помощью которых можно получить ключи шифрования, до способа шифрования. Кроме того, можно обговорить режим взаимодействия. Другими словами клиент и сервер договариваются подписывать цифровой подписью запросы, шифровать или и то и другое. Тогда как SSL гарантирует, что соединение между программой просмотра и клиентом устанавливается с сервером и ни с кем иным, то S -HTTP предоставляет широкий спектр инструментов шифрования и делает это на уровне отдельного документа. Значительным преимуществом S -HTTP над SSL можно считать использование цифровой подписи. Так же, в отличие от SSL, протокол S-HTTP полностью совместим с отличными от S-HTTP серверами Web, хотя, в этом случае, информация не будет защищена, если хотя бы один из игроков не озабочен защитой.

Подводя итоги, SSL в настоящее время является де-факто стандартом, обеспечивающим конфиденциальность информации. Он поддерживается всеми известными браузерами, однако алгоритм шифрования SSL недостаточно надежен.

Протокол S-HTTP предназначен только для HTTP-серверов и не работает на других платформах Internet, распространенность S -HTTP только среди производителей Web-серверов. Общей чертой SSL и S -HTTP является то, что разрабатывающие их компании делают ставку на защиту денежных расчетов.

Литература

1. Арипов М. Англо-русско-узбекский словарь сокрашенных слов по информатике. Т., Университет, 2001 г.
2. Евсеев Г. Специальная информатика. Учебное пособие. М., 2002 г.
3. Молдовян К. Безопасность глобальных сетевых технологии. М., 2002 г.

Р.Р. Абраров, М.Е. Бурлаков

ОРГАНИЗАЦИЯ ДЕЦЕНТРАЛИЗОВАННОЙ, БЕЗОПАСНОЙ И АНОНИМНОЙ MESH-СЕТИ

(Самарский университет)

Достижение надежных и эффективных сетей передачи данных является сложной задачей. Беспроводные Mesh-сети (Wireless Mesh Network) – это один из примеров обеспечения широкополосной, надежной и масштабируемой сети передачи данных. Беспроводные ячеистые сети могут объединять в единую сеть различные устройства. WMN обеспечивает лучшую мобильность, более низкую стоимость развертывания, простое расширение сети, а также надежные соединения [1].

На рисунке 1 представлены возможности протоколов Mesh-сетей. Существующие протоколы Mesh-сетей могут организовать сеть только при наличии маршрутизатора. Однако, с развитием технологий, внедряемых в мобильные

устройства, появляется возможность соединения двух и более устройств напрямую без обязательного соединения к маршрутизатору. Это возможно сделать с помощью Bluetooth и технологий WiFi Direct на Android и Multipeer Connectivity Framework на устройствах Apple. Также эти протоколы не обеспечивают анонимность узлов Mesh-сети.

	CJDNS	B.A.T.M.A.N.	DTN	Netsukuku	OSPF
Авто-назначение адреса	Да	Нет	Нет	Да	Нет
Авто-конф. Маршрутизация	Да	Да	Да	Да	Частично
Распределенная маршрутизация	Да	Да	Да	Да	Частично
Объеденение сетей	Да	Нет	Нет	Нет	Нет
IPv4/v6	IPv6	IPv4/v6	IPv4/v6	IPv4	IPv4
Шифрование трафикка внутри сети	Да	Нет	Нет	Нет	Нет
Авто-настройка	Да	Да	Да	Нет	Да
Разработка	Активная	Закончена	Активная	Нет	Закончена
Поддержка UNIX\LINUX\OpenWRT	Да	Да	Да	Да	Да
Поддержка Windows	В разработке	Нет	Нет	Нет	Нет
Поддержка Mac OS X	Да	Да	Да	Да	Да
Потребление ресурсов	Низкое	Низкое	Низкое	Высокое	Низкое
Оверлейны режим работы	Да	Нет	Нет	Нет	Нет
Интеграция в ядро Linux	Нет	Да	Нет	Нет	Да
Анонимность сети	Нет	Нет	Нет	Нет	Нет
Организация сети без выделенного роутера	Нет	Нет	Нет	Нет	Нет

Рис. 1. Возможности протоколов Mesh-сетей

Технология Multipeer Connectivity Framework поддерживает одноранговые соединения, обнаружение ближайших устройств и соединение с этими устройствами. Устройства iOS соединяются с помощью сети Wi-Fi, Wi-Fi Peer-to-Peer и Bluetooth. В macOS и tvOS используются сети Wi-Fi, Wi-Fi Peer-to-Peer и Ethernet [2].

На рисунке 2 изображен принцип соединения устройств от компании Apple с помощью технологии Multipeer Connectivity Framework.

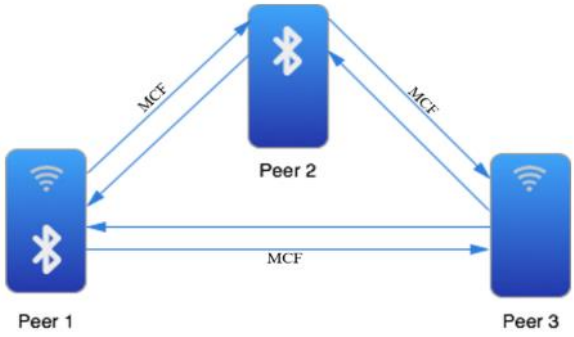

Рис. 2. Принцип соединения устройств Apple с помощью технологии Multipeer Connectivity Framework

Устройства, поддерживающие технологию WiFi Direct, могут соединяться друг с другом без подключения к традиционной домашней или офисной горячей точке. Мобильные телефоны, камеры, принтеры, ПК и игровые устрой-

ства, поддерживающие эту технологию, могут соединяться друг с другом напрямую для передачи данных [3]. Сразу же стоит отметить, что скорость передачи данных при прямом подключении может достигать 200-250 Мбит/с. При этом радиус действия при прямой видимости равен 200 метрам и около 50-100 метрам в зданиях. Также особого внимания достоин уровень безопасности такого канала связи.

Для организации сети предполагается использование стандарта IEEE 802.11s. Стандарт 802.11s позволяет WiFi устройствам самоорганизовываться и автоматически настраивать топологию сети. WiFi 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 [4]. Гибридный беспроводной протокол Mesh-сети (Hybrid Wireless Mesh Protocol) является протоколом по умолчанию для маршрутизации в стандарте 802.11s [5].

Безопасность сети. Предполагается, что для распределения сетевых адресов будет использоваться протокол IPv6, что обеспечивает неограниченное количество адресов. Учитывая то, что узлами сети потенциально могут стать устройства, задействованные в Интернете вещей, использование этого протокола становится необходимым. Однако выходные узлы (узлы, которые имеют возможность выхода в глобальную сеть Интернет) будут иметь как адрес IPv4, так и IPv6. Так как выходные узлы связаны с глобальной сетью, то и все устройства Mesh-сети имеют возможность выхода в Интернет через эти узлы.

Скорость соединения устройств Mesh-сети с глобальной сетью зависит от количества узлов, необходимых для достижения выходных узлов, и от скорости Интернет соединения самих выходных узлов. Так как выходных узлов в Mesh-сети может быть достаточно много, то потенциальных маршрутов до глобальной сети становится достаточно, чтобы обеспечить отказоустойчивость сети, распределение передаваемых данных и меньшую нагрузку для выходных узлов. Также это гарантируют анонимность узлов Mesh-сети, где глобальной сети известен только выходной узел.

Для определения необходимой пропускной способности выходного узла сети рассмотрим метод, основанный на усредненной оценке входных параметров рассматриваемой сети. Приведем пример, в котором используются фактически введенные входные параметры: количество узлов сети (S) – 15 000; пропускная способность выходного узла (A) – 10 Мбит/с; средний размер файла (F) – 120 000 байт; средний размер пакета (P) – 250 байт; вероятность перегрузки узла (α) – 5 %.

Вычисляем количество запросов к выходному узлу в секунду:

$$\lambda=\frac{S\times M}{3600}=15000\times 3/3600 = 12{,}5 \quad (1)$$

Вычисляем время прохождения пакета для заданной пропускной способности выходного узла:

$$T = \frac{T\times F}{A\times 10^6} = 12 \times 8 \times 10^4/10^7 \approx 0.1 \quad (2)$$

Вычисляем количество одновременных запросов в секунду: P[N>n]<α для данного n=3:

$$P[N > n] = \sum_{i=n+1}^{\infty} \mathrm{i}\lambda\mathrm{T}\alpha - \lambda\mathrm{T}/\mathrm{i} \quad (3)$$

Получаем количество пакетов, передаваемых маршрутизатору в секунду:

$$R = (A \times \frac{P[N>n]}{8})/P = \frac{10\times10^6}{8\times250} = 5000 \quad (4)$$

Получаем общее количество пакетов, передаваемых в секунду выходному узлу, учитывая 3 одновременных запроса:

$$C = R \times N = 5000 \times 3 = 15000 \quad (5)$$

Метод вычисления оптимальной пропускной способности выходного узла может применяться для определения кратчайшего маршрута передачи данных.

Выходные и промежуточные узлы могут быть ненадежными и могут видеть, проходящий через них, трафик. Поэтому сеть обеспечивает автоматическое сквозное шифрование. В сквозном шифровании конечными пунктами передачи являются непосредственно устройства отправителя и получателя. Сообщение шифруется локально на устройстве отправителя и может быть расшифровано исключительно на устройстве получателя. Сквозное шифрование реализовано только в протоколе Mesh-сети cjdns. Не смотря на шифрование трафика внутри сети, в cjdns не реализованы механизмы анонимизации узлов Mesh-сети.

Передача сообщений в существующих сетях осуществляется в соответствии с моделью «клиент-сервер». Сохранение данных о пользователях на центральных серверах ставит под угрозу конфиденциальности этих данных. Данные могут быть получены третьими лицами в результате взлома сервера.

Основной идеей Mesh-сети является децентрализованный обмен сообщениями. Суть этой идее заключается в создании сети, которая обеспечит анонимность и конфиденциальность пользователей, а также отсутствие единой точки отказа.

Mesh-сети реализуют концепцию взаимодействия одноранговых сетей (P2P). В сетях P2P клиенты подключаются напрямую друг к другу для передачи данных. Основной проблемой сетей P2P является поиск других узлов. Чтобы решить эту проблему, предлагается использовать решение, применяемое в протоколе BitTorrent – DHT (распределенная хеш-таблица).

BitTorrent использует DHT для хранения информации о контактах для «трекер-торрентов». По сути, каждый равноправный узел становится трекером. Протокол основан на Kademila и реализован по UDP. Каждый узел поддерживает таблицу маршрутизации известных узлов. Узлы в таблице маршрутизации используются в качестве отправных точек для запросов в DHT.

Для обеспечения анонимности узлов внутри Mesh-сети предполагается использование технологии Onion-маршрутизации. В луковой сети сообщения инкапсулируются в слои шифрования. Зашифрованные данные передаются через промежуточные узлы сети, называемых луковыми маршрутизаторами, каждый из которых расшифровывает один слой, открывая следующий узел назначения данных. Когда сообщение достигает узла назначения, расшифровывается

последний слой шифрования. Отправитель остается анонимным, потому что каждый промежуточный узел знает только о местоположение непосредственно предшествующих и следующих узлов сети.

Таким образом, использование современных технологий дает возможность организации Mesh-сети, в которой предусмотрены вопросы безопасности. Такая сеть обеспечивает безопасность передаваемых данных, анонимность узлов Mesh-сети, а также невозможность проведения атак типа «человек по середине» из-за своей распределенной структуры.

Литература

1. A Security Analysis of the 802.11s Wireless Mesh Network Routing Protocol and Its Secure Routing Protocols [Электронный ресурс]. – Режим доступа: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3821297, свободный (дата обращения: 19.03.2018).

2. Wi-Fi Direct [Электронный ресурс]. – Режим доступа: https://www.wi-fi.org/discover-wi-fi/wi-fi-direct, свободный (дата обращения: 10.03.2018).

3. Multipeer Connectivity Framework [Электронный ресурс]. – Режим доступа: https://developer.apple.com/documentation/multipeerconnectivity, свободный (дата обращения: 15.03.2018).

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

5. Zapata M.G., Mobile Ad Hoc Networking Working Group INTERNET DRAFT Secure Ad Hoc On-Demand Distance Vector (SAODV) [Электронный ресурс]. – Режим доступа: http://people.ac.upc.edu/guerrero/papers/draft-guerrero-manet-saodv-06.txt, свободный (дата обращения: 15.03.2018).

Т.Е. Андросова, В.А. Федосеев

МЕТОД ВСТРАИВАНИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯ В ФОРМАТЕ JPEG 2000

(Самарский университет)

Формат сжатия изображений JPEG 2000, несмотря на меньшую в сравнении с JPEG популярность у пользователей, позволяет обеспечивать лучшее сжатие и потому широко применяется, в частности, в системах дистанционного зондирования, медицинской визуализации и ряде других областей [1]. Это обусловливает актуальность задачи защиты изображений в формате JPEG 2000 от несанкционированных изменений. Так, например, получателю данных дистанционного зондирования необходимо иметь уверенность в отсутствии их фальсификаций, а доктор, ставящий диагноз на основании цифрового снимка, должен быть убеждён в его подлинности и в отсутствии искажений, вызванных чрезмерным сжатием данных.