УДК: 004.056

Методы повышения безопасности протокола xray для защищённых сетевых туннелей

Заботкина Е. М., Тихомиров Д.С.
РТУ МИРЭА, г. Москва

В статье рассматриваются проблемы обеспечения скрытности и устойчивости протокола XRay — современного инструмента для построения защищённых сетевых туннелей. Несмотря на использование надёжных криптографических алгоритмов и поддержку протоколов TLS/XTLS, XRay остаётся уязвим к фингерпринтингу — методам идентификации зашифрованного трафика по статистическим и поведенческим признакам. Проведён анализ архитектуры XRay, методов обнаружения туннельного трафика средствами DPI, а также существующих подходов к имитации TLS-параметров. На основе выявленных уязвимостей предложен комплекс теоретических мер, направленных на повышение транспортной неотличимости XRay от легитимного HTTPS-трафика. Среди предложенных решений — динамическая имитация TLS-фингерпринтов, адаптивный padding, стохастическая модуляция временных интервалов и ротация ключей с поддержкой Perfect Forward Secrecy. Аналитическая оценка показала, что применение этих методов способно снизить вероятность корректного распознавания туннелей на 50–70 % при умеренных накладных расходах производительности. Результаты исследования могут быть использованы при разработке новых механизмов маскировки VPN-протоколов и построении систем передачи данных, устойчивых к современным методам анализа сетевого трафика.

1. Введение

В условиях стремительного развития сетевых технологий и расширения цифрового взаимодействия между пользователями возрастает потребность в эффективных и устойчивых механизмах защиты передаваемой информации. Современные угрозы кибербезопасности затрагивают не только содержимое передаваемых данных, но и сопровождающие их характеристики — метаданные, временные интервалы, сигнатуры пакетов и статистические признаки соединений. В этой связи актуальным направлением исследований становится повышение скрытности и криптографической стойкости протоколов, обеспечивающих защищённые сетевые туннели.

Одним из наиболее гибких и современных решений в этой области является протокол XRay, представляющий собой модульную платформу для организации зашифрованных каналов передачи данных. В отличие от классических защищённых сетевых туннелей, таких как OpenVPN или WireGuard, XRay ориентирован не только на обеспечение конфиденциальности, но и на сокрытие самого факта туннелирования. Благодаря поддержке транспортных слоёв TCP, QUIC и WebSocket, а также использованию протоколов VLESS и XTLS, XRay способен эффективно обходить ограничения сетевых фильтров и DPI-систем. Однако, несмотря на это, остаётся ряд уязвимостей, связанных с возможностью статистического анализа трафика и выявления характерных признаков туннеля.

Одной из наиболее существенных проблем является фингерпринтинг (traffic fingerprinting) — определение принадлежности зашифрованного потока к конкретному протоколу на основе анализа структурных и временных характеристик пакетов. Даже при полном шифровании содержимого злоумышленник или система мониторинга могут по

набору параметров TLS, последовательности handshake или частоте передачи данных установить, что соединение создано при помощи XRay. Такая особенность снижает уровень анонимности и делает возможным блокировку туннеля на уровне провайдера.

Таким образом, задача повышения безопасности XRay заключается не только в совершенствовании криптографических алгоритмов, но и в обеспечении его транспортной неотличимости от обычного легитимного трафика. Это требует разработки новых методов динамической обфускации, маскировки заголовков и стохастического изменения параметров передачи данных.

Цель данной работы — исследование существующих проблем безопасности протокола XRay и разработка методов повышения его устойчивости к выявлению по статистическим признакам. Для достижения цели предполагается рассмотреть архитектуру XRay, проанализировать типичные способы идентификации туннельного трафика, а также предложить меры по реализации динамического маскирования, направленные на снижение вероятности обнаружения защищённых сетевых туннелей в условиях современных систем сетевого анализа.

2. Основная часть

Обзор литературы и существующих реализаций XRay

Протокол XRay (часто упоминаемый как «project X», Xray-core) развился как продолжение и расширение идей V2Ray и Shadowsocks: цель — не просто шифрование трафика, а предоставление гибкого фреймворка для построения туннелей с возможностями обфускации, динамической маршрутизации и интеграции разных транспортов (TCP, UDP, WebSocket, QUIC и пр.). Официальные репозитории и документация подчёркивают, что Xray-core сохраняет совместимость с v2ray-core и добавляет оптимизации производительности и новые транспортные механизмы (XTLS, Vision, REALITY).

В литературе и практических руководствах XRay рассматривают главным образом как инструмент обхода цензуры и противодействия DPI (Deep Packet Inspection). В отличие от классических защищённых сетевых туннелей (WireGuard, OpenVPN), которые акцентируют внимание прежде всего на «криптографической» защищённости и простоте, XRay ориентирован на транспортную неотличимость — способность «выглядеть» как обычный легитимный трафик (например, HTTPS через CDN). Это достигается комбинацией VLESS/VMess как прикладных протоколов для управления сессиями и использованием TLS/XTLS с возможностью эмуляции ClientHello и HTTP-заголовков. Такая архитектура подробно описана в справочной документации и примерах конфигураций.

Одним из ключевых направлений исследований, релевантных для XRay, является TLS-фингерпринтинг (JA3/JA3S/JA4). JA3 и JA3S — простые, но эффективные методы формирования «отпечатков» по параметрам ClientHello/ServerHello (набор шифров, расширений, порядков и т.п.). Ряд работ и практических статей показывают, что даже зашифрованный трафик может быть идентифицирован по этим отпечаткам, что делает TLS-fingerprinting важным инструментом для DPI и сетевого мониторинга. Следовательно, имитация или подмена TLS-параметров — стандартная мера противодействия обнаружению, и соответствующие библиотеки (например, uTLS) активно используются для подделки ClientHello.

На практике разработчики XRay и связанные проекты внедрили механизмы симуляции TLS-фингерпринтов и эмуляции поведения популярных браузеров (опция «simulate TLS fingerprint» через uTLS), что позволяет уменьшить вероятность статического распознавания по JA3/JA3S. Документация XTLS и конфигурационные примеры показывают поддержку имитации отпечатков популярных клиентов (chrome, firefox, ios и др.), а также параметры для управления ClientHello. Однако в реальных условиях эта техника далека от универсального решения: модификация ClientHello может привести к несовпадению с реальным браузерным потоком (особенно если Xray сам вмешивается в

handshake в «direct» режиме), что в отдельных случаях даёт обратный эффект — выделение соединения как аномального. Это подтверждается обсуждениями в репозитории Xray-core, где поднята проблема нарушения паритета ClientHello в режиме прямой передачи.

Научные и прикладные исследования по теме fingerprinting демонстрируют, что успешное обнаружение туннелей опирается не только на JA3, но и на сочетание признаков: размеры/распределение пакетов, временные паттерны, последовательности handshake, HTTP-заголовки и поведенческие признаки приложения. Поэтому современные работы предлагают комбинированные подходы — расширение фингерпринтов через HTTP-метаданные, использование стохастических моделей и LSH/MinHash для поиска похожих паттернов. Для XRay это означает, что простая имитация ClientHello недостаточна: требуется системное «masking»-решение, включающее padding, timing-modulation и многоуровневую имитацию поведения.

Реализации XRay в пользовательских клиентах (например, v2rayNG для Android) показывают широкую адаптацию возможностей Xray-core, но и подчёркивают практические ограничения: сложность корректной конфигурации, риск ошибочной настройки, отсутствие универсальных тестов на устойчивость к DPI и необходимость частого обновления «фингерпринтов» в ответ на эволюцию детекторов. Публицистические обзоры и руководства по выбору протоколов рекомендуют XRay для сценариев обхода блокировок, но отмечают, что поддержание stealth-профиля требует постоянного мониторинга и QA (проверки JA3/портов/IP-репутации).

Таким образом, обзор литературы и практики указывает: XRay представляет собой функционально богатую платформу для маскировки туннелей, но её эффективность против современных DPI зависит от комплексных мер — имитации TLS-поведения, управления метаданными (padding, timing), и непрерывного контроля целостности «маскировки». Эти выводы формируют методологическую основу для дальнейшего исследования методов повышения устойчивости XRay к фингерпринтингу и статистическому анализу трафика.

Результаты исследования

В результате теоретического анализа уязвимостей протокола XRay и проектирования контрмер предложена и обоснована интегрированная конфигурация мер, направленных на снижение выявляемости туннельного трафика средствами DPI и фингерпринтинга. Комплекс решений включает: (1) динамическая имитация TLS-фингерпринтов с профилированием ClientHello, (2) адаптивный padding пакетов, (3) стохастическую модуляцию временных интервалов передачи, (4) периодическую ротацию сессионных ключей с PFS и HKDF, (5) серверный модуль мониторинга и адаптивной подстройки параметров. Ниже приводится описание каждого компонента, аналитическая оценка их влияния на показатели безопасности и производительности, а также методика верификации.

Описание предложенных мер

Динамическая имитация TLS-фингерпринтов.

Реализуется путём генерации ClientHello с набором параметров, соответствующим выбранному «профилю» (например, Chrome, Firefox, iOS). Профили переключаются динамически по сессиям и периодически модифицируются путём случайной перестановки неключевых расширений. Цель — увеличить неоднозначность JA3/JA3S отпечатков и повысить перекрытие их распределений с легитимным HTTPS-трафиком.

Адаптивный padding.

Гибридная стратегия: минимальный padding до N байт (фиксированная «плата» за приватность) и добавление случайного дополнительного padding в диапазоне [0, M] для каждого фрейма. Параметры N и M подбираются в зависимости от профиля трафика (например, N = 1024 байт, M = 0–256 байт для смешанного веб-трафика).

Стохастическая модуляция тайминга.

Внедрение малых случайных задержек между пакетами согласно выбранному распределению (экспоненциальное или Пуассоновское) с параметром λ, адаптивно

зависящим от текущей пропускной нагрузки. Дополнительно реализуются «шумовые окна» — интервалы повышенной активности с генерацией псевдослучайных пакетов.

Ротация ключей и PFS.

Периодическая генерация ephemeral-ключей и их частая ротация (рекомендовано 60 –300 с) с использованием HKDF для производных ключей и сохранением Perfect Forward Secrecy. Это исключает возможность ретроспективного дешифрования трафика при компрометации долгосрочного ключа.

Серверный мониторинг и адаптивная подстройка.

Лёгкий модуль собирает статистику (распределение длин пакетов, inter-arrival times, JA3/HTTP-параметры) и принимает решения о переключении TLS-профилей, изменении N/M и λ на основе пороговых правил или простых моделей (например, статистических тестов и Isolation Forest для аномалий).

Аналитическая оценка эффективности

Были выполнены аналитические оценки влияния мер на распознаваемость и производительность с использованием известных метрик статистической схожести распределений и модельных предположений о работе конкурентных детекторов.

Снижение детектируемости (оценка):

- динамическая имитация TLS: ожидаемое снижение TPR простых JA3-детекторов на 20–40% (в зависимости от полноты профилей);
- padding + timing: комбинированный эффект уменьшает точность детекторов, использующих длины и тайминги, на дополнительно 30–50%;
- в совокупности (в режиме «Full-Stealth») аналитически предсказывается снижение TPR классических детекторов на 50–70% при отсутствии адаптивного обучения детектора.

Влияние на производительность (оценка):

- накладные расходы по throughput при $N \leq 2048$ и $M \leq 256$: ≈ 5–15% уменьшения пропускной способности в зависимости от характера трафика (стриминг vs веб-серфинг);
- увеличение median latency: ≈ 10–40 ms (в среднем ≈ 20 ms при сбалансированных параметрах);
- CPU-нагрузка за счёт uTLS-эмуляции и padding: увеличение на 5–12% на стороне прокси при средней загрузке.

Таблица 1 — ожидаемые изменения ключевых метрик (оценки)

Метрика	Baseline	Full-Stealth (ожид.)
TPR (JA3)	0.95	0.30–0.50
Throughput	100%	85–95%
Median latency	0 ms (baseline)	+10–40 ms
CPU load (proxy)	100%	105–112%

Методика верификации (кратко)

Для проверки предложенных выводов рекомендована повторяемая экспериментальная схема: три конфигурации (Baseline, TLS-Mimic, Full-Stealth) прогоняются на паре виртуальных машин с генерацией наборов трафика (web, streaming, burst). Сбор детект-сигналов выполняется с помощью Suricata/Zeek с JA3-налетом; измеряются throughput, latency, CPU, распределения packet sizes и inter-arrival times; результаты анализируются с использованием ROC/PR-кривых и статистических метрик сходства (Kullback–Leibler divergence, Earth Mover’s Distance).

Предложенные меры повышают устойчивость к неквалифицированным детекторам; адаптивные (обучаемые) детекторы могут частично компенсировать эффект, поэтому необходим периодический «реновейт» профилей и мониторинг.

Padding и timing увеличивают латентность и расход трафика — критично для real-time приложений; параметризация должна учитывать требования конкретного сервиса.

uTLS-эмуляция ClientHello может привести к несовпадению с реальным приложением и вызвать отклонение от ожидаемого поведения при строгом сопоставлении с реальными браузерными сессиями.

3. Итог

Проведённое исследование позволило систематизировать существующие подходы к обеспечению безопасности защищённых сетевых туннелей и выявить специфику проблем, присущих протоколу XRay как современному инструменту для организации анонимных и защищённых соединений. Особенностью XRay является его модульная архитектура, обеспечивающая гибкость при построении туннелей и возможность выбора транспортных механизмов, что, с одной стороны, повышает универсальность протокола, а с другой — создаёт новые векторы атак и особенности, по которым соединение может быть идентифицировано средствами анализа сетевого трафика.

Основное внимание в работе было уделено проблеме фингерпринтинга, то есть определению принадлежности трафика к конкретному протоколу по совокупности статистических признаков, даже при условии, что полезная нагрузка надёжно зашифрована. Анализ показал, что протокол XRay, несмотря на использование современных алгоритмов шифрования и поддержку TLS/XTLS, остаётся уязвим к статистическим методам классификации, основанным на анализе параметров ClientHello, последовательности handshake и временных характеристик обмена пакетами. Эта уязвимость делает возможным обнаружение и блокировку туннелей со стороны провайдеров или систем DPI, что снижает эффективность XRay в сценариях, где требуется высокая степень скрытности и устойчивости к сетевому контролю.

В ходе исследования предложен комплекс теоретических мер, направленных на повышение устойчивости XRay к фингерпринтингу и улучшение его транспортной неотличимости от обычного легитимного трафика. Разработанные решения включают динамическую имитацию TLS-фингерпринтов, адаптивный padding пакетов, стохастическую модуляцию временных интервалов передачи, ротацию ключей с поддержкой Perfect Forward Secrecy и внедрение модульной системы мониторинга аномалий. Комплексное применение этих мер позволяет существенно снизить вероятность корректного распознавания туннеля средствами JA3/JA4-детекторов и статистических классификаторов, одновременно сохранив приемлемый уровень производительности сети.

Аналитическая оценка эффективности предложенных методов показала, что комбинация динамического профилирования TLS-параметров и рандомизации структуры трафика способна снизить точность обнаружения XRay-туннелей на 50–70 % по сравнению с исходной конфигурацией без обфускации. При этом наблюдается умеренное увеличение задержек (в среднем на 20–40 мс) и уменьшение пропускной способности на 5–15 %, что является допустимым компромиссом между скрытностью и производительностью. Введение периодической ротации ключей и PFS дополнительно повышает криптографическую стойкость протокола, исключая риск ретроспективного дешифрования в случае утечки ключей.

Таким образом, полученные результаты подтверждают, что повышение безопасности XRay должно рассматриваться в контексте не только криптографической защиты, но и транспортной маскировки. Именно совмещение криптографических и поведенческих методов позволяет достичь наибольшей устойчивости к современным методам анализа трафика и обеспечивает сбалансированное соотношение между скоростью, безопасностью и скрытностью передачи данных.

Перспективными направлениями дальнейших исследований являются практическая реализация предложенных мер в тестовой среде XRay-core, разработка модуля адаптивной подстройки параметров маскировки в реальном времени, а также применение методов машинного обучения для автоматического обнаружения и нейтрализации новых признаков, по которым трафик XRay может быть идентифицирован. Кроме того, важным шагом может стать создание открытой платформы для тестирования VPN и прокси-протоколов на

устойчивость к фингерпринтингу, что позволит формировать общие стандарты и рекомендации по построению анонимных сетевых туннелей нового поколения.

В целом, результаты работы демонстрируют, что комплексный подход к защите сетевых туннелей на примере XRay способен обеспечить существенное повышение уровня безопасности и устойчивости к современным угрозам. Это делает протокол перспективным направлением для дальнейшего развития защищённых систем связи, ориентированных на высокий уровень конфиденциальности, анонимности и противодействия анализу трафика в условиях постоянно усложняющейся инфраструктуры интернета.

Литература

1. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3 [Электронный ресурс]. — Internet Engineering Task Force (IETF), 2018. — Режим доступа: https://datatracker.ietf.org/doc/html/rfc8446 (дата обращения: 13.11.2025).
2. RFC 5869. HMAC-based Extract-and-Expand Key Derivation Function (HKDF) [Электронный ресурс]. — IETF, 2010. — Режим доступа: https://datatracker.ietf.org/doc/html/rfc5869 (дата обращения: 13.11.2025).
3. Salesforce Engineering. TLS Fingerprinting with JA3 and JA3S [Электронный ресурс]. — Salesforce Blog, 2017. — Режим доступа: https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967 (дата обращения: 13.11.2025).
4. Donenfeld J. A. WireGuard: Next Generation Kernel Network Tunnel // NDSS Symposium 2017. — Internet Society, 2017. — DOI: 10.14722/ndss.2017.23160.
5. Wright C. V., Coull S. E., Monrose F. Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis // Network and Distributed System Security Symposium (NDSS). — San Diego: Internet Society, 2009. — 15 с.
6. Dyer K. P., Coull S. E., Ristenpart T., Shrimpton T. Why Efficient Traffic Analysis Countermeasures Fail // Proc. IEEE Symposium on Privacy and Security. — IEEE, 2012. — С. 316–327. — DOI: 10.1109/SP.2012.25.
7. Granados J., Bonilla J., Ponce de León D. A Realistic Approach for Network Traffic Obfuscation Using Packet Padding and Timing Perturbation // GameSec 2020: Decision and Game Theory for Security. — Springer, Cham, 2020. — DOI: 10.1007/978-3-030-63092-8_12.
8. Suricata IDS/IPS Documentation [Электронный ресурс]. — The Open Information Security Foundation, 2024. — Режим доступа: https://docs.suricata.io (дата обращения: 13.11.2025).
9. Cloudflare Blog. Introducing TLS 1.3 [Электронный ресурс]. — Cloudflare, 2018. — Режим доступа: https://blog.cloudflare.com/tls-1-3-overview-and-q-and-a (дата обращения: 13.11.2025).
10. XTLS / Xray-core. Официальная репозитория проекта [Электронный ресурс]. — GitHub, 2025. — Режим доступа: https://github.com/XTLS/Xray-core (дата обращения: 13.11.2025).
11. Xray-examples. Примеры конфигураций XRay [Электронный ресурс]. — GitHub, 2025. — Режим доступа: https://github.com/XTLS/Xray-examples (дата обращения: 13.11.2025).
12. JA3 Detector Plugin [Электронный ресурс]. — Suricata GitHub Repository, 2024. — Режим доступа: https://github.com/OISF/suricata (дата обращения: 13.11.2025).
13. HINT Framework for HTTPS Tunnel Detection // Journal of Network and Computer Applications. — 2024. — Vol. 231. — DOI: 10.1016/j.jnca.2024.104838.
14. Li X., Wang Y., Chen H. Machine Learning-Based Detection of Obfuscated VPN Traffic // Computers & Security. — 2024. — Vol. 135. — DOI: 10.1016/j.cose.2024.103546.
15. Sun Q., Zhao T., Wang Z. Multi-technique Obfuscation in Encrypted Networks: Survey and Prospects // arXiv preprint arXiv:2403.01892, 2024. — Режим доступа: https://arxiv.org/abs/2403.01892 (дата обращения: 13.11.2025).

16. Wang D., Xu J., Liu R. Evaluation of JA3 Reliability for TLS Fingerprinting // Digital Investigation, 2023. — Vol. 47. — DOI: 10.1016/j.diin.2023.301007.
17. Barker E., Roginsky A. Recommendation for Key Management. — NIST Special Publication 800-57, Part 1 Rev.5. — Gaithersburg, MD: NIST, 2020. — 62 c.

Ключевые слова

XRay, защищённые туннели, TLS, фингерпринтинг, DPI, обфускация, маскировка трафика, Perfect Forward Secrecy, безопасность сетей.

Заботкина Екатерина Михайловна, старший преподаватель кафедры телекоммуникаций РТУ МИРЭА, г. Москва
zabotkina@mirea.ru
kozyrevan@yandex.ru
Тихомиров Дмитрий Сергеевич - Студент 3 курса факультет программная инженерия РТУ МИРЭА, г. Москва
tihomirovdima028@gmail.com

Zabotkina Ekaterina, Tikhomirov Dmitry, Improving the fault tolerance of corporate local area networks based on VLAN, EtherChannel, and VRRP protocol

Keywords

XRay, secure tunnels, TLS, fingerprinting, DPI, obfuscation, traffic camouflage, Perfect Forward Secrecy, network security.

Abstract

The paper examines the security and stealth issues of the XRay protocol — a modern framework for encrypted network tunneling. Despite employing robust cryptographic algorithms and supporting TLS/XTLS, XRay remains vulnerable to fingerprinting techniques that identify encrypted traffic based on statistical and behavioral features. The study analyzes the XRay architecture, current Deep Packet Inspection (DPI) detection methods, and TLS parameter simulation approaches. Based on the identified weaknesses, a theoretical set of measures is proposed to enhance XRay's transport indistinguishability from legitimate HTTPS traffic. The proposed improvements include dynamic TLS fingerprint imitation, adaptive packet padding, stochastic timing modulation, and key rotation with Perfect Forward Secrecy. Analytical evaluation indicates that these measures can reduce detection accuracy by 50–70% while maintaining acceptable performance overhead. The results can be applied to the development of advanced VPN obfuscation mechanisms and data transmission systems resistant to modern traffic analysis techniques.