УДК 004.056.53

Методы обеспечения защиты информации в беспроводных сетях

А. Кулмаханов
("Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики")
Научный руководитель - к. т. н., доцент В. И. Поляков
("Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики")

На сегодняшний день невозможно представить современное информационное общество без постоянного доступа к сети передачи данных. Основной задачей операторов, предоставляющих доступ к сети, является развертывание качественных и высокопроизводительных сетей. Одной из таких технологий, которая позволяет реализовать беспроводное подключение к сети передачи данных является беспроводное соединение Wi-Fi. Проблема обеспечения надежности и конфиденциальности передаваемой информации в беспроводных сетях, как и в любой технологии телекоммуникаций является немаловажным направлением.

Целью данной работы является повышение показателей надежности в беспроводных линиях связи с помощью алгоритмов шифрования для защиты передаваемой конфиденциальной информации. Для успешного достижения цели работы необходимо решить следующие задачи:

1. Изучить особенности и узкие места при передаче информации в беспроводных линиях связи, а также историю формирования беспроводной среды передачи данных. Ознакомиться с существующими угрозами безопасности в беспроводных сетях и способами борьбы с ними.
2. Исследовать существующие методы защиты информации в беспроводных сетях передачи данных. Выявить недостатки существующих мер защиты.
3. Программно реализовать алгоритмы шифрования каждого из рассмотренных методов, с целью сравнения их на практике.
4. Разработать алгоритм повышения показателей надежности при передаче данных посредством беспроводной сети. Обосновать эффективность разработанного алгоритма.

В работе рассмотрены такие методы аутентификации в беспроводных сетях Wi-Fi, как WEP, WPA, WPA2. Протоколы и алгоритмы шифрования каждого режима аутентификации описаны в работе в соответствии со стандартами [1].

Сравнительный анализ вышеописанных методов был проведен на основе таблицы, в которой указаны характеристики и свойства, а также реализующиеся в них протоколы. Программная реализация алгоритмов шифрования каждого метода выполнена с целью обоснования результатов сравнительного анализа на практике.

Исходя из сравнительного анализа, было определено, что режим аутентификации WPA2 является наиболее оптимальным решением в сфере обеспечения безопасности в беспроводных сетях передачи данных в силу алгоритмов шифрования и протоколов аутентификации, которые в нем используются. Но, несмотря на это данный режим аутентификации имеет ряд узких мест. Таким образом, учитывая недостатки и узкие места данного режима аутентификации, разработан алгоритм шифрования для повышения защищенности беспроводного канала связи.

Эффективность разработанного алгоритма обуславливается добавлением нескольких шагов в используемый в режиме аутентификации WPA2 алгоритм AES. Промежуточный результат шифрования представляется в виде прямоугольного массива байтов, который имеет 4 строки и переменное количество столбцов. Это позволяет сгенерировать надежный криптографический ключ для каждого этапа шифрования. Также

трансформация промежуточного массива при дешифрации производится дважды, с целью проведения вторичной обработки выработанного ключа. Таким образом, вышеописанные шаги значительно увеличивают надежность передачи информации посредством беспроводной сети.

ЛИТЕРАТУРА

1. William Stallings. Network Security Essentials. Applications and Standards / William Stallings, 2002, 432 с.
2. Гордейчик С. В., Дубровин В. В., Безопасность беспроводных сетей. Горячая линия — Телеком, 2008 г.
3. Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. Л., Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005 г.
4. Щербаков В. Б., Ермаков С. А. Безопасность беспроводный сетей: стандарт IEEE 802.11. - М: РадиоСофт, 2010. - 255 с.
5. Федоров С. А. ОБЗОР УГРОЗ И ТЕХНОЛОГИЙ ЗАЩИТЫ WI-FI СЕТЕЙ // Научное сообщество студентов XXI столетия. ТЕХНИЧЕСКИЕ НАУКИ: сб. ст. по мат. XLV междунар. студ. науч.-практ. конф. № 8(44).

Студент гр. Р4201	Кулмаханов А.
Научный руководитель, к. т. н., доцент	Поляков В. И.
Декан факультета ПИиКТ	Кустарев П. В.