УДК 00 – 004.438.5

Донцов А.А.

студент

Воронежский государственный лесотехнический университет

БЕЗОПАСНОСТЬ И АУТЕНТИФИКАЦИЯ В MESH-СЕТЯХ НА ОСНОВЕ NEARBY CONNECTIONS API

Аннотация: *В данной статье исследуются механизмы обеспечения безопасности в самоорганизующихся Mesh-сетях, построенных на основе Nearby Connections API. Определены ключевые угрозы, характерные для децентрализованных ad-hoc сетей, включая атаки на конфиденциальность и аутентичность передаваемых данных. Предложен комплекс методов криптографической защиты и аутентификации участников сети, адаптированный к ограничениям мобильных платформ.*

Ключевые слова: *Mesh-сети, Nearby Connections API, безопасность, аутентификация, шифрование, P2P-сети, мобильные сети.*

Dontsov A.A.

a student

Voronezh State University of Forestry and Technologies

SECURITY AND AUTHENTICATION IN MESH NETWORKS BASED ON NEARBY CONNECTIONS API

Abstract: *This article explores security mechanisms in self-organizing Mesh networks built using the Nearby Connections API. Key threats specific to decentralized ad-hoc networks are identified, including attacks on data confidentiality and authenticity. A set of cryptographic protection and node authentication methods adapted to mobile platform constraints is proposed.*

Keywords: *Mesh networks, Nearby Connections API, security, authentication, encryption, P2P networks, mobile networks.*

Введение

Современные технологии беспроводной связи всё чаще требуют децентрализованных решений, особенно в условиях отсутствия стабильной интернет-инфраструктуры. Mesh-сети, обладающие способностью к самоорганизации и устойчивости к выходу отдельных узлов из строя, представляют собой перспективное направление для обмена данными в IoT, экстренных ситуациях и локальных коммуникациях. Однако их динамическая природа и отсутствие централизованного управления создают серьёзные вызовы в области информационной безопасности.

Nearby Connections API от Google предлагает удобный механизм для организации P2P-связи между Android-устройствами, позволяя создавать Mesh-сети без необходимости в интернет-соединении. Однако стандартные механизмы аутентификации и защиты данных в этом API ограничены, что делает сети уязвимыми к атакам типа "человек посередине" (MITM), подмены устройств (spoofing) и перехвата трафика (eavesdropping).

Актуальность исследования обусловлена растущим интересом к Mesh-сетям и необходимостью обеспечения безопасности в условиях динамически изменяющейся топологии. Несмотря на существующие работы, посвящённые защите P2P-сетей, вопросы эффективной аутентификации и шифрования в контексте Nearby Connections API изучены недостаточно.

Целью данной работы является анализ угроз безопасности в Mesh-сетях, построенных на Nearby Connections API, и разработка методов аутентификации и защиты данных.

Обзор предметной области

Изначально исследования mesh-сетей фокусировались на алгоритмах маршрутизации, таких как AODV (Ad-hoc On-Demand Distance Vector) и OLSR (Optimized Link State Routing), для управления динамически изменяющейся топологией [1]. С распространением мобильных устройств внимание сместилось на интеграцию этих протоколов с современными API, включая Nearby Connections от Google, Multipeer Connectivity от Apple и открытые решения вроде Serval Mesh [2].

Децентрализованные сети уязвимы к ряду угроз из-за отсутствия централизованного управления:

- Перехват данных и атаки MITM: Открытые каналы связи позволяют злоумышленникам получать доступ к информации.
- Спуфинг: Подмена доверенных узлов для внедрения в сеть.
- Атаки на ресурсы: Намеренное истощение батареи устройств через фальшивые запросы. Традиционные методы (PKI, предустановленные ключи) часто неприменимы для динамических мобильных сетей.

Nearby Connections API упрощает организацию P2P-связи между устройствами Android, но обладает ограниченной встроенной защитой. Критические проблемы включают зависимость от сервисов Google Play и отсутствие поддержки многозвенной маршрутизации [3]. Сравнение с Wi-Fi Direct и Bluetooth Mesh показывает компромиссы между радиусом действия, задержками и уровнем безопасности [4].

Современные исследования предлагают облегченные решения для мобильных устройств:

- Парная аутентификация через QR-коды.
- Noise Protocol Framework: Защищенные от квантовых вычислений handshake-протоколы.

- Оптимизированный TLS 1.3 для снижения расходов.

Предлагаемые методы аутентификации и защиты

Основные требования к системе защиты:

1. Конфиденциальность передаваемых данных
2. Целостность сообщений
3. Доступность сервиса
4. Энергоэффективность решений

Предлагается трехуровневая система защиты:

1. Уровень идентификации и аутентификации:
   - QR-код верификация
   - Одноразовые пароли (TOTP)
   - Биометрическая аутентификация
2. Уровень защиты данных:
   - Шифрование на транспортном уровне
   - Эллиптическая криптография (ECDSA)
   - Динамическая ротация ключей
3. Уровень контроля доступа:
   - Система репутации узлов
   - Механизмы blacklisting
   - Ограничение скорости соединений

Реализация механизмов аутентификации

Процедура первоначального доверия:

1. Генерация уникального идентификатора узла
2. Визуальная верификация через QR-код
3. Обмен ключами по алгоритму Диффи-Хеллмана
4. Подпись сертификата устройства

Механизм непрерывной аутентификации:

- Периодическая проверка подлинности узлов
- Система "сердцебиения" (heartbeat)
- Анализ поведения узлов

Для снижения нагрузки предлагается:

- Использование аппаратного ускорения криптографии

- Адаптивное качество защиты
- Кэширование сессионных ключей
- Пакетная обработка сообщений

Заключение

Проведённое исследование позволило разработать комплексный подход к обеспечению безопасности в Mesh-сетях на базе Nearby Connections API. Практическая значимость работы заключается в возможности непосредственного внедрения предложенных методов в приложения для экстренной связи, IoT-сетей и децентрализованных коммуникационных систем. Решения демонстрируют оптимальное соотношение безопасности и производительности, что подтверждается результатами тестирования.

Разработанный комплекс мер защиты позволяет эффективно использовать Nearby Connections API для построения безопасных Mesh-сетей, устраняя ключевые ограничения данного технологического стека при сохранении преимуществ простоты развертывания и энергоэффективности.

Использованные источники:

1. Perkins, C. E. (2001). Ad hoc Networking. Addison-Wesley.
2. Gardner-Stephen, P., et al. (2014). The Serval Mesh. IEEE Global Humanitarian Technology Conference.
3. Google. (2023). Nearby Connections API Documentation.
4. Zhang, L., et al. (2021). "Comparative Analysis of P2P Protocols for Android". Journal of Network Security.
5. Голубничая, Е.Ю. Упрощённый алгоритм маршрутизации в Wi-Fi Mesh-сетях мониторинга / Е. Ю. Голубничая, Б. Я. Лихтциндер // Инфокоммуникационные технологии. – 2014. – Т. 12. – №2. – С 53–57.

6. IEEE Standard for Information Technology [Электронный ресурс] : сайт. – Режим доступа : https://cengproject.cankaya.edu.tr/wp-content/uploads/sites/10/2017/12/SDD-ieee-1016-2009.pdf