Федеральное государственное автономное образовательное учреждение
высшего образования
«Омский государственный технический университет»

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

Диссертация
на соискание ученой степени
кандидата технических наук

Научный руководитель
кандидат технических наук, доцент
Щерба Евгений Викторович

Омск – 2023

Оглавление

Введение

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 положения, 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 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 Международная молодежная научно-практическая конференция 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 23 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;

• 18 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.

Глава 1 Проблема обеспечения безопасности маршрутизации в самоорганизующихся сетях

1.1 Маршрутизация в самоорганизующихся сетях: протоколы и модели

Совершенствование беспроводных технологий передачи данных за последние 25 лет способствовало образованию новых форм сетевого взаимодействия. В частности, распространение получили сети с ячеистой топологией (mesh), каждый узел которых может напрямую взаимодействовать с другими узлами сети, которые находятся в пределах его диапазона передачи. Для связи с узлами, находящимися за пределами диапазона, узел должен полагаться на промежуточные узлы, выполняющие ретрансляцию сообщений. Таким образом, каждый узел такой сети должен предоставлять услуги пересылки пакетов для других устройств, т.е. фактически выступать в качестве маршрутизатора.

Дальнейшее развитие указанной концепции и появление множества мобильных беспроводных устройств различного типа и назначения привело к формированию технологий беспроводных самоорганизующихся сетей [1]. Такие сети формируются динамически автономной системой мобильных узлов, соединенных беспроводными каналами без использования существующей сетевой инфраструктуры или централизованного администрирования. Узлы могут свободно перемещаться и произвольно устанавливать сетевые соединения друг с другом. Таким образом, топология таких сетей является динамической, так как может меняться быстро и непредсказуемо.

Среди большого количества исследований по различным аспектам функционирования беспроводных самоорганизующихся сетей принято выделять несколько основных направлений, которые охватывают технологии самоорганизующихся сетей мобильных устройств (MANET), самоорганизующихся сетей беспилотных летательных аппаратов (FANET), самоорганизующихся сетей интеллектуальной транспортной системы (VANET) и другие [3, 4].

Указанные типы самоорганизующихся сетей имеют специфические характеристики в рамках данной классификации. Например, скорость и направление движения, плотность узлов на рассматриваемой площади, количество связей между узлами и т.д. Многие ключевые показатели эффективности и свойства беспроводных самоорганизующихся сетей различных типов, таких как MANET, VANET, FANET и др., напрямую зависят от протокола маршрутизации, используемого в сети [2].

Маршруты между узлами в беспроводной самоорганизующейся сети могут включать в себя несколько переходов, и, следовательно, такие сети уместно называть многошаговыми. Маршрутизация в таких сетях является сложной задачей, а подходы, являющиеся эффективными в сетях с постоянной топологией, работают неэффективно или не работают вовсе. Таким образом, для применения в самоорганизующихся сетях был разработан ряд специализированных протоколов маршрутизации, которые учитывают возможность их применения на каждом узле сети и обеспечивают быструю адаптацию маршрутов к изменениям сетевой топологии.

Протоколы маршрутизации мобильных самоорганизующихся сетей можно классифицировать на следующие основные группы: протоколы проактивной маршрутизации, протоколы реактивной маршрутизации, гибридные протоколы, а также протоколы, использующие данные о географическом положении узлов [5]. Указанная классификация отражает основные подходы, которые сложились к настоящему времени при анализе проблемы маршрутизации в самоорганизующихся сетях и указывает на возможность применения указанных групп протоколов в различных сценариях (рисунок 1).

Проактивные протоколы обуславливают наличие на каждом узле таблицы маршрутизации, которая на постоянной основе содержит оптимальные маршруты до каждого узла сети. В данном классе протоколов узлы осуществляют периодический обмен управляющими сообщениями с целью поддержки целостности и достоверности информации о сетевой топологии.

Использование проактивных протоколов приводит к быстрому росту загрузки сети и потреблению энергоресурсов каждым узлом при увеличении подвижности и количества узлов. К протоколам проактивного типа маршрутизации можно отнести: **TBRPF** (Topology dissemination base on reverse-path forwarding), **DSDV** (Destination-Sequenced Distance-Vector Routing), **FSR** (Fisheye State Routing), **OLSR** (Link State Routing Protocol), а также некоторые другие.

Рисунок 1. Классификация протоколов маршрутизации

При использовании реактивных протоколов узел начинает поиск маршрута до узла назначения только при необходимости доставки пакета. Для отправки пакета узел может использовать существующий маршрут, хранящийся в таблице маршрутизации, либо обнаружить новый маршрут, используя доступные каналы связи. Основным недостатком данной группы протоколов является рост задержек на поиск первичного маршрута при увеличении подвижности и количества узлов. К протоколам реактивного типа можно отнести: **LMR** (Lightweight Mobile Routing), **TORA** (Temporally-Ordered Routing Algorithms), **AODV** (Ad-hoc On demand Distance Vector Routing), **DSR** (Dynamic Source Routing) [6], а также некоторые другие.

Гибридные протоколы сочетают в себе механизмы проактивных и реактивных протоколов на разных уровнях иерархии, определяя помимо метода поиска маршрута и метод разбития сети на иерархические структуры или домены. Недостатками гибридных протоколов являются относительная

сложность реализации и снижение производительности маршрутизации, что связано с необходимостью разбиения структуры сети на кластеры. К наиболее известным протоколам такого типа можно отнести: **HWMP** (Hybrid Wireless Mesh Protocol), **HDVG** (Hierarchical Distance-Vector Georouting), **ZRP** (Zone Routing Protocol).

Для их успешного применения в самоорганизующихся сетях протоколы маршрутизации должны [7]:

- функционировать в одноранговой сетевой архитектуре, где все узлы априори являются равноправными и каждый из узлов может выступать в качестве маршрутизатора;
- способствовать надежной доставке пакетов в условиях динамической сетевой топологии, когда использование классических механизмов гарантированной доставки затруднено;
- обеспечивать обнаружение маршрута за малое время при постоянно изменяющейся топологии сети;
- обладать механизмами оперативного обнаружения разрыва маршрута и его восстановления;
- не допускать образования цикличных маршрутов;
- минимизировать объем служебных данных, рассылаемых в процессе своего функционирования;
- обладать высокой масштабируемостью;
- поддерживать обеспечение гарантированного качества связи (QoS).

Протоколы маршрутизации проактивного типа хранят информацию о найденных маршрутах в течение заданного временного периода, что позволяет сократить время на нахождение маршрута в случае его необходимости. Протокол **Optimized Link State Routing** (OLSR) относится к группе протоколов, учитывающих характеристики доступных каналов связи при определении маршрутов, и является одним из наиболее известных, распространённых и широко используемых проактивных протоколов маршрутизации в самоорганизующихся сетях малого и среднего размера [9].

Протокол OLSR отличается концепцией многоточечных ретрансляторов – шлюзов MPR (Multi Point Relay), которая оптимизирует процесс рассылки служебных данных, значительно сокращая потребление ресурсов [9, 11]. Указанная концепция позволяет существенно уменьшить количество отправляемых служебных сообщений по сравнению с традиционным широковещательным процессом рассылки, в рамках которого каждый узел объявляет маршруты и ретранслирует получаемые служебные сообщения всем соседним узлам [12].

Каждый узел в рамках указанного протокола регулярно производит обнаружение соседних узлов, доступных за один и за два перехода, на основе широковещательных сообщений приветствия (HELLO). Среди всех узлов, доступных за один переход, осуществляется оптимальный выбор подмножества шлюзов MPR, совокупно обеспечивающих связь со всеми узлами, доступными для исходного узла за два перехода. Выбор набора шлюзов MPR некоторым узлом осуществляется каждый раз, когда обнаруживается изменение топологии в сфере с радиусом 1 или 2 перехода по отношению к рассматриваемому узлу. Сама процедура выбора шлюзов MPR не стандартизована, её реализация остается на усмотрение разработчика [9].

Итак, каждый узел сети определяет свой набор шлюзов MPR из его симметричного одноперехoдного окружения. Выбор осуществляется таким образом, чтобы суммарное радиочастотное покрытие входящих в набор MPR узлов охватывало все симметричное двупереходное окружение исходного узла. Полученный набор шлюзов MPR должен удовлетворять следующему требованию: каждый узел в строгом симметричном двупереходном окружении узла N должен иметь прямой симметричный канал связи с одним из шлюзов MPR(N).

Каждый узел, выбранный в качестве шлюза MPR, хранит информацию о наборе соседей, которые выбрали его в качестве MPR. Этот набор именуется множеством узлов-селекторов (MPR Selector Set) узла и периодически

обновляется после приема сообщений HELLO от соседних узлов. Каждый шлюз MPR производит рассылку широковещательных сообщений TC (Topology Control), которые в обязательном порядке содержат объявления маршрутов к узлам-селекторам, выбравшим данный узел в качестве шлюза MPR. Данные сообщения принимаются и обрабатываются всеми соседними узлами, но ретранслируются далее по сети только узлами, выбранными в качестве шлюзов MPR. Соседним узлам некоторого узла, не входящим в его набор шлюзов MPR, запрещается ретранслировать широковещательный трафик, поступающий от рассматриваемого узла. Применение узлов ретрансляторов позволяет добиться уменьшения объема трафика посредством исключения избыточных ретрансляций, производимыми узлами в одной и той же области сети. В целом, чем меньше будет суммарное число шлюзов MPR среди всех узлов сети, тем меньше будет объем широковещательного трафика в этой сети [14, 15].

В рамках протокола OLSR служебные сообщения содержат порядковые номера, которые последовательно увеличиваются при появлении новых сообщений. Таким образом, получатель контрольных сообщений может обеспечить корректность обновления информации в локальной базе данных сетевой топологии.

На основе полученных служебных сообщений HELLO и TC каждый узел производит построение сетевой топологии и определяет оптимальные маршруты до всех получателей на основе алгоритма Дейкстры в соответствии с установленной метрикой [8]. В результате в пересылке пакетов данных могут участвовать только узлы, выбранные в качестве шлюза MPR каким-либо другим узлом.

Протокол OLSR является полностью распределенным, он не требует наличия каких-либо управляющих узлов. Кроме того, каждый узел периодически отправляет контрольные пакеты, поэтому протокол относительно устойчив к частичным потерям контрольных сообщений, что

довольно часто случается при передаче данных в беспроводных сетях с динамической топологией [14].

Наилучшие результаты протокол демонстрирует в сетях с большим количеством узлов. Благодаря проактивному подходу он обладает естественным контролем за объемом и периодичностью служебного трафика и по сравнению с реактивными протоколами, при использовании которых могут возникать всплески служебного трафика в ходе поиска необходимого маршрута, обеспечивает более высокую стабильность каналов в сети. В сетях с высокой плотностью узлов протокол OLSR может обеспечивать сокращение объема служебного трафика на несколько порядков по сравнению с протоколами, использующими традиционные техники ретрансляции [12].

Спецификации протокола определяют базовую и дополнительную составляющие части. Базовая часть обеспечивает функционирование замкнутой самостоятельной самоорганизующейся сети, дополнительные функции служат для расширения стандарта. Протокол допускает наличие гетерогенных узлов, одни из которых поддерживают некоторые дополнительные функции, а другие – нет.

Базовое ядро регламентирует поведение узла, укомплектованного сетевым интерфейсом OLSR, являющегося членом самоорганизующейся сети и использующего OLSR в качестве протокола маршрутизации [9]. В частности, определяются:

- Формат пакета и метод распространения служебного многоадресного трафика. Определение активности каналов между локальным интерфейсом и удаленными интерфейсами узлов-соседей через периодическую пересылку сообщения HELLO, отдельно для каждого интерфейса, активность канала на котором проверяется. Если канальный уровень стека протоколов содержит информацию о наличии активного соединения, она может быть использована вместо обмена сообщениями HELLO;

- Регистрация узлов-соседей. В случае сети, состоящей из узлов с одним сетевым интерфейсом, каждый узел может определить набор соседей и их сетевых адресов непосредственно из процедуры определения активности канала. В случае наличия узлов с несколькими интерфейсами необходима дополнительная информация, чтобы соотнести адреса сетевых интерфейсов с адресами узла. Эта дополнительная информация распространяется через сообщения MID (Multiple Interface Declaration);
- Выбор шлюзов MPR и сигнализирование. Задача выбора шлюзов MPR некоторым узлом заключается в вычислении такого набора соседних узлов, чтобы широковещательное сообщение, ретранслированное этими соседями, было получено всеми узлами, находящимися на расстоянии в два шага (перехода) от данного узла. MPR набор определяется для каждого интерфейса узла отдельно. Информация, необходимая для этого, передается через периодический обмен сообщениями HELLO;
- Процедура распространения сообщений о топологии сети посредством сообщений TC (Topology Control). Как проактивный протокол маршрутизации, OLSR поддерживает на каждом узле актуальную таблицу активных соединений в сети, необходимую для вычисления маршрутов;
- Вычисление маршрутов. Исходя из таблицы активных соединений и конфигурации сетевых интерфейсов узлов сети, на каждом узле вычисляется таблица маршрутизации. Это процесс специфицирован в разделе 19 стандарта RFC 7181 [9].

Стандарт также поддерживает следующий дополнительный функционал, который предусматривает ситуации, возможные при реализации протокола:

- Узлы могут иметь более одного сетевого интерфейса и совместно использовать другие протоколы маршрутизации;
- Предоставление дополнительной информации об используемом аппаратном обеспечении протоколами канального уровня;
- Необходимость сбора дополнительных сведений о топологии сети за счет увеличения количества передаваемой информации.

1.2 Угрозы безопасности маршрутизации в самоорганизующихся сетях

Обеспечение безопасности маршрутизации пакетов является одной из принципиальных проблем беспроводных самоорганизующихся сетей. Поскольку в таких сетях каждое устройство обеспечивает передачу пакетов для других устройств, т.е. по сути выступает в роли маршрутизатора, существует значительное количество общих и специфичных сетевых атак на процесс маршрутизации пакетов в беспроводных самоорганизующихся сетях.

Сетевые атаки на процесс маршрутизации пакетов в беспроводных самоорганизующихся сетях традиционно можно классифицировать как активные и пассивные. Совершение пассивной атаки узлом нарушителем связано с прослушиванием передаваемых данных и не приводит к созданию, изменению или уничтожению передаваемых сетевых пакетов [17, 18].

В ходе активной сетевой атаки узел нарушителя осуществляет воздействие на процесс маршрутизации, которое приводит к нарушению конфиденциальности, целостности или доступности передаваемой информации. Проведение активной атаки может быть связано, например, с изменением полей передаваемых сообщений, перенаправлением сетевого трафика, или уничтожением сетевых пакетов. Принято выделять следующие активные атаки на маршрутизацию в самоорганизующихся сетях [19, 22, 23]:

- Атаки на истощение сетевых ресурсов;
- Атаки с фильтрацией пакетов;
- Атаки с использованием фальсификации;
- Атака типа «червоточина»;
- Атака типа «воронка».

Активные атаки могут выполняться независимо, либо в комбинации с пассивными атаками, для сбора информации о поведении узлов сети.

Атаки на истощение сетевых ресурсов направлены на нарушение доступности передаваемой информации. Примером традиционной атаки данного типа может выступать атака переполнением таблиц маршрутизации (Routing Table Overflow) соседних устройств посредством объявления

большого числа маршрутов к несуществующим узлам. В случае переполнения таблицы маршрутизации добавить в неё новые легитимные маршруты уже не получится и, как следствие, доставка пакетов станет невозможной. Другая специфичная атака данного класса производится посредством истощения источников питания узлов. Для достижения целей атаки производится отправка фиктивных пакетов, обязательных для обработки [29]. Атакуемые узлы обязаны будут потратить вычислительную мощность и энергию своего элемента питания для обработки полученного сообщения.

Атака с фильтрацией пакетов также направлена на нарушение доступности передаваемой информации. Для достижения целей атаки узел нарушителя осуществляет препятствование распространению сетевых пакетов посредством их полной или частичной фильтрации [24, 25]. Фильтрация может затрагивать либо не затрагивать служебные пакеты протоколов маршрутизации. Атака с полной фильтрацией пакетов именуется как «черная дыра» (blackhole). В рамках данной атаки узел нарушителя отказывается от дальнейшей ретрансляции всех полученных пакетов данных (рисунок 2). Как правило, фильтрация служебных пакетов протокола маршрутизации не осуществляется. В противном случае узел может быть исключен из процесса сетевого взаимодействия в результате отсутствия маршрутов.

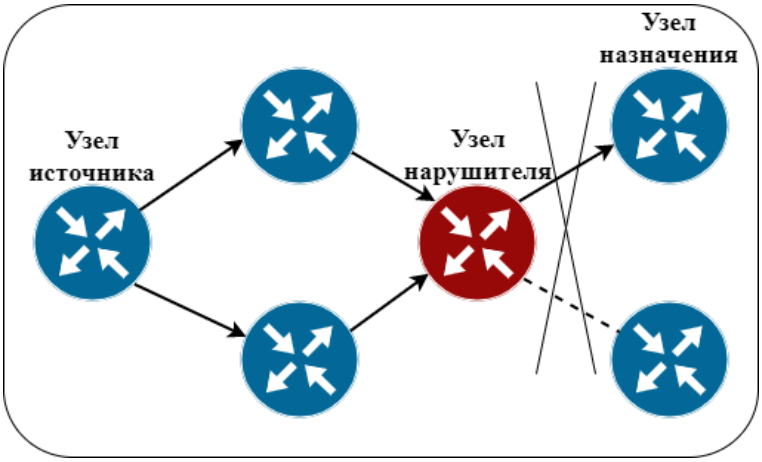

Рисунок 2. Схема атаки типа «черная дыра»

Атака с частичной фильтрацией пакетов именуется как «серая дыра» (grayhole). В рамках данной атаки узел нарушителя осуществляет уничтожение поступающих сетевых пакетов по определенным критериям, например, сетевой адрес узла источника или узла назначения, номера портов и т.д. [26]. Атака типа «серая дыра» может быть сложнее в отслеживании, так как набор правил и условий для фильтруемых узлом нарушителем пакетов заранее не известен (рисунок 3).

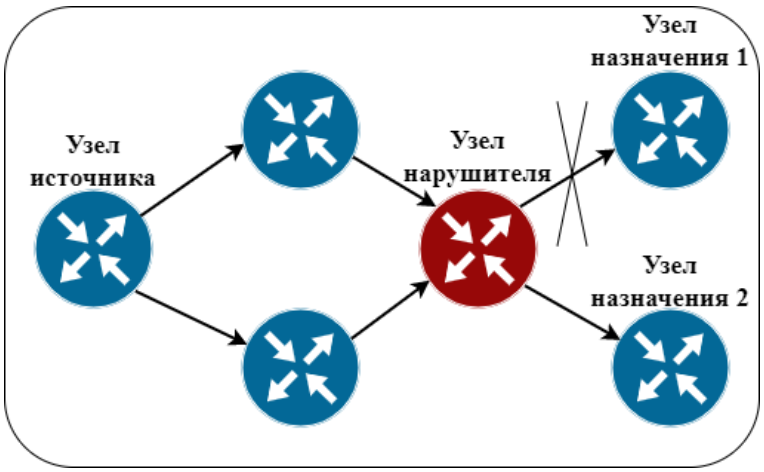

Рисунок 3. Схема атаки типа «серая дыра»

В рамках **атак с использованием фальсификации** узел нарушителя осуществляет рассылку фиктивных сетевых пакетов [27]. Указанные атаки могут быть направлены на нарушение конфиденциальности, целостности либо доступности информации. Помимо ранее рассмотренной атаки переполнения таблиц маршрутизации, путем фальсификации сообщений об ошибках маршрута, узел нарушителя может успешно реализовать атаку типа «отказ в обслуживании», рассылая ложные сообщения о недоступности легитимного узла. Также, путем фальсификации сообщений протокола маршрутизации, узел нарушителя может формировать ложные объявления маршрута до легитимного узла, реализуя атаку типа «человек посередине».

Атака типа «воронка» (sinkhole) представляет собой частный случай атаки с использованием фальсификации. Посредством рассылки фиктивных

сообщений протокола маршрутизации узел нарушителя может ввести в заблуждение соседние узлы, предоставив несуществующий оптимальный маршрут до любого узла назначения [28]. Таким образом узел нарушителя может перенаправить потоки сетевого трафика на своё устройство с большого количества узлов (рисунок 4).

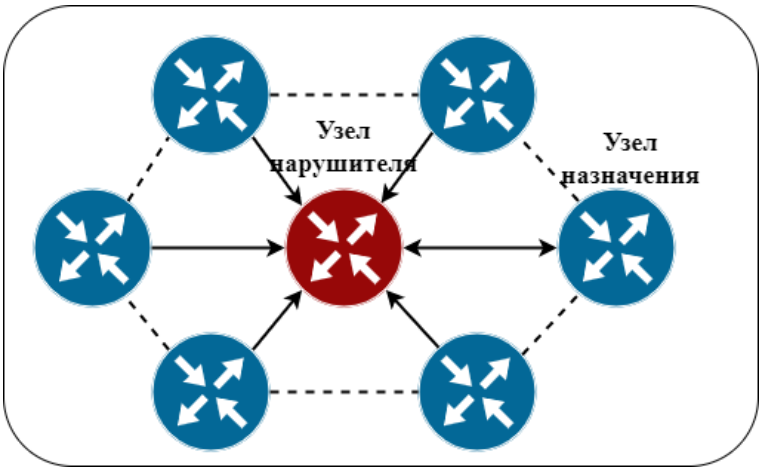

Рисунок 4. Схема атаки типа «воронка»

В рамках **атаки типа «червоточина»** (wormhole) осуществляется несанкционированный доступ к пакетам соседних устройств, передаваемых до получателя по реально существующему высококачественному каналу связи, созданному группой узлов нарушителей [23].

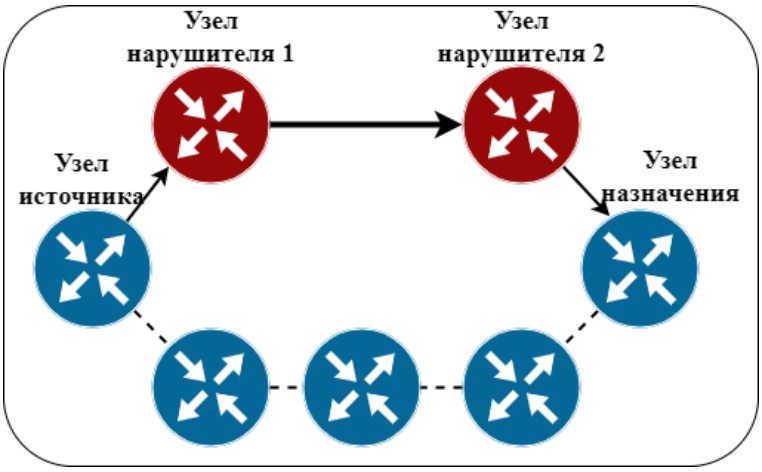

Рисунок 5. Схема атаки типа «червоточина»

1.3 Криптографический подход к обеспечению безопасности маршрутизации в самоорганизующихся сетях

В значительном количестве проектов, направленных на разработку технологий и протоколов передачи данных для самоорганизующихся сетей, в целях обеспечения безопасности маршрутизации пакетов задействуются криптографические механизмы. Как правило, цифровые сертификаты используются для аутентификации взаимодействующих сторон, цифровая подпись используется для обеспечения целостности и аутентичности передаваемых сообщений, а шифрование используется для защиты их конфиденциальности [33, 34].

Особое внимание ученых и разработчиков было уделено обеспечению безопасности реактивных протоколов маршрутизации. В частности, протокол SAODV (Secure AODV) был разработан для защиты службеных сообщений протокола AODV с помощью асимметричной криптосистемы [34]. Для аутентификации сообщений RREQ и RREP данного протокола был использован механизм электронных подписей. Каждое служебное сообщение должно быть подписано секретным ключом узла отправителя этого сообщения. Промежуточные устройства и узлы назначения должны производить проверку подписи и выполнять дальнейшую обработку и передачу сообщений только в результате подтверждения их подлинности.

Поскольку формат сообщений RREQ и RREP подразумевает наличие поля Hop_Count (количество переходов), модифицируемого в ходе передачи сообщения, аутентификация данного поля выполняется независимо при помощи цепочки хеш-значений. В момент запуска процесса поиска маршрута узел-источник определяет некоторое случайное число (seed) и верхнее ограничение числа переходов (MHC). После чего данный узел рассчитывает хеш-значение Hash от начального числа h(seed) и значение Top_Hash, как h^{MHC}(seed). При получении служебного сообщения все промежуточные узлы выполяют проверку допустимости значения Top_Hash, имея в виду настоящее значение поля Hop_Count, а затем увеличивают значение поля

Hop_Count и рассчитывают новое значение Hash как h(Hash) перед последующей отправкой служебного сообщения RREQ. При этом, одним из основных недостатков протокола SAODV можно считать сложность организации защищенного распределения ключей (уязвимость к сетевым атакам «человек посередине»).

Попытка устранить указанный недостаток была предпринята в рамках реактивного протокола маршрутизации ARAN (Authenticated routing for ad hoc networks) [35]. Данный протокол требует присутствия в самоорганизующейся сети удостоверяющего центра, при этом взаимная аутентификация узлов и обеспечение целостности передаваемых данных базируются на использовании криптографических сертификатов. Запутанный и ресурсоёмкий процесс аутентификации не позволил протоколу ARAN найти широкое применение. К прочим недостаткам указанного протокола маршрутизации следует отнести подверженность к атакам типа «вормхол».

Схема защиты проактивного протокола OLSR, предложенная в работе [36], также предусматривает применение инфраструктуры открытых ключей в целях формирования и проверки подписи каждого управляющего сообщения протокола. Генерируемая подпись содержит штамп времени и применяется для противодействия фальсификации или изменению распространяемых служебных пакетов, используемых для построения сетевой топологии. Вместе с тем, как уже было обозначено, проблема установления инфраструктуры открытых ключей ограничивает возможность использования предложенного решения в самоорганизующихся сетях.

Альтернативный подход к защите OLSRv1 на основе асимметричной криптографии предложен разработчиками протокола SLSP (Secure Link State Routing Protocol) [37]. В рамках указанного протокола каждый узел независимо формирует ключевую пару и распространяет сгенерированный открытый ключ, используя соседние узлы. Отправляемые пакеты HELLO и TC содержат электронную подпись отправителя сообщений. Таким образом,

указанный подход позволяет исключить задачу организации выделенного центра распределения ключей.

В результате протокол позволяет организовать безопасное установление отношений соседства и распространение данных о сетевых соединениях. Следует отметить, что протокол SLSP не подвержен атакам на таблицу маршрутизации, осуществляемым для её переполнения. Каждый узел определяет значение приоритета для всех соседних узлов. При этом узлы, формирующие наибольший объём обновлений маршрутизации, получают наименьший приоритет, что помогает исключить возможность организации атак типа «отказ в обслуживании». Несмотря на то, что данный протокол позволяет обеспечить защиту от индивидуальных внешних атак на процесс доставки сетевых пакетов, он не позволяет противостоять различным атакам сговора нескольких нарушителей.

В спецификациях RFC7181 был представлен механизм цифровой подписи для аутентификации и авторизации в OLSRv2 [10]. Авторы вводят концепцию управления доступом для сетей OLSRv2 и предлагают расширение безопасности на основе цифровых подписей. Они сравнивают несколько стандартных алгоритмов цифровой подписи, таких как: RSA, DSA, ECDSA и HMAC. Цель состоит в том, чтобы разрешить доверенным узлам и запретить нелегитимным узлам участвовать в обмене управляющими сообщениями между маршрутизаторами, тем самым обеспечивая режим работы, аналогичный традиционному механизму, используемому для контроля целостности в маршрутизируемых сетях. Кроме того, представлено исследование производительности предлагаемого расширения для количественной оценки влияния увеличения накладных расходов управляющего трафика и увеличения генерации сообщений, а также времени обработки. Авторы заметили, что HMAC требует значительно меньше времени, чем ECDSA, DSA и RSA, для создания и проверки подписи сообщения.

1.4 Обеспечение безопасности маршрутизации на основе концепции доверия и репутации узлов

Для защиты конфиденциальности и целостности передаваемых данных могут применятся криптографические преобразования, но указанный подход к обеспечению безопасности не позволяет обеспечить доступность информации в случае сетевых атак типа «черная дыра» и «серая дыра», реализуемых посредством полной или частичной фильтрации сетевого трафика внутренними узлами нарушителями [31].

В рамках противодействия указанным атакам повышение надёжности передачи данных может быть достигнуто посредством определения более безопасного маршрута между узлом отправителем и узлом получателем. Выбор безопасного маршрута доставки пакетов с учетом уровня доверия к узлам и каналам связи самоорганизующейся сети должен позволить исключить из процесса маршрутизации вредоносные узлы. Установление доверия в самоорганизующейся сети может осуществляться на основе моделей расчета репутации узлов и каналов связи [2, 3]. Для протоколов маршрутизации, предусматривающих кооперацию участников сети на основе предварительно установленных отношений доверия, репутация является главным показателем узлов и каналов связи. Посредством коллективного решения в отношении участников сети с низкой репутацией данные узлы могут быть исключены из процесса сетевого взаимодействия, т.е., иначе говоря, изолированы.

Основные принципы концепции доверия в сетях самоорганизующихся были сформированы в работе [38].

1. Метод определения доверия к взаимодействующему узлу должен быть полностью распределенным ввиду отсутствия третьей доверенной стороны (по типу удостоверяющего центра).
2. Определение доверия должно производиться гибким настраиваемым способом без излишней вычислительной и коммуникационной нагрузки, с учётом всей сложности и полноты доверительных отношений.

3. Определение доверия в самоорганизующейся сети не должно строиться на готовности к сотрудничеству всех узлов. В условиях ограниченных ресурсов эгоизм сторон может преобладать над готовностью к сотрудничеству, например, для экономии вычислительной мощности или расхода заряда батареи.

4. Доверие является динамическим, а не статическим.

5. Доверие носит субъективный характер.

6. Доверие не обязательно транзитивно. Тот факт, что A доверяет B и B доверяет C, не означает, что A доверяет C.

7. Доверие асимметрично и не обязательно является взаимным.

8. Доверие зависит от контекста. A может доверять B в одном качестве и не доверять в другом. Например, для решения трудоёмкой вычислительной задачи в самоорганизующейся сети узел с высокой вычислительной мощностью будет рассматриваться как доверенный, в то время как узел, который имеет низкую вычислительную мощность, но не является вредоносным, будет рассматриваться как не доверенный.

Возможно, впервые концепция установления доверительных отношений между участниками сети с целью их последующего взаимодействия была реализована в рамках протокола маршрутизации CORE [39]. Данный протокол использует принципы реактивного протокола DSR и предусматривает вычисление каждым участником сети базовой и косвенной репутации других участников сети. Базовая репутация вычисляется в результате собственного опыта, в то время как косвенная репутация формируется при получении информации от других узлов. Помимо этого, в рамках протокола определяется понятие функциональной репутации, ассоциированной с некоторой выбранной задачей (например, ретрансляция данных), и глобальной репутации, которая устанавливается на основе значений функциональных репутаций и соответствующих стоимостных мультипликаторов. Протокол позволяет узлам сети принимать решение об исключении узлов с низкой репутацией из процесса маршрутизации. К

важным свойствам протокола CORE можно отнести невозможность распространения негативных значений репутации, что способствует противодействию атакам типа «отказ в обслуживании», но, с другой стороны, оставляет возможность кооперации вредоносных узлов для необоснованного увеличения значения репутации.

Протокол CONFIDANT разработан как расширение для реактивных протоколов маршрутизации источника, предусматривающее установление отношений доверия и сотрудничество узлов [41]. Протокол определяет систему компонентов, которые взаимодействуют друг с другом для мониторинга, создания отчетов и определения маршрутов в обход узлов с некорректным поведением. В перечень компонентов входит сетевой монитор, подсистема репутации, диспетчер доверия и диспетчер маршрутов.

Монитор каждого узла в рамках протокола отслеживает поведение соседних узлов и соответствующим образом обновляет значение их репутации. Если узлы обнаруживают вредоносный узел, они могут сообщить об этом доверенным узлам, отправив сообщение тревоги (ALARM) с помощью диспетчера доверия. Входящие сигналы тревоги проверяются на достоверность. Когда другой узел получает такое сообщение, он вычисляет уровень доверия к этому сообщению на основании источника сигнала тревоги и общего количества тревожных сообщений о некорректном поведении узлов. Диспетчер доверия взаимодействует с таблицей сигналов тревоги, таблицей уровней доверия и таблицей всех доверенных узлов, которым узел будет отправлять сигналы тревоги.

Подсистема репутации отвечает за ведение локальной таблицы репутации узлов и «черного» списка. Доверенные узлы периодически обмениваются указанными списками, чтобы избежать их устаревания. Узел придает большее значение прямым наблюдениям по сравнению с информацией, полученной от других узлов. Всякий раз, когда значение репутации некоторого узла сети снижается ниже порогового значения, менеджер маршрутов выполняет их перестроение исходя из принятой метрики

безопасности, удаляя маршруты, проходящие через вредоносные узлы, и игнорируя любые запросы от нелегитимных узлов. При этом источнику пакета отправляется специальное предупреждение для того, чтобы он мог обнаружить какой-либо другой маршрут. Нужно отметить, что подсистема репутации, основанная на обнаружении, имеет несколько ограничений, при этом маршрутизация пакетов может оставаться уязвимой для атак с фальсификацией сообщений.

Несколько различных расширений безопасности, базирующихся на реализации концепции доверия, разработано для реактивного протокола маршрутизации AODV. В частности, в исследовании [41] представлен адаптивный протокол, в рамках которого для каждого участника сети вычисляется уровень доверия, определяющий длину используемых ключей, что позволяет снизить накладные расходы на криптографические преобразования.

Ключевая особенность протокола Trusted AODV (TAODV) [42], также выступающего в качестве расширения протокола AODV, заключается в установлении доверительных отношений не только между соседними узлами, а между всеми участниками сети. Некоторый узел использует для передачи пакетов только те узлы, с которыми ранее были определены доверительные отношения. Участники сети, преднамеренно осуществляющие вредоносные операции, после детектирования должны быть изолированы. Модель доверия, положенная в основу протокола TAODV, базируется на специальной трехкомпонентной метрике, рассматриваемой в следующем разделе работы.

Попытка упростить вычисления и минимизировать накладные расходы предпринята в рамках протокола GradeTrust [43]. Данный протокол не предусматривает сотрудничества участников сети при расчете уровня доверия к некоторому узлу. С другой стороны, протокол сохраняет принцип категорирования всех участников сети согласно уровню доверия к этим узлам на три равномощных множества для того, чтобы исключить из

процесса маршрутизации пакетов участников сети с низким уровнем доверия. Очевидно, что такой упрощенный подход не позволяет организовать противодействие как нарушениям типа «грейхол», так и более сложным сетевым атакам.

Помимо обеспечения безопасности реактивных протоколов, концепция установления доверительных отношений и сотрудничества узлов также может быть задействована для защиты проактивных и гибридных протоколов маршрутизации. Например, в работе [44] представлена схема комплексного обеспечения безопасности проактивного протокола маршрутизации OLSR на базе криптографических преобразований и реализации концепции доверия. Все участники сети при установлении соседских отношений с другими узлами обмениваются открытыми ключами своей ключевой пары. В дальнейшем отправитель каждого служебного сообщения протокола формирует электронную подпись, используемую для аутентификации этих сообщений. Дополнительно безопасность рассматриваемого протокола маршрутизации базируется на контроле корректности всех сообщений HELLO и сообщений TC, отправляемых и ретранслируемых шлюзами MPR. Все участники сети устанавливают доверительные отношения с симметричными соседними узлами. Каждый участник сети, в сотрудничестве с доверенными узлами, осуществляет проверку сообщений, получаемых от соседних узлов, на их соответствие существующей сетевой топологии и спецификациям OLSR.

Участники сети имеют возможность контролировать соответствие содержимого получаемых служебных пакетов благодаря зависимостям, которые должны наблюдаться между сообщениями, полученными от различных устройств. Легитимный участник сети может разорвать отношения доверия и отношения соседства OLSR с некоторым узлом сети, если зарегистрирует нарушение спецификаций протокола этим узлом. При регистрации нарушений со стороны некоторого шлюза MPR вышеперечисленных правил данный участник сети лишается статуса шлюза

и отношения доверия с указанным участником также прекращаются. Следует отметить, что участники сети, зарегистрировавшие нарушения вышеуказанных правил, рассылают соответствующие широковещательные уведомления, прикладывая для доказательства оригинальные служебные пакеты за подписью узла нарушителя. Сотрудничество участников сети дает возможность распространять по сети данные уведомления и осуществлять изоляцию вредоносных, а также эгоистичных, узлов на основе этих уведомлений.

Ещё один подход к обеспечению безопасности проактивного протокола маршрутизации OLSR посредством реализации концепции доверия был использован в исследовании [45]. В рамках представленного протокола FPNT-OLSR авторы предлагают использовать кооперацию узлов для расчета уровней доверия к участникам самоорганизующейся сети с помощью разработанной модели на основе нечетких сетей Петри. Также в работе предложен алгоритм поиска маршрута с наиболее высоким уровнем доверия среди всех доступных маршрутов. Продемонстрированные результаты экспериментальных исследований позволили обосновать эффективность предложенного подхода.

В рамках протокола RBC-OLSR, предложенного в работе [28], значение репутации узлов зависит от их готовности выполнять маршрутизацию пакетов для других узлов и используется для оплаты услуг, предоставляемых другими узлами. В результате эгоистичные и вредоносные узлы могут быть изолированы вследствие низкого значения их репутации.

Заслуживающий внимания подход к противодействию сетевым атакам на маршрутизацию пакетов, включая атаки типа «черная дыра» и «синкхол», предложен при разработке системы ActiveTrust [47]. Предварительный поиск совокупности различных маршрутов используется для проактивного обнаружения узлов нарушителей. Вредоносные узлы могут быть найдены и изолированы в результате расчета уровня доверия к участникам сети, осуществляющим маршрутизацию пакетов, с учетом информации,

полученной от других участников сети и последующего сравнения вычисленного уровня доверия с определяемым пороговым значением.

Базовые положения концепции доверия и кооперации участников достаточно широко применяются в некотором количестве других проектов, направленных на противодействие сетевым атакам в самоорганизующихся сетях различных типов [48, 49, 50, 51, 52].

1.5 Модели определения доверия и репутации

Модели вычисления репутации широко применяются для создания доверительных отношений среди пользователей онлайн-сообществ, где участники взаимодействия не знают друг друга заранее. Основная идея использования репутации заключается в накоплении опыта взаимодействия с оцениваемым пользователем для принятия решения о взаимодействии с ним в будущем. Таким образом, репутация является показателем надежности объекта оценки и предоставляемых им услуг на основе его поведения в прошлом. Когда пользователю необходимо принять решение о взаимодействии с другим пользователем в сети, он может принять во внимание репутацию этого пользователя и начать взаимодействие с ним, только если репутация узла превышает некоторое пороговое значение. Таким образом, репутационная модель, которая помогает управлять репутацией (например, путем сбора, распространения и агрегирования информации о поведении пользователей), становится фундаментальным компонентом архитектуры безопасности любой платформы [54, 55].

Большинство моделей вычисления репутации, разработанных к настоящему времени, предназначены для решения специализированных задач. В настоящее время различные репутационные системы всё чаще применяются для оценки надежности узлов и достоверности информации в сетевой инфраструктуре. Вместе с тем, репутационные модели доверия должны учитывать специфику конкретной задачи, чтобы их можно было

использовать для её решения. Это требует понимания возможностей и ограничений существующих репутационных моделей.

1.5.1 Доверие и репутация в телекоммуникационных сетях

Исследования и разработки по имплементации репутационных моделей в динамически организуемых сетях различных типов ведутся как российскими [55, 56, 57, 58, 59], так и зарубежными учёными и научными группами [60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71]. Можно выделить ряд признаков и свойств репутационных моделей, которые используются для их классификации.

Во-первых, оценка репутации либо может быть выражена в абсолютном значении, либо представлена по отношению к другим узлам. Нужно учитывать, что если модель позволяет только ранжировать узлы, то узлы, не заслуживающие доверия, могут занимать достаточно высокие позиции в рейтинге. Часть моделей позволяет учитывать различные аспекты взаимодействия узлов (контекст взаимодействия) и различать взаимодействия на основе их стоимости. Свойство транзитивности позволяет репутационным моделям устанавливать новые доверительные отношения из существующих доверительных отношений. Например, если узел *i* доверяет узлу *j*, то он также имеет некоторое доверие к узлам, которым доверяет узел *j*. Однако способность узла предоставлять услугу может отличаться от его способности давать рекомендации другим узлам. В этом отношении некоторые модели различают функциональное доверие, то есть доверие к способности узла предоставлять услугу, и реферальное доверие, то есть доверие к способности узла предоставлять рекомендации.

Возможность внедрения и применения репутационной модели зависит от её способности отражать фактическую надежность узлов, участвующих в коммуникации. Качество оценки репутации зависит от количества информации, используемой для её расчета. Система вычисления репутации должна использовать достаточное количество информации. Тем не менее,

сложно установить минимальный объем данных, который необходим для расчета репутации, кроме того, различные узлы могут по-разному воспринимать репутацию в зависимости от их отношения к риску. Например, некоторые узлы могут установить доверительные отношения с оцениваемым узлом, имеющим высокую репутацию на основании очень небольшого количества прошлых взаимодействий, в то время как другим узлам может потребоваться больше данных, подтверждающих положительную оценку взаимодействия.

Как правило, формальное определение репутационной модели включает в себя определение репутационной меры и математическую модель агрегирования информации о поведении узлов и вычисления значения репутации. Определение значения репутации может быть основано на простом суммировании оценок [39] или вычислении их среднего значения на потоковых моделях [60, 61, 62, 63, 64, 65], вероятностных моделях, таких как байесовские системы [66, 67], и моделях на основе субъективной логики [68, 69, 70].

Рассмотренный ранее в разделе 1.4 протокол маршрутизации для динамически организуемых сетей CORE представляет классический пример применения репутационной модели, основанной на взвешенном усреднении оценок [39]. Использованная модель поддерживает только положительные оценки и разделяет функциональное и реферальное доверие.

Репутационные модели, в основе которых используется потоковая модель вычисления значения репутации, используют понятие транзитивного доверия. В таких репутационных моделях оценки значения репутации, полученные от других узлов, агрегируются и нормализуются для построения цепи Маркова. Вектор репутации, включающий оценки значения репутации всех участников взаимодействия, вычисляется как вектор стационарного распределения цепи Маркова. Каждый узел начинает с вектора начальных значений репутации, а затем многократно выполняет переход, пока не будет

достигнуто стационарное распределение. Это соответствует учету все большего количества косвенных свидетельств о поведении узлов сети.

Модели, основанные на субъективной логике, используют теорию Демпстера-Шафера [71]. Субъективная логика обеспечивает математическую основу для работы с мнениями других пользователей и обладает естественной способностью явно выражать неопределенность. Упрощенно, неопределенность отражает погрешность в расчете значения репутации и может возникать из-за ограниченного количества имеющейся информации о поведении узлов. Модель с использованием субъективной логики использует оператор консесуса «⊕» для объединения независимых мнений и оператор дисконтирования «⊗» для вычисления транзитивного доверия. Таким образом, модель на основе субъективной логики может быть использована для вычисления значения репутации, учитывая существующие отношения доверия между узлами.

1.5.2 Потоковые модели

Одной из самых известных и широко используемых потоковых репутационных моделей является EigenTrust [60, 61]. Применение данной модели в системах управления доверием в сети позволяет снизить воздействие вредоносных узлов и уменьшить их влияние на процесс передачи информации.

Все узлы сети взаимодействуют друг с другом для предоставления услуг, совершая так называемые транзакции. Узел i может оценить транзакцию с узлом j, как положительную ($\mathrm{tr}(i, j) = 1$) или отрицательную ($\mathrm{tr}(i, j) = -1$).

Локальное значение доверия узла i к узлу j обозначается S_{ij} и определяется как разница между числом положительных и отрицательных транзакций соответствующих узлов:

$$S_{ij} = \mathrm{sat}(i, j) - \mathrm{unsat}(i, j)$$

Дальнейшая нормализация позволяет исключить возможность формирования произвольно высоких и произвольно низких значений

локального доверия в результате кооперации вредоносных узлов. Нормализованное локальное значение доверия C_{ij} узла i к узлу j определяется как:

$$C_{ij} = \frac{\max(S_{ij},0)}{\sum_k \max(S_{ik},0)}, \text{ если } \sum_k \max(S_{ik},0) \neq 0. \qquad (1)$$

При этом, если некоторый узел i ранее не потреблял услуги других узлов сети, то $S_{ij} = 0$ для любого j. В этом случае нормализованное значение локального доверия $C_{ij} = P_j$, где $P_j = 1/|P|$, если $j \epsilon P$, иначе $P_j = 0$. При этом P представляет собой множество изначально доверенных узлов.

Нормализованное значение локального доверия может рассматриваться как вероятностная мера, поскольку:

$$0 \leq C_{ij} \leq 1, \ \sum_k C_{ik} = 1$$

Свойство транзитивности доверия позволяет каждому узлу сети i агрегировать локальные значения репутации некоторого узла k, предоставленные другими узлами сети, для получения значения глобального доверия к соответствующему узлу:

$$t_{ik} = \sum_j C_{ij} C_{jk}$$

Вектор соответствующих значений для всех узлов сети образует вектор глобального доверия. Тогда определив $\mathbf{C}$ как матрицу значений нормализованных значений $[C_{ij}]$ локального доверия между узлами сети, вектор глобального доверия можно получить следующим образом:

$$\overline{\mathbf{t}}_i = \mathbf{C}^{\mathbf{T}} \overline{\mathbf{c}}_i$$

Благодаря свойствам $\mathbf{C}$, при увеличении количества итераций n, вектор глобального доверия сходится к общему вектору для каждого узла i (левому собственному вектору указанной матрицы):

$$\overline{\mathbf{t}} = (\mathbf{C}^{\mathbf{T}})^n \overline{\mathbf{c}}_i$$

Таким образом, глобальная оценка репутации узлов сети соответствует элементам полученного вектора.

Используя вектор глобального доверия, вычисленный в результате k итераций, можно вычислить значение данного вектора на следующем шаге:

$$\overline{\mathbf{t}}^{(k+1)} = (1-a)\mathbf{C}^{\mathbf{T}}\overline{\mathbf{t}}^{(k)} + a\overline{\mathbf{p}}. \qquad (2)$$

Здесь $\overline{\mathbf{p}}$ – вектор априорного доверия к узлам сети, и a – некоторая постоянная, необходимая для противодействия кооперации узлов нарушителей, причем $0 < a < 1$.

Применение модели EigenTrust для оценки репутации узлов сети передачи данных можно продемонстрировать на следующем примере (рисунок 6).

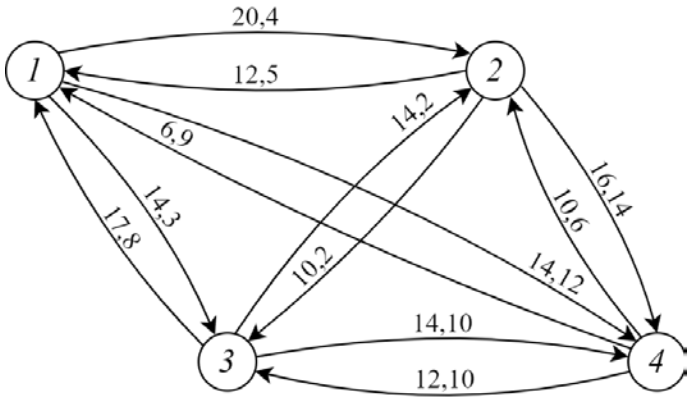

Рисунок 6. Пример топологии для демонстрации модели EigenTrust с указанием числа положительных и отрицательных транзакций

Пусть узел 4 является нарушителем, уничтожающим большую часть пакетов, полученных от других узлов сети. При этом по результатам сетевого взаимодействия получена совокупная статистика положительных и отрицательных транзакций для каждой пары узлов. Указанные значения приписаны соответствующим дугам сети на рисунке 6.

Используя имеющуюся статистику, каждый узел определяет нормализованное локальное значение доверия к остальным узлам сети в соответствии с формулой (1):

$$\mathbf{C}=\begin{pmatrix} 0 & 0{,}55 & 0{,}37 & 0{,}08 \\ 0{,}41 & 0 & 0{,}47 & 0{,}12 \\ 0{,}36 & 0{,}48 & 0 & 0{,}16 \\ 0 & 0{,}66 & 0{,}34 & 0 \end{pmatrix}$$

На основе формулы (2) может быть предложен простой алгоритм для вычисления вектора глобального доверия с заданной точностью ε (рисунок 7).

Пусть задано значение a = 0,5, допустимое стандартное отклонение глобального вектора доверия ε = 0,01, а также значение каждого элемента начального вектора глобального доверия принимается равным 1/|P|.

В результате вычисления вектора глобального доверия на первом шаге алгоритма получено стандартное отклонение δ_1 = 0.2175, что превышает допустимое значение.

Алгоритм 1 Алгоритм EigenTrust

Вход: $\mathbf{C}$, $\bar{t}^{(0)}$, ε
Выход: $\bar{t}$
1: **Повторять**
2: $\quad \bar{t}^{(k+1)} \leftarrow \mathbf{C}^{\mathbf{T}}\bar{t}^{(k)}$
3: $\quad \delta \leftarrow \|\bar{t}^{(k+1)} - \bar{t}^{(k)}\|$
4: **Пока** $\delta < \varepsilon$
5: **Вернуть** $\bar{t}^{(k+1)}$

Рисунок 7. Алгоритм EigenTrust

Для достижения требуемого значения стандартного отклонения необходимо выполнить четыре шага алгоритма. Значение вектора глобального доверия, полученное на четвертом шаге алгоритма, представлено в таблице 1.

Таблица 1. Результат работы алгоритма EigenTrust

Шаг	Вектор глобального доверия				δ
	1	2	3	4	
0	0,25	0,25	0,25	0,25	-
1	0,2213	0,3363	0,2725	0,17	0,2175

2	0,2430	0,3073	0,2739	0,1758	0,0578
3	0,2373	0,3156	0,2721	0,1751	0,0164
4	0,2387	0,3133	0,2728	0,1752	0,00448

Анализ результатов работы алгоритма позволяет сделать вывод о том, что глобальное доверие к узлу 4 ниже, чем к остальным участникам сетевого взаимодействия. На практике если репутация узла падает ниже некоторого порогового значения, сетевой узел может быть исключен из процесса маршрутизации, или, иначе говоря, изолирован [62].

Один из недостатков модели EigenTrust заключается в том, что нормализация значений доверия не позволяет отличить узлы с отрицательной репутацией от узлов с нейтральной репутацией. Кроме того, оценка доверия в рамках модели является относительной, а не абсолютной, т.е. по сути только позволяет сформировать рейтинг надёжности узлов.

Система PeerTrust [63] представляет еще одну потоковую репутационную модель, изначально разработанную для пиринговых сетей. Хотя PeerTrust имеет много общего с EigenTrust, при оценке уровня доверия к узлам сети учитывается большее количество факторов. В модели PeerTrust репутация узла, который не взаимодействовал с другими узлами, остается неопределенной. Кроме того, PeerTrust обеспечивает поддержку контекста взаимодействия, что позволяет учитывать, например, важность транзакций при оценке уровня доверия.

Комбинированный показатель доверия объединяет сразу несколько факторов, что позволяет эффективно противодействовать вредоносному поведению узлов. Важно, что оценки, предоставляемые другими узлами, являются взвешенными по уровню надежности этих узлов. Исходя из этого, адекватность репутационной модели PeerTrust может значительно снижаться в некоторых сценариях сетевого взаимодействия. В частности, узел может обеспечивать высококачественные услуги в качестве маршрутизатора, в то же время предоставляя вредоносные оценки для других узлов сети.

Одно из возможных решений указанной проблемы было предложено в рамках репутационной системы BP/P2P [64]. Для каждого узла сети определяется показатель репутации, вычисляемый на основе его качества обслуживания, и показатель достоверности, вычисляемый на основе оценок, которые предоставляет этот узел после каждой транзакции. Таким образом, модель разделяет функциональное и реферальное доверие.

В рамках полностью децентрализованной репутационной модели VectorTrust происходит построение сети доверия на базе сети передачи данных [65]. Вектор доверия (trust vector) представляет собой дугу между двумя узлами соответствующего графа, вес которой определяется по результатам прямых транзакций между соответствующими узлами. Таким образом, каждый узел определяет уровень прямого доверия к соседним узлам сети, которое хранится в локальных таблицах доверия. Модель подразумевает транзитивность доверия и позволяет быстро агрегировать векторы доверия с помощью специального алгоритма, основанного на алгоритме Беллмана-Форда. В результате формируется таблица маршрутов с максимальным уровнем доверия до всех узлов сети.

Применение модели VectorTrust для поиска наиболее безопасных маршрутов можно продемонстрировать на следующем примере. Пусть задана сетевая топология из шести узлов (рисунок 8).

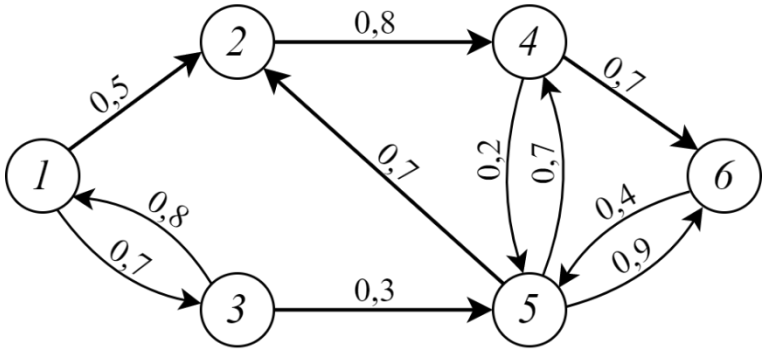

Рисунок 8. Пример топологии для демонстрации модели VectorTrust с указанием прямого доверия между соседними узлами сети

Каждый узел предоставляет услуги маршрутизации, при этом узел 5 является нарушителем, отбрасывающим большую часть пакетов, полученных от других узлов сети, что отражается результатами прямых наблюдений соседних узлов. Рассмотрим задачу поиска маршрута с максимальным уровнем доверия от узла 1 до узла 6.

На начальном этапе каждый узел формирует таблицу маршрутов исходя из локальной таблицы доверия. Далее на каждом шаге алгоритма соседние узлы обмениваются таблицами маршрутов и агрегируют получаемую информацию. Например, на первом шаге узел 1 получает таблицу маршрутов от узла 2, в которой содержится маршрут из узла 2 до узла 4 с уровнем доверия $T_{2,4} = 0,8$. Учитывая существующий маршрут от узла 1 до узла 2 с уровнем доверия $T_{1,2} = 0,5$, в таблицу узла 1 добавляется новый маршрут до узла 4 с уровнем доверия $T_{1,4} = T_{1,2} * T_{2,4} = 0,4$.

Далее продолжается обмен таблицами вплоть до достижения их сходимости. В результате работы алгоритма каждый узел получил таблицу маршрутов, каждый из которых имеет максимально возможный уровень доверия. Совокупность этих данных представлена в табл. 2. Первое значение в каждой ячейке таблицы представляет узел следующего перехода, а второе – уровень доверия к маршруту.

Таблица 2. Совокупная таблица маршрутов

Узел назначения	Узел источника					
	1	2	3	4	5	6
1	1; 1	-	1; 0,8	-	-	-
2	2; 0,5	2; 1	1; 0,4	6; 0,196	2; 0,7	5; 0,28
3	3; 0,7	-	3; 1	-	-	-
4	2; 0,4	4; 0,8	1; 0,32	4; 1	4; 0,7	5; 0,28
5	3; 0,21	4; 0,4	5; 0,3	6; 0,28	5; 1	5; 0,4
6	2; 0,28	4; 0,56	5; 0,27	6; 0,7	6; 0,9	6; 1

Используя таблицу 2, наиболее безопасный маршрут от узла 1 к узлу 6 может быть определен как «1 –>2–>4–>6».

По сравнению с другими моделями, включая EigenTrust и PeerTrust, при увеличении количества узлов модель VectorTrust эффективно масштабируется благодаря высокой скорости конвергенции и умеренной вычислительной нагрузке. Вместе с тем, по сравнению с моделью PeerTrust, модель VectorTrust не позволяет учитывать достоверность агрегируемых оценок.

1.5.3 Модели на основе субъективной логики

Альтернативное направление исследований по обеспечению безопасности маршрутизации в динамически организуемых сетях связано с разработкой репутационных моделей на базе субъективной логики. Субъективная логика представляет собой алгебру доверия, основанную на байесовской теории и булевой логике, и может быть использована для моделирования и анализа сетей доверия [68, 72]. Центральным понятием модели является трехэлементный кортеж, именуемый мнением. Мнение узла A о некотором узле X обозначается как:

$$\omega_X^A = (b_X^A, d_X^A, u_X^A)$$

где $b, d, u \in [0, 1]$ и $b + d + u = 1$. Здесь b, d и u отражают уровень доверия, недоверия и неопределенности соответственно.

Трехэлементное мнение может быть расширено с помощью четвертого параметра $a \in [0, 1]$, называемого базовым коэффициентом. Тогда прогнозируемая вероятность легитимности узла X по мнению узла A определяется как:

$$P_X^A = b_X^A + a_X^A u_X^A$$

В отсутствие каких-либо конкретных свидетельств о рассматриваемой сети базовый коэффициент определяет априорное доверие, которое будет оказано любому узлу сети.

Мнения основаны на свидетельствах. Свидетельства могут быть представлены в виде пары неотрицательных конечных чисел (p, n), где p – количество позитивных свидетельств, подтверждающих предположение, а n – количество негативных свидетельств, которые ему противоречат.

Одна из первых попыток применить модель на основе субъективной логики для обеспечения безопасности маршрутизации была выполнена в рамках протокола TAODV [42]. Позитивными и негативными свидетельствами могут являться положительные и отрицательные транзакции (доставленные и недоставленные пакеты соответственно). Как правило, в контексте сетей доверия, базовый коэффициент можно исключить из рассмотрения, потому что он не изменяется никакими вычислениями на основе мнений.

Пусть p – количественный показатель успешно доставленных узлом X пакетов, n – количественный показатель недоставленных пакетов, тогда расчет показателей доверия, недоверия, неопределенности производится следующим образом:

$$b_X = \frac{p}{p+n+2},$$
$$d_X = \frac{n}{p+n+2},$$
$$u_X = \frac{2}{p+n+2}.$$

Для объединения нескольких мнений в рамках модели на основе субъективной логики предложен ряд операций. Операция дисконтирования позволяет узлу A вычислить мнение об узле C, дополнительно опираясь на мнение промежуточного узла B о целевом узле:

$$b_C^{A\otimes B} = b_B^A b_C^B,$$
$$d_C^{A\otimes B} = b_B^A d_C^B,$$
$$u_C^{A\otimes B} = d_B^A + u_B^A + b_B^A u_C^B.$$

Операция консенсуса позволяет согласовать два независимых мнения узлов *A* и *B* об узле C:

$$b_C^{A\oplus B} = b_C^A u_C^B + b_C^B u_C^A \big/ u_C^A + u_C^B - u_C^A u_C^B,$$
$$d_C^{A\oplus B} = d_C^A u_C^B + d_C^B u_C^A \big/ u_C^A + u_C^B - u_C^A u_C^B,$$
$$u_C^{A\oplus B} = u_C^A u_C^B \big/ u_C^A + u_C^B - u_C^A u_C^B.$$

Применение репутационной модели на основе субъективной логики для выбора наиболее безопасного маршрута можно продемонстрировать на следующем примере (рисунок 9).

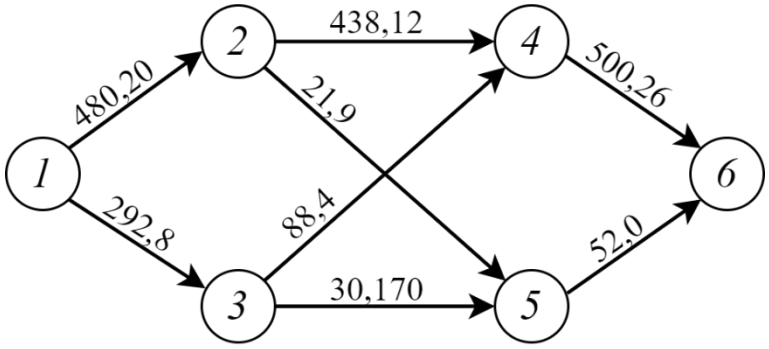

Рисунок 9. Топология для демонстрации модели на основе субъективной логики с указанием числа положительных и отрицательных транзакций

Пусть узел 5 является вредоносным и фильтрует большую часть пакетов, полученных от других узлов сети. Вес каждой дуги в представленной сети соответствует количеству позитивных и негативных свидетельств, накопленных в результате прямого взаимодействия двух узлов к некоторому моменту времени.

Рассмотрим задачу поиска маршрута с максимальным уровнем доверия от узла 1 до узла 6. Базовый коэффициент a принимается равным 0,5 для всей сети.

Результаты вычислений для рассматриваемого примера представлены в таблице 3. Для агрегирования мнений узлы сети обмениваются полученными результатами. Таким образом, узел 1 получает возможность сформировать мнение о всех узлах сети.

Таблица 3. Совокупная таблица прямых мнений

Мнение	b	d	u
ω_2^1	0,956	0,04	0,004
ω_3^1	0,967	0,026	0,007
ω_4^2	0,969	0,027	0,004
ω_5^2	0,656	0,281	0,063
ω_4^3	0,936	0,043	0,021
ω_5^3	0,149	0,842	0,009
ω_6^4	0,947	0,049	0,004
ω_6^5	0,963	0	0,037

Используя операции дисконтирования и консенсуса узел 1 вычисляет мнение об узле 4 и узле 5:

$$\omega_4^1 = \omega_4^{(1\otimes 2)\oplus(1\otimes 3)} = (0{,}94,\ 0{,}034,\ 0{,}026),$$

$$\omega_5^1 = \omega_5^{(1\otimes 2)\oplus(1\otimes 3)} = (0{,}292,\ 0{,}677,\ 0{,}031).$$

Каждый из этих узлов является прямым соседним узлом для узла 6 и может предложить маршрут до этого узла. Исходя из (3), вероятность легитимности узла 4 по мнению узла 1 превосходит соответствующую вероятность для узла 5:

$$P_4^1 = 0{,}953,\ P_5^1 = 0{,}308.$$

Таким образом, построение маршрута до узла 6 производится через узел 4. Учитывая, что, по мнению узла 1, вероятность легитимности узла 2 превосходит вероятность легитимности узла 3, наиболее безопасный маршрут от узла 1 до узла 6 определяется как «1->2->4->6».

Несмотря на уникальную возможность учитывать неопределенность информации, базовая модель на основе субъективной логики имеет ряд недостатков. Учитывая, что расчет репутации зависит от топологии доверительной сети и графа взаимодействий, имплементация модели в

рамках протоколов маршрутизации сдерживается проблемой автоматизации вычислений.

Важно, что операция дисконтирования не имеет естественной интерпретации по отношению к учету свидетельств [69]. Кроме того, дисконтирование не является дистрибутивным по отношению к операции консенсуса.

Операция дисконтирования накладывает ограничения на свидетельства, которые можно агрегировать. Требуется, чтобы свидетельства были независимыми [72]. В тоже время четко определить понятие независимости свидетельств достаточно трудно. Таким образом, может возникнуть проблема повторного учета свидетельств. В соответствии с [73], можно удалить некоторые ребра из сети для решения указанной проблемы. При этом качество получаемых репутационных оценок снижается, поскольку учитывается не вся доверительная информация.

В работе [69] предпринята попытка объединить достоинства подхода на основе субъективной логики и потоковых репутационных моделей. Авторы работы предложили альтернативную операцию дисконтирования, которая вместо перемножения мнений предполагает учитывать некоторую часть доказательств узла пропорционально вероятности легитимности этого узла. В результате можно представить себе дисконтирование как физическую передачу свидетельств от узла *B* к узлу *A*, во время которой из-за недоверия и неопределенности сохраняется только некоторая их часть. В работе представлено доказательство, что предложенная операция дисконтирования является дистрибутивной относительно операции консенсуса и позволяет исключить двойной учет свидетельств.

Представленную алгебру мнений авторы работы именуют субъективной логикой, основанной на доказательствах (EBSL, Evidence Base Subjective Logic). Показано, что новая алгебра EBSL позволяет определить итерационный алгоритм для расчета репутации узлов в сетях доверия произвольного вида. Основное достоинство предложенного подхода

заключается в возможности обеспечить качество агрегируемых свидетельств, поскольку удалять ребра из сети больше не требуется. Полученные результаты позволяют на базе EBSL разработку новых репутационных моделей.

Вместе с тем, предложенный подход также имеет недостатки. В частности, при формировании мнений не учитываются отрицательные свидетельства, а для получения адекватных репутационных оценок требуется корректное определение системного параметра, связанного с максимально допустимым количеством положительных свидетельств.

1.6 Постановка задач исследования

Таким образом, был сформирован ряд требований, которым должна удовлетворять репутационная модель для решения проблемы обеспечения безопасности маршрутизации в самоорганизующихся сетях. Учитывая сложные топологии динамически организуемых сетей, используемая модель должна поддерживать передачу доверия, т.е. быть транзитивной. При этом процедура агрегирования оценок может быть интегрирована в процесс объявления сетевых маршрутов. Оценка репутации в рамках модели должна быть абсолютной, а не относительной. Для противодействия вредоносным узлам модель должна учитывать качество источника получаемых оценок, поскольку оценки, полученные от разных узлов, могут иметь различный вес. Необходимо, чтобы модель (например, за счёт показателя неопределенности либо другим способом) учитывала количество информации, использованной для формирования оценки. Модель должна поддерживать возможность расширения, чтобы различать функциональное и реферальное доверие, а также учитывать контекст взаимодействия. Кроме того, для динамически организуемых сетей важно, чтобы используемая модель обеспечивала минимальный уровень вычислительных и сетевых накладных расходов.

В результате анализа, представленного в разделе 1.5, можно сделать вывод, что разработка эффективной модели с указанными характеристиками

для обеспечения безопасности маршрутизации в динамически организуемых сетях по-прежнему представляет актуальную проблему.

Таким образом, для достижения поставленной цели была выполнена постановка задач диссертационного исследования:

- Разработка новой репутационной модели доверия для обеспечения безопасности маршрутизации в самоорганизующихся сетях;
- Разработка алгоритма поиска наиболее безопасных маршрутов для его применения в рамках разработанной репутационной модели;
- Реализация разработанной репутационной модели и алгоритма на базе одного из существующих проактивных протоколов маршрутизации для самоорганизующихся сетей;
- Экспериментальное обоснование эффективности предложенных решений в различных сценариях.

1.7 Выводы по главе

1. В рамках данной главы выполнен анализ существующих угроз безопасности маршрутизации в самоорганизующихся сетях. 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 доверия в самоорганизующейся сети, что позволит избегать при доставке пакетов ненадёжные узлы с низкой репутацией и тем самым повысить безопасность процесса маршрутизации.
2. Проанализированы существующие модели определения доверия и вычисления репутации, включая модели, основанные на суммировании и усреднении оценок, потоковые модели и модели на основе

субъективной логики. Исследована проблематика их применения для определения уровня доверия к узлам и маршрутам в самоорганизующейся сети.

3. 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. Таким образом, доказана актуальность данного исследования.
4. На основании всего вышеуказанного 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.

Глава 2 Разработка репутационной модели маршрутизации

2.1 Модель определения репутации

По результатам сравнительного анализа существующих репутационных моделей и исследования их применимости в самоорганизующихся сетях разработана новая транзитивная модель оценки репутации каналов связи самоорганизующейся сети. Разработанная модель предназначена для оценки глобального функционального доверия к сетевым маршрутам и позволяет полностью учитывать источники получаемых оценок.

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 $r_s(u,v) \in \{0,1\}$.

Модель поддерживает различные способы оценки локальной репутации каналов связи. В работе предложен способ оценки локальной репутации каналов связи при помощи отправки скрытых проверочных пакетов [78]. 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.

Применение логической репутационной модели позволяет обеспечить поиск наиболее безопасных маршрутов от заданного источника ко всем возможным узлам назначения [79]. Для поиска маршрутов используется модель булевозначной сети [80], которая представляет собой ориентированный мультиграф, каждой дуге которой присвоен некоторый элемент $c(e)$ из фиксированной конечной булевой алгебры B.

В рамках описания модели введем 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 наиболее безопасных маршрутов каждый узел независимо производит построение булевозначной сети. 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. Рассчёт 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 $P = (s, e_0, ..., e_j, t)$ 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). 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.

Предложенная модель подразумевает, что каждый узел сети динамически производит построение булевозначной сети, соответствующей текущему состоянию сети передачи данных, и вычисляет маршруты до всех доступных узлов назначения, используя разработанный алгоритм поиска наиболее безопасных маршрутов в булевозначной сети. Разработанная модель предложена в работе [81].

Для описания применения разработанной репутационной модели использована самоорганизующаяся сеть на рисунке 10.

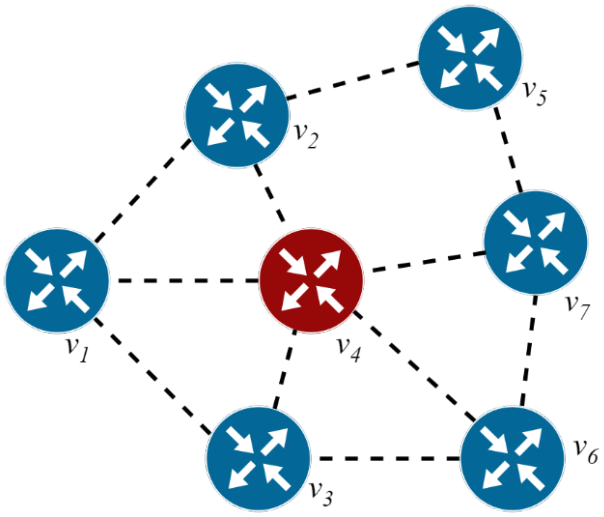

Рисунок 10. Пример сетевой топологии с узлом нарушителя v_4

В рассматриваемом примере заданная сеть состоит из 7 узлов, причем узлы v_1, v_2, v_3, v_5, v_6, v_7 являются легитимными и имеют нормальное поведение, а узел v_4 является узлом нарушителя и выполняет атаку типа

«серая дыра». Пусть необходимо определить наиболее безопасный путь из узла v_1 до узла v_7.

Предполагается, что в рассматриваемой сети был произведён обмен специальными сообщениями с целью проверки работоспособности каналов связи. Проверка позволила произвести оценку каждого канала связи каждым узлом. С начального момента каждый узел успел отправить по 2 проверочных пакета (таблица 4). Отправленные пакеты позволили каждому узлу сети получить локальные значения репутации каналов связи.

Таблица 4. Результаты оценки каналов связи узлами сети

Узел	Путь	Оценка каналов связи, составляющих путь
v_1	(v_1, v_2, v_5)	1
v_1	(v_1, v_3, v_6)	1
v_2	(v_2, v_4, v_6)	0
v_2	(v_2, v_5, v_7)	1
v_3	(v_3, v_4, v_7)	0
v_3	(v_3, v_6, v_7, v_5)	1
v_4	(v_4, v_2, v_5)	1
v_4	(v_4, v_7, v_5)	1
v_5	(v_5, v_7, v_6, v_3)	1
v_5	(v_5, v_2, v_1)	1
v_6	(v_6, v_3, v_1)	1
v_6	(v_6, v_7, v_5)	1
v_7	(v_7, v_6, v_3)	1
v_7	(v_7, v_5, v_2)	1

Предполагается, что в рамках сетевой атаки типа «серая дыра» узел нарушителя отбросил проверочные сетевые пакеты, отправленные узлами v_2 и v_3, что отразилось на локальной репутации соответствующих каналов

связи. В результате, каждый узел определил локальные значения репутации каналов связи (таблица 5).

Таблица 5. Локальные значения репутации каналов связи

Каналы связи / Узлы	(v_1, v_2)	(v_1, v_3)	(v_1, v_4)	(v_2, v_4)	(v_3, v_4)	(v_2, v_5)	(v_3, v_6)	(v_4, v_6)	(v_4, v_7)	(v_5, v_7)	(v_6, v_7)
v_1	1	1	1	0	0	1	1	0	0	0	0
v_2	1	0	0	0	0	1	0	0	0	1	0
v_3	0	1	0	0	0	0	1	0	0	1	1
v_4	0	0	1	1	1	1	0	1	1	1	0
v_5	1	0	0	0	0	1	1	0	0	1	1
v_6	0	1	0	0	0	0	1	1	0	1	1
v_7	0	0	0	0	0	1	1	0	1	1	1

После определения локальной репутации каналов связи, узлы производят широковещательный обмен соответствующими значениями. Узлы сети используя значения локальной репутации, полученные от других узлов сети, способны определить вектор глобальной репутации для всех каналов связи (таблица 6).

Таблица 6. Глобальная репутация каналов связи

Канал связи	Вектор глобальной репутации
(v_1, v_2)	(1,1,0,0,1,0,0)
(v_1, v_3)	(1,0,1,0,0,1,0)
(v_1, v_4)	(1,0,0,1,0,0,0)
(v_2, v_4)	(0,0,0,1,0,0,0)
(v_3, v_4)	(0,0,0,1,0,0,0)
(v_2, v_5)	(1,1,0,1,1,0,1)
(v_3, v_6)	(1,0,1,0,1,1,1)
(v_4, v_6)	(0,0,0,1,0,1,0)
(v_4, v_7)	(0,0,0,1,0,0,1)

(v_5, v_7)	(0,1,1,1,1,1,1)
(v_6, v_7)	(0,0,1,0,1,1,1)

Используя полученные векторы глобальной репутации, может быть рассчитана стоимость для всех каналов связи в сети. Таким образом формируется булевозначная сеть, соответствующая текущей сетевой топологии (рисунок 11).

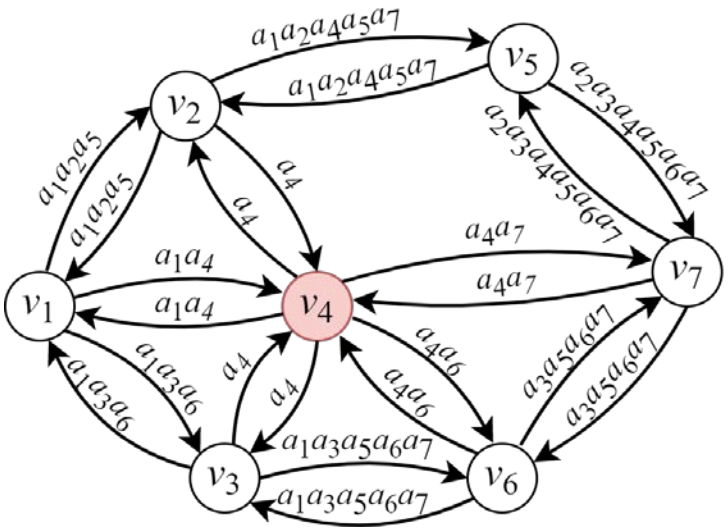

Рисунок 11. Булевозначная сеть для расчёта наиболее безопасных маршрутов

Далее в рамках модели необходимо произвести поиск наиболее безопасного маршрута из узла v_1 в узел v_7 как маршрута, «рекомендованного» максимально возможным количеством узлов. В рассматриваемой сети существует два таких маршрута с уровнем доверия равным 2, которые имеют значение глобальной репутации $\{a_2a_5\}$ и $\{a_3a_6\}$ соответственно. Указанные маршруты изображены на рисунке 12. Маршрут (v_1, v_4, v_7) через узел нарушителя v_4, имеет значение глобальной репутации $\{a_4\}$ и меньший уровень доверия, равный 1, что исключает возможность его использования.

Поскольку оба указанных пути с максимальным уровнем доверия имеют одинаковое расстояние, любой из соответствующих маршрутов может быть внесен в таблицу маршрутизации.

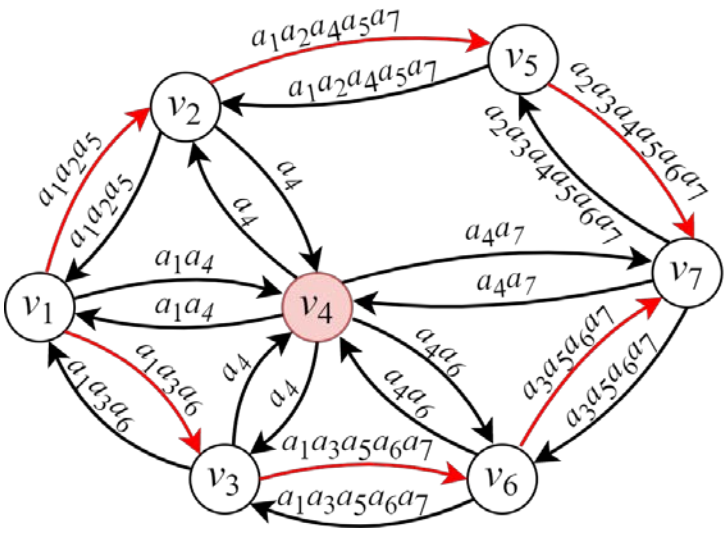

Рисунок 12. Два наиболее безопасных маршрута из узла v_1 в узел v_7

Для поиска наиболее безопасных маршрутов до всех узлов сети был разработан соответствующий алгоритм, представленный в следующем разделе работы.

2.2 Алгоритм поиска наиболее безопасных маршрутов

В рамках концепции проактивной маршрутизации каждый узел самоорганизующейся сети осуществляет поиск оптимальных маршрутов до остальных узлов сети. Для обеспечения поиска каждый узел, на основе активных интерфейсов и полученных сообщений протокола, формирует базу данных сетевой топологии, производит построение ориентированного графа и использует алгоритм поиска кратчайших маршрутов, основанный на алгоритме Дейкстры [8].

В соответствии с предложенной моделью оценки репутации каналов связи самоорганизующейся сети, каждый узел также принимает, обрабатывает и использует при построении сетевой топологии репутационные сообщения от других узлов сети. Сетевая топология представляется при помощи булевозначной сети, каждой дуге которой ставится в соответствие метка её глобальной репутации, отражающая уровень доверия других узлов к данному каналу связи. При этом для поиска

наиболее безопасного маршрута требуется соответствующий алгоритм поиска кратчайшего пути с максимальной мощностью (уровнем доверия) в булевозначной сети. Указанный алгоритм был разработан в рамках диссертационного исследования и представлен на рисунке 13.

Алгоритм 2 Алгоритм поиска наиболее безопасных маршрутов

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

```
1: P ← {∅}, A ← {s}, A* ← {∅}, L(s) ← {1}
2: Для всех v ∈ V(G)\{s}
3:    L(v) ← {∅}
4: Пока A ≠ {∅}
5:    Для всех u ∈ A
6:       Для всех v ∈ V(G)
7:          L*(v) ← L(v)
8:          Если (u, v) ∈ E(G) то
9:             L(v) ← MAX(L(v)∪(L(u)∧c(u, v)))    // MAX(X) - возвращает множество
               максимальных элементов частично-упорядоченного множества X
10:            Если L*(v) ≠ L(v) то
11:               A* ← A* ∪ {v}
12:   A ← A*, A* ← {∅}
13: Для всех v ∈ V(G)\{s}
14:   P* ← {∅}
15:   Для всех max ∈ L(v)    // max - элемент с максимальной мощностью
16:      G* ← G
17:      Для всех e ∈ E(G*)
18:         Если q(e) ⊈ max то
19:            УДАЛИТЬ e ИЗ E(G*)
20:      p ← НАЙТИ КРАТЧАЙШИЙ s − v ПУТЬ ИЗ G*
21:      P* ← P* ∪ {p}
22:   p ← ВЫБРАТЬ КРАТЧАЙШИЙ s − v ПУТЬ ИЗ P*
23:   P ← P ∪ {p}
24: Вернуть P
```

Рисунок 13. Алгоритм поиска наиболее безопасных маршрутов

Пусть задан вход алгоритма: 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. На каждой итерации первого этапа алгоритма происходит переформирование меточного множества L для всех вершин, в которые ведут дуги из активных вершин множества 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 завершению итерации отлично от пустого множества. После завершения данного этапа, любое множество $L(v)$ будет содержать значения глобальной репутации для всех путей с максимальным уровнем доверия до вершины v. Если в рассматриваемой сети 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 длинны и помещается в множество P. По завершению второго этапа P содержит множество кратчайших путей с максимальной мощностью из узла s до всех узлов сети. Алгоритм представлен в работе [82].

Пусть на вход алгоритма подаётся булевозначная сеть, представленная на рисунке 11. Входными данными, описывающими сеть являются конечное множество элементов $M = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$, $P(M) = \{0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_1a_2, a_1a_3, a_1a_4, \ldots, a_1a_2a_3, a_1a_2a_4, \ldots, a_1a_2a_3a_4, \ldots, a_1a_2a_3a_4a_5, \ldots,$

$a_1a_2a_3a_4a_5a_6$, …, 1}. Множество $P(M)$ считается частично упорядоченным множеством и имеет мощность равную $|P(M)| = 2^7 = 128$.

В таблице 6 содержатся глобальные значения репутации каждого канала связи, позволяющие сформировать булевозначную сеть. Для поиска наиболее безопасных маршрутов необходимо воспользоваться алгоритмом, представленным на рисунке 13. В ходе выполнения первого этапа алгоритма было выполнено 6 итераций, результаты которых представлены в таблице 7.

Таблица 7. Результаты выполнения первого этапа Алгоритма 2

I	***A***	***A****	**Набор меток для каждой вершины**						
			***L*(v_1)**	***L*(v_2)**	***L*(v_3)**	***L*(v_4)**	***L*(v_5)**	***L*(v_6)**	***L*(v_7)**
0	{v_1}	{*0*}	{*1*}	{*0*}	{*0*}	{*0*}	{*0*}	{*0*}	{*0*}
1	{v_1}	{v_2,v_3,v_4}	{*1*}	**{$a_1a_2a_5$}**	**{$a_1a_3a_6$}**	**{a_1a_4}**	{*0*}	{*0*}	{*0*}
2	{v_2,v_3,v_4}	{v_2,v_3,v_5, v_6,v_7}	{*1*}	**{$a_1a_2a_5$, a_4}**	**{$a_1a_3a_6$, a_4}**	{a_1a_4}	**{$a_1a_2a_5$}**	**{$a_1a_3a_6$, a_4}**	**{a_4}**
3	{v_2,v_3,v_5, v_6,v_7}	{v_4,v_5,v_7}	{*1*}	{$a_1a_2a_5$, a_4}	{$a_1a_3a_6$, a_4}	**{a_1a_4, a_6}**	**{$a_1a_2a_5$, a_4}**	{$a_1a_3a_6$, a_4}	**{a_4, a_2a_5, a_3a_6}**
4	{v_4,v_5,v_7}	{v_5,v_6}	{*1*}	{$a_1a_2a_5$, a_4}	{$a_1a_3a_6$, a_4}	{a_1a_4, a_6}	**{$a_1a_2a_5$, a_4, a_3a_6}**	**{$a_1a_3a_6$, a_4, a_5}**	{a_4, a_2a_5, a_3a_6}
5	{v_5,v_6}	{v_3}	{*1*}	{$a_1a_2a_5$, a_4}	**{$a_1a_3a_6$, a_4, a_5}**	{a_1a_4, a_6}	{$a_1a_2a_5$, a_4, a_3a_6}	{$a_1a_3a_6$, a_4, a_5}	{a_4, a_2a_5, a_3a_6}
6	{v_3}	{*0*}	{*1*}	{$a_1a_2a_5$, a_4}	{$a_1a_3a_6$, a_4, a_5}	{a_1a_4, a_6}	{$a_1a_2a_5$, a_4, a_3a_6}	{$a_1a_3a_6$, a_4, a_5}	{a_4, a_2a_5, a_3a_6}

На втором этапе алгоритма поиск наиболее безопасных маршрутов поочередно выполняется до всех узлов назначения. Рассмотрим поиск наиболее безопасного маршрута до узла назначения v_7. По результатам выполнения первого этапа алгоритма была определена максимальная мощность путей до узла назначения v_7 равная 2. Этой мощности соответствует два элемента из множества $L(v_7)$. Далее, поочередно рассматривая каждый из этих элементов, осуществляется переход к частному подграфу G и поиск кратчайшего пути в указанном подграфе, используя алгоритм Дейкстры. Построение частного подграфа производится путем

удаления из графа G всех дуг, стоимость которых не включает рассматриваемый элемент.

В частности, рассматривая элемент $\{a_2a_5\}$, производится построение подграфа, представленного на рисунке 14.

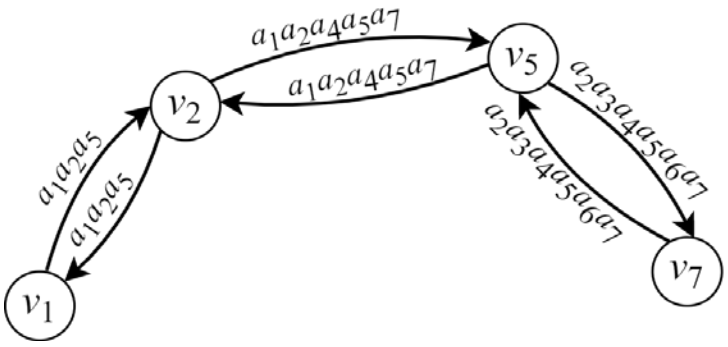

Рисунок 14. Подграф G, стоимость всех дуг которого включает $\{a_2a_5\}$

Применяя в образованной булевозначной сети классический алгоритм Дейкстры, кратчайший путь между узлами v_1 и v_7 определяется как: $<v_1, v_2, v_5, v_7>$. Указанный маршрут длинны 3 изображен на рисунке 15.

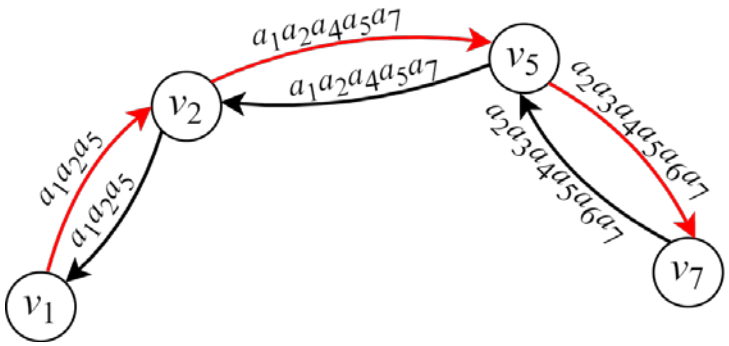

Рисунок 15. Кратчайший маршрут из узла v_1 в узел v_7 с оценкой пути $\{a_2a_5\}$

Далее, рассматривая элемент $\{a_3a_6\}$, производится построение подграфа, представленного на рисунке 16. Применяя в образованной булевозначной сети классический алгоритм Дейкстры, кратчайший путь между узлами v_1 и v_7 определяется как: $<v_1, v_3, v_6, v_7>$. Указанный маршрут длины 3 изображен на рисунке 16.

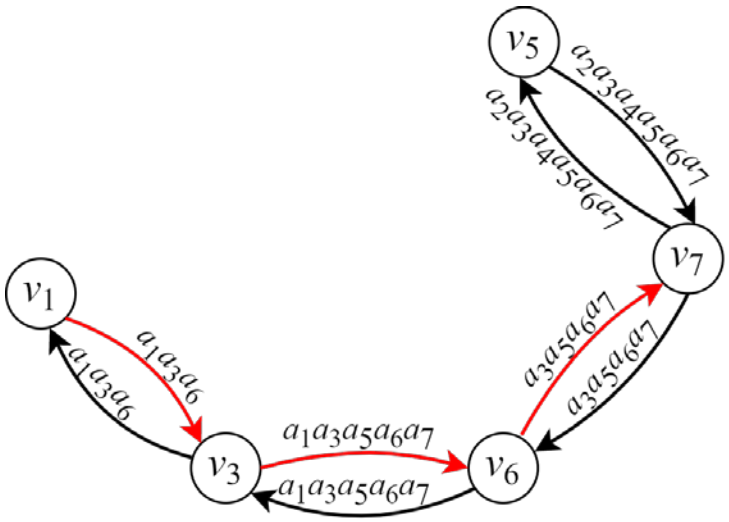

Рисунок 16. Кратчайший маршрут из узла v_1 в узел v_7 с оценкой пути $\{a_3a_6\}$

Учитывая, что оба пути, найденных из узла v_1 в узел v_7 с максимальной мощностью, имеют одинаковую длину, любой из них может быть выбран в качестве наиболее безопасного маршрута.

Таким образом, в результате применения алгоритма был найден маршрут в самоорганизующейся сети, каналы связи которого одновременно «рекомендованы» максимальным количеством узлов. Предложенный алгоритм имеет теоретическую временную сложность $O(n^3)$.

Организация процесса многопутевой маршрутизации является одним из ключевых методов противодействия атакам на доступность передаваемых сетевых пакетов. Выбор конкретной стратегии зависит от существующих задач, но практически в любом случае наличие нескольких непересекающихся путей в сетях с динамической топологией позволяет существенно повысить надёжность, безотказность и жизнеспособность сетевого взаимодействия.

Проблема определения некоторого множества оптимальных непересекающихся путей может рассматриваться как расширение задачи поиска кратчайшего пути, решаемой с помощью алгоритма Дейкстры [8]. Существуют различные хорошо изученные постановки указанной проблемы, включая поиск непересекающихся путей с минимальной суммой их весов,

поиск непересекающихся путей с минимальным весом худшего из путей и некоторые другие. Эффективный алгоритм для поиска k непересекающихся путей с минимальной суммой впервые был предложен Суурбалле [83], и в дальнейшем был трансформирован Бхандари [84] для применения в телекоммуникационных сетях. Оригинальный алгоритм используется для поиска реберно-непересекающихся путей, но может быть легко адаптирован для поиска вершинно-непересекающихся путей посредством несложной операции.

Формальная задача поиска наиболее безопасного множества непересекающихся путей с учетом разработанной репутационной модели заключается в том, чтобы найти два или несколько непересекающихся путей, все дуги которых одновременно «рекомендованы» наибольшим числом узлов сети. Указанное множество непересекающихся путей будет обладать максимальной мощностью (уровнем доверия). Решение данной проблемы является важным для обеспечения безопасной многопутевой маршрутизации пакетов во всех типах сетей с динамической топологией. Практическое применение алгоритмов поиска непересекающихся путей для сетей с динамической топологией можно встретить в работах [85, 86].

Рассмотрим множество P из k реберно-непересекающихся (s,t)-путей в булевозначной сети $G(V,E,c)$. Реберно-непересекающиеся пути в сети не имеют общих ребер. Определим $b(P)$ как пересечение глобальной репутации всех путей в P. Мы также определим, что множество P содержит k наиболее безопасных реберно-непересекающихся (s,t)-путей в $G(V,E,c)$, если $b(P)$ имеет максимально возможную мощность и, среди всех множеств с одинаковыми значениями $|b(P)|$, множество P содержит пути с минимально возможной совокупной длиной. Таким образом, далее рассматривается задача нахождения k наиболее безопасных реберно-непересекающихся (s,t)-путей в булевозначной сети.

С одной стороны, невозможно напрямую использовать алгоритм Бхандари для решения поставленной задачи. С другой стороны, наиболее

безопасный путь в булевозначной сети, который может быть найден с помощью алгоритма на рисунке 13, может не иметь ничего общего с решением задачи.

На основе алгоритма Бхандари и алгоритма нахождения наиболее безопасного пути в булевозначной сети был предложен точный алгоритм нахождения *k* наиболее безопасных реберно-непересекающихся путей в булевозначной сети (рисунок 17).

Алгоритм 3 Алгоритм поиска наиболее безопасного множества из k непересекающихся маршрутов

Вход: G, c, s, t, k
Выход: Множество P наиболее безопасных реберно-непересекающихся путей из s в t

$P \leftarrow \{\varnothing\}$, $A \leftarrow \{s\}$, $A^* \leftarrow \{\varnothing\}$, $Q \leftarrow \{\varnothing\}$, $R \leftarrow \{\varnothing\}$, $L(s) \leftarrow \{1\}$
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 $b \in L(t)$
  $Q \leftarrow Q \cup \mathcal{P}(b)$ // $\mathcal{P}(b)$ - *множество всех подмножеств* b
Пока $Q \neq \{\varnothing\}$ И $R = \{\varnothing\}$
  $Q^* \leftarrow \mathrm{MAX}(Q)$
  Для всех $b \in Q^*$
    $G^* \leftarrow G$
    Для всех $e \in E(G^*)$
      Если $b \not\subseteq c(e)$ **то**
        УДАЛИТЬ e FROM $E(G^*)$
    $P \leftarrow \{\mathrm{BHANDARI}(G^*, k)\}$
    $R \leftarrow R \cup \{P\}$
  $Q \leftarrow Q\backslash Q^*$
$P \leftarrow$ ВЫБРАТЬ ИЗ R МНОЖЕСТВО $s - t$ ПУТЕЙ МИНИМАЛЬНОЙ СОВОКУПНОЙ ДЛИНЫ
Вернуть P

Рисунок 17. Алгоритм поиска наиболее безопасного множества непересекающихся маршрутов до заданного узла

Основная идея алгоритма состоит в том, чтобы найти все возможные нижние оценки (*s*,*t*)-путей на первом этапе. В конце первого этапа множество *Q* будет содержать все возможные нижние оценки (*s*,*t*)-путей.

На втором этапе с помощью множества *Q* и алгоритма Бхандари производится поиск *k* реберно-непересекающихся путей, имеющих одинаковую нижнюю оценку (глобальную репутацию). Поочередно рассматриваются элементы максимальной мощности из *Q*, а булевозначная сеть преобразовывается так, чтобы она содержала только те дуги, стоимость которых содержит рассматриваемый элемент из *Q*. В преобразованной булевозначной сети каждый раз используется алгоритм Бхандари. Если найдено несколько множеств непересекающихся путей для элементов одинаковой мощности, выбирается множество, содержащее пути наименьшей совокупной длины. Предложенный алгоритм также имеет теоретическую временную сложность O(n^3).

Работа предложенного алгоритма может быть продемонстрирована на следующем примере. Пусть задана булевозначная сеть на рисунке 18.

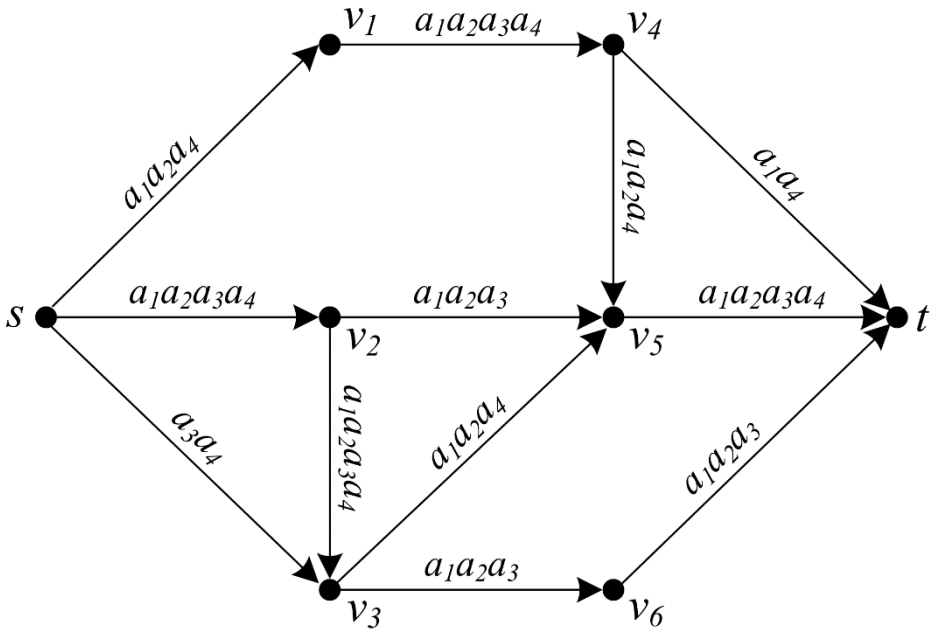

Рисунок 18. Булевозначная сеть для расчёта множества непересекающихся наиболее безопасных маршрутов

Предположим, что требуется найти множество из двух наиболее безопасных реберно-непересекающихся путей из s в t. На первом этапе алгоритма вычисляется множество $L(t) = \{a_1a_2a_3,\ a_1a_2a_4\}$. Результаты всех итераций первого этапа представлены в таблице 8.

Таблица 8. Результаты выполнения первого этапа Алгоритма 3

I	A	A^*	**Набор меток для каждой вершины**							
			$L(s)$	$L(v_1)$	$L(v_2)$	$L(v_3)$	$L(v_4)$	$L(v_5)$	$L(v_6)$	$L(t)$
0	$\{s\}$	$\{\}$	$\{1\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
1	$\{s\}$	$\{v_1,v_2,v_3\}$	$\{1\}$	$\{a_1a_2a_4\}$	$\{1\}$	$\{a_3a_4\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
2	$\{v_1,v_2,v_3\}$	$\{v_3,v_4,v_5,v_6\}$	$\{1\}$	$\{a_1a_2a_4\}$	$\{1\}$	$\{1\}$	$\{a_1a_2a_4\}$	$\{a_1a_2a_3,a_4\}$	$\{a_3\}$	$\{0\}$
3	$\{v_3,v_4,v_5,v_6\}$	$\{v_5,v_6,t\}$	$\{1\}$	$\{a_1a_2a_4\}$	$\{1\}$	$\{1\}$	$\{a_1a_2a_4\}$	$\{a_1a_2a_3,a_1a_2a_4\}$	$\{a_1a_2a_3\}$	$\{a_1a_2a_3,a_1a_4\}$
4	$\{v_5,v_6,t\}$	$\{t\}$	$\{1\}$	$\{a_1a_2a_4\}$	$\{1\}$	$\{1\}$	$\{a_1a_2a_4\}$	$\{a_1a_2a_3,a_1a_2a_4\}$	$\{a_1a_2a_3\}$	$\{a_1a_2a_3,a_1a_2a_4\}$
5	$\{t\}$	$\{\}$	$\{1\}$	$\{a_1a_2a_4\}$	$\{1\}$	$\{1\}$	$\{a_1a_2a_4\}$	$\{a_1a_2a_3,a_1a_2a_4\}$	$\{a_1a_2a_3\}$	$\{a_1a_2a_3,a_1a_2a_4\}$

Далее, рассматривая каждый элемент $L(t)$ как отдельный набор атомов, формируется множество $Q = \{a_1a_2a_3,\ a_1a_2a_4,\ a_1a_2,\ a_1a_3,\ a_2a_3,\ a_1a_4,\ a_2a_4,\ a_1,\ a_2,\ a_3,\ a_4\}$ как объединение всех полученных множеств.

На следующем шаге извлекаются элементы $\{a_1a_2a_3,\ a_1a_2a_4\}$ из Q, имеющие максимальную мощность. Рассматривая $\{a_1a_2a_3\}$, из булевозначной сети удаляются все дуги, стоимость которых не содержит указанный элемент (рисунок 19), и производится поиск двух реберно-непересекающихся путей, используя оригинальный алгоритм Бхандари. Можно заметить, что таких путей в рассматриваемой сети нет.

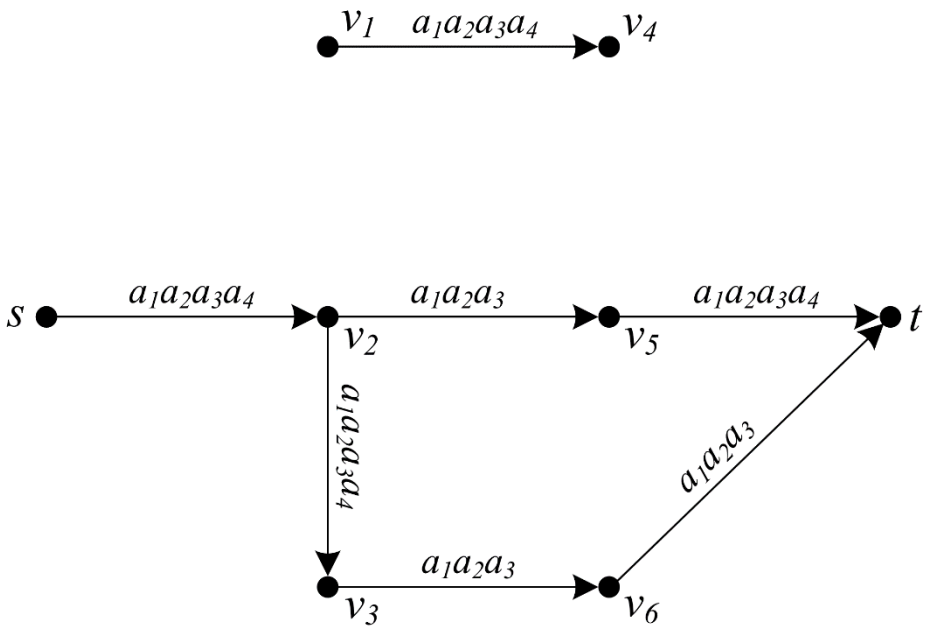

Рисунок 19. Сеть без дуг, стоимость которых не содержит $\{a_1a_2a_3\}$.

Аналогично рассматривается еще один элемент $\{a_1a_2a_4\}$. В этом случае реберно-непересекающихся путей из s в t также не существует (рисунок 20).

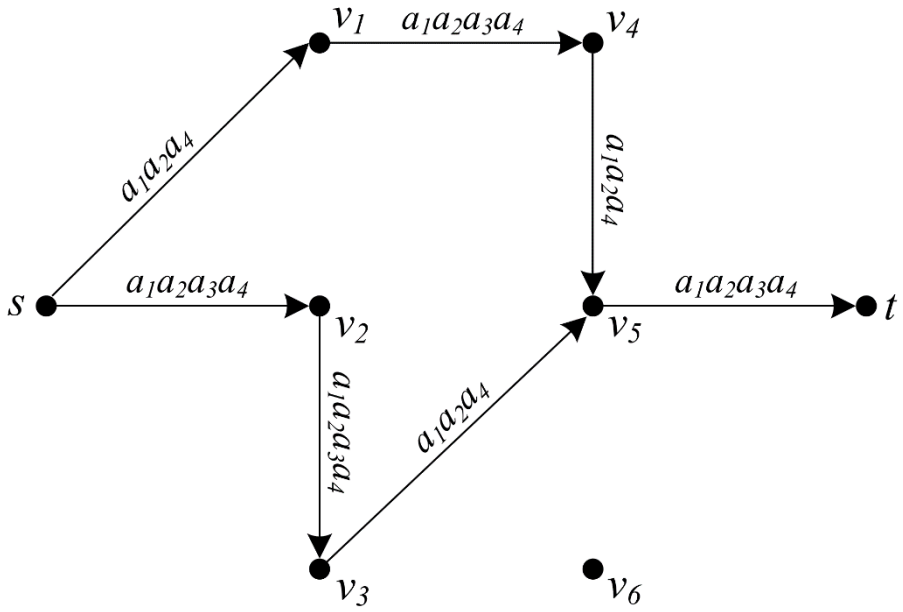

Рисунок 20. Сеть без дуг, стоимость которых не содержит $\{a_1a_2a_4\}$.

Далее из Q извлекаются элементы $\{a_1a_2, a_1a_3, a_2a_3, a_1a_4, a_2a_4\}$, имеющие максимальную мощность из оставшихся. Рассматривая $\{a_1a_2\}$, из

булевозначной сети удаляются все дуги, стоимость которых не содержит указанный элемент (рисунок 21).

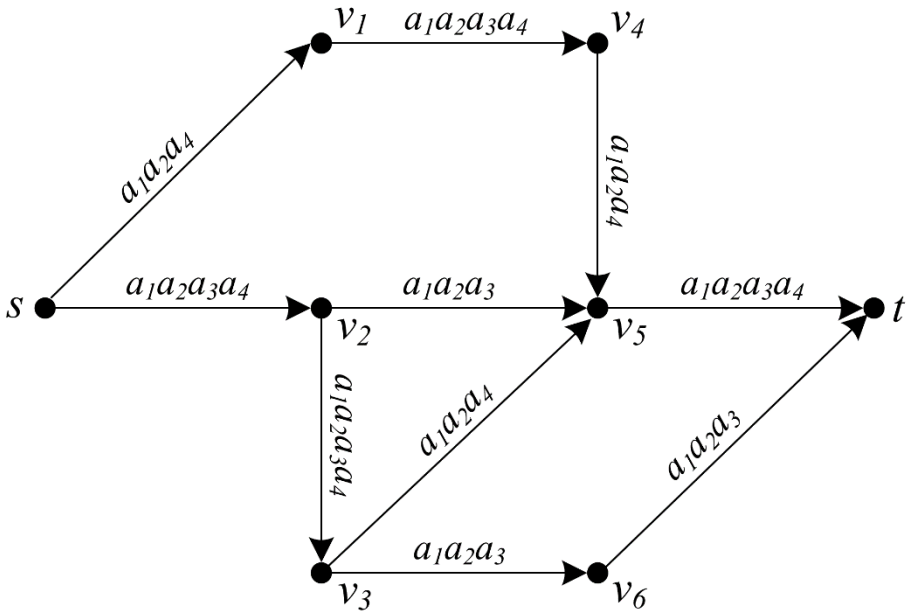

Рисунок 21. Сеть без дуг, стоимость которых не содержит $\{a_1a_2\}$.

Затем, в соответствии с алгоритмом Бхандари, сначала можно найти кратчайший путь из *s* в t в полученной сети (рисунок 22).

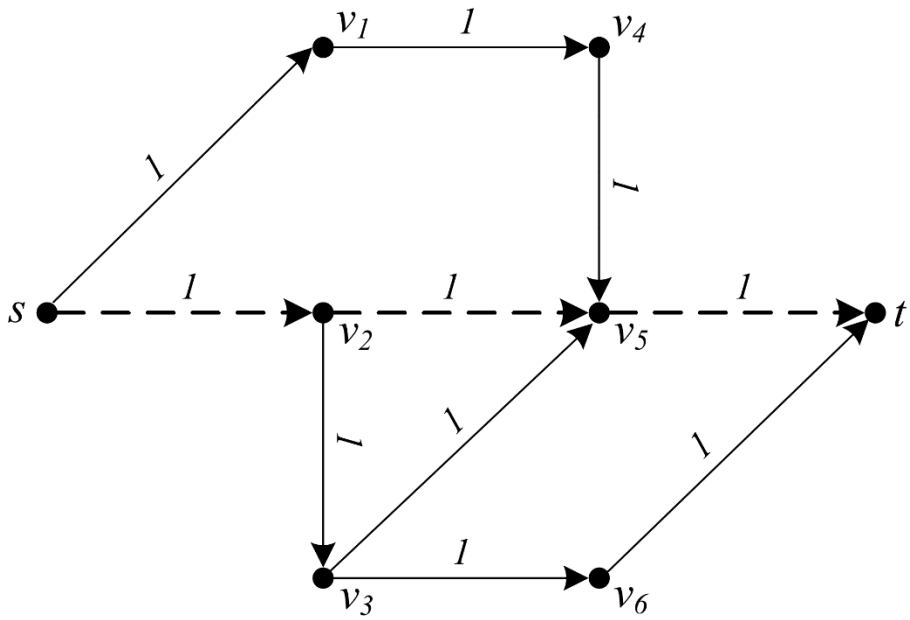

Рисунок 22. Результат первого шага алгоритма Бхандари

После этого дуги кратчайшего пути инвертируются и производится повторный поиск кратчайшего пути (рисунок 23).

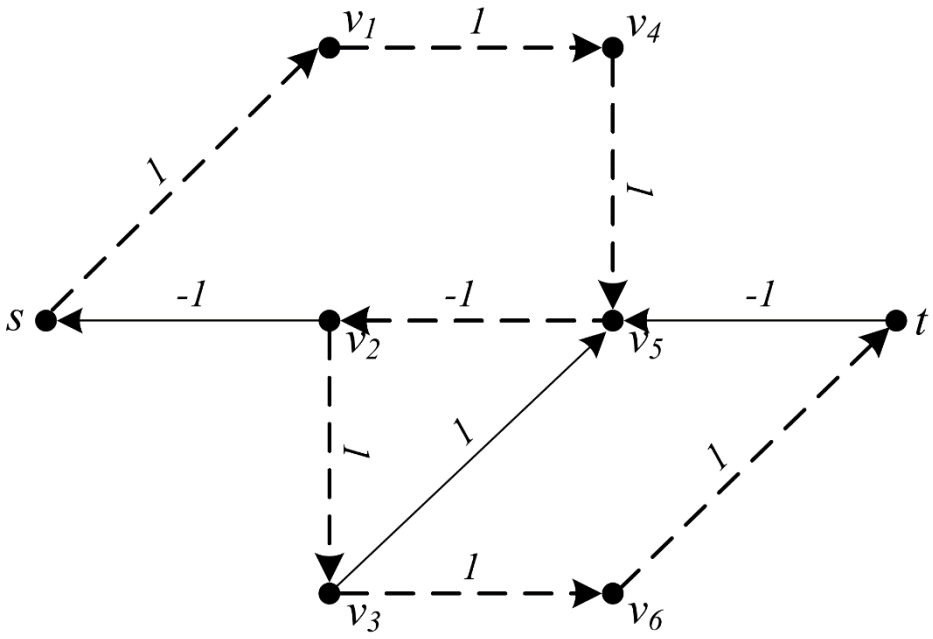

Рисунок 23. Результат второго шага алгоритма Бхандари

Объединив результаты двух шагов, может быть найдено множество P_1 двух реберно-непересекающихся (s,t)-путей с глобальной репутацией $b(P_1) = \{a_1a_2\}$ и общим числом дуг, равным 8 (рисунок 24).

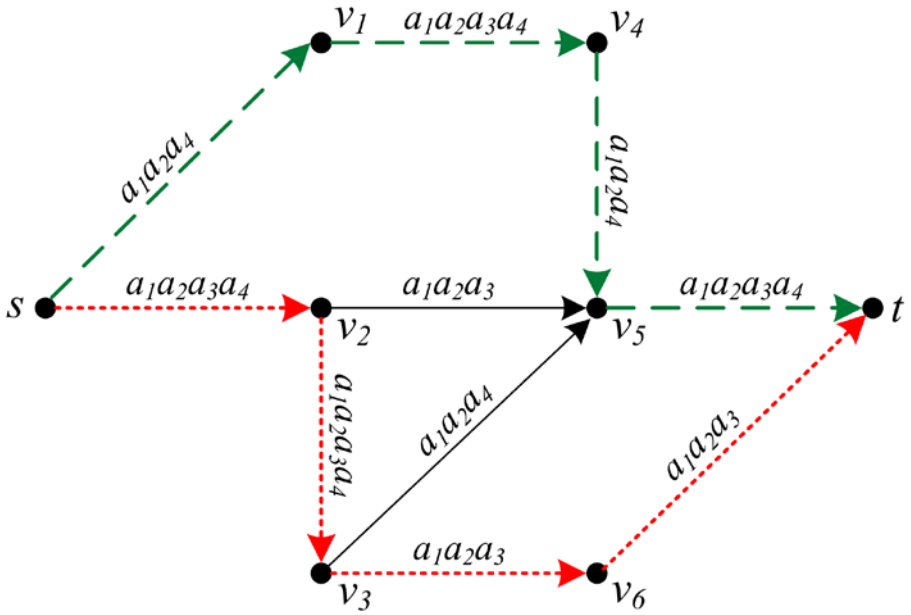

Рисунок 24. Результат работы алгоритма Бхандари в рассматриваемой сети

Далее рассматриваются остальные элементы той же мощности, извлеченные ранее из Q, и процедура повторяется заново.

Удалив из исходной булевозначной сети дуги, вес которых не содержит элемента $\{a_1a_4\}$, с помощью алгоритма Бхандари может быть найдено множество P_2 двух реберно-непересекающихся (s,t)-путей с глобальной репутацией $b(P_2) = \{a_1a_4\}$ и общим числом дуг, равным 7 (рисунок 25).

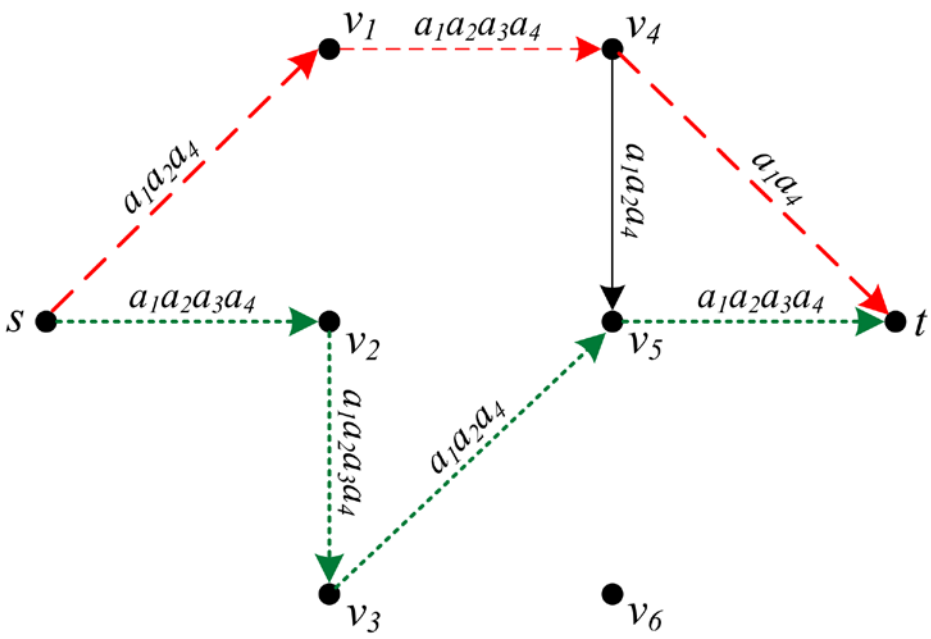

Рисунок 25. Два наиболее безопасных реберно-непересекающихся (s,t)-пути

Выбрав из полученных множеств Pj реберно-непересекающихся путей множество, содержащее пути с минимальным общим числом дуг, можно прийти к выводу, что два наиболее безопасных реберно-непересекающихся (s,t)-пути – это $<s, v_1, v_4, t>$ и $<s, v_2, v_3, v_5, t>$.

2.3 Экспериментальная оценка сложности разработанного алгоритма

Для экспериментальной оценки временной сложности разработанного алгоритма в рамках научно-исследовательской работы была разработана программа для генерации моделей беспроводных самоорганизующихся сетей с заданными параметрами (рисунок 26).

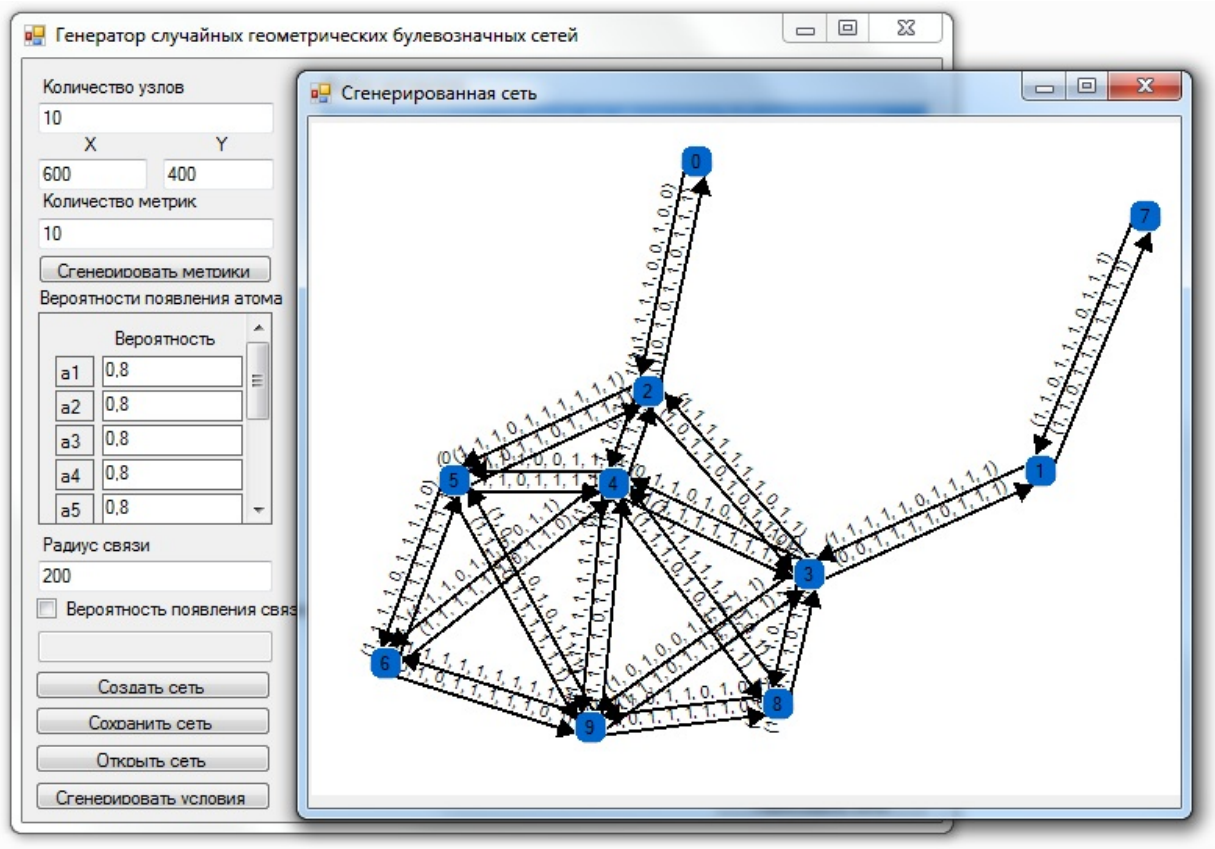

Рисунок 26. Экранная форма генератора случайных геометрических булевозначных сетей

Моделируемая самоорганизующаяся сеть представляется при помощи случайной геометрической булевозначной сети, в которой множество вершин соответствует множеству взаимодействующих узлов, множество дуг соответствует множеству каналов связи. В рамках рассматриваемой модели каждый узел размещается на плоскости в точке с координатами (x,y), значение которых определяется случайно в рамках заданного диапазона в соответствии с равномерным законом распределения.

Случайные геометрические графы широко используются для представления самоорганизующихся беспроводных сетей с динамической топологией благодаря их основному свойству. Два некоторых узла сети связаны дугой (каналом связи), только если расстояние между ними не превышает некоторого наперед заданного значения (радиус приема-передачи).

Для генерации случайных геометрических сетей также была использована модель Эрдеша-Реньи, расширенная для решения задач исследования – каждой дуге сети случайным образом ставится в соответствие элемент задаваемой булевой алгебры [87]. В рамках данной расширенной модели каждая пара узлов сети связана каналом связи, уровень безопасности которого $c(u,v)$ включает атом булевой алгебры a_i с вероятностью p_i. Таким образом, произвольный канал «рекомендован» одновременно всеми узлами сети с вероятностью $p_1p_2…p_n$ и не рекомендован ни одним из узлов с вероятностью $(1-p_1)(1-p_2)...(1-p_n)$.

Разработанное программное обеспечение поддерживает запись сгенерированных геометрических булевозначных сетей в файл формата GraphML [88], что позволяет экспортировать и импортировать моделируемые сети, используя стороннее программное обеспечение. Функционал разработанной системы позволяет в сгенерированной сети применить алгоритм поиска наиболее безопасного пути между заданной (или произвольной) парой узлов. Сети с небольшим количеством узлов могут быть визуализированы для более наглядного представления работы алгоритма. Для обеспечения серии экспериментальных исследований система также поддерживает пакетную генерацию требуемого количества различных сетей с заданными параметрами. Разработанная программа была зарегистрирована в Реестре программ для ЭВМ Роспатента [74] и использована для обеспечения имитационного моделирования поиска наиболее безопасных маршрутов в сетях с различными характеристиками.

В ходе серии испытаний производилась генерация моделей случайных беспроводных самоорганизующихся сетей с заданными параметрами и осуществлялся поиск наиболее безопасных маршрутов для некоторого узла сети. В результате указанных испытаний было определено среднее время, затраченное на поиск маршрутов, при различных экспериментальных параметрах. Результаты моделирования позволили экспериментально

подтвердить полученную ранее теоретическую оценку временной сложности разработанного алгоритма.

2.4 Имплементация разработанной модели и алгоритма для протокола маршрутизации OLSR

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 соответствии с разделом 2.2. Внесенные изменения описаны в работе [76].

Базовый протокол маршрутизации OLSR включает 4 типа сообщений (HELLO, TC, MID и HNA), которые широковещательно отправляются через существующие сетевые подключения [9]. Данные сообщения позволяют обеспечить обмен актуальной информацией о состоянии каналов связи. В рамках имплементации репутационной модели было предложено добавить два дополнительных типа сообщений протокола:

RM_MESSAGE – тип сообщений для распространения информации о состоянии каналов связи, проверенных отправителем пакета (рисунок 27).

ECHO_MESSAGE – тип сообщений для проверки каналов связи случайно выбранного маршрута (рисунок 28).

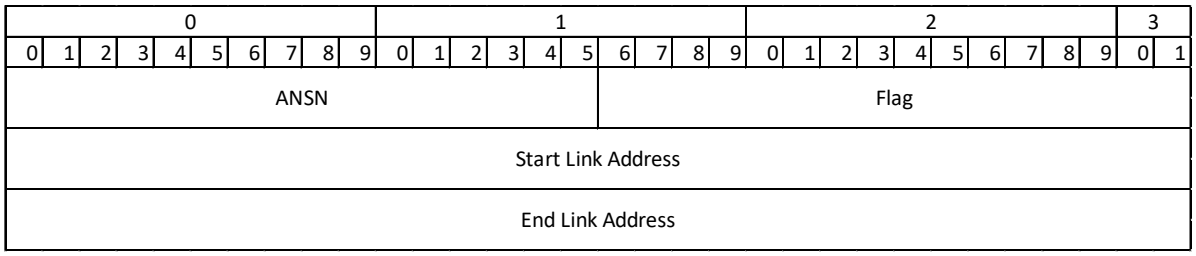

Рисунок 27. Структура RM сообщения

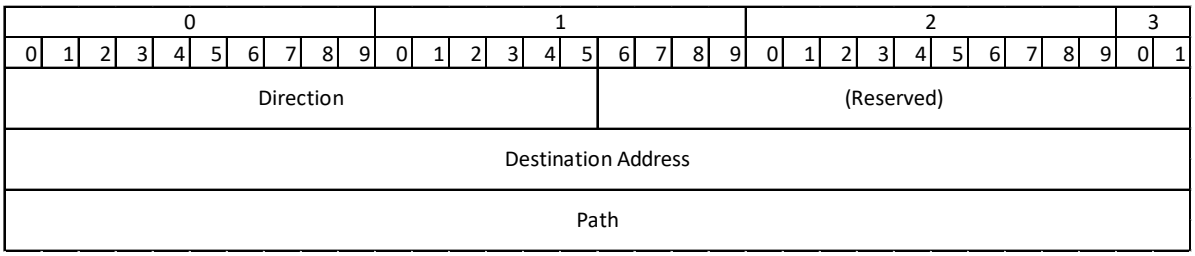

Рисунок 28. Структура ECHO сообщения

В сообщении RM поле Flag может принимать значение 0 либо 1, и указывает на анонсируемое значение локальной репутации для заданного канала связи, определяемого полями Start Link Address и End Link Address. Поле ANSN (Advertised Neighbor Sequence Number) используется как порядковый номер и позволяет узлам отслеживать, является ли полученное значение репутации более новым, чем то, которое уже имеется. В сообщении ECHO поле Direction может принимать значение 0 либо 1, и указывает на тип передаваемого сообщения, где 0 соответствует сообщению запроса, а 1 – ответному сообщению. Поле Destination Address указывает на адрес целевого узла, а Path – на проверяемый маршрут, используемый для доставки запроса.

Полученные в сообщениях RM 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.

Данные о состоянии каналов связи сети хранятся локально на каждом устройстве. Для хранения информации используется три таблицы [9]: таблица каналов связи до соседних узлов (**Neighbor Set**), таблица каналов связи от соседних узлов до узлов, доступных за два перехода (**2-hop Neighbor Set**), таблица всех остальных каналов связи (**Topology Information Base**).

Каждый прямой двусторонний направленный канал связи в указанных таблицах идентифицируется упорядоченной парой узлов (узлом источника и узлом назначения) на двух сторонах этого канала связи. Информация о

состоянии каналов связи, хранящаяся в указанных таблицах, регулярно используется для вычисления таблицы маршрутизации на каждом узле. В рамках имплементации репутационной модели структура вышеуказанных таблиц была модифицирована. В структуру каждой таблицы было добавлено новое поле «Recommendation», используемое для хранения вектора глобальной репутации для каждого канала связи в сетевой топологии. На рисунке 29 изображена структура модифицированных таблиц **Neighbor Set**, **2-hop Neighbor Set** и **Topology Information Base** соответственно, где зеленым цветом обозначены добавленные поля.

NeighborTuple			
Ipv4Address	enum	uint8_t	vector<Ipv4Address>
neighborMainAddr	statusSymmetric	willingness	recommendationInterfaceAddresses

TwoHopNeighborTuple			
Ipv4Address	Ipv4Address	Time	vector<Ipv4Address>
neighborMainAddr	twoHopNeighborAddr	expirationTime	recommendationInterfaceAddresses

TopologyTuple				
Ipv4Address	Ipv4Address	uint16_t	Time	vector<Ipv4Address>
destAddr	lastAddr	sequenceNumber	expirationTime	recommendationInterfaceAddresses

Рисунок 29. Модифицированные структуры хранения информации о состоянии каналов

2.5 Способ определения репутации каналов связи

Для определения локальной репутации проверяемых каналов связи в рамках протокола была сформирована дополнительная локальная таблица **Echo Requests**, 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 протокола. Ещё один дополнительный параметр определяет время ожидания ответного пакета при проверке маршрута. В случае если ответный тестовый пакет не был получен в течение заданного временного периода, проверяющий узел считает маршрут небезопасным, 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. При получении сообщений RM_MESSAGE узлы обновляют состояние каналов связи в своих таблицах и производят пересчёт наиболее безопасных маршрутов.

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 со значением 0 в поле Direction, зашифрованное и подписанное отправителем [78]. 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, значение поля Direction которого равно 1. Указанное ответное сообщение содержит информацию об обратном маршруте и подтверждает его актуальность.

На рисунке 30 приведен пример проверки маршрута Узлом 1 до Узла 7 посредством отправки сообщения ECHO_MESSAGE. Все устройства на пути следования пакета выполняют его маршрутизацию по направлению к узлу назначения.

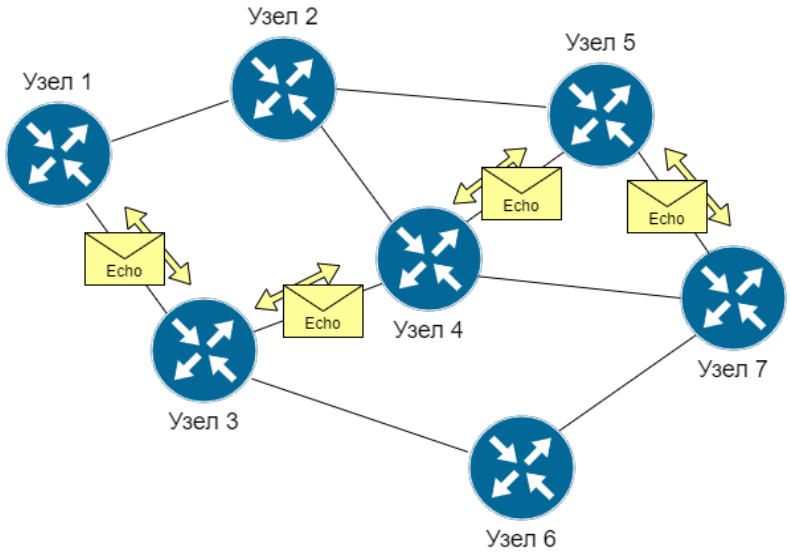

Рисунок 30. Отправка проверочного сообщения ECHO для оценки репутации каналов связи проверяемого маршрута

Узел 1, после получения ответного сообщения от Узла 7, изменяет локальное значение репутации соответствующих каналов связи и производит рассылку широковещательного пакета с сообщением RM_MESSAGE, которое содержит последовательность проверенных каналов связи и локальное значение репутации для каждого канала, равное 1 в рассматриваемом примере на рисунке 31.

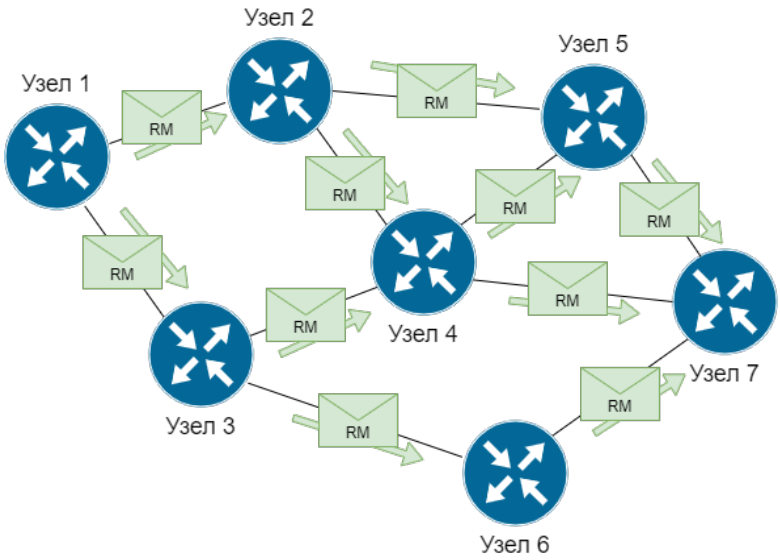

Рисунок 31. Широковещательная рассылка сообщений RM для распространения значений локальной репутации каналов связи

В рамках имплементации репутационной модели были внесены изменения в алгоритм вычисления маршрутов протокола OLSR. Модифицированная версия протокола получила название *Boolean Optimized Link State Routing* (BOLSR). Базовая функция вычисления таблицы маршрутизации была расширена посредством дополнительного вычисления наиболее безопасных маршрутов с использованием репутационной информации о состоянии каналов связи. Указанная информация используется для построения булевозначной сети, к которой применяется разработанный алгоритм [62]. В результате вычисления в таблицу маршрутизации заносятся наиболее безопасные маршруты до всех узлов сети, если таковые имеются. При отсутствии безопасного маршрута до некоторого узла в таблице сохраняется исходный маршрут протокола OLSR. При достижении сходимости таблиц протокола после передачи сообщений RM_MESSAGE, согласно разработанной репутационной модели, совокупность векторов глобальной репутации каналов связи будет идентичной на всех сетевых устройствах, что позволит обеспечить согласованный расчет таблиц маршрутизации.

2.6 Реализация протокола маршрутизации BOLSR на базе NS-3

Для имплементации предложенного комплекса решений в рамках протокола маршрутизации OLSR был выбран сетевой симулятор Network Simulator 3 (NS-3) [75]. Указанный сетевой симулятор обладает рядом ключевых преимуществ. В частности, NS-3 поддерживает работу всех широко используемых сетевых протоколов в соответствии с открытыми документами и стандартами RFC, обладает открытым исходным кодом, что позволяет эффективно расширять функциональность существующих протоколов, а также обеспечивает симуляцию процесса сетевого взаимодействия на всех уровнях модели представления сети для каждого устройства. Описанные преимущества позволили реализовать комплекс предложенных решений на базе существующего протокола маршрутизации

OLSR, проанализировать их эффективность и оценить различные факторы, влияющие работу полученного протокола BOLSR.

Программная реализация протокола маршрутизации OLSR в рамках сетевого симулятора NS-3 содержит четыре взаимодействующих модуля: *olsr-header*, *olsr-repositories*, *olsr-state* и *olsr-routing-protocol*. В целях имплементации комплекса предложенных решений в существующие программные модули протокола OLSR были внесены изменения, представленные на рисунке 32. Указанные на рисунке блоки отражают проделанные изменения, причем блоки синего цвета соответствуют модифицированным элементам программной реализации протокола, а зеленым цветом помечены функции, сообщения и структуры данных, которые были добавлены в результате имплементации.

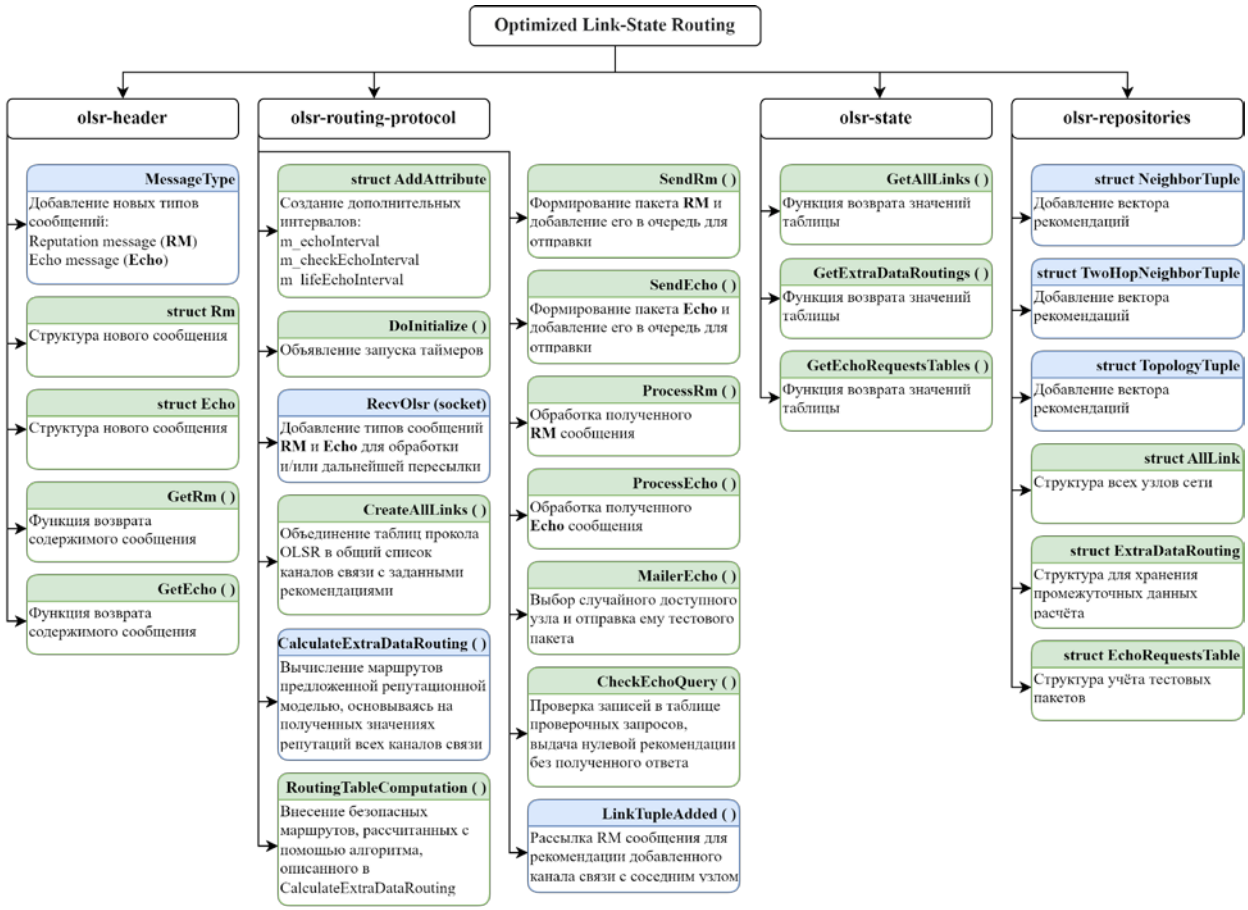

Рисунок 32. Имплементация комплекса решений для протокола OLSR в NS-3

Модуль *olsr-header* содержит описание всех поддерживаемых типов сообщений протокола OLSR, описание структуры сообщений и методы получения содержимого. Посредством изменения данного модуля были добавлены новые типы сообщений, используемых для обеспечения работы протокола: *RM_MESSAGE* и *ECHO_MESSAGE*. Добавлены соответствующие структуры сообщений: *structRm, structEcho*. Реализована функция возврата содержимого сообщения: *GetRm, GetEcho*.

Модуль *olsr-repositories* содержит в себе описание всех структур данных, необходимых для поддержания внутренней работы узла. В частности, в указанном модуле описана структура таблиц, используемых для хранения информации о состоянии каналов связи всей сети. Структуры *NeighborTuple*, *TwoHopNeighborTuple*, *TopologyTuple* были расширены с помощью дополнительного поля для хранения вектора глобальной репутации. Также в указанный модуль было добавлено описание вспомогательных структур для хранения промежуточных результатов вычислений и описание структуры отслеживания сообщений запроса *ECHO_MESSAGE*, отправленных для проверки маршрутов.

Модуль *olsr-state* включает реализацию всех функций, необходимых для управления внутренним состоянием узла. Для реализации предложенного подхода к поиску маршрутов, текущий модуль был расширен дополнительными функциями. Для получения состояния всех каналов связи подготовлена функция *GetAllLinks*, позволяющая объединить данные из таблиц *Neighbor Set, 2-hop Neighbor Set* и *Topology Information Base*. Реализована функция *GetExtraDataRouting*, позволяющая получить наиболее безопасные маршруты, ранее рассчитанные с помощью предложенного алгоритма. Подготовленная функция *GetEchoRequestsTables* позволяет получить перечень текущих запросов на проверку маршрутов, для формирования репутации каналов связи, образующих маршрут.

Модуль *olsr-routing-protocol* содержит основные функции и параметры для вычисления маршрутов. Протокол предусматривает периодическую

рассылку служебных пакетов. Периодичность рассылки задаётся с помощью специальных таймеров. В частности, таймер *m_echoInterval* был добавлен для рассылки сообщений *Echo*. Добавленный таймер *m_lifeEchoInterval* позволяет задать временной интервал актуальности проверочного запроса. Добавленный таймер *m_checkEchoInterval* определяет период проверки состояния текущих запросов *Echo* с целью поиска маршрутов, время проверки которых истекло.

Указанные выше таймеры объявляются в рамках функции *DoInitialize*, которая инициирует отправку сообщений протокола с заданной периодичностью с момента начала его работы на устройстве. Функция *RecvOlsr*, вызываемая при получении служебного сообщения с целью его последующей обработки, была расширена для обработки и ретрансляции дополнительных типов служебных сообщений.

Функции *SendRm* и *SendEcho* добавлены для формирования и отправки соответствующих служебных сообщений протокола. Аналогично функции *ProcessRm* и *ProcessEcho* добавлены для обработки сообщений *RM_MESSAGE* и *ECHO_MESSAGE*.

Добавленная функция *MailerEcho* инициирует отправку сообщения запроса *ECHO_MESSAGE* до случайно выбранного узла сети с целью определения локальной репутации каналов связи по маршруту до этого узла. Для периодической проверки состояния текущих запросов и отслеживания полученных ответов *Echo* добавлена функция *CheckEchoQuery*. При отсутствии ответа на запрос в заданный временной период, локальная репутация всех каналов, образующих проверяемый маршрут, обнуляется.

В целях реализации предложенного алгоритма поиска наиболее безопасных маршрутов на основе значений глобальной репутации каналов связи в модуль *olsr-routing-protocol* добавлена новая функция *CalculateExtraDataRouting*. Полученные маршруты используются при формировании таблицы маршрутизации устройства посредством расширенной функции *RoutingTableComputation*.

2.7 Выводы по главе

1. В целях обеспечения безопасности маршрутизации предложена новая транзитивная модель оценки репутации каналов связи самоорганизующейся сети. В рамках указанной модели глобальная репутация каналов связи определяется посредством булевозначного вектора, что позволяет полностью учитывать локальные значения репутации, полученные от различных узлов.
2. Для предложенной репутационной модели был разработан способ взаимодействия узлов сети в целях определения репутации каналов связи узлами сети. Указанный способ основан на периодической отправке специальных скрытых сообщений запроса другим узлам сети. Отслеживание ответов на отправленные запросы используется для определения локальной репутации каналов связи, образующих маршрут до получателя запроса.
3. На основе предложенной репутационной модели 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.
4. Для решения указанной формальной задачи 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 $O(n^3)$.
5. Для экспериментальной оценки временной сложности предложенного алгоритма была разработана программа для генерации моделей

беспроводных самоорганизующихся сетей с заданными параметрами. Результаты моделирования поиска наиболее безопасных маршрутов в случайных беспроводных самоорганизующихся сетях позволили экспериментально подтвердить полученную ранее теоретическую оценку временной сложности алгоритма.

6. В целях обеспечения безопасности маршрутизации сетевых пакетов в самоорганизующихся сетях, комплекс разработанных решений был имплементирован на базе существующего открытого 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 для дальнейшего экспериментального исследования эффективности предложенных моделей и алгоритма поиска наиболее безопасных маршрутов.

Глава 3 Исследование разработанных моделей и алгоритма

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. Проведение имитационного моделирования проводилось в сетях со статической и динамической топологией, в соответствии с выбранной моделью мобильности узлов, определяющей их перемещение в заданном ограниченном пространстве.

Имитационное моделирование является стандартным и широко используемым способом верификации различных сетевых протоколов и алгоритмов благодаря возможности точно контролировать условия тестирования, что обеспечивает воспроизводимость экспериментов [89]. Применение имитационного моделирования предоставляет ряд преимуществ для достижения поставленной цели. В частности, таким образом можно исследовать работу протоколов в различных сценариях и условиях, значительно снизить затраты, сократить время, затраченное на проведение экспериментов, и за счет большого количества испытаний более точно выявить закономерности на основе наблюдаемых сетевых характеристик.

Исходя из программной реализации протокола маршрутизации BOLSR, разработанной и представленной в разделе 2.6 настоящей работы, моделирование сетевого взаимодействия производилось на базе сетевого симулятора NS-3. Данный симулятор зарекомендовал себя среди групп ученых по всему миру для моделирования сетевых процессов и является стандартом де-факто в научно-исследовательской среде. В рамках указанной системы моделирование проводится на основе дискретных событий, что отвечает задачам исследования различных сетевых протоколов посредством анализа характеристик узлов сети, каналов связи и сеансов передачи данных. Симулятор NS-3 обеспечивает встроенную поддержку различных моделей мобильности узлов, включая модель случайного блуждания (Random Walk,

RW) [90], модель случайного блуждания с остановками (Random Waypoint, RWP) [91], модель случайного направленного движения (Random Direction, RD) [92], Манхэттенскую модель (Manhattan Mobility) [93] и некоторые другие.

В рамках экспериментального исследования разработанного комплекса решений по обеспечению безопасности маршрутизации пакетов в самоорганизующихся сетях были сформулированы следующие задачи:

1. Проверка адекватности предложенной и реализованной модели нарушителя в самоорганизующихся сетях при условии использования протокола маршрутизации OLSR для обнаружения маршрутов.

2. Сравнительный анализ эффективности процесса маршрутизации сетевых пакетов при использовании протоколов маршрутизации OLSR и BOLSR в условиях воздействия на указанный процесс различного количества вредоносных узлов.

3. Сравнительный анализ характеристик используемых маршрутов при использовании протоколов маршрутизации OLSR и BOLSR в условиях воздействия на процесс маршрутизации пакетов различного количества вредоносных узлов.

3.1 Модель нарушителя

Модель нарушителя представляет предположения о возможностях и ограничениях нарушителя, которые он может использовать для разработки и проведения атак. Разработка модели нарушителя является неотъемлемой частью решения задачи обеспечения информационной безопасности. Для составления модели нарушителя не существует строгой стандартизированной методики, вследствие чего модель часто имеет свободный неформальный характер [94]. Этапы построения модели нарушителя могут включать определение перечня защищаемой информации, выявление актуальных угроз и установление возможностей нарушителя. В рамках настоящей диссертационной работы была определена модель нарушителя, используемая

для оценки уязвимости проактивной маршрутизации пакетов в беспроводных самоорганизующихся сетях и оценки эффективности обеспечения безопасности маршрутизации на основе комплекса предложенных решений.

Помимо информации, которая традиционно относится к защищаемой в любых информационных системах, в беспроводных самоорганизующихся сетях к защищаемой также относится любая информация, связанная с пользовательскими сеансами, включая идентификаторы и временные метки, конфигурационная информация, включая настройки безопасности и сетевые параметры, данные вспомогательных сетевых протоколов, включая данные о сетевых маршрутах. В рамках принятой модели защите по характеристике доступности должны подлежать любые пакеты данных, передаваемые в беспроводной самоорганизующейся сети. Обеспечение защиты информации в беспроводных самоорганизующихся сетях по характеристикам конфиденциальности и целостности в настоящей работе не рассматривается.

Перечень актуальных угроз процессу маршрутизации в беспроводных самоорганизующихся сетях сформулирован в разделе 1.2 настоящей диссертационной работы. Обеспечение защиты беспроводных самоорганизующихся сетей от внешних нарушителей, как правило, эффективно достигается средствами аутентификации, авторизации и учета доступа, а также криптографическими преобразованиями передаваемых данных. В то время как внутренние узлы могут быть скомпрометированы и представлять угрозу доступности маршрутизируемых через эти узлы пакетов. Таким образом, в рамках принятой модели нарушителя рассматривается угроза частичного или полного нарушения доступности передаваемых данных посредством действий узла нарушителя, препятствующих дальнейшей передаче поступающих пакетов по направлению к узлу назначения.

Исходя из принятой модели, любой узел нарушителя является внутренним узлом беспроводной самоорганизующейся сети и, как следствие, вместе с остальными узлами должен участвовать в маршрутизации сетевых пакетов.

Реализация узлом нарушителя угрозы нарушения доступности сетевых пакетов возможна посредством организации сетевой атаки типа «черная дыра» или «серая дыра». Реализация угрозы нарушения доступности данных в беспроводной самоорганизующейся сети с помощью данной сетевой атаки может иметь критические последствия в военной, медицинской, финансовой и других сферах. В результате действий нарушителя в ходе проведения указанной атаки все или некоторая часть поступающих от других узлов сетевых пакетов отбрасывается 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.

Узел нарушителя может использовать различные методы для привлечения пакетов данных от других узлов в сети, включая направленные перемещения в пространстве и объявление фиктивных маршрутов. При выполнении атаки в активном режиме узел нарушителя объявляет несуществующие маршруты к другим узлам сети, что позволяет повысить эффективность атаки. С другой стороны, реализация атаки в пассивном режиме позволяет избежать обнаружения со стороны соседних узлов.

В рамках принятой модели узел нарушителя выполняет атаку типа «черная дыра» посредством фильтрации всех поступающих пакетов данных и не осуществляет подозрительную активность в сети с целью избежать раскрытия. Схема поведения узла нарушителя в рамках проведения сетевой атаки типа «черная дыра» представлена на рисунке 33.

Последовательность действий нарушителя в рамках принятой модели может быть сформулирована следующим образом:

1. Злоумышленник создает узел в самоорганизующейся сети и настраивает свой беспроводной интерфейс для прослушивания входящих пакетов данных;

2. Злоумышленник выполняет отправку и прием служебных сообщений, используемого проактивного протокола маршрутизации, объявляя маршруты к другим узлам соответственно поведению легитимного узла сети;
3. Злоумышленник выполняет перехват и полную фильтрацию поступающих на интерфейс пакетов данных от других узлов в сети. Узел нарушителя отбрасывает пакеты, которые он получает от соседних узлов, фактически создавая «черную дыру» в сети;
4. Атака узла нарушителя продолжается в пассивном режиме до тех пор, пока узел злоумышленника не покинет сеть.

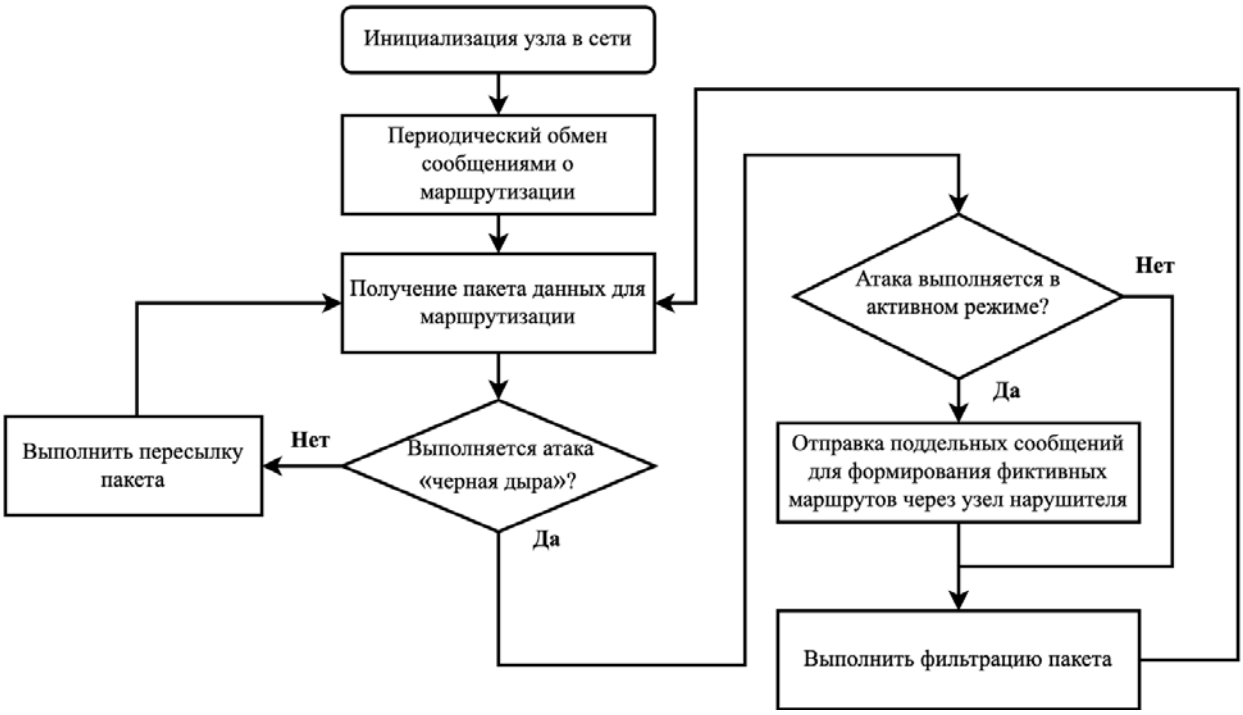

Рисунок 33. Схема поведения узла нарушителя в самоорганизующейся сети

Указанная модель нарушителя была реализована на базе проактивного протокола маршрутизации OLSR в рамках сетевого симулятора NS-3. Экспериментальные исследования посредством имитационного моделирования взаимодействия узлов в беспроводных самоорганизующихся сетях с разным числом узлов нарушителей позволили подтвердить адекватность предложенной модели [95].

3.2 Имитационное моделирование маршрутизации с использованием разработанного протокола

При решении задач экспериментального исследования посредством имитационного моделирования сетевого взаимодействия для каждого испытания должна быть определена начальная топология сети, состоящая из множества узлов и множества каналов связи между ними, модель перемещения узлов и тип сетевого трафика, передаваемого между узлами сети.

В целях проведения имитационного моделирования был разработан план экспериментальных исследований, определены основные параметры начальной сетевой топологии и узлов сети. Для экспериментальной оценки безопасности маршрутизации сетевых пакетов был выбран стандартный сценарий типа «транзитная сеть» [96, 97]. В рамках указанного сценария два узла, выступающие в качестве источника и получателя сетевых пакетов, выполняют роль стационарных базовых станций и находятся за пределами прямой видимости, а устройства, размещенные в области между базовыми станциями, выступают в роли ретрансляторов, обеспечивающих связь между ними. В такой сети мобильность, как правило, минимальна или отсутствует полностью, так как устройства, которые остаются неподвижными, обеспечивают более высокую производительность сети. Применение такого сценария уже рассматривалось во время сравнительного анализа протоколов AODV и OLSR в работе [98].

Все узлы, задействованные в испытаниях, использовали согласованный набор сетевых протоколов, стандартов и характеристик на физическом, канальном, сетевом и транспортном уровне, что обеспечило возможность взаимодействия устройств на всех вышеперечисленных уровнях. Согласно выбранному сценарию, всем интерфейсам сетевых устройств были назначены уникальные сетевые адреса, которые использовались для их идентификации и обеспечения сквозной передачи сетевых пакетов 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 900х600 м^2. Задание области прямоугольной формы приводит к построению более длинных маршрутов по сравнению с областью квадратной формы, при этом плотность узлов на единицу площади остаётся неизменной [98]. 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 решения задач исследования в рамках выбранного сценария было проведено несколько экспериментов с разным числом транзитных узлов нарушителей (от 0 до 6 узлов). Таким образом, 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. Исходя из модели и схемы, предложенной в разделе 3.1, узлы нарушителей в рамках выбранного сценария осуществляли сетевую атаку типа «черная дыра» посредством фильтрации всех поступающих пакетов данных, в то время как передача сообщений вспомогательных сетевых протоколов, включая протоколы маршрутизации, выполнялась без изменений. При этом каждое легитимное сетевое устройство обеспечивало маршрутизацию всех поступающих сетевых пакетов.

Учитывая, что в сетях со статической и динамической топологией эффективность предложенного комплекса решений по обеспечению маршрутизации пакетов может значительно варьироваться, все эксперименты производились, как в сетях со стационарными, так и в сетях с мобильными узлами. Для моделирования движения узлов в двумерном пространстве была

выбрана модель случайного направленного движения Random Direction 2D. Указанная модель обладает рядом достоинств и позволяет достаточно точно отразить мобильность узлов в рамках самоорганизующихся сетей различных типов [99, 100]. Согласно данной модели мобильности, каждое устройство в течение заданного временного интервала движется в случайном направлении со скоростью, определяемой случайным образом в пределах заданного диапазона. По завершении заданного временного интервала устройство может изменять направление своего движения. В рамках симулятора NS-3 указанный интервал может быть задан при помощи соответствующего параметра «time interval». Кроме того, модель позволяет учитывать наличие стен и препятствий, которые могут повлиять на движение устройств. При достижении некоторым узлом границ области моделирования или любого препятствия, данный узел случайным образом изменяет параметры своего движения.

Несмотря на то, что выбранная модель мобильности узлов в беспроводной сети Random Direction 2D является достаточно простой и не учитывает множество объективных факторов взаимодействия, включая перегруженность каналов связи, внешние помехи, изменение условий распространения сигнала и некоторые другие, возможное влияние перечисленных факторов на результаты моделирования не препятствует качественному решению сформулированных задач экспериментальных исследований.

Процесс генерации трафика является неотъемлемой частью имитационного моделирования сетевого взаимодействия, поскольку он напрямую влияет на достоверность моделирования и имеет критическую важность для оценки эффективности различных сетевых протоколов и технологий. В рамках экспериментального исследования для генерации трафика на узлах сети была выбрана модель с постоянной производительностью (Constant Bit Rate, CBR), которая позволяет создавать и отправлять равные по объему сетевые пакеты через одинаковые временные

интервалы в течение заданного периода [101]. Указанная модель, с одной стороны, достаточно точно подходит для описания трафика множества различных приложений самоорганизующихся сетей, а с другой стороны позволяет обеспечить постоянную нагрузку и полную предсказуемость трафика, что позволяет свести к минимуму влияние данного фактора на результаты испытаний.

Данные, генерируемые по модели CBR, инкапсулировались в сегменты протокола UDP. Применение указанного протокола на транспортном уровне позволяет реализовать потоковую передачу данных, что широко используется для доставки аудиоданных и видеоданных в режиме реального времени. В результате выбора протокола UDP, в ходе проведения имитационного моделирования была получена возможность оценить эффективность доставки данных на основе коэффициента доставленных пакетов.

Несмотря на то, что протокол TCP позволяет гарантировать надёжную доставку данных, а также даёт возможность упорядочить полученные сегменты данных, его применение для передачи данных на транспортном уровне ведет к значительным накладным расходам. Помимо этого, при использовании протокола TCP невозможно напрямую оценить потери сегментов данных, возникающие при их доставке, что, в свою очередь, затрудняет сравнение различных методов и протоколов маршрутизации. Приняв во внимание рекомендации, изложенные в работах [102, 103], проведение исследования с использованием протокола TCP не проводилось.

Для выбранного сценария имитационного моделирования, перечень определяемых параметров эксперимента также включает внутренние параметры работы протоколов. Все действия узлов в рамках протокола имеют определенную периодичность, определяемую значениями его параметров. В рамках проведенного эксперимента использовались фиксированные параметры протоколов OLSR и BOLSR.

Значение параметра HELLO_INTERVAL позволяет определить время широковещательной рассылки HELLO сообщений по всей сети. В рекомендациях стандарта RFC 3626 значение параметра HELLO_INTERVAL не должно превышать REFRESH_INTERVAL.

Сообщение HELLO может быть частичным, например, из-за ограничений размера сообщения, наложенных сетью и т.д. Для каждого интерфейса любой канал связи с соседним узлом должен быть указан в HELLO сообщении по крайней мере один раз в течение заранее определенного периода обновления – REFRESH_INTERVAL. Чтобы отслеживать быстрые изменения в сети, сообщение HELLO должно отправляться в течение заданного периода HELLO_INTERVAL, которое должно быть меньше или равно REFRESH_INTERVAL.

Параметры TC_INTERVAL, MID_INTERVAL, HNA_INTERVAL описывают время периодической рассылки соответствующих сообщений. Назначение этих сообщений в работе протокола OLSR описано в разделе 1.1.

Значение таймера NEIGHB_HOLD_TIME определяет время удержания информации о соседних узлах в локальных таблицах, после которого информация становится недействительной.

Параметры TOP_HOLD_TIME, MID_HOLD_TIME, HNA_HOLD_TIME определяют временные интервалы, в течение которых информация о соответствующих записях в таблицах, хранящих информацию о сетевой топологии, является актуальной.

Таймер DUP_HOLD_TIME представляет собой временной интервал, в течение которого шлюзы MPR записывают информацию о пересылаемых пакетах.

Описанные выше параметры позволяют настроить работу протоколов OLSR и BOLSR для различных рассматриваемых сценариев. По результатам предварительных экспериментов принято решение сохранить параметры работы протокола OLSR в стандарте RFC 3626 для предложенного сценария

имитационного моделирования. Выбранные параметры работы протоколов представлены в таблице 9.

Таблица 9. Параметры протоколов OLSR и BOLSR

Параметр	**Значение**
HELLO_INTERVAL	2.0 с
REFRESH_INTERVAL	2.0 с
TC_INTERVAL	5.0 с
MID_INTERVAL	5.0 с
HNA_INTERVAL	5.0 с
NEIGHB_HOLD_TIME	3 * REFRESH_INTERVAL
TOP_HOLD_TIME	3 * TC_INTERVAL
MID_HOLD_TIME	3 * MID_INTERVAL
HNA_HOLD_TIME	3 * HNA_INTERVAL
DUP_HOLD_TIME	30 с

Разработанный протокол BOLSR имеет дополнительные параметры, определяющие период рассылки новых типов сообщений. Назначение указанных параметров представлено в разделе 2.6. Предложенные значения параметров были экспериментально определены для предложенного сценария (таблица 10).

Таблица 10. Дополнительные параметры протокола BOLSR

Параметр	**Значение**
CHECK_ECHO_INTERVAL	2 с
LIFE_ECHO_INTERVAL	5 с
ECHO_INTERVAL	2 с

Для экспериментальной оценки эффективности предложенного комплекса решений посредством имитационного моделирования сетевого

взаимодействия в симуляторе NS-3 был использован ряд нижеследующих показателей:

Коэффициент доставки пакетов (Packet Delivery Ratio, PDR) – это ключевой и наиболее широко используемый показатель при оценке качества различных маршрутов доставки пакетов в самоорганизующихся сетях [104, 105]. Данный коэффициент представляет отношение успешно доставленных до получателей пакетов к общему числу отправленных пакетов, т.е. фактически позволяет оценить процент успешно доставленных пакетов.

Относительное количество маршрутов через узлы нарушителей – данный показатель соответствует отношению числа используемых сетевых маршрутов, проходящих через узлы нарушителей, к общему числу используемых маршрутов доставки пакетов. Данный показатель объективно отражает возможность протокола маршрутизации адаптироваться к изменению условий сетевого взаимодействия, включая возможность изоляции узлов нарушителей. При условии изоляции узлов нарушителей относительное количество маршрутов через узлы нарушителей с течением времени должно стремиться к нулю.

Средняя длина маршрутов – данный показатель отражает усредненное по всем используемым сетевым маршрутам количество переходов пакетов для достижения узла назначения. В рамках сформулированных задач экспериментального исследования измерение данного показателя представляет наиболее простой способ сравнительно оценить возможное изменение производительности сетевого взаимодействия. При прочих равных использование более длинных маршрутов может приводить к снижению производительности взаимодействия и увеличению задержек.

Оценка эффективности разработанного комплекса решений по обеспечению безопасности маршрутизации пакетов была выполнена на основе сравнительного анализа вышеуказанных показателей сетевого взаимодействия при использовании протоколов OLSR и BOLSR.

На рисунке 34 в качестве примера представлена одна из случайных сетевых топологий, использованных в рамках имитационного моделирования, и обозначены маршруты доставки пакетов от отправителя до получателя, определенные при помощи протоколов OLSR и BOLSR. Пунктирной линией ограничена область расположения транзитных узлов.

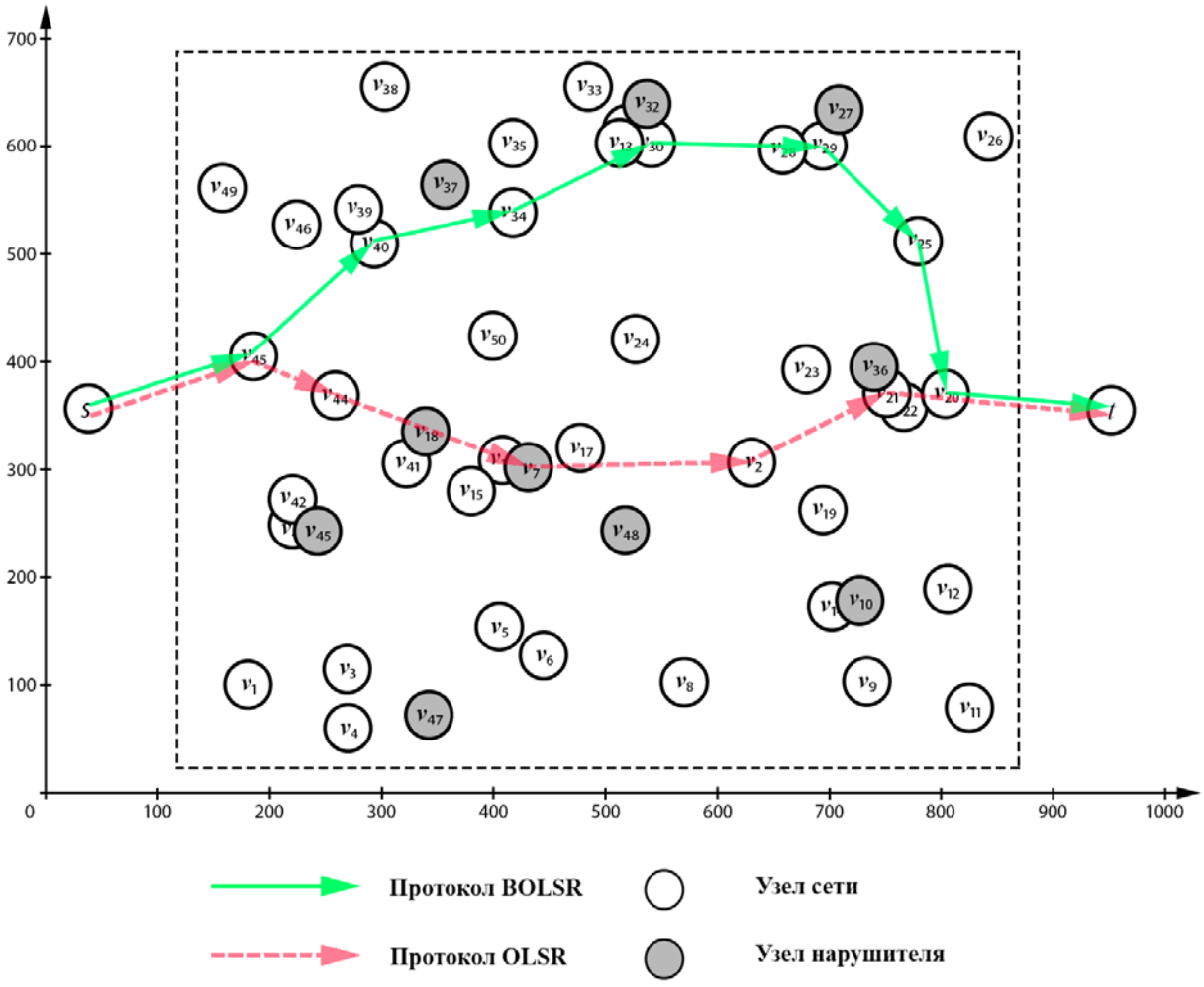

Рисунок 34. Пример различного выбора маршрутов при использовании OLSR и BOLSR

Следует обратить внимание, что в предложенном примере при использовании протокола OLSR был выбран маршрут доставки пакетов, проходящий через узел нарушителя. В то время как при использовании протокола BOLSR был найден альтернативный маршрут доставки пакетов.

Несмотря на то, что данный маршрут не является кратчайшим по количеству переходов, маршрут исключает узлы нарушителей при доставке пакетов до получателя.

Основные условия проведенного экспериментального исследования в сетевом симуляторе NS-3 представлены в таблице 11. Для повышения точности оценки указанных характеристик в рамках каждого эксперимента с заданным набором входных параметров было проведено 100 независимых испытаний. Топология транзитной сети для каждого испытания включала 50 устройств, положение которых 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. Выбор параметров эксперимента обоснован предыдущими экспериментальными исследованиями в работах [106, 107].

Таблица 11. Параметры экспериментального исследования

Параметры эксперимента	**Значение**
Количество испытаний	100
Время моделирования	180 с
Область расположения узлов	600м х 900м
Количество устройств в сети	52
Модель мобильности узлов	[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

Результат каждого испытания в сетевом симуляторе NS-3 был записан в файл трассировки, включающий информацию обо всех отправленных и полученных пакетах каждым устройством сети. Файл трассировки предоставляет подробную запись событий и потоков данных, наблюдаемых во время моделирования, которую можно использовать для апостериорного анализа производительности и других показателей сетевого взаимодействия. Посредством анализа файлов трассировки для каждой серии испытаний был определен средний коэффициент доставки пакетов.

Кроме того, в ходе каждого испытания фиксировалась расширенная таблица маршрутизации узла, выполняющего отправку пакетов. Расширенная версия таблицы маршрутизации помимо адреса следующего перехода включает также весь предполагаемый маршрут доставки пакетов до узла назначения. Полученная информация позволила определить среднюю длину используемых маршрутов до всех узлов сети и относительное количество маршрутов, проходящих через узлы нарушителей.

Таким образом, по результатам каждой серии испытаний с заданным набором входных параметров был произведен расчёт среднего коэффициента доставки пакетов, относительного количества маршрутов через узлы нарушителей и средней длины маршрутов. Анализ указанных показателей позволил обеспечить решение сформулированных задач экспериментального исследования.

3.3 Анализ и сравнение полученных результатов

В ходе решения первой задачи экспериментального исследования было проанализировано изменение коэффициента доставки пакетов в сетях со статической топологией в условиях воздействия на процесс маршрутизации пакетов различного количества вредоносных узлов, реализующих сетевую атаку типа «черная дыра» (рисунок 35).

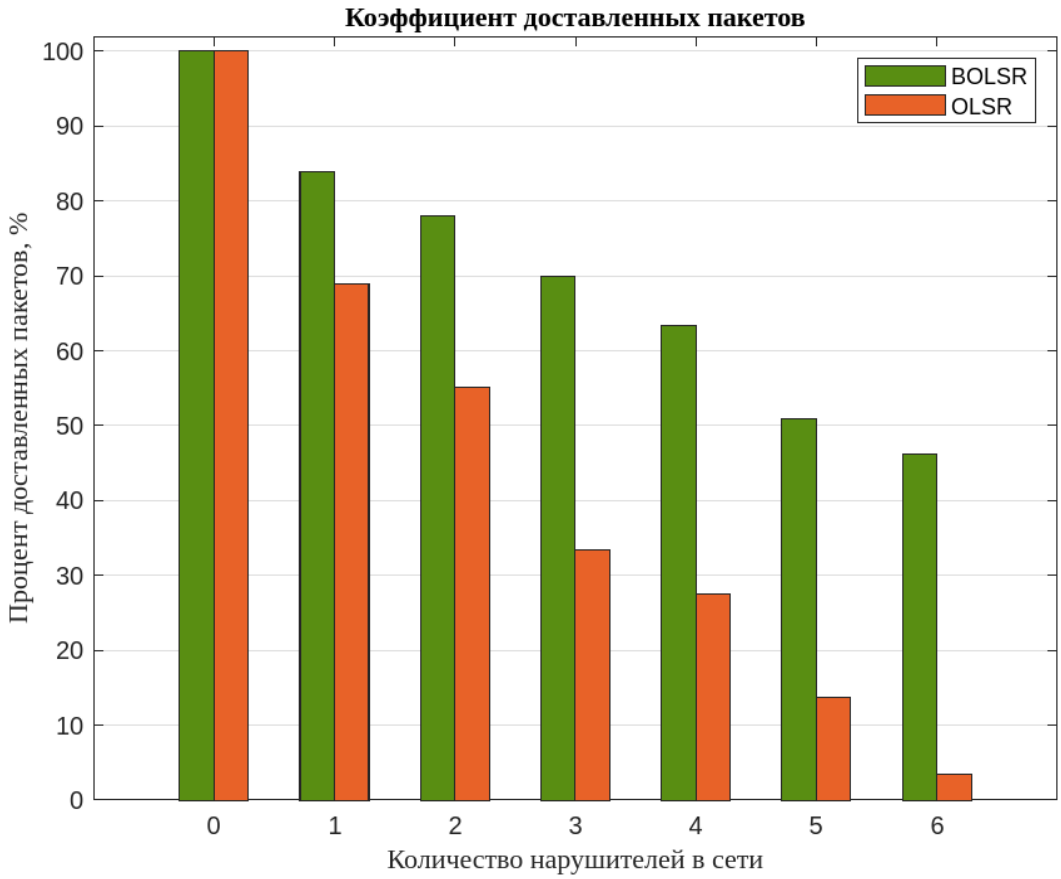

Рисунок 35. Коэффициент доставки пакетов в сетях со статической топологией при различном количестве узлов нарушителей

В результате анализа можно отметить, 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. При

использовании протокола маршрутизации OLSR среднее снижение коэффициента доставки пакетов составляет от 31% в сетях в одним узлом нарушителя до 96% в сетях с 6 узлами нарушителей. Наблюдаемое изменение коэффициента доставки пакетов, очевидно, связано с тем, что при увеличении числа узлов нарушителей в сети увеличивается относительное количество маршрутов доставки пакетов через эти узлы, что, в свою очередь, приводит к успешной реализации сетевых атак типа «черная дыра», выполняемых в соответствии с выбранной моделью узла нарушителя.

Соответствующий анализ изменения коэффициента доставки пакетов в условиях воздействия на процесс маршрутизации различного количества вредоносных узлов также был выполнен в сетях с динамической топологией, с использованием модели мобильности узлов Random Direction 2D. Результаты экспериментальной оценки коэффициента доставки пакетов в сетях с динамической топологией представлены на рисунке 36. Несмотря на то, что снижение коэффициента доставки пакетов в рамках данного эксперимента может быть обусловлено мобильностью узлов, увеличение количества узлов нарушителей в сети также приводит к непрерывному снижению коэффициента доставки пакетов. При использовании протокола маршрутизации OLSR среднее снижение коэффициента доставки пакетов составляет от 29% в динамических сетях в одним узлом нарушителя до 94% в динамических сетях с 6 узлами нарушителей.

Таким образом, в результате анализа изменения коэффициента доставки пакетов в сетях со статической и динамической топологией было получено экспериментальное обоснование адекватности предложенной и реализованной модели нарушителя в самоорганизующихся сетях.

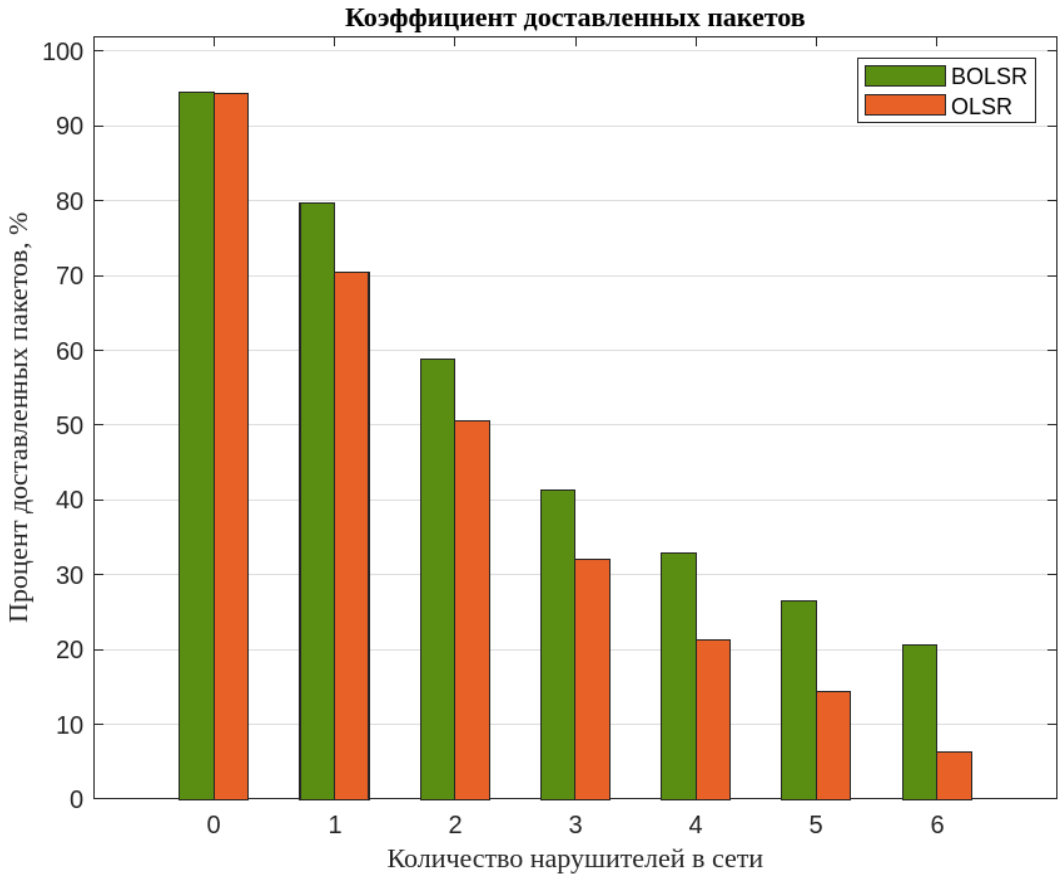

Рисунок 36. Коэффициент доставки пакетов в сетях с динамической топологией при различном количестве узлов нарушителей

В рамках решения второй задачи экспериментального исследования был выполнен сравнительный анализ изменения коэффициента доставки пакетов при использовании протоколов маршрутизации OLSR и BOLSR в условиях воздействия на процесс маршрутизации различного количества вредоносных узлов. Учитывая результаты моделирования в сетях со статической топологией (рисунок 35), можно отметить, что применение разработанного протокола маршрутизации BOLSR вместо протокола OLSR позволило увеличить значение коэффициента доставки пакетов по сравнению с использованием оригинального протокола OLSR в диапазоне от 15% (увеличение в 1,2 раза в сети с одним узлом нарушителя) до 42% (увеличение в 11,5 раз в сети с 6 узлами нарушителей). Важно, что при увеличении числа нарушителей в сети коэффициент доставки пакетов снижается медленнее в случае использования протокола маршрутизации BOLSR.

В результате анализа результатов моделирования в сетях с динамической топологией (рисунок 36) было установлено, что применение протокола маршрутизации BOLSR вместо протокола OLSR позволило увеличить значение коэффициента доставки пакетов по сравнению с использованием оригинального протокола OLSR в диапазоне от 9% (увеличение в 1,12 раза в сети с одним узлом нарушителя) до 15% (увеличение в 3,5 раз в сети с 6 узлами нарушителей). Можно отметить, что рамках данного эксперимента коэффициент доставки пакетов имеет более низкие значения по сравнению с предыдущим экспериментом в сетях со статической топологией. Также, можно отметить, что эффективность применения протокола BOLSR в сетях с динамической топологией снижается при увеличении числа нарушителей. Данный факт объясняется необходимостью временных затрат для формирования вектора глобальной репутации каналов связи, вновь образованных в результате мобильности узлов сети. В сетях с низкой мобильностью узлов существующие каналы связи являются более стабильными, что повышает эффективность применения предложенного комплекса решений для обеспечения безопасности маршрутизации.

Для решения третьей задачи экспериментального исследования был выполнен сравнительный анализ средней длины используемых маршрутов и относительного количества маршрутов, проходящих через узлы нарушителей, при использовании протоколов маршрутизации OLSR и BOLSR, в условиях воздействия на процесс маршрутизации различного количества вредоносных узлов. Важным результатом исследования является тот факт, что применение протокола маршрутизации BOLSR позволяет сократить количество маршрутов, проходящих через узлы нарушителей, по сравнению с исходным протоколом OLSR.

Результаты экспериментальной оценки среднего относительного количества маршрутов, проходящих через узлы нарушителей, в сетях со статической топологией представлены на рисунке 37. Необходимо отметить, применение протокола маршрутизации BOLSR вместо протокола OLSR

позволило сократить количество маршрутов через узлы нарушителей в среднем в 1,53 раза, при этом при увеличении числа узлов нарушителей в сети количество маршрутов через эти узлы растёт медленнее в случае использования протокола маршрутизации BOLSR.

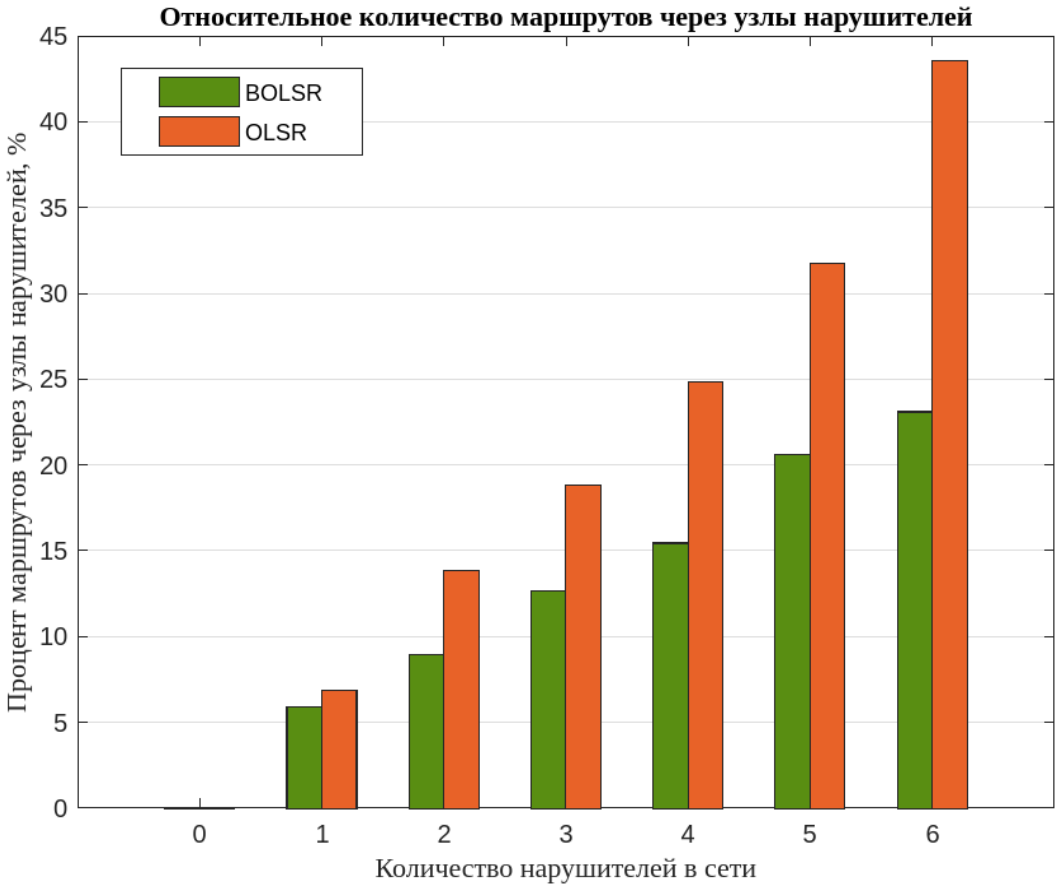

Рисунок 37. Относительное количество маршрутов через узлы нарушителей в сетях со статической топологией

Наличие мобильных узлов в сети приводит к изменениям топологии сети, а следовательно, и к изменению маршрутов, используемых для доставки пакетов. Новообразованные каналы связи, между узлами сети, нуждаются в определении их глобальной репутации, что требует определенных временных затрат. При отсутствии маршрута до узла назначения с ненулевым уровнем доверия маршруты, вычисляемые протоколами OLSR и BOLSR, совпадают. Этот факт может приводить к снижению эффективности

протокола BOLSR в сетях с высокой мобильностью узлов, что отчасти подтверждается результатами экспериментальных исследований.

Результаты экспериментальной оценки среднего относительного количества маршрутов, проходящих через узлы нарушителей, в сетях с динамической топологией, при использовании модели мобильности узлов Random Direction 2D, представлены на рисунке 38. Применение протокола маршрутизации BOLSR вместо протокола OLSR в сетях с динамической топологией позволило сократить количество маршрутов через узлы нарушителей в среднем в 1,27 раза.

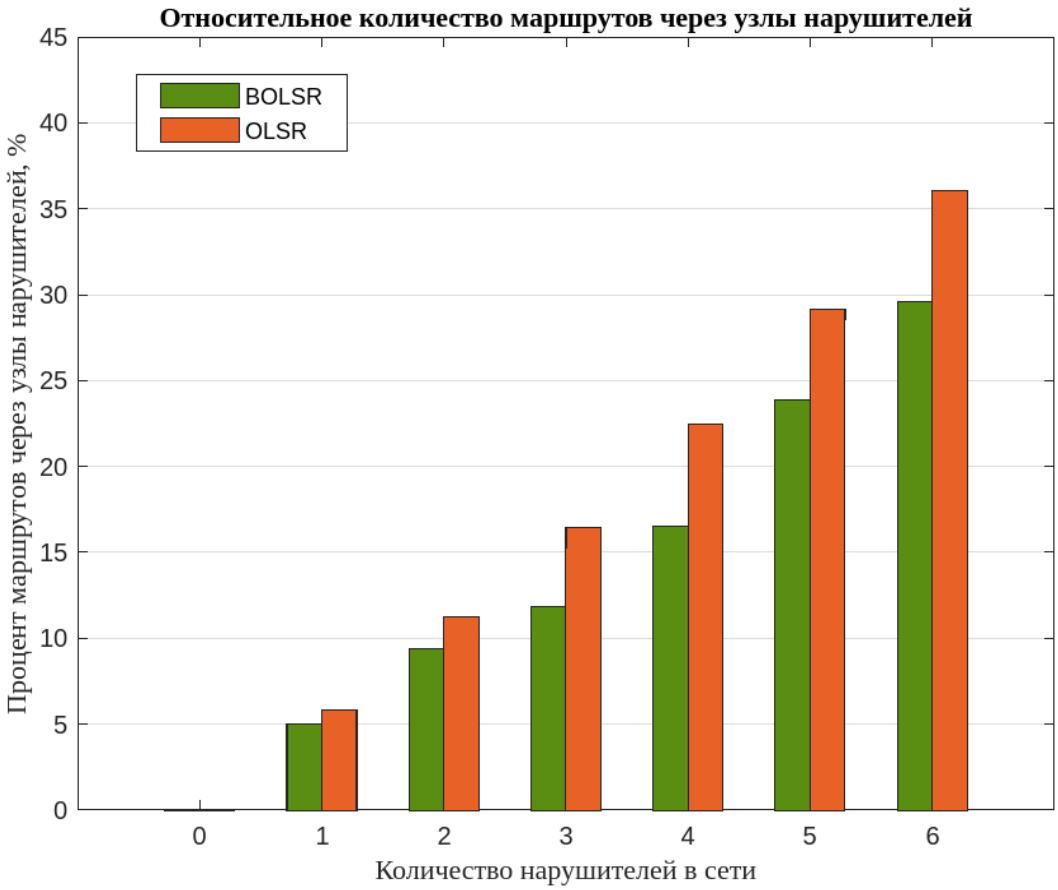

Рисунок 38. Относительное количество маршрутов через узлы нарушителей в сетях с динамической топологией

Для оценки возможного изменения производительности сетевого взаимодействия был выполнен сравнительный анализ средней длины всех маршрутов, вычисляемых при использовании протоколов маршрутизации

OLSR и BOLSR, в условиях воздействия на процесс маршрутизации различного количества вредоносных узлов. Результаты экспериментальной оценки средней длины маршрутов в сетях со статической топологией представлены на рисунке 39. В рамках заданного эксперимента средняя длина маршрутов при использовании протоколов маршрутизации BOLSR и OLSR находилась в диапазоне от 3 до 4 переходов. Можно отметить, 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.

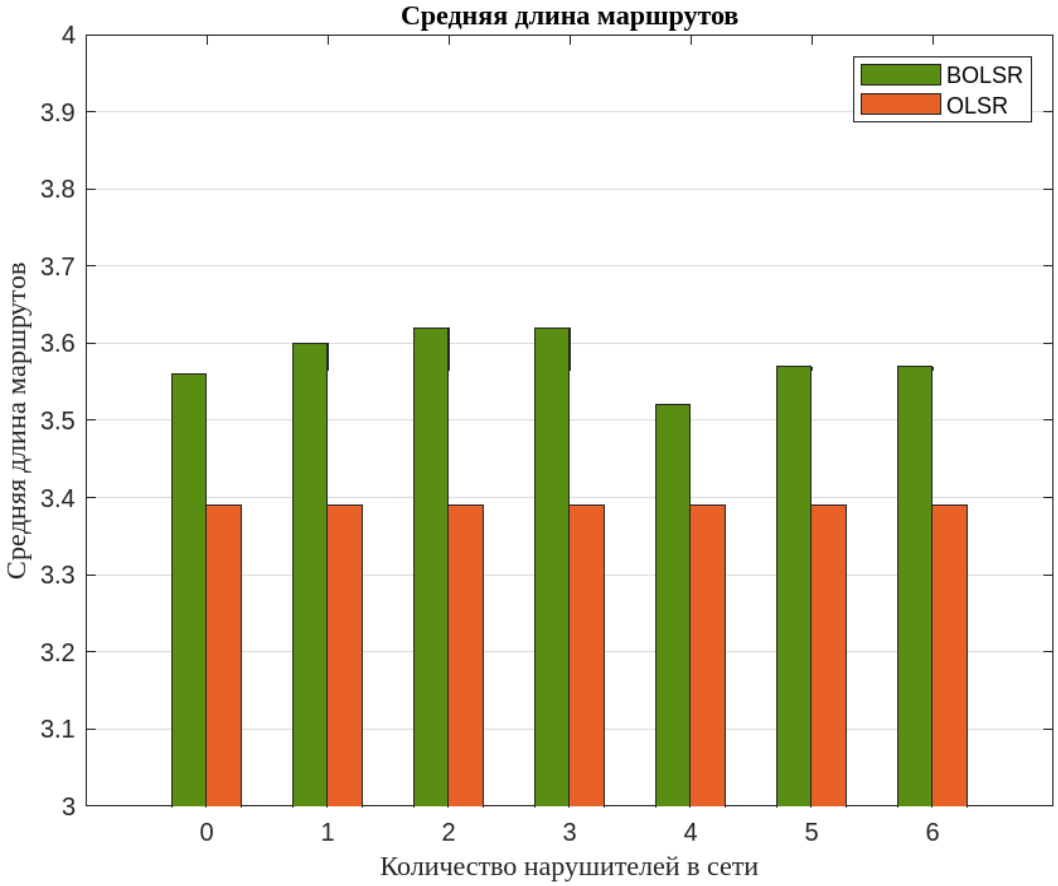

Рисунок 39. Средняя длина маршрутов в сетях со статической топологией

Результаты экспериментальной оценки средней длины маршрутов в сетях с динамической топологией при использовании модели мобильности узлов Random Direction 2D представлены на рисунке 40. Можно отметить, что при

использовании протокола маршрутизации BOLSR вместо протокола OLSR в сетях с динамической топологией в рамках заданного эксперимента средняя длина маршрутов практически не изменилась вне зависимости от числа узлов нарушителей (увеличение средней длины маршрутов не превысило 1%).

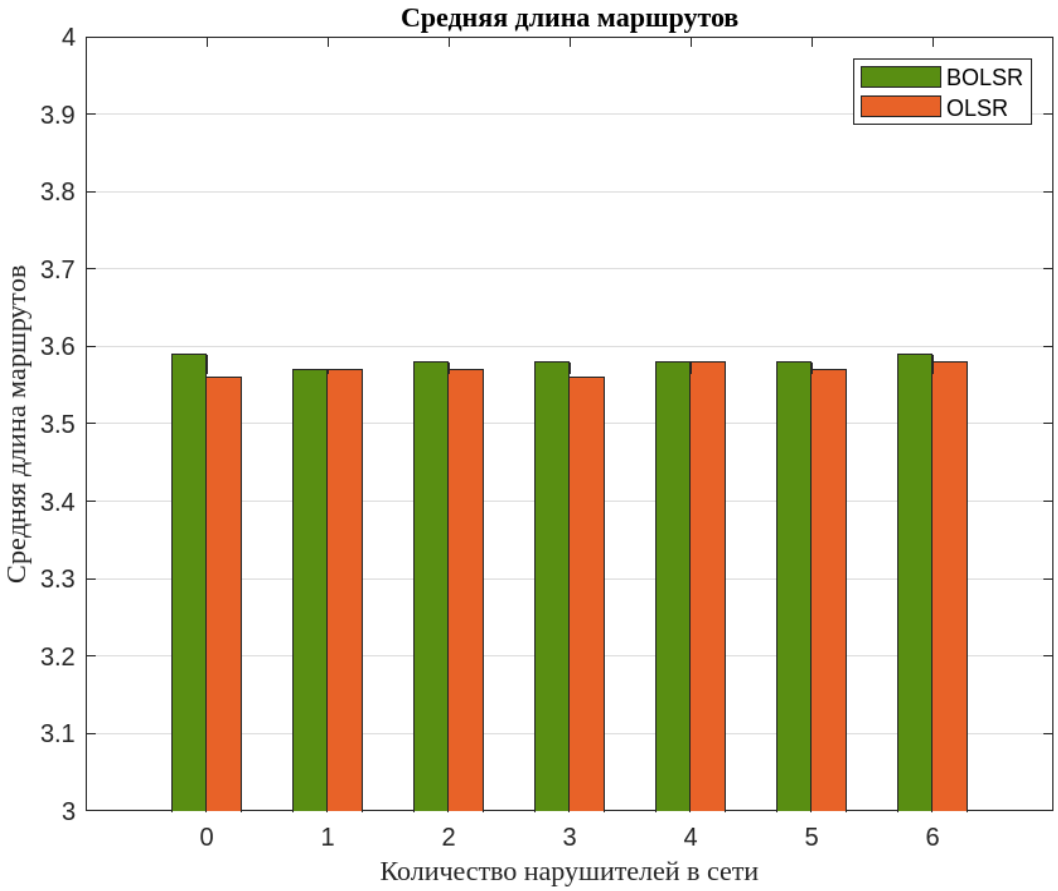

Рисунок 40. Средняя длина маршрутов в сетях с динамической топологией

Таким образом, в результате решения третьей задачи экспериментального исследования было установлено, что применение протокола маршрутизации BOLSR вместо протокола OLSR позволило существенно 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 незначительном увеличении средней длины маршрутов (увеличение составило до 7% в сетях со статической топологией и до 1% в сетях с динамической топологией).

Полученные результаты были подтверждены дальнейшими испытаниями программного модуля протокола маршрутизации BOLSR в динамически организуемых телекоммуникационных сетях на базе отдела радиотехнических систем российского системного интегратора ООО «Хайтэк», что позволило получить дополнительное практическое обоснование эффективности разработанного комплекса решений.

3.4 Выводы по главе

1. Для оценки уязвимости проактивной маршрутизации пакетов в беспроводных самоорганизующихся сетях и оценки эффективности обеспечения безопасности маршрутизации на основе комплекса предложенных решений была предложена модель и определена схема поведения узла нарушителя в самоорганизующейся сети. Согласно предложенной модели, вредоносный узел реализует угрозу полного нарушения доступности передаваемых данных посредством действий, препятствующих дальнейшей передаче поступающих пакетов по направлению к узлу назначения. Указанная модель была реализована в рамках сетевого симулятора NS-3.
2. Для экспериментального исследования разработанного комплекса решений по обеспечению безопасности маршрутизации пакетов в самоорганизующихся сетях был разработан сценарий эксперимента, сформулированы задачи, определены основные параметры и наблюдаемые показатели. Исследование было выполнено посредством имитационного моделирования сетевого взаимодействия в «транзитной сети» на базе сетевого симулятора NS-3 при использовании протоколов маршрутизации OLSR и BOLSR в условиях воздействия на процесс маршрутизации пакетов различного количества вредоносных узлов.
3. В результате решения первой задачи экспериментального исследования посредством анализа изменения коэффициента доставки пакетов в сетях со статической и динамической топологией было получено

экспериментальное обоснование адекватности предложенной и реализованной модели нарушителя в самоорганизующихся сетях. Было установлено, что с увеличением числа узлов нарушителей в сети коэффициент доставки пакетов непрерывно снижается.

4. В результате решения второй и третьей задачи экспериментального исследования было получено экспериментальное обоснование эффективности разработанного комплекса решений по обеспечению безопасности маршрутизации пакетов в самоорганизующихся сетях. В частности, было установлено, что применение протокола маршрутизации BOLSR вместо протокола OLSR позволило существенно 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), что, в свою очередь, позволило повысить значение коэффициента доставки пакетов в сетях со статической топологией в диапазоне от 15% (увеличение в 1,2 раза в сети с одним узлом нарушителя) до 42% (увеличение в 11,5 раз в сети с 6 узлами нарушителей) и в сетях с динамической топологией в диапазоне от 9% (увеличение в 1,12 раза в сети с одним узлом нарушителя) до 15% (увеличение в 3,5 раза в сети с 6 узлами нарушителей).
5. Также в результате решения третьей задачи экспериментального исследования было установлено, что применение разработанного комплекса решений по обеспечению безопасности маршрутизации пакетов не приводит к значительному увеличению средней длины вычисляемых маршрутов, это позволяет сохранить производительность сетевого взаимодействия. В частности, увеличение средней длины маршрутов при использовании протокола маршрутизации BOLSR вместо протокола OLSR составило до 7% в сетях со статической топологией и до 1% в сетях с динамической топологией.

Заключение

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

1. Выполнен анализ угроз безопасности маршрутизации в самоорганизующихся сетях. Отмечено, что криптографические методы не позволяют обеспечить защиту от внутренних узлов нарушителей, реализующих сетевые атаки типа «черная дыра» или «серая дыра» на доступность информации. Обоснована необходимость применения концепции доверия и кооперации узлов в самоорганизующейся сети в целях исключения ненадёжных узлов с низкой репутацией из процесса маршрутизации сетевых пакетов;
2. Выполнен анализ существующих моделей определения доверия и вычисления репутации. Проанализированы модели, основанные на суммировании и усреднении оценок, потоковые модели и модели на основе субъективной логики. 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 для обеспечения безопасности маршрутизации в самоорганизующихся сетях;
3. 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;

4. 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 $O(n^3)$;
5. 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 для дальнейшего экспериментального исследования эффективности предложенных моделей и алгоритма поиска наиболее безопасных маршрутов;
6. Выполнено экспериментальное обоснование эффективности комплекса разработанных решений в различных сценариях посредством имитационного моделирования маршрутизации в сетевом симуляторе NS-3. В частности, было установлено, что применение протокола маршрутизации BOLSR вместо протокола OLSR позволило существенно 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), что, в свою очередь, позволило повысить значение коэффициента доставки пакетов в сетях со статической топологией в диапазоне от 15% (увеличение в 1,2 раза в сети с одним узлом нарушителя) до 42% (увеличение в 11,5 раза в сети с 6 узлами нарушителей) и в сетях с динамической топологией в диапазоне от 9% (увеличение в 1,12 раза в сети с одним узлом нарушителя) до 15% (увеличение в 3,5 раза в сети с 6 узлами нарушителей). Также было отмечено, что применение разработанного комплекса решений по обеспечению безопасности маршрутизации пакетов не приводит к значительному увеличению средней длины вычисляемых маршрутов, что позволяет сохранить производительность сетевого взаимодействия.

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.

Выполнено внедрение предложенного комплекса решений при разработке дополнительного модуля для операционной системы UBLinux в ООО «Юбисофт», результаты внедрены и использовались при проведении испытаний в системном интеграторе ООО «ХайТэк». Результаты работы используются в учебном процессе кафедры «Комплексная защита информации» по направлениям подготовки 10.03.01 «Информационная безопасность» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» в Омском государственном техническом университете.

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 сокращений

BOLSR	– Boolean Optimized Link State Routing
OLSR	– Optimized Link State Routing
TCP/IP	– Transmission Control Protocol / Internet Protocol
MANET	– Mobile Ad hoc Network
VANET	– Vehicular Ad Hoc Network
FANET	– Flying Ad Hoc Network
GPS	– Global Positioning System
QoS	– Quality of Service
MPR	– MultiPoint Relay
TC	– Topology Control
MID	– Multiple Interface Declaration
RFC	– Request for Comments
RREQ	– Route Request
RREP	– Route Reply
DSR	– Dynamic source routing
AODV	– Ad hoc On-Demand Distance Vector
TAODV	– Trusted Ad hoc On-Demand Distance Vector
BP/P2P	– Belief Propagation / Peer-to-peer
EBSL	– Evidence Base Subjective Logic
NS-3	– Network Simulator 3
RM_MESSAGE	– Reputation Message
ECHO_MESSAGE	– Echo Message
CBR	– Constant Bit Rate
UDP	– User Datagram Protocol
PDR	– Packet Delivery Ratio

Библиографический список

1. Кучерявый, А. Е. Самоорганизующиеся сети и новые услуги / А. Е. Кучерявый // Электросвязь. – 2009. – №. 1. – С. 19–23.
2. Корячко, В. П. Корпоративные сети: технологии, протоколы, алгоритмы : моногр. / В. П. Корячко, Д. А. Перепелкин. – Москва : Горячая линия - Телеком, 2011. – 216 с. – ISBN 978-5-9912-0202-2.
3. Bekmezci, I. Flying Ad-Hoc Net-works (FANETs): A survey / I. Bekmezci, O. K. Sahingoz, S. Temel // Ad Hoc Networks. – 2013. – Vol. 11, no. 3. – P. 1254–1270.
4. Кучерявый, А. Е. Интернет вещей / А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 21–24.
5. Карманов, М. Л. Протокол маршрутизации для ad-hoc сетей / М. Л. Карманов // Вестник Южно-Уральского государственного университета. Сер. Компьютерные технологии, управление, радиоэлектроника. – 2009. – № 26 (159). – С. 47–51.
6. Johnson, D. B. DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks / D. B. Johnson, D. A. Maltz, J. Broch // Ad hoc networking. – 2001. – Vol. 5, no. 1. – P. 139–172.
7. Маршрутизация в беспроводных мобильных Ad hoc-сетях / В. Ю. Винокуров, А. В. Пуговкин, А. А. Пшенников [и др.] // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – № 2-1 (22). – С. 288–292.
8. Dijkstra, E. W. A note on two problems in connexion with graphs / E. W. Dijkstra. – DOI: 10.1007/BF01386390 // Numerische Mathematik. – 1959. – Vol. 1. – P. 269–271.
9. Clausen, T. Optimized Link State Routing Protocol (OLSR) / T. Clausen, P. Jacquet. – URL: http://www.ietf.org/rfc/rfc3626.txt (дата обращения: 14.04.2023).

10. RFC7181: The Optimized Link State Routing Protocol. Version 2 / T. Clausen, C. Dearlove, P. Jacquet, U. Herberg. – 2014. – URL: https://tools.ietf.org/html/rfc7181 (дата обращения: 14.04.2023).
11. Härri, J. OLSR and MPR: mutual dependences and performances / J. Härri, C. Bonnet, F. Filali // Challenges in Ad Hoc Networking: Fourth Annual Mediterranean Ad Hoc Networking Workshop, June 21–24 2005. – Île de Porquerolles, France : Springer US, 2006. – P. 67–71.
12. Chen, Jie. Comparison of optimized flooding techniques for mobile ad hoc networks / Chen Jie. – URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f2488f3d9a7a8fc2faa78dfd2438ba7107d41ac0 (дата обращения: 14.04.2023).
13. Toutouh, J. Intelligent OLSR Routing Protocol Optimization for VANETs / J. Toutouh, J. Garcia-Nieto, E. Alba // IEEE Transactions on Vehicular Technology. – 2012. – Vol. 61, no. 4. – P. 1884–1894.
14. Williams, B. Comparison of broadcasting techniques for mobile ad hoc networks / B. Williams, T. Camp // Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing - 2002. – New York, 2002. – P. 194–205.
15. Zhang, X. Performance of Routing Protocols in Very Large-Scale Mobile / X. Zhang, G. F. Riley // Proceedings of the 13th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (Atlanta, GA, 27–29 September 2005). – IEEE, 2005. – P. 115–124.
16. Performance analysis of OLSR Multipoint Relay flooding in two ad hoc wireless network models / P. Jacquet, A. Laouiti, P. Minet, L. Viennot. – URL: http://hal.inria.fr/docs/00/07/23/27/PDF/RR-4260.pdf (дата обращения: 14.04.2023).
17. Никонов, В. И. Проблемы безопасности протоколов маршрутизации в самоорганизующихся сетях беспроводных мобильных устройств / В. И.

Никонов, Г. С. Никонова // Техника радиосвязи. – 2017. – № 4 (35). – С. 23–34.

18. Бельфер, Р. А. Угрозы информационной безопасности в беспроводных саморегулирующихся сетях / Р. А. Бельфер // Вестник Московского государственного технического университета им. Н. Э. Баумана. Сер. Приборостроение. – 2011. – Спец. вып. Технические средства. – С. 116–124.
19. Ghaffari, A. Vulnerability and security of mobile ad hoc networks / A. Ghaffari // Proceedings of the 6th WSEAS international conference on simulation, modelling and optimization. – 2006. – P. 124–129. – URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1e4c557f9b97e95ac01c05c57cd8b660bfcc806c (дата обращения: 14.04.2023).
20. Гришечкина, Т. А. Анализ атак на сетевые протоколы в мобильных сенсорных сетях Ad hoc / Т. А. Гришечкина // Известия Южного Федерального университета. Технические науки. – 2012. – № 12 (137). – С. 68–74.
21. Система обнаружения атак в беспроводных сенсорных сетях промышленного Интернета вещей / В. И. Васильев, А. М. Вульфин, В. М. Катрак [и др.] // Труды Института системного анализа Российской академии наук. – 2019. – Т. 69, № 4. – С. 70–78.
22. Kayarkar, H. A survey on security issues in ad hoc routing protocols and their mitigation techniques / H. Kayarkar // International Journal Advanced Networking and Applications. – 2012. – Vol. 3, no. 5. – P. 1338–1351.
23. A survey of routing attacks in mobile ad hoc networks / B. Kannhavong, H. Nakayama, Y. Nemoto [et al.] // IEEE Wireless communications. – 2007. – Vol. 14, no. 5. – P. 85–91.
24. Tseng, F.-H. A survey of black hole attacks in wireless mobile ad hoc networks / F.-H. Tseng, L.-D. Chou, H.-C. Chao // Human-Centric Computing and Information sciences. – 2011. – Vol. 1, no. 1. – P. 1–16.

25. Black hole attack detection and ignoring in OLSR protocol / K. Saddiki, S. B. Hacene, M. Gilg, P. Lorenz // International Journal of Trust Management in Computing and Communications. – 2017. – Vol. 4, no. 1. – P. 75–93.
26. Shanmuganathan, V. A survey on gray hole attack in manet / V. Shanmuganathan, T. Anand // IRACST - International Journal of Computer Networks and Wireless Communications. – 2012. – Vol. 2, no. 6. – P. 647–650.
27. Gagandeep, A. Analysis of different security attacks in MANETs on protocol stack A-review / A. Gagandeep, P. Kumar // International Journal of Engineering and Advanced Technology. – 2012. –Vol. 1, no. 5. – P. 269–275.
28. Jathe, S. R. Indicators for detecting Sinkhole Attack in MANET / S. R. Jathe, D. M. Dakhane // International Journal of Emerging Technology and Advanced Engineering. – 2012. – Vol. 2, no. 1. – P. 369–372.
29. L'Hospital: Self-healing Secure Routing for Mobile Ad-hoc Networks. Technical Report CSD-TR040055 / J. Kong, X. Hong, J. S. Park [et al.] ; Dept. of Computer Science, UCLA, 2005. – P. 1–25.
30. Актуальные угрозы безопасности VANET/MANET-сетей / П. Д. Зегжда, Д. В. Иванов, Д. А. Москвин, Г. С. Кубрин // Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 2. – С. 41–47.
31. 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.
32. Обобщенная модель системы криптографически защищенных вычислений / Л. К. Бабенко, Ф. Б. Буртыка, О. Б. Макаревич, А. В. Трепачева // Известия Южного федерального университета. Технические науки. – 2015. – № 5 (166). – С. 77–88.

33. Варлатая, С. К. Криптографические методы и средства обеспечения информационной безопасности : учеб.-метод. комплекс / С. К. Варлатая, М. В. Шаханова. – Москва : Проспект, 2015. – 152 с. – ISBN 978-5-392-34300-3.
34. Zapata, M. G. Secure ad hoc on-demand distance vector routing / M. G. Zapata // ACM SIGMOBILE Mobile Computing and Communica-tions Review. – 2002. – Vol. 6, no. 3. – P. 106–107.
35. A secure routing protocol for ad hoc networks / K. Sanzgiri, B. Dahill, B. N. Levine [et al.] // 10th International Conference on Network Protocols (Paris, 12–15 November 2002). – IEEE, 2002. – P. 78–87.
36. Securing the OLSR protocol / C. Adjih, T. Clausen, P. Jacquet [et al.] // Proc. of Med-Hoc-Net. – Tunisia, IFIP, 2003. – P. 25–27.
37. Papadimitratos, P. Secure link state routing for mobile ad hoc networks / P. Papadimitratos, Z. J. Haas // Symposium on Applications and the Internet Workshops (Orlando, FL, 27–31 January 2003). – IEEE, 2003. – P. 379–383.
38. Cho, J. H. A survey on trust management for mobile ad hoc networks / J. H. Cho, A. Swami, R. Chen // Communications Surveys & Tutorials. – 2011. – Vol. 13, no. 4. – P. 562–583.
39. Michiardi, P. CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks / P. Michiardi, R. Molva // Advanced communications and multimedia security. – Portorož, Slovenia : Springer US, 2002. – P. 107–121.
40. Buchegger, S. Performance analysis of the CONFIDANT protocol / S. Buchegger, J. Y. Le Boudec // Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. – New York, 2002. – P. 226–236.
41. Nekkanti, R. K. Trust based adaptive on demand ad hoc routing protocol / R. K. Nekkanti, C. W. Lee // Proceedings of the 42nd annual Southeast regional conference. – New York, 2004. – P. 88–93.

42. Li, X. A trust model based routing protocol for secure ad hoc networks / X. Li, M. R. Lyu, J. Liu // Aerospace Conference Proceedings. – IEEE, 2004. – Vol. 2. – P. 1286–1295.
43. Airehrour, D. GradeTrust: A secure trust based routing protocol for MANETs / D. Airehrour, J. Gutierrez, S. K. Ray // International Telecommunication Networks and Applications Conference (ITNAC). – IEEE, 2015. – P. 65–70.
44. Adnane, A. Trust-based security for the OLSR routing protocol / A. Adnane, C. Bidan, R. T. de Sousa Júnior // Computer Communications. – 2013. – Vol. 36, no. 10-11. – P. 1159–1171.
45. Tan, S. Trust based routing mechanism for securing OSLR-based MANET / S. Tan, X. Li, Q. Dong // Computer Communications. – 2015. – Vol. 30. – P. 84–98.
46. Robert, J.-M. RBC-OLSR: Reputation-based clustering OLSR protocol for wireless ad hoc networks / J.-M. Robert, H. Otrok, A. Chriqi // Computer Communications. – 2012. – Vol. 35, no. 4. – P. 487–499.
47. Liu, Y. ActiveTrust: Secure and trustable routing in wireless sensor networks / Y. Liu, M. Dong, K. Ota, A. Liu // Transactions on Information Forensics and Security. – 2016. – Vol. 11, no. 9. – P. 2013–2027.
48. Васильев, В. И. Обнаружение аномалий в системах промышленного интернета вещей на основе искусственной иммунной системы / В. И. Васильев, В. Е. Гвоздев, Р. Р. Шамсутдинов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2021. – Т. 24, №. 4. – С. 40–45.
49. Naderi, O. A trust based routing protocol for mitigation of sinkhole attacks in wireless sensor networks / O. Naderi, M. Shahedi, S. M. Mazinani // International Journal of Information and Education Technology. – 2015. – Vol. 5, no. 7. – P. 520–526.
50. Poongodi, M. A novel intrusion detection system based on trust evaluation to defend against DDoS attack in MANET / M. Poongodi, S. Bose //

Arabian Journal for Science and Engineering. – 2015. – Vol. 40, no. 12. – P. 3583–3594.

51. Enhanced trust aware routing against worm-hole attacks in wireless sensor networks / R. W. Anwar, M. Bakhtiari, A. Zainal [et al.] // International Conference on Smart Sensors and Application (Kuala Lumpur, 26–28 May 2015). – IEEE, 2015. – P. 56–59.
52. Ishmanov, F. Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues / F. Ishmanov, Y. Bin Zikria // Journal of Sensors. – 2017. – Vol. 2017 (1). – P. 1–16.
53. Минин, А. А. Применение роевых алгоритмов для построения безопасных маршрутов в одноранговых сетях с динамической организацией / А. А. Минин, М. О. Калинин // Методы и технические средства обеспечения безопасности информации. – 2015. – № 24. – С. 28–29.
54. Грищенко, В. С. Метрики репутации: модели и алгоритмы построения открытых информационных сред : специальность 05.13.18. «Математическое моделирование, численные методы и комплексы программ» : дис. … канд. физ.-мат. наук / В. С. Грищенко. – Екатеринбург, 2007. – 124 с.
55. Абрамов, Е. С. Разработка системы управления уровнем доверия в мобильной кластерной беспроводной сенсорной сети / Е. С. Абрамов, Е. С. Басан, А. С. Басан // Известия ЮФУ. Технические науки. – 2015. – № 7 (168). – С. 41–52.
56. Басан, А. С. Методика оценки доверия в беспроводной сенсорной сети / А. С. Басан, Е. С. Басан // Безопасные информационные технологии (БИТ-2016) : сб. тр. Седьмой Всерос. науч.-техн. конф. (Москва, 16–17 нояб. 2016 г.) / под ред. В. А. Матвеева. – Москва : Изд-во Моск. гос. техн. ун-та им. Н. Э. Баумана, 2016. – С. 38–40.

57. Basan, A. Analysis of Ways to Secure Group Control for Autonomous Mobile Robots / A. Basan, E. Basan, O. Makarevich // ACM International Conference Proceeding Series : Security of Information and Networks : 10th International Conference (Jaipur, 13–15 окт. 2017). – Jaipur : Association for Computing Machinery, 2017. – P. 134–139.
58. Калинин, М. О. Выявление угроз информационной безопасности в сетях с динамической топологией за счет контроля активности узлов / М. О. Калинин, А. А. Минин // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 4. – С. 23–31.
59. Овасапян, Т. Д. Обеспечение безопасности wsn-сетей на основе модели доверия / Т. Д. Овасапян, Д. В. Иванов, Д. П. Зегжда // Региональная информатика и информационная безопасность (Санкт-Петербург, 1–3 нояб. 2017 г.). – Санкт-Петербург : С.-Петерб. общество информатики, вычислительной техники, систем связи и управления, 2017. – Т. 4. – С. 421–422.
60. Kamvar, S. D. The EigenTrust algorithm for reputation management in P2P networks / S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina // 12th international conference on World Wide Web. – New York, 2003. – P. 640–651.
61. Kurdi, H. A. HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems / H. A. Kurdi // Journal of King Saud University: Computer and Information Sciences. – 2015. – Vol. 27 (3). – P. 315–322.
62. A Framework for Packet-Droppers Mitigation in OLSR Wireless Community Networks / F. S. Proto, A. Detti, C. Pisa, G. Bianchi // International Conference on Communications (Kyoto, Japan, 5–9 June 2011). – IEEE, 2011. – P. 1–6.
63. Xiong, L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities / L. Xiong, L. Liu // IEEE Transactions on Knowledge and Data Engineering. – 2004. – Vol. 16, no. 7. – P. 843–857.

64. Ayday, E. BP-P2P: Belief propagation-based trust and reputation management for P2P networks / E. Ayday, F. Fekri // 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON) (Seoul, Korea, 18–21 June 2012). – IEEE, 2012. – P. 578–586.
65. Zhao, H. VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks / H. Zhao, X. Li // The Journal of Supercomputing, 2013. – Vol. 64 (3). – P. 805–829.
66. Tavakolifard, M. A probabilistic reputation algorithm for decentralized multi-agent environments / M. Tavakolifard, S. Knapskog // Electronic Notes in Theoretical Computer Science. – 2009. – Vol. 244. – P. 139–149.
67. An efficient and versatile approach to trust and reputation using hierarchical bayesian modeling / W. T. L. Teacy, M. Luck, A. Rogers, N. R. Jennings // Artificial Intelligence. – 2012. – Vol. 193. – P. 149–185.
68. Josang, A. Trust network analysis with subjective logic / A. Josang, R. Hayward, S. Pope // Conference Proceedings of the Twenty-Ninth Australasian Computer Science Conference (ACSW). – Australian Computer Society, 2006. – P. 85–94.
69. Škorić, B. Flow-based reputation with uncertainty: evidence-based logic / B. Škorić , S. J. de Hoogh, N. Zannone // International Journal of Information Security. – 2016. – Vol. 15 (4). – P. 381–402.
70. TrustyFeer: A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds / H. Kurdi, B. Alshayban, L. Altoaimy, S. Alsalamah // Wireless Communications and Mobile Computing. – 2018. – Vol. 2018. – P. 1–13.
71. Shafer, G. A mathematical theory of evidence / G. Shafer. – Princeton University Press, 1976. – Vol. 42. – 298 p.
72. Jsang, A. Subjective Logic - A Formalism for Reasoning Under Uncertainty / A. Jsang. – Springer, 2018. – 326 p.

73. Jøsang A., Gray E., Kinateder M. Simplification and analysis of transitive trust networks. Web Intelligence and Agent Systems: An International Journal, 2006, vol. 4(2), pp. 139–161.
74. Свидетельство о государственной регистрации программы для ЭВМ 2018666677. Генератор случайных геометрических булевозначных сетей / Г.А. Литвинов, Е.В. Щерба; правообладатель Омский гос. техн. ун-т. — № 2018666677; заявл. 07.12.2018; зарегистр. 19.12.2018; опубл. 19.12.2018, Бюл. № 1. — 1 с.
75. Riley G. F., Henderson T. R. The ns-3 network simulator // Modeling and tools for network simulation. – 2010. – С. 15-34.
76. 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.
77. 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.
78. Vilela, J. P. A feedback reputation mechanism to secure the optimized link state routing protocol / J. P.Vilela, J. Barros // Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm (Nice, France, 17–21 September 2007). – IEEE, 2007. – P. 294–303.
79. Математические модели исследования алгоритмов маршрутизации в сетях передачи данных / М. П. Березко, В. М. Вишневский, Е. В. Левнер, Е. В. Федотов // Информационные процессы. – 2001. – Т. 1, № 2. – С. 103–125.
80. Салий, В. Н. Оптимизация в булевозначных сетях / В. Н. Салий // Дискретная математика. – 2005. – Т. 17, № 1. – С. 141–146.
81. 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.

82. 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.
83. Suurballe, J. W. Disjoint paths in a network / J. W. Suurballe // Networks. – 1974. – Vol. 4, no. 2. – P. 125–145.
84. Bhandari, R. Survivable networks: algorithms for diverse routing / R. Bhandari. – Springer Science & Business Media, 1999. – 200 p.
85. Abe, J. O. k-Maximally disjoint path routing algorithms for SDN / J. O. Abe, H. A. Mantar, A. G. Yayimli // International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (Xi'an, China, 17–19 September 2015). – IEEE, 2015. – P. 499–508.
86. Doshi, M. Multi-constraint QoS disjoint multipath routing in SDN / M. Doshi, A. Kamdar // Moscow Workshop on Electronic and Networking Technologies (Moscow, 14–16 March 2018). – IEEE, 2018. – P. 1–5.
87. Берновски, М. М. Случайные графы, модели и генераторы безмасштабных графов / М. М. Берновски, Н. Н. Кузюрин // Труды Института системного программирования РАН. – 2012. – Т. 22. – С. 419–434.
88. GraphML Progress Report Structural Layer Proposal: Structural Layer Proposal / U. Brandes, M. Eiglsperger, I. Herman [et al.] // Graph Drawing : 9th International Symposium (Vienna, Austria, September 23–26, 2001). – Springer Berlin Heidelberg, 2002. – P. 501–512.
89. Кобелев, Н. Б. Имитационное моделирование : учеб. / Н. Б. Кобелев, В. В. Девятков, В. А. Половников. – Москва : Курс, 2020. – 352 с. – ISBN 978-5-907228-65-8.
90. Roy, R. R. Random walk mobility / R. R. Roy // Handbook of mobile ad hoc networks for mobility models. – Springer, 2011. – P. 35–63.

91. Hyytiä, E. Random waypoint mobility model in cellular networks / E. Hyytiä, J. Virtamo // Wireless Networks. – 2007. – Vol. 13, no. 2. – P. 177–188.
92. Gloss, B. A more realistic random direction mobility model / B. Gloss, M. Scharf, D. Neubauer // TD (05). – 2005. – Vol. 52. – P. 13–14.
93. Bai, F. IMPORTANT: A framework to systematically analyze the Impact of Mobility on Performance of RouTing protocols for Adhoc NeTworks / F. Bai, N. Sadagopan, A. Helmy // INFOCOM 2003. Twenty-second Annual Joint Conference of the Computer and Communications Societies (IEEE Cat. no. 03CH37428) (San Francisco, CA, 30 March – 3 April 2003). – IEEE, 2003. – Vol. 2. – P. 825–835.
94. Егошин, Н. С. Формирование модели нарушителя / Н. С. Егошин, А. А. Конев, А. А. Шелупанов // Безопасность информационных технологий. – 2017. – Т. 24, № 4. – С. 19–26.
95. 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.
96. Communication and networking of UAV-based systems: Classification and associated architectures / I. Jawhar, N. Mohamed, J. Al-Jaroodi [et al.] // Journal of Network and Computer Applications. – 2017. – Vol. 84. – P. 93–108.
97. Bujari, A. FANET application scenarios and mobility models / A. Bujari, C. E. Palazzi, D. Ronzani // Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications. – New York, 2017. – P. 43–46.
98. 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.

99. Properties of random direction models / P. Nain, D. Towsley, B. Liu, Z. Liu // Proceedings 24th Annual Joint Conference of the Computer and Communications Societies. – IEEE, 2005. – Vol. 3. – P. 1897–1907.

100. Route stability in MANETs under the random direction mobility model / G. Carofiglio, C. F. Chiasserini, M. Garetto, E. Leonardi // IEEE transactions on Mobile Computing. – 2009. – Vol. 8, no. 9. – P. 1167–1179.

101. Ammar, D. A new tool for generating realistic internet traffic in ns-3 / D. Ammar, T. Begin, I. Guerin-Lassous // 4th international ICST Conference on Simulation Tools and Techniques. – Publisher ICST, 2012. – URL: https://eudl.eu/pdf/10.4108/icst.simutools.2011.245548 (дата обращения: 14.04.2023).

102. Vasiliev, D. S. Simulation-based comparison of AODV, OLSR and HWMP protocols for flying Ad Hoc networks / D. S. Vasiliev, D. S. Meitis, A. Abilov // Internet of Things, Smart Spaces, and Next Generation Networks and Systems : 14th International Conference NEW2AN-2014, 7th Conference ruSMART-2014 (St. Petersburg, August 27–29 2014). – Springer International Publishing, 2014. – P. 245–252.

103. A performance comparison of multi-hop wireless ad hoc network routing protocols / J. Broch, D. A. Maltz, D. B. Johnson [et al.] // Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking. – Dallas, Texas, USA, 1998. – P. 85–97. – URL: https://dl.acm.org/doi/pdf/10.1145/288235.288256 (дата обращения: 14.04.2023).

104. Tsirigos, A. Analysis of multipath routing-Part I: The effect on the packet delivery ratio / A. Tsirigos, Z. J. Haas // IEEE Transactions on wireless communications. – 2004. – Vol. 3, no. 1. – P. 138–146.

105. Zhao, J. Understanding packet delivery performance in dense wireless sensor networks / J. Zhao, R. Govindan // Proceedings of the 1st

international conference on Embedded networked sensor systems. – New York, 2003. – P. 1–13.

106. 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.

107. 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.

108. 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.

Приложение А Фрагменты кода

Приложение А.1 Способ определения репутации каналов связи

```
void
RoutingProtocol::SendEcho(Ipv4Address dA, std::vector<Ipv4Address> path, uint16_t
direction)
{
    olsr::MessageHeader msg;

    msg.SetVTime (OLSR_TOP_HOLD_TIME);
    msg.SetOriginatorAddress (m_mainAddress);
    msg.SetTimeToLive (255);
    msg.SetHopCount (0);
    msg.SetMessageSequenceNumber (GetMessageSequenceNumber ());

    olsr::MessageHeader::Echo &echo = msg.GetEcho ();
    echo.destinationAddress = dA;
    echo.direction = direction;
    echo.path = path;

    QueueMessage (msg, JITTER);
}
```

```
void
RoutingProtocol::ProcessEcho(const olsr::MessageHeader &msg,
                             const Ipv4Address &senderIface)
{
    Time now = Simulator::Now ();
    const olsr::MessageHeader::Echo &echo = msg.GetEcho ();

    if(echo.destinationAddress == m_mainAddress){
        if(echo.direction == 0){
            SendEcho(msg.GetOriginatorAddress(), echo.path, 1);
        }else{
            EchoRequestsTable *EchoTableRow = m_state.FindIfaceEchoRequestsTables
(msg.GetOriginatorAddress());
            if(EchoTableRow != NULL) {
                if((now - EchoTableRow->SendTime).GetSeconds() >
m_lifeEchoInterval.GetSeconds()){
                    for (size_t n = 0; n < EchoTableRow->Path.size ()-1; n++)
                    {
                        SendRm(EchoTableRow->Path[n], EchoTableRow->Path[n+1],
0);
                    }
                    for (size_t n = EchoTableRow->Path.size ()-1; n > 0; n--)
                    {
                        SendRm(EchoTableRow->Path[n], EchoTableRow->Path[n-1],
0);
                    }
```

```
                    m_state.EraseIfaceEchoRequestsTables(msg.GetOriginatorAddress
());
                    return;
                }
                for (size_t n = 0; n < EchoTableRow->Path.size ()-1; n++)
                {
                    SendRm(EchoTableRow->Path[n], EchoTableRow->Path[n+1], 1);
                }
                for (size_t n = EchoTableRow->Path.size ()-1; n > 0; n--)
                {
                    SendRm(EchoTableRow->Path[n], EchoTableRow->Path[n-1], 1);
                }
                m_state.EraseIfaceEchoRequestsTables(msg.GetOriginatorAddress());
            }
        }
    }
}
```

Приложение А.2 Рассылка и обработка значений локальной репутации каналов связи

```
void
RoutingProtocol::SendRm (Ipv4Address dA, Ipv4Address lA, uint16_t flag)
{
  olsr::MessageHeader msg;

  msg.SetVTime (OLSR_TOP_HOLD_TIME);
  msg.SetOriginatorAddress (m_mainAddress);
  msg.SetTimeToLive (255);
  msg.SetHopCount (0);
  msg.SetMessageSequenceNumber (GetMessageSequenceNumber ());

  olsr::MessageHeader::Rm &rm = msg.GetRm ();
  rm.ansn = m_ansn;
  rm.flag = flag;
  rm.destAddress = dA;
  rm.lastAddress = lA;

  QueueMessage (msg, JITTER);
}
```

```
void
RoutingProtocol::ProcessRm (const olsr::MessageHeader &msg,
                            const Ipv4Address &senderIface)
{
    const olsr::MessageHeader::Rm &rm = msg.GetRm();
    Time now = Simulator::Now();

    const LinkTuple *link_tuple = m_state.FindSymLinkTuple(senderIface, now);
    if (link_tuple == NULL) {
```

```
        return;
    }

    if(rm.flag) {
        if (rm.lastAddress == m_mainAddress) {
            NeighborTuple *nb_tuple = m_state.FindNeighborTuple(rm.destAddress);
            if (nb_tuple != NULL) {
                if(SearchIndex(msg.GetOriginatorAddress(), nb_tuple-
>recommendationInterfaceAddresses) < 0) {
                    nb_tuple-
>recommendationInterfaceAddresses.push_back(msg.GetOriginatorAddress());
                    return;
                }
            }
        }

        TwoHopNeighborTuple *nb2hop_tuple =
m_state.FindTwoHopNeighborTuple(rm.lastAddress, rm.destAddress);
        if (nb2hop_tuple != NULL) {
            if(SearchIndex(msg.GetOriginatorAddress(), nb2hop_tuple-
>recommendationInterfaceAddresses) < 0) {
                nb2hop_tuple-
>recommendationInterfaceAddresses.push_back(msg.GetOriginatorAddress());
            }
        }

        TopologyTuple *topologyTuple = m_state.FindTopologyTuple(rm.destAddress,
rm.lastAddress);
        if (topologyTuple != NULL) {
            if(SearchIndex(msg.GetOriginatorAddress(), topologyTuple-
>recommendationInterfaceAddresses) < 0) {
                topologyTuple-
>recommendationInterfaceAddresses.push_back(msg.GetOriginatorAddress());
            }
        }
    }else{
        if (rm.lastAddress == m_mainAddress) {
            NeighborTuple *nb_tuple = m_state.FindNeighborTuple(rm.destAddress);
            if (nb_tuple != NULL) {
                if(SearchIndex(msg.GetOriginatorAddress(), nb_tuple-
>recommendationInterfaceAddresses) >= 0) {
                    nb_tuple->recommendationInterfaceAddresses.erase (nb_tuple-
>recommendationInterfaceAddresses.begin() +
                    SearchIndex(msg.GetOriginatorAddress(), nb_tuple-
>recommendationInterfaceAddresses));
                }
            }
        }

        TwoHopNeighborTuple *nb2hop_tuple =
m_state.FindTwoHopNeighborTuple(rm.lastAddress, rm.destAddress);
```

```
        if (nb2hop_tuple != NULL) {
            if(SearchIndex(msg.GetOriginatorAddress(), nb2hop_tuple-
>recommendationInterfaceAddresses) >= 0) {
                nb2hop_tuple->recommendationInterfaceAddresses.erase
(nb2hop_tuple->recommendationInterfaceAddresses.begin() +
                SearchIndex(msg.GetOriginatorAddress(), nb2hop_tuple-
>recommendationInterfaceAddresses));
            }
        }

        TopologyTuple *topologyTuple = m_state.FindTopologyTuple(rm.destAddress,
rm.lastAddress);
        if (topologyTuple != NULL) {
            if(SearchIndex(msg.GetOriginatorAddress(), topologyTuple-
>recommendationInterfaceAddresses) >= 0) {
                topologyTuple->recommendationInterfaceAddresses.erase
(topologyTuple->recommendationInterfaceAddresses.begin() +
                SearchIndex(msg.GetOriginatorAddress(), topologyTuple-
>recommendationInterfaceAddresses));
            }
        }
    }
}
```

Приложение А.3 Вычисление наиболее безопасных маршрутов

```
std::vector<ExtraDataRouting::Length>
RoutingProtocol::CalculateExtraDataRouting ()
{
    bool checkAdd;
    int count_atom;
    int count_packet_atom;
    int count_vector_atom;
    bool packet_in_vector;
    bool vector_in_packet;
    std::vector<ExtraDataRouting::Length> LzRemoved;
    std::vector<Ipv4Address> CalcUpath;
    AllLinks &viewlink = m_state.GetAllLinks();
    ExtraDataRouting extrdata;
    extrdata.Az.push_back(m_mainAddress);
    while (extrdata.Az.size() > 0){
        extrdata.A.clear();
        for (std::vector<Ipv4Address>::const_iterator it = extrdata.Az.begin ();
it != extrdata.Az.end (); it++){ extrdata.A.push_back(*it); }
        extrdata.L.clear();
        for (std::vector<ExtraDataRouting::Length>::const_iterator it =
extrdata.Lz.begin (); it != extrdata.Lz.end (); it++){
            extrdata.L.push_back(*it);
        }
        extrdata.Az.clear();
```

```
        for (std::vector<Ipv4Address>::const_iterator newip = extrdata.A.begin
(); newip != extrdata.A.end (); newip++){
            for (AllLinks::iterator it = viewlink.begin (); it != viewlink.end
(); it++){
                checkAdd = false;
                AllLink const &allip = *it;
                if(allip.From == *newip) {
                    if(m_mainAddress == *newip){
                        ExtraDataRouting::Length LtoPush;
                        LtoPush.number = allip.To;
                        LtoPush.nextHop = allip.To;
                        for (std::vector<Ipv4Address>::const_iterator Lip =
allip.Recomend.begin(); Lip != allip.Recomend.end(); Lip++) {
                            LtoPush.U.push_back(*Lip);
                        }
                        LtoPush.Up.push_back(allip.From);
                        if(LtoPush.U.size() && m_mainAddress != allip.To) {
                            extrdata.Lz.push_back(LtoPush);
                            checkAdd = true;
                        }
                    }
                    for (std::vector<ExtraDataRouting::Length>::iterator
extrdata_item = extrdata.L.begin (); extrdata_item != extrdata.L.end ();
                    extrdata_item++){
                        if(*newip == extrdata_item->number){
                            CalcUpath.clear();
                            for (std::vector<Ipv4Address>::const_iterator Lip =
allip.Recomend.begin(); Lip != allip.Recomend.end(); Lip++) {
                                if(SearchIndex(*Lip, extrdata_item->U) >= 0) {
                                    CalcUpath.push_back(*Lip);
                                }
                            }
                            packet_in_vector = false;
                            vector_in_packet = false;
                            count_packet_atom = CalcUpath.size();
                            LzRemoved.clear();
                            for (std::vector<ExtraDataRouting::Length>::iterator
vector_item = extrdata.Lz.begin ();
                            vector_item != extrdata.Lz.end (); vector_item++){
                                if(vector_item->number == allip.To) {
                                    count_atom = 0;
                                    count_vector_atom = vector_item->U.size();
                                    for (std::vector<Ipv4Address>::const_iterator
atom = CalcUpath.begin(); atom != CalcUpath.end(); atom++) {
                                        if(SearchIndex(*atom, vector_item->U) >=
0) {

                                            count_atom++;
                                        }
                                    }
                                    if(count_packet_atom == count_atom){
                                        packet_in_vector = true;
```

```
                                    }
                                    if(count_vector_atom == count_atom){
                                        vector_in_packet = true;
                                    }
                                    if(count_vector_atom != count_atom){
                                        LzRemoved.push_back(*vector_item);
                                    }
                                }else{
                                    LzRemoved.push_back(*vector_item);
                                }
                            }
                            ExtraDataRouting::Length LtoPush;
                            LtoPush.number = allip.To;
                            LtoPush.nextHop = extrdata_item->nextHop;
                            for (std::vector<Ipv4Address>::const_iterator Lip =
CalcUpath.begin(); Lip != CalcUpath.end(); Lip++) {
                                LtoPush.U.push_back(*Lip);
                            }
                            for (std::vector<Ipv4Address>::const_iterator Lip =
extrdata_item->Up.begin(); Lip != extrdata_item->Up.end(); Lip++) {
                                LtoPush.Up.push_back(*Lip);
                            }
                            LtoPush.Up.push_back(allip.From);
                            if(LtoPush.U.size() && m_mainAddress != allip.To &&
!packet_in_vector) {
                                if(vector_in_packet && extrdata.Lz.size() !=
LzRemoved.size()
                                ){checkAdd = true;}
                                if(vector_in_packet && extrdata.Lz.size() !=
LzRemoved.size()){
                                    extrdata.Lz.clear();
                                    for
(std::vector<ExtraDataRouting::Length>::const_iterator it = LzRemoved.begin ();
it != LzRemoved.end (); it++){
                                        extrdata.Lz.push_back(*it);
                                    }
                                }
                                extrdata.Lz.push_back(LtoPush);
                                checkAdd = true;
                            }
                        }
                    }
                }
                if(checkAdd == true and SearchIndex(allip.To, extrdata.Az) < 0){
                    extrdata.Az.push_back(allip.To);
                }
            }
        }
    }

    std::vector<ExtraDataRouting::Length> BestResultingRoutes;
```

```
    LzRemoved.clear();
    int32_t destinationFind;
    for (std::vector<ExtraDataRouting::Length>::iterator extrdata_item =
extrdata.L.begin (); extrdata_item != extrdata.L.end (); extrdata_item++){
        destinationFind = 0;
        LzRemoved.clear();
        for (std::vector<ExtraDataRouting::Length>::iterator best_item =
BestResultingRoutes.begin (); best_item != BestResultingRoutes.end ();
best_item++){
            if(extrdata_item->number == best_item->number){
                destinationFind = 1;
                if(extrdata_item->U.size() > best_item->U.size()){
                    LzRemoved.clear();
                    for (std::vector<ExtraDataRouting::Length>::iterator item =
BestResultingRoutes.begin (); item != BestResultingRoutes.end (); item++){
                        if(extrdata_item->number != item->number){
                            LzRemoved.push_back(*item);
                        }
                    }
                    destinationFind = 0;
                }
                if(extrdata_item->U.size() <= best_item->U.size() &&
extrdata_item->Up.size() < best_item->Up.size()){
                    LzRemoved.clear();
                    for (std::vector<ExtraDataRouting::Length>::iterator item =
BestResultingRoutes.begin (); item != BestResultingRoutes.end (); item++){
                        if(extrdata_item->number != item->number){
                            LzRemoved.push_back(*item);
                        }
                    }
                    destinationFind = 0;
                }
            }
        }
        if(destinationFind == 0){
            if(LzRemoved.size() > 0) {
                BestResultingRoutes.clear();
                for (std::vector<ExtraDataRouting::Length>::iterator item =
LzRemoved.begin();
                     item != LzRemoved.end(); item++) {
                    BestResultingRoutes.push_back(*item);
                }
            }
            BestResultingRoutes.push_back(*extrdata_item);
        }
    }
    return BestResultingRoutes;
}
```

Приложение Б Акты внедрения

УТВЕРЖДАЮ
Заместитель технического
директора по специальным
системам
ООО «ХайТэк»
_____ А.А. Кирсанов
«30» 03 2023 г

АКТ
об использовании результатов диссертационной работы
Литвинова Георгия Александровича
на тему «Обеспечение безопасности маршрутизации в самоорганизующихся сетях на основе репутационной модели»,
представленной на соискание ученой степени кандидата технических наук
по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

Разработанные в рамках диссертационной работы Литвинова Г. А. на тему «Обеспечение безопасности маршрутизации в самоорганизующихся сетях на основе репутационной модели», представленной на соискание ученой степени кандидата технических наук, программная реализация модели доверия на основе репутации узлов и алгоритма поиска наиболее безопасного маршрута, имитационные модели типовых сценариев применения для самоорганизующихся сетей различных типов, а также программа для автоматизации процесса проведения имитационного моделирования и анализа полученных результатов были использованы при выполнении научно-исследовательской работы. Были получены следующие результаты:

1. Сформирована и апробирована методика проведения испытаний и оценки эффективности предложенных моделей и алгоритмов в динамически организуемых телекоммуникационных сетях различных типов.

2. Разработано программное обеспечение для организации проактивной маршрутизации сетевых пакетов в динамически организуемых телекоммуникационных сетях различных типов.

3. Использование разработанной модели доверия на основе репутации узлов и алгоритма поиска наиболее безопасного маршрута в тестовых

самоорганизующихся сетях с различной мобильностью и плотностью узлов, а также с различным количеством вредоносных и легитимных узлов в целом позволило увеличить коэффициент доставленных пакетов по сравнению с оригинальным протоколом маршрутизации OLSR на значение от 10% до 70% в зависимости от количества нарушителей в сети. При этом количество маршрутов, определяемых через узлы нарушителей, в рамках исследуемых сетевых топологий при использовании разработанного программного обеспечения сократилось в среднем в 1,58 раза по сравнению с протоколом маршрутизации OLSR.

Главный эксперт отдела разработки специальных систем  Е.Ф. Лобанов

УТВЕРЖДАЮ
Генеральный директор
ООО «Юбисофт»
_____ Д.А. Разумов
«14» 03 2023 г

АКТ

о внедрении результатов диссертационной работы Литвинова Г.А.
на тему «Обеспечение безопасности маршрутизации в самоорганизующихся сетях на основе репутационной модели»,
представленной на соискание ученой степени кандидата технических наук
по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

Настоящий Акт составлен в том, что результаты диссертационной работы Литвинова Георгия Александровича, а именно:

- модель оценки репутации каналов связи и метрика безопасности маршрутов, позволяющая учитывать их репутацию;
- алгоритм поиска наиболее безопасных маршрутов до всех узлов сети;
- модель обеспечения безопасности проактивной маршрутизации, основанная на имплементации, разработанной репутационной модели и алгоритма поиска наиболее безопасных маршрутов для существующего протокола маршрутизации OLSR;

использовались ООО «Юбисофт» при создании дополнительного модуля динамической маршрутизации для операционной системы UBLinux.

Председатель комиссии: Д.А. Разумов

Члены комиссии: О.Б. Васильев
А.К. Павлушина
Д.А. Разумов
Д.В. Буцик

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОМСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

от «16» 03 2023 г.
г. Омск
Об использовании научных исследований и разработок в учебном процессе

УТВЕРЖДАЮ
Проректор по образовательной деятельности
А.С. Полынский
«16» 03 2023 г.

АКТ ВНЕДРЕНИЯ

Основание: научные исследования, выполненные старшим преподавателем кафедры «Комплексная защита информации» Литвиновым Г.А.

Составлен комиссией в составе:

Председатель комиссии	–	П.И. Пузырев, декан РТФ;
Член комиссии	–	П.С. Ложников, зав. кафедрой КЗИ;
Член комиссии	–	А.Е. Самотуга, доцент кафедры КЗИ.

1. Теоретические разработки Литвинова Г.А., опубликованные в статьях:

Щерба Е. В., Никонов В. И., Литвинов Г. А. Обеспечение безопасности протоколов маршрутизации для телекоммуникационных сетей с динамической топологией //Доклады Томского государственного университета систем управления и радиоэлектроники. – 2018. – Т. 21. – №. 3. – С. 19-29.

Литвинов Г. А., Щерба Е. В. Применение моделей доверия и репутации для обеспечения безопасности маршрутизации в динамически организуемых сетях //Вестник УрФО. Безопасность в информационной сфере. – 2021. – №. 3 (41). – С. 12-23.

Litvinov G., Shcherba E. Implementation of the Reputation Model for Secure Routing Based on the OLSR Protocol //2021 International Conference Engineering and Telecommunication (En&T). – IEEE, 2021. – С. 1-4.

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.

используются в следующих учебных дисциплинах кафедры КЗИ:

– «Системы и сети передачи данных»;

– «Сетевое администрирование»;

– «Безопасность вычислительных сетей»;

а также при руководстве курсовым и дипломным проектированием и научно-исследовательской деятельности студентов.

2. В основе учебно-методических разработок, используемых в перечисленных учебных дисциплинах кафедры КЗИ, лежат следующие научные результаты исследований Литвинова Г.А.:

– способ определения репутации каналов связи в самоорганизующихся сетях с динамической топологией посредством отправки тестовых пакетов;

– репутационная модель для вычисления значений глобальной репутации каналов связи посредством агрегирования локальных значений, полученных от других узлов сети;

– алгоритм поиска наиболее безопасных маршрутов до всех узлов сети, позволяющий найти маршруты с наилучшей репутацией;

– имитационная модель протокола маршрутизации BOLSR, основанная на имплементации, разработанной репутационной модели и алгоритма поиска наиболее безопасных маршрутов для существующего протокола маршрутизации OLSR.

Председатель комиссии _____ / П.И. Пузырев

Члены комиссии _____ / П.С. Ложников

_____ / А.Е. Самотуга

Приложение В Свидетельства о регистрации программ для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018666677

«Генератор случайных геометрических булевозначных сетей»

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный технический университет» (RU)***

Авторы: ***Литвинов Георгий Александрович (RU),***
Щерба Евгений Викторович (RU)

Заявка № **2018664100**
Дата поступления **07 декабря 2018 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***19 декабря 2018 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019666281

Моделирование атаки с изменением служебных сообщений протокола маршрутизации OLSR

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования "Омский государственный технический университет" (RU)***

Авторы: ***Литвинов Георгий Александрович (RU),***
Щерба Евгений Викторович (RU)

Заявка № **2019664929**
Дата поступления **22 ноября 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***06 декабря 2019 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2021661846

Репутационный модуль поиска наиболее безопасных маршрутов для протокола маршрутизации OLSR

Правообладатель: ***федеральное государственное бюджетное образовательное учреждение высшего образования "Омский государственный технический университет" (RU)***

Авторы: ***Литвинов Георгий Александрович (RU), Щерба Евгений Викторович (RU)***

Заявка № **2021661027**
Дата поступления **14 июля 2021 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***16 июля 2021 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0x02A5CFBC00B1ACF59A40A2F08D92E9A118
Владелец **Ивлиев Григорий Петрович**
Действителен с 15.01.2021 по 15.01.2035

Г.П. Ивлиев