электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 02, февраль 2016

УДК 621.391

Угрозы безопасности сенсорных сетей

***Эренджeнова Д.С.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

***Чубатая А.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

***Куянов М.С.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Бельфер Р.А., к.т.н, доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
a.belfer@yandex.ru

ВВЕДЕНИЕ

Беспроводная сенсорная сеть WSN (Wireless Sensor Network) – это распределенная сеть необслуживаемых миниатюрных электронных устройств (сенсоров), которые осуществляют сбор данных о параметрах внешней среды и передачу их на базовую станцию посредством ретрансляции от узла к узлу с помощью беспроводной связи [1].

К отличительным особенностям беспроводных сенсорных сетей относится свойство самоорганизации сети, беспроводная среда передачи информации, автономное питание узлов сети, высокая отказоустойчивость, малый объем передаваемой по сети информации.

Кластерная организация узлов (рис. 1) считается эффективным методом снижения энергопотребления сети при условии рационального выбора головного узла кластера [2]. Головной узел может расходовать достаточно большое количество энергии на передачу сообщений от всех сенсорных узлов кластера к базовой станции. Поэтому головным узлом в кластере назначается сенсорный узел, имеющий наибольший запас энергии в данный момент времени.

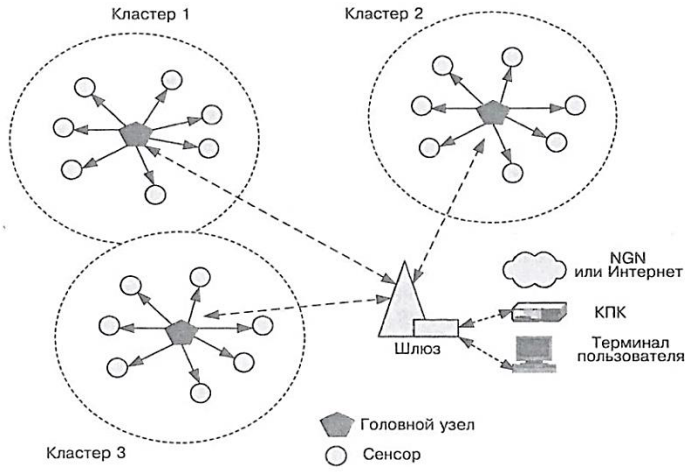

Рис. 1. Кластерная организация WSN

Сенсорные сети стремительно развиваются и находят применение в различных областях. Для них, как для самоорганизующихся беспроводных сетей, свойственно большое количество разнообразных угроз безопасности.

Атака отказа в обслуживании в сенсорных сетях и сетях в целом определяется как любое событие, которое лишает сеть способности выполнять свою функцию. Это происходит из-за непреднамеренного отказа узлов датчиков. Простейшая атака DoS пытается исчерпать ресурсы, доступные узлу, путем передачи дополнительных ненужных пакетов данных. Таким образом, она препятствует работе легитимных узлов сети и получению необходимых ресурсов. Атакой отказа в обслуживании (DoS) может быть любое действие, которое уменьшает возможности сенсорной сети, нарушая ее функционирование и предоставление каких-либо услуг.

Настоящая работа посвящена анализу следующих DoS-атак: атака Сибиллы (sybil attack), атака «воронка» (sinkhole attack), атака «червоточины» (wormhole attack), атака затопления «HELLO» (HELLO flood attack), а также атаки выбрасывания пакетов (packet dropping attacks) – серая дыра (gray hole attack) и черная дыра (black hole attack). Рассматриваются сценарии создания данных атак, а также механизмы их обнаружения и предотвращения.

АНАЛИЗ УГРОЗ

Атака затопления «HELLO» (HELLO Flood Attack)

Некоторые протоколы маршрутизации сенсорных сетей требуют, чтобы узлы отправляли hello-сообщения. Узел, получающий такое сообщение, может считать, что он находится в пределах радиодоступности отправителя. Однако, в некоторых случаях, данное предположение может оказаться ложным. Вредоносный узел, представляющий собой ноутбук или другое мощное устройство передачи данных, может убедить любой узел в сети в том, что он является соседом и может обеспечить лучший маршрут к базовой станции. В результате, те узлы, которые находятся достаточно далеко от противника, будут посылать сообщения, которые никогда не будут получены из-за недостаточной мощности передатчика и огромного расстояния. В основном, от такого типа атак страдают протоколы, зависящие от обмена информацией между соседними узлами для поддержания топологии или управления потоками данных [3].

Механизмы обнаружения и предотвращения:

- Существует криптографический метод для предотвращения флуд-атаки: любые два датчика имеют один и тот же секретный ключ. Каждый новый ключ шифрования генерируется сразу же во время соединения. Такой подход гарантирует, что только достижимые узлы могут расшифровать и проверить сообщение и, следовательно, помешать противнику.
- Один из видов защитных механизмов основан на мощности сигнала и информацией о местоположении. Идея состоит в том, чтобы сравнить уровень принятого сигнала с ожидаемым значением, рассчитанным с использованием информации о местоположении узла и заданных характеристик передатчика. Скорость обнаружения зависит от различных параметров, таких как плотность сети, коэффициент мощности передачи вредоносного узла и т.д.
- Также существует решение, взятое из MANET. Мобильные узлы используют пороговое значение, чтобы проверить, являются ли соседи злоумышленниками или нет. Когда количество пакетов запросов маршрута, транслируемых узлом, превышает заданное пороговое значение, то он рассматривается как нарушитель и сенсорная сеть перестает с ним взаимодействовать.

Атака выбрасывания пакетов (Packet Dropping Attack)

В случае данной атаки злоумышленник выборочно или полностью выбрасывает пакеты, нарушая нормальную работу сети. В зависимости от модели, данная атака может

быть разделена на два типа:

Черная дыра (Black Hole Attack). Узел злоумышленника объявляет себя знающим точный и короткий путь к необходимому узлу для того, чтобы иметь возможность перехватывать пакеты, вводя в заблуждение легитимные узлы сети. Наконец, когда все пакеты до необходимого узла передаются к узлу атакующего, он осуществляет их выброс. Данная атака ухудшает доступность, так как после ее проведения узлы в сети начинают использовать неоптимальные маршруты. Конфиденциальность нарушается из-за того, что злоумышленник может перед выбросом прослушать весь целевой трафик, идущий к целевому узлу.

Серая дыра (Gray Hole Attack). Атака производится аналогично принципу «черной дыры», только здесь выбрасываются не все пакеты, а лишь выборочные, согласно намерениям злоумышленника.

Очевидно, что обе «дыры» также позволяют злоумышленнику нарушить целостность передаваемой информации.

Механизмы обнаружения и предотвращения:

- Протокол маршрутизации Ариадна использует механизм хеширования на каждом узле для аутентификации каждого сообщения-запроса о маршруте. Для предотвращения данной атаки метод использует такие криптографические методы как MAC (Message Authentication Code) и т.д. Криптографические методы используются для каждого управляющего пакета, что предполагает определенную вычислительную нагрузку.
- Также была предложена распределенная схема обнаружения (distributed detection scheme), которая использует подтверждения от промежуточных узлов. В этой схеме каждый промежуточный узел, пересылающий сообщение, отвечает за обнаружение вредоносных узлов. Если промежуточный узел обнаруживает неправильное поведение своих последующих (или предыдущих) узлов, он создает сигнальный пакет и отправляет его на исходный узел (или на базовую станцию). Затем базовая станция и узел-источник могут использовать более сложные системы обнаружения вторжения IDS (Intrusion Detection System) для принятия решений.

Атака Сибиллы (Sybil Attack)

При атаке Сибиллы один из вредоносных узлов может иметь несколько идентификаторов. Злоумышленник, таким образом, маскируется под группу одновременно работающих легитимных узлов сети, используя их идентификаторы и верительные данные. Подделка идентификации может привести к тому, что

подконтрольные злоумышленнику узлы могут доказывать свою подлинность путем предоставления ложных удостоверений для привлечения к узлам злоумышленника больших объемов трафика, а также для осуществления ряда задач [4]:

- *Нарушение алгоритмов маршрутизации.* Вредоносный узел может с помощью атаки Сибиллы нарушить работу маршрутизации, используя свои идентификаторы для перенастройки путей, сбивая с толку систему сети.
- *Нарушение распределенного хранения данных***.** Атака Сибиллы может поразить механизм репликации и фрагментации данных в системе, используя его для хранения данных идентификаторов Сибиллы, генерируемых одним и тем же вредоносным узлом.
- *Голосование.* Беспроводные сенсоры могут использовать голосование для ряда задач. Атака Сибиллы может быть использована для «вброса в урну» голосов стольких идентификаторов узлов, сколькими располагает злоумышленник, чтобы изменить вердикт в свою пользу. Например, зловредные идентификаторы могут поручиться друг за друга, когда легитимные узлы путем голосования решают, являются ли идентификаторы Сибиллы вредоносными. Или же идентификаторы Сибиллы могут проголосовать против каких-то легитимных узлов, указывая на их «опасность» для сети.
- *Нарушение перераспределения ресурсов***.** Атака Сибиллы может быть использована для неравномерного распределения ресурсов между узлами в пользу вредоносного.
- *Применение системы обнаружения недостойного поведения по отношению к легитимным узлам*. В случае если сеть умеет определять конкретный тип неправомерного поведения узлов, она может принять определенные меры по отношению к нарушителям. Атака Сибиллы может спровоцировать эти меры к легитимным узлам, подставляя их. Сеть после этого считает их вредоносными и изолирует от себя такие узлы.

Механизмы обнаружения и предотвращения:

Аутентификация и шифрование могут помешать атакующему извне начать атаку Сибиллы в сенсорной сети. Однако атакующему изнутри может быть отказано в участии в работе сети, поэтому он может принять участие, только используя идентификаторы скомпрометированных узлов. Использование глобально распределенных ключей позволяет атакующему изнутри маскироваться под любой (возможно даже

несуществующий) узел. Шифрование открытым ключом может предотвратить такую атаку изнутри, но использовать данный способ в сенсорной сети с ограниченными ресурсами вычислительно затратно. Одним из решений является наличие у каждого узла уникального симметричного ключа с доверенной базовой станцией. Оба узла могут затем использовать протокол, подобный протоколу Нидхема-Шрёдера, чтобы удостоверить личность друг друга и создать общий ключ. Таким образом, пара соседних узлов могут использовать полученный ключ для реализации аутентификации и зашифрованного канала связи между ними. Примером протокола, использующего такую схему, является протокол LEAP, который поддерживает создание четырех типов ключей.

В целом, любая сеть с равноправными узлами (особенно беспроводные AdHoc-сети) уязвима к атаке Сибиллы. Однако, в сенсорной сети с базовыми станциями или шлюзами, данная атака может быть предотвращена с помощью эффективных протоколов. Доусер показал [5], что без логически централизованной власти атака Сибиллы возможна только при крайне нереалистичных допущениях. Однако обнаружить узлы, подвергшиеся атаке Сибиллы, не так просто. В качестве одного из способов используется тестирование радиоресурсами.

Атака «Воронка» (Sinkhole Attack)

Воронка является серьезной атакой, которая препятствует получению базовой станцией полных и корректных данных, создавая угрозу приложениям более высокого уровня. С помощью этой атаки злоумышленник может притянуть почти весь трафик из определенной области. Воронка активизируется, заставляя злонамеренный узел выглядеть особенно привлекательным для окружения узлов относительно слабых алгоритмов маршрутизации. Данная атака может также повлиять даже на узлы, находящиеся на значительном расстоянии от базовой станции [6].

Механизмы обнаружения и предотвращения:

- *Исследование потоков данных в сети (Network flow information approach).* Базовая станция по сети рассылает сообщения-запросы о пострадавших узлах. Пострадавшие узлы в ответ отправляют базовой станции сообщение, содержащее их ID, ID следующего узла и расходы, требуемые для передачи сообщения. Полученная информация используется базовой станцией, чтобы создать потоковый граф для идентификации Воронки. Алгоритм также устойчив в случае сотрудничающих вредоносных узлов, которые пытаются скрыть настоящего злоумышленника. При моделировании данный алгоритм продемонстрировал эффективность и точность, а также довольно низкие для сенсорных сетей расходы.

- *Контрольная схема подсчета скачков (Hop count monitoring scheme).* Схема основывается на мониторинге количества скачков, т.е. количество узлов, через которое сообщение проходит в процессе перемещения от исходного узла до узла назначения. Функцию количества скачков легко получить из таблиц маршрутизации, поэтому система обнаружения аномалий ADS (Anomaly Detection System) проста в реализации. Кроме того, предложенная ADS применима к любому протоколу маршрутизации, который поддерживает параметр для измерения количества скачков. Схема может обнаружить атаки с точностью 96 % при отсутствии ложных срабатываний.
- *Схема, основанная на RSSI (RSSI based scheme).* Подход основан на индикации уровня принимаемого сигнала RSSI (Received Signal Strength Indication). С помощью данного метода оценивается расстояние всех узлов относительно базовой станции. Эта информация затем используется для обнаружения атаки Воронки. Предложенный механизм не вызывает никаких коммуникационных накладных расходов.
- *Мониторинг процессора узла (Monitoring node's CPU usage).* Базовая станция контролирует использование ЦП каждым узлом и сравнивает полученное значение с пороговым. После этого базовая станция может определить, является ли данный узел вредоносным или нет.
- *Использование алгоритма Message Digest (Using message digest algorithm).* Основная цель протокола состоит в том, чтобы обнаружить точную воронку, используя односторонние цепочки хэшей. Адресат обнаруживает атаку только тогда, когда хэш, полученный из доверительного прямого канала и хэш, полученный через доверительный узел имеют разные значения. Этот метод гарантирует целостность данных сообщений, переданных с помощью доверительного канала. Алгоритм также надежен, в случае если сотрудничающие вредоносные узлы будут скрывать настоящего злоумышленника.

Атака «червоточина» (Wormhole Attack)

Червоточина предусматривает создание специального пути (туннеля) между двумя и более злонамеренными узлами сенсорной сети для передачи от одного узла сети в другой отдаленный узел перехваченных пакетов [7]. Как правило, для создания такого пути на физическом уровне используется иной диапазон частот, чем в атакуемой сенсорной сети. В результате такой атаки DoS получатель принимает нелегитимный

пакет данных. Атака «червоточины» препятствует протоколам маршрутизации, использующимся в сети (таким как DSR и AODV), правильно выстраивать маршруты между узлами, находящимися на расстоянии в один или нескольких узлов. Вследствие атаки червоточины нарушается доступность узлов сети, а, значит, нарушается работоспособность сети.

Атака «червоточина» в протоколе маршрутизации RPL. Следует отметить, что некоторые важные задачи защиты от угроз ИБ в сенсорных сетях остаются не решенными. Это относится, в частности, к протоколам маршрутизации. Многие из этих протоколов разрабатываются для определенной области применения сенсорной сети. В работе [8] отмечается, что в приведенных там около двух десятков протоколов маршрутизации ни в одном из них не предусмотрены все необходимые меры по защите от угроз безопасности. В настоящем разделе рассматривается протокол маршрутизации для сетей с низким потреблением энергии и потерями RPL (Routing protocol for low power and lossy networks), в котором предусмотрены механизмы защиты от угроз нарушения маршрутизации. RPL превосходит другие протоколы для сенсорных сетей в части качества обслуживания (QoS), производительности и энергосбережения. Приведем более подробно сценарий атаки «червоточины» этого протокола маршрутизации. Предварительно опишем принцип работы протокола. В RPL, основанном на ориентированном направленном графе расстояний DODAG (Destination Oriented Directed Acyclic Graph), каждому узлу ставится в соответствие определённый ранг таким образом, что он возрастает по мере удаления от корневого узла (маршрутизатора). Пересылка пакета корневому узлу состоит в пересылке его соседнему узлу с наименьшим рангом – предпочтительному родителю. Узлы обмениваются сигнальной информацией, т.н. информационными объектами графа расстояний DIO (DODAG Information Object), для поддержания графа DODAG в актуальном состоянии. Все узлы в сети периодически генерируют DIO-пакеты для оповещения соседей о своем ранге. Каждый узел кроме информации о предпочтительном родителе хранит информацию об альтернативных родителях с большими рангами, и при выходе из строя предпочтительного родительского узла или нарушении связи с ним передача пакетов будет идти через один из резервных узлов. Это позволяет обеспечить отказоустойчивость сети.

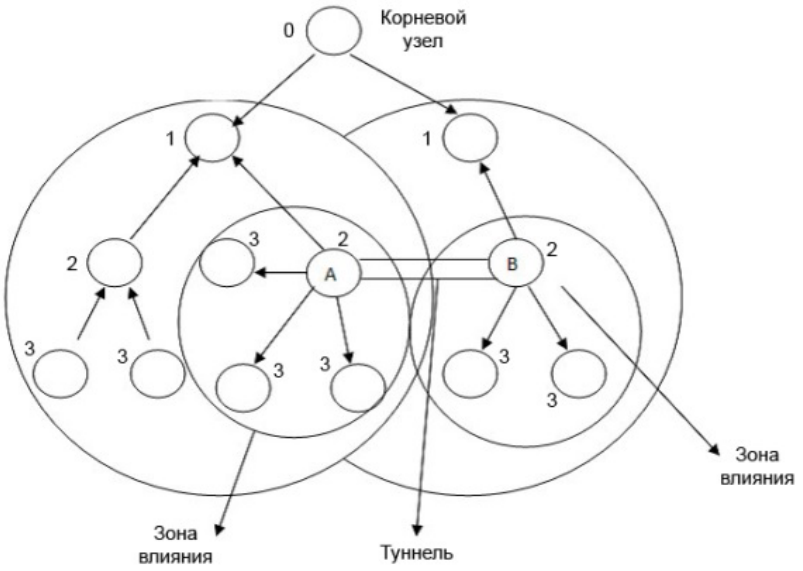

Рис. 2. Wormhole в протоколе RPL

На рисунке 2 покажем сценарий атаки «червоточина» в RPL. Вредоносные узлы строят туннель с быстрой передачей пакетов в другую часть сети [9]. Атака происходит, когда вредоносный узел присоединяется к сети и посылает DIO-сообщения с намерением выбрать в качестве предпочтительного родителя как можно больше узлов. Этот предпочтительный родитель после получения пакетов из окружающей его среды, передает их через туннель в другой вредоносный узел, который передает пакеты окружающим его узлам.

Механизмы обнаружения и предотвращения:

- *Маркировка пакетов (Packet leashes).* Маркер (метка) – это информация, указывающая на максимально допустимую дальность передачи пакета. Различают два типа: географический маркер (geographical leashes) и временной маркер (temporal leashes). С помощью географических меток каждый узел узнает информацию о местоположении другого узла. Географические метки гарантируют, что получатель находится в пределах допустимого расстояния от отправителя. Временная метка оценивает границу времени жизни пакета, что, в свою очередь, также ограничивает максимально допустимое расстояние между узлами.
- *EDWA (end-to-end detection of wormhole attack).* Алгоритм EDWA оценивает количество узлов, необходимое для передачи сообщения, используя информацию о местоположении узла-передатчика. Атака червоточины может быть обнаружена, в случае если расчетное количество узлов больше количества узлов, через которые фактически прошло сообщение. После обнаружения атаки авторы предлагают

использовать алгоритм трассировки (TRACING algorithm), чтобы определить конечные узлы червоточины.

ЗАКЛЮЧЕНИЕ

Проведенный анализ атак DoS в беспроводных сенсорных сетях может быть использован при дальнейшей работе для оценки уровня угроз безопасности этих сетях. Знание уровня угроз информационной безопасности позволяет при проектировании, испытаниях и эксплуатации сенсорной сети принимать решения по повышению ее ИБ за счет усиления защиты от тех угроз, которым соответствует наиболее высокий уровень риска безопасности.

Список литературы

[1]. Мочалов В.А., Пшеничников А.П. Принципы построения и функционирования сенсорных сетей связи. 2-е изд. М.: МТУСИ, 2014. 53 с.

[2]. Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN. СПб.: БХВ-Петербург, 2013. 160 с.

[3]. Singh P.V., Jain S., Singhai J. Hello Flood Attack and its Countermeasures in Wireless Sensor Networks // International Journal of Computer Science. 2010. Vol. 7. No. 11. P. 23–27.

[4]. Newsome J., Shi E., Song D., Perrig A. The Sybil Attack in Sensor Networks: Analysis & Defences // In Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN 2004). Berkeley, CA, 2004. P. 259–268.

[5]. Douceur J.R. The Sybil attack // In Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS'02). London, UK, 2002. P. 251–260.

[6]. Soni V., Modi P., Chaudhri V. Detecting Sinkhole Attack in Wireless Sensor Network // International Journal of Application or Innovation in Engineering & Management. 2013. Vol. 2, No. 2, P. 29–32.

[7]. Hu Y.-C., Perrig A., Johnson D.B. Wormholes Attacks in Wireless Networks // IEEE Journal on Selected Areas in Communications. 2006. Vol. 24. No. 2. P. 370–380.

[8]. Anjali, Shikha, Sharma M. Wireless Sensor Networks: Routing Protocol and Security Issues // IEEE Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT). Hefei, Anhui, China, 2014. P. 1–5.

[9]. Khan F.I., Shon T., Lee T., Kim K. Wormhole Attack prevention mechanism for RPL based LLN network // In Proceedings of the Fifth International Conference on Ubiquitous and Future Networks (ICUFN). Da Nang, Vietnam, 2013. P. 149–154.