К ВОПРОСУ ОБ ЭФФЕКТИВНОСТИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

В. В. Шахов*, В. Е. Стрельников**, Нгуен Ван Дюк***

*Институт вычислительной математики и математической геофизики
СО РАН, 630090, Новосибирск, Россия;[1]
**Новосибирский государственный технический университет
630073, Новосибирск, Россия;
***Ханойский университет науки и технологий
Ханой, Вьетнам

УДК 621.391

Беспроводные сенсорные сети обладают серьезным потенциалом для внедрения в самых разных отраслях. Специалистами ведущих компаний отмечено, что сенсорные сети могут помочь улучшить наше представление об окружающем мире, тем самым открыв возможности для создания принципиально новых приложений. Таким образом, технология является очень привлекательной. Однако при этом стоимость сенсоров должна быть низкой, что влияет на надежность рассматриваемых систем. В данной статье мы анализируем вопросы, связанные с поиском компромисса между надежностью системы и затратами на ее развертывание, приводим соответствующий обзор публикаций.

Ключевые слова: беспроводные сенсорные сети, надежность, производительность.

Wireless sensor networks is a technology with a high potential for different areas. It is mentioned that sensor networks can vastly enrich our understanding of how the world works and opening the door to entirely new computing applications. Therefore it is a very attractive technology. However, sensors have to be inexpensive. It leads to systems unreliability. In this paper, we present a review of the problems related to the tradeoff between system performance and system deployment cost for the mentioned networks.

Key words: wireless sensor networks, survivability, reliability, performance.

Введение. Последние достижения в области технологий микроэлектроники и беспроводной связи позволили создавать недорогие, маломощные, многофункциональные моты (узлы, сенсоры), обладающие небольшими размерами и способные кооперироваться друг с другом для участия в сборе и передаче данных. Технологиям, основанным на использовании беспроводных сенсорных сетей (БСС), предсказан рыночный успех. В настоящее время данным сетям уделяется повышенное внимание в отечественных и иностранных исследовательских центрах. Беспроводные сенсорные сети основаны на совместной работе большого числа крошечных узлов, каждый из которых состоит из модуля сбора и обработки данных, источника питания, а также приемопередатчика. Некоторые узлы (моты), располагаются близко к наблюдаемому явлению, осуществляют его мониторинг, другие узлы могут и не участвовать в мониторинге, но служить для передачи наблюдаемых сведений в центр сбора информации.

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 14-07-00769).

Сенсорные сети могут состоять из различных типов датчиков, например, сейсмических, датчиков определения магнитного поля, тепловых, инфракрасных, акустических, которые в состоянии осуществлять самые разнообразные измерения условий окружающей среды, таких как температура, влажность, давление, уровень шума и др.

Моты могут использоваться для непрерывного зондирования, обнаружения и идентификации событий. Концепция микрозондирования и беспроводное соединение обещают много новых областей применения для таких сетей: системы военного назначения, исследование окружающей среды, здравоохранение, экологический мониторинг, системы „умный дом“ и др.

Положение мотов не всегда нужно предварительно рассчитывать. Как правило, предполагается, что моты случайным образом распределены в труднодоступных местах, например, разбросаны с вертолета в лесу. Также возможно использование мотов в местах, где требуется быстрое реагирование на какое-либо явление, например, природная или техногенная катастрофа. Наиболее важной особенностью сенсорных сетей является совместная работа отдельных узлов. Моты оснащены микропроцессором, поэтому вместо передачи исходных данных они могут их обрабатывать, выполняя простые вычисления, и передавать далее только необходимые и частично обработанные данные. Это означает, что сетевые протоколы и алгоритмы работы мотов должны обладать возможностью самоорганизации, а также сеть должна быть отказоустойчивой при каком-либо внешнем воздействии. В то же время, согласно требованиям рынка стоимость узлов должна быть дешевой, что серьезно влияет на надежность и производительность сети. В данной работе проводится анализ проблем, обусловленных необходимостью поиска компромисса между производительностью БСС и стоимостью сетевых узлов. Рассматриваются наиболее популярные разрушающие воздействия на беспроводные сенсорные сети, выделяются их характерные признаки. Анализируется возможность снижения стоимости БСС за счет уменьшения количества используемых сенсоров.

1. Обзор разрушающих воздействий в БСС. Узлы БСС могут выйти из строя из-за истощения батареи, физических повреждений или стороннего вмешательства. Отказ узла не должен повлиять на работу сенсорной сети, она должна обладать свойством отказоустойчивости, т. е. способностью поддерживать функциональность сенсорной сети без сбоев при выходе из строя некоторых ее элементов.

Стоит обратить внимание на то, что протоколы и алгоритмы могут быть ориентированы на уровень отказоустойчивости, требуемый для построения сенсорных сетей. Если среда, в которой узлы размещены, мало подвержена вмешательствам, то протоколы могут быть менее отакзоустойчивыми. Например, если сенсоры установлены в домах, чтобы следить за влажностью и уровнем температуры, требования к отказоустойчивости могут быть низкими, поскольку такого рода сенсорные сети редко выходят из стоя, и „шум“ окружающей среды не влияет на их работу. С другой стороны, если узлы используются на поле боя для наблюдения, то отказоустойчивость должна быть высокой, поскольку наблюдения являются критически важными и узлы могут быть уничтожены во время военных действий. В результате уровень отказоустойчивости зависит от применения сенсорных сетей, и модели должны быть разработаны с учетом этого.

В работе [1] Вуд и Станкович классифицировали различные разрушающие воздействия на сенсорные сети в соответствии с сетевыми уровнями. В таблице приведены типичные угрозы, а также возможные способы защиты от них. Рассмотрим их подробно.

Физический уровень.

Глушение. Широко известная атака на беспроводные связи путем вмешательства в радиочастоты, которые используются узлами сети. Небольшое количество случайно распределенных узлов глушения может нарушить работу всей сети и привести к выходу из строя всех узлов сети.

Подделка. Крупномасштабная сенсорная сеть может состоять из тысяч сенсоров, которые могут быть рассредоточены по большой площади. Это непрактично предполагать, что можно контролировать и защищать каждый отдельный датчик от нападений. Злоумышленник может захватить узел и исследовать его физически. Если злоумышленник „вскроет“ узел, то он может извлечь из него ключевую информацию, данные и коды, которые хранятся на этом узле. Злоумышленик может также перепрограммировать захваченный узел или клонировать несколько узлов из захваченного узла. Большое количество атак может быть осуществлено после получения криптографических ключей и кодов.

Канальный уровень.

Создание коллизий. Сенсорные узлы взаимодействуют друг с другом через общий беспроводной канал. Злоумышленник может вызвать коллизию одновременной передачей в диапазоне помех. Один байт коллизии может повредить весь кадр. Поврежденный пакет маршрутизации или кадр управления MAC может привести к большим накладным расходам.

Разрядка. Если в сети используется протокол MAC, злоумышленник может попытаться сделать передачу к узлу неоднократно, и это приводит к тому, что соседние узлы не могут передать ему какой-либо кадр. Например в некоторых протоколах существуют сообщения Request-To-Send (RTS), Clear-To-Send (CTS) и Data-Ack, для того чтобы зарезервировать доступ к каналу и передавать данные. Злоумышленник может неоднократно запросить доступ к каналу с помощью RTS, вызывая реакцию CTS от соседа. Если злоумышленник обладает узлом с большой мощностью (например, ноутбук с большой дальностью передачи и перезаряжаемым энергоснабжением), то он способен блокировать передачу датчиков в большой области, а также исчерпать энергию целевых узлов.

Сетевой уровень.

Манипулирование маршрутной информацией. Самой прямой атакой против протокола маршрутизации является целевой захват маршрутной информации, которой обмениваются между узлами [2]. Подменив маршрутную информацию, злоумышленник сможет создать маршрутные петли, фильтровать сетевой трафик, увеличить или сократить исходные маршруты, создавать ложные сообщения об ошибке, разделении сети, увеличении задержки и т. д.

Выборочная передача пакетов. Многие протоколы маршрутизации сенсоров основаны на предположении, что участвующие узлы будут добросовестно передавать принятые пакеты. В атаке выборочной передачи измененные или вредоносные узлы могут выборочно передавать некоторые пакеты, а другие просто подавлять. Обычно злоумышленник заинтересован в подавлении или изменении пакетов от некоторых отдельных узлов и может спокойно передавать оставшийся трафик и сводить свое подозрение к минимуму. Подобная атака, как правило, наиболее эффективна, когда злоумышленник явно подключен к маршруту.

„Sybil Attack“. В атаке данного типа [3] один узел представляет несколько „личностей“ другим узлам в сети. Атака Sybil может заметно уменьшить эффективность отказоустойчивых схем: распределенное хранилище, маршрутизация через несколько путей и

Таблица

Классификация DoS-атак

Уровень	Атаки	Возможный способ защиты
Физический	Глушение	Использование широкополосного вещания
	Ручное вмешательство	Эффективное управление ключами
Канальный	Создание коллизии	Коды коррекции ошибок
	Разрядка батареи	Ограничение скорости связи
Сетевой	Фальсификация маршрутной информации	Аутентификация, кодирование
	Выборочная передача пакетов	Зондирование
	„Sybil attack“	Аутентификация
	„Blackhole attack“	Авторизация, слежение
	„Wormhole attack“	Слежение, гибкий выбор маршрута
	„Hello Flood“	Двухсторонняя аутентификация
Транспортный	„Наводнение“	Ограничение количества соединений
Другие	„Clone attack“	Криптография

обслуживание топологий. Атаки также представляют собой значительную угрозу для географических протоколов маршрутизации. Географическая маршрутизация часто требует от узлов обмениваться пакетами с координатами со своими соседями для эффективной маршрутизации. Разумно ожидать, что узел должен принять один набор координат от каждого из своих соседей, но с помощью данной атаки злоумышленник может быть больше чем в одном месте.

„Blackhole Attack“. В данной атаке [2] целью злоумышленника является передача всего трафика из конкретной области через взломанный узел, создавая метафорическую черную дыру со злоумышленником в центре. Подобные атаки могут включать в себя атаки другого типа, например, выборочную передачу пакетов. Обычно при подобной атаке используется взломанный узел, который очень „привлекателен“ соседним узлам по отношению к алгоритму маршрутизации. Например, взломанный узел может сообщить соседям, что через него проходит самый качественный путь к базе. Некоторые протоколы могут проверить качество данного маршрута. В этом случае злоумышленник с ноутбуком и мощным передатчиком может обеспечить высококачественный маршрут, передавая с достаточной мощностью, чтобы достичь базу в один прыжок. В связи с этим каждый сосед взломанного узла будет пересылать весь свой трафик через него, а также сообщать своим соседям об этом маршруте.

„Wormhole attack“. В данной атаке [4] злоумышленник перехватывает сообщения, полученные в одной части сети по каналу низкой задержки и дублирует их в другой части. Обычно данная атака включает два удаленных вредоносных узла в сговоре занижать их расстояние между друг другом, передавая пакеты вдоль канала, который доступен только для злоумышленника. Злоумышленник, который находится в непосредственной близости к базе, может полностью нарушить маршрутизацию, создав хорошо установленный „wormhole“. Злоумышленник через „wormhole“ может убедить узлы, которые находятся далеко от базы, в том, что они от нее в двух хопах. Такая атака используется в сочетании с выборочной передачей пакетов. Обнаружение почти невозможно.

„Hello Flood“. В работе [2] авторы представили тип разрушающего воздействия на сенсорные сети, сходный по способу с атаками в традиционных IP сетях. Эта атака использует однонаправленные соединения между узлами. Многие протоколы требуют от узлов трансляции приветственных пакетов, чтобы объявить себя для своих соседей, и узел, который принял такой пакет, может считать, что он находится в необходимом радиодиапазоне отправителя. Это предположение может быть неверным, отсюда и появляются проблемы одноранговых сетей. Например, злоумышленник с мощным устройством (ноутбук), который вещает информацию маршрутизации с достаточно большой мощностью передачи, может убедить достаточно много узлов, что он является одним из их соседей. Но так как узлы находятся далеко от злоумышленника, они будут посылать пакеты в пустоту, из-за этого сеть будет находиться в состоянии растерянности.

Специфика оставшихся угроз существенно не отличается от рассмотренных выше.

3. Математические методы. В данном разделе рассмотрим математические методы для оптимизации БСС при ограниченных ресурсах.

Надежность $R_k(t)$ или отказоустойчивость узла часто моделируется с помощью распределения Пуассона [5], т. е. для определения вероятности отсутствия неисправности узла в период времени $(0; t)$:

$$R_k(t) = exp(-\lambda_k t),$$

где λ_k и t являются интенсивностью отказа сенсорного узла k и периодом времени соответственно. Таким образом, для анализа надежности (и производительности) БСС в достаточно большом количестве случаев можно использовать математический аппарат, основанный на цепях Маркова. Следовательно, если для конкретной ситуации можно составить диаграмму состояний, то можно определить вероятности состояний, пребывание в которых отражает надежность системы. Используя полученные значения, можно вычислять метрики, связанные с отказоустойчивостью (производительностью) системы, такие как среднее время жизни сети, время до отказа узла, коэффициент утилизации и т. д. Таким образом, получаем способ формирования целевых функций и ограничений в экстремальных задачах, связанных с поиском компромисса между надежностью сети и затрачиваемыми ресурсами [6–8].

В более общем случае аналитические методы для оптимизации БСС, как правило, не пригодны. Приходится использовать имитационное моделирование для сравнения альтернативных стратегий организации сетей. Однако и в данном случае необходимо решить ряд математических проблем. В частности, на адекватность выводов серьезно влияет выбор алгоритма генерации псевдослучайных топологий БСС [9, 10].

Существенного снижения стоимости БСС можно добиться путем уменьшения количества узлов в сети, если при этом производительность остается на приемлемом уровне. Указанная экономия возможна за счет оптимизации размещения сенсоров, настройки сетевых протоколов, снижения избыточности сенсоров при их случайном распределении. Для постановки данных оптимизационных задач необходимо повысить точность измерений, проводимых узлами БСС. Основным инструментом, позволяющим извлечь наибольшее количество сведений о наблюдаемых процессах, является теория оптимального планирования эксперимента [11–13].

К настоящему времени можно выделить два основных направления в математической теории планирования экспериментов: планирование экстремальных экспериментов и планирование экспериментов по выяснению механизма явлений.

Планирование первого типа применяется в тех случаях, когда интересуют условия, при которых изучаемый процесс удовлетворяет некоторому критерию оптимальности. Обычно необходимо выяснить поведение исследуемого объекта в целом или выяснить механизм явления.

Исследование математического вида зависимости некоторой величины от соответствующих факторов дает информацию, на основе которой, привлекая необходимый инструментарий, делаются выводы о конкретном виде элементарных взаимодействий.

Рассмотрим подробнее математическую постановку проблемы планирования экспериментов по выяснению механизма явления. Обычно измеряемая величина зависит от одного или нескольких факторов, называемых „контролируемыми переменными“, т. е. значения каждого из факторов могут быть выбраны произвольно из некоторой заданной области. В качестве контролируемых переменных в зависимости от типа эксперимента могут фигурировать самые разнообразные величины, например: время, угол рассеяния падающих на мишень частиц, температура, напряжение, подаваемое на испытываемый прибор, процентное содержание реагентов в химических или биологических исследованиях и т. д. Каждому набору указанных величин сопоставляется вектор-столбец

$$X = \left\| \begin{matrix} x_1 \\ x_2 \\ \dots \\ x_k \end{matrix} \right\|,$$

координаты которого $x_1, x_2, \dots, x_k$ равны значениям контролируемых переменных, занумерованных в удобном для экспериментатора порядке.

Пространство размерности к, в котором определен вектор X, называется факторным пространством или пространством контролируемых переменных. Совокупность точек этого пространства, где измерения возможны (т. е. соответствующие значения контролируемых переменных $x_1, x_2, \dots, x_k$ могут быть реализованы экспериментатором), называется областью возможных измерений или областью действия.

Определение границ области X играет важную роль в практических задачах при планировании оптимальных экспериментов. В некоторых случаях эти границы определяются самой природой контролируемой переменной. Например, процентное содержание вредных примесей в среде, мониторинг которой осуществляет БСС, не может быть меньше нуля и больше 100 %, размеры исследуемых объектов – отрицательными и т. д. В других случаях, встречающихся значительно чаще, границы области действия определяются характеристиками аппаратуры, которой обладает узел БСС (исследователь, экспериментатор), или видом исследуемого процесса.

Задачей эксперимента для подбора математической модели является отыскание связи между измеряемыми переменными. Так как результаты наблюдений — величины случайные, то в большинстве случаев имеет смысл говорить о связи средних значений исследуемых величин с контролируемыми переменными. В дальнейшем будем предполагать, что эта связь может быть описана некоторой функцией:

$$E\left(\frac{y}{x}\right) = \mu(x),$$

где $E(y/x)$ — среднее значение исследуемой величины y при значениях контролируемых переменных, определяемых координатами вектора x, функция $\mu(x)$ зависит от неизвест-

ных параметров $\vartheta_1, \vartheta_2, \ldots, \vartheta_m$, и в общем случае ее вид может быть также неизвестен. В научных статьях и монографиях по статистическим методам данная функция называется поверхностью отклика.

Приступая к поиску математической модели (функции μ(x)), экспериментатор обладает некоторой априорной информацией. Степень его информированности можно характеризовать тремя основными уровнями.

1) Функция $\mu(x) = \mu(x, \vartheta)$ известна. Требуется определить или уточнить неизвестные параметры

$$\vartheta = \begin{Vmatrix} \vartheta_1 \\ \vartheta_2 \\ \ldots \\ \vartheta_k \end{Vmatrix}.$$

2) Известно, что функция $\mu(x)$ совпадает с одной из функций

$$\mu(x) = \begin{cases} \mu_1(x, \vartheta_1), \\ \mu_2(x, \vartheta_2), \\ \ldots \\ \mu_k(x, \vartheta_k) \end{cases}.$$

Требуется определить, какая из функций является истинной, и найти неизвестные параметры.

3) Вид функции $\mu(x)$ неизвестен. Известно лишь, что данная функция в интересующей исследователя области может быть достаточно хорошо аппроксимирована конечным рядом по некоторой системе наперед заданных функций. Требуется найти наилучшее описание функции $\mu(x)$.

Хотя приведенное выше разбиение не вполне подробно, и можно привести примеры, когда ситуация занимает промежуточное состояние между какими-либо двумя описанными выше уровнями, оно удобно с точки зрения существующих методов планирования эксперимента и хорошо описывает большинство реальных случаев.

Математический аппарат планирования экспериментов при условиях, соответствующих первому уровню, достаточно хорошо разработан. Для данного случая развиты эффективные методы статического и последовательного планирования экспериментов. Под статическим планированием эксперимента здесь понимается априорное планирование всего эксперимента в целом; под последовательным планированием — планирование эксперимента по этапам, т. е. планируются одно или несколько измерений, затем эти измерения реализуются, проводится обработка полученных данных, и затем вновь приступают к планированию и т. д.

Методы планирования экспериментов по выбору модели из некоторой заданной совокупности моделей появились относительно недавно. Следует отметить, что указанные методы планирования экспериментов тем эффективней, чем меньше число конкурирующих моделей отклика. Этим иллюстрируется основная закономерность планирования эксперимента: чем больше мы знаем, тем лучше, эффективней можем планировать. Отсюда следует важность задачи сужения множества моделей для выбора.

Наиболее сложной является задача планирования эксперимента, когда функция отклика совершенно неизвестна. Невозможно спланировать эксперимент, который позволил бы

разрешить проблему в целом. Однако ее решение можно свести к последовательной процедуре, которая подразумевает чередование экспериментов (планирование и практическое осуществление) следующих видов:

а) функциональный вид поверхности отклика известен, требуется определить или уточнить ее параметры;

б) на основании теоретического анализа или в результате предыдущих экспериментов выдвинуто две (или несколько) гипотезы о виде поверхности отклика.

Требуется найти зависимость, наилучшим образом описывающую изучаемый объект.

Если функция отклика после оценки параметров удовлетворяет экспериментальным данным, то эксперимент либо прекращается, либо планируется дополнительный эксперимент по уточнению всей совокупности параметров или некотрого наиболее важного подмножества параметров. Если полученная функция отклика не удовлетворяет экспериментальным данным, то возникает необходимость более тщательного анализа происходящих явлений. Возможно, потребуется проведение большого количества уточняющих экспериментов.

Рассмотренные подходы к планированию эксперимента могут быть использованы для повышения эффективности БСС.

Одним из наиболее важных показателей эффективности сенсоров беспроводных сетей является качество инструментов, необходимых для обнаружения рассматриваемого события. Чувствительная способность беспроводных сенсоров описывается моделью чувствительности сенсоров. Выбор модели сильно влияет на проектирование беспроводных сенсорных сетей и выполнение протоколов [14], таких как агрегации трафика, радиовещание, маршрутизация, передача сигналов или помех в зоне действия и т. д. Поэтому полезно исследовать природу чувствительности сенсоров, их свойства и то, каким образом они зависят от характеристик беспроводных сенсорных сетей. Модели чувствительности сенсоров непосредственно влияют на общее проектирование беспроводной сенсорной сети, и было бы очень трудно разработать эффективные беспроводные сенсорные сети без соответствующих моделей чувствительности сенсоров.

Вероятностное обнаружение является преобладающей методологической основой для моделирования диапазона чувствительности. Его использование зачастую требует некоторых упрощений, однако эти модели обеспечивают основу для адекватных приближений диапазона чувствительности, а также ценных результатов и стоящих идей. Хорошо известен факт, что стоимость компонентов сенсора является основным фактором при разработке реальных сенсорных сетей. Стоимость сенсорной сети увеличивается с увеличением мощности аккумулятора сенсора. Зачастую, в обычных беспроводных сенсорных сетях экономически выгодно отказываться от мощных аккумуляторов и просто подзаряжать сенсоры. По этой причине заряд аккумулятора обычно является уязвимым элементом беспроводных сенсоров. С другой стороны, от производительности аккумулятора зависит диапазон чувствительности. Таким образом, мы не можем игнорировать коэффициент потери информации в процессе обнаружения события. Это означает, что неподходящие модели чувствительности сенсоров приводят к повышению или понижению стоимости сенсора (или количеству сенсоров в сети), неэффективному управлению циклами работы сенсоров, неэффективному распределению сенсоров и т. д.

Как уже было сказано выше, возможность обнаружения события сенсором обычно оценивается вероятностно. Вероятность обнаружения событий уменьшается с увеличением расстояния между сенсором и целью. Как правило, коэффициент вероятности обнаруже-

ния события (модель чувствительности сенсора) указан. Тем не менее, имеется неизвестный параметр, который должен быть экспериментально оценен. Этот параметр зависит от конкретной ситуации: условия распространения сигнала и т. д. Правильный выбор параметров модели чувствительности сенсоров определяет адекватность этой модели.

В литературе описано несколько типов моделей чувствительности сенсоров. Первый тип — двоичная модель чувствительности. Возможность обнаружения событий (вероятность) двоичной модели определяется следующим образом [15]:

$$P = \begin{cases} 1, x < R \\ 0, x \geq R, \end{cases}$$

где x — евклидово расстояние между сенсором и событием, R — диапазон чувствительности данного сенсора. Модель может быть использована в некоторых приложениях. Однако бинарная модель не является адекватной в большинстве случаев.

Самой распространенной моделью является вероятностная модель чувствительности сенсоров [16]:

$$P = \begin{cases} 1, x \leq R \\ e^{-\alpha(x-R)}, x > R. \end{cases}$$

Теперь диапазон чувствительности R выражает зону обнаружения, внутри которой сенсор может обнаружить событие без потерь. Положительный параметр α используется для оценки качества обнаружения сенсором события вне диапазона чувствительности R. Обычно величина α зависит от окружающей среды и характеристик сенсора. Должна использоваться оптимальная экспериментальная методика для получения этих параметров. Заметим, что площадь, покрытая беспроводной сенсорной сетью, может быть гетерогенной (неоднородной), а параметр может получать различные значения в пределах этой сети. В этом случае требуется серия распределенных наблюдений, при этом резко возрастает стоимость эксперимента, поэтому оптимальное планирование эксперимента становится очень важной и актуальной проблемой.

В литературе предложены еще несколько альтернативных моделей качества чувствительности сенсоров. Принято считать, что функция качества чувствительности сенсора нелинейно уменьшается с увеличением расстояния между сенсором и событием.

Покажем, что имеется влияние точности оценки параметров модели на производительность беспроводной сенсорной сети, и приведем примеры снижения стоимости БСС, основываясь на данных знаниях. Рассмотрим вероятностную модель (не учитывая общие потери), в которой $R = 0$. Пусть для обнаружения события используется группа сенсоров. Разумно уменьшить стоимость системы, т. е. числа сенсоров (n) при условии, что вероятность обнаружения события не менее установленного порога q. Предположим, что расстояние от каждого сенсора до цели одинаково и равно x. Вероятность обнаружения события вычисляется следующим образом:

$$P(n) = 1 - (1 - e^{-\alpha x})^n.$$

Необходимое количество сенсоров для обеспечения вероятность $P(n) \geqslant q$ считается по формуле:

$$n \geq \frac{\ln(1-q)}{\ln(1-e^{-\alpha x})}.$$

Пусть $q = 0,99, x = 2, \alpha = 1$. Таким образом, оптимальное количество датчиков равно 32. Если значение α недооценивается, то требование качества чувствительности может быть нарушено. Если $\alpha = 1,1$, то n равно 40. Таким образом, если относительная погрешность в оценке параметра составляет 10 %, то используются 25 % избыточных сенсоров. Поэтому затраты на проектирование сети в основном завышены. Также увеличена стоимость коммуникаций.

Рассмотрим беспроводные сенсоры с рабочим циклом на еще одном примере. Предположим, достаточно использовать один сенсор для охвата цели, если вероятность обнаружения больше или равна q. Таким образом, избыточные датчики переходят на спящий режим и ждут их очереди рабочего цикла. Пусть плотность распределения сенсоров в зоне наблюдения постоянна. Количество сенсоров, распределенных в некоторой области, прямо пропорционально площади этой области. Сенсор используется для охвата цели, если расстояние между ним и целью является следующим:

$$x \leq -\frac{\ln q}{\alpha}.$$

Если $q = 0,9, \alpha = 1$ и оценочная стоимость $\alpha = 1,1$, то площадь поля, содержащего подходящие сенсоры, снижена. В этом примере, по оценкам, число сенсоров для охвата цели уменьшается на 17 % по сравнению с реальными данными. Таким образом, рабочий цикл уменьшен на 17 %, и срок службы сети уменьшается.

Заключение. В заключение обобщим некоторые направления развития математических методов для повышения эффективности БСС. В достаточно большом количестве практических приложений можно использовать Пуассоновский процесс для моделирования потоков в БСС. Указанное допущение позволяет использовать аппарат Марковских цепей для вычисления вероятностей состояний и, затем, метрик, связанных с эффективностью БСС. Полученные метрики, в свою очередь, используются в формировании оптимизационных задач. В качестве эффективного инструментария, позволяющего снизить количество узлов БСС, можно использовать методы теории оптимального планирования эксперимента.

Список литературы

1. Wood A. D., Stankovic J. A. Denial of service in sensor networks // Comp. 2002. V. 35, N. 10. P. 54–62.

2. Karlof C., Wagner D. Secure routing in sensor networks: Attacks and countermeasures // Proc. of First IEEE Intern. Workshop on sensor network protocols and applications, 2003.

3. Douceur J. R. The Sybil Attack, John // Proc. of the 1st Intern. Workshop on peer-to-peer systems (IPTPS), 2002. P. 251–260.

4. Hu Y.-C., Perrig A., Johnson D. B. Wormhole detection in wireless ad hoc networks // Department of Computer Science, Rice University, Tech. Rep. TR01-384.

5. Hoblos G., Staroswiecki M., Aitouche A. Optimal design of fault tolerant sensor networks // IEEE Intern. conf. on control applications, anchorage, AK, Sept. 2000. P. 467-–472.

6. Shakhov V., Sokolova O., Акнмет M. Fault tolerance analysis in wireless sensor networks // Proc. of the 9th Asian Intern. workshop „Optimization problems for complex systems“, Almaty (Kazakhstan), 2013. P. 342–345.

7. Шахов В. В. Оценка экономической целесообразности внедрения механизмов противодействия DDoS атакам // Материалы 15-й Междунар. науч.-техн. конф. „Информационно-вычислитель-ные технологии и их приложения“, Пенза, 24—26 мая 2011 г. С. 159–161.

8. Шахов В. В. О применении теории СМО в задачах экономики. Там же. С. 161–163.

9. Shakhov V. V., Sokolova O. D., Yurgenson A. N. An efficient method for pseudo-random UDG graph generating // Proc. of the 7th Intern. workshop on simulation, Rimini (Italy), May 21–25, 2013. P. 325–326.

10. Шахов В. В., Соколова О. Д., Юргенсон А. Н. Эффективный метод для генерации псевдослучайных UDG-графов // Труды конференции „Информационные технологии и системы - 2013“, Калининград, 2013. С. 411–414.

11. Федоров В. В. Теория оптимального эксперимента. М.: „Наука“, 1971.

12. Хикс Ч. Основные принципы планирования эксперимента М.: Книга по Требованию, 2013.

13. Сидняев Н. И. Введение в теорию планирования эксперимента : Учеб. пособие / Н. И. Сидняев, Н. Т. Вилисова. М.: Изд-во МГТУ им. Н. Э. Баумана, 2011.

14. Wang H., Zalyubovskiy V., Shakhov V. V., Choo H. TA-MAC: A traffic-adaptive MAC protocol for asynchronous wireless // Proc. of the World congr. on computer science, computer engineering, and applied computing, Las Vegas (USA), July 16–19, 2012.

15. Akyildiz I.F., Sankarasubramaniam Y., Cayirci E. Wireless sensor networks: a survey // Broaband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA.

16. Shakhov V. V. Experiment design for parameter estimation in sensing models / V. V. Shakhov // Proc. of the 1st Intern. workshop „Wireless access flexibility“ (WiFlex 2013), Kaliningrad, Sept. 4–6, 2013. P. 151–158. (LNCS ; v. 8072).

Шахов Владимир Владимирович — канд. физ.-мат. наук,
науч. сотр. Института вычислительной математики
и математической геофизики СО РАН;
e-mail: shakhov@rav.sscc.ru
Стрельников В. Е., магистрант
Новосибирского государственного технического университета;
e-mail: kafedra_vt@vt.cs.nstu.ru; тел.: +7 (383) 3460492
Нгуен Ван Дюк, PhD, профессор
Hanoi University of Science and Technology
Tel/Fax: (++)84-4-8692241
email: duc.nguyenvan1@hust.vn

Дата поступления — 29.04.2014