УДК 51-74
DOI: 10.15827/0236-235X.117.034-039
Дата подачи статьи: 19.08.16
2017. Т. 30. № 1. С. 34–39

МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ АТАКИ BLACK HOLE НА БЕСПРОВОДНЫЕ СЕТИ

В.В. Шахов, к.ф.-м.н., доцент, старший научный сотрудник, shakhov@rav.sscc.ru;
А.Н. Юргенсон, к.ф.-м.н., научный сотрудник, nastya@rav.sscc.ru;
О.Д. Соколова, к.т.н., старший научный сотрудник, olga@rav.sscc.ru
(Институт вычислительной математики и математической геофизики СО РАН, просп. Академика Лаврентьева, 6, г. Новосибирск, 630090, Россия)

Технологии, основанные на беспроводных сенсорных сетях, проникают в самые важные сферы жизнедеятельности общества. Многие решения в области архитектуры Интернета вещей опираются на результаты исследований беспроводных сенсорных сетей, в частности, это касается предложений, разработанных в рамках ряда проектов Седьмой рамочной программы Европейского союза по развитию научных исследований и технологий. Следовательно, особое внимание необходимо уделять обеспечению безопасности таких сетей.

В статье обсуждаются проблемы функционирования сетей в условиях несанкционированных вторжений. Обеспечить абсолютную защиту, полностью нивелировать последствия вторжений возможно далеко не во всех случаях. Однако эффективный выбор механизмов защиты позволит существенно снизить ущерб. Для этого необходимо разрабатывать и исследовать адекватные математические модели.

Авторы рассматривают моделирование атаки Black Hole на узлы беспроводных сенсорных сетей и исследуют оценку нанесенного ущерба. Эта атака является одним из наиболее опасных разрушающих информационных воздействий, в результате ее может теряться более 90 % информации, передаваемой в сток. В качестве модели беспроводной сети используются графы единичных кругов (UDG-графы), которые наиболее адекватно описывают связи в этих сетях, где передача информации между узлами возможна, если они находятся в пределах взаимной достижимости радиосигнала.

Для моделирования передачи данных по выбранному алгоритму маршрутизации в графе строится остовное дерево. Авторами получены формулы для вычисления аналитических оценок для некоторых случаев вида остовного дерева. Чтобы оценить уязвимость дерева передачи данных к атакам, использовалась величина «нормированное число вершин, от которых потеряна информация» – среднее число вершин, от которых потеряна информация, деленное на общее число вершин в дереве.

Полученные аналитические результаты согласуются с результатами имитационного моделирования. Предложен метод противодействия атакам типа Black Hole, оценена его эффективность.

Ключевые слова: *беспроводные сенсорные сети, безопасность, атака Black Hole.*

Новейшие достижения в области сетевых технологий, физики полупроводников и материаловедения позволили приступить к повсеместной разработке и внедрению *беспроводных сенсорных сетей* (БСС). Первоначально научно-исследовательские и конструкторские работы по данной теме проводились при поддержке Агентства по перспективным научно-исследовательским разработкам при министерстве обороны США (Defense Advanced Research Projects Agency, DARPA). Однако в настоящее время технологии БСС находят применение в самых разных сферах человеческой жизнедеятельности: изучение биологии диких животных и птиц, обнаружение лесных пожаров и наводнений, мониторинг загрязнения воздуха, системы «умный дом», системы предупреждения техногенных аварий, контроль состояния пожилых людей и пациентов госпиталя, новейшие методы медицинской диагностики, отслеживание транспортных потоков, индустриальные робототехнические системы, современные сельскохозяйственные технологии и т.д. Интенсивные исследования по проблематике БСС проводятся не только ведущими мировыми научными центрами, но и коммерческими компаниями, такими как IBM, Intel, Samsung, Cisco Systems, Google и др. Для координации работ в области БСС создан альянс ZigBee, куда вошли крупнейшие разработчики аппаратных и программных средств. Результатом усилий альянса стала спецификация протоколов сетевого и прикладного уровня, разработанная на основе стандарта IEEE 802.15.4, описывающего физический уровень и нижний канальный подуровень (управление доступом к среде) для низкоскоростных беспроводных персональных сетей [1]. Недавно альянс анонсировал единый стандарт ZigBee 3.0, объединяющий лидирующие на рынке беспроводные стандарты, позиционируя его как удобное средство для разработчиков продуктов и услуг, относящихся к Интернету вещей (Internet of Things, IoT).

Следует отметить, что развитию Интернета вещей уделяется особое внимание во многих странах. Данный рынок является очень перспективным: по оценкам специалистов Cisco Systems, число устройств, подключенных к Интернету, уже составляет десятки миллиардов. Международные консалтинговые компании, специализирующиеся на рекомендациях по стратегическому управлению, прогнозируют в ближайшие несколько лет крупный экономический эффект от развития Интернета вещей. Фондом развития интернет-инициатив (Российским фондом венчурных инвестиций)

объявлено о создании консорциума для формирования российского пакета технологий Интернета вещей в партнерстве с инвестиционным холдингом GS Group и операторами сотовой связи. Многие решения в области архитектуры IoT опираются на результаты исследований БСС [2], в частности, предложения, разработанные в рамках проектов Седьмой рамочной программы Европейского союза по развитию научных исследований и технологий [3].

Таким образом, технологии, основанные на БСС, проникают в самые важные сферы жизнедеятельности общества, следовательно, особое внимание необходимо уделять вопросам безопасности указанных сетей. Из-за ограничений, налагаемых требованиями рынка на компоненты БСС, и особенностей функционирования БСС указанные сети легко подвергаются атакам. Обеспечить абсолютную защиту БСС, полностью нивелировать последствия несанкционированных вторжений возможно далеко не во всех случаях. Однако эффективный выбор механизмов защиты позволит существенно снизить ущерб. Для этого необходимо разрабатывать и анализировать соответствующие математические модели.

В данной статье дано общее описание БСС, рассмотрены причины их уязвимости и некоторые атаки. Рассмотрены вопросы моделирования БСС. Предлагаются подходы к моделированию атаки Black Hole, к оценке нанесенного сети ущерба, рассматривается способ противодействия данной атаке. Анализ эффективности предлагаемого механизма противодействия атаке и выводы завершают статью.

Беспроводные сенсорные сети

БСС образованы большим количеством сетевых узлов [4], называемых мотами, – миниатюрных автономных устройств, способных собирать информацию с территории в определенном радиусе действия и передавать ее другим устройствам. Каждое такое устройство содержит модуль сбора данных (температуры, давления, освещенности и т.д.) и автономный источник питания. Также каждый мот оснащен радиотрансивером или другим устройством беспроводной связи, то есть данные передаются в сети по радиоканалу. Для аккумулирования всей собираемой информации сеть содержит мощный узел (сток, базовая станция), подключенный к стационарному источнику питания. Данные собираются в этот сток по определенному алгоритму маршрутизации. Объединенные в беспроводную сеть, все узлы образуют распределенную самоорганизующуюся систему сбора и передачи информации. Преимущества систем на основе сенсорных сетей – возможность развертывания в труднодоступных местах, беспроводная связь, самоорганизация (возможность перераспределения маршрутов в случае выхода из строя некоторых узлов).

Несмотря на очевидные преимущества систем с беспроводной связью, они отличаются и большей по сравнению с проводными сетями уязвимостью. Для обеспечения отказоустойчивости БСС необходимо решить ряд проблем, возникающих вследствие обмена информацией в открытой распределенной самоорганизующейся системе, топология которой может изменяться во времени [5].

Основные причины уязвимости БСС: доступность среды передачи, незащищенность узлов, относительная невозможность анализа всего трафика на предмет обнаружения аномалий, невозможность использования криптографии и сложного математического аппарата из-за ограниченности ресурсов. Именно ограниченность ресурсов сенсора позволяет легко выводить его из строя или использовать по усмотрению злоумышленника. Отказы узлов могут возникать в случае как несанкционированных вторжений в сеть, так и сбоев легальных протоколов. Выход из строя всего одного сенсора может привести к тому, что теряются потоки данных от множества других сенсоров, использующих атакованный узел в качестве промежуточного на пути к стоку. Следовательно, ущерб в этом случае будет нанесен значительному сегменту сети.

Для организации разрушающего воздействия используются радиопомехи, вредоносные программы с целью перехвата информации, перевод узла в спящий режим [6] и др. Например, целью атаки Node replication (клонирование узла) является фальсификация данных, передаваемых в сток. Атака Jamming (создание помех) оказывает воздействие на каналы и затрудняет передачу информации. Атака Black Hole (черная дыра) использует уязвимость протоколов маршрутизации БСС: атакуемый узел посылает соседним узлам информацию о том, что он находится близко к стоку, вследствие чего маршрутизация меняется, потоки данных проходят через этот узел, далее информация блокируется. Если сеть обладает способностью к самовосстановлению, то есть протоколы передачи данных позволяют обнаруживать неисправные узлы и исключать их из маршрутов, эффект от указанных разрушающих воздействий не будет продолжительным. Однако существуют и более успешные способы организации атак [7, 8].

Для противодействия атакам необходимо повышать надежность используемых протоколов маршрутизации, обеспечивать мобильность стоков (возможность замены стока) или принимать другие меры. Отсюда вытекает необходимость умения моделировать работу сети в различных режимах, особенно под влиянием воздействий, чтобы определить оптимальный уровень защиты.

Моделирование сенсорных сетей

БСС удобно моделировать графом, в котором вершины распределены случайным образом на об-

ласти с евклидовой метрикой. Так как сигнал от каждого узла распространяется во все стороны, место, где сигнал может быть получен другим узлом, моделируется кругом. Один узел может передавать информацию другому, если они находятся в пределах взаимной достижимости сигнала. Следовательно, две вершины графа соединяются ребром, если одна вершина находится в круге, образованном другой вершиной. Если все узлы имеют передатчики одинаковой мощности, круги имеют один и тот же радиус. Это означает, что в моделируемом графе ребро между двумя вершинами существует, если расстояние между ними в евклидовой метрике меньше заданного числа либо равно ему. В этом случае в качестве модели удобно использовать класс графов, которые называются Unit Disk Graphs (UDG-графы).

Определение [9]. 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 только в том случае, когда в евклидовой метрике расстояние между u и v меньше либо равно 1.

Рассмотрим граф единичных кругов $G=(V, E)$, $|V|=n$, в котором всем ребрам $e \in E$ приписаны некоторые веса $f(e)$, зависящие от их длины. Например, потребление энергии для передачи данных от одного узла к другому пропорционально квадрату расстояния между ними. Надежность соединения, а значит, и количество повторных передач также зависят от расстояния [10]. В графе G выделяем одну вершину s – сток, то есть узел, в котором собирается вся информация, передаваемая вершинами сети. Остальные вершины могут принимать и передавать информацию для отправки ее в сток. Существует множество алгоритмов передачи данных в сенсорных сетях, которые оптимизируют различные показатели, например, количество потребляемой энергии, скорость передачи данных и др. На основе таких алгоритмов разрабатываются протоколы маршрутизации, по которым осуществляются сбор информации со всех узлов сети и передача ее в сток. Для построения маршрутов от каждой вершины к стоку на графе строится остовное дерево T (то есть дерево, содержащее все вершины графа) с направленными ребрами. Алгоритм построения такого дерева зависит от выбранного алгоритма маршрутизации [11, 12]. По ребрам дерева T происходит передача данных от каждой вершины v_i в сток s.

Количество направленных дуг, входящих в вершину v_i, будем обозначать $d^+(v_i)$. Степенью вершины $d(v_i)$ будем называть число входящих и исходящих из нее дуг.

Атака Black Hole

Одним из наиболее опасных разрушающих воздействий в БСС является атака Black Hole. В результате действия атак этого типа может теряться более 90 % информации, передаваемой в сток [13]. Атаку можно организовать двумя способами. Один способ – размещение злоумышленником в области действия сети нового узла, с помощью которого в дальнейшем организуется атака. Воздействия такого рода относительно легко обнаруживаются и локализуются стандартными механизмами БСС. Более опасным является другой способ, когда осуществляется взлом одного из легальных узлов, уже участвующих в информационном обмене.

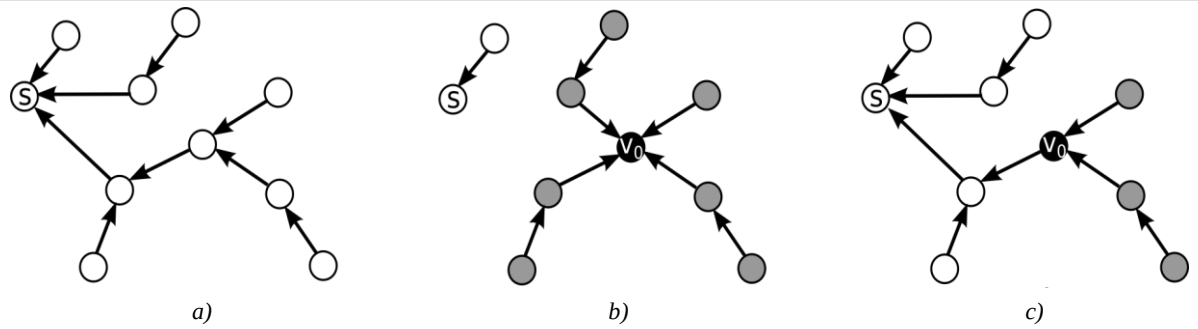
Контролируемый злоумышленником узел удаляет все пакеты, переданные в него другими узлами для транзитной передачи. Кроме того, взломанный узел v_0 может распространять по сети информацию, что он является ближайшим узлом к стоку s, вследствие чего самоорганизующаяся сеть, каковой является БСС, меняет маршрутизацию, и остальные узлы, находящиеся ближе к v_0 , чем к s, передают в v_0 свои пакеты для дальнейшей передачи в s.

В основе предлагаемого авторами метода защиты от атаки Black Hole лежит следующая идея. Так как в результате атаки собранная в узле v_0 информация блокируется, интенсивность транзитного трафика и нагрузки на сток s снижается. Основываясь на наблюдениях показателей трафика и используя методы обнаружения разладки случайных процессов, можно обнаружить несанкционированное вторжение. Как только возникает подозрение на наличие атаки, всем узлам отправляется команда вернуться к прежнему выбору транзитных узлов на пути к стоку. Данный сигнал может, например, передаваться мощным передатчиком, интегрированным со стоком, сразу для всех узлов сети. В случае использования злоумышленником нового узла эффект атаки полностью нивелируется. Если же для атаки использовался узел, участвовавший ранее в маршрутизации, восстановление маршрутов позволяет снизить потери, так как пропадает только информация, передаваемая транзитом через v_0 (ситуация показана на рисунке 1).

Оценим эффективность данного способа защиты. В остовном дереве T, построенном в графе G, множество узлов, информация от которых потеряна, образует подмножество $V' \subseteq V$. Таким образом, для оценки устойчивости дерева T к атаке удобно взять в качестве параметра количество таких узлов $n'=|V'|$ или нормированное количество: n', деленное на общее число вершин в графе $n= |V|$.

Для некоторых простых случаев вида остовного дерева T можно вычислить аналитические оценки среднего числа вершин, от которых теряется информация. Например, простым случаем можно считать дерево, у которого каждая вершина имеет одинаковое число потомков.

Рассмотрим дерево T, имеющее n вершин, для каждой вершины v значение $d^+(v)= k$, кроме вер-



a) *b)* *c)*

Рис. 1. Маршрутизация в сети: a) без воздействия атаки; b) при атаке Black Hole (черным цветом отмечена атакованная вершина, серым – вершины, информация от которых будет потеряна); c) с возвратом к предыдущей маршрутизации (серым помечены вершины, информация от которых будет потеряна)

Fig. 1. Network routing: a) without the attack impact; b) Black Hole attack (the attacked vertex is marked black, the vertices with lost data are marked gray); c) a return to the previous routing (the vertices with lost data are marked gray)

шин последнего уровня. Считаем, что каждая ветвь дерева имеет одинаковое число уровней.

Пронумеруем уровни в дереве: сток считаем нулевым уровнем; вершины, передающие информацию в сток, – первый уровень и т.д., последний уровень имеет номер a (рис. 2). Тогда величины a и k связаны следующим соотношением: $k^{a+1}= n(k–1)+1$.

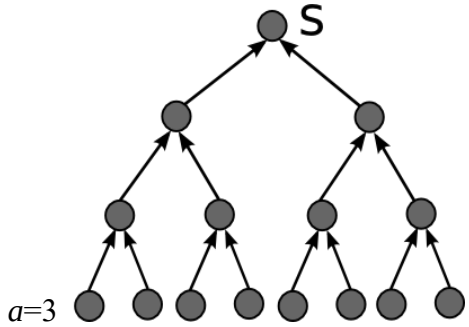


Рис. 2. Пример дерева с одинаковым значением $d^+(v)$ для вершин (кроме последнего уровня)

Fig. 2. The example of a tree with the same value of $d^+(v)$ for vertices (except the last level)

Считаем, что каждая вершина в дереве с равной вероятностью может подвергнуться атаке. Отсюда следует, что математическое ожидание числа вершин n', от которых теряется информация под воздействием атаки Black Hole, равно:

$$E(n') = \frac{1}{n}\left(n + \sum_{j=1}^{a} k^j \sum_{i=1}^{a-j} k^i \right) = a + 1 - \frac{1 - \frac{a+1}{n}}{k-1}. \quad (1)$$

То есть чем больше число k, тем меньше $E(n')$.

В общем случае, когда нет условия о равенстве величины $d^+(v)$ для всех вершин и отсутствует ограничение на количество уровней, математическое ожидание числа вершин n', от которых теряется информация под воздействием атаки Black Hole, будет следующим:

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

где $V_j \subseteq V$ – вершины, принадлежащие уровню j.

Из формулы (2) следует, что, чем меньше число транзитов для передачи данных от вершины к стоку (число хопов), тем меньше $E(n')$.

Величину $E(n')$ можно интерпретировать как средний номер уровня для вершин (то есть сумма номеров уровней всех вершин, деленная на количество вершин). Таким образом получаем приближенную оценку количества атакованных узлов.

Выводы

Исследование воздействия атаки Black Hole в общем случае проведено с помощью имитационного моделирования. Для генерации случайных UDG-графов, отображающих топологию БСС, использовался подход, описанный в работе [14]. В качестве алгоритма маршрутизации выбран Minimum Energy Route [15]. Для оценки уязвимости дерева передачи данных к атакам использовалась величина «нормированное число вершин, от которых потеряна информация» – среднее число вершин, от которых потеряна информация, деленное на общее число вершин в дереве. Так, для БСС, содержащей 500 узлов, количество атакованных узлов не превышает 10 %, а для БСС, содержащей 2 000 узлов, из строя будет выведено примерно 5 % узлов. Полученные в результате имитационного моделирования оценки хорошо согласуются с формулами, выведенными в предыдущем разделе.

Заметим, что ущерб от разрушающего воздействия атаки Black Hole на узлы беспроводной сенсорной сети существенно зависит от того, какой алгоритм маршрутизации применяется в сети для сбора данных. За счет выбора надлежащего алгоритма можно существенно повысить надежность и живучесть БСС. Данное направление является темой будущих исследований авторов.

Работа выполнена при поддержке РФФИ, грант № 14-07-00769 а.

Литература

1. Oliveira T., Godoy E. ZigBee wireless dynamic sensor networks: feasibility analysis and implementation guide. IEEE Sensors Jour., 2016, vol. 16, iss. 11, pp. 4614–4621.

2. McEwen A., Cassimally H. Designing the Internet of Things. John Wiley & Sons Ltd, UK, 2014, 336 p.

3. Uckelmann D., Harrison M., Michahelles F. Architecting the Internet of Things. Springer-Verlag Berlin Heidelberg, 2011, 356 p.

4. Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E. Wireless sensor networks: a survey. Comp. Networks, 15 March 2002, vol. 38, iss. 4, pp. 393–422.

5. Иващенко А.В., Минаев А.А., Сподобаев М.Ю. Шаблон агента-медиатора для программного обеспечения сенсорных сетей // Программные продукты и системы. 2015. № 3. С. 166–170.

6. Shakhov V.V., Popkov V.K. Performance analysis of sleeping attacks in wireless sensor networks. Proc. IEEE Region 8th Intern. Conf. on Computational Technologies in Electrical and Electronics Engineering (SIBIRCON), 2008, pp. 418–420.

7. Cayirci E., Rong C. Security in Wireless Ad Hoc and Sensor Networks. John Wiley & Sons, 2009, 280 p.

8. Praveen K.S., Gururaj H.L., Ramesh B. Comparative analysis of Black Hole attack in ad hoc network using AODV and OLSR protocols. Procedia Comp. Sc., 2016, vol. 85, pp. 325–330.

9. Clark A., Colbourn C., Johnson D. Unit disk graphs. Discrete Mathematics, 1990, vol. 86, pp. 165–177.

10. Shakhov V. Experiment design for parameter estimation in sensing models. Springer LNCS, 2013, vol. 8072, pp. 151–158.

11. Singh S.K., Singh M.P., Singh D.K. Routing protocols in wireless sensor networks – a survey. IJCSES, 2010, vol. 1, no. 2, pp. 63–83.

12. Safonov A., Lyakhov A., Urgenson A., Sokolova O. Wireless groupcast routing with palette of transmission methods. Multiple Access Communications, 2012, pp. 97–108.

13. Dokurer S., Erten Y., Acar C. Performance analysis of ad-hoc networks under black hole attacks. Proc. of IEEE Int. Conf. Southeast, March, 2007, pp. 148–153.

14. Shakhov V.V., Sokolova O., Yurgenson N. A fast method for network topology generating. Lecture notes in comp. sc., Springer, 2014, vol. 8715, pp. 96–101.

15. Yang L., Yang H.C. and Wu K. Minimum-energy route configuration for wireless ad hoc networks. 2006 IEEE Intern. Performance Comp. and Communications Conf., Phoenix, AZ, 2006, pp. 6–14.

Software & Systems
DOI: 10.15827/0236-235X.117.034-039

Received 19.08.16
2017, vol. 30, no. 1, pp. 34–39

MODELLING AND SIMULATION OF BLACK HOLE ATTACK ON WIRELESS NETWORKS

V.V. Shakhov[1], *Ph.D. (Physics and Mathematics), Associate Professor, Senior Researcher, shakhov@rav.sscc.ru*
A.N. Yurgenson[1], *Ph.D. (Physics and Mathematics), Research Associate, nastya@rav.sscc.ru*
O.D. Sokolova[1], *Ph.D. (Engineering), Senior Researcher, olga@rav.sscc.ru*

[1] *Institute of Computational Mathematics and Mathematical Geophysics SB RAS, Academician Lavrentev Ave. 6, Novosibirsk, 630090, Russian Federation*

Abstract. The technologies based on wireless sensor networks can be used in a wide range of vital applications. There are several implementations of the Internet of Things architecture based on wireless sensor networks. For example, the core objective in the projects of the 7th Framework Programme funded by the European Union was to provide the technical foundation for WSN technology in IoT products and services. As wireless sensor networks based applications are deployed, security becomes an essential requirement.

In this paper the authors discuss the state-of-arts for security issues in WSN. It is impossible in all cases to provide absolute protection and eliminate the consequences of intrusion. However, the effective range of protection mechanisms will significantly reduce the damage. To achieve this it is necessary to develop and explore appropriate mathematical models.

The paper focuses on the attack named Black Hole. This attack has one of the most dangerous destructive information impacts. As a result, more than 90 % of the information transmitted to the sink may be lost. The direct transmission of information between the nodes in WSN is possible if they are within each other's radio reachability. Therefore, the unit disk graphs (UDG-graphs) might be used as a wireless network model. Communication in these networks are described by UDG-models the most appropriate. To simulate data transmission by the routing algorithm in the graph, a spanning tree is constructed. The authors have obtained the formula for calculating analytical estimates for some cases of a spanning tree structure. To assess the vulnerability of this tree to attacks the authors used the value “normalized number of vertices with lost information”. It shows the average number of vertices which lose information, divided by the total number of nodes on the tree. The analytical results are consistent with simulation results. The paper offers a counteracting method against Black Hole and provides the corresponding performance analysis as well.

Keywords: wireless sensor networks, security, Black Hole attack.

Acknowledgements. *The research has been financially supported by RFBR, grant no. 14-07-00769 a.*

References

1. Oliveira T., Godoy E. ZigBee Wireless Dynamic Sensor Networks: Feasibility Analysis and Implementation Guide. *IEEE Sensors Jour*. 2016, vol. 16, iss. 11, pp. 4614–4621.

2. McEwen A., Cassimally H. *Designing the Internet of Things*. John Wiley & Sons Publ., UK, 2014.
3. Uckelmann D., Harrison M., Michahelles F. *Architecting the Internet of Things*. Springer-Verlag Berlin Heidelberg Publ., 2011.
4. Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E. Wireless sensor networks: a survey. *Computer Networks*. 2002, vol. 38, iss. 4, pp. 393–422.
5. Ivaschenko A.V., Minaev A.A., Spodobaev M.Yu. A mediator pattern for sensor networks software. *Programmnye produkty i sistemy* [Software & Systems]. 2015, no. 3, pp. 166–170 (in Russ.).
6. Shakhov V.V., Popkov V.K. Performance analysis of sleeping attacks in wireless sensor networks. *Proc. IEEE Region 8 Int. Conf. on Computational Technologies in Electrical and Electronics Engineering (SIBIRCON)*. 2008, pp. 418–420.
7. Cayirci E., Rong C. *Security in Wireless Ad Hoc and Sensor Networks*. John Wiley & Sons Publ., 2009.
8. Praveen K.S., Gururaj H.L., Ramesh B. Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols. *Procedia Computer Science*. 2016, vol. 85, pp. 325–330.
9. Clark A., Colbourn C., Johnson D. Unit disk graphs. *Discrete Mathematics*. 1990, vol. 86, pp. 165–177.
10. Shakhov V. Experiment Design for Parameter Estimation in Sensing Models. *Springer LNCS*. 2013, vol. 8072, pp. 151–158.
11. Singh Sh.K., Singh M.P., Singh D.K. Routing Protocols in Wireless Sensor Networks – A Survey. *Int. Jour. of Computer Science & Engineering Survey (IJCSES)*. 2010, vol. 1, no. 2, pp. 63–83.
12. Safonov A., Lyakhov A., Urgenson A., Sokolova O. Wireless groupcast routing with palette of transmission methods. *Multiple Access Communications*. 2012, pp. 97–108.
13. Dokurer S., Erten Y., Acar C. Performance analysis of ad-hoc networks under black hole attacks. *Proc. of IEEE Int. Conf. SoutheastCon 2007*. 2007, pp. 148–153.
14. Shakhov V.V., Sokolova O., Yurgenson N. A Fast Method for Network Topology Generating. *Lecture Notes in Computer Science*. Springer Publ., 2014, vol. 8715, pp. 96–101.
15. 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.

Примеры библиографического описания статьи

1. Шахов В.В., Юргенсон А.Н., Соколова О.Д. Моделирование воздействия атаки Black Hole на беспроводные сети // Программные продукты и системы. 2017. Т. 30. № 1. С. 34–39; DOI: 10.15827/0236-235X.117.034-039.

2. Shakhov V.V., Yurgenson A.N., Sokolova O.D. Modelling and simulation of Black Hole attack on wireless networks. *Programmnye produkty i sistemy* [Software & Systems]. 2017, vol. 30, no. 1, pp. 34–39 (in Russ.); DOI: 10.15827/0236-235X.117.034-039.