УДК 004.056.5
DOI: 10.15827/0236-235X.136.564-571
Дата подачи статьи: 20.09.21
2021. Т. 34. № 4. С. 564–571

Имитационная модель оценки срока службы интернета вещей в условиях атакующих воздействий, источающих энергию узлов

Т.М. Татарникова [1,2]*, д.т.н., профессор, tm-tatarn@yandex.ru*
П.Ю. Богданов [2]*, старший преподаватель, 45bogdanov@gmail.com*

[1] *Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), г. Санкт-Петербург, 197376, Россия*
[2] *Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, 190000, Россия*

Малая мощность сенсорных узлов интернета вещей обусловливает поиск решения нескольких актуальных задач: увеличение срока службы сенсорных узлов и безопасность интернета вещей. В качестве источника питания сенсорные узлы используют батареи, ресурсы которых ограничены, и, если сенсорная сеть установлена и развернута в удаленном географическом пространстве для наблюдения за физическими явлениями, подзарядка или замена сенсорных узлов может стать невозможной или дорогостоящей из-за местоположения.

Энергопотребление – один из важных показателей качества интернета вещей, определяемый как количество энергии, используемой и потраченной сенсорными узлами. От энергопотребления зависит срок службы сети – время, в течение которого она будет полностью функционировать. Внедрение механизмов защиты интернета вещей требует дополнительных затрат энергии, связанных с их реализацией, однако отсутствие этих механизмов чревато распространением атак, истощающих энергию узлов, и сокращением срока службы интернета вещей.

В статье приведены результаты имитационного эксперимента, доказывающие, что своевременное обнаружение атак способствует увеличению срока службы сети по сравнению с сетью, в которой механизмы безопасности отсутствуют. Для понимания принципов работы имитационной модели описываются ее основные модули, имитирующие реальные объекты сети интернета вещей: сенсорные узлы, маршрутизаторы, протоколы, каналы связи, атаки, пакеты данных. Оценки потребляемой энергии и срока службы приведены в виде графиков зависимостей от разных параметров сети интернета вещей.

Ключевые слова: *сеть интернета вещей, срок службы интернета вещей, энергопотребление, имитационная модель, эксперимент на модели.*

Основными показателями качества *беспроводной сенсорной сети* (БСС), образующей физический уровень интернета вещей (Internet of Things, IoT), являются безопасность и срок службы сенсорных узлов (датчиков). В качестве источника питания сенсорные узлы используют батареи, ресурсы которых ограничены [1].

Энергопотребление – количество энергии, используемой и потраченной узлами БСС. Единица измерения – джоуль. От энергопотребления зависит срок службы БСС [2].

Срок службы сети – время, в течение которого БСС будет полностью функционировать. Единица измерения – секунды. Срок службы БСС может быть измерен с помощью следующих параметров:

– число активных узлов – количество узлов, которые еще функционируют и имеют энергию для работы;

– время «смерти» первого узла – время до тех пор, пока уровень остаточной энергии первого сенсорного узла не упадет до критического состояния;

– коэффициент доставки пакетов – отношение числа доставленных адресату пакетов к числу отправленных.

Беспроводные сети обычно развертываются в удаленных и враждебных средах и, как правило, остаются без присмотра. В силу этого они не имеют физической защиты (например, отсутствуют коммутаторы или шлюзы для отслеживания потока информации), что может привести к компрометации узла. Поэтому требуются эффективные механизмы защиты от атак в БСС с учетом ограничений по электропитанию *сенсорных устройств* (СУ) [3, 4].

Внедрение механизмов защиты данных требует дополнительных затрат энергии, свя-

занных с их реализацией, однако отсутствие этих механизмов чревато распространением атак, истощающих энергию узлов, и сокращением срока службы IoT. Очевидно, что своевременное обнаружение подобных атак способствует увеличению срока службы сети по сравнению с той, в которой механизмы безопасности отсутствуют [5].

В статье приведены результаты имитационного эксперимента, доказывающие данное утверждение.

Описание объектов имитационной модели

Имитационная модель IoT, как и реальная сеть, состоит из модулей, только программных, и создана на программной платформе C++.

В процессе разработки использованы принципы объектно-ориентированного программирования, что позволило выделить отдельные сущности, описывающие состояние и поведение узлов IoT-сети. Далее перечислены основные программные интерфейсы, описывающие компоненты модели IoT-сети.

1. Packet – программный агент, представленный в виде записи следующих значений:

– момент генерации пакета;

– время, зафиксированное после свершения очередного события относительно момента генерации;

– адрес назначения пакета;

– статус пакета: активный (true) – пакет может обрабатываться или передаваться, пассивный (false) – в противном случае.

2. Node – СУ (узел) БСС, которое характеризуется идентификатором (номером), местоположением (координатами), запасом энергии, законом генерации следующих данных:

– сообщение-маяк, оповещающее о присутствии сенсора в данном кластере;

– пакет с данными, содержащий зарегистрированные данные об окружающей среде – измерения;

– сообщение о местоположении узла (может не использоваться).

В свою очередь, СУ принимает управляющие сообщения от головного узла кластера (*главы кластера* – ГК), обнаруживает его аномальное поведение и участвует в выборе головного узла кластера путем расчета уровня остаточной энергии.

3. HeadNode – головной узел кластера, характеризующийся идентификатором, местоположением (координатами), запасом энергии, законом генерации следующих данных:

– сообщений о синхронизации по времени;

– управляющих пакетов данных – команд;

– данных от СУ главе кластера;

– агрегированных данных маршрутизатору.

В свою очередь, головной узел кластера получает сообщения-маяки от узлов при их выходе из кластера и входе в него, анализирует статистические характеристики получаемых пакетов данных.

Назначение ГК выполняется по протоколу LEACH (Low-Energy Adaptive Clustering Hierarchy). Это самоорганизующийся адаптивный протокол кластеризации, который использует рандомизацию для равномерного распределения энергетической нагрузки между датчиками в сети.

Функции аутентификации СУ и головного узла в имитационной модели не рассматриваются.

4. Protocol – программный интерфейс, используемый для описания процесса доступа СУ к головному узлу кластера. Сеть состоит из набора кластеров. Каждый кластер управляется ГК.

Все кластеры имеют свои собственные узлы, называемые узлами кластера. Головной узел устанавливает расписание множественного доступа с временным разделением (Time-division multiple access, TDMA) и передает это расписание всем узлам своего кластера. Затем узлы *i*-го кластера передают свои измерения соответствующему головному узлу.

После этого головные узлы кластеров объединяют данные и пересылают их на ближайший маршрутизатор.

5. BaseStation – маршрутизатор БСС, агрегирующий данные со всех узлов БСС. Маршрутизатор находится в центре сенсорного поля и в отличие от других узлов БСС в имитационной модели имеет неограниченный запас энергии и не может быть подвергнут атакующему воздействию.

Маршрутизатор имеет полную информацию о каждом ГК (номер и MAC-адрес). Также в процессе моделирования маршрутизатор используется для подсчета правильно доставленных пакетов и обменивается данными с внешней сетью.

6. Network – вся IoT-сеть, совокупность всех узлов и маршрутизатора. Используется

для создания компонентов сети, первоначального размещения узлов, моделирования появления данных на узлах, инициализации атакующих узлов, а также для сбора данных о состоянии узлов сети.

7. Attack – программный интерфейс, описывающий поведение узлов, моделирующих атакующее воздействие.

Программная реализация модели позволяет имитировать работу БСС с различным числом узлов и топологий, моделировать аномальное поведение СУ путем настройки узлов на атакующее поведение, проводить сравнение работы сети с узлами, использующими предлагаемое решение для защиты, с такой же сетью, не использующей защиту [6, 7].

В результате работы программы генерируются текстовые лог-файлы, содержащие список событий, произошедших в БСС, например, появление, передачу или прием данных. Помимо этого, имеется возможность добавления инструкций, вычисляющих другую информацию о сети в зависимости от задачи, в частности, долю потерянных пакетов.

Особенности реализации имитационной модели

В таблице приведены основные модули модели, имитирующие реальные объекты сети IoT.

Алгоритм выбора ГК приведен на рисунке 1.

Выбор ГК выполняется в каждом новом раунде работы БСС. Происходит это следующим образом [8]: в начале раунда независимо друг от друга на каждом СУ (пусть их количество равно N) генерируется случайное число $z_i \in [0, 1]$, $i = \overline{1, N}$, которое участвует в вычислении некоторого порогового значения i-го СУ согласно выражению

$$Th_i = \frac{P}{1 - P(r \bmod i)}, \quad (1)$$

где P – априорная вероятность, задающая допустимое число ГК (кластеров) в сенсорном поле, как правило, $P \le 0.25$; i – порядковый номер СУ; r – номер текущего раунда.

СУ назначается ГК, если $z_i < Th_i$, иначе назначается простым узлом кластера.

Алгоритм работы объекта Protocol заключается в следующем.

СУ начинают передачу данных только по запросу головного узла. Время отдельного опроса – временной интервал, разделенный на блоки – окна. Размер окон определяется количеством слотов, на которые они делятся. Размер слота – фиксированная величина для каждого СУ. Так как слот – это тоже временной интервал, его размер определяется скоростью передачи данных от СУ до узла, то есть его определяет оборудование, используемое в системе [9].

В начале процесса узел посылает сигналы опроса всем СУ, находящимся в зоне его покрытия. В этих сигналах содержатся время начала доступа и продолжительность, то есть количество слотов. СУ, приняв эти сигналы, случайным образом выбирают слот, в котором будут передавать свои данные.

В процессе доступа в слоте возможно возникновение трех состояний:

– пусто (ни одно из СУ не выбрало текущий слот для передачи данных);

– успех (только одно СУ передает данные в текущем слоте);

– конфликт (коллизия) (более одного СУ начинают передавать данные в текущем слоте).

Опрос СУ, находящихся в зоне покрытия головного узла, заканчивается, когда в окне

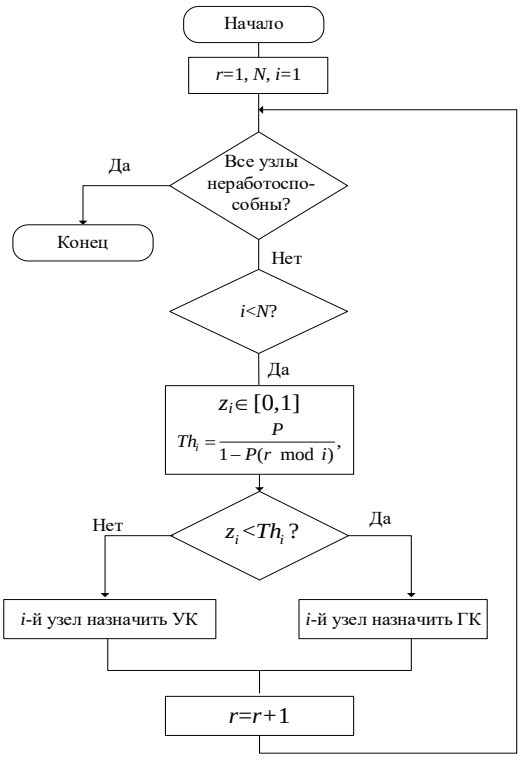

Рис. 1. Алгоритм выбора ГК сенсорной сети

Fig. 1. The algorithm for selecting the head of the sensor network cluster

появляются только слоты с успешной передачей и пустые.

Головной узел анализирует каждый слот и снимает информацию, переданную в них.

Объекты имитационной модели

Simulation objects

Реальный объект	**Модуль модели, имитирующий реальный объект**	**Параметры**
Packet	Генератор информационных пакетов. Генератор управляющих пакетов (команд)	λ_{IP} – интенсивность поступления информационных пакетов. λ_{MP} – интенсивность поступления управляющих пакетов. $f(\lambda_{IP}, t, p)$ – функция распределения случайной величины t – промежутков времени между поступлениями информационных пакетов, где p – параметр(ы) распределения (закон поступления информационных пакетов). $f(\lambda_{MP}, t, p)$ – функция распределения случайной величины t – промежутков времени между поступлениями информационных пакетов, где p – параметр(ы) распределения (закон поступления информационных пакетов). $f(L_i, p_i)$ – функция распределения дискретной случайной величины L_i – длины i-го информационного пакета с вероятностью p_i, $i = \overline{1,K}$, где K – число возможных значений L
Node	Функция, имитирующая процесс передачи пакетов данных головному узлу кластера. Функция, имитирующая прием пакетов данных от головного узла кластера. Функция, задающая мобильность СУ	Размеры сенсорного поля $X \times Y$. Координаты расположения СУ в сенсорном поле. Время передачи пакета длиной L головному узлу кластера: $t^{send} = \bar{L}/C$. Расход энергии $E^{send}(L, d)$ для отправки L-битного сообщения на расстояние d: $E^{send}(L,d) = E'L + E''Ld^2$, где E' – энергия, необходимая для генерации одного бита, Дж/бит; E'' – энергия, необходимая для передачи одного бита, Дж/бит/м^2. Время приема пакета длиной L от головного узла кластера: $t^{recive} = \bar{L}/C$. Расход энергии $E^{recive}(L)$ для получения L-битного сообщения: $E^{recive}(L) = E'L$, где p – вероятность мобильности устройства, разыгрывается как дискретная случайная величина z методом Монте-Карло: если случайная величина $z < p$, узел остается на месте с координатами (x, y), если $z > p$, узел перемещается внутри сенсорного поля на случайное расстояние l
HeadNode	Функция реализации протокола LEACH. Функция реализации сигнала опроса t_{sur} СУ кластера. Функция реализации приема пакетов данных от всех СУ кластера	Раунд взаимодействия головного узла с N СУ составляет случайное суммарное время $T = Nt^{send}$. Общий расход энергии головного узла кластера учитывает общее количество пакетов (отправленных и полученных): $E^{over} = \sum_{i=1}^{S} E^{send}(L_i, d_i) + \sum_{j=1}^{R} E^{recive}(L_j)$. Координаты расположения головного узла в сенсорном поле
Protocol	Функция, имитирующая доступ СУ к головному узлу кластера	Матрица принадлежности всех СУ к определенному кластеру. Продолжительность сигнала опроса. Временная метка начала передачи каждому СУ кластера. Пропускная способность канала C, бит/с
BaseStation	Функция, имитирующая процесс обслуживания входящего потока данных на маршрутизаторе	Параметры входящего основного (имитируемого) потока данных в виде распределения Парето $P(\alpha, K)$ для случайной величины τ: $F(\tau) = 1 - (K/\tau)^{\alpha}$, где τ – интервал времени между поступлением очередных заявок; α – показатель степени, характеризующий тяжелый хвост; K – коэффициент масштаба распределения, задающий минимально возможное значение τ. Параметры нерассматриваемой части сети в виде транзитных потоков также согласно распределению Парето $P(\alpha, K)$. Закон обслуживания с параметром $T_{\text{обс}}$., – средним временем обслуживания поступившего пакета данных. Флаг состояния – занято/свободно. Координаты расположения маршрутизатора
Network	Модель логического канала, связывающего источник с адресатом	Число маршрутизаторов (хопов) от источника к адресату. Матрица инцидентности маршрутизаторов
Attack	Генератор атак	$f(\lambda, p)$ – функция запуска «пустых» запросов (пакетов) с интенсивностью λ, требующих обработки на головном узле, где p – вероятность запуска генератора атак
Queue	Связный список	Адрес, указывающий на начало первого элемента связного списка
TimeModel	Искусственное (модельное) время	Схема процессов и событий

Продолжительность обслуживания СУ t^{serv} при опросе формируется следующим образом:

$$t^{serv} = t^{sur} + t^{send}. \quad (2)$$

Полный цикл взаимодействия головного узла с N СУ составляет случайное суммарное время $T = Nt_s$.

Связь этих переменных показана на рисунке 2.

На рисунке 3 приведен алгоритм моделирования случайного события – генерации атаки.

Модель Network представляет собой модель *виртуального канала* (ВК) – коммутационный канал, обеспечивающий транспортировку информационных пакетов между двумя удаленными *маршрутизаторами* (М) сети, то есть некоторый маршрут в сети, состоящий из последовательности маршрутизаторов с интенсивностью обслуживания μ, по которому осуществляется передача информации из узла-источника в узел-адресат [10].

Пакеты, посылаемые абонентами и устройствами виртуального канала (рис. 4), называются выделенным потоком. Предполагается, что они образуют агрегированный поток Парето с параметром λ^B сообщений/с [11]. При прохождении по линии от маршрутизатора к маршрутизатору вдоль линии следования эти пакеты в каждом узле встречаются с так называемыми внешними потоками данных, с которыми разделяют логическую линию. Внешние пакеты, следующие по собственному логическому пути, могут поступать в данный маршрутизатор от других узлов сети или впервые поступать в сеть извне в данном узле. Этот поток назовем транзитным с параметром λ^T.

Одна и та же модель ВК для представления разных маршрутов будет отличаться только параметрами, а генераторы фоновых потоков компенсируют нерассматриваемую часть IoT-сети.

Результаты имитационного эксперимента на модели БСС

Моделируемая БСС представляет собой совокупность из 100 одинаковых по характеристикам сенсорных узлов, расположенных на территории размером 200 на 200 метров. СУ задается местоположением – координатами X, Y в сенсорном поле. Узлы распределены случайно согласно равномерному закону, задающему плотность распределения

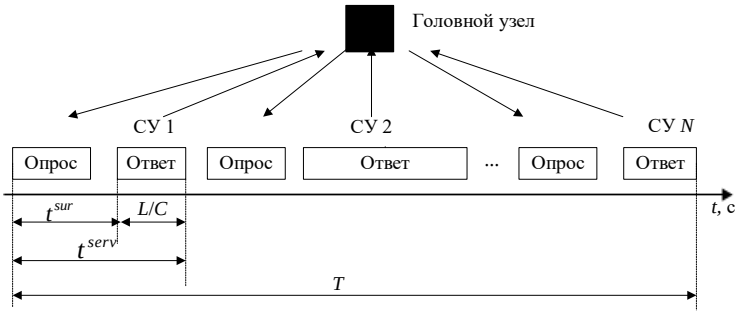

Рис. 2. Временная диаграмма взаимодействия СУ с головным узлом кластера

Fig. 2. The timing diagram of the interaction of a sensory node with the cluster head node

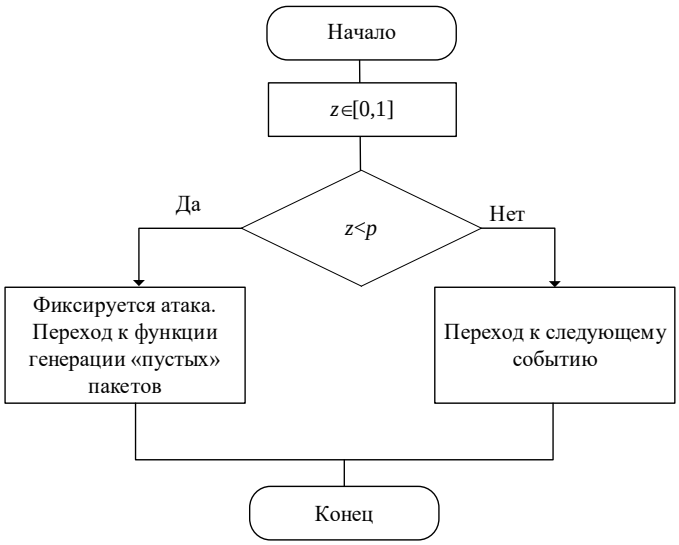

Рис. 3. Алгоритм моделирования случайного события – генерации атаки

Fig. 3. The algorithm for modeling a random event – attack generation

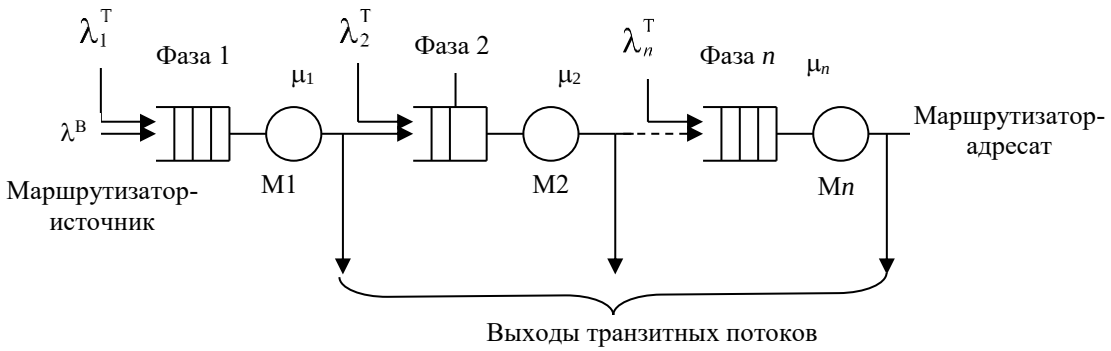

Рис. 4. Модель ВК

Fig. 4. A virtual channel model

СУ. Внутри сенсорного поля узлы могут перемещаться случайным образом в радиусе 2 метров за одну итерацию. Радиус действия узлов – 25 метров. E' = 50 нДж/бит, E''= 100 пДж/бит/м^2.

Для оценки потребляемой энергии проведено сравнение между двумя сетями – с функционирующим модулем Attack и без него. На рисунке 5 показана зависимость потребляемой энергии в БСС с течением времени, на рисунке 6 – зависимость количества функционирующих СУ с течением времени, на рисунке 7 – зависимость коэффициента доставки данных с течением времени.

График на рисунке 5 показывает, что атаки начинают быстро расходовать энергию БСС и в какой-то момент сеть станет неработоспособной из-за отсутствия возможности установить маршрут до адресата. График на рисунке 6 показывает, что на 100-й единице модельного времени БСС начинает терять свои узлы. График на рисунке 7 демонстрирует разницу в значениях коэффициента доставки для сети, не подверженной атакам (идеальный случай), и для сети, подверженной атакам, – на 240-й единице модельного времени сеть потеряла четверть своих узлов, что не позволило выстроить маршруты до адресата и доставить предназначающиеся ему пакеты данных.

Заключение

Для демонстрации необходимости внедрения механизмов защиты БСС от атак, истощающих энергию узлов, разработана имитационная модель IoT-сети. Приведены некоторые особенности программной реализации основных модулей имитационной модели.

Результаты имитационного эксперимента показывают, что своевременное обнаружение атак, направленных на истощение энергии сенсорных узлов, способствует увеличению

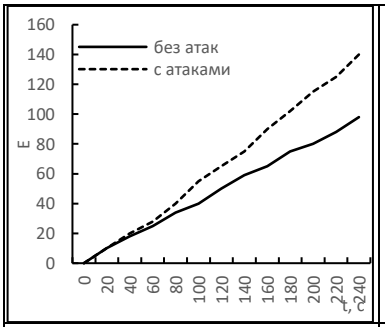

Рис. 5. Зависимость потребления энергии в БСС

Fig. 5. The dependence of energy consumption in the sensor network

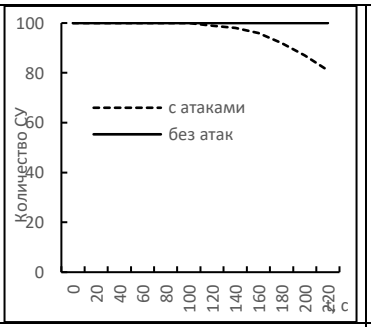

Рис. 6. Зависимость количества функционирующих СУ в БСС

Fig. 6. The dependence of the number of functioning sensory nodes in the sensor network

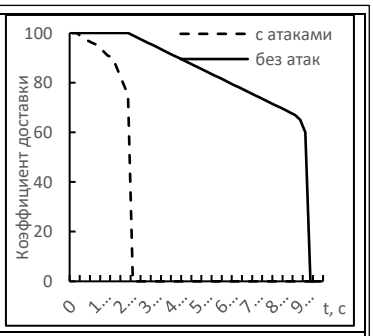

Рис. 7. Зависимость коэффициента доставки в БСС

Fig. 7. The dependence of the delivery rate in the sensor network

срока службы сети и коэффициента доставки пакетов адресату по сравнению с сетью, в которой механизмы противодействия атакам отсутствуют.

Литература

1. Варгаузин В.А. Радиосети для сбора данных от сенсоров, мониторинга и управления на основе стандарта IEEE 802.15.4 // ТелеМультиМедиа. 2005. № 6. С. 23–27.

2. Татарникова Т.М., Богданов П.Ю., Краева Е.В. Предложения по обеспечению безопасности системы умного дома, основанные на оценке потребляемых ресурсов // Проблемы информационной безопасности. Компьютерные системы. 2020. № 4. С. 88–94.

3. Kind A., Stoecklin M.P., Dimitripoulos X. Histogram-basedtraffic anomaly detection. IEEE Transactions on Network and Service Management, 2009, vol. 6, no. 2, pp. 110–121. DOI: 10.1109/TNSM.2009.090604.

4. Татарникова Т.М., Журавлев А.М. Нейросетевой метод обнаружения вредоносных программ на платформе Android // Программные продукты и системы. 2018. Т. 33. № 3. С. 543–547. DOI: 10.15827/0236-235X.123.543-547.

5. Киричек Р.В., Парамонов А.И., Прокопьев А.В., Кучерявый А.Е. Эволюция исследований в области беспроводных сенсорных сетей // ИТТ. 2014. Т. 2. № 4. С. 29–41. URL: http://www.sut.ru/doci/nauka/review/4-14.pdf (дата обращения: 15.08.2021).

6. Baddar S.A.-H., Merlo A., Migliardi M. Anomaly detection in computer networks: A state-of-the-art review. JoWUA, 2014, vol. 5, no. 4, pp. 29–64. DOI: 10.22667/JOWUA.2014.12.31.029.

7. Simmross-Wattenberg F., Asensio-Perez J.I., Casaseca-de-la-Higuera P., Martin-Fernandez M. et al. Anomaly detection of network traffic based on statistical inference and a-stable modeling. IEEE Transactions on Dependable and Secure Computing, 2011, vol. 8, no. 4, pp. 494–509. DOI: 10.1109/TDSC.2011.14.

8. Жарков С.Н. Стохастическое формирование проактивного множества при кластеризации в мобильных беспроводных сенсорных сетях // T-Comm – телекоммуникации и транспорт. 2013. Т. 7. № 5. С. 29–34.

9. Переспелов А.В., Богданов П.Ю., Краева Е.В. Применение технологии виртуализации для организации разграничения доступа // Изв. вузов. Приборостроение. 2021. Т. 64. № 5. С. 364–369. DOI: 10.17586/0021-3454-2021-64-5-364-369.

10. Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN. СПб: БХВ-Петербург, 2014. 160 с.

11. Викулов А.С., Парамонов А.И. Анализ трафика в сети беспроводного доступа стандарта IEEE 802.11 // Тр. учебных заведений связи. 2017. Т. 3. № 3. С. 21–27.

Software & Systems
DOI: 10.15827/0236-235X.136.564-571

Received 20.09.21
2021, vol. 34, no. 4, pp. 564–571

A simulation model for estimating the service life of the Internet of Things under the conditions of attacking effects emitting the node energy

T.M. Tatarnikova [1,2], *Dr.Sc. (Engineering), Professor, tm-tatarn@yandex.ru*
P.Yu. Bogdanov [2], *Senior Lecturer, 45bogdanov@gmail.com*

[1] *St. Petersburg Electrotechnical University "LETI", St. Petersburg, 197376, Russian Federation*
[2] *St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, 190000, Russian Federation*

Abstract. The low power of the sensor nodes of the Internet of Things determines the search for solving several urgent problems: increasing the service life of sensor nodes and the security of the Internet of Things. Sensor nodes use batteries with limited resources as a power source, therefore if a sensor network is installed and deployed in a remote geographic space to observe physical phenomena, then recharging or replacing sensor nodes may become impossible or expensive due to the long distance.

Power consumption is one of the important quality indicators of the Internet of Things defined as the amount of energy used and spent by sensor nodes. Energy consumption determines the network lifespan – the time when the sensor network is fully functional. On the other hand, the implementation of IoT security

mechanisms requires additional energy costs associated with their implementation. However, the lack of security mechanisms causes the proliferation of attacks that emit the node energy, as well as reduced service life of the Internet of Things.

The paper presents the results of a simulation experiment proving that timely detection of attacks contributes to an increase in the service life of the network compared to a network with no security mechanisms. To understand the operation principles of the simulation model, there is a a description of its main modules, which simulate real objects of the Internet of Things network: sensor nodes, routers, protocols, communication channels, attacks, data packets. The estimates of energy consumption and service life are given in the form of graphs of dependences on various parameters of the Internet of Things network.

Keywords: internet of things network, lifespan of Internet of Things, power consumption, simulation model, model experiment.

References

2. Vargauzin V.A. Radio networks for data collection from sensors, monitoring and control based on the IEEE 802.15.4 standard. *TeleMultiMedia*, 2005, no. 6, pp. 23–27 (in Russ.).

3. Tatarnikova T.M., Bogdanov P.Yu., Kraeva E.V. Smart home security proposals based on the assessment of consumption resources. *Information Security Problems. Computer Systems*, 2020, no. 4, pp. 88–94 (in Russ.).

4. Kind A., Stoecklin M.P., Dimitripoulos X. Histogram-basedtraffic anomaly detection. *IEEE Trans. on Network and Service Management*, 2009, vol. 6, no. 2, pp. 110–121. DOI: 10.1109/TNSM.2009.090604.

5. Tatarnikova T.M., Zhuravlev A.M. A neural network method for detecting malicious programs on the Android platform. *Software & Systems*, 2018, vol. 33, no. 3, pp. 543–547. DOI: 10.15827/0236-235X.123.543-547 (in Russ.).

6. Kirichek R.V., Paramonov A.I., Prokopyev A.V., Kucheryavy A.E. The investigation evolution in the wireless sensor networks area. *IJITT*, 2014, vol. 2, no. 4, pp. 29–41. Available at: http://www.sut.ru/doci/nauka/review/4-14.pdf (accessed August 15, 2021) (in Russ.).

7. Baddar S.A.-H., Merlo A., Migliardi M. Anomaly detection in computer networks: A state-of-the-art review. *JoWUA*, 2014, vol. 5, no. 4, pp. 29–64. DOI: 10.22667/JOWUA.2014.12.31.029.

8. Simmross-Wattenberg F., Asensio-Perez J.I., Casaseca-de-la-Higuera P., Martin-Fernandez M. et al. Anomaly detection of network traffic based on statistical inference and a-stable modeling. *IEEE Trans. on Dependable and Secure Computing*, 2011, vol. 8, no. 4, pp. 494–509. DOI: 10.1109/TDSC.2011.14.

9. Zharkov S.N. Stochastic generation proactive set clustering in mobile wireless sensor networks. *T-Comm*, 2013, vol. 7, no. 5, pp. 29–34 (in Russ.).

10. Perespelov A.V., Bogdanov P.Yu., Kraeva E.V. Application of virtualization technology to organize access control. *J. of Instrument Engineering*, 2021, vol. 64, no. 5, pp. 364–369. DOI: 10.17586/0021-3454-2021-64-5-364-369 (in Russ.).

11. Goldstein B.S., Kucheryavy A.E. *Post-NGN Communication Networks*. St. Petersburg, 2014, 160 p. (in Russ.).

12. Vikulov A.S., Paramonov A.I. Traffic analysis in a wireless access network of IEEE 802.11. *Proc. of Telecommunication Univ.*, 2017, vol. 3, no. 3, pp. 21–27 (in Russ.).

Для цитирования

Татарникова Т.М., Богданов П.Ю. Имитационная модель оценки срока службы интернета вещей в условиях атакующих воздействий, источающих энергию узлов // Программные продукты и системы. 2021. Т. 34. № 4. С. 564–571. DOI: 10.15827/0236-235X.136.564-571.

For citation

Tatarnikova T.M., Bogdanov P.Yu. A simulation model for estimating the service life of the Internet of Things under the conditions of attacking effects emitting the node energy. *Software & Systems*, 2021, vol. 34, no. 4, pp. 564–571 (in Russ.). DOI: 10.15827/0236-235X.136.564-571.