

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК _____

Шеремет
Анастасия Геннадьевна

Модели обработки вызовов в инфокоммуникационных сетях

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-45 80 02 Телекоммуникационные системы и
компьютерные сети

Научный руководитель

Цветков Виктор Юрьевич

Кандидат технических наук, доцент

Минск 2015

ВВЕДЕНИЕ

Одним из наиболее перспективных направлений в развитии систем беспроводного доступа являются сети транспортных средств VANET (Vehicular Ad Hoc Network). Сети VANET принадлежат классу мобильных Ad Hoc сетей MANET (Mobile Ad Hoc Network), хоть им присущ и ряд особенностей, как с точки зрения применения, так и с точки зрения протоколов. Следует заметить, что, несмотря на название VANET, в этих сетях предусматривается не только режим функционирования Ad Hoc, но и комбинированный, когда элементы сети VANET могут соединяться с инфраструктурными узлами сети. Кроме того предусматривается широкое использование сенсоров для сбора различной информации в сетях автомобильного транспорта. Создание сетей VANET имеет вполне ясную коммерческую составляющую.

Сеть VANET является одной из базовых составляющих интеллектуальной транспортной системы (ИТС), в состав которой наряду с VANET также входят Спутниковые системы позиционирования (ГЛОНАСС, GPS, GALILEO), сотовые сети связи разных стандартов, придорожная инфраструктура, системы взаимодействия и оплаты на основе протокола DSRC (Dedicated Short Range Communications), системы экстренного вызова в случае аварийных ситуаций e-call и ЭРА-ГЛОНАСС.

Интеллектуальная транспортная система является симбиозом сетей связи и информационных возможностей транспортных средств и систем управления автомобильным движением.

В данной работе рассматриваются модели обработки вызовов сети VANET, как разновидности инфокоммуникационной сети. В инфокоммуникационных сетях “вызов” рассматривается как запрос на получение доступа к инфокоммуникационной услуге. Доступ к данным услугам осуществляется по средствам протоколов маршрутизации. Таким образом, протоколы маршрутизации можно рассматривать как модели обработки вызовов в инфокоммуникационных сетях.

Настоящая работа посвящена изучению протоколов маршрутизации (OLSR, AODV, DSDV) и оценке их эффективности для выбора наиболее подходящей модели обработки вызовов в сети VANET, а также разработка рекомендаций по обеспечению безопасности беспроводных одноранговых сетей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы: в настоящее время интенсивно развивается направление по разработке инфокоммуникационных систем (ИКС) с динамической топологией сети (ДТС), которые обеспечивают передачу информации непосредственно между подвижными объектами (людьми, автомобилями, более крупным транспортом). Примером реализации ИКС с ДТС стали VANET системы. Они предназначены для повышения эффективности и безопасности дорожного движения. В настоящее время при поддержке индустрии, государственных и академических институтов в мире выполняются несколько научно-исследовательских проектов, направленных на разработку и принятие стандартов таких автомобильных сетей.

Целью данной работы является изучению протоколов маршрутизации (OLSR, AODV, DSDV) и оценка их эффективности для выбора наиболее подходящей модели обработки вызовов в сети VANET, а также разработка рекомендаций по обеспечению безопасности беспроводных одноранговых сетей.

При выполнении работы применялся сетевой симулятор NS-3, который обеспечивает надежность и корректность расчетов характеристик телекоммуникационного трафика.

В ходе выполнения исследований была разработана сеть VANET в среде NS-3. Для того чтобы приблизить моделируемую сеть к реальным условиям окружающей сети, были использованы различные модели потерь распространения сигналов и сравнивалась работа вышеуказанных протоколов в различных условиях. Так как контекст окружающей среды сильно влияет на эффективность радиоволн из-за потерь на трассе, затухания, экранирования, которые сильно отличаются между окружающей обстановкой пригородных, городских и магистральных транспортных сетей. Так же проводились исследования работы данных протоколов маршрутизации при изменении скорости движения и количества узлов сети. По результатам исследований можно сделать вывод, что в качестве протокола маршрутизации VANET может быть использован AODV, то есть реактивный протокол.

Так как для всех беспроводных самоорганизующихся сетей связи одной из важных является задача обеспечения информационной безопасности, в данной работе предложены рекомендации для многоуровневой системы защиты беспроводной мобильной ячеистой сети с учетом гибридной эталонной модели взаимодействия открытых систем.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, четырех глав, заключения (выводов) и приложения. Объем диссертационной работы: 54 страницы.

Во введении обоснована актуальность темы, описаны цели и задачи работы.

В первой главе “Инфокоммуникационные сети” изложено описание принципа работы инфокоммуникационных сетей, особенностей инфокоммуникационных услуг и предъявляемых к ним требований. Также представлена модель когнитивной инфокоммуникационной системы и определены ключевые функции для ее пяти подсистем. Если инфокоммуникационную систему образует совокупность сети телекоммуникаций (телекоммуникационной подсистемы), прикладной подсистемы (средств хранения и обработки информации, прикладных процессов), а также подсистемы источников и потребителей информации (пользовательские подсистемы), то когнитивная инфокоммуникационная система дополнительно включает в себя элементы, обеспечивающие функциональность когнитивной системы (элементы ментальной деятельности, функции мониторинга, сбора информации, исполнительные устройства и др.) во всех перечисленных подсистемах.

Во второй главе под названием “VANET как инфокоммуникационная сеть” даются определение и основные характеристики беспроводных одноранговых сетей. Перечислены отличительные особенности технологии VANET, которая является одним из наиболее перспективных направлений в развитии систем беспроводного доступа, и принадлежащей классу MANET.

Для всех беспроводных самоорганизующихся сетей связи одной из важных является задача обеспечения информационной безопасности. Поэтому во второй главе описаны приведены особенности угроз информационной безопасности VANET, а также перечислены характерные типы нарушителей, которые могут быть причиной угроз информационной безопасности в данной сети.

Третья глава “Протоколы маршрутизации VANET”. В ней представлена классификация протоколов маршрутизации в ad-hoc сетях, а также более подробно описаны наиболее популярные при построении современных Ad-Hoc сетей протоколы AODV, OLSR и DSDV, эффективность которых исследуется в четвертой главе настоящей работы.

В четвертой главе “Оценка эффективности протоколов маршрутизации VANET при помощи NS-3” приведены результаты исследования протоколов маршрутизации VANET. Здесь дается

обоснование выбора среды моделирования сети – сетевого симулятора NS-3. Также представлены основные параметры и исходные данные моделируемой сети, приводится описание моделей распространения потерь, используемых в NS-3 для создания реалистичных условий распространения сигналов (потери, затухания, отражения радиоволн от различных поверхностей и тому подобное). В настоящей работе используются различные модели распространения потерь, чтобы максимально приблизить имитируемую сеть к условиям реальной окружающей среды, и сравнивается эффективность протоколов маршрутизации AODV, OLSR и DSDV для VANET при различных условиях (исследовались такие параметры как отношение доставки пакетов, пропускная способность, задержка распространения пакетов). Для эксперимента были выбраны следующие модели: Friis Propagation Model, Two Ray Ground Model, Log Distance Path Loss Model, Random Propagation Loss, Three Log Distance Model, Maximal Range, которые наиболее подходят для моделирования VANET. Исследования эффективности работы вышеупомянутых протоколов также при изменении скорости движения узлов сети (15, 20, 25, 30 м/с – скорости движения автомобилей в условиях городской транспортной сети) и при изменении количества узлов сети. По результатам измерений видно, что отношение доставки пакетов (PDR) выше у реактивных протоколов (AODV), а значение задержки доставки пакетов лучше у проактивных.

В данной главе также представлены рекомендации для многоуровневой системы защиты беспроводной мобильной ячеистой сети с учетом гибридной эталонной модели взаимодействия открытых систем.

В заключении подводятся итог проделанной работы, сделаны выводы по полученным результатам исследований.

В приложении размещен программный код моделируемой сети в сетевом симуляторе NS-3.

ЗАКЛЮЧЕНИЕ

Развитие сетей телекоммуникаций является элементом общего процесса развития общества и тесно взаимосвязано практически со всеми процессами, происходящими в общественных отношениях, науке и технике, промышленности и других областях деятельности человека. Рост потребности в информационном обмене и его значимости в жизни обеспечивает благоприятные условия для развития и внедрения новейших технологий в сетях телекоммуникаций. Последние, в свою очередь, также оказывают влияние на процессы, происходящие в жизни и деятельности человека. В ходе эволюционного развития изменяются объемы передаваемой информации, виды ее представления, способы передачи и хранения, численность источников и потребителей, распределение между пользователями, требования к своевременности и достоверности (качеству). Рост значимости информации в жизни общества, а также развитие средств ее передачи, обработки и хранения приводят к усилению роли инфокоммуникационной системы, то есть области деятельности, включающей все информационные объекты (пользователи и другие источники и потребители информации) и средства и способы доставки информации (телекоммуникационные системы).

В настоящее время интенсивно развивается направление по разработке инфокоммуникационных систем с динамической топологией сети, которые обеспечивают передачу информации непосредственно между подвижными объектами (людьми, автомобилями, более крупным транспортом). Примером реализации такой сети стали VANET системы.

В данной работе были рассмотрены протоколы маршрутизации в VANET (AODV, OLSR, DSDV), а также исследована эффективность их работы при различных условиях окружающей среды, различных скоростях движения узлов сети и при изменении количества узлов сети. В качестве среды моделирования был выбран сетевой симулятор ns-3, где была смоделирована сеть, максимально приближенная к VANET.

По результатам исследования можно сделать выводы, что при небольшом количестве узлов все рассмотренные протоколы показали неплохой процент доставки пакетов, однако, AODV показал результаты лучше, чем проактивные протоколы. Причиной является невозможность реконструкции маршрута, в случае обрыва связи у протоколов OLSR и DSDV. При увеличении количества узлов в сети видно, что пропускная способность всех протоколов снизилась, однако стоит отметить, что на больших скоростях лучшие результаты показал протокол AODV, а на низких – OLSR и DSDV. При исследовании задержки распространения

пакетов, следует отметить, что независимо от количества узлов в сети и скорости движения узлов, проактивные протоколы превосходят реактивные. Причина состоит в том, что табличные протоколы маршрутизации, не должны находить маршрут прежде, чем передать пакеты. Таким образом, задержка доставки пакетов довольно стабильна. А реактивные протоколы подвергаются дополнительной задержке из-за процедуры нахождения маршрута.

Важной проблемой для VANET также является обеспечение безопасности. В данной работе дана рекомендации по обеспечению безопасности на всех уровнях (физическом, передачи данных, сетевом, транспортном, прикладном) гибридной модели взаимодействия открытых систем. На физическом уровне для противодействия средствам радиоэлектронной борьбы предлагается использовать смарт-антенны, на уровне передачи данных – протоколы с шифрованием, например WEP в сетях Wi-Fi. На сетевом уровне следует использовать протокол IPv6, содержащий элементы повышения сетевой безопасности. Протоколы маршрутизации для опорной сети, работающие на уровне передачи данных или сетевом должны содержать средства проверки подлинности, целостности обновлений и их шифрование. В случае необходимости для важной части трафика следует задействовать VPN на основе IPSec. Защита на транспортном уровне возможна за счет протоколов TLS/SSL или решений на их основе (OpenVPN, SSH и др.).

Проведенный предварительный анализ эффективности использования протоколов маршрутизации инфокоммуникационных систем с динамической топологией сети для обслуживания транспортных объектов (VANET), показал, что AODV может быть использован в качестве протокола маршрутизации в VANET.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Юревич, А.А. Модели сети передачи данных группировки беспилотных летательных аппаратов / А.А. Юревич, А.Г. Шеремет, Ю.Ф. Яцына // Актуальные вопросы науки и техники в сфере развития авиации: Тезисы докладов IV Междунар. н.-т. конф. авиационного факультета УО «Военная академия Республики Беларусь» 15-16 мая 2014 г., Минск. – Минск: ВА РБ, 2014. – С. 213.

2. Юревич, А.А. Построение многоуровневой системы защиты беспроводной мобильной ячеистой сети с учетом гибридной эталонной модели взаимодействия открытых систем / А.А. Юревич, А.Г. Шеремет // технические средства защиты информации: Тезисы докладов XII Бел.-рос. н.-т. конф. 28-29 мая 2014 г., Минск. – Минск: БГУИР, 2014. – С. 40.

Библиотека БГУИР