

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

УДК 004.057.4: 621.391

Нгуен Чонг Тхань
Алгоритмы защиты мобильных ad-hoc сетей от несанкционированного
доступа

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-36 80 08 «Инженерная геометрия и компьютерная
графика»

Научный руководитель
Цветков Виктор Юрьевич
профессор кафедры ИКТ
профессор; доктор технических наук

Минск 2023

ВВЕДЕНИЕ

В настоящее время беспроводные сети широко используются в жизни. Известные своим удобством использования и высокой эстетикой, когда не нужны провода, беспроводные сети присутствуют в таких областях, как развлечения, образование, транспорт и особенно беспроводные сети, отвечающие строгим требованиям в армии.

Поскольку для передачи сигналов не требуются провода, беспроводные сети используют радиоволны в качестве среды передачи, что позволяет узлам в сети свободно перемещаться. Более того, сетевые узлы могут выступать как в качестве терминалов, так и в качестве промежуточных узлов при передаче сигналов, таких как маршрутизаторы.

В рамках данной диссертации автор фокусируется на исследовании мобильной одноранговой сети - модели беспроводной сети, в которой узлы сети имеют характеристики непрерывного движения, энергия для узлов ограничена и обусловлена характером сети. вещество, передающееся с помощью радиоволн, поэтому его очень легко атаковать путем фальсификации пакетов или даже разрушения всей конфигурации сети.

В поставленной проблеме атака вредоносных узлов, зараженных вредоносным кодом, приводит к изменению протокола маршрутизации этих узлов, что приводит к тому, что пакет при передаче на зараженный узел вместо этого будет прерван, потому что пересылка на узел назначения.

Основной целью диссертации является изучение форм атак в MANET, в частности атака «черная дыра» на протокол маршрутизации AODV, из чего можно установить оценку производительности по таким параметрам, как коэффициент успешной передачи пакетов данных, средняя задержка. Проанализируйте и оцените производительность некоторых расширенных протоколов маршрутизации, таких как IDSAODV, RAODV. На основе этого анализа даются идеи, решения и предложения по улучшению протокола AODV для предотвращения атак черной дыры.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы магистерской диссертации:

В настоящее время, в связи с сильным развитием информационных технологий, это глубоко затронуло большинство сфер жизни. Значительное увеличение количества портативных мобильных устройств, таких как мобильные телефоны, планшеты и т. д. С функцией беспроводной связи, создает множество проблем в оптимизации пропускной способности и механизме управления безопасностью, безопасной связи между устройствами. Мобильная беспроводная сеть (MANET) — это сеть, в которой он состоит из автономных самоуправляемых узлов без какой-либо инфраструктуры. Каждый сетевой узел играет роль хоста и берет на себя функцию маршрутизатора данных. Из-за своей небезопасной природы мобильные беспроводные сети являются целью большинства атак от самого нижнего уровня до самого высокого в модели OSI, особенно на сетевом уровне.

Цель и задачи исследования:

Целью работы является повышение защищенности сети manet от несанкционированного доступа.

Для достижения поставленной цели решались следующие задачи:

- исследовать характеристики Ad hoc сети;
- исследовать уязвимость, типы атак в Ad hoc сети, особенно атак на протоколы маршрутизации сети Ad hoc сети;
- исследовать протоколов безопасной маршрутизации в MANET
- имитировать MANET-атаки с помощью программного обеспечения NS2.

Объект исследования: защищенность протоколов маршрутизации ad hoc сети от атак.

Предмет исследования: зависимости защищенности протоколов маршрутизации ad hoc сети от типов атак, алгоритмов защиты и условий функционирования.

Магистерская диссертация выполнена самостоятельно, проверена в системе «Антиплагиата». Процент оригинальности составил 82,17%. Заимствования, самоцитирования и цитирования обозначены ссылками на публикации, указанные в «Списке литературы».

Основные положения, выносимые на защиту

- Характеристики MANET, проблемы сетевой безопасности, с которыми сталкиваются MANET, особенно на сетевом уровне.

– Исследование распространенных атак в MANET и протоколов маршрутизации безопасности MANET.

– Как отредактировать, чтобы создать новый протокол в программе моделирования NS2.

– Моделирование протоколов безопасной маршрутизации MANET с атакой черной дыры, используя программное обеспечение для эмуляции NS2. Оттуда проанализируйте полученные результаты, чтобы оценить производительность протоколов маршрутизации.

Публикации

Основные положения работы и результаты диссертации представлены в статье в периодическом научном журнале.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, четыре главы с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

Первая глава: Обзор технологий Мобильных сети ad-hoc.

Вторая глава: Проблемы безопасности в MANET, методы атак в MANET.

Третья глава: Атака черной дыры на протокол маршрутизации AODV и некоторые меры по предотвращению атак черной дыры.

Четвёртая глава: Оценка безопасных протоколов маршрутизации в manet с использованием эмулятора ns2

Общий объем диссертации составляет 82 страница включая 40 иллюстрации, 15 таблицы, библиографический список из 30 наименований, 4 приложения.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** разделе представлены вопросы, изучаемые в диссертационной работе.

В **первой главе** представлен обзор технологий MANET, их характеристики и назначения, протоколы маршрутизации.

Во **второй главе** представлены проблемы безопасности в MANET и методы атаки в протоколе сетевой маршрутизации MANET.

В **третьей главе** представлена атака черной дыры, уязвимость протокола маршрутизации AODV и методы улучшения протокола AODV для защиты от атак черной дыры, таких как SAODV, ARAN, IDSAODV, RAODV.

В **четвертой главе** введение в программное обеспечение для моделирования NS2 и как установить атаку черной дыры, установить протоколы безопасной маршрутизации IDSAODV, RAODV. Оттуда настроить симуляции и оценить производительность протоколов безопасной маршрутизации на основе параметров: коэффициент успешной доставки пакетов, средняя задержка и - Накладные расходы маршрутизации.

В **заключении** сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

В данной диссертации было сделано основное исследование о вызовах и угрозах безопасности, а также влиянии атаки черной дыры в протоколе AODV. Были представлены некоторые решения для борьбы с атаками черной дыры, такие как IDSAODV и RAODV. Кроме того, в диссертации использовался инструмент моделирования NS-2 для симуляции процесса атаки черной дыры и оценки эффективности предлагаемых решений через несколько различных сценариев. Результаты симуляции показывают следующие выводы:

- В нормальных условиях, когда узлы сети перемещаются со скоростью 0 - 15 м/с, протоколы AODV и IDSAODV достигают очень высокой производительности, протокол RAODV несколько ниже.

- Когда в сети появляется атака черной дыры и количество узлов черной дыры увеличивается, производительность протокола AODV заметно снижается, вызывая большие потери пакетов. Хотя протокол IDSAODV снижает плохое влияние от узла черной дыры, эффективность не высока, преимущество этого решения в том, что оно не генерирует новые пакеты, не вызывает задержек в сети. Протокол RAODV имеет более высокую производительность и стабильность, чем предыдущее решение, но недостаток этого решения в том, что он вызывает задержки в сети, общая стоимость во много раз выше, чем у двух протоколов AODV и IDSAODV.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Нгуен Ч.Т. Атака червоточины в мобильных ad-hoc сетях / Ч.Т. Нгуен // информационная безопасность: Сборник материалов 59-ой научной конференция аспирантов, магистрантов и студентов БГУИР, Минск, 17 – 21 апреля 2023 г. – Минск : БГУИР, 2023. – С. 122 – 126.
2. Нгуен Ч.Т. Моделирование проколов маршрутизации при атаке чёрной дыры в мобильных ad-hoc сетях / Ч.Т. Нгуен // информационная безопасность: Сборник материалов 59-ой научной конференция аспирантов, магистрантов и студентов БГУИР, Минск, 17 – 21 апреля 2023 г. – Минск : БГУИР, 2023. – С. 127 – 131.