Раздел II. Безопасность информационных систем и сетей

УДК 004.056: 004.73

Е.С. Абрамов, Е.С. Басан

РАЗРАБОТКА МОДЕЛИ ЗАЩИЩЕННОЙ КЛАСТЕРНОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ*

Защита беспроводных сенсорных сетей (БСС) является актуальной проблемой, так как узлы сети имеют небольшую вычислительную мощность, ограниченный заряд батареи и располагаются в незащищенных местах, а информация передается по беспроводным каналам, то любое нарушение работы сети может привести к нежелательным последствиям. На сегодняшний день разработано большое количество методов защиты БСС, а также систем обнаружения вторжений, но данные методы в основном предназначены для статических БСС. Также существует необходимость в разработке комплексного подхода к защите БСС, который смог бы противодействовать большинству существующих атак.

В данной статье рассматривается кластерная беспроводная сенсорная сеть, к которой должны быть применены методы защиты. Главная цель данной статьи – разработка защищенной модели кластерной беспроводной сенсорной сети (КБСС) со встроенными механизмами обнаружения и предотвращения атак. В статье представлены алгоритмы вычисления уровня доверия и определения главы кластера представлены, а также описана защищенная модель КБСС.

Беспроводные сенсорные сети; кластеризация; атаки; доверие, алгоритмы; обнаружение аномалий; подлинность; метод обнаружения вторжений; оценка уровня доверия.

E.S. Abramov, E.S. Basan

DEVELOPMENT OF A SECURE CLUSTER-BASED WIRELESS SENSOR NETWORK MODEL

Protection of wireless sensor networks (WSN) is an important issue, since the nodes have low processing power, limited battery life and are located in disadvantaged areas , and the information is transmitted over wireless channels , any violation of the network can lead to undesirable consequences. To date, a large number of methods to protect WSN were developed, as well as intrusion detection systems, but these techniques are mainly designed for static WSN. There is also a need to develop an integrated approach to the protection of WSN, which could resist most of the existing attacks.

In this paper we consider a clustering wireless sensor network which needs to be protected. The main aim of this article is development of a secure clustering wireless sensor network model with built-in detection and counteraction mechanisms against malicious impacts (attacks). Trust level calculation algorithm and cluster head (CH) election algorithm are introduced and secure clustering WSN model is described.

Wireless sensor networks; clustering; attacks; trust; algorithms; anomaly detection; authenticity; intrusion detection method; trust evaluation.

* Работа выполнена при поддержке грантов РФФИ № 12-07-92693-ИНД_а, № 12-07-00013-а.

Введение. Беспроводные сенсорные сети (БСС) – это принципиально новый тип беспроводных сетей, которые строятся на основе неограниченного количества небольших датчиков с ограниченным зарядом батареи, предназначенных для сбора информации и контроля объекта. Кластеризация является базовым методом для организации большого количества объектов в группы ограниченного размера для многих научных и инженерных областей. Каждый кластер/группа должна иметь лидера, который обычно представлен, как Глава кластера (ГК). В общем случае ГК это узел, который имеет большие ресурсы, чем остальные узлы. Он способен определять маршрут внутри кластера и таким образом сокращает размер таблицы маршрутизации, хранящейся на отдельном узле [1]. Можно выделить следующие уязвимости КБСС:

- Уязвимость каналов к прослушиванию и подмене сообщений, в связи с общей доступностью среды передачи, как и в любых беспроводных сетях.
- Незащищённость узлов от злоумышленника, который легко может получить один узел в распоряжение, так как обычно они не находятся в безопасных местах, таких как сейфы.
- Отсутствие инфраструктуры делает классические системы безопасности, такие как центры сертификации и центральные серверы, неприменимыми.
- Динамически изменяющаяся топология требует использования сложных алгоритмов маршрутизации, учитывающих вероятность появления некорректной информации от скомпрометированных узлов или в результате изменения топологии [2].
- «Бутылочное горлышко», когда две большие группы связаны одним устройством.
- Ограниченное (4–14) число каналов в диапазоне WiFi – приводит к засорению эфира.
- Проблема «темных углов» сети: наличие глухих мест, не связанных с другими ни через узлы одноранговой сети, ни посредством шлюзов.

В настоящее время существует больше количество возможных атак на БСС. Полный обзор атак представлен в [3]. Кратко, можно отметить, что большинство атак направлены на выведение из строя беспородных узлов сети, на дезориентацию протоколов маршрутизации, а также сбой работы сети в целом.

Таким образом, наша КБСС устроена так, что все узлы сети являются мобильными и поэтому выбор ГК необходимо осуществлять динамически. В основном выбор ГК производится согласно параметрам местоположения и остаточного запаса энергии, в связи с чем, высока вероятность того, что злоумышленник, внедрившись в сеть, сможет стать ГК, что сможет нарушить работу всей сети. Поэтому необходимо внедрить дополнительную защиту при выборе ГК.

Целью является разработка: модели кластерной беспроводной сенсорной сети, реализующей алгоритмы определения уровня доверия узла и выбора ГК; модифицированного протокола управления кластеризацией сети; методов обнаружения атак и вторжений. Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ существующих методов защиты КБСС, атак и уязвимостей КБСС.
2. Разработать архитектуру защищенной КБСС с встроенной системой обнаружения атак и вторжений, а также архитектуру каждого типа узла сети.
3. Получить набор метрик, по которым будет рассчитываться уровень доверия к узлу, а также подобрать формулы для расчетов.
4. Разработать алгоритм определения уровня доверия к узлу, для определения того, что узел является подлинным.
5. Разработать алгоритм выбора ГК.

1. Предыдущие исследования. Что касается методов обнаружения атак в БСС, как второй линии защиты сети, то существует большое количество различных методов, полный обзор методов обнаружения атак представлен в статье [2]. В каждом методе есть свои достоинства и недостатки, но особое внимание заслуживает: «Комплексная система обнаружения вторжений (IIDS) в БСС на основе кластера» [4]. Данная система учитывает особенности кластерных сетей и принцип самоорганизации. Недостатком является устаревшая база атак для обучения нейронной сети, что снижает качество работы системы.

Помимо системы обнаружения атак и вторжений для дополнительной защиты может использоваться показатель – уровень доверия к узлу. Проблема доверия рассматривается многими авторами, наиболее полный перечень метрик доверия представлен в источнике [5], здесь же имеются формулы для расчета уровня доверия. Но предложенные метрики либо не учитывают некоторых возможных угроз и атак, либо являются излишними, поэтому необходимо пересмотреть и дополнить данный список.

В источнике [6] рассматривается кластерная БСС. Данная БСС имеет некоторые особенности – ГК выбирается динамически согласно параметрам остаточный заряд энергии и местоположение. В данной статье четко описана архитектура кластерной БСС, предложен энергетически эффективный алгоритм выбора главы кластера, но не рассматривается вопрос безопасности. Выбор главы кластера также рассматривается многими авторами. К примеру, в статье [7] рассматривается проблема выбора ГК с учетом требований безопасности. В данном случае при расчете уровня доверия используется недостаточное количество метрик, а также используется подписание сертификата, что значительно усложняет процедуру выбора и вводит дополнительные трудности. Необходимо отметить, что выбор ГК хотя и происходит с согласия всех членов кластера, но не контролируется вышестоящей базовой станцией, что снижает уровень безопасности.

2. Защищенная модель кластерной БСС. В данной работе используется кластерная БСС, которая способствует разделению сети на небольшие группы, для упрощения процесса обеспечения безопасности. Пример кластерной БСС изображен на рис. 1.

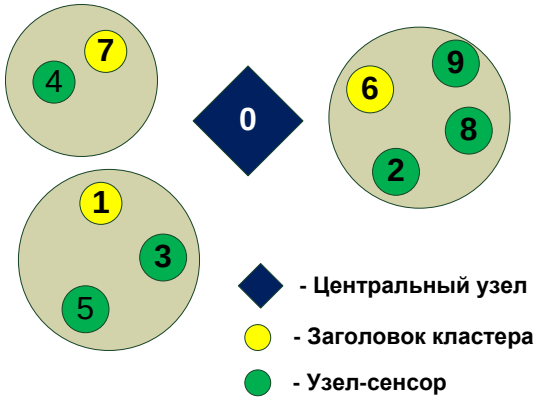

Рис. 1. Кластерная БСС

Данная БСС имеет несколько особенностей: ГК отвечает за авторизацию других членов кластера, а базовая станция (БС) отвечает за авторизацию ГК. При этом любой узел-сенсор может стать главой кластера, если его показатели будут выше, чем у его соседей. В качестве метода обнаружения атак, как было сказано ранее, используется «Комплексная система обнаружения вторжений для КБСС», предло-

женная в [4]. Данная система специально разработана для использования в кластерной БСС и основным принципом ее построения является разделение полномочий каждого типа узлов. Данная схема состоит из трех уровней компонентов СОВ: Модуль обнаружения злоупотреблений установлен на узлах сенсорах; гибридная система обнаружения вторжений (HIDS) установлена на ГК; гибридная интеллектуальная система обнаружения вторжений (IHIDS) установлена на центральном узле. Система (IIDS) состоит из модулей определения злоупотреблений и аномального поведения. Система (IHIDS) состоит из модуля обнаружения аномалий, обнаружения злоупотреблений, изучающего модуля и модуля принятия решений. Рассмотрим основные возможности узлов сети.

Модель сенсора: Поведение сенсора в сети можно охарактеризовать следующим образом: сенсор воспринимает информацию об окружающей среде и разделяет ее на нормальную и аномальную. Сенсор может отправлять несколько типов сообщений: 1. Сообщение-маяк, оповещающее о присутствии сенсора в данном кластере, данное сообщение может быть двух типов, которое отправляется: при входе в кластер и при выходе из него. 2. Пакет с данными – отправляется при необходимости, несет в себе информацию об окружающей середе, если все нормально. 3. Сообщение – оповещение данное сообщение сигнализирует об отклонениях в окружающей среде, которые необходимо исправить или регулировать. 4. Сообщение о место положения узла – оповещает заголовок кластера или соседние узлы о положении узла в пространстве (может не использоваться). Сенсор получает управляющие сообщения от ГК; обнаруживает наличие атаки и оповещает заголовок кластера; участвует в выборе ГК путем расчета уровня доверия.

Модель базовой станции (БС): узлы-сенсоры могут отправлять данные базовой станции через ГК; БС имеет полную информацию о каждом ГК (номер и MAC-адрес); удаление или добавление любого узла в кластере отслеживается БС (через ГК); БС отслеживает активность ГК и принимает решения о наличие атаки (связанной с подменой ГК); а также принимает участие в расчете уровня доверия узлов; анализирует данные полученные от ГК и обменивается данными с внешней сетью.

Модель злоумышленника: Злоумышленник может: получить информацию об узлах сети, топологии сети, протоколах сети; проникнуть в сеть под видом законного пользователя; перенаправить на себя маршруты, чтобы сенсоры передавали данные через него; блокировать перенаправляемые на него сообщения, задерживать их, скремблировать, изменять, передавать по туннелю сообщения другому злоумышленному узлу; посылать в сеть поддельные сообщения (посылая сообщения непрерывно, злоумышленник влияет на скорость истощения ресурсов датчика, посылая сообщения об изменении маршрута, злоумышленник изменяет таблицу маршрутизации); посылать сообщения о наличие маршрута высокого качества, перенаправляя все сообщения на себя. Злоумышленник может: отправлять поддельный пакет-маяк или украденный пакет-маяк, чтобы выдать себя за законный узел; модифицировать сообщения, использовать уязвимости протоколов маршрутизации. (перехватывать сообщения типа запрос о маршруте RREQ и отправлять на них ответ не проверяя валидность маршрута.).

Модель главы кластера: Глава кластера может: рассылать сообщения о синхронизации по времени; рассылать сообщения-маяки; получать сообщения – маяки от узлов при их выходе и входе в кластер; получать и анализировать сообщения – оповещения от узлов сети; проходить аутентификацию у БС; передавать данные БС; отвечает за маршрутизацию сообщений; проводить аутентификацию узлов-сенсоров; участвовать в процессе обнаружения атаки, путем сбора данных от узлов, анализа трафика сети и передачи оповещений центральному узлу. Функциональная модель ГК представлена на рис. 2.

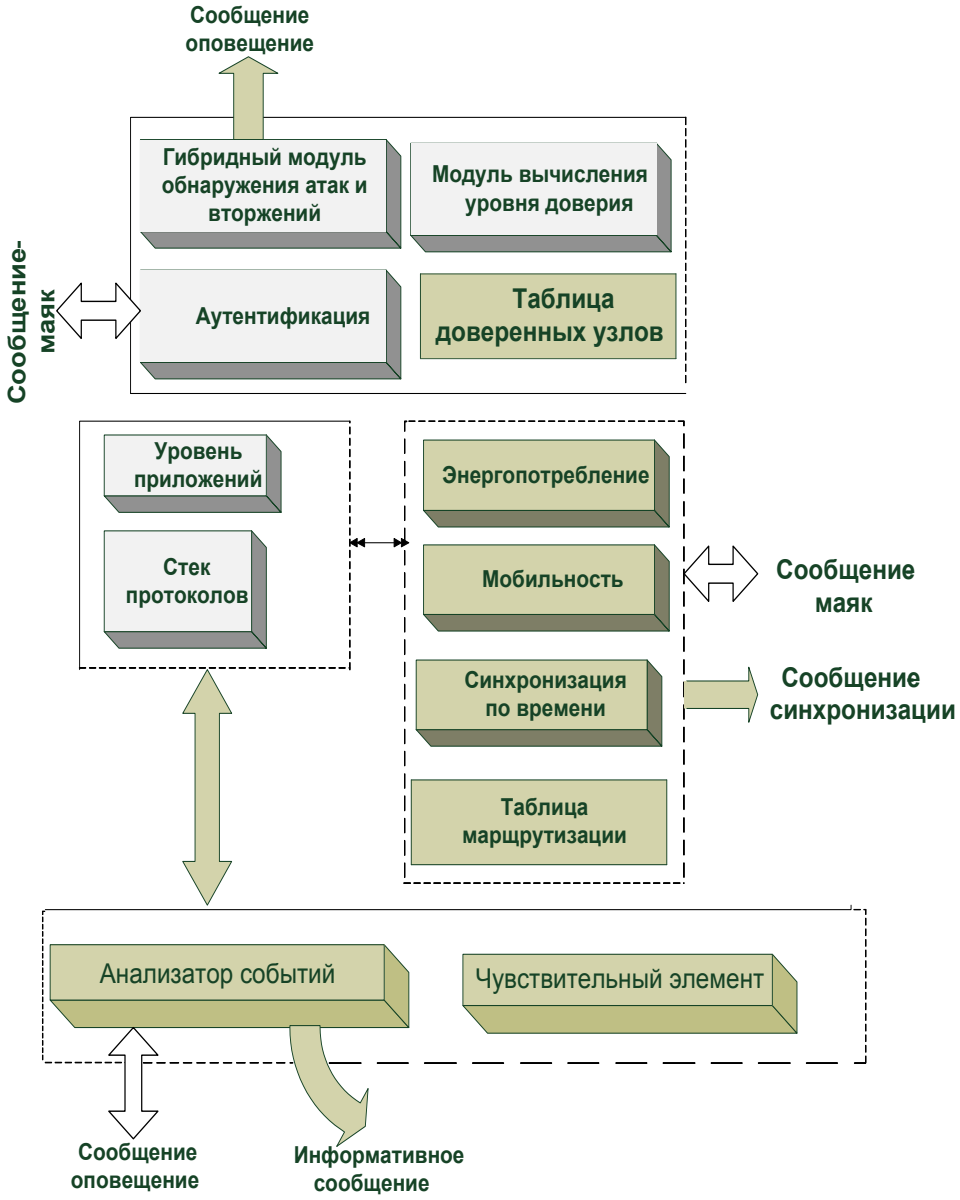

Рис. 2. Функциональная схема главы кластера

3. Алгоритмы определения уровня доверия к узлу и главы кластера. Если ГК будет выбираться согласно двум параметрам – уровень остаточной энергии и местоположение, то злоумышленник с легкостью сможет подделать эти параметры и стать главой кластера. Поэтому необходимо вводить дополнительный параметр – уровень доверия к узлу. Для того чтобы рассчитать уровень доверия к узлу необходимо определить метрики, которые будут участвовать при расчетах. Набор таких метрик представлен в табл. 1.

Таблица 1

Метрики для расчета уровня доверия

№	Метрика доверия	Наблюдаемое поведение	Атака
1	Пакеты данных	Передача сообщений\пакетов с данными	Черная дыра, выборочная переадресация, отказ в обслуживании, эгоистичное поведение
2	Управляющие пакеты: сообщения о месте положения, сообщения-маяки.	Передача управляющих пакетов	Отбрасывание управляющих сообщений и сообщений маршрутизации
3	Точность пакетов данных	Целостность данных	Изменение сообщений с данными
4	Точность управляющих пакетов	Целостность управляющих пакетов	Сибил атака, и любая атака на изменение сообщений протокола маршрутизации
5	Доступность на основе пакетов-маяков или “hello” сообщений	Своевременная передача периодической маршрутной информации о доступности линии связи или узла	Пассивное прослушивание, эгоистичное поведение
6	Изменение адреса пакета	Адрес пересылаемого пакета	Сибил атака, туннельная атака
7	Работа протокола маршрутизации: АСК пакеты, Сообщения RREQ, RREP, RERR	Особые действия протокола маршрутизации (реакция на особые сообщения протокола маршрутизации)	Аномальное поведение, связанное с особыми действиями протокола маршрутизации
8	Заряд батареи\время жизни	Оставшиеся запасы энергии	Доступность узла
9	Передача измерений	Отчет о событиях (специализированных для приложений)	Эгоистичное поведение узла на уровне приложений
10	Репутация	Значение доверия полученной третьей стороной	Атака типа шантаж, компрометация

В источнике [5]. Даны формулы для расчета уровня доверия.

$$T_i^{A,B} = \frac{a_i s_i^{A,B} - b_i F_i^{A,B}}{c_i s_i^{A,B} - d F_i^{A,B}}, \quad (1)$$

где T_i^{AB} – это значение доверия узла А относительно узла В. S_i^{AB} – это количество успешных событий типа i, которые измерил узел А для узла В, .F_i^{AB} – это количество неудачных событий типа i, которые измерил узел А для узла В и a_i,b_i,c_i,d_i вес/значимость успешных событий по сравнению с весом/значимостью неуспешных событий. Данное значения уровня доверия рассчитывается для каждого события сети, которое рассмотрено в таблице.

Эти значения доверия, связанные с поведением, умножаются на весовой коэффициент (Wi), отражающий их значение в иерархии безопасности и затем суммируются, для вычисления общего значения надежности узла, как показано в следующем уравнении.

$$DT^{A,B} = \sum_{i=1}^{k} W_i * T_i^{A,B}. \quad (2)$$

В целом, прямые наблюдения считаются более важными, чем косвенная информация о доверии, в то время как косвенная информация становится важной для новых узлов, которые имеют ограниченный опыт по взаимодействию со своими соседями.

Также необходимо рассчитывать разницу между настоящим и прошлым значениями для того, чтобы знать, как изменяется уровень доверия узла.

$$T = \gamma Tnew + (1 - \gamma)Told. \quad (3)$$

В разработанном методе определения уровня доверия учитывается не только рассчитанное по формуле (4) доверие, но и влияние уровня энергии на уровень доверия. Существует несколько способов расчета уровня энергии, затрачиваемого за один цикл работы. В данном случае будет использоваться формула, предложенная в [8]:

$$E_S = P_{ПР} \cdot T \cdot n, \quad (4)$$

где T – время, затрачиваемое на передачу одного информационного пакета, n – число СУ в данном кластере, $P_{ПР=}S$ = чувствительность приемника

$$P_{ПР} = P_{ПЕР} + G_{ПЕР} + G_{ПР} + W_{СВ} \ [дБ], \quad (5)$$

здесь $G_{ПЕР} = G_{ПР} = 0$, $W_{CB} = 10\lg(\frac{\lambda}{4\pi\rho})^2$ – ослабление сигнала в свободном пространстве на расстоянии ρ, λ = c / f – длина волны рабочей частоты f , ρ – расстояние между головным и оконечными узлами. Так для стандарта IEEE 802.15.4 рабочая частота f = 868 МГц, скорость передачи информации C = 20 кбит/с, что позволяет вычислить W_{CB} и T = I/C , где I – объем информационного пакета. $P_{ПЕР}$ – передатчик.

Остаточное количество энергии для каждого из узлов с учетом (4) определяется из разности:

$$Q_i^{\,k}(E) = Q_{k-1} - k*E_i, \quad (6)$$

где k – номер очередного цикла работы СС.

Далее, необходимо рассчитать среднее значение уровня остаточной энергии всех узлов и пороговые значения.

$$Qi\ k_{cp} = \frac{\sum Qi\ k}{N}, \quad (7)$$

где N – это общее количество узлов.

Алгоритм определения уровня доверия узла

1. Узел собирает данные от соседних узлов согласно тем метрикам, которые заданы ранее (в таблице).

2. Узел рассчитывает уровень доверия согласно уравнению (1), (2).

3. Узел рассчитывает остаточное количество энергии (4)–(6).

4. Узел отправляет полученные данные БС и соседним узлам (находящимся на расстоянии одного прыжка).

5. БС рассчитывает среднее количество энергии по формуле (7).

6. БС также отслеживает трафик и рассчитывает собственные значения (п. 1–3 алгоритма).

7. БС сравнивает свои значения, с полученными от узлов значениями:

а) если все верно, то продолжение алгоритма;

б) если не верно, то узел приславший неверные значения становится не доверенным и продолжение алгоритма.

8. БС отправляет рассчитанные значения узлам.

9. Далее узел вычисляет значение остаточной энергии и уровня доверия по формуле (3). При этом необходимо обратить особое внимание на значение остаточной энергии:

а) значение остаточной энергии узла не должно увеличиться;

б) если значение узла резко уменьшилось, то необходимо установить причину, проанализировав нагрузку: необходимо установить, каких пакетов было больше отправлено и получено. Если было получено большое количество пакетов маяков, пакетов синхронизации и других управляющих пакетов, то это говорит о том, что он подвергся Dos атаке. Если узел сам отправлял большое количество управляющих пакетов, то он проводил атаку. Если пакеты маршрутизации узла были отброшены или заблокированы, то он также подвергся атаке. При этом если узел подвергся атаке, то уровень доверия снижается, если он был атакующим, то узел изолируется.

в) если значение энергии узла не изменилось, то также необходимо провести проверку активности узла. При этом если узел был неактивным, то уровень доверия узла оставить неизменным. Если узел выполнял активность, то провести анализ пакетов аналогично, как в п. 9.б. и применить те же действия.

10. Если узел обнаружил, что его сосед(и) являются атакующими или подверглись атаке, то он оповещает базовую станцию.

11. Базовая станция, получив оповещение, сверяет полученные данные со своими измерениями:

а) если они совпадают, то рассылается сообщение-оповещение об атаке;

б) если данные не совпали, то центральный узел полагает, что имеет место атака компрометации узла.

Дополнительно необходимо отметить, что узел, являющийся ГК на текущий момент времени не участвует в выборах ГК. Текущий ГК оценивается и контролируется исключительно БС. ГК должен контролироваться отдельно, так как:

- уровень энергии ГК будет существенно быстрее снижаться, чем уровень энергии узлов-сенсоров;
- ГК отправляет большее количество управляющих сообщений, чем узлы-сенсоры;
- ГК отвечает за межкластерную маршрутизацию.

Алгоритм выбора главы кластера

1. БС объявляет начало процедуры выбора ГК на новом цикле работы алгоритма, рассылая сообщения-оповещения заголовкам кластера.

2. ГК рассчитывают остаточную энергию по формуле(6).

3. ГК рассчитывают значения уровня доверия друг друга согласно формулам (1), (2).

4. Полученные значения главы кластеров отправляют БС для проверки.

5. БС рассчитывает среднее значение и среднее отклонение, согласно полученным значениям.

6. БС сравнивает среднее значение с полученными значениями: если значения ГК не выходят за допустимое, то ГК остается заголовком; если выходят за допустимое, то ГК перестает быть главой и продолжение алгоритма.

7. ГК объявляет процедуру выбора главы кластера узлам-сенсорам.

8. Узлы-сенсоры выполняют алгоритм определения подлинности узла, после чего один из узлов-сенсоров выбирается ГК.

9. Старый ГК рассылает сообщение о снятии полномочий.

10. Новый ГК рассылает сообщения-оповещения узлам-сенсорам.

Выводы. В данной статье был предложен алгоритм определения подлинности узла и модель защищенной кластерной БСС. Данный алгоритм необходим для выбора ГК, что позволит избежать ситуации, когда злоумышленник становится

главой кластера. Модель БСС подразумевает три типа узлов, для каждого из которых были предложены механизмы защиты. В дальнейшем исследовании предполагается доработка системы обнаружения вторжений, так как в ней имеются существенные недостатки. Также разработан протокол управления кластерной БСС, который будет учитывать требования безопасности. Необходимо доработать алгоритм определения подлинности узла для контроля заголовков кластера центральным узлом. Приоритетной задачей является моделирование описанной модели сети и ее тестирование [9].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Akkaya K. and Younis M.* A survey on routing protocols for wireless sensor networks // Elsevier Journal of Ad Hoc Networks. – 2005. – № 3 (3). – P. 325.349.
2. *Абрамов Е.С., Басан Е.С.* Анализ сценариев атак на беспроводные сенсорные сети // Материалы XIII Международной научно-практической конференции «ИБ-2013». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2013. – С. 60-72.
3. *Абрамов Е.С., Басан Е.С.* Разработка архитектуры системы обнаружения вторжений для беспроводных сенсорных сетей // Материалы XIII Международной научно-практической конференции «ИБ-2013». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2013. – С. 72-79.
4. *Wang S.S., Yan K.Q., Wang S.C., Liu C.W.* An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks // Expert Syst. – Appli., 2011. – № 38. – P.15234-15243.
5. *Теплицкая С.Н., Хусейн Я.Т.* Энергетически эффективный алгоритм самоорганизации в беспроводной сенсорной сети // Восточно-Европейский журнал передовых технологий. – 2012. – № 2/9 (56). – С. 25-29.
6. *Zahariadis1 T., Leligou1 H.C., Trakadas P., Voliotis S.* Trust management in wireless sensor networks // Eur. Trans. Telecomms. – 2010. – P. 386-395
7. *Mills K.L.* A brief survey of self-organization in wireless sensor networks // Wireless Communications and Mobile Computing. – 2007. – Vol. 7, № 7. – P. 823-834.
8. *Chatterjee P.* Trust based clustering and secure routing scheme for mobile Ad Hoc networks // International Journal of Computer Networks & Communications (IJCNC). – 2013. – P. 86-395.
9. *Abramov E.S., Andreev A.V., Mordvin D.V., Makarevich O.B.* Corporate networks security evaluation based on attack graphs. // Proceedings of the 4th international conference on Security of information and networks (SIN '11)-ACM. – New York, NY, USA, 2011. – P. 29-36.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Абрамов Евгений Сергеевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: abramoves@sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Басан Елена Сергеевна – e-mail: ele-barannik@yandex.ru; кафедра безопасности информационных технологий; аспирантка.

Abramov Evgeny Sergeevich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: abramoves@sfedu.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; associate professor.

Basan Elena Sergeevna – e-mail: ele-barannik@yandex.ru; the department of security in data processing technologies; postgraduate student.