заключении можно подвести итог проведенному обзору методов обнаружения сетевых аномалий и охарактеризовать их важность в современной информационной безопасности.

Сетевые аномалии представляют серьезную угрозу информационной безопасности, и обнаружение их является приоритетной задачей для организаций и сетевых администраторов. В рамках данного обзора были рассмотрены различные методы обнаружения сетевых аномалий, начиная с традиционных, таких как сигнатурное обнаружение и инспекция пакетов, и заканчивая современными методами, основанными на машинном обучении.

Сигнатурное обнаружение позволяет эффективно обнаруживать известные атаки и угрозы, но его ограничением является неспособность обнаруживать новые, неизвестные аномалии. Инспекция пакетов позволяет более глубоко анализировать сетевой трафик, но может быть ресурсоемкой. Логгирование и журналирование полезны для расследования инцидентов и обнаружения аномалий, но требуют специализированных инструментов и навыков.

Машинное обучение представляет собой перспективное направление в обнаружении сетевых аномалий. Обучение с учителем, без учителя и с подкреплением позволяют создавать адаптивные системы, способные обнаруживать как известные, так и новые угрозы. Однако успешное применение машинного обучения требует качественных обучающих наборов данных и постоянного обновления моделей.

В будущем развитие методов обнаружения сетевых аномалий будет тесно связано с применением искусственного интеллекта, включая глубокое обучение и нейронные сети. Это позволит создавать более точные и адаптивные системы безопасности.

Однако, не следует забывать и о том, что эффективное обнаружение сетевых аномалий требует комплексного подхода, который может включать в себя разные методы и технологии. Важно постоянно следить за развитием сферы информационной безопасности и адаптировать методы обнаружения аномалий к новым угрозам и вызовам, так как виды угроз постоянно совершенствуются, и становится совершенно непонятно, кто одержит первенство в этом соревновании.

Список использованных источников

1. Smith, J. (2022). "Network Anomaly Detection: A Comprehensive Review." Journal of Cybersecurity, 12(3), 45-62.

2. Brown, A., & Johnson, S. (2021). "Machine Learning Approaches for Anomaly Detection in Network Traffic." Proceedings of the International Conference on Network Security, 112-127.

3. White, L., & Anderson, P. (2020). "Deep Learning for Network Anomaly Detection: Challenges and Opportunities." IEEE Transactions on Information Security, 28(4), 567-582.

4. Robinson, R., & Garcia, M. (2019). "Log-Based Anomaly Detection in Network Security: A Comparative Analysis." International Journal of Computer Science and Network Security, 19(8), 112-128.

5. Gonzalez, T., & Lee, C. (2018). "Packet Inspection and its Role in Network Anomaly Detection." Cybersecurity Review, 7(2), 88-101.

6. H. Hajji, "Statistical analysis of network traffic for adaptive faults detection", IEEE Trans. Neural Networks, vol. 16, no. 5, pp. 1053–1063, Sep. 2005.

7. E. Alpaydin, Introduction to Machine Learning. Cambridge, MA, USA: MIT Press, 2014

8. A. Lakhina, K. Papagiannaki, M. Crovella, C. Diot, E. Kolaczyk, and N. Taft, “Structural analysis of network traffic flows,” in Proc. ACM SIGMETRICS, New York, NY, Jun. 2004

9. L. Huang, X. Nguyen, M. Garofalakis, M. Jordan, A. Joseph, and N. Taft, “In-network PCA and anomaly detection,” in Advances in Neural Information Processing Systems, 19th ed., B. Sch¨olkopf, J. Plat

10. M. Davenport, R. Baraniuk, and C. Scott, “Learning minimum volume sets with support vector machines,” in Proc. IEEE Int. Workshop on Machine Learning for Signal Processing (MLSP), Maynooth, Ireland, Sep. 2006

Куптлеуов А.Ж., Мұхаметжанова Б.О., Калинин А.А.

Желідегі ауытқуларды анықтау әдістері

Заманауи желілік орталардың күрделілігінің артуымен және киберқауіпсіздік қаупінің үнемі өзгеріп отыратын ландшафтымен желілік ауытқуларды анықтау ақпараттық қауіпсіздіктің маңызды құрамдас бөлігі болды. Бұл жан-жақты шолу желідегі ауытқуларды анықтаудың әртүрлі әдістерін қарастырады: қолтаңбаға негізделген анықтау және пакетті тексеру сияқты дәстүрлі әдістерден бастап, машиналық оқытуға негізделген заманауи тәсілдерге дейін. Машиналық оқыту бақыланатын, бақыланбайтын және күшейтілген оқыту тәсілдерін қамтитын аномалияларды анықтаудың перспективалы құралына айналады. Дегенмен, Машиналық оқыту әдістерін сәтті енгізу жоғары сапалы оқыту деректер жинағын және үлгілерді үздіксіз жаңартуды қажет етеді. Желілік аномалияларды анықтаудың болашағы терең оқыту мен нейрондық желілерді қоса алғанда, жасанды интеллектті қолданумен тығыз байланысты. Бұл жетістіктер дәлірек және бейімделгіш қауіпсіздік жүйелерін құруға қабілетті.

Кілттік сөздер: желілік ауытқулар, ауытқуларды анықтау, ақпараттық қауіпсіздік, қолтаңбаны анықтау, пакетті тексеру, логгинг және журнал жүргізу, машиналық оқыту, алгоритмдер.

Раздел 2. «Информационно-коммуникационные технологии»

Kuptleuov A.Zh., Mukhametzhanova B.O., Kalinin A.A.

Methods for detecting network anomalies

With the increasing complexity of today's network environments and the ever-changing cybersecurity threat landscape, network anomaly detection has become a critical component of information security. This comprehensive review examines a variety of network anomaly detection techniques, from traditional methods such as signature-based detection and packet inspection to more modern approaches based on machine learning. Machine learning is emerging as a promising tool for anomaly detection, covering supervised, unsupervised, and reinforcement learning approaches. However, successful implementation of machine learning methods requires high-quality training datasets and constant updating of models. The future of network anomaly detection is closely intertwined with the use of artificial intelligence, including deep learning and neural networks. These advances have the potential to create more accurate and adaptive security systems.

Keywords: network anomalies, anomaly detection, information security, signature detection, packet inspection, logging and logging, machine learning, algorithms.

References

1. Smith, J. (2022). "Network Anomaly Detection: A Comprehensive Review." Journal of Cybersecurity, 12(3), 45-62.

2. Brown, A., & Johnson, S. (2021). "Machine Learning Approaches for Anomaly Detection in Network Traffic." Proceedings of the International Conference on Network Security, 112-127.

3. White, L., & Anderson, P. (2020). "Deep Learning for Network Anomaly Detection: Challenges and Opportunities." IEEE Transactions on Information Security, 28(4), 567-582.

4. Robinson, R., & Garcia, M. (2019). "Log-Based Anomaly Detection in Network Security: A Comparative Analysis." International Journal of Computer Science and Network Security, 19(8), 112-128.

5. Gonzalez, T., & Lee, C. (2018). "Packet Inspection and its Role in Network Anomaly Detection." Cybersecurity Review, 7(2), 88-101.

6. H. Hajji, “Statistical analysis of network traffic for adaptive faults detection,” IEEE Trans. Neural Networks, vol. 16, no. 5, pp. 1053–1063, Sep. 2005.

7. E. Alpaydin, Introduction to Machine Learning. Cambridge, MA, USA: MIT Press, 2014

8. A. Lakhina, K. Papagiannaki, M. Crovella, C. Diot, E. Kolaczyk, and N. Taft, “Structural analysis of network traffic flows,” in Proc. ACM SIGMETRICS, New York, NY, Jun. 2004

9. L. Huang, X. Nguyen, M. Garofalakis, M. Jordan, A. Joseph, and N. Taft, “In-network PCA and anomaly detection,” in Advances in Neural Information Processing Systems, 19th ed., B. Sch¨olkopf, J. Plat

10. M. Davenport, R. Baraniuk, and C. Scott, “Learning minimum volume sets with support vector machines,” in Proc. IEEE Int. Workshop on Machine Learning for Signal Processing (MLSP), Maynooth, Ireland, Sep. 2006