УДК 004.056.5

ОЦЕНКА КИБЕРБЕЗОПАСНОСТИ БЕСПРОВОДНОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ В P2P ГРУППЕ WI-FI DIRECT

М.В. Мамченко
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: markmamcha@gmail.com

Р.А. Емельянов
Институт интеллектуальных кибернетических систем НИЯУ МИФИ
Россия, 115409, г. Москва, Каширское ш., 31
E-mail: milkywar@yandex.ru

Ключевые слова: кибербезопасность, Wi-Fi Direct, P2P группа, кибератака, беспроводной канал передачи данных.

Аннотация: В работе проведен обзор технологии Wi-Fi Direct, исследованы особенностей шифрования данных и этапы установления соединения между устройствами. Рассмотрены основные типовые атаки на устройства и беспроводное соединение Wi-Fi Direct, в том числе DOS-атака, атаки с помехами, «Маскарад», «Человек посередине», подслушивания, деаутентификации и подбора ключа (атака по словарю). Предложена стратегия действий по защите беспроводного соединения Wi-Fi Direct (в P2P группе), включающую пассивные (задание сложного для взлома (при проведении атаки по словарю) пароля) и активные (мониторинг внедрения пакетов деаутентификации и DOS-атак) меры защиты беспроводного канала передачи данных в P2P группе Wi-Fi Direct.

1. Введение

В типичной сети Wi-Fi различные устройства (мобильные телефоны, камеры, принтеры и т.д.) не обмениваются данными напрямую, а подключаются к точкам доступа, функции которых чаще всего выполняют сетевые маршрутизаторы/роутеры [1]. Вместе с тем существует технология передачи данных непосредственно между двумя устройствами с поддержкой стандартов беспроводной передачи данных – Wi-Fi Direct. Устройства в сети Wi-Fi смогут устанавливать соединение «один к одному» (P2P – peer-to-peer), либо образовывать одноранговую сеть из нескольких устройств [2].

В российских и зарубежных научных статьях технология Wi-Fi Direct рассматривается в основном в качестве средства обеспечения передачи данных в беспроводных одноранговых сетях и применительно к различным сферам, в частности, в среде умного города [3], реагирования на чрезвычайные ситуации [4], а также для других целей [5]. Однако вопрос защищенности передачи данных при использовании данной технологии практически не исследуется. В открытых источниках существуют единичные статьи, посвященные данному вопросу, в частности, в работах [6-8] рассматриваются некоторые аспекты безопасности технологии Wi-Fi Direct и приводится описание отдельных атак.

Таким образом, тематика оценки безопасности технологии Wi-Fi Direct и выработки предложений по повышению защищенности беспроводного соединения в

P2P группах Wi-Fi Direct полагается актуальной. В разделе 2 представлены этапы установления соединения между устройствами в P2P группе, в разделе 3 – типовые атаки на устройства и беспроводное соединение Wi-Fi Direct.

2. Этапы установления соединения для обмена данными в P2P группе с использованием Wi-Fi Direct

Установление соединения с устройством для подготовки к использованию P2P Wi-Fi Direct состоит из нескольких этапов (рисунок 1): обнаружение, формирование группы, установление защищенной связи с использованием Wi-Fi Protected Setup (WPS), конфигурация IP-адреса и работа в P2P-группе. На рисунке 1 представлены этапы установления соединения с устройством для обмена данными P2P [9]. Рассмотрим каждый этап подробнее.

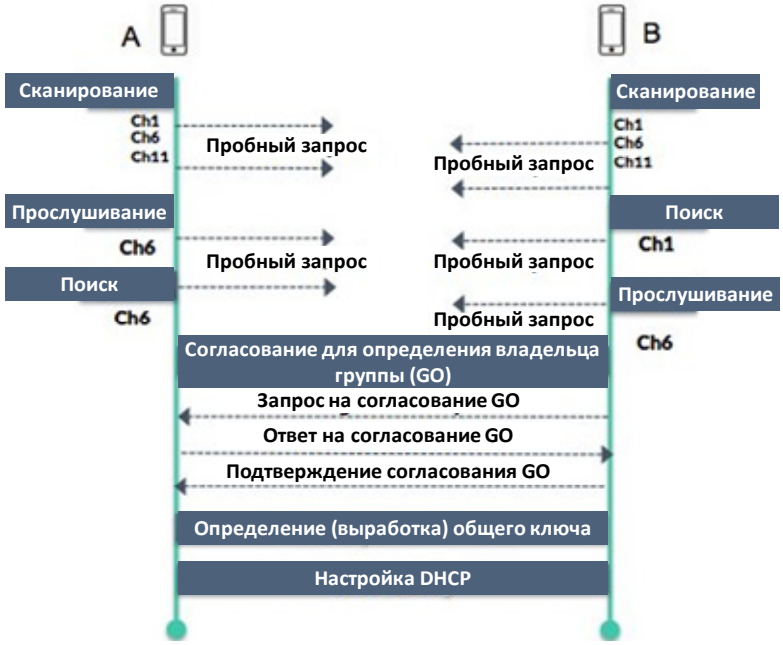

Рис. 1. Этапы установления P2P-соединения с устройством для обмена данными посредством Wi-Fi Direct [9].

1) Обнаружение устройства. Этап начинается с обмена пробными кадрами запроса/ответа, которые позволяют обнаруживать узлы одноранговой сети, затем происходит обмен запросами на приглашение и ответами для формирования группы.
2) Формирование группы. Этап начинается с процедуры трехэтапного «рукопожатия» для отправки запроса, получения ответа и подтверждения владельца группы. В результате одно из устройств определяется владельцем группы (GO – Group Owner). GO выполняет роль точки доступа для предоставления клиентам возможности подключения. Другие устройства обнаруживают наличие GO и, минуя этап обнаружения, и присоединяются к группе. Существует несколько способов, с помощью которых два устройства могут создать группу P2P, в зависимости, например, от того, должны ли они согласовать роль P2P GO, или доступна ли какая-либо априорная информация об уровне защищенности группы:

- стандартный – P2P-устройства должны сначала обнаружить друг друга, а затем согласовать, какое устройство будет выступать в качестве P2P GO;
- автономный – устройство может самостоятельно создать P2P-группу, где оно сразу же получает функции P2P GO;
- постоянный – в процессе формирования P2P-группы устройства могут объявить группу в качестве постоянной, используя соответствующий флаг в атрибуте возможностей P2P.

3) Wi-Fi Protected Setup. Как только устройства обнаружили друг друга и «договорились» о соответствующих ролях, происходит установление защищенной связи с использованием технологии WPS. Настройка защиты WPS состоит из двух этапов [10]. На первом этапе GO отвечает за генерацию и выдачу сетевых данных (т.е. ключей безопасности) участнику – P2P-клиенту. На втором этапе P2P-клиент отключается и повторно подключается, используя новые данные для аутентификации. Если два устройства уже имеют требуемые сетевые данные (например, при наличии постоянной P2P-группы), осуществляется переход к процедуре аутентификации.
4) Конфигурация IP-адреса. После согласования предварительного общего ключа PSK устройство P2P, выступающее в роли GO, запускает режим DHCP [11] для автоматического назначения IP-адресов всем остальным членам группы. Он начинается с запросов обнаружения от клиентов. Затем P2P GO отвечает на запрос, предлагая набор возможных IP-адресов для клиента, после чего клиент отвечает на запрос, выбирая один из предложенных адресов. Наконец, P2P GO направляет ответ и подтверждает клиента.

3. Известные типы атак на P2P группу Wi-Fi Direct

Основными, наиболее известными атаками на P2P-группу Wi-Fi Direct являются: DOS-атака, атака с помехами, атака «Маскарад», атака «Человек по середине» и атака подслушивания [12-16]. Рассмотрим каждую атаку подробнее.

1) DOS-атака. Распределенная атака типа «отказ в обслуживании» (DOS – Denial of Service) – это тип атаки, направленный на вывод из строя устройство сети путем заполнения беспроводного канала большим количеством сгенерированных сообщений [12]. Цель атаки – сделать беспроводное соединение в группе недоступными для легитимных пользователей. Отказ в обслуживании в некоторых случаях приводит к разрушению целостности группы P2P.
2) Атака с помехами. Атака с помехами нацелена на связность элементов системы P2P. Суть атаки заключается в том, что злоумышленник генерирует «шумовой» сигнал, чтобы перегрузить беспроводной канал и нарушить общение в группе между легитимными пользователями [13]. Целью атаки является снижение отношения сигнал/шум в беспроводном канале до критических (недопустимых) значений.
3) Атака «Маскарад». Суть атаки заключается в том, что злоумышленник присоединяется к P2P-группе, выдавая себя за легитимного и аутентифицированного пользователя [13]. Сначала отправляется запрос одному из пользователей группы P2P. Затем легитимный участник P2P-системы отвечает, используя широковещательный идентификатор, который является MAC-адресом мобильного устройства. Наконец, злоумышленник использует этот MAC-адрес для связи с другими пользователями группы, что позволяет ему выдавать себя за легитимного пользователя. Цель атаки – получение доступа в группу P2P для перехвата передаваемых данных, либо недопущение присоединения к группе легитимного пользователя.

4) Атака «Человек посередине». При проведении атаки «Человек посередине» (MITM – Man in the Middle) злоумышленник, расположенный между легитимными пользователями группы, успешно присоединяется к группе и перехватывает трафик, передаваемый по беспроводным каналам [12]. Злоумышленник отправляет сообщение клиенту группы P2P, а затем использует данные, полученные из ответного сообщения, для связи с другими пользователями группы. Пользователи группы не могут отличить легитимного пользователя от злоумышленника из-за используемых им учетных данных. Атака «Человек посередине» остается одной из наиболее опасных для P2P-систем.
5) Атака подслушивания. Данная атака схожа с атакой «Человек посередине», однако в данном случае злоумышленник использует учетные данные легитимных пользователей для перехвата трафика, чтения передаваемых сообщений, кражи учетных данных пользователей [14].
6) Атака деаутентификации. Если функция Wi-Fi Direct активирована на двух устройствах, то злоумышленник может получить информацию о подключении Wi-Fi Direct (добавления в группу) посредством т.н. «сниффинга» (анализа) передаваемого трафика. Затем злоумышленник получает MAC-адрес устройства из полученного дампа и осуществляет подмену MAC-адрес устройства [14]. После этого может быть проведена другая атака, например, деаутентификации.
7) Атака подбора ключа (атака по словарю). Технология Wi-Fi Direct имеет встроенные механизмы безопасности за счет использования WPA2. В случае WPA2-PSK можно выполнить взлом ключа с помощью атаки по словарю, если ключ небольшой длины и состоит только из цифр и/или букв. Взлом ключа возможен, если злоумышленник получит пакеты четырехстороннего «рукопожатия» после анализа передаваемого трафика. Анализ и т.н. «очистка рукопожатия» возможна, например, с использованием с помощью программы Wireshark [14]. Далее возможно проведение атаки по словарю и подбор значения ключа. Зная ключ, злоумышленник может подключиться к P2P-группе, провести дополнительные атаки (например, DOS-атаку, атаку деаутентификации), либо начать перехват пакетов данных, передаваемых между легитимными пользователями [15, 16].

3.1. Стратегия защиты

На основании проведенного исследования и с учетом работы [17] возможно предложить следующие меры повышения безопасности передачи данных посредством Wi-Fi Direct:

- при наличии возможности в настройках Wi-Fi Direct следует задать пароля размером не менее 16 символов, включающих строчных и заглавные буквы английского алфавита, цифры и специальные знаки;
- возможно также развертывание дополнительного автоматизированного рабочего места с установленным программным обеспечением типа Waidps или WireShark для отслеживания признаков совершения атак DOS и/или деаутентификации.

4. Заключение

В работе проведен обзор технологии Wi-Fi Direct, исследованы особенностей шифрования данных и этапы установления соединения между устройствами. Рассмотрены основные типовые атаки на устройства и беспроводное соединение Wi-Fi Direct, в том числе DOS-атака, атаки с помехами, «Маскарад», «Человек посередине», подслушивания, деаутентификации и подбора ключа (атака по словарю). Предложена

стратегия действий по защите беспроводное соединение Wi-Fi Direct (P2P соединения), включающую пассивные (задание сложного для взлома (при проведении атаки по словарю) пароля) и активные (мониторинг внедрения пакетов деаутентификации и DOS-атак) меры защиты беспроводного канала передачи данных в P2P группе Wi-Fi Direct.

Список литературы

1. 10 Wi-Fi Predictions for 2024. https://techeconomy.ng/10-wi-fi-predictions-for-2024/ (дата обращения 18.01.2024).
2. Yoon S., Park S.-T., Park H., Yoo H.S. Security analysis of vulnerable Wi-Fi Direct // 2012 8th International Conference on Computing and Networking Technology (INC, ICCIS and ICMIC). 2012. P. 340-343.
3. Jung W.-S., Ahn H., Ko Y.-B. Designing content-centric multi-hop networking over Wi-Fi Direct on smartphones // 2014 IEEE Wireless Communications and Networking Conference (WCNC). 2014. P. 2934-2939.
4. Shuhaimi N.I., Heriansyah, Juhana T. Comparative performance evaluation of DSRC and Wi-Fi Direct in VANET // 2015 4th International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME). 2015. P. 298-303.
5. Khan G.Z., Gonzalez R., Park E.-C., Wu X.-W. A reliable multicast MAC protocol for Wi-Fi Direct 802.11 networks // 2015 European Conference on Networks and Communications (EuCNC). 2015. P. 224-228.
6. Зонин Л.М., Сидоров С.Г. Использование технологии Wi-Fi Direct в разработке программного обеспечения // Энергия-2022. Математическое моделирование и информационные технологии: семнадцатая Всероссийская (девятая Международная) научно-техническая конференция студентов, аспирантов и молодых ученых: материалы конференции. 2022. Т. 5. С. 67.
7. Zou Y., Zhu J., Wang X., Hanzo L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends // Proceedings of the IEEE. 2016. Vol. 104, No. 9. P. 1727-1765.
8. Hadiks A., Chen Y., Li F., Liu B. A study of stealthy denial-of-service attacks in Wi-Fi direct device-to-device networks // 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC). 2014. P. 507-508.
9. Belghazi Z., Benamar N., Addaim A., Kerrache C.A. Secure WiFi-Direct Using Key Exchange for IoT Device-to-Device Communications in a Smart Environment // Future Internet. 2019. Vol. 11, No. 251. P. 1-15.
10. Camps-Mur D., Garcia-Saavedra A., Serrano P. Device-to-device communications with Wi-Fi Direct: overview and experimentation // IEEE Wireless Communications. 2013. Vol. 20, No. 3. P. 96-104.
11. Lee J.-S., Su Y.-W., Shen C.-C. A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi // IECON 2007 - 33rd Annual Conference of the IEEE Industrial Electronics Society. 2007. P. 46-51.
12. Arnaboldi V., Campana M.G.G., Delmastro F. Context-Aware Configuration and Management of WiFi Direct Groups for Real Opportunistic Networks // 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). 2017. P. 266-274.
13. Gandotra P., Jha R.K., Jain S. A survey on device-to-device (D2D) communication: Architecture and security issues // Journal of Network and Computer Applications. 2017. Vol. 78. P. 9-29.
14. Haus M., Waqas M., Ding A.Y., Li Y., Tarkoma S., Ott J. Security and Privacy in Device-to-Device (D2D) Communication: A Review // IEEE Communications Surveys & Tutorials. 2017. Vol. 19, No. 2. P. 1054-1079.
15. Bettini C., Riboni D. Privacy protection in pervasive systems: State of the art and technical challenges // Pervasive and Mobile Computing. 2015. Vol. 17, Part B. P. 159-174.
16. Camps-Mur D., Garcia-Saavedra A., Serrano P. Device-to-device communications with Wi-Fi Direct: overview and experimentation // IEEE Wireless Communications. 2013. Vol. 20, No. 3. P. 96-104.
17. Мамченко М.В. Анализ кибербезопасности беспроводного канала управления беспилотного летательного аппарата потребительского сегмента // Труды 13-й Мультиконференции по проблемам управления (МКПУ-2020): конференции «Управление в аэрокосмических системах» (УАКС-2020) им. академика РАН Е.А. Микрина. 2020. С. 26-28.