ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Сентябрь 2020 Том 8 № 3 ISSN 2307-1303 http://ijitt.ru
TELECOM IT
September 2020 Vol. 8 Iss. 3 ISSN 2307-1303 http://ijitt.ru

МОДЕЛИРОВАНИЕ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

В. А. Десницкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация

Адрес для переписки: desnitsky@comsec.spb.ru

Аннотация—В работе представлены результаты анализа угроз информационной безопасности в беспроводных сенсорных сетях и средств их моделирования. **Предмет исследования.** Предметом исследования являются средства моделирования и анализа угроз информационной безопасности беспроводных сенсорных сетей. **Метод.** В работе используются методы математического моделирования и системного анализа. **Основные результаты.** Проведен анализ актуальных угроз информационной безопасности беспроводных сенсорных сетей. Проведен сравнительный анализ средств имитационного моделирования беспроводных сенсорных сетей и атакующих воздействий в них. Предложены две модели представления беспроводных сенсорных сетей для решения задач моделирования угроз. **Практическая значимость.** Результаты работы могут быть использованы для моделирования и оценки защищенности сложных беспроводных сенсорных сетей с большим числом узлов в условиях организационной сложности использования полнофункциональных экземпляров беспроводных сенсорных сетей для решения задач обеспечения информационной безопасности.

Ключевые слова—беспроводные сенсорные сети, моделирование, информационная безопасность.

Информация о статье
УДК 004.733
Язык статьи – русский.
Поступила в редакцию 23.07.20, принята к печати 23.09.20.

Ссылка для цитирования: Десницкий В. А. Моделирование и анализ угроз информационной безопасности в беспроводных сенсорных сетях // Информационные технологии и телекоммуникации. 2020. Том 8. № 3. С. 102–111. DOI 10.31854/2307-1303-2020-8-3-102-111.

MODELING AND ANALYSIS OF INFORMATION SECURITY THREATS IN WIRELESS SENSOR NETWORKS

V. Desnitsky*

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

St. Petersburg Federal Research Center Russian Academy of Sciences,
St. Petersburg, 199178, Russian Federation

*Corresponding author: desnitsky@comsec.spb.ru

Abstract—The paper presents results of analysis of information security threats in wireless sensor networks and means for their modeling. **Research subject.** The subject of the research is means for modeling and analyzing information security threats to wireless sensor networks. **Method.** The work uses methods of mathematical modeling and system analysis. **Core results.** The analysis of actual threats to information security of wireless sensor networks is performed. A comparative analysis of means for simulation modeling of wireless sensor networks and attacking influences is performed. Two models of presentation of wireless sensor networks are proposed for solving the problems of threat modeling. **Practical significance.** The results of the work can be used for modeling and evaluation of security of complex wireless sensor networks with a large number of nodes in conditions of organizational complexity of using full-featured instances of wireless sensor networks to solve information security problems.

Keywords—wireless sensor networks, modeling, information security.

Article info
Article in Russian.
Received 23.07.20, accepted 23.09.20.

For citation: Desnitsky V.: Modeling and Analysis of Information Security Threats in Wireless Sensor Networks // Telecom IT. 2020. Vol. 8. Iss. 3. pp. 102–111 (in Russian). DOI 10.31854/2307-1303-2020-8-3-102-111.

Введение

Беспроводные сенсорные сети, объединяющие множества встроенных устройств и сенсоров представляют сравнительно новый вид информационно-телекоммуникационных инфраструктур, которые отличаются наличием специфичных угроз информационной безопасности, обусловленных появлением новых классов осуществляемых на такие системы программно-информационных и физических воздействий и требующих новых путей и механизмов защиты. Проведение анализа защищенности в беспроводных сенсорных сетях обосновывается необходимостью обнаружения вторжений в систему, попыток несанкционированной модификации данных и программного кода устройств, атак подмены сенсоров и нарушения аутентичности устройств, атак истощения энергоресурсов устройств и др., а также уведомление о состоянии критически важных параметров сети с учетом семантики предоставляемых ей сервисов.

Настоящая работа направлена на совершенствование средств моделирования и анализа угроз информационной безопасности беспроводных сенсорных сетей с использованием комплексного подхода к анализу данных, поступающих от устройств и сенсоров сети. Исследование беспроводных сенсорных сетей производится в условиях наличия разнородных и взаимодействующих между собой устройств, использующих беспроводные протоколы передачи данных с учетом повышенных требований к защищенности таких систем.

1 Подходы к моделированию и анализу угроз

В [1] обосновывается сложность применения традиционных средств анализа защищенности и обеспечения безопасности в беспроводных сенсорных сетях с большим числом сенсоров, а также ограничениями на производительность узлов сети, доступную память и типы задач, решаемых на узлах сети. Разворачивание беспроводных сенсорных сетей с защищенными от вмешательств узлами представляется сложным организационно-техническим процессом, требующим значительных финансовых затрат. При этом к основным свойствам информационных объектов, критически важных при достижении информационной безопасности, отнесены аутентичность, целостность, приватность, неотказуемость и невозможность повторного воспроизведения [2].

Denial-of-Service (DoS) атаки направлены на истощение ресурсов узла-жертвы путем отправки серий атакующим пакетов, делающее данный узел недоступным легитимным пользователям [1]. В беспроводных сенсорных сетях DoS-атаки могут проводиться на различных уровнях, в том числе на физическом уровне в виде jamming-атак, направленных на зашумление физического канала передачи беспроводного сигнала [3], и физического вмешательств в работу узла сети, в том числе атака подмены сенсора [4], атака извлечения данных при прямом доступе нарушителя к узлу [5]; на канальном уровне – атаки внесения коллизий при использовании одного и того же частотного канала и атаки истощения ресурсов узлов сети, в том числе путем принудительной ретрансляции поврежденных пакетов адресату. На сетевом уровне – различные воздействия на протоколы маршрутизации, включая подмену данных маршрутизации, примером таких атак являются атаки типа Black Hole. Еще одним примером атаки на сетевом уровне – атака типа Selective Forwarding, предполагающая осуществление выборочной пересылки скомпрометированным узлом передаваемых через него пакетов с игнорированием остальных [6].

Атака типа Acknowledgment Spoofing представляет собой формирование ложных подтверждений о факте «жизни» неактивного узла, направляемых его соседям или определенному узлу [5]. Атака типа Misdirection предполагает перенаправление легитимных пакетов неправильным получателям [7]. На транспортном уровне примерами атак на узлы беспроводных сенсорных сетей являются – Flooding-атаки, в том числе с целью истощения памяти устройств или других аппаратных ресурсов (атаки истощения), и атаки нарушения синхронизации, в том числе внесение ошибок для препятствования передачи легитимным узлом его данных [1].

При работе централизованных вычислительных алгоритмов в беспроводной сенсорной сети Sybil-атаки предполагают нарушение процесса распределения

данных и их избыточности, выполняемые с использованием нескольких идентификаторов узла, которые предоставляются легитимным узлам для доступа к ресурсам остальной сети и осуществления информационного обмена. В частности, в условиях использования одновременной доставки некоторых данных несколькими маршрутами в сети с целью гарантировать их неизменность Sybil-атаки могут оказаться достаточно эффективными [8].

Blackhole-атака направлена на нарушение процесса корректной маршрутизации сети, причем при динамическом выборе «конкурирующих» маршрутов злонамеренный узел уведомляет, что способен доставить пакет данных между любыми двумя заданными узлами с максимальным качеством, выражаемом в минимизации времени, количества промежуточных узлом или какой-либо другой характеристике, существенной для учета в процессе динамического выстраивания маршрутов доставки данных в сети [9]. В результате атакующий оказывается способным перенаправить на себя большую часть трафика или, как минимум, необходимые ему пакеты. Такие пакеты данных оказываются полностью контролируемы атакующим, могут служить основой для детального обследования сети, ее структуры и ее поведенческих особенностях, могут быть модифицированы, потеряны, перенаправлены другим узлам сети для нарушения ее работы.

Помимо базовых целей информационной безопасности, выражаемых в виде свойств конфиденциальности, целостности, доступности и их производных в [10] явным образом формулируются т. н. вторичные цели информационной безопасности, которые должны учитываться в процессе анализа защищенности программно-аппаратных компонентов беспроводных сенсорных сетей. Такие цели формулируются для конкретной области приложения с учетом следующих характеристик: (1) свежесть данных; (2) возможность самоорганизации сети; (3) синхронизация по времени, в особенности важная при коллаборативной работе узлов; (4) локализация безопасности, предполагающая возможности отслеживания каждого из узлов и локализации инцидентов безопасности с определением конкретных узлов, которые в них задействованы. Помимо этого, могут учитываться доступность узлов сети и данных, получаемых от них.

2 Анализ средств моделирования угроз информационной безопасности беспроводных сенсорных сетей

Рассмотрим следующие основные программные средства, которые используются для решения задач моделирования угроз БСС.

NS-2 – средства имитационного моделирования с открытым исходным кодом (https://sourceforge.net/projects/nsnam). Это средство применяется для имитационного моделирования сети дискретных событий. К достоинствам NS-2 можно отнести поддержку большого числа протоколов на различных уровнях сетевого взаимодействия. Его недостатками являются – отсутствие графического интерфейса; необходимо использование скриптового языка для проведения моделирования, который сложен в использовании; сложность адекватного моделирования процессов энергопотребления в БСС [11].

TOSSIM – программный эмулятор дискретных событий БСС. Можно проводить моделирование сенсорных устройств, работающих на TinyOS

(http://tinyos.net). К достоинствам TOSSIM можно отнести его свободное распространение; наличие графического интерфейса TinyViz, который отображает взаимодействия элементов сети; масштабируемость моделируемой сети (до 1 000 узлов). Существенным недостатком является возможность проводить моделирование сети, основанной только на операционной системе TinyOS, то есть возможно моделировать только однотипные узлы.

EmStar – программный эмулятор, с помощью которого возможно проводить трассировку процесса функционирования сети в реальном времени. В состав входят множество библиотек, инструментов, аппаратных характеристик сенсоров [12]. Достоинствами данного средства являются – наличие графического интерфейса; модульность; наличие удобной документации к продукту. К недостаткам можно отнести существенные ограниченная масштабируемость.

OMNeT++ – бесплатный для некоммерческого пользования дискретный сетевой эмулятор событий, построенный на языке C++ (https://omnetpp.org). Имеет встроенный графический интерфейс. Этот инструмент поддерживает протоколы MAC, а также некоторые другие виды протоколов беспроводных сенсорных сетей. OMNeT++ может использоваться для моделирования управления каналами в БСС и для моделирования задач энергопотребления. Достоинства OMNeT++ – наличие графического интерфейса; наличие большого числа программных сред и модулей, расширяющих функционал, например NesCT, который позволяет моделировать БСС на операционной системе TinyOS; поддержка множества протоколов БСС, например MAC-протоколы; возможность моделирования потребления энергии узлами БСС. К недостаткам можно отнести сложность добавления новых протоколов взаимодействия элементов БСС.

J-Sim – сетевой эмулятор событий, построенный на языке программирования Java (https://www.physiome.org/jsim). Этот эмулятор предоставляет графический интерфейс и библиотеку для математического моделирования на языке, специально разработанном для моделей J-Sim. Имеет возможность моделировать процессы реального времени. Его достоинства – наличие графического интерфейса; наличие большого числа протоколов; возможность моделирования маршрутов в БСС; возможность моделирования радиоканалов; возможность моделирования потребления энергии; масштабируемость. Недостатки – слабая расширяемость по части добавления новых протоколов.

ATEMU – программный эмулятор для систем на базе процессоров AVR (https://atemu-sensor-node-simulator-or-debugger.soft112.com). Кроме AVR включает в себя поддержку других периферийных устройств, например датчика типа MICA2 и радиоканала. С помощью ядра эмулятора ATEMU можно моделировать произвольное число узлов и взаимодействия между ними. К преимуществам данного средства можно отнести его масштабируемость; наличие графического интерфейса; возможность обеспечения высокого уровня детализации в процессе моделирования; возможность моделирования разнородных сетей. Недостатками являются – увеличенные временные затраты на моделирование по сравнению с другими средствами; ограниченный состав функций для моделирования маршрутизации и кластеризации.

Avrora – средство для моделирования, ориентированное на анализ БСС (https://sourceforge.net/projects/avrora). Позволяет моделировать микроконтроллерные сенсорные узлы MICA2 на основе AVR. У Avrora отсутствует графический

интерфейс, но она поддерживает моделирование процессов энергопотребления. Также не позволяет моделировать алгоритмы управления сетью, потому что он не имеет сетевых средств коммуникации [13]. К его преимуществам можно отнести высокую скорость моделирования; лучшую точность по равнению с TOSSIM; возможность моделирования процессов энергопотребления. Недостатками являются – отсутствие графического интерфейса и отсутствие возможности моделирования алгоритмов управления сетью [13].

Castalia – средство для моделирования беспроводных сенсорных сетей и сетей с устройствами с низким энергопотреблением (https://sourceforge.net/projects/castalias). Данное средство основана на платформе OMNeT++. Может использоваться для тестирования алгоритмов или протоколов в моделях с учетом особенностей радиоканала с детализацией поведения узлов. Castalia также может использоваться для оценки различных характеристик платформы в рамках конкретных приложений [14]. К его преимуществам можно отнести возможность моделирования свойств радиоканала; наличие графического интерфейса; поддержка протоколов маршрутизации и MAC; возможность моделирования физического процесса передачи данных, задания шумов и чувствительности устройства; платформа-независимость. Недостатками являются – отсутствие привязки к платформе БСС, выражаемая, в частности, в сложности моделирования в привязке к конкретной платформе/операционной системе, например TinyOS [14].

QualNet – эмулятор БСС, имеет графический интерфейс, используемый для дизайна, анимации и анализа БСС [14]. Его достоинствами являются: его масштабируемость; наличие графического интерфейса; поддержка различных моделей представления устройств; наличие функций оценки эффективности протоколов на каждом уровне; поддерживается многопроцессорными системами и системами с распределенными вычислениями (https://www.scalable-networks.com/products/qualnet-network-simulation-software-tool). Недостатками являются достаточно высокая стоимость, а также медленный графический интерфейс на основе платформы Java.

InsightMaker – бесплатное средство для моделирования БСС, которое предоставляется в виде Web-сервиса (https://insightmaker.com). Поддерживает множество протоколов, а также возможность визуального создания моделей и анимации.

WSNet – свободно распространяемый эмулятор БСС (http://wsnet.gforge.inria.fr). Поддерживает архитектуры со сложными узлами, моделирование энергопотребления, моделирование некоторых видов физических явлений.

Отметим, что перечисленные инструменты относятся к классу средств имитационного моделирования. Применение подобных средств позволяет нивелировать или уменьшить влияние следующих ограничений, связанные с моделирование и анализом средств оценки угроз информационной безопасности сложных крупномасштабных БСС. Во-первых, ограничения на имеющиеся в наличие аппаратные коммуникационно-вычислительные активы сети, а также стоимость их приобретения и обслуживания, в том числе ограничения на число одновременно моделируемых устройств. Во-вторых, временные ограничения, усложняющие

возможность моделирования продолжающихся во времени многошаговых воздействий, которые требуют одновременного вовлечения, настройки и координированного управления большим числом беспроводных узлов. В-третьих, ограничения безопасности, обуславливаемыми необходимостью учета возможных побочных эффектов на анализируемую инфраструктуру.

Выбор конкретного средства моделирования определяется указанными особенностями каждого из них, включающими в том числе целевую направленность; множество термов и операций, доступных к использованию; программную совместимость и наличие программного интерфейса (API) и внешних библиотек для интеграции со сторонними компонентами моделирования или средствами инфраструктуры и условия использования.

В работе предложен комплексный подход к применению существующих средств моделирования угроз информационной безопасности в беспроводных сенсорных сетях. В условиях разнородности угроз информационной безопасности и их проявлении на различных уровнях сетевого взаимодействия и на различных этапах жизненного цикла БСС, а также в результате особенностей эксплуатируемых программно-аппаратных активов представляется целесообразной возможность комбинирования существующих средств моделирования. При этом комбинирование осуществляется в первую очередь в форме интеграции результатов моделирования отдельных построенных моделей.

3 Модели представления беспроводных сенсорных сетей

Для решения задач моделирования и анализа угроз информационной безопасности в беспроводных сенсорных сетях предложен ряд моделей представления беспроводных сенсорных сетей, агрегирующей основные данные о сети и правила для анализа угроз ее информационной безопасности. Данные модели используются в процессе моделирования для обобщения и спецификации необходимых исходных данных.

Формирование моделей представления БСС направлено на формализацию предметной области БСС, повышение структуризации знаний о сети, ее составе, отображение физических и логических связи между узлами, спецификацию типов узлов сети и их ролей в контексте свойств самоорганизации сети и процессов маршрутизации в ней. Такие модели предназначены также для отображения динамических характеристик и потоков данных в сети, создания верхнеуровневых профилей по настройке параметров узлов, отправке, получению и распознаванию тестовых и сервисных команд в сети.

Модели представления БСС предназначены также для проведения экспертного анализа сетевых спецификаций, а также для верификации с использованием автоматизированных средств поддержки процессов принятия решений проектирования, разработки, обеспечения и анализа защищенности сети. Помимо этого, модели предназначены также для анализа атакующих воздействий и инцидентов безопасности на уровне манипуляции командами представления с использованием унифицированных команд обращения к узлам беспроводной сенсорной сети, ее данным и предоставляемым сервисам. Разработанные модели предполагает наличие обратных связей от модели к объектам программно-аппаратной инфраструктуры сети в виде специализированных программно-аппаратных триггеров и исполнительных элементов, инициирующих конкретные события в сети,

такие как отправка пакета данных по заданному адресу, обновление ключа симметричного шифрования, используемого в сети и пр.

Для представления беспроводной сенсорной сети предложены две модели представления: (1) на основе JSON-формата, удобного для формирования, модификации и использования данных, как вручную, так и при помощи автоматизированных программных средств обработки данных; (2) на основе UML-диаграмм, позволяющих специфицировать, как статическую, так и изменяющуюся во времени структуру сети, сценарии работы сети, протоколы взаимодействия и различные операционные процедуры.

Модель представления на основе JSON-формата включает упорядоченный массив пар {ключ, значение}, где под «ключом» понимается обозначение некоторой характеристики сети, тогда как поле «значение» содержит, собственно, бинарное, числовое, символьное, строковое и пр. значение этой характеристики. Например, подобным образом модель задает версию сетевого протокола, используемого в рамках БСС; числовое значение PAN_ID (*personal area networks identifier*), определяющее уникальный идентификатор беспроводной сети; значение длины ключа шифрования, используемого для обеспечения конфиденциальности данных и другие характеристики.

Основанная на UML, модель представления включает серию диаграмм, специфицирующих структурные, функциональные, поведенческие особенности сети, в частности, (1) диаграмм классов – для определения видов сущностей БСС и отношений между ними, в том числе отношения иерархии; (2) диаграмм сетевой архитектуры – для задания структуры конкретной сети и экземпляров ее устройств, а также задания физических и логических связей между узлам сети, их типов, ролей; (3) диаграмм последовательности – позволяющих специфицировать сценарии работы сети, процессы и протоколы взаимодействия ее элементов, в том числе процессы аутентификации узлов сети, процессы динамической маршрутизации в сети и пр.

Выбор обоих типов моделей представления обусловлен их возможностями по отображению информации о БСС, удобному для дальнейшего их использования при решении задач, запланированных на второй этап настоящего Проекта.

А именно, структурно-функциональные и процессные представления в виде соответствующих UML-диаграмм в рамках решаемых задач анализа защищенности в большей степени подходят для выражения семантики структуры, функций и процессов сети. В частности, такие диаграммы целесообразно использовать в качестве формализованных, но, тем не менее, достаточно наглядных форм для экспертного анализа сети – анализа возможных связей, информационных потоков в сети, функциональных и логических отношений и зависимостей между объектами сети, анализа особенностей процессов распространения и передачи информации и анализа защищенности.

В отличие от UML-диаграмм, модели представления на основе JSON-формата в рамках задачи анализа защищенности в большей степени ориентированы на формальную спецификацию технических характеристик сети и их значений с последующим использованием этих данных в рамках автоматизированных средств анализа защищенности программно-аппаратных компонентов БСС, в том числе формирование тестовых векторов данных и наборов правил функциониро-

вания сети и правил политик безопасности сети для проведения процессов верификации и валидации процессов и данных сети, а также для детектирования различных аномалий в беспроводной сети.

Заключение

В статье представлен обзор работ, затрагивающих вопросы моделирования и анализа угроз информационной безопасности беспроводных сенсорных сетей. Проведенный анализ показал разнородность существующих угроз и необходимость комплексного подхода к их анализу с учетом уязвимостей, которые могут эксплуатироваться нарушителем в процессе атаки и проявляться на различных уровнях сетевого взаимодействия.

Анализ программных средств, пригодных для моделирования беспроводных сенсорных сетей и угроз информационной безопасности позволил установить целесообразность применения комплексного подхода к моделированию с использованием различных видов представления и способов обработки данных. Кроме того, каждый их приведенных методов моделирования, обладая своими достоинствами и недостатками, позволяет получить оценку защищенности сети в заданных ограничениях. Для обеспечения процесса моделирования и подготовки исходных данных в работе были предложены две модели представления БСС.

Отметим, что имитационное моделирование позволяет воспроизвести динамически основные процессы, проистекающие в сети без необходимости привлечения значительных аппаратных и вычислительных ресурсов, которых может не быть в наличие. Такой вид моделирования позволяет в частности, смоделировать угрозы, связанные с процессами масштабирования БСС. Отметим, что в общем случае натурное моделирование является наиболее приближенным к реальным условиям функционирования сети, и поэтому является наиболее адекватным. Вместе с тем, возможная техническая и организационная сложность некоторых видов атак оказывается существенным препятствием для их моделирования при помощи натурного моделирования [15].

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

Литература/References

1. Pathan, A. S. K.; Lee, H.-W.; Hong, C. S. Security in wireless sensor networks: issues and challenges // Proceedings of 8th International Conference Advanced Communication Technology. 2006. pp. 1043–1048.

2. Undercoffer, J.; Avancha, S.; Joshi, A.; Pinkston J. Security for Sensor Networks // Proceedings of CADIP Research Symposium. 2002.

3. Khan, M. A.; Khan, M. A Review on Security Attacks and Solution in Wireless Sensor Networks // American Journal of Computer Science and Information Technology. 2019. Volume 7. No. 1:31.

4. Becher, A.; Benenson, Z.; Dornseif, M. Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks // Security in Pervasive Computing. SPC 2006. Springer. Lecture Notes in Computer Science. 2006. Vol. 3934.

5. Wang, Y.; Attebury, G.; Attebury, G. A Survey of Security Issues In Wireless Sensor Networks // CSE Journal Articles. 2006. Volume 8. No. 2. pp. 2–22.

6. Karlof, C.; Wagner, D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures // Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications. 2003. pp. 113–127.

7. Pathan, A-S. K., Hong, C. S. Security Attacks and Challenges in Wireless Sensor Networks // Encyclopedia on Ad Hoc and Ubiquitous Computing. 2009. pp. 397–425.

8. Newsome, J., Shi, E., Song, D., Perrig, A. The sybil attack in sensor networks: analysis & defenses // Proceedings of the third international symposium on Information processing in sensor networks. ACM. 2004. pp. 259–268.

9. Ghugar, U.; Pradhan, J. A Study on Black Hole Attack in Wireless Sensor Networks // Proceedings of Conference: National Conference on Next Generation Computing and its Applications in Science & Technology (NGCAST)-2016, At IGIT, SARANG. 2016. Volume 5.

10. Kumar, S.; Duttagupta, S.; Rangan, V. P.; Ramesh M. V. Reliable network connectivity in wireless sensor networks for remote monitoring of landslides // The Journal of Mobile Communication, Computation and Information. Wireless Networks. 2019. pp. 1–16.

11. Xue, Y.; Lee, H. S.; Yang, M.; Kumarawadu, P.; Ghenniwa, H. H.; Shen, W. Performance Evaluation of NS-2 Simulator for Wireless Sensor Networks // Canadian Conference on Electrical and Computer Engineering (CCECE 2007). 2007. pp. 1372–1375.

12. Girod, L.; Elson, J.; Cerpa, A.; Stathopoulos, T.; Ramanathan, N.; Estrin, D. EmStar: a Software Environment for Developing and Deploying Wireless Sensor Networks // USENIX Technical Conference. 2004.

13. Yi, S.; Min, H.; Cho, Y.; Hong, J. SensorMaker: A Wireless Sensor Network Simulator for Scalable and Fine-Grained Instrumentation // Computational science and its application-ICCSA. 2008. Volume 5072/2008. pp. 800–810.

14. Chhimwa,l P.; Rai, D. S., Rawat, D. Comparison between Different Wireless Sensor Simulation Tools // IOSR Journal of Electronics and Communication Engineering (IOSR-JECE). 2013. Volume 5. Issue 2. pp. 54–60.

15. Desnitsky, V. A.; Kotenko, I. V. Modeling and analysis of security incidents for mobile communication mesh ZigBee-based network // Proceedings of 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM). 2017. pp. 500–502.

Десницкий Василий Алексеевич – кандидат технических наук, доцент кафедры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук Санкт-Петербургского Федерального исследовательского центра Российской академии наук, desnitsky@comsec.spb.ru

Desnitsky Vasily – Candidate of Engineering Sciences, Associate Professor, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications; senior re-search fellow in laboratory of computer security problems of St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg Federal Research Center Russian Academy of Sciences, desnitsky@comsec.spb.ru