

МОДЕЛИРОВАНИЕ ДЕЙСТВИЯ АТАК НА БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ

О. Д. Соколова¹, В. В. Шахов^{1,2}, А. Н. Юргенсон¹

¹ *Институт вычислительной математики и математической геофизики СО РАН, 630090, Новосибирск*

² *Новосибирский государственный технический университет, 630073, Новосибирск*

УДК 51-74

Рассматривается задача функционирования беспроводных сетей в условиях несанкционированных вторжений, под действием атак. Исследуется моделирование атак Black Hole и Jamming на узлы БСС. В качестве модели беспроводной сети используются графы единичных кругов (UDG-графы), которые наиболее адекватно описывают связи в беспроводных сетях, где передача информации между узлами возможна, если они находятся в пределах взаимной достижимости радиосигнала. Полученные аналитические результаты согласуются с результатами имитационного моделирования.

Ключевые слова: беспроводные сенсорные сети, несанкционированные вторжения, атаки Black Hole и Jamming.

Введение

Технологии, основанные на беспроводных сенсорных сетях, используются во многих сферах, и с каждым годом это использование расширяется. Очевидно, что необходимо уделять особое внимание вопросам безопасности функционирования БСС. Из-за присущих сенсорным узлам ресурсных ограничений, существующие методы сетевой безопасности, в том числе разработанные для мобильных сетей Ad-Hoc, плохо подходят для БСС. В качестве важного вопроса безопасность в беспроводных сенсорных сетях привлекает многих исследователей. Полностью нивелировать последствия несанкционированных вторжений в сеть возможно далеко не во всех случаях. Однако можно снизить последствия атак, если выбрать правильные способы защиты.

1 Беспроводные сенсорные сети

Беспроводные технологии становятся все более популярными в повседневной жизни. Они позволяют использовать для сбора данных с больших территорий несколько устройств без физических соединений, без необходимости подключения к сети. Беспроводные сенсорные сети [1], используемые в различных областях (например, мониторинг территории), обычно образованы большим количеством сетевых узлов — автономных устройств, с помощью которых можно получать информацию о наблюдаемых параметрах и передавать ее для дальнейшей обработки. Каждый узел в сети должен иметь модуль для сбора данных и автономный источник питания (чаще всего непополняемый). Кроме того, узлы должны быть оснащены устройствами беспроводной связи, чтобы передавать собранную информацию по радиоканалу. Все собранные данные передаются в один или несколько стоков, которые затем передают информацию базовой станции. Сбор данных и передача в стоки происходит по некоторым алгоритмам маршрутизации. Таким образом, все узлы образуют распределенную, самоорганизующуюся систему.

Несмотря на очевидные преимущества систем с беспроводной связью, они отличаются также и большей по сравнению с проводными сетями уязвимостью. Вследствие организации связей без физических соединений, БСС подвержены многочисленным угрозам безопасности — нарушить беспроводную передачу можно либо непреднамеренно (из-за существующих помех) либо в результате преднамеренного вторжения. Для

Работа выполнена при частичной финансовой поддержке проекта № 11 Программы фундаментальных исследований Президиума РАН.

организации воздействия используются радиопомехи, различные программы с целью изменения или ликвидации информации и др. В простейшей форме злоумышленник препятствует набору частотных диапазонов, используемых для связи, путем передачи непрерывного сигнала помех или нескольких коротких импульсов помех. Целью атаки Node replication (клонирование узла) является изменение данных, которые передаются в базовую станцию. Атака Jamming (создание помех) воздействует на узлы и на каналы передачи данных и затрудняет передачу информации. Действие атаки Black Hole (“черная дыра”) оказывается возможным вследствие уязвимости протоколов маршрутизации БСС — узел, который подвергся атаке, рассылает всем смежным узлам ложную информацию о том, что он находится близко к стоку, вследствие чего происходит изменение маршрутизации и вся передаваемая информация теперь проходит через атакованный узел, вследствие чего она может быть заблокирована. Для обнаружения вторжений в БСС и умения противодействовать атакам необходимо использовать надежные протоколы маршрутизации, средства обнаружения вторжений в сеть. Следовательно, важным становится процесс моделирования работы сети, передачи информации в ней, особенно под влиянием воздействий.

2 Моделирование сенсорных сетей

В качестве модели для современных сетей передачи данных (в частности, для БСС) удобно использовать случайные геометрические графы, в котором вершины распределены случайным образом на области с евклидовой метрикой. Будем считать, что сигнал от каждого узла распространяется во все стороны с одинаковым для всех устройств радиусом. Узлы могут получать и передавать данные друг другу, если они находятся в пределах взаимной достижимости сигнала. Поэтому смежность двух вершин в таком графе равносильна расположению одной вершины в круге, образованном другой вершиной. Это означает, что в моделируемом графе ребро между двумя вершинами существует, если расстояние между ними в евклидовой метрике меньше либо равно заданного числа. В этом случае удобно использовать в качестве моделей для топологии сети подкласс случайных геометрических графов — графы единичных кругов (Unit Disk Graphs, UDG-графы) [3, 9].

Определение Граф $G = (V, E)$ называется UDG-графом (unit disk graph, граф единичных кругов) если ребро $e = (u, v)$ между вершинами $u, v \in V$ существует в том и только том случае, когда в Евклидовой метрике расстояние между u и v меньше либо равно 1 (или некоторого заданного числа r).

Рассмотрим граф единичных кругов $G = (V, E)$, $|V| = n$, для каждого ребра $e \in E$ поставим в соответствие величину $f(e)$, зависящую от его длины. Это может быть, например, величина, отражающая потребление энергии для передачи данных от одного узла к другому, которая пропорционально квадрату расстояния между узлами. От расстояния между узлами также зависит и количество повторных передач для обеспечения надежной доставки информации [4]. В множестве вершин графе G выделяем одну вершину s — сток, т.е. узел (или один из узлов, если стоков несколько), в который должна собираться информация, передаваемая вершинами сети. Для построения маршрутов от каждой вершины к стоку, на графе строится остовное дерево T (т.е. дерево, содержащее все вершины графа), с направленными ребрами. Алгоритм построения такого дерева зависит от выбранного алгоритма маршрутизации [4, 6]. По направленным дугам от каждой вершины v_i дерева T происходит передаются данные к стоку s .

Количество направленных дуг, входящих в вершину v_i , будем обозначать $d^+(v_i)$.

Для генерации топологий беспроводных сетей использовался метод, описанный в работе [8].

3 Моделирование атак на сенсорную сеть

В качестве критерия устойчивости сенсорной сети будем рассматривать функционирование сети в условиях воздействия различных атак на ее узлы. В результате действия атак может выходить из строя один узел (атака Black Hole) или несколько узлов (атака Jamming). Если какой-то узел, подвергшийся атаке, выходит из строя, то вся информация, переданная в него другими узлами, будет потеряна. В остовном дереве T , построенном по некоторому алгоритму маршрутизации, множество таких узлов (информация от которых потеряна) образует подмножество $V' \in V$. Таким образом, в качестве критерия устойчивости построенного дерева к определенной атаке удобно взять параметр — количество таких узлов $n' = |V'|$ или их нормированное количество: n' деленное на общее число вершин в графе $|V|$.

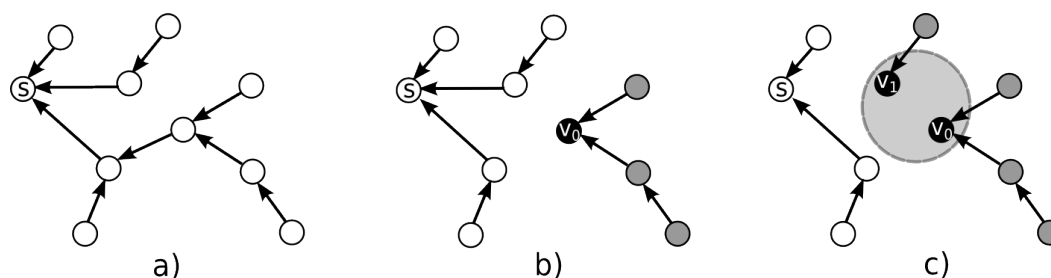


Рис. 1: а) БСС без воздействия атаки; б) атака Black Hole (черным отмечена атакованная вершина, серым — вершины от которых будет потеряна информация); в) атака Jamming (черным отмечены атакованные вершины, попавшие в область действия источника помех, серым — вершины от которых будет потеряна информация).

4 Атака Black Hole

Одним из наиболее опасных разрушающих воздействий в БСС является атака Black Hole [2, 7]. В связи с особенностями развертывания БСС, слабыми методами защиты передачи информации, осуществление атаки Black Hole на узлы сети все чаще используется при несанкционированном вторжении. Такую атаку можно организовать двумя способами: разместив в области действия сети новый узел, с помощью которого организуется атака на другие узлы (с целью захвата передаваемой информации) либо взломав один из узлов, участвующих в сборе и передаче информации. Атакованный узел может удалить все пакеты, переданные в него другими узлами для транзитной передачи. Кроме того, этот узел v_0 может распространять по сети ложную информацию, что он является ближайшим узлом к стоку s , а это приводит к изменению маршрутизации.

Для моделирования способов сбора информации от всех узлов и передачи ее в стоки строится дерево T — остовное дерево графа G . Будем считать, что в этом построенном дереве множество узлов, информация от которых потеряна, образует подмножество $V' \in V$. Для оценки устойчивости рассматриваемой сети к атакам будем рассматривать параметр — количество таких узлов $n' = |V'|$ (в численных расчетах будем использовать нормированное количество: n' деленное на общее число вершин в графе $n = |V|$).

Рассмотрим остовное дерево T , построенное для анализа функционирования сети, пусть в нем имеется n вершин, из них одна вершина является стоком. Для удобства обозначим уровни в этом дереве: сток считаем нулевым уровнем; вершины, которые сразу передают информацию в сток — первый уровень и т.д., номер последнего уровня обозначим a .

В [4] авторами было показано, что математическое ожидание числа вершин n' , от которых будет потеряна информация после атаки Black Hole, равно:

$$E(n') = \frac{1}{n}(1 + 2|V_1| + \dots + (a-1)|V_a|), \quad (1)$$

где $V_j \in V$ — вершины, принадлежащие уровню j . В этом случае из формулы (1) следует, что чем меньше число транзитов для передачи от данных от вершины к стоку (число хопов), тем меньше $E(n')$.

5 Атака Jamming

Рассмотрим теперь сеть с такой же топологией, где сбор данных идет по тому же самому остовному дереву T , но внешнее воздействие осуществляется другой атакой — “Jamming”. Подвергаться атаке может не одна вершина, а k вершин, находящихся в зоне действия атаки.

Предположим, на расстоянии R или меньше от источника помех приемники сенсоров гарантировано не могут принять сигнал, тогда k пропорционально площади зоны действия атаки: $k = \rho\pi R^2$, где ρ — плотность, т.е. количество вершин на единицу области.

Для некоторых простых случаев вида остовного дерева T можно вычислить аналитические оценки математического ожидания величины n' .

Рассмотрим “симметричное” остовное дерево T , имеющее n вершин, для каждой вершины v значение $d^+(v) = m$, кроме вершин последнего уровня (рис. 2). Считаем, что каждая ветвь дерева имеет одинаковое

число уровней. В этом случае номер последнего уровня a связан с m следующим соотношением:

$$n = 1 + m + m^2 + \dots + m^a. \quad (2)$$

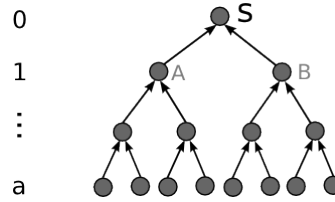


Рис. 2: Пример “симметричного” остовного дерева.

Утверждение. Пусть число атакованных различных вершин $k = 2$ ($k \leq m$), вершины атакованы с равной вероятностью независимо друг от друга, тогда

$$E(n') = 2 + \frac{1}{n(n-1)} \left(2m^2(1 + 2m + 3m^2 + \dots + am^{a-1})(n - m^a) - \right. \\ \left. - 2m((1 + m + \dots + m^{a-1}) + 2m(1 + m + \dots + m^{a-2}) + \dots + am^{a-1}) \right), \quad (3)$$

Доказательство. Для вычисления $E(n')$ нужно перебрать все варианты возможных расположений атакованных вершин (это $n(n-1)$ вариантов), и для каждого варианта вычислить значение n' , затем разделить его на $n(n-1)$.

1) Если атакована вершина уровня 0, то теряется информация от всех n вершин. Такое может случиться в $k(n-1)$ случаях, получаем слагаемое $\frac{k(n-1)n}{n(n-1)} = k$.

2) Атакованные вершины попадают в разные поддеревья уровня 1 (например, поддеревья A и B на рис. 2). Обозначим (аналог формулы (1)) $\xi = 1 + 2m + 3m^2 + \dots + am^{a-1}$ — количество вершин, от которых потеряна информация, если атакована одна вершина в поддереве A (с учетом всевозможных ее расположений). Тогда, учитывая все возможные расположения второй атакованной вершины, в этом случае число вершин, от которых будет потеряна информация, равно $2\xi(1 + m + \dots + m^{a-1})$. Используя формулу (2) получим: $2\xi(n - m^a)$. На уровне 1 располагается m вершин и следовательно мы имеем m поддеревьев. Атакованные вершины могут попадать в разные поддеревья или в одно поддерево, значит второе слагаемое в формуле (3): $m^2\xi(n - m^a + 1)$.

3) Если атакованные вершины попадают в одно поддерево (m случаев), то надо учесть случай, когда одна атакованная вершина является потомком другой атакованной вершины (и наоборот, т.е. множитель 2). Т.е. нужно вычесть количество вершин, попадающих в такие пересечения. Поддерево уровня 1 повторно считается 1 раз в поддереве A , т.е. вершин в пересечении $1 + m + \dots + m^{a-1}$. Поддеревья уровня 2 (их m в поддереве A) повторно считаются 2 раза (если вторая атакованная вершина попадает в уровень 2 и уровень 1). В поддереве уровня 2 число вершин равно $1 + m + \dots + m^{a-2}$. Всего вершин $2m(1 + m + \dots + m^{a-2})$. На последнем уровне это число равно am^{a-1} .

Получаем последнее слагаемое в формуле (3):

$$-2m((1 + m + \dots + m^{a-1}) + 2m(1 + m + \dots + m^{a-2}) + \dots + am^{a-1}). \quad \square$$

Вариант атаки, описанный в утверждении 1, назовем “Random” (случайный). Необходимо учесть, что при атаке “Jamming” из-за свойства UDG-графа большая часть атакуемых вершин является “потомками” других атакованных вершин. Т.е. формула (3) не может быть использована, удобнее применить имитационное моделирование.

Следует учитывать, что некоторые узлы могут быть поражены вне зоны действия радиуса R (будем обозначать такую атаку “Jamming R”). Для таких узлов вероятность $p(x)$ выхода из строя зависит от расстояния x до источника атаки. В этом случае оценка количества атакованных узлов вычисляется по формуле:

$$N = \rho\pi R^2 + 2\pi\rho \int_R^\infty xp(x)dx$$

Так, если вероятность $p(x)$ является экспоненциальной убывающей функцией [5]: $p(x) = e^{-(x-R)}$, $x > R$, то $N = \rho\pi(R^2 + 2R + 2)$.

6 Результаты моделирования воздействия атак

В работе [4] были представлены результаты экспериментов для атаки Black Hole на БСС. Аналогично предложенному в работе методу были проведены эксперименты для воздействия атак “Jamming” и “Jamming R”. Для проведения экспериментов “Jamming” и “Jamming R”. Рассматривались графы с количеством вершин $|V| = 500$ (радиус достижимости вершин $r = 30$). Было проведено моделирование воздействия атак на случайную область (420x420 точек) с заданным радиусом.

Предполагалось, что атака “Jamming R” выводит из строя вершины с вероятностью $p(x) = 1/10x$, где x расстояние от вершины до источника атаки.

На рис. 3 представлены результаты экспериментов воздействия атак “Jamming” и “Jamming R” и “Random” (число атакованных вершин совпадает с числом атакованных вершин при атаке “Jamming”, но вершины атакуются случайно и независимо друг от друга) на остовное дерево (для построения остовного дерева использовался алгоритм маршрутизации Minimum Hop Route [10]). По оси ординат отчается нормированное среднее число вершин, от которых потеряна информация. По оси абсцисс — различные радиусы поражения атаки.

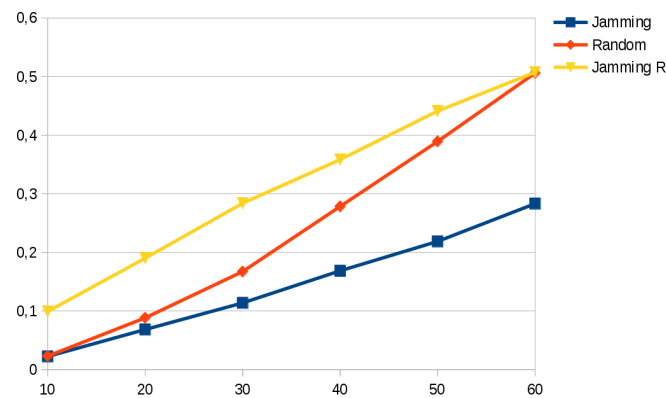


Рис. 3: Нормированное среднее число вершин, от которых теряется информация для разных типов атаки “Jamming”.

На рис. 4 и 5 представлены результаты экспериментов воздействия атак “Jamming” и “Jamming R” на каждое из остоных деревьев, построенных для разных алгоритмов маршрутизации (описанными в [4] алгоритмами). Из рисунка видно, что дерево, построенное алгоритмом Minimum Energy Route (Greedy), является самым уязвимым, а алгоритм Minimum Hop Route строит наиболее устойчивое дерево. Хотя, если сравнивать веса остоных деревьев, то алгоритм Minimum Energy Route является лучшим.

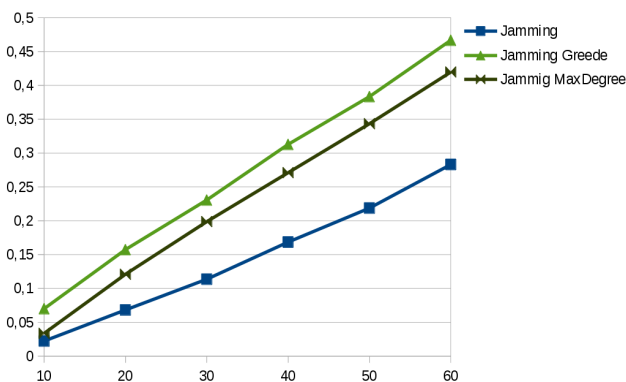


Рис. 4: Нормированное среднее число вершин, от которых теряется информация после атаки “Jamming”.

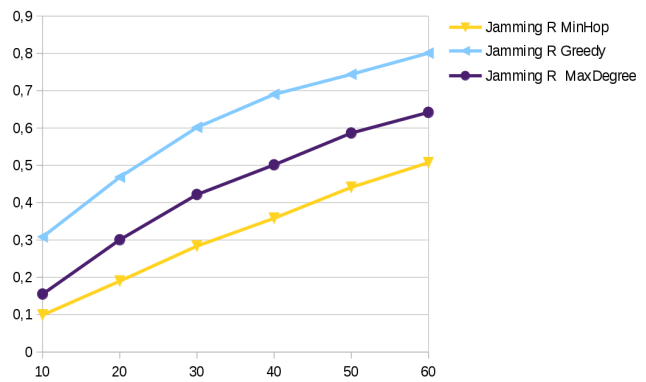


Рис. 5: Нормированное среднее число вершин, от которых теряется информация после атаки “Jamming R” для разных алгоритмов маршрутизации.

Интересно, что для атаки “Jamming” среднее число вышедших из строя вершин линейно зависит от радиуса атаки и плотности размещения вершин на заданной области.

Заключение

Исследование воздействия атаки Jamming в общем случае проведено с помощью имитационного моделирования. Чтобы оценить уязвимость остоного дерева передачи данных, в качестве критерия рассматривался параметр — «нормированное число вершин, от которых потеряна информация». Результаты, полученные после экспериментов, хорошо согласуются с формулами, полученными в предыдущем разделе. Очевидно, что ущерб от разрушающего воздействия атаки Jamming на узлы БСС существенно зависит от того, какой алгоритм маршрутизации применяется в сети для сбора и передачи пакетов. Таким образом, надежность сети можно повысить, выбрав более защищенный метод.

Список литературы

- [1] E. Cayirci, C. Rong. Security in Wireless Ad Hoc and Sensor Networks. John Wiley & Sons, 2009.
- [2] K.S. Praveen, H.L. Gururaj, B. Ramesh. Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols. Procedia Computer Science, vol. 85, 2016, P. 325–330.
- [3] A. Clark, C. Colbourn, D. Johnson. Unit disk graphs // Discrete Mathematics, vol.86, 1990, Pages 165–177.
- [4] Шахов В.В., Юргенсон А.Н., Соколова О.Д. Моделирование воздействия атаки Black Hole на беспроводные сети // Программные продукты и системы. 2017. Том 30. № 1. С. 34–39.
- [5] Vladimir V. Shakhov. Experiment Design for Parameter Estimation in Sensing Models. Springer Lecture Notes in Computer Science, vol. 8072, 2013, P 151–158.
- [6] A. Safonov, A. Lyakhov, A. Urgenson, O. Sokolova Wireless groupcast routing with palette of transmission methods // Multiple Access Communications, 2012, p. 97–108.
- [7] S. Dokurer, Y. Erten, C. Acar. Performance analysis of ad-hoc networks under black hole attacks. In Proc. of IEEE Int. Conf. SoutheastCon 2007, March 2007, P. 148–153.
- [8] Vladimir V. Shakhov, Olga Sokolova, Nastya Yurgenson. A Fast Method for Network Topology Generating. Lecture Notes in Computer Science, Springer, vol. 8715, 2014, P. 96–101.
- [9] В. В. Шахов, А. Н. Юргенсон, О. Д. Соколова “Эффективный метод генерации случайных геометрических графов для моделирования беспроводных сетей” // Прикладная дискретная математика, — 2016, — № 4(34), — С. 99–109
- [10] Yang L., Yang H.C., Wu K. Minimum-energy route configuration for wireless ad hoc networks. 2006 IEEE Int. Performance Computing and Communications Conf. Phoenix, AZ, 2006, pp. 6–14.

*Владимир Владимирович Шахов — к.ф.-м.н., ст. науч.сотр. Института
вычислительной математики и математической геофизики СО РАН;
Новосибирский государственный технический университет;
e-mail: shakhov@rav.sccc.ru;*

*Соколова Ольга Дмитриевна — к.т.н., ст. науч.сотр. Института вычислительной
математики и математической геофизики СО РАН;
e-mail: olga@rav.sccc.ru;*

*Анастасия Николаевна Юргенсон — к.ф.-м.н., науч.сотр. Института
вычислительной математики и математической геофизики СО РАН;
e-mail: nastya@rav.sccc.ru.*

Дата поступления — 1 июня 2017 г.