**Использование криптографических методов защиты процесса аутентификации устройств через технологию беспроводного доступа Wi-Fi**

*- Поскольку у тебя половина материала – рассуждения о вай-фае, а вторая половина о том, как происходит процесс аутентификации и криптография, то в названии их обоих нужно указать*

*-- Не пугайся моего любимого термина «защита информации», ибо он является синонимом слову «аутентификация»*

# **Введение**

За последнее десятилетие был совершён огромный скачок в сфере робототехники. Всё чаще и чаще люди прибегают к помощи роботов. На сегодняшний день роботы применяются в различных сферах: они задействованы в медицине, в военном деле, сфере обслуживания и просто для бытовых целей. Основным предназначением роботов является упрощение жизни человека, делая её более комфортной, избавив от выполнения тяжёлых и сложных рабочих процессов. Иными словами, можно утверждать следующее, умные устройства не должны препятствовать или полностью подменить человека, сколько освободить его от монотонной ненужной и малоэффективной работы, тем самым автоматизировать большинство производственных и домашних задач. Сегодня роботов, исходя из их назначения и применения, подразделяют на следующие виды: исследовательские, строительные, промышленные, бытовые, транспортные. Все они имеют разные размеры, подвиды, направления, а также способ управления. Часто, при разработке робототехнических комплексов необходима идентификация отдельных роботов. В свою очередь производители автономных роботов используют закрытые протоколы собственной разработки, используемые для управления одним типом оборудования. Это значительно усложняет разработку и интеграцию новых роботов. Актуальность выбранной темы обусловлена наличием уязвимостей удалённого управления автономными роботами по интерфейсу WI-FI. В результате чего, необходимо разработать алгоритм идентификации роботов, который может быть применён в различных типах робототехнических систем, а также в личных интересах (домашних делах), с целью расширения функционала управления роботом.

## Технология WI-FI

Во всём мире происходит непрерывное развитие интернета и глобальной компьютеризации общества, что привело к огромному скачку развития беспроводных технологий. Технология WI-FI позволяет подключать удаленные объекты, заменяя провода и экономя немало денег. Она так же позволяет, перемещаться в зоне покрытия сети оставаясь на связи, тем самым став востребованной на телекоммуникационном рынке. Разработка этих стандартов ведется в рамках рабочей группы 802.11 Института инженеров по электротехнике и электронике (IEEE). Почти все современные ноутбуки и другие электронные девайсы так или иначе умеют работать в сетях Wi-Fi.

Для подключения к Wi-Fi-сети достаточно, чтобы электронный гаджеты, были оснащены беспроводными адаптерами.

Главное предназначение Wi-Fi — объединять компьютеры в локальную сеть. Wi-Fi может связывать между собой не только компьютеры.Существует три типа беспроводных сетей

− WPAN ( Wireless Personal Area Network) беспроводные персональные сети;

− WLAN (Wireless Local Area Network) беспроводные локальные сети;

− BWA (Broadband Wireless Access) беспроводная глобальная сеть.

На рисунке 1 представлен радиус действия беспроводных сетей.

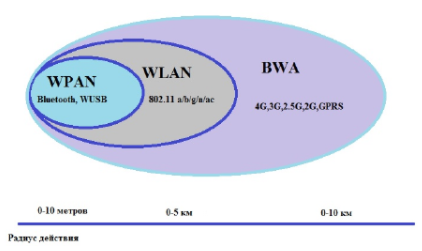


Рисунок 1 - Радиус действия типов беспроводных сетей

При построении сетей WLAN и WPAN, а также систем широкополосного беспроводного доступа BWA (Broadband Wireless Access) используются похожие технологии. Главное отличие между ними – диапазон рабочих частот и характеристики радио интерфейса (рисунок 2).

Сеть WLAN — вид локальной вычислительной сети (LAN), использующий для связи и передачи данных между узлами высокочастотные радиоволны, а не кабельные соединения. Это гибкая система передачи данных, которая применяется как расширение или альтернатива кабельной локальной сети внутри одного здания или в пределах определенной территории.

## 1.4 Основные стандарты беспроводного доступа

Беспроводные локальные сети создаются на основе семейства стандартов IEEE 802.11.

В 1990 г. Комитет по стандартам IEEE 802 (Institute of Electrical and Electronic Engineers). сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11. Это группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2.4 ГГц со скоростями 1 и 2 Мбит/с. Работа по созданию стандарта были завершены через семь лет, и в июне 1997 г. была ратифицирована первая спецификация 802.11.

Стандарт IEEE 802.11 стал первым стандартом для продуктов WLAN от независимой международной организации. Однако к моменту выхода стандарта в свет первоначально заложенная в нем скорость передачи данных оказалась недостаточной. Это послужило причиной последующих доработок, поэтому сегодня можно говорить о группе стандартов.

В таблице 1 представлены основные характеристики стандартов группы IEEE 802.11.

Таблица 1 - Основные характеристики стандартов группы IEEE 802.11

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Стандарт** | **802.11b** | **802.11a** | **802.11g** | **802.11n** | **802.11ac** |
| **Год ратификации** | 1999 | 1999 | 2003 | 2009 | 2014 |
| **Рабочая частота** | 2.4 ГГц | 5 ГГц | 2.4 ГГц | 2.4/5 ГГц | 5 ГГц |
| **Частотные каналы** | 20 МГц | 20 МГц | 20 МГц | 20/40 МГц | 20/40/80/160 МГц |
| **Пиковая физическая**  **Скорость(PHY)** | 11 Мбит/c | 54 Мбит/c | 54 Мбит/c | 600 Мбит/c | 6.8 Гбит/c |
| **Модуляция** | DSSS, CCK | OFDM | OFDM | OFDM | OFDM |

**Стандарт IEEE 802.11b**

**Стандарт IEEE 802.11а**

**Стандарт IEEE 802.11g**

**Стандарт IEEE 802.11n**

**Стандарт IEEE 802.11ac**

## Технология безопасного доступа WPA (Wi-Fi Protected Access).

WEP уже давно устарела. На смену этой технологии пришел WPA, а также на горизонте виднеется новый стандарт 802.11i (некоторые производители преподносят его, как WPA2). Но при использовании WPA2 в качестве защищённого удалённого управления автономными роботами, может значительно затормозить этот процесс, таким образом в большинстве случаев для удалённого управления автономными роботами применяется технология WPA. Стандарт WPA использует 802.1x и Расширенный протокол аутентификации (Extensible Authentication Protocol, EAP) в качестве основы для механизма аутентификации. Аутентификация требует, чтобы пользователь предъявил свидетельства/мандат (credentials) того, что ему позволено получать доступ в сеть. Для этого права пользователя проверяются по базе данных зарегистрированных пользователей. Для работы в сети пользователь должен обязательно пройти через механизм аутентификации. База данных и система проверки в больших сетях обычно принадлежат специальному серверу — чаще всего RADIUS. Однако, поскольку применение WPA подразумевается всеми категориями пользователей беспроводных сетей, стандарт имеет упрощенный режим, который не требует использования сложных механизмов.

Этот режим называется Pre-Shared Key (WPA-PSK рис.5) — при его использовании необходимо ввести один пароль на каждый узел беспроводной сети (точки доступа, беспроводные маршрутизаторы, клиентские адаптеры, мосты). До тех пор, пока пароли совпадают, клиенту будет разрешен доступ в сеть.

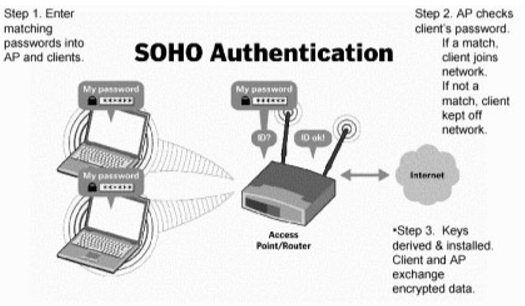


Рисунок 5 - Режим WPA-PSK

В беспроводной сети адаптеры на каждом компьютере преобразуют цифровые данные в радиосигналы, которые они передают на другие сетевые устройства. Они же преобразуют входящие радиосигналы от внешних сетевых элементов обратно в цифровые данные.

Стандарт IEEE 802.11n основан на технологии OFDM-MIMO. Увеличение скорости передачи в стандарте IEEE 802.11n достигается, во-первых, благодаря удвоению ширины канала с 20 до 40 МГц, а во-вторых, за счет реализации технологии MIMO, представлена на рисунке 6. Технология MIMO (Multiple Input Multiple Output) это множественная передача информации с нескольких передатчиков и её получение, а также обработка на нескольких приемниках. Основные задачи MIMO – повысить пропускную способность беспроводного канала и качество связи.

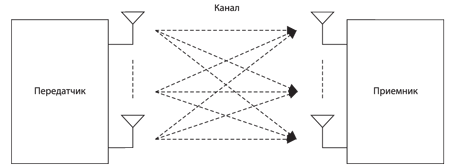


Рисунок 6 - Принцип реализации технологии MIMO

Передаваемая последовательность делится на параллельные потоки, из которых на приемном конце восстанавливается исходный сигнал. Здесь возникает некоторая сложность — каждая антенна принимает суперпозицию сигналов, которые необходимо отделять друг от друга. Для этого на приемном конце применяется специально разработанный алгоритм пространственного обнаружения сигнала. Этот алгоритм основан на выделении поднесущей и оказывается тем сложнее, чем больше их число. Единственным недостатком использования MIMO является сложность и громоздкость системы и, как следствие, более высокое потребление энергии.

## Шифрование через TKIP протокол

За шифрование данных в WPA отвечает протокол TKIP, который, хотя и использует тот же алгоритм шифрования — RC4 — что и в WEP, но имеет следующие усовершенствования:

* *Пофреймовое изменение ключей шифрования*. *WEP*-ключ быстро изменяется, и для каждого фрейма он другой;
* *Контроль целостности сообщения*. Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения скрытых манипуляций с фреймами и воспроизведения фреймов;
* *Усовершенствованный механизм управления ключами*.

Несмотря на то, что предшественник WPA, протокол WEP, не имел каких-либо механизмов аутентификации вообще, ненадежность WEP заключается в криптографической слабости алгоритма шифрования. Как известно, ключевая проблема WEP кроется в слишком похожих ключах для различных пакетов данных.

Части TKIP, MIC и 802.1X уравнения WPA играют свою роль в усилении шифрования данных сетей с WPA. TKIP увеличивает размер ключа с 40 до 128 бит и заменяет один статический ключ WEP ключами, которые автоматически создаются и распространяются сервером аутентификации. TKIP использует иерархию ключей и методологию управления ключами, которая убирает предсказуемость, использовавшеюся взломщиками для снятия защиты ключа WEP.

С помощью значительного увеличения размера ключей и числа используемых ключей, а также создания механизма проверки целостности, TKIP преумножает сложность декодирования данных в беспроводной сети. TKIP значительно увеличивает силу и сложность беспроводного шифрования, делая процесс вторжения в беспроводную сеть намного более сложным, если не невозможным вообще.

Важно отметить, что механизмы шифрования, используемые для WPA и WPA-PSK, являются одинаковыми. Единственное отличие WPA-PSK заключается в том, что там аутентификация производится по какому-либо паролю, а не по мандату пользователя. Также WPA-PSK снимает путаницу с ключами WEP, заменяя их целостной и четкой системой на основе цифробуквенного пароля.

IEEE адаптировала схему, известную как пофреймовое изменение ключа (per-frame keying). Основной принцип, на котором основано пофреймовое изменение ключа, состоит в том, что IV, MAC-адрес передатчика и *WEP*-ключ обрабатываются вместе с помощью двухступенчатой функции перемешивания. Результат применения этой функции соответствует стандартному 104-разрядному *WEP*-ключу и 24-разрядному IV.

IEEE предложила также увеличить 24-разрядный вектор инициализации до 48-разрядного IV.

Процесс пофреймового изменения ключа можно разбить на следующие этапы (рис. 7):

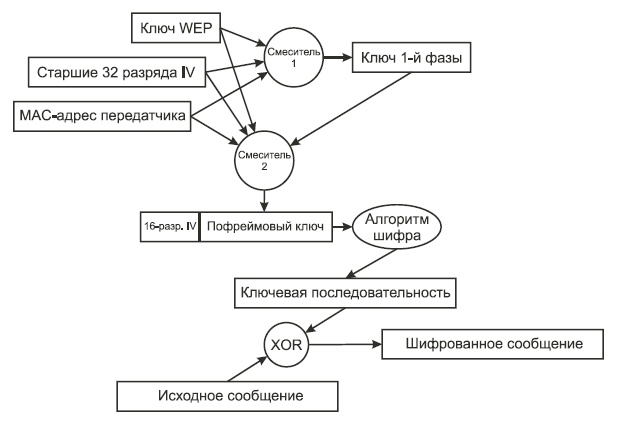


Рисунок 8 - Процесс создания шифрованного сообщения в WPA

## 2.4 Контроль целостности сообщения

Для усиления малоэффективного механизма, основанного на использовании контрольного признака целостности (ICV) стандарта *802.11*, будет применяться контроль целостности сообщения (*MIC*). Благодаря *MIC* могут быть ликвидированы слабые места защиты, способствующие проведению атак с использованием поддельных фреймов и манипуляции битами. IEEE предложила специальный алгоритм, получивший название Michael чтобы усилить роль ICV в шифровании фреймов данных стандарта *802.11*.

*MIC* имеет *уникальный ключ*, который отличается от ключа, используемого для шифрования фреймов данных. Этот *уникальный ключ* перемешивается с назначенным MAC-адресом и исходным MAC-адресом фрейма, а также со всей незашифрованной частью фрейма. На рис.8 показана работа алгоритма Michael *MIC*.



Рисунок 9 -Работа алгоритма Michael MIC

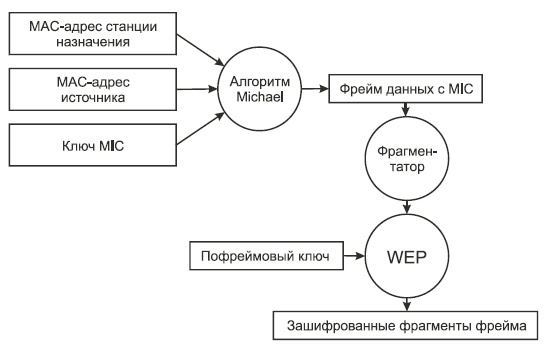


Рисунок 10 - Механизм шифрования TKIP

Аналогично процессу шифрования по алгоритму *TKIP*, процесс дешифрования по этому алгоритму выполняется следующим образом ([рис.10](http://mayoroven.ru/docum/intuit/course-307-html/#ID.9.image.9.11)):

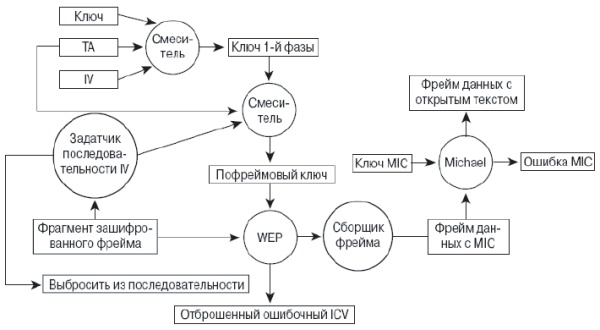


Рисунок 11 - Механизм дешифровки TKIP

*WPA* может работать в двух режимах: *Enterprise* (корпоративный) и *Pre-Shared Key* (персональный).

В первом случае хранение базы данных и проверка *аутентичности* по стандарту 802.1x в больших сетях обычно осуществляются специальным сервером, чаще всего RADIUS (Remote Authentication Dial-In User Service).

## Угрозы безопасности WPA

Протокол WPA, хоть и является более защищённым, чем WEP, но имеет уязвимости, обусловленные используемым алгоритмом шифрования RC4 и использованием алгоритма CRC32, который не дотягивает по требованиям до криптографической хеш-функции.Перебор — это единственный способ подобрать ключ для закрытой WPA/WPA2 сети. Метод гарантирует успех, но если ключ достаточно длинный и не находиться в словарях, то можно считать себя защищенным от этой атаки. Зато, таким образом взламываются как wpa-tkip так и wpa2-ccmp сети, но лишь в PSK режиме. Эта атака встроена в пакет aircrack-ng.Сначала нужно словить аутентификацию клиента, чтобы на основании ее уже восстанавливать основной ключ. Это проще всего сделать запустив *airodump-ng* и дождавшись аутентификации, либо запустив атаку деаутентификации

убыстрить процесс поможет использование специализированных микроконтроллеров или, как мы раньше описывали — видеокарт. Без этого перебор всех возможных ключей займет слишком много времени.

***--Тут можно ещё немного добавить про атаки на устройства интернет вещей…***

**Заключение**

описание и выявлено предназначение беспроводной технологии WI-FI. Описан протокол безопасного доступа WPA.

Во второй главе Рассмотрен механизм шифрования сообщения в WPA. Также описан основной способ перехвата сообщения по протоколу WPA.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Беспроводные сети WI-FI. – М.: Интернет – университет информационных технологий, Бином. Лаборатория знаний, 2013 – 216 c.
2. Брэгг, Р. Безопасность сетей: полное руководство [Текст] / Р. Брэгг, М. Родс-Оусли, К. Страссберг. – М.: Эком, 2015 – 912 c.
3. «Беспроводные сети. Первый шаг» / Джим Гейер. – М.: Издательство: Вильямс, 2010
4. «Секреты беспроводных технологий» / Джек Маккалоу. – М.: НТ-Пресс, 2009
5. «Современные технологии беспроводной связи» / Шахнович И. – М.: Техносфера, 2014
6. «Сети и системы радиодоступа» / Григорьев В.А., Лагутенко О.И., Распаев Ю.А. – М.: Эко-Трендз, 2016