## ****Протоколы обеспечения конфиденциальности и целостности****

## ****данных****

**За всю историю разработок механизмов защиты информации для беспроводных сетей стандарта 802.11 было официально принято три протокола инкапсуляции, основное назначение которых обеспечить конфиденциальность и целостность передаваемой информации. Такимипротоколамиявляются:**

* **WEP (WiredEquivalentPrivacy) – первый протокол инкапсуляции стандарта 802.11, принятый в 1999 году Институтом инженеров электротехники и электроники.**
* **TKIP (TemporaryKeyIntegrityProtocol) – протокол целостности временного ключа.**
* **CCMP (CounterModewithCipherBlockChainingMessageAuthenticationProtocol) – протокол инкапсуляции, который использует алгоритм блочного шифрования AES в режиме счетчика для шифрования данных и AES в режиме сцепления блоков для выработки кода аутентичности сообщения.**

**WEP(WiredEquivalentPrivacy)**

WEP—протокол инкапсуляции, принятый в стандарте IEEE 802.11в 1999г. для обеспечения безопасности беспроводной сети**. Основной задачей при разработке являлось обеспечить с помощью данного алгоритма безопасность беспроводной сети эквивалентную безопасности проводной [20].**

Кадр WEP (Рис. 18) включает в себя следующие поля:

1. IV (Initialization Vector)
   * Вектор инициализации (InitializationVector)
   * Пустое место (Pad)

* Идентификатор ключа (Key ID)

1. Данные (Data)
2. ICV (Integrity Check Value)

### 

Рис. 18. Формат кадра WEP

Согласно спецификации, WEP использует алгоритм шифрования RC4 с 40-битным или 104-битным ключом. В WEP используется генератор псевдослучайных чисел (Pseudo-RandomNumberGenerator - PRNG) для создания криптографического ключевого потока. PRNG генерирует последовательность битов, которая затем объединяется с открытым текстом, посредством суммирования по модулю два. Для обеспечения целостности сообщений в WEP используется специальное числовое значение, называемое IntegrityCheckValue (ICV), которое вычисляется по алгоритму нахождения контрольной суммы CRC-32 (CyclicRedudancyCheck). Для осуществления процедуры шифрования протокол генерирует ключ для каждого MPDU, называемый WEPSeed, путем объединения 24-битного вектора инициализации и 104-битного ключа шифрования.

В протоколе инкапсуляции WEP (Рис. 19) осуществляется три преобразования открытого текста MPDU для осуществления инкапсуляции:

1. Вычисление ICV через открытый текст MPDU
2. Шифрование открытого текста MPDU и ICV с помощью ARC4
3. Кодирование вектора инициализации и добавление идентификатора ключа (keyidentifier) в поле IV.



Рис.19. Протокол инкапсуляции WEP

Для декапсуляции к MPDU также применяется три преобразования:

1. WEP извлекает вектор инициализации и идентификатор ключа из принятого MPDU
2. WEP использует сконструированный WEPSeed для расшифровки сообщения и получения открытого текста и ICV. Расшифрование состоит из регенерации ключевого потока и суммирования его с шифрограммой по модулю два для восстановления исходного текста. Другая главная часть алгоритма - функция инициализации, которая использует ключ переменной длины для создания начального состояния генератора ключевого потока.
3. Далее происходит вычисление ICV и сравнение полученного значения с принятым.

**TKIP(Temporal Key Integrity Protocol)**

### Протокол инкапсуляции TKIP (Рис. 20)был разработан рабочей группой IEEE 802.11iи объединением производителей беспроводных устройств Wi-FiAliance как временное решение, призванное заменить WEP, не требуя замены оборудования. Это было необходимо, поскольку к тому времени было осуществлено несколько успешных атак на WEP, поэтому разрабатываемое решение должно было быть применимо к уже развернутым аппаратным средствам. TKIPбольше не считается безопасным. В стандарте 802.11 – 2012 TKIPопределяется как необязательный алгоритм концепции RSNи использование его возможно только для защиты кадров данных.

TKIP, также, как и WEP использует RC4 для шифрования, но в отличие от него в TKIP присутствует ряд улучшений[10]:

### 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.

Процесс инкапсуляции состоит из следующих этапов:

### Вычисляется MIC. Вычисление MIC позволяет защитить поле данных MSDU и поля адреса источника и назначения.

### При необходимости происходит фрагментация MSDU вместе с MIC на несколько MPDU. TKIP устанавливает монотонно возрастающее значение TKIPSequenceCounter (TSC) и следит за тем, чтобы для всех MPDU полученных из одного MSDU поле ExtendenIV (расширенный вектор инициализации) было одинаково.

### Для каждого MPDU в TKIP используется функция смешивания ключей, для получения WEPSeed, который представляет из себя совокупность ключа и вектора инициализации для алгоритма шифрования RC4 [21].

### WEPSeed передается вместе с каждым MPDU в блок шифрования для получения.

Рис. 20.ИнкапсуляцияTKIP

Для декапсуляциисообщения (Рис. 21) протокол TKIP выполняет следующие действия:

### Перед деапсуляцией принятого MPDU извлекается порядковый номер TSC и идентификатор ключа из полей WEPIV и extendedIV и переходит к построению WEPSeed. Если в результате проверки TSC обнаружится, чтоMPDU нарушает правила упорядоченности, он будет отброшен.

### Вычисляется WEPSeed, который представляется как вектор инициализации и ключ шифрования.

### Далее проверяется ICV. Если проверка прошла успешно, происходит дефрагментация MPDU в MSDU. Проверяется MIC. Если дефрагментация не удается – пакет отбрасывается.На этапе проверки MIC, преемник вычисляет свое собственное значение кода целостности и сравнивает его с полученным в сообщении.Если принятый и локально вычисленный MIC идентичны, MSDU передается на уровень выше, если значения отличаются, MSDU отбрасывается и алгоритм переходит к контрмерам.



Рис. 21.ДекапсуляцияTKIP

**CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)**

CCMP –протокол инкапсуляции, который создавался в рамках поправки кстандарту [802.11i](http://ru.wikipedia.org/wiki/IEEE_802.11) для замены[TKIP](http://ru.wikipedia.org/wiki/TKIP),как боле енадёжный вариант [10].CCMP является обязательным для применения в стандарте [WPA2](http://ru.wikipedia.org/wiki/WPA2), и необязательнымв стандарте [WPA](http://ru.wikipedia.org/wiki/WPA).CCMPиспользуетблочный шифрAdvancedEncryptionStandard ([AES](http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard)) вместо потокового шифра RC4 в WPEи TKIP. Для шифрования данных CCMP использует шифр AESв режиме счетчика (CounterMode) и для обеспечения целостности и аутентичности сообщений AESв режиме сцепления блоков (CipherBlockChaining)

CCMP обеспечивает целостность как поля данных пакета [MPDU](http://ru.wikipedia.org/w/index.php?title=MPDU&action=edit&redlink=1), то есть пакета, передающегося по сети, так и некоторых частей заголовка пакета стандарта [IEEE 802.11](http://ru.wikipedia.org/wiki/IEEE_802.11). Все процедуры AES, производимые в CCMP, осуществляютсяс помощью 128-битного [ключа](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) со 128-битным блоком. CCM имеет два параметра (М и L), и в алгоритме CCMP они имеют следующие значения [22]:

* M = 8 (указывает, что длина поля MIC 8 октетов);
* L = 2 (указывает, что длина поля составляет 2 октета).

На вход алгоритма CCMподаются следующее параметры:

* временный ключ (TK);
* nonce - случайное числовое значение;
* AAD (AdditionalAuthenticationData) - дополнительные аутентификационные данные;
* IEEE 802.11 MPDU –тело кадра.

Необходимое требование алгоритма CCM - использования нового временного ключа для каждой новой сессии [10]. Значения временных ключей начинаются со значения временного ключа, являющегосялибо частью PTK, полученного в результате процедуры выработки ключей для защиты одноадресноготрафика, либо частью GTK, полученного в результате процедуры выработки ключей для защиты широковещательного и многоадресноготрафика.104-битный Nonceформируется из номера пакета (PacketNumber – PN), из поля Priority, в котором указываются данные о приоритете кадра, используемые в QoSи поля Address 2 (A2), в котором хранится адрес передатчика [23]. 48-разрядный номер пакета (PN) увеличивается на единицу после каждой передачи кадра. ЗначениеNonce для каждого кадра, защищённого конкретным временным ключом должно быть уникально.Дополнительные аутентификационные данные строятся из частей заголовка MAC и необходимы для защиты целостности этих частей [23].IEEE 802.11 MPDU –тело кадра которое будет инкапсулировано в MSDUболее высокого уровня и защищено MIC.При инкапсуляции CCMPисходный размер MPDUувеличивается на 16 октетов, 8 октетов для поля Заголовок MAC и 8 октетов для поля MIC(Рис. 22).



Рис. 22. Формат пакета CCMP

CCMPшифрует содержимое открытого текста MPDUи инкапсулирует полученный шифротекст (Рис. 23), выполняя следующие преобразования:

### Номер пакета увеличивается на единицу. Это необходимо, чтобы обеспечить новый номер пакета для каждого нового MPDU.

### С помощью полей в заголовке MACконструируется AdditionalAuthenticationDataдля CCM.

### С помощью полей PN, A2 и Приоритет MPDU (в существующей реализации поле Приоритет MPDU (Priority) является зарезервированным и устанавливается в ноль)строится CCMNonceblock, который является вектором инициализации.

### Формируется заголовок CCMP.

### CCMPзапускает AESв режиме счетчика и с помощью временного ключа, AAD, Nonce формирует шифротекст и MIC.

### ЗашифрованныйMPDUформируется конкантенацией оригинального заголовка MAC, заголовка CCMP, зашифрованных данных и MIC.



Рис. 23. Инкапсуляции CCMP

### Процесс декапсуляции (Рис. 24) состоит из следующих этапов:

### ЗашифрованныйMPDU анализируется для построения Nonce и AAD.

### AAD формируется из заголовка зашифрованного MPDU.

### С помощью полей PN, A2 и Приоритет MPDU строится CCMNonceblock.

### MIC извлекается и используется для проверки целостности сообщения.

### Процесс дешифрования CCM использует временный ключ, AAD, Nonce, MIC и шифротекстMPDU ля восстановления открытого текста MPDU, а также для проверки целостности восстановленного открытого текста и AAD.

### Проверяется номер пакета для предотвращения повторной передачи MPDU.



Рис. 24. ДекапсуляцииCCMP