МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКИЙ ФИЗИКО - ТЕХНИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

кафедра радиотехники

Безопасность в беспроводных сетях стандарта IEEE 802.11: Протокол WEP

Эссе по курсу "Защита информации"
студента 011 группы Лютова Владимира.

Долгопрудный, 2004

Введение

В последние годы беспроводные сети передачи информации стали одним из основных направлений развития сетевой индустрии. Изначально беспроводные сети применялись при объединении и расширении существующих проводных сетей, а также для решения проблемы «последней мили». С расширением рынка портативных и карманных компьютеров (PDAs) беспроводные технологии стали использоваться и для обеспечения мобильного доступа к ресурсам Internet - появились так называемые точки доступа “Hot Spot” и небольшие локальные “ad hoc” сети, состоящие из мобильных терминалов пользователей.

Одним из наиболее распространённых стандартов, используемых при построении беспроводных сетей, является IEEE 802.11. Он описывает физический и канальный уровни (согласно модели OSI ISO) сети, затрагивая также некоторые вопросы безопасности. Именно аспектам безопасности сетей стандарта IEEE 802.11 и будет посвящена данная работа.

В беспроводной сети проблема прослушивания имеет особую важность, и для её решения в стандарте 802.11 определяется протокол WEP (Wired Equivalent Privacy). Схема WEP предназначена, главным образом, для обеспечения:

- *Конфиденциальности*: предотвращение элементарного прослушивания.
- *Контроля доступа*: защита сети от несанкционированного доступа к её ресурсам.
- *Целостности данных*: обнаружение искажений и изменений в передаваемых данных (эту функцию выполняет поле CRC - Cyclic Redundancy Check).

Особенности WEP-протокола:

- Достаточно устойчив к атакам, связанным с простым перебором ключей шифрования, что обеспечивается необходимой длиной ключа и частотой смены ключей и инициализирующего вектора.
- Самосинхронизация для каждого сообщения. Это свойство является ключевым для протоколов уровня доступа к среде передачи (Data Link in OSI reference model), где высок уровень искажённых и потерянных пакетов.
- Эффективность: WEP может быть легко реализован.
- Открытость.
- Использование WEP-шифрования не является обязательным в сетях стандарта IEEE 802.11.

Шифрование WEP

Пусть $E_k(\cdot)$ – процесс шифрования с ключом k; P – открытый текст; C – шифротекст; $D_k(\cdot)$ – процесс расшифрования. Тогда,

$$E_k(P) = C$$

$$D_k(C) = P$$

$$D_k(E_k(P)) = P$$

Общая схема процесса обмена информацией между передатчиком и приёмником приведена на Рисунке 1.

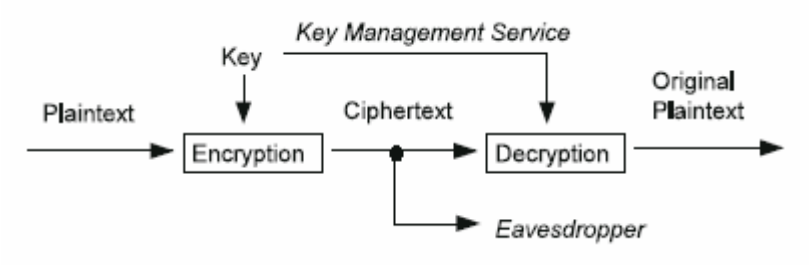


Рис.1

В WEP используется симметричный алгоритм шифрования, в котором один и тот же ключ используется как для шифрования, так и для обратного процесса – расшифрования.
Итак, шифрование происходит следующим образом (см. Рисунок 2). До начала процесса шифрования 40-битный секретный ключ распределяется между всеми станциями, входящими в беспроводную сеть. К секретному ключу добавляется вектор инициализации (*IV*). Получившийся блок – это начальное число генератора псевдослучайной последовательности (PRNG), определённого в RC4. Генератор создаёт последовательность битов, длина которой равна длине блока данных MAC-кадра плюс CRC. Алгоритм обеспечения целостности – это простая 32-битная последовательность циклической проверки чётности с избыточностью (CRC-32), присоединяемая к концу блока данных MSDU (MAC Service Data Unit). Побитовое применение операции исключающего ИЛИ к MSDU (+*ICV*) и псевдослучайной последовательности даёт шифрованный текст. К данному тексту присоединяется вектор инициализации и результат передаётся.

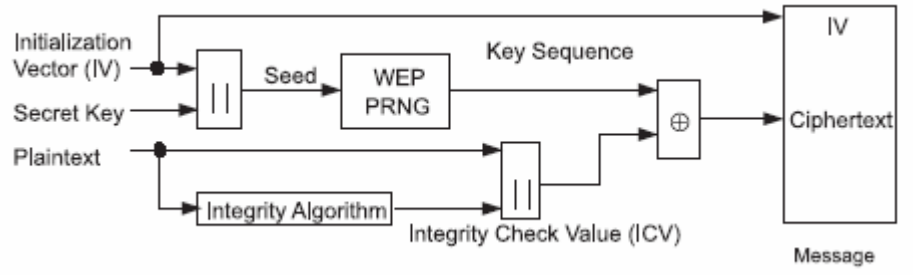


Рис.2

Генератор псевдослучайной последовательности (PRNG) играет ключевую роль в процессе шифрования. Он преобразует относительно короткий ключ в последовательность произвольной длины. Начальный вектор (*IV*) увеличивает «время жизни» ключа и обеспечивает самосинхронизацию протокола после каждого этапа шифрования. Его значение может меняться при каждой передаче MAC-кадра, а, следовательно, меняется и псевдослучайная последовательность, что усложняет задачу дешифрования перехваченного текста.

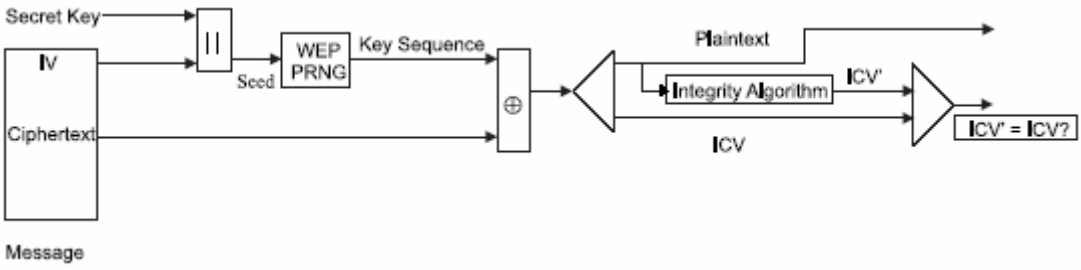


Рис.3

После получения сообщения (см. Рисунок 3) приёмник извлекает вектор инициализации и присоединяет его к совместно используемому секретному ключу, после чего генерирует ту же

псевдослучайную последовательность, что и источник. К полученному таким образом ключу и поступившим данным побитово применяется операция исключающего ИЛИ, результатом которой является исходный текст: $(A \oplus B) \oplus B = A$.

Приёмник сравнивает полученное значение *ICV* и *ICV*, вычисленное по восстановленным данным: если величины совпадают, то данные считаются неповреждёнными.

Структура блока данных MAC-кадра.

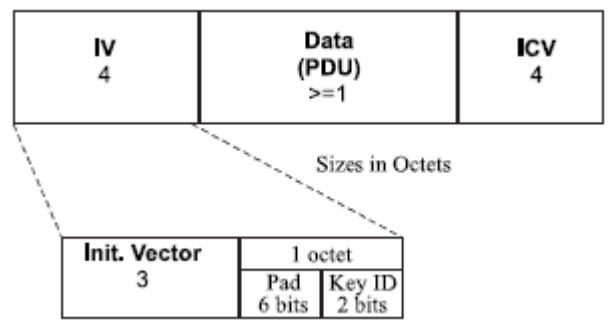


Рис.4

Поле IV содержит 3-х байтовое значение вектора инициализации, 2-х битовый идентификатор ключа и 6 «пустых» бит (заполняются нулями). Идентификатор ключа определяет один из 4-х возможных секретных ключей.

Генератор случайной последовательности – шифр RC4

RC4 – это потоковый шифр с переменным размером ключа, разработанный в 1987 году RSA Data Security, Inc.

Операции производятся над байтами начального вектора, состоящего из секретного ключа *K* и вектора инициализации *IV*; причём для одного и того же блока данных каждый раз получаются различные последовательности (за счёт случайности выбора *IV*).

Используется массив S размером 16x16 байт, элементы которого – числа от 0 до 255. В алгоритме применяются два счётчика – i и j.

Инициализация S производится следующим образом:

- сначала заполняем его линейно - $S_0 = 0,\ S_1 = 1,\ \ldots,\ S_{255} = 255$;
- затем заполняем начальным вектором (*K* + *IV*) другую 256-байтовую матрицу - $I_0, I_1, \ldots, I_{255}$;
- $j = 0$;
- for $i = 0$ to 255:
  $j = (j + S_i + I_i) \bmod 256$;
- поменять местами S_i и S_j.

Теперь для генерации случайного байта *K* используется следующая последовательность действий (начальные значения счётчиков равны нулю):

- $i = (i + 1) \bmod 256$
- $j = (j + S_i) \bmod 256$
- поменять местами S_i и S_j
- $t = (S_i + S_j) \bmod 256$
- $K = S_t$

Для получения необходимого количества байтов, составляющих псевдослучайную последовательность, производят соответствующее число итераций генерирования байта *K*. Шифрование RC4 легко реализуемо и выполняется примерно в 10 раз быстрее, чем DES. Разработчики алгоритма утверждают, что он устойчив к дифференциальному и линейному криптоанализу, и что в нём отсутствуют короткие циклы.

Аутентификация

Стандарт IEEE 802.11 предполагает два типа аутентификации: «открытая система» и «открытый ключ». *Аутентификация открытых систем* просто позволяет двум сторонам договориться о передаче данных без рассмотрения вопросов безопасности. *Аутентификация с общим ключом* требует, чтобы две стороны совместно владели секретным ключом, не доступным третьей стороне. Процедура аутентификации такого типа между двумя сторонами, **A** и **B**, выглядит следующим образом.

1. **A** посылает кадр аутентификации, в котором указан тип «общий ключ» и идентификатор станции, определяющий станцию-отправителя.
2. **B** отвечает кадром аутентификации, который включает 128-октетный текст запроса. Текст запроса создаётся с использованием генератора случайных чисел WEP. Ключ и вектор инициализации, используемые при генерации запроса, не важны, поскольку далее в процедуре они не используются.
3. **A** передаёт кадр аутентификации, который включает полученный от **B** текст запроса. Кадр шифруется с использованием схемы WEP.
4. **B** получает зашифрованный кадр и дешифрует его, используя WEP и секретный ключ. Если дешифрование прошло успешно (совпали *CRC*), **B** сравнивает принятый текст запроса с текстом, который был послан на втором этапе процедуры. После этого **B** передаёт **A** сообщение аутентификации, содержащее код состояния (успех или неудача).

Уязвимость WEP

- Отсутствие сервиса распределения ключей.
  Чтобы обеспечить необходимый уровень безопасности секретный ключ должен достаточно часто меняться и быть уникальным для каждой пары взаимодействующих станций. Кроме того, для предоставления по-настоящему мобильного доступа в сеть Интернет назначение ключей должно быть динамическим. Все эти механизмы не оговорены в стандарте и не используются на практике.

- Недостаточная длина секретного ключа.

- Короткий вектор инициализации.
  При условии, что инициализирующий вектор изменяется при каждой новой попытке передачи кадра, активно работающая базовая станция (при среднем размере пакета - 500 байт и скорости передачи - 5 Mbit/s) исчерпает весь диапазон значений *IV* менее, чем за полдня. Длина IV фиксирована, она просто «встроена в стандарт» и её нельзя изменить, что является существенным недостатком внутренней структуры протокола, ограничивающим настройку параметров безопасности.

Поэтому легко может быть реализована «атака с известным открытым текстом»:

$$C_1 = P_1 \oplus RC4(IV, K_{BSS})$$

$$C_2 = P_2 \oplus RC4(IV, K_{BSS})$$

тогда $C_1 + C_2 = (P_1 \oplus RC4(IV, K_{BSS})) \oplus (P_2 \oplus RC4(IV, K_{BSS})) = P_1 \oplus P_2$

- таким образом, зная P_1 можно легко вычислить P_2.

- Генерирование вектора инициализации происходит неслучайно.
  В идеальном случае выборка нового вектора *IV* происходит случайно, но на самом деле реализация этого процесса целиком зависит от производителя сетевого оборудования, поскольку стандарт WEP не определяет алгоритм генерирования *IV*. Часто вектор *IV* просто линейно увеличивается или уменьшается при каждой передаче – такой подход противоречит одному из основных принципов обеспечения конфиденциальности при шифровании: случайность выборки ключей.

- Линейность CRC.
  Пусть $A \to B : (IV, C)$ и $C = RC4(IV, K_{BSS}) \oplus (M, CRC(M))$,
  тогда без труда можно подменить исходное сообщение M на M' - нужно лишь вместо *C* передать

$$C' = C \oplus (\sigma, CRC(\sigma)) = RC4(IV, K_{BSS}) \oplus (M, CRC(M)) \oplus (\sigma, CRC(\sigma)) =$$

$$= RC4(IV, K_{BSS}) \oplus (M \oplus \sigma, CRC(M) \oplus CRC(\sigma)) =$$

$$= RC4(IV, K_{BSS}) \oplus (M \oplus \sigma, CRC(M \oplus \sigma)) =$$

$$= RC4(IV, K_{BSS}) \oplus (M', CRC(M')),$$

  где σ - сообщение той же длины, что и *M*, в котором двоичные единицы определяют позиции инвертируемых битов открытого текста *M*. Таким образом, во власти стороны, перехватившей сообщение, внести в него контролируемые изменения.

- Уязвимость RC4.
  Scott Fluhrer из Cisco Systems, а также Itsik Mantin и Adi Shamir из института Weizmann Institute установили[1], что имеются целые классы «ненадежных» ключей, когда малая часть секретного ключа определяет большое число битов выходных данных. И если одна часть ключа известна злоумышленнику (вектор инициализации *IV*), остальная часть легко вычисляется. Используя эту особенность алгоритма RC4, Adam Stubblefield из университета Rice University, John Ioannidis и Aviel Rubin из AT&T Labs с помощью обычного доступного оборудования и ПО смогли взломать шифр WEP в тестовой сети всего за несколько часов[2].

Заключение

Существует несколько реализаций протокола WEP: «классический» WEP – тот, что описан в стандарте, и расширенные версии, разработанные некоторыми производителями сетевого оборудования. В стандартной реализации размер ключа равен 40-ка битам – такая длина была выбрана в связи с ограничениями, вводимыми правительством США, на технологии, разработанные на территории этой страны и используемые вне её пределов. Такой ключ легко находится простым перебором. В свою очередь, расширенные версии используют “128-битный” WEP (секретный ключ, на самом деле, имеет длину 104 бита; остальные 24

[1] См. [5]
[2] См. [6]

бита – вектор инициализации). Но, как показывает практика, существуют «быстрые» атаки, не требующие полного перебора – таким образом, и расширенные версии WEP оказываются незащищёнными.
Во всех этих случаях протокол WEP полагается только лишь на трудность нахождения ключа путём простого перебора, что, конечно же, не могло не повлиять на уровень безопасности, гарантируемый таким шифрованием. В итоге, ни одна из целей, обозначенных в системе WEP для обеспечения безопасности, не достигнута.

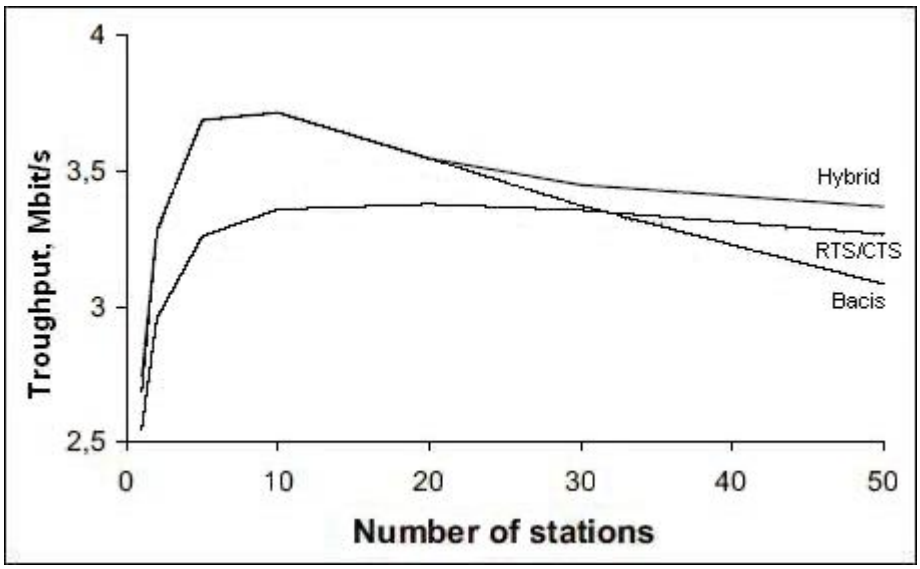
Для улучшения защищённости сетей стандарта IEEE 802.11 предложено несколько решений, все они различаются уровнем дополнительной безопасности и степенью совместимости с существующими технологиями беспроводных сетей. Сейчас готовятся к принятию в качестве стандартов новые протоколы WPA и WPA2, основывающиеся на AES-шифровании, которые в будущем полностью заменят существующий стандарт WEP.

Приложение

(некоторые справочные сведения)

- длина ключа *K*: 40 бит;
- длина вектора инициализации *IV*: 24 бита;
- длина контрольной суммы *CRC*: 32 бита.

Загруженность сети типа “ad hoc” (в Мбит/с)[1] в зависимости от числа активных станций для различных механизмов доступа к среде[2].



Примечание: Здесь измеряется суммарная пропускная способность для всех N станций; для каждой отдельной станции, соответственно, реальная скорость передачи данных в N раз меньше.

Литература

[1] При использовании расширения IEEE 802.11b стандарта IEEE 802.11, допускающего передачу данных со скоростью 11 Мбит/с.
[2] См. [1]

[1] Вишневский В.М. Теоретические основы проектирования компьютерных сетей. - М.: Техносфера, 2003. – 512с.

[2] Столлингс В. Беспроводные линии связи и сети: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 640с.: ил. – Парал. тит. англ.

[3] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: "Триумф", 2002 - 816 с.: ил.

[4] Borisov N., Goldberg I., Wagner D. Intercepting Mobile Communications: The Insecurity of 802.11.
http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf, 2001.

[5] Fluhrer S., Mantin I., Shamir A. Weaknesses in the key scheduling algorithm of RC4.
http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf, 2001.

[6] Stubblefield A., Ioannidis J., Rubin A. Using the Fluhrer, Mantin, and Shamir Attack To Break WEP
http://downloads.securityfocus.com/library/wep_attack.pdf, 2001

[7] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. - ANSI/IEEE Std 802.11, 1999 Edition.