ПРОТОКОЛЫ ЗАЩИТЫ БЕЗОПАСНОСТИ ДЛЯ БЕСПРОВОДНЫХ СЕТЕЙ WLAN

Ибрагимов Дониёр Бахтиярович
ассистент каведры СТРВ, ТУИТ

https://doi.org/10.5281/zenodo.20527292

Аннотатция: В этой статье рассмотрены беспроводные сети Wireless Local Area Network (WLAN), которые позволяют пользователям получать доступ к сети интернет без использования проводов. Однако такие сети могут стать уязвимыми для атак со стороны злоумышленников, поэтому для обеспечения безопасности существуют различные протоколы защиты. Также для обеспечения безопасности в беспроводных сетях WLAN рассмотрены существующие протоколов защиты, такие как WEP, WPA и WPA2.

Ключевые слова: беспроводные сети, WLAN, безопасность, протоколы защиты, WEP, WPA, WPA2, шифрование.

По сравнению с проводными сетями беспроводные сети имеют то преимущество, что позволяют избежать развертывания дорогостоящей кабельной инфраструктуры. Ниже на рисунке показано действующие беспроводных сетей, где проиллюстрировано семейство WPAN, WLAN и WMAN, которые дополняют друг друга с целью предоставления пользователям повсеместных широкополосных беспроводных услуг [1]. Целью рис. 1 является сравнение методов WPAN, WLAN и WMAN с разных точек зрения с точки зрения их промышленных стандартов, зоны покрытия и пиковых скоростей передачи данных. В частности, WPAN обычно используется для соединения с персональными устройствами (например, клавиатурой, аудио гарнитурой, принтером и т. д.) при относительно низкой скорости передачи данных и в небольшой зоне покрытия. Например, Bluetooth — это распространенный стандарт WPAN, использующий радиопокрытие ближнего действия в промышленном, научном и медицинском диапазоне, охватывающем полосу частот 2400–2480 МГц, что может обеспечить пиковую скорость передачи данных 2 Мбит/с и диапазон до 100 м [2]. На рис. 1 также показано, что WLAN обычно имеет более высокую скорость передачи данных и более широкую зону покрытия, чем WPAN, которая используется для подключения беспроводных устройств через точку доступа в пределах локальной зоны покрытия. Например, IEEE 802.11 (также известный как Wi-Fi) состоит из ряда промышленных стандартов WLAN. Современные стандарты Wi-Fi способны поддерживать пиковую скорость передачи данных 150 Мбит/с и максимальную дальность 250 м [3].

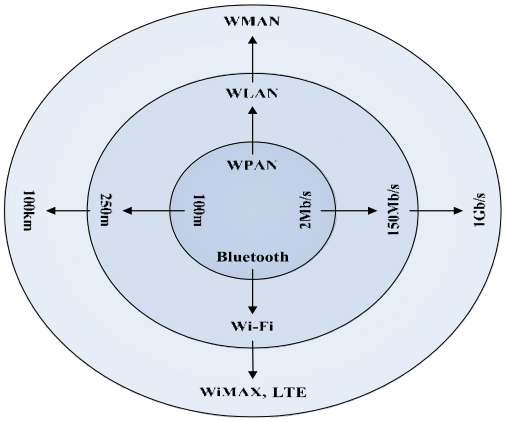

Рис. 1. Семейство беспроводных сетей, состоящее из WPAN, WLAN и WMAN

Наконец, WMAN обычно используется для подключения мегаполиса с более высокой скоростью и большей зоной покрытия, чем WPAN и WLAN. Например, на рис. 1 представлены два типа промышленных стандартов для WMAN, а именно WiMAX и LTE [4], [5].

Далее мы представим обзор протоколов безопасности, используемых в беспроводных стандартах WLAN для защиты подлинности, конфиденциальности, целостности и доступности законных передач через сеть. беспроводная среда распространения.

Наиболее распространенными протоколами защиты для беспроводных сетей WLAN являются WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) и WPA2. Протокол WEP является наименее надежным и может быть легко взломан, поэтому современные беспроводные сети чаще используют протоколы WPA и WPA2. Семейство сетей Wi-Fi, в основном основанных на стандартах IEEE 802.11 b/g, стремительно расширяется. Наиболее распространенные протоколы безопасности в Wi-Fi называются WEP и WPA [6]. WEP был предложен в 1999 году в качестве меры безопасности для сетей Wi-Fi, чтобы сделать беспроводную передачу данных такой же безопасной, как и в традиционных проводных сетях. Однако было показано, что WEP является относительно слабым протоколом безопасности, имеющим многочисленные недостатки. Следовательно, его можно «взломать» за несколько минут с помощью простого портативного компьютера. В качестве альтернативы WPA был предложен в 2003 году для замены WEP, а улучшенный WPA2 представляет собой обновленную версию стандарта WPA. Как правило, WPA и WPA2 более безопасны, чем WEP, поэтому они широко используются в современных сетях Wi-Fi. Ниже мы подробно описываем процессы аутентификации и шифрования протоколов WEP, WPA и WPA2.

Протокол WEP состоит из двух основных частей, а именно части аутентификации и части шифрования, направленных на установление контроля доступа путем предотвращения несанкционированного доступа без соответствующего ключа WEP и, следовательно, они обеспечивают конфиденциальность данных путем шифрования потоков данных с помощью ключа WEP. Аутентификация WEP использует четырехэтапное рукопожатие «запрос-ответ» между клиентом Wi-Fi и точкой доступа, работающей с

помощью общего ключа WEP. Чтобы быть точным, клиент сначала отправляет запрос аутентификации на точку доступа, которая затем отвечает вызовом открытого текста. После этого клиент шифрует полученный «текст запроса» с помощью предварительно общего ключа WEP и отправляет зашифрованный текст на точку доступа. Затем он расшифровывает полученный зашифрованный текст с помощью предварительно общего ключа WEP и пытается сравнить расшифрованный текст с исходным открытым текстом. Если совпадение найдено, точка доступа отправляет клиенту индикатор успешной аутентификации. В противном случае аутентификация считается неудачной.

После аутентификации WEP активирует процесс шифрования потоков данных с использованием простого алгоритма Rivest Cipher 4, работающего с помощью предварительно общего ключа WEP [7]. На рис. 2 показана блок-схема WEP-шифрования, где сначала вектор инициализации (IV) размером 24 бита соединяется с ключом WEP размером 40 бит. Это приводит к 64-битному начальному числу для PRNG (Pseudorandom number generator), которое затем используется для генерации потока ключей.

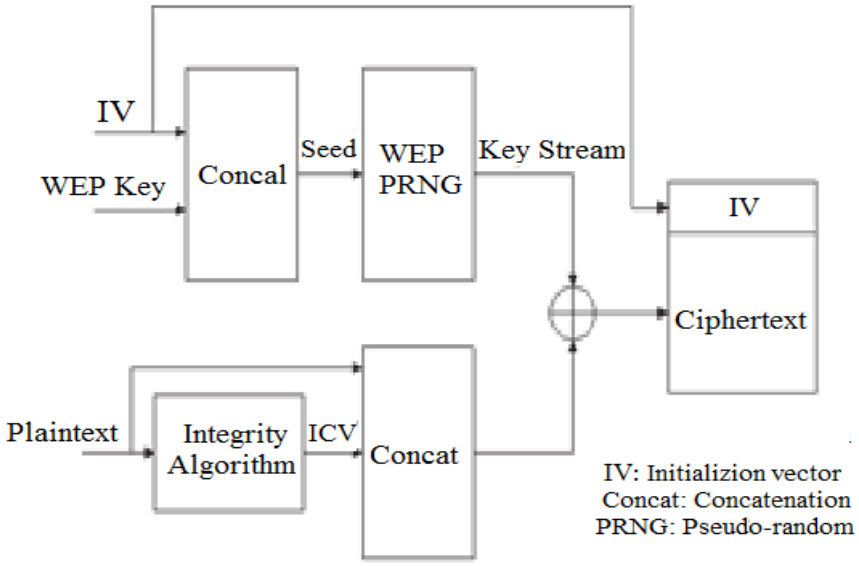

Рис. 2. Блок-схема шифрования WEP

Кроме того, выполняется алгоритм проверки целостности, такой как проверка циклическим избыточным кодом открытого текста для получения Integrity check value (ICV), который затем можно использовать для защиты передачи данных от злонамеренного вмешательства. Затем ICV объединяется с открытым текстом, который затем объединяется с вышеупомянутым потоком ключей по модулю 2 для генерации зашифрованного текста. Хотя WEP выполняет функции как аутентификации, так и шифрования, он по-прежнему подвержен угрозам безопасности. Например, WEP не может защитить информацию от атак подделки и повторного воспроизведения, поэтому злоумышленник может намеренно изменить или воспроизвести пакеты данных, при этом законные пользователи не узнают о фальсификации и/или воспроизведении данных. Кроме того, секретные ключи, используемые в WEP, могут быть «взломаны» за несколько минут с помощью простого портативного

компьютера [8]. Кроме того, злоумышленнику легко подделать сообщение аутентификации в WEP, что позволяет неавторизованным пользователям легко выдавать себя за законных пользователей и, следовательно, красть конфиденциальную информацию [9].

В качестве средства защиты WPA был предложен для решения вышеупомянутых проблем безопасности WEP, что было достигнуто пользователями Wi-Fi без необходимости замены своего оборудования. Стандарт WPA имеет два основных типа:

1) персональный WPA в основном используется дома без использования сервера аутентификации, где между клиентом и точкой доступа предварительно распределяется секретный ключ, который называется WPA-PSK (preshared key);

2) корпоративный WPA, используемый для корпоративных сетей, для которого требуется сервер аутентификации 802.1x для осуществления контроля безопасности с целью эффективной защиты от вредоносных атак.

Основное преимущество WPA по сравнению с WEP заключается в том, что WPA использует более мощное шифрование данных, называемое TKIP (Temporal key integrity protocol), которому помогает MIC (Message integrity check), вызываемый для защиты целостности данных и конфиденциальности сетей Wi-Fi [10], [11]. На рис. 3 показан процесс шифрования TKIP, в котором TA (Transmitter address), TK (Temporal key) и TSC (TKIP sequence counter) составляют входные данные процесса смешивания ключей фазы I, вызываемого для получения так называемого TTAK (TKIP-mixed transmit address and key), который затем обрабатывается далее с TSC на этапе смешивания ключей фазы II для получения начального числа WEP, включая WEP IV и базовый ключ.

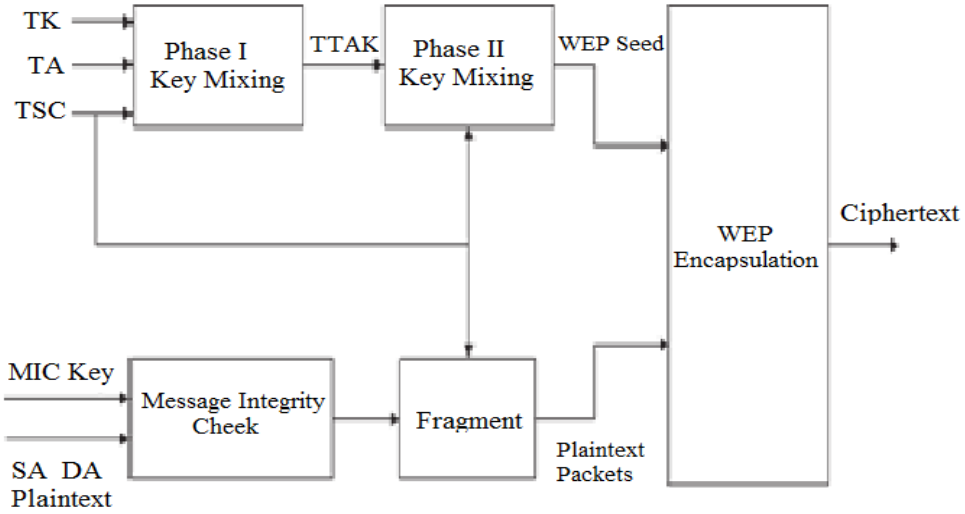

Рис. 3. Иллюстрация процесса шифрования TKIP

Кроме того, обратите внимание на рис. 3, что MIC выполняется как для SA (Source address), так и для DA (Destination address) и открытого текста. Результирующий MIC будет затем присоединен к открытому тексту, который далее фрагментируется на несколько пакетов, каждому из которых назначается уникальный TSC. Наконец, начальное число WEP и пакеты открытого текста используются для получения зашифрованного текста путем

вызова шифрования WEP, как описано на рис. 3, которое часто реализуется в аппаратном обеспечении устройств Wi-Fi. Отметим, что даже WPA, опирающийся на TKIP, остается уязвимым для различных практических атак [12].

Adabiyotlar, References, Литературы:

1. C. Stevenson et al., “IEEE 802.22: The first cognitive radio wireless regional area network standard,” IEEE Commun. Mag., vol. 47, no. 1, pp. 130–138, Jan. 2009.
2. E. Ferro and F. Potorti, “Bluetooth and Wi-Fi wireless protocols: A survey and a comparison,” IEEE Wireless Commun., vol. 12, no. 1, pp. 12–26, Feb. 2005.
3. M. Polla, F. Martinelli, and D. Sgandurra, “A Survey on security for mobile devices,” IEEE Commun. Surv. Tut., vol. 15, no. 1, pp. 446–471, Mar. 2013.
4. D. Pareit, I. Moerman, and P. Demeester, “The history of WiMAX: A complete survey of the evolution in certification and standardization for IEEE 802.16 and WiMAX,” IEEE Commun. Surv. Tut., vol. 14, no. 4, pp. 1183–1211, Oct. 2012.
5. J. Cao, H. Ma, H. Li, and Y. Zhang, “A survey on security aspects for LTE and LTE-A networks,” IEEE Commun. Surv. Tut., vol. 15, no. 2, Apr. 2013
6. A. Lashkari, M. Danesh, and B. Samadi, “A survey on wireless security protocols (WEP, WPA and WPA2/802.11i),” in Proc. 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol., Beijing, China, Aug. 2009, pp. 48–52.
7. J. Lee and C. Fan, “Efficient low-latency RC4 architecture designs for IEEE 802.11i WEP/TKIP,” in Proc. Int. Symp. Intell. Signal Process. Commun. Syst., Xiamen, China, Nov. 2007, pp. 56–59.
8. A. Stubbleleld, J. Ioannidis, and A. D. Rubin, “A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP),” ACM Trans. Inf. Syst. Security, vol. 7, no. 2, pp. 319–332, May 2004.
9. E. Tews, R.-P. Weinmann, and A. Pyshkin, “Breaking 104 bit WEP in less than 60 seconds,” in Information Security Applications. Lecture Notes in Computer Science, Berlin, Germany: Springer-Verlag, 2007, vol. 4867, pp. 188–202.
10. J. Lin, Y. Kao, and C. Yang, “Secure enhanced wireless transfer protocol,” in Proc. 1st Int. Conf. Availab. Reliab. Security, Vienna, Austria, Apr. 2006, pp. 536–543.
11. C. Nancy, H. Russ, W. David, and W. Jesse, “Security flaws in 802.11 data link protocols,” Commun. ACM, vol. 46, no. 5, pp. 35–39, May 2003.
12. E. Tews and M. Beck, “Practical attacks against WEP and WPA,” in Proc. 2nd ACM Conf. Wireless Netw. Security, Zurich, Switzerland, Mar. 2009, pp. 79–86.