УДК-004.728.4(045)

Дворская Л.А.

H-SPREAD: ГИБРИДНАЯ МНОГОПУТЕВАЯ СХЕМА ДЛЯ БЕЗОПАСНОГО И НАДЕЖНОГО СБОРА ДАННЫХ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Институт компьютерных технологий
Национального авиационного университета

Предлагается гибридная многопроходная схема (H-SPREAD) сбора и передачи информации, позволяющая повысить надежность и защищенность обмена информацией в беспроводной сенсорной сети. Схема основана на распределенном N-to-1 многопутевом протоколе обнаружения, позволяющем в течение одного процесса обнаружения пути связи каждого датчика одновременно определить несколько путей.

Введение

Современные возможности вычислительной техники и беспроводных сетей, а также технологии связи привели к внедрению беспроводных сенсорных сетей. Беспроводная сенсорная сеть (БСС) состоит из большого количества датчиков, с помощью которых осуществляется сбор информации для решения задач управления в реальном времени внутри определенной области и может обеспечить решения многих информационных задач. Хотя некоторые технологии беспроводных сетей *ad hoc* (*MANET*) применимы к БСС, однако БСС отличаются от мобильных сетей *ad hoc* во многих аспектах [1]. Например, количество узлов в БСС обычно намного больше, чем в *MANET*. Обычные датчики более ограничены в ресурсах мощности, вычислительных возможностях и памяти. Топология развертывания датчиков не предопределяется. Во многих случаях узлы сети являются статическими, топология может меняться часто из-за недостаточной надежности беспроводной связи и погрешностей измерений датчиками.

Более того, *MANET* обычно лишены инфраструктуры, связь между двумя конечными пунктами являются обычной структурой связи. Для БСС же характерно наличие одной (или больше) базовой станции (БС). Обычно все датчики предназначены для того, чтобы считывать датчик локальной среды и, по запросу, отправлять необходимую информацию к базовой станции, являющейся пунктом концентрации БСС и связью, соединяющей БСС с остальным миром.

Важными задачами, которые должны решаться в БСС, являются задачи обеспечения необходимого уровня надежности при сборе и передаче информации и обеспечения соответствующего уровня защиты информации, поскольку беспроводная передача информации между узлами доступна для многих видов вмешательств. Наиболее эффективной стратегией повышения надежности является многопроходное рассредоточение трафика [2].

Повышение надежности может быть достигнуто ценой чрезмерной избыточности, то есть отправкой большего количества информации, чем необходимо по одному маршруту таким образом, что восстановление первоначальной информации может допускать определенное количество ошибок маршрута или потерянных пакетов информации. В [3] предложен Секретный протокол *Secure Protocol for Reliable Data Delivery (SPREAD*) для доставки сообщений секретным шифрованием в *MANET*. Вместо использования единственного самого короткого пути при доставке данных от одного узла к другому *SPREAD* разбивает сообщение на многократные доли, используя схему секретного разделения, и осуществляет доставку части сообщения адресату через многократные независимые дорожки. Идея *SPREAD* показала себя эффективной для повышения безопасности в том смысле, что она более стойкая к организованным вмешательствам. Однако требуемая избыточность информации делает безопасность и надежность, по-видимому, проти-

воречащими задачами для схем, основанных на многопутевой маршрутизации.

С использованием распределенного *N-to*-1 протокола многопроходного обнаружения предлагается гибридная многопутевая схема для решения задачи более надежного и более безопасного сбора данных в БСС. В то время как большинство протоколов многопутевой маршрутизации инициализированы источником и стремятся находить многократные непересекающиеся или частично непересекающиеся дорожки между единственной парой исходных адресатов [4-11], многопутевой *N-to*-1 протокол обнаружения инициализирован получателем (то есть, инициализирован БС) и находит каждый узел датчика и набор непересекающихся дорожек к БС одновременно в конце одного процесса обнаружения маршрута.

Это очень эффективно со средним распределением меньше одного направленного сообщения на один путь. Результаты исследования гибридной многопутевой схемы сбора данных, объединяющей постоянное параллельное многопутевое рассредоточение для сбора данных сквозного шифрования и маршрутизацию обходными путями для каждой отдельной передачи пакета, показывают, что гибридная схема *Hybrid-SPREAD (H-SPREAD)* может достигнуть значительно лучшей надежности и безопасности с малой избыточностью или даже отсутствием таковой. Предлагаемая схема БСС является чрезвычайно удобной для БСС, где главная задача – одновременный сбор данных от всех узлов датчиков для базовой станции.

Краткий обзор идеи распространения (SPREAD)

В [3], предложена схема распространения *SPREAD* как дополнительного механизма для повышения конфиденциальности данных в сетях *MANET*. Основная идея и принципы работы метода распределения *SPREAD* состоит в следующем. Секретное сообщение *m* представляется в виде многократных частей *S1,S2,⋯*, в соответствии со схемой разделения секрета и доставляется адресату через множество независимых путей. Из-за существенных особенностей разделения секрета, и распределенного способа многопутевой доставки сообщения распространение *SPREAD* представляется более эластичным по отношению к организованному вмешательству до определенного числа поставленных под угрозу узлов, а поскольку даже в том случае, когда небольшое количество путей/узлов/частей и компрометировано, сообщение в целом не будет поставлено под угрозу.

Для повышения уровня надежности можно использовать множество кодирующих схем для уменьшения трафика при многопутевой маршрутизации. В качестве примера можно привести код Рида-Соломона, разнесенный прием кодирования [12], кодирование многократного описания и т.д. В схеме распространения *SPREAD* [3] используется схема порогового способа разделения секрета для разбиения информации. Схема порогового способа разделения секрета *threshold secret sharing scheme* (*T, N*) делит информацию на оптимальное количество частей *N*, названных долями (*shares or shadows*). Хорошим качеством долей *N* является то, что, имея любое количество частей менее *T*, нельзя получить никаких данных о сути информационного содержания, в то время как используя эффективный алгоритм, можно восстановить информацию, имея любое количество *T* из долей *N*. Формирование долей осуществляется с помощью оценки полинома степени *(T−1)*

$$f(x) = (a_0 + a_1 x + ... + a_{T-1} x^{T-1}) \bmod p$$

в точке $x = i$, чтобы получить *i*–ую долю:

$$S_i = f(i),$$

где $a_0, a_1, a_2, ..., a_{T-1}$ – секретные биты, пока *p* является простым числом, большим любого из коэффициентов. В случае использования коэффициентов для переноса секретных битов доля избыточной информации определяется как $\frac{N-T}{N}$. Если *T=N*, то избыточная информация, вызванная разделением секрета, отсутствует.

Согласно фундаментальной теореме алгебры значения *T* полинома степени $(T-1)$ могут полностью определить полином (т.е., все его коэффициенты), в то время как любое меньшее значение не

может определить полином (по крайней мере, в вычислительном отношении это трудно). Таким образом, любые доли T могут восстановить первоначальные секретные биты, но любое меньшее количество долей не может. Для определения полинома и интерполяции [13] разработаны эффективные алгоритмы $\left(O\left(T\log^2 T\right)\right)$. Кроме того, восстановление выполняется на базовой станции, которая в вычислительном отношении в принципе не очень ограничена. В схеме гибридного распространения *H-SPREAD*, выбран метод разделения секрета как схема кодирования.

Протокол многопутевого обнаружения N-TO-1

Выбор подходящих и эффективных протоколов многопутевой маршрутизации является определенной проблемой для любой схемы многопутевой маршрутизации. В [3] анализируются методики многопутевого обнаружения между отдельной парой, определенной исходным адресатом. В соответствии со структурой связи в БСС и анализом вышеупомянутых методик предлагается новый *N-to*-1 многопутевой протокол обнаружения (*multipath discovery protocol*). Вместо того, чтобы находить множество путей между определенным источником и определенным адресатом, предложенный многопутевой *N-to-1* протокол обнаружения использует преимущества лавинной маршрутизации (*flooding*) в процессе обычного обнаружения пути и находит множество непересекающихся путей от каждого узла датчика до общего адресата (то есть, узел слива) одновременно. Предлагаемый многопутевой *N-to-1* протокол обнаружения наиболее приемлем для гибридной схемы сбора данных. Определим возможности распределенного протокола в отыскании пути.

Типичной задачей БСС является сбор данных. Базовая станция передает запрос об интересующих данных и каждый узел датчика (или узлы, которые имеют интересующие данные) посылает свои показания назад к базовой станции. Для этой цели базовая платформа датчика Беркли *TinyOS* (*Berkeley's TinyOS sensor platform*) использует протокол указания пути на основе лавинной маршрутизации (*flooding-based beaconing protocol*). Базовая станция периодически передает обновление маршрута. Каждый узел датчика, получая обновление впервые, ретранслирует обновление и указывает узел, от которого он получил обновление как исходный. Это продолжается рекурсивно, пока каждый узел в сети не ретранслирует обновление и найдет его исходник.

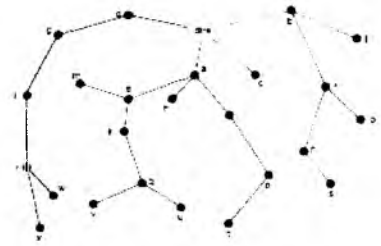

Рис.1 Схема распределения на основе лавинной маршрутизации

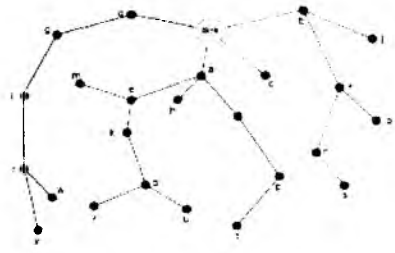

Рис.2 Простое многопутевое распространение лавинной маршрутизации

Из этого следует, что каждый узел отправляет пакеты, которые получил или сгенерировал соседнему узлу до тех пор, пока пакеты не достигнут базовой станции [14]. Как показано на рис.1, протокол испускания маяка (*beaconing protocol*) по существу создает широту, сначала строящую дерево с разводкой от базовой станции. Он находит каждому узлу датчика свой оптимальный путь к базовой станции. Однако, надежность и безопасность страдают из-за маршрутизации единственным путем. Отказ одного узла или связи разрушат поток данных от узла непосредственно и всех его дочерних узлов. Точно так же компрометация одного из узлов приведет к утечке информации от этого узла и всех дочерних.

Предложенный протокол многопутевого обнаружения *N-to-1* основан на простой лавинной маршрутизации, инициализированной на базовой станции. Тогда, с помощью введения двух разных механизмов в структуру протокола, он может найти для каждого узла датчика мно-

жество непересекающихся путей к базовой станции в конце процесса обнаружения распределенного пути. Можно представить процедуру многопутевого обнаружения в двух фазах, в каждой из которых осуществляется реализация одного из механизмов. Фактически, вторая фаза может начаться в каждом отдельном узле с помощью распределенного способа, не ожидая завершения фазы в других узлах. Механизм, используемый в первой фазе, называемый лавинной маршрутизацией методом ветвей (*branch aware flooding*), использует преимущества технологии простой лавинной маршрутизации. Не вводя дополнительных направляемых сообщений, механизм способен найти определенное количество непересекающихся путей в зависимости от плотности топологии сети. Механизм, используемый во второй фазе, названный многопутевым распространением лавинной маршрутизации *(multipath extension of flooding*), помогает менять непересекающиеся пути, найденные в первой фазе между узлами в разных ветках. Выполнением некоторых обменов сообщений он способен увеличить количество путей, найденных на каждом узле датчика. Рассмотрим более подробно.

Первая фаза: Лавинная маршрутизация методом переходов (branch aware flooding)

Общая форма направленных сообщений в обеих фазах – *{mtype,mid, nid, bid, cst, path}*,где:

mtype определяет тип сообщения. Определяем *mtype*= "*RPRI*" для первой фазы. Она обращается к "первичному" пути, потому что первичные пути (пути, которые находятся на самом коротком дереве маршрута), найдены этим типом сообщений;

mid является порядковым номером текущего обновления маршрутизации;

nid – идентификатор узла, отсылающего сообщение;

bid – идентификатор ветки, определяемой как *nid* узла, самого близкого к базовой станции на этой ветке;

path содержит последовательность узлов, которые сообщение уже прошло;

cst - стоимость пути.

Распространение сообщений *RPRI* следует точно тем же самым путем, как протокол испускания маяка *TinyOS* (*TinyOS beaconing protocol*). Базовая станция инициализирует обновление маршрутизации периодически (или по требованию), передавая сообщение *{RPRI,mid, Sink,Ø, 0, (Sink)}*. Каждый узел, допустим *z*, видя сообщение *{RPRI,mid, nid, bid, cst, path}* впервые, указывает узел *nid* как «первичный», и он также изучает первичный путь назад к базовой станции, следуя обратному порядку $p = path + (z)$. Это формирует новое направленное сообщение *{RPRI,mid, z, (bid == Ø)?z : bid, cst +cost(z, parent(z)), path + (z)}* согласно следующим правилам:

– - заменяя поля *nid* его собственным *ID*; если поле *bid* является *Ø*;

– - заменяя поле *bid* его собственным *ID*, или сохраняя оригинал *bid* неизмененным;

– - обновляя поле *cst* добавлением стоимости *z* к узлу, от которого получено это сообщение;

– - обновляя поле *path,* прилагая его *ID* в конце старого пути.

Узел *z* тогда повторно передает новое сообщение соседнему узлу.

В простом протоколе лавинной маршрутизации (типа протокола испускания маяка) узел просто игнорирует повторяющееся сообщение обновления маршрута от других узлов. Однако, при лавинной маршрутизации методом ветвей, когда узел *z* видит повторное сообщение (то есть, идентифицированный таким же *mid*) от соседней ячейки, он проверит содержание сообщения и обозначит соседнюю ячейку соответственно. Если сообщение имеет такой же *bid*, как узел *z*, *z* отметит этот соседствующий узел как дочерний (*child* или *sibling*) в соответствии с путем, содержавшимся в сообщении, если сообщение имеет другое значение *bid*, что значит, что сообщение от другой ветки, *z* отметит этот соседствующий узел как *cousin*. Узел *z* содержит набор дополнительных путей Q_z. Получив сообщения от узла *cousin*, *z* далее исследует путь, содержавшийся в сообщении. Если новый путь $q = path + (z)$ является непересекающимся с первичным путем *p* и любой

другой дополнительный путь сократит стоимость Q_z, новый путь q будет добавлен в Q_z, в то время, как дорожки с большей стоимостью, чем q, которые разделяют общие узлы с q, будут удалены с Q_z. Так же, как и протокол испускания маяка, распространение сообщений *RPRI* заканчивается на концевых узлах, когда каждый узел ретранслирует сообщение однажды и только однажды.

Технология маршрутизации методом переходов (*branch aware routing technique*) фактически основана на следующих наблюдениях. Количество ветвей (рис.2), которые имеет дерево, зависит от количества непосредственно граничащих узлов, которые имеет базовая станция (например, 4 перехода на рис.2). Максимальное количество непересекающихся путей от любого узла к базовой станции, таким образом, ограничено количеством переходов. Обратим внимание на то, что в то время как каждый узел имеет первоначальный путь к базовой станции, следуя по соединениям дерева вверх, связь между двумя узлами, которые принадлежат двум различным веткам, будет обеспечивать каждому узлу дополнительный непересекающийся путь к базовой станции через другой. Например, (рис.2), в то время, как узел w имеет первичный путь ($w - r - l - g - d - Sink$) назад к базовой станции, он изучает другой дополнительный путь ($w - v - q - k - e - a$ - *Sink*) от узла v, который не в том же переходе, как w, рассматривая трансляцию v. Лавинная маршрутизация методом ветвей разработана для того, чтобы позволить узлам проходить по связям *cousin*, обнаруживая таким способом непересекающиеся пути в других переходах. Этот механизм использует преимущества природы трансляции беспроводной связи. Не вводя дополнительных сообщений маршрутизации, узлы, которые имеют соседствующие *cousin*, способны найти несколько непересекающихся путей.

Вторая фаза: Многопутевое распространение лавинной маршрутизации (Multipath Extension of Flooding)

Способность находить дополнительные пути с помощью лавинной маршрутизации методом переходов ограничена узлами, которые имеют соседствующие узлы *cousin*. Представим другой механизм/фазу для предлагаемого *N-to*-1 протокола многопутевого обнаружения – технологию многопутевого распространения лавинной маршрутизации, которая в состоянии найти больше непересекающихся путей на каждом узле датчика за счет обмена дополнительным сообщением.

Вторая фаза обмена сообщения использует такой же формат сообщения, но с полем *mtype*, установленным как "*RALT*", который называют "дополнительным", потому что этот тип сообщений находит дополнительные пути. Сообщения *RALT* используются для дальнейшего распространения дополнительных путей, найденные в одном узле соседствующим с ним узлам *parent* и *sibling/cousin*. Распространение сообщений *RALT* инициализировано дистрибутивно и независимо в каждом узле, где найден дополнительный непересекающийся путь (пути) в течение лавинной маршрутизации методом переходов. Для каждого дополнительного пути q, узел z формирует сообщение *RALT {RALT,mid, z, q.bid, q.cst, q}* и передает его соседствующим ячейкам.

После получения сообщения *RALT {RALT,mid, nid, bid, cst, path}*, узел z будет игнорировать его, если оно поступило от соседнего узла *parent*. В ином случае, он проверит и обнаружит, находится ли он непосредственно на пути, содержавшимся в сообщении. В противном случае узел z узнает о новом пути $q = path + (z)$. Снова, узел z добавляет новый путь q в свой дополнительный набор путей Q_z, если q является непересекающимся с любым другим путем в Q_z с меньшей стоимостью. Если q добавлен, узел z исключает его из набора путей Q_z пути с большей стоимостью, которые пересекаются с q. Всякий раз, когда новый путь q добавляется к Q_z, узел z формирует новое сообщение *RALT {RALT,mid, z, q.bid, q.cst, q}* и передает его соседнему узлу.

Распространение сообщений *RALT* прекращается, когда ни один новый путь

не прибавляется ни к одному набору путей. В это время каждый узел определился набором непересекающихся путей к базовой станции.

Структура двух механизмов фазы объясняется тем, что он должен максимально увеличить количество непересекающихся путей в каждом узле дальнейшим распространением дополнительных путей, найденных в первой фазе через множество переходов. Используя тот же пример (рис.2), обратим внимание на тот факт, что, если *w* далее распространяет непересекающиеся пути, полученные им от соседствующих узлов, узлы *parent* или узлы одного уровня *siblings/cousins* могут изучить новые непересекающиеся пути также. Например, узел r имеет первичный путь (*r − l − g − d − Sink)*. Когда он находит непересекающийся путь (*w − v − q − k − e − a − Sink*) от w и еще не определен путь через переход *a*, узел *z* анализирует новый непересекающийся путь (*r−w−v−q−k−e −a−Sink*). Обмен второй фазы означает, что она находит больше непересекающихся путей с помощью дополнительных сообщений маршрутизации.

Таблица 1. Имитируемые параметры сети

Диапазон передачи (*TR*)	15м	20м	25м	30м
Средняя степень узлов (*d*)	6,05	10,19	15,29	3,85
Средний диаметр сети (*D*)	10,56	6,09	4,72	3,85

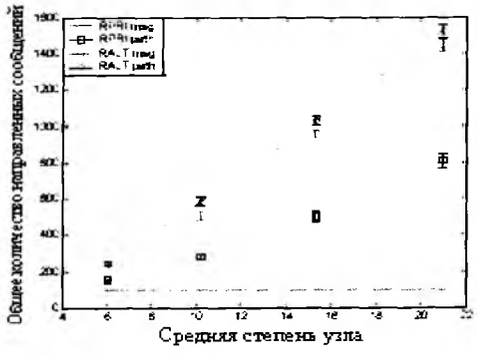

Рис.3. Возможность нахождения путей

Оценка эффективности

Для оценки эффективности работы предложенного *N-to-*1 протокола многопутевой маршрутизации используем симулирование. Симулируем сеть БСС, состоящую из 100 узлов, беспорядочно распределенных в области $100\times100\,м^2$. Базовая станция расположена в середине одного из ребер. Узлы имеют тот же диапазон передачи, что и в первом эксперименте. Для оценки воздействия плотности ребра на работу изменим диапазон передачи в разных экспериментах, чтобы адаптировать плотность ребер в сети. Используем четыре различных диапазона передачи: 15, 20, 25, и 30 метров. Выполним суммирование некоторых симулируемых топологических параметров сетей, используя различные диапазоны передачи среднюю степень узла *d* (то есть, количество соседствующих узлов) и средний диаметр сети *D* (то есть, максимальное число шагов от любого узла датчика до базовой станции самым коротким путем маршрутизации). Результаты симулирования (табл.1) составлены в среднем из более чем 60 случайных развертываний сетей. 95 процентов конфиденциальных интервалов показаны на рис.3.

Определено общее количество сообщений маршрутизации и общее количество непересекающихся путей (рис.3), найденных в симулируемой сети. Замечено, что механизм лавинной маршрутизации методом переходов находит непересекающиеся пути, не вводя никаких обменов дополнительными сообщениями. При высокой плотности ребра эта простая модификация может найти в среднем 8 непересекающихся путей на один узел. Предлагаемое многопутевое распространение механизма лавинной маршрутизации, также требуя большего обмена сообщениями, способно найти больше дорожек. Результаты показывают, что, в общем, алгоритм маршрутизации очень эффективен для обнаружения путей.

Особенности найденных путей проиллюстрированы на рис.3,4,5. На рис.4 показано распределение узлов относительно от их расстояния до базовой станции.

Среднее количество непересекающихся найденных путей на один узел относительно расстояния между узлами датчика и базовой станцией представлено на рис.5.

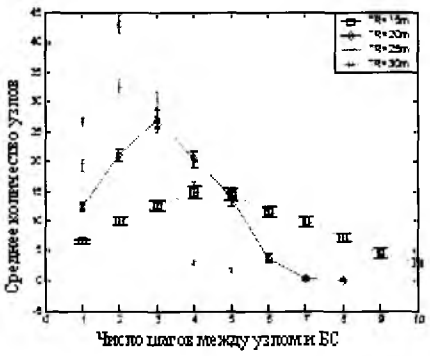

Рис.4. Распространение узлов относительно расстояния

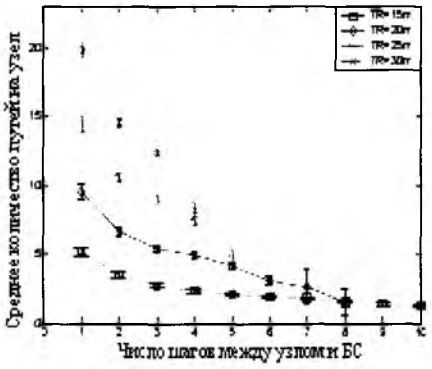

Рис.5. Распространение путей относительно расстояния

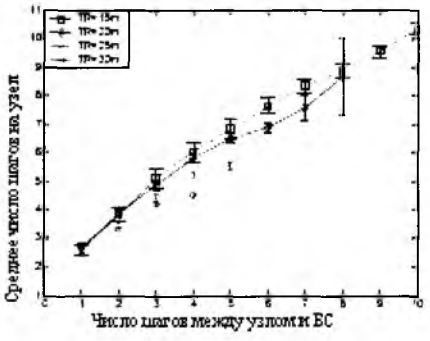

Рис.6. Качество дополнительных путей

Можно отметить тот факт, что чем ближе узел к базовой станции, тем больше путей от этого узла к базовой станции. Это разумно, потому что тяжелее найти непересекающиеся пути, когда узлы находятся далеко от базовой станции, поскольку каждый дополнительный путь должен найти большее количество неиспользованных узлов, чтобы достигнуть адресата. Это свойство характерно для рассматриваемых задач. Так как обычная задача сети состоит в том, чтобы собрать данные от всех узлов датчиков, пакеты перемещаются отовсюду к базовой станции. Узлы, которые находятся ближе к базовой станции, будут больше использоваться для уменьшения трафика. Таким образом, более желательно для таких узлов быть более надежными. Большее количество дополнительных путей дает узлу больше возможностей выбора относительно ошибки узла или связи. Среднее число шагов в одном пути показано на рис.6. Самое короткое расстояние к базовой станции отображено пунктирной линией. Наблюдается, что средняя длина дорожки обычно на один или два шага дольше, чем самый короткий путь, независимо от длины самого короткого пути.

Обычный сбор данных в сети БСС включает следующий характеристики связи:

а – передача от базовой станции к узлам датчика (например, запросы интересующих данных);

б – от узлов датчиков к базовой станции (например, посылая назад показания датчика);

в – связь от узла к узлу (например, если применяется скопление показаний датчиков).

Предложим протокол многопутевого обнаружения, который, как и все протоколы маршрутизации по требованию, запускается после обновления маршрута, инициализированного на базовой станции. Это обновление маршрута – широкая трансляция сети, таким образом, может использоваться для выполнения вышеупомянутой связи типа (а). Тогда в конце обнаружения каждый узел сможет найти ряд множества непересекающихся путей к базовой станции, с которыми предложенная гибридная схема сбора данных может быть применена для связи типа (б). При этом не рассматривается скопление данных явно. Однако центры скопления данных должны быть применены. Иерархическая структура маршрутизации может быть создана таким образом: от каждого узла датчика к центру скопления формируется нижний уровень и от каждого центра скопления к базовой станции формируется высший уровень. Предложенный алгоритм может быть применимым к каждому уровню отдельно.

Определение уровня безопасности и надежности H-SPREAD

Рассмотрим методику для определения уровня безопасности и надежности, который может быть достигнут с помо-

щью предложенной схемы распространения *H-SPREAD*. В данном случае под надежностью подразумевается вероятность того, что сообщение, сгенерированное в одном узле датчика, может фактически быть направлено к базовой станции, а под безопасностью – вероятность перехвата передаваемого сообщения. Цель исследования безопасности и надежности двойная:

а – обеспечить аналитические меры для определения уровня безопасности и надежности доставки данных с применением предлагаемой схемы

б – построение схемы распределения частей, которая не пострадает в целом в результате отказов и компрометированных узлов.

Анализ безопасности

Допустим, что M непересекающихся путей были отобраны, чтобы доставить сообщение. Вектор $\bar{q}=[q_1,q_2,...,q_M]$ определяет характеристики безопасности пути, где q_1 - вероятность того, что i-ый путь может быть компрометирован. Пусть вектор $\bar{n}=[n_1,n_2,...n_M]$ определяет распределение частей, при этом n_i пакетов назначены для доставки i-ому пути (n_i – положительное целое число и $\sum_{i=1}^{M} n_i = N$). Предполагается, что, если один путь компрометирован, то все части, проходящие по этой дорожке, компрометированы. Так как дорожки являются взаимно непересекающимися, далее предполагается, что компрометация каждого пути происходит независимо. Пусть $\psi(i)$ - функция индикатора на i-ом пути: значение $\psi(i)=1$ означает, что i-ый путь скомпрометирован с вероятностью q_i, и $\psi(i)=0$ указывает, что i-ый путь не скомпрометирован, с вероятностью $(1-q_i)$. Когда определено количество скомпрометированных частей, распределение $\bar{n}$ определяется $\sum_{i=1}^{M}\psi(i)n_i$. Заметим, что должно быть компрометировано минимальное число T частей, чтобы скомпрометировать сообщение. Вероятность того, что сообщение может быть скомпрометировано, определяется следующим образом:

$$P_C(\bar{n}) = \Pr\{J \geq T\} = \Pr\left\{\sum_{i=1}^{M}\psi(i)n_i \geq T\right\}, \quad (1)$$

где J – общее число компрометированных частей из N пакетов, доставленных через M путей.

В [3], показано, что в зависимости от числа путей M, отобранных для доставки сообщения, максимальная безопасность может быть достигнута при распределении N частей на M путях таким способом, что должны быть компрометированы все M путей, чтобы компрометировать сообщение. Максимальная безопасность, измеряемая как минимальная вероятность того, что сообщение может быть скомпрометировано, P_C определяется следующим образом:

$$P_C(\bar{n}) = \prod_{i=1}^{M} q_i .$$

В [3] показано, что схема распространения *SPREAD* может быть разработана таким способом, что определенная степень избыточности может быть добавлена без ущерба безопасности. Максимальная избыточность, которая может быть добавлена без ущерба безопасности, ограничена величиной:

$$r < 1/M , \quad (2)$$

где r - фактор избыточности и определятся как:

$$r = 1 - T/N ,$$

а M – число путей, отобранных для доставки частей сообщения. Тогда могут быть выбраны определенные величины T,N и разработаны оптимальные распределения частей так, чтобы достигнуть максимального уровня безопасности и при этом можно допустить определенную степень потерь пакета. Например, для M=3, T=8, N=10, оптимальное распределение частей будет [4 3 3], с которым должны быть скомпрометированы все эти три пути, чтобы получить достаточное количество частей, в то время как схема может допустить потерю двух пакетов. Заметим, что предложенные оптимальные распределения частей в отношении безопасности фактически не допускают поте-

ри целого пути. Повышенная надежность, полученная от этого типа уменьшения трафика, по существу исходит от избыточности, прибавленной к трафику данных, которого должно быть более чем достаточно, чтобы допускать отказ одного или более путей. Это делает безопасность и надежность двумя противоречивыми целями при использовании параллельного подхода многопутевой маршрутизации, так как надежность полагается на чрезмерную избыточность, в то время как безопасность требует отсутствия или небольшой избыточности.

Вычислить вероятность P_C не так просто, так как для этого нужно перечислить все возможные (2^M) комбинации $\psi(i)$ и просуммировать вероятности. Однако, были разработаны эффективные алгоритмы для решения проблемы в определении уровня надежности *k-out-of-n* моделей системы. Данная проблема подобна оценке надежности систем *weighted-k-out-of-n*, которая была предложена в [13] и представлен эффективный алгоритм для вычисления надежности системы. Вычисление вероятности P_C может быть произведено следующим образом. Без потери целостности принимается, что $q_1 \le q_2 \le ..., \le q_m$. Пусть значение $R(j,i)$ определяет вероятность того, что минимальное количество j пакетов компрометировано от первых i путей. Тогда значение вероятности P_C может быть вычислено как:

$$P_C(\bar{n}) = R(T,M),$$

где *R(T,M)* может быть определено с помощью выражения

$$R(j,i) = q_i R(j-n_i, i-1) + (1-q_i) R(j, i-1), \quad (3)$$

которое требует следующие граничные условия:

$$R(j,i) = 1, \text{ для } j \le 0, i \ge 0,$$

$$R(j,0) = 0, \text{ для } j > 0.$$

Сложностью при вычислении значения *R(T,M)* является выражение *O(T(M−T+1))*, когда $n_i = 1$ для всех i. Промежуточные значения *R(j,i)* для $1 \le j \le T$ и $1 \le i \le M$ являются полезными для исследования вероятности *P* в общем.

Анализ надежности

Оценим надежность предлагаемой схемы сбора данных. Определим насколько надежно сгенерированное в одном узле датчика сообщение может быть направлено к БС. Фактически, в сети БСС, и узлы датчика и беспроводные связи подвержены ошибкам. Отказ узла может быть вызван физической неисправностью узла или тяжелой перегрузкой в узле, что вызывает потерю пакета в связи с буферным переполнением. Отказ связи может быть вызван проблемой конкуренции доступа, вмешательством множества пользователей или любым вмешательством, которое вызывает радиосигнал, неправильно декодируемый предназначенным получателем. Если предположить, что каждый узел имеет равную вероятность p_{n0} надежной передачи пакета с необходимой степенью надежности, и каждая связь имеет равную вероятность p_{l0} надежной доставки пакета, то вероятность *P* того, что путь, состоящий из *H* шагов, может успешно доставить пакет, будет равна $p = p_{n0}^{\ H} p_{l0}^{\ H}$ (при предположении, что адресат надежен).

В [2] предложена аналитическая модель для оценки надежности многопутевой маршрутизации в мобильных сетях *ad hoc*. Рассматривается потеря пакета ввиду топологических изменений, поэтому выполняется моделирование каждого пути как чистого канала со стиранием (*pure erasure channel*), а именно, в том случае, если путь неудачен, все переданные этим путем части, будут потеряны, в ином случае – все доли на части пути будут получены. Эта модель подобна модели, которая описана выше при анализе безопасности, и может рассматриваться как модель проблемы отказа узла в данном случае. В [2] предложено использование Гауссова приближения (*Gaussian approximation*) для вычисления надежности. Результаты аналитических исследований показали, что многопутевая маршрутизация более стойка к проблеме отказа узла и доставка пакета может быть улучшена. Однако улучшенная надежность очень полагается на добавление чрезмерной избыточности (фактически избыточных путей), которая

будет определенным образом препятствовать достижению цели обеспечения необходимого уровня безопасности.

В дальнейшем оценим надежность с позиции наличия отказа связи. Предполагается сеть с идеально надежными узлами, но ненадежными связями. Потеря пакета при передаче вызвана отказом связи и независима от других передач. Это предположение связано с тем, что проблема отказа связи воздействует на многопутевую маршрутизацию. Кроме того, в комбинаторике надежности сети неориентированная проблема отказов узлов может быть преобразована в направленную проблему без отказов узлов [14]. В некоторых случаях это предположение может быть устранено. Например, в вышеупомянутом примере, надежность пути с отказами узлов – только вероятность того, что все узлы являются рабочими.

Подобно формулировке проблемы для анализа безопасности, предполагается, что было отобрано M непересекающихся путей, каждый из которых надежно доставляет пакеты с вероятностью p_i $(i=1,2,...,M)$. Используем вектор $\underline{n}=[n_1,n_2,...n_M]$, обеспечивающий распределение частей n_i пакетов на i-ом пути. Пусть $x_i(j)$ определяет функцию индикатора на i-ом пути: $x_i(j)=0$ указывает, что j-ый пакет доставлен успешно, а значение $x_i(j)=1$ указывает, что j-ый пакет потерян. Таким образом, $p_i=\Pr\{x_i(j)=0\}$ и $\sum_j^{n_i} x_i(j)$ - число пакетов, потерянных на i-ом пути. Основываясь на этом предположении и том факте, что пока общее количество потерянных пакетов из числа N пакетов меньше или равно $N-T$, первичная информация может быть правильно возобновлена БС, получаем вероятность успешной доставки P_R, определяемую следующим выражением:

$$P_R(\underline{n})=\Pr\{L\le N-T\}=\Pr\left\{\sum_{i=1}^{M}\sum_{j=1}^{n_i} x_i(j)\le N-T\right\}, \quad (4)$$

где L – общее количество потерянных пакетов из числа N пакетов, доставленных M путями.

Фактически, решение этой проблемы такое, что, имея вероятность надежной доставки пакета $\bar{p}$, можно максимизировать эту вероятность, отправив как можно больше частей самыми надежными путями и как можно меньше – наименее надежными путями. Этот результат фактически подразумевает то, что с учетом неустойчивой модели отказа пакетов лучшая надежность достигается распределением всех пакетов по наиболее надежным путям.

Многопутевая маршрутизация может объединить ограниченную пропускную способность, чтобы уменьшить трафик пакетной передачи с целью уменьшения перегрузки сети, улучшения отказоустойчивость, и, что наиболее важно, повышения надежности. Несколько протоколов многопутевой маршрутизации предложены с целью поиска множества непересекающиеся или частично пересекающихся путей между парой отдельного источника и адресата [5] - [11], [15, 16].

Выводы

Сбор данных - важная задача в сетях БСС. Надежные и безопасные методики предпочтительны для эффективного выполнения задач. Проведен анализ функционирования БСС, где типичной задачей является распространения запросов данных от базовой станции ко всем узлам датчиков и сбор показаний датчиков от каждого узла датчика к базовой станции. Предлагается эффективный *N-to*-1 протокол многопутевого обнаружения, который периодически или по требованию инициализирует обновление маршрута на базовой станции и в конце каждого процесса обнаружения, находит каждый узел датчика, набор непересекающихся путей к базовой станции. Основываясь на наличии множества путей на каждом узле, предлагается гибридная схема многопутевой маршрутизации для выполнения задачи безопасного и надежного сбора данных. Предложенная гибридная схема многопутевого сбор данных более эластична к отказам узла/связи и организованным атакам компрометированных узлов. Она очень эффективна для повыше-

ния одновременно и надежности, и безопасности.

Предложенное решение проблемы повышения надежности и безопасности передачи информации отличается от большинства предыдущих работ следующим:

а) протокол многопутевого обнаружения *N-to-*1 является инициализированным получателем (в отличие от общего инициализированного источником маршрута обнаружения) и протокол эффективен в том, что находит многопутевые маршруты от каждого узла датчика до базовой станции, которая хорошо соответствует специальной структуре связи в сети БСС;

б) принимается подход многопутевой гибридной маршрутизации для доставки данных. Используется параллельная многопутевая схема для рассредоточения трафика на многократные непересекающиеся пути для доставки данных

в) общая схема улучшает и безопасность, и надежность.

Список литературы

1. *A. F. Akyildiz, W. Su, Y. Sankarasubramainiam, E. Cayirci*, "A survey on sensor networks", IEEE Communications Magazine, August 2002

2. *A. Tsirigos, Z.J. Haas,* "Multipath routing in the presence of frequent topological changes", IEEE Communication Magazine, Nov 2001

3. *W. Lou, W. Liu, Y. Fang,* "SPREAD: Enhancing data confidentiality in mobile ad hoc networks, IEEE INFOCOM 2004, HongKong, China, March 2004

4. *S.K. Das, A. Mukherjee,* et al, "An adaptive framework for QoS routing through multiple paths in ad hoc wireless newtorks", J. Parallel Distributed Computing, 63(2003)141-153

5. *S. De, C. Qiao, H. Wu,* "Meshed multipath routing: an efficient strategy in sensor networks", IEEE Wireless Communications and Networking Conference (WCNC'03), New Orleans, LA, Mar 2003

6. *M. K. Marina, S. R. Das,* "On-demand multipath distance vector routing in ad hoc networks", 9th International Conference on Network Protocols, Riverside, CA, November, 2001

7. *M.R. Pearlman, Z.J. Haas, P. Sholander, S. S. Tabrizi,* "On the impact of alternate path routing for load balancing in mobile ad hoc networks", The ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC'00), Boston, MA, August 2000.

8. *S.-J. Lee, M. Gerla,* "AODV-BR: backup routing in ad hoc networks", IEEE Wireless Communications and Networking Conference (WCNC'00), Sep 2000

9. *S.-J. Lee, M. Gerla,* "Split multipath routing with maximally disjoint paths in ad hoc networks", International Conference on Communications (ICC'01), Helsinki, Finland, June 2001.

10. *K. Zeng, K. Ren, W. Lou,* "Geographic on-demand disjoint multipath routing in wireless ad hoc networks", IEEE MILCOM, Oct 2005

11. *Z. Ye, S. V. Krishnamurthy, S. K. Tripathi,* "A framework for reliable routing in mobile ad hoc networks", IEEE INFOCOM 2003, Sanfrancisco CA, Mar 2003

12. *T. Cormen, C. Leiserson, R. Rivest,* Introduction to algorithms, MIT Press, 1990

13. *J-S. Wu, R-J. Chen*, "An algorithm for computing the reliability of weighted-k-out-of-n systems", IEEE Transactions on Reliability, 43(2):327-328, June 1994

14. *C.J. Colbourn,* The Combinatorics of Network Reliability, Oxford University Press, 1987

15. *D. Ganesan, R. Govindan, S. Shenker, D. Estrin,* "Highly-resilient, energy-efficient multipath routing in wireless sensor networks", Mobile Computing and Communication Review, 5(4):10-24, Oct 2001

16. *Жуков І.А., Алішов Н.І., Салім Аль Шибані*, Алгоритм и средства оптимальной коммутации пакетов в компьютерных сетях / Проблеми інформатизації та управління. – К.: НАУ, 2006. – Вип. 3 (18). – С. 12-19.