Шаханова М.В., Четвертик М.А., Шаханова Д.С. Механизмы защиты информации в беспроводных сетях // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 75–79

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.5

МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

[1]Шаханова М.В., Четвертик М.А, Шаханова Д.С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

Беспроводные технологии активно распространяются среди населения. Сети с беспроводным подключением имеют ряд недочетов, связи с чем постоянно подвергаются атакам с целью перехвата конфиденциальной информации и нарушения целостности данных. Однако технологии стремительно развиваются, создаются новые методы защиты передаваемой информации. В данной статье будут приведены основные механизмы защиты при использовании беспроводных сетей.

Ключевые слова: беспроводная сеть, защита информации, беспроводные технологии, механизм защиты.

INFORMATION PROTECTION MECHANISMS IN WIRELESS NETWORKS

[1]Shakhanova M. V., Chetverik M.A., Shakhanova D.S.
Maritime State University named after G.I. Nevelskoy, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

Wireless technologies are actively spreading among the population. Wireless networks have a number of shortcomings, and therefore are constantly being attacked in order to intercept confidential information and violate data integrity. However, technologies are rapidly developing, new methods of protecting the transmitted information are being created. This article will describe the main protection mechanisms when using wireless networks.

Keywords: wireless network, information protection, wireless technologies, protection mechanism.

Беспроводная сеть – компьютерная сеть, которая использует беспроводные соединения для передачи данных между узлами сети. [1]

Беспроводные технологии позволяют передавать сигналы на большие расстояния без электрических кабелей. Возможность быстрого обмена сигналами и независимость от места подключения привлекает людей использовать беспроводную сеть.

У беспроводной сети есть ряд недостатков.

- Отсутствие стабильности. Перебои на станциях, временные отключения доступа, ограниченная дальность действия, а также риск снижения качества подключения из-за воздействия электроприборов - приводят к нарушению стабильности и возможному отказу в обслуживании.
- Безопасность. Информацию, передаваемую по каналам беспроводной связи можно перехватить. Для решения этой проблемы стали использовать шифрование сигнала, но и это не стало гарантией полной защищенности. Старые алгоритмы шифрования легко

взламываются, а для современных алгоритмов создаются новые методы взломов. Беспроводные сети обеспечивают анонимность атаки, не позволяя без соответствующего оборудование определить местоположение.

- Скорость передачи. При большом количестве пользователей, скорость подключения делится между всеми клиентами, что приводит к ее снижению. Помехи, рельеф местности, воздействие других сетей – создают преграды в свободном распространении сигнала, приглушая его и снижая скорость. [2]

Но говоря о недостатках, нельзя исключать факт того, что беспроводные сети имеют ряд преимуществ.

- Экономичность. Общая стоимость оборудование снижается из-за отсутствия надобности в дополнительных приборах.
- Простота настройки и подключения.
- Гибкость. Беспроводные сети могу служить как добавлением, так и заменой проводных сетей.
- Мобильность. Отсутствие проводов способствует легкому и быстрому перемещению и повторной установки оборудования. Пользователь «не привязан» к месту.

Наиболее известными беспроводными технологиями являются – Wi-Fi, Bluetooth и WiMAX.

Wi-Fi – это беспроводная технология передачи данных, при которой трафик преобразуется в радиоволны и распространяется в форме радиосигнала (рисунок 1). Клиентская аппаратура расшифровывает сигнал и извлекает из него информацию. Функциональность Wi-Fi схожа с функциональностью мобильных сетей.

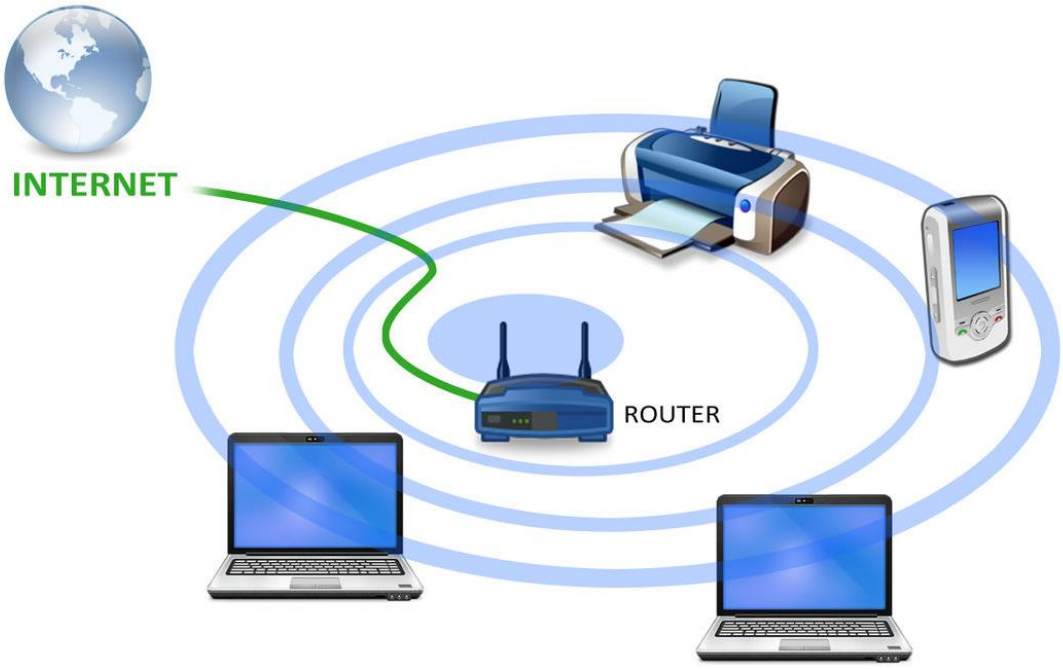

Рисунок 1 – Принцип работы Wi-Fi

Как и любая другая беспроводная сеть, Wi-Fi подвержена угрозам. Радиосигнал может быть перехвачен с целью нарушения целостности и конфиденциальности данных. Элементы защиты, предусмотренные в Wi-Fi, имеют свои недостатки. Существует несколько механизмов защиты:

- OPEN – отсутствие всякой защиты. Данные передаваемые по радиоканалам не шифруются, что становится причиной утечки данных. И если при использовании проводной сети злоумышленнику понадобится прямое подключение, то к беспроводной сети можно подключиться из любого места, что делает открытую передачу данных по сети более опасной.
- WEP – первый стандарт защиты. Данный стандарт взламывается множеством разных способов, степень его защиты немного лучше, чем открытые сети, из-за чего у пользователей часто возникало ложное чувство безопасности. Злоумышленники перехватывали пакеты, которые переносили по несколько байт временного ключа, что в условиях активного пользования сети было достаточно для раскрытия.
- WPA – второй стандарт. Он шифровал данные каждого клиента по отдельности. При проникновении в сеть отсутствовала возможность прочитать другие пакеты, сначала их нужно было перехватить.
- WPA2 – обновленная версия WPA. Стандарт поддерживает два разных режима аутентификации.
- WPS – позволяет клиенту подключиться к сети по 8-символьному коду. Но из-за допущенной ошибки в стандарте, угадать нужно всего лишь 4 [2-3].

В отличие от Wi-Fi технология WiMAX обеспечивает передачу на большие расстояния как в прямой видимости, так и вне поле зрения. Wi-Fi же обеспечивает эффективную связь лишь по прямой линии.

WiMAX – телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств [4].

Принцип работы данной технологии аналогичен работе Wi-Fi и сотовой связи. Вышки с передатчиками WiMAX свободно подключаются к Интернету. Станции покрывают большие территории и могут быть расположены на расстоянии до 50 километров. Сигналы передаются по цепочке от вышки к вышке, по крайней мере одна из которых связана с сетью провайдера при помощи проводов. С последнего передатчика на принимающую антенну с помощью зашифрованных ключей поступает сигнал (рисунок 2). Принимающей антенной может быть, как роутер, так и пользовательское устройство [4].

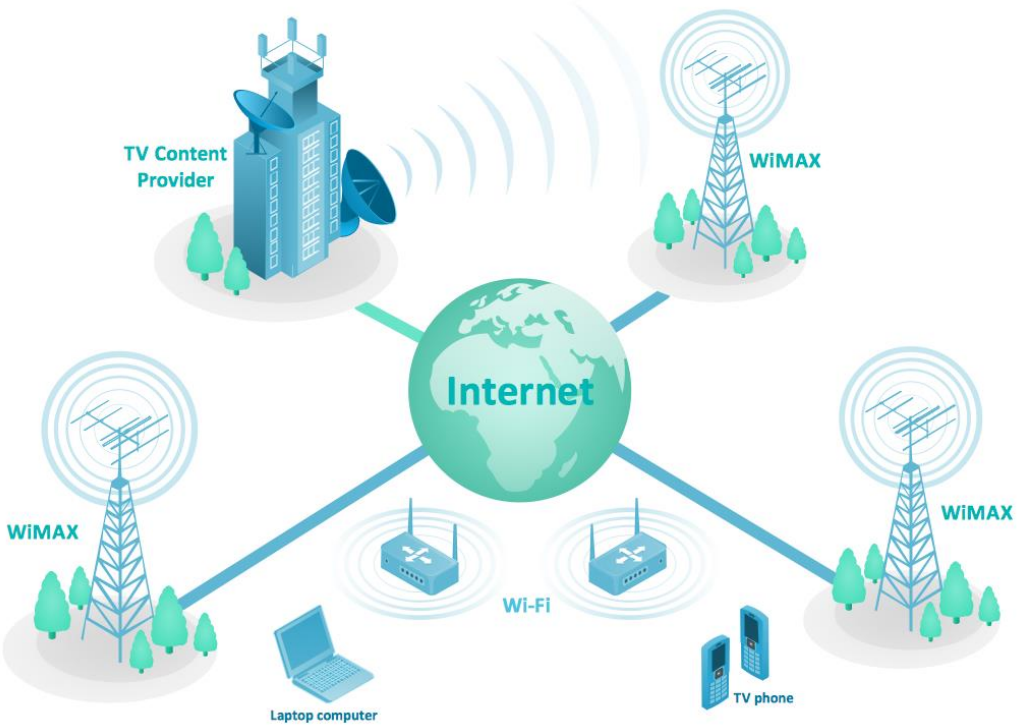

Рисунок 2 – Принцип работы WiMAX

Технология WiMAX изначально разрабатывалась со всеми учетами безопасности. Трафик должен быть зашифрован с использованием алгоритма AES, для аутентификации используется протокол на основе TLS с шифрованием открытым ключом. В стандартах технологии WiMAX изначально заложены серьезные функции безопасности:

- Аутентификация клиентского оборудования при помощи обмена сертификатами с базовой станцией для исключения неавторизированного терминала.
- Аутентификация пользователя с использованием протокола EAP.
- Кодирование передаваемых данных с использованием стандарта AES. Возможность избежать перехвата и расшифровки трафика, путем шифрования каждой из услуг собственными ключами [4].

Bluetooth – стандарт беспроводной сети, позволяющий передавать данные на небольшое расстояние при помощи радиоволн. Для передачи информации необходимо наличие у обоих устройств специального модуля. Главное отличие Bluetooth от Wi-Fi, в том, что Bluetooth используется для передачи данных между двумя устройствами без построения локальной сети [2].

Для защиты Bluetooth используется шифрование данных и авторизация устройств. Для шифрования используется ключ длиной от 8 до 128 бит. Это способствует тому, что спонтанно устройства соединяться не смогут, что снижает риск утечки данных. У технологии есть четыре режима безопасности:

- 1 режим используется по умолчанию и не предоставляет никакой защиты.
- 2 режим защищен на уровне приложения. После соединения происходит аутентификация.

- 3 режим защищен на уровне канала связи. В этом этапе после аутентификации применяется прозрачное шифрование. В данном режиме риск взлома устройство по-прежнему велик.
- 4 режим представляет собой усовершенствованный 2 режим. После установления соединения функции безопасности реализуются. Для генерации ключа используется протокол ECDH [2].

Таким образом, основной целью статьи являлось исследование методов защиты информации в беспроводных сетях. Стоит отметить, что с увеличением заинтересованности людей в использовании беспроводных сетей передачи информации увеличилось и количество случаев перехвата данных с целью нанесения вреда владельцу. При этом существующие методы не всегда справлялись с угрозой, что породило необходимость в разработке новых методов защиты информации. Понимание угроз безопасности – первый шаг к их предотвращению.

Список литературы

1. Shahrabi Alireza, Morteza Mohammadi Zanjireh, и Larijani Hadi ANCH: A New Clustering Algorithm for Wireless Sensor Networks // ResearchGate. 2013.
2. Гейер Джим Беспроводные глобальные и персональные сети // Беспроводные сети. 2005.
3. Пролетарский А. В., Басков И. В., Федотов Р.А., Бобков А. В., Чирков Д.Н., Платонов В.А. Основы протоколов безопасности беспроводных сетей и криптографии // Организация беспроводных сетей. 2006.
4. Архипкин А. Стандарт WiMAX: техническое описание, варианты реализации и специфика применения // Технологии и стандарты. 2006.

References

1. Shahrabi Alireza, Morteza Mohammadi Zanjireh, and Larijani Hadi ANCH: A New Clustering Algorithm for Wireless Sensor Networks // ResearchGate. 2013.
2. Geyer Jim Wireless global and personal networks // Wireless networks. 2005.
3. Proletarsky A. V., Baskov I. V., Fedotov R. A., Bobkov A. V., Chirkov D. N., Platonov V. A. Fundamentals of security protocols for wireless networks and cryptography // Organization of wireless networks. 2006.
4. Arkhipkin A. WiMAX standard: technical description, implementation options and application specifics // Technologies and standards. 2006.