УДК 621.391

Защита информационной безопасности сенсорной сети кластерной архитектуры с помощью механизма обнаружения вторжения

Р.А. Бельфер [1], И.С. Огурцов [2]

[1] МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

[2] НИИЦ БТ МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Показана актуальность использования механизма обнаружения вторжения IDS в кластерной беспроводной сенсорной сети (БСС) для противодействия атакам, проводимым путем вброса злоумышленником нелегитимного сенсорного узла. Выполнение этим узлом функций головного узла кластера приводит к большому риску информационной безопасности всей кластерной области БСС. Дается описание предлагаемой системы обнаружения вторжений IDS на основе аномалий. При этом рассматриваются физический и канальный уровни сенсорного узла кластерной области.

Email: a.belfer@yandex.ru

Ключевые слова: *информационная безопасность, беспроводная сенсорная сеть, головной узел кластера, механизм обнаружения вторжения, IDS, обнаружение вторжений на основе аномалий.*

Беспроводная сенсорная сеть (Wireless sensor networks — WSN) — это распределенная сеть необслуживаемых миниатюрных сенсорных узлов, осуществляющих контроль и сбор данных. Существует множество приложений, для которых производители выпускают разные узлы для создания сенсорных сетей. По области применения приложения сенсорных сетей можно подразделить на следующие категории [1]: метеорологические данные (температура, давление), телемедицина, чрезвычайные ситуации (пожары, катастрофы и др.), военные операции (определение местоположения движущихся целей, территориальное распространение химического оружия) и др. Эти данные переносятся по беспроводному каналу в базовую станцию (БС). На рис. 1 приведен пример архитектуры БСС для приложения в военной области [2].

Узел сети, называемый сенсором, содержит датчик, воспринимающий данные от внешней среды (сенсор), микроконтроллер, память, радиопередатчик, автономный источник питания и иногда исполнительные механизмы. Для БСС характерны следующие факторы, которые влияют на обеспечение информационной безопасности (ИБ): ограничения сенсорных узлов в энергоресурсах; производительность процессора, памяти; подверженность удаления узла из сети или замены его; использование уязвимых к нарушению ИБ беспроводных каналов связи. Одна из особенностей сенсорных сетей состоит в том, что для выполнения функций сенсорные узлы располагают часто в тех местах, где человек не может находиться.

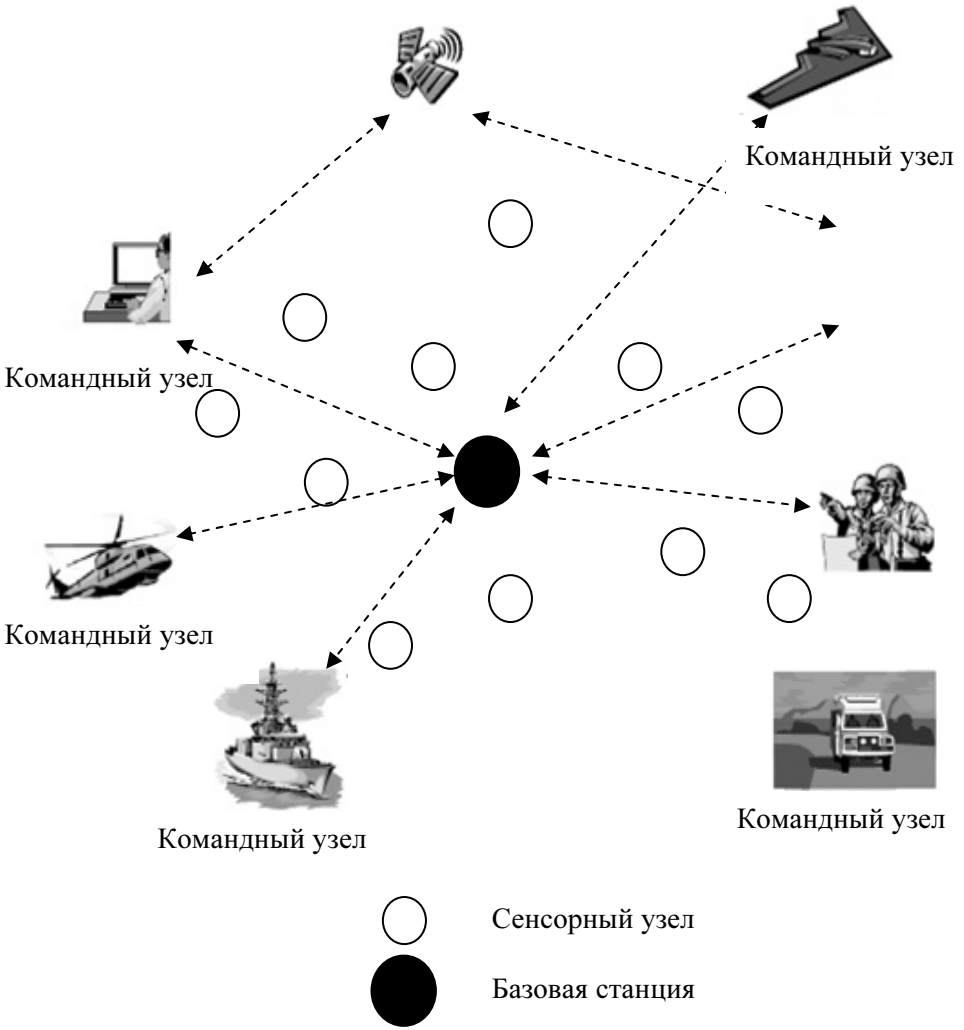

Рис. 1. Схема архитектуры БСС для приложения в военной области

Ограничение в энергоресурсах для узлов БСС является одним из важных факторов, влияющих на время функционирования всей сети или ее части. Основное энергопотребление сенсорных узлов падает на вычислительные процессы и обмен сообщениями между узлами. Поэтому один из способов снижения энергопотребления заключается в сокращении потребляемой мощности за счет уменьшения расстояния между взаимодействующими узлами. С этой целью используют кластерную архитектуру построения БСС. В этом случае узлы группируют в кластеры (группы), обмен данными с БС проводится через выделенный головной узел кластера (Cluster Head — CH), который собирает данные (концентратор нагрузки) для их дальнейшей передачи. На рис. 2 приведена схема БСС кластерной архитектуры

(два кластера), концентрирующая информацию от сенсорных узлов к БС. Группированием сенсорных узлов в кластерные области достигается масштабируемость БСС. Часто для БСС характерно большое число сенсорных узлов, расположенных с высокой плотностью [3], для чего требуется построение многоуровневой иерархической архитектуры головных узлов кластерных областей.

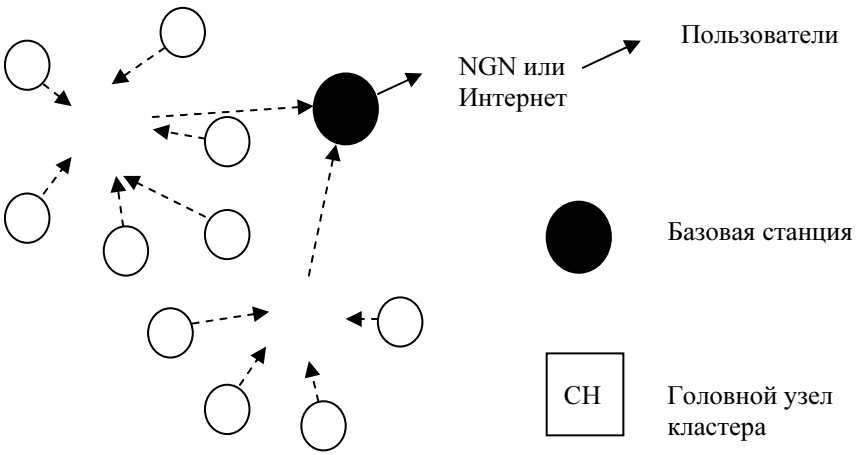

Рис. 2. Схема БСС кластерной архитектуры

Приведенная на рис. 1 архитектура относится к одноранговой, при которой все узлы БСС взаимодействуют с БС напрямую.

Риск угрозы выполнения функций головного узла нелегитимным сенсорным узлом. К СН предъявляют высокие требования по энергопотреблению, поскольку через него проходят все сообщения сенсорных узлов кластерной области. Применяют следующие стратегии определения головного узла кластера СН — назначение при проектировании или выбор одного из сенсорных узлов кластерной области в качестве СН. Выбор может быть фиксированным или переменным, любого узла или узла с наибольшими сохранившимися ресурсами (энергообеспечения, памяти). Высокие требования к ИБ головного узла являются причиной периодической смены головного узла кластерной области [4]. Анализу в данной работе подлежит обеспечение ИБ кластерной области при реализации одной из угроз, приводящей к высокому риску информационной безопасности. Согласно Рекомендации МСЭ-Т Е.408 [5] по требованиям к безопасности сетей электросвязи, характеристика риска ИБ определяется двумя показателями — вероятностью угрозы безопасности и последствием ее воздействия при атаке злоумышленника (реализации этой угрозы).

Для БСС характерна высокая вероятность реализации угрозы информационной безопасности — вброс в сеть (в данном случае в кла-

стерную область) злоумышленником нелегитимного сенсорного узла. Высокий риск ИБ в части последствия будет иметь место в том случае, если этот узел станет выполнять функцию головного сенсорного узла СН. Это может выражаться в различных формах последствий атаки «отказ в обслуживании» (DoS) маршрутизации, выраженных в прекращении функционирования части или всей сети [1]:

– истощение сетевых ресурсов сенсорных узлов;

– головной узел уничтожает все пакеты или выборочно те, которые он получает для последующей передачи;

– сфальсифицированная, измененная или нелегитимно повторенная информация полученного пакета для последующей передачи и др.

Способы обеспечения ИБ многих сетей связи включают как традиционные механизмы защиты (криптография, аутентификация и др.), так и механизмы обнаружения вторжения (Intrusion Detection System — IDS). Независимо от того, какие средства защиты предусмотрены, злоумышленник в такой уязвимой к угрозам ИБ сети, как БСС, может с помощью специальных протоколов найти лазейки, чтобы нарушить безопасность. Согласно работе [6], это является причиной того, что защита от угроз ИБ в сенсорных сетях начинается с работы механизмов IDS. Это же относится и к случаю рассматриваемой в данной работе атаки (вброс злоумышленником в кластерную область нелегитимного узла с целью выполнения им функций головного узла).

Обнаружение вторжений в общем случае — это процесс мониторинга и определения попыток реализации угроз ИБ. В данной работе это определение попыток вброса нелегитимного сенсорного узла в кластерную область БСС и использование его в качестве головного узла кластера СН.

Механизмы обнаружения вторжения в кластерную область. Принято классифицировать механизмы обнаружения вторжений на три типа [7]:

– обнаружение на основе сигнатур. Под сигнатурой понимают характеристики (профили) известных атак злоумышленника: IDS сравнивает текущую работу с каждым из хранящихся профилей. При совпадении с одним из них механизм обнаружения вторжения оповещает об этом. Недостаток такого механизма состоит в том, что он не позволяет выявить новый (неизвестный) вид атаки;

– обнаружение на основе аномалий. Суть работы такого механизма заключается в установке профилей при нормальном поведении системы (обычно это устанавливается автоматизированным способом) и выявлении отклонения от него при текущей работе. Основной недостаток такого механизма состоит в том, что он ошибочно оповещает много атак злоумышленника, которых на самом деле не было;

– обнаружение, основанное на спецификациях. Этот тип сочетает оба предыдущих.

Использование одновременно обоих типов механизмов позволяет уменьшить указанные недостатки и повысить ИБ сенсорной сети.

Далее рассмотрим некоторые механизмы обнаружения вторжений на основе аномалий при вбросе злоумышленником нелегитимного сенсорного узла. Мониторинг осуществляется для предотвращения этим нелегитимным узлом выполнения функций головного узла. На рис. 3 приведена структура потоков данных в БСС, включающая пакеты данных от сенсоров и пакеты механизма обнаружения вторжений IDS. На рисунке показаны две кластерные области на нижнем иерархическом уровне структуры БСС. Сообщения из головных узлов этих кластерных областей направляются в головной узел верхнего уровня и далее на базовую станцию.

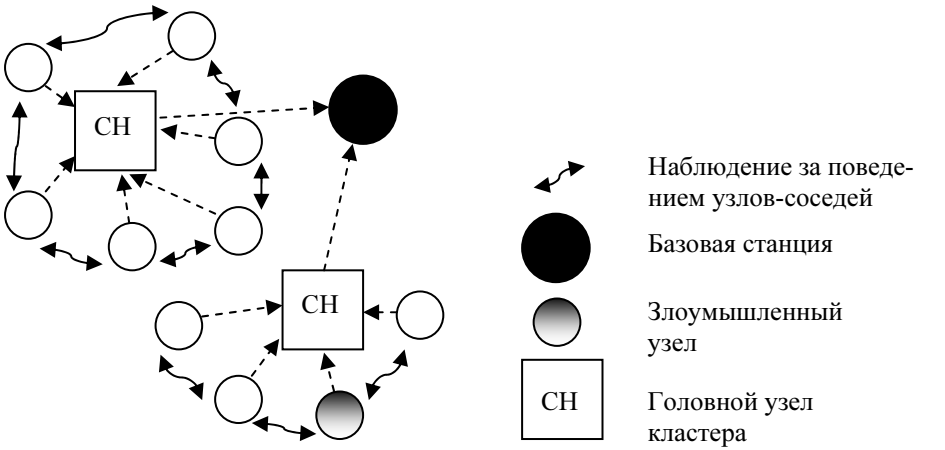

Рис. 3. Принцип работы механизма обнаружения вторжений в БСС

На рис. 3 показан принцип работы механизма обнаружения вторжений, в основе которого лежит постоянный мониторинг каждого из сенсорных узлов кластерной области за поведением их узлов-соседей. Собранные данные механизма обнаружения вторжений анализируются каждым сенсорным узлом и направляются для окончательной обработки головному узлу кластера. В случае выявления злоумышленного поведения головной узел оповещает о злоумышленном узле соседние с ним узлы. В результате взаимодействие с ним прекращается.

Механизмы обнаружения на основе аномалий вторжений нелегитимного сенсорного узла кластерной области. Рассмотрим атаку в кластерной области БСС путем вброса нелегитимного сенсорного узла при стратегии смены во время эксплуатации головных узлов в зависимости от степени истощения их энергии. При такой смене функции CH возлагаются на тот оконечный узел, который сохранил наибольшую электроэнергию. Задача обеспечения ИБ кластерной области распадается на две: обнаружение нелегитимного сенсорного узла и, в случае безуспешного решения этой задачи, обнаружение выполнения функций головного узла нелегитимным вброшенным злоумышленником сенсорным узлом.

Далее приведено описание механизмов системы обнаружения вторжений IDS на основе аномалий. Рассматриваются физический и канальный уровни сенсорного узла кластерной области [8]. При этом делается акцент на характеристику, позволяющую обнаружить вторжение, но не приводится, каким образом обрабатывается этот сигнал.

1. *Защита на физическом уро*вне. Проблема защиты радиоинтерфейса (защита от прослушивания канала передачи и зашумления) интенсивно исследуется для всех беспроводных сетей. Предложено много решений, таких как широкополосная передача и скачкообразная перестройка частоты. Когда узел принимает пакет, трудно определить, пришел ли пакет от заявленного отправителя, если не применяется аутентификация.

На физическом уровне сенсорного узла используется величина мощности принимаемого сигнала RSSI (Received Signal Strength Indicator). Современные операционные системы для БСС, такие как TinyOS, предоставляют возможность получения значения RSSI. Для беспроводной среды передачи RSSI зависит от расстояния между узлами. При развертывании БСС значения RSSI позволяют определить узлы-соседи. При функционировании БСС узлы следят за этими значениями, поступаемыми от соседних сенсорных узлов. Получение неожидаемого значения RSSI отличается подозрительным аномальным поведением от возможного вброса нелегитимного сенсорного узла для подмены легитимного узла. Существует немало факторов (фоновый шум, погодные условия), которые с большой вероятностью могут вызвать ложные подозрения. Поэтому этот подход следует использовать в комбинации с другими (на других уровнях).

2. *Защита на канальном уровне*. Если для управления разграничением доступа используют протоколы установки расписания, то для каждого из узлов выделяется уникальный временной слот. Для подмены легитимного узла при вбросе нелегитимного сенсорного узла необходимо, чтобы он использовал тот же временной слот. Если вброшенный злоумышленником сенсорный узел не следует этому временному расписанию и пытается выдать себя за легитимный узел, в то время как для этого узла передача не предполагается, то соседние с ним узлы могут определить такой нелегитимный узел. Ниже показано, каким образом фиксируется аномальное явление при выполнении протокола временного множественного доступа TDMA (Time Division Multiple Access) и протокола S-MAC (Sensor MAC), выполняющего переключение спящего и рабочего режимов.

Передача данных от сенсорных узлов в головной узел кластерной области осуществляется по схеме множественного доступа с временным разделением TDMA [4]. При этом каждому сенсорному узлу присваивается определенный интервал времени (слот) одинаковой несущей частоты. Получение сообщения на непредназначенном для него слоте отмечается как подозрительное аномальное явление от

возможного вброса нелегитимного дополнительного сенсорного узла или для подмены легитимного узла.

В соответствии с протоколом S-MAC [9] для снижения потребления электроэнергии сенсорный узел БСС работает по определенному циклу, включающему кроме режима передачи и приема сообщений еще ждущий и спящий режимы. Потребление энергии в каждом из этих режимов разное. Соседние сенсорные узлы с помощью обмена сообщениями устанавливают согласованное расписание временных периодов этих режимов. Получение сообщения на непредназначенном для него режиме отмечается как подозрительное аномальное явление от возможного вброса нелегитимного нового сенсорного узла или для подмены легитимного узла.

СПИСОК ЛИТЕРАТУРЫ

1. Бельфер Р.А. Угрозы информационной безопасности в беспроводных самоорганизующихся сетях // Вестник МГТУ им. Н.Э. Баумана. — Сер. Приборостроение. Спец. вып. «Технические средства и системы защиты информации». 2011. С. 116–124.
2. Abbasi A.A., Younis M. A survey on clustering algorithms for wireless sensor networks // Computer Communications. 2007. Vol. 30. P. 2826–2841.
3. Wang Y., Allebury G., Ramamurtby B. Security in wireless sensor networks / Y. Zang, J. Zheng, H. Hu (eds.) // Security in Wireless Mesh Networks. 2009. P. 433–490.
4. Wang G., Cho G. Proactive key variation owing to dynamic clustering (PERIODIC) in sensor networks // Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. CRC Press, 2011. P. 437–464.
5. ITU-T Recommendation E.408 // Telecommunication Network Security Requirement, 2004. URL.: http://www.itu.int/
6. Zang Y., Kitsos P. Security in RFID and sensor networks // Intrusion detection in wireless sensor networks. 2009. P. 321–340.
7. Md. Safiqul Islam, Rasib Hayat Khan, Dewan Muhammad Barry. A hierarchical intrusion detection system in wireless sensor networks // int. j. of computer science and network security. 2010. Vol. 10. No 8.
8. Кучерявый Е.А., Молчанов С.А., Кондратьев В.В. Принципы построения сенсоров и сенсорных сетей. Информационная безопасность сети связи для соединений абонентов ТфОП/ISDN через SIP-T // Электросвязь. 2006. № 6. С. 10–15.
9. Erdal C., Chunming R. Security in wireless ad hoc and sensor networks. N.Y.: John Willey & Sons Ltd: 2009. P. 257.

Статья поступила в редакцию 25.10.2012