На правах рукописи

Иванов Денис Вадимович

ПРОТИВОДЕЙСТВИЕ ИНФОРМАЦИОННЫМ УГРОЗАМ VANET-СЕТЯМ НА ОСНОВЕ АППАРАТА ФРАКТАЛЬНЫХ ГРАФОВ

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Санкт-Петербург – 2018

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО СПбПУ) на кафедре «Информационная безопасность компьютерных систем».

Научный руководитель:
Москвин Дмитрий Андреевич, кандидат технических наук.

Официальные оппоненты:
Присяжнюк Сергей Прокофьевич,
доктор технических наук, профессор, генеральный директор ЗАО «Институт телекоммуникаций».

Сухопаров Михаил Евгеньевич,
кандидат технических наук, старший научный сотрудник лаборатории Интеллектуальных систем ФГБУН «Санкт-Петербургский институт информатики и автоматизации Российской академии наук».

Ведущая организация:
ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения».

Защита состоится "___" декабря 2018 г. в __ ч. на заседании диссертационного совета Д 212.229.31 на базе ФГАОУ ВО СПбПУ по адресу: 195251, Санкт-Петербург, ул. Политехническая, 29, ауд. 175.

С диссертацией и авторефератом можно ознакомиться в библиотеке и на сайте ФГАОУ ВО СПбПУ (www.spbstu.ru).

Автореферат разослан "___" октября 2018 г.
Отзыв на автореферат в двух экземплярах, заверенный печатью организации, просим направлять по адресу ученого совета университета.

Ученый секретарь
диссертационного совета Д 212.229.31,
кандидат технических наук,
доцент Супрун Александр Федорович

Общая характеристика работы

Актуальность. Информационные технологии давно проникли в самые различные сферы человеческой жизни. Практически любой современный бизнес-процесс автоматизирован и выполняется компьютером: документооборот, логистика, денежные переводы, различные технологические процессы, все эти процессы переданы под контроль вычислительным системам. Такая тенденция сохраняется, и масштабы повсеместной автоматизации продолжают расти. Вместе с масштабами сетей растет и сложность контроля над ними, процесс администрирования крупных разнородных сетей требует все больше ресурсов для мониторинга, выявления и предотвращения возможных деструктивных информационных воздействий на них.

Таким образом, современная инфраструктура нуждается в инструментарии, выстраивающим упорядоченный процесс мониторинга, управления и реакции на отклонения в работе крупномасштабных сетей.

Одним из перспективных видов таких крупномасштабных сетей являются сети транспортных средств VANET (Vehicular Ad-hoc Networks). Технология VANET является расширением технологии беспроводных самоорганизующихся сетей (Ad-hoc), где в качестве приемника и передатчика информации выступают автомобили. Основной задачей таких сетей является повышение эффективности и безопасности дорожного движения за счет:

- помощи водителю (навигация, предотвращение столкновений);
- информирования (об ограничении скорости, зонах ремонтных работ);
- предупреждения (послеаварийные, о состоянии дорог).

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.

Специфика VANET-сетей проявляется в динамической природе сети, что ведет к необходимости разработки специальных механизмов обеспечения безопасности.

Проблеме обеспечения информационной безопасности VANET-сетей посвящено множество исследований российских и иностранных ученых, таких как Р.А. Бельфер, М.О. Калинин, Д.П. Зегжда, Е.А. Кучерявый, М. Герлах, Х. Хасруни, Г. Гуйет. Предлагаемый автором подход развивает существующую методологию обеспечения

безопасности VANET-сетей в части децентрализации и основывается на применении теории фрактальных графов. Такой подход позволяет выявлять самоподобные характеристики сети, в противном случае сигнализируя об аномалии в работе сети с целью дальнейшего исследования причин ее возникновения.

Объектом исследования являются автомобильные сети связи VANET, в отношении которых осуществляются информационные деструктивные воздействия.

Предметом исследования являются подходы и методы противодействия информационным угрозам VANET-сетям.

Целью работы является обеспечение защищенности VANET-сетей на основе автоматизированного противодействия информационным угрозам безопасности путем саморегуляции структуры сети с использованием теории фрактальных графов.

Для достижения поставленной цели в работе решались следующие задачи:

1. Исследование специфики построения VANET-сетей и применяемых в них механизмов безопасности.
2. Разработка модели угроз VANET-сетям на основе графового представления.
3. Разработка метода автоматизированной саморегуляции структуры сети на основе теории фрактальных графов и его исследование с использованием имитационной модели VANET-сети.
4. Разработка методики проверки защищенности VANET-сетей от информационных угроз сетевого уровня.
5. Построение архитектуры и разработка прототипа децентрализованной системы, реализующей предложенную методику проверки защищенности.

Научная новизна диссертационной работы состоит в следующем:

1. Впервые предложено для предотвращения угроз VANET-сетей использовать теорию фрактальных графов.
2. Сформулирована теорема о необходимом условии достижимости состояния защищенности от угроз сетевого уровня в VANET-сетях.
3. Для оценки топологических характеристик сети разработана система рекурсивной адресации узлов.
4. Разработана методика проверки защищенности VANET-сетей от информационных угроз сетевого уровня на основе теории фрактальных графов.

Теоретическую значимость работы составляет представление VANET-сети в виде предфрактального графа, разработка метода автоматизированной саморегуляции структуры и определение условий защищенности сети.

Практическая значимость. Полученные основные научные результаты диссертационного исследования используются при реализации ПНИЭР "Исследование и разработка технологии автоматического управления кибербезопасностью в крупномасштабных коммуникационных сетях беспилотного транспорта на базе суперкомпьютерных эластичных вычислений" ФЦП "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы" Министерства образования и науки Российской Федерации (соглашение №14.578.21.0224, уникальный идентификатор соглашения RFMEFI57816X0224).

Результаты исследования используются в рамках проектной деятельности ООО Научно-производственное предприятие «Новые технологии телекоммуникаций» для исследования и разработки перспективных телекоммуникационных решений, направленных на развитие эффективности и безопасности беспроводных сетей связи.

Результаты работы применяются в практической и исследовательской деятельности ООО «Технологии автоматизации и программирования» для развития направления обеспечения информационной безопасности беспроводных самоорганизующихся сетей связи.

Методы исследования. Для решения поставленных задач использовались теория графов, теория фракталов, теория алгоритмов, методы компьютерного моделирования, математической статистики и теория защиты информации.

Положения, выносимые на защиту:

1. Модель угроз безопасности VANET-сетям.
2. Метод автоматизированной саморегуляции структуры сети на основе теории фрактальных графов.
3. Условия защищенности VANET-сети от информационных угроз, основанные на сохранении фрактальных свойств ее топологии.
4. Теорема о необходимом условии достижимости состояния защищенности от угроз сетевого уровня в VANET-сетях.

5. Децентрализованная архитектура VANET-сети, способная поддерживать защищенное состояние в условиях информационных угроз.

Соответствие специальности научных работников. Диссертация соответствует специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» отрасли технических наук – пп. 3, 9 раздела 2 «Области исследования» паспорта специальности: «Методы и модели выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса»; «Модели и методы оценки защищенности информации и информационной безопасности объекта».

Степень достоверности результатов исследования подтверждается их внутренней непротиворечивостью и адекватностью физическим представлениям об исследуемом объекте.

Апробация работы. Основные результаты исследований и научных разработок обсуждались на конференциях: международная конференция International Conference on Security of Information and Networks, SIN 2015, научно-техническая конференция «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2014, 2017 и 2018 гг.). Работа победила в конкурсе грантов Правительства Санкт-Петербурга для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга, в 2014 году.

Публикации по теме диссертации. Результаты диссертационной работы отражены в 14 публикациях, в том числе 4 публикациях в издании из перечня РИНЦ, 6 публикаций в рецензируемых журналах из перечня ВАК, 2 публикаций в изданиях из перечня Scopus.

Объем и структура диссертации. Диссертация состоит из введения, пяти глав, заключения и списка литературы из 93 наименований. Общий объем работы составляет 133 страницы, в том числе 60 рисунков и 6 таблиц.

Содержание работы

Во введении обоснована актуальность темы диссертационного исследования, сформулированы и обоснованы цель и задачи исследования, определена научная новизна и положения, выносимые на защиту.

В первой главе исследуется специфика построения VANET-сетей и применяемых в ней механизмов безопасности. Анализируются особенности архитектуры VANET-сетей, а также существующие стандарты построения и безопасности, применяемые в подобных сетях. Также рассматриваются существующие проекты VANET-сетей и используемые в них механизмы безопасности.

Основным недостатком существующих проектов с точки зрения обеспечения безопасности является применение механизмов, работа которых возможна исключительно в условиях централизованной архитектуры. Построение VANET-сетей с централизованной архитектурой противоречит основной идее создания одноранговых сетей и превращает их в традиционные сети передачи данных. Присутствие в сети отдельных выделенных узлов и серверов, отвечающих за функции обеспечения безопасности, делает узлы основными целями кибератак, в результате реализации которых отказ в обслуживании одного центрального сервера приводит к нарушению функционирования всей сети. Например, использование централизованной инфраструктуры PKI для организации аутентификации ведёт к необходимости защиты инфраструктуры PKI, которая становится критическим элементом функционирования сети.

Также в рассмотренных проектах не предусмотрены механизмы обеспечения контроля доступности на сетевом уровне сети, что может привести к использованию нарушителями уязвимостей в протоколах маршрутизации и отказу в обслуживании узлов сети VANET.

Механизмы обнаружения аномального поведения, описываемые в рассмотренных проектах, базируются только на анализе целостности сообщений, что позволяет выявлять узкий класс атак. В свою очередь подходы к анализу целостности носят вероятностный характер, из-за чего возможно появление ошибок первого и второго рода.

Во второй главе описана разработка модели угроз VANET-сетям. В целях формирования систематизированного перечня угроз безопасности VANET-сетей построена их классификация.

Анализ источников, посвященных выявлению наиболее актуальных и специфичных для VANET-сетей угроз безопасности, позволил определить множество

таких угроз. Все выявленные угрозы распределены по группам в соответствии с разработанной классификацией.

Наибольший интерес с точки зрения целей и задач исследования представляют угрозы, реализуемые на сетевом уровне, т.е. угрозы, направленные на вмешательство в работу протоколов маршрутизации и принципов адресации узлов сети. Кроме того, этот класс угроз традиционно считается наиболее специфичным и актуальным для любых Ad-hoc сетей. Угрозы, реализуемые на нижних уровнях стека протоколов, влияют и воздействуют на саму природу сигнала и низкоуровневые характеристики передаваемых данных, и не являются специфичными для VANET-сетей, в связи с чем для защиты от этих угроз возможно использование существующих методов и подходов.

Обеспечение защиты сети от угроз, реализуемых на уровне приложений, напрямую зависит и базируется на методах и механизмах обеспечения безопасности на более низких уровнях (в том числе сетевом).

Таким образом, наиболее важным с точки зрения обеспечения безопасности VANET-сетей является сетевой уровень, защита которого должна строиться, в первую очередь, не за счет различных надстроек над существующими уязвимыми протоколами, а за счет разработки алгоритмов маршрутизации и подходов к построению киберустойчивой архитектуры сети, способной самостоятельно и адаптивно реагировать на возможные информационные угрозы.

К угрозам, реализуемым на сетевом уровне, относятся угрозы «множественной идентификации», «имперсонации», «Black hole», «Gray hole», «пересылки сообщений по выделенному каналу», «фальсификации параметров маршрутизации».

При этом основными причинами появления и существования угроз безопасности VANET-сети на сетевом уровне являются:

– невозможность проверки и мониторинга состояния каждого вновь прибывшего узла в условиях отсутствия централизованных серверов аутентификации;

– отсутствие сегментирования инфраструктуры;

– маршруты передачи данных оптимизируются исключительно по длине, без учета требований безопасности.

В третьей главе описывается метод автоматизированной саморегуляции VANET-сети с фрактальной топологией. Метод основывается на подходах и

алгоритмах к построению, адресации и маршрутизации в предфрактальных структурах, описанных в разделе 3.1. Под термином «саморегуляция» подразумевается способность сети к перестроению своей топологии без нарушения фрактальности, а также способность к построению оптимальных маршрутов на основе описанного алгоритма маршрутизации. В данном разделе описывается процесс построения VANET-сети с предфрактальной топологией.

Предфрактальным графом называется граф, образованный с использованием рекурентного применения операции замены вершины затравкой (ЗВЗ) на каждом шаге роста его траектории для каждой из вершин графа.

Затравкой называется любой связный граф $H(W, Q)$, где W – множество вершин графа, а Q – множество ребер, из которого будет получаться новый – предфрактальный граф. Появление нового предфрактального графа возможно в результате операции ЗВЗ.

Вводятся два типа ЗВЗ, отличие между которыми заключается в применении одной из операций: добавление вершины (1)

$$A: H(W, Q) \to H'(W', Q'), \quad (1)$$

где $W' = W \cup w'$, $Q' = Q \cup q'$;

или подразбиение ребра (2)

$$B: H(W, Q) \to H''(W'', Q''), \quad (2)$$

где $W'' = W \cup w''$, $Q'' = (Q \,/\, q) \cup q''_1 \cup q''_2$.

ЗВЗ(А) инициирует рост предфрактального графа «наружу», а при использовании ЗВЗ(В) граф растет «внутрь». С точки зрения формального описания графов это различие можно сформулировать следующим образом: если после операции ЗВЗ у вершин первоначального графа не изменились степени связности, то граф вырос «внутрь», иначе – граф вырос «наружу».

После описания процесса построения VANET-сети с предфрактальной топологией предлагается система рекурсивной адресации узлов сети. Суть подхода к адресации (индексации) предфрактальных графов состоит в возможности присвоения каждой вершине затравки уникального адреса (индекса). Затем, используя свойство самоподобия фрактальных графов, возможно присвоить каждому подграфу-затравке предфрактального графа второго порядка те же идентификаторы. Повторяя эту операцию для вершин вновь образованных затравок на каждом шаге траектории роста

предфрактального графа, каждая вершина будет иметь уникальный индекс. Уникальный индекс вершины образуется в результате конкатенации индексов, полученных на каждом шаге роста траектории предфрактального графа. Разряды индекса, начиная с некоторой позиции, могут быть равны «0», это означает, что, начиная с некоторого шага траектории, над вершиной более не производилась операция ЗВЗ. Пример проиндексированного предфрактального графа третьего порядка, в котором над вершиной с индексом «bb0» операция ЗВЗ не производилась, начиная с третьего шага траектории, а для вершины «d00», начиная со второго, представлен на рисунке 1.

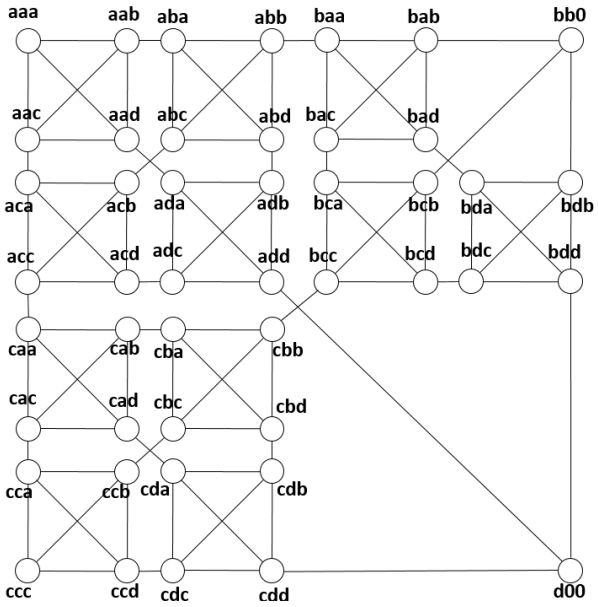

Рисунок 1 — Проиндексированный предфрактальный граф третьего порядка

Далее предлагается алгоритм маршрутизации в VANET-сетях с предфрактальной топологией. Для перехода из одного сегмента X в другой сегмент Y необходимо на каждом шаге перемещаться в вершину *y внутри затравки, а затем в единственную соседствующую затравку. Под сегментом понимается предфрактальный граф образованный на предыдущем шаге траектории роста. Например, в предфрактальном графе n-го порядка, представленном на рисунке 2, для того чтобы добраться до сегмента, например, D, из любого другого сегмента (A, B, C), необходимо добраться до единственного ребра, соединяющего эти сегменты, т.е. «add..», «bdd..», «cdd..». В свою очередь, для этого необходимо добраться до сегмента D в подграфе предыдущего порядка, и так далее.

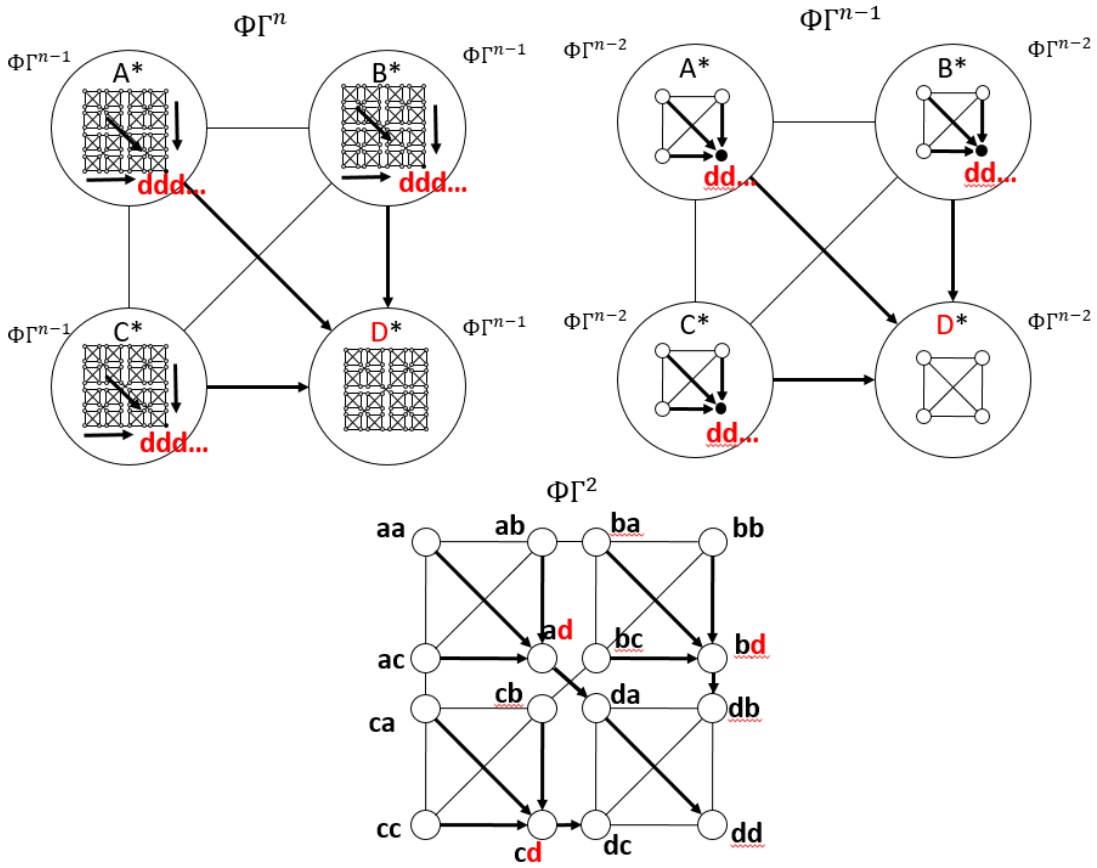

Рисунок 2 – Процесс перехода из одного сегмента в другой для предфрактального графа

Метод саморегуляции VANET-сети должен применяться при любом изменении в топологии сети (добавлении, удалении узла) и заключается в следующем:

1. Выявление узла (узлов) не входящих в структуру предфрактального графа.
2. Определение информации, необходимой узлу, чтобы он смог стать частью предфрактального графа (войти в новый подграф-затравку).
3. Связь узла с другими узлами графа, выявление висячих узлов и выбор способа их включения в предфрактальный граф.
4. Перестроение индексов узлов предфрактального графа.
5. Построение маршрутов согласно разработанному алгоритму маршрутизации.

Таким образом, метод саморегуляции VANET-сети с фрактальной топологией включает построение, адресацию и маршрутизацию узлов сети, гарантирующую сохранение фрактальных свойств на каждом шаге роста графа.

Работоспособность и состоятельность метода подтверждена опытным путем с использованием разработанной имитационной модели. График зависимости процента вошедших в сеть с предфрактальной топологией узлов от количества машин на участке дорожной карты для различных затравок представлен на рисунке 3.

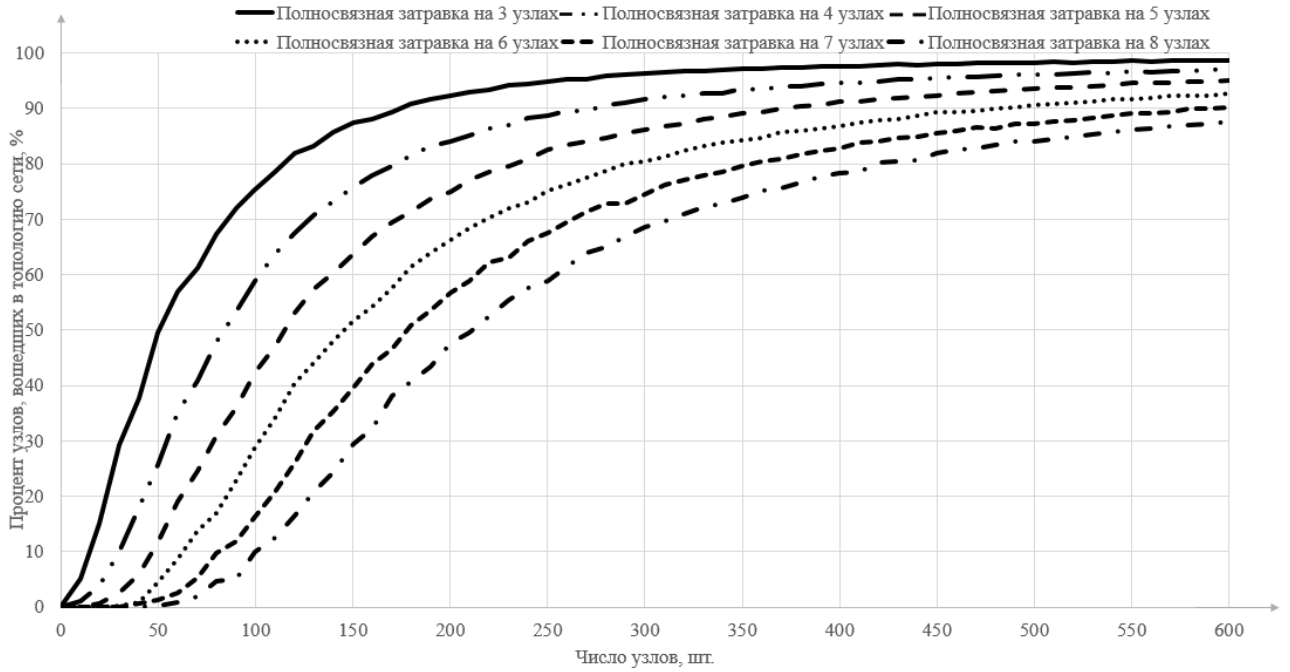

Рисунок 3 – График зависимости доли вошедших в сеть с предфрактальной топологией узлов от количества машин на участке дорожной карты для различных видов затравки

Результаты позволяют сделать вывод о том, что при наличии на участке небольшого количества автомобилей предпочтительно использовать небольшие затравки, при увеличении количества автомобилей можно увеличивать количество вершин в затравке, повышая реберную связность графа сети.

В главе 4 описана методика проверки защищенности VANET-сетей от информационных угроз сетевого уровня на основе принципа самоподобия. Данная методика основывается на подтверждении выполнения правил построения, адресации и маршрутизации в VANET-сетях, описанных в главе 3, а также на подтверждении применения описанных механизмов безопасности. При этом необходимым условием

защищенности является сохранение фрактальности графа, в связи с чем может быть предложена теорема «О необходимом условии достижимости состояния защищенности от угроз сетевого уровня в VANET-сетях».

Теорема. Граф сети с реберной связностью $m-1$ способен сохранять фрактльность n-го порядка если:

количество узлов k удовлетворяет следующему выражению (3)

$$k = n(m-1)+1, \quad (3)$$

а диаметр графа D удовлетворяет неравенству (4)

$$n \leq D \leq 2^n - 1, \quad (4)$$

где m – количество вершин в затравке.

Теорема доказывается по индукции.

Для проверки защищенности VANET-сетей от информационных угроз сетевого уровня на основе принципа самоподобия необходимо выполнение следующих операций:

1. Каждый новый узел, попадая в зону действия RSU, должен внести данные о своем публичном и секретном идентификаторе в таблицу присутствия RSU.
2. Каждый новый узел может стать участником VANET-сети только в результате применения операции ЗВЗ(А) или ЗВЗ(В), при этом в каждой ЗВЗ участвуют одновременно n-1 узлов, где n количество вершин в затравке.
3. В результате каждой ЗВЗ, новым узлам присваиваются адреса согласно правилам их образования, старые узлы меняют свои адреса в зависимости от типа ЗВЗ.
4. Все основные маршруты передачи данных строятся согласно разработанному алгоритму маршрутизации.
5. При передаче информации от одного узла к другому строятся дублирующие маршруты, количество которых равно $m-2$, где m - количество вершин в затравке (согласно механизму, описанному в 4.2.2).
6. Каждый транзитный узел, проверяет легитимность маршрута передачи данных, основываясь на механизме, описанном в 4.2.3.
7. Длины маршрутов должны удовлетворять теореме о необходимом условии достижимости состояния защищенности от угроз сетевого уровня в VANET-сетях.

8. Информация считается корректно переданной, в случае, когда приёмник получил данные по основному маршруту; получил подтверждения и контрольные суммы по всем дублирующим маршрутам; контрольные суммы сошлись.

В таблице 1 представлены условия, соблюдение которых позволяет утверждать о защищенности VANET-сети от угроз на сетевом уровне. В правом столбце таблицы указаны последствия от невыполнения указанных условий.

Таблица 1 – Условия защищенности VANET-сети от угроз на сетевом уровне

№	Условие	Последствия невыполнения
1	Все узлы VANET-сети вносят публичный и секретный идентификатор в таблицу присутствия	Возможна угроза множественной идентификации
2	Новые узлы попадают в сеть только в результате операций ЗВЗ	Нарушена предфрактальная топология. Возможны все угрозы сетевого уровня
3	Узлы получают новые адреса в соответствии с правилами адресации	Отсутствует возможность построения оптимальных маршрутов
4	Маршруты строятся в соответствии с правилами маршрутизации	Построенные маршруты не будут удовлетворять условию оптимальности
5	Строятся дублирующие маршруты передачи данных	Возможна угроза Black hole и Gray Hole
6	Каждый транзитный узел проверяет легитимность маршрута	Возможна угроза имперсонации
7	Длина маршрута удовлетворяет теореме о необходимом условии достижимости состояния защищенности от угроз сетевого уровня в VANET-сетях	Нарушена предфрактальная топология. Возможны все угрозы сетевого уровня
8	Получены данные по основному и дублирующему маршрутам, сошлись контрольные суммы	Реализована угроза Black hole или Gray Hole

Таким образом, методика проверки защищенности VANET-сетей от информационных угроз сетевого уровня на основе теории фрактальных графов включает в себя следующие этапы:

1. Проверка наличия всех активных узлов VANET в таблице присутствия.
2. Проверка соблюдения фрактальности топологии графа сети.
3. Проверка выполнения правил маршрутизации.
4. Верификации передаваемых данных с помощью дублирующих маршрутов.

5. Проверка корректности длины маршрутов передачи данных по теореме о длине оптимального маршрута.

При успешном прохождении всех проверок VANET-сеть считается защищённой от информационных угроз сетевого уровня. Пре неуспешном результате хотя бы одной проверки сеть считается подверженной угрозам в соответствии с таблицей 1, безопасность сети должна быть восстановлена с использованием метода автоматизированной саморегуляции структуры сети.

В главе 5 предложен подход к построению двухуровневой децентрализованной архитектуры VANET-сети (рисунок 4) с фрактальной топологией. Первый уровень представляет собой множество статических (с точки зрения физического положения) узлов, связанных так же статического вида связями. В контексте VANET-сетей такими узлами выступают придорожные станции (RSU). Второй уровень представляет собой динамическую структуру, в которой с течением времени меняется количество автомобилей (OBU) и связей. Именно сеть второго уровня рассматривается в качестве фрактальной, т. е. топология которой соответствует виду предфрактального графа.

Рисунок 4 – Архитектура децентрализованной системы, реализующей предложенную методику проверки защищенности

Описаны алгоритмы поведения узлов сети на всех этапах жизненного цикла, начиная от появления до удаления из сети. Описанные алгоритмы легли в основу

разработанного макета OBU автомобиля, который позволяет осуществлять коммуникацию с OBU других автомобилей и с RSU. Макет OBU имеет CAN-интерфейс для коммуникации с бортовым оборудованием и радиоканал для коммуникации с другими OBU и RSU.

Макет OBU содержит следующие функциональные блоки (рисунок 5):

– микроконтроллер для реализации алгоритмов построения, адресации и маршрутизации;

– постоянное запоминающее устройство для хранения сетевых данных;

– радиопередатчик для осуществления радиосвязи;

– усилитель мощности радиосигнала для увеличения дальности передачи;

– всенаправленная антенна для отправки и приема радиосигнала.

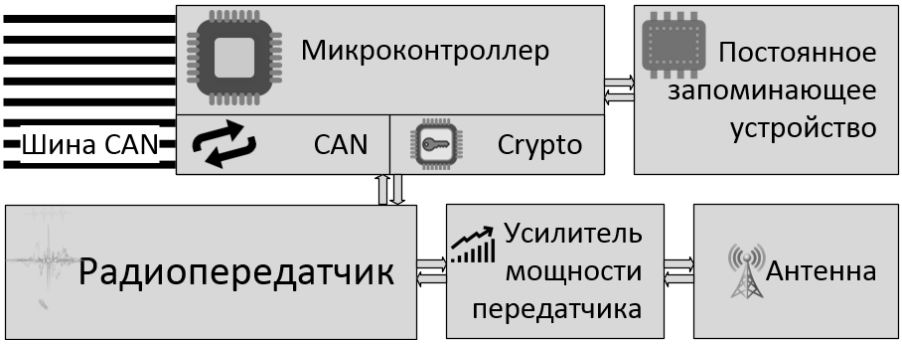

Рисунок 5 – Функциональные блоки OBU

Разработанный макет OBU позволяет развернуть прототип децентрализованной системы, реализующей предложенные методы обеспечения безопасности VANET-сетей, который обеспечивает связь между узлами в радиусе одного км в городе, со скоростью передачи данных до 2 Мбит/сек.

В заключении приведены основные результаты и выводы, полученные в ходе выполнения работы.

В работе получены следующие основные результаты:

1. Исследована специфика существующих проектов VANET-сетей и используемых механизмов безопасности, выделены их недостатки.

2. Разработана модель угроз VANET-сетям на основе графового представления.

3. Разработан метод автоматизированной саморегуляции структуры сети на основе теории предфрактальных графов; его работоспособность подтверждена с помощью построенной имитационной модели VANET-сети.

4. Разработана методика проверки защищенности VANET-сетей от информационных угроз сетевого уровня на основе теории фрактальных графов, включающая:

– проверку соблюдения фрактальности топологии графа сети;

– проверку выполнения правил маршрутизации;

– проверку удовлетворения топологических характеристик сети допустимым значениям.

5. Построена архитектура и разработан прототип децентрализованной системы, реализующей предложенные методы обеспечения безопасности VANET-сетей.

Основные результаты диссертационной работы изложены в 14 печатных трудах. Ниже приведены основные из них:

1. Зегжда, П.Д. Актуальные угрозы безопасности VANET/MANET-сетей / П.Д. Зегжда, **Д.В. Иванов**, Д.А. Москвин, Г.С. Кубрин // Проблемы информационной безопасности. Компьютерные системы. - СПб., 2018. - № 2. - С. 41-47.

2. Зегжда, П.Д. Применение рядов смежности для распознавания предфрактальных графов при оценке кибербезопасности VANET-сетей / П.Д. Зегжда, **Д.В. Иванов**, Д.А. Москвин, А.А. Иванов // Проблемы информационной безопасности. Компьютерные системы. - СПб., 2018. - № 1. - С. 10-26.

3. Овасапян, Т.Д. Обеспечение безопасности WSN-сетей на основе модели доверия / Т.Д. Овасапян, **Д.В. Иванов** // Проблемы информационной безопасности. Компьютерные системы. - СПб., 2017. - № 4. - С. 64-72.

4. Москвин, Д.А. Методы защиты самоорганизующихся сетей от атак на маршрутизацию сетей / Д.А. Москвин, **Д.В. Иванов** // Проблемы информационной безопасности. Компьютерные системы. - СПб., 2015. - № 2. - С. 91-97.

5. Москвин, Д.А. Исследование безопасности беспроводных самоорганизующихся сетей / Д.А. Москвин, **Д.В. Иванов** // Информация и безопасность. – В., 2014. - № 2. – С. 296-299.

6. Москвин, Д.А., Разработка и экспериментальная оценка методов защиты беспроводных самоорганизующихся сетей / Д.А. Москвин, **Д.В. Иванов** // Математические структуры и моделирование. - О., 2014. - № . - С. 247-253.

7. Москвин, Д.А. Разработка методов защиты и моделирование безопасности беспроводных самоорганизующихся сетей / Д.А. Москвин, **Д.В. Иванов** // Информатика и кибернетика (ComCon-2015): сборник докладов студенческой научной конференции Института информационных технологий и управления. 2015. С. 242-244.

8. Москвин, Д.А. Использование mesh-топологии для управления сетями роботизированных объектов: удобно или безопасно? / Д.А. Москвин, **Д.В. Иванов** // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 2014. С. 32-34.

9. Москвин, Д.А. Разработка методов защиты беспроводных ad-hoc сетей, на основе оценки физических характеристик узлов сети / Д.А. Москвин, **Д.В. Иванов** // Актуальные направления фундаментальных и прикладных исследований. Материалы IV международной научно-практической конференции. 2014. С. 149.

10. **Ivanov, D.V.** «Methods of protecting self-organizing networks against attacks on traffic routing / **D.V. Ivanov**, D.A. Moskvin // Automatic Control and Computer Sciences. - 2015. - Vol. 49. - Issue №8. - P. 745-750.

11. **Ivanov, D.** Cybersecurity of ad-hoc distributed systems / **D. Ivanov**, D. Moskvin // Proceedings of the 8th International Conference on Security of Information and Networks (ACM), 2015. – P.150-153