НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2016 Том 16 № 3 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2016 Vol. 16 No 3 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.021

ИССЛЕДОВАНИЕ ДОСТУПНОСТИ УДАЛЕННЫХ УСТРОЙСТВ БЕСПРОВОДНЫХ СЕТЕЙ

Н.А. Бажаев[a], И.Е. Кривцова[a], И.С. Лебедев[a]

(*публикуется в порядке дискуссии*)

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: nurzhan_nfs@hotmail.com

Информация о статье
Поступила в редакцию 11.01.16, принята к печати 10.04.16
doi: 10.17586/2226-1494-2016-16-3-467-473
Язык статьи – русский

Ссылка для цитирования: Бажаев Н.А., Кривцова И.Е., Лебедев И.С. Исследование доступности удаленных устройств беспроводных сетей // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 3. С. 467–473. doi: 10.17586/2226-1494-2016-16-3-467-473

Аннотация

Рассмотрена беспроводная сеть, подвергающаяся атаке, направленной на организацию «широковещательного шторма», с целью определения доступности автономных узлов, способности выполнения возложенных на них функциональных задач при информационном воздействии. Определен ряд условий для организации атак данного типа со стороны потенциального нарушителя информационной безопасности. Проведен анализ доступности устройств систем, базирующихся на беспроводных технологиях. Рассмотрено удаленное устройство беспроводной самоорганизующейся сети как система массового обслуживания *M*/*M*/*1*/*n*. Показаны модельные зависимости функционирования системы в обычном состоянии и при осуществлении информационного воздействия на систему со стороны потенциального нарушителя. Проведено аналитическое моделирование функционирования беспроводной сети в обычном режиме и при проведении атаки, направленной на организацию «широковещательного шторма». Проведен эксперимент, обеспечивающий получение статистической информации о работе удаленных устройств беспроводной сети. Представлены результаты эксперимента проведения атаки типовой системы, осуществляющей передачу данных, с помощью широковещательного пакета сканирования сети при различных значениях интенсивностей шумовых сообщений со стороны нарушителя информационной безопасности. Предложенная модель может быть использована для определения технических характеристик устройств беспроводной самоорганизующейся сети и выработки рекомендаций по конфигурации узлов, направленных на противодействие «широковещательному шторму».

Ключевые слова

информационная безопасность, беспроводные сети, мультиагентные системы, уязвимость, доступность устройств, модель информационной безопасности

AVAILABILITY RESEARCH OF REMOTE DEVICES FOR WIRELESS NETWORKS

N.A. Bazhayev[a], I.E. Krivtsova[a], I.S. Lebedev[a]

(*published as a discussion*)

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: nurzhan_nfs@hotmail.com

Article info
Received 11.01.16, accepted 10.04.16
doi: 10.17586/2226-1494-2016-16-3-467-473
Article in Russian

For citation: Bazhayev N.A., Krivtsova I.E., Lebedev I.S. Availability research of remote devices for wireless networks. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2016, vol. 16, no. 3, pp. 467–473. doi: 10.17586/2226-1494-2016-16-3-467-473

Abstract

We consider the wireless network under attack, aimed at "broadcast storm" initiation, in order to determine the availability of stand-alone units and the ability to carry out their functional tasks under information exposure. We determine a set of conditions for such type of attacks on the part of potential information interloper. The functional analysis of the systems based on wireless technology is made. We examine the remote device of a self-organizing wireless network as a queuing system *M*/*M*/*1*/*n*. Model dependencies are shown for normal system performance and at information exposure on the part of potential information interloper. Analytical simulation of wireless network functioning is carried out in the normal mode and

under the attack aimed at "broadcast storm" initiation. An experiment is described which provides statistical information on operation of network remote devices. We present experiment results on carrying out attack at typical system transferring data by broabcast net scanning package at different noise intensities on the part of information interloper. The proposed model can be used to determine the technical characteristics of wireless ad-hoc network, develop recommendations for node configuration, aimed at countering "broadcast storm".

Keywords
information security, wireless networks, multi-agent systems, vulnerability, device availability, information security model

Введение

Постоянное снижение стоимости устройств беспроводных сетей и повышение показателей временных, энергетических, информационных характеристик датчиков и сенсоров позволяет использовать эти технологии в ряде перспективных направлений автоматизированных систем управления технологическим процессом – «Умный город», «Умный дом», «Интернет вещей». Гибкая архитектура, достаточная вычислительная мощность отдельных узлов позволяют не только переориентироваться с типовых проводных устройств, но и осуществлять построение относительно самодостаточных мультиагентных систем, выполняющих прием, обработку, анализ принимаемых и передаваемых данных.

Внедрение самоорганизующихся беспроводных сетей сопровождается необходимостью решения дополнительных проблемных вопросов обеспечения информационной безопасности (ИБ) [1, 2].

Среди основных уязвимостей можно выделить возможность прослушивания каналов, посылка «внешних» сообщений, осуществление физического доступа злоумышленника к узлу, недостаточная стандартизация интеллектуальных алгоритмов маршрутизации, учитывающих состояние сети. Большое количество устройств, обеспечивающих интеллектуальную передачу, сбор, обработку информационных пакетов, их относительная удаленность, автономность функционирования, динамически изменяющаяся топология, слабая проработка моделей, методов и алгоритмов оперативного обнаружения некорректной информации от скомпрометированных узлов определяют сложность создания классических систем защиты [3–5].

Некоторые из потенциально возможных уязвимостей связаны с особенностями функционирования отдельных узлов, например, необходимость обмена служебной информацией при возникновении ряда внутренних и внешних событий вызывает рассылку широковещательных сообщений между узлами сети и повышение объема «мусорного трафика».

Постановка задачи исследования

Типовой узел сети включает в себя приемо-передающее устройство, элемент питания, процессорный модуль, к которому могут быть подключены различные датчики. В виду подобной структуры возникает необходимость эффективного решения задач, связанных с сохранением энергии, обеспечением вычислительных мощностей системы и пропускных характеристик каналов [6]. Совокупное решение перечисленных задач приводит к присутствию в большинстве протоколов ряда проблемных вопросов имплозии, наложения и слепых ресурсов, что делает подобные технологии уязвимыми для проведения ряда атак со стороны злоумышленника [7, 8].

Основываясь на особенностях функционирования беспроводных сенсорных сетей и применяя рекомендуемые настройки, направленные на оптимизацию работы удаленного узла беспроводной сети, нарушитель может реализовать атаку типа «широковещательный шторм» [9–11].

Технология проведения этой атаки связана с использованием уязвимостей, которые приводят к большому увеличению служебных сообщений в сети. В простейшем случае, если позволяют правила, заданные системным администратором, для роста мусорного трафика могут генерироваться широковещательные сообщения. Анализ [6, 8, 10] позволяет выявить ряд условий в конфигурационных настройках для проведения данного типа атак:

- длительный интервал времени жизни пакета;
- наличие правил, позволяющих передавать кадр с широковещательным адресом всем, кроме узла от которого он ушел;
- внедрение устройств, непрерывно генерирующих сообщения.

Особо необходимо отметить, что для совершения деструктивных воздействий потенциальный нарушитель может обладать минимальными возможностями по рассылке некорректных сообщений. В результате тратятся ресурсы на прием, передачу, обработку служебной информации, находящаяся под нагрузкой беспроводная сенсорная сеть не только не выполняет свои функции, но и становится неуправляемой [9]. Отсутствует возможность оперативного доступа и управления автономными устройствами, которые без остановки реагируют на события в сети. Происходит реализация угрозы доступности устройств беспроводной сети из-за преднамеренных действий со стороны злоумышленника по увеличению количества широковещательных и других служебных сообщений, в результате чего блокируется доступ к каналам связи и узлам вычислительной системы. Подавляющее большинство моделей, описывающих протекающие в беспроводной сети процессы, не учитывает возможность информационного воздействия со стороны потенциального злоумышленника.

Таким образом, при обеспечении ИБ беспроводной сети возникает задача вероятностной оценки доступности устройств, подвергающейся атаке типа «широковещательный шторм».

Моделирование воздействия на систему

Проведение атаки со стороны злоумышленника сводится к увеличению интенсивности поступления заявок, приводящей к невозможности обслуживания суммарного потока сообщений устройством. Такое состояние может возникать в случае при заполнении конфигурируемого буфера устройства, имеющего заданный объем, или недоступности канала, что приводит к потере заявки. Возникает угроза доступности, связанная с ограничениями на санкционированный доступ к элементам сети, хранимой информации, потокам данных, к услугам и приложениям из-за событий, влияющих на сеть [10].

Примером относительно простых, не обладающих большой вычислительной мощностью устройств беспроводной сети, которые могут быть подвергнуты атаке, являются технологии ZigBee, имеющие ограниченный функционал, принимающие и передающие небольшой ограниченный набор типов сообщений без приоритетов с заранее сконфигурированными параметрами. Длительность обслуживания в них зависит от числа событий в заданном интервале времени. Допустив, что процесс поступления заявок на устройство в определенных конфигурациях системы является пуассоновским, а длительность обслуживания распределена по экспоненциальному закону. Тогда становится возможным рассмотреть процессы сбора, обработки и передачи информации как систему массового обслуживания *M*/*M*/*1*/*n*.

Особенности аппаратной реализации автономных удаленных узлов беспроводных сетей предполагают наличие буфера, который позволяет хранить несколько сообщений, поступивших на обработку.

Применяя теорию систем массового обслуживания, можно предположить, что вероятность потери сообщения в обычном режиме работы системы, не подвергающейся воздействию со стороны злоумышленника, при передаче от A к B через одно устройство C будет определяться по формуле (1):

$$P_{loss} = \rho^m \frac{1-\rho}{1-\rho^{m+1}},\ \rho = \frac{\lambda}{\mu}, \tag{1}$$

где λ – интенсивность входного потока; μ – интенсивность обслуживания; m – размер входного буфера устройства обработки.

В процессе передачи информации в беспроводной сети информационный поток проходит через несколько подобных устройств. Для оценки вероятности потери сообщения, проходящего через k устройств, выражение (1) примет вид

$$P_{loss} = 1 - \left(1 - \rho^m \frac{1-\rho}{1-\rho^{m+1}}\right)^k, \tag{2}$$

Большинство реализуемых вероятностных моделей оценки систем не предполагает наличие потенциального злоумышленника, действия которого направлены на использование уязвимостей используемых протоколов и узлов системы. Однако определенная открытость и доступность сети позволяет нарушителю осуществлять действия по увеличению интенсивности рассылки сообщений, не содержащих корректной информации, с плохой контрольной суммой, неправильным заголовком, которые приводят к неоправданной трате ресурсов со стороны системы.

На рис. 1 представлено воздействие на последовательность цепочки устройств, передающих информационные сообщения с интенсивностью λ_p. Злоумышленник в сети увеличивает число событий, вызывающих генерацию широковещательных сообщений, с интенсивностью λ_{sh}.

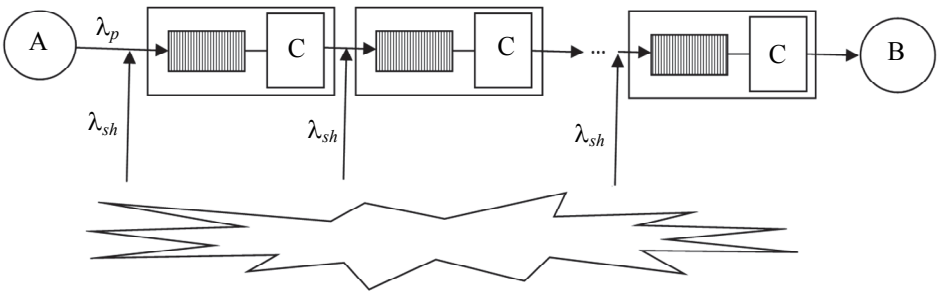

Рис. 1. Воздействие на цепочку устройств

Поступившее широковещательное сообщение обрабатывается устройством беспроводной сети и ретранслируется на следующий узел. При наличии у лица, оказывающего деструктивное воздействие, достаточно мощного передатчика возможно одновременное воздействие на множество узлов беспровод-

ной сети. Используя выражения (1) и (2), вероятность потери сообщения в сети, подверженной атаке типа «широковещательный шторм» при условии стационарного режима, можно представить в виде следующего выражения:

$$\begin{cases} P_{loss} = 1 - \left(1 - \left(\dfrac{\lambda_p + \lambda_{sh}}{\mu}\right)^m \dfrac{1 - \left(\dfrac{\lambda_p + \lambda_{sh}}{\mu}\right)}{1 - \left(\dfrac{\lambda_p + \lambda_{sh}}{\mu}\right)^{m+1}}\right) \prod_{k=2}^{r} \left(1 - \left(\dfrac{\lambda_p + k\lambda_{sh}}{\mu}\right)^m \dfrac{1 - \left(\dfrac{\lambda_p + k\lambda_{sh}}{\mu}\right)}{1 - \left(\dfrac{\lambda_p + k\lambda_{sh}}{\mu}\right)^{m+1}}\right), k \geq 2; \\ P_{loss} = 1 - \left(1 - \left(\dfrac{\lambda_p + \lambda_{sh}}{\mu}\right)^m \dfrac{1 - \left(\dfrac{\lambda_p + \lambda_{sh}}{\mu}\right)}{1 - \left(\dfrac{\lambda_p + \lambda_{sh}}{\mu}\right)^{m+1}}\right), k = 1, \end{cases} \quad (3)$$

где λ_p – интенсивность полезного трафика; λ_{sh} – интенсивность формируемого нарушителем ИБ шумового трафика; k – номер в последовательности устройств, встречающихся на пути информационного сообщения; r – общее количество устройств, встречающихся на пути информационного сообщения.

На рис. 2 приведены зависимости вероятности потери сообщения в сети от: λ_{sh} – интенсивности шумового трафика формируемого нарушителем ИБ (для соотношений $\lambda_{sh}1 < \lambda_{sh}2 < \lambda_{sh}3$), λ_p – интенсивности полезного трафика (для соотношений $\lambda_p 1 < \lambda_p 2 < \lambda_p 3$), μ – интенсивности обслуживания (для соотношений $\mu 1 < \mu 2 < \mu 3$).

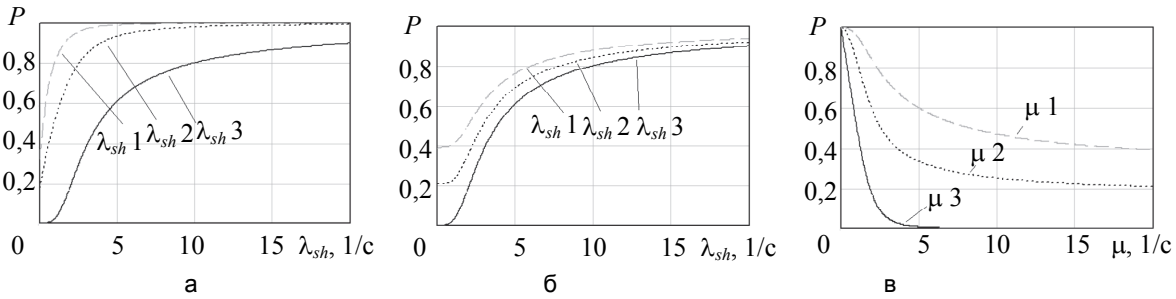

Рис. 2. Зависимости вероятности потери информационного сообщения при изменении: интенсивности шумового трафика, формируемого нарушителем информационной безопасности (а); интенсивности, с учетом действий нарушителя информационной безопасности: полезного трафика λ_p (б); обслуживания μ (в)

Несмотря на ограничивающие возможности допущенных предположений, характерных для математического аппарата систем массового обслуживания, подобные модели позволяют оценить вероятностное состояние системы и показатели, характерные для ее функционирования в агрессивных режимах и средах с учетом злоумышленника. Применительно к рассматриваемому типу атак, модель учитывает возможности лица, осуществляющего воздействие, по интенсивности событий, вызывающих генерацию широковещательных пакетов.

Эксперимент

Для реализации эксперимента была сконфигурирована беспроводная сеть на основе устройств Telegesis, представленная на рис. 3, состоящая из нескольких узлов. От узла A к узлу B через устройства беспроводной сети U передавались сообщения со скоростью 250 кбит/с. Узел C содержал сниффер, генерирующий широковещательные пакеты.

Цель эксперимента состояла в получении количественных показателей доступности оконечного устройства. В качестве метрики использовался процент потерянных сообщений. Каждый узел мог принимать сообщения только от двух узлов, одним из которых был сниффер, рассылающий широковещательные сообщения, а другим – узел, обеспечивающий информационный трафик путем ретрансляции всех принятых пакетов. На оконечном узле анализировались принимаемые сообщения и определялась статистика потерянных и нераспознанных сообщений.

Процент потерянных и нераспознанных информационных сообщений в сконфигурированном канале связи для скорости 250 кбит/с при различных частотах генерации сообщений, опрашивающих узлы в сети, от сниффера (7, 10, 14 сообщений в секунду) представлен на рис. 4, 5.

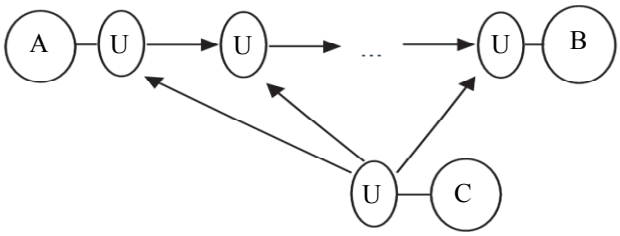

Рис. 3. Схема системы для проведения эксперимента

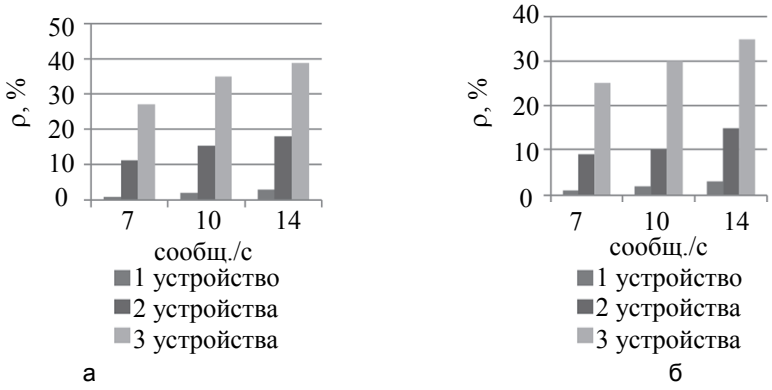

Рис. 4. Потери сообщений ρ (%) в зависимости от количества устройств, частоты передачи (7, 10, 14 сообщений в секунду) широковещательных команд типа: запрос информации о параметрах устройств AT+N (а); запрос идентификаторов взаимодействующих соседей AT+SN:00 (б)

Анализ полученных результатов эксперимента

Сравнивая графики теоретической вероятности P_{loss} потери сообщений рис. 5 и значения в таблице с гистограммами на рис. 4, можно составить качественное представление о близости теоретического и экспериментального распределений вероятности потери сообщений при различных значениях λ_{sh}.

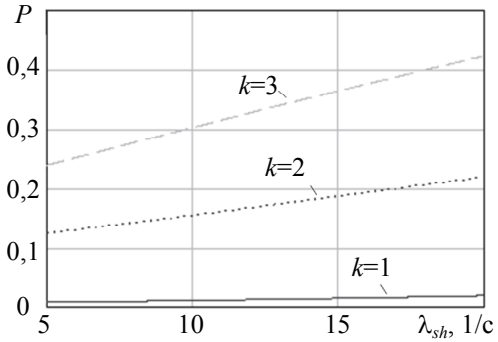

Рис. 5. Модельные зависимости для экспериментальных значений

Параметр	Значения для эксперимента
λ_p	120 сообщений в секунду
λ_{sh}	от 1 до 16
μ	180 сообщений в секунду
m	размер буфера 10 сообщений
k	1, 2, 3

Таблица. Значения параметров для построения модельных зависимостей и получения статистических данных эксперимента

На рис. 6 приведены гистограммы экспериментальных значений потерь сообщений при различных значениях λ_{sh} для k=3 устройств.

Проверка статистической гипотезы о том, что полученное экспериментальное распределение не отличается от теоретического, проводилась на уровне значимости α=0,05 по критерию Пирсона (χ^2-критерию):

$$\chi_{\nu}^2 = \sum_{j=1}^{l} \frac{(n_j^* - np_j)^2}{np_j} \qquad (4)$$

при числе степеней свободы ν=9, объеме выборки n=100 сообщений, числе интервалов разбиения l=12.

Известно [12], что число событий np_j в формуле (4), ожидаемых в интервалах значений параметра λ_{sh}, может быть равным 3 или 2, если $l \geq 10$. Исходя из этого, в соответствии с формулой (3), например, при k=3 достаточно, чтобы $\lambda_{sh} \geq 5$. Критическое значение критерия найдено по соответствующей таблице [12] и равно $\chi^2_{кр}$=16,92. Экспериментальное значение критерия $\chi^2_{экс}$ вычислено по формуле (4) и равно 4,427 и 1,425 для широковещательных сообщений AT+N и AT+N:00 соответственно. При этом в обоих случаях выполняется неравенство $\chi^2_{экс} < \chi^2_{кр}$. Отсюда следует, что на уровне значимости α=0,05 можно утверждать, что расхождения между теоретическим P_{loss} и экспериментальным ρ распределениями вероятности потери сообщений в сети, подверженной широковещательному шторму, при различных указанных значениях интенсивности шумового трафика λ_{sh} статистически недостоверны.

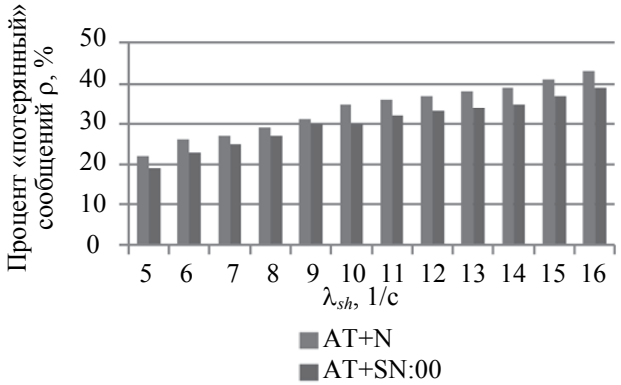

Рис. 6. Экспериментальные значения потерь сообщений ρ (%) для k=3

Таким образом, предположения о пуассоновском потоке процесса поступления заявок и экспоненциальном распределении длительности обслуживания подтверждены данными статистического анализа нагрузки беспроводных сетей.

Заключение

Повсеместное появление беспроводных сетей и возможность их обнаружения вне контролируемой зоны делают их очень привлекательной мишенью для попыток проведения различного рода атак. Потенциальный злоумышленник, имеющий сканер радиоэфира, протокольный сканер, программное обеспечение для декодирования защитного ключа, обладает достаточными возможностями по организации подслушивания, радиоперехвата и организации простейших атак на сеть.

Реализация большого числа проектов на базе технологий Bluetooth, ZigBee, WiFi, их применение в интеллектуальных транспортных системах, локальных сетях, сенсорных сетях вызывает необходимость обеспечения требуемого уровня безопасности циркулирующих в них данных [13–17].

Предлагаемая модель дает возможность исследовать доступность устройств беспроводной сети, подверженной атаке «широковещательный шторм», основываясь на показателях интенсивностей передаваемых и принимаемых информационных сообщений, что позволяет оценить доступность устройств при различных значениях длины, интенсивности пакетов, размера буфера устройств, ограничивающих «конечность тех или иных системных ресурсов».

Предложенная модель учитывает характеристики поведения злоумышленника и не требует значительных затрат вычислительных ресурсов и постановки специальных вычислительных экспериментов, при выявлении общих закономерностей в поведении системы.

Литература

1. Kumar P., Ylianttila M., Gurtov A., Lee S.-G., Lee H.-J. An efficient and adaptive mutual authentication framework for heterogeneous wireless sensor networks-based applications // Sensors. 2014. V. 14. P. 2732–2755. doi: 10.3390/s140202732
2. Sridhar P., Sheikh-Bahaei S., Xia S., Jamshidi Mo. Multi agent simulation using discrete event and soft-computing methodologies // Proc. IEEE Int. Conf. on Systems, Man and Cybernetics. 2003. V. 2. P. 1711–1716.
3. Page J., Zaslavsky A., Indrawan M. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities // Proc. of the First International Workshop on Safety and Security in Multi-Agent Systems (SASEMAS 2004), 2004. P. 85–101.

4. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5 (87). С. 149–154.
5. Zikratov I.A., Lebedev I.S., Gurtov A.V. Trust and reputation mechanisms for multi-agent robotic systems // Lecture Notes in Computer Science. 2014. V. 8638. P. 106–120. doi: 10.1007/978-3-319-10353-2_10
6. Wyglinski A.M., Huang X., Padir T., Lai L., Eisenbarth T.R., Venkatasubramanian K. Security of autonomous systems employing embedded computing and sensors // IEEE Micro. 2013. V. 33. N 1. P. 80–86. doi: 10.1109/MM.2013.18
7. Lebedev I.S., Korzhuk V.M. The monitoring of information security of remote devices of wireless networks // Lecture Notes in Computer Science. 2015. V. 9247. P. 3–10. doi: 10.1007/978-3-319-23126-6_1
8. Prabhakar M., Singh J.N., Mahadevan G. Nash equilibrium and Marcov chains to enhance game theoretic approach for vanet security // Proc. Int. Conf. on Advances in Computing (ICAdC 2012). Bangalore, Karnataka, India, 2012. V. 174. P. 191–199. doi: 10.1007/978-81-322-0740-5_24
9. Korzun D.G., Nikolaevskiy I., Gurtov A.V. Service intelligence support for medical sensor networks in personalized mobile health systems // Lecture Notes in Computer Science. 2015. V. 9247. P. 116–127. doi: 10.1007/978-3-319-23126-6_11
10. Рекомендация МСЭ-Т X.805. Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами. 2003.
11. Nikolaevskiy I., Lukyanenko A., Polishchuk T., Polishchuk V.M., Gurtov A.V. isBF: Scalable in-packet bloom filter based multicast // Computer Communications. 2015. V. 70. P. 79–85. doi: 10.1016/j.comcom.2015.05.002
12. Куликов Е.И. Прикладной статистический анализ: учебное пособие для вузов. 2-е изд. М.: Горячая линия-Телеком, 2008. 464 с.
13. Комов С.А. и др. Термины и определения в области информационной безопасности. М.: АС-Траст, 2009. 304 с.
14. Kumar P., Gurtov A.V., Linatti J., Ylianttila M., Sain M. Lightweight and secure session-key establishment scheme in smart home environments // IEEE Sensors Journal. 2015. V. 16. N 1. P. 254–264. doi: 10.1109/JSEN.2015.2475298
15. Al-Naggar Y., Koucheryavy A. Fuzzy logic and Voronoi diagram using for cluster head selection in ubiquitous sensor networks // Lecture Notes in Computer Science. 2014. V. 8638. P. 319–330. doi: 10.1007/978-3-319-10353-2_28
16. Chehri A., Moutah H.T. Survivable and scalable wireless solution for E-health and emergency applications // Proc. 1st Int. Workshop on Engineering Interactive Computing Systems for Medicine and Health Care (EICS4MED 2011). Pisa, Italy, 2011. P. 25–29.
17. Омётов А.Я., Кучерявый Е.А., Андреев Д.С. О роли беспроводных технологий связи в развитии "Интернета вещей" // Информационные технологии и телекоммуникации. 2014. № 3 (7). С. 31–40.

Бажаев Нуржан Аманкулулы – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, nurzhan_nfs@hotmail.com

Кривцова Ирина Евгеньевна – старший преподаватель, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ikr@cit.ifmo.ru

Лебедев Илья Сергеевич – доктор технических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, lebedev@cit.ifmo.ru

Nurzhan Bazhayev – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, nurzhan_nfs@hotmail.com

Irina E. Krivtsova – senior lecturer, ITMO University, Saint Petersburg, 197101, Russian Federation, ikr@cit.ifmo.ru

Ilya S. Lebedev – D.Sc., Associate professor, Associate professor, ITMO University, Saint Petersburg, 197101, Russian Federation, lebedev@cit.ifmo.ru