Математические структуры и моделирование
2014. № 4(32). С. 247–253

УДК 004.056.57

РАЗРАБОТКА И ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА МЕТОДОВ ЗАЩИТЫ БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ

Д.А. Москвин
кандидат технических наук, доцент, e-mail: moskvin@ibks.ftk.spbstu.ru
Д.В. Иванов
аспирант, e-mail: 9361023@gmail.com

Санкт-Петербургский государственный политехнический университет

Аннотация. Рассматривается безопасность беспроводных самоорганизующихся сетей, исследована и проанализирована атака «Чёрная дыра», направленная на нарушение работоспособности таких сетей, а также приведены рекомендации по борьбе с ней.

Ключевые слова: самоорганизующиеся сети, ad-hoc, mesh, безопасность, атака.

Международный опыт последних лет показывает, что привычная ИТ-инфраструктура в любой момент может дать сбой, обусловленный совершенно разными причинами. После этого связь определённого сегмента с остальной сетью теряется. Например, на Гаити после землетрясения в 2010 году главным средством связи стали спутниковые телефоны, предоставленные в качестве помощи. Использование таких телефонов стало скорее вынужденной мерой, а не эквивалентной альтернативой существующим средствам связи. Основная проблема в том, что не только природные катаклизмы способны вывести из строя современную инфраструктуру, но и банальное отключение электропитания способно превратить наши мобильные устройства и компьютеры в «бесполезные игрушки» [1, с. 297].

Адекватной реакцией на такие проблемы является растущий интерес к идее создания беспроводной самоорганизующейся (или динамической, ad-hoc) сети. Беспроводные самоорганизующиеся сети — децентрализованные сети, не имеющие постоянной структуры. Клиентские устройства соединяются «на лету», образуя между собой сеть. Каждый узел сети может являться посредником в передаче данных, предназначенных другим узлам. При этом поиск получателя данных производится динамически, на основании текущей связности сети. Данная особенность беспроводных самоорганизующихся сетей является их основным отличием от проводных сетей и управляемых беспроводных сетей, в которых задачу управления потоками данных выполняют маршрутизаторы (в проводных сетях) или точки доступа (в управляемых беспроводных сетях). Такая сеть способна формировать сама себя каждый раз, когда специальным образом запрограммированные мобильные устройства (телефоны, планшеты,

ноутбуки и др.) оказываются в пределах прямого доступа. Каждое из таких устройств исполняет роль и приёмника, и передатчика, а также является ретранслятором для других устройств в сети. Устройства, расстояние между которыми превышает дальность прямого доступа, могут поддерживать между собой связь посредством других устройств в сети, образуя, таким образом, подобие цепочки из узлов, где каждый из них передаёт информацию своему соседу [2, с. 43].

Использование самоорганизующихся сетей будет полезно не только в случае стихийных бедствий. Такие сети будут также востребованы в случае, если возведение стационарной базы является слишком дорогостоящим, долгим или трудоёмким процессом. Например, удалённые поселения, возведение в которых стационарных баз не планируется, смогут получить доступ в сеть Интернет посредством беспроводных самоорганизующихся сетей. Другой пример — при организации «умного» дома все домашние устройства смогут передавать информацию друг другу, освобождая от необходимости прокладки дополнительных проводов и объединяя всю домашнюю технику в один удобный комплекс. Также сети подобного класса широко применяются военными ведомствами разных стран для организации оперативной связи в тактических целях, например, во время проведения антитеррористических операций, в зонах локальных военных конфликтов.

Плюс ко всему вышеперечисленному, в последнее время получили распространение телекоммуникационные сети передачи данных, организованные в соответствии с топологией самоорганизующихся сетей. Масштабы таких проектов увеличились до сотен тысяч пользователей по всему миру. Сети с динамической организацией предоставляют наиболее практичные решения, интегрирующие различные беспроводные технологии. Возможность организации с помощью динамической топологии локальных и городских (LAN и MAN) сетей, легко интегрируемых в глобальные сети (WAN), является хорошей перспективой для операторов связи, разворачивающих свои сети в мегаполисах, и это ещё раз подтверждает релевантность и актуальность использования самоорганизующихся сетей.

Известные атаки на сети с динамической организацией на самом верхнем уровне делятся на пассивные и активные. Пассивные атаки преследуют лишь цель прослушивания и перехвата передающейся в сети информации (нарушение конфиденциальности), что делает их крайне тяжёлыми для обнаружения. Активные атаки, в свою очередь, направлены на непосредственное взаимодействие с информацией в сети: изменение или скрытие пакетов данных является основной целью таких атак (нарушение целостности и доступности). Также различают атаки внешние (организует внешний нарушитель) и внутренние (внутренний нарушитель).

Наиболее специфичной для самоорганизующихся сетей является атака «Чёрная дыра». Она заключается в том, что устройство-злоумышленник маскируется под узел сети, через который проходит кратчайший путь к узлу, информацию от и для которого злоумышленник хочет получить. На самом деле узел-злоумышленник может быть вообще не связан с узлом-жертвой в рамках

сети.

Традиционным методом решения проблем безопасности в беспроводных самоорганизующихся сетях является использование шифрования на прикладном уровне, что не всегда удобно, требует лишних затрат ресурсов, а также не защищает от угроз, направленных на доступность информации. Поэтому для обеспечения безопасности сетей с динамической организацией необходимо применять специфические методы защиты.

Многие протоколы взаимодействия в сетях с динамической организацией используют следующий механизм для нахождения оптимального пути до узла цели: узел-инициатор посылает широковещательный RREQ-запрос, который запускает процедуру поиска кратчайшего маршрута. Каждый последующий узел сети передаёт RREQ-запрос дальше по цепочке, пока он не дойдёт до узла-цели. Узел-цель ответит RREP-ответом, который будет передан в обратном направление через те же узлы, что и RREQ-запрос [3, с. 2].

Атака «Чёрная дыра» реализуется за счёт того, что узел-злоумышленник может, получив RREQ-запрос, не смотря на своё положение относительно узла-цели, передать обратно RREP-ответ, так, как будто именно через него проходит оптимальный маршрут, при этом злоумышленник не обязательно находится на оптимальном пути между узлом-инициатором связи и узлом-целью.

У каждого узла сети, в контексте реактивных протоколов, существует собственный номер последовательности, который изменяется лишь в двух случаях, как это описывается в стандарте RFC 3561 [4, с. 11].

Для защиты от атаки «Чёрная дыра», которая была описана ранее, можно использовать следующий метод. Все узлы в сети должны хранить таблицу номеров последовательностей всех узлов, от которых были приняты данные. Для этого при инициализации сети все участники обмениваются друг с другом Hello-сообщениями. При запуске процедуры поиска маршрута узел-инициатор отправляет RREQ-запрос, на который узел-цель или промежуточный узел с «freshenough» маршрутом должен отправить источнику номер последовательности, с которым он в последний раз контактировал с узлом-целью.

Затем промежуточный узел (узел проверки) сравнивает разницу между номером последовательности, отправленным узлом с «fresh-enough» маршрутом и номером последовательности, с которым он сам последний раз взаимодействовал с узлом-целью. Если это значение превышает заранее оговорённую величину L, то узел, отправивший этот RREP, вероятно, является злоумышленником.

Величина L измеряется статистическим образом для каждой целевой сети и представляет из себя среднее значение разности между номером последовательности, отправленным узлом с «fresh-enough» маршрутом, и номером последовательности, с которым узел проверки сам последний раз взаимодействовал с узлом-целью.

Для оценки предложенного метода построен макет MANET-сети. Программная реализация макета осуществляется с помощью средств языка программирования Java. Упрощенная схема генерируемого программой макета представлена на рисунке 1.

Смоделированная сеть работает следующим образом: на участке размером 1000 на 1000 метров случайным образом генерируются узлы сети путём задачи каждому из них уникальной пары координат (double x,y). Количество узлов равно 25.

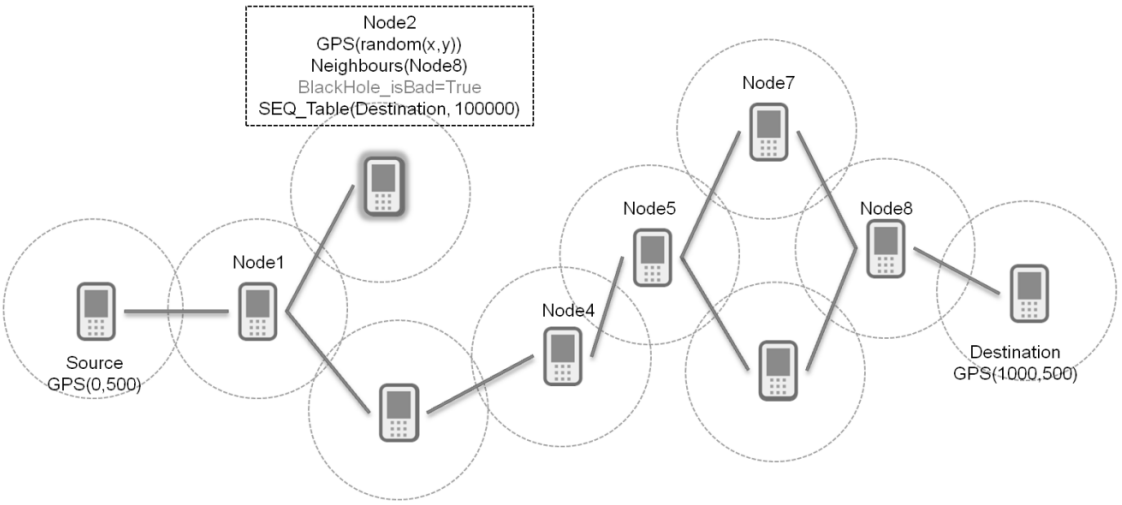

Рис. 1. Упрощённая схема макета сети из 10 узлов на плоскости 1000×1000 метров

После этого узлы проверяют связанность с соседями и объединяются с ними каналами связи. Связанность с соседями проверяется путём сравнения расстояния между узлами на двумерной плоскости и радиуса охвата технологии передачи данных. Для простоты радиус охвата в макете принят за 150 метров. Эта величина может легко быть изменена.

Также в макете сети задаются узел-источник (source) и узел-получатель (destination) между которыми налаживается связь.

Некоторые из узлов генерируются как узлы, обладающие freshenough маршрутом до узла-получателя.

Один узел сети гарантированно назначается в макете нарушителем в зависимости от моделируемой атаки (BlackHole_isBad=true).

Прежде чем говорить об оценке метода защиты от атаки «Чёрная дыра», нужно затронуть вопрос выбора оптимального значения лимита разницы между номерами последовательности узлов.

Суть заключается в том, что взяв за лимит очень маленькое значение разности, мы обезопасим себя от пропуска атак (ошибок первого рода), но будем вынуждены терпеть большое количество ложных срабатываний, так как разность номеров последовательности очень часто будет превышать лимит. Взяв за значение лимита слишком большое число, доля ложных срабатываний будет стремиться к нулю, но количество пропусков атаки возрастёт.

Таким образом, метод должен настраиваться на конкретной целевой системе для поиска баланса между долями ошибок первого и второго рода. Стоит

заметить, что баланс не фиксирован и зависит от конкретных предпочтений и приоритетов сети: если сеть терпима к ложным срабатываниям, то стоит отдать предпочтение уменьшению доли пропуска атак и значение лимита стоит искать левее точки, обозначенной на рисунке. С другой стороны, если сеть не может позволить себе слишком часто блокировать узлы, ложно обвинённые в атаке, то стоит искать значение лимита, как показано на рисунке 2. И в третьем, самом редком случае, когда отсутствие ложных срабатываний важнее отсутствия пропусков атаки, стоит искать значение лимита правее точки отмеченной на рисунке.

В результате многочисленных проверок было выявлено, что оптимальным лимитом для разности номеров последовательности получателя является 11 000. Здесь лимит высчитан для нейтральной ситуации, где нет предпочтений между ошибками первого и второго рода.

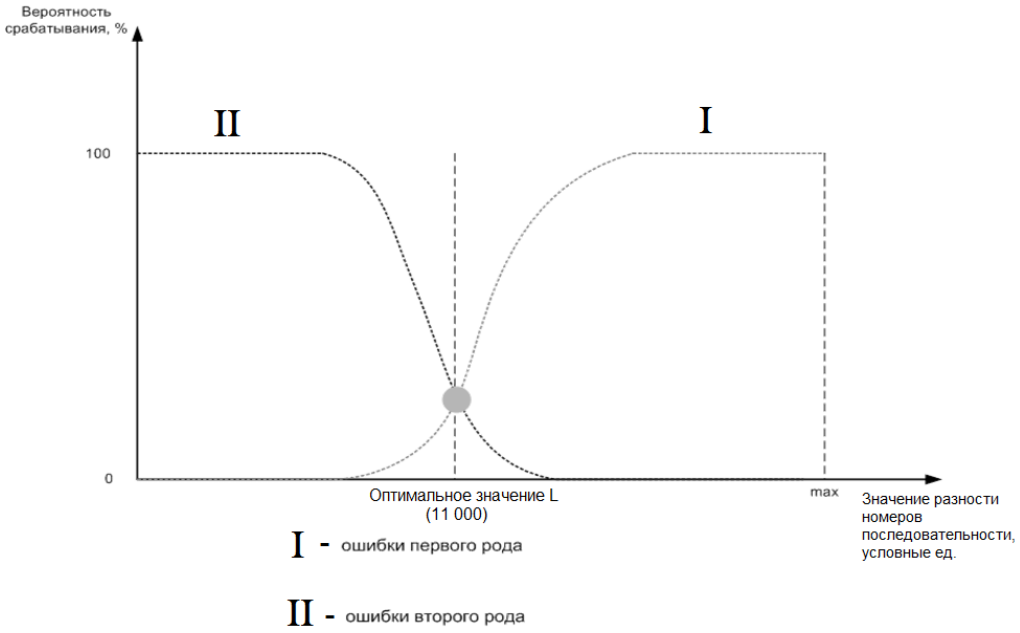

Рис. 2. График изменения доли ошибок первого и второго рода в зависимости от значения лимита

Результат тысячи испытаний создания уникального макета и оценки на нем метода защиты от атаки «Черная дыра» показал следующие результаты, отраженные на рисунке 3.

Из 1000 испытаний 834 сценария были легитимными, в 24 случаях из них происходили ложные срабатывания. 166 сценариев прошли как атакующие, и лишь в 7 случаях был зарегистрирован пропуск атаки.

Доля ошибок первого рода (пропуск атаки) составила 4%, В свою очередь доля ошибок второго рода (ложное срабатывание) составила 3%, что является хорошим показателем.

Таким образом, технология беспроводных самоорганизующихся сетей является перспективным и актуальным для исследований направлением. В свою

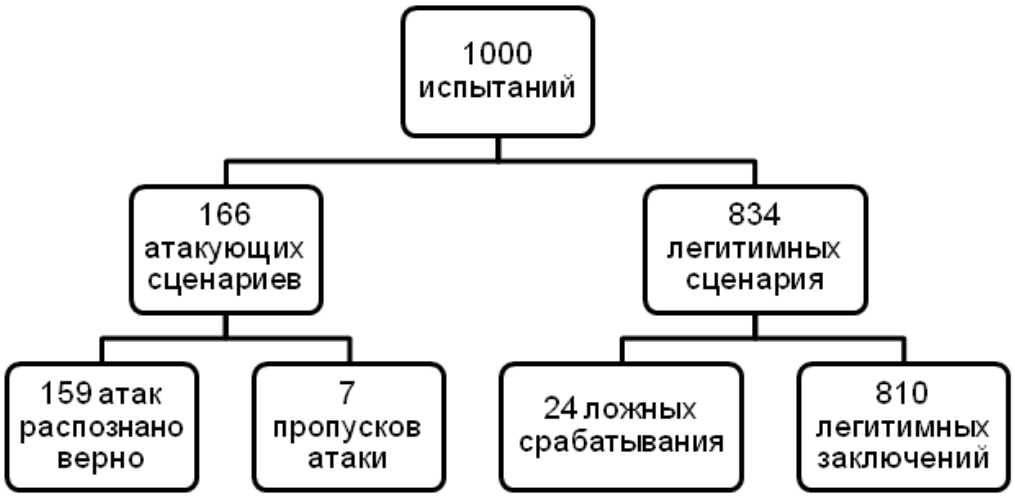

Рис. 3. Результаты тысячи испытаний метода защиты от атаки «Черная дыра»

очередь существование атак на подобные сети делает технологию важной для изучения с точки зрения информационной безопасности. Разработчики mesh-сетей изначально предусмотрели использование механизмов защиты, но основную угрозу они видели во внешней среде — в Интернете и в других внешних нарушителях. И это отлично работало, когда mesh-сети использовались локально, для решения узкого круга зачастую кратковременных задач, и в них присутствовало фиксированное множество доверенных узлов. Однако в последнее время вследствие роста количества и масштаба mesh-сетей на доверие ко всем узлам рассчитывать уже не приходится — появилась угроза внутреннего нарушителя, к которому mesh-сети оказались не готовы. Поэтому для дальнейшего развития и использования WMNs необходима разработка новых технологий и средств для их защиты.

Литература

1. Москвин Д.А., Иванов Д.В. Исследование безопасности беспроводных самоорганизующихся сетей // Информация и безопасность. Воронежский государственный технический университет, 2014.
2. Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А. Самоорганизующиеся сети. СПб.: Любавич, 2011.
3. Om Sh., Talib M. Wireless Ad-hoc Network under Black-hole Attack // International Journal of Digital Information and Wireless Communications. С. 591–596.
4. Сайт "ietf". Электрон. дан. 2003. URL: `http://www.ietf.org/rfc/rfc3561.txt/` (дата обращения: 10.05.2014).

DEVELOPMENT AND ASSESSMENT OF WIRELESS SELF-ORGANIZING NETWORKS CYBER SECURITY METHODS

D.A. Moskvin
Ph.D. (Eng.), Associate Professor, e-mail: moskvin@ibks.ftk.spbstu.ru
D.V. Ivanov
Postgraduate Student, e-mail: 9361023@gmail.com

St.Petersburg State Polytechnic University

Abstract. The article considers rapidly developing technology of self-organizing wireless networks. "Blackhole" attack targeting security breach of such networks is investigated and analyzed. The recommendations for defending from such attack are provided.

Keywords: self-organization, network, ad-hoc, mesh, security, attack.