Иерархическая система обнаружения вторжений для беспроводных промышленных самоорганизующихся сенсорных сетей

А.Н. Кокоулин,
доц., к.т.н., a.n.kokoulin@gmail.com,
Р.В. Чураков,
студ. магистр.,
ПНИПУ, г. Пермь

В последние годы технологии беспроводных самоорганизующихся (ad-hoc) сенсорных сетей становятся все более популярными при разработке и проектировании систем управления и мониторинга, как для гражданских, так и для военных объектов. Однако существует серьезная проблема в обеспечении информационной безопасности для сенсорных сетей, развертываемых в открытой и незащищенной среде. В большинстве случаев использования только алгоритмов криптографической защиты недостаточно для защиты сенсорной сети от внешних атак, поэтому целесообразно использовать систему обнаружения и предотвращения вторжений (IDS/IPS, Intrusion detection/protection system). Вопросы создания таких систем в гетерогенных беспроводных самоорганизующихся сетях, объединяющих множество видов сенсоров и узлов обработки данных, являются актуальными.

In recent years, wireless ad-hoc sensor networks have become increasingly popular in the design and project of control and monitoring systems for both civilian and military installations. However, there is a serious problem in providing information security for sensor networks deployed in an open and unprotected environment. In most cases, using only cryptographic protection algorithms is not enough to protect the sensor network from external attacks, therefore it is advisable to use the Intrusion Detection and Prevention System (IDS / IPS). The questions creation of such systems in heterogeneous wireless ad-hoc networks, which combine many types of sensors and data processing nodes, are offer relevant.

Введение

Сейчас существуют системы обнаружения вторжений (СОВ), которые предназначены для беспроводной самоорганизующейся сети. Большинство из них работают на распределенной среде, что означает, что они работают независимо от отдельных узлов и пытаются обнаружить вторжение путем изучения отклонений в поведении своих соседей. Для этого требуется больше вычислительной мощности, резервного питания аккумулятора и места для хранения, из-за чего системы обнаружения вторжений становятся более дорогостоящими и неосуществимыми для большинства приложений.

Некоторые СОВ используют в распределенной среде мобильных агентов. Этот агент поддерживает мобильность датчиков, умную маршрутизацию данных вторжения по всей сети, устраняет сетевую зависимость конкретных узлов. Но этот механизм по-прежнему не пользуется популярностью для СОВ из-за архитектурно-унаследованной уязвимости безопасности и большой нагрузки.

Некоторые из СОВ сосредоточенны только на одном типе атаки. Некоторые из них используют централизованную инфраструктуру, благодаря которой СОВ может использовать высокую вычислительную мощность персонального компьютера, огромное количество памяти и неограниченное резервное питание батареи.

Большинство СОВ нацелены только на уровень маршрутизации, который можно улучшить для обнаружения различных типов атак на других сетевых уровнях. Большинство архитектур основаны на обнаружении аномалий, которые анализируют статистический анализ деятельности узлов. Для обнаружения вторжений большинство СОВ используют файлы системных журналов, сетевой трафик или пакеты в сети для сбора информации. Некоторые обнаруживают только вторжение, а некоторые из них получают дополнительную информацию, например, тип атаки, местоположения злоумышленника и т. д. Хотя для беспроводной самоорганизующейся сети предлагается большое количество механизмов СОВ, очень немногие из них могут быть применимы для беспроводной сенсорной сети (БСС) из-за ограниченности ресурсов.

1. Существующие проблемы

Существующие системы обнаружения вторжений не являются подходящими для защиты беспроводных сенсорных сетей от внутренних и внешних угроз. Ни одна из них не является полной. Например, большинство подходов предлагают методы кластеризации без упоминания того, как они будут сформированы и как они будут вести себя с остальной частью системы. Большинство существующих СОВ имеют дело с проводной архитектурой, за исключением их беспроводного аналога. Архитектура беспроводной сенсорной сети еще сложнее, чем архитектура беспроводной самоорганизующейся сети. Таким образом, требуется СОВ с возможностью обнаружения внутри и снаружи, известных и неизвестных атак с низким уровнем ложной тревоги. Существующая архитектура СОВ, специально разработанная для сенсорных сетей, страдает от недостатка ресурсов: вычислительной мощности, памяти, питания батареи и т. д.

2. Обзор беспроводной сенсорной сети

Беспроводная сенсорная сеть - распределённая, самоорганизующаяся сеть множества датчиков и исполнительных устройств, объединённых между собой посредством радиоканала. Область покрытия подобной сети может составлять от нескольких метров до нескольких километров за счёт способности ретрансляции сообщений от одного узла к другому. Сенсорная сеть позволяет подключать до 65 000 датчиков. [1]

2.1. Сфера использования

Сенсорные сети обладают широкими возможностями применения. Основной областью применения является контроль и наблюдение измеряемых параметров физических сред и предметов. Беспроводные сенсорные сети, в частности, могут использоваться для предсказания отказа оборудования в аэрокосмических системах и автоматизации зданий. Из-за своей способности к самоорганизации, автономности и высокой отказоустойчивости такие сети активно применяются в системах безопасности и военных приложениях. Успешное применение беспроводных сенсорных сетей в медицине для мониторинга здоровья связано с разработкой биологических сенсоров совместимых с интегральными схемами сенсорных узлов. Но наибольшее распространение беспроводные сенсорные сети получили в области мониторинга окружающей среды и живых существ.

2.2. Архитектура

Беспроводные сенсорные сети (БСС) состоят из двух основных типов узлов:

1. Сенсоры (сенсорные узлы), которые развертывают в местах мониторинга (сенсорное поле) для сбора данных изучаемого явления или процесса и их передачи на базовые станции, где осуществляется централизованное управление и сбор данных.
2. Базовая станция (БС), также известная как шлюз (Gateway) или приемник (Sink), является интерфейсом, соединяющим сенсорную сеть с внешним миром. БС несет ответственность за получение данных от сенсоров, их обработку и доставку конечному пользователю. Как правило, базовые станции - это мощные устройства с большим объёмом памяти для хранения входящих данных. Базовая станция может иметь неограниченное количество источников питания и высокую пропускную способность канала для связи с другими базовыми станциями. Узлы беспроводных датчиков, напротив, являются маломощными, обладают низкой пропускной способностью и короткой дальностью связи.

2.3. Классификация

В зависимости от типа узлов в сети, в зависимости от окружающей среды, в которой они развернуты, а также в зависимости от метода развертывания или в зависимости от расположения узлов в сети беспроводные сенсорные сети могут быть классифицированы следующим образом:

- *Проактивные и реактивные.* На основе способа функционирования и целевого применения сенсорных сетей они могут быть классифицированы на проактивные и реактивные БСС. В проактивной БСС сенсорные узлы в сети периодически проверяют среду и передают данные, представляющие интерес для БСС. В реактивных БСС узлы оперативно реагируют на внезапные и резкие изменения в области сенсорного поля.
- *Гомогенные (однородные)* и *гетерогенные (неоднородные).* В однородных беспроводных сенсорных сетях все сенсорные узлы одинаковы с точки зрения энергии батареи и аппаратной сложности. Гетерогенные же сенсорные сети могут содержать два, три или больше типов узлов, соответственно с различными энергетическими и функциональными возможностями
- *Одноранговые и иерархические.* В одноранговой сети все узлы выполняют одинаковые задачи, и передача данных на шлюз или базовую станцию осуществляется непосредственно. В иерархических сетях узлы подразделяются на головные и сенсорные узлы. Сенсорные узлы собирают данные, а головные занимаются их обработкой, анализом и передачей на шлюз или БС.
- *Случайное и детерминированное размещение сенсорных узлов.* При случайном размещении сенсорные узлы могут быть случайным образом разбросаны по некоторой области. Детерминированное размещение предполагает размещение узлов в соответствии с предварительно определенным планом построения сети.
- *Статичность и мобильность.* Сенсорные узлы, используемые в БСС, могут быть стационарными или мобильными. При этом мобильные сенсорные узлы могут перемещаться с места на место, из-за чего связь между двумя узлами в сенсорной сети с мобильными узлами может быть очень сложной.
- *Двумерные и трёхмерные.* Несмотря на то, что большинство существующих работ в области беспроводных сенсорных сетей в настоящее время посвящены двумерному пространству, на самом деле такие сети работают в трехмерном пространстве, особенно с учетом появления новых приложений, таких как летающие сенсорные сети. [2]

2.4. Угрозы и проблемы безопасности в БСС

Описание существующих известных угроз и атак для БСС:

- Attack on Information in transit (Атака на передаваемую информацию). Сведения, которые должны быть отправлены могут быть модифицированы, изменены, воспроизведены, подделаны, или же украдены злоумышленником.
- Hello Flood (Привет, Флуд). Злоумышленник посылает большое количество пакетов Hello, чтобы объявить о себе большому количеству узлов в сети, убеждая себя в качестве соседа.
- Sybil attack (Атака Сибиллы). Использование множества поддельных идентификаторов для атаки на целостность и доступность данных.
- Wormhole Attack (Атаки червоточины). Передача информации в тайне между двумя узлами БСС.
- Black Hole Attack (Атака чёрной дыры). Злоумышленник поглощает все сообщения.
- Sink Hole Attack (Атака воронки). Подобно черной дыре. Исключение: злоумышленник вещает неверную информацию о маршрутизации.
- Selective Forwarding (Выборочная переадресация). Злоумышленник пересылает сообщения на основе заранее выбранного критерия.
- Jamming (Искажение сигнала). Это одна из причин отказа в обслуживании, в которой злоумышленник пытается нарушить работу сети, передавая высокоэнергетический сигнал.

- Flooding (Флудинг). Злоумышленник совершает новые запросы на подключение до тех пор, пока ресурсы, необходимые для каждого подключения, не будут исчерпаны или не достигнут максимального предела.
- Path-based DOS attack (Атака отказ в обслуживании на основе пути). Ввод ложных или повторно воспроизведенных пакетов в сети на конечных узлах. [3]

3. Архитектура СОВ

Система обнаружения вторжений - это аппаратное или программное средство, которое контролирует и проверяет компьютерную систему или сеть на наличие вредоносной активности или нарушения правил.

Системы обнаружения вторжений можно классифицировать по месту обнаружения вторжений и по используемому методу обнаружения вторжений.

По месту обнаружения вторжений:

- Сетевые системы обнаружения вторжений (Network-based IDS, NIDS) следят за трафиком в сети и, если обнаруживают подозрительную активность, которая может являться атакой или несанкционированными действиями, отправляет администратору предупреждение.
- Системы обнаружения вторжений хоста (Host-based IDS, HIDS) контролируют входящие и исходящие пакеты с данного устройства и предупреждает администратора, если обнаружена подозрительная активность.

По методу обнаружения вторжений:

- Signature-based (сигнатурный метод). Этот метод обнаруживает атаки путем поиска определенных шаблонов, таких как последовательности байтов в сетевом трафике или известные вредоносные последовательности команд, используемые вредоносными программами.
- Anomaly-based (метод аномалий). Метод аномалий используется для обнаружения неизвестных атак. Создаётся модель нормального поведения пользователей, а затем сравнивается с новой моделью поведения. Хотя такой метод позволяет обнаруживать ранее неизвестные атаки, он может страдать от ложных срабатываний: ранее неизвестная законная деятельность может быть классифицирована как вредоносная.
- Specification-based (метод спецификаций). СОВ на основе спецификации определяет протокол или правильную работу программы. Вторжение обозначается в соответствии с этими ограничениями. Такая СОВ может обнаруживать неизвестные атаки, при этом показывая низкий процент ложных срабатываний. [4]

Беспроводная самоорганизующаяся сеть определена в трех основных категориях, которые могут быть установлены для СОВ в архитектуре БСС:

- Автономные. Каждый узел действует как независимая СОВ и обнаруживает атаки для себя, не разделяя никакой информации с другим узлом СОВ, даже не взаимодействуя с другими системами. Таким образом, все решения по обнаружению вторжений основаны на информации, доступной для отдельного узла. Его влияние слишком ограничено. Эта архитектура лучше всего подходит в среде, где все узлы способны запускать СОВ.
- Распределённые и совместные. Несмотря на то, что каждый узел запускает свои собственные СОВ, они взаимодействуют друг с другом, чтобы сформировать глобальную СОВ. Эта архитектура больше подходит для плоских беспроводных сенсорных сетей, где глобальная СОВ инициируется из-за возникновения незавершенных вторжений, обнаруженных отдельным узлом.
- Иерархическая. Эта архитектура подходит для многослойной беспроводной сети. Здесь сеть делится на кластеры с головными кластерами. Головной кластер действует как небольшая базовая станция для узлов внутри кластера. Он также объединяет информацию из узлов о вредоносных действиях. Головной кластер обнаруживает атаки, так как узлы могут перенаправить, изменить или удалить пакет во время передачи. В то же время все головные кластеры могут взаимодействовать с центральной базовой станцией для формирования глобальной СОВ.

4. Новая модель СОВ

Новая модель СОВ, сосредоточена на экономии мощности сенсорных узлов, распределяя ответственность за обнаружение вторжений на трехуровневые узлы с помощью системы управления сетью на основе политик. Модель использует иерархическую схему наложения (HOD - hierarchical overlay design). Каждая область сенсорных узлов делится на гексагональную область. Сенсорные узлы в каждой из гексагональной области контролируются кластерным узлом. Затем каждый узел кластера контролируется региональным узлом. В свою очередь, региональные узлы будут контролироваться и управляться базовой станцией.

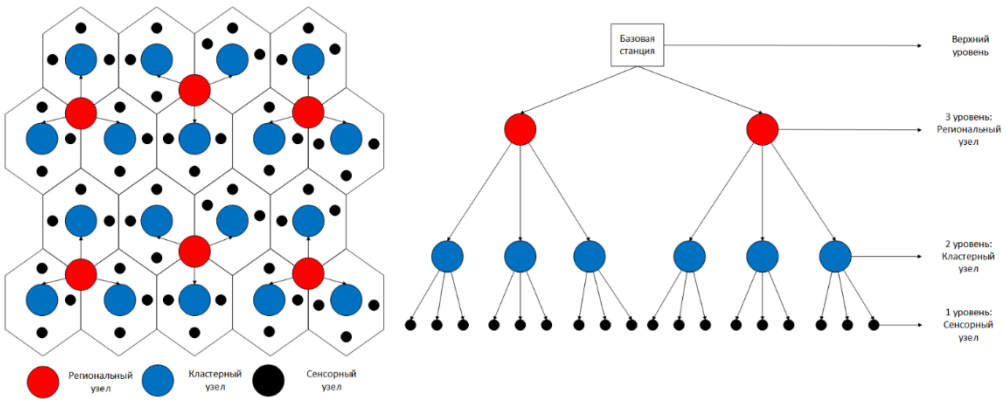

рис. 1 Иерархическая схема наложения

Эта СОВ на основе HOD объединяет два подхода к методам обнаружения вторжений (сигнатурный метод и метод аномалий) для борьбы с существующими угрозами. Сигнатуры известных атак распространяются от базовой

станции до конечного узла уровня. Репозиторий сигнатур на каждом уровне обновляется по мере обнаружения новых форм атак в системе. Предлагаемая СОВ может идентифицировать как известные, так и неизвестные атаки.

4.1. Объекты обнаружения

Сенсорные узлы имеют два типа функциональных возможностей: зондирование и маршрутизация. Каждый из сенсорных узлов будет воспринимать среду и обмениваться данными между сенсорными узлами и узлом кластера.

Кластерный узел играет роль узла монитора для сенсорных узлов. Один кластерный узел назначается для каждой из гексагональной области. Он будет получать данные от сенсорных узлов, анализировать и обобщать информацию и отправлять ее на региональный узел. Он более мощный, чем сенсорные узлы, и обладает встроенной функцией обнаружения вторжений.

Региональный узел будет отслеживать и получать данные от соседних кластерных узлов и отправлять объединенный сигнал тревоги на базовую станцию, находящуюся на верхнем уровне. Он также является узлом монитора, как и кластерные узлы со всеми функциональными возможностями СОВ. Это делает сенсорную сеть более масштабируемой.

Базовая станция является самой верхней частью архитектуры, наделенной поддержкой человека. Он будет получать информацию от региональных узлов и распространять информацию пользователям по их требованию.

4.2. СОВ на основе политик

Политика подразумевает заданный шаблон действий, который применяется при возникновении определенных условий. Для того чтобы достигнуть управления на основе политик для СОВ предлагаемая архитектура должна включать в себя несколько компонентов, которые оценивают следующие политики: BPDP - a Base Policy decision Point (пункт определения базовой политики (ПОБП)), RPA - Regional Policy Agent (агент региональной политики (АРП)), LPA - Local Policy Agent (агент локальной политики (АЛП)) и PEP - Policy Enforcement Point ((пункт обеспечения соблюдения политики (ПОСП)).

ПОБП является управляющим компонентом архитектуры. Он реализует политики или правила вторжения, созданные средством обнаружения вторжений (IDT), от произошедших событий, оценки аномальных условий и применения новых правил, алгоритмов, пороговых значений и т.д. IDT поддерживает создание, удаление, модификацию и проверку конфигураций и политик агента. Он может добавлять новые объекты, например, новую сигнатуру вторжения, изменение или удаление существующих объектов в АРП и АЛП.

АЛП управляет узлами датчиков, которые являются более мощными, чем сенсорные узлы. АЛП выполняют локальную настройку политик, фильтрацию, мониторинг и отчетность, что снижает пропускную способность управления и вычислительные затраты от сенсорных узлов конечного уровня для повышения эффективности сети и эффективности обнаружения вторжений. АРП может управлять несколькими АЛП. ПОБП контролирует и управляет всеми АРП.

ПОСП - это сенсорные узлы нижнего уровня.

Политики распространяются с ПОБП на АРП и АЛП. Описанные выше агенты политики помогают СОВ реагировать на изменения статуса сети глобально или локально. Это помогает автоматически перенастроить сеть для устранения сбоев и ухудшения производительности в соответствии с ответом на вторжение.

4.3. Структура агента обнаружения вторжений

Агент обнаружения вторжений (АОВ) содержится на каждом уровне иерархической архитектуры управления политикой СОВ. АОВ состоит из следующих компонентов: препроцессор, процессор сигнатур, процессор аномалий и постпроцессор.

Препроцессор либо собирает сетевой трафик датчика конечного уровня, когда он действует как АЛП, либо получает отчеты от АОВ нижнего уровня. Собранные данные из трафика датчика затем абстрагируются до набора переменных, называемых вектором стимула.

Процессор сигнатур поддерживает ссылочную модель или базу данных (Signature Record – Запись Сигнатур) типичных известных несанкционированных вредоносных угроз и действий с высоким риском и сравнивает отчеты от препроцессора с известными сигнатурами атаки.

Процессор аномалий анализирует вектор из препроцессора для обнаружения аномалии в сетевом трафике. Профиль нормальной активности, который распространяется от базовой станции, хранится в базе данных. Если активность, полученная от препроцессора, отличается от обычного профиля или превышает некоторые определенные пороговые значения, то атаки отмечаются.

Постпроцессор составляет и отправляет отчеты для агента верхнего уровня или базовой станции. Он может использоваться для отображения статуса агента через пользовательский интерфейс.

4.4. Выбор узла СОВ

Активация каждого узла в качестве СОВ приводит к потере энергии. Поэтому необходимо минимизировать количество узлов для запуска обнаружения вторжений. Существует несколько стратегий, связанные с выбором узла обнаружения вторжений.

Новая модель СОВ соответствует стратегии защиты ядра, где головной кластер является центральной точкой для защиты от злоумышленников. В стратегии защиты ядра отношение предупрежденных узлов и общего количества узлов в сети падает, что делает потребление энергии очень низким, и соответственно делает его более экономичным в использовании энергии, поскольку оно показывает наименьшее количество широковещательных сообщений в случае атаки. Он имеет сильную защиту во внутренней сети. Здесь СОВ должна ждать, пока злоумышленник достигнет области, что является одним из недостатков этой стратегии, поскольку узлы могут быть захвачены без уведомления.

4.5. Механизм СОВ в сенсорных узлах

Вторжения могут быть обнаружены в сенсорных узлах на нескольких уровнях (физический, канальный, сетевой и прикладной уровень).

На физическом уровне Jamming (воздействие преднамеренных помех) является основной атакой физического уровня. Идентификация jamming атаки может быть выполнена с помощью индикатора силы принимаемого сигнала, среднего времени, необходимого для определения незанятого канала (время восприятия несущей) и коэффициента доставки пакетов. В случае беспроводной среды уровень принимаемого сигнала зависит от расстояния между узлами. Утилизация и уничтожение узлов - это еще одна атака физического уровня, которая может быть предотвращена путем размещения узлов в защищенном месте. Во время процесса инициализации АЛП кластерного узла будет хранить значение силы принимаемого сигнала для связи между узлом кластера с сенсорными узлами конечного уровня и датчиком в сенсорном узле. Позже, во время мониторинга, процессор аномалий в АЛП будет контролировать, является ли полученное значение неожиданным. Если да, это будет обратная связь АРП, создавая соответствующий сигнал тревоги.

Атаки на канальном уровне - это коллизии, отказ от сна, переименование пакетов и т.д. Здесь S-MAC - Sensor Media Access Control (сенсорное управление доступом к среде) и TDMA - Time Division Multiple Access (множественный доступ с разделением по времени) могут использоваться для обнаружения аномалии. TDMA - это процесс цифровой передачи, в котором каждый узел кластера назначает разные временные интервалы для разных сенсорных узлов в своей области. В этом интервале каждый сенсорный узел имеет доступ к радиочастотному каналу без помех. Если какой-либо атакующий отправляет пакет с использованием адреса источника любого узла, например, A, но этот интервал не назначен для A, тогда АЛП процессора аномалий могут легко обнаружить это вторжение. Протокол S-MAC используется для назначения времени сна и пробуждения для сенсорных узлов. Поскольку датчик имеет ограниченную мощность, S-MAC может быть использован для экономии энергии. Если какой-либо пакет будет получен от источника, например, A, в период сна, тогда АЛП может легко обнаружить несостыковку.

Трассировка маршрута сетевого уровня используется для определения того, действительно ли пакет был получен из наилучшего маршрута. Если пакет приходит к месту назначения не по заданному маршруту, а по какому-то другому, то процессор аномалий может обнаружить возможное вторжение в соответствии с предопределенными правилами.

На прикладном уровне используются сторожевые устройства на трёх уровнях - базовой станции, региональном узле и кластерном узлах. Таким образом, если какой-либо один узел будет взломан злоумышленником, то сторожевое устройство с более высоким уровнем может легко обнаружить атаку и сгенерировать сигнал тревоги.

4.6. Реагирование на вторжение

Существует два разных подхода к реагированию на вторжение: «Горячий ответ» или «Ответ на основе политики». Горячий ответ реагирует путем запуска локального действия на целевом компьютере для завершения процесса или на целевом сенсорном узле для блокировки трафика. Например, отключить любой процесс, сброс соединения и т. д. Это не препятствует возникновению атаки в будущем. Ответ на основе политики работает в более широкой области. Он рассматривает угрозы, о которых сообщается в предупреждениях, ограничениях и объектах информационной системы сети. Он изменяет или создает новые правила в репозитории политик, чтобы предотвратить атаку в будущем.

Вторжение может быть обнаружено либо в кластерном узле, либо в региональном узле. Вторжения обнаруживаются автоматически в соответствии с политикой, реализованной ПОБП. [5]

Заключение

БСС подвержены вторжениям и угрозам безопасности. В этой статье рассматривается новая архитектура СОВ для самоорганизующейся сенсорной сети на основе иерархической схемы наложения и механизма ответа в соответствии с предлагаемой архитектурой. Новая модель СОВ распределяет общую задачу обнаружения вторжения. Новая модель СОВ отделяет общую работу по обнаружению вторжений с четырехуровневой иерархией, которая приводит к высокой энергосберегающей структуре. Каждый монитор должен контролировать только несколько узлов в пределах своего диапазона и, следовательно, на это не должно тратиться много энергии. Из-за иерархической модели система обнаружения работает очень структурированным образом и может эффективно обнаруживать любые вторжения. В целом каждая область управляется одним головным кластером, так что обнаружение происходит очень быстро, и сигнал тревоги подается на базовую станцию через головную область, что позволяет ему принимать надлежащие меры. Кластерные узлы или региональные узлы считаются более мощными, чем обычные сенсорные узлы. Хотя это увеличивает общую стоимость установки сети, но для повышения надежности, производительности и эффективности СОВ для большой географической области, где расположены тысячи сенсорных узлов, стоимость приемлема.

Литература

1. Беспроводная сенсорная сеть [Электронный ресурс] // Wikipedia.org. - URL: https://ru.wikipedia.org/wiki/Беспроводная_сенсорная_сеть (дата обращения: 25.11.2017).
2. Аль-Кадами Нассер Ахмед Салех. Исследование алгоритмов кластеризации в беспроводных сенсорных сетях. Санкт-Петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича, Санкт-Петербург, 2016.
3. Monika roopak. Review of Threats in Wireless Sensor Networks. International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (1), 2014, 25-31.
4. Intrusion detection system [Электронный ресурс] // Wikipedia.org. - URL: https://en.wikipedia.org/wiki/Intrusion_detection_system (дата обращения: 25.11.2017).
5. Mohammad Saiful Islam Mamun. Hierarchical Design Based Intrusion Detection System for Wireless Ad hoc Sensor Network. International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010, 102-117.