



ИССЛЕДОВАНИЕ УЯЗВИМОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

Грунина Ирина Анатольевна

студент, Поволжский государственный университет, РФ, г. Самара

Уразова Оксана Владимировна

студент, Поволжский государственный университет, РФ, г. Самара

WLAN сеть (беспроводная сеть) представляет собой локальную вычислительную сеть, использующую ВЧ радиоволны для передачи данных между узлами. Она является альтернативой проводной сети, обеспечивая передачу данных в любой точке сети без непосредственного подключения к проводу. Беспроводные сети обладают гибкой архитектурой, высокой скоростью передачи данных, быстротой развертывания, высоким уровнем защиты и отказом от дорогостоящей проводной инфраструктуры.

Беспроводные сети подразделяются по способу обработки информации (цифровые и аналоговые), ширине полосы передачи (узкополосные, широкополосные, сверхширокополосные), локализации абонентов (подвижные и фиксированные), географической протяженности (персональные, локальные, региональные, глобальные) и виду передаваемой информации (речь, видео, данные).

Стандарт IEEE 802.11, известный также как Wi-Fi, является одним из наиболее широко используемых протоколов беспроводной связи. Он обеспечивает передачу данных в беспроводных сетях и имеет несколько вариантов и расширений, таких как 802.11a, 802.11b, 802.11g, 802.11n и т.д. Каждый из этих протоколов имеет свои особенности и характеристики, которые влияют на производительность и эффективность беспроводной сети [1].

Для полного понимания и оценки существующих протоколов стандарта IEEE 802.11 необходимо провести исследование и анализ каждого из них. Рассмотрим некоторые из ключевых протоколов и их особенности:

1. 802.11a: Этот протокол использует радиочастоту в 5 ГГц и обеспечивает более высокую скорость передачи данных по сравнению с предыдущими протоколами. Он поддерживает множество каналов и обладает лучшей пропускной способностью, но имеет более ограниченную дальность передачи.
2. 802.11b: Этот протокол работает на частоте 2,4 ГГц и обеспечивает более широкий диапазон покрытия, но с более низкой скоростью передачи данных по сравнению с 802.11a. Он поддерживает меньше каналов и более подвержен помехам от других устройств, работающих на той же частоте.
3. 802.11g: Этот протокол также работает на частоте 2,4 ГГц и представляет собой комбинацию характеристик 802.11a и 802.11b. Он обеспечивает более высокую скорость передачи данных по сравнению с 802.11b, сохраняя при этом широкий диапазон покрытия.

4. 802.11n: Этот протокол представляет собой значительное усовершенствование предыдущих протоколов. Он поддерживает использование нескольких антенн и технологию MIMO (Multiple-Input Multiple-Output), что позволяет достичь более высокой пропускной способности и лучшей стабильности соединения. Протокол 802.11n также обладает более широким диапазоном покрытия и поддерживает обратную совместимость с предыдущими протоколами.

5. 802.11ac: Этот протокол представляет следующий уровень развития стандарта и обеспечивает еще более высокую скорость передачи данных. Он работает на частоте 5 ГГц и поддерживает широкий канал передачи данных, что позволяет достичь высокой производительности в сетях с высокой загруженностью.

Стандарт IEEE 802.11n является улучшенной версией предыдущих стандартов IEEE 802.11a/b/g. Технология MIMO (Multiple Input Multiple Output) позволяет использовать несколько приемных и передающих антенных устройств для повышения скорости передачи данных [1].

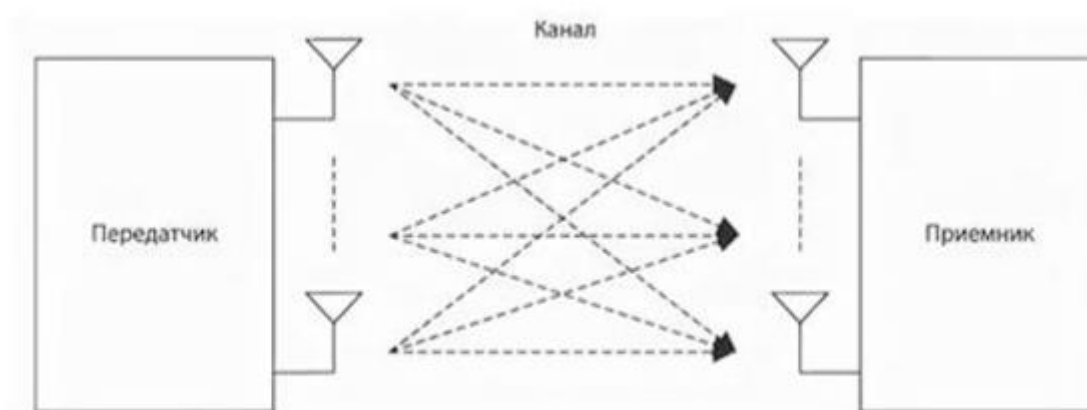


Рисунок 1. Принцип работы технологии MIMO

Технология MIMO разделяет передаваемые данные на параллельные потоки и восстанавливает их в приемном устройстве, обеспечивая увеличение скорости передачи данных. Развитие и применение данной технологии значительно улучшили производительность и эффективность беспроводных сетей, открывая новые возможности в области коммуникаций и передачи данных. Результаты исследования уязвимости беспроводных сетей позволяют лучше понять риски и угрозы, связанные с использованием таких сетей. Это знание помогает разработать эффективные методы защиты и снизить уязвимости, обеспечивая безопасность передачи данных и защиту конфиденциальности пользователей беспроводных сетей.

Безопасность беспроводных сетей определяется различными факторами. Хотя стандарт 802.11n включает многоуровневые меры защиты, он все еще уязвим. Для обеспечения надежной защиты передаваемой информации необходим комплексный подход к обеспечению безопасности, который не ограничивается только программными средствами и требует грамотной настройки и использования таких средств.

Ниже рассмотрены некоторые возможности обеспечения безопасности беспроводных сетей

1. Ограничение доступа к передающим устройствам и в зоне действия сети. На этапе проектирования системы необходимо провести организационные и проектно-конструкторские решения, чтобы ограничить доступ к устройствам.

2. Корректная настройка оборудования. Это позволяет обеспечить правильное функционирование системы. Большинство пользователей не знает о возможностях своего оборудования и неумело настраивает, и использует средства защиты.

3. Защита устройств пользователей, таких как ноутбуки, планшеты, смартфоны и ПК. Это создает первую линию защиты, обезопасив пользователей без применения методов внутренней защиты беспроводной сети (аутентификация, шифрование и т. д.).

4. Установка антивирусного программного обеспечения и использование последних версий программного обеспечения и механизмов, предусмотренных операционными системами. Эти меры не обеспечат полную защиту от уязвимостей, но важно использовать их при комплексном подходе.

5. Мониторинг беспроводной сети для обнаружения "опасного" оборудования, такого как несанкционированные точки доступа. Локализация и отключение такого оборудования, а также применение методов обнаружения атак, помогут обезопасить сеть.

6. Использование методов защиты передаваемой информации для точек доступа, работающих в открытом режиме. Например, включение функции VPN-клиента на приемной стороне, что обеспечит безопасность передаваемых данных.

Правильное применение этих мер позволит повысить безопасность беспроводных сетей, уменьшить уязвимости и обеспечить защиту передаваемой информации.