МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**

ИНТЕРНЕТ/WI-FI ТЕХНОЛОГИИ

РЕФЕРАТ

студента 2 курса 251 группы
направления 09.03.04 — Программная инженерия
факультета КНиИТ
Григорьева Данилы Евгеньевича

Проверено:

доцент, к. ф.-м. н. _____ Черкассова О. А.

Саратов 2024

СОДЕРЖАНИЕ

1 Введение 2
1 Электромагнитные волны 4
1.1 Характеристики волны 4
1.2 Виды электромагнитных волн 5
1.3 Принцип формирования волн 6
1.4 Уравнения Максвелла 6
1.5 Свойства волн 6
2 Аналоговые и цифровые сигналы 7
2.1 Синусоида 7
2.2 Затухания и полоса пропускания 7
2.3 Помехи 7
2.4 Пропускная способность 7
2.5 Модуляция сигнала 7
2.5.1 Амплитудная модуляция 7
2.5.2 Частотная модуляция 7
2.5.3 Фазовая модуляция 7
2.5.4 Квадратурная амплитудная модуляция 7
3 Стандарты Wi-Fi 8
3.1 Некоторые юридические аспекты 8
4 Физический уровень 9
4.1.1 Расширение спектра 9
4.1.2 Мультиплексирование 9
4.1.3 Антенны MIMMO 9
5 Канальный уровень 10
5.1.1 Методы определения и коррекции ошибок 10
6 Атаки на беспроводные сети 11
6.1 Атаки отказа в обслуживании (DoS и DDoS) 11
6.2 Разведка и перехваты пакетов 11
6.2.1 Перехват пакетов 11
6.3 Атака получения доступа 11
6.4 Принудительная смена алгоритма шифрования 11
6.5 Атаки человека посередине 11
6.6 Атаки подмены ARP записей 11
7 Способы защиты от атак на Wi-Fi сети 12
7.1 Идентификация устройства, атакующего на отказ в обслуживании 12
7.2 Секретность на уровне проводной сети (WEP) 12
7.2.1 WEPCrack 12
8 Заключение 13
8 Список использованных источников 14

ВВЕДЕНИЕ

На заре развития компьютерных сетей, когда встала необходимость обеспечения обмена разнообразными данными между различными сетевыми устройствами, для задания единообразного способа передачи информации возникли различные соглашения интерфейса — протоколы передачи данных — а Международная организация по стандартизации (ИСО) представила модель сетевых протоколов OSI/ISO (также OSI), которая разделила различные уровни взаимодействия систем и, таким образом, стала путеводной звездой при разработке будущих протоколов, эталонной моделью взаимосвязи открытых систем. Она состоит из семи уровней, каждый из которых выполняет определённые задачи. Эти уровни, начиная с нижнего, самого нигкоуровневого, включают:

1. Физический уровень (У1)
2. Канальный уровень (У2)
3. Сетевой уровень (У3)
4. Транспортный уровень (У4)
5. Сеансовый уровень (У5)
6. Представительский уровень (У6)
7. Прикладной уровень (У7)

Каждый уровень модели OSI отвечает за свою часть процесса передачи данных, обеспечивая абстракцию и независимость от конкретных технологий.

Физический уровень является первым и самым низким уровнем модели OSI. Он отвечает за передачу необработанных битов данных по физическим носителям, таким как кабели и радиоволны. Он определяет способы передачи битов по физическим носителям, включая медные и оптоволоконные кабели, беспроводные каналы. Также У1 описывает электрические, механические и функциональные характеристики для активации и поддержания соединений между устройствами связи. Собственно, здесь определяются и сами физические носители, коих немалое количество от коаксиального кабеля до оптоволокна и любой беспроводной среды.

Следующий за ним канальный уровень обеспечивает контроль стабильности физического канала связи и непосредственно общение между узлами одного сегмента локальной сети. На втором уровне модели OSI данные делятся на кадры, содержащие полезную нагрузку — данные — и служебную информацию — метаданные (это, в частности, могут быть сетевые адреса отправителя и получателя). Для обнаружения и даже по мере возможности исправления ошибок передачи, как правило, используются контрольные суммы. Также канальным уровнем определяются правила доступа к физическому носителю, что предотвращает коллизии.

Общепринятые и наиболее распространённые на текущий момент времени стандарты обоих уровней разработаны Институтом инженеров электротехники и электроники США (IEEE). В первую очередь это группа IEEE 802, которая состоит из нескольких наборов стандартов. Один из них — IEEE 802.11. В нём описаны нормы и

правила работы беспроводных компьютерных с использованием радиоволн и видимого света, а сам этот набор известен под торговой маркой Wi-Fi.

В рамках своей работы мною рассмотрен как сам стандарт, так и принцип его работы с физической точки зрения, а, кроме того, мною затронуты некоторые аспекты компьютерной безопасности, связанные с атакой и защитой беспроводных сетей на физическом уровне.

1 Электромагнитные волны

Волна — это процесс переноса энергии без переноса вещества, связанный с колебаниями частиц среды или полей. Механические волны требуют наличие среды для распространения, а примечательное свойство электромагнитных волн состоит в том, что им и вакуум не страшен. Именно они используются в технологиях радиосвязи и, в том числе, на физическом уровне стандартов Wi-Fi.
Электромагнитные волны представляют собой колебания электрического и магнитного полей, которые распространяются в пространстве с конечной скоростью. Основной их источник — это движущиеся с ускорением заряженные частицы.

1.1 Характеристики волны

Любые волны — как механические, так и электромагнитные — обладают пятью основными характеристиками, а именно:

1. Амплитуда A
2. Частота V
3. Период $T = \frac{1}{V}$
4. Длина волны λ
5. Скорость распространения v
6. Фаза

Амплитуда — это максимальное отклонение волны от её равновесного положения, связанная с величиной электрического и магнитного полей. Она напрямую зависит от переносимой волной энергией: чем её больше, тем выше амплитуда.

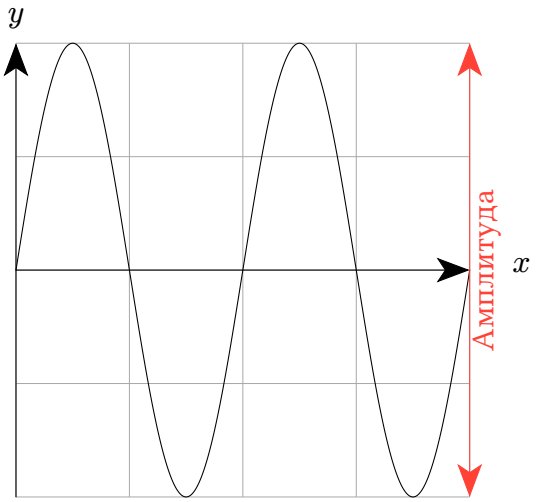

Рисунок 1: Амплитуда колебаний

Если амплитуда определяет энергию волны, то частота и период описывают временные характеристики волн.

Частота — это количество полных колебаний, которые происходят за единицу времени (секунду). Она измеряется в Герцах и, нетрудно догадаться, $1\ \text{Гц} = 1\ \text{с}^{-1}$.

Период — время, которое требуется для завершения одного полного цикла колебания. Само собой, оно измеряется в секундах.

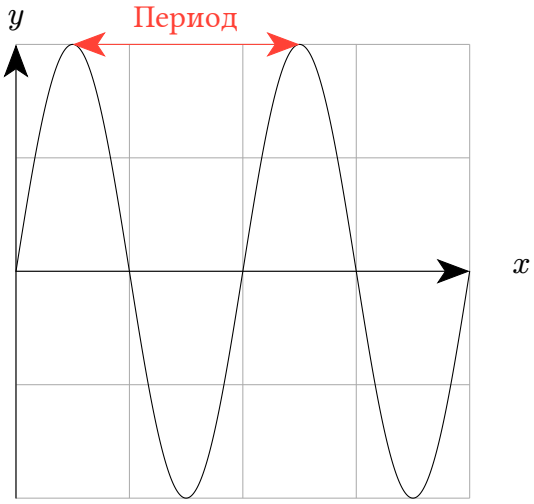

Рисунок 2: Период колебания

Фаза — относительное значение, которое показывает, какая часть перода $\frac{t}{T}$ прошла с момента последнего прохождения функции волны через нуль.

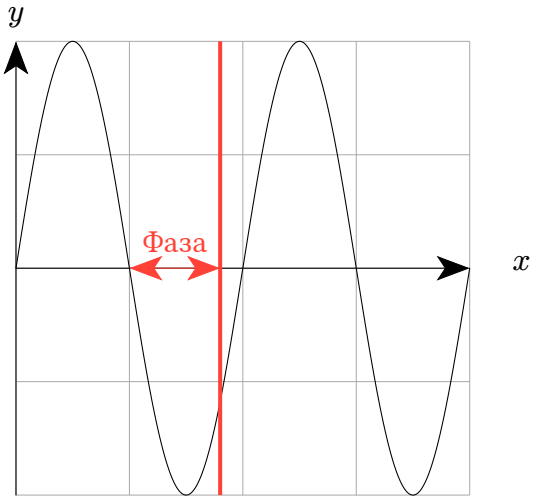

Рисунок 3: Фаза колебания

1.2 Виды электромагнитных волн

Электромагнитные волны возникают при движении заряженных частиц и по частоте колебаний делятся на:

Диапазон		λ	V	**Источники**
Радио	Сверхдлинные	>10км	<30кГц	Атмосферные и магнитосферные явления. Радиосвязь
	Длинные	10км — 1км	30кГц — 300кГц	
	Средние	1км — 100м	3МГц — 30МГц	
	Короткие	100м — 10м	3МГц — 300ГГц	
	Ультракороткие	10м — 1мм	30МГц — 300ГГц	
Инфракрасное излучение		1мм — 780нм	300ГГц — 429ТГц	Излучение молекул и атомов при тепловых и электрических воздействиях
Видимое излучение		780 нм — 380 нм	429 ТГц — 750ТГц	
Ультрафиолет		380 нм — 10 нм	$7,5 \cdot 10^{14}$ Гц — $3 \cdot 10^{16}$ Гц	Излучение атомов под воздействием ускоренных электронов
Рентген		10 нм — 5 пм	$3 \cdot 10^{16}$ Гц — $6 \cdot 10^{19}$ Гц	Атомные процессы при воздействии ускоренных заряженных частиц
Гамма		<5 пм	$> 6 * 10^{19}$ Гц	Ядерные и космические процессы, радиоактивный распад

Table 1: Частотные диапазоны электромагнитного излучения

1.3 Принцип формирования волн

1.4 Уравнения Максвелла

1.5 Свойства волн

2 Аналоговые и цифровые сигналы

2.1 Синусоида

2.2 Затухания и полоса пропускания

2.3 Помехи

2.4 Пропускная способность

2.5 Модуляция сигнала

2.5.1 Амплитудная модуляция

2.5.2 Частотная модуляция

2.5.3 Фазовая модуляция

2.5.4 Квадратурная амплитудная модуляция

3 Стандарты Wi-Fi

3.1 Некоторые юридические аспекты

4 Физический уровень

4.1.1 Расширение спектра

4.1.2 Мультиплексирование

4.1.3 Антенны MIMMO

5 Канальный уровень

5.1.1 Методы определения и коррекции ошибок

Коды обнаружения ошибок, коды с коррекцией ошибок, протоколы с автоматическим запросом повторной передачи

6 Атаки на беспроводные сети

6.1 Атаки отказа в обслуживании (DoS и DDoS)

Создание широкополосных помех с помощью радио-джаммеров. Это эквивалент DoS-атаки, но только на физическом уровне радиосреды. Противостоять подобного рода атаке средствами инфраструктуры Wi-Fi практически невозможно, если мощность излучения высока

6.2 Разведка и перехваты пакетов

6.2.1 Перехват пакетов

Самый универсальный способ атаки на точку доступа — вычисление ее ключа WPA2 по отдельным сообщениям (M1-M4) из перехваченных хендшейков. Он срабатывает практически всегда, но требует больших затрат (особенно времени). Перехват «рукопожатий» всегда выполняется в режиме мониторинга, который поддерживает далеко не каждый Wi-Fi-чип и драйвер. Для ускорения сбора хендшейков потребуется функция инжекта пакетов, которая деавторизует подключенных к AP клиентов и заставляет их чаще отправлять «рукопожатия». Она и вовсе встречается у единичных Wi-Fi-модулей.

6.3 Атака получения доступа

6.4 Принудительная смена алгоритма шифрования

6.5 Атаки человека посередине

6.6 Атаки подмены ARP записей

7 Способы защиты от атак на Wi-Fi сети

7.1 Идентификация устройства, атакующего на отказ в обслуживании

спользовать специальные технологии для идентификации типа устройства, создающего помехи и определения его физического местоположения в зоне покрытия. Например, это может быть выполнено с большой эффективностью в случае, если сеть построена на оборудовании Cisco Systems и Точки Доступа WiFi поддерживают технологию CleanAir (модельные ряды Cisco 3700, 3600, 2700, 1550 и тд). После обнаружения местоположения излучателя, в данную точку могут быть направлены сотрудники службы безопасности для физического устранения проблемы.

7.2 Секретность на уровне проводной сети (WEP)

7.2.1 WEPCrack

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Линь Лай Тхи, Дык Буй Минь, Хуи Нгуен Нгок, Чыонг Нгуен Динь, Хю Нгуен Ба, Хыонг Лыу Чан Сетевая модель OSI // Научные исследования. 2017. №1 (12). URL: https://cyberleninka.ru/article/n/setevaya-model-osi (дата обращения: 29.10.2024).
2. Сложно о простом. Физический уровень (L1) модели OSI https://habr.com/ru/companies/timeweb/articles/825344/
3. Степанов Н. С. Волны // Большая российская энциклопедия: научно-образовательный портал – URL: https://bigenc.ru/c/volny-11a6a9/?v=10134364. – Дата публикации: 16.01.2024. – Дата обновления: 29.03.2024