УДК 004.056

Ф. Г. Максимов-Наливайко

ЗАЩИЩЕННАЯ ОТПРАВКА СООБЩЕНИЙ ПО МЕШ-СЕТИ НА ОСНОВЕ BLUETOOTH

Рассмотрены основные проблемы, решение которых необходимо для обеспечения безопасности конфиденциальности коммуникации между участниками мобильных меш-сетей на основе смартфонов. Представлены важные характеристики технологий Bluetooth и Bluetooth Low Energy, с помощью которых можно решить часть проблем. Кратко описана криптография на эллиптических кривых, выбрана конкретная кривая. На основе обмена ключами на эллиптических кривых и различных криптопримитивов построена гибридная модель шифрования, позволяющая обмениваться защищенной информацией с использованием симметричного шифрования. Показаны процессы зашифрования и расшифрования сообщений с использованием данной схемы. В результате описанные технологии и гибридная схема объединяются в базовый алгоритм защищенной передачи данных по меш-сети на основе Bluetooth, достаточный для программной реализации.

In the paper we discuss the main problems that have to be solved to ensure the confidentiality of communication between the nodes of mesh networks based on smartphones. We describe the important details of Bluetooth and Bluetooth Low Energy technologies, using which you can solve some of the problems described. Next, we briefly describe elliptic curve cryptography and choose a specific curve for it. We build an Elliptic Curve Integrated Encryption Scheme based on the elliptic curves key exchange and various crypto primitives that allows exchanging protected information using symmetric encryption. We also describe the processes of encryption and decryption of messages using this. As a result, the described technologies and the hybrid scheme are combined into the basic algorithm for secure data transmission over a mesh network based on Bluetooth, sufficient for software implementation.

Ключевые слова: меш-сеть, Bluetooth, BLE, эллиптические кривые, криптография, гибридная схема.

Keywords: mesh network, Bluetooth, BLE, elliptic curve, cryptography, ECIES.

Введение

В настоящее время активно развиваются альтернативные методы передачи данных, не связанные или только частично связанные с использованием централизованных коммерческих и государственных сетей. Подобно тому как криптовалюты позволяют людям совершать операции с деньгами без участия и контроля государства и банков, построенные на клиентских устройствах меш-сети дают пользователям возможность общения друг с другом без участия государственных органов и операторов связи. Помимо этого, развертка меш-сети помогает в тех ситуациях, когда обычные сети не покрывают данную область либо не справляются с нагрузкой: на природе, концертах и т. п.

Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2020. № 4. С. 26 – 33.

Одной из основных проблем в меш-сетях является обеспечение безопасности при передаче информации. Поскольку меш-сеть может покрывать большую площадь, а подключиться к ней есть возможность у любого человека, необходимо заботиться о защите сети от действий злоумышленников.

В данной работе рассматриваются технические основы меш-сетей, Bluetooth и Bluetooth Low Energy, а также описываются необходимые криптопримитивы. На основе этих технологий и алгоритмов строится прообраз сети, в которой можно обеспечить необходимую защиту при передаче сообщений.

Меш-сети

Беспроводная меш-сеть (wireless mesh network, WMN) — это сеть, которая включает в себя различные беспроводные устройства с точками доступа. Каждый клиент в сети также является сервером, передавая данные дальше по сети. Поскольку сеть децентрализована, передать данные узел может только своим соседям. Обычно в таких сетях используются технологии Wi-Fi, Wi-Fi Direct и Bluetooth.

Визуально архитектура WMN представляет собой связный граф, обычно со множеством циклов. Данные, направляясь от адресата к получателю, проходят через цепочку устройств посередине, совершая последовательность коротких «прыжков» (hops). Устройства посередине цепи могут передавать данные либо всем своим соседям, либо, зная маршрут до получателя, выбирать конкретные узлы для уменьшения нагрузки на сеть.

Необходимо решить основные проблемы безопасности меш-сетей.

1. *Доступность*, в частности:

а) *помехи*. Злоумышленник может атаковать доступность сети, создавая помехи и препятствуя коммуникации на физическом уровне. Эта проблема может возникать также вследствие естественных физических причин;

б) *отказ в обслуживании (DoS)*, обычно это лавинная передача запросов по сети, из-за которых сеть становится неспособной исполнять запросы обычных пользователей;

в) *истощение батареи*. В сетях, основанных на мобильных устройствах, атаки истощения батареи могут быть даже опаснее, чем DoS, так как они способны не только временно вывести из строя сеть, но и полностью вывести из строя устройства, на которых она основывается.

2. *Аутентификация*. Злоумышленник может замаскировать узел, получая неавторизованный доступ к ресурсам, чувствительной информации, а также возможность влиять на деятельность других узлов. Обычные способы аутентификации задействуют централизованную систему, которая администрирует ограничения согласно спискам доступа или сертификатам. В меш-сети наличие таких центров по большей части невозможно.

3. *Целостность*. Атаки на целостность сообщений обычно имеют своей причиной либо умышленное изменение данных злоумышленником, либо случайные ошибки в передаче, связанные с работой сети и отдельных устройств.

4. *Конфиденциальность* является ключевой проблемой в меш-сети, так как необходимо защитить коммуникацию с аутентифицированным пользователем в условиях, когда нет ни доверенных центров, ни единой структуры сети.

Bluetooth и Bluetooth Low Energy

Основная технология, на которой основана меш-сеть, — это семейство протоколов Bluetooth. **Bluetooth** представляет собой технологический стандарт беспроводного обмена данными на коротком расстоянии через радиосвязь. На сегодняшний день существует пять основных версий стандарта, последняя — Bluetooth 5.2.

Сосредоточимся на тех характеристиках Bluetooth, которые помогут нам решить некоторые из вышеописанных проблем меш-сетей.

В Bluetooth используется технология FHSS — псевдослучайная перестройка рабочей частоты. При передаче сигнала участники коммуникации 1600 раз в секунду меняют рабочую частоту внутри заданного диапазона. Для этого они используют секретную матрицу времени-частоты, доступную только двум участникам контакта. Благодаря FHSS сигнал, во-первых, устойчив к узкополосной интерференции, то есть, по сути, к *помехам*, а во-вторых, его становится сложнее перехватить, так как последовательность переключения частот неизвестна сторонним пользователям.

При передаче Bluetooth разделяет данные на пакеты, а затем передает каждый пакет по одному из доступных каналов. При передаче текстовой информации Bluetooth отвечает за целостность передаваемых и получаемых данных. Тем самым решена проблема *целостности* данных.

Для обеспечения *аутентификации* участников диалога в Bluetooth используется механизм сопряжения: перед началом обмена информацией устройства должны добавить друг друга в список связанных. В смартфонах это происходит с незначительным участием пользователя: он должен подтвердить соединение. Установив сопряжение, пользователи смогут иметь защищенный канал связи, однако он действует, только пока они находятся в непосредственной близости.

Bluetooth Low Energy (BLE) — спецификация ядра Bluetooth, которая значительно уменьшает энергопотребление при обмене данными ценой небольшого снижения скорости передачи данных. BLE программно несовместим с классическим Bluetooth, однако поддерживается в подавляющем большинстве современных смартфонов. Несмотря на то что передавать долгие сообщения по BLE бессмысленно, мы можем использовать BLE для передачи коротких и/или редких сообщений, например сообщений маршрутизации. Использование BLE помогает решить проблему *истощения батареи*.

Криптография на эллиптических кривых

В работе будут рассматриваться только несингулярные эллиптические кривые, так как в противном случае проблема дискретного логарифма, на которой основана криптографическая стойкость, будет легко решена.

Эллиптическая кривая E над полем K обозначается как E/K и определяется уравнением Вейерштрасса:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

где коэффициенты $a_1, a_2, a_3, a_4, a_6 \in K$ таковы, что для каждой точки (x_1, y_1) с координатами в $\overline{K}$, удовлетворяющими уравнению кривой, частные производные $2y_1 + a_1x_1 + a_3$ и $3x_1^2 + 2a_2x_1 + a_4 - a_1y_1$ не равны нулю одновременно. Это условие равнозначно тому, что кривая будет несингулярной или гладкой.

Из всех точек кривой можно составить группу с операцией, которую обычно обозначают как «+». Многократное применение этой операции к одной и той же точке кривой P обозначают как $[n]P$ и называют умножением на скаляр:

$$[n]: E \to E,$$

$$P \mapsto [n]P = \underbrace{P + P + \ldots + P}_{n \text{ раз}}.$$

Отметим, что $[0]P = P_\infty$ и $[n]P = [-n](-P)$, $n < 0$. Подробные формулы и разъяснения приведены во многих учебниках и статьях, например в [1].

Выберем в качестве поля K конечное поле $\mathbb{F}_p$, где p — простое число $(p > 3)$. Точки кривой (вместе с «точкой на бесконечности») образуют конечную циклическую группу. Если сложить две точки кривой или умножить одну из точек на скаляр, результирующая точка будет находиться в той же циклической группе.

Введем понятие **проблемы нахождения дискретного логарифма на эллиптических кривых** (ECDLP): имея эллиптическую кривую, определенную над конечным полем $\mathbb{F}_p$, образующую точку G и выбранную произвольным образом точку P кривой, необходимо найти целое число k такое, что $P = [k]G$. Несмотря на то что в некоторых случаях эту проблему можно решить довольно быстро, в общем случае самый быстрый алгоритм требует $\sqrt{k}$ шагов для ключа размером в k бит.

На основе этой проблемы можно построить аналог **обмена ключами Диффи — Хеллмана** на эллиптических кривых: вместо возведения

в степень по модулю здесь используется умножение точек эллиптической кривой на элементы конечного поля. Алгоритм основывается на следующем свойстве в группе точек эллиптической кривой:

$$[b]([a]G) = [a]([b]G).$$

Назовем стороны обмена Алисой и Бобом. В общем алгоритм выглядит так:

1. Алиса генерирует случайную пару: закрытый ключ d_A — случайно выбранное число из интервала $[1 \ldots n-1]$ и открытый ключ $Q_A = [d_A]G$.

2. Боб аналогично вычисляет пару d_B, Q_B.

3. Алиса и Боб обмениваются своими открытыми ключами Q_A, Q_B по публичному каналу.

4. Алиса вычисляет общий секрет $s = [d_A]Q_B$.

5. Боб вычисляет общий секрет $s = [d_B]Q_A$.

6. Теперь у обеих сторон есть одинаковый общий секрет s.

Кривая Curve25519

На практике при реализации криптографии на эллиптических кривых обычно выбирают конкретную кривую из числа рекомендованных стандартизирующими организациями. Для дальнейшей реализации выберем кривую Curve25519.

Эллиптическая кривая в форме Монтгомери

$$y^2 = x^3 + 486662x^2 + x,$$

определенная над полем $\mathbb{F}_{p^2}$, где $p = 2^{255} - 19$ — простое число, имеет название **Curve25519**.

В качестве первой координаты базовой точки используется $x = 9$. Эта точка генерирует циклическую подгруппу простого порядка, что предотвращает использование атаки с помощью алгоритма Полига — Хеллмана [2]. Данная кривая обеспечивает 128-битный уровень криптостойкости.

Благодаря форме Монтгомери можно эффективно применять групповые операции, используя только координаты X, Z. В качестве ключа в итоге используется только x-координата. В числе преимуществ при использовании этой кривой можно также отметить:

- постоянное время работы, что обеспечивает защиту от атак по времени;
- возможность использовать короткие открытые и закрытые ключи в 32 байта;
- нет необходимости валидировать публичный ключ — подойдет любая 32-байтная строка.

Благодаря своим преимуществам данная кривая была стандартизирована сообществом IETF и используется во многих популярных протоколах и приложениях: TLS 1.3, WhatsApp, Viber, Proton Mail, Tor, I2P.

Гибридная схема шифрования

Обычно данные не зашифровывают напрямую с помощью эллиптических кривых из-за проблем со скоростью. Вместо этого используют **гибридные схемы шифрования**, включающие обмен ключами на эллиптических кривых (ECIES).

Для реализации подобной схемы необходимо иметь:

- *функцию выработки ключа* (KA), которая генерирует общий секрет;
- *функцию формирования ключа* (KDF) — механизм, производящий набор ключей для симметричного шифрования на основании уже существующих асимметричных ключей;
- *симметричный алгоритм шифрования* (Enc);
- *имитовставку* (MAC) — данные аутентификации сообщения;
- *хеш-функцию* (Hash), которая используется в KDF и MAC.

Допустим, Алиса хочет отослать Бобу сообщение m.

1. Предварительно Алиса и Боб генерируют закрытые и открытые ключи. Обозначим через U, V их открытые ключи (точки кривой), u, v — закрытые (элементы поля).

2. Алиса использует KA: вычисляя $s = [u]V$, она получает общий секрет.

3. Алиса использует KDF, получая симметричный ключ и ключ имитовставки: $k_E \,||\, k_M := KDF(s, i)$, где i — необязательный параметр дополнительной информации.

4. Алиса шифрует сообщение m симметричным шифром Enc: $c = Enc(k_E, m)$.

5. Алиса вычисляет имитовставку $tag = MAC(k_M, c, i')$, где i' — необязательная дополнительная информация.

6. Наконец, Алиса отсылает криптограмму, состоящую из публичного ключа U, имитовставки tag и шифротекста c.

Чтобы получить исходное сообщение m из набора (U, tag, c), Боб должен сделать следующее:

1. Используя эфемерный открытый ключ U и собственный закрытый ключ v, получить общий секрет $s = [v]U$.

2. С помощью KDF получить ключи $k_E \,||\, k_M := KDF(s, i)$, i — необязательный параметр дополнительной информации.

3. Проверить правильность полученной криптограммы, вычислив имитовставку аналогичным образом: $tag' = MAC(k_M, c, i')$. Если $tag \neq tag'$, необходимо отклонить криптограмму как ошибочную.

4. Если имитовставки сошлись, можно расшифровать полученный шифротекст: $m = Enc^{-1}(k_E, c)$.

Единого набора конкретных алгоритмов, которые реализуют необходимые для данной схемы функции, не существует, однако, опираясь на стандарты ANSI X9.63, IEEE 1363a, ISO/IEC 18033-2 и SECG SEC 1, выберем следующие алгоритмы:

- KA: обмен ключами по Диффи — Хеллману, описанный выше на кривой;
- KDF: алгоритм KDF2, описанный в [3];
- симметричный шифр: AES в режиме сцепления блоков шифротекста (CBC-mode);
- MAC: HMAC-SHA-512;
- хеш-функция: SHA-512.

В связи с тем что обычно в среде разработки (в частности, для ОС Android) уже реализованы алгоритмы AES, SHA-512, KDF2 и HMAC, не будем останавливаться на их описании подробно. При необходимости их реализации можно обратиться к [3].

Защищенная передача сообщений по меш-сети

Итак, мы хотим получить меш-сеть, основанную на Bluetooth и BLE, с возможностью отправки защищенных сообщений участникам сети. У пользователей на устройстве установлено созданное нами ПО. В этом программном обеспечении реализованы криптографические примитивы, объединенные в гибридную схему шифрования на эллиптической кривой Curve25519, а также алгоритмы отправки данных по Bluetooth и BLE. Опишем теперь, как построить желаемую сеть.

Первый этап, который необходимо проделать, — **обмен ключами** между будущими сторонами коммуникации. Чтобы быть уверенными в том, что другой участник сети — тот, за кого себя выдает, для обмена потребуется находиться в зоне действия Bluetooth. Тогда мы можем открыть защищенный канал связи по Bluetooth вне основной сети. По этому каналу стороны должны установить общий секрет, а также, используя гибридную схему, описанную выше, произвести обмен пробными сообщениями, например подобный рукопожатию протокола TCP.

Если обе стороны успешно обменялись сообщениями, необходимо **сохранить** их **пары ключей** для дальнейшей коммуникации: теперь можно использовать общую сеть для обмена зашифрованными сообщениями через гибридную схему. При отправке в общую сеть в «заголовке» сообщения мы должны передавать открытые MAC-адрес адресата и имя отправителя, а в «теле» — шифртекст.

Работа сети будет поддерживаться следующим образом: каждый участник пересылает в незащищенном режиме сообщения своему окружению. Если один из участников обнаруживает рядом с собой адресата текущего сообщения, оно передается адресату с пометкой, что

предназначено именно ему. Получатель, зная отправителя, расшифровывает шифртекст по общему с отправителем ключу.

Для маршрутизации можно использовать оповещения через BLE, а для большей экономии батареи применять гибкий подход, например как описано в [4]. Для отражения атак отказа в обслуживании можно вести «черный список» узлов: если какое-то из устройств попытается отправлять значительно больше запросов, чем соседние точки, его можно временно игнорировать, с каждым разом увеличивая время ожидания.

Более гибкие подходы к маршрутизации включают в себя применение специальных алгоритмов для мобильных меш-сетей, например AODV, OLSR или DSR. Это позволит значительно уменьшить нагрузку на сеть в целом и на конкретные устройства-узлы в частности.

Общие результаты

Описанные выше технологии, криптопримитивы и общий алгоритм защищенной передачи закрывают большую часть проблем безопасности беспроводных меш-сетей. Полученного алгоритма достаточно для дальнейшей программной реализации защищенного обмена сообщениями на основе операционных систем Android и iOS.

Несмотря на то что каждая из частей алгоритма заслуживает детальной проработки и оптимизации, с помощью представленного подхода мы получим сеть, достаточную для реального применения.

Список литературы

1. *Avanzi R.M., Cohen H., Doche Ch. et al.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, 2006.

2. *Bernstein D.J.* Curve25519: new Diffie-Hellman speed records // Public Key Cryptography — PKC 2006. Springer, 2006. URL: https://cr.yp.to/ecdh/curve25519-20060209.pdf (дата обращения: 11.10.2020).

3. *ISO/IEC* 18033-2:2006. Information technology — Security techniques — Encryption algorithms. Part 2 : Asymmetric ciphers. 2006. URL: https://www.iso.org/ru/standard/37971.html (дата обращения: 11.10.2020).

4. *Brandão A.S., Lima M.C., Abbas C.J.B. et al*. An Energy Balanced Flooding Algorithm for a BLE Mesh Network // IEEE Access. 2020. Vol. 8. URL: https://ieeexplore.ieee.org/document/9091162/ (дата обращения: 31.10.2020).

Об авторе

Филипп Геннадиевич Максимов-Наливайко — студент, Балтийский федеральный университет им. И. Канта, Россия.

E-mail: phmaksimov@gmail.com

The author

Filipp G. Maksimov-Nalivaiko, Student, Immanuel Kant Baltic Federal University, Russia.

E-mail: phmaksimov@gmail.com