УДК 004.056.5

МОДЕЛИРОВАНИЕ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ ТИПА DENIAL-OF-SLEEP В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

В.А. Десницкий, кандидат технических наук;
Н.Н. Рудавин.
Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Представлены результаты моделирования и анализа атакующих воздействий типа Denial-of-Sleep на узлы беспроводной сенсорной сети. Особенность моделируемой атаки состоит в том, что нарушитель воздействует при помощи модуля-паразита на некоторый легитимный узел, который эксплуатируется для отправки нелегитимных запросов на автономно работающие узлы беспроводной сенсорной сети. По результатам моделирования определены возможные перспективные меры для противодействия данному виду атак, которые применимы, в том числе для повышения защищенности беспроводных коммуникационных сетей оперативного управления и реагирования в чрезвычайных ситуациях.

Ключевые слова: атака типа Denial-of-Sleep, беспроводная сенсорная сеть, моделирование атак

MODELING OF DENIAL-OF-SLEEP ATTACKS IN WIRELESS SENSOR NETWORKS

V.A. Desnitsky; N.N. Rudavin.
Saint-Petersburg institute of informatics and automation of the Russian academy of sciences

The paper comprises results of modeling and analysis of Denial-of-Sleep attacks on nodes of a wireless sensor network. A feature of the modeled attack is that the intruder acts with the help of a parasite module on some legitimate node, which is used to send illegitimate requests to autonomously working sensor nodes. Based on the modeling results, possible promising measures have been identified to counter this type of attack. The obtained results are applicable in a range of systems to increase their security, including wireless communication networks of operational control and response in emergency situations.

Keywords: Denial-of-Sleep attack, wireless sensor network, attack modeling

Атаки, направленные на истощение энергоресурсов автономно работающих устройств, представляют существенную угрозу безопасности современных беспроводных сенсорных сетей (БСС). Данный вид атак характеризуется относительной легкостью их осуществления – для успешной атаки зачастую нарушителю достаточны лишь минимально необходимые программно-аппаратные средства, небольшие навыки программирования, работы с микроконтроллерами и другим современным телекоммуникационным оборудованием. Возникновение атак истощения энергоресурсов в критически важных киберфизических системам и сетях, таких как программно-технические комплексы управления и реагирования в чрезвычайных ситуациях, может приводить к серьезным и даже катастрофическим последствиям техногенного и социального характера. Сложность обнаружения атак истощения энергоресурсов и их предотвращения во много связана с недостаточным развитием инструментов анализа процессов расхода

энергоресурсов в динамике и сопоставления увеличения расхода заряда с возможными действиями нарушителей.

В статье проводятся моделирование и анализ атаки типа Denial-of-Sleep – разновидности атак истощения энергоресурсов, при которой нарушитель формирует атакующие пакеты данных и маскирует их под нормальный трафик, используя некоторый скомпрометированный узел БСС. К данному узлу подключается атакующий модуль «паразит», способный заставить эксплуатируемый узел генерировать атакующий трафик на другие узлы сети и истощать их энергоресурсы. Эксперименты на физической реализации БСС показывают практическую выполнимость данного вида атак. Кроме того, результаты экспериментов используются также для анализа возможных контрмер. К основным элементам новизны настоящей работы относятся модель атакующего воздействия со специфичным набором параметров атаки, результаты сравнений и комбинирования нормального и атакующего трафика, а также интерпретация результатов визуального анализа такого комбинирования с использованием графических представлений.

Атака типа Denial-of-Sleep применима к устройствам, работающим автономно, от исчерпаемого источника электропитания, и имеющим два режима работы – режима полного функционирования и, так называемого, «режима сна», в который устройство переводится на определенные промежутки времени. Как правило, данный режим применяется на удаленных физически или перемещающихся в пространстве устройствах для экономии энергии при условии, что ежесекундная связь с устройством не требуется. В режиме сна в целях энергоэффективности наиболее энергозатратные функции устройства отключаются с последующим возвращением в режим полного функционирования через заданный промежуток времени для обработки вновь поступивших запросов и выполнения других операций. При реализации Denial-of-Sleep атаки цель нарушителя – не допустить переход узла-жертвы в спящий режим, чтобы увеличить расход энергоресурсов данного узла. Суть атаки состоит в том, что из-за более частых запросов конечные устройства вынуждены чаще отвечать и поэтому не успевают уйти в спящий режим, расходуя дополнительный заряд батареи.

В качестве модели атакуемой сети выбрана БСС на базе модулей Digi XBee v2. Оконечные устройства такой сети способны работать в спящем режиме, тогда как роутеры и координирующий узел поддерживают только полнофункциональный режим работы. Оконечные узлы и роутеры включают в свой состав: модуль беспроводной передачи данных XBee, микроконтроллер Arduino UNO, GPS-модуль, комбинированный аппаратный интерфейс управления для отправки и приёма данных, а также элементы ввода-вывода пользовательских данных.

На базе сенсорной сети произведено моделирование нормальной работы сети с целью проверки влияния атак на процесс истощение энергоресурсов, а также для оценки возможности пресечения подобных атак. В процессе моделирования нормальной работы сети производится обмен данными между узлами сети. В рамках эксперимента, не умаляя общности, узлы сети осуществляют коммуникацию лишь при помощи запросов GPS-координат и ответов на них. Так, предполагается, что пользователи или сервисы конечных узлов запрашивают местоположение других узлов сети и анализируют эти данные в рамках своих операционных процессов, в том числе для обеспечения свойств доступности сети [1]. Технически информация о местоположении приходит на узел после отправки этим узлом запросов на другие узлы с определенной периодичностью и в определенном количестве [2].

Вместе тем предполагаем, что все прикладные сообщения отправляются группами – «пачками» с известными частотными характеристиками интервала между пачками, числа сообщений в пачке, интервалами между сообщениями в пачке и допустимыми максимальными отклонениями от этих значений. Каждое из сообщений в пачке может отвечать за запрос GPS-данных либо узла, на который поступил данный запрос, либо узла, располагающегося далее по сети, и коммуникация с которым осуществляется через данный

узел. Примеры используемых в процессе моделирования комбинаций параметров нормального трафика показаны в таблице. Для каждого из трех параметров трафика при помощи обозначений L и H эвристически определено по два варианта значений – малое и большое, соответственно. В качестве примера, конкретный набор из трех параметров трафика указывается в виде LLH, которому соответствует формальная тройка (5 000 мс, 5 шт, 2 000 мс).

Таблица. **Параметры моделируемого трафика**

Режим настройки	Выбранная настройка					
	1		2		3	
	Интервал между пачками (мс)	Максимальное отклонение (+/-)	Число сообщений в пачке	Максимальное отклонение (+/-)	Интервал между сообщениями в пачке (мс)	Максимальное отклонение (+/-)
L	5000	500	5	2	500	167
H	20000	2000	20	8	2000	666

В рамках эксперимента моделируемая сеть имеет следующие основные элементы:

– узел-координатор, необходимый для обеспечения стабильной работы сети – через Serial-интерфейс подключен к координирующему компьютеру;

– узел-жертва, который представляет оконечный узел сети, состоящий из микроконтроллера Arduino, XBee модуля и автономного источника питания. Для экономии энергоресурсов узел на время простоя переводится в спящий режим. Дополнительно, для обеспечения процесса моделирования атаки, узел подключается через USB-интерфейс к ЭВМ для перехвата входящего трафика и его последующего анализа;

– типовой эксплуатируемый нарушителем узел сети, к отличительным особенностям которого можно отнести, во-первых, наличие на нём аппаратного интерфейса настройки его работы, во-вторых, реализацию программируемой функции отправки сообщений узлу-жертве, в-третьих, возможность подключения к нему атакующего модуля-паразита, инициирующего атаку [3]. Схема устройства такого узла показана на рис. 1;

– модуль-паразит, подключающийся к эксплуатируемому модулю для инициации отправки от его имени атакующего трафика.

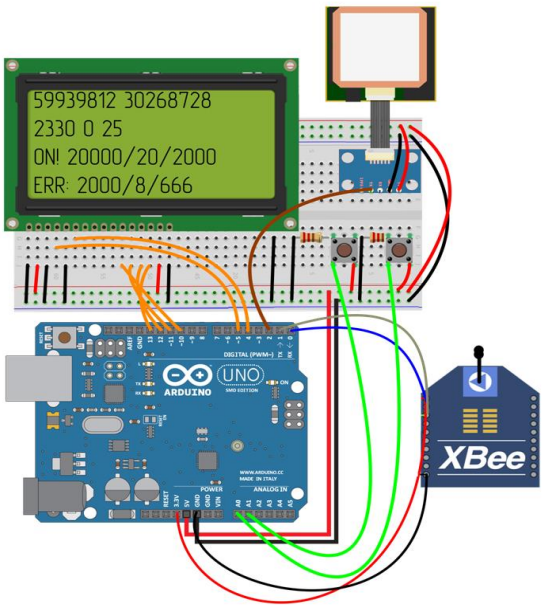

Рис. 1. **Схема эксплуатируемого нарушителем узла**

На рис. 1 индикатор показывает текущие GPS-данные узла: в первых двух строках – широту, долготу, направление, скорость, высоту, в нижних двух строках – параметры отправки сообщений со значениями параметров, соответствующих значениям в таблице.

Моделируется следующий сценарий атаки на узел сети. Нарушитель подсоединяет устройство-паразит к эксплуатируемому узлу при помощи подключения к его Serial-интерфейсу. Схема подключения показана на рис. 2. Сообщения паразита (слева) передаются через виртуальный Serial-порт (аппаратный пин № 2) на эксплуатируемый узел (справа) через Serial-порт, используемый для обмена данным с сетью посредством модуля XBee (пин № 0).

Паразит начинает генерировать пакеты данных с заданной частотой – пакеты, схожие по своей структуре с пакетами-запросами GPS-координат. При этом устройство-паразит указывает в поле отправителя адрес узла-жертвы. В эксперименте это производится автоматически, причем интервал настраивается с шагом 100 мс. В рамках эксперимента паразит также имеет свой аппаратный интерфейс – LED-экрана и две тактовые кнопки для ввода параметра интервала для настройки параметров генерации атакующего трафика.

В свою очередь, эксплуатируемый модуль, к которому подключен паразит, принимает поступающие запросы и отправляет узлу-жертве пакеты со своими координатами. По сути, это позволяет производить атаку пакетами, не имеющими явной аномальной структуры. В результате будет затруднена фильтрация узлом-жертвой таких пакетов, так как они имеют нормальную структуру и целостность пакетов формально не нарушена.

Отметим, что узел-жертва одновременно принимает и легитимные пакеты как с других узлов сети, так и инициированные модулем-паразитом. В результате такой атаки при достаточно частом интервале между пакетами динамически определяемый параметр ST – промежуток времени сна узла-жертвы уменьшается, и он перестает «засыпать», потребляя значительно больше энергоресурсов в процессе своего функционирования.

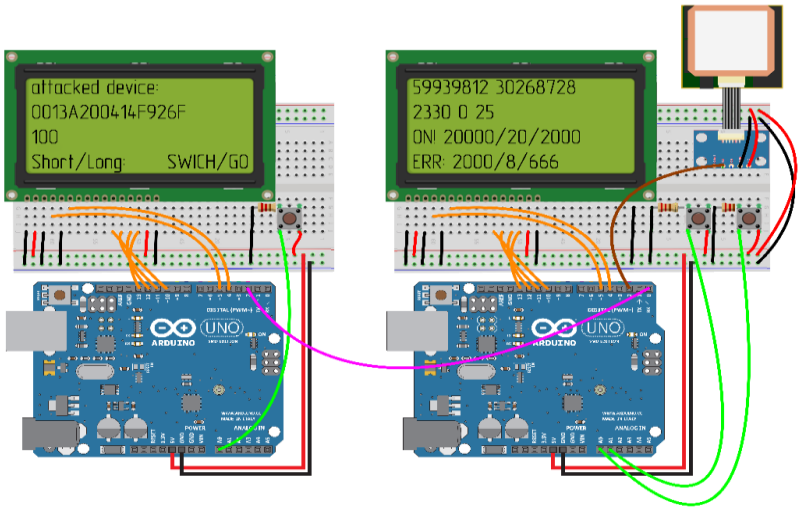

Рис. 2. **Моделирование подключения узла-паразита к эксплуатируемому узлу**

В рамках эксперимента с узла-жертвы произведены записи поступающего на него нормального трафика, чем подтверждена корректность работы разработанных программных прошивок микроконтроллеров. Число вариантов записей трафика составляет 8, что согласно допустимым значениям из таблицы соответствует всем возможным режимам работы узла. Визуальное представление нормального трафика приведено на рис. 3.

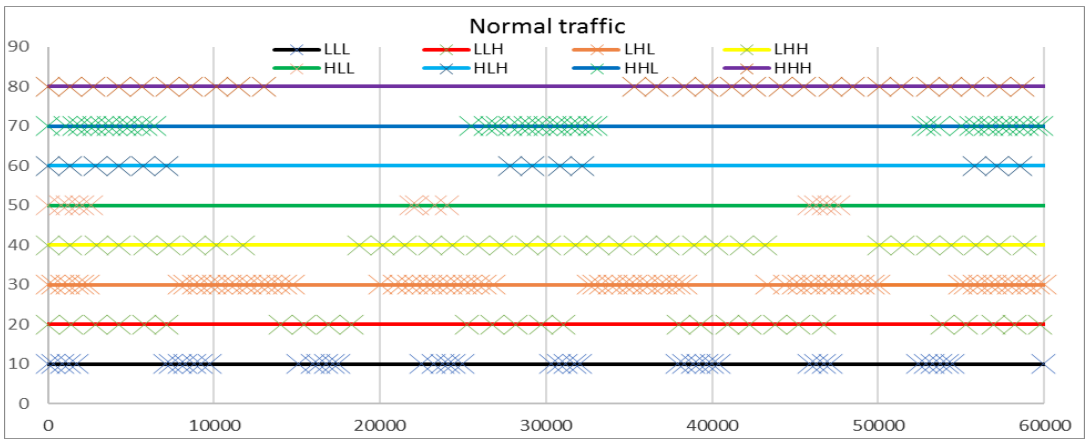

Рис. 3. **Запись нормального трафика**

На рис. 3 на горизонтальной оси показано время в миллисекундах, а на вертикальной – перечень моделей трафика, соответствующих таблице. В частности, на диаграмме видно, что наиболее активно спящий режим используется в режимах HLL и HLH, так как там сообщения передаются редко и в достаточно малых количествах. Поэтому применение спящего режима сократит энергопотребление в несколько раз. И, в результате, устройства, работающие на этих режимах, будут более уязвимы перед атакой типа Denial-of-Sleep. Атака производится с интенсивностью, схожей с интенсивностью отправки сообщений в нормальном режиме работы. Во-первых, это позволяет нарушителю максимально замаскироваться под реальный трафик. Во-вторых, нарушителю нет необходимости отправлять сообщения чаще, поскольку предполагается, что параметры спящего режима должны быть уже настроены так, чтобы конечное устройство не «засыпало» пока продолжается сеанс связи. Результаты моделирования атаки показаны на рис. 4.

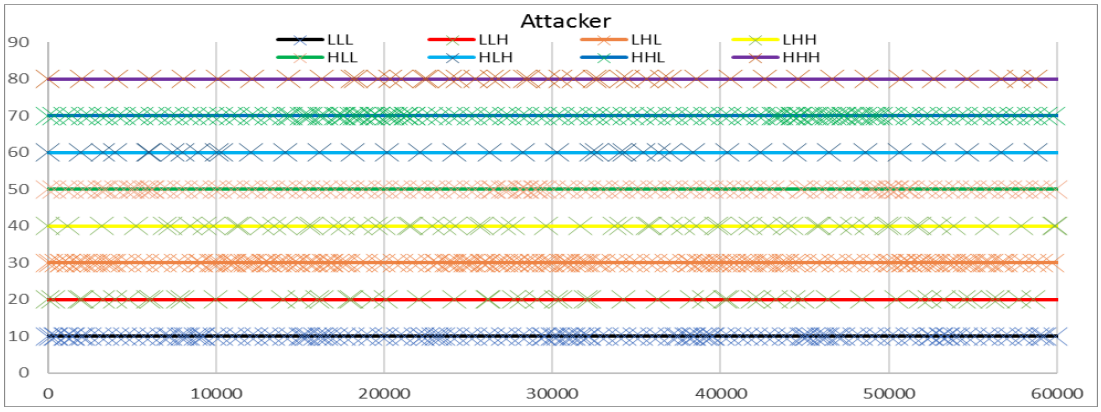

Рис. 4. **Запись трафика с атакой**

Полное отсутствие непересеченных длинных отрезков для всех восьми режимов свидетельствует об успешном моделировании атаки. По сути, все пакеты, отправленные атакующим устройством-паразитом, были распознаны как нормальный трафик и переданы узлу-жертве. В целом за исключением тонкостей реализации и преследуемой цели данная атака имеет некоторую схожесть с классическими DoS-атаками на беспроводные сенсорные сети, но в качестве специфики действует не посредством поражения пропускной способности коммуникационных каналов, а через истощение батареи, что может достаточно сложно поддаваться отслеживанию.

Проанализируем некоторые возможные контрмеры. Для защиты от исследуемой разновидности Denial-of-Sleep атак возможно применение схемы, описанной в работе [4] в качестве средств противодействия истощению энергоресурсов сенсорной сети. В частности, в работе [4] предложен комплексный подход к параллельному обнаружению и пресечению действий нарушителя. Однако следует учесть, что в рассматриваемом в настоящей работе сценарии нарушитель эксплуатирует легитимный модуль, при помощи которого осуществляются формирование и отправка атакующего трафика. Этот модуль может являться критически важным элементом сети, и в случае, если атаку удастся распознать, то в качестве меры противодействия простое отключение данного узла может привести даже к более серьезным негативным последствиям, таким как нарушение доступности БСС. Поэтому при разработке средств защиты от атак истощения энергоресурсов важным фактором должно быть недопущение доступа и проникновения атакующего на каждый элемент сети, в особенности критически важный. Например, подобно предложенному в работе [5] решению, позволяющему осуществить кластеризацию сети, для повышения уровня защищенности от Denial-of-Sleep атак возможно наложить специальные ограничения на узлы-роутеры. В частности, эти ограничения позволят ввести запрет на взаимодействие роутеров с конечными устройствами сети, находящимися, в особенности, вне зоны прямой радиосвязи. Поэтому даже в случае успешной реализации атаки, она сможет поразить лишь некоторую часть их имеющихся устройств сети.

Кроме того, основываясь на примере реализации контрмер, предложенных в работе [6], для защиты от рассматриваемого типа атак можно применять серию мер противодействия непосредственно на конечных устройствах. В частности, возможны принудительное снижение мощности антенного устройства или ввод в спящий режим в случае подозрения или точного детектирования атаки в рамках полномочий самого конечного устройства.

Возможно также разработать определенные шаблоны взаимодействия, сверяя которые, конечные устройства смогут обнаруживать атакующий трафик с определенной точностью [7]. Еще одним перспективным решением представляется ведение статистики трафика устройствами-роутерами и передача её на координирующий компьютер, который будет определять наличие атаки и место ее возникновения, а также принимать меры ее пресечения посредством предложенных решений.

Перечисленные возможные направления противодействия могут быть использованы для разработки новых и совершенствования существующих средств противодействия атакующим воздействиям в различных киберфизических системах, в том числе в коммуникационных сетях оперативного управления и реагирования в чрезвычайных ситуациях.

В настоящей работе проведены анализ и моделирование атак типа Denial-of-Sleep атак на БСС. На разработанном программно-аппаратном прототипе осуществлено моделирование Denial-of-Sleep атаки, проведены эксперименты и проанализированы возможные контрмеры. В качестве будущих направлений исследований планируются аналитическое и имитационное моделирование атак истощения энергоресурсов путем введения в действие нарушителем намеренно некорректных или неоптимальных настроек программно-аппаратного обеспечения, а также определение эффективности таких атак, их сложности и сравнения с другими видами атак истощения энергоресурсов.

Работа выполнена при финансовой поддержке гранта Российского Фонда Фундаментальных Исследований (РФФИ) № 19-07-00953.

Литература

1. Desnitsky V., Kotenko I., Rudavin N. Ensuring Availability of Wireless Mesh Networks for Crisis Management // Intelligent Distributed Computing XII. Studies in Computational Intelligence. Springer-Verlag. 2018. Vol. 798. P. 344–353.

2. Desnitsky V., Kotenko I. Security event analysis in XBee-based wireless mesh networks // Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2018). 2018. P. 42–44.

3. Vasserman E.Y., Hopper N. Vampire attacks: draining life from wireless ad hoc sensor networks // IEEE transactions on mobile computing. 2013. Vol. 12. Issue 2. P. 318–332.

4. Du X., Samachisa A., Hei X., Lukowiak M. Defending resource depletion attacks on implantable medical devices // Global telecommunications conference (GLOBECOM 2010), IEEE. 2010. P. 1–5.

5. Shakhov V., Koo I., Rodionov A. Energy exhaustion attacks in wireless networks // Engineering, Computer and Information Sciences (SIBIRCON), Proceedings of 2017 International Multi-Conference on, IEEE. 2017. P. 1–3.

6. Shakhov V., Koo I. Depletion-of-Battery Attack: Specificity, Modelling and Analysis // Sensors. 2018. Vol. 18. Issue 6. P. 1849.

7. Hsueh C.T., Wen C.Y., Ouyang Y.C. A secure scheme for power exhausting attacks in wireless sensor networks // Proceedings of 2011 IEEE Third International Conference on Ubiquitous and Future Networks (ICUFN). 2011. P. 258–263.

References

1. Desnitsky V., Kotenko I., Rudavin N. Ensuring Availability of Wireless Mesh Networks for Crisis Management // Intelligent Distributed Computing XII. Studies in Computational Intelligence. Springer-Verlag. 2018. Vol. 798. P. 344–353.

2. Desnitsky V., Kotenko I. Security event analysis in XBee-based wireless mesh networks // Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2018). 2018. P. 42–44.

3. Vasserman E.Y., Hopper N. Vampire attacks: draining life from wireless ad hoc sensor networks // IEEE transactions on mobile computing. 2013. Vol. 12. Issue 2. P. 318–332.

4. Du X., Samachisa A., Hei X., Lukowiak M. Defending resource depletion attacks on implantable medical devices // Global telecommunications conference (GLOBECOM 2010), IEEE. 2010. P. 1–5.

5. Shakhov V., Koo I., Rodionov A. Energy exhaustion attacks in wireless networks // Engineering, Computer and Information Sciences (SIBIRCON), Proceedings of 2017 International Multi-Conference on, IEEE. 2017. P. 1–3.

6. Shakhov V., Koo I. Depletion-of-Battery Attack: Specificity, Modelling and Analysis // Sensors. 2018. Vol. 18. Issue 6. P. 1849.

7. Hsueh C.T., Wen C.Y., Ouyang Y.C. A secure scheme for power exhausting attacks in wireless sensor networks // Proceedings of 2011 IEEE Third International Conference on Ubiquitous and Future Networks (ICUFN). 2011. P. 258–263.