ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное образовательное бюджетное учреждение высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

На правах рукописи

Богданов Игорь Александрович

ИССЛЕДОВАНИЕ ПОТОКОВ ЛОЖНЫХ СОБЫТИЙ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

05.12.13 – Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
доктор технических наук, профессор
Кучерявый Андрей Евгеньевич

Санкт Петербург – 2016

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Развитие сетей связи в настоящее время и в долгосрочной перспективе происходит на основе концепции Интернета Вещей. Эта концепция основана на идее о том, что наиболее существенную часть клиентской базы сетей связи будут составлять вещи. Внедрение концепции Интернета Вещей предполагает коренные изменения в архитектуре сетей связи, услугах, сетевой безопасности и т.д. Сети связи из инфраструктурных превращаются в самоорганизующиеся, появляются услуги машина-машина, предоставляемые без участия человека, в области сетевой безопасности наряду с традиционными видами атак и вторжений появляются новые, обусловленные новизной архитектуры и услуг сетей. Эти качественные изменения являются следствием количественных изменений клиентской базы сетей связи. Существенно большее число вещей приводит к созданию в перспективе триллионных сетей связи, а прогнозы развития предполагают появление до 50 триллионов вещей, являющихся элементами сетей связи.

Технологической базой для внедрения концепции Интернета Вещей в настоящее время являются беспроводные сенсорные сети, имеющие также название всепроникающих сенсорных сетей за счет предполагаемого повсеместного использования сенсорных узлов. Исследования беспроводных сенсорных сетей являются одним из наиболее широко распространенных направлений научной деятельности в области систем, сетей и устройств телекоммуникаций во всем мире, начиная с первого десятилетия 21 века. Разработка алгоритмов выбора головного узла кластера, исследования связности и надежности сенсорных сетей, сенсорных сетей с мобильными узлами представляют собой известные примеры этой деятельности.

Существенную роль в исследованиях по сенсорным сетям играют, естественно, и вопросы информационной безопасности. Наряду с исследованиями традиционных для сетей связи атак и вторжений, в последние годы после выхода

рекомендации Сектора Стандартизации Международного Союза Электросвязи (МСЭ-Т) X.1311“Структура безопасности для всепроникающих сенсорных сетей” появились и работы, связанные с атаками на энергетическую систему сенсорных сетей, а также с их клонированием. Отметим, что МСЭ-Т рассматривает проблемы так называемой сетевой безопасности, определяемой на участке от пользовательского интерфейса до пользовательского интерфейса, что исследуется также и в настоящей диссертации.

Беспроводные сенсорные сети в качестве своих приложений достаточно часто используют слежение за целью и защиту территорий от вторжений. В работе предлагается и исследуется новый вид вторжений в беспроводные сенсорные сети, основанный на создании потоков ложных событий. С учетом изложенного тема диссертации представляется актуальной.

Степень разработанности темы. В области Интернета Вещей и беспроводных сенсорных сетей известны основополагающие работы отечественных и зарубежных ученых Б.С.Гольдштейна, Р.А.Бельфера, А.Е.Кучерявого, Е.А.Кучерявого, Д.А.Молчанова, В.А.Мочалова, А.В.Рослякова, А.П.Пшеничникова, К.Е.Самуйлова, В.К.Сарьяна, В.Н.Туруты, М.А.Шнепса, I.Akyildiz, W.Heinzelman, J.V.Nickerson, S.Olariu, T.Bhattassali, R.Chaki, S.Sanyal. Тема диссертации относится к исследованиям вторжений в беспроводные сенсорные сети, имеющих своей целью уменьшение жизненного цикла сенсорной сети. В этой связи можно отметить работы T.Bhattassali, R.Chaki, S.Sanyal, в которых уменьшение жизненного цикла сенсорной сети достигалось за счет лишения сенсорных узлов спящего режима. В диссертации предлагается и исследуется новый вид вторжений в беспроводные сенсорные сети, основанный на создании потоков ложных событий, воздействующих на любые сенсорные узлы сети независимо от их состояния в конкретный момент времени.

Цель работы и задачи исследования. Целью диссертации является разработка и исследование моделей вторжений в беспроводные сенсорные сети на основе потоков ложных событий и метода защиты от этих вторжений.

Для достижения поставленной цели в диссертационной работе последовательно решаются следующие задачи:

- анализ концепции Интернета Вещей, принципов построения самоорганизующихся сетей и особенностей построения беспроводных сенсорных сетей;

- анализ видов вторжений в сетях связи и особенностей вторжений для беспроводных сенсорных сетей;

- разработка модели вторжения в сенсорные сети потоков ложных событий;

- исследование воздействия на жизненный цикл беспроводной сенсорной сети пуассоновского и детерминированного потоков ложных событий;

- разработка метода защиты беспроводной сенсорной сети от потоков ложных событий путем придания мобильности сенсорным узлам;

- определение структурных характеристик беспроводной сенсорной сети для выявления ложных событий с заданной вероятностью обнаружения;

- разработка структурного метода защиты беспроводной сенсорной сети от потоков ложных событий.

Научная новизна. В диссертации получены следующие основные новые научные результаты:

- разработана модель вторжения в беспроводную сенсорную сеть с целью уменьшения ее жизненного цикла, отличающаяся от известных тем, что для достижения данной цели используются потоки ложных событий,

- в отличие от известных результатов установлено, что длительность жизненного цикла беспроводной сенсорной сети зависит от вида потока ложных событий,

- разработан метод защиты беспроводных сенсорных сетей, отличающийся тем, что в условиях вторжения потоков ложных событий для увеличения длительности жизненного цикла сети сенсорным узлам придается мобильность со скоростью 2 м/с,

- разработан метод защиты беспроводных сенсорных сетей, отличающийся тем, что в условиях вторжения потоков ложных событий модифицируются структурные характеристики сенсорного поля путем изменении распределения плотности сенсорных узлов по сравнению с равномерной.

Теоретическая и практическая значимость исследования. Теоретическая значимость работы состоит в разработке новой модели вторжения в беспроводные сенсорные сети на основе потоков ложных событий и структурного метода защиты беспроводных сенсорных сетей от этих потоков. Важным для теории является также доказательство зависимости уровня воздействия на сенсорную сеть от вида потока и скорости перемещения сенсорных узлов, а также существования оптимального соотношения плотностей узлов, обеспечивающего максимальное время жизни сенсорной сети.

Практическая ценность работы состоит в обеспечении возможности при планировании сети заранее определить ее характеристики так, чтобы беспроводная сенсорная сеть была наиболее устойчива к воздействиям в виде потоков ложных событий. Для планирования беспроводных сенсорных сетей могут быть использованы численные значения оптимальной плотности распределения сенсорных узлов на плоскости, длительности жизненного цикла беспроводной сенсорной сети в зависимости от вида потока ложных событий и скорости перемещения сенсорных узлов.

Результаты работы использованы в ОКР акционерного общества “Московский ордена Трудового Красного Знамени научно-исследовательский радиотехнический институт” (АО “МНИРТИ”), а также в учебном процессе Военно-космической Академии им. А.Ф. Можайского и Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича.

Методология и методы исследования. Методология исследования основана на обобщении передового опыта и анализе особенностей беспроводных сенсорных сетей. В качестве методов исследования использовались методы

теории телетрафика, теории вероятностей, теории оптимизации. Для моделирования использовался пакет программ C#.NET.

Предмет исследования. Предметом исследования являются беспроводные сенсорные сети.

Объект исследования. Объектом исследования являются вторжения в беспроводные сети в виде потоков ложных событий.

Положения, выносимые на защиту.

- модель вторжения в беспроводную сенсорную сеть на основе потоков ложных событий,
- зависимость длительности жизненного цикла беспроводной сенсорной сети от вида потока ложных событий,
- метод защиты беспроводной сенсорной сети от потоков ложных событий, состоящий в придании сенсорным узлам мобильности,
- метод защиты беспроводных сенсорных сетей от потоков ложных событий, состоящий в изменении распределения плотности сенсорных узлов по сравнению с равномерной.

Степень достоверности и апробация результатов. Достоверность результатов диссертационной работы подтверждается корректным применением математического аппарата, результатами имитационного моделирования, а также достаточно широким спектром публикаций и выступлений на международных и российских конференциях.

Основные результаты работы докладывались и обсуждались на 13й Международной конференции «Internet of Things, Smart Spaces, and Next Generation Networking NEW2AN» (Санкт-Петербург, август 2013 г.), на 68-й конференции СПбНТОРЭС им. А. С. Попова. (Санкт-Петербург, апрель 2013 г.), 2, 4 и 5-ой Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» СПбГУТ (Санкт-Петербург, февраль 2013, март 2015, апрель 2016), Международной конференции “Интернет Вещей” (Санкт-Петербург, ноябрь 2014), а также на заседаниях кафедры Сетей связи и передачи данных СПбГУТ.

Публикации. Основные результаты диссертации опубликованы в 9 работах, из них 3 статьи в журналах из перечня ВАК Министерства образования и науки Российской Федерации.

Структура и объем диссертации. Диссертация содержит 118 страниц текста и состоит из введения, 4 глав, заключения, списка сокращений и обозначений, списка литературы из 130 наименований и приложения, включающего акты внедрения.

Личный вклад. Все результаты диссертационной работы получены автором самостоятельно.

Краткое содержание работы.

Во введении обосновывается актуальность темы диссертационной работы, формулируются цель и задачи исследования, научная новизна и положения, выносимые на защиту. Здесь же приводятся теоретическая и практическая ценность диссертационной работы, ее апробация, достоверность, сведения о публикациях, личный вклад автора.

В первой главе анализируется содержание концепции Интернета Вещей, численный анализ развития которой приводит к необходимости создания самоорганизующихся сетей. Анализируются основные характеристики самоорганизующихся сетей, включая наиболее значимые их приложения. Отдельный раздел посвящен беспроводным сенсорным сетям, в том числе особенностям их построения и самоорганизации, что должно позволить в последующих главах создать адекватные реальным модели сенсорных полей при вторжении на эти поля потоков ложных событий. Завершается глава анализом видов вторжений на сетях связи в соответствии с рекомендациями МСЭ-Т. При этом в соответствии с рекомендацией МСЭ-Т Y.2701 формулируется понятие сетевой безопасности. В главе также предложена классификация ложных структур для Интернета Вещей, где наряду с потоками ложных событий рассматриваются ложные облака и клонированные интернет вещи. Дано определение ложных облаков и рассмотрены примеры клонирования сенсорных

полей. Приведены основные характеристики ложных облаков и клонирования для Интернета Вещей.

Вторая глава посвящена разработке модели потоков ложных событий и ее исследованию в условиях детерминированного и пуассоновского потока. На основе результатов имитационного моделирования было выявлено свойство зависимости длительности жизненного цикла беспроводной сенсорной сети от вида потока ложных событий. Исследовались беспроводные сенсорные сети со стационарными и мобильными сенсорными узлами. Для мобильных узлов помимо собственно сенсорных узлов изучено также влияние на длительность жизненного цикла сети скорости перемещения узлов для мобильных Ad Hoc сетей. При исследованиях воздействия потоков ложных событий на сенсорное поле было установлено, что придание сенсорным узлам мобильности позволяет увеличить жизненный цикл сети. Результаты этих исследований также приведены в данной главе.

В третьей главе определены характеристики беспроводной сенсорной сети для выявления вторжений в виде потоков ложных событий с заданной вероятностью обнаружения. Рассматривается модель беспроводной сенсорной сети, представляющая собой пуассоновское сенсорное поле и поток событий в виде ложных объектов, пересекающих заданную плоскость. По результатам исследований определены плотность распределения расстояния, которое должен пройти ложный объект до первого сенсора, необходимая плотность сенсорных узлов и необходимый радиус обнаружения сенсорного узла при заданной вероятности обнаружения ложного объекта, число сообщений, передаваемых в сети, при прохождении ложного объекта через сенсорное поле.

Четвертая глава посвящена разработке метода защиты беспроводных сенсорных сетей от потоков ложных событий, состоящего в изменении распределения плотности сенсорных узлов по сравнению с равномерной, и поиску оптимального значения распределения плотности (числа) узлов на плоскости, обеспечивающего максимальное время жизни сенсорной сети.

В заключении сформулированы основные результаты, полученные в диссертационной работе.

В приложении приведены акты внедрения результатов диссертационной работы.

ГЛАВА 1

АНАЛИЗ ТЕНДЕНЦИЙ РАЗВИТИЯ СЕТЕЙ СВЯЗИ И ОСОБЕННОСТЕЙ ПОСТРОЕНИЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

1.1 Концепция Интернета Вещей

Уже несколько лет развитие сетей и систем связи проходит при определяющей роли концепции Интернета Вещей [12, 15, 19, 34, 43, 77]. Сформулированная в рекомендации Y.2060 Сектора Стандартизации Телекоммуникаций Международного Союза Электросвязи (МСЭ-Т) в начале второго десятилетия 21 века [103], концепция Интернета Вещей существенным образом преобразовала представления о развитии сетей и систем связи.

В основе создания концепции Интернета Вещей лежит положение о том, что именно вещи, а не человек являются центральным звеном клиентской базы сетей связи. В соответствии с этим положением архитектура сети, предоставляемые сетью услуги, классы и параметры качества обслуживания, методы обеспечения сетевой безопасности должны основываться на понимании того факта, что вещей в сети будет неизмеримо больше, чем людей, и сеть должна быть построена с учетом этого нового явления.

Прежде чем оценить, а сколько же вещей может быть в сети, остановимся на определении вещей, данном в рекомендациях МСЭ-Т Y.2060 и Y.2069 [103, 104]. В соответствии с этими рекомендациями под вещами в концепции Интернета Вещей понимаются как объекты физического мира, так и объекты информационного мира. При этом существуют только два условия, для того, чтобы объект был признан Интернет вещью: объект физического или информационного мира должен быть идентифицирован в сети и иметь интерфейс с сетью. Идентификация в простейшем случае может быть проведена по адресу. Предположение о чрезвычайно большом числе вещей однозначно требует для

внедрения приложений концепции Интернета Вещей реализации на сетях связи протокола IPv6 [106]. Отметим, что приведенное определение вещи не противоречит классическому определению вещи Г. Ф. Гегелем как “вещи-в-себе”, проявляющей себя только во взаимодействии с внешним миром [14].

В соответствии с прогнозами World Wireless Research Forum число Интернет вещей к 2017-2020 годам должно составить 7 триллионов [117]. Известный французский специалист Ж.-Б. Вальднер в своей книге “Нанокомпьютеры и роевой интеллект” [120] определил и предельное число Интернет вещей в сети в 30-50 триллионов вещей. В обоих случаях мы видим, что речь идет о сетях связи, в которых клиентская база будет составлять триллионы единиц. Такие сети вполне уместно назвать триллионными [33], и они должны обладать некими иными особенностями, чем те сети связи, которые до настоящего времени создавало человечество. Действительно, созданные сети являются в количественном соотношении миллиардными и вряд ли принципы их построения, как, впрочем, и иные характеристики могут быть слепо перенесены на триллионные сети.

Для сетей связи важнейшим параметром является трафик, который создается клиентской базой. Действительно, вещей может быть очень много, но определяющим для сети является все-таки создаваемый трафик и его характеристики. По оценкам достаточно известного агентства Mason Ltd число сообщений от Интернет вещей будет составлять от 1000 до 10000 на жителя планеты в день [78]. Сравним эти значения с известными на сегодня значениями для самых развитых технологий телекоммуникаций [79]. Среднее число сообщений в современных мобильных сетях составляет 3,3 на пользователя в день. В Facebook средний пользователь создает 70 сообщений в месяц и имеет 130 друзей. Как видим, эти современные технологии по числу сообщений в день на жителя планеты существенно уступают даже нижней оценке прогнозируемого числа сообщений для Интернета Вещей. Более близкими, но опять-таки к нижней границе прогноза, являются Твиттер и электронная почта. В Твиттере ежедневно создается 60 миллионов сообщений в день, что в пересчете на одного

пользователя при 126 последователях для данной услуги составляет 344 сообщения в день на пользователя Твиттера, а не на жителя планеты. Электронная почта генерирует 247 миллиардов сообщений в день, что составляет 176 сообщений в день на жителя планеты в день, но 81% этой информации относится к спаму. Таким образом, внедрение концепции Интернета Вещей приведет к возникновению чрезвычайно большого объема сообщений, которые надо передать по сети, и пока еще малоизученному характеру потоков этих сообщений [90].

Как уже выше отмечалось, к Интернет вещам могут быть отнесены вещи физического и вещи информационного мира. Эволюция концепции Интернета Вещей в настоящее время привела к созданию достаточно большого числа ее приложений, реализуемых для физических вещей. Общее название для сетей, обеспечивающих услугами физические интернет вещи, в настоящее время выглядит как машина-машина M2M (Machine-to-Machine) [47, 67, 98, 113, 114, 115, 130]. Примерами сетей M2M являются всепроникающие сенсорные сети USN(Ubiquitous Sensor Networks) [18, 27, 36, 48, 69, 70, 95], целевые сети для транспортных средств VANET (Vehicular Ad Hoc Networks) [35, 91, 102], мобильные целевые сети MANET (Mobile Ad Hoc Networks) [38]. Диссертация посвящена исследованию проблем обеспечения сетевой безопасности для всепроникающих сенсорных сетей. Всепроникающий характер этих сетей был подчеркнут в названии в рекомендации МСЭ Y.2062 [105] и последующих за ней. В научной литературе большее использование находит упрощенный вариант названия – беспроводные сенсорные сети, которым далее будем пользоваться и мы. Беспроводные сенсорные сети достаточно часто называют технологической основой реализации концепции Интернета Вещей, имея ввиду как всепроникающий характер этих сетей, так и достаточно широкое их внедрение уже в настоящее время. В Российской Федерации исследования беспроводных сенсорных сетей при их использовании на сетях связи общего пользования (ССОП) [16, 18] широко проводятся, начиная с 2005 года [20, 21, 22, 23]. При этом достигнут существенный прогресс в области создания алгоритмов для

функционирования этих сетей [1, 3, 24, 25, 26], изучения моделей потоков трафика [31, 32, 39], а результаты этих работ получили заслуженное международное признание [83, 84, 85, 86, 87, 88, 89, 90]. Однако в области сетевой безопасности беспроводных сенсорных сетей масштабных исследований пока проведено не было, а научно-исследовательские работы посвящались, в основном, исследованию традиционных проблем обеспечения информационной безопасности применительно к беспроводным сенсорным сетям [4]. Беспроводные же сенсорные сети по своей природе являются самоорганизующимися, к тому же состоящими из очень большого числа сенсорных узлов, что требует выявления и исследования особенностей обеспечения сетевой безопасности в беспроводных сенсорных сетях.

1.2 Беспроводные сенсорные сети

Беспроводные сенсорные сети представляют собой самоорганизующиеся сети множества сенсорных узлов, выполняющих различные задачи по мониторингу внешней среды, процессов, событий и т.д. [2, 18, 19, 28, 29, 37]. Достаточно часто множество расположенных на плоскости сенсорных узлов называют сенсорным полем. На рисунке 1.1 в качестве примера приведено пуассоновское сенсорное поле, т.е. такое поле, на котором сенсорные узлы распределены случайным образом в соответствии с равномерным распределением.

Число сенсорных узлов на одном сенсорном поле может быть очень велико. Например, при использовании широко распространенного для беспроводных сенсорных сетей протокола ZigBee число узлов на одном сенсорном поле может превышать 64000 [19]. Отсюда понятно и стремление к самоорганизации сети, поскольку трудно представить себе неиерархическую сеть в 64000 узлов, связанных между собой постоянно. Еще сложнее представить такую же

иерархическую сеть с постоянными узлами разной степени иерархии, поскольку все сенсорные узлы, как правило, одинаковы. В таких случаях говорят еще об однородной или гомогенной сенсорной сети.

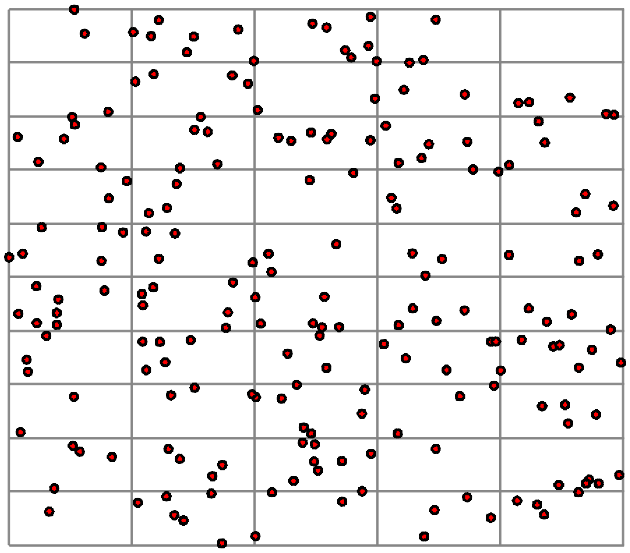

Рисунок 1.1 - Пуассоновское сенсорное поле

Естественно, могут рассматриваться и гетерогенные сенсорные сети, в которых, например, у различных сенсорных узлов различный радиус зоны мониторинга происходящих событий [84]. Но это либо исключение из правил, либо вырождающаяся однородная сенсорная сеть, в которой многие сенсоры частично потеряли энергетичские возможности и, соответсвенно, уменьшился их радиус действия.

Самоорганизация сенсорной сети заключается в том, что взамимосвязи между узлами являются случайными и образуются только для передачи информации между ними о происходящем событии или результатах мониторинга [19]. При этом, большую часть времени сенсорные узлы находятся в спящем состоянии, что позволяет уменьшать потребляемую ими энергию. Зачастую сенсорный узел не имеет возможности восстановления энергетических характеристик за счет подключения к стацинарной электросети или путем замены элемента питания в процессе выполнения той или иной задачи. Поэтому, одними

из наиболее важных исследовательских задач при построении беспроводных сенсорных сетей являлись и являются задачи, связанные с оптимизацией энергопотребления как отдельными узлами, так и сенсорной сетью в целом [49, 69].

Широкое распространение при построении беспроводных сенсорных сетей нашли кластерные структуры [55, 56, 61, 62, 63, 64, 93, 118, 122, 126-130]. При этом головной узел кластера периодически подвергается ротации, что позволяет при использовании тех или иных алгоритмов выбора головного узла уменьшать суммарную потребляемую кластером энергию и увеличивать жизненный цикл кластера и сенсорной сети в целом. Базовый алгоритм выбора головного узла LEACH (LowEnergyAdaptiveClusterHierarchy) [73, 74, 75] для стационарных сенсорных узлов позволяет, например, снизить потребление энергии в 7-8 раз по сравнению с таким же сенсорным полем, в котором головные узлы выбираются случайным образом. На рисунке 1.2 приведена архитектура кластерной беспроводной сенсорной сети. Головные узлы кластера выделены оранжевым цветом, а члены кластера имеют желтую окраску.

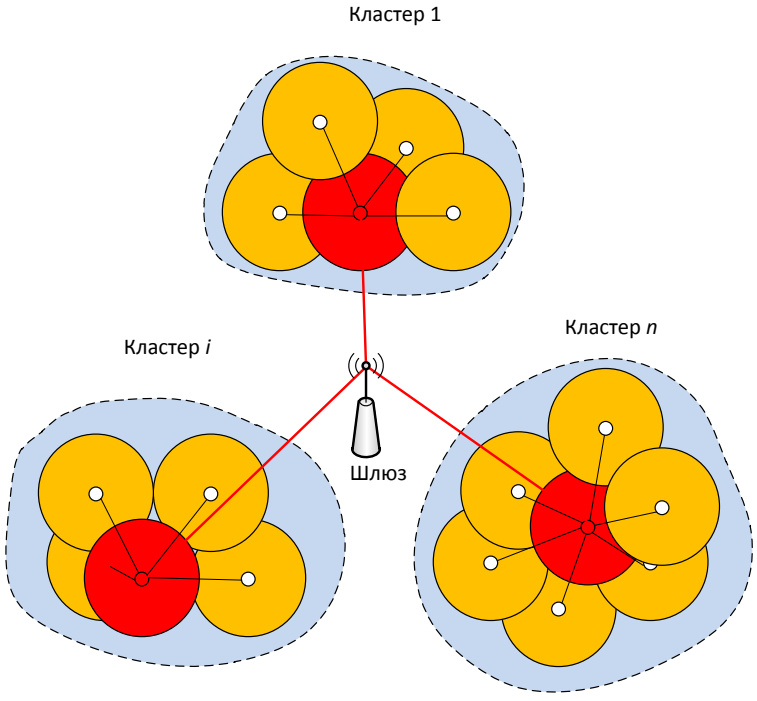

Рисунок 1.2 - Архитектура кластерной беспроводной сенсорной сети

С момента появления алгоритма LEACH предпринималось множество попыток его улучшить и достаточно часто это удавалось для конкретных приложений беспроводных сенсорных сетей или для иных условий их использования, например для мобильных сенсорных сетей. Вместе с тем, оптимального алгоритма для выбора головного узла в беспроводных сенсорных сетях так и не найдено, что вполне резонно объясняется практически неограниченным числом приложений таких сетей и большой вариативностью параметров беспроводных сенсорных сетей в зависимости от приложений.

Для некотрых задач кластеризация не используется в силу их специфики. Например, в задачах слежения за целью могут использоваться структуры, для которых расположение сенсорных узлов заранее задано для обеспечения возможности отслеживания цели на всей траектории ее движения . В таких задачах рассматривают как линейно движущуюся цель, так и цель со случайной траекторией движения [72, 88, 92, 119]. Однако и для подобных задач увеличение длительности жизненного цикла беспроводной сенсорной сети, а значит и уменьшение потребления энергии, является наиважнейшим. Достигается это, как будет показано в главах 3 и 4 диссертации, за счет оптимального распределения плотности сенсорных узлов на сенсорном поле.

Несмотря на достаточно большое число алгоритмов для выбора головного узла кластера для беспроводных сенсорных сетей, исследования в этой области активно продолжаются. В последние годы появились новые работы, посвященные алгоритмам выбора головного узла кластера беспроводной сенсорной сети в n-мерном пространстве [1, 46, 54]. При этом основные показатели, которые подвергаются исследованиям, не изменились по сравнению с работами в области беспроводных сенсорных сетей на плоскости. Это по-прежнему длительность жизненного цикла сети и остаточная энергия.

В настоящее время появляется еще один класс беспровдных сенсорных сетей – летающие сенсорные сети FUSN (FlyingUbiquitousSensorNetworks), использование которых позволяет расширить применение беспроводных сенсорных сетей на такие задачи как, например, мониторинг и сбор данных с

виноградников, мониторинг состояния крыш домов и т.д. [11, 13, 112]. На рисунке 1.3 приведен пример простейшей FUSN [11], включающей в себя наземную сеть и один узел летающей сети в виде квадрокоптера Fantom, оснащенного соответствующими техническими средствами для его функционирования в беспроводной сенсорной сети – сбора данных, взаимодействия с сенсорными узлами наземной сети, выполнения при необходимости функций головного узла для наземной сети.

Заметим, что задача о целесообразности выполнения летающим фрагментом FUSN функций головного узла еще не решена, но в ее постановке в качестве основных параметров фигурируют и жизненный цикл наземной сети и летающей сети в целом, и остаточная энергия.

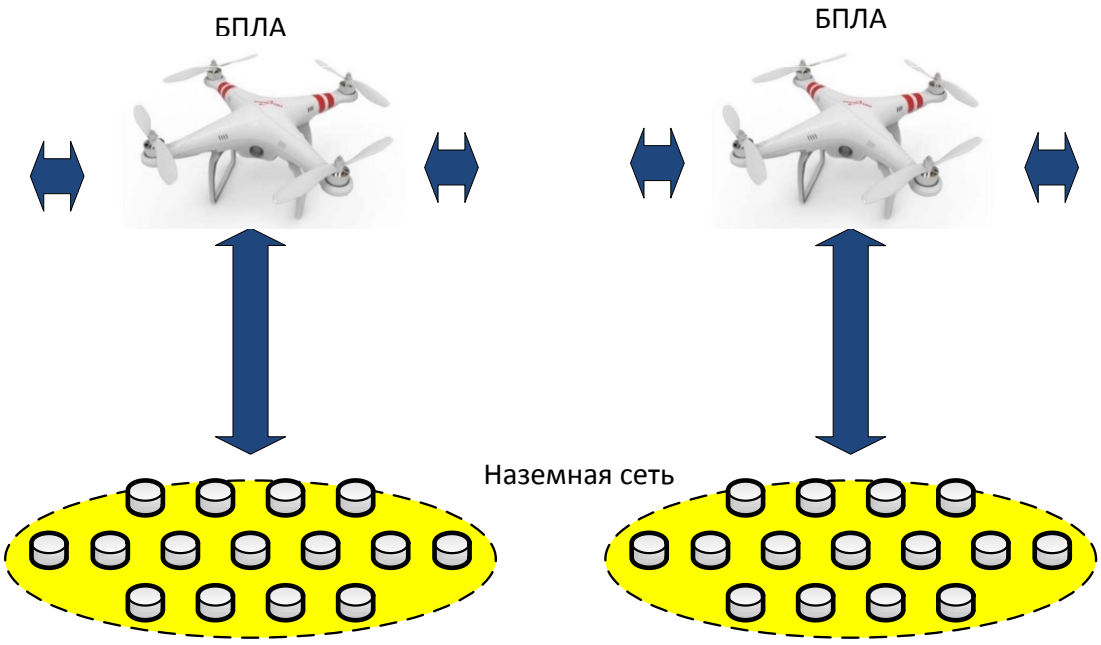

Рисунок 1.3 - Летающая сенсорная сеть

Такая ЛСС относится к классу сетей DTN (Delay Tolerant Network), т.е. сетей толерантных к задержкам, изучению которых посвящено достаточно много работ в области межпланетарного Интернет и спутниковых сетей связи. Особенностью ЛСС даже в этом простейшем случае является возможно очень большое число сенсорных узлов наземной сети. Действительно, только одно

сенсорное поле при использовании протокола ZigBee может содержать более 64 000 тысяч сенсорных узлов. Поэтому, целесообразно, как и в существующих структурах ВСС, кластеризовать наземный сегмент сети с той разницей, что в качестве головного узла кластера резонно использовать БПЛА. При этом в момент времени t_1 БПЛА будет являться головным узлом для первого кластера, а в момент времени t_n для n-ого кластера как это показано на рисунке 1.4. Заметим, что БПЛА тогда должен быть оснащен техническими и программными средствами, позволяющими выполнять функции головного узла кластера ВСС, т.е. реализовывать физический и канальный уровни протокола IEEE 802.15.4, поддерживать обмен информацией по протоколам ZigBee, 6LoWPAN, RPL, обеспечивать реконфигурацию кластера, особенно для мобильного наземного сегмента ЛСС и т.д. Поэтому, данные сети и называются летающими сенсорными сетями.

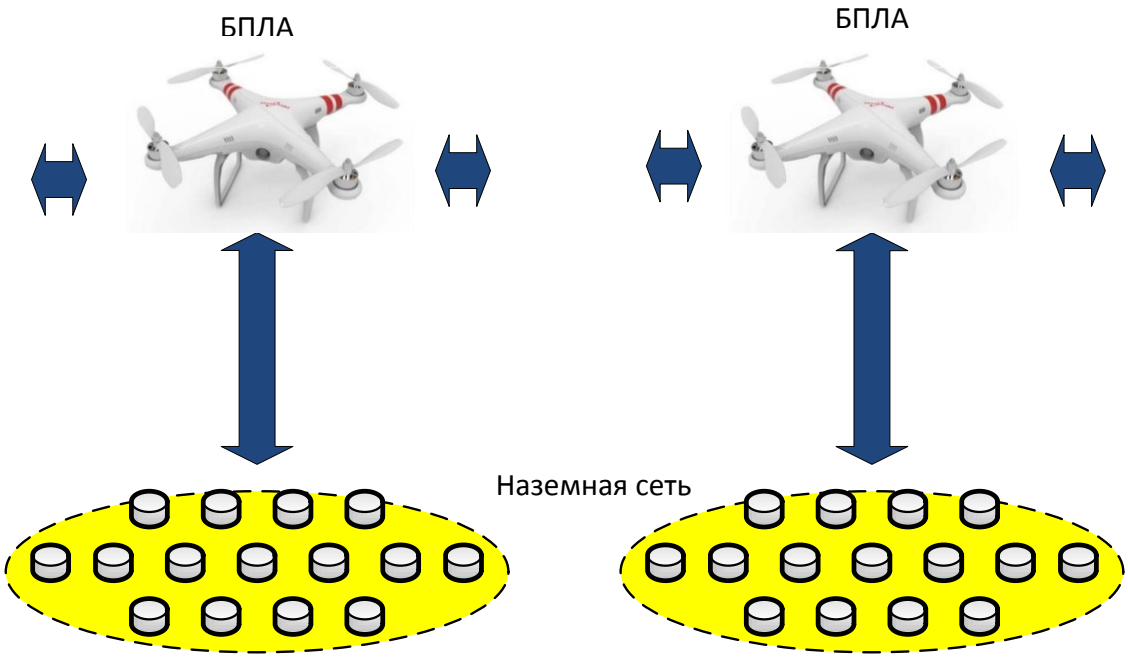

Рисунок 1.4 - ЛСС с одним БПЛА и кластерной наземной сетью

На рисунке 1.5 приведена архитектура ЛСС с несколькими БПЛА, которые могут взаимодействовать между собой и с наземным сегментом ЛСС.

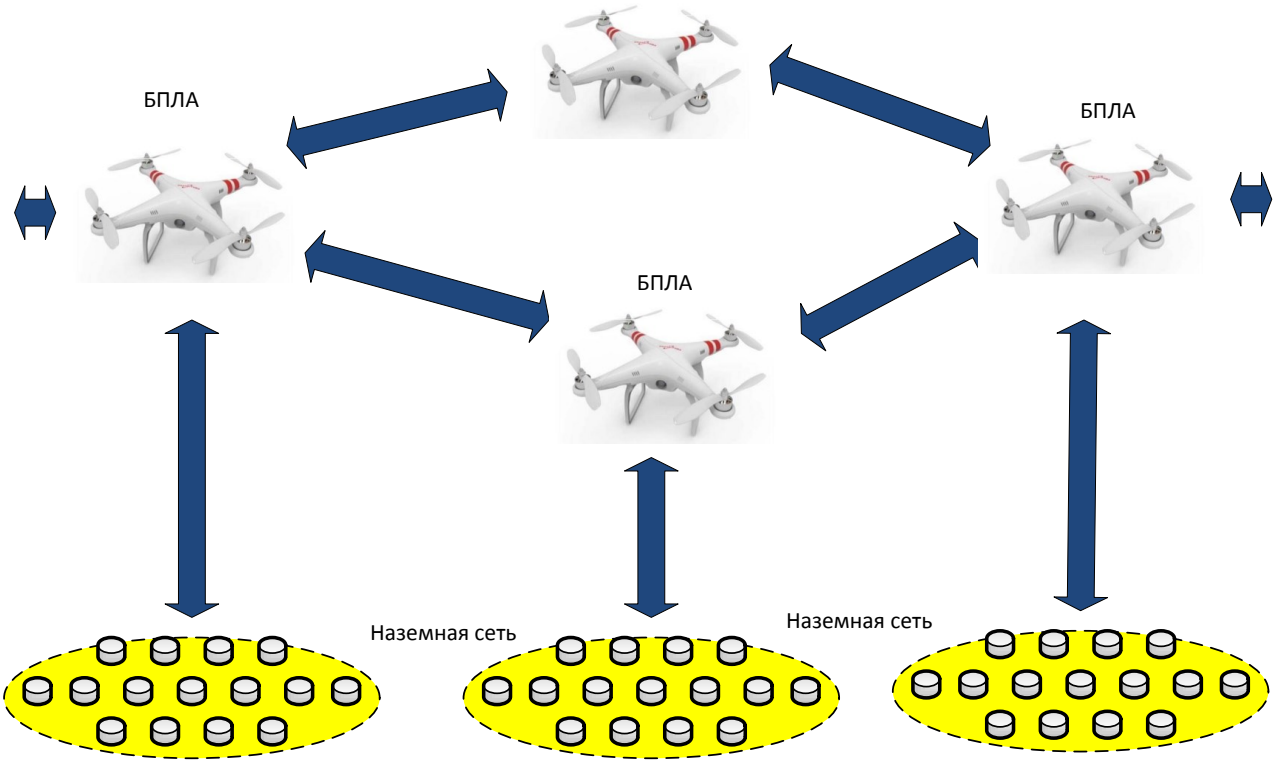

Рисунок 1.5 - ЛСС с несколькими БПЛА и наземной кластерной сетью

Для такой архитектуры сети актуальным становится вопрос об организации кластерной сети для летающего сегмента ВСС, тем более, что использование множества БПЛА позволяет избавиться от ограничений, налагаемых структурой сетей, толерантных к задержкам. Естественно, что кластеризация возможна и для наземного сегмента.

Таким образом, анализ научно-исследовательских работ, проводимых в области построения беспроводных сенсорных сетей, показал, что основные усилия направлены на увеличение длительности жизненного цикла беспроводной сенсорной сети за счет уменьшения энергетических затрат и увеличения остаточной энергии. Диссертация посвящена проблемам обеспечения сетевой безопасности беспроводных сенсорных сетей, что дает основания для детального исследования воздействий на энергетическую систему этих сетей и разработки методов защиты от вторжений в беспроводные сенсорные сети, связанных с попытками уменьшить жизненный цикл беспроводной сенсорной сети за счет уменьшения остаточной энергии.

1.3 Виды вторжений в сетях связи

В предыдущих разделах диссертации были рассмотрены основополагающие вопросы развития сетей связи: концепция Интернета Вещей и ее технологическая база – всепроникающие сенсорные сети USN. Проведенный анализ показывает, что на горизонте планирования до 2020 года USN будет одной из основных технологий, обеспечивающих развитие сетей связи. К настоящему времени в рамках научно-исследовательских работ в области USN решено множество новых задач – разработаны алгоритмы выбора головного узла в кластере, исследованы характеристики трафика в стационарных и мобильных сенсорных сетях, разработаны спецификации протоколов сигнализации и т.д. USN, как и любая сеть, обладает атрибутами, присущими ей как именно сети [101, 105, 108]. И среди этих атрибутов одним из важнейших является безопасность, в области исследований которой до настоящего времени много нерешенных вопросов, связанных с особенностями построения и функционирования USN. Вопросы безопасности в USN являются ключевыми в диссертации, поэтому прежде, чем перейти к их решению, остановимся на понятии безопасности и иных терминологических вопросах в соответствии с рекомендациями Сектора Стандартизации Телекоммуникаций Международного Союза Электросвязи (МСЭ-Т).

Сам по себе термин безопасность может быть всеобъемлющим и, поэтому, МСЭ-Т сосредотачивается на так называемой сетевой безопасности (network-based security), что планируется в качестве предмета исследования и в настоящей диссертации. В соответствии с рекомендацией МСЭ-Т Y.2701 [109] для сетей связи следующего поколения NGN сетевая безопасность включает в себя:

- инфраструктуру провайдеров сетей и услуг и ее составляющие (например, сетевые элементы, системы, интерфейсы, данные, информацию), ресурсы и

возможности (например, сигнализацию, управление, передачу трафика), предоставляемые провайдерами услуги,

- услуги и возможности сети NGN,

- информацию и связи конечного пользователя в сети (например, персональные данные).

Вместе с тем, в рекомендации подчеркивается, что безопасность пользовательских сетей (например, локальной сети) и безопасность при взаимодействии пользователей в одноранговых сетях (peer-to-peer) не являются предметом требований к безопасности в NGN.

Базовая рекомендация МСЭ-Т по безопасности X.805 [110], принятая в 2003 году и основанная в рассматриваемых вопросах на рекомендации X.800 от 1991 года, являющейся аналогом стандарта ISO 7498-2 для модели взаимодействия открытых систем, определяет следующие атрибуты безопасности:

- управление доступом,

- аутентификация.

- безотказность,

- конфиденциальность данных,

- безопасность связи,

- целостность данных,

- доступность,

- персональные данные.

В рекомендации X.805 определяются также возможные угрозы (threats) для сетевой безопасности:

- уничтожение информации и/или других ресурсов,

- искажение или модификация информации,

- хищение, удаление или потеря информации и/или других ресурсов,

- раскрытие информации,

- прерывание услуг.

Соответствие атрибутов безопасности и угроз безопасности приведено в таблице 1.1. Знаком “x” отмечена необходимость учета угрозы для конкретного атрибута.

Следует отметить, что эти угрозы сформулированы как высокоуровневые элементы безопасности, в то время как для более конкретного проявления вмешательства в функционирование сети чаще используются понятия атак (attack) и вторжений (intrusion).

Определение атаки можно найти в рекомендации H.235.0 [107]. Под атакой понимается предпринимаемое действие, которое направлено на обход механизмов системы безопасности или использование их недостатков в своих целях. Атаки на систему делятся на прямые и косвенные. Наиболее известной из сетевых атак является DoS (Denial of Service), определенная в рекомендации X.800 как отказ в авторизованном доступе к системе или создание задержек, критичных ко времени выполнения операций.

В отечественной литературе способы атак (нападений) рассмотрены достаточно полно применительно к компьютерным сетям. Так, например, в [17] приводится классификация способов атак на компьютерные сети. При этом отмечается, что эффективность атаки напрямую связана с несовершенством системы защиты атакуемой компьютерной сети.

Одной из важнейших задач создания беспроводных сенсорных сетей является обеспечение мониторинга процессов производства, функционирования механизмов, состояния биомасс и т.д. Очевидно, что мониторинг осуществляется в каком-то n-мерном пространстве, достаточно часто называемом сенсорным полем. Поэтому, наиболее подходящим термином для исследования безопасности беспроводных сенсорных сетей является вторжение, однозначно связанное с тем или иным нарушением пространства сенсорного поля. Это термин нашел широкое применение в научной литературе по безопасности беспроводных сенсорных сетей [4, 7, 8, 9, 53, 58].

Таблица 1.1 - Соответствие атрибутов и угроз безопасности

Атрибуты/Угрозы	Уничтожение информации	Искажение информации	Хищение информации	Раскрытие информации	Прерывание услуг
Управление доступом	X	X	X	X	
Аутентификация			X	X	
Безотказность	X	X	X	X	X
Конфиденциальность данных			X	X	
Безопасность связи			X	X	
Целостность данных	X	X			
Доступность	X				X
Персональные данные				X	

1.4 Особенности вторжений в беспроводные сенсорные сети. Новые виды вторжений

Как уже выше отмечалось, всепроникающие (беспроводные) сенсорные сети являются самоорганизующимися сенсорными сетями структурно построенными, как правило, с помощью кластеризации и состоящими из очень большого числа сенсорных узлов. Основными характеристиками таких сетей являются жизненный цикл и доля покрытия пространства в течение этого жизненного цикла, что определяет возможности беспроводной сенсорной сети по реализации задач мониторинга процессов, состояний, явлений и т.д. Кроме того, вследствие большого числа узлов в кластере и большого числа кластеров в сети, а также проблемами с восстановлением электропитания отдельных сенсорных узлов, важнейшей составляющей сенсорной сети является ее энергосистема. Возможность минимизации расхода энергии узлами в течение жизненного цикла сети рассматривается как одна из приоритетных задач при создании всепроникающих сенсорных сетей. Все вышесказанное приводит к наличию целого ряда особенностей в обеспечении безопасности беспроводных сенсорных сетей.

Анализ особенностей обеспечения безопасности в беспроводных сенсорных сетях начнем с рекомендации МСЭ-Т X.1311 “Структура безопасности для всепроникающих сенсорных сетей” [111].

В рекомендации X1311 “Структура безопасности для всепроникающих сенсорных сетей” выделяются пять категорий взаимосвязей в USN, которые могут представлять интерес с точки зрения сетевой безопасности:

- взаимодействие сенсорного узла с базовой станцией (шлюзом),
- взаимодействие базовой станции (шлюза) с сенсорным узлом,
- взаимодействие базовой станции со всеми сенсорными узлами, например, при перепрограммировании сенсорной сети,

- взаимодействие между узлами сенсорной сети, включая взаимодействие головного узла кластера с сенсорными узлами и взаимодействие близлежащих сенсорных узлов между собой,

- взаимодействие между базовой станцией (шлюзом) и определенной группой сенсорных узлов, объединенных, например, общим местоположением.

Приведенный перечень взаимосвязей достаточно полно характеризует USN, за исключением такого специфичного взаимодействия как взаимодействие головного узла кластера с головным узлом другого кластера.

Далее в рекомендации X.1311 отмечается, что особенности построения и функционирования беспроводных сенсорных сетей предопределяют проблемы с использованием традиционных способов и средств обеспечения безопасности в сетях связи.

Действительно, сложно использовать общеупотребительную систему криптографических ключей вследствие достаточно строгих требований к сенсорным узлам по вычислительной мощности, объему памяти и энергопотреблению. Эти же требования способствуют и повышенной уязвимости сенсорных узлов из-за отсутствия экономической возможности сделать их защищенными при массовом применении. Кроме того, при создании сенсорной сети ее узлы размещаются на сенсорном поле, как правило, случайным образом, исходя из чего, возникают проблемы с определением местоположения при использовании традиционных протоколов безопасности. Достаточно сложной проблемой обеспечения безопасности в USN является также тот факт, что базовая станция (шлюз) является точкой концентрации всей информации от всех сенсорных узлов сети, что делает ее привлекательным объектом для разнообразных атак.

Для USN, естественно, как для сети, возможны все виды угроз (вторжений), рассмотренные выше в разделе 1.3. Однако особенности построения и функционирования всепроникающих сенсорных сетей

порождают как новые виды угроз (вторжений), так и модифицируют содержание существующих.

Наиболее оригинальными и новыми угрозами являются так называемые энергетические вторжения, призванные уменьшить жизненный цикл сенсорной сети за счет несанкционированного использования ограниченных ресурсов энергетической системы сенсорной сети. Этому вопросу в рамках рекомендации X.1311, к сожалению, не уделено должного внимания, и он будет рассмотрен отдельно в заключительной части настоящего раздела. В рекомендации X1311 рассматриваются следующие угрозы, имеющие существенную специфику для всепроникающих сенсорных сетей:

- уязвимость отдельных сенсорных узлов,
- секретность данных сенсорных сетей и съем информации,
- отказ в обслуживании,
- злонамеренное использование сенсорных сетей.

В части уязвимости отдельных сенсорных узлов можно отметить, что каждый из них индивидуально может быть подвергнут различным атакам. Кроме того, в сеть могут быть внедрены злонамеренные узлы по своим характеристикам не отличающиеся от легальных сенсорных узлов, но выполняющие задачи в иных целях, чем атакуемая сенсорная сеть. Такие вторжения во всепроникающие сенсорные сети называют клонированием, и выявление клонированных узлов представляет собой достаточно сложную задачу. В случае обнаружения клонированный узел должен быть изолирован от сети. Атакованные легальные сенсорные узлы могут изменить свои свойства, и для их возвращения в режим штатного функционирования может потребоваться перепрограммирование узла или перезапуск сенсорной сети в целом при достаточно большом числе поврежденных узлов.

В составе информации, собираемой сенсорной сетью, возможно присутствие информации, имеющий конфиденциальный или частный характер. Действительно, информация об энергопотреблении в квартире или

освещенности имеет частный характер и может свидетельствовать об активности, которую проявляют хозяева дома (квартиры) в течение определенного отрезка времени. Таких примеров можно привести достаточно много, но особенно актуальны эти примеры в области медицинских показателей и в системе электронного здоровья (e-health) [52, 80]. Поэтому, проблемы секретности информации и ее съема являются чрезвычайно актуальными для всепроникающих сенсорных сетей. Наиболее приемлемым решением таких проблем представляется передача информации по разным маршрутам, но этот метод можно использовать только при широком внедрении протокола RPL (Routing Protocol for Low energy and lossy networks) [40] и ему подобных.

Хорошо известные атаки DoS (Denial of Service) – отказ в обслуживании - в сенсорных сетях проявляются, например, на физическом уровне в форме джамминга (глушение радиопередачи). Наиболее сложное и новое проявление DoS атак в соответствии с рекомендацией X.1311 – энергетические вторжения, хотя на наш взгляд к DoS атакам энергетические вторжения имеют весьма опосредованное отношение.

Злонамеренное использование сенсорных сетей возможно криминальными элементами для реализации нелегальных целей. Это относится и к собственно сенсорным сетям, но, в первую очередь, все-таки к сенсорно-актуаторным сетям, в которых возможен не только сбор данных с Интернет вещей, но и управление ими.

Кроме рассмотренных выше атак и угроз, существенное значение имеют также атаки, направленные на маршрутизацию сообщений. Среди этих атак выделяются следующие. Атаки по созданию ложной информации маршрутизации (spoof), видоизмененной информации (alter), замещению информации (replay) направлены на увеличение задержки при передаче информации из конца в конец сети, изменение маршрута, перераспределение трафика в сети. Атаки по избирательной переадресации (selective forwarding) предусматривают отказ в передаче определенных сообщений, сброс сообщений, которые должны были быть направлены в определенных

направлениях. Атаки типа “бездонная воронка” (sinkhole) направлены на то, чтобы обеспечить передачу всего трафика из вполне определенной зоны через клонированный или специально поврежденный узел сенсорной сети. Один или несколько злонамеренных (клонированных) узлов могут иметь множество псевдо идентификаторов, в том числе и по местоположению. В этом случае имеет место так называемая “колдовская” атака (Sybil). Атака “червоточина” (wormhole) предусматривает создание специального пути между двумя и более злонамеренными узлами сенсорной сети для передачи по ним перехваченных пакетов, доступных только для атакующей системы. Как правило, для создания такого пути на физическом уровне используется иной диапазон частот, чем в атакуемой всепроникающей сенсорной сети. Атака “переполнение” (HELLO flood attack) является широковещательной атакой, призванной направить в сенсорную сеть массу необязательных сообщений, которые должны лишить сеть разнообразных ресурсов – канальной емкости, вычислительной мощности, энергетических и т.д. Задача атаки “ложное подтверждение” (acknowledgement spoofing) сфабриковать пакет “подтверждение”, например, от погибшего сенсорного узла.

Поскольку USN хотя и самоорганизующаяся, но все-таки сеть, ей присущи все атрибуты безопасности, которые были рассмотрены в разделе 1.3. Вместе с тем, самоорганизация привносит и некоторые новые отличительные свойства, связанные, в первую очередь, с тем, что после атак или во время атаки USN может быть реконфигурирована. Поэтому, в атрибуты безопасности для всепроникающих сенсорных сетей добавляется эластичность к атакам (resilience to attack). С учетом изложенного в таблице 1.2 приведено соответствие атрибутов и угроз безопасности для USN при широкополосных атаках со стороны базовой станции, в таблице 1.3 – для внутри сетевых угроз безопасности, в таблице 1.4 – для внешних угроз безопасности. Заметим, что в таблице 1.3 и таблице 1.4 атрибут аутентификации подразделяется на два: аутентификацию сообщений и идентификацию. Последнее связано с особенностями вторжений в сенсорных сетях, таких как клонирование, когда мало провести аутентификацию узла, надо проверить еще и его легальность.

Таблица 1.2 - Соответствие атрибутов и угроз безопасности для USN при широкополосных атаках со стороны базовой станции

Атрибуты/Угрозы	Уничтожение информации	Искажение информации	Хищение информации	Раскрытие информации	Прерывание услуг, DoS
Управление доступом	X	X	X	X	
Аутентификация		X	X	X	
Безотказность	X		X		X
Конфиденциальность данных			X	X	
Безопасность связи			X	X	
Целостность данных	X	X			
Доступность	X				X
Персональные данные				X	
Эластичность к атакам	X	X	X	X	X

Таблица 1.3 - Соответствие атрибутов и внутри сетевых угроз безопасности для USN

Атрибуты/Угрозы	Sybil	Hello flood	Sinkhole	Selective forwarding	Wormhole	ACK spoofing
Управление доступом						
Аутентификация сообщений	X		X	X		X
Идентификация	X		X	X		X
Безотказность						
Конфиденциальность данных	X		X	X		X
Безопасность связи						
Целостность данных						
Доступность						
Персональные данные						
Эластичность к атакам	X	X	X	X	X	X

Таблица 1.4 - Соответствие атрибутов и внешних угроз безопасности для USN

Атрибуты/Угрозы	Sybil	Hello flood	Sinkhole	Selective forwarding	Wormhole	ACK spoofing
Управление доступом						
Аутентификация сообщений	X		X	X		X
Идентификация	X		X	X		X
Безотказность						
Конфиденциальность данных	X		X	X		X
Безопасность связи				X		
Целостность данных						
Доступность						
Персональные данные			X	X	X	
Эластичность к атакам			X	X		

Эластичность к атакам во всепроникающей сенсорной сети может быть поддержана распределением ключей третьей стороной или созданием доверительного модуля для противодействия “колдовским” атакам и ложным подтверждениям, двусторонней верификацией линии передачи информации для противодействия атакам переполнения, передачей информации по различным маршрутам для противодействия атакам избирательной переадресации и “бездонной воронки”, выбором небольшой длительности синхронизации для противодействия атакам “червоточина”.

Все эти виды атак и их проявления для беспроводных сенсорных сетей достаточно подробно рассмотрены в рекомендации X.1311 “Структура безопасности для всепроникающих сенсорных сетей”. Однако, как выше уже отмечалось, специфика беспроводных сенсорных сетей, связанная как с самоорганизацией, так и с предназначением (мониторинг) требует пристального внимания к еще одному принципиально новому виду атак – энергетическим атакам [6]. Следует заметить, что специфика предназначения беспроводных сенсорных сетей, заключающаяся в мониторинге n-мерного пространства, приводит к тому, что для исследования безопасности в сенсорных сетях наибольшее употребление нашел термин вторжение. При этом зачастую рассматриваются как односторонние вторжения, так и периметрические.

В [96] рассмотрены концептуальные вопросы использования периметрической защиты для всепроникающих сенсорных сетей. Используется плоскостная модель сенсорной сети, в которой границы сенсорного поля представляют собой окружность радиусом R. В работах по сенсорным сетям, как правило, в качестве плоскостной модели рассматривается квадрат. Однако рассмотрение вместо квадрата вписанной в квадрат со стороной 2R окружности практически не влияет на суть результатов. Шлюз находится в центре сети и основной задачей по защите от вторжений является обеспечение раннего предупреждения шлюза об обнаружении вторжения. На рисунке 1.6 приведена традиционная модель однородной беспроводной сенсорной сети, из которой видно, что ряд сенсорных узлов перекрывают периметрическую границу и,

естественно, эти узлы могут обеспечивать раннее предупреждение шлюза о вторжении.

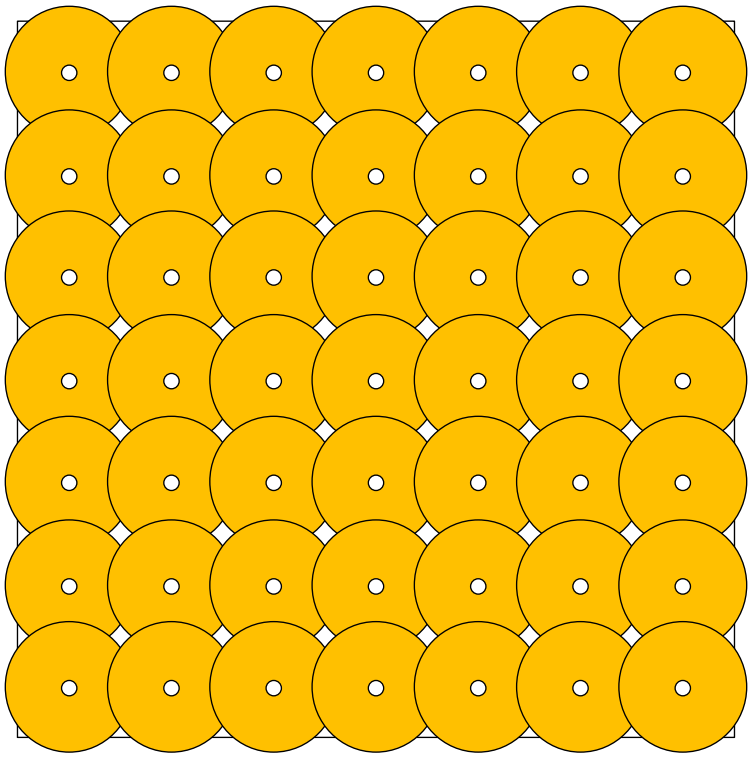

Рисунок 1.6 - Модель беспроводной сенсорной сети с покрытием по периметру

С целью усиления безопасности беспроводных сенсорных сетей в [96] предлагается в границах сенсорного поля создавать несколько слоев, обеспечивающих заблаговременное предупреждение шлюза о вторжении.

В [59] предложен новый вид вторжений во всепроникающие сенсорные сети, предусматривающий лишение сна сенсорных узлов, находящихся в момент вторжения в спящем состоянии. Это достаточно эффективное воздействие на беспроводные сенсорные сети в [58] рассматривается как вторжение на физическом и канальном уровнях.

В диссертации предлагается новый вид вторжений – создание потоков ложных событий, который должен воздействовать на сеть на сетевом уровне модели взаимодействия открытых систем [5, 7, 8, 9 ,60]. Ложное событие так же, как и легальное событие требует реакции от сенсорного узла, которая в данном случае выражается в детектировании события и формировании пакета

информации для передачи информации о возникновении события либо для головного узла кластера, либо непосредственно от головного узла к шлюзу. Это требует дополнительного расхода энергии и уменьшает жизненный цикл сети. Имея информацию о реальных потоках событий, технически несложно создать подобные им потоки ложных событий. Возможно, что вид потока влияет на длительность жизненного цикла сети, что будет исследовано в диссертации. В последние годы все больше внимания в научных исследованиях уделяется беспроводным сенсорным сетям с мобильными узлами. Поэтому, указанные выше задачи должны быть решены как для беспроводных сенсорных сетей со стационарными узлами, так и с мобильными.

Естественно, предлагая новый вид вторжений, необходимо разработать и методы защиты от них, чему посвящены третья и четвертая главы диссертации.

Беспроводные сенсорные сети являются в настоящее время технологической основой для внедрения концепции Интернета Вещей. В концепции Интернета Вещей предполагается, что вещи не могут эффективно функционировать в сети без наличия облаков. Идея о потоках ложных событий может быть развита и на создание ложных облаков, чему посвящен следующий раздел диссертации.

1.5 Ложные структуры в Интернете Вещей

Внедрение концепции Интернета Вещей привело к пониманию новых особенностей сетей связи, которые проявляются и в архитектуре сети, и в моделях трафика, и в сетевой безопасности и т.д. Выделим следующие особенности концепции Интернета Вещей, которые оказывают непосредственное влияние на сетевую безопасность при ее внедрении.

Требования по низкому энергопотреблению для приложений Интернета Вещей, в первую очередь беспроводных сенсорных сетей, связаны как с тем, что

число Интернет Вещей очень велико, так и с тем, что во многих случаях электропитание, например сенсорных узлов, осуществляется за счет не возобновляемых источников энергии. Последнее определяет новую существенную проблему в области сетевой безопасности для приложений Интернета Вещей, а именно: проведение атак на энергетическую систему сетей связи с целью преднамеренного отъема энергии, например, у сенсорных узлов. С этой целью в диссертации предложено использовать потоки ложных событий.

Облачные технологии играют ключевую роль в архитектуре сетей при реализации концепции Интернета Вещей. Действительно, зачастую Интернет Вещи имеют ограниченные вычислительные возможности, и использование облачных ресурсов является единственной возможностью эффективной организации сети. При этом передаваемые в облако данные могут представлять интерес для различного рода злоумышленников. Сетевая безопасность такой структуры в условиях повсеместного распространения облаков не может быть гарантирована по многим показателям, а наиболее современный подход, предложенный в [124], заключается в создании ложных облаков.

Прогнозируемое чрезвычайно большое число интернет вещей требует самоорганизации при построении сетей. Кроме того, во многих приложениях концепции Интернета Вещей узлы таких сетей очень просты физически и имеют низкую стоимость. Поэтому еще одно направление создания ложных структур в сетях приложений Интернета Вещей – клонирование элементов таких сетей. Проблемы клонирования изучались, например, в [125].

На рисунке 1.7 приведена классификация ложных структур при внедрении Интернета Вещей [125].

Рисунок 1.7 - Ложные структуры в Интернете Вещей

Исследованию потоков ложных событий и их воздействию на беспроводные сенсорные сети посвящена настоящая диссертация. Далее рассмотрим основные положения по ложным облакам и клонированию, также входящим в ложные структуры Интернета Вещей.

Концепция и методы реализации ложных облаков представлены в [124]. Там же предложены и методы защиты от сбора информации со стороны ложных облаков. Для получения доступа к конфиденциальным данным, идущим от типовой интернет вещи к облаку, предложено использовать метод клонирования пакетов и их последующую отправку к дублирующему облаку (ложному облаку).

Для отправки данных в облако интернет вещь должна иметь подключение к точке доступа сети связи общего пользования. Перехват и перенаправление данных может быть реализован в непосредственной близости к каналу связи «интернет вещь – точка доступа».

Метод защиты от использования ложных облаков на базе применения алгоритмов гибридного шифрования (например, RSA-512 и AES-128) требует относительно больших вычислительных мощностей интернет вещи и не может быть реализован для вещей на базе микроконтроллеров, имеющих 8-и или 16-ти битную разрядность ЦПУ (например, AVR или ARM), а также для устройств с малым объемом памяти.

В [124] предложен метод создания уникальных паттернов сетевого трафика интернет вещи, который может быть использован и для маломощных интернет

вещей на базе микроконтроллера, и для более мощных вещей на базе микропроцессоров.

Миниатюрные размеры и низкая стоимость таких интернет вещей как сенсорные узлы, а также самоорганизация этих узлов в сеть, способствовали появлению новых методов вторжения в приложения Интернета Вещей, получивших название клонирования. Клонирование отдельных сенсорных узлов рассмотрено, например, в [125]. Однако, для клонирования подходят не только отдельные узлы, но и сенсорные поля в целом, и их фрагменты. При этом могут быть определены два сценария клонирования. В первом (рисунок 1.8) клонированная сеть или ее фрагменты располагаются непосредственно на территории сенсорного поля, а во втором сценарии клонированная сеть образует новое поле (рисунок 1.9), располагающееся в непосредственной близости от легального сенсорного поля. Второй сценарий должен найти широкое применение для летающих сенсорных сетей.

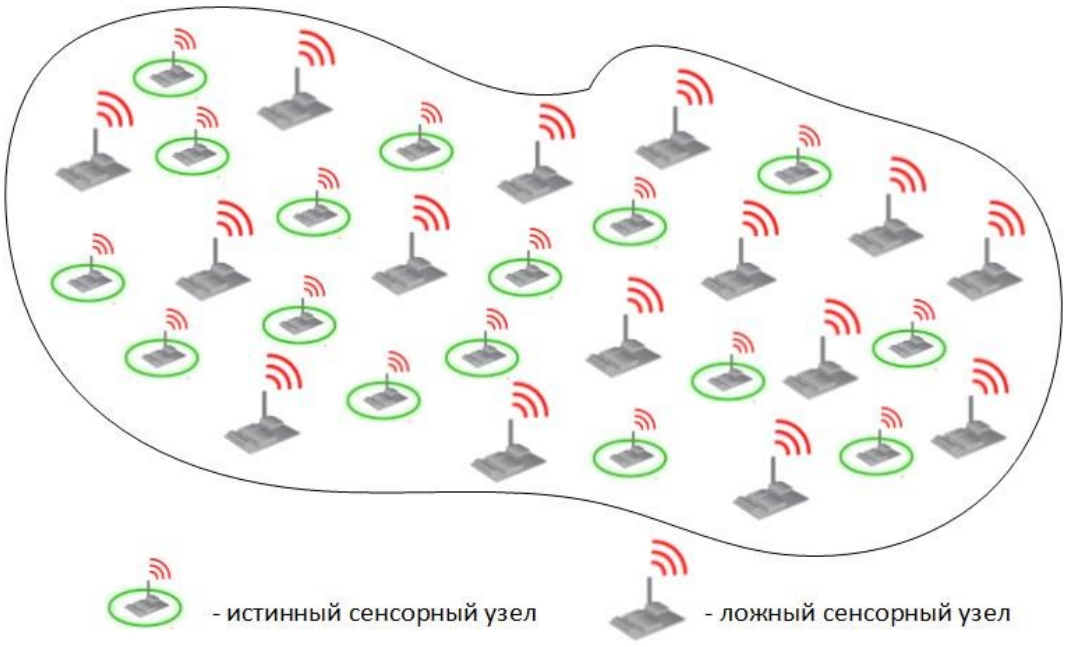

Рисунок 1.8 - Клонирование сенсорного поля или его фрагмента на территории легального поля

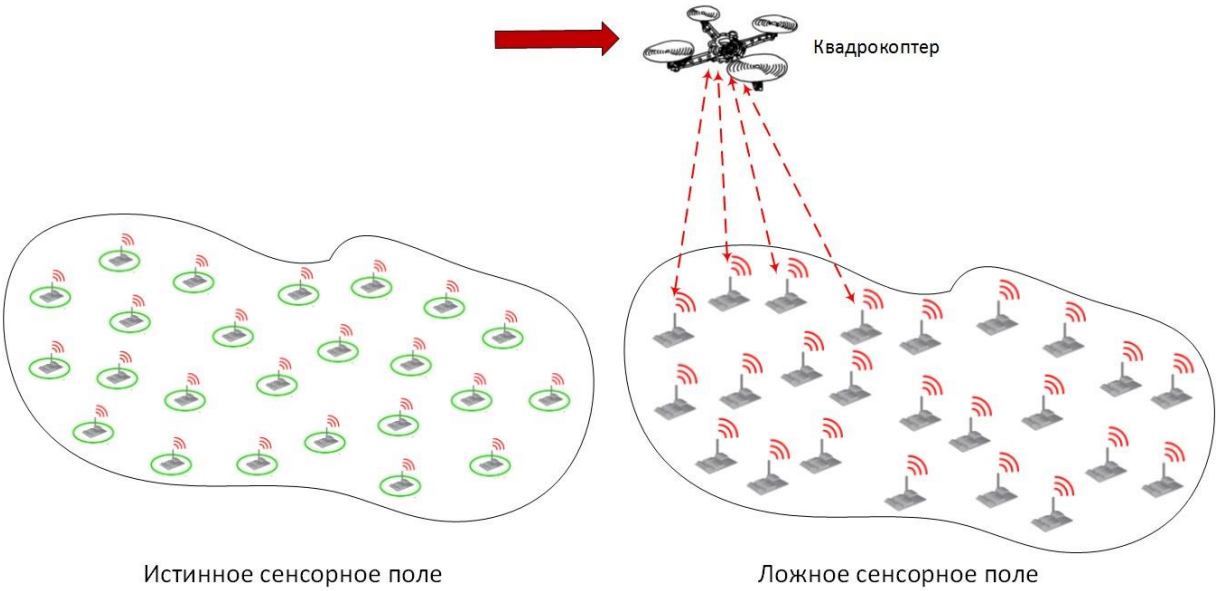

Рисунок 1.9 - Клонирование сенсорного поля или его фрагмента путем создания клонированного поля в непосредственной близости от легального.

Для выявления клонированных сенсорных полей или их фрагментов можно использовать характеристики трафика, циркулирующего в сети или, например, уже упоминавшийся метод создания уникальных паттернов.

1.6. Выводы

1. Развитие сетей связи в среднесрочной и долгосрочной перспективе будет осуществляться на основе концепции Интернета Вещей. Технологической основой для реализации концепции Интернета Вещей в настоящее время являются беспроводные сенсорные сети.

2. Беспроводные сенсорные сети обладают целым рядом особенностей по сравнению с существующими сетями, ключевой из которых является их самоорганизация. Важнейшими характеристиками беспроводных сенсорных сетей

являются длительность жизненного цикла и остаточная энергия. Особенности, присущие беспроводным сенсорным сетям, определяют новые проблемы обеспечения сетевой безопасности для этих сетей.

3. Предложен новый вид вторжений в беспроводные сенсорные сети – создание потоков ложных событий с целью уменьшения длительности жизненного цикла сети за счет воздействия на ее энергетическую систему. Сформулированы основные задачи для решения в диссертационной работе, а именно:

- разработка модели вторжения в сенсорные сети для потоков ложных событий;

- исследование воздействия на жизненный цикл беспроводной сенсорной сети пуассоновского и детерминированного потоков ложных событий;

- исследование воздействия на жизненный цикл беспроводной сенсорной сети скорости перемещения сенсорных узлов;

- определение структурных характеристик беспроводной сенсорной сети для выявления ложных событий с заданной вероятностью обнаружения;

- разработка структурного метода защиты беспроводной сенсорной сети от потоков ложных событий.

4. Предложена классификация ложных структур для Интернета Вещей, где наряду с потоками ложных событий рассматриваются ложные облака и клонированные интернет вещи. Дано определение ложных облаков и рассмотрены примеры клонирования сенсорных полей. Приведены основные характеристики ложных облаков и клонирования для Интернета Вещей.

ГЛАВА 2
РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛИ ПОТОКОВ ЛОЖНЫХ СОБЫТИЙ

2.1. Виды потоков трафика в беспроводных сенсорных сетях

Как и для всех сетей связи, для беспроводных сенсорных сетей важнейшее значение имеют параметры трафика [41, 42]. Модели трафика в теории телетрафика представляются в соответствии с классификацией Кендалла-Башарина [18]. При этом простейшая модель выглядит следующим образом: M/M/1. Первое обозначение определяет вид потока, M в приведенном примере соответствует пуассоновскому или простейшему потоку. Вторая буква характеризует закон, по которому осуществляется обслуживание вызовов, пакетов, событий и т.д. Здесь M соответствует экспоненциальному закону обслуживания. Наконец, последнее обозначение характеризует ресурсы системы, а в данном конкретном примере соответствует однолинейной системе или системе с одним обслуживающим прибором. Пуассоновские потоки и экспоненциально распределенная длительность обслуживания долгое время и с достаточной для практик степенью точности использовались для представления и расчетов в телефонных сетях связи общего пользования. С появлением же пакетных сетей связи общего пользования NGN для услуг передачи данных и видео оказалось, что циркулирующие в сети потоки достаточно часто являются самоподобными [45].

Первые наблюдения самоподобных потоков относятся к середине 90-х годов прошлого века, когда I.Norros [97] выявил наличие самоподобия потоков при передаче файлов. Чуть позже этому явлению в сетях связи было дано и теоретическое обоснование [121], а самоподобные свойства нашли и для потоков видео [45, 81, 85], и для электронной почты [76], и для трафика WEB-приложений

[65], и для трафика Skype [94]. При этом следует отметить, что для трафика речи, даже в условиях сети All over IP, поток трафика оставался пуассоновским [57, 99]. Самоподобными потоками в соответствии с [18] называются такие потоки, для которых функции распределения исходного и агрегированных потоков одинаковы. Степень самоподобия при этом оценивают с помощью параметра (коэффициента) Херста H. Поток относится к самоподобным, если $0.5<H<1$. При $H=0.5$ поток является пуассоновским, а при $H=1$ называется детерминированным. Степень самоподобия показывает, насколько самоподобный поток фрактален, т.е. как часто в этом потоке повторяются те или иные предыдущие характеристики потока. При этом максимальное самоподобие достигается в случае детерминированного потока, а при пуассоновском потоке самоподобие отсутствует полностью. С учетом изложенного считают, что поток обладает малой степенью самоподобия, если $0.5<H<0.65$, средней степенью самоподобия, если $0.65<H<0.75$ и высокой степенью самоподобия, если $0.75<H<1$.

Первые работы по изучению трафика беспроводных сенсорных сетей и его характеристик относятся к началу второго десятилетия 21 века. Все эти работы посвящены исследованию характеристик потоков трафика, поскольку в беспроводных сенсорных сетях для передачи информации, как правило, достаточно одного пакета и длительность его обработки представляется распределенной по детерминированному закону. Кроме того, число сенсоров даже на одном сенсорном поле может быть так велико, что ресурсы сенсорного поля для обработки пакетов представляются практически неограниченными. Естественно, что все это относится к сенсорному полю, в котором все сенсорные узлы в момент времени t работоспособны и имеют достаточный энергетический запас для обработки информации. Поэтому, до настоящего времени основные исследования в области моделей трафика для беспроводных сенсорных сетей были сосредоточены в области потоков трафика и их характеристик [31, 87, 88, 89, 90, 19].

В работе [87] было доказано, что трафик для беспроводных сенсорных сетей, задачей которых является сбор телеметрической информации, имеет

самоподобный характер. При этом, если для трафика телеметрии наблюдается средняя степень самоподобия (H=0.68), то трафик сигнализации имеет высокую степень самоподобия (H=0.82). Для трафика медицинских сетей в [88] значение параметра Херста H=0.66, что близко к низкой степени самоподобия для такого трафика. В исследованиях в области беспроводных сенсорных сетей слежения за целью при линейном ее движении [119] значение параметра Херста составило около H= 0.8. Это соответствует среднему уровню самоподобия. В работах по изучению потоков трафика передачи изображений в беспроводных сенсорных сетях степень самоподобия изменялась от средней для черно-белых изображений до высокой при передаче трафика цветных изображений [89]. Таким образом, потоки трафика в беспроводных сенсорных сетях весьма разнообразны. Исходя из проведенного анализа, представляется целесообразным при исследованиях воздействия на беспроводные сенсорные сети потоков ложных событий использовать как пуассоновский поток, так и детерминированный, что позволит перекрыть все указанные выше значения параметра Херста для потоков трафика.

Для оценки качества функционирования беспроводных сенсорных сетей помимо таких известных параметров, как потери, задержки и т.п., используется несколько новых параметров. Два из них тесно взаимосвязаны между собой – это длительность жизненного цикла и остаточная энергия. В беспроводных сенсорных сетях зачастую может отсутствовать возможность восстановления затраченной на функционирование сети энергии и, поэтому, длительность жизненного цикла и остаточная энергия являются важными оценками качества функционирования для таких сетей. Однако длительность жизненного цикла не всегда зависит только от остаточной энергии. Как уже отмечалось выше, беспроводные сенсорные сети достаточно часто используются для мониторинга пространства, внешней среды, производственных процессов и т.п. При этом важнейшим параметром является доля покрытия пространства, позволяющая получать информацию в необходимом и достаточном объеме. Поэтому, для таких задач длительность жизненного цикла определяют как длительность, в течение которой беспроводная сенсорная сеть обеспечивает заданную долю покрытия

пространства, несмотря на число сенсорных узлов, продолжающих выполнять свои функции [66, 86]. В задачах слежения за целью жизненный цикл может определяться как длительность функционирования беспроводной сенсорной сети, в течение которой сенсорные узлы обеспечивают обнаружение цели с заданной вероятностью [10].

В последующих исследованиях для определения воздействия различных потоков ложных событий на беспроводную сенсорную сеть будет использоваться наиболее общая модель, когда длительность жизненного цикла сети определяется по моменту гибели последнего сенсорного узла. При определения оптимальной плотности сенсорных узлов для защиты беспроводной сенсорной сети от потока ложных событий в 3-ей 4-ой главах длительность жизненного цикла определяется как для сетей слежения за целью, т.е. как длительность функционирования беспроводной сенсорной сети, в течение которой сенсорные узлы обеспечивают обнаружение цели с заданной вероятностью.

2.2 Модель вторжения в сенсорные сети потоков ложных событий

По результатам раздела 2.1 для исследования вторжений потоков ложных событий в сенсорные сети будем использовать модель сети, на которую поступает пуассоновский или детерминированный поток ложных событий. Кроме того, длительность жизненного цикла исследуемой сети, а это – основной параметр, который требуется найти в процессе исследований, - определяется моментом гибели последнего сенсорного узла.

В последние годы достаточно много внимания уделяется мобильным беспроводным сенсорным сетям MWSN (Mobile Wireless Sensor Networks) [56, 82, 86]. Поэтому, в модели вторжения в сенсорные сети потоков ложных событий наряду со стационарными сенсорными узлами будут рассмотрены и мобильные

сенсорные узлы. В исследованиях по MWSN скорость перемещения сенсорного узла составляет, как правило, 2 м/с. Это значение скорости соответствует быстро идущему пешеходу. В качестве базовой такое значение скорости и будем использовать в модели. В классификации самоорганизующихся сетей важное место занимают мобильные Ad Hoc сети MANET (Mobile Ad Hoc Networks) [38,112], которые отличаются от MWSN как по числу узлов в сети, так и по скорости перемещения узлов. Для MANET скорость перемещения выбирается от 8-10 м/с (средняя скорость автомобиля в городских условиях) и выше, что определяется приложениями MANET, такими как целевые автомобильные сети VANET(Vehicular Ad Hoc Networks). Диапазон скоростей от 2 м/до 8 м/с как пограничный между MWSN и MANET, также будет рассмотрен в модели, но для MWSN основным значением скорости перемещения сенсорного узла является 2 м/с.

Беспроводные сенсорные сети могут быть гомогенными и гетерогенными. Поскольку сенсорные узлы являются достаточно простыми устройствами, то, как правило, в исследованиях сенсорных сетей используют понятие гомогенной сети, состоящей из множества сенсорных узлов с одинаковыми исходными характеристиками, такими как радиус действия сенсорного узла, начальная энергия, затраты энергии на передачу информации и т. п. В разрабатываемой модели сенсорная сеть будет рассматриваться как гомогенная.

Как уже отмечалось в первой главе, с целью увеличения остаточной энергии и длительности жизненного цикла сенсорных сетей при их построении используются различные алгоритмы кластеризации. Наиболее известным и широко применяемым в исследованиях по беспроводным сенсорным сетям является алгоритм LEACH (Low Energy Adaptive Cluster Hierarchy). В основе использования алгоритма LEACH лежит правило, в соответствии с которым сенсорный узел, который был головным в предыдущем цикле жизни сенсорной сети, не может быть им в текущем цикле. Такое, простое на первый взгляд, правило обеспечивает увеличение жизненного цикла беспроводной сенсорной сети в 7 раз по сравнению со случайным выбором головного узла. Для мобильных

сенсорных сетей была разработана модификация алгоритма LEACH, имеющая название LEACH-M. Для проводимого исследования, в котором участвуют и стационарные, и мобильные сенсорные узлы, нет принципиальной разницы в использовании LEACH или LEACH-M для мобильных узлов. Поэтому, далее при кластеризации исследуемой сети во всех случаях используется алгоритм LEACH.

Как и во всех типовых моделях беспроводных сенсорных сетей [73, 74, 75, 86], радиус действия сенсорного узла принимается равным 25 м, запас энергии в каждом узле – 2Дж, расход энергии на прием - 50 нДж/бит, на передачу – 50 нДж/бит и дополнительно 100 пДж/кв.м. Расположение шлюза выбирается в центре плоскости, а ее размер - 200×200 м. При моделировании, как это принято для сенсорных сетей, длительность жизненного цикла сенсорной сети измеряется в раундах или итерациях [73, 74, 75, 86]. При этом одна итерация равна 1 секунде, а соотношение между раундами и итерациями 1:5 (в одном раунде 5 итераций). Период, в течение которого исследуется жизненный цикл беспроводной сенсорной сети, как и в базовой работе по LEACH выбран длительностью 1000с. Заметим, что головной узел подлежит ротации в каждом раунде.

Таким образом, для исследования вторжений потоков ложных событий на беспроводную сенсорную сеть разработана следующая модель [5, 9, 60]. 100 мобильных узлов распределены изначально случайным образом на плоскости размером 200 на 200 метров. Радиус действия сенсорного узла – 25 м, средняя скорость от 2 м/с (быстро идущий пешеход) до 10 м/с (автомобиль в городских условиях) запас энергии в каждом узле – 2Дж, расход энергии на прием - 50 нДж/бит, на передачу – 50 нДж/бит и дополнительно 100 пДж/кв.м. Все сенсорные узлы однородны, т.е. имеют одинаковый радиус действия и начальные энергетические характеристики. В соответствии с практикой использования алгоритма LEACH доля головных узлов предопределена в количестве 5% от общего числа сенсорных узлов. Шлюз расположен в центре сети.

На указанную сеть воздействуют вторжения в виде потоков ложных событий. Исследуется и сравнивается воздействие пуассоновского и детерминированного потоков. Значения параметров жизненного цикла атакуемой

сенсорной сети для самоподобных потоков с параметром Херста от 0.5 (пуассоновский поток) до 1 (детерминированный поток) будут находиться внутри интервала полученных значений для пуассоновского и детерминированного потоков. Интенсивность потока ложных событий изменяется в пределах от одного до 10 событий в секунду. Скорость перемещения подвижных сенсорных узлов в модели варьируется в пределах от 2 м/с до 10 м/с. Ложные события материализованы в виде ложных объектов, проникающих на территорию сенсорной сети. При обнаружении ложного объекта сенсорным узлом информация о ложном событии передается на шлюз и этот объект уничтожается.

Исследования проводятся методом имитационного моделирования, программное обеспечение написано на языке C#.NET.

На рисунках 2.1-2.4 приведены экранные формы, иллюстрирующие исходное состояние сети, процесс ее кластеризации, состояние сети с половиной живущих узлов и состояние сети перед гибелью последних узлов. Ложные объекты, занимающие все большее пространство сенсорного поля по мере гибели сенсорных узлов, изображены черными точками, головные узлы – зеленым цветом, сенсорные узлы – члены кластера – розовым цветом.

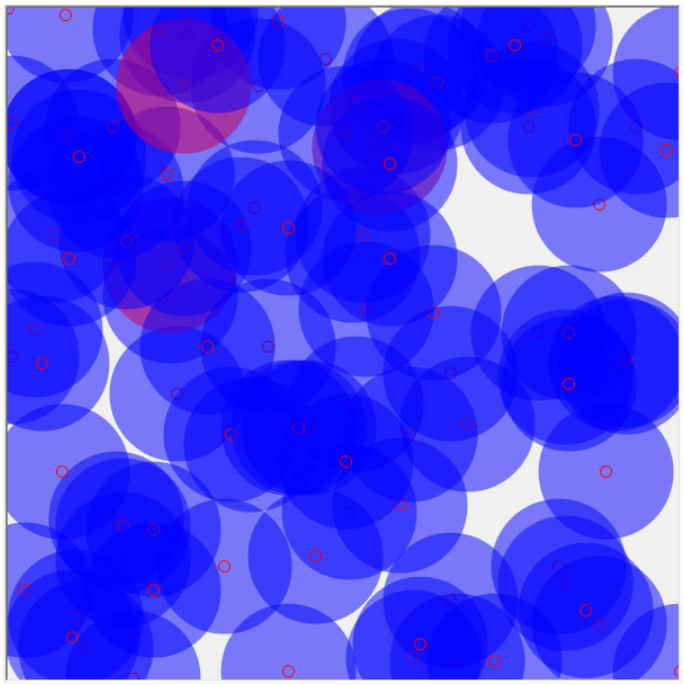

Рисунок 2.1 - Сенсорное поле до кластеризации

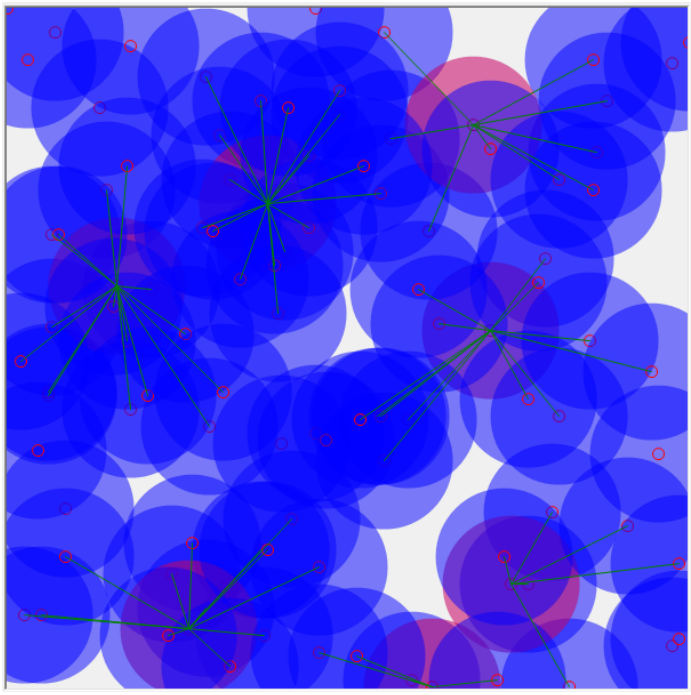

Рисунок 2.2 - Кластеризованная беспроводная сенсорная сеть

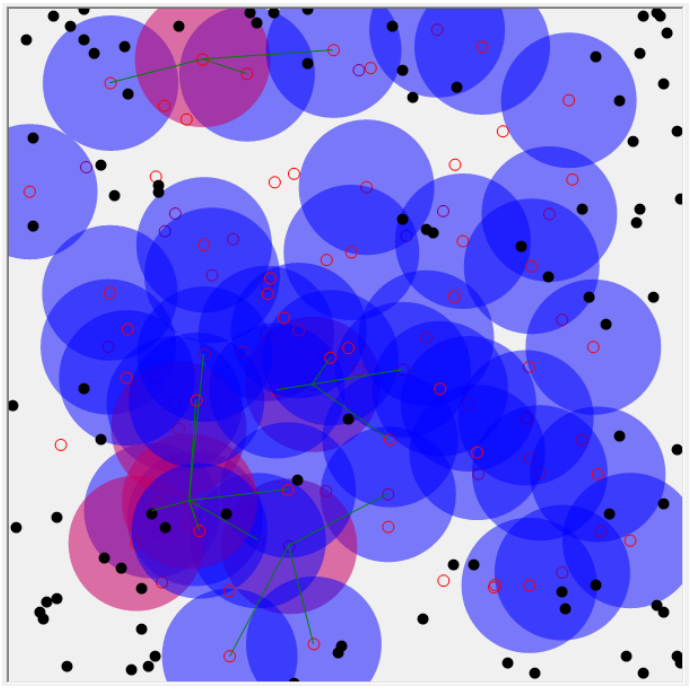

Рисунок 2.3 - Сенсорное поле с половиной живых узлов

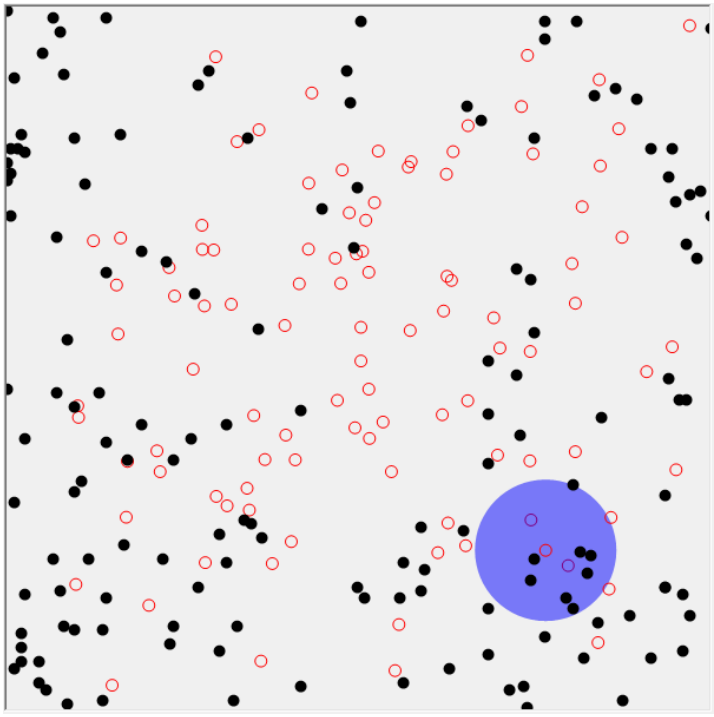

Рисунок 2.4 - Сенсорное поле перед гибелью последнего сенсорных узлов

2.3 Характеристики жизненного цикла беспроводной сенсорной сети при воздействии различных потоков ложных событий

На рисунке 2.5 представлены результаты моделирования для пуассоновского потока ложных событий при различной его интенсивности и различных значениях скорости перемещения сенсорных узлов. Анализ результатов, приведенных на рис.2.5, показывает, что потоки ложных событий могут в существенной степени уменьшать длительность жизненного цикла беспроводной сенсорной сети [5, 7, 9, 60].

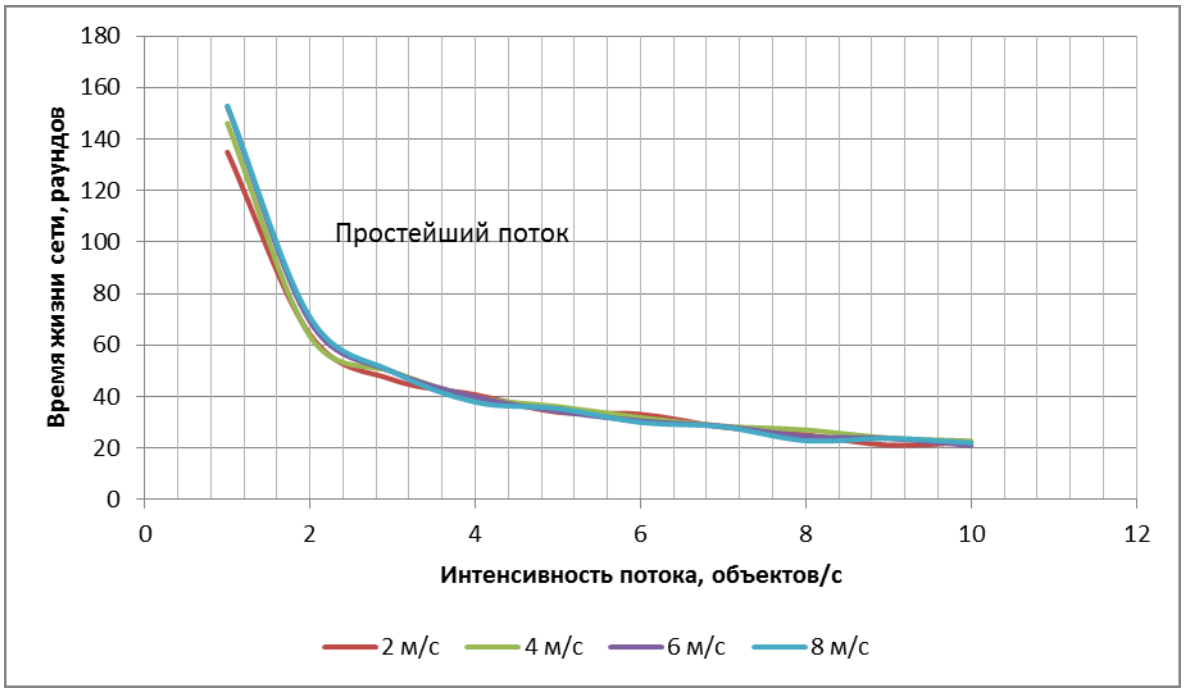

Рисунок 2.5 - Длительность жизненного цикла беспроводной сенсорной сети при воздействии пуассоновского потока и различных значениях скорости перемещения сенсорных узлов.

Увеличение интенсивности поступающего потока от одного события в секунду до двух приводит к уменьшению длительности жизненного цикла беспроводной сенсорной сети более чем в 2 раза. Однако при дальнейшем увеличении интенсивности потока до 4-х, 6-и и т.д. ложных событий в секунду, уменьшение длительности жизненного цикла сенсорной сети уже не так существенно в численном выражении. Влияние скорости перемещения объекта наблюдается в области интенсивности потока ложных событий в 1-2 м/с. Этот эффект будет подробно исследован в разделе 2.4.

На рисунке 2.6 представлено сравнение длительности жизненного цикла пуассоновского и детерминированного потоков при скорости перемещения сенсорных узлов 2 м/с. Как видим, для детерминированного потока при интенсивности потока до 4-х, 6-и и т.д. ложных событий в секунду, уменьшение длительности жизненного цикла сенсорной сети не так существенно в численном выражении, как и для пуассоновского. Мало того, уменьшение длительности

жизненного цикла беспроводной сенсорной сети при таких значениях интенсивности потока ложных событий практически не зависит от вида потока.

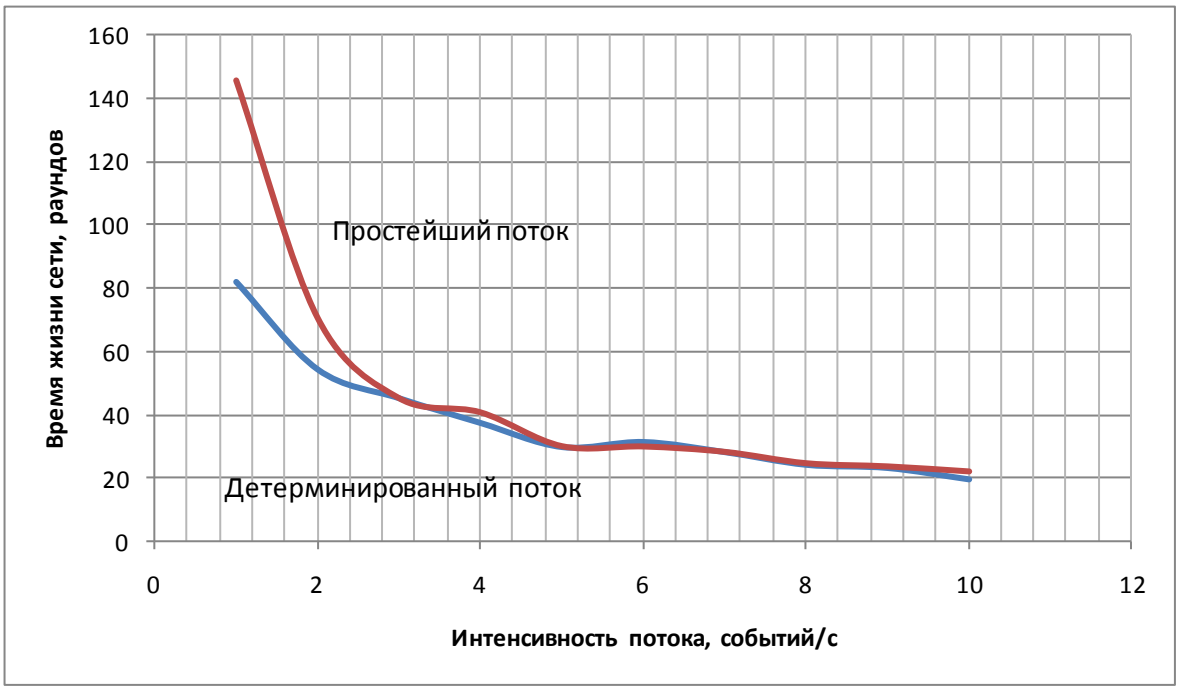

Рисунок 2.6 - Сравнение длительности жизненного цикла пуассоновского и детерминированного потоков при скорости перемещения сенсорных узлов 2 м/с.

В области же интенсивности потока ложных событий менее 2 м/с детерминированный поток ложных событий в более существенной степени снижает длительность жизненного цикла сенсорной сети, чем пуассоновский. Это явление можно использовать при планировании вторжений в беспроводные сенсорные сети методом создания потоков ложных событий.

2.4 Метод защиты беспроводных сенсорных сетей от потоков ложных событий путем придания сенсорным узлам мобильности

Как уже отмечалось выше, для пуассоновского потока при моделировании было выявлено влияние скорости перемещения сенсорных узлов на длительность жизненного цикла беспроводной сенсорной сети при интенсивности потока ложных событий в районе одного события в секунду. На рисунке 2.7 представлены результаты моделирования для пуассоновского потока ложных событий с интенсивностью 1 событие/с и различных скоростей перемещения объектов [5, 60]. Анализ результатов моделирования показывает, что придание сенсорным узлам мобильности до 2 м/с, что соответствует исследуемой области мобильных сенсорных сетей WMSN, может существенно, до двух раз, приводить к увеличению остаточной энергии в течение жизненного цикла беспроводной сенсорной сети.

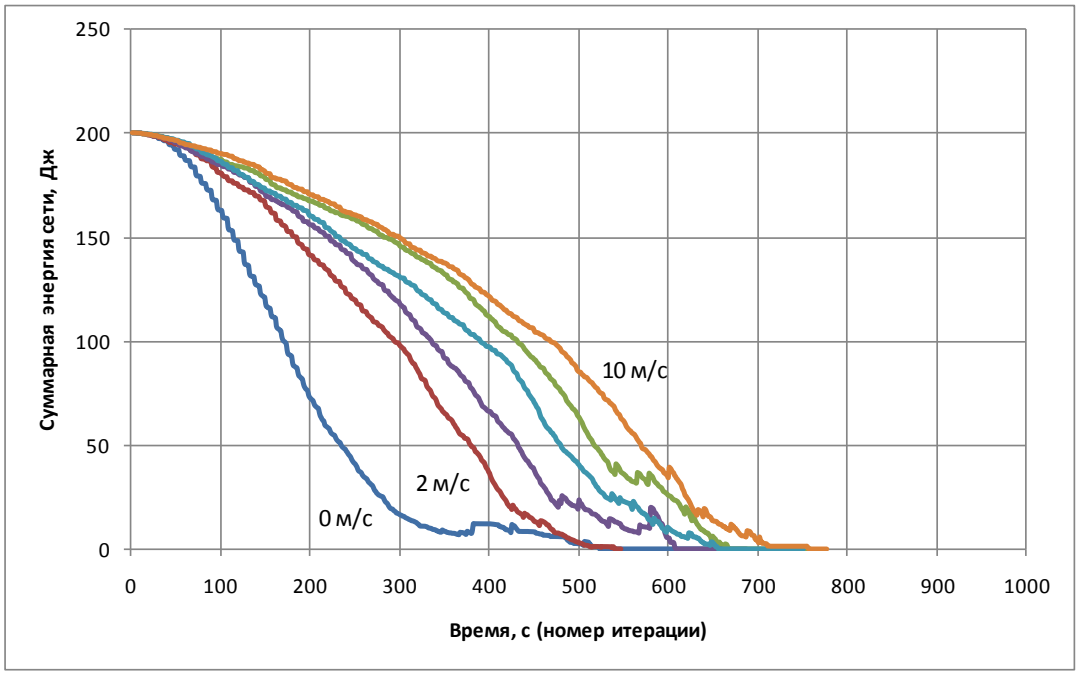

Рисунок 2.7 - Остаточная энергия для пуассоновского потока ложных событий с интенсивностью 1 событие/с и различных скоростей перемещения объектов

Дальнейшее увеличение скорости перемещения объектов, вплоть до используемых скоростей в сетях MANET, также может привести к экономии остаточной энергии, но уже не в столь существенной степени.

На рис.2.8 приведена аппроксимация результатов моделирования функцией вида:

$$E(t) = \frac{n}{1 + e^{\frac{t - t_0}{K}}} \tag{2.1}$$

где

n – начальное число узлов;

t_0 – точка полуперегиба;

K – коэффициент (характеризует скорость уменьшения числа узлов).

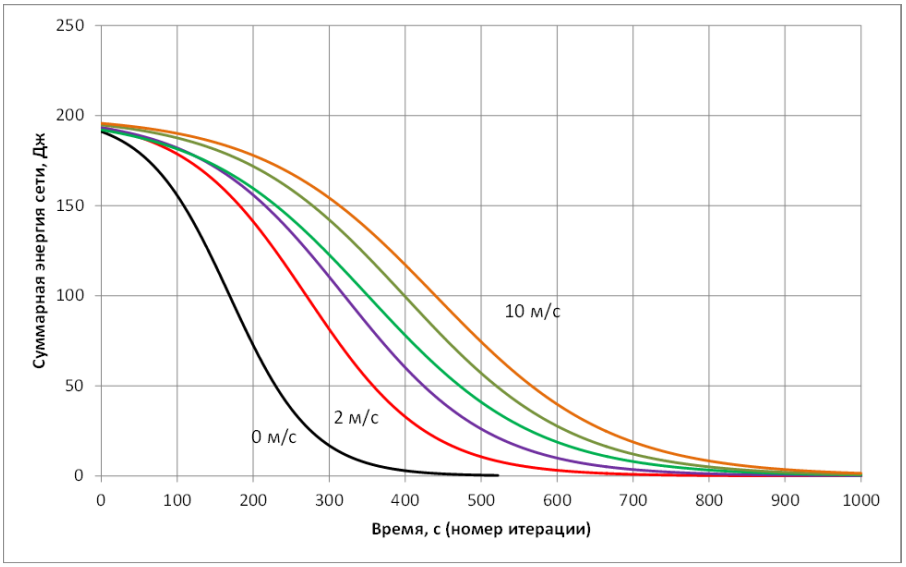

Рис.2.8. Аппроксимация результатов имитационного моделирования

На рисунке 2.9 и рисунке 2.10 приведены зависимости длительности жизненного цикла беспроводной сенсорной сети при воздействии потоков ложных событий с различной интенсивностью от 1 м/с до 10 м/с в зависимости от скорости перемещения сенсорных узлов для пуассоновского и детерминированного потоков соответственно [60].

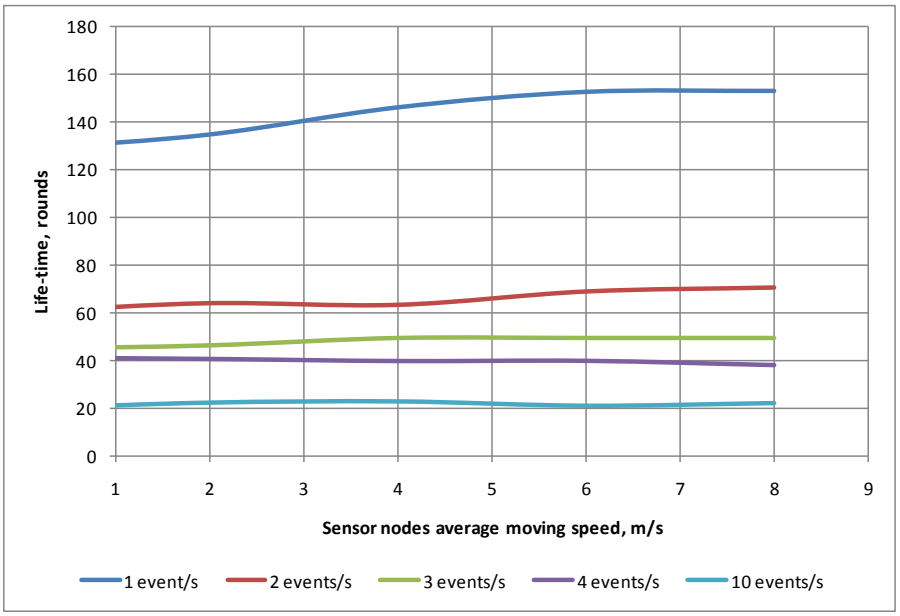

Рисунок 2.9 - Длительность жизненного цикла беспроводной сенсорной сети при воздействии потоков ложных событий с различной интенсивностью от 1 м/с до 10 м/с в зависимости от скорости перемещения сенсорных узлов. Пуассоновский поток.

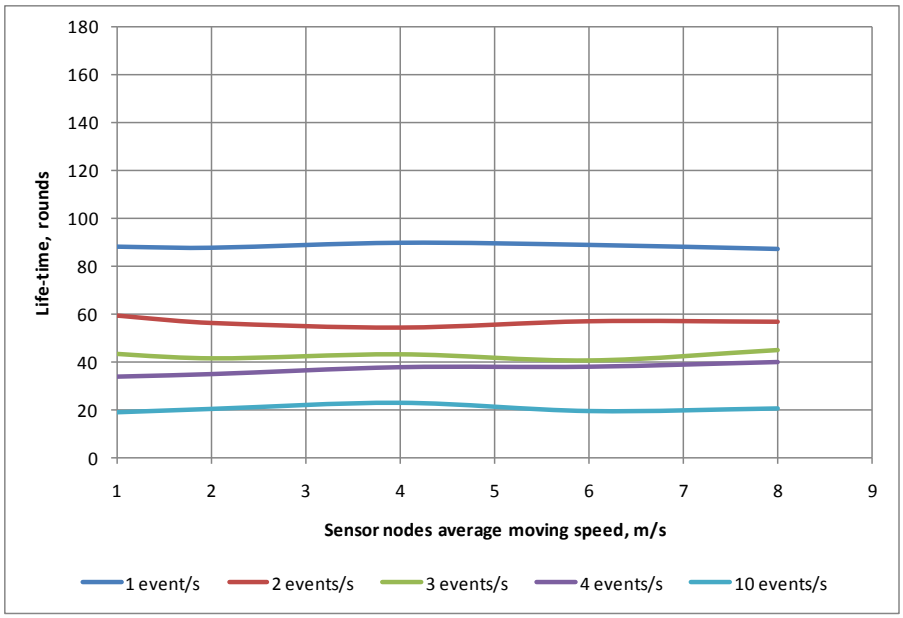

Рисунок 2.10 - Длительность жизненного цикла беспроводной сенсорной сети при воздействии потоков ложных событий с различной интенсивностью от 1 м/с до 10 м/с в зависимости от скорости перемещения сенсорных узлов. Детерминированный поток.

Анализ результатов моделирования показывает, что остаточную энергию и жизненный цикл беспроводной сенсорной сети при воздействии потоков ложных событий можно увеличить, если придать сенсорным узлам мобильность со скоростью 2 м/с (скорость быстро идущего пешехода). Это утверждение справедливо при интенсивности потока ложных событий в 1 событие/с. При увеличении интенсивности потока ложных событий влияние скорости перемещения сенсорного узла нивелируется. Для интенсивности потока ложных событий в 1 событие/с жизненный цикл беспроводной сенсорной сети может быть увеличен и при более высоких скоростях вплоть до 10 м/с.

2.5 Выводы

1. Анализ потоков трафика в беспроводных сенсорных сетях показывает, что трафик имеет самоподобный характер с параметром Херста, зависящим от приложения и изменяющимся в широких пределах. Последнее требует проведения исследований вторжений потоков ложных событий в беспроводные сенсорные сети для пуассоновского и детерминированного потоков, что позволяет перекрыть всю область изменения вида потоков.

2. Разработана модель вторжения в беспроводную сенсорную сеть с целью уменьшения ее жизненного цикла, отличающаяся от известных тем, что для достижения данной цели используются потоки ложных событий. Модель разработана на основе типовых геометрических, количественных и энергетических параметров беспроводных сенсорных сетей с использованием базового алгоритма кластеризации для гомогенной мобильной сенсорной сети при вторжении в сеть пуассоновского и детерминированного потоков ложных событий.

3. Выявлено в отличие от известных результатов, что длительность жизненного цикла беспроводной сенсорной сети может существенно зависеть от

вида потока ложных событий и при прочих равных условиях при воздействии детерминированного потока может быть почти в два раза меньше, чем при воздействии пуассоновского.

4. Установлено в отличие от известных результатов, что остаточную энергию и длительность жизненного цикла беспроводной сенсорной сети при воздействии потоков ложных событий можно увеличить, если придать сенсорным узлам мобильность со скоростью 2 м/с (скорость быстро идущего пешехода).

ГЛАВА 3
СТРУКТУРНЫЕ ХАРАКТЕРИСТИКИ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ ДЛЯ ВЫЯВЛЕНИЯ ЛОЖНЫХ СОБЫТИЙ С ЗАДАННОЙ ВЕРОЯТНОСТЬЮ ОБНАРУЖЕНИЯ

3.1 Статичная модель беспроводной сенсорной сети и анализ ее основных характеристик

Существует достаточно много работ, посвященных проблемам защиты сенсорных сетей от разнообразных вторжений [4, 53, 58, 59, 96]. Однако в области защиты беспроводных сенсорных сетей от потоков ложных событий пока не было предложено эффективных методов. Как справедливо отмечено в известной книге [44], проблемы защиты сетей, построенных на узлах с ограниченными возможностями, затруднены тем обстоятельством, что внедрение сложных систем защиты от вторжений практически невозможно из-за ограничений энергетической системы сенсорных сетей и параметров сенсорных узлов.

Обнаружение ложных событий в сенсорной сети можно рассматривать как задачу слежения за целью [119], с той лишь разницей, что в задачах по борьбе с вторжениями источник ложного события при его обнаружении уничтожается. В задачах слежения за целью в сенсорных сетях [68, 72, 92] выделяют следующие возможности для обеспечения требуемых характеристик слежения:

- использование сетевой архитектуры,
- использование специальных алгоритмов,
- использование специальных сенсоров,
- варьирование числа целей,
- использование специальных технологий.

С учетом низкой стоимости одного типового сенсорного узла, далее будем исследовать влияние плотности размещения сенсоров для выявления ложных событий с заданной вероятностью обнаружения.

Рассмотрим следующую модель сенсорной сети и поступающего потока ложных событий [8]:

- сенсорные узлы расположены на плоской поверхности, ограниченной прямоугольником *ABCD*, определяющим сенсорное поле;

- сенсорные узлы способны детектировать наличие ложного события в зоне действия сенсора, которая представляет собой круг радиуса *r*;

- с одной стороны сенсорного поля поступает детерминированный поток ложных объектов с интенсивностью λ и скоростью v;

- каждый из ложных объектов, попав в зону действия сенсорного узла, расценивается как событие, приводящее к генерации сообщения данным узлом сети;

- сообщение доставляется через сеть в центр обработки данных. Через некоторое время τ, после этого объект считается обнаруженным и исключается из дальнейшего рассмотрения;

- если на пути следования ложный объект не попадает в зону действия ни одного из узлов, то он беспрепятственно проходит через сенсорное поле.

Целью исследования данной модели является определение характеристик сенсорной сети, в первую очередь плотности размещения сенсорных узлов, обеспечивающих заданную вероятность обнаружения ложных событий.

Модель приведена на рисунке 3.1.

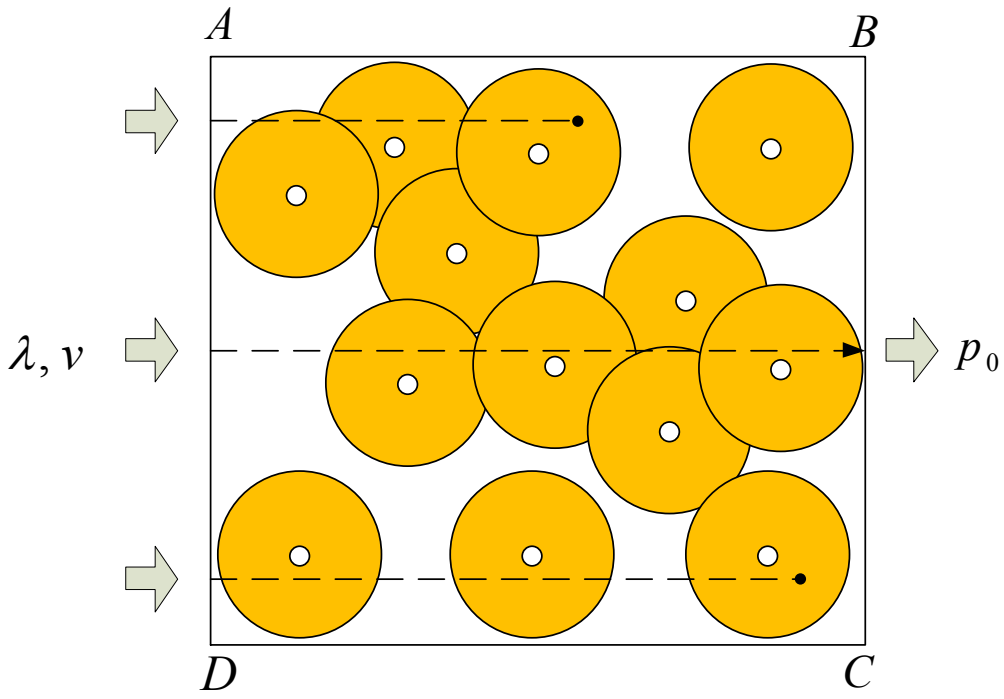

Рисунок 3.1 - Поток объектов в сенсорном поле

Рассмотрим далее поставленную задачу применительно к одному ложному объекту, а затем обобщим ее на произвольное число ложных объектов. Предположим, что траектория движения объекта – произвольная линия. Объект попадет в зону действия сенсора, если в прямоугольнике *abcd* расположен хотя бы один сенсорный узел сети. Таким образом, обнаружение объекта возможно, когда в фигуре *afgd* имеется хотя бы один сенсор.

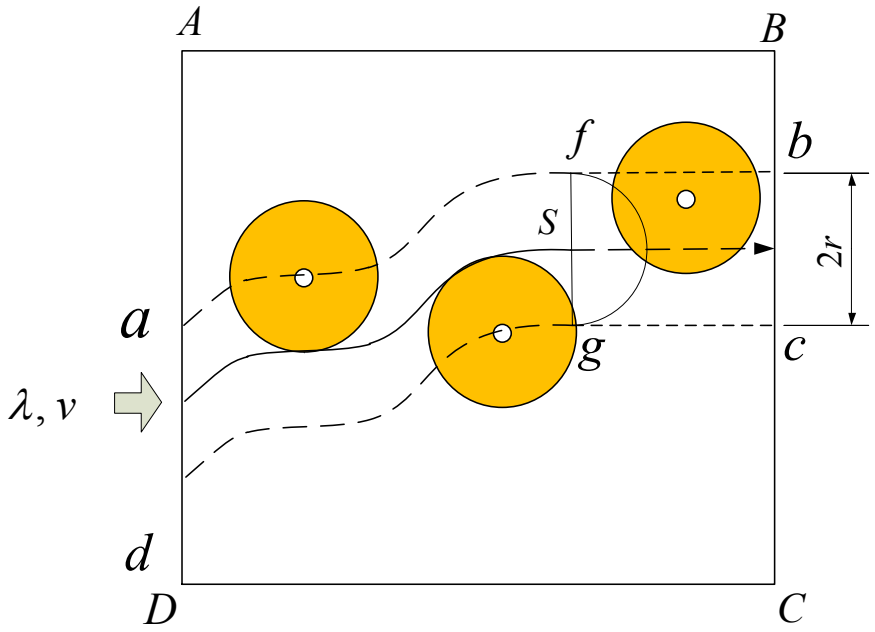

Рисунок 3.2 - Модель обнаружения объекта сенсорами.

Предположим, что узлы сети (сенсоры) образуют пуассоновское сенсорное поле точек на плоскости. Тогда, вероятность попадания в область площадью S заданного числа m точек (узлов) равна

$$p_m = \frac{a^m}{m!} e^{-a}, \qquad (3.1)$$

где $a = \rho \cdot S$;

ρ - число точек на единицу площади;

S - площадь области.

Вероятность того, что объект будет обнаружен в области *afgd,* определяется вероятностью того, что в данной области будет расположено не менее одного узла. Тогда с учетом (3.1) получаем:

$$p_d = p(m \geq 1) = 1 - p_0 = 1 - e^{-\rho \cdot S} \qquad (3.2)$$

В общем случае, площадь плоской фигуры *afgd* может быть вычислена как интеграл

$$S = \iint_G dxdy$$

где G - означает взятие интеграла по контуру фигуры *afgd.*

Легко заметить, что в случае равномерного распределения узлов сети по территории (пуассоновского поля) вероятность попадания узла в фигуру *afgd* будет тем меньше, чем меньше ее площадь. Следовательно, наименьшая вероятность обнаружения объекта будет в случае, когда траектория его движения имеет минимальную длину, т.е. лежит на прямой линии, перпендикулярной границам зоны обслуживания. Данный случай является наиболее «тяжелым» для сети с точки зрения вероятности обнаружения объекта. Поэтому, рассмотрим далее именно этот случай и определим зависимости между вероятностью обнаружения объекта и такими параметрами сети как радиус действия сенсорного узла и плотность расположения узлов на территории (рисунок 3.3).

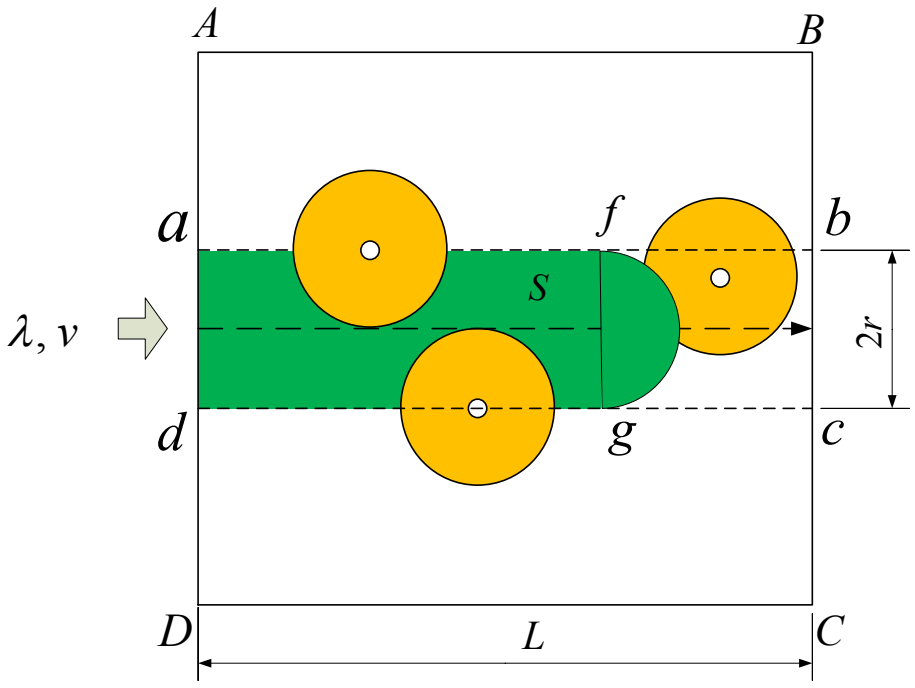

Рисунок 3.3 - Модель обнаружения объекта сенсорами.

Зависимость вероятности обнаружения объекта от параметров зоны обслуживания можно получить, выразив S через значения r, v, τ и L

$$S = 2r \cdot (L - v\tau) \tag{3.3}$$

$$p_d = 1 - e^{-2\rho \cdot r \cdot (L - v\tau)} \tag{3.4}$$

Считаем, что обнаружение объекта происходит, когда он попадает в зону действия первого встретившегося на пути сенсора. Функция распределения расстояния до ближайшего сенсора может быть определена как вероятность того, что в область *kmnq*, приведенную на рисунке 3.3, попадет хотя бы один сенсор.

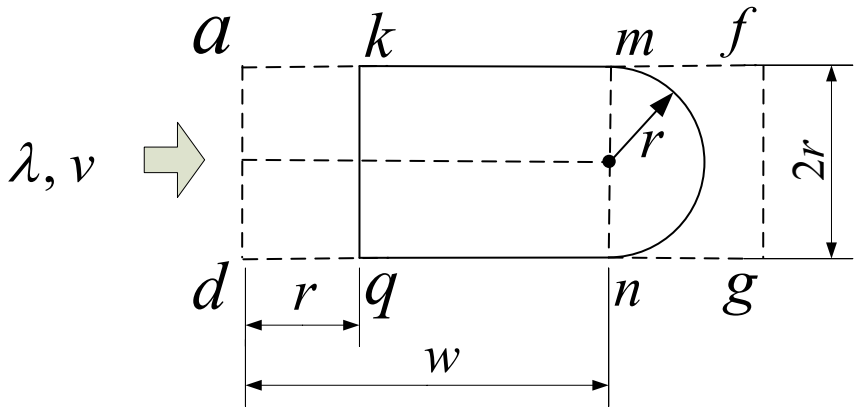

Рисунок 3.4 - Оценка расстояния до ближайшего сенсора.

Согласно свойствам пуассоновского поля эта вероятность равна

$$p_w = 1 - e^{-\rho \cdot W}, \tag{3.5}$$

где W - площадь фигуры *kmnq,* описывающей зону обнаружения объекта сенсорами сети.

Зависимость площади W от пройденного пути $W(w)$ на участке $0 \le w < r$ можно представить как

$$W_1(w) = r^2 \cdot \arccos\left(\frac{r-w}{r}\right) - (r-w)\sqrt{2rw-w^2} \tag{3.6}$$

На участке $w \geq r$ эта зависимость определяется следующим образом:

$$W_2(w) = 2r \cdot w + \frac{\pi \cdot r^2}{2} \tag{3.7}$$

$$F(w) = \begin{cases} 0 & w < 0 \\ 1 - e^{-\rho \cdot \left(r^2 \cdot \arccos\left(\frac{r-w}{r}\right) - (r-w)\sqrt{2rw-w^2} \right)} & 0 \leq w < r \\ 1 - e^{-\rho \cdot \left(2r \cdot w + \frac{\pi \cdot r^2}{2} \right)} & w \geq r \end{cases} \tag{3.8}$$

Тогда плотность вероятности расстояния, пройденного объектом до первого сенсора, будет равна

$$f(w) = \begin{cases} 0 & w < 0 \\ 2\rho \cdot \sqrt{2rw-w^2} \cdot e^{-\rho \cdot \left(r^2 \cdot \arccos\left(\frac{r-w}{r}\right) - (r-w)\sqrt{2rw-w^2} \right)} & 0 \leq w < r \\ 2\rho \cdot r \cdot e^{-\rho \cdot \left(2r \cdot w + \frac{\pi \cdot r^2}{2} \right)} & w \geq r \end{cases} \tag{3.9}$$

На рисунке 3.5 приведены функция распределения и плотность вероятности для значений расстояния до первого сенсора, который и обнаружит ложный объект.

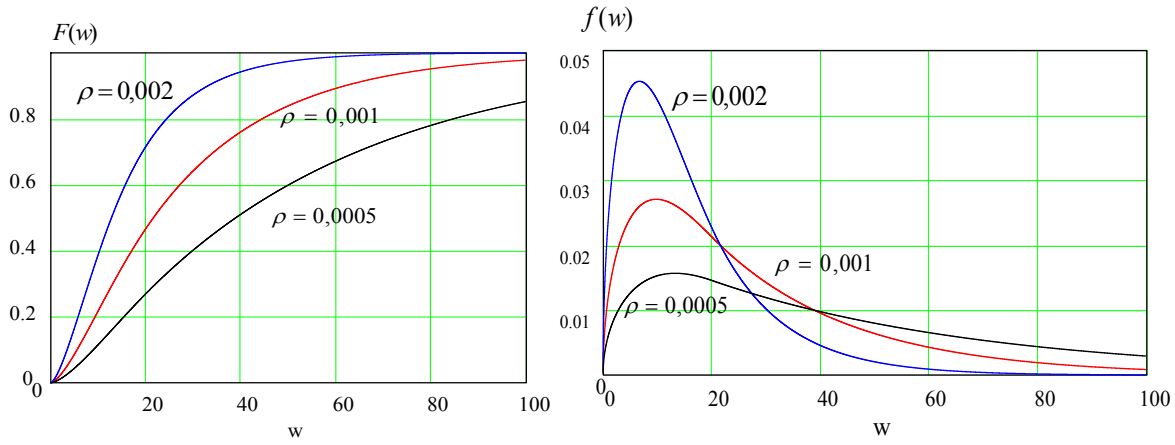

Рисунок 3.5 - Функция распределения и плотность вероятности расстояния до первого сенсора.

Математическое ожидание пройденного расстояния до первого сенсора (момента обнаружения) можно определить как

$$w_0 = \int_0^{\infty} w \cdot f(w) dw \qquad (3.10)$$

где $f(w)$ - функция плотности вероятности (3.9).

Выражение (3.10) не приводится к виду аналитической функции от переменных ρ и r.Поэтому, рассмотрим зависимость математического ожидания от плотности сенсоров и радиуса их действия $w_0(\rho, r)$, полученную численным методом (рисунок 3.6).

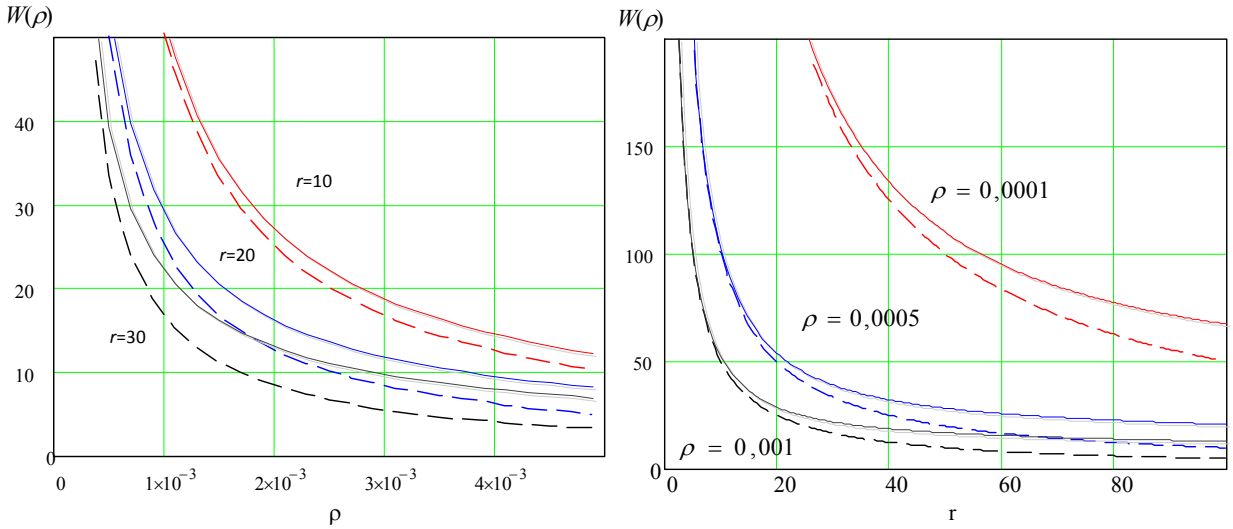

Рисунок 3.6 - Зависимость математического ожидания расстояния до обнаружения от плотности сенсоров и радиуса зоны сенсора

На рисунке 3.6 показаны зависимости, полученные согласно (3.10) (сплошные линии), и приблизительные оценки (пунктирные линии), полученные из выражения

$$\widetilde{w}_0 = \frac{1}{2 \cdot \rho \cdot r} \qquad (3.11)$$

Выражение (3.11) соответствует случаю, когда $w>>r$, т.е. при рассмотрении вероятности попадания узла сети в прямоугольник со сторонами $2r$ и w.

Как можно видеть из рисунка 3.6, выражение (3.11) дает некоторую ошибку в сторону занижения длины пути до обнаружения объекта. Величина этой ошибки в области практических значений ρ и r не превосходит 20%, что позволяет использовать (3.11) для практических расчетов.

Приближенное значение математического ожидания расстояния до первого сенсора можно получить также при допущении, что область обнаружения сенсора представляет собой квадрат, вписанный в круг радиуса r. Тогда,

$$\hat{w}_0 = \frac{1}{2}\sqrt{\frac{\pi}{\rho}} + \frac{e^{-\rho \cdot r^2}}{2\rho \cdot r}\left(1 + 2\rho \cdot r^2\right) \qquad (3.12)$$

По сравнению со значением математического ожидания, выражение (3.12) дает завышенную оценку математического ожидания.

Рассмотрим случай, когда требуется определить параметры сети, при заданной вероятности обнаружения объекта p_0. Выражение (3.8) дает возможность оценить вероятность того, что расстояние до первого сенсора не превысит некоторой величины Z.

$$p_0 = p(w < Z) = F(w) \qquad (3.13)$$

Из (3.8) и (3.13) при условии, что $w \geq r$, максимальное расстояние до обнаружения объекта при заданной вероятности обнаружения p_0 составит

$$Z(\rho, r, p_0) = r + \frac{1}{2}\left(\frac{p_0}{\rho \cdot r} - \frac{\pi \cdot r}{2}\right), \quad Z \geq r \qquad (3.14)$$

Выражение (3.14) дает возможность оценить требуемую длину зоны сенсорного поля для обеспечения гарантированного (с вероятностью p_0) обнаружения объекта.

Из (3.13) при тех же условиях можно получить выражение для выбора необходимой плотности сенсорного поля

$$\rho(Z, r, p_0) = \frac{p_0}{r \cdot \left(2(Z - r) - \frac{\pi \cdot r}{2}\right)}, \quad Z \geq r \qquad (3.15)$$

Аналогичным образом можно получить и выражение для радиуса действия сенсорного узла *r*.

$$r(Z,\rho,p_0)=\frac{\sqrt{2\rho\cdot\left(2\cdot Z^2+p_0(4-\pi)\right)}+2\rho\cdot Z}{\rho(4-\pi)},\quad Z\ge r \tag{3.16}$$

Если предположить, что объект пересекает сенсорное поле (как рассмотрено выше), размер которого выбран согласно (3.14), то на своем пути он попадет в зоны действия некоторого числа сенсоров. Математическое ожидание этого числа может быть получено из (3.14).

$$n_{\min}=2r\rho Z=2r\rho\cdot\left(r+\frac{1}{2}\left(\frac{p_0}{\rho\cdot r}-\frac{\pi\cdot r}{2}\right)\right) \tag{3.17}$$

Выражение (3.17) может быть использовано для оценки нижней границы числа сообщений (пакетов), передаваемых по сети, при пересечении сенсорного поля объектом по кратчайшему маршруту.

Верхнюю границу числа сообщений можно оценить, предположив что траектория движения объекта произвольна и не выходит за границу сенсорного поля, т.е. объект перемещается внутри поля до того момента, когда будет остановлен. Среднее значение расстояния, пройденного до момента обнаружения, оценим с помощью (3.11). Остальная часть расстояния определяется временем реакции на событие обнаружения объекта τ и скоростью перемещения объекта. Приближенная оценка среднего расстояния составит

$$\widetilde{w}=\frac{1}{2\rho\cdot r}+\tau\cdot v \tag{3.18}$$

Тогда среднее число сообщений может быть определено как

$$\widetilde{m}=\begin{cases}2r\rho\cdot W_{\max} & при\quad W_{\max}\le L\\ 2r\rho\cdot L & при\quad W_{\max}>L\end{cases}=\begin{cases}1+2r\rho\cdot\tau\cdot v & при\quad W_{\max}\le L\\ 2r\rho\cdot L & при\quad W_{\max}>L\end{cases} \tag{3.19}$$

Так как мы рассматриваем только зону обслуживания, то можно предположить, что $W_{\max} \le L$, т.е.

$$\tilde{m} = 1 + 2r\rho \cdot \tau \cdot v \qquad (3.20)$$

Обобщим полученные результаты на произвольное число ложных объектов. При этом будем считать, что:

-моменты поступления объектов в зону действия сети случайны и независимы;

-объекты перемещаются по случайным траекториям, представляющим собой прямые;

-интенсивность поступления объектов равна λ.

3.2 Динамическая модель, анализ числа сообщений, обслуживаемых сетью

Рассмотрим следующую модель. Ложные объекты движутся со стороны границы *AD* (рис.3.1). При этом точка, в которой объект входит в сенсорное поле, случайна, а величина y_{in} распределена равномерно на отрезке $[0; h]$ (рисунок 3.7). Аналогичными свойствами обладает и точка выхода объекта из сенсорного поля: величина y_{out} распределена равномерно на отрезке $[0; h]$.

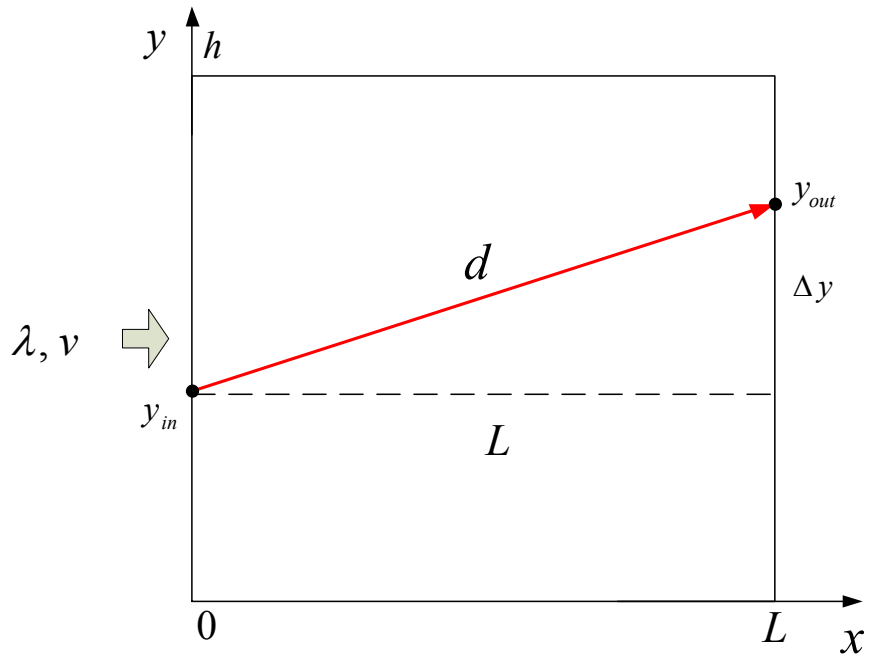

Рисунок 3.7 - Модель траектории движения объекта в сенсорном поле

Расстояние, пройденное объектом d, может быть вычислено следующим образом:

$$d = \sqrt{L^2 - (y_{out} - y_{in})^2} = \sqrt{L^2 - \Delta y^2} \qquad (3.21)$$

Так как величины y_{in} и y_{out} имеют равномерное распределение вероятности, то их разность Δy имеет распределение Симпсона (треугольное распределение) на интервале $[0; h]$

$$f(y) = \begin{cases} 0 & y < 0 \\ 2\dfrac{(h-y)}{h^2} & 0 \le y \le h \\ 0 & y > h \end{cases} \qquad (3.22)$$

Тогда плотность вероятности расстояния, пройденного объектом, можно определить как

$$f(w)=\begin{cases} 0 & w<L \\ \dfrac{2w}{h^2}\cdot\left(\dfrac{h}{\sqrt{w^2-L^2}}-1\right) & L\le w\le\sqrt{L^2+h^2} \\ 0 & w>\sqrt{L^2+h^2} \end{cases} \qquad (3.23)$$

Соответствующая плотность вероятности приведена на рисунке 3.8.

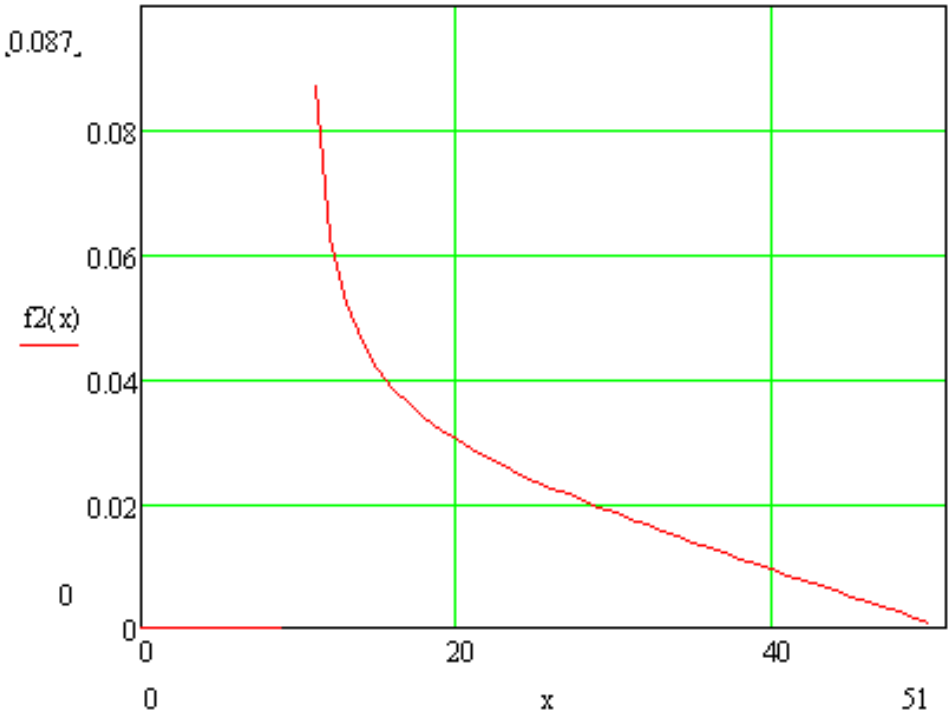

Рисунок 3.8 - Плотность вероятности расстояния, пройденного объектом

Из (3.23) можно определить математическое ожидание расстояния, пройденного объектом до пересечения границы сенсорного поля

$$\hat{w}=\sqrt{L^2+h^2}+\frac{L^2}{h}\ln\left(\frac{\sqrt{L^2+h^2}+h}{L}\right)+\frac{2}{3h^2}\left(L^3-\sqrt{\left(L^2+h^2\right)^3}\right) \qquad (3.24)$$

Проходя через сенсорное поле, объект попадает в зоны обнаружения некоторого числа узлов, в результате чего каждый из этих узлов производит

сообщение, которое передается по сети. Число производимых сообщений отражается на параметрах функционирования сети, так как при передаче сообщения узлы сети расходуют энергию, запас которой ограничен. Число узлов на пути объекта можно оценить на основе свойств сенсорного поля

$$\overline{m} = 2r\rho \cdot \hat{w} \tag{3.25}$$

С учетом (3.24) и (3.25) можно определить плотность вероятности числа передаваемых сообщений при прохождении объектом сенсорного поля как

$$f(m) = \begin{cases} 0 & m < 2L\rho r \\ \dfrac{m}{2(\rho r)^2 h^2} \cdot \left(\dfrac{h}{\sqrt{\left(\dfrac{m}{2\rho r}\right)^2 - L^2}} - 1 \right) & 2L\rho r \le m \le 2\rho r\sqrt{L^2 + h^2} \\ 0 & m > 2\rho r\sqrt{L^2 + h^2} \end{cases} \tag{3.26}$$

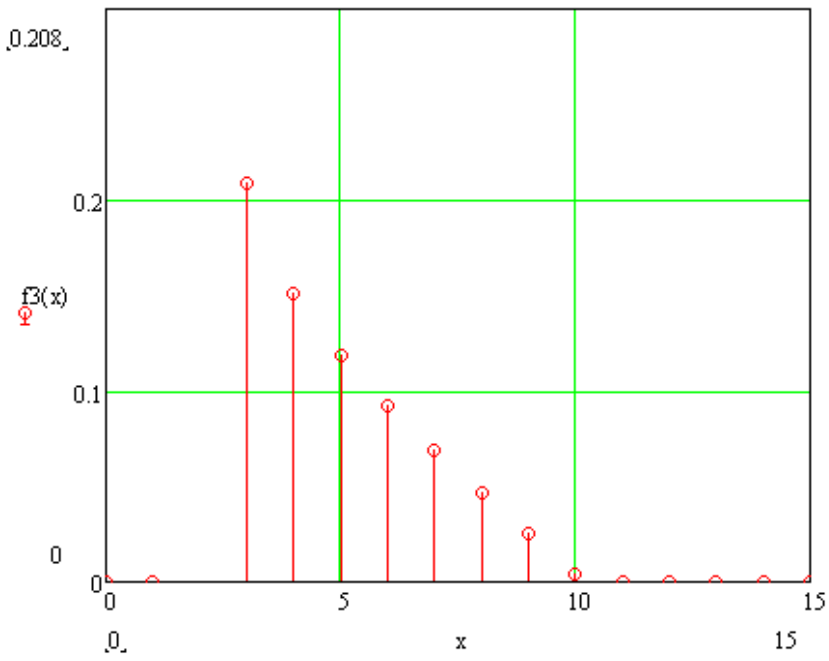

Рисунок 3.9 - Плотность вероятности числа сообщений

Математическое ожидание числа сообщений тогда будет равно

$$\overline{m} = 2\rho \cdot r\sqrt{L^2 + h^2} + \frac{4\rho \cdot r}{3h^2}\left(L^3 - \sqrt{\left(L^2 + h^2\right)^3}\right) + \frac{2L^2\rho \cdot r}{h}\ln\left(\frac{\sqrt{L^2 + h^2} + h}{L}\right) \qquad (3.27)$$

Из (3.27) можно определить расход энергии сенсорными узлами и, соответственно, жизненный цикл сенсорной сети.

3.3 Основные характеристики беспроводной сенсорной сети для выявления вторжений в виде потоков ложных событий

В таблице 3.1 приведены полученные в диссертации основные характеристики беспроводной сенсорной сети для выявления вторжений в виде потоков ложных событий. Результаты могут быть использованы для планирования сенсорных сетей, обеспечивающих заданную вероятность обнаружения ложных событий.

Таблица 3.1. – Основные характеристики сенсорной сети для выявления вторжений в виде ложных событий.

	Характеристика	**Модель**
1	Расстояние до первого сенсора (момента обнаружения)	Плотность вероятности $f(w) = \begin{cases} 0 & w < 0 \\ 2\rho \cdot \sqrt{2rw - w^2} \cdot e^{-\rho\left(r^2 \cdot \arccos\left(\frac{r-w}{r}\right) - (r-w)\sqrt{2rw-w^2}\right)} & 0 \le w < r \\ 2\rho \cdot r \cdot e^{-\rho\left(2r \cdot w + \frac{\pi \cdot r^2}{2}\right)} & w \ge r \end{cases}$

2	Среднее расстояние до первого сенсора	Приближенная оценка снизу $\tilde{w}_0 = \frac{1}{2 \cdot \rho \cdot r}$ Приближенная оценка сверху $\hat{w}_0 = \frac{1}{2}\sqrt{\frac{\pi}{\rho}} + \frac{e^{-\rho \cdot r^2}}{2\rho \cdot r}\left(1 + 2\rho \cdot r^2\right)$
3	Максимальное расстояние до обнаружения объекта при заданной вероятности обнаружения p_0	(оценка необходимой длины зоны обслуживания) $Z(\rho, r, p_0) = r + \frac{1}{2}\left(\frac{p_0}{\rho \cdot r} - \frac{\pi \cdot r}{2}\right), \quad Z \geq r$
4	Необходимая плотность сенсорного поля при заданной вероятности обнаружения p_0	(оценка необходимой плотности сенсорного поля) $\rho(Z, r, p_0) = \frac{p_0}{r \cdot \left(2(Z - r) - \frac{\pi \cdot r}{2}\right)}, \quad Z \geq r$
5	Необходимый радиус обнаружения сенсорного узла при заданной вероятности обнаружения p_0	(оценка необходимого радиуса обнаружения сенсора) $r(Z, \rho, p_0) = \frac{\sqrt{2\rho \cdot \left(2 \cdot Z^2 + p_0(4 - \pi)\right)} + 2\rho \cdot Z}{\rho(4 - \pi)}, \quad Z \geq r$
6	Число сообщений,	$\tilde{m} = 1 + 2r\rho \cdot \tau \cdot v$

	передаваемых в сети при прохождении объекта	
7	Расстояние, пройденное объектом, до границы сенсорного поля	Плотность вероятности $$f(w)=\begin{cases}0 & w<L\\ \frac{2w}{h^2}\cdot\left(\frac{h}{\sqrt{w^2-L^2}}-1\right) & L\le w\le\sqrt{L^2+h^2}\\ 0 & w>\sqrt{L^2+h^2}\end{cases}$$
8	Среднее расстояние, пройденное объектом, до границы сенсорного поля	$$\hat{w}=\sqrt{L^2+h^2}+\frac{2}{3h^2}\left(L^3-\sqrt{\left(L^2+h^2\right)^3}\right)+\frac{L^2}{h}\ln\left(\frac{\sqrt{L^2+h^2}+h}{L}\right)$$
9	Число сообщений при пересечении объектом сенсорного поля	Плотность вероятности $$f(m)=\begin{cases}0 & m<2L\rho r\\ \frac{m}{2(\rho r)^2h^2}\cdot\left(\frac{h}{\sqrt{\left(\frac{m}{2\rho r}\right)^2-L^2}}-1\right) & 2L\rho r\le m\le 2\rho r\sqrt{L^2+h^2}\\ 0 & m>2\rho r\sqrt{L^2+h^2}\end{cases}$$
10	Математическое ожидание числа сообщений при пересечении	$$\overline{m}=2\rho\cdot r\sqrt{L^2+h^2}+\frac{4\rho\cdot r}{3h^2}\left(L^3-\sqrt{\left(L^2+h^2\right)^3}\right)+\frac{2L^2\rho\cdot r}{h}\ln\left(\frac{\sqrt{L^2+h^2}+h}{L}\right)$$

	объектом сенсорного поля	

3.4 Модель времени жизни сети

Передача каждого сообщения влечет расход энергии узлами сети. При этом расход энергии зависит не только от числа передаваемых сообщений, но и от способа организации сети, т.к. в процессе передачи сообщения, в общем случае, участвует несколько узлов сети (узлы, образующие маршрут от источника сообщения до шлюза сети). Будем полагать, что на доставку одного сообщения сетью расходуется энергия ε_0. Запас энергии в узле сети конечен и при передаче некоторого числа сообщений (пакетов) снижается до нуля или величины недостаточной для функционирования узла, тогда узел исключается из сети. Таким образом, во время функционирования сети происходит уменьшение числа узлов сети, т.е. уменьшение плотности узлов ρ в зоне обслуживания. Соответственно уменьшается вероятность обнаружения объекта (3.13). Этот процесс следует учитывать при построении сети, рассчитанной на определенное время функционирования, выбирая заведомо большее значение плотности узлов, чем это требуется для обеспечения заданной вероятности обнаружения объектов сети. Однако, большая плотность узлов сети приводит увеличению числа сообщений (3.19), что в свою очередь ускоряет процесс расхода энергии.

Рассмотрим модель сети с учетом расхода энергии.

Запас энергии узла сети равен ε_0, на передачу одного сообщения тратится энергия e. Таким образом, один узел способен обслужить $\frac{\varepsilon_0}{e}$ сообщений.

Будем полагать, что события, связанные с расходом энергии равновероятны для всех узлов сети. При интенсивности поступления объектов λ интенсивность расхода энергии сетью составит

$$\mathrm{E} = \overline{m} \cdot e \cdot \lambda \text{ Дж/ед. времени} \qquad (3.28)$$

где $\overline{m}$ - среднее число сообщений, вырабатываемое в сети при прохождении объекта, определяется формулой (3.22), (3.23).

Тогда доля расходуемой энергии (или доля израсходовавших энергию узлов) за интервал времени Δt может быть вычислена как

$$\zeta = \frac{E}{n_0 \varepsilon_0} \Delta t \qquad (3.29)$$

где n_0 - общее число узлов в сети в начальный момент ее функционирования.

Тогда изменение числа активных узлов сети за короткий интервал времени Δt составит

$$\Delta n = -n \cdot \frac{E}{n_0 \varepsilon_0} \Delta t \qquad (3.30)$$

где n - число узлов в сети в текущий момент времени.

При $\Delta t \to 0$ получим дифференциальное уравнение

$$\frac{dn}{dt} = -n \cdot \frac{E}{n_0 \varepsilon_0} \qquad (3.31)$$

Подставляя E из (3.28) и $\overline{m}$ из (3.19) получим

$$\frac{dn}{dt} = -n \cdot \frac{2r\rho \cdot \widetilde{w} \cdot e \cdot \lambda}{n_0 \varepsilon_0} \tag{3.32}$$

Раскрыв ρ

$$\frac{dn}{dt} = -n \cdot \frac{2r \frac{n}{L \cdot h} \cdot \widetilde{w} \cdot e \cdot \lambda}{n_0 \varepsilon_0} = -n^2 \frac{2r \cdot \widetilde{w} \cdot e \cdot \lambda}{n_0 \varepsilon_0 L \cdot h} \tag{3.33}$$

Получаем общее дифференциальное уравнение вида

$$\frac{dn}{dt} = -k \cdot n^2 \tag{3.34}$$

Где $k = \frac{2r \cdot \widetilde{w} \cdot e \cdot \lambda}{n_0 \varepsilon_0 L \cdot h}$ (3.35)

Решением данного уравнения является функция, выражающая зависимость числа узлов от времени

$$n(t) = \frac{1}{k \cdot t + C} \tag{3.36}$$

где C - константа интегрирования.

Из начальных условий $C = \frac{1}{n_0}$, с учетом последнего

$$n(t) = \frac{n_0}{n_0 \cdot k \cdot t + 1} \tag{3.37}$$

Зависимость плотности активных узлов от времени составит

$$\rho(t) = \frac{n(t)}{L \cdot h} = \frac{n_0}{(n_0 \cdot k \cdot t + 1)Lh} \qquad (3.38)$$

Характер зависимости плотности активных узлов от времени приведен на рисунке 3.10.

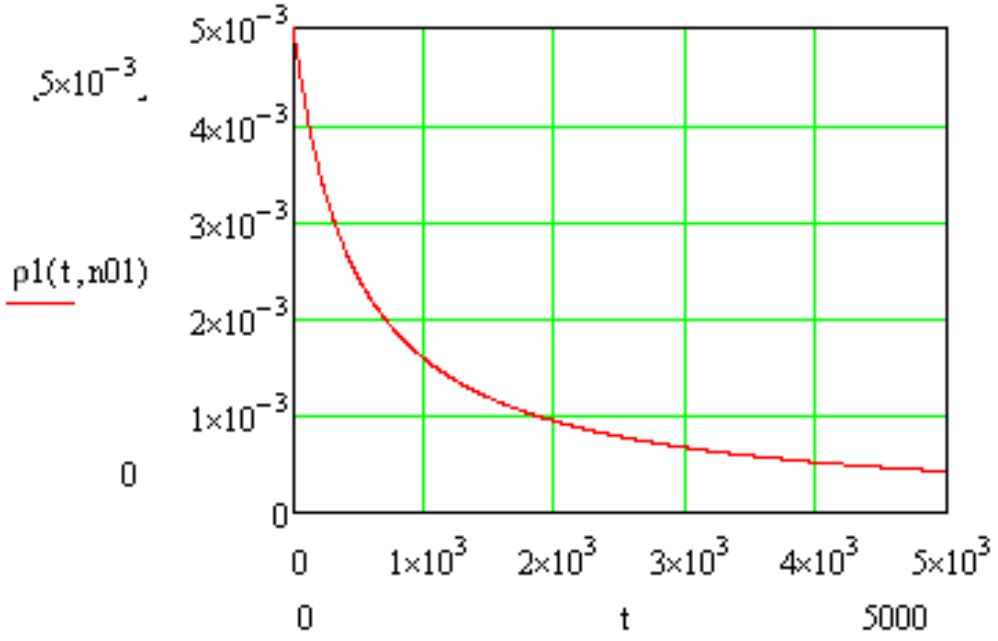

Рисунок 3.10 - Характер зависимости плотности активных узлов от времени

3.5 Влияние характеристик потока ложных событий на функционирование сети

Приведенные выше рассуждения и модели получены для общего случая, т.е. для произвольного характера потока объектов, поступающих в зону обслуживания. При анализе функционирования предполагалось, что узлы сети обслуживают события мгновенно, т.е. время детектирования объекта и время обработки и доставки сообщения по сети пренебрежимо мало по сравнению с интервалами времени между моментами поступления объектов. Такое

приближение допустимо при малой и средней интенсивности поступления объектов. При высокой интенсивности объектов, когда интервалы времени между моментами поступления объектов соизмеримы с временем передачи сообщения (временем обслуживания) характер потока заявок может оказывать влияние на функционирование сети. Для оценки этого влияния будем рассматривать узлы сети как СМО, использующие комбинированную дисциплину обслуживания (с ожиданием и потерями).

Рассмотрим два случая, когда поток объектов представляет собой детерминированный поток и этот поток является случайным. Время обслуживания события узлом определяется суммой времени обработки и времени передачи сообщения. Обслуживание события связано с выполнением некоторой работы контроллера и времени передачи пакета данных. При обслуживании однотипных событий и передаче однотипных сообщений можно предположить, что эти затраты времени одинаковы для всех обрабатываемых событий. Поэтому, сделаем допущение о том, что время обслуживания события узлом постоянно и равно t_0.

Рассмотрим два варианта потока объектов.

1. Детерминированный поток: объекты поступают в зону обслуживания через равные промежутки времени z_0, причем $z > t_0$.

2. Случайный поток: простейший поток, объекты поступают в зону обслуживания через случайные промежутки времени со средним значением $\bar{z}$, причем $\bar{z} > t_0$, длина интервала распределена по экспоненциальному закону.

В первом случае система обслуживания функционирует как полностью детерминированная система D/D/1/K. При выполнении условия $z > t_0$ вероятность отказа (потери пакета) равна нулю $p_0 = 0$.

Во втором случае система обслуживания функционирует как полностью СМО M/D/1/K. При выполнении условия $\bar{z} > t_0$ вероятность отказа (потери пакета), согласно [71] равна

$$p_0 = \frac{(1-y)E_K}{1-yE_K} \qquad (3.38a)$$

где

$$E_K = 1-(1-y)\sum_{j=0}^{K}\frac{(-1)^j y\cdot(K-j)^j}{j!}e^{y(K-j)}; \qquad (3.38b)$$

$y = \frac{t_0}{\vec{z}} = t_0 \cdot \lambda$ нагрузка на узел;

K число мест ожидания в буфере.

Таким образом, в зависимости вида и интенсивности потока объектов сеть обслужит различную долю сообщений. В условиях рассмотренного примера, в случае детерминированного потока узел сети обслужит все события, а в случае простейшего потока 1- p_0 событий. Полагая, что расходуемая сетью энергия пропорциональна числу сообщений, можно ожидать, что время жизни сети, в случае воздействия детерминированного потока, будет меньше, чем в случае воздействия простейшего потока, за счет потерь части событий и как следствие, передачи меньшего числа сообщений.

3.6 Выводы

1. Обнаружение ложных событий в беспроводной сенсорной сети можно рассматривать как задачу слежения за целью, а для выявления ложных событий с заданной вероятностью с учетом ограниченных возможностей сенсорных узлов целесообразно использовать архитектурные характеристики сети, например, распределение плотности размещения узлов на сенсорном поле.

2. Определены следующие характеристики беспроводной сенсорной сети для выявления вторжений в виде ложных событий:

- расстояние до первого сенсора (момента обнаружения),

- среднее расстояние до первого сенсора,

- максимальное расстояние до обнаружения объекта при заданной вероятности обнаружения p_0,

- необходимая плотность сенсорного поля при заданной вероятности обнаружения p_0,

- необходимый радиус обнаружения сенсорного узла при заданной вероятности обнаружения p_0,

- число сообщений, передаваемых в сети при прохождении объекта,

- расстояние, пройденное объектом, до границы сенсорного поля,

- среднее расстояние, пройденное объектом, до границы сенсорного поля,

- число сообщений при пересечении объектом сенсорного поля,

- математическое ожидание числа сообщений при пересечении объектом сенсорного поля.

ГЛАВА 4
РАЗРАБОТКА МЕТОДА ЗАЩИТЫ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ ОТ ПОТОКОВ ЛОЖНЫХ СОБЫТИЙ ПУТЕМ МОДИФИКАЦИИ СТРУКТУРНЫХ ХАРАКТЕРИСТИК СЕНСОРНОГО ПОЛЯ

4.1 Модель сети и потоков вызовов

В работе [68], посвященной классификации систем слежения за целью, реализованных на сенсорных сетях [119], в качестве одного из направлений улучшения характеристик сенсорной сети рассматриваются архитектурные методы. Воспользуемся подобным методом в нашем исследовании, предполагая, что изменение плотности размещения сенсорных узлов на сенсорном поле может увеличить жизненный цикл в условиях воздействия на сеть потока ложных событий.

В качестве модели сети [10] используется типовая модель из N сенсорных узлов, образующая пуассоновское поле на плоскости размером 200 на 200 метров (рисунок 4.1). Радиус действия сенсорного узла – 20 м, запас энергии в каждом узле – 2Дж, расход энергии на передачу сообщения – 2мДж. Все сенсорные узлы однородны, т.е. имеют одинаковый радиус действия и начальные энергетические характеристики.

Поток объектов представляет собой смесь потоков двух типов объектов $\lambda = \lambda_1 + \lambda_2$, где λ_1 и λ_2 интенсивности. Первый поток представляет собой поток ложных событий (объектов), направленных только на уменьшение жизненного цикла сети, а второй поток – поток событий (объектов), который должен быть обнаружен сенсорной сетью. Сенсоры способны идентифицировать тип объекта. Когда в области обслуживания O_1 обнаруживается объект первого типа, передается соответствующее сообщение по сети (области O_1) и данный объект

считается обнаруженным, т.е. исключается из дальнейшего рассмотрения. Объекты второго типа в области O_1 не обнаруживаются. Таким образом, в область O_2 поступают только объекты второго типа и часть объектов первого типа, необнаруженных в области O_1.

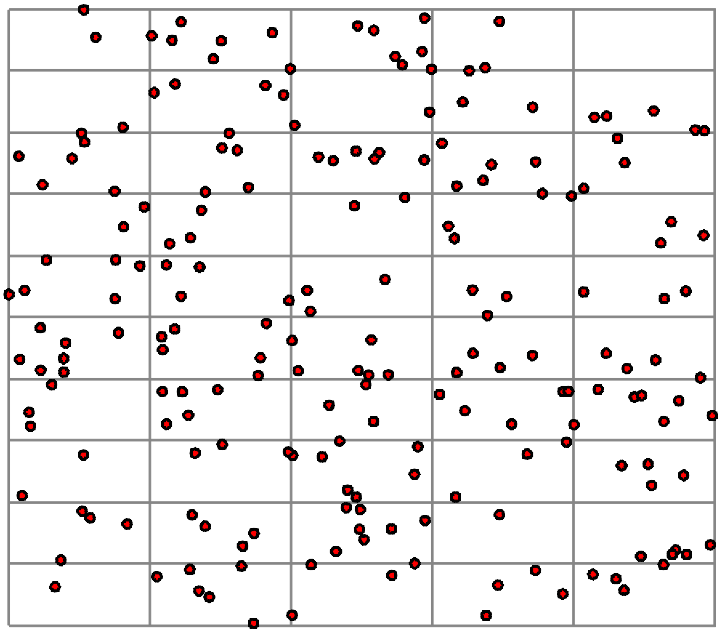

Рисунок 4.1 - Пуассоновское сенсорное поле

Сенсоры второго типа одинаково реагируют на объекты обоих типов, т.е. вырабатывают сообщения при нахождении в зоне обнаружения любого объекта.

Зона обслуживания сети имеет две области: область обнаружения объектов первого типа и область обнаружения всех типов объектов, рисунок 4.2.

Задача состоит в том, чтобы при заданном числе узлов сети оценить значения плотностей размещения сенсоров ρ_1 и ρ_2, при которых достигается максимальное время жизни сети. Под временем жизни сенсорной сети понимается длительность функционирования, в течение которого сеть выполняет свои функции, т.е. вероятность обнаружения объектов во второй области не ниже заданной величины p_0.

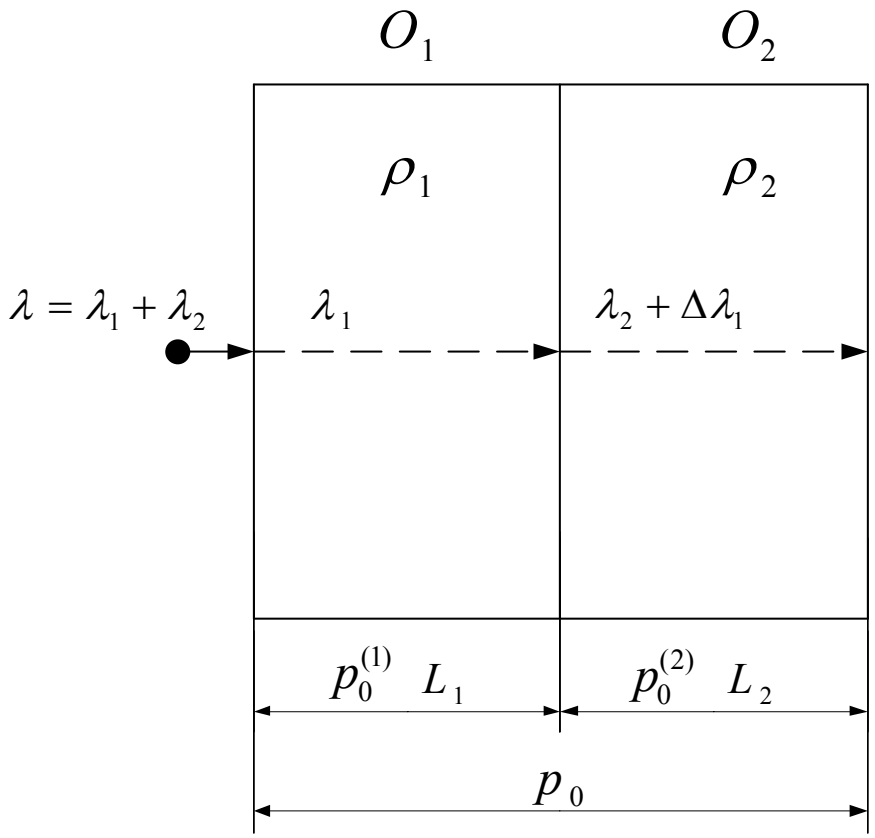

Рисунок 4.2 - Структура зоны обслуживания сети

4.2 Оптимизация длительности жизни беспроводной сенсорной сети

Зависимость вероятности обнаружения объектов первого типа от времени может быть определена в соответствии с работой автора [8] следующим образом:

$$p_0^{(1)}(t) = F(L_1, t) = \begin{cases} 0 & L_1 < 0 \\ 1 - e^{-\rho_1(t)\cdot\left(r^2\cdot\arccos\left(\frac{r-L_1}{r}\right)-(r-w)\sqrt{2rL_1-L_1^2}\right)} & 0 \le L_1 < r \\ 1 - e^{-\rho_1(t)\cdot\left(2r\cdot L_1+\frac{\pi\cdot r^2}{2}\right)} & L_1 \ge r \end{cases} \quad (4.1)$$

где L_1 - длина области O_1 (м);

r - радиус зоны обнаружения сенсора (м);

$$\rho_1(t) = \frac{n_0^{(1)}}{\left(n_0^{(1)} \cdot k_1 \cdot t + 1\right) L_1 h} \tag{4.2}$$

где $n_0^{(1)}$ - начальное число узлов сети в области O_1;

t - время (с);

h - ширина областей O_1 и O_2 (м);

$$k_1 = \frac{2r \cdot \widetilde{w} \cdot e \cdot \lambda_1}{n_0 \varepsilon_0 L_1 \cdot h} \tag{4.3}$$

λ_1 - интенсивность поступления объектов 1 типа (объектов/ед. времени);

ε_0 - запас энергии одного сенсорного узла в начальный момент функционирования сети (Дж);

e - энергия, расходуемая узлом на передачу одного сообщения (Дж);

$n_0 = n_0^{(1)} + n_0^{(2)}$ - общее число активных узлов сети в начальный момент ее функционирования;

$\widetilde{w}$ - средняя длина пути, объекта до момента его обнаружения (м), определяемая в соответствии с [8] как:

$$\widetilde{w} = \frac{1}{2 \cdot \rho \cdot r} \tag{4.4}$$

Зависимость вероятности обнаружения объектов во второй области сети от времени может быть получена аналогично, с учетом изменения интенсивности объектов, при прохождении через первую область. В первой области происходит обнаружение объектов первого типа с вероятностью $p_0^{(1)}$, следовательно,

интенсивность объектов первого типа, поступающих во вторую область, может быть определена как $\lambda_1 \cdot \left(1 - p_0^{(1)}\right)$. Тогда интенсивность поступления объектов первого и второго типов во вторую область будет определяться как $\lambda_2 + \Delta\lambda_1$, где $\Delta\lambda_1 = \lambda_1 \cdot \left(1 - p_0^{(1)}\right)$.

$$p_0^{(2)}(t) = F(L_2, t) = \begin{cases} 0 & L_2 < 0 \\ 1 - e^{-\rho_2(t)\cdot\left(r^2 \cdot \arccos\left(\frac{r-L_2}{r}\right) - (r-w)\sqrt{2rL_2 - L_2^2}\right)} & 0 \le L_2 < r \\ 1 - e^{-\rho_2(t)\cdot\left(2r\cdot L_2 + \frac{\pi\cdot r^2}{2}\right)} & L_2 \ge r \end{cases} \qquad (4.5)$$

где L_2 - длина области O_2 (м);

$$\rho_2(t) = \frac{n_0^{(2)}}{\left(n_0^{(2)} \cdot k_2 \cdot t + 1\right) L_2 h} \qquad (4.6)$$

где $n_0^{(2)}$ - начальное число узлов сети в области O_2;

$$k_2 = \frac{2r \cdot \widetilde{w} \cdot e \cdot \left(\lambda_2 + \lambda_1 (1 - p_0^{(1)})\right)}{n_0 \varepsilon_0 L_2 \cdot h} \qquad (4.7)$$

λ_2 - интенсивность поступления объектов 2 типа (объектов/ед. времени).

Выражения (4.1) и (4.5) определяют зависимость вероятностей обнаружения объектов первого типа в области 1 и объектов первого и второго типа в области 2 соответственно.

Задача выбора значений ρ_1 и ρ_2, при которых достигается максимальное время жизни сети, является задачей оптимизации. В этой задаче переменными (параметрами) управления являются значения ρ_1 и ρ_2, а параметром состояния является время жизни сети, которое из (4.5) можно определить как

$$t_0 = \arg\left(p_0^{(2)}(t) = p_0\right) \tag{4.8}$$

где p_0 - заданная вероятность обнаружения объектов в области 2.

Тогда задача оптимизации может быть определена следующей целевой функцией

$$t_{\max} = \max_{n_1, n_2} \left\{\arg\left(p_0^{(2)}(t) \geq p_0\right)\right\} \tag{4.9}$$

при ограничениях

$$\begin{aligned} &\rho_1 \geq 0 \\ &\rho_2 \geq 0 \\ &n = n_1 + n_2 = const \\ &p_0 = const \\ &L_1 = const \\ &L_2 = const \\ &h = const \end{aligned} \tag{4.10}$$

4.3 Решение задачи оптимизации

Для решения неравенства $p_0^{(2)}(t) \geq p_0$ из (4.9) относительно t использовался численный метод Риддера из пакета программного обеспечения Mathcad.

Выбор метода решения задачи оптимизации (4.9), (4.10) зависит от вида оптимизируемой функции. Анализ выражений (4.1) – (4.8) позволяет сделать вывод о том, что в условиях (4.10) данная задача является задачей выпуклой оптимизации. Для оптимизации выпуклой функции могут быть использованы различные методы условной оптимизации функции нескольких переменных. Выбор того или иного метода может существенно влиять на время решения задачи (объем вычислений), но, практически, не отражается на решении. Ввиду

того, что в данном случае вычислительная эффективность метода не имеет существенного значения, для решения задачи был выбран реализованный во многих прикладных системах метод сопряженных градиентов с учетом ограничений (4.10). Вероятность обнаружения объектов p_0 в области 2 задаем на уровне 0,9.

Зависимость максимального времени жизни сети от числа (плотности) узлов в первой и второй областях можно представить поверхностью. На рисунке 4.3. приведена зависимость максимального времени жизни сети от числа узлов в первой и второй областях без учета ограничений (левый рисунок) и с учетом ограничения общего числа узлов. Интенсивности поступления объектов первого и второго типа были выбраны равными.

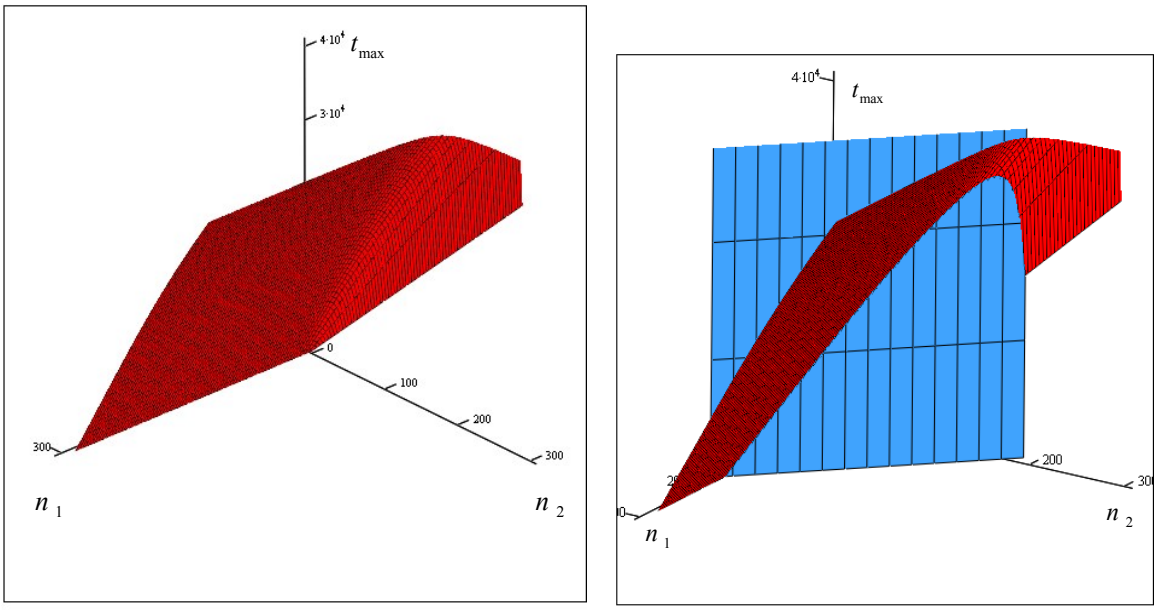

Рисунок 4.3 - Зависимости максимального времени жизни сети от числа узлов в первой и второй областях без учета ограничений и с учетом ограничения общего числа узлов

Анализ рисунка 4.3 доказывает, прежде всего, что существует некое соотношение узлов в первой и второй областях, которое обеспечивает максимальное время жизни сети, под которым по-прежнему понимается интервал

времени, в течение которого объекты во второй области обнаруживаются с заданной вероятностью.

Из рисунка 4.3 видно также, что пересечение поверхности функции максимального времени жизни с областью ограничений представляет собой унимодальную функцию, имеющую выраженный максимум.

Рисунок 4.3. конкретизирует зависимость числа узлов в первой и второй областях от общего числа узлов для сенсорного поля 200×200 м, изначально заявленного в исследовании как типового. При указанном на рис.4.3 числе узлов в первой и второй областях достигается максимальное время жизни сети. Как видим, при небольших плотностях сенсорных узлов доля узлов первой области может составлять до 40%, в то время как с увеличением плотности узлов эта доля уменьшается, сохраняя практически неизменным численное значение примерно в 25 узлов в первой области. Интенсивности поступления объектов первого и второго типа для зависимостей рисунок 4.4 равны.

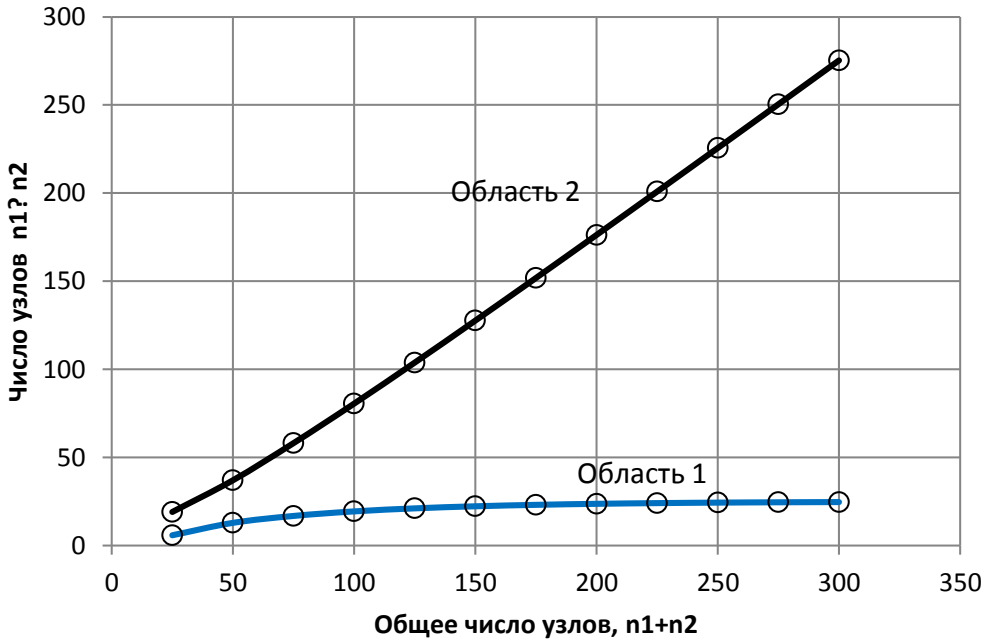

Рисунок 4.4 - Зависимость числа узлов в первой и второй областях от общего числа узлов для сенсорного поля 200×200 м

На рисунке 4.5 представлены зависимости максимального времени жизни сети от общего числа узлов в условиях отсутствия сенсорных узлов в области O_1 (n_1=0) и при оптимальном соотношении n_1 и n_2 в зависимости от общего числа сенсорных узлов (плотности сенсорного поля). Размеры сенсорного поля по-прежнему 200×200 м, а интенсивности поступления объектов первого и второго типа равны. Как видим, для типового сенсорного поля в 100 узлов время жизни сенсорной сети увеличивается в 2 раза по сравнению с тем случаем, когда зона O_1 отсутствует.

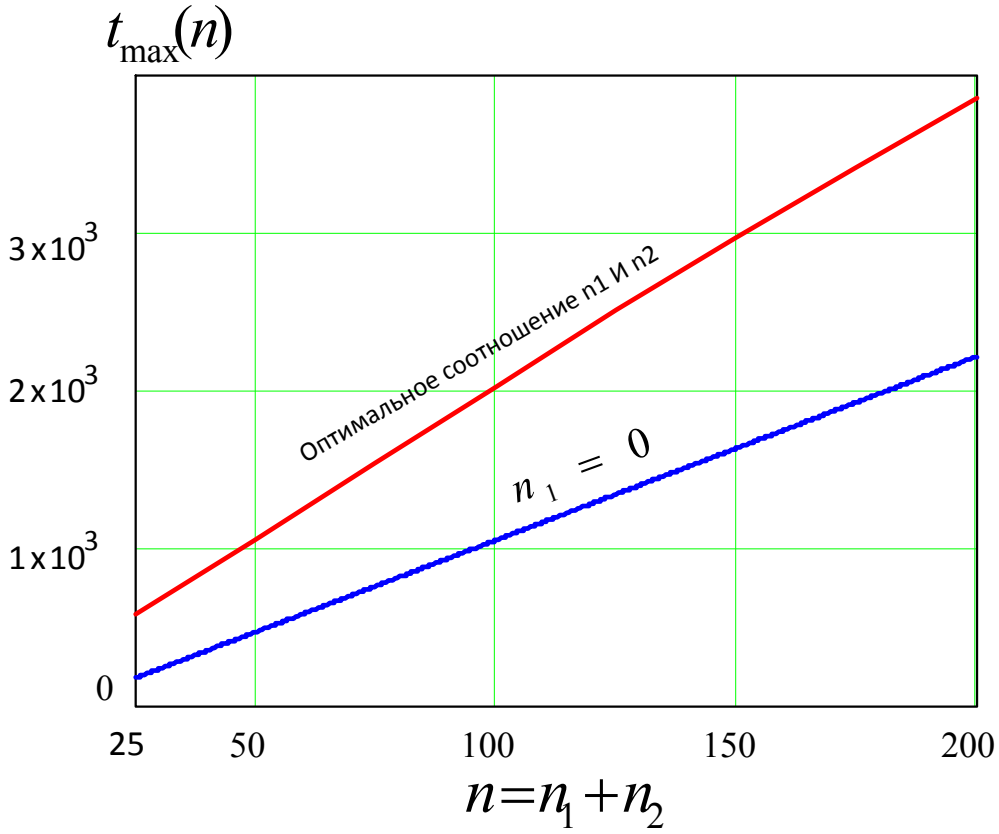

Рисунок 4.5 - Зависимость максимального времени жизни сенсорной сети от общего числа узлов при оптимальном соотношении n_1 и n_2 и при n_1=0

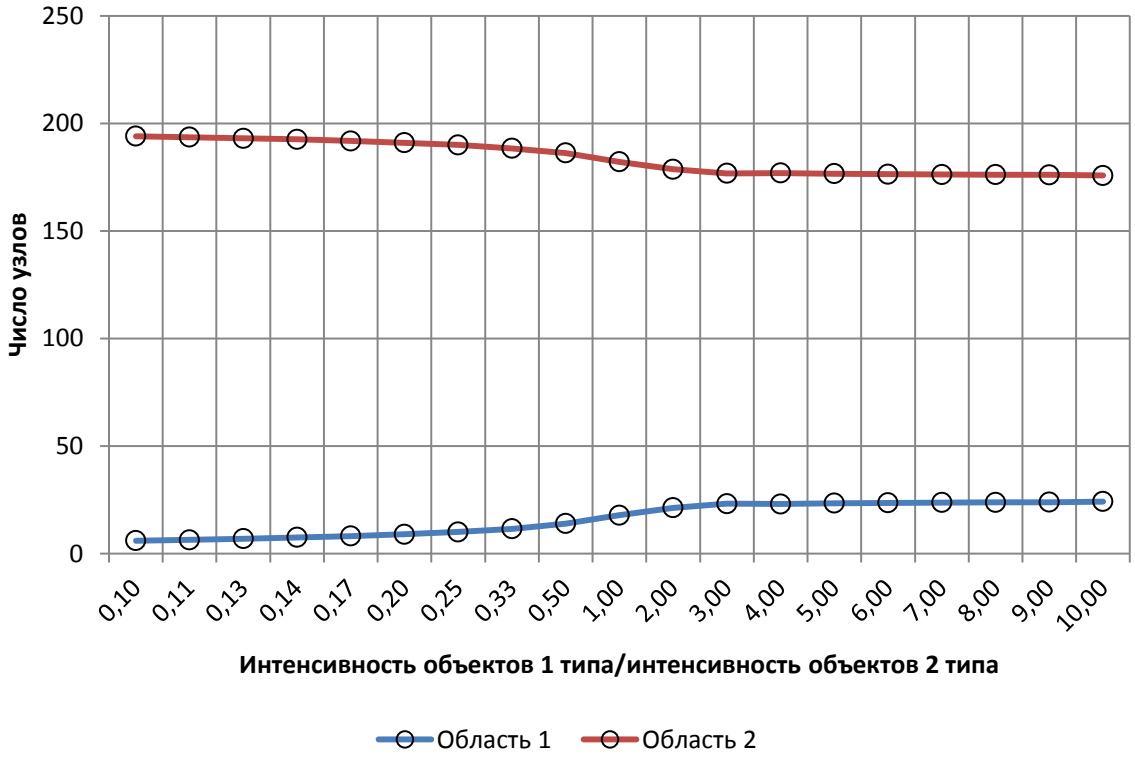

Рисунок 4.6 - Результаты оптимизации значений плотности узлов в областях 1 и 2 при различном соотношении интенсивности потока объектов первого и второго типов

При решении задачи оптимизации были получены также значения плотностей узлов в первой и второй зонах обслуживания при различном соотношении интенсивностей поступления объектов $\frac{\lambda_1}{\lambda_2}$ от 1 до 10 и вероятности обнаружения объектов второго типа 0,9. Результаты приведены на рисунке 4.6.

Из анализа рисунка 4.6 следует, что при соотношении интенсивностей первого и второго потоков меньше единицы в первой области требуется наличие небольшого числа узлов для отслеживания объектов первого типа. Максимального значения число узлов первого типа достигает при соотношении интенсивностей первого и второго потоков 3-4, практически не изменяясь при дальнейшем увеличении этого соотношения.

4.4 Выводы

1. Разработан метод защиты беспроводных сенсорных сетей от потоков ложных событий путем изменения структурных характеристик сенсорного поля, состоящий в изменении распределения плотности сенсорных узлов по сравнению с равномерной.

2. Доказано, что существует оптимальное значение плотности (числа) узлов в первой и второй областях сенсорного поля, обеспечивающее максимальное время жизни сенсорной сети, и определены соответствующие численные характеристики для различных значений общего числа узлов на сенсорном поле, а также в условиях различных соотношений интенсивностей потоков ложных и реальных событий.

ЗАКЛЮЧЕНИЕ

В диссертационной работе получены следующие основные новые научные результаты:

1. Беспроводные сенсорные сети обладают целым рядом особенностей по сравнению с существующими сетями, ключевой из которых является их самоорганизация. Важнейшими характеристиками беспроводных сенсорных сетей являются длительность жизненного цикла и остаточная энергия. Особенности, присущие беспроводным сенсорным сетям, определяют новые проблемы обеспечения сетевой безопасности для этих сетей.

2. Предложен новый вид атаки на беспроводные сенсорные сети – создание потоков ложных событий с целью уменьшения длительности жизненного цикла сети за счет воздействия на ее энергетическую систему.

3. Разработана модель вторжения в беспроводную сенсорную сеть с целью уменьшения ее жизненного цикла, отличающаяся от известных тем, что для достижения данной цели используются потоки ложных событий. Модель разработана на основе типовых геометрических, количественных и энергетических параметров беспроводных сенсорных сетей с использованием базового алгоритма кластеризации для гомогенной мобильной сенсорной сети при вторжении в сеть пуассоновского и детерминированного потоков ложных событий.

4. Выявлено в отличие от известных результатов, что длительность жизненного цикла беспроводной сенсорной сети может существенно зависеть от вида потока ложных событий и при прочих равных условиях при воздействии детерминированного потока может быть почти в два раза меньше, чем при воздействии пуассоновского.

5. Установлено в отличие от известных результатов, что остаточную энергию и длительность жизненного цикла беспроводной сенсорной сети при

воздействии потоков ложных событий можно увеличить, если придать сенсорным узлам мобильность со скоростью 2 м/с (скорость быстро идущего пешехода).

6. Обнаружение ложных событий в беспроводной сенсорной сети можно рассматривать как задачу слежения за целью, а для выявления ложных событий с заданной вероятностью с учетом ограниченных возможностей сенсорных узлов целесообразно использовать архитектурные характеристики сети, например, распределение плотности размещения узлов на сенсорном поле. Определены следующие характеристики беспроводной сенсорной сети для выявления вторжений в виде ложных событий:

- расстояние до первого сенсора (момента обнаружения),

- среднее расстояние до первого сенсора,

- максимальное расстояние до обнаружения объекта при заданной вероятности обнаружения p_0,

- необходимая плотность сенсорного поля при заданной вероятности обнаружения p_0,

- необходимый радиус обнаружения сенсорного узла при заданной вероятности обнаружения p_0,

- число сообщений, передаваемых в сети при прохождении объекта,

- расстояние, пройденное объектом, до границы сенсорного поля,

- среднее расстояние, пройденное объектом, до границы сенсорного поля,

- число сообщений при пересечении объектом сенсорного поля,

- математическое ожидание числа сообщений при пересечении объектом сенсорного поля.

7. Разработан метод защиты беспроводных сенсорных сетей от потоков ложных событий путем изменения структурных характеристик сенсорного поля, состоящий в изменении распределения плотности сенсорных узлов по сравнению с равномерной.

8. Доказано, что существует оптимальное значение плотности (числа) узлов в первой и второй областях сенсорного поля, обеспечивающее максимальное

время жизни сенсорной сети, и определены соответствующие численные характеристики для различных значений общего числа узлов на сенсорном поле, а также в условиях различных соотношений интенсивностей потоков ложных и реальных событий.

9. Предложена классификация ложных структур для Интернета Вещей, где наряду с потоками ложных событий рассматриваются ложные облака и клонированные интернет вещи. Дано определение ложных облаков и рассмотрены примеры клонирования сенсорных полей. Приведены основные характеристики ложных облаков и клонирования для Интернета Вещей.

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

Аббревиатура	Расшифровка на английском	Расшифровка на русском
ACK	Acknolegement	Подтверждение
DoS	Denial of Service	Отказ в обслуживании
DTN	Delay Tolerant Networks	Сети, толерантные к задержкам
FUSN	Flying Ubiquitous Sensor Network	Летающая всепроникающая сенсорная сеть
IPv6	IP version 6	Протокол IP 6-ой версии
ISO	International Standard Organization	Международная организация стандартизации
LEACH	Low Energy Adaptive Clustering Algorithm	Энергетически эффективный адаптивный алгоритм кластеризации
LEACH-M	Low Energy Adaptive Clustering Algorithm - Mobile	Энергетически эффективный адаптивный алгоритм кластеризации для мобильных сенсорных сетей
M2M	Machine-to-Machine	Сети машина-машина
MANET	Mobile Ad Hoc Network	Мобильная целевая сеть
MWSN	Mobile Wireless Sensor Network	Мобильная беспроводная сенсорная сеть

NGN	Next Generation Networks	Сети связи следующего поколения
RPL	Routing Protocol for Low energy and lossy networks	Протокол маршрутизации для малопотребляющих сетей с потерями
USN	Ubiquitous Sensor Network	Всепроникающая сенсорная сеть
VANET	Vehicular Ad Hoc Network	Целевая сеть для транспортных средств
6LoWPAN	IPv6 Low Energy Wireless Personal Area Networks	Протокол IP шестой версии для низко потребляющих беспроводных персональных сетей
БПЛА		Беспилотный летательный аппарат
ВСС		Всепроникающие сенсорные сети
ЛСС		Летающие сенсорные сети
МСЭ-Т		Сектор стандартизации телекоммуникаций Международного Союза Электросвязи
ССОП		Сеть связи общего пользования

СПИСОК ЛИТЕРАТУРЫ

1. Абакумов, П. А. Алгоритм выбора головного узла кластера сенсорной сети в трехмерном пространстве / П. А. Абакумов // Электросвязь. – 2014.–№4. – С.17-19.

2. Аджемов, А. С. От e-России к u-России: направления развития телекоммуникаций / А. С. Аджемов, А. Е. Кучерявый // Инновационная экономика России. – апрель 2006.- С. 56 - 59.

3. Аль-Наггар, Я. М. Алгоритм выбора головного узла кластера для всепроникающих сенсорных сетей с использованием нечеткой логики и диаграмм Вороного / Я. М Аль-Наггар // Электросвязь.– 2014.–№9.-С.14-18.

4. Бельфер, Р.А. Защита информационной безопасности сенсорной сети кластерной архитектуры с помощью механизма обнаружения вторжения / Р.А.Бельфер, И.С.Огурцов // Инженерный журнал: наука и инновации, №2 (14), 2013.

5. Богданов, И.А. Характеристики жизненного цикла мобильной сенсорной сети при различных потоках ложных событий / И.А. Богданов, А.И. Парамонов, А.Е. Кучерявый // Электросвязь, 2013.- №1. - С.32-33.

6. Богданов И.А. Сетевая безопасность в беспроводных сенсорных сетях / И.А.Богданов // 68-я Научно-техническая конференция НТОРЭС им. Попова. Труды конференции, Апрель, 2013.

7. Богданов И.А. Влияние мобильности узлов беспроводной сенсорной сети на жизненный цикл при вторжении в виде потоков ложных событий / И.А.Богданов // 68-я Научно-техническая конференция НТОРЭС им. Попова. Труды конференции, Апрель, 2013.

8. Богданов, И.А. Характеристики беспроводной сенсорной сети для выявления вторжений в виде потоков ложных событий [Электронный ресурс] / И.А. Богданов, А.Е. Кучерявый // Информационные технологии и

телекоммуникации. Электронный научный журнал. СПб ГУТ, выпуск 3 (7), 2014, с.59-74. Режим доступа: https://sut.ru/. – (Дата обращения: 20.09.2016)

9. Богданов, И.А. Особенности вторжений во всепроникающие сенсорные сети. Новые виды вторжений / И.А. Богданов, А.И. Парамонов, А.Е. Кучерявый // 2-ая Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сборник научных статей, СПб., 26-27 февраля 2013. – С. 49 – 52.

10. Богданов, И.А. Структурный метод защиты беспроводной сенсорной сети от потоков ложных событий / И.А.Богданов // Электросвязь, 2014.- №11.- С.14-17.

11. Богданов И.А. Летающие сенсорные сети/И.А. Богданов /А.Е. Кучерявый, А.Г.Владыко, Р.В.Киричек, А.И.Парамонов, А.В. Прокопьев, И.А. Богданов, А.А. Дорт-Гольц//Электросвязь, 2014.-№9.-С. 2-5.

12. Бутенко, В.В. IoT – новая точка развития ИКТ и средство кардинального повышения адаптивных возможностей человека при взаимодействии с ухудшающейся антропогенной средой / В.В.Бутенко, А.П.Назаренко, В.К.Сарьян // Труды 54-й научной конференции МФТИ. Радиотехника и кибернетика. 10-30 ноября, 2011 г. М., МФТИ.

13. Васильев, Д.С. Протоколы маршрутизации в MANET / Д.С. Васильев, А.В. Абилов // Электросвязь.-2014.-№11- С.52-54.

14. Гегель, Г.В.Ф. Наука логики / СПб, “Наука”.-1997.-800 с.

15. Гольдштейн, Б.С. Сети связи пост-NGN /Б.С. Гольдштейн, А.Е. Кучерявый. - БХВ, С.Петербург, 2013.-160с.

16. Гольдштейн, Б.С. Сети связи. Учебник для ВУЗов /Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. - BHV, С. Петербург, 2010.-400с.

17. Зима, В.М. Безопасность глобальных сетевых технологий. 2-е издание / В.М. Зима, А.А. Молдовян, Н.А. Молдовян. - БХВ-Петербург, 2003, 368с.

18. Кучерявый, А.Е. Сети связи общего пользования. Тенденции развития и методы расчёта / А.Е. Кучерявый, А.И. Парамонов, Е.А. Кучерявый. - ФГУП ЦНИИС, 2008.-290с.

19. Кучерявый, А.Е. Самоорганизующиеся сети / А.Е. Кучерявый, А.В. Прокопьев, Е.А. Кучерявый. – СПб : Любавич, 2011. – 312 с.

20. Кучерявый, А.Е. От e-России к u-России: тенденции развития электросвязи/А.Е. Кучерявый, Е.А. Кучерявый//Электросвязью-2005.-№5-С.10-12.

21. Кучерявый, А.Е. От e-России к u-России. Сенсорные сети /А.Е. Кучерявый, Е.А. Кучерявый, А.И. Парамонов//5-я Международная конференция по NGN (NGN – 2005): материалы, Н. Новгород, 23-25 августа 2005. –С. 33 – 35.

22. Кучерявый, А.Е. На пути к u-России и u-сетям. Международный телекоммуникационный /А.Е. Кучерявый, Е.А. Кучерявый// симпозиум «Мультисервисные услуги в высокоскоростных системах мобильной связи»: сборник трудов – СПб : СПб ГУТ, 27-30 июня, 2006. – С. 95 – 99.

23. Кучерявый, А.Е. Сенсорные сети как перспективное направление развития телекоммуникаций / А.Е. Кучерявый // 59-я Научно-техническая конференция профессорского профессорско-преподавательского состава СПбГУТ им. Бонч-Бруевича: материалы.–СПб, 22-26 января, 2007.–С.5–7.

24. Кучерявый, А.Е. Выбор головных узлов в однородной беспроводной сенсорной сети для обеспечения полного покрытия / А.Е. Кучерявый, А. Салим // 64-я Научно-Техническая Конференция НТОРЭС им. А.С.Попова. Труды конференции. Апрель 2009.- С.106.

25. Кучерявый, А.Е. Диаграммы Вороного для Беспроводных Сетей / А.Е. Кучерявый, А. Салим // 64-я Научно-Техническая Конференция НТОРЭС им. А.С.Попова. Труды конференции. Апрель 2009.-С.108.

26. Кучерявый, А.Е. Выбор головного узла кластера в однородной беспроводной сенсорной сети / А.Е. Кучерявый, А. Салим // Электросвязь, 2009.- № 8.-С.32-36.

27. Кучерявый, А.Е. Целевые сети / А.Е. Кучерявый // 63-я Научно-техническая конференция, посвященная Дню Радио : труды конференции. – СПб : СПб ГЭТУ «ЛЭТИ, Апрель 2008. – С. 163 – 164.

28. Кучерявый, А.Е. Самоорганизующиеся сети и новые услуги / А.Е. Кучерявый. – М. : Электросвязь, 2009. - №1. – С. 19-23.

29. Кучерявый, А.Е. Самоорганизующиеся сети и новые услуги / А.Е. Кучерявый // 62-я Научно-техническая конференция СПбГУТ: материалы. – СПб, 8-12 февраля 2010. – С. 14 – 16.

30. Кучерявый, А.Е. Введение в наносети / А.Е. Кучерявый // 66-я Научно-техническая конференция НТОРЭС им. Попова : труды конференции. – СПб., апрель, 2011. – С. 186 – 187.

31. Кучерявый, А.Е. Исследование нагрузки в сетях Интернета вещей / А.Е. Кучерявый, А.С. Мутханна, А.В. Прокопьев // 67-я Научно-техническая конференция НТОРЭС им. Попова : труды конференции. – СПб., апрель, 2012. – С.114 – 115.

32. Кучерявый, А.Е. Интернет Вещей и самоорганизующиеся сети / А.Е. Кучерявый // Научно-техническая школа-семинар “Инфокоммуникационные технологии в цифровом мире” : сборник докладов. - СПб ГЭУ “ЛЭТИ”, 2012. – С. 3 – 5.

33. Кучерявый, А.Е. Триллионные сети / А.Е.Кучерявый // Телекоммуникации : спецвыпуск, 2013. – С. 19 – 22.

34. Кучерявый, А.Е. Интернет Вещей / А.Е. Кучерявый. - М. : Электросвязь. – 2013. - №1. – С. 21 - 24.

35. Кучерявый, Е.А. Особенности развития и текущие проблемы автомобильных беспроводных сетей VANET / Кучерявый Е.А., Винель, А. В., Ярцев, С. В.// Электросвязь.-2009.-№1.-С.24

36. Кучерявый, Е.А. Принципы построения сенсоров и сенсорных сетей / Е.А. Кучерявый, С.А. Молчан, В.В. Кондратьев//Электросвязь.–2006.-№6.– С.10-15.

37. Молчанов, Д.А. Приложения беспроводных сенсорных сетей / Д.А. Молчанов, Е.А. Кучерявый // Электросвязь. – 2006. - №6. – С. 20 - 23.

38. Молчанов, Д.А. Самоорганизующиеся сети и проблемы их построения / Д.А. Молчанов // Электросвязь. – 2006. - №6. – С. 24 – 28.

39. Мочалов, В.И. Разработка и исследование алгоритмов построения отказоустойчивых сенсорных сетей: автореферат дис. … канд. техн. наук / В.И. Мочалов. – М. : МТУСИ, 2011. – 21 с.

40. Мутханна, А.С. Сравнение протоколов маршрутизации для всепроникающих сенсорных сетей / А.С. Мутханна // Электросвязь.-2014.-№9-С. 5–10.

41. Парамонов, А.И. Модели трафика для сенсорных сетей в u-России / А.Е. Кучерявый, А.И. Парамонов //Электросвязь. – 2006. - №6. – С. 15 - 18.

42. Парамонов, А.И. Миграция речевого трафика в современных сетях связи / А.И.Парамонов, А.Е.Кучерявый//Электросвязь.–2007.- №12. – С. 20 - 22.

43. Росляков, А.В. Интернет Вещей / А.В.Росляков, С.В.Ваняшин, А.Ю. Гребешков, М.Ю. Самсонов. - ПГУТИ, Самара, 2014.-342с.

44. Таненбаум, Э.Д. Компьютерные сети. 5-е издание / Э. Таненбаум, Д. Уэзеролл. – СПб.: Питер., 2012.- С.960

45. Шелухин, О.И. Самоподобие и фракталы. Телекоммуникационные приложения / О.И. Шелухин, А.В. Осин, С.М. Смольский. - М. : Физматлит. – 2008.–368с.

46. Abakumov, P. The Cluster Head Selection Algorithm in the 3D USN . P. Abakumov, A. Koucheryavy // Proceedings, International Conference on Advanced Communication Technology, 2014. ICACT 2014. Phoenix Park, Korea. PP. 462-466.

47. Andreev, S. Energy-Efficient Client Relay Scheme for Machine-to-Machine Communication / S.Andreev, O.Galinina, Y.Koucheryavy // IEEE Globecom 2011, Houston, TX, USA. PP. 1-5.

48. Akyildiz, I.F. Wireless Sensor Networks: A Survey revisited / I.F. Akyildiz, M.C. Vuran, O.B. Akan, W. Su.// Computer Networks Journal, 2005.-45 p.

49. Akyildiz, I.F. Key Wireless Networks Technologies in the Next Decade / I.F. Akyildiz // WWIC 2005 Keynote Speech, Xanthi, Greece, May 2005.

50. Akyildiz, I.F. Nanonetworks: A new communication paradigm / I.F. Akyildiz at all // Computer Networks, Elsevier, 2008. - PP. 2260-2279.

51. Akyildiz, I.F. The Internet of Nano-Things / I.F.Akyildiz, J.M.Jornet // IEEE Wireless Communications. December 2010, V.17, № 6. - PP. 58-63.

52. Al-Naggar, Y. The QoS Estimation for Physiological Monitoring Service in the M2M Network / Y.Al-Naggar, A.Koucheryavy // Internet of Things and its Enablers (INTHITEN). Conference, State University of Telecommunication, St. Petersburg, Russia, June 3-4, 2013. Proceedings. - PP. 133-139.

53. Alrajeh, N.A. Intrusion Detection Systems in Wireless Sensor Networks: A Review / N.A.Alrajeh, S.Khan, B.Shams // International Journal of Distributed Sensor Networks, Volume 2013.-7 p.

54. Attarzadeh, N. A New Three Dimensional Clustering Method for Wireless Sensor Networks / N.Attarzadeh, M.Mehrani // Global Journal of Computer Science and Technology. V.11, issue 6, version 1.0, April 2011. – 6 p.

55. Aziz, A. Adaptive and Efficient Compressive Sensing based Technique for Routing in Wireless Sensor Networks / A.Aziz, A.Salim, W.Osamy // Proceedings, INTHITEN (IoT and its Enablers) conference. St.Petersburg, State University of Telecommunication, 3-4 June, 2013. - PP. 46-59.

56. Benmansour, T. GMAC: Group Mobility Adaptive Clustering Scheme for Mobile Wireless Sensor Networks / T.Benmansour, S.Moussaoui // International Symposium on Programming and Systems (ISPS). Proceedings, Algiers, Algeria, 25-27 April, 2011.- PP. 67-73.

57. Birke, R. Experience of VoIP Traffic Monitoring in a Commercial ISP / Birke, R., Mellia, M., Petracca, M., Rossi, D. // International Journal of Network Management, vol. 20, Issue 5, 2010. - PP. 339-359.

58. Bhattasali, T.R. A Survey of Recent Intrusion Detection Systems in Wireless Sensor Networks / T.Bhattasali, R.Chaki // Advanced in Network Security and Applications. Conference Proceedings of Fourth International Conference on Network security and Applications (CNSA 2011), Chennai, India, July 15-17, 2011. - PP. 268-280.

59. Bhattassali, T. Sleep Deprivation Attack Detection in Wireless Sensor Networks / T.Bhattassali, R.Chaki, S.Sanyal // International Journal of Computer Applications, v.40, №15, February 2012.- PP. 19-25.

60. Bogdanov, I. The mobile Sensor Network Life-Time under Different Spurious Flows Intrusion / I.Bogdanov, A.Koucheryavy, A.Paramonov // LNCS, Springer. 13 th NEW2AN, LNCS 8121, August, 2013. - PP. 312-317.

61. Borsani, L. Tree-Based Routing Protocol for Wireless Sensor Networks / L.Borsani, S.Guglielmi, A.Redondi, M.Cesana // 8th International Conference on Wireless On-Demand Network Systems and Services, WONS'2011, Bardoneecchia, Italy, January 2011. - PP.164-170.

62. Chatterjee, M. WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks / M. Chatterjee et al // Journal of Cluster Computing, V. 5/2, April, 2002.- PP. 193-204.

63. Chen, B. Span: an energy efficient coordination algorithm for topology maintenance in ad hoc wireless networks / B. Chen, K. Jamieson, H. Balakrishnan, R. Morris // Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, 2001.- 12 p

64. Chen, H. Energy residue aware (ERA) clustering algorithm for leach-based wireless sensor networks / H. Chen, C. S. Wu, Y. S. Chu, C. C. Cheng, and L. K. Tsai //2nd Int. Conf. Systems and Networks Communications (ICSNC), Proceedings, Cap Esterel, French Riviera, France, Aug. 2007.-40 p

65. Mark E. Crovella. Self-Similarity in Wide Web Traffic: Evidence and Possible Causes / Mark E.Crovella, Azer Bestavors //IEEE/ACM Transaction on Networking, Vol 5, Number 6, December, 1997. - PP.835-846.

66. Dashkova, E. Survey on Congestion Control Mechanism for Wireless Sensor Networks / E.Dashkova, A.Gurtov // The 12th International Conference on Next Generation Wired/Wireless Networking NEW2AN 2012. Aug. 2012 Saint-Petersburg. Springer LNCS 7469. - PP.75-85.

67. Drajic, D. Traffic Generation Application for Simulating Online Games and M2M applications via Wireless Networks / D.Drajic and all // 9th Conference on

Wireless On-demand Network Systems and Services WONS 2012, January 9-11, 2012. Courmayeur, Italy. - PP.167-174.

68. Mohsin Fayyaz. Classification of Object Tracking Techniques in Wireless Sensor Networks / Mohsin Fayyaz // Wireless sensor Networks, April 2011, №3. - PP.121-124.

69. Garg, V. Wireless Communications and Networking / V.Garg // Morgan Kaufmann, 2006.

70. Gorlatova M. Energy Harvesting Active Networked Tags (EnHANTs) for Ubiquitous Object Networking /M.Gorlatova at all //IEEE Wireless Communications, December 2010, v.17, №6. - PP.18-25.

71. Dong-Won Seo. Explicit Formulae for Characteristics of Finite-Capacity M/D/1 Queues [Электронный ресурс] / Dong-Won Seo // ETRI Journal, Volume 36, Number 4, August 2014.-PP.609-616. Режим доступа: http:// http://etrij.etri.re.kr – (Дата обращения: 25.09.2016).

72. Tian, He. Achieving Real-Time Target Tracking Using Wireless Sensor Networks / Tian He and all // 12th IEEE Real-Time and Embedded Technology and Applications Symposium. April 4-7, 2006, San Jose, California, USA.-PP.37-48.

73. Heinzelman, W. Adaptive protocols for information dissemination in wireless sensor networks / W. Heinzelman, J. Kulik, H. Balakrishnan // Proceedings, ACM/IEEE 5th International Conference Mobile Computing and Networking MobiCom. Seattle, Washington, USA, Aug. 1999.-PP.174-185.

74. Heinzelman, W. An application specific protocol architecture for wireless microsensor networks / W. Heinzelman, A. Chandrakasan, H. Balakrishnan // IEEE Transactions on Wireless Communications 1 (4), 2002.-PP.660-670.

75. Heinzelman, W. Energy-efficient communication protocol for wireless microsensor networks / W. Heinzelman, A. Chandrakasan, H. Balakrishnan // Proceedings 33rd Hawaii International Conference on System Sciences (HICSS), Wailea Maui, Hawaii, USA, Jan. 2000. PP.3005-3014.

76. Ho, J. Throughput and buffer analysis for GSM general packet radio service / J.Ho, Y. Zhu, S.Madhavapaddy // Proceedings WCNC'99, New Orleans, USA, September 1999.-PP.1427-1431.

77. Iera, A. The Internet of Things / A.Iera, C.Floerkemeier, J.Mitsugi, G.Morabito // IEEE Wireless Communications. December 2010, v.17, №6.-PP. 8-9.

78. Internet 3.0. The Internet of Things. Analysis Mason Limited, 2010.

79. IoT Strategic Research Roadmap [Электронный ресурс] / IoT European Research Cluster, 2012.- Режим доступа: https: http://www.internet-of-things-research.eu. - (Дата обращения: 12.09.2016).

80. ITU Technology Watch Report. E-health Standards and Interoperability [Электронный ресурс] / Geneva, April, 2012.-p24.- Режим доступа: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000170001PDFE.pdf. - (Дата обращения: 25.09.2016).

81. Janevski, T. Statistical Analysis of Multicast versus Instant Channel Changing Unicast IPTV Provisioning / Janevski, T., and Vanevski, Z. // 16th Telecommunications Forum TELFOR 2008, Belgrade, Serbia, 25-27 November 2008, PP. 96-99.

82. Kim, D.-S. Self-Organization Routing Protocol Supporting Mobile Nodes for Wireless Sensor Networks / D.-S. Kim, Y.-J. Chung // IMSCCS'06. Proceedings. Zhejiang University, China, June 20-24, 2006.-PP. 622-626.

83. Koucheryavy, A. Cluster head selection for homogeneous Wireless Sensor Networks / A. Koucheryavy, A. Salim // Proceedings, International Conference on Advanced Communication Technology, 2009. ICACT 2009. Phoenix Park, Korea.-PP.2141-2148.

84. Koucheryavy, A. Cluster-based Perimeter-coverage Technique for Heterogeneous Wireless Sensor Networks / A. Koucheryavy, A. Salim // Proceedings, ICUMT 2009 International Conference IEEE on Ultra Modern Telecommunications, Saint-Petersburg, Russian. 2009.-PP. 1-7.

85. Koucheryavy, A. The Video Streaming Monitoring in the Next Generation Network / A.Koucheryavy, D.Tarasov, A.Paramonov // LNCS, Springer. 9 th NEW2AN, LNS 5764, 15-18, September, 2009.-PP.191-205.

86. Koucheryavy, A. Prediction-based Clustering Algorithm for Mobile Wireless Sensor Networks / A. Koucheryavy, A. Salim // Proceedings, International Conference on Advanced Communication Technology, 2010. ICACT 2010. Phoenix Park, Korea.-PP.1209-1215.

87. Koucheryavy, A Ubiquitous Sensor Networks Traffic Models for Telemetry Applications / A.Koucheryavy, A.Prokopiev // Smart Spaces and Next Generation Wired/Wireless Networking.11th International Conference, NEW2AN 2011, and 4th Conference on Smart Spaces, ruSMART 2011. St.Petersburg, Russia, August 2011, Proceedings. LNCS 6869. Springer, 2011, PP.287-294.

88. Koucheryavy, A. Ubiquitous Sensor Networks Traffic Models for Medical and Tracking Applications / A. Koucheryavy, A. Vybornova // in The 12th International Conference on Next Generation Wired/Wireless Networking NEW2AN 2012. Aug. 2012 Saint-Petersburg. Springer LNCS 7469 - PP. 338-346.

89. Koucheryavy, A. Ubiquitous Sensor Networks Traffic Models for Image Applications / A.Koucheryavy, A.Muthanna, A.Prokopiev // Internet of Things and its Enablers (INTHITEN). Conference, State University of Telecommunication, St. Petersburg, Russia, June 3-4, 2013. Proceedings.- PP. 124-131.

90. Koucheryavy, A. State of Art and Research Challenges for USN Traffic Flow Models / A.Koucheryavy // ICACT'2014, Proceedings, 16-19 February, Phoenix Park, Korea.- PP. 336-340.

91. Koucheryavy, Y. Research Challenges in Vehicular Ad hoc Networks / Y.Koucheryavy, J. Jakubiak // Proceedings, IEEE CCNC 2008, January 10-12, 2008. Las Vegas, USA.- PP.912-916.

92. Chih-Yu Lin, Efficient In-Network Moving Object Tracking in Wireless Sensor Networks / Chih-Yu Lin, Wen-Chih Peng, and Yu-Chee Tseng // IEEE Transaction on Mobile Computing. V.5, issue 8, 2006.- PP.1044-1056.

93. Lindsey, S. PEGASIS: Power-efficient gathering in sensor information systems / S. Lindsey, C. S. Raghavendra // Proceedings IEEE Aerospace Conference, vol. 3, Big Sky, Montana, USA, 2002.- PP.1125-1130.

94. Markovich, N.M. Statistical Analysis and Modeling of Peer-to-Peer Multimedia Traffic / Markovich, N.M., Krieger, U.R. // LNCS 5233, Next Generation Internet (Ed. D.Kouvatsos), 2011.- PP.70-97.

95. Marrocco, G. Pervasive Electromagnetics: Sensing Paradigms by Passive RFID Technology / G.Marrocco //IEEE Wireless Communications. December 2010, V.17, № 6.- PP.10-17.

96. Nickerson, J.V. Protecting with Sensor Networks: Attention and response / J.V.Nickerson, S.Olariu // HICSS 2007. 40th Hawaii International Conference on System Science. 3-6 January, 2007. Waikoloa, Big Island, HI, USA.- 10p.

97. Norros, I. The Management of Large Flows of Connectionless Traffic on the Basis of Self-similar Modeling / Norros, I. // International Conference on Communications ICC'95. Proceedings, 18-22 June 1995, Seattle, USA.- PP.451-455.

98. Potsch, T. Influence of Future M2M Communication on the LTE System / T.Potsch, S.N.K.Marwat, Y.Zaki, C.Gorg // Wireless and Mobile Networking Conference. Dubai, United Arab Emirates, 23-25 April, 2013.- 4 p.

99. Recommendation Q.3925. Traffic Flow Types for Testing Quality of Service Parameters on Model Networks. March 2012, ITU-T, Geneva.

100. Recommendation Y. 1541. Network Performance Objectives for IP-based Services. 2006.

101. Recommendation Y. 2221. Requirements for Support of Ubiquitous Sensor Network (USN) Applications and Services in the NGN Environment. 2010.

102. Recommendation ITU-T Y.2281. Framework of networked vehicle services and applications using NGN. ITU-T, 2011.

103. Recommendation Y.2060. Overview of Internet of Things. ITU-T, February 2012, Geneva.

104. Recommendation Y.2069. Framework of the WEB of Things. ITU-T, July 2012, Geneva.

105. Recommendation Y.2062. Framework of Object-to-Object Communication using Ubiquitous Networking in NGN. ITU-T, February 2012. Geneva.

106. Recommendation Y.2051. General Overview of IPv6-based NGN. ITU-T, February 2008. Geneva.

107. Recommendation H.235.0. H.323 Security: Framework for Security in ITU-T H-series (ITU-T H.323 and other ITU-T H.245-based) Multimedia Systems. ITU-T, January 2014. Geneva.

108. Recommendation Y.2221. Requirements for Support of USN Applications and Services in the NGN Environment. ITU-T, January 2010, Geneva.

109. Recommendation Y.2701. Security Requirements for NGN Release 1. ITU-T, Geneva, April 2007.

110. Recommendation X.805. “Security Architecture for Systems Providing End-to-End Communications”. ITU-T, Geneva, October, 2003.

111. Recommendation X.1311. Security Framework for Ubiquitous Sensor Networks. ITU-T, Geneva, February 2011.

112. Rosario, D. A Comparative Analysis of Beaconless Opportunistic Routing Protocols for Video Dissemination over Flying Ad-Hoc Networks / D.Rosario, Z.Zhao, T.Braun, E.Cerqueira, A.Santos // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. The 14th International Conference NEW2AN 2014. Aug. 2014 Saint-Petersburg. Springer LNCS 8638.- PP.253-265.

113. Schneps-Schneppe, M. M2M Applications and Open API: What Could Be Next? / M.Schneps-Schneppe, D.Namiot // in The 12th International Conference on Next Generation Wired/Wireless Networking NEW2AN 2012. Aug. 2012 Saint-Petersburg. Springer LNCS 7469.- PP. 429-439.

114. Schneps-Schneppe, M. On M2M communications standards for smart metering. Internet of Things and its Enablers (INTHITEN). / M.Schneps-Schneppe, A.Maximenko, D.Namiot // Conference, State University of Telecommunication, St. Petersburg, Russia, June 3-4, 2013. Proceedings.- PP.15-18.

115. Shafig, M.Z. A First Look at Cellular Machine-to-Machine Traffic: Large Scale Measurement and Characterization. / M.Z.Shafig and all.// 12th ACM Sigmetrics/Performance International Conference. June 11-15, London, England, UK, 2012.- PP.65-76.

116. Shelby, Z. Embedded Web Services / Z.Shelby // IEEE Wireless Communications. December 2010, V.17, № 6.- PP.52-57.

117. Sorensen, L. Use scenarios 2020 – a worldwide wireless future. Visions and research directions for the Wireless World / L.Sorensen, K.E.Skouby // Outlook. Wireless World Research Forum. July 2009, №4.- 42 p.

118. Tharini, C. An Energy Efficient Spatial Correlation Base Data Gathering Algorithm for Wireless Sensor Networks / C. Tharini, V. Ranjan //. International Journal of Distributed and Parallel Systems (IJDPS), v.2, №3, May, 2011.- PP.16-24.

119. Vybornova, A. Traffic Analysis in Target Tracking Ubiquitous Sensor Networks. / A.Vybornova, A.Koucheryavy // In The 14th International Conference on Next Generation Wired/Wireless Networking NEW2AN 2014. Aug. 2014 Saint-Petersburg. Springer LNCS 8638.- PP.389-398.

120. Waldner, J.-B. Nanocomputers and Swarm Intelligence / J.-B.Waldner // ISTE, Wiley&Sons, 2008).- 285 p.

121. W.Willinger, M.Taqqu, R.Sherman, D.Wilson. Self-similarity through high-variability IEEE/ACM Transactions on Networking, Vol. 5, No. 1, 1997.- PP.71-86.

122. Younis, O. Node clustering in wireless sensor networks: Recent developments and deployment challenges / O. Younis, M. Krunz, S. Ramasubramanian // IEEE Network, vol. 20, no. 3, 2006.- PP.20-25.

123. Хоанг, Л.Ч. Модель периметрической защиты беспроводной сенсорной сети от потоков ложных событий / Хоанг Л.Ч., Парамонов А.И., Кучерявый А.Е. // Информационные технологии и телекоммуникации, 2015, №1 (9)-С.145-156.

124. Киричек, Р.В. Ложные облака для Интернета Вещей. Методы защиты. / Киричек Р.В., Кулик В.А., Владыко А.Г., Богданов И.А., Кучерявый А.Е. // Информационные технологии и телекоммуникации, 2015, №3 (11), с.27-39.

125. Богданов, И.А. Ложные структуры в Интернете Вещей. / Богданов И.А., Кучерявый А.Е. // Информационные технологии и телекоммуникации, 2015, №4 (12). - С.4-10.

126. Гимадинов, Р.Ф. Кластеризация в сетях 5G / Гимадинов Р.Ф., Мутханна А.С., Кучерявый А.Е. // СПбГУТ. Информационные технологии и телекоммуникации. 2015. - №1(9). - С.35-41.

127. Аль-Наггар, Я.М Кластеризация в беспроводных нательных сенсорных сетях / Аль-Наггар, Я.М // СПбГУТ. Информационные технологии и телекоммуникации. 2015. - №1(9). - С.4-18

128. Динь Чыонг Зюи. Обзор методов инсталляции сенсорных узлов с квадрокоптера / Динь Чыонг Зюи, Киричек Р.В., Кучерявый А.Е. // СПбГУТ. Информационные технологии и телекоммуникации. 2015. - №1(9). - С.50-61.

129. Захаров, М.В. Задача распределения ресурсов в группах БПЛА / Захаров М.В., Киричек Р.В., Парамонов А.И. // СПбГУТ. Информационные технологии и телекоммуникации. 2015. - №1(9). - С.62-70.

130. Парамонов, А. И. Разработка и исследование комплекса моделей трафика для сетей связи общего пользования: дис. на соиск. учен. степ. доктора техн. наук (05.12.13) / Парамонов Александр Иванович; СПбГУТ. – СПб, 2014. – 325 с.

Приложение

Акты о внедрении

Утверждаю

Заместитель первого проректора –

начальник учебного управления

к.т.н. С. И. Ивасишин

9.09.16

Акт

о внедрении научных результатов,

полученных Богдановым Игорем Александровичем в диссертационной работе "Исследование потоков ложных событий в беспроводных сенсорных сетях".

Комиссия в составе декана факультета Инфокоммуникационных сетей и систем Л.Б. Бузюкова, заместителя заведующего кафедрой сетей связи и передачи данных Р.В. Киричка и заведующей лабораторией кафедры сетей связи и передачи данных А.Ф. Вороновой составила настоящий акт в том, что научные результаты, полученные в диссертации "Исследование потоков ложных событий в беспроводных сенсорных сетях", использованы при чтении лекций, проведении практических занятий и лабораторных работ по следующей дисциплине:

1. Интернет Вещей и самоорганизующиеся сети (Рабочая Программа № 02.12.12/717, утверждена Первым проректором-проректором по учебной работе Г.М. Машковым 18.09.2015), разделы Программы:

– Ad Hoc или самоорганизующиеся сети. Приложения самоорганизующихся сетей. Всепроникающие сенсорные сети как технологическая основа внедрения концепции Интернета Вещей. Кластеризация сенсорных сетей и основные методы кластеризации, включая биоподобные алгоритмы. Особенности сетевой безопасности в сенсорных сетях.

При этом используются следующие новые научные результаты, полученные И.А. Богдановым в диссертационной работе:

– модель вторжения в беспроводную сенсорную сеть на основе потоков ложных событий,

– зависимость длительности жизненного цикла беспроводной сенсорной сети от вида потока ложных событий,

– метод защиты беспроводной сенсорной сети от потоков ложных событий, состоящий в придании сенсорным узлам мобильности,

– метод защиты беспроводных сенсорных сетей от потоков ложных событий, состоящий в изменении распределения плотности сенсорных узлов по сравнению с равномерной.

Декан факультета ИКСС Л.Б. Бузюков

Зам. заведующего кафедрой сети связи Р.В. Киричек

Зав. лабораторией кафедры сетей связи А.Ф. Воронова

АКЦИОНЕРНОЕ ОБЩЕСТВО
МОСКОВСКИЙ ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ РАДИОТЕХНИЧЕСКИЙ ИНСТИТУТ
(АО «МНИРТИ»)
JSC «MOSCOW RESEARCH SCIENTIFIC RADIO COMMUNICATION INSTITUTE»

РОССИЙСКАЯ ФЕДЕРАЦИЯ, 109028, МОСКВА, БОЛЬШОЙ ТРЕХСВЯТИТЕЛЬСКИЙ ПЕР., Д.2/1
ТЕЛ.: 495 917-09-90, 495 626-23-68, ФАКС: 495 917-34-23, E-mail: astra@mnirti.ru

_____№_____

на №_____от_____

УТВЕРЖДАЮ

Заместитель генерального
директора по научной работе
АО «МНИРТИ», д.т.н., профессор

АО «МНИРТИ» _____ А.В.Шевырев

«24» марта 2016 г.

АКТ

внедрения результатов диссертационной работы И.А. Богданова на тему «Исследование потоков ложных событий в беспроводных сенсорных сетях», представленную на соискание ученой степени кандидата технических наук

Комиссия АО «МНИРТИ» в составе:

Председатель – начальник отдела, д.т.н., профессор Л.О. Мырова;

Члены комиссии – начальник отдела А.Г. Самородов; начальник сектора, к.т.н. П.Н. Пименов; ведущий инженер, к.т.н. И.А. Фомина

составила настоящий акт о том, что в диссертационной работе И.А. Богданова на тему «Исследование потоков ложных событий в беспроводных сенсорных сетях» рассмотрен ряд важных теоретических и практических положений, имеющих существенное значение для проектирования и разработки программного обеспечения бортового радиоэлектронного оборудования летательных аппаратов, в том числе и беспилотных (БЛА).

Принципиально важным является новый методический аппарат, позволяющий оценить степень вторжения в беспроводную сенсорную сеть бортовых радиоэлектронных средств (БРЭС) БЛА и разработать комплекс мероприятий для защиты и диагностики перспективных БРЭС летательных аппаратов.

Основные результаты диссертационной работы внедрены в практику деятельности АО «МНИРТИ» при создании перспективного бортового оборудования беспилотных летательных аппаратов в работах ОКР «ЛИСт», а именно:

- модель вторжения в беспроводную сенсорную сеть путем создания потоков ложных событий;

- метод защиты беспроводных сенсорных сетей в условиях создания ложных событий путем изменения структурных характеристик сенсорного поля, состоящего в изменении распределения плотности сенсорных узлов по сравнению с равномерной.

Следует отметить практическую полезность экспериментальных результатов, внедрение которых позволит значительно сократить стоимость мероприятий на возможную последующую доработку изделия.

Председатель комиссии Л.О. Мырова

Члены комиссии П.Н. Пименов

И.А. Фомина

УТВЕРЖДАЮ
Заместитель начальника академии
по учебной и научной работе
доктор технических наук профессор
полковник
Ю.Кулешов
«25» августа 2016 г.

АКТ
о внедрении результатов диссертационной работы
Богданова Игоря Александровича
«Исследование потоков ложных событий в беспроводных сенсорных сетях»
в учебный процесс Военно-космической академии
имени А.Ф.Можайского

Комиссия в составе: председателя комиссии – врио начальника учебно-методического отдела подполковника Пальгунова В.Ю.; членов комиссии заместителя начальника 24 кафедры кандидата технических наук доцента полковника Васильева А.С., старшего преподавателя 24 кафедры кандидата технических наук подполковника Соколовского А.Н. установила, что основные научные результаты диссертационной работы Богданова Игоря Александровича внедрены в учебный процесс академии на 24 кафедре (информационно-вычислительных систем и сетей) по дисциплине «Компьютерные сети и сетевые технологии» по специальности «Эксплуатация и администрирование вычислительных систем и сетей», а именно:

в текст лекции № 7 («Беспроводные локальные сети», 2 часа) включено рассмотрение следующих актуальных вопросов:

зависимость длительности жизненного цикла беспроводной сенсорной сети от свойств потока ложных событий;

метод защиты беспроводной сенсорной сети от потоков ложных событий, состоящий в придании сенсорным узлам мобильности.

Изменения, внесенные в текст лекции № 7, рассмотрены и одобрены на заседании 24 кафедры (информационно-вычислительных систем и сетей) Военно-космической академии имени А.Ф.Можайского (протокол № 4 от 25.03.2016 г.).

Внесение изменений и дополнений в учебно-методические материалы темы № 1 «Принципы построения компьютерных сетей» по дисциплине «Компьютерные сети и сетевые технологии» позволили:

более широко раскрыть особенности внедрения и обеспечения функционирования сетей ЭВМ на основе анализа свойств потока ложных событий;

повысить понимание обучающимися принципов обеспечения безопасной передачи данных в беспроводных компьютерных сетях.

Результаты внедрения диссертационных исследований в учебный процесс академии рассмотрены и обсуждены на заседании 24 кафедры (информационно-вычислительных систем и сетей) (протокол № 12 от 24.08.2016 г.).

Председатель комиссии: врио начальника учебно-методического отдела
подполковник
В.Пальгунов

Члены комиссии: заместитель начальника кафедры
информационно-вычислительных систем и сетей
кандидат технических наук доцент
полковник
А.Васильев

старший преподаватель кафедры
информационно-вычислительных систем и сетей
кандидат технических наук
подполковник
А.Соколовский