

О КАЧЕСТВЕ РОУМИНГА МОБИЛЬНЫХ УСТРОЙСТВ В КОРПОРАТИВНЫХ БЕСПРОВОДНЫХ СЕТЯХ

В статье представлено практическое исследование процесса передачи управления между точками доступа на канальном уровне с детализацией добавления задержки в различных компонентах. Исследование показало, что различные процедуры на уровне доступа вносят основной вклад в общую задержку передачи управления, что отрицательно влияет на качество обслуживания (QoS) многих приложений, таких как IP-телефония. Также показано существенное изменение величины задержки при передаче управления от одной точки доступа к другой, особенно при условии разных производителей оборудования точек доступа.

Ключевые слова: IEEE 802.11, беспроводной роуминг, сканирование, ассоциация, аутентификация, задержка.

Последние несколько лет наблюдается существенный рост беспроводных локальных сетей (WLAN) на основе протоколов семейства IEEE 802.11 [1]. WLAN обеспечивает не только удобное подключение к сети, но и высокую скорость соединения до 300 Мбит/с (802.11n). Далее будем рассматривать только сети IEEE 802.11n в диапазоне 2,4 ГГц.

Спецификация уровня доступа сети (MAC) IEEE 802.11 имеет 2 режима работы – специальный режим и режим инфраструктуры. В специальном режиме две и более беспроводные станции (STA) распознают друг друга и устанавливают соединение без использования другого оборудования, в то время как в режиме инфраструктуры имеется сущность, называемая точкой доступа, которая централизованно управляет передачей данных между ассоциированными с ней клиентами. Точка доступа и ассоциированные с ней клиенты образуют так называемый BSS (basic service set, зону с базовым набором услуг), работающий в нелицензируемом радиочастотном диапазоне.

Несколько точек доступа, подключаемых через распределенные системы (DS, distribution system) расширяет BSS в ESS (enhanced service set, расширенный набор услуг) (рисунок 1).

Передача управления от одной точки доступа к другой происходит, когда мобильная станция перемещается за пределы диапазона одной точки доступа и входит в другой BSS (на уровне доступа). Во время передачи управления происходит обмен управляющими кадрами между станциями (STA) и точкой досту-

па. Кроме того, точки доступа могут обмениваться определенной контекстно-зависимой информацией (набор правил и параметров), специфичной для станции. Следовательно, существует задержка, связанная с процессом передачи управления, при котором клиент не может отправлять или получать трафик.

Мобильность беспроводных сетей обеспечивает возможность существования многих перспективных мультимедиа и пиринговых приложений (таких как VoIP, 802.11 телефония, мобильные видеоконференция и чат). К сожалению, качество сетевого подключения может пострадать от непостоянства задержки при передаче обслуживания на другую точку доступа. Проведенные измерения [4] показали, что кроме довольно больших величин самих задержек, они существенно различаются для разных конфигураций станций и точек доступа.

Несмотря на растущую популярность беспроводных локальных сетей, пока нет математического аппарата измерения процесса пере-

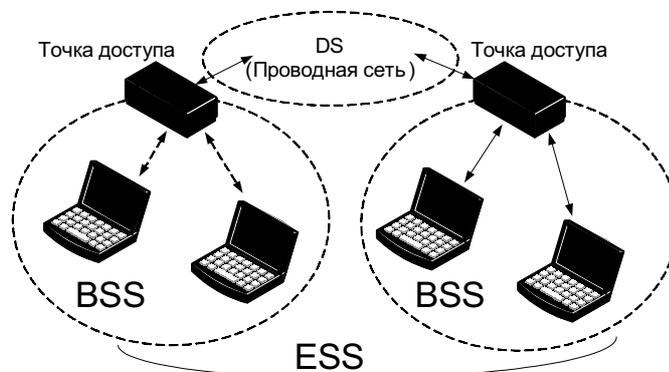


Рисунок 1. Схема работы ESS

дачи управления. Существуют работы по измерению в беспроводных сетях АТМ и сотовых беспроводных сетях.

В работе [2] представлены экспериментальные характеристики поведения пользователей и производительности сети в публичных беспроводных локальных сетях, где показано различное количество передач управления с течением времени. В работе [3] также представлена разработка новой схемы передачи управления с акцентом на снижение задержки передачи управления в беспроводных сетях, но ни один из представленных методов не позволяет оценить текущие задержки передачи управления.

В данном исследовании проведены эксперименты для точного измерения задержки передачи управления в беспроводной сети здания. Измерения проводились для двух беспроводных сетей (с использованием точек доступа Linksys и TP-Link) и трех беспроводных адаптеров разных производителей (Intel, D-Link, Atheros). Задержка передачи управления анализируется путем разбиения всего процесса на различные этапы для того, чтобы оценить влияние каждого этапа на задержку. Полученные результаты показывают, что этап сканирования сети вносит значительный вклад в задержку передачи управления, следовательно, акцент нужно делать на изучении времени сканирования T_{probe} .

Постановка задачи

Процесс передачи управления зависит от последовательности сообщений, которыми обмениваются точки доступа и станции на физическом уровне, от информации о состоянии станций. Таким образом, передача управления – это функция физического уровня, осуществляемая по меньшей мере при наличии трех компонентов: станции, предыдущей точки доступа, следующей точки доступа. Точка доступа (ТД), к которой станция была подключена на физическом уровне до передачи управления, является предыдущей ТД, в то время как ТД, к которой станция подключается после передачи управления, является следующей ТД. Передаваемая информация о состоянии обычно состоит из учетных данных клиента (которые позволяют ему получить доступ к сети). Эта передача может быть обеспечена протоколом IAPP, Atheros LWAPP или через другой протокол. Для сетей IEEE 802.11, которые не имеют механизма уп-

равления доступом, разница между полноценным новым подключением и передачей управления незначительна. С другой стороны, задержка передачи управления будет больше, чем задержка ассоциации, т. к. к ней добавляется задержка при соединении точек доступа.

Весь процесс передачи управления можно разделить на два логических шага – открытие и повторная аутентификация (Reauthentication).

1. Сканирование радиодиапазона. Из-за мобильности мощность сигнала и отношение сигнал – шум от текущей точки доступа станции может ухудшиться, и клиент может потерять связь и инициировать связь с другой точкой доступа (передать управление). В произвольный момент времени клиент может не иметь возможности обмениваться данными с текущей точкой доступа, т. е. клиенту нужно найти потенциальные точки доступа (в заданном диапазоне), с которыми он сможет быть ассоциирован. Это достигается за счет функции уровня доступа – сканирования. Во время сканирования сетевая карта принимает специальные сообщения от точек доступа (периодически рассылается точками доступа с интервалом 10 мс) по каждому из частотных каналов. Таким образом, станция может создать список точек доступа с приоритетом по принимаемому сигналу.

Существует два режима сканирования, определенных в стандарте: активный и пассивный. Как видно из названия, в активном режиме, кроме прослушивания сообщений (который является пассивным), станция посылает дополнительно ширококвещательные сканирующие пакеты на каждый канал и получает ответы на точки доступа. Таким образом, станция активно зондирует точки доступа.

2. Повторная аутентификация: станция пытается повторно аутентифицироваться для доступа в соответствии со списком приоритетов. Процесс повторной аутентификации обычно включает в себя аутентификацию и повторную ассоциацию со «следующей» ТД. Этап повторной аутентификации предполагает передачу полномочий и другой учетной информации от «предыдущей» ТД. Это может быть достигнуто использованием различных протоколов. В экспериментах, описанных в статье, используются собственные протоколы связи между точками доступа (где все ТД одного производителя).

Таким образом, этап аутентификации в представленных экспериментах опускается.

На рисунке 2 показана последовательность сообщений, которая обычно наблюдается в процессе передачи управления другой точке доступа. Процесс передачи управления начинается с первого сканирующего сообщения и заканчивается сообщением-ответом повторной ассоциации от ТД. Все задержки передачи управления делятся на три вида:

1. Задержка сканирования. Сообщения А, В, С, D, Е являются сканирующими сообщениями при активном сканировании. Фактически количество сообщений во время процесса сканирования может варьироваться от 3 до 11.

2. Задержка аутентификации. Это задержка, возникающая при обмене кадров аутентификации (сообщения Е и F). Аутентификация состоит из двух или четырех последовательных кадров в зависимости от метода аутентификации, используемого точкой доступа. Некоторые беспроводные сетевые адаптеры пытаются инициировать повторную ассоциацию до аутентификации, что приводит к дополнительным задержкам в процессе передачи управления, а также к нарушениям протокола IEEE 802.11.

3. Задержка повторной ассоциации. Это задержка, возникающая при передаче кадров ассоциации (сообщения G и H). После успешного процесса аутентификации станция передает точке доступа кадр запроса повторной ассоциации, принимает кадр ответа и тем самым успешно завершает передачу управления.

Исходя из вышесказанного, задержка сканирования возникает на этапе сканирования доступных сетей, в то время как задержки аутентификации и ассоциации возникают на этапе повторной аутентификации. Наряду с задер-

жками, описанными выше, возможно появление задержки для обновления mac-адреса (при использовании протокола STP IEEE 802.1d) Ethernet-коммутатором, который является системой распределения (DS). Результаты представленных экспериментов не будут отражать эту задержку.

Материалы и методы экспериментального исследования

Экспериментальный стенд состоит из двух беспроводных сетей, мобильного беспроводного клиента и мобильной сниффер-системы. Как показано на рисунке 3, основной методологией эксперимента является использование сниффера (физически в пределах радиочастотного спектра клиентов в любое время), чтобы захватить все связанные с клиентом пакеты для анализа.

В здании находятся две беспроводные сети с названиями SAU и CiscoAcad. Эксперименты проводились в перекрывающихся зонах покрытия обеих сетей. Сеть SAU состоит в основном из ТД TP-Link, а сеть CiscoAcad – из ТД Linksys. Плотность сети SAU составляет 6 точек на одном этаже здания, а CiscoAcad – 8

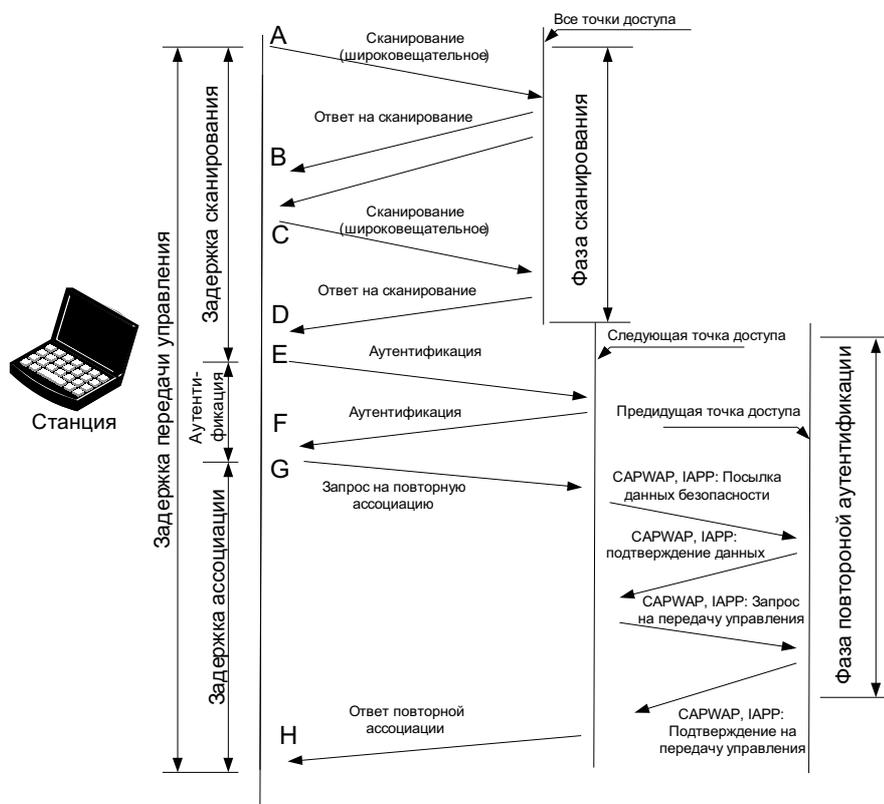


Рисунок 2. Процесс передачи управления

точек на другом этаже. Распределение каналов по сети осуществляется таким образом, что нет никаких помех между соседними точками доступа, так что нет соседних ТД, которые использовали бы один и тот же канал. В данном эксперименте для беспроводной связи используются каналы 1, 6 и 11.

Для мобильной станции используется FreeBSD 9.1 на ноутбуке Acer One 751 с Intel Atom 1,3 ГГц и 1 Гб оперативной памяти. В мобильной станции в ходе эксперимента были использованы следующие беспроводные карты: D-Link DWA-125, Atheros HB63, Intel 4965agn.

Эксперименты проводились следующим образом. Человек с мобильной станцией передвигается по зданию по фиксированному пути (чтобы минимизировать эффекты от расположения точек доступа) во время каждого эксперимента. Продолжительность одного эксперимента составляет примерно 30 минут. Каждый эксперимент характеризуется 1) используемым в мобильной станции беспроводным сетевым адаптером и 2) используемой беспроводной сетью. Мобильный клиент периодически посылает небольшие ICMP-сообщения в сеть для отслеживания соединений. Так как станция движется, происходит передача управления, поскольку она покидает одну BSS и входит в другую.

Во время передачи управления точки доступа и мобильная станция обмениваются набором управляющих кадров, таких как зонд, кадры аутентификации и ассоциации. При sniff-финге всех управляющих кадров из радиочастотной среды (с временными метками) вычисляется задержка передачи управления как интервал между первым кадром запроса зонда и кадром ответа ассоциации (рисунок 2). Кроме

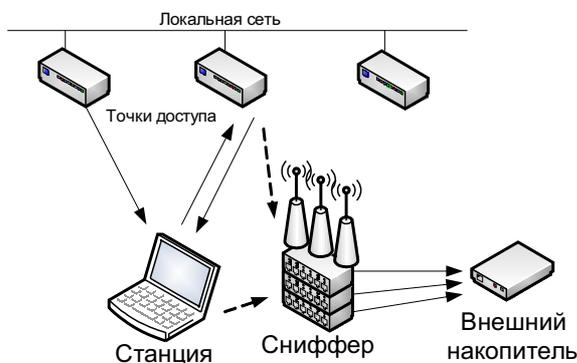


Рисунок 3. Схема эксперимента

того, измеряется время, потраченное на каждую фазу, как показано в [5]. Этот анализ выполняется в автономном режиме после сбора трафика. Для того чтобы перехватить каждый кадр управления в радиочастотной среде применен отдельный аппаратный сниффер на базе точки доступа с прошивкой OpenWRT и пакетом airodump-ng. Сниффер физически прикреплен к мобильной станции.

Так как соседние точки доступа используют разные каналы, сниффер-система должна быть способна захватить отдельные кадры со всех трех используемых каналов, например, 1, 6 и 11 одновременно.

Беспроводные карты Atheros, применяемые в точках доступа, имеют режим монитора, который позволяет приложениям получать все IEEE 802.11 кадры на одном конкретном канале. Таким образом, путем захвата трафика из трех карт (на каналах 1, 6, 11), можно перехватить все пакеты, передаваемые участниками эксперимента.

Чтобы перехватывать данные на нескольких каналах, были созданы три такие сниффер-системы. Чтобы не допустить неточности, вызванной несоответствием системных часов двух машин, они были синхронизированы с использованием Network Time Protocol (NTP) через соединение Ethernet. На протяжении эксперимента часы сохранили точность в пределах 50 мс.

Результаты исследования

На рисунках 4, 5 и 6 показана задержка передачи управления для трех клиентских карт (D-Link, Atheros, Intel) с ТД TP-Link сети SAU. По оси X порядковый номер передачи управления, а по оси Y – задержка передачи управления в каждой из трех фаз.

На рисунке 7 показаны средние значения для всех экспериментов со всеми сетями.

Исходя из результатов эксперимента, можно сделать следующие выводы.

1. Задержка при сканировании является доминирующей: из графиков (рисунки 4–7) очевидно, что эта задержка составляет более 90% от общей задержки передачи управления, независимо от конкретной комбинации станции и ТД. Кроме того, даже при обмене сообщениями между станцией и ТД, этап сканирования занимает более 80% во всех экспериментах. Таким образом, любая схема передачи управления, ис-

пользующая методы, позволяющие кэшировать или отслеживать информацию о ТД, но не выполняющие на самом деле полное сканирование, будет заведомо быстрее.

2. Используемые беспроводные аппаратные средства (ТД, станции) влияют на задержку передачи управления: этот вывод легко сде-

лать, исходя из различий в масштабах оси Y графиков. При одинаковых точках доступа очевидно, что тип беспроводной карты клиента влияет на задержку. Разность средних задержек карты D-Link и Atheros составляет 335 мс. При фиксированной карте клиента ТД также влияет на задержку, но в гораздо меньшей степени (раз-

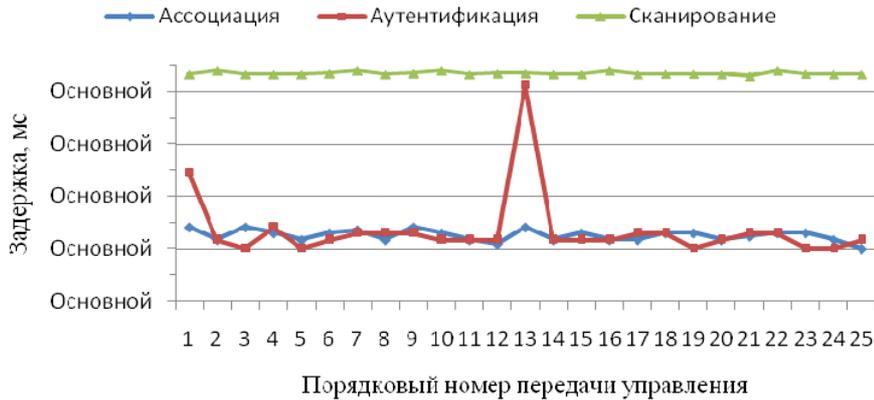


Рисунок 4. Измерения на сетевой карте D-Link

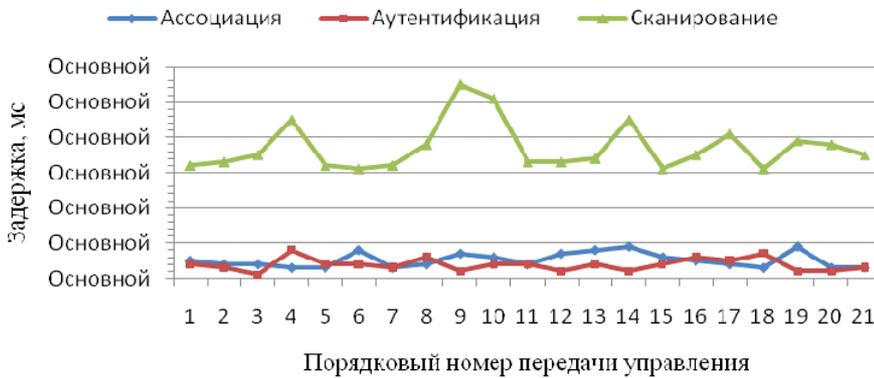


Рисунок 5. Измерения на сетевой карте Atheros

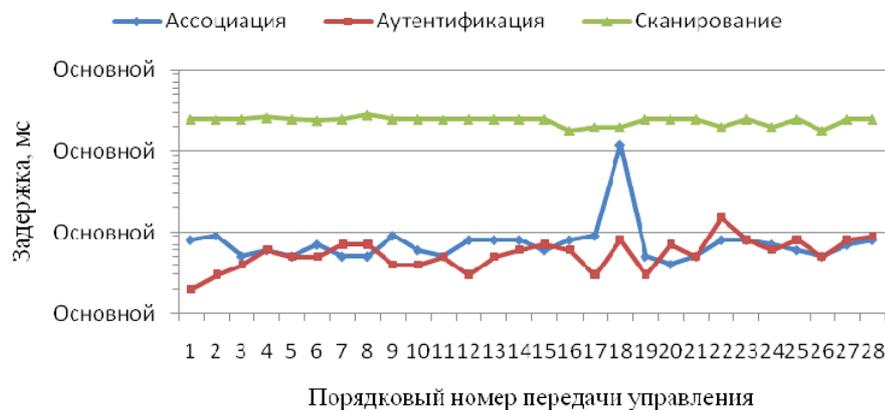


Рисунок 6. Измерения на сетевой карте Intel

ность средних значений примерно на 50% меньше, 159 мс).

3. Существуют большие дисперсии задержки передачи управления. Наряду с изменениями задержки при различных конфигурациях, имеют место существенные различия в задержке передачи управления в рамках одного набора оборудования. Кроме того, для тех же станций точки доступа Atheros имеют более низкую дисперсию, чем ТД Linksys.

4. Различные беспроводные карты имеют различные последовательности сообщений. Это выяснилось при анализе файлов с перехваченными пакетами. Обнаружено, что карты Intel

имеют несколько иную процедуру, чем остальные. Карта посылает сообщение ассоциации до аутентификации. Эта последовательность сообщений для повторной аутентификации нарушает протокол IEEE 802.11, но несколько ускоряет общий процесс.

01.04.2013

Исследования выполнены при поддержке Министерства образования и науки Российской Федерации в рамках проектов № 14.514.11.4048 ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007–2013 годы» и № 14.В37.21.1881 ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы» и РФФИ (проекты №12-07-31089 и №12-07-31022)

Список литературы:

1. IEEE. Часть 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Стандарт IEEE 802.11, 1999.
2. Mishra, M. Shin, W. Arbaugh, An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process. ACM SIGCOMM Computer Communications Review, 2003. – Vol. 33, № 2. – P. 93–102.
3. Давиденко, И. Н. Распределенное управление трафиком в мобильных сетях / И. Н. Давиденко // Актуальные проблемы автоматизации и информационных технологий. – 2008. – Т. 2. – С. 113–124.
4. Тарасов, В. Н. Анализ и оптимизация локальных сетей и сетей связи с помощью программной системы OPNET MODELER / В. Н. Тарасов, А. Л. Коннов, Ю. А. Ушаков // Вестник Оренбургского государственного университета. – 2006. – № 6. – С. 197–204.
5. Тарасов, В. Н. Анализ производительности сети кампуса на основе имитационного моделирования / В. Н. Тарасов, А. Л. Коннов // Вестник Оренбургского государственного университета. – 2011. – № 4. – С. 147–151.

Сведения об авторах:

Тарасов Вениамин Николаевич, профессор кафедры системного анализа и управления
Оренбургского государственного университета, доктор технических наук
460019, г. Оренбург, Шарлыкское шоссе, 5, ауд. 14108, тел. (3532) 372557

Ушакова Маргарита Викторовна, ассистент кафедры администрирования информационных систем
Оренбургского государственного университета
460018, г. Оренбург, пр-т Победы, 13, ауд. 1502, тел. (3532) 372539, e-mail: m.v.ushakova@mail.ru