Анализ безопасности беспроводных сетей в стандарте IEEE 802.11

Выполнил:
Студент 911 гр.
Якимов Михаил

Долгопрудный
2003

1. Обеспечение безопасности в стандарте IEEE 802.11

Безопасность в стандарте IEEE 802.11 обеспечивается с помощью сервиса аутентификации и механизма WEP (Wired Equivalent Privacy). Область применения этих сервисов ограничивается обменом данными непосредственно между станциями. Сервис, предлагаемый реализацией механизма WEP – это шифрование MSDU (MAC Service Data Unit).
WEP обеспечивает :

1) конфеденциальность;
2) аутентификацию;
3) управление доступом (в данной статье не рассматривается).

2. Алгоритм WEP

2.1 Введение

Подслушивание является основной проблемой всех беспроводных технологий. Протокол 802.11 определяет алгоритм защиты информации эквивалентный проводной LAN. WEP вводится для защиты авторизованных пользователей беспроводной LAN от случайного подслушивания. Этот сервис предназначен обеспечивать беспроводную LAN функциональными возможностями эквивалентными функциональным возможностям проводной среды.

2.2 Свойства алгоритма WEP

1) Разумная криптостойкость:
   Защита, предоставляемая алгоритмом, основывается на сложности вскрытия секретного ключа прямым перебором. Это в свою очередь связано с длиной секретного ключа и частотой смены ключей. WEP позволяет замену ключа (k) и частое изменение Вектора Инициализации (IV).
2) Самосинхронизация:
   Алгоритм WEP самосинхронизован для каждого сообщения. Это свойство критично для алгоритма шифрования канального уровня, так как интенсивность потерь пакетов может быть довольно высокой.
3) Эффективность:
   Алгоритм WEP эффективен и может быть реализован как аппаратно так и программно.
4) Дополнительность:
   Реализация и использование алгоритма WEP – дополнение протокола 802.11

2.3 Работа алгоритма WEP

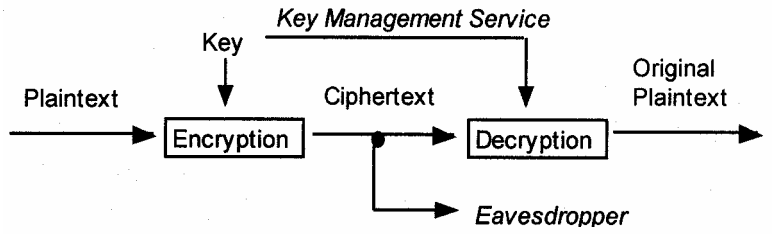

Схема 1, Защищенный информационный канал

Алгоритм WEP является формой электронной кодовой книги, в которой блоки открытого текста побитно складываются с последовательностью псевдослучайных ключей такой же длины. Последовательность ключей генерируется алгоритмом WEP.

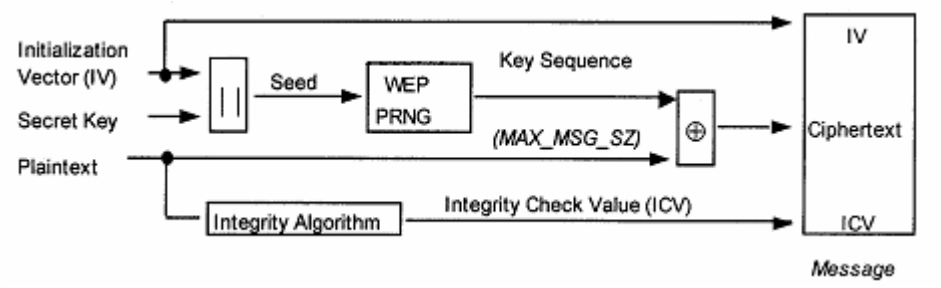

Схема 2, Процедура шифрования

Процедура шифрования начинается с выбора секретного ключа, который распределяется между станциями с помощью внешнего сервиса управления ключами. WEP является симметричным алгоритмом, в котором один ключ используется и для шифрования и для расшифрования.
Секретный ключ соединяют с Вектором Инициализации, а результат (Seed) подают на вход генератора псевдослучайных чисел (PRNG). В PRNG используется алгоритм RC-4. На выходе PRNG появляется ключевая последовательность k псевдослучайных бит длиной равной максимальной длине MPDU (MAC Protocol Data Unit). К открытому тексту применяются два процесса. Для защиты от неавторизованного изменения данных, действуя интегральным алгоритмом на открытый текст, получают интегральную сумму (ICV). Шифрование заканчивается побитным сложением ключевой последовательности с открытым текстом. В результате получают сообщение, содержащее шифротекст, IV и ICV.
Критической частью процедуры шифрования является генерация псевдослучайных чисел с помощью PRNG, так как он преобразует относительно короткий секретный ключ в ключевую последовательность произвольной длины. Это значительно упрощает задачу распространения ключей, так как станциям нужно сообщить только секретный ключ. IV продлевает срок действия секретного ключа и обеспечивает свойство самосинхронизации алгоритма. Секретный ключ остается постоянным, пока IV периодически изменяется. Каждый новый IV “порождает” новую ключевую последовательность, таким образом существует взаимооднозначное соответствие между IV и k. IV можно изменять для каждого MPDU и так как IV передается вместе с сообщением, приемник всегда сможет расшифровать любое сообщение. IV можно распространять не шифруя, так как он не обеспечивает атакующую сторону какой-либо информацией о секретном ключе.
Алгоритм WEP применяется ко всему MPDU. Триплет {IV, MPDU, ICV} формирует информацию, которую нужно послать в информационном фрейме.
Для того чтобы WEP защищал фреймы, первые 4 байта тела фрейма содержат поле IV:

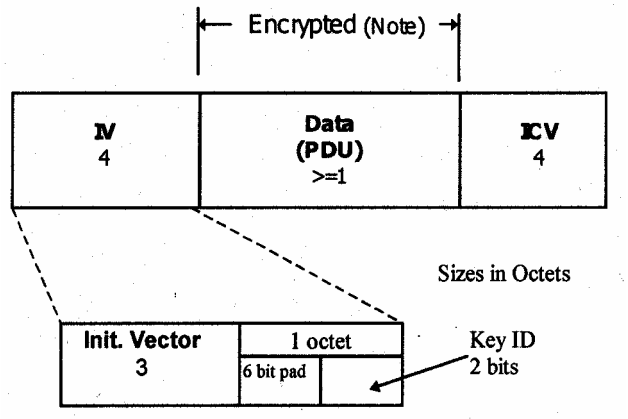

Схема 3, Расширенный MPDU

IV предшествует MPDU, за которым следует 32-х битный ICV, полученная с помощью алгоритма CRC-32.
Расшифрование начинается с приходом сообщения. IV входящего сообщения будет использоваться для генерирования ключевой последовательности, необходимой для расшифрования этого сообщения. Смешивание текста с надлежащей ключевой последовательностью дает исходный открытый текст. Корректное расшифрование будет

проверено алгоритмом интегральной проверки, сравнением интегральных сумм, полученных применением к расшифрованному тексту этого алгоритма и непосредственно из сообщения. Если эти суммы не равны, то принятый MPDU считается принятым по ошибке.

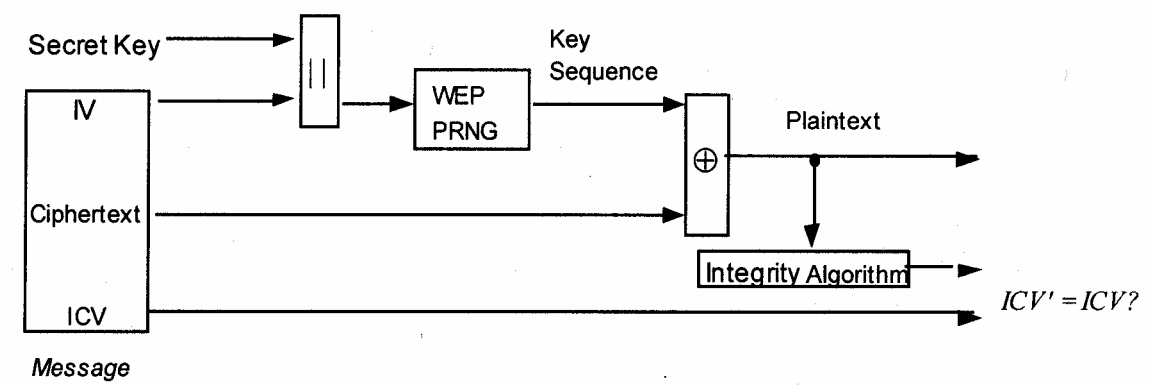

Схема 4, Процедура расшифрования

3. Недостатки алгоритма WEP и способы их устранения

3.1 Недостатки и уязвимости алгоритма WEP

A) Ключ RC-4, используемый для шифрования информационного фрейма, является комбинацией IV и секретного ключа. К сожалению, в алгоритме RC-4, первые байты ключа предсказуемы при достоверно известных значениях IV. А так как IV, используемый для шифрования данного фрейма, передается открыто, то пассивный наблюдатель может легко распознать фреймы направляющиеся адресату и провести атаку.
B) При достаточно большом количестве станций возможно совпадение значений IV, что влечет за собой возможность атаки, направленной на извлечение шифрованной информации.
C) Секретный ключ непосредственно используется в качестве секретной части ключа шифрования.

3.2 Расширение алгоритма шифрования

Расширения алгоритма шифрования определяются для более надежного шифрования данных, аутентификации беспроводного MAC-уровня и для стандартизации использования аутентификации на вышележащих уровнях [2].
Разработаны 2 возможных улучшенных метода шифрования:

A) Улучшенная версия алгоритма RC-4 (RC-4/per-frame IV);
B) Применение 128-битного AES.

Предложены 4 возможных дополнения к алгоритму WEP:

A) Использование пакетной хэш-функции и правила выбора последовательных IV [3][4];
B) Использование алгоритмов генерации временных ключей;
C) Использование механизмов перемены ключей;
D) Использование кода аутентификации сообщения, названного интегральным кодом сообщения.

3.2.1 Пакетная хэш-функция

Пакетная хэш-функция введена в основном для того, чтобы не было возможности извлечь секретный ключ из IV, кроме того в ней определена возможность использования MAC-адреса передающей станции в качестве входного параметра. Это позволяет каждой передающей станции генерировать уникальный поток IV и тем самым предотвращать повторы значений IV среди станций, использующих общий секретный ключ. Значения IV не должны многократно использоваться для избежания повтора ключевых потоков, а следовательно и атак, направленных на восстановление шифрованных данных.
Ниже рассмотрено упрощенное описание алгоритма пакетной хэш-функции. Детальное описание алгоритма приведено в [3]. Алгоритм описывается за 2 шага, каждый из

которых использует S-боксы для перемешивания и замены 16-и битных величин. На первом шаге 128-и битный временный ключ и старшие 32 бита MAC-адреса передающей станции хэшируются в 128-и битную величину, состоящую из 8-и 16-и битных значений, как показано на схеме 5:

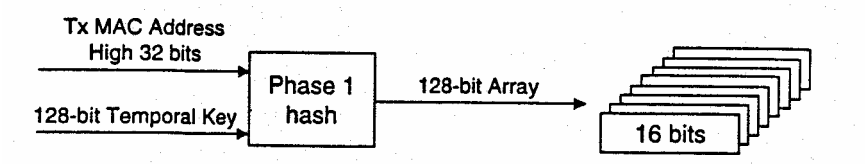

Схема 5, Первый шаг хэширования

На втором шаге берется 128-и битный массив из шага 1 вместе с IV и генерируется 128-и битный пакетный ключ. Этот ключ, согласно своему названию, будет использоваться только для одного пакета. Второй шаг хэширования выполняется для каждого шифруемого пакета :

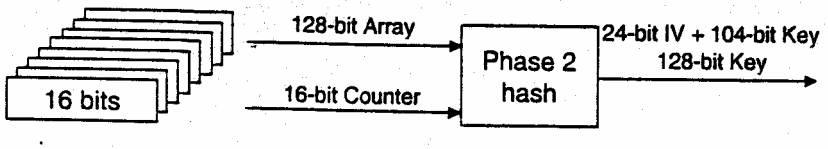

Схема 6, Второй шаг хэширования

Второй шаг состоит из 3-х подшагов : перемешивания в S-боксах, оперирующих над 16-и битными полями массива, применения функции перемешивания, использующей операции побитового сдвига и сложения и вычисления 24-х битного значения WEP IV. Второй шаг хэширования устраняет недостатки алгоритма выработки ключей WEP/RC-4.

3.2.2 Метод генерация временных ключей

Генерация временных ключей определяется методом, посредством которого секретный ключ не используется напрямую для шифрования пакетов данных, а лишь является основой для построения временных ключей. Эти временные ключи после могут быть использованы в качестве входных данных описанной выше пакетной хэш-функции. Заметим, что этот подход заметно отличается от изначального определенного в стандарте 802.11, в котором секретный ключ используется напрямую в качестве секретной части ключа шифрования.
Одним из предлагаемых методов генерации временных ключей является использование псевдослучайной функции, параметры которой:

Секретный ключ;
Строка текста;
MAC-адрес одной из станций;
Некое известное число.

На схеме 7 показано, как используются групповой секретный ключ и псевдослучайная функция для генерирования переходного ключа:

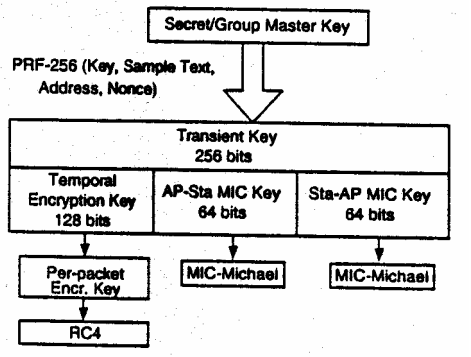

Схема 7, Пример генерирования временного ключа

Переходный ключ обеспечивает ключами не только протокол шифрования RC-4, но и функцию вычисления интегрального кода сообщения.
Использование временных ключей устраняет проблему повторного использования IV, так как относительно небольшое 24-х битное пространство IV векторов связывается с использованием одного секретного ключа шифрования. Чтобы временный ключ можно было применять для шифрования сообщений, новый секретный ключ нужно начинать использоваться до истощения пространства векторов IV. Таким образом размерность пространства векторов IV определяет то, как часто должен вычисляться временный ключ. Пакетная хэш-функция, описанная выше, поддерживает 16-и битный IV, требуя новый временный ключ через каждые 65536 пакетов. Важно, однако, что при любом ключе данный IV применяется для шифрования одного и только одного пакета.

3.2.3 Интегральный код сообщения

Интегральный код сообщения (MIC) нужен для проверки правильности переданного пакета с данными. При использовании MIC проверяется, что пакет не был изменен при передаче или что адреса источника и приемника не были изменены. MIC необходимо использовать для предотвращения “bit-flipping” атак.

3.2.4 Шифрование AES

Шифрование на MAC-уровне также может быть усилено использованием дополнительного алгоритма шифрования. Для этих целей можно выбрать алгоритм AES Rijndael. Это алгоритм шифрования следующего поколения, заменивший DES и 3DES.

3.3 Определение и распространение ключей шифрования

В стандарте 802.11 определены два метода использования WEP ключей между двумя станциями: ключи по-умолчанию (Default Keys) и метод таблиц ключей (Mapped Keys).

3.3.1 Описание метода ключей по-умолчанию

В настоящее время метод ключей по-умолчанию поддерживается большинством продуктных реализаций протокола 802.11. Он основывается на использовании на каждой станции набора четырех ключей по-умолчанию, один из которых обозначается в качестве передающего ключа. Все четыре ключа могут быть использованы для расшифрования приходящих фреймов. Поле IV в принятом фрейме указывает, какой ключ по-умолчанию был использован при шифровании. Такой же ключ должен быть использован и при расшифровании.
В этом случае таблица ключей содержит значения только четырех ключей:

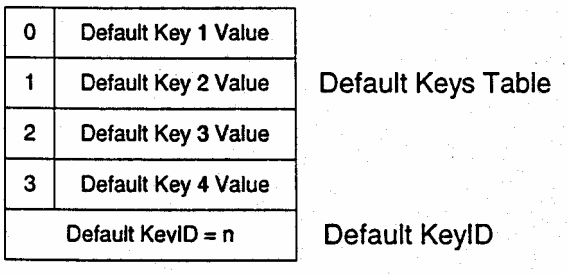

Схема 8, Таблица ключей по-умолчанию

3.3.2 Описание метода таблиц ключей

Метод таблиц ключей дает способ использования уникальных ключей при соединении между двумя станциями. Станция пользующаяся этим методом хранит таблицу, которая сопоставляет MAC-адреса значениям ключей.
Если нужно передать фрейм станции, MAC-адрес которой есть в таблице, то для шифрования используется ключ, соответствующий этой станции. Если фрейм принимается от станции, MAC-адрес которой есть в таблице, то для расшифрования используется ключ, соответствующий этой станции. Во всех фреймах ,передаваемых таким способом, биты KeyID поля IV должны быть нулевыми. Работа по этому методу

означает, что таблицы двух станций, которым нужно связаться, должны содержать MAC-адреса друг друга и поставленные в соответствие этим MAC-адресам значения ключей. Базовая станция может поддерживать оба метода использования ключей одновременно. Если в сопоставляющей таблице присутствует необходимый элемент, то применяется метод таблиц ключей. Метод ключей по-умолчанию должен использоваться только если в сопоставляющей таблице нет соответствующей записи.
Так методы смены ключа используют возможности как ключей по-умолчанию, так и таблиц ключей.

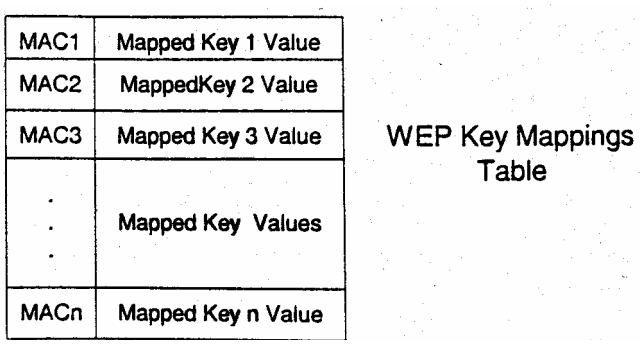

Схема 9, Сопоставляющая таблица

3.3.3 Методы смены ключа

A) Использование неявного временного метода;
B) Использование управляющих сообщений MAC-уровня;
C) Использование аутентификационных сообщений более высоких уровней (в данной статье не рассматривается)

3.3.3.1 Метод управляющих сообщений MAC-уровня

В этом подходе происходит явное выражение инициализации ключей и смены ключей с помощью введения новых управляющих сообщений MAC-уровня.Определяются пять новых типов сообщений. Простой пример показан на схеме:

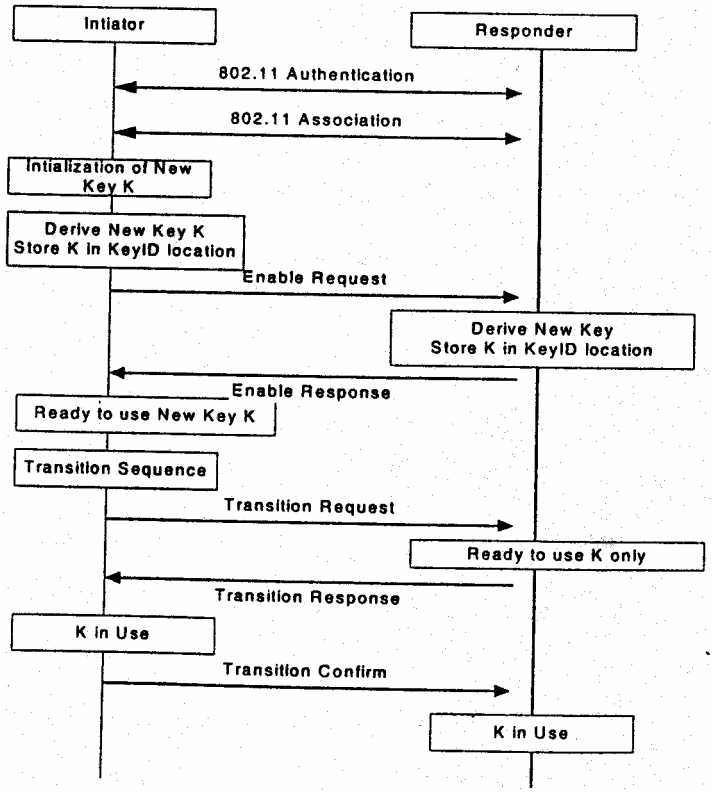

Схема 10, Пример потока сообщений о смене ключа

Преимущество этого подхода состоит в однозначности перехода к новому ключу. Обе стороны убеждаются в том, что у них нет дополнительных сообщенийна отправку, которые могут быть зашифрованы предыдущим ключом.

3.3.3.2 Временной метод

Временной метод использует синхронизирующие сообщения, определенные протоколом 802.11, для предоставления данных для генерации временного ключа и для индикации события изменения ключа. Эти сообщения посылаются через определенное протоколом время TBTT (Targeted Beacon Transmit Time).Состояние TBTT может быть использовано для определения требуется ли новая безопасная хэш и какой набор ключей используется.

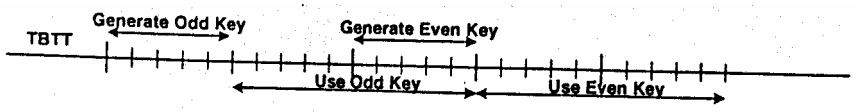

Схема 10, Изменение ключа с изменением TBTT

8 octets	4 octets	1 octet	4 octets	1 octet	1 octet	8 octets
Nonce	Cipher Suite	KeyID	Key Sequence Number	Rekey Count	Rekey Period	MIC

Схема 11, Информационная часть самосинхронизирующегося фрейма смены ключа

Над синхронизирующим сообщением также осуществляется алгоритм интегрального кода сообщения, что защищает поля синхронизирующего фрейма от подделки атакующей стороной.

3.3.4 Генерация и распространение секретного ключа

Механизм распределения ключей не определен в протоколе. В методах использования ключей предполагается, что ключи обеспечиваются прикладными методами более высоких уровней. В настоящее время используется автоматическое распределение ключей с помощью специальных инструментальных средств и с помощью ручного ввода ключей.

4. Текущие проблемы и прикладные решения

В последнее время большое внимание уделяется тому факту что алгоритм WEP, определяемый протоколом IEEE802.11, не достаточно устойчив к различного рода атакам. Уязвимости алгоритма WEP обсуждаются в статьях [8] и [9]. В этом разделе представлен обзор доступных на сегодняшний день прикладных решений предотвращающих недостатки WEP.
Одним из способов исправления недостатков WEP на MAC–уровне является использование шифрования на более высоких уровнях. Согласно IEEE и WECA(Wireless Ethernet Compatibility Alliance),” Уровни безопасности могут располагаться над уровнем беспроводной LAN. Здесь можно привести пример использования Виртуальных Частных сетей(VPNs), для которых беспроводная LAN просто прозрачна”[10]. Покрытие Виртуальной Частной Сетью беспроводной LAN может быть дорогостоящим, требовать дополнительного оборудования(VPN серверы) и затрат на техническую поддержку. Однако, некоторые приложения могут отлично работать с помощью VPN. Так, для удаленного доступа обычно используются IPSec клиенты. Такая же VPN инфраструктура может использоваться для беспроводного клиентского доступа. Большинство базовых станций (точек доступа) беспроводных LAN, включая базовую станцию ORiNOCO AP-500, AP-1000 и AP-2000, предназначены для прозрачной работы с VPN.
Для некоторых пользователей желателен ввод в действие недорогих базовых станций, обеспечивающих безопасность на уровне приложений. Так, например, в общественных местах основные интересы многих операторов связаны в основном с экономическим

аспектом вопроса распространения беспроводных сетей. Провайдеры обеспечивают доступ огромному количеству пользователей и обеспечивают простые в использовании Web интерфейсы для регистрации пользователей. При этом безопасность обеспечивается на сетевом уровне с помощью IPSec доступа к VPN корпоративных сетей.
Для приложений, требующих более сильного шифрования на беспроводном MAC уровне, где технология VPN не используется, так же существуют некоторые решения. Например, ORiNOCO Access Server (AS-2000) обеспечивает шифрование отличное от WEP на программном уровне, исключающее множество уязвимостей WEP и является сессионным, а не пакетным(см. 3.2). В этом случае состояние алгоритма не сбрасывается каждый раз при передаче нового пакета, как это реализовано в алгоритме WEP. Вместо этого состояние алгоритма в конце передачи предыдущего пакета используется для начала шифрования следующего. Кроме того, для шифрования изходящего и входящего трафика на каждой станции используются уникальные пользовательские ключи. Пользовательское сессионное шифрование, поддерживаемое AS-2000, обеспечивает защиту от пассивных атак прослушивания эфира. Примерами собственно решений в этой области являются Reefedge connect Server [10] и Musenki Layer 2 IPSec [11].
Для дальнейшего развития 802.11 беспроводных сетей требуются решения, основанные на определенных стандартах, улучшающие взаимодействие различных устройств и способные к развитию. Эти решения должны улучшать характеристики и безопасность протокола 802.11b, а также поддерживать необходимую полосу пропускания в протоколах 802.11a и 802.11g. Для этого является существенным улучшенное шифрование, аутентикация и управление ключами. Ожидается, что в продукты большинства производителей будет включена поддержка стандарта 802.11i.

Литература:

[1] IEEE 802.11b, See section 8.3.2(pp. 65-69) and annex B (pp. 477-481)
[2] http://grouper.ieee.org/groups/802/11
[3] R. Housley and D. Whiting, “Temporal Key Hash”, IEEE 802.11-01/550.
[4] R. Housley, D. Whiting and N. Ferguson, “Alternative Temporal Key Hash ”, IEEE 802.11i, 11-02-282r0.
[5] http://www.esat.kuleuven.ac.be/~rijmen/rijndael
[6] W. Diepstraten, et al., “Extended WEP Proposal”, August 2001draft .
[7] N. Borisov, I. Goldberg, and D. Wagner “802.11 Security” , http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[8] J. Walker, “Unsafe at Any Key Size: An Analysis of the WEP Encapsulation”, November 2000
[9] IEEE Wi-Fi WEP Security , www.wi-fi.org/pdf/Wi-FiWEPSecurity.PDF
[10] See http://www.reefedge.com
[11] See http://www.musenki.com