Глазунов В. В., Курочкин М. А.

*Санкт-Петербургский государственный*

*политехнический университет*

**МЕТОДЫ ЗАЩИТЫ МУЛЬТИПРОТОКОЛЬНЫХ СИСТЕМ МОБИЛЬНОЙ СВЯЗИ С ОБЛАЧНОЙ СРЕДОЙ**

Расширение спектра информационных услуг, предоставляемых владельцам автотранспорта, вызывает увеличение объема двунаправленного потока сообщений в сетях передачи данных и формирует новые требования к обеспечению защиты данных передаваемых по мобильным сетям. В первую очередь безопасность и целостность передаваемых данных необходимо поддерживать в задачах, повышения безопасности движения, мониторинга технического состояния автомобилей и финансовых расчетах.

Пользователями информационных услуг систем мобильной связи являются: аналитический центр автопроизводителей; водители, пассажиры и владельцы автомобиля; участники дорожного движения; региональные службы управления движением; сервисные центры обслуживания автомобилей; службы технической помощи на дорогах; региональные службы специального назначения; экстренные службы, такие как E-call и Эра-Глонасс; элементы «умной» дороги. Их оперативное взаимодействие обеспечивает:

1. Мониторинг технического состояния автомобилей и сокращение числа обращений в сервисные центры.
2. Мониторинг обстановки на трассе движения и экстренную помощь в сложных или аварийных ситуациях.
3. Упрощение финансовых расчетов клиентов компании при эксплуатации автомобиля.
4. Комплексное решение эксплуатационных и транспортных задач.
5. Расширение области информационно-развлекательных услуг.
6. Улучшение экологической обстановки на автотрассах.

Особую актуальность вопросы защиты данных приобретают в зонах с неустойчивой связью, для которых перспективным направлением развития информационной сети рассматривается самоорганизующаяся гетерогенная сеть автомобилей с точками выхода в облачную среду. В такой модели обмен сообщениями между автомобилем и облаком может осуществляться по нескольким альтернативным путям, а совокупность автомобилей на трассе можно рассматривать как подвижную локальную сеть с изменяющейся топологией и составом с переменным числом точек обмена данными с облачной средой. Базовой технологией передачи данных между автомобилями и облачной средой является mesh-сеть.

Основной сложностью обеспечения передачи данных при использовании подвижного mesh 802.11s является динамичное изменение структуры сети, требующее использования дополнительных средств для поддержки маршрутизации сетевого трафика. Изменение доступных маршрутов передачи данных во время передачи сообщения приводит в увеличению времени передачи и, возможно, к потере сообщения. Основными параметрами влияющими на свойства подвижной mesh-сети(802.11s) передачи данных являются скорости движения объектов, территориальное расположение узлов сети, радиус действия передатчиков и время подключения к сети.

Основные проблемы защиты данных при передаче по mesh-сетям определяют:

– дублирование переданных данных,

– неопределенное время жизни данных в сети,

– постоянно изменяющаяся топология сети,

– ограниченная пропускная способность сети,

– ограниченные ресурсы оборудования.

На рисунке 1, показаны каналы передачи данных в локальных и глобальных сетях. Наиболее уязвимыми сетями являются сети, образованные между автомобилями и элементами дорожной инфраструктуры, которые являются транспортом для сообщений, передаваемых в глобальную облачную среду.

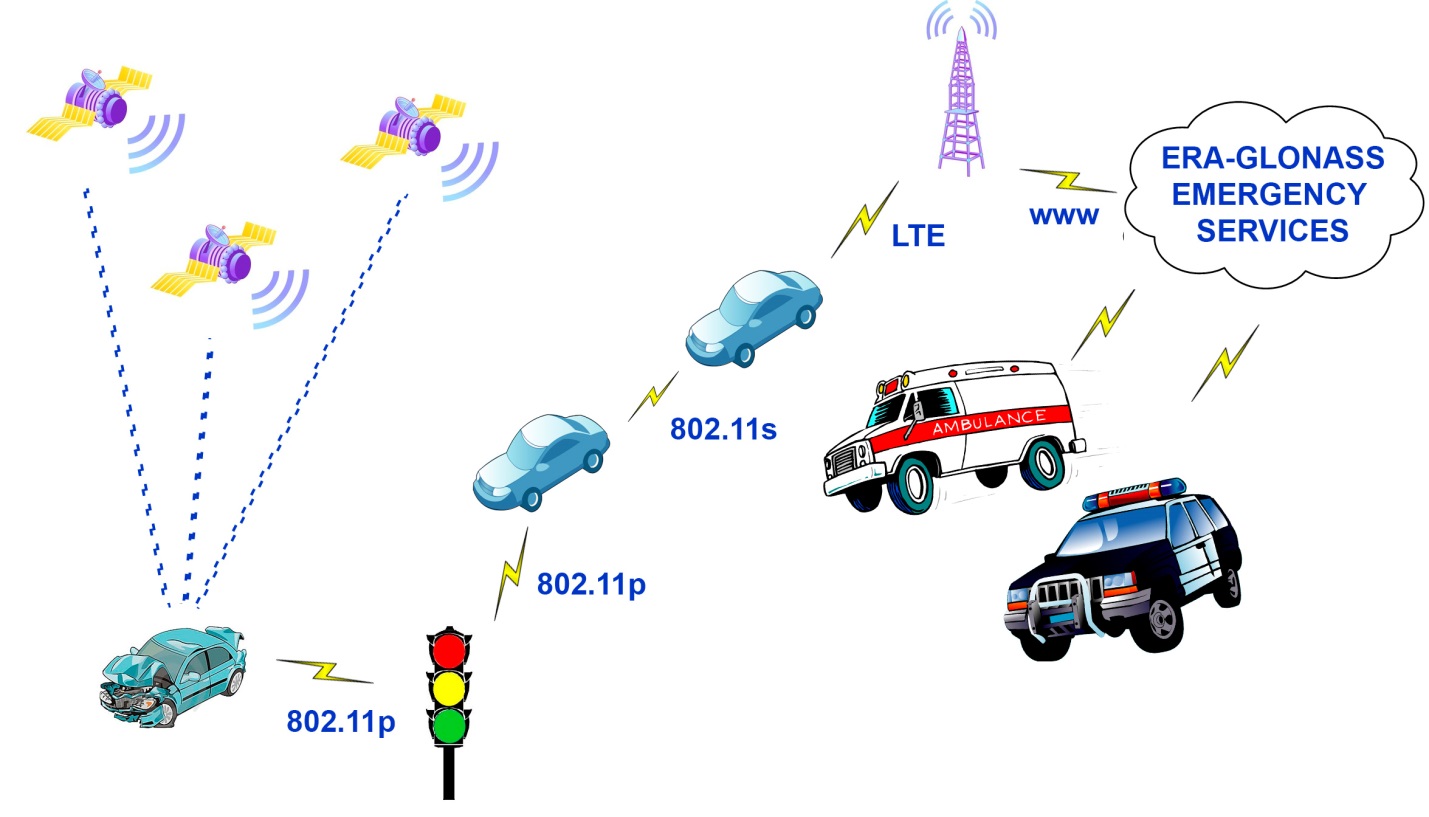


Рисунок 1. Траектории передачи сообщений в мультипротокольной мобильной сети.

Основными показателями качества передачи данных для мобильных систем являютсявероятность доставки сообщения конкретному адресату и время доставки сообщения.

Разделим потоки сообщений на три класса. Введем следующую классификацию: V>1Mb – большой, 5K<V<1Mb – средний, V<5Kb –малый, где V – объем сообщения.

Малые объемы данных характерны для:

– сообщений о погодных условиях и состоянии дорожного покрытия;

– сообщений об оперативных изменениях транспортной сети;

– сообщений об аварийных ситуациях;

– транзакций о финансовых расчетах;

– сообщений “SOS” ближайшим участникам дорожного движения;

– сообщений от систем охранной сигнализации;

– сообщений об отказах и сбоях автомобильного оборудования;

– сообщений сервисных служб.

Средние объемы данных характерны для:

– Уточнения данных о дорожной обстановке в центре управления транспортными средствами. (Голосовые консультации);

– аудио консультаций водителя о техническом состоянии автомобиля. (Голосовые консультации)

–дистанционного управления агрегатами автомобиля. (Дистанционное управление);

–централизованного сбора и хранения данных об особенностях конкретного автомобиля. (Мониторинг автомобиля);

–Мониторинга и отображения данных о местоположении автомобилей других участников движения.

Большие объемы данных характерны для:

–Автоматического сохранения треков движения транспортного средства с видеофиксацией ключевых точек движения по времени или по событию;

–дистанционной загрузки новых версий программного обеспечения бортового компьютера;

–поддержки телекоммуникационной среды для пассажиров автомобилей;

–проведения видео консультаций водителя автомобиля.

Данная классификация показывает, что для наиболее приоритетных сообщений, определяющих безопасность движения, характерны малые объемы. Кроме этого одна часть данных этой категории предназначена для региональных служб, а другая для удаленных пользователей.

Некоторые из выделенные классов передаваемых сообщений, требуют конфиденциальности данных и защиты от перехвата злоумышленниками. Другие, такие как дистанционная загрузка новых версий программного обеспечения, требует целостности и достоверности данных, принятых от производителя.

В настоящее время известны типы атак на сообщения, передаваемые по mesh-сети. К ним относятся: Man in the Middle, DoS (отказ в обслуживании), пассивное прослушивание, вторжение в сеть.

От атак связанных с проникновением в локальную сеть и подменой передаваемых пакетов можно защититься, используя безопасные протоколы маршрутизации. Атаки, основанные на перехвате самих передаваемых пакетов можно отбить путем шифрования передаваемого траффика.

На данный момент одним из классических решений является использование защищенных соединений SSL/TLS, работающих на сессионном уровне сетевой модели OSI. Это означает, что для работы этого протокола необходима его непосредственная поддержка самим приложением, и модификации приложений, входящих в облачную инфраструктуру.

Другим решением проблемы является использованием протоколов семейства IPSec, работающих на сетевом уровне модели OSI. Их применение позволяет непосредственно организовать шифрование и проверку целостности данных между абонентами, без предварительной модификации самого приложения.

Рассматривая протоколы IPSec в рамках данной задачи, наибольший интерес предсталяют протоколы AH (Authentication Header) и ESP (Encapsulating Security Payload). Протокол AH используется для аутентификации отправителя информации и обеспечения целостности данных – с целью убедиться, что данные не были изменены в процессе связи. Протокол AH не шифрует данные и не обеспечивает конфиденциальности. В отличие от AH, ESP обеспечивает конфиденциальность информации, так как непосредственно шифрует данные совместно с проверкой подлинности и целостности.

Протокол IPSec функционирует в двух режимах: транспортном и туннельном, которые представляют собой два разных подхода к обеспечению безопасности. В транспортном режиме шифруются только полезные данные, то есть непосредственно информация, подлежащая передаче в процессе сеанса связи. В туннельном режиме шифрованию подлежат заголовок и маршрутная информация, однако в этом режиме довольно сложно организовать маршрутизацию и преобразование адресов между различными сетями.

Эту проблему детально анализируют A. Adas и T. A. Shawly [1], на основании чего можно сделать выводы, что накладные расходы на проверку целостности данных посредством протокола AH, входящего в IPSec, незначительны.

Авторы проводили исследование достоверности передачи данных между абонентами mesh-сети и облачной средой, основываясь на данных описанных в статье накладные расходы на аутентификацию заголовков составят дополнительно 20 байт, при размере экстренного сообщения в 1024 байта. Полученные результаты показывают, что накладные расходы не превышают 2% пропускной способности канала. При использовании протокола ESP и шифрования накладные расходы – на сообщения в 1024 байта дополнительно будут около 3%, но время на обработку такого пакета будет потрачено значительно больше. Допускается использование одновременного применения протоколов AH и ESP в рамках одного пакета, что позволит обеспечить конфиденциальность и целостность данных.

Другим аспектом обеспечения безопасности является обеспечение безопасности передаваемых маршрутов [2]. Для маршрутизации в mesh-сетях используются протоколы AODV, DSDV, OLSR, HWMP к этим протоколам могут быть применены как пассивные, так и активные атаки, позволяющие перехватить или подменить данные, передаваемые в сети. Чтобы решить эту проблему предлагается использовать защищенные протоколы маршрутизации: SRP, ARIADNE, ARAN, среди которых есть как протоколы, работающие в реактивном, так и в проактивном режимах маршрутизации. Однако эти протоколы не учитывают особенности стандартов для избыточных самоорганизующихся mesh-сетей 802.11s/p. Кроме этого они не учитывают различные каналы передачи данных доступные в мультипротокольном узле.

В качестве среды моделирования протоколов передачи данных используется среда имитационного моделирования – ns-3, в которой разработаны модели как проводных, так и беспроводных сетей, позволяющие проводить моделирование смешанных сетей с топологиями различной сложности. Особый интерес в рамках проведенного исследования представляет реализация mesh-сетей на основе стека протоколов 802.11s. В настоящее время рассматриваются варианты мультипротокольных узлов в сетях 802.11s [3] [4] и LTE с протоколами маршрутизации AODV, DSDV, OLSR, HWMP. Включение в этот набор протоколов семейства IPSec позволит учесть вычислительные затраты на шифрование и дешифрование сообщений, которые выполняют мобильные устройства и облачные сервисы.

Список литературы.

[1] Simulation of IPSec Protocol in Ad-Hoc Networks. A. A. Adas and T. A. Shawly Department of Electrical and Computer Engineering, Faculty of Engineering.

[2] Ad hoc networks security. Pietro Michiardi and Refik Molva.

[3]HIGHWAY MOBILITY AND VEHICULAR AD-HOC NETWORKS IN NS-3. Hadi Arbabi Michele C. Weigle http://arxiv.org/pdf/1004.4554v2.pdf

[4]IEEE 802.11s Mesh Networking NS-3 Model. Kirill Andreev, Pavel Boyko <http://www.nsnam.org/workshops/wns3-2010/dot11s.pdf>