

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное
образовательное учреждение высшего образования
«Южно-Уральский государственный университет» (НИУ)
Высшая школа электроники и компьютерных наук
Кафедра «Инфокоммуникационные технологии»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой ИКТ,
д.т.н. _____ С.Н. Даровских
« ____ » _____ 2020 г.

Сети VANET: обзор принципов организации и функционирования

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ–Д.11.03.02.2020.087.00 ПЗ ВКР

Руководитель работы
Новиков В.В. _____
« ____ » _____ 2020 г.

Автор работы,
студент группы КЭ-411
Абанин П.О. _____
« ____ » _____ 2020 г.

Нормоконтролер,
Спицына В.Д. _____
« ____ » _____ 2020 г.

Челябинск 2020

РЕФЕРАТ

Выпускная квалификационная работа 44 с.,
4 ч., 18 рис., 5 табл., 10 источников.

Сети VANET: обзор принципов организации и функционирования.

Цель работы – сделать обзор на сети VANET.

В данной выпускной квалификационной работе был произведен обзор сетей VANET, используемых стандартов для их построения, обзор архитектуры, видов организации, взаимодействия, а также развитие перспектив применения сетей VANET в России и мире в будущем.

Работа состоит из четырех разделов.

1. Сети VANET: общие сведения, архитектура, организация.
2. VANET: стандарты.
3. Обзор проектов VANET.
4. Применение.

					ЮУрГУ-Д.11.03.02.2020.087.00 ПЗ		
Изм.	Лист	№ докум.	Подпись	Дата			
Разраб.		Абанин П.О.			Сети VANET: обзор принципов организации и функционирования		
Проверил		Новиков В.В.					
					Д	3	47
Н. Контр.		Спицына В.Д.			ЮУрГУ Кафедра ИКТ		
Утв.		Даровских С.Н.					

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	6
1 Сети VANET: общие сведения, архитектура, организация	7
1.1 Общие сведения	7
1.2 Роль VANET в структуре ИТС	8
1.3 Архитектура.....	9
1.4 Состав VANET	10
1.5 Виды взаимодействия.....	11
1.6 Топологии VANET.....	12
1.7 Приложения VANET	13
1.7.1 Приложения безопасности	13
1.7.2 Приложения управления транспортными потоками.....	15
1.7.3 Приложения общего назначения	15
1.8 Недостатки сетей VANET	16
1.8.1 Проблема обеспечения помехоустойчивости	16
1.8.2 Проблема обеспечения безопасности передаваемых данных	17
1.8.3 Проблема эффективности маршрутизации	19
2 VANET: стандарты.....	21
2.1 Стандарты построения VANET сетей.....	21
2.2 Технология DSRC	22
2.3 Анализ стандарта IEEE 802.11p.....	25
2.3.1 Физический уровень 802.11p	26
2.3.2 Канальный уровень 802.11p.....	27
3 Обзор проектов VANET	33
3.1 Проект V2V Communication NHTSA	33
3.2 Проект NoW	34
3.3 Проект COMeSafety	35
3.4 Проект AutoNet2030.....	37

3.5 Проект SARTRE	38
4 Применение VANET в России и мире	41
4.1 Применение VANET в ближайшие годы	41
4.2 Технологии компании Qualcomm.....	42
4.3 Умные дороги в России.....	44
ЗАКЛЮЧЕНИЕ	46
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	47

ВВЕДЕНИЕ

В начале 21 века в связи с развитием сетей с пакетной коммуникацией и интернета в целом, мировое телекоммуникационное сообщество приступило к реализации NGN – сетей следующего поколения (Next Generation Networks). Технологии NGN прошли эволюционный путь развития от гибкого программного коммутатора для обеспечения функций телефонной связи SoftSwitch до подсистем мультимедийной связи IMS (IP Multimedia Subsystem) и беспроводных высокоскоростных сетей с долговременной эволюцией LTE (Long-Term Evolution). Однако предполагалось, что основными пользователями NGN-сетей будут люди и, как подразумевалось, максимальное число абонентов в таких сетях будет ограничено численностью населения планеты Земля.

Однако, в последнее время, развитие получили другие технологии. Например, технология беспроводной передачи данных малого радиуса действия NFC (Near Field Communication), которая даёт возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров. В данной выпускной квалификационной работе данную технологию мы рассматривать не будем.

Перед нами предстоит цель рассмотреть одну из инфокоммуникационных сетей пост-NGN, а именно, сети для транспортных средств VANET (Vehicular ad-hoc Networks).

Для достижения поставленной цели были обозначены следующие задачи:

- а) обзор истории создания VANET;
- б) разбор традиционной архитектуры;
- в) анализ стандартов VANET;
- г) обзор принципов организации и функционирования;
- д) определение практического применения в России и мире;
- е) выявление перспектив развития сетей VANET.

1 Сети VANET: общие сведения, архитектура, организация

1.1 Общие сведения

Уровень развития современных технологий беспроводной передачи данных позволяет использовать информационные сервисы практически из любого места, используя небольшие или относительно недорогие мобильные устройства. Технология автомобильных специальных сетей VANET (Vehicular ad-hoc Network) стала важной областью исследований за последние несколько лет. Сети VANET – это радиосети со случайными мобильными абонентами, обеспечивающие полностью децентрализованное управление, когда отсутствуют базовые станции или опорные узлы. Сети VANET относятся к классу мобильных самоорганизующихся сетей MANET (Mobile ad-hoc Network). Сети VANET обладают рядом особенностей как с точки зрения используемых протоколов, так и с точки зрения реализации. В настоящее время VANET сети создаются как надежные сети, которые транспортные сети в будущем будут использовать в целях связи на автомагистралях или в городских условиях. Наряду с этими преимуществами, в VANET возникает большое количество проблем, таких как обеспечение качества обслуживания (QoS – Quality of Service), широкие возможности подключения и пропускная способность, а также безопасность для транспортных средств и индивидуальная конфиденциальность.

Хотя автомобильная специальная сеть VANET не является новой темой, она продолжает создавать новые исследовательские задачи и проблемы. Основная задача VANET – своевременно помочь группе транспортных средств создать коммуникационную сеть связи между ними и поддерживать ее без использования какой-либо центральной базовой станции или какого-либо контроллера. Одно из основных применений VANET заключается в критических медицинских чрезвычайных ситуациях, когда отсутствует инфраструктура, в то время как крайне важно передавать информацию для спасения человеческих жизней. Однако наряду с этими полезными приложениями VANET возникают новые испытания и проблемы. Отсутствие инфраструктуры накладывает

дополнительную ответственность на транспортные средства. Каждое транспортное средство становится частью сети, а также управляет и контролирует коммуникацию в этой сети наряду со своими собственными требованиями к связи.

Сеть VANET считается одной из составляющих интеллектуальной транспортной системы (ИТС), которая вместе с VANET также включает:

- спутниковые системы позиционирования (GPS, GALILEO, ГЛОНАСС);
- системы оплаты и взаимодействия на основании протокола связи DSRC;
- сотовые сети связи разных стандартов;
- системы экстренного вызова в случае аварийных ситуаций e-call и ЭРА-ГЛОНАСС.

Интеллектуальная транспортная система – это симбиоз коммуникационных и информационных возможностей транспортных средств и систем управления движением.

1.2 Роль VANET в структуре ИТС

Автомобильная самоорганизующаяся сеть VANET является одним из важных компонентов ИТС, узлы которой представлены самими транспортными средствами с установленными на них коммуникационными модулями связи. Основная цель этой разновидности сетей – это информирование участников дорожного движения о возникновении непредвиденных ситуаций. Этот функционал организуется при помощи автоматической рассылки сообщений от приложений, связанных с безопасностью дорожного движения через самоорганизующуюся сетевую структуру. Одной из актуальных проблем, которая может быть решена путем обеспечения того, чтобы водители были в курсе ситуации на дорогах, является перераспределение транспортных потоков и, это, таким образом, может позволить уменьшить величину пробок на дорогах.

VANET считается частью концепции интеллектуальной транспортной системы, которая выполняет роль формирования самоорганизующейся и высокодинамичной сетевой структуры, которая, в свою очередь, передает информацию о дорожном трафике и авариях. Сети VANET являются отправной точкой для создания полноценной ИТС, так как они могут работать как совместно с инфраструктурными станциями, так и отдаленно от них. Кроме того, высокая стоимость развертывания инфраструктурной части ИТС подчеркивает весомость сетей VANET в составе общей комплексной системы.

Сети VANET наделены особенностями, например, такими, как: высокая скорость движения транспортного средства, высокая плотность узлов, непостоянство структуры и состава сетей, зачастую кластеризация на изолированные участки. Все эти особенности налагают специальные требования на параметры и режимы функционирования сети. Особенно, ключевое требование – это минимизирование задержек для передачи сообщений из приложений безопасности дорожного движения и сохранение высокого уровня связности сети. Такие требования требуют использовать специализированную технологию беспроводной связи, которой стала WAVE.

1.3 Архитектура

Сети VANET являются беспроводными самоорганизующимися децентрализованными сетями, которые состоят из мобильных устройств. Всякое такое устройство, вне зависимости от любого направления, может передвигаться, и, в связи с чем, часто устанавливать и разрывать соединение с соседями. На данной схеме (рисунок 1) изображена традиционная архитектура VANET сетей:

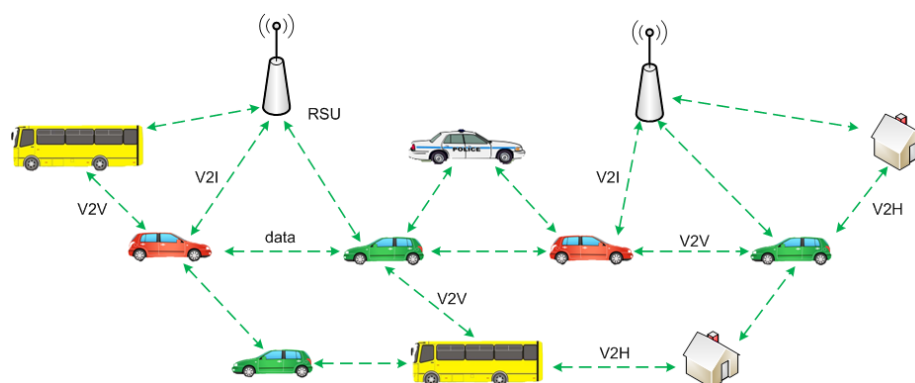


Рисунок 1 – Традиционная архитектура VANETсети

Главная особенность VANETсетей – это максимальная децентрализация, когда в сети нет выделенного сервера, и вся инфраструктура распределена между узлами связи. Данная особенность провоцирует возникновение большого количества существенных недостатков, которые мешают внедрению данной технологии.

1.4 Состав VANET

В состав основных элементов архитектуры VANET входят телекоммуникационные модули OBU (On Board Unit), которые устанавливаются на транспортное средство, кроме этого, инфраструктурные базовые станции RSU (Roadside Unit) с таким же набором интерфейсов связи. OBU – Это модули, которые интегрированы в бортовую систему, с собственными вычислительными ресурсами, информационным дисплеем и антенной. Чтобы эти модули взаимодействовали, в состав VANET, помимо программно-аппаратных модулей, входят коммуникационные интерфейсы. С учётом направления передачи информации между объектами, различают следующие виды интерфейсов:

- Vehicle-to-Vehicle (V2V) – вид интерфейса, когда взаимодействующими объектами являются модули OBU. В случае отсутствия инфраструктурных базовых станций, данный тип взаимодействия является основным. Он позволяет организовать обмен сообщениями между ТС и участниками дорожного движения с целью повышения степени безопасности дорожного движения;

– Vehicle-to-Infrastructure (V2I) – когда передача информации ведется от OBU к RSU. Используется в случаях передачи информации через инфраструктуру, в целях разгрузки беспроводных интерфейсов. Также позволяет организовать сбор информации в центры управления и организовать системы управления средствами контроля и регулирования транспортных потоков;

– Vehicular to Home (V2H) – обеспечивает взаимодействие OBU с другими IoT объектами, установленными в пределах домашней локации. В дополнении, через V2H может производиться автономная диагностика ТС, с последующей отсылкой данных в сервисные службы. Данный интерфейс позволяет расширить область сервисов, обеспечивающих комфортность поездок. Для этого, к примеру, в бортовой компьютер может быть заблаговременно загружен маршрут предстоящего путешествия со всеми точками интересов.

1.5 Виды взаимодействия

Европейский институт по стандартизации в области телекоммуникаций в стандарте ETSI TS 102 636-2 в сфере телекоммуникаций просматривает сценарии для трех ситуаций: V2V, V2I, R2V. Сценарий R2V обозначает взаимодействие транспортного средства с придорожной сетью по инициативе самой придорожной сети.

В вышеупомянутых сценариях этого стандарта рассматриваются четыре вероятных типа взаимосвязи:

- «Точка-точка»;
- «Точка-много точек»;
- «Геонаправленный»;
- «Геошироковещательный».

«Точка – точка» означает связь одной станции ИТС только с одной другой станцией. «Точка – много точек» - одной станции ИТС со многими. Сценарии «геонаправленный» (GeoAnycast) и «геошироковещательный» (GeoBroadcast) основаны на использовании протокола GeoNetworking.

«Геонаправленный» сценарий предполагает передачу информации от одной ИТС-станции к произвольной ИТС-станции в границах географической области обслуживания определенной ИТС.

«Геошироковещательный» сценарий предполагает передачу информации от одной ИТС ко всем ИТС станциям в границах географической области обслуживания определенной ИТС.

На рисунке 2 показан пример «геонаправленного» сценария, а на рисунке 3 – «геошироковещательного». Приемные и передающие станции представлены с наклонной и горизонтальной штриховкой, транзитные представлены с вертикальной, а прочие участники дорожного движения представлены серым цветом без штриховки.

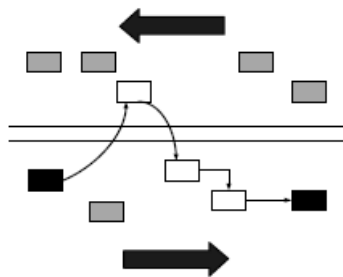


Рисунок 2 – «Геонаправленный» сценарий

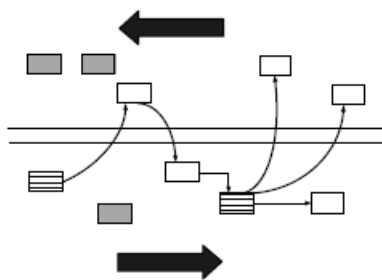


Рисунок 3 – «Геошироковещательный» сценарий

1.6 Топологии VANET

В соответствии с составом автомобильных сетей, становится ясно, что они могут создавать как одноранговую структуру, так и иерархическую.

В случае одноранговой структуры, применение RSU не предполагается. Передача информации проводится или в режиме «точка-точка», или в режиме «точка-много точек». Последний для случаев широковещательной трансляции

сообщений. Этот режим соответствует сетевой топологии «звезда».

Вовлечение в обмен информацией инфраструктурных базовых станций (RSU) даёт право организовать топологию типа «кластерное дерево». Обмен данными между специализированными телекоммуникационными модулями OBU, и вдобавок к этому взаимодействие с другими сервисами интеллектуальной транспортной системы ведётся через ближайшую RSU. RSU, соединённые друг с другом, позволяют организовать межкластерный сетевой информационный обмен. Это даёт право повысить связность сети и существенно разгрузить беспроводной канал связи. На рисунке 4 предлагаются варианты сетевых технологий, образуемых компонентами VANET.

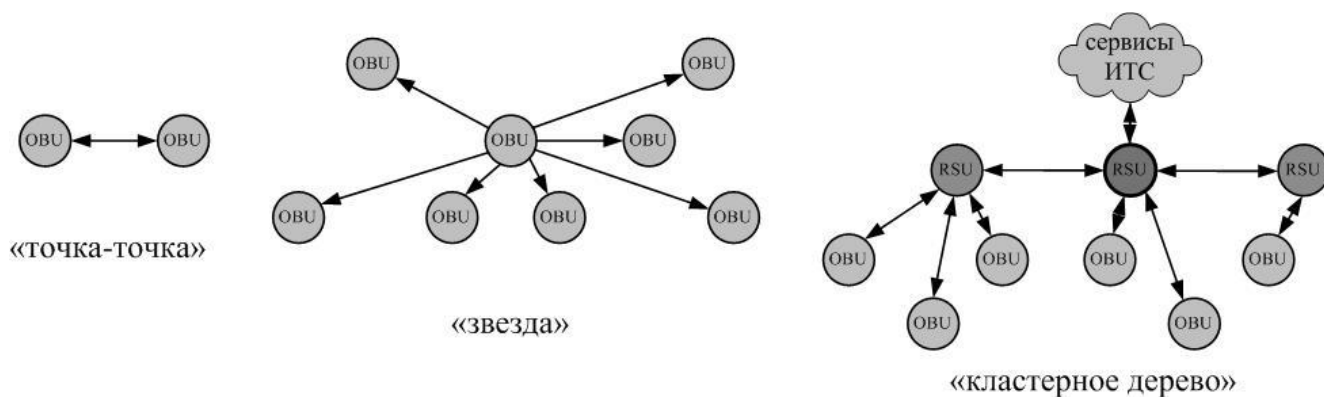


Рисунок 4 – Виды топологий VANET.

1.7 Приложения VANET

Приложения VANET группируются в соответствии с их главной целью:

- приложения безопасности — это приложения, которые повышают безопасность ТС на дорогах;
- приложения общего назначения – приложения, которые предоставляют развлекательные или коммерческие услуги, часть которых может оказаться с добавленной стоимостью;
- приложения управления транспортными потоками – это приложения, которые формируют инфокоммуникационную структуру, преследующие цель оптимизации перевозок.

1.7.1 Приложения безопасности

Главной задачей приложений безопасности является повышение уровня общественной безопасности, а также минование человеческих жертв. Основной характеристикой таких приложений является, как правило, то, что данные от приложений безопасности поступают заинтересованным узлам, например, транспортным средствам, которые приближаются в течение ограниченного времени к опасной зоне. Исходя из критичности ко времени эти приложения, как правило, требуют наличия прямой взаимосвязи между узлами.

Задача по достижению повышения безопасности дорожного движения и устранению несчастных случаев может реализоваться при помощи осуществления своевременного информационного обмена типа V2V или V2I, с помощью использования беспроводных технологий связи. Это помогает как снизить риски гибели людей, так и повысить чистоту окружающей среды благодаря предотвращению всяких разливов загрязняющих жидкостей, которые зачастую возникают в результате аварий.

Относящиеся к безопасности приложения можно сгруппировать в три основных класса:

- информирование (о зоне ремонтных работ или об ограничении скорости движения);
- предупреждение (послеаварийные, о состоянии дороги или препятствиях);
- помощь (управление сменой полос, навигация, предотвращение коллективных столкновений).

Уведомление об экстренном торможении может быть, в качестве примера, предупреждающим приложением. Тогда при возникновении ДТП, или при срабатывании подушек безопасности, или же просто о внезапном резком торможении, машинам позади нас отправляется уведомление. Машинам, движущимся во встречном направлении движения, будет разослана точно такая же информация. В конечном итоге будут проинформированы все автомобили,

которые, вероятно, могут попасть в ДТП.

Существует и другой, более сложный пример реализации приложений безопасности. Эти примером является система совместного вождения, которая построена на обмене данными от бортовых датчиков или иной технической информацией между машинами. Ключевая идея этой системы стоит в том, чтобы расширить поля зрения водителя благодаря обработке поступающей информации автономными приложениями. В итоге, водители тех автомобилей, которые следуют по той же дороге, получают информацию об опасностях, препятствиях, транспортном потоке времени, что, вследствие, приводит к более эффективному и безопасному вождению. Как можно заметить, работоспособность подобного приложения крайне зависит от количества автомобилей, которые оснащены VANET системами.

1.7.2 Приложения управления транспортными потоками

Одна из главных задач, которая возлагается на ИТС в городском окружении, является интеллектуальное управление транспортными потоками. Для этой цели с помощью датчиков, которые установлены на камерах наблюдения, базовых станциях и иных систем детектирования, собирается информация о текущем состоянии транспортных потоков с соединением к участкам дорог. Полученная информация рассматривается в центрах координации и на основании итогов анализа осуществляются управляющие воздействия на средства координации дорожных потоков. К такого рода управляющим воздействиям можно отнести: изменение скоростного режима, изменение схемы работы светофоров и разного рода предупреждения на информационных экранах.

Другим средством воздействия на транспортные потоки является распространение информации о дорожной обстановке и пробках, непосредственно на ОВУ. Эта информация может изображаться на бортовых средствах навигации и побуждать к действию водителей на выбор альтернативных маршрутов.

1.7.3 Приложения общего назначения

Главная цель приложений общего назначения – это улучшение комфорта пассажиров. Пассажиры ТС, которые проводят очень много времени в поездках, могут стать заинтересованы в данной области применения автомобильных сетей. Она состоит в предоставлении пользователям множества различных видов информации. Благодаря этому способу, пассажирам могут быть предоставлены виды информации, например, информация о погоде, объявления, развлекательный контент, кроме этого, полные указания местоположения ближайшего кафе, ресторана, отеля. Для водителей предоставляется дополнительная информация о расположении ближайших парковок или заправочных станций. Пассажиры могут смотреть видео, играть в онлайн игры, получать доступ к Интернету, пользоваться почтой и общаться с людьми, пока к инфраструктурной сети подключено ТС.

У коммерческих приложений есть главная особенность – приложениям безопасности они не обязаны мешать. Подходящим решением в данном контексте будет использование отдельных физических каналов и приоритезация трафика.

1.8 Недостатки VANET сетей

Традиционным VANET сетям свойственна максимальная децентрализация, когда в сети отсутствует выделенный сервер, и вся инфраструктура распределяется по узлам связи. Данная особенность провоцирует возникновение следующих недостатков, таких как: низкие мобилизационные способности и большое время реакции системы на внешние воздействия.

На сегодняшний день VANETs поддерживают большое количество новых сервисов и протоколов. Тем не менее, все еще существует целый ряд проблем, препятствующих к полноценному внедрению данной технологии в жизнь.

1.8.1 Проблема обеспечения помехоустойчивости

Транспортным сетям VANET характерно большое количество помех различного вида. Обеспечить максимальное снижение влияния помех можно с помощью регулирования мощностей приемников и передатчиков устройств в сети

или путем выбора оптимальной частоты канала, но в классических сетях VANET данная проблема остается нерешенной и оказывает существенное влияние на функционирование сети. На рисунке 5 изображена сеть VANET, красным цветом помечены связи между узлами, на пути которых возникли помехи:

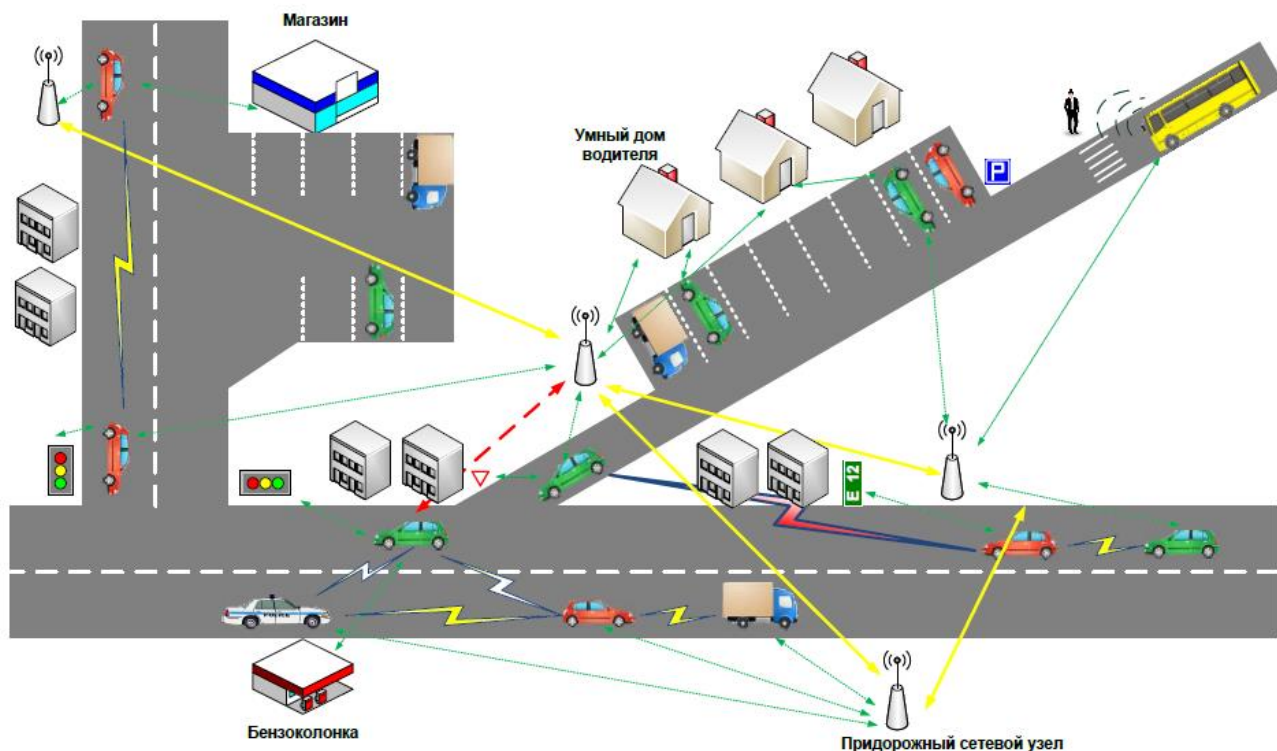


Рисунок 5 – Помехи в сетях VANET

1.8.2 Проблема обеспечения безопасности передаваемых данных

Причинами проблем, связанными с информационной безопасностью транспортных сетей VANET, являются:

- отсутствие средств защиты узлов от злоумышленников;
- возможность прослушивания каналов и подмены сообщений по причине общей доступностью среды передачи;
- невозможность применения классической системы обеспечения безопасности из-за особенностей классической архитектуры сетей VANET;
- необходимость использования сложных алгоритмов маршрутизации, учитывающих вероятность появления некорректной информации от скомпрометированных узлов в результате изменения топологии сети;

- любой узел, находящийся в диапазоне источника сигнала, знающий частоту передачи и другие физические параметры (модуляцию, алгоритм кодировки) потенциально может перехватить и раскодировать сигнал. При этом ни источник сигнала, ни получатель не будут об этом знать;

- невозможность реализации политики безопасности ввиду особенностей классической архитектуры VANET сетей, таких как отсутствие фиксированной топологии и центральных узлов.

Таким образом, можно отметить, что самоорганизующиеся VANET сети уязвимы к классическим типам атак, присущим большинству беспроводным сетям, так и имеют свои отличительные уязвимости. Так как беспроводные самоорганизующиеся сети не имеют фиксированной топологии, центральных узлов, широкополосного канала, стабильных источников питания, постоянной связи узлов, реализация успешной атаки злоумышленником становится легко выполнимой. Атаки в транспортных сетях VANET можно разделить на пассивные и активные.

При пассивных атаках злоумышленник обычно скрыт, он подсоединяется к линиям связи для сбора определенных данных. Пассивные атаки могут быть разбиты на два класса: анализ трафика и перехват (сниффинг).

При активных атаках злоумышленник оказывает прямое влияние на работу системы, происходящие в атакуемой сети. Явное отличие активного воздействия от пассивного — принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят некоторые изменения. Активные атаки могут быть классифицированы на следующие группы:

- физические;
- фальсификация (спуфинг), повтор и изменение сообщений;
- отказ в обслуживании.

В качестве примера на рисунке 6 изображена атака Man-on-the-Middle в VANET сети. Два автомобиля обмениваются сообщениями. Злоумышленник, находящийся в этой же сети, хочет перехватывать сообщения между этими

узлами. Во время атаки ARP-spoofing злоумышленник отправляет два ARP ответа (без запроса) автомобилям. Так как автомобили поддерживают самопроизвольный ARP, то, после получения ARP-ответа, они изменяют свои ARP таблицы. Тем самым атака ARP-spoofing выполнена, и теперь все пакеты между автомобилями проходят через злоумышленника.

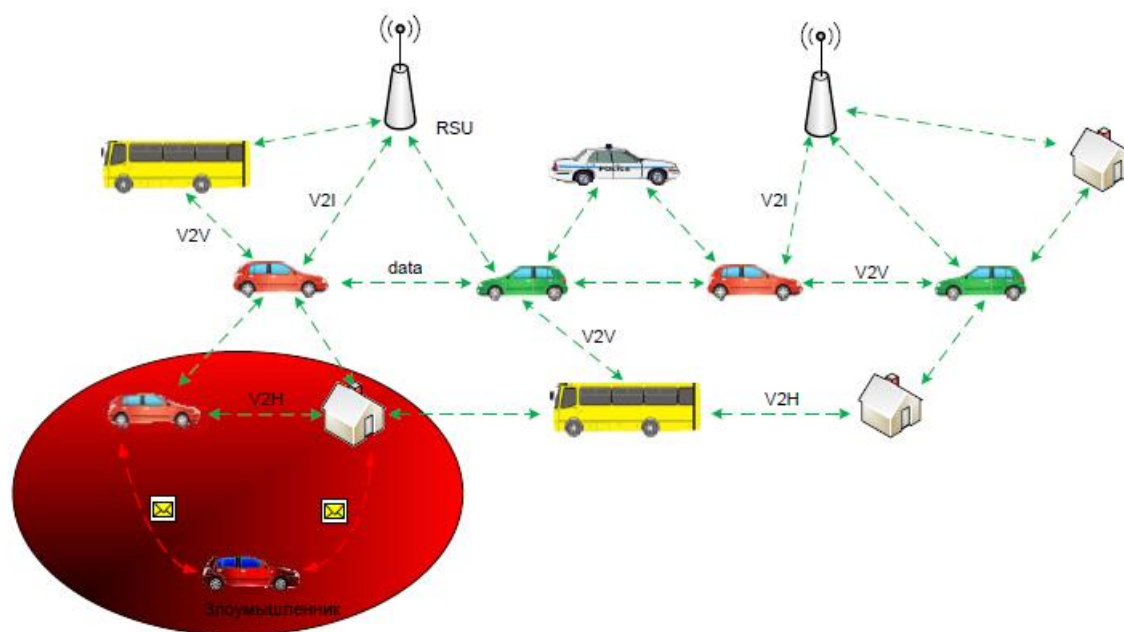


Рисунок 6 – Атака Man-on-the-Middle в VANET сети

1.8.3 Проблема эффективности маршрутизации

В VANET сетях проблема пропускной способности наиболее обостряется при одновременной передаче большого количества видеoinформации. Ситуация усугубляется при неэффективности методов маршрутизации, когда сеть переполняется широковещательными запросами или образуется «бутылочное горлышко». На рисунке 7 изображен пример неэффективной маршрутизации, когда весь трафик проходит через один узел:

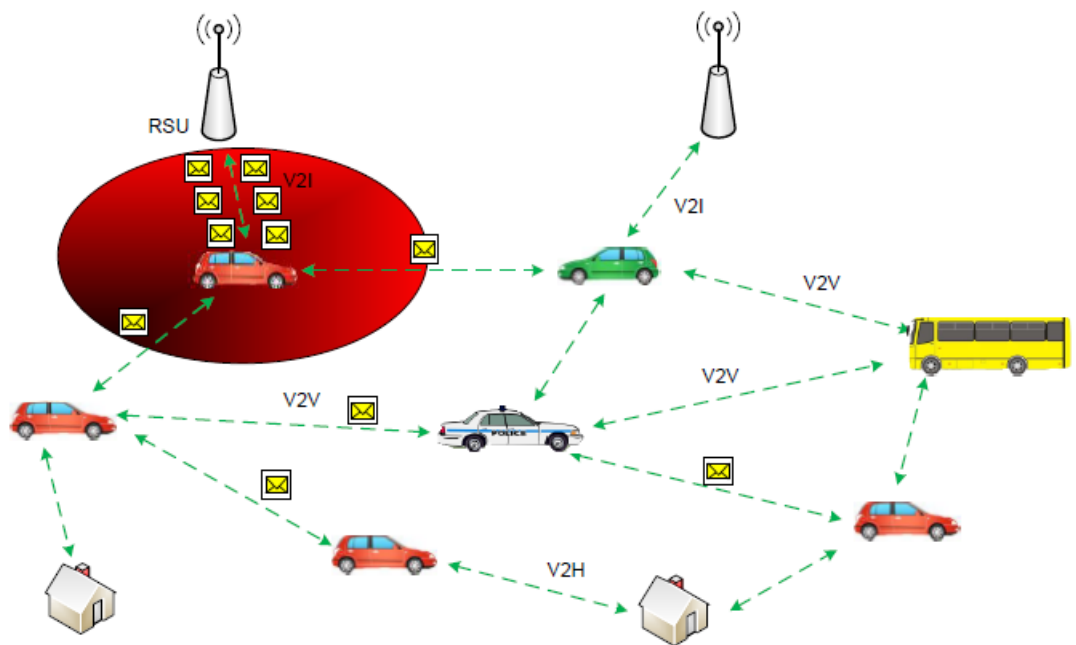


Рисунок 7 – Неэффективная маршрутизация в VANET сети

2 VANET: стандарты

2.1 Стандарты построения VANET сетей.

Для того, чтобы рассмотреть архитектуры VANET сетей, нужно начать удобно использовать иерархическую сетевую модель, которая подобна модели OSI. В этом разделе мы будем рассматривать специфику построения VANET на разного рода уровнях сети. Далее мы проведем сравнение стандартов, существующих для построения VANET сетей со стекком протоколов TCP/IP.

На физическом уровне VANET сети разделяются на два подуровня: аппаратный подуровень, в котором подробно рассматриваются особенности построения узлов VANET, а также сетевой подуровень, который включает в себя узлы сети и среду передачи данных.

На аппаратном подуровне VANET имеет отличие от традиционных сетей передачи данных. А именно, строение узлов мобильной сети. Устанавливаемый в мобильных узлах модуль OBU выполняет две основные функции. Сначала он собирает данные с множества автомобильных датчиков, а затем по сети передает результаты обработки собранных данных. В режиме реального времени производится обработка данных. Это связано с требованиями приложений по обеспечению безопасности дорожного движения.

На сетевом подуровне VANET применяются беспроводные типы соединений. Для соединений Vehicle-to-Infrastructure (V2I) могут быть использованы мобильные сети сотовой связи. Для соединений Vehicle-to-Vehicle (V2V) может применяться технология Wi-Fi. Для Wi-Fi стандарты разрабатывались без учёта требований для VANET сетей. Для того, чтобы повысить надёжность и уменьшить задержку при передаче данных, для VANET сетей был разработан новый стандарт беспроводной связи – IEEE 802.11p. Под необходимость приложений, которые обеспечивают безопасность дорожного движения в Европе и США, были выделены каналы частот, названные DSRC (Dedicated Short-Range Communications – радиосвязь ближнего радиуса действия).

На физическом уровне повышение надёжности передачи данных в

стандарте IEEE 802.11p можно достичь путём уменьшения частоты передачи, тем самым коллизия при передаче пакетов снижается.

На канальном уровне, в связи с тем, что есть требования чувствительных к задержкам приложений в реализациях VANET сетей, используются протоколы, которые поддерживают механизмы приоритезации трафика. Таким образом, стандарт IEEE 802.11p реализует приоритезацию трафика, которая поддерживается при помощи знака EtherType на канальном уровне сети при помощи специального алгоритма управления доступом к среде передачи данных. В стандарте IEEE 802.11p еще более приоритетный трафик имеет меньшее значение временных задержек в механизме множественного доступа к среде передачи данных.

В VANET на сетевом уровне есть возможность применения специфических протоколов маршрутизации, которые базируются на информации о географической позиции узла. У этих протоколов служебные сообщения имеют исключительно информацию об позиции идентификатора и его узле, что, в конечном итоге, сокращает объём служебного трафика в сети по отношению к протоколам маршрутизации на основе топологии.

В частности, при построении VANET, свойственно использовать стек протоколов с двумя независимыми решениями для сетевого уровня. Сетевой уровень стека TCP/IP нередко выступает в роли одного из решений. Он используется для трафика, который не требует низких задержек при передаче. Для трафика, который чувствительный к задержкам, применяется отдельное решение на сетевом уровне. Оно обеспечивает низкие задержки при передаче сообщений. Нередко такое решение основывается на широковещательной рассылке сообщений.

2.2 Технология Dedicated Short-Range Communications (DSRC)

Технология DSRC — это вид связи стандарта IEEE 802.11p, его часто называют «автомобильный Wi-Fi». DSRC может очень серьезно повлиять на рынок мобильных сервисов на базе V2V и V2I. В 2010 году стандарт был

принят. DSRC, в отличие от сетей сотовой связи, стабильно передает данные при движении транспортного средства со скоростью до 250 км/ч. Ожидается что в будущем, благодаря этой технологии, можно будет значительно снизить вероятность столкновения автомобилей. Более того, технологии на базе DSRC позволят быстро и недорого строить одноранговые сети и, таким образом, снизить нагрузку на сети сотовой связи.

Настоящий прорыв в использовании технологий VANET, которые предполагают установку прямой связи между машинами и объектами на дороге, минуя сотовые вышки, спутники, и другое «промежуточное» оборудование, ожидается, когда регулирующие органы в различных странах всерьез озаботятся предотвращением столкновений и использованием «активной» дорожной инфраструктуры для регулирования транспортных потоков. DSRC связь, на протяжении ближайших 20 лет, появится в каждом транспортном средстве, включая легковые автомобили. Она будет дополнять технологии, обеспечивающие передачу данных по сетям сотовой связи и позиционирование в пространстве.

Фактически большинство задач, характерных для транспортных систем управления и связи, технология DSRC позволяет решить с учетом совместного применения технологии динамической маршрутизации для построения одноранговых сетей (Delay & Disruption-Tolerant Networking, DTM) и систем глобального геопозиционирования GPS/ГЛОНАСС. Фактически осуществляется кооперация с мобильной и наземной связью, когда скорости, надежности и гибкости других систем связи оказывается недостаточно, — получаются совершенно новые решения.

В Америке эта технология строится на архитектуре, которая получила название WAVE (Wireless Access for the Vehicular Environment). Она позволяет в транспортных системах обеспечить стандартизацию беспроводного доступа, регламентирует взаимодействие всех участников процесса, включая производителей транспортных средств и компонентов, организации,

обеспечивающие общественную безопасность, и транспортные компании. Технология используется как основа для DSRC проектов в США. В 1991 году была создана комиссия по «интеллектуализации» дорожного движения (Intelligent Transportation Society, ITS America). В США в 1999 г. Федеральная комиссия по связи (FCC) выделила 75 МГц в диапазоне 5,9 ГГц (5,875...5,925) для беспроводных сетей малого радиуса действия (DSRC) исключительно в целях безопасности дорожного движения — технологии коммуникаций транспортных средств на ближних расстояниях.

Коммуникационные протоколы для VANET стандартизированы IEEE. Физический и MAC уровни определены в спецификации IEEE 802.11p. Верхние уровни описываются группой протоколов IEEE 1609x, и вместе они образуют технологию под названием «беспроводной доступ для транспортной среды» (WAVE). Иногда технологию WAVE называются CALM M5. Стандарт IEEE 802.11p определяет физический и канальный уровень и принят в июне 2011 году как дополнение к основному стандарту IEEE 802.11.

В 2015 году представитель исследовательской группы, проводившей двухгодичное тестирование DSRC в США, а также представитель национального управления безопасностью движения на трассах США сообщили, что для спектра DSRC должна быть гарантирована доступность и надежность, не должно возникать интерференции с нелицензируемым Wi-Fi. В исследовании участвовали 47 компаний и 2843 транспортных средства, собраны 115 миллиардов сообщений.

Европейская стандартизация получила название ITS-G5, о ней мы поговорим ниже. ITS-G5 отличается от WAVE, в целом, в верхних слоях архитектуры, также есть отличия и в терминологии. Несмотря на это, она также, как и WAVE, основана на стандарте IEEE 802.11p. Главными являются различия в структуре приема-передачи станции ITS-G5 и WAVE. В Европе выделена полоса шириной 30 МГц в диапазоне 5.9 ГГц (5.875 ... 5.905). Возможно также использование 20 МГц в промышленной, научной и медицинской полосах частот ниже 5.875 ГГц.

Японский стандарт 5.8 ГГц DSRC значительно отличается от американской технологии WAVE 5.9 ГГц, так как он используется только для взаимодействия автомобилей с придорожным оборудованием. Для V2V-коммуникаций выделено 10 МГц в диапазоне 700 МГц (так, например, все оборудование, разработанное по заказу Toyota, также работает на данной частоте).

В России в 2011 г. вышло постановление ГКРЧ, согласно которому решено:

– Выделить полосу радиочастот 5855–5925 МГц для применения юридическими и физическими лицами придорожных и автомобильных РЭС интеллектуальных систем на транспорте (ITS) без оформления отдельных решений ГКРЧ.

– Применение РЭС интеллектуальных систем на транспорте (ITS) в выделенной в п. 3 настоящего решения ГКРЧ полосе радиочастот должно осуществляться при выполнении следующих условий:

а) соответствия технических характеристик, применяемых РЭС интеллектуальных систем на транспорте (ITS), основным техническим характеристикам, указанным в приложении к настоящему решению;

б) получения для придорожных РЭС интеллектуальных систем на транспорте (ITS) в установленном порядке разрешения на использование радиочастот на основании заключения экспертизы радиочастотной службы о возможности использования заявляемых РЭС и об их электромагнитной совместимости с действующими и планируемыми для использования РЭС.

2.3 Анализ стандарта IEEE 802.11p

IEEE 802.11p — это одобренная поправка к стандарту IEEE 802.11 для добавления беспроводного доступа в автомобильную среду. Стандарт IEEE 802.11p является набором спецификаций, которые нужны для того, чтобы обеспечить взаимодействие между беспроводными узлами, стремящимися связаться в условиях быстро изменяющегося окружения. Транзакции в этих

ситуациях должны реализовываться в течение временного интервала, который много меньше, чем это предназначено для стандартных IEEE 802.11 сетей. Также, данный временной интервал должен быть меньше, чем время, которое требуется чтобы выполнить стандартную аутентификацию и подключиться к точке доступа. Для того, чтобы достичь этих показателей, протоколом переопределяются механизмы работы физического и канального уровней.

2.3.1 Физический уровень 802.11р

Физический уровень стандарта IEEE 802.11р является некоторой модификацией физического уровня стандарта IEEE 802.11а с параметрами, которые приведены в таблице 1. Внесенные изменения в 802.11р преследуют задачу приспособления стандарта к часто меняющейся топологии сети, условиям высокой мобильности абонентов, и требованиям автомобильных приложений.

Таблица 1 - Параметры протоколов IEEE 802.11а и IEEE 802.11р

Параметры	IEEE 802.11а	IEEE 802.11р
Тип модуляции	BPSK, QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM
Битовая скорость (Мбит\с)	6, 9, 12, 18, 24, 36, 48, 54	3, 4.5, 6, 9, 12, 18, 24, 27
Кодовая скорость	1/2, 2/3, 3/4	1/2, 2/3, 3/4
Кол-во поднесущих	52	52
Длительность символа	4 мкс	8 мкс
Защитный интервал	0.8 мкс	1.6 мкс
FFT период	3.2 мкс	6.4 мкс
Длительность преамбулы	16 мкс	32 мкс
Интервал между поднесущими	0.3125 МГц	0.15625 МГц

В VANET, для того, чтобы организовать процесс обмена данными, применяется OFDM модуляция с разделением общей полосы пропускания в 75МГц на подканалы по 10 МГц. С помощью этого достигается скорость передачи данных от 3 до 27 Мбит/с. Таким же образом есть возможность соседние подканалы объединить в один, шириной 20МГц, это позволит достичь скорости передачи данных в 54 Мбит/с.

Под задачи VANET в США зарезервирован диапазон частот 5.85...5.925 ГГц. В этом диапазоне предусмотрено формирование одного управляющего канала CCH (Control Channel) и до шести служебных каналов SCH (Service Channel) с номерами 172-176 и 180-182. На рисунке 8 показано распределение частотного спектра по подканалам. Управляющий канал CCH предназначен для управления сетью и передачи сообщений, которые связаны с безопасностью дорожного движения. Служебные каналы SCH служат и для передачи трафика приложений, связанных с безопасностью дорожного движения, и прочего трафика, например, пользовательского IP-трафика.

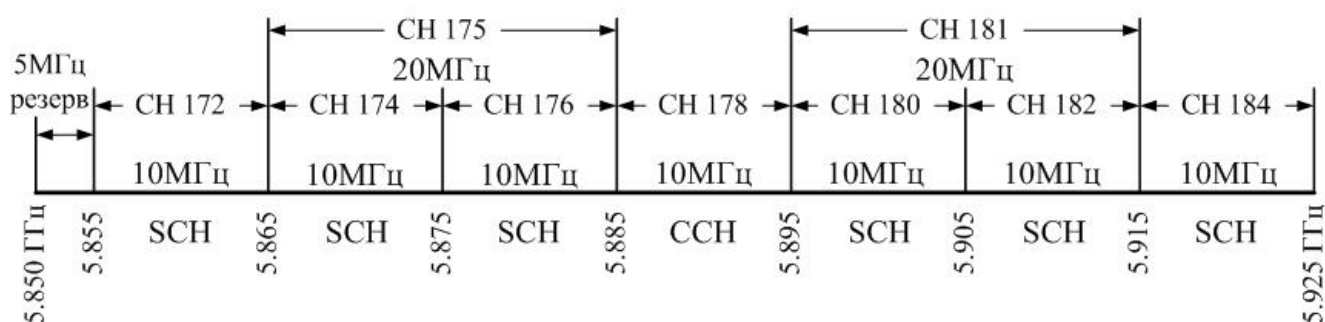


Рисунок 8 – Распределение частотного спектра в США

Под задачи VANET в Европе выделили такой же диапазон частот, но способ его распределения по подканалам, который приведен на рисунке 9, немного отличается от используемого в США. Кроме того, реализуемую на двух нижних уровнях технологию доступа в совокупности с уровнем LLC (LogicaLinkControl), в Европе, согласно стандарту EN 302 665, выделили в отдельный элемент архитектуры и назвали ITS-G5. Этот элемент архитектуры отвечает за организацию взаимодействия узлов без предварительного установления соединения, т.е. в режиме ad-hoc. Согласно стандарту EN 302 663 v1.2.1, весь выделенный диапазон частот разбит для задач ITS-G5 на три поддиапазона:

Первый поддиапазон - ITS-G5A (диапазон частот 5,875...5,905 ГГц) – имеет три канала по 10 МГц и предназначен для реализации устройствами ITS-G5 сервисов, связанных с безопасностью дорожного движения;

Второй поддиапазон - ITS-G5B (диапазон частот 5,855...5,975 ГГц) –

имеет два канала по 10 МГц и предназначен для исполнения услуг прочих приложений;

Третий поддиапазон - ITS-G5D (диапазон частот 5,905...5,925 ГГц) – имеет два канала по 10 МГц и предназначен для исполнения услуг новых приложений ИТС.

На рисунке 9 приведено распределение частотного спектра по подканалам:

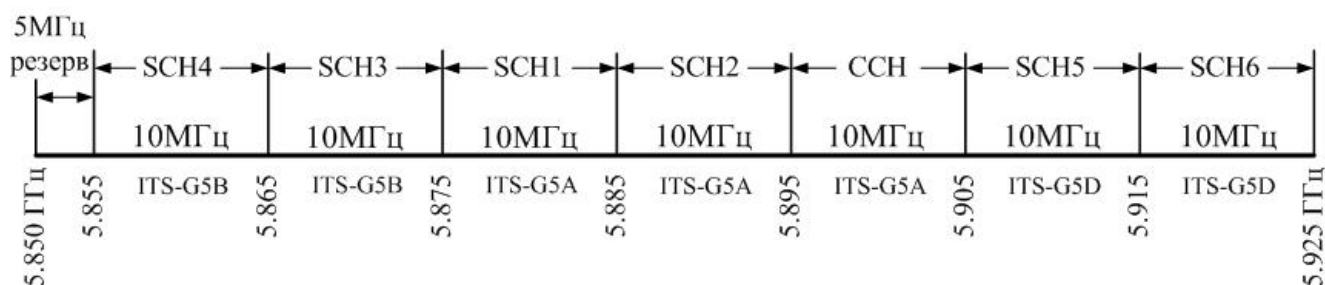


Рисунок 9 – Распределение частотного спектра в Европе

В WAVE, кроме частотного разделения, предусматривается временное разделение ресурсов каждого из каналов. Чтобы это сделать, ресурс предоставляется в виде «таймслотов» (временных интервалов), в пределах которого станции производят информационный обмен. В результате, применение узлами VANET радиоканалов, которые приведены на рисунке 8, возможно в одном из трех режимов:

- непрерывный режим – узлы взаимодействуют непрерывно либо лишь через управляющий канал CCH, либо лишь через служебные каналы SCH (рисунок 10 а);

- альтернативный режим – предусматривает поочередное взаимодействие через два канала CCH и SCH, или SCH и другой SCH. Смена канала производится в каждом новом таймслоте (рисунок 10 б);

- безотлагательный режим – предоставляет возможность по запросу от верхнеуровневых приложений переключиться с одного канала на другой, не дожидаясь окончания текущего таймслота (рисунок 10 в).

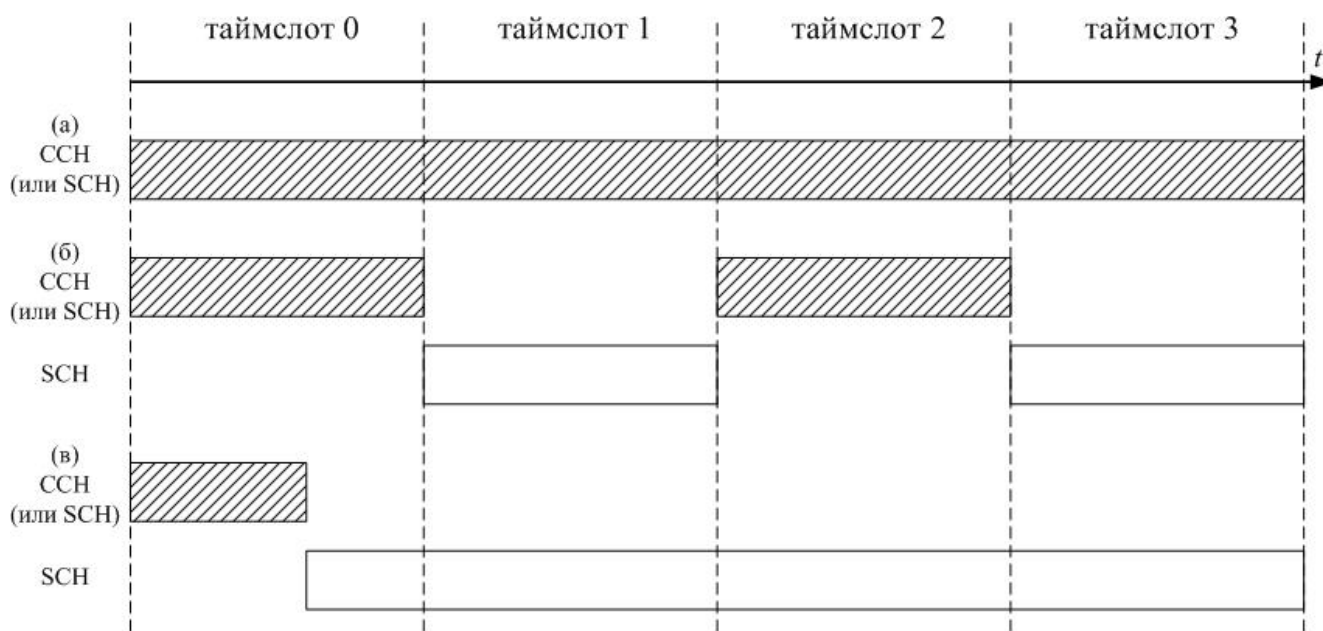


Рисунок 10 – Распределение временного ресурса по подканалам

2.3.2 Канальный уровень 802.11p

Алгоритмы канального уровня предназначены для того, чтобы принимать решение, а именно, в какой период времени узел обладает возможностью осуществить передачу, опираясь на текущий статус канала и на состоянии очереди передачи. Основной целью этого функционала считается минимизирование интерференции с параллельным повышением вероятности удачного приема переданной информации. В автомобильных сетях MAC алгоритмы определяются стандартом IEEE 802.11p.

Стандарт IEEE 802.11p, который адаптирован с целью организации взаимодействия типа V2V, унаследовал от стандарта IEEE 802.11a достаточно много характеристик. Особенно важная среди этих характеристик — это система распределения прав доступа к каналу. В стандарте 802.11p учитывается три вида координации доступа на MAC уровне: HCF (Hybrid Coordination Function), DCF (Distributed Coordination Function) и PCF (Point Coordination Function).

Распределенный режим доступа DCF считается ключевой технологией ad-hoc взаимодействия, если имеется в виду отсутствие центрального координирующего устройства. Технология DCF получила название EDCA,

благодаря сочетанию с добавленными для VANET сетей механизмами управления качеством обслуживания (QoS), которые были частично заимствованы из протокола IEEE 802.11e. EDCA была создана на технологии Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA), в соответствии с которой перед реализацией передачи фрейма, поступившего на MAC уровень, производится прослушивание статуса канала в течении межкадрового интервала AIFS (Arbitration Inter-Frame Spacing). Если происходит неудачная попытка передачи, то для узла устанавливается интервал отсрочки CW (Contention Window), в процессе которого узел не предпринимает попыток отправки.

QoS, применяемый на канальном уровне, допускает градацию всех отправляемых данных на восемь категорий пользователей UPs (User Priorities) и четыре категории доступа ACs (Access Categories), приведенных в таблице 2. Начальный приоритет имеет категория с номером 0, категория 7 – самый большой.

Таблица 2 - Категории доступа для EDCA

Номер категории	Категория пользователя	Категория доступа	Тип трафика
0	Best effort (BE)	AC_BE	Best effort
1	Background (BK)	AC_BK	Background
2	Spare (-)	AC_BK	Background
3	Excellent effort (EF)	AC_BE	Best effort
4	Controlled load	AC_VI	Video
5	Video (VI)	AC_VI	Video
6	Voice (VO)	AC_VO	Voice
7	Network control (NC)	AC_VO	Voice

Для AIFS итоговое значение для каждой категории доступа рассчитывается по следующей формуле:

$$IFS[AC] = AIFSN[N] * ASlotTime + ASIFTime \quad (1)$$

где $ASlotTime$ – это длительность одного временного слота;

$ASIFTime$ – длительность интервала SIFS (Short Inter-Frame Space), определенная на PHY и приведенная в таблице 4.

Величина интервала отсрочки CW, вычисляемого при каждой итерации неудачной попытки отправки, также как и $AIFS[AC]$, зависит от категории

доступа. Методика расчета его значения приведена в таблице 3.

Таблица 3 – Методика расчета величины интервала отсрочки

Категория доступа	CW_{min}	CW_{max}	$AIFSN$
AC_BK	aCW_{min}	aCW_{max}	9
AC_BE	aCW_{min}	aCW_{max}	6
AC_VI	$(aCW_{min}+1)/2-1$	aCW_{min}	3
AC_VO	$(aCW_{min}+1)/4-1$	$(aCW_{min}+1)/2-1$	2

Таблица 4 – Параметры OFDMPHY, используемые в IEEE 802.11p

Параметр	Значение
$ASlotTime$	13 мкс
$ASIFTime$	32мкс
aCW_{min}	15
aCW_{max}	1023

Таким образом, используя данные в таблице 4 значения, а также формулу (1) и формулы из таблицы 3, мы рассчитываем итоговые значения AIFS и CW для различных ACs протокола IEEE 802.11p, которые приведены в таблице 5.

Таблица 5 – Расчетные значения CWи AIFS для IEEE 802.11p

Категория доступа	CW_{min}	CW_{max}	$AIFS$ (мкс)
AC_VO	3	7	58
AC_VI	7	15	71
AC_BE	15	1023	110
AC_BK	15	1023	149

Для того, чтобы подробно разобраться в процессах подготовки данных к передаче, принимая во внимание работу механизма EDCA, мы обращаемся к архитектуре передающей части узла сети стандарта IEEE 802.11p, которая приведена на рисунке 11. Эта архитектура описывает следующие операции: обработка очередей с учетом приоритизации, маршрутизация каналов и управление каналами передачи. Отсюда можно заметить, что в структуре передающего тракта управление каналами CCH и SCH реализуется отдельно.

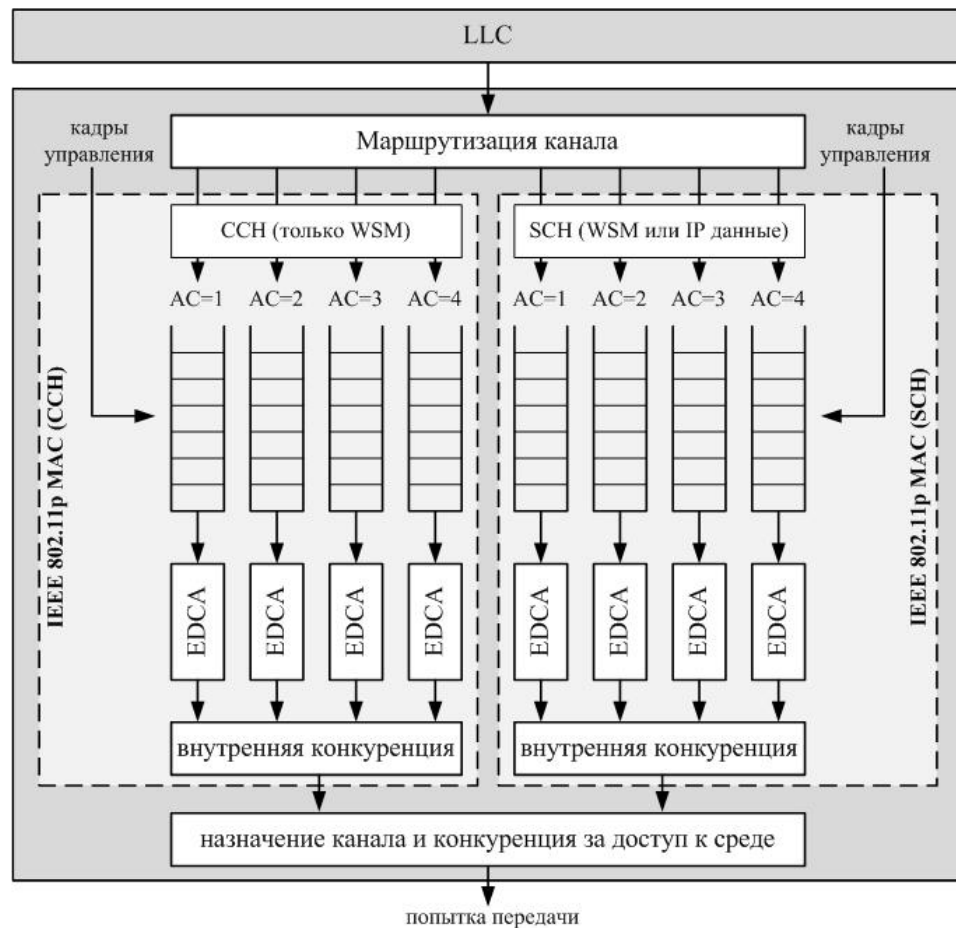


Рисунок 11 – Архитектура передающей части узла сети VANET

Среда WAVE подразумевает возможность передачи трех видов информации

- контрольные кадры – они реализуют функциональность, которая аналогично описана в стандарте IEEE 802.11, без каких-либо расширений;
- кадры данных;
- кадры управления – они передаются на любом из каналов, и рассчитаны чтобы передавать информацию о синхронизации, кроме это они нужны для объявления предлагаемых сервисов.

В данной выше архитектуре видно, что для данных, передаваемых с верхних уровней, поддерживается и WSM, и протокол IPv6. Но, в то же время, WSM передаются по любому из каналов, а IPv6 данные только по SCH. Реализация обмена WSM между узлами VANET считается в большей степени важным функционалом, который требует детального исследования, потому что, собственно, с помощью них передаются данные от приложений, связанных с БДД.

3 Обзор проектов VANET

3.1 Проект V2V Communication | NHTSA

Национальное управление безопасности дорожного движения на трассах NHTSA (National Highway Traffic Safety Administration) совместно с Министерством транспорта США DOT (US Department Of Transportation) создали семейство проектов, которые реализуют разного рода варианты введения VANET в систему управления дорожным движением США. Эти проекты решают две основные задачи, а именно: обеспечение кибербезопасности реализуемой сети VANET и обеспечение функционирования приложений по обеспечению безопасности дорожного движения. Для того, чтобы решить первую задачу, в каждом проекте применяется механизм передачи сообщений по связям V2V, созданный на специализированном протоколе передачи базовых сообщений безопасности и на основе беспроводных соединений 802.11p. Для того, чтобы обеспечить безопасность сети, применяется инфраструктура PKI. Для того, чтобы обеспечить связь между инфраструктурой выдачи сертификатов и сетью VANET, реализация предлагается одним из двух методов:

- связь мобильных узлов с инфраструктурой PKI по средствам RSU с использованием беспроводной связи стандарта 802.11p;
- связь мобильных узлов с инфраструктурой PKI по средствам инфраструктуры мобильной сотовой сети и сети спутниковой связи.

На рисунке 12 приведена архитектура безопасности проектов V2V, разработанных агентством NHTSA. Она реализует следующие механизмы:

- механизм сертификатов на основе PKI;
- анализ целостности сообщений с блокировкой узлов нарушителей;
- защита OBU от изменения режима функционирования;
- центр выдачи анонимных сертификатов (псевдонимов);
- прокси-сервер скрытия позиции узла (Location Obscure Proxy).

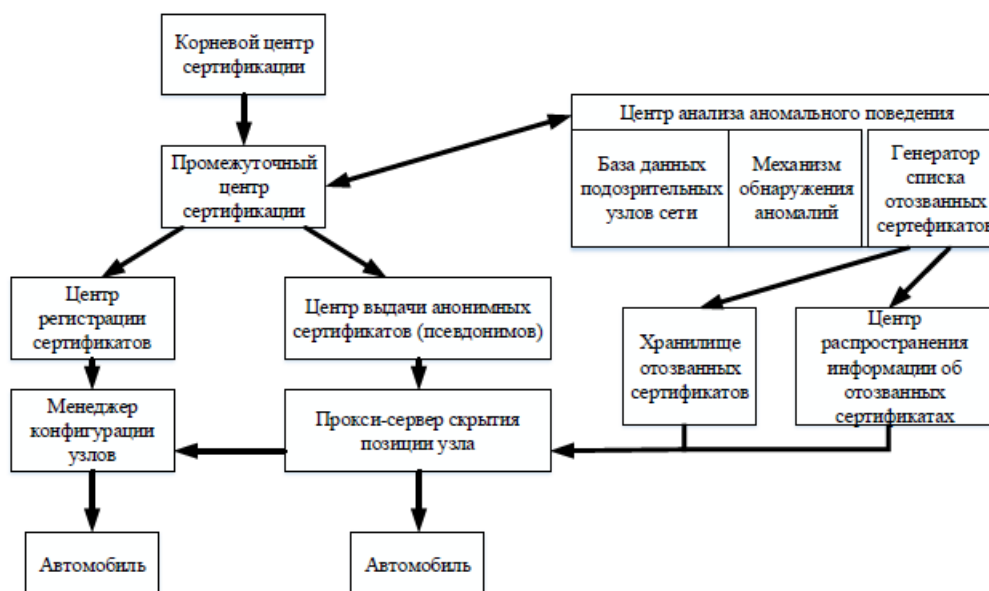


Рисунок 12 – Архитектура системы безопасности проекта V2VNHTSA

3.2 Проект NoW

NoW (Network on Wheels) является первым научно-исследовательским европейским проектом, ориентированный на применение VANET в системах безопасности дорожного движения. Во время этого проекта был разработан протокол Geocast – протокол маршрутизации на основе географического местоположения, позже использованный в стеке протоколов C-ITS.

Проект NoW использует архитектуру PKI в основе собственной архитектуры безопасности, которая описана в стандарте IEEE 1609. На рисунке 13 мы рассмотрим размещение механизмов безопасности по уровням сети на примере данного проекта.

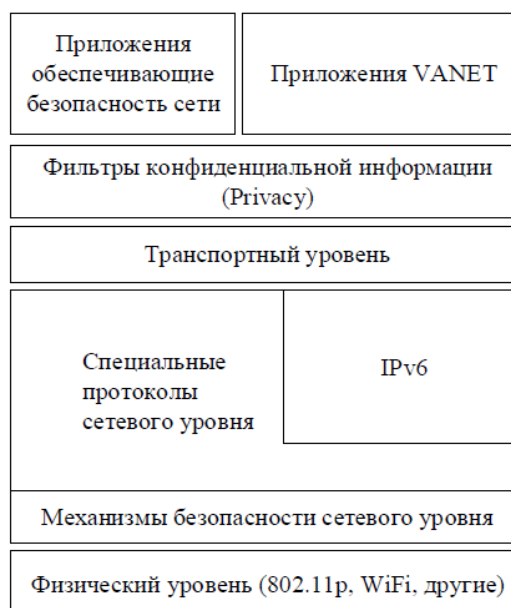


Рисунок 13 - Размещение механизмов безопасности по уровням сети проекта NoW

В проекте NoW реализуемые на сетевом уровне механизмы безопасности отвечают за контроль целостности передаваемых данных с помощью контроля попадания в заранее установленные границам значений и за шифрование сообщений.

Приложения, взаимодействующие с РКІ, реализуются на прикладном уровне с целью получения и обновления сертификатов. На прикладном уровне, кроме этого, фильтруются конфиденциальные данные.

3.3 Проект COMeSafety (Communications for eSafety)

COMeSafety – это европейский проект, направленный на интеграцию VANET в системы управления дорожным движением. Проект COMeSafety основывается на стеке протоколов C-ITS и помогает развитие проектов, которые реализуют приложения для данного стека протоколов (проекты GeoNet, PreVENT, CarTalk 2000).

В рамках проекта COMeSafety проводились полевые испытания проекта PRE-DRIVE C2X, направленные на исследования эффективности использования VANET в системах управления дорожного движения.

По ходу реализации этих проектов были сделаны контроллеры,

устанавливаемые в мобильные узлы (ITS Vehicle Station) и придорожные станции (ITS Roadside Station). ITS Station имеет модульную архитектуру. На рисунке 14 показана структура ITS Station. Она состоит из нескольких модулей приложений и модуля управления.

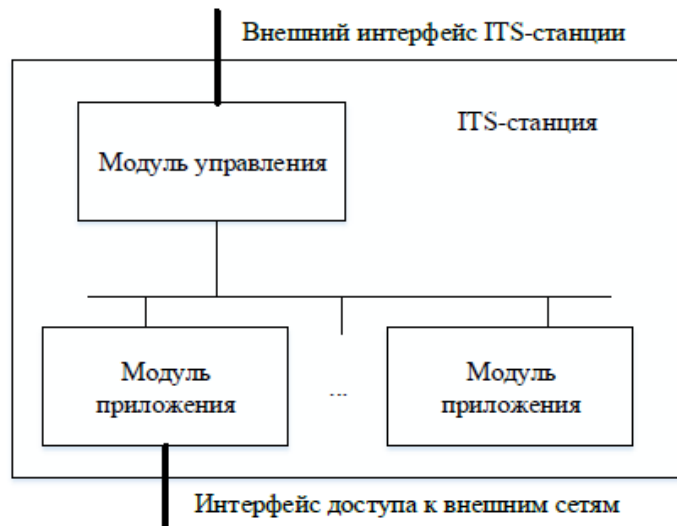


Рисунок 14 – Структура ITS Station

На рисунке 15 показана сеть из ITS станций в рамках данных проектов, разбиваемая на несколько подсетей:

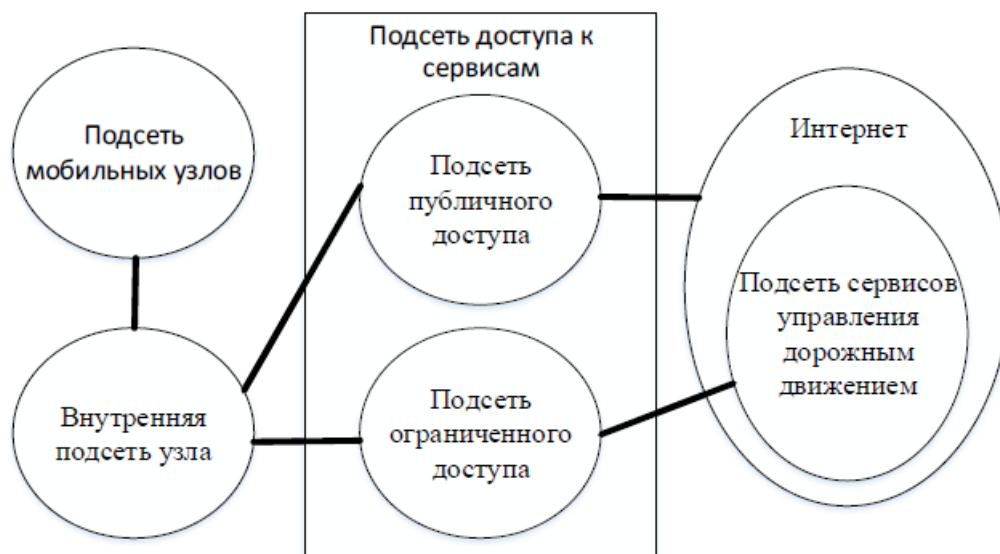


Рисунок 15 - Архитектура сети проекта COMeSafety

– подсеть мобильных узлов – это сеть, динамически образуемая придорожными станциями и мобильными узлами;

- внутренняя подсеть узла – это внутренняя сеть узла, обеспечивающая связь управляющего модуля с модулями приложений;
- подсеть доступа к сервисам – эта подсеть, в зависимости от требований к конфиденциальности, дополнительно разбивается на два уровня: подсеть публичного доступа к сервисам обеспечивает доступ к интернету, подсеть ограниченного доступа обеспечивает доступ к внутренним сервисам системы управления дорожным движением;
- подсеть сервисов управления дорожным движением.

Проект COMeSafety схож с архитектурой безопасности проекта NHTSA, в центре которой также лежит использование инфраструктуры PKI и доверенной аппаратной платформы. В дополнение к этому в архитектуре безопасности этого проекта возникает требование к механизму администрации ITS-станций. Процесс администрации предполагает перед выдачей идентификатора периодическую проверку исправности станций.

3.4 Проект AutoNet2030

Проект AutoNet2030 ориентирован на реализацию автономных транспортных средств благодаря реализации информационного обмена с датчиков между автономными автомобилями путём интеграции VANET в систему управления дорожным движением. Применение VANET нужно по причине того, что информации с датчиков одного автомобиля с целью организации его безопасного автономного движения недостаточно.

У проекта AutoNet2030 есть особенность по отношению к предыдущим аналогичным проектам, которые реализуют автономное безопасное движение автомобилей. Особенность заключается в том, что в проекте учтено в одно время езда на дороге и машин, оснащенных средствами автоматизации, и машин, которые управляются вручную. Проект AutoNet2030 выделяет три класса автомобилей по признаку оснащённости средствами автоматизации:

- автомобили, управляемые вручную (Legacy vehicles);

– автономные автомобили (Automated cooperative vehicles). Автомобили этого класса поддерживают функцию автономного движения, однако при этом могут управляться вручную, подобно автомобилям с системой оповещения водителя;

– автомобили, оснащённые системой совместного движения (Cooperative vehicles). Автомобили этого класса управляются вручную. Тем не менее, при этом, автомобиль обеспечен системой рекомендаций для водителя, регенерирующийся на основе информации от датчиков и сообщений от соседних автомобилей, передаваемых по VANET.

Автономные и кооперативные автомобили реализовывают обмен сообщениями о событиях дорожного движения. Автомобили этих классов способны организовываться в конвои и группы совместного режима круиз контроля C-ACC (Cooperative Adaptive Cruise Control). В проекте AutoNet2030, для организации управления описанными группами автомобилей, используются инфраструктурные базовые станции RSU и механизм выбора лидирующего автомобиля.

В проекте AutoNet2030 организация VANET сети базируется на стеке протоколов C-ITS. Адресация узлов возникает на уровне приложений в заголовках сообщений C-ITS. Данное решение вызвано использованием широковещательной рассылки без использования адресов в протоколе GeoNetworking.

3.5 Проект SARTRE

Европейский проект SARTRE (Safe Road Trains for the Environment) – является проектом компании Volvo, который реализует автоматический совместный круиз контроль нескольких автомобилей с использованием VANET. Тестируемые автомобили этого проекта имели право создавать группы (автомобильные поезда), движущиеся с одной скоростью. В то же время все автомобили в группе, за исключением ведущего, управлялись автоматически. Таким образом, организация потока автомобилей позволяет сократить

потребление топлива.

Этот проект использовал стандарт IEEE 802.11p для организации связи между автомобилями. Протоколы стека TCP/IP использовались на сетевом и транспортном уровне (рисунок 16).

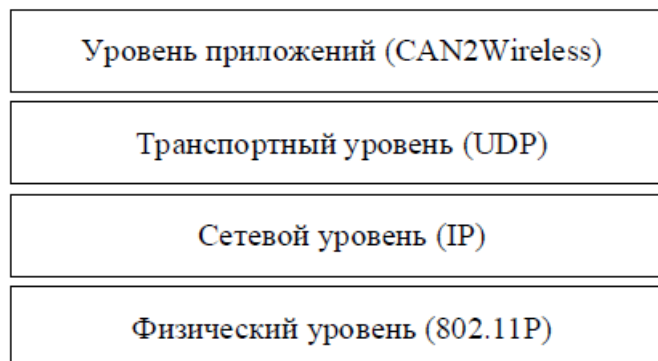


Рисунок 16 - Стек протоколов, используемых в проекте SARTRE

На уровне приложений применялся специализированный протокол CAN2Wireless, производящий широковегательную рассылку сообщений, полученных по внутренней сети микроконтроллеров (CAN) между участниками VANET сети. Чтобы уменьшить нагрузки на канал, связанной с использованием стека TCP/IP, в протоколе CAN2Wireless предусмотрена буферизация сообщений перед отправкой. На рисунке 17 показаны проекты, реализующие сеть VANET.

Название	Временные рамки	Используемые протоколы и стандарты
V2V NHTSA NoW	С 2016 года 2004-2008	802.11p, 4G LTE
COMeSafty	2006-2009, 2011-2014	Стек протоколов C-ITS
AutoNet2030	2013-2016	Стек протоколов C-ITS
SARTRE	2009-2012	802.11p, сетевой и транспортный уровень стека TCP/IP

Рисунок 17 - Проекты, реализующие сеть VANET

Главным недостатком существующих решений в области VANET считается отсутствие специализированного протокола сетевого уровня с поддержкой адресации узлов сети. Существующие решения, которые адаптируют сетевой уровень стека TCP/IP, не удовлетворяют требованиям для критических по

временным задержкам приложений. Параллельно, в связи с этим, используются альтернативные протоколы сетевого уровня, базирующиеся на широковещательной рассылке (WSM, GeoNetworking).

4 Применение VANET в России и мире

4.1 Применение VANET в ближайшие годы

В июне 2016 года ABI Research опубликовала прогноз, согласно которому к 2025 году около 67 млн автомобилей будут использовать сервисы 5G.

Три миллиона из них - самоуправляемые автомобили. Технология 5G, благодаря более быстрому отклику, станет предпочтительной для широкополосного потокового мультимедиа, отправки диагностической информации сервисному центру, использования в системах VANET.

Чтобы технология VANET стала реальностью, две области – автомобильная и телекоммуникационная, должны расширить зону охвата 5G-сигнала и обеспечить уверенный приём. ABI Research ожидает, что это станет вполне реальным к 2025 году. 5G позволит мобильным операторам внедрить больше услуг с добавленной стоимостью для автомобильной экосистемы. Аналитики ABI Research ожидают появления новых бизнес-моделей и новых возможностей для автомобильной отрасли благодаря низкой задержке при установке соединения – до 1 мс. Рисунок 18 – будущее межмашинного общения.



Рисунок 18 – Будущее межмашинного общения

Благодаря технологии VANET, подключенные автомобили в скором времени смогут сообщить водителю, что расположено впереди вне его поля

зрения. На 2017 год технология самоуправляемых автомобилей развивается настолько быстро, что трудно предсказать технические характеристики машин, которые будут сходиться с конвейера к концу следующего десятилетия.

Еще одним преимуществом VANET перед другими сенсорами является ее диапазон. Сотовые и Wi-Fi передатчики имеют гораздо больший диапазон, что позволяет им отправлять и получать данные намного раньше времени. Диапазон других датчиков примерно составляет от 15 метров (примерно 50 футов) до 75 метров (примерно 250 футов).

Ожидается, что беспроводная связь станет играть гораздо более важную роль, чем в 2017 году. В первую очередь, пассажиры в салоне получают новые сервисы, базирующиеся на доступе в интернет и определении местоположения, независимо от типа автомобиля: традиционного или которые перемещаются самостоятельно. Однако последний тип машин будет гораздо лучше осведомлен об окружающей обстановке, чем самые высокотехнологичные автомобили Tesla или элитные Mercedes Benz, что представлены на рынке сейчас.

Многие автомобили используют радар для предупреждения столкновений, а самоуправляемые автомобили для осуществления навигации по заданным маршрутам полагаются на камеры, радары и лидары (высокоточные датчики на основе отражения света от различных поверхностей). Технология позволит водителям и самоуправляемым автомобилям не только избежать столкновений, но также отправлять и получать все типы данных, чтобы помочь уравновесить городской трафик и сэкономить топливо. Беспроводная технология, также известная по сокращению VANET, получит наибольшее распространение.

4.2 Технологии компании Qualcomm

10 января 2020 года компания Qualcomm Technologies представила референсную платформу Qualcomm C-V2X для бортовых и придорожных блоков (RSU). Платформа Qualcomm C-V2X дополняет коммуникационные C-V2X (VANET) решения, предлагая необходимую вычислительную мощность для реализации полного спектра решений беспроводной связи 4G, 5G и C-V2X, таких

как мульти частотные сервисы GNSS для точного определения местоположения, обеспечение информационной безопасности, подписывание и верификация сообщений VANET, и стеки приложений VANET интеллектуальной транспортной системы. Платформа Qualcomm C-V2X базируется на архитектуре малой мощности Qualcomm Technologies, ее оптимизация для использования с программными приложениями направлена на ускорение развертывания бортовых C-V2X систем и придорожных блоков в США и других странах.

Характеристики и возможности платформы C-V2X:

- Платформа Qualcomm Snapdragon 2150, прикладной процессор Qualcomm Technologies разработаны для бортовых и придорожных блоков «умной» транспортной инфраструктуры;
- глубоко интегрированное VANET решение, включающее прикладной процессор, стек ITS, технологию Aerolink Security, подписывание сообщений, верификацию до 2500 сообщений в секунду, модем PC5/Uu, подключение Wi-Fi 6 и BT 5.1, MF-GNSS, поддержку сети контроллеров (controller area network, CAN);
- чистая архитектура с модульной, масштабируемой и современной схемой;
- поддержка безопасной изоляции доменов между C-V2X и телематическими стеками, и приложениями;
- поддержка функционала VANET, включая стеки ITS, решение безопасности Aerolink VANET с интегрированной верификацией и подписыванием сообщений.;
- оптимизированная связь с платформами Qualcomm Snapdragon Automotive 4G и 5G с интегрированной технологией C-V2X, включая одновременную связь по сети WWAN Uu и прямую передачу по каналу C-V2X PC5;
- драйверы модемного интерфейса и комплекты разработчика ПО для телематики и C-V2X ускоряют интеграцию и разработку приложений и сервисов;
- поддержка драйверов для Linux BSP;

– поддержка драйверов для аппаратных модулей безопасности сторонних производителей.

По информации компании, на январь 2020 года технология C-V2X глобально совместима с 5G и дополняет прочие датчики системы содействия водителю (Advanced Driver Assistance Systems, ADAS) такие, как видеокамеры, радары и лидары (Light Detection and Radar, LIDAR). Режим прямой связи C-V2X с низкой задержкой предназначен для непосредственной связи автомобилей друг с другом, дорожной инфраструктурой и пешеходами без использования сотовой сети в выделенном и гармонизованном ITS-диапазоне 5,9 ГГц.

Если говорить о перспективе бортовых и инфраструктурных решений, то платформы Snapdragon 4G и 5G одновременно поддерживают близкую связь C-V2X и дальнюю связь: Snapdragon 4G поддерживает технологию LTE, Snapdragon 5G — технологию 5G в диапазоне sub-6 ГГц. В одном референсном решении Qualcomm Technologies в сочетании с платформой Snapdragon 2150 поддерживается полный комплекс коммуникаций C-V2X, LTE и 5G, включая ближнюю связь, необходимую вычислительную мощность для верификации сертификатов и приложения VANET.

Полевые испытания с использованием решений Qualcomm Technologies продемонстрировали существенные преимущества прямой связи C-V2X с точки зрения дальности, надежности и производительности по сравнению со стандартом IEEE802.11p. Технология C-V2X показала более чем двукратное превосходство по дальности и, что самое главное, большую надежность. Кроме того, с учетом развития C-V2X в направлении 5G New Radio, эта технология предлагает более широкие и дифференцированные возможности.

4.3 Умные дороги в России

15 апреля 2020 года стало известно о появлении в России умных дорог, предупреждающих водителей о пешеходах и открытых люках поблизости. Такие пилотные проекты запущены в Курске, Волгограде и Самаре.

По его словам, технология призвана снизить на дорогах количество опасных ситуаций и ДТП с участием пешеходов, особенно в условиях плохой видимости (ночью, в дождь, туман). Интерес к этой системы проявили 20 регионов России, в том числе Красноярский край, Хабаровский край, Республика Башкирия, Калининградская и Пензенская области.

Система фиксирует вибрацию от пешеходов и открытых люков на дорогах и передает данные на бортовой компьютер через технологию VANET — она позволяет автомобилям взаимодействовать между собой и окружающей инфраструктурой. Кроме того, информация об открытых люках будет передаваться в систему «Безопасный регион».

Вся собранная информация будет храниться на платформе «Автодата». Речь идёт о данных об эксплуатации автомобиля, а также о внешней окружающей среде — качестве дороги, погодных условиях, географии использования.

По результатам обработки данных водители будут видеть процентное соотношение загруженности ряда на 500 м и 1 км. Технология позволяет определить точность расположения события до 1 м. Плотность определения — до 20 человек на 20 м участка обочины. Воспользоваться сервисом можно будет с помощью мобильного приложения.

ЗАКЛЮЧЕНИЕ

Беспроводная связь между транспортными средствами является объектом исследований как в научном сообществе, так и в автомобильной промышленности. Автомобильные сети VANET все больше развиваются, создавая большое поле для новых разработок и открытий.

Ежегодно во всем мире на дорогах совершается очень много дорожно-транспортных происшествий. От этого, к сожалению, никто не застрахован. Даже в ночное время суток на трассе, пешеход, переходя дорогу по зеленому сигналу светофора, может не увидеть быстро движущийся автомобиль. Водитель, в свою очередь, даже с включенными фарами на большой скорости не сразу заметит пешехода. VANET поможет, если не сократить число дорожно-транспортных происшествий, то хотя бы сократить их число. Поэтому сети VANET – это уникальное решение проблемы аварий, в случае которой могут быть летальные исходы.

По оценкам NHTSA США, если бы была внедрена система VANET, то число дорожно-транспортных происшествий сократилось бы минимум на 13%, что привело бы к снижению числа аварий на 439 000 человек в год.

Само развертывание технологии VANET будет происходить постепенно с течением времени. Новые автомобили будут оснащены любой из этих двух технологий примерно с 2020 года, и их доля на дорогах, как ожидается, будет постепенно увеличиваться. Volkswagen Golf 8-го поколения был первым легковым автомобилем, оснащенным технологией VANET. В то же время существующие транспортные средства будут продолжать существовать на дороге. Это означает, что транспортные средства с поддержкой VANET должны будут сосуществовать с другими транспортными средствами с этой технологией, или с транспортными средствами несовместимой технологии VANET.

Основными препятствиями для его принятия являются правовые вопросы и тот факт, что, если почти все транспортные средства не примут его, его эффективность будет ограничена.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сети связи пост-NGN / составители Гольдштейн Б.С., Кучерявый А.Е. – Санкт-Петербург 2014. – 160 с.
2. Исследование и разработка моделей и методов распределения широкополосного трафика в сетях VANET/ составитель Ярцев С.В. – Самара, 2018. – 203 с.
3. Противодействие информационным угрозам VANET-сетям на основе аппарата фрактальных графов / составитель Иванов Д.В. – Санкт Петербург, 2018. – 133 с.
4. Архитектуры построения защищенных транспортных сетей на основе технологии SDN / составитель Калинин М.О – Санкт Петербург, 2017. – с. 53-61.
5. Особенности развития и текущие проблемы автомобильных беспроводных сетей VANET / составитель Ярцев С.В. – Санкт Петербург, 2009. – с. 24-28.
6. Сайт <http://www.tadviser.ru/>
7. Сайт <http://vestnik-glonass.ru/>
8. Сайт https://en.wikipedia.org/wiki/IEEE_802.11p
9. СТО ЮУрГУ 19–2008 Стандарт организации. Выпускная квалификационная научно-исследовательская работа студента. Структура и правила оформления / составители: Т.И. Парубочая, Н.В. Сырейщикова, С.Д. Ваулин, В.Р. Гофман. – Челябинск: Изд-во ЮУрГУ, 2008. – 29 с.
10. ГОСТ 2.105-95 ЕСКД «Общие требования к текстовым документам». – М.: Изд-во стандартов, 1998. – 29 с.