На правах рукописи

ЛИТВИНОВ Георгий Александрович

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ МАРШРУТИЗАЦИИ В САМООРГАНИЗУЮЩИХСЯ СЕТЯХ НА ОСНОВЕ РЕПУТАЦИОННОЙ МОДЕЛИ

Специальность 2.3.6. Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Омск – 2023

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Омский государственный технический университет» на кафедре «Комплексная защита информации».

Научный руководитель: **Щерба Евгений Викторович**
кандидат технических наук, доцент,
ФГАОУ ВО «Омский государственный технический университет», доцент кафедры «Комплексная защита информации»

Официальные оппоненты: **Аникин Игорь Вячеславович**
доктор технических наук, профессор,
ФГБОУ ВО «КНИТУ-КАИ»,
заведующий кафедрой систем информационной безопасности

Ручай Алексей Николаевич
кандидат физико-математических наук, доцент,
ФГБОУ ВО «ЧелГУ»,
заведующий кафедрой компьютерной безопасности и прикладной алгебры

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский университет науки и технологий», г. Уфа

Защита диссертации состоится «21» сентября 2023 г. в 14:00 часов на заседании диссертационного совета 24.2.350.07, созданного на базе ФГАОУ ВО «Омский государственный технический университет», по адресу: 644050, г. Омск, проспект Мира, 11, Главный корпус, ауд. П-202.

С диссертацией можно ознакомиться в библиотеке ФГАОУ ВО «Омский государственный технический университет» и на сайте www.omgtu.ru.

Отзыв на автореферат в двух экземплярах, заверенный печатью учреждения, просьба направлять по адресу: 644050, г. Омск, пр. Мира, 11, ученому секретарю диссертационного совета 24.2.350.07. Тел.: (3812) 65-24-79, e-mail: dissov_omgtu@omgtu.ru.

Автореферат разослан «__ _» _____ 2023 года.

Ученый секретарь диссертационного совета 24.2.350.07, кандидат технически наук, доцент

А.С. Грицай

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Развитие концепции самоорганизующихся сетей способствует появлению новых технологий «Интернета вещей» и согласуется с ключевыми приоритетами Стратегии научно-технологического развития РФ. В настоящее время самоорганизующиеся сети находят применение во множестве областей, включая медицинские системы, интеллектуальные транспортные системы и сети беспилотных летательных аппаратов.

Самоорганизующиеся или многошаговые сети являются децентрализованными и могут объединять множество мобильных или стационарных устройств, которые способны самостоятельно устанавливать и поддерживать беспроводные соединения с другими устройствами в пределах своей зоны радиопокрытия. Как правило, узлы беспроводной самоорганизующейся сети имеют возможность перемещаться в пространстве, устанавливая новые связи с соседними узлами и теряя ранее имевшиеся. Таким образом, топология самоорганизующихся сетей является динамической. При этом каждый узел сети помимо роли оконечного устройства, выполняет роль маршрутизатора, т.е. принимает сетевые пакеты, адресованные другим устройствам, и осуществляет дальнейшую пересылку пакетов в соответствии с выбранным направлением. Для организации многошаговых соединений узлы используют протоколы адаптивной маршрутизации, что также позволяет обеспечивать устойчивость к изменениям топологии сети.

С другой стороны, в результате проникновения технологий «Интернета вещей» во все сферы человеческой деятельности, постоянно повышается роль обеспечения кибербезопасности и защиты сетевого взаимодействия. В результате, развитие технологий на базе самоорганизующихся сетей сдерживается угрозами информационной безопасности. Множественный доступ к среде передачи данных, динамическая топология и особенности маршрутизации пакетов в беспроводных самоорганизующихся сетях повышают сложность обеспечения их безопасной доставки до получателя.

Учитывая открытый характер множества самоорганизующихся сетей и проблему внутренних нарушителей в закрытых сетях, модель поведения участников сетевого взаимодействия может оставаться неопределенной. В частности, участники сетевого взаимодействия в целях экономии ресурсов могут игнорировать необходимость дальнейшей передачи сетевых пакетов, полученных от других узлов. Кроме того, вредоносные узлы могут целенаправленно препятствовать сетевому взаимодействию посредством различных сетевых атак. В результате одной из наиболее актуальных проблем остается проблема обеспечения безопасности маршрутизации сетевых пакетов.

Криптографические методы защиты позволяют обеспечить конфиденциальность и целостность пересылаемых пакетов данных, но их применение сопряжено с рядом трудностей. В условиях ограниченности ресурсов устройств в беспроводных самоорганизующихся сетях данные механизмы могут быть чересчур затратными, кроме того возникает задача распределения ключей в децентрализованной архитектуре. Помимо этого, сохраняется угроза нарушения доступности информации в результате сетевых атак внутренних нарушителей и зараженных узлов. Таким образом, в самоорганизующихся сетях безопасность маршрутизации не может быть гарантирована в рамках схем защиты, основанных исключительно на криптографических преобразованиях и классической модели доверия на основе сертификации.

В качестве альтернативы может быть использована модель доверия, основанная на кооперации и оценке репутации участников сетевого взаимодействия. Репутационные модели имеют широкий спектр применения, включая системы электронной торговли и социальные сети. Применение репутационной модели в самоорганизующейся сети позволяет избегать ненадёжные узлы с низкой репутацией при доставке пакетов и тем самым повысить безопасность процесса маршрутизации. Установление отношений доверия и сотрудничество узлов сети позволяет определять узлы нарушителей и исключать их из процесса сетевого взаимодействия. Узлы, препятствующие пересылке пакетов, не должны

иметь доверия у других узлов сети. Определение доверия к узлам сети может осуществляться на основе вычисления значения репутации этих узлов другими узлами сети.

Данная диссертационная работа посвящена разработке новой репутационной модели и её имплементации на базе существующего протокола маршрутизации для обеспечения безопасности процесса пересылки сетевых пакетов в самоорганизующихся сетях. Вышеуказанные факторы обуславливают актуальность темы диссертационного исследования.

Степень разработанности темы исследований

За последние 25 лет в научных работах зарубежных и отечественных авторов было предложено множество моделей, методов и протоколов маршрутизации для сетей с динамической топологией. Существенный вклад в повышение их эффективности внесли Кучерявый А.Е., Вишневский В.М., Киричек Р.В., Перепелкин Д.А., Jacquet P., Clausen T., Herberg U., Perkins C.E. и др.

В последние годы особое внимание уделяется проблеме обеспечения безопасности в самоорганизующихся сетях. Проблема обнаружения аномального поведения узлов затрагивается в работах Зегжды П.Д., Калинина М.О., Васильева В.И., Гвоздева В.Е., Adnane A., Sun B. и др.

Исследования Макаревича О.Б., Бабенко Л.К., Абрамова Е.С., Michiardi P., Molva R., Kamvar S.D. и других авторов охватывают вопросы применения моделей доверия для обеспечения безопасности узлов сети. Вместе с тем существующие репутационные модели имеют ряд особенностей, которые ограничивают возможность их применения. В частности, не все модели учитывают объем данных, используемый для расчета репутации, при этом оценки, полученные из различных источников, смешиваются при определении значения репутации. Другой проблемой является определение порогового значения репутации, используемого для принятия решения об изоляции некоторого участника сети. В целом, проблема применения репутационных моделей для обеспечения безопасности маршрутизации в самоорганизующихся сетях остается малоизученной.

Объект исследования – безопасность сетевого взаимодействия в самоорганизующихся сетях**.**

Предмет исследования – протоколы и модели обеспечения безопасности маршрутизации сетевых пакетов в самоорганизующихся сетях**.**

Цель работы – повышение безопасности маршрутизации сетевых пакетов в динамически организуемых телекоммуникационных сетях посредством разработки и имплементации репутационной модели доверия для узлов сети.

Для достижения этой цели в рамках диссертационного исследования были сформулированы следующие **задачи**:

1. Проанализировать угрозы безопасности маршрутизации в самоорганизующихся сетях;
2. Проанализировать возможность применения существующих моделей оценки репутации узлов в самоорганизующихся сетях;
3. Разработать новую репутационную модель доверия для обеспечения безопасности маршрутизации в самоорганизующихся сетях;
4. Разработать алгоритм поиска наиболее безопасных маршрутов для его применения в рамках разработанной репутационной модели;
5. Реализовать разработанную репутационную модель и алгоритм на базе одного из существующих проактивных протоколов маршрутизации для самоорганизующихся сетей;
6. Экспериментально обосновать эффективность предложенных решений в различных сценариях.

Основные научные результаты, выносимые на защиту

1. Новая транзитивная булевозначная модель оценки репутации каналов связи и метрика безопасности маршрутов, позволяющая учитывать их репутацию (п. 5, 9 паспорта специальности).

2. Эффективный алгоритм поиска наиболее безопасных маршрутов до всех узлов сети. Указанный алгоритм основан на булевозначном представлении сети и позволяет находить маршруты с наилучшей репутацией, что приводит к изоляции узлов нарушителей с низкой репутацией (п. 5, 15 паспорта специальности).

3. Модель обеспечения безопасности проактивной маршрутизации, основанная на имплементации, разработанной репутационной модели и алгоритма поиска наиболее безопасных маршрутов для существующего протокола маршрутизации OLSR. По результатам экспериментальной оценки, полученный протокол BOLSR позволил повысить коэффициент доставки пакетов в сетях со статической топологией в среднем в 3,68 раза и в сетях с динамической топологией в среднем в 1,75 раза при незначительном увеличении средней длины маршрутов (в среднем в 1,03 раза) по сравнению с оригинальным протоколом OLSR (п. 15 паспорта специальности).

Научная новизна результатов

1. Разработана новая транзитивная булевозначная модель оценки репутации каналов связи. Новизна разработанной модели заключается в определении глобальной репутации каналов связи посредством булевозначного вектора, что позволяет учитывать количество оценок, используемых для расчета репутации, и не смешивать оценки репутации, полученные из различных источников.

2. Разработан новый алгоритм поиска наиболее безопасных маршрутов до узлов сети. Учитывая вогнутую метрику безопасности маршрутов, определенную в рамках репутационной модели, указанный алгоритм позволяет находить маршруты с наилучшей репутацией, что позволяет избегать узлы с низкой репутацией при доставке пакетов и тем самым повысить безопасность процесса маршрутизации.

3. Разработана оригинальная модель проактивного протокола маршрутизации сетевых пакетов, безопасность которого обеспечивается на основе комплекса предложенных решений. В рамках указанного протокола предложен способ взаимодействия узлов сети, позволяющий определить глобальную репутацию каналов связи и маршрутов в сети.

Теоретическая и практическая значимость

Теоретическая значимость исследования определяется её вкладом в совершенствование моделей и методов обеспечения безопасности сетевого взаимодействия, которые позволяют противодействовать возникающим угрозам и обеспечивать доступность передаваемых данных.

Практическая значимость работы состоит в возможности использования разработанного протокола динамической проактивной маршрутизации BOLSR для обеспечения безопасности маршрутизации в самоорганизующихся сетях.

Методы исследования

При получении основных результатов диссертационной работы использовались общие методы дискретной и вычислительной математики, теория вероятностей, методы математической статистики, теория защиты информации и методы имитационного моделирования.

Достоверность полученных результатов

Достоверность результатов исследования подтверждается корректным и обоснованным применением математического аппарата, данными имитационного моделирования, а также успешной апробацией на всероссийских и международных научных конференциях.

Реализация и внедрение результатов работы

Основные теоретические и практические результаты исследования использованы в научно-исследовательской работе «Исследование и адаптация репутационных моделей для динамически организуемых телекоммуникационных сетей» (№ госрегистрации АААА-А20-120100890016-6), научно-исследовательской работе «Разработка и исследование моделей безопасной маршрутизации для телекоммуникационных сетей с динамической топологией» (№ госрегистрации АААА-А18-118112390046-6). Результаты

диссертационной работы внедрены и использовались в ООО «Юбисофт» при разработке дополнительного модуля для операционной системы UBLinux, при проведении испытаний в системном интеграторе «ХайТэк», а также в учебном процессе кафедры «Комплексная защита информации» при подготовке научно-исследовательских работ студентов, чтении лекций и проведении лабораторных работ по дисциплинам «Сетевое и системное администрирование», «Безопасность вычислительных сетей», «Системы и сети передачи данных» в ходе обучения студентов по направлениям подготовки 10.03.01 «Информационная безопасность» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» в Федеральном государственном автономном образовательном учреждении высшего образования «Омский государственный технический университет», что подтверждается соответствующими актами внедрения.

Апробация результатов

Основные результаты и положения диссертационного исследования докладывались и обсуждались на следующих международных и всероссийских научных, научно-технических конференциях:

• 19th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM), Novosibirsk, Russia, 2018;

• 14th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), Novosibirsk, Russia, 2018;

• 12th, 13th International IEEE Scientific and Technical Conference on Dynamics of Systems, Mechanisms and Machines (Dynamics), Omsk, Russia, 2018;

• 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 2019;

• International IEEE Scientific and Technical Conference on Dynamics of Systems, Mechanisms and Machines (Dynamics), Omsk, Russia, 2019;

• IX Международной молодежной научно-практической конференции с элементами научной школы «Прикладная математика и фундаментальная информатика», Омск, Россия, 2020;

• VIII International Conference «Engineering & Telecommunication — En&T-2021», Moscow Institute of Physics and Technology, Russia, 2021.

Публикации

По теме диссертационного исследования опубликовано 22 работы, отражающие основные полученные результаты, включая:

• 5 статей в ведущих научных журналах из Перечня рецензируемых научных изданий ВАК при Министерстве науки и высшего образования РФ;

• 17 научных работ в изданиях, индексируемых ведущими международными реферативными базами Web of Science и Scopus.

Во время выполнения научного исследования диссертантом были разработаны три программы для ЭВМ. Свидетельства о государственной регистрации программ для ЭВМ № 2018666677, № 2019666281, № 2021661846.

Сведения о личном вкладе автора

Основные результаты диссертационного исследования получены автором самостоятельно. Научный руководитель принимал участие в постановке цели и задач исследования, планировании экспериментов, предварительном анализе результатов экспериментов. В работах, опубликованных в соавторстве, диссертанту принадлежит ключевая роль.

Структура и объем работы

Диссертационное исследование объемом 143 страницы состоит из оглавления, введения, основной части (поделённой на 3 главы), заключения, списка литературы из 108 цитируемых источников, 3 приложений, а также 40 рисунков и 11 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность темы диссертационного исследования, определена цель работы и сформулированы задачи, которые необходимо решить для достижения поставленной цели. Изложена степень разработанности темы исследования, научная новизна результатов, их теоретическая и практическая значимость, а также основные положения, выносимые на защиту.

Первая глава диссертационной работы посвящена анализу проблемы обеспечения безопасности маршрутизации пакетов в самоорганизующихся сетях. Представлена классификация протоколов и моделей маршрутизации, применяемых в беспроводных самоорганизующихся сетях различных типов, определены их основные особенности. Описана функциональность проактивного протокола маршрутизации OLSR, в дальнейшем использованного в работе. Обращается внимание, что в условиях, когда каждое устройство сети может выступать в роли маршрутизатора, а топология сети постоянно изменяется, проблема обеспечения безопасности маршрутизации пакетов значительно усложняется.

Выполнен анализ существующих угроз безопасности маршрутизации в самоорганизующихся сетях, включая сетевые атаки с фильтрацией пакетов, атаки на истощение ресурсов, атаки с использованием фальсификации и некоторые другие. Отмечено, что безопасность маршрутизации в самоорганизующихся сетях не может быть гарантирована в рамках схем защиты, основанных исключительно на криптографических преобразованиях и классической модели доверия на основе сертификации. Указанный подход не позволяет обеспечить защиту от внутренних узлов нарушителей, реализующих сетевые атаки типа «черная дыра» или «серая дыра». Обоснована необходимость применения репутационной модели в самоорганизующейся сети, что позволит избегать при доставке пакетов ненадёжные узлы с низкой репутацией и тем самым повысить безопасность процесса маршрутизации.

Проанализированы существующие модели определения доверия и вычисления репутации, включая модели, основанные на суммировании и усреднении оценок (модели протоколов CORE и CONFIDANT), потоковые модели (EigentTrust, PeerTrust, BP/2P, VectorTrust) и модели на основе субъективной логики (модель протокола TAODV и EBSL). Исследована проблематика их применения для определения уровня доверия к узлам и маршрутам в самоорганизующейся сети. Показано, что существующие репутационные модели имеют ряд особенностей, которые ограничивают возможность их применения. В частности, не все модели учитывают объем данных, используемый для расчета репутации, при этом оценки, полученные из различных источников, смешиваются при определении значения репутации. Другой проблемой является определение порогового значения репутации, используемого для принятия решения об изоляции некоторого участника сети. В целом проблема применения репутационных моделей для обеспечения безопасности маршрутизации в самоорганизующихся сетях остается малоизученной.

По результатам проделанного анализа, сформирован ряд требований, которым должна удовлетворять репутационная модель для решения проблемы обеспечения безопасности маршрутизации в самоорганизующихся сетях. Выполнена постановка задач исследования и сформулирована цель диссертационной работы, которая заключается в обеспечении безопасности маршрутизации сетевых пакетов в динамически организуемых телекоммуникационных сетях посредством разработки и имплементации новой репутационной модели доверия для узлов сети.

Во **второй главе** представлено описание разработанной модели оценки репутации каналов связи самоорганизующейся сети и способа взаимодействия узлов сети в целях определения репутации каналов связи узлами сети.

В рамках разработанной репутационной модели рассматриваемая телекоммуникационная сеть, состоящая из n узлов, представляется в виде ориентированного графа $G(V,E)$, где множество вершин V соответствует конечному

множеству узлов сети, а множество дуг E соответствует конечному множеству каналов связи, соединяющих узлы.

Каждый узел сети независимо от других узлов определяет локальное значение репутации существующих каналов связи. В частности, некоторый узел s определяет локальное значение репутации прямого канала связи между узлом u и узлом v как $r_s(u,v)$. Предложенная репутационная модель является булевозначной, таким образом значение $r_s(u,v) \in \{0,1\}$.

В рамках описания модели введены следующие обозначения. Пусть задано конечное множество элементов атомов $M = \{a_1, a_2, \ldots, a_n\}$, где некоторый атом a_i соответствует положительному значению репутации, сформированному узлом i. Пусть $P(M)$ – множество всех подмножеств множества M. Булева алгебра $B = (P(M), \wedge, \vee, \neg, 0, 1)$ представляет собой множество $P(M)$, на котором определены стандартные логические операции, минимальный элемент 0 (соответствует пустому множеству) и максимальный элемент 1 (соответствует элементу $a_1a_2\ldots a_n$).

При каждом изменении локального значения репутации для некоторого канала связи $r_i(u,v)$ узел i сообщает это значение другим узлам сети. В результате узлы обмениваются локальными значениями репутации друг с другом, что позволяет определить вектор глобальной репутации $(r_1(u,v), r_2(u,v), \ldots, r_n(u,v))$ для каждого канала связи (u,v) в сетевой топологии. Вектор глобальной репутации для некоторого канала связи включает все локальные значения репутации для данного канала связи, определяемые всеми узлами сети соответственно.

На основе вектора репутации каждый узел вычисляет значение глобальной репутации $r(u,v)$ как элемент множества $P(M)$ для каждого канала связи (u,v) в сетевой топологии. Указанные значения глобальной репутации используются узлами для определения доверия к каналам связи. В случае, когда ни один из узлов не установил положительную локальную репутацию некоторого канала связи, глобальная репутация этого канала связи представляет нулевой элемент множества $P(M)$.

Для поиска маршрутов каждый узел независимо производит построение булевозначной сети, которая представляет собой ориентированный мультиграф, каждой дуге которого присвоен некоторый элемент $c(e)$ из фиксированной конечной булевой алгебры B.

Значение стоимости некоторой дуги $c(u,v)$ в рассматриваемой булевозначной сети определяется глобальной репутацией соответствующего канала связи $r(u,v)$, что обеспечивает согласованность представлений, используемых узлами сети. Расчёт глобального значения репутации некоторого канала связи выполняется посредством объединения соответствующих атомов булевой алгебры B. Стоимость дуги $c(u,v)$ включает в себя атом a_i тогда, и только тогда, когда i-й элемент соответствующего вектора глобальной репутации равен 1. То есть каждая дуга булевозначной сети помечена объединением атомов B, соответствующих тем узлам, которые «рекомендуют» рассматриваемый канал связи. Таким образом, для всех узлов определена булевозначная сеть $G(V,E)$ с функцией стоимости $c(u,v)$.

Маршрут доставки пакетов представляет собой путь P из узла s в узел t, состоящий из последовательности дуг множества E. Для оценки безопасности маршрутов в сети была определена соответствующая вогнутая метрика безопасности маршрутов, или глобальная репутация пути P. Глобальная репутация (нижняя оценка) некоторого пути $P = (s, e_0, \ldots, e_j, t)$ определяется как пересечение стоимостей всех дуг, образующих этот путь:

$$b(P) = c(e_0) \wedge \ldots \wedge c(e_j).$$

Мощность или уровень доверия к некоторому пути, определяется как количество атомов из B, которые содержатся в его нижней оценке (глобальной репутации). Суть предложенной метрики отражает тот факт, что для маршрута, «рекомендованного» наибольшим количеством узлов, значение метрики будет включать максимально возможное количество атомов. Можно считать, что наиболее безопасному маршруту для

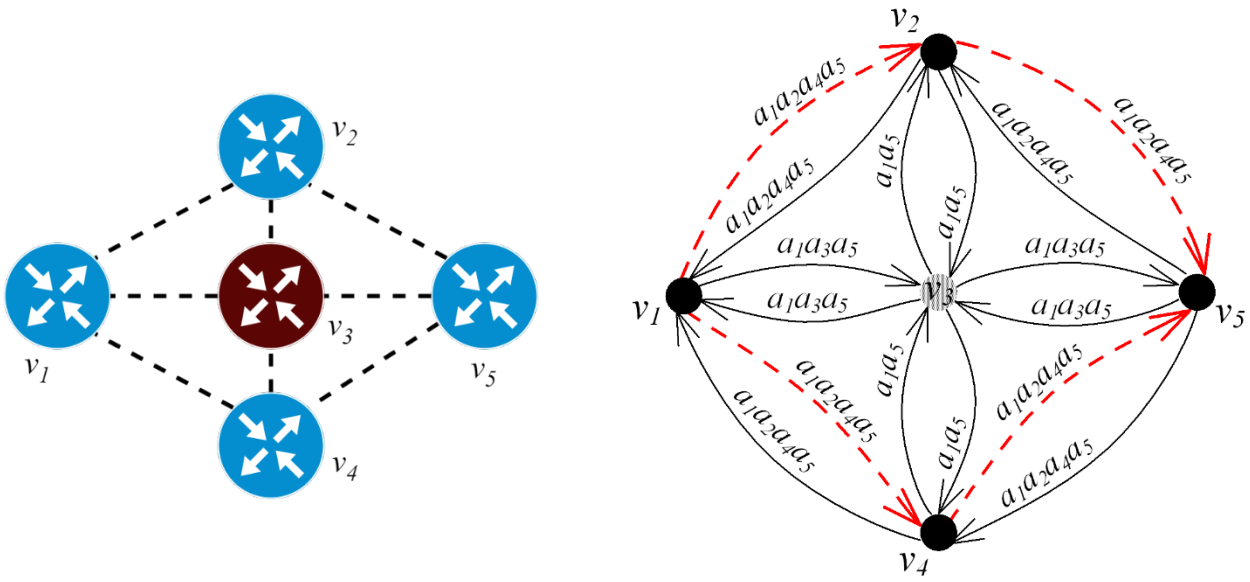
доставки пакетов будет соответствовать путь в булевозначной сети, все дуги которого одновременно рекомендованы наибольшим числом узлов сети, то есть путь с максимальной мощностью (уровнем доверия). Таким образом, для определения наиболее безопасного маршрута от некоторого узла отправителя s до узла получателя t необходимо среди всех путей с максимальной мощностью из вершины s в вершину t в булевозначной сети $G(V,E)$ определить кратчайший путь P.

Например, если в сети из 5 узлов (рисунок 1*а*), узлы v_1, v_2, v_4, v_5 являются легитимными и имеют нормальное поведение, а узел v_3 является вредоносным и выполняет атаку типа «серая дыра», глобальная репутация каналов связи может быть определена в соответствии с таблицей 1.

Таблица 1. Глобальная репутация каналов связи

(u,v)	(v_1,v_2) (v_2,v_1)	(v_1,v_3) (v_3,v_1)	(v_1,v_4) (v_4,v_1)	(v_2,v_3) (v_3,v_2)	(v_2,v_5) (v_5,v_2)	(v_3,v_4) (v_4,v_3)	(v_3,v_5) (v_5,v_3)	(v_4,v_5) (v_5,v_4)
$r(u,v)$	(1,1,0,1,1)	(1,0,1,0,1)	(1,1,0,1,1)	(1,0,0,0,1)	(1,1,0,1,1)	(1,0,0,0,1)	(1,0,1,0,1)	(1,1,0,1,1)

Исходя из указанных значений, может быть построена булевозначная сеть, соответствующая текущей сетевой топологии (рисунок 1*б*). В данном случае из узла v_1 в узел v_5 существует два наиболее безопасных маршрута, соответствующих путям мощности 4 с глобальной репутацией $\{a_1a_2a_4a_5\}$ (выделены пунктирной линией). Все пути через узел нарушителя имеют более низкую мощность.



а) *б)*

Рисунок 1. Графическая интерпретация применения разработанной модели

Разработанная модель поддерживает различные способы оценки локальной репутации каналов связи. В работе предложен способ оценки локальной репутации каналов связи при помощи отправки скрытых проверочных пакетов. Для оценки состояния каналов, узел s выбирает случайный доступный узел t и отправляет ему проверочные пакеты, скрытые в обычном трафике, по заранее определенному маршруту. Маршрут, сформированный от узла s к узлу t, представляет собой путь P в соответствующем графе, который включает все дуги (u,v), соответствующие каналам связи, образующим маршрут. Узел назначения t при получении скрытого проверочного пакета, должен сформировать ответный пакет и отправить его обратно. Если узел s получил ответный пакет, это означает, что все узлы, маршрутизирующие скрытый пакет, успешно справились со своей задачей и узел s устанавливает каждому каналу связи (u,v) пути P положительное локальное значение

репутации $r_s(u,v) = 1$. В противном случае, если узел s не получил ответ на скрытый проверочный пакет в течение заданного временного интервала, маршрут, соответствующий пути P, считается ненадежным и проверяющий узел s устанавливает для всех каналов связи (u,v), входящих в соответствующий маршрут, локальное значение репутации $r_s(u,v) = 0$. Указанная процедура повторяется многократно на постоянной основе с заданной периодичностью каждым узлом сети.

На основе предложенной репутационной модели была формализована задача поиска наиболее безопасного маршрута до некоторого узла в самоорганизующейся сети как маршрута с наилучшей репутацией. Указанный маршрут соответствует кратчайшему пути среди всех путей с максимальной мощностью в соответствующей булевозначной сети, используемой в качестве модели самоорганизующейся сети.

Для решения указанной формальной задачи был разработан алгоритм поиска наиболее безопасных маршрутов от некоторого узла до всех узлов сети (рисунок 2). Учитывая вогнутую метрику безопасности маршрутов, определенную в рамках репутационной модели, указанный алгоритм позволяет находить маршруты с наилучшей репутацией, что позволяет избегать узлы с низкой репутацией при доставке пакетов и тем самым повысить безопасность процесса маршрутизации.

Алгоритм 1 Алгоритм поиска наиболее безопасных маршрутов

Вход: G, c, s
Выход: Множество P наиболее безопасных путей из s до всех доступных узлов G

$P \leftarrow \{\varnothing\}$, $A \leftarrow \{s\}$, $A^* \leftarrow \{\varnothing\}$, $L(s) \leftarrow \{1\}$
Для всех $v \in V(G)\backslash\{s\}$
  $L(v) \leftarrow \{\varnothing\}$
Пока $A \neq \{\varnothing\}$
  Для всех $u \in A$
    Для всех $v \in V(G)$
      $L^*(v) \leftarrow L(v)$
      Если $(u,v) \in E(G)$ **то**
        $L(v) \leftarrow \mathrm{MAX}(L(v) \cup (L(u) \wedge c(u,v)))$ // $\mathrm{MAX}(X)$ - *возвращает множество максимальных элементов частично-упорядоченного множества* X
        Если $L^*(v) \neq L(v)$ **то**
          $A^* \leftarrow A^* \cup \{v\}$
  $A \leftarrow A^*$, $A^* \leftarrow \{\varnothing\}$
Для всех $v \in V(G)\backslash\{s\}$
  $P^* \leftarrow \{\varnothing\}$
  Для всех $max \in L(v)$ // max - *элемент с максимальной мощностью*
    $G^* \leftarrow G$
    Для всех $e \in E(G^*)$
      Если $q(e) \not\subseteq max$ **то**
        УДАЛИТЬ e ИЗ $E(G^*)$
    $p \leftarrow$ НАЙТИ КРАТЧАЙШИЙ $s - v$ ПУТЬ ИЗ G^*
    $P^* \leftarrow P^* \cup \{p\}$
  $p \leftarrow$ ВЫБРАТЬ КРАТЧАЙШИЙ $s - v$ ПУТЬ ИЗ P^*
  $P \leftarrow P \cup \{p\}$
Вернуть P

Рисунок 2. Алгоритм поиска наиболее безопасных маршрутов

На вход алгоритма поступает булевозначная сеть $G(V,E)$ с функцией стоимости $c(u,v)$, узел отправителя s, узел получателя t, множество атомов M, равномощное множеству узлов сети. Выход алгоритма представляет собой множество наиболее безопасных маршрутов как множество P кратчайших путей среди всех путей с максимальной мощностью до каждого из узлов сети.

На первом этапе работы алгоритма производится поиск нижних оценок всех путей с максимальной мощностью. Этот этап представляет некоторую сложность в связи с тем, что метки дуг являются элементами частично упорядоченного множества. В связи с этим множество $L(v)$ используется как меточное множество для некоторой вершины $v \in V$. Изначальное значение элементов множества L имеет значение $L(v) = \{0\}$ для всех $v \in V$ отличных от s. Множество A используется для хранения списка активных вершин на текущей итерации, а в множестве A^* формируется список активных вершин для следующей итерации.

На каждой итерации первого этапа алгоритма происходит переформирование меточного множества для всех вершин, в которые ведут дуги из активных вершин A. Вершины v, в которых изменилось значение множества $L(v)$, заносятся в множество A^*. После полного пересмотра меточных множеств происходит замена множества A на множество A^*, а множество A^* очищается. Работа первого этапа продолжается до тех пор, пока множество A^* по завершении итерации отлично от пустого множества. После завершения данного этапа, множество $L(v)$ будет содержать нижние оценки всех путей с максимальной мощностью до некоторой вершины v. Если в заданной сети для заданного набора ограничений существует путь из s в v, «рекомендуемый» всеми узлами сети, то $L(v) = \{1\}$.

На втором этапе работы алгоритма для каждой вершины v поочередно рассматривается один из максимальных по мощности элементов a из множества $L(v)$. В сети G окрашиваются только дуги, стоимость которых больше либо равна элементу a. Все пути из узла s в узел v по окрашенным дугам имеют максимальную мощность. В сети, которая образована окрашенными дугами, с помощью алгоритма Дейкстры осуществляется поиск кратчайшего пути из s в v. Среди всех найденных кратчайших путей с максимальной мощностью до вершины v отбирается путь минимальной длины и помещается в множество P. По завершении второго этапа P содержит множество кратчайших путей с максимальной мощностью из узла s до всех узлов сети.

В целях практического применения разработанной репутационной модели и алгоритма поиска наиболее безопасного маршрута указанный комплекс решений был имплементирован в рамках протокола маршрутизации OLSR для обеспечения безопасности маршрутизации пакетов в самоорганизующихся сетях. В ходе имплементации разработанной модели и алгоритма, структуры данных и служебные сообщения, используемые в рамках протокола OLSR, были дополнены, а алгоритм выбора оптимальных маршрутов был изменен.

В рамках имплементации репутационной модели было введено два дополнительных типа сообщений протокола:

RM_MESSAGE – тип сообщений для распространения по сети субъективной информации о состоянии канала связи, проверенного отправителем пакета;

ECHO_MESSAGE – тип сообщений для проверки каналов связи случайно выбранного маршрута.

Предложенные типы сообщений позволяют узлам сети обмениваться информацией о локальном значении репутации каналов связи. Полученные значения локальной репутации используются для формирования векторов глобальной репутации каналов связи, которые в дальнейшем используются узлами для поиска наиболее безопасных маршрутов и расчёта таблицы маршрутизации.

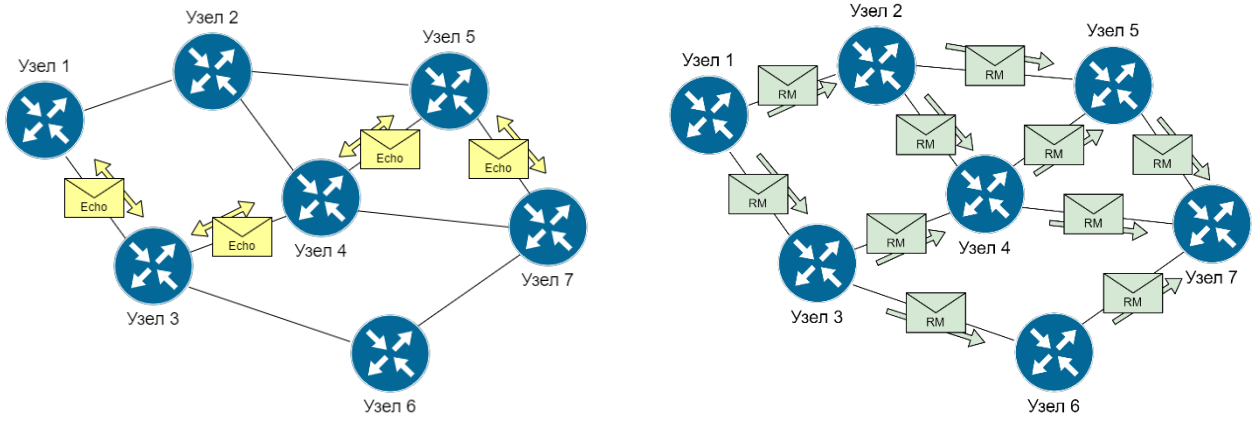
Для локального хранения информации о состоянии каналов связи на каждом устройстве используется несколько таблиц: таблица каналов связи до соседних узлов,

доступных за один переход, таблица каналов связи от соседних узлов до узлов, доступных за два перехода, таблица всех остальных каналов связи. В рамках имплементации репутационной модели в структуру каждой таблицы было добавлено новое поле, используемое для хранения вектора глобальной репутации для каждого канала связи в сетевой топологии.

Для определения локальной репутации проверяемых каналов связи в рамках протокола была сформирована дополнительная локальная таблица, которая хранит в себе информацию о маршрутах, проверяемых в настоящее время, и временную метку начала проверки. Проверка маршрутов выполняется каждым узлом с определенной периодичностью, определяемой дополнительным параметром.

Все маршруты, присутствующие в таблице маршрутизации некоторого узла, могут подлежать проверке этим узлом. В ходе проверки некоторому случайно выбранном узлу, маршрут до которого хранится в таблице маршрутизации, отправляется проверочное сообщение запроса ECHO_MESSAGE, зашифрованное и подписанное отправителем. При получении пакета запроса легитимным узлом сети, сообщение дешифруется и производится проверка его подлинности, после чего проверяемый узел формирует и отправляет проверяющему узлу пакет с зашифрованным и подписанным ответным сообщением ECHO_MESSAGE (рисунок 3*а*). Указанное ответное сообщение содержит информацию об обратном маршруте и подтверждает его актуальность.

В случае если ответный тестовый пакет не был получен в течение заданного временного периода, маршрут считается ненадежным, проверяющий узел устанавливает локальное значение репутации всех каналов связи, образующих проверяемый маршрут, равным 0 и отправляет сообщение RM_MESSAGE для того, чтобы распространить набор соответствующих значений по другим узлам сети. Все узлы, выступающие в качестве шлюзов MPR, выполняют ретрансляцию сообщений RM_MESSAGE, используя доступные каналы связи (рисунок 3*б*).



а) *б)*

Рисунок 3. Схемы отправки сообщений ECHO для оценки репутации каналов связи (*а*) и сообщений RM для распространения значений локальной репутации (*б*)

В рамках имплементации репутационной модели были внесены изменения в алгоритм вычисления маршрутов протокола OLSR. Базовая функция вычисления таблицы маршрутизации была расширена посредством предварительного вычисления наиболее безопасных маршрутов с помощью разработанного алгоритма с использованием репутационной информации о состоянии каналов связи.

Указанная имплементация была программно реализована в качестве протокола маршрутизации Boolean Optimized Link State Routing (BOLSR). В ходе имплементации комплекса предложенных решений в существующие программные модули протокола OLSR были внесены изменения, представленные на рисунке 4. Указанные блоки отражают проделанные изменения, при этом блоки, выделенные сплошной линией, соответствуют

модифицированным элементам программной реализации протокола, а пунктирной линией выделены функции, сообщения и структуры данных, которые были добавлены в результате имплементации.

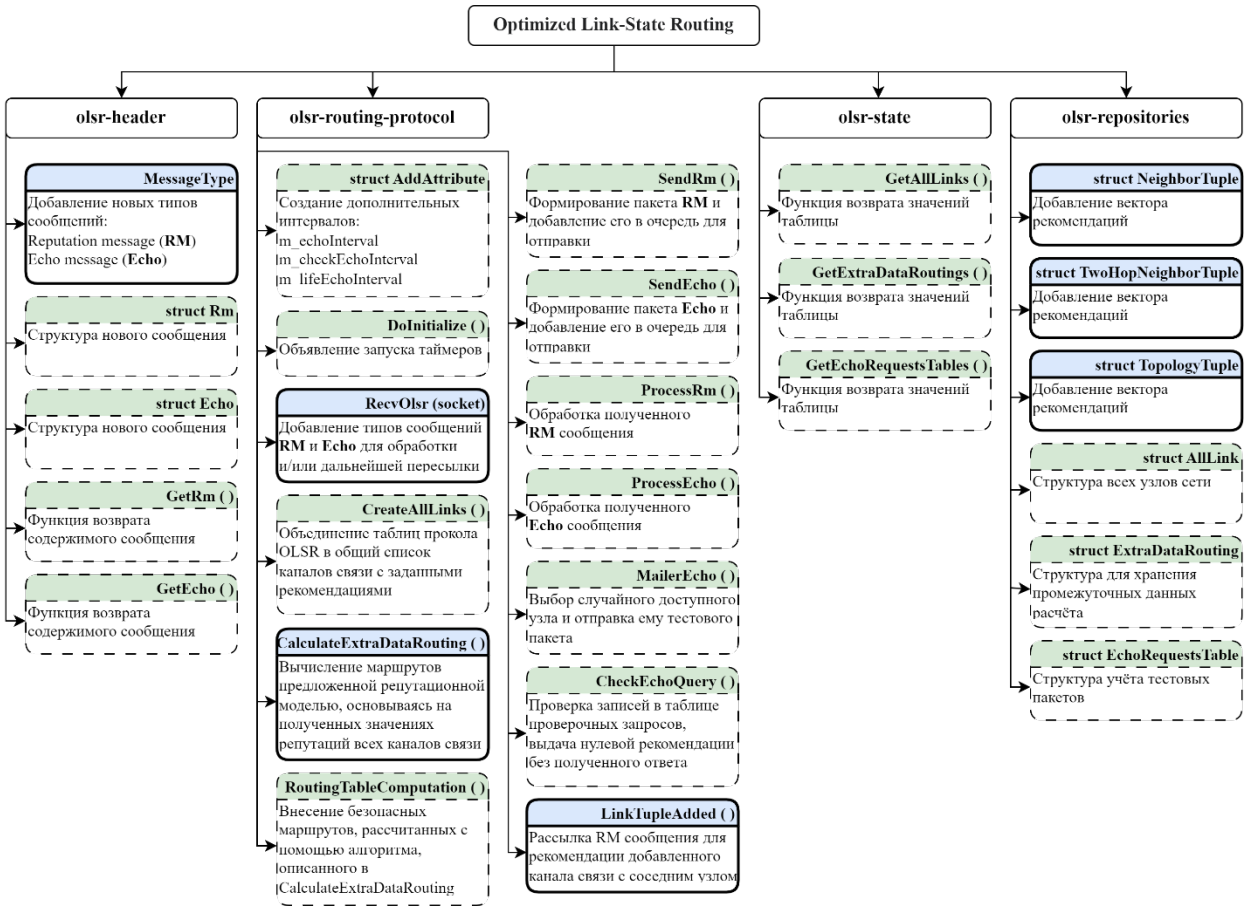


Рисунок 4. Имплементация разработанного комплекса решений на базе OLSR

В **третьей главе** было предложено описание модели нарушителя, используемой в работе. В рамках принятой модели нарушителя, реализуется угроза частичного или полного нарушения доступности передаваемых данных посредством действий узла нарушителя, препятствующих дальнейшей передаче поступающих пакетов по направлению к узлу назначения.

Было сделано предположение, что любой узел нарушителя является внутренним узлом беспроводной самоорганизующейся сети. Реализация узлом нарушителя угрозы нарушения доступности сетевых пакетов осуществляется посредством организации сетевой атаки типа «черная дыра» или «серая дыра». В результате действий нарушителя в ходе проведения указанной атаки все или некоторая часть поступающих от других узлов сетевых пакетов уничтожается без дальнейшей передачи по направлению к целевому узлу. В то же время в рамках принятой модели, узел нарушителя может продолжать отправку и маршрутизацию служебных пакетов, что позволяет ему скрывать проведение сетевой атаки и продолжать участие в объявлении сетевых маршрутов. Указанная модель нарушителя была реализована на базе проактивного протокола маршрутизации OLSR в рамках сетевого симулятора NS-3.

В целях анализа эффективности предложенного комплекса решений по обеспечению безопасности маршрутизации сетевых пакетов был разработан план экспериментальных исследований посредством имитационного моделирования передачи сетевых пакетов в самоорганизующихся сетях с участием узлов нарушителей. Для экспериментальной оценки безопасности маршрутизации сетевых пакетов был выбран стандартный сценарий типа

«транзитная сеть». В рамках указанного сценария два узла, выступающие в качестве источника и получателя пакетов, выполняют роль стационарных базовых станций и находятся за пределами прямой видимости, а устройства, размещенные в области между ними, выступают в роли ретрансляторов, обеспечивающих связь между ними.

Каждый проведенный эксперимент представлял серию независимых испытаний с идентичными входными параметрами. В ходе каждого испытания для определения начальной сетевой топологии 50 транзитных узлов распределялись случайным равномерным образом по области размерности 900x600 м^2. Последовательное применение протоколов маршрутизации OLSR и BOLSR для обнаружения маршрутов доставки пакетов в рамках каждого испытания на основе определенной начальной сетевой топологии было использовано в целях последующего сравнительного анализа полученных результатов.

Для графической демонстрации схемы проведения экспериментальных исследований на рисунке 5 представлена одна из использованных сетевых топологий и обозначены маршруты доставки пакетов от отправителя до получателя, определенные при помощи OLSR и BOLSR. Пунктирной линией ограничена область расположения транзитных узлов.

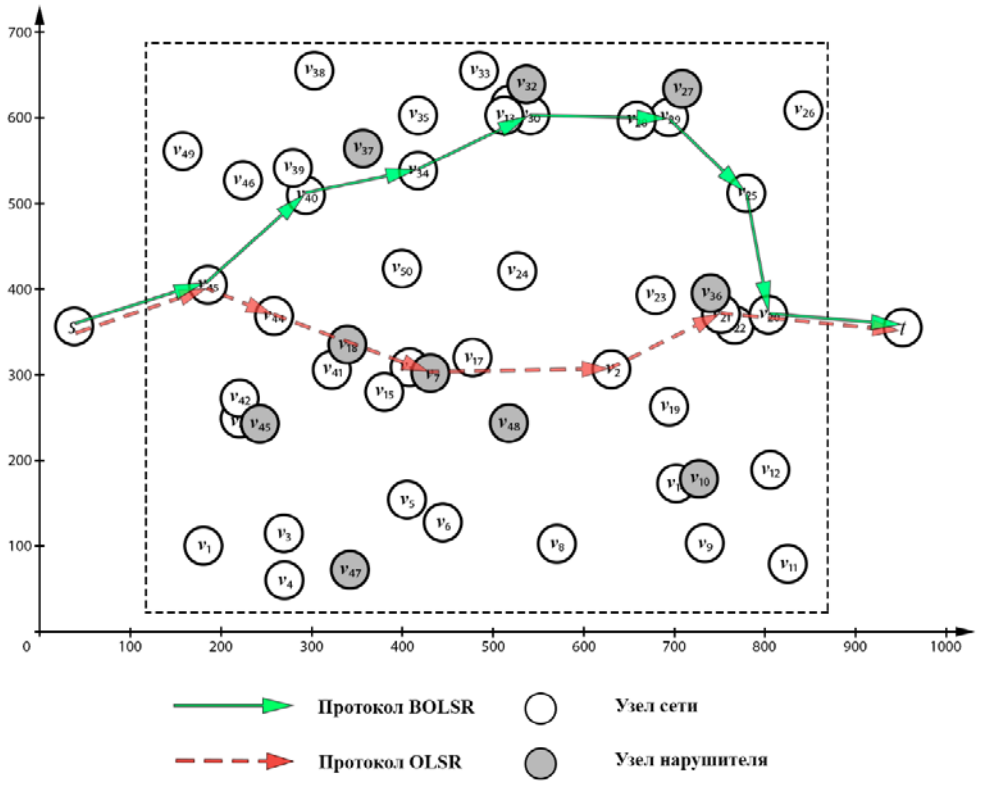


Рисунок 5. Выбор маршрутов при использовании OLSR и BOLSR

В рамках выбранного сценария было проведено несколько экспериментов с разным числом транзитных узлов нарушителей (от 0 до 6 узлов). Учитывая ограничение на общее число узлов нарушителей в соответствии с параметрами каждого эксперимента, в рамках каждого испытания любой транзитный узел выступал либо в качестве легитимного, либо в качестве вредоносного узла.

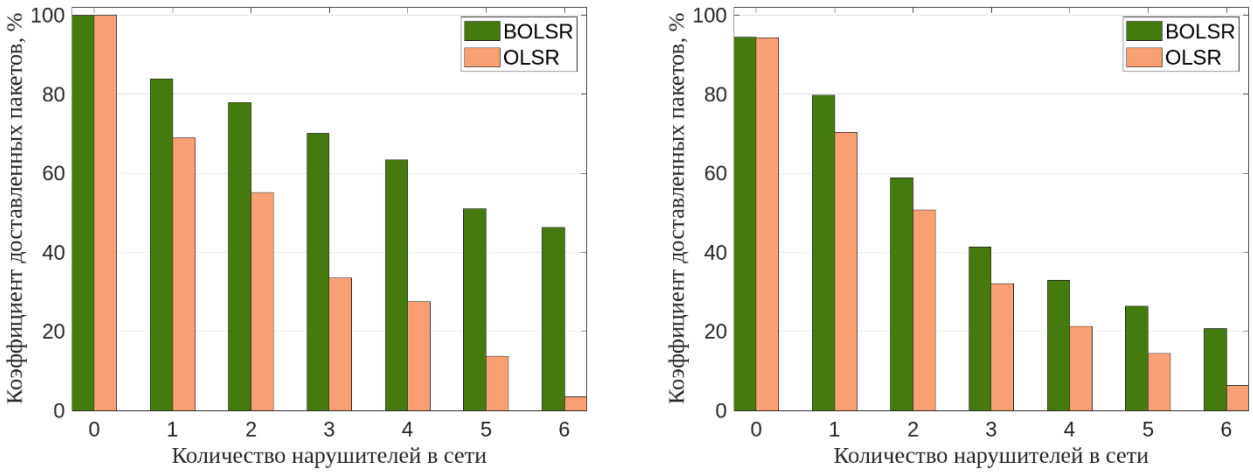
Основные условия проведенного экспериментального исследования в сетевом симуляторе NS-3 представлены в таблице 2. Для повышения точности оценки указанных характеристик в рамках каждого эксперимента с заданным набором входных параметров было проведено 100 независимых испытаний. Положение транзитных устройств определялось случайным образом согласно модели симулятора «Random Rectangle Position Allocator». В рамках испытаний в сетях с динамической топологией была предусмотрена мобильность устройств согласно модели случайного направленного движения «Random Direction 2D» со скоростью в диапазоне от 0 до 10 м/с. В ходе каждого испытания

выделенным узлом-источником осуществлялась отправка сетевых пакетов с постоянной скоростью передачи до выделенного узла-назначения.

Таблица 2. Параметры экспериментального исследования

Параметры эксперимента	**Значение**
Количество повторений	100
Время симуляции	180 с
Площадь расположения узлов	600м x 900м
Количество устройств в сети	52
Мобильность устройств	[Статическая, Случайное направленное движение]
Радиус взаимодействия	200 м
Протоколы маршрутизации	[OLSR, BOLSR]
Передаваемые данные	UDP
Частота отправки пакетов	CBR - 1 пакет (64 байта) / сек.
Количество нарушителей	[0 - 6]
Наблюдаемые характеристики	Коэффициент доставки пакетов, Количество маршрутов через узлы нарушителей, Средняя длина маршрута

На первом этапе было проанализировано изменение коэффициента доставки пакетов в сетях со статической и динамической топологией в условиях воздействия на процесс маршрутизации пакетов различного количества вредоносных узлов (рисунок 6).



а) *б)*

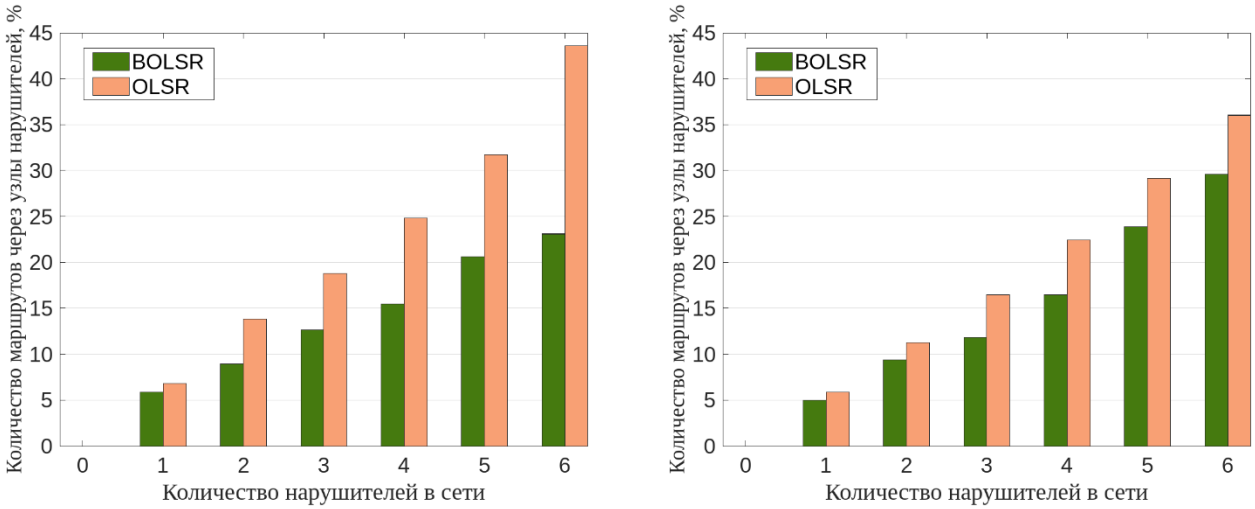
Рисунок 6. Коэффициент доставки пакетов в сетях со статической топологией (*а*) и динамической топологией (*б*) при различном количестве узлов нарушителей

В результате анализа было отмечено, что при отсутствии в сети узлов нарушителей, доставка пакетов через транзитные узлы сети происходит в штатном режиме, а коэффициент доставки пакетов принимает максимально возможное значение вне зависимости от используемого протокола маршрутизации. В то же время с увеличением числа узлов нарушителей в сети коэффициент доставки пакетов непрерывно снижается. Таким образом, было получено экспериментальное обоснование адекватности предложенной и реализованной модели нарушителя в самоорганизующихся сетях.

Далее был выполнен сравнительный анализ изменения коэффициента доставки пакетов при использовании протоколов маршрутизации OLSR и BOLSR (рисунок 6). Было отмечено, что применение разработанного протокола маршрутизации BOLSR вместо протокола OLSR позволило повысить коэффициент доставки пакетов в сетях со статической топологией в среднем в 3,68 раза и в сетях с динамической топологией в среднем в 1,75 раза.

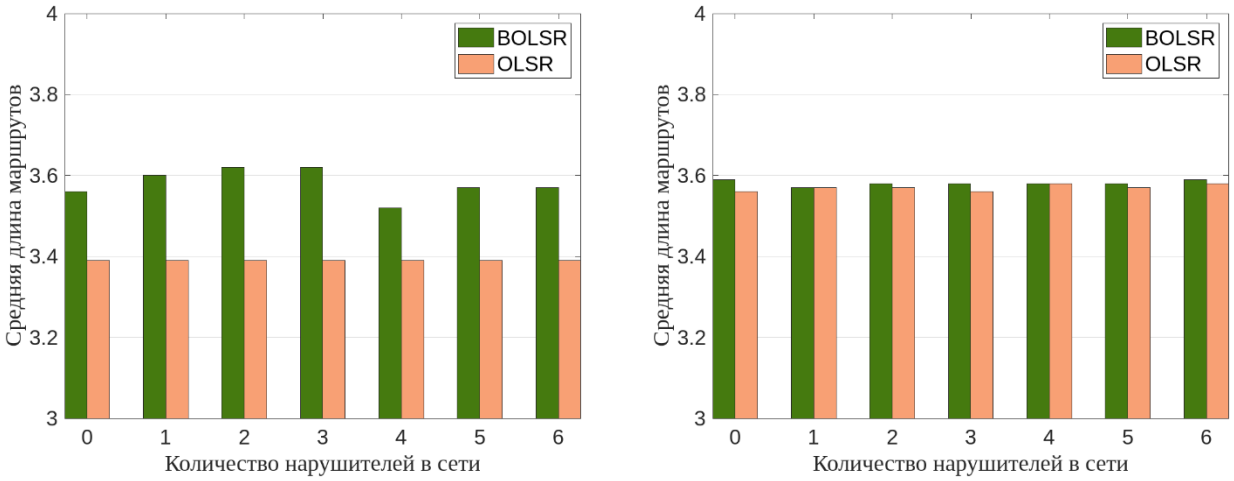
Кроме того, был выполнен сравнительный анализ средней длины используемых маршрутов и относительного количества маршрутов, проходящих через узлы нарушителей, при использовании протоколов маршрутизации OLSR и BOLSR.

Результаты экспериментальной оценки среднего относительного количества маршрутов, проходящих через узлы нарушителей, представлены на рисунке 7. Было отмечено, что применение протокола маршрутизации BOLSR вместо протокола OLSR позволило сократить относительное количество маршрутов через узлы нарушителей в сетях со статической и динамической топологией (в среднем в 1,53 раза в сетях со статической топологией и в 1,27 в сетях с динамической топологией). При этом при увеличении числа узлов нарушителей в сети количество маршрутов через эти узлы растёт медленнее в случае использования протокола маршрутизации BOLSR.



а) *б)*

Рисунок 7. Относительное количество маршрутов через узлы нарушителей в сетях со статической топологией (*а*) и динамической топологией (*б*)



а) *б)*

Рисунок 8. Средняя длина маршрутов в сетях со статической топологией (*а*) и динамической топологией (*б*)

Результаты экспериментальной оценки средней длины маршрутов представлены на рисунке 8. Было отмечено, что применение протокола маршрутизации BOLSR вместо протокола OLSR в сетях со статической топологией в рамках заданного эксперимента привело к незначительному увеличению средней длины маршрутов в пределах от 3 до 7% в зависимости от числа узлов нарушителей. При этом в сетях с динамической топологией увеличение средней длины маршрутов не превысило 1%.

Таким образом, было установлено, что применение протокола маршрутизации BOLSR вместо протокола OLSR позволило существенно сократить относительное количество маршрутов через узлы нарушителей при незначительном увеличении средней длины маршрутов.

В заключении представлены основные результаты и выводы, полученные в ходе проведения диссертационного исследования.

В приложениях приведены фрагменты листингов программной реализации, документы, подтверждающие внедрение, свидетельства о регистрации программ для ЭВМ.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ

Основные результаты и выводы, полученные в ходе проведения диссертационного исследования, заключаются в следующем:

1. Разработана новая репутационная модель доверия для обеспечения безопасности маршрутизации в самоорганизующихся сетях. В рамках указанной модели глобальная репутация каналов связи определяется посредством булевозначного вектора, что позволяет полностью учитывать объем данных, используемый для расчета репутации, при этом оценки, полученные из различных источников, не смешиваются при определении значения репутации, что позволяет учитывать качество источника получаемых оценок. Оценка репутации в рамках модели имеет абсолютное, а не относительное значение. Модель допускает возможность расширения для поддержки функционального и реферального доверия. Для предложенной репутационной модели был разработан способ взаимодействия узлов сети в целях определения репутации каналов связи узлами сети;

2. Разработан алгоритм поиска наиболее безопасных маршрутов от некоторого узла до всех узлов сети. Учитывая вогнутую метрику безопасности маршрутов, определенную в рамках репутационной модели, указанный алгоритм позволяет находить маршруты с наилучшей репутацией, что позволяет избегать узлы с низкой репутацией при доставке пакетов и тем самым повысить безопасность процесса маршрутизации. Предложенный алгоритм имеет теоретическую временную сложность $O(n^3)$;

3. Выполнена имплементация разработанной репутационной модели и алгоритма поиска наиболее безопасных маршрутов для проактивного протокола маршрутизации OLSR. Применение предложенной репутационной модели в рамках полученного протокола маршрутизации позволяет формировать и использовать наиболее безопасные сетевые маршруты и тем самым повысить безопасность передачи пакетов данных в сравнении с исходным протоколом OLSR. Указанная имплементация была программно реализована в качестве протокола маршрутизации BOLSR;

4. Выполнено экспериментальное обоснование эффективности комплекса разработанных решений в различных сценариях посредством имитационного моделирования маршрутизации в сетевом симуляторе NS-3.

Таким образом, все задачи, поставленные в рамках диссертационного исследования, были успешно выполнены. Диссертация представляет собой законченную самостоятельную научно-квалификационную работу, в которой решена научная задача повышения безопасности маршрутизации сетевых пакетов в динамически организуемых телекоммуникационных сетях посредством разработки и имплементации новой репутационной модели доверия для узлов сети.

Перспективы дальнейшего развития диссертационного исследования заключаются в разработке новых способов определения репутации каналов связи (с целью дальнейшего

повышения эффективности применения разработанной репутационной модели), в разработке эвристического алгоритма поиска наиболее безопасных маршрутов (с целью повышения производительности обнаружения маршрутов в условиях динамически изменяемой топологии сети), в расширении предложенной репутационной модели для поддержки реферального и функционального доверия, а также контекста взаимодействия участников самоорганизующейся сети.

СПИСОК ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях из Перечня ВАК:

1. **Литвинов, Г. А.** Экспериментальное исследование репутационной модели для поиска маршрута в самоорганизующихся сетях / Г. А. Литвинов // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 3 (45). – С. 69–75.
2. **Литвинов, Г. А.** Применение моделей доверия и репутации для обеспечения безопасности маршрутизации в динамически организуемых сетях / Г. А. Литвинов, Е. В. Щерба // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 3 (41). – С. 12–23.
3. Щерба, Е. В. Алгоритм поиска оптимального маршрута для обеспечения качества обслуживания в переограниченных случаях / Е. В. Щерба, **Г. А. Литвинов** // Вестник компьютерных и информационных технологий. – 2020. – Т. 17, № 3. – С. 3–10.
4. Щерба, Е. В. Задача обеспечения качества обслуживания на базе протокола маршрутизации OLSR: подходы, алгоритмы, решения / Е. В. Щерба, **Г. А. Литвинов**, М. В. Щерба // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2019. – Т. 22, № 1. – С. 55–65.
5. Щерба, Е. В. Обеспечение безопасности протоколов маршрутизации для телекоммуникационных сетей с динамической топологией / Е. В. Щерба, В. И. Никонов, **Г. А. Литвинов** // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2018. – Т. 21, № 3. – С. 19–29.

Публикации в изданиях, индексируемых базами данных Scopus и Web of Science:

6. **Litvinov, G.** Implementation of the Reputation Model for Secure Routing Based on the OLSR Protocol / G. Litvinov, E. Shcherba // International Conference Engineering and Telecommunication. – IEEE, 2021. – С. 1–4.
7. Shcherba, E. V. A Novel Reputation Model for Trusted Path Selection in the OLSR Routing Protocol / E. V. Shcherba, **G. A. Litvinov**, M. V. Shcherba // International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2019. – P. 1–5.
8. Shcherba, E. V. Securing the Multipath Extension of the OLSR Routing Protocol / E. V. Shcherba, **G. A. Litvinov**, M. V. Shcherba // Dynamics of Systems, Mechanisms and Machines (Dynamics) / Omsk State Technical University. – IEEE, 2019. – P. 1–4.
9. **Litvinov, G.** Modeling Message Spoofing Attacks on the OLSR Routing Protocol / G. Litvinov, E. Shcherba // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) (Yekaterinburg, 25–26 April 2019). – IEEE, 2019. – P. 299–302.
10. Shcherba, E. V. Modeling the Optimal Path for QoS-aware Routing in the Over-Constrained Case / E. V. Shcherba, **G. A. Litvinov** // Dynamics of Systems, Mechanisms and Machines (Dynamics) / Omsk State Technical University. – IEEE, 2018. – P. 1–5.
11. Leonov, A. V. Simulation-Based Performance Evaluation of AODV and OLSR Routing Protocols for Monitoring and SAR Operation Scenarios in FANET with Mini-Uavs / A. V. Leonov, **G. A. Litvinov** // Dynamics of Systems, Mechanisms and Machines (Dynamics) / Omsk State Technical University. – IEEE, 2018. – P. 1–6.
12. Leonov, A. V. Considering AODV and OLSR routing protocols to traffic monitoring scenario in FANET formed by mini-UAVs / A. V. Leonov, **G. A. Litvinov** // XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). – IEEE, 2018. – P. 229–237.

13. Leonov, A. V. About applying AODV and OLSR routing protocols to relaying network scenario in FANET with mini-UAVs / A. V. Leonov, **G. A. Litvinov** // XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). – IEEE, 2018. – P. 220–228.
14. Korneev, D. A. Estimation of mini-UAVs network parameters for search and rescue operation scenario with Gauss-Markov mobility model / D. A. Korneev, A. V. Leonov, **G. A. Litvinov** // Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). – IEEE, 2018. – P. 1–7.
15. Leonov, A. V. Simulation and analysis of transmission range effect on AODV and OLSR routing protocols in flying ad hoc networks (FANETs) formed by mini-UAVs with different node density / A. V. Leonov, **G. A. Litvinov**, D. A. Korneev // Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). – IEEE, 2018. – P. 1–7.
16. **Litvinov, G. A.** Applying static mobility model in relaying network organization in mini-uavs based FANET / G. A. Litvinov, A. V. Leonov, D. A. Korneev // Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). – IEEE, 2018. – P. 1–7.
17. Leonov, A. V. Simulation-based packet delivery performance evaluation with different parameters in flying ad-hoc network (FANET) using AODV and OLSR / A. V. Leonov, **G. A. Litvinov** // Journal of Physics: Conference Series. – IOP Publishing, 2018. – T. 1015, № 3. – P. 1–15.
18. Leonov, A. V. Simulation and comparative analysis of packet delivery in flying ad hoc network (FANET) using AODV / A. V. Leonov, **G. A. Litvinov**, E. V. Shcherba // 19th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM). – IEEE, 2018. – P. 71–78.
19. Leonov, A. V. Simulation-based packet delivery performance evaluation with different parameters in flying ad-hoc network (FANET) using OLSR / A. V. Leonov, **G. A. Litvinov**, D. A. Korneev // 19th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM). – IEEE, 2018. – P. 79–85.
20. Leonov, A. V. Applying AODV and OLSR routing protocols to air-to-air scenario in flying ad hoc networks formed by mini-UAVs / A. V. Leonov, **G. A. Litvinov** // Systems of Signals Generating and Processing in the Field of on Board Communications. – IEEE, 2018. – P.1–10.
21. Shcherba, E. V. On an optimal solution for multi-constrained routing problem in the over-constrained case / E. V. Shcherba, **G. A. Litvinov** // Moscow Workshop on Electronic and Networking Technologies (MWENT). – IEEE, 2018. – P. 1–4.
22. Shcherba, E. V. Finding Disjoint Paths in Boolean-Valued Networks / E. V. Shcherba, **G. A. Litvinov** // 26th Telecommunications Forum (TELFOR). – IEEE, 2018. – P. 1–4.

Свидетельства о регистрации программ для ЭВМ:

23. Свидетельство о государственной регистрации программы для ЭВМ № 2018666677. Российская Федерация. Генератор случайных геометрических булевозначных сетей : № 2018664100 : заявл. 07.12.2018 : опубл. (зарег.) 19.12.2018 / **Г. А. Литвинов**, Е. В. Щерба ; заявитель ОмГТУ.
24. Свидетельство о государственной регистрации программы для ЭВМ № 2019666281. Российская Федерация. Моделирование атаки с изменением служебных сообщений протокола маршрутизации OLSR : № 2019664929 : заявл. 22.11.2019 : опубл. (зарег.) 06.12.2019 / **Г. А. Литвинов**, Е. В. Щерба ; заявитель ОмГТУ.
25. Свидетельство о государственной регистрации программы для ЭВМ 2021661846. Российская Федерация. Репутационный модуль поиска наиболее безопасных маршрутов для протокола маршрутизации OLSR : № 2021661027 : заявл. 14.07.2021 : опубл. (зарег.) 16.07.2021 / **Г. А. Литвинов**, Е. В. Щерба ; заявитель ОмГТУ.

Диссертант Г.А. Литвинов

Печатается в авторской редакции

Подписано в печать 26.06.23 г. Формат 60x84/16.
Отпечатано на дупликаторе. Усл.печ.л. 1,16.
Тираж 100 экз. Заказ 121.

Типография: 644050, Омск-50, пр. Мира, 11, т.: 65-32-08.
Омский государственный технический университет,
отдел научной информации