ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

УДК 004.056
DOI: 10.17586/0021-3454-2018-61-4-291-297

АНАЛИЗ АТАК ИСТОЩЕНИЯ ЭНЕРГОРЕСУРСОВ НА СИСТЕМЫ БЕСПРОВОДНЫХ УСТРОЙСТВ

В. А. Десницкий[1], И. В. Котенко[1,2]

[1]*Санкт-Петербургский институт информатики и автоматизации РАН, 199178,Санкт-Петербург, Россия*

[2]*Университет ИТМО, 197101, Санкт-Петербург, Россия*
E-mail: ivkote@comsec.spb.ru

В настоящее время все большее значение приобретает проблема подверженности устройств современных беспроводных сетей Интернета вещей атакам, направленным на истощение энергоресурсов (атакам истощения энергоресурсов). Будучи скрытными для самого объекта и систем мониторинга защищенности, такие атаки способны за достаточно короткий период исчерпать энергоресурс устройства и тем самым нарушить его работоспособность и доступность. Проанализированы возможные виды атак истощения энергоресурсов, предложена обобщенная модель нарушителя применительно к данному виду атак, проведены экспериментальные исследования на основе двух разработанных программно-аппаратных стендов моделирования с использованием программно-аппаратных устройств на базе платформ Android 5.1 и Digi XBee v2.

Ключевые слова: *информационная безопасность, атаки истощения энергоресурсов, моделирование, анализ, Интернет вещей*

К основным особенностям атак, направленных на снижение заряда аккумуляторной батареи автономно функционирующего (в течение дней, месяцев или даже нескольких лет) устройства (атак истощения энергоресурсов, ИЭ-атак), можно отнести сложность их обнаружения, относительную эффективность и вариативность. Сложность обнаружения ИЭ-атак вызвана, во-первых, тем, что на атакуемое устройство воздействуют, как правило, не напрямую, а опосредованно — путем отправки на него через сеть Интернет или некоторый локальный коммуникационный порт серии ложных запросов, которые не всегда возможно идентифицировать как атакующие. Во-вторых, для того чтобы отслеживать ИЭ-атаки, нужно фиксировать не только процесс разряжения батареи, но также изменения скорости разрядки. В-третьих, обнаружение ИЭ-атак могут осложнять объективные факторы: разрядка батареи может быть связана с действиями самого пользователя.

Целями настоящей статьи являются анализ работ, посвященных возможным видам ИЭ-атак на устройства систем Интернета вещей, построение обобщенной модели нарушителя, выполняющего ИЭ-атаки, а также моделирование ИЭ-атак и анализ их эффективности. Такие атаки оказываются особенно актуальными для систем автономно работающих коммуникационно-вычислительных устройств в условиях невозможности, сложности или нецелесообразности оперативного восполнения потребленного заряда без приостановки ключевых функций устройств, в том числе для программно-технических комплексов управления и

реагирования в чрезвычайных ситуациях, характеризующихся повышенными требованиями к показателям надежности и бесперебойности целевых функций системы.

В работе [1] анализируются некоторые виды ИЭ-атак на беспроводные интерфейсы Wi-Fi и Bluetooth, чтобы понять их влияние на сроки службы батареи. В статье [2] описана система защиты от атаки типа *Battery-Sensing Intrusion Protection System* (B-SIPS) на истощение батареи для мобильных компьютеров. Система предупреждает об изменениях мощности обнаруженных атак на небольших беспроводных устройствах, используя алгоритм динамического расчета Threshold. В [3] предлагается механизм создания эффективной защиты от атак типа Sleep Deprivation, Barrage, Replay, Broadcast, Collision and Synchronization attacks [3], направленных на истощение батареи с использованием сетевого взаимодействия на стыке физического и канального уровней. В [4] описывается реализация атаки истощения батареи путем эксплуатации уязвимостей mms-сообщений (Multimedia Messaging Service) мобильных устройств. Злоумышленник собирает список мобильных устройств (в том числе их сотовые номера, IP-адреса, а также сведения о модели за счет использования сообщений, уведомления mms), а затем истощает заряд батареи устройства, периодически посылая UDP-пакеты с использованием сохраненных контекстов PDP и канала поискового вызова.

Выделяются следующие четыре класса ИЭ-атак: *принудительный вывод устройств из сна* (режима пониженного энергопотребления) атакой типа Denial-of-Sleep [1, 2]; *атака увеличения объема* входящего или исходящего трафика, выполняющаяся без необходимой в иных случаях авторизации нарушителя на атакуемом устройстве; *создание электромагнитных помех на беспроводных каналах* передачи данных, вынуждающих устройства генерировать сигнал повышенной мощности для передачи данных [6]; *нештатное использование ПО* устройств, включающее множественный запуск приложений, нарушение оптимизаций. Атаки нештатного использования ПО, включающие активацию энергозатратных функций и модулей устройства, например, принудительное включение GPS-датчика, предполагают предварительное установление удаленного доступа. В настоящей работе проведен детальный анализ условий выполнимости атак, определены цели нарушителя и способы их достижения, а также особенности атакующих воздействий и условия успешного выполнения атак. На основе анализа имеющейся информации авторами построена модель нарушителя.

Модель представляется следующим формальным кортежем (G, O, A, R, C, E). Элемент G определяет цели ИЭ-атак: выведение из строя некоторого устройства, работающего от автономного источника питания, цели в зависимости от специфики устройств системы и мотивов нарушителя цель могут достигаться постепенно или стремительно. O задает объекты прямого и опосредованного воздействия ИЭ-атак: сенсоры, считывающие характеристики физического окружения устройства, коммуникационные каналы, программные компоненты, процессы операционной системы устройства и пр. A — последовательность действий атакующего для достижения цели G. R — необходимые системные ресурсы, оборудование и инструменты, используемые при атаке, знания и практические навыки нарушителя, которыми он должен обладать, а также требуемое время проведения атаки. C — характеристики взаимодействия нарушителя с атакуемым устройством [5]. E определяет эффективность атаки — среднее увеличение скорости разрядки батареи, вызванной атакой, по отношению к нормальному (штатному) режиму работы.

Все элементы модели нарушителя, кроме E, могут быть определены аналитически. Найти E можно лишь экспериментально. С этой целью были построены два программно-аппаратных стенда моделирования. Оба стенда характеризуются различными типами и спецификой атакуемых устройств, видами беспроводных сетевых протоколов, реализованными возможностями по программному и программно-аппаратному съему данных об энергопотреблении.

Стенд *„Мобильная сеть“* представляет собой фрагмент TCP/IP-сети, объединяющей мобильные устройства при помощи беспроводных коммуникационных протоколов, таких как Bluetooth и Wi-Fi. Эти устройства предназначены для организации коммуникации с другими устройствами с помощью программных приложений. Для устройств, работающих в TCP/IP-сети, наиболее опасны атаки, направленные на увеличение объема трафика. Также выполняются атаки, предполагающие повышение общего уровня шума или экранирование электромагнитных волн. В рассматриваемом случае атаки нештатного использования ПО сложны в реализации.

На рис. 1 продемонстрирован ход атаки принудительного перевода мобильного смартфона LG Nexus 5 под управлением ОС Android 5.1 в более энергозатратный режим путем эксплуатации его беспроводного коммуникационного интерфейса. Смоделирована атака на модуль Bluetooth-устройства с использованием средств ОС Kali Linux, запущенных на атакующем ноутбуке. Атака основана на выполнении утилиты *Bluetoothctl*, используемой для обнаружения атакуемого устройства и получения информации о нем, и *l2ping*, при помощи которой выполняется последовательная отправка ping-запросов.

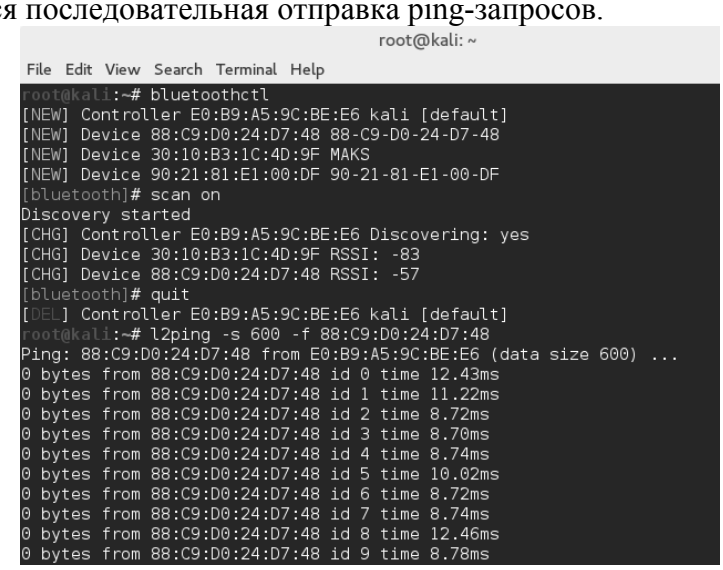

Рис. 1

Расход батареи определяется программно путем обращения к переменной *BatteryManager.EXTRA_LEVEL* (*Q*), определяющей уровень заряда. Результаты измерений в нормальном режиме *1* и при атаке *2* показаны на рис. 2.

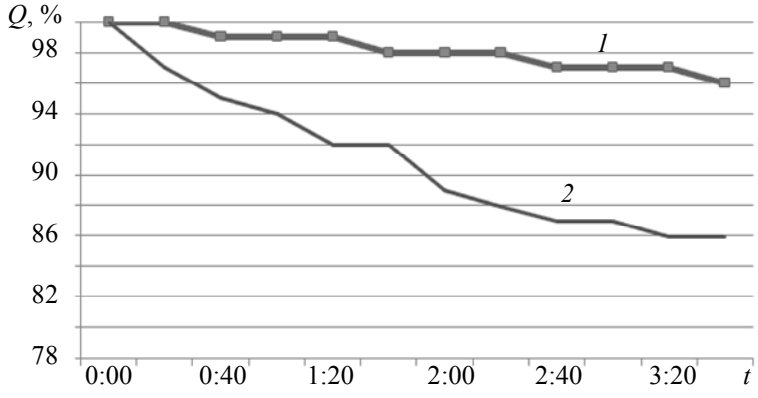

Рис. 2

На основе представленных на рис. 2 значений показатель эффективности атаки *E* вычислялся как отношение изменения заряда при атаке к изменению заряда в нормальном режиме за анализируемый промежуток времени (отметим, что этот способ позволяет получить лишь грубые оценки значений *E*). В качестве альтернативы могут использоваться программные профилировщики, позволяющие получать более точные данные, однако такие средства

сами могут быть достаточно энергоемкими. Помимо этого, не все модели мобильных устройств имеют встроенные средства точного измерения потребляемого тока.

Стенд *„Беспроводная самоорганизующаяся сеть на основе протокола ZigBee“* представляет собой самоорганизующуюся ZigBee-сеть, ключевым элементом которой являются беспроводные модули Digi XBee серии 2. Модуль XBee может выступать в роли координатора сети, маршрутизатора или конечного (терминального) устройства. XBee настраивается на получение и последующую отправку данных от подключаемых к нему сенсоров. Модуль XBee в роли конечного устройства поддерживает режим сна, наличие которого обусловливает его подверженность атакам типа Denial-of-Sleep.

Помимо Denial-of-Sleep-атаки на модули XBee может быть выполнена атака увеличения объема трафика атака с созданием электромагнитных помех. Возможность атак нештатного использования ПО устройств ограничена, поскольку нарушители могут лишь настраивать конфигурационные параметры атакуемого модуля при прямом физическом подключении к нему.

На стенде „Беспроводная самоорганизующаяся сеть на основе протокола ZigBee“ была продемонстрирована комбинированная атака на конечный узел XBee (рис. 3), функционирующий в режиме энергосбережения с запланированной периодичностью перехода из режима сна в режим нормального функционирования. Атака осуществляется путем отправки запросов со стороны ложного XBee-узла. В условиях эксперимента на целевом узле заданы следующие настройки: режим цикличного сна, время работы ST = 1000 мс и время одного цикла сна SP = 10 000 мс.

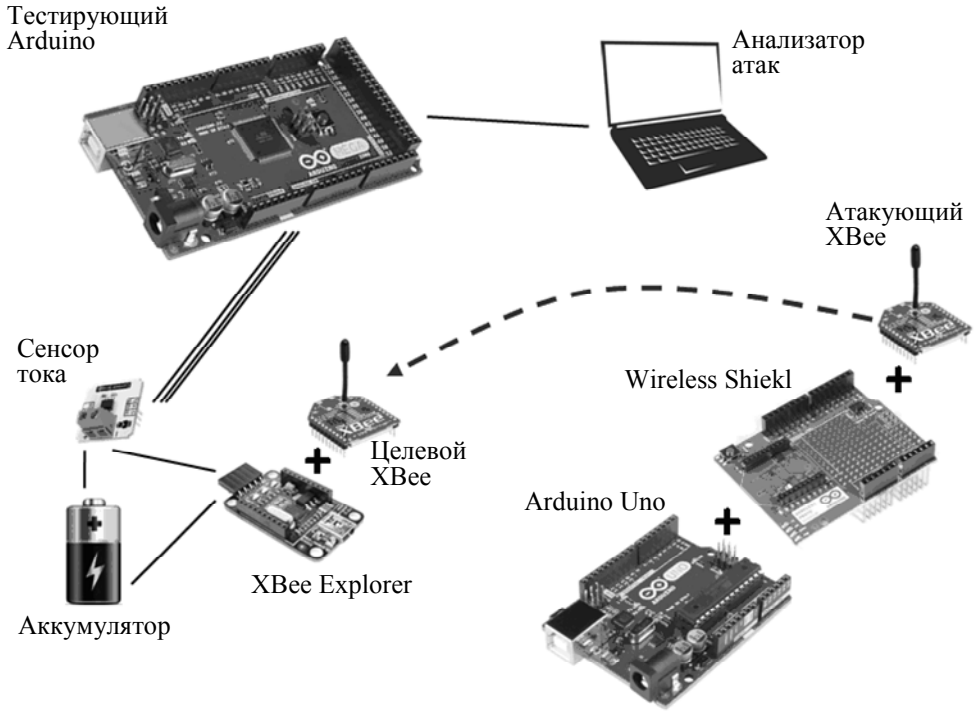

Рис. 3

Действия нарушителя, эксплуатирующего ложный узел XBee, состоят в регулярной отправке на атакуемый узел сообщений (два в секунду), которые будут обнулять таймер ST, не давая узлу перейти в состояние сна. Особенность этой атаки состоит в том, что помимо препятствования переходу целевого узла в режим сна, дополнительное энергопотребление происходит также в результате нахождения в режиме ST вместо режима SP.

Стенд включает модуль XBee серии 2 ZB с профилем End Device, являющийся объектом атаки. К разъему питания данного модуля подсоединен датчик тока на базе микроконтроллера Allegro ACS712. По отдельному управляющему каналу от датчика сведения о текущем по-

треблении тока считываются тестирующим микроконтроллером Arduino Mega 2560. После этого данные измерений тока в виде логов передаются через UART-интерфейс микроконтроллера на персональный компьютер для последующей обработки и анализа. Атакующий узел сети включает микроконтроллер Arduino Uno R3, к которому подсоединен XBee-модуль. На Uno загружен программный код прошивки, регулярно отправляющий данные по заданному адресу ZigBee-сети. Результаты измерений потребления тока в режиме простоя с регулярным переходом в режим сна на период SP и в случае атаки приведены в таблице (приведены усредненные данные на один цикл ST продолжительностью 1 с — сон продолжительностью 10 с).

Результаты энергопотребления XBee в нормальном режиме и при атаке

Потребляемый ток, мА	Промежутки времени, мс	
	0—1000	1000—11000
I_{norm}	45	8
I_{attack}	51	51

При допущении, что интенсивность атаки неизменна на всем ее протяжении, потребление в режиме атаки является постоянным: $I_{\text{attack}} = 51\,\text{мА}$, потребление в режиме сна составляет 8 мА. В результате эффективность такой атаки рассчитывается по формуле $E = I_{\text{attack}}(t_2 - t_1) / \int_{t_1}^{t_2} I_{\text{norm}}(t)dt$, потребление в режиме простоя I_{norm} определяется путем вычисления определенного интеграла по заданному интервалу времени, который вычисляется с использованием интерполяции по Лагранжу. Эксперимент проводился циклично на интервале времени $t_2 - t_1 = 600\,\text{с}$. Полученная эффективность $E = 4,488$ означает, что такая атака способна более чем в четыре раза быстрее исчерпать оценочное время работы батареи узла XBee в условиях заданных параметров режима сна.

Таким образом, вариативность ИЭ-атак определяется разнообразием способов воздействий на наиболее энергозатратные модули устройств с целью незапланированного повышения интенсивности их использования. Требование бесперебойной работы устройств делает такие атаки особенно опасными.

Рассмотренный процесс обнаружения ИЭ-атак является специфичным конкретному виду устройств Интернета вещей. Общий подход к обнаружению должен включать детальное отслеживание процесса энергопотребления, а также анализ логов перехода устройств и программных и аппаратных модулей между различными режимами их работы, запуска и приостановки программных приложений, обращений к носителям данных и пр. [7]. Все эти данные должны использоваться для генерации событий и проверки выполнимости правил корреляции с целью выявления признаков ИЭ-атак.

Эксперименты демонстрируют возможность внедрения в процесс разработки систем Интернета вещей методик анализа типовых ИЭ-атак с их моделированием на физическом оборудовании и последующей разработкой специализированных компонентов защиты против таких атак на основе предложенного авторами подхода [8, 9].

Работа выполнена при финансовой поддержке РФФИ (проекты 16-29-09482 и 18-07-01488) по бюджетной теме № АААА-А16-116033110102-5.

СПИСОК ЛИТЕРАТУРЫ

1. *Moyers B. R., Dunning J. P., Marchany R. C., Tront J. G.* Effects of Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices // Proc. of 43rd Hawaii Intern. Conf. on System Sciences. 2010. P. 1—9. DOI: 10.1109/HICSS.2010.170.

2. *Buennemeyer T. K., Gora M., Marchany R. C., Tront J. G.* Battery Exhaustion Attack Detection with Small Handheld Mobile Computers // Proc. of IEEE Intern. Conf. on Portable Information Devices. 2007. P. 1—5. DOI: 10.1109/PORTABLE.2007.35.

3. *Boubiche D. E., Bilami A.* A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks // J. of Emerging Technologies in Web Intelligence. 2013. Vol. 5, N 1. P. 18—27.

4. *Racic R., Chen D. M., Chen H.* Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery // Proc. of 2006 SecureComm and Workshops. 2006. P. 1—10. DOI: 10.1109/SECCOMW.2006.359550.

5. *Abraham D. G., Dolan G. M., Double G. P., Stevens J. V.* Transaction security system // IBM Systems J. 1991. Vol. 30, N 2. P. 206—228. DOI: 10.1147/sj.302.0206.

6. *Karpagam R., Archana P.* Prevention of Selective Jamming Attacks Using Swarm intelligence Packet-Hiding Methods // Intern. J. of Engineering and Computer Science. 2013. Vol. 2. P. 2774—2778.

7. *Десницкий В. А., Котенко И. В.* Модель конфигурирования защищенных и энергоэффективных встроенных систем // Изв. вузов. Приборостроение. 2012. Т. 55, № 11. С. 52—57.

8. *Chechulin A., Kotenko I., Desnitsky V.* An approach for network information flow analysis for systems of embedded components // Lecture Notes in Computer Science. 2012. Vol. 7531. P. 146—155. DOI: 10.1007/978-3-642-33704-8_13.

9. *Desnitsky V., Chechulin A., Kotenko I., Levshun D., Kolomeec M.* Application of a technique for secure embedded device design based on combining security components for creation of a perimeter protection system // Proc. of 24th Euromicro Intern. Conf. on Parallel, Distributed, and Network-Based Processing (PDP 2016). 2016. P. 609—616. DOI: 10.1109/PDP.2016.99.

Сведения об авторах

Василий Алексеевич Десницкий — канд. техн. наук; Санкт-Петербургский институт информатики и автоматизации РАН, лаборатория проблем компьютерной безопасности; E-mail: desnitsky@comsec.spb.ru

Игорь Витальевич Котенко — д-р техн. наук, профессор; Санкт-Петербургский институт информатики и автоматизации РАН, лаборатория проблем компьютерной безопасности; Университет ИТМО; E-mail: ivkote@comsec.spb.ru

Поступила в редакцию
08.09.17 г.

Ссылка для цитирования: *Десницкий В. А., Котенко И. В.* Анализ атак истощения энергоресурсов на системы беспроводных устройств // Изв. вузов. Приборостроение. 2018. Т. 61, № 4. С. 291—297.

ANALYSIS OF ENERGY RESOURCE DEPLETION ATTACKS ON WIRELESS DEVICES

V. A. Desnitsky[1], I. V. Kotenko[1,2]

[1]*St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, 199178, St. Petersburg, Russia*

[2]*ITMO University, 197101, St. Petersburg, Russia*
E-mail: ivkote@comsec.spb.ru

Currently the problem of energy depletion attacks on modern wireless Internet-of-Things devices becomes increasingly important. While latent to attack targets and their monitoring systems, such attacks can exhaust the energy resource of the device in a fairly short period and thereby disrupt its operability and availability. Possible types of energy resource depletion attacks are analyzed. A generalized model of an intruder conducting attacks of this type are proposed, experimental studies are carried out using two developed software and hardware simulation stands with hardware and software devices based on Android 5.1 and Digi XBee v2 platforms.

Keywords: information security, energy exhaustion attacks, modeling, analysis, Internet of Things

Data on authors

Vasily A. Desnitsky — PhD, St. Petersburg Institute for Informatics and Automation of the RAS, Laboratory of Computer Security Problems;
E-mail: desnitsky@comsec.spb.ru

Igor V. Kotenko — Dr. Sci., Professor; St. Petersburg Institute for Informatics and Automation of the RAS, Laboratory of Computer Security Problems; ITMO University, International Laboratory “Information Security of Cyber-physical Systems”; E-mail: ivkote@comsec.spb.ru

For citation: Desnitsky V. A., Kotenko I. V. Analysis of energy resource depletion attacks on wireless devices. *Journal of Instrument Engineering*. 2018. Vol. 61, N 4. P. 291—297 (in Russian).

DOI: 10.17586/0021-3454-2018-61-4-291-297