Анализ и моделирование vampire-атак в самоорганизующихся беспроводных сенсорных сетях

В. А. Десницкий

Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»

desnitsky@comsec.spb.ru

И. В. Котенко

Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»

ivkote@comsec.spb.ru

Аннотация. **Работа включает исследование вопросов информационной безопасности самоорганизующихся беспроводных сенсорных сетей (БСС). Объектом исследования являются vampire-атаки, присущие БСС и направленные на истощение энергоресурсов узлов, функционирующих от ограниченных автономных источников энергопитания. Такая атака базируется на эксплуатации злоумышленником одного или нескольких скомпрометированных узлов, к которым у нарушителя имеется доступ. Атака включает нарушение процессов маршрутизации в самоорганизующейся БСС со злонамеренным изменением фактических маршрутов следования пакетов данных. Тем самым нарушитель заставляет узлы расходовать значительно больше энергоресурса. Это в свою очередь приводит к значительно более быстрому разряду батарей, в результате чего сеть перестает полноценно функционировать, и предоставляемые ею прикладные сервисы оказываются недоступными конечным пользователям. В частности, такие последствия становятся особенно критичными в случае сетей, функционирующих в рамках важных инфраструктурных объектов, производств непрерывного цикла, на транспорте. В работе предлагается обобщенная имитационная модель vampire-атак, основанная на правилах и пригодная при имплементации широкого спектра БСС. Модель оценивается на примере фрагмента прототипа самоорганизующейся беспроводной сенсорной сети с узлами Digi XBee серии 2. По результатам моделирования сформулированы основные выводы.**

Ключевые слова: беспроводная сенсорная сеть; безопасность; vampire-атака; анализ; моделирование

I. Введение

В настоящее время беспроводные сенсорные сети получают все большее распространение в различных прикладных областях, таких как сети соединенных автомобилей, дронов, коммуникационные системы для поддержки операционных процессов на производствах, в торговых и складских помещениях, на территориях морских портов и пр. Ввиду критически важного характера таких систем в условиях работы в потенциально ненадежном и не доверенном окружении, особого внимания заслуживают вопросы информационной безопасности таких систем. В частности, скомпрометировав один или несколько узлов БСС, атакующий может осуществить различные атаки, направленные на нарушение аутентичности циркулирующих по сети данных и нарушение доступности устройств.

Наличие в таких системах автономных модулей, формирующих мобильные и перемещаемые в пространстве узлы БСС, обуславливает подверженность таких устройств атакам истощения энергоресурсов. При помощи таких атак злоумышленник воздействует на доступные ему проводные и беспроводные коммуникационные интерфейсы узлов сети, другие аппаратные модули БСС, на хранимые и передаваемые по сети данные, на среду окружения сети, на пользователей для единовременного, скачкообразного или постепенного снижения заряда батарей атакуемых узлов. Помимо прямого воздействия, такие атаки, называемые атака типа Denial-of-Sleep, могут осуществляться опосредованно, например, путем периодической отправки на узел-жертву запросов, нарушающих процесс периодического нахождения узла в режиме экономного энергопотребления [1]. Сложность идентификации такого воздействия связана с тем, что оно осуществляется не напрямую, а с вовлечением других легитимных узлов сети. При этом трафик, исходящий от каждого такого узла, сам по себе сложно идентифицируем в качестве атакующего, тогда как группа таких узлов формирует атаку в совокупности.

Еще в качестве одного характерного примера разновидности атак истощения энергоресурсов можно выделить vampire-атаки, которые направлены на постепенное исчерпание заряда группы узлов путем эксплуатации уязвимостей протоколов маршрутизации [3]. Модификация полей пакета в процессе его ретрансляции на скомпрометированном промежуточном узле позволяет потенциально неограниченное число раз перенаправлять этот пакет по тем же маршрутам повторно, тем самым истощая энергозаряд автономно функционирующих узлов, располагающихся по данному маршруту. И в общем случае выявление таких атакующих пакетов представляется сложно осуществимой задачей ввиду изменчивости таких пакетов и их маскировки под доброкачественный трафик

Исследование выполнено за счет гранта Российского научного фонда № 24-21-00486, https://rscf.ru/project/24-21-00486/.

штатных прикладных сервисов сети. Таким образом, для решения задач обнаружения vampire-атак и повышения защищенности от них необходимы дополнительные исследования данного вида атак, включающее анализ их существующих и возможных особенностей и разновидностей, а также их моделирование, что необходимо для повышения их детектируемости.

В работе проведен анализ существующих моделей и решений по моделированию vampire-атак в БСС. Предлагается обобщенная имитационная модель vampire-атак, основанная на правилах и пригодная для имплементации для широкого класса беспроводных сенсорных сетей, поддерживающих программно определяемые процессы маршрутизации с использованием современных сетевых протоколов БСС, таких как ZigBee, Wi-Fi, LPWAM-протоколы, в том числе Sigfox, LoRa и др. Модель апробирована на примере фрагмента прототипа самоорганизующейся беспроводной сенсорной сети с узлами Digi XBee серии 2. По результатам моделирования сформулированы основные выводы. К отличительным элементам новизны предлагаемой модели относится ее универсальный характер, предполагающий ее применимость для широкого класса беспроводных БСС, способных функционировать в различных условиях и окружениях, а также позволяющий моделировать различные вариации атаки, в том числе, эксплуатирующие уязвимости используемых протоколов сетевого уровня и функций маршрутизации, в частности.

II. Анализ предметной области

Vampire-атаки, проводимые на сетевом уровне взаимодействия, являются в достаточной степени универсальными и применимы к множеству различных протоколов функционирования БСС [3]. Такие атаки, как правило, базируются на недостаточной защищенности протокола на сетевом уровне и эксплуатируют уязвимости протокола, связанные в том числе с нарушением целостности адресов, выполненных хопов пакета, меток времени и других данных, содержащихся в служебных полях сетевого протокола. При этом ряд исследований подтверждает достаточно высокую эффективность таких атак, выражаемую при помощи показателей скорости истощения батареи атакуемого узла, в количестве таких одновременно атакуемых узлов, а также в скрытности такой атаки [4], [5].

В рамках существующих или проектируемых БСС принципиально важной оказывается необходимость оценки потенциального ущерба от применения vampire-атак, учитывающей как особенности конкретного используемого беспроводного протокола, так и характеристик самой сети. В зависимости от этого должны выбираться и применяться, как контрмеры, так и средства обнаружения, позволяющие выявить необходимость применения какой-либо контрмеры [6].

Однако стоит обращать внимание на комплексный характер vampire-атак, в процесс выполнения которых может вовлекаться различное число уязвимых узлов, которые нарушитель способен эксплуатировать. Кроме того, атака может учитывать такие характеристики как ширину коммуникационного канала, разветвленность и динамизм сетевой топологии, величину средней передаваемой полезной нагрузки, состав аппаратной части узлов, энергоресурсы узлов, а также свойства самоорганизации и децентрализации БСС. Поэтому оценка эффективности vampire-атак в конкретной БСС с заданным сценарием функционирования зачастую оказывается проблематичной и практически невыполнимой при помощи исключительно лишь средств аналитического исследования.

В результате этого возникает потребность в проведении натурных исследований таких атак, что в свою очередь, как правило, затруднено из-за технической сложности натурного моделирования такой атаки с необходимостью одновременного скоординированного воздействия на ряд узлов, а также воспроизведением репрезентативных экспериментальных условий нормального функционирования БСС с заданной сетевой нагрузкой и проведением измерений. Также часто оказывается, в особенности в случае работы БСС в рамках критически важных инфраструктур, нет ни юридической, ни фактической возможности натурного тестирования моделей атак на имеющейся аппаратной инфраструктуре, штатная работа которой не может быть нарушена или приостановлена. Все это определяет потребность в проведении имитационного моделирования vampire-атак, которое бы являлось, во-первых, настраиваемым под различные виды сетей, сценариев, различный состав сетей, различные виды беспроводных технологий, во-вторых, адекватно отражало процессы функционирования сети под атакой и, в-третьих, было бы практически выполнимым с точки зрения технических ограничений и компетенций, а также затрачиваемых на него ресурсов [7]. Поэтому, все это позволяет сделать вывод о высокой актуальности и важности решения задач настоящего исследования.

III. Моделирование БСС и атак

Для имитационного моделирования атаки в первую очередь необходимо провести моделирование нормального поведения БСС. Не умаляя общности процесса моделирования, рассматриваем следующую сетевую топологию БСС, состоящую из пяти узлов и представляемую при помощи графа. В каждой вершине графа располагается некоторый узел сети, а линии между вершинами обозначают имеющиеся физические беспроводные двунаправленные каналы связи. Каждый канал связи предполагает ровно двух абонентов.

Нормальное сетевое поведение узлов БСС представляет собой регулярную отправку показаний сенсоров в сеть по заданному адресу, отправку и получение служебных сетевых команд, подтверждающих живучесть узла и формирующих другие системные характеристики. В рамках проводимого моделирования такое поведение узлов задается при помощи генератора псевдослучайных чисел на основе случайной величины с нормальным распределением путем задания математического ожидания *mu*, описывающего усредненное значение промежутка времени, через которое узел будет отправлять очередное сообщение в сеть и *si* – среднеквадратичное отклонение. Такое распределение позволяет смоделировать в первом приближении

наиболее характерное усредненный временной интервал с учетом рандомизации фактического формирования сообщений в заданных временных рамках.

В рамках проводимого моделирования для пяти узлов используются следующий вектор значений

$$\{(mu_t, si_t)\}_{t=1..5} = \{(A_{mu}(1), A_{si}(0.1)), (B_{mu}(2), B_{si}(0.1)), (C_{mu}(-), C_{si}(-)), (D_{mu}(2), D_{si}(0.2)), (E_{mu}(-), E_{si}(-))\},$$

где узлы помечены буквами алфавита от *A* до *E*, а числовые значения заданы в секундах. При обозначении математического ожидания и среднеквадратичного отклонения дефис обозначает отсутствие событий генерации сообщений на данном узле. Возможные нулевые значения случайной величины игнорируются в процессе моделирования, тогда как отрицательные значения берутся по модулю. При этом для каждого узла *X*, генерирующего сообщения конечный адресат каждого сообщения *Y* определяется равновероятно из оставшихся четырех узлов сети с вероятностью $P(dest(X) = Y) = 0.25$. Старт процесса имитационного моделирования БСС производится от нулевого момента времени с естественной скоростью течения времени. В качестве полезной нагрузки нормальных пакетов данных используются произвольные данные фиксированной длины, что как-либо ощутимо не влияет на процесс моделирования. Для моделирования vampire-атаки узлы *C* и *D* моделируются как контролируемые атакующим. Предполагается, что атакующий имеет полный доступ к их таблицам маршрутизации и способен создавать и отправлять любые пакеты данных, перехватывать и модифицировать любые системные поля и полезную нагрузку любые сообщений, проходящих через данный узлы *C* и *D*.

Для реализации модели vampire-атаки нарушитель злонамеренно модифицирует правила маршрутизации на этих двух узлах следующим образом. Во всех ZigBee-пакетах, у которых в качестве конечного адреса указан адрес узда *C*, на узле *C* осуществляется подмена, адреса на узел *E* для того, чтобы пакет продолжил дальнейшее движение по сети на узел *E* через узел *D*. В зависимости от реализации протокола, для этого могут также корректироваться такие поля заголовков как sequence number пакета, хэш-сумма, метка времени и пр., чтобы пакет не было отброшен автоматически из-за того, что он превысил число хопов. Аналогичным образом, любой пакет пришедший на узел E с узла C подвергается замене адреса снова на адрес C и отправляется в качестве промежуточного узла на узел *A*. На рис. 1 схематично показана моделируемая сеть для случая БСС на основе узлов Digi XBee серии 2, причем узел *B* функционирует от автономного, ограниченного источника питания, и является узлом-жертвой vampire-атаки.

Происходит фактическое зацикливание пакета данных, и он способен пройти по кругу *C→D→E→A→B→C* подряд потенциально неограниченное число раз. Однако, для злоумышленника, чтобы снизить вероятность обнаружения нелегитимного трафика в сети, количество таких циклом может быть ограничено до нескольких штук в зависимости от условий и целей vampire-атаки. Кроме того, в целях скрытности атаки в качестве подобных циклически пересылаемых пакетов потенциальному нарушителю целесообразно использовать уже существующие легитимные пакеты, не создавая новых искусственно, чтобы простейшие механизмы безопасности, основанные на шаблонах разрешенных потоков данных, не выявили бы такой аномальный пакет.

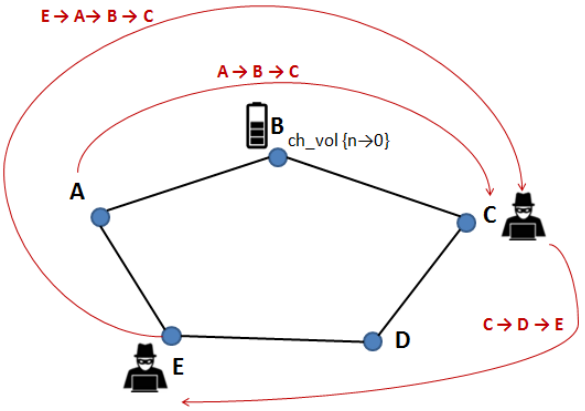

Рис. 1. Моделирование vampire-атаки в самоорганизующейся беспроводной сенсорной сети

Моделирование расхода заряда батареи автономно работающего узла *B* производится с использованием целочисленной переменной *ch_vol*, которой задается некоторое начальное значение $n \leq 1$ перед стартом процесса имитационного моделирования. Процесс изменения данной переменной с течением времени задается в виде правил вида

$$ch\_vol(e) \text{ -= } d,$$

где *e* определяет экземпляр события определенного вида, d задает усредненную величину изменения нормированного заряда батареи узла, тогда как символ '-=' обозначает бинарную операцию изменения левого операнда на величину значения правого операнда. Кроме того, независимо от происходящих в сети событий, в которые вовлечен узел *B*, применяется следующее правило

$$ch\_vol(t \mid t=1,2,...) \text{ -= } \Delta,$$

где *t* определяет дискретный счетчик времени, исчисляемый в секундах, инициализируемая значением 0 в момент запуска имитационной модели и увеличиваемый на 1 по прошествии каждой очередной секунды функционирования модели. Значение Δ задает константную усредненную величину уменьшения заряда в условиях фонового функционирования узла *B*. Отметим, что для запуска модели значения *d* и Δ устанавливаются экспертно.

IV. Реализация и дискуссия

Предложенная имитационная модель реализована с использованием языка Python, и в ее основу заложены модель состояния узлов сети, задающая узлы БСС, коммуникационные каналы, характеристики узлов, в том числе величину заряда, а также генерация и движение пакетов данных по сети. Реализованный комбинаторный алгоритм при помощи генераторов псевдослучайных чисел генерирует события, как нормального функционирования, так и события, инициируемые

атакующим. Выходными данными разработанного Python-скрипта, является лог, содержащий последовательности моделируемых событий, снабженных метками относительно времени, в том числе лог, получаемый в результате моделирования приведенной в разделе 3 vampire-атака с использованием скомпрометированных узлов *C* и *E*.

Результаты экспериментов по моделированию vampire-атак в условиях отличающейся интенсивности атаки приведены на рис. 2. В зависимости от значения показателя скрытности атаки *L*, варьирующего в диапазоне (0, 1) в зависимости от интенсивности воздействий, в каждой из итерации эксперимента вычислялась эффективность атаки. Максимальная скрытность атаки, соответствует значению 1, тогда как минимальное значение – 0. В последнем случае атака считается хорошо наблюдаемой, и, как предполагается, она высоковероятно может быть обнаружена. Эффективность выражается в виде отношения снижения величины заряда узла-жертвы, находящегося под атакой к величине снижения заряда данного узла при нормальной работе сети. Величины изменения заряда делимого и делителя рассматриваются за одинаковый промежуток времени, по умолчанию равный 1 сек. К особенностям осуществленного моделирования можно отнести довольно низкие затраты на вычислительные ресурсы, позволяющие его проводить на типовом пользовательском персональном компьютере.

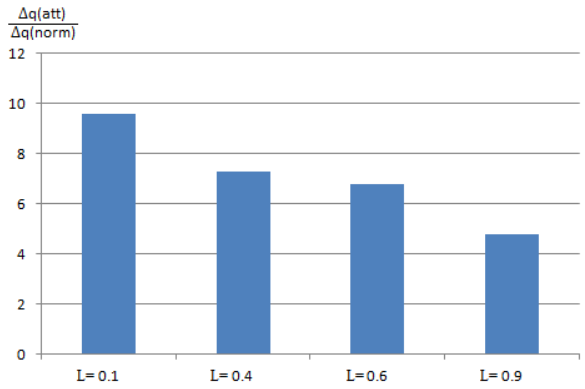

Рис. 2. Оценка эффективности vampire-атаки

Проведенные эксперименты подтверждают выполнимость имитационного моделирования vampire-атак без необходимости вовлечения каких-либо значительных вычислительных мощностей. Вместе с тем моделирование подтверждает потенциально высокую эффективность таких атак при различных величинах скрытности атаки. Поэтому, в частности, такую атаку целесообразно учитывать в рамках комплексных моделей атак в самоорганизующихся децентрализованных БСС. Возможность динамического перераспределения функций сбора, обработки данных, а также функций управления сетью открывают широкие возможности для атакующего злонамеренно эксплуатировать автономно работающие узлы БСС для значительно более быстрого исчерпания энергоресурса.

В целом vampire-атакам в особенности оказываются подверженными и наиболее критичными БСС в областях, где киберфизические устройства, такие как БПЛА, оказываются в тесном сопряжении с информационно-вычислительными процессами сети. К значимым последствиям успешной vampire-атаки можно отнести не только внезапная приостановка пользовательских сервисов, которые такой БПЛА предоставляет, но также и физическое крушение самого дрона, его разрушение и возможное причинение вреда окружающей инфраструктуре сети [8]. Ввиду того, что vampire-атака проявляется на сетевом уровне сетевого взаимодействия, то к перспективным способам предотвращения таких атак, не требующего для этого значительных ресурсов узлов, или, как минимум, к способам повышения сложности осуществления таких атак, можно отнести повышение защищенности протоколов маршрутизации в БСС. В частности, возможно встраивание в протокол проверок неизменности маршрута пакета данных на протяжении его передачи. В частности, для этого может использоваться технология блокчейна, но требования к ресурсам БСС должны быть дополнительно изучены.

V. Заключение

В рамках дальнейшей работы по данному направлению планируется расширение экспериментальной части моделирования vampire-атак с целью получения расширенного набора выходных логов, которые будут обладать высокой вариативностью, а также репрезентативностью для задач построения классификаторов, как средств программного обнаружения vampire-атак.

Список литературы

[1] Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning // Studies in Computational Intelligence. 2020. Т. 868. С. 350-355.

[2] Hatfield J.W., Kominers S.D. A Simple Theory of Vampire Attacks // SSRN-Elsevier, 2023. https://ssrn.com/abstract=4377561. DOI: 10.2139/ssrn.4377561.

[3] Channawar P.M., Chavan Y.V. Vampire Attack: Energy Efficient Trust Based Solution // International Journal of Science and Research (IJSR). 2012. Т. 3, Вып. 12. С. 314-317.

[4] Juneja V., Dinkar S.K. An Approach against Vampire Attack for Successful Transmission in Wireless Sensor Network // 2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT). 2023. С. 1-7.

[5] Alkwai L., Aledaily A., Almansour S., Alotaibi S., Yadav K., Lingamuthu V. Vampire attack mitigation and network performance improvement using probabilistic fuzzy chain set with authentication routing protocol and hybrid clustering-based optimization in wireless sensor network // Hindawi, Mathematical Problems in Engineering. 2022. № 4948190. С. 1-11.

[6] Srikaanth P.B., Nagarajan V. Fuzzy rough set derived probabilistic variable precision-based mitigation technique for vampire attack in MANETs // Wireless Personal Communications. Springer. 2021. Т. 121. С. 1085–1101.

[7] Verma V., Jha V.K. Detection and prevention of vampire attack for MANET // Nanoelectronics, Circuits and Communication Systems. Lecture Notes in Electrical Engineering, Springer. 2021. Т. 692. С. 81–90.

[8] Desnitsky V., Kotenko I. Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures // Simulation Modelling Practice and Theory. 2021. № 102244. С. 107.