УДК 622.276.001

Р.Р. Абраров, М.Е. Бурлаков

Самарский национальный исследовательский университет им. С.П. Королева, Самара, Россия

УЯЗВИМОСТИ ПРОТОКОЛА МАРШРУТИЗАЦИИ В MESH-СЕТИ СТАНДАРТА 802.11S

Беспроводные ячеистые сети (Wireless Mesh Network) могут объединять в единую сеть различные устройства. WMN обеспечивает лучшую мобильность, более низкую стоимость развертывания, простое расширение сети и надежные соединения. Гибридный беспроводной протокол mesh-сети (Hybrid Wireless Mesh Protocol – HWMP) является стандартным протоколом маршрутизации по умолчанию для стандарта 802.11s. Протокол маршрутизации является одной из наиболее важных частей сети и требует защиты, особенно в беспроводной среде. Существующие протоколы безопасности, такие как протокол целостности широковещания (Broadcast Integrity Protocol), блочный шифр сообщений кода аутентификации (Cipher Block Chaining Message Authentication Code Protocol), безопасный HWMP (Security HWMP), идентификация на основе шифрования HWMP (Identity Based Cryptography HWMP), эллиптические кривые цифровой подписи HWMP (Elliptic Curve Digital Signature Algorithm HWMP), сторожевые HWMP (Watchdog HWMP) нацелены на защиту кадров в протоколе HWMP.

В этой статье рассматриваются вопросы безопасности передаваемых данных в mesh-сети стандарта 802.11s. Описаны основные принципы работы протокола маршрутизации по умолчанию в стандарте 802.11s – HWMP. Приведены и проанализированы возможные атаки на маршрутизацию кадров в mesh-сети. Проанализированы принципы работы основных протоколов безопасности в стандарте 802.11s. Проведен анализ уязвимостей существующих протоколов безопасности в HWMP. Результаты анализа существующих протоколов безопасности показывают, что ни один из этих протоколов не способен удовлетворить все требования безопасности. По результатам проделанной работы даны общие рекомендации для дальнейшего развития протоколов безопасности в маршрутизации кадров в mesh-сети стандарта 802.11s.

Ключевые слова: гибридный беспроводной протокол mesh-сети, безопасная маршрутизация, беспроводная ячеистая сеть, стандарт 802.11s.

R.R. Abrarov, M.E. Burlakov

Samara National Research University named after S.P. Korolev, Samara, Russian Federation

THE VULNERABILITIES OF ROUTING PROTOCOL IN MESH NETWORK IN STANDART 802.11S

Wireless Mesh Network can integrate various devices into a single network. WMN provides with the best mobility, lower cost of deployment, easy extension of network and reliable connections. Hybrid Wireless Mesh Protocol (HWMP) is the basic protocol of the default routing for standard 802.11s. Routing protocol is one of the most important parts of the network and it requires protection, especially in a

wireless environment. Existing security protocols, such as broadcast integrity protocol (BIP), block cypher of messages of authentication code (CCMP), secure HWMP (SHWMP), identification, based on encryption HWMP (IBC-HWMP), elliptic curves of digital signature HWMP (ECDSA-HWMP), watchdog HWMP are targeted to protect frames in the HWMP protocol.

Issues related to the security of data transmitted in Mesh-networks of 802.11s standard are reviewed in this article. Besides, there were described the basic principles of working of the default routing protocol for standard 802.11s – HWMP. Moreover, possible attacks on frames routing in a Mesh-network were mentioned and analyzed. There were explored the concepts of the main security protocols for 802.11s standard. The analysis of the vulnerabilities of existing security protocols in HWMP was conducted. The results of the analysis of existing security protocols show that none of these protocols is able to satisfy all requirements of security. Due to the results of this work general recommendations for the further development of security protocols in routing of frames in the Mesh-network standard 802.11s were presented.

Keywords: Hybrid wireless mesh network protocol, secure routing, wireless mesh network, standard 802.11s.

Введение. В современном мире системы связи играют важную роль в обществе. Качество, доступность и скорость соединения между абонентами сети во многом определяют уровень развития общества. Развитие технологий позволяет организовывать новые виды соединений устройств внутри сети. Одной из технологий физической организации сети является ячеистая топология. В отличие от звездообразной топологии, требующей маршрутизатор для соединения с Интернетом, сетевые узлы в ячеистой сети могут соединяться друг с другом напрямую, без подключения к Интернету. Ячеистая топология подходит для многих приложений, в том числе широкополосного доступа для домашних сетей, корпоративных сетей и систем автоматизации зданий.

Mesh-сеть (WMN – Wireless Mesh Network) основана на ячеистой топологии и представляет собой объединение между собой нескольких компьютеров или иных устройств в единую сеть, в которой отсутствует единый центральный сервер. WMN обеспечивает лучшую мобильность, более низкую стоимость развертывания, простое расширение сети, а также надежные соединения [1]. Именно эта структура обеспечивает одно из основных преимуществ mesh-сетей – адаптивную топологию, которая способна перестраиваться в случае недоступности или перегруженности одного из узлов сети.

1. Реализация и принцип работы протокола маршрутизации в стандарте 802.11s. Стандарт 802.11s позволяет Wi-Fi-устройствам самоорганизовываться и автоматически настраивать топологию сети. Wi-Fi-устройства mesh-сети называются сетчатыми станциями (STA – Station Networking). STA, которые находятся далеко друг от друга, могут связываться друг с другом, используя беспроводную маршрутизацию, когда пакеты данных передаются через промежуточные узлы.

Гибридный беспроводной протокол mesh-сети (HWMP) является протоколом по умолчанию для маршрутизации в стандарте 802.11s. Он реализован на канальном уровне по модели OSI [2].

Сетка STA может автоматически и эффективно формировать беспроводное соединение. Лучший путь может быть найден с помощью HWMP, который основан на алгоритме кратчайшего пути. Для определения кратчайшего пути используются алгоритмы Беллмана–Форда или Дейкстры [3]. Для выбора оптимальных маршрутов в сети используются различные критерии (метрики). Метрики могут включать в себя такую информацию, как длина пути, надежность, задержка, пропускная способность, загрузка и стоимость передачи трафика.

Гибридный протокол маршрутизации HWMP (Hybrid Wireless Mesh Protocol) использует стандартный набор служебных пакетов, правил их создания и обработки, наподобие протокола дистанционно-векторной маршрутизации по запросу (Ad Hoc On Demand Distance Vector, AODV) [4]. HWMP адаптирован для работы с адресами MAC-уровня и метриками путей. Гибридным он назван потому, что объединяет в себе два режима построения путей, которые могут быть использованы как по отдельности, так и одновременно в одной сети:

1) реактивный режим – построение маршрутных таблиц в узлах mesh-сети непосредственно перед передачей данных (по запросу);

2) проактивный режим – регулярная процедура обновления информации в маршрутных таблицах узлов всей сети. Процедуру инициирует корневой узел, в результате строится граф (дерево) путей с вершиной в корневом узле.

Существует четыре типа кадров в HWMP, непосредственно участвующие в процессе обнаружения пути:

1) путь запроса – Path Request (PREQ);
2) путь ответа – Path Reply (PREP);
3) ошибка пути – Path Error (PERR);
4) корневое объявление – Root Announcement (Rann).

На рис. 1 отображены форматы кадров в HWMP [1].

Каждый из этих кадров имеет поле: длина кадра (Length) и флаг (Flags), определяющий формат передачи (01 – роль портала, 10 – групповая передача, 11 – индивидуальная передача). Поле Hop Count в кадрах PREQ, PREP, RANN определяет количество прошедших узлов при передачи от узла отправителя к узлу назначения. Если узел назначения

не найден, то в поле Element ID устанавливается значение Error. Поле PREQ ID содержит уникальный идентификатор кадра PREQ. Поле Originator Address содержит MAC-адрес отправителя. Поле порядкового номера инициатора (Originator Sequence Number) кодируется как целое без знака и содержит порядковый номер, специфичный для отправителя. Поле Originator External Address определяет MAC-адрес проксируемого объекта в случае, если PREQ кадр сгенерирован за границей mesh-сети. Поле Lifetime устанавливает время в течении которого кадр считается действительным. Target count дает количество направлений, содержащихся в этом PREQ. Поле Target Address представляется как 48-битный MAC-адрес узла назначения.

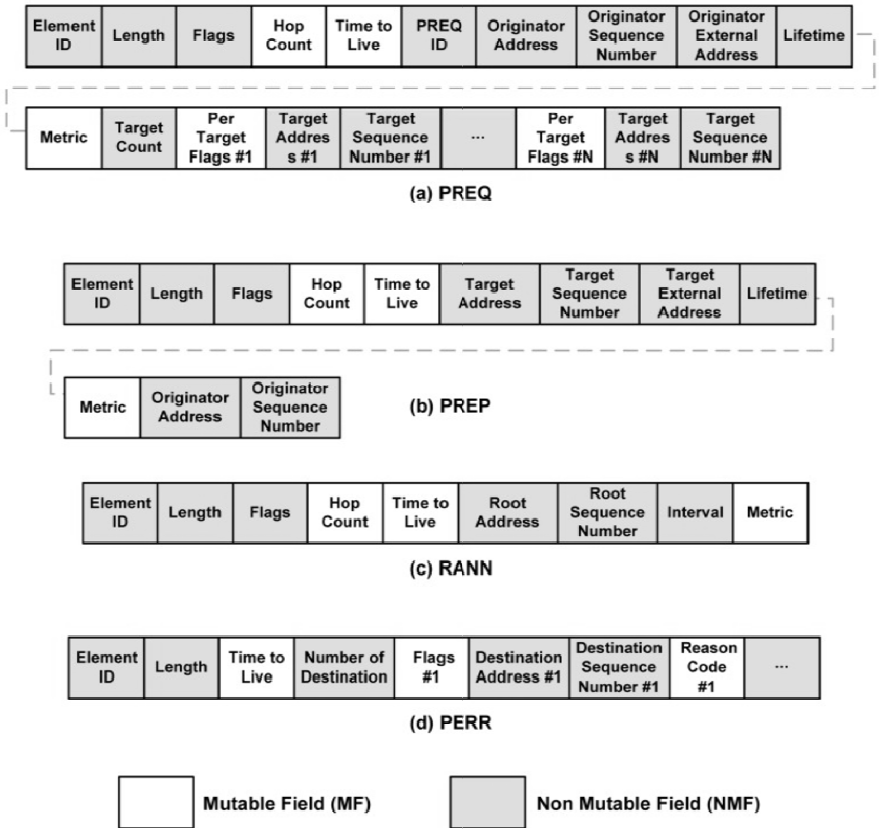

Рис. 1. Формат кадров в HWMP

В кадрах HWMP есть изменяемые (MF – Mutable Field) и неизменяемые (NMF – Non Mutable Field) поля [3]. MF содержит информацию, которая будет обновляться по мере распространения кадров в се-

ти. NMF содержит информацию, которая не может быть изменена в промежуточных узлах STA.

В реактивном режиме HWMP узел отправляет широковещательный PREQ-кадр. Пути выбираются на основании метрики, для распространения информации служит специальное поле в служебных пакетах запроса пути. Этот пакет распространяется через соседние узлы по всей сети, пока не достигнет узла-назначения [3]. По мере продвижения от узла к узлу модифицируется поле метрики пути. В итоге формируется полная метрика пути «получатель-отправитель». Узел-адресат может отправлять инициатору пакет подтверждения PREP, содержащий итоговое значение метрики пути «отправитель-получатель», в этом случае соединение является зарегистрированным. Приняв его, узел-инициатор получает информацию об установленном пути. В реактивном режиме пакеты подтверждения PREP может отправлять не только узел назначения, но и все промежуточные узлы, успешно принявшие пакет запроса PREQ (если в пакете установлены соответствующие флаги).

Все узлы mesh-сети хранят информацию о каждом узле сети, обновляя ее на основании полученных служебных пакетов. Такая информация в данных пакетах передается в полях «адрес отправителя», «метрика пути», «порядковый номер запроса» (Originator's DSN (OSN)) [5]. Помимо полей метрики пути по мере прохождения от узла к узлу в пакете может изменяться значение поля «время жизни» (Time to Live, TTL). Если этот параметр используется, он декрементируется в каждом узле следования. В маршруте следования пакетов могут быть замкнутые маршруты (циклы). Чтобы избежать таких циклов, используется порядковый номер запроса. Этот параметр служит номером при рассылке пакетов поиска пути. Каждое mesh-устройство имеет свой собственный DSN. Перед началом процедуры поиска пути DSN инициатора увеличивается на 1 и записывается в поле Originator's DSN пакета запроса PREQ [2]. Кроме того, в пакете содержится адрес инициатора (адрес начала пути). Все узлы сети хранят информацию о каждом узле mesh-сети, обновляя ее на основании полученных служебных пакетов. Такая информация в данных пакетах передается в полях «адрес отправителя», «метрика пути», «порядковый номер».

Узел, получив пакет PREQ, сравнивает значение OSN с ранее сохраненным значением для этого же отправителя. Устройство принимает, обрабатывает и ретранслирует пакет PREQ, только если текущий

OSN в пакете больше ранее сохраненного или они равны, но метрика пути ранее полученного пакета хуже, чем у вновь полученного (т.е. повторного приема и ретрансляции одного и того же пакета быть не может). В реактивном режиме пакеты подтверждения PREP может отправлять не только узел назначения, но и все промежуточные узлы, успешно принявшие пакет запроса PREQ (если в пакете установлены соответствующие флаги).

В проактивном режиме назначается корневой узел (или узлы). Этот узел периодически рассылает пакеты PREQ, которые распространяются по всей сети. Все узлы сети, принявшие проактивный PREQ, сохраняют адрес узла-отправителя и широковещательно транслируют PREQ с измененными полями (поля метрики и TTL) и отправляют PREP корневому узлу, если установлен соответствующий флаг в PREQ. Помимо описанных методов выбора пути на основе пакетов PREQ и PREP стандарт предусматривает процедуру на основе пакетов оповещения о корневом узле Rann. Этот метод принципиально не отличается от уже рассмотренного метода.

2. Уязвимости протокола маршрутизации HWMP. По мере распространения кадров по сети некоторые части кадров могут быть изменены в промежуточных узлах. Наиболее часто измененные части сообщения маршрутизации включают счетчик переходов и метрику пути запрашиваемого узла. С точки зрения сетевой безопасности промежуточные узлы сети не являются доверенными узлами. Для обеспечения безопасности маршрутизации сообщений, для двух типов частей кадров, изменяемых и неизменяемых полей, нужны различные требования защиты. Изменяемые поля должны обновляться в соответствии с правилами маршрутизации по мере продвижения кадров в сети. Каждый узел требует криптографической защиты для обнаружения незаконно измененной информации в сообщении. Безопасность неизменяемых полей и целостности данных должна осуществляться аутентификация полей при передачи кадров между узлами источника и назначения.

В то время как принципы работы HWMP определены в разработанном стандарте, функции безопасности не описываются для этого протокола [1]. Атаки на протоколе маршрутизации можно разделить на внешние и внутренние. Внешние атаки относятся к нападениям злоумышленника, который не имеет доступа к сети. Внутренние атаки относятся к нападениям узла, прошедшего проверку подлинности в сети.

Существуют следующие типы внешних атак на mesh-сети:

1) переполнение – злоумышленник может транслировать PREQ-кадры непрерывно, что вызовет переполнение сети [6]. PREQ-кадры непрерывно распространяются по всему WMN. Атакующий может использовать адрес получателя, которого не существует в WMN, из-за чего PREQ-кадры будут распространяться по всей сети. Злоумышленник может также непрерывно транслировать Rann-кадры. Это непрерывное вещание заставит другие узлы сети отвечать на Rann-запросы. Если пути известны, злоумышленник может отправить поддельные PERR-кадры [7]. Это ложное сообщение об ошибке приведет к удалению информации о маршруте целевого узла в таблице маршрутизации. Узел сети будет вынужден запрашивать новые пути из-за поддельных PERR-кадров;

2) диверсия – злоумышленник может увеличить порядковый номер запроса в PREQ-кадре, тем самым обманув другие сетки STA. В этом случае таблица маршрутизации для каждого узла будет обновляться на основе предположения, что PREQ-кадр содержит новую информацию. Злоумышленник также может понизить значение метрики, чтобы путь стал лучше, когда на самом деле существуют наиболее оптимальные пути;

3) атаки типа Wormhole и Blackhole – в случае Wormhole-атаки злоумышленник может следить за передаваемыми пакетами данных [7]. В Blackhole-атаке передаваемые пакеты данных будут удалены злоумышленником во время пересылки [8]. В этих атаках маршрут должен проходить через узел злоумышленника;

4) имперсонация – есть четыре поля адреса в рамках HWMP: передатчик, приемник, отправитель и цель [9]. Злоумышленник может выдавать себя за другую сетку STA, изменяя адреса в этих областях. Имперсонация может быть использована для создания цикла, изменив адреса передатчика и приемника. Также атакующий, выдавая себя другим узлом, может инициировать PREQ-запрос. Эта имперсонация выполняется путем манипулирования адресов отправителя и цели;

5) атака типа Replay (воспроизведение) – злоумышленник может перехватить на нескольких сеансах связи передаваемые пакеты. Отправляя перехваченные кадры PREQ и подменяя MAC-адрес жертвы, злоумышленник убедит узел назначения в том, что узел жертвы снова пытается связаться с узлом назначения. Узел назначения отвечает

с PREP для атакующего узла. На данный момент злоумышленник начинает осуществлять связь с узлом назначения, а узел-адресат считает, что злоумышленник является первоисточником;

6) подслушивание – HWMP-кадры содержат информацию о маршрутизации. Информация о маршрутизации может быть получена путем прослушивания обмена кадрами в HWMP. Эта информация может быть полезной или бесполезной. В некоторых случаях число узлов сети в WMN должно храниться в секрете. Если WMN используется в военной области, противник может анализировать военный потенциал, основываясь на количестве узлов. Кроме того, информация о пути маршрутизации может быть использована для анализа положения и расстояния других узлов сети [10].

Внутренние злоумышленники являются узлами WMN. Внутренние атакующие имеют все необходимые ключи безопасности. В этих атаках могут быть применены все типы внешних атак. Обнаружить и предотвратить внутренние атаки гораздо сложнее, чем внешние. Реальной проблемой в WMN является возможность внутренней атаки. Внутренние злоумышленники могут использовать в HWMP-пути переадресации атаки для создания Wormhole и Blackhole [11]. Внутренний злоумышленник может также претендовать на роль корня в сети. Когда сетка STA пытается посылать пакеты, он будет инициализировать процесс обнаружения пути до цели. Если нет пути в маршрутных таблицах отправителя, узел будет передавать пакеты корню. Таким образом, можно будет следить за первыми несколькими пакетами данных.

Существует несколько протоколов безопасности кадров HWMP:

- протокол целостности широковещания (BIP);
- блочный шифр сообщений кода аутентификации (CCMP);
- безопасный HWMP (SHWMP);
- идентификация на основе шифрования HWMP (IBC-HWMP);
- эллиптические кривые цифровой подписи HWMP (ECDSA-HWMP);
- сторожевые HWMP (Watchdog HWMP).

На рис. 2 показано, как кадры могут быть защищены с помощью протокола CCMP [6].

Протокол CCMP шифрует тело кадра и код целостности сообщения (MIC) [1]. Заголовок HDR в CCMP содержит информацию, необ-

ходимую для дешифрования и проверки целостности, например, номер пакета (Packet Number – PN), вектор инициализации (Initialization Vector – IV) и идентификатора ключа. MAC HDR содержит MAC-адреса передатчика и приемника.

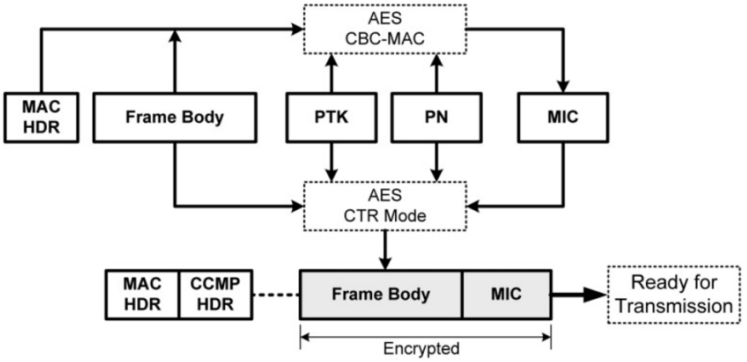

Рис. 2. Принцип работы CCMP

На рис. 3 показано, как кадры могут быть защищены с помощью протокола BIP [6].

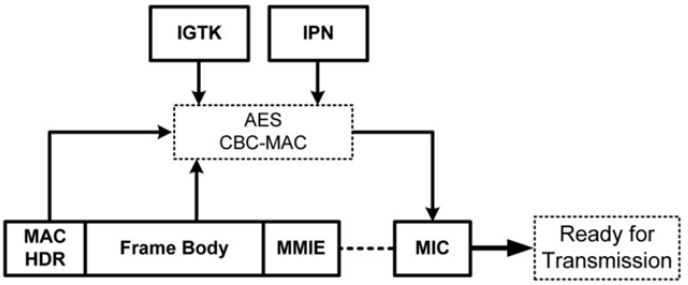

Рис. 3. Принцип работы BIP

Протокол безопасности BIP вводит целостность IGTK (Integrity Group Temporal Key) и номер пакета целостности (Integrity Packet Number – IPN), которые используются исключительно в BIP. Использование IGTK и IPN похоже на использование PTK (Pairwise Transient Key) и PN в CCMP [12]. Элемент целостности кода сообщения (MIC Integrity Element – MMIE) содержит информацию, необходимую для проверки целостности, включая IPN и идентификатор ключа.

Протокол BIP не обеспечивает шифрование и предназначен для широковещательных кадров, то время как CCMP предназначен для однонаправленных кадров.

Безопасный HWMP обеспечивает защиту кадров от внешних атак. Для создания кода целостности MIC изменяемых полей используется алгоритм дерева Merkle [6]. Код целостности шифруется с помощью PTK/GTK для обеспечения аутентификации и целостности изменяемых полей. Неизменяемые поля также шифруются с использованием PTK/GTK, которое обеспечивает конфиденциальность кадров. Для кадров PREQ счетчик количества узлов, время жизни (TTL), метрика и флаг назначения являются изменяемыми элементами. Количество переходов, TTL и метрика являются изменяемыми элементами для кадров PREP и Rann. Безопасный HWMP не предоставляет службы безопасности для PERR-кадров.

Протокол SHWMP концентрируется на защиту кадров от внешних атак. GTK обеспечивает защиту только между пиринговыми соседями. Недостатком протокола SHWMP является то, что он не обеспечивает защиты от внутренних атак, а также не обеспечивает надежную аутентификацию и проверку целостности кадров [7]. Этот протокол также не имеет каких-либо схем безопасности для PERR-кадров. Протокол не обеспечивает проверку подлинности и целостности неизменяемых полей в кадрах при передаче через промежуточные узлы от узла-источника до узла-назначения. Кроме того, в SHWMP не существует защиты от атак типа Replay.

MAC-адрес используется в качестве идентификатора узла STA в IBC-HWMP [13]. Закрытые ключи используется для зашифровки изменяемых полей кадров PREQ и PREP. Открытые ключи распространяются для проверки подписей. Схема подписи и ECDSA используются для создания подписей для протоколов IBC-HWMP и ECDSA-HWMP [14]. Для реализации ECDSA-HWMP в сети должен передаваться цифровой сертификат, что требует третьего доверенного центра сертификации. В беспроводной ячеистой сети внедрение центра сертификации нецелесообразно.

Протокол IBC-HWMP не обеспечивает защиту Rann и PERR-кадров, а также защиту аутентификации и целостности для неизменяемых полей при передаче кадров от узла-источника к узлу-назначения. Кроме того, не существует защиты от атак типа Replay.

Сторожевой HWMP может обнаружить незаконное изменение полей кадров [15]. При передаче PREQ-кадра узел-отправитель широковещательно транслирует этот кадр всем соседним узлам. Соседние

узлы, получившие PREQ-кадр, также начинают широковещательно транслировать этот кадр. При достижении кадром PREQ узла назначения этот узел принимает кадры PREQ от соседних узлов и сравнивает их с оригинальным. Это означает, что все узлы должны хранить информацию о всех передаваемых PREQ-кадрах и сравнивать их со всеми PREQ-кадрами соседних узлов. По мере увеличения числа узлов ухудшается пропускная способность, что в значительной степени отражается на эффективности протокола Watchdog HWMP.

Выводы. Таким образом, существующие протоколы безопасности в HWMP не обеспечивают должной защиты сети. Мы имеем следующие рекомендации для дальнейшего развития протокола безопасности HWMP. Должны быть реализованы:

– целостность кадров. Это будет препятствовать промежуточным сеткам STA изменять порядковый номер или выдавать себя за отправителя или получателя;

– уровень доверия, выполненный так, чтобы только авторизованные сетки STA могли назначать себя в качестве корневого узла сети;

– эффективный метод для обнаружения поддельной метрики пути от любого вредоносного узла сети;

– разработанная схема безопасности Rann- и PERR-кадров;

– аутентификация и целостность передаваемых данных от узла-источника промежуточным узлам на пути передачи. Эта реализация обеспечит защиту от модификации или подделки кадров, нарушения маршрута, переполнения ресурсов сети и атак от изоляции узла;

– защита от атаки Replay.

Библиографический список

1. A Security Analysis of the 802.11s Wireless Mesh Network Routing Protocol and Its Secure Routing Protocols [Электронный ресурс]. – URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3821297/ (дата обращения: 22.06.2017).

2. Ghumman S.A. Per-Arne-Wiberg. Security in Wireless Mesh Networks // School of Information Science, Computer and Electrical Engineering, Halmstad University. – 2009. – № 1. – P. 1–54.

3. Вишневский В.М., Гузаков Н.Н., Лаконцев Д.В. Mesh-сети стандарта IEEE 802.11s: протоколы маршрутизации // Первая миля. – 2009. – № 1. – С. 16–21.

4. Zapata M.G. Mobile Ad Hoc Networking Working Group INTERNET DRAFT Secure Ad Hoc On-Demand Distance Vector (SAODV) [Электронный ресурс]. – 2013. – URL: http://people.ac.upc.edu/guerrero/papers/draft-guerrero-manet-saodv-06.txt (дата обращения: 10.05.2017).

5. Akyildiz F.I., Wang X., Wang W. Wireless mesh networks // A survey. Comput. Netw. ISDN Syst. – 2005. – № 1. – P. 445.

6. Islam M.S., Hamid M.A., Hong C.S. SHWMP: A secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh network // Trans. Comput. Sci. – 2009. – № 6. – P. 95–114.

7. A survey on security in wireless mesh networks / P. Yi, Y. Wu, F. Zou, N. Liu // IETE Tech. Rev. – 2010. – № 27. – P. 6–14.

8. Al-Shurman M., Yoo S.M., Park S. Black Hole Attack in Wireless Ad Hoc Networks // Proceedings of ACM 42nd Southeast Conference, Huntsville, AL, USA. – 2004. – P. 1–3.

9. Passive Security Threats and Consequences in IEEE 802.11 Wireless Mesh Networks / S. Khan, N. Mast, K.K. Loo, A. Salahuddin // Int. J. Dig. Cont. Tech. – 2008. – P. 4–8.

10. Naeem T., Loo K.K. Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks // Int. J. Dig. Cont. Tech. – 2009. – P. 88–93.

11. PA-SHWMP: A privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks / H. Lin, J. Ma, J. Hu, K. Yang // EURASIP J. Wirel. Commun. Netw. – 2012. – P. 69.

12. 802.11 Working Group of the IEEE 802 Committee. IEEE P802.11s // D4.01 Draft Standard. – IEEE, Washington, DC, USA. – 2010.

13. Ben-Othman J., Benitez Y.I.S. IBC-HWMP: A novel secure identity-based cryptography-based scheme for hybrid wireless mesh protocol for IEEE 802.11s // Concurr. Comput. Pract. Exper. – 2011. – P. 1982–2000.

14. Vulnerability assessment of AODV and SAODV routing protocols against network routing attacks and performance comparisons [Электронный ресурс]. – URL: http://ieeexplore.ieee.org/document/5983282/?reload=true (дата обращения: 22.06.2017).

15. Naeem T., Loo K.K. Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks // Int. J. Dig. Cont. Tech. Appl. – 2009. – P. 88–93.

References

1. A Security Analysis of the 802.11s Wireless Mesh Network Routing Protocol and Its Secure Routing Protocols, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3821297/ (accessed 22 June 2017).

2. Ghumman S.A. Per-Arne-Wiberg. Security in Wireless Mesh Networks. School of Information Science, Computer and Electrical Engineering, Halmstad University, 2009, no. 1, pp. 1-54.

3. Vishnevskii V.M., Guzakov N.N., Lakontsev D.V. Mesh-seti standarta IEEE 802.11s: protokoly marshrutizatsii [Mesh networks of the IEEE 802.11s standard: routing protocols]. Pervaia milia, 2009, no. 1, pp. 16-21.

4. Zapata M.G. Mobile Ad Hoc Networking Working Group INTERNET DRAFT Secure Ad Hoc On-Demand Distance Vector (SAODV), 2013, available at: http://people.ac.upc.edu/guerrero/papers/draft-guerrero-manet-saodv-06.txt (accessed 10 May 2017).

5. Akyildiz F.I., Wang X., Wang W. Wireless mesh networks: a survey. Computer Networks and ISDN System, 2005, no. 1, p. 445.

6. Islam M.S., Hamid M.A., Hong C.S. SHWMP: a secure hybrid wireless mesh protocol for ieee 802.11s wireless mesh network. *IEEE Transactions on Computers in Science*, 2009, no. 6, pp. 95-114.

7. Yi P., Wu Y., Zou F., Liu N. A survey on security in wireless mesh networks. *IETE Tech. Rev*, 2010, no. 27, pp. 6-14.

8. Al-Shurman M., Yoo S.M., Park S. Black Hole Attack in Wireless Ad Hoc Networks. Proceedings of ACM 42nd Southeast Conference, Huntsville, AL, USA, 2004, pp. 1-3.

9. Khan S., Mast N., Loo K.K., Salahuddin A. Passive Security Threats and Consequences in IEEE 802.11 Wireless Mesh Networks. *Int. J. Dig. Cont. Tech*, 2008, pp. 4-8.

10. Naeem T., Loo K.K. Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks. *Int. J. Dig. Cont. Tech,* 2009, pp. 88-93.

11. Lin H., Ma J., Hu J., Yang K. PA-SHWMP: A privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks. *EURASIP J. Wirel. Commun. Netw,* 2012. 69 p.

12. 802.11 Working Group of the IEEE 802 Committee. IEEE P802.11s. D4.01 Draft Standard. IEEE, Washington, DC, USA, 2010.

13. Ben-Othman J., Benitez Y.I.S. IBC-HWMP: A novel secure identity-based cryptography-based scheme for hybrid wireless mesh protocol for IEEE 802.11s. *Concurr. Comput. Pract. Exper*, 2011, pp. 1982-2000.

14. Vulnerability assessment of AODV and SAODV routing protocols against network routing attacks and performance comparisons, available at: http://ieeexplore.ieee.org/document/5983282/?reload=true (accessed 22 June 2017).

15. Naeem T., Loo K.K. Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks. *Int. J. Dig. Cont. Tech. Appl,* 2009, pp. 88-93.

Сведения об авторах

Абраров Рафаэль Рашитович (Самара, Россия) – студент Самарского национального исследовательского университета им. академика С.П. Королева (443086, Самара, ул. Московское шоссе, 34, e-mail: rafaelabrarov@gmail.com).

Бурлаков Михаил Евгеньевич (Самара, Россия) – старший преподаватель кафедры безопасности информационных систем Самарского национального исследовательского университета им. академика С.П. Королева (443086, Самара, ул. Московское шоссе, 34, e-mail: knownwhat@gmail.com).

About the authors

Abrarov Rafael Rashitovich (Samara, Russian Federation) is a Student Samara National Research University (443086, Samara, 34, Moskovskoye Shosse, e-mail: den1008@bk.ru).

Burlakov Mikhail Evgenyevich (Samara, Russian Federation) is a Senior Lecturer in Department of information security systems Samara National Research University (443086, Samara, 34, Moskovskoye Shosse, e-mail: knownwhat@gmail.com).

Получено 31.07.2017