Система обнаружения атак в беспроводных сенсорных сетях промышленного Интернета*

В.И. Васильев[I], А.М. Вульфин[I], В.М. Картак[I], А.Д. Кириллова[I], К.В. Миронов[I]

[I] Уфимский государственный авиационный технический университет, г. Уфа, Россия

Аннотация. Целью исследования является повышение эффективности функционирования системы обнаружения сетевых атак за счет применения алгоритмов нейросетевого анализа сетевого трафика в беспроводной сенсорной сети промышленного мониторинга и управления. Решаются задачи разработки структурной схемы системы обнаружения сетевых атак и алгоритмов интеллектуального анализа сетевого трафика. Выполнена оценка эффективности предложенного алгоритма анализа на натурных данных.

Ключевые слова: *система обнаружения сетевых атак, беспроводные сенсорные сети, интеллектуальный анализ данных.*

DOI: 10.14357/20790279190409

Введение

На сегодняшний день осуществляется переход на автоматизированное цифровое производство, управляемое интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой, выходящее за границы одного предприятия, с перспективой объединения в глобальную промышленную сеть вещей и услуг. Данный подход развивается в концепции «Индустрия 4.0» и характеризует текущий тренд развития автоматизации и обмена данными, который включает в себя киберфизические системы, Интернет вещей и облачные вычисления [1, 2, 3]. Существует множество преимуществ использования беспроводных сенсорных сетей (WSN, Wireless sensor network) как среды беспроводного взаимодействия цифровых объектов в составе сети промышленного интернета вещей в различных автоматизированных системах [4, 5, 6]:

– возможность расположения в труднодоступных местах, где сложно и дорого применять проводные технологии;
– оперативность и удобство развертывания и обслуживания системы;
– высокий уровень проникновения сквозь препятствия и стойкость к электромагнитным помехам.

Примером данного подхода является использование беспроводных сенсорных сетей на электрических подстанциях [1, 2, 7, 8, 9]. Компактность и автономность сенсорных узлов позволяют установить их в труднодоступные места без решения задач организации проводных каналов связи для передачи телеметрической информации такой, как: перетоки в энергетической системе, контроль активной и реактивной мощности, частота и напряжение на определенных участках на диспетчерский пункт. Из-за перехода от проводных к беспроводным сетевым технологиям для сбора данных телеметрии защищенность сети определяется не только аппаратными и программными решениями для промышленных контроллеров и сенсорных узлов, но и выбранными принципами их информационного взаимодействия в процессе синтеза топологии сети, определения параметров маршрутизации и передачи данных.

Целью приведенных ниже исследований является повышение эффективности функционирования системы обнаружения сетевых атак за счет применения алгоритмов нейросетевого анализа сетевого трафика в беспроводной сенсорной сети промышленного мониторинга и управления. Для достижения поставленной цели необходимо решить следующие задачи:

– разработка структурной схемы системы обнаружения сетевых атак на основе алгоритмов интеллектуального анализа данных;

* Работа выполнена при финансовой поддержке РФФИ, грант № 17-48-020095.

– разработка алгоритма анализа сетевого трафика в составе модуля анализа сетевого трафика в беспроводной сенсорной сети;
– оценка эффективности предложенного решения на натурных данных.

1. Анализ подходов к решению задачи защиты информации в беспроводных сенсорных сетях

Беспроводная сенсорная сеть [4, 8] состоит из большого количества автономных сенсорных узлов, распределенных в зонах промышленной системы, представляющих интерес для сбора оперативных данных и совместной передачи собранных данных по беспроводным каналам в центральный узел, являющийся узлом или базовой станцией

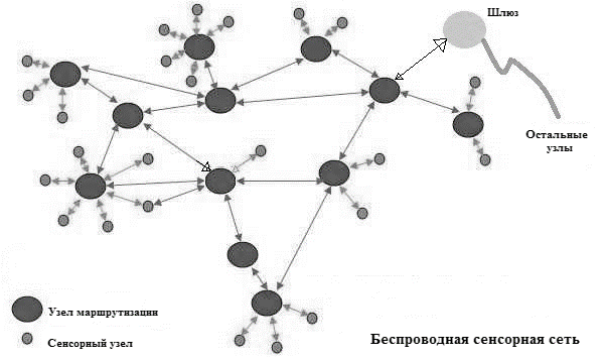

Рис. 1. Структура беспроводной сенсорной сети

(BS). Схематично часть такой сети представлена на рисунке 1.

Большинство угроз информационной безопасности в беспроводных сетях схожи с угрозами и атаками на проводные сети, за исключением того, что беспроводные сети труднее защитить, вследствие использования открытой среды в качестве канала передачи данных и широковещательной природы беспроводных соединений. Защита сети осложняется из-за ограниченных ресурсов: энергии автономного источника питания и вычислительных ресурсов. Такие предельные характеристики делают традиционные меры безопасности, к примеру – использование сложных алгоритмов шифрования, многофакторной аутентификации, межсетевые экраны и т.п. [5, 10, 11] – не всегда достаточными. Существенным фактором являются требования к временным задержкам при передаче данных в транспортной среде и закрытые протоколы функционирования программного и аппаратного обеспечения АСУ ТП, которые не всегда позволяют внедрить технологии защиты с использованием IPSec, SSL, VPN.

Современная тенденция развития транспортной среды промышленных сетей заключается в использовании самоорганизующихся беспроводных сетей с равноправием узлов, динамически меняющейся топологией, возможностью реконфигурации, самовосстановлением, динамической маршрутизацией и т. д.

Классификация атак на беспроводные сенсорные сети по направлению воздействия приведена на рисунке 2 [5, 12-17].

Возможная классификация атак на беспроводные сенсорные сети с акцентом на активные атаки, затрагивающие параметры маршрутизации, представлена на рисунке 3.

Активные атаки представляют собой различные модификации данных во время коммуникации, осуществляемые неавторизованными лицами. Наибольший интерес представляют атаки маршрутизации, реализуемые на сетевом уровне. Наиболее часто встречающиеся атаки представлены в таблице 1.

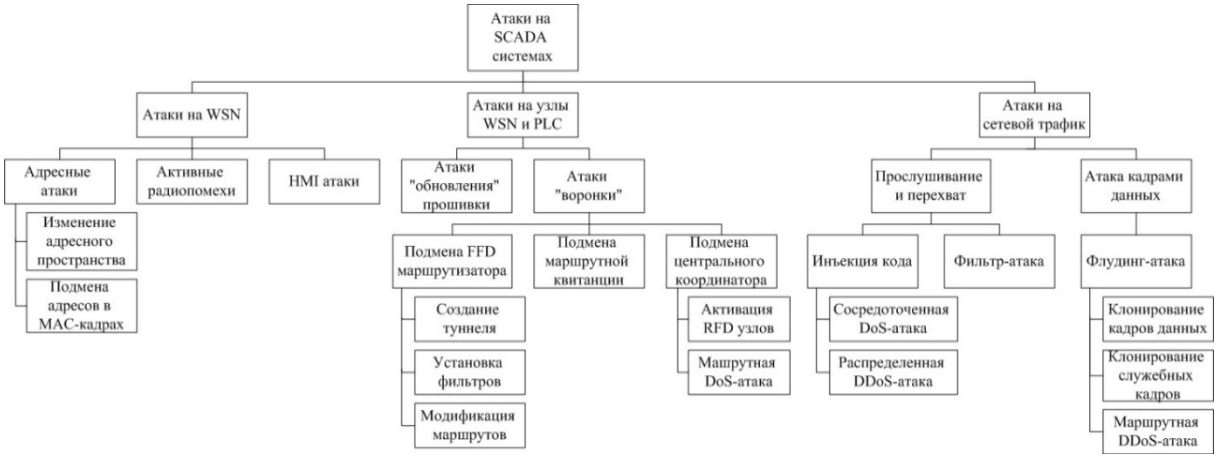

Рис. 2. Классификация атак в промышленных беспроводных сенсорных сетях по направлению воздействия

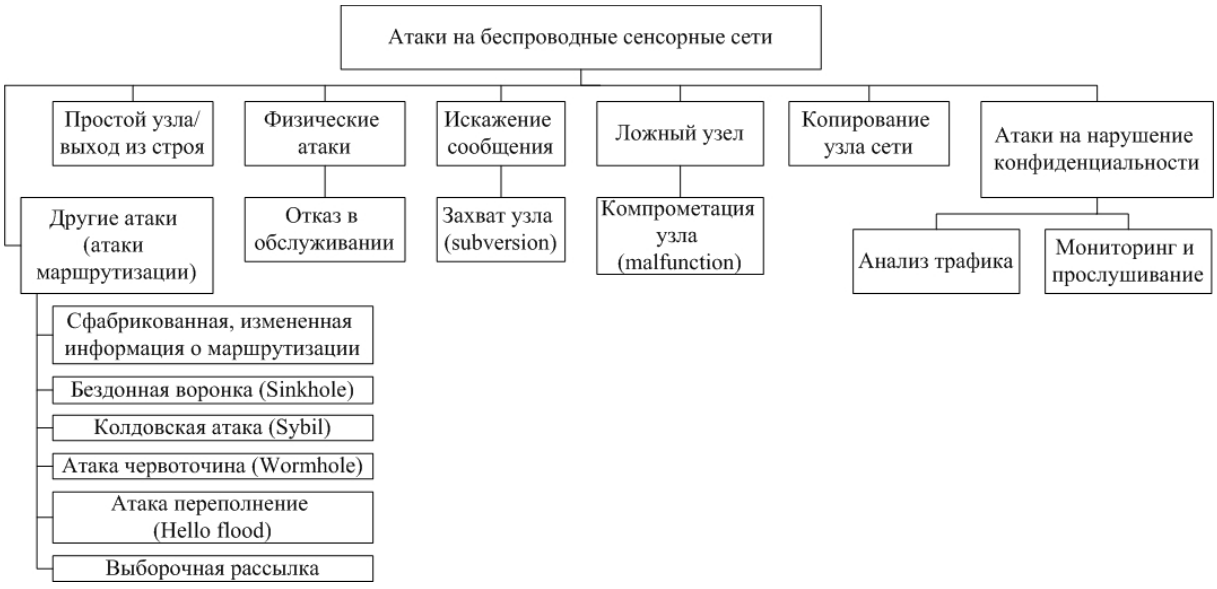

Рис. 3. Классификация атак на беспроводные сенсорные сети

Табл. 1

Классификация атак в промышленных беспроводных сенсорных сетях по направлению воздействия [4, 5, 12, 13, 18]

Тип атаки	Описание
Измененная маршрутная информация	Наибольшая угроза для децентрализованных сетей; Последствия: увеличение времени доставки пакета данных;
Выборочная рассылка	Поврежденный узел сенсорной сети способен избирательно стирать необходимые пакеты. Последствия: нарушение целостности и доступности данных;
Атака «бездонная воронка» (Sinkhole Attack)	Поврежденный узел сети меняет свое нормальное поведение в системе и начинает перенаправлять на себя весь трафик сенсорной сети, напоминая «воронку». Последствия: как только поврежденный узел смог стать посредником между сенсорным узлом и базовой станцией, он способен производить манипуляции с перехваченными пакетами данных.
Атака «червоточина» (Wormhole attack)	Организация транспортной среды между поврежденными узлами сенсорной сети для транспортировки перехваченных пакетов для атакующей системы. Не требует компрометации узла сенсорной сети.
«Колдовская» атака (Sybil attack)	Использование поврежденным узлом сенсорной сети нескольких лжеидентификаторов, представляясь одновременно несколькими узлами сети. Последствия: нарушение правильной работы распределенного хранения, маршрутизации, агрегации данных, голосования в сенсорной сети.
Атака «переполнение» («HELLO» flood attack)	Вид широковещательной атаки. Злоумышленник, используя высокочастотный радиопередатчик с большой вычислительной мощностью, организует рассылку «Hello»-пакетов всем узлам беспроводной сенсорной сети, что интерпретируется узлами, получившими Hello-пакеты, как посылку данных от своего соседа, при этом пакеты будут исходить от пораженных узлов.
Атаки по расписанию	Изменение поведения широковещательной рассылки по расписанию временного мультиплексирования канала (TDMA). Последствия: коллизия пакетов, которая приводит к потере данных.

2. Разработка системы обнаружения сетевых атак в беспроводной сенсорной сети промышленного мониторинга и управления на основе технологий искусственного интеллекта

Система обнаружения сетевых атак беспроводной сенсорной сети (Wireless Intrusion Detection System – WIDS) [5, 13, 19, 20] представляет собой программно-техническое решение, в состав которого входят программные агенты, выполняющие функцию сбора, обработки и анализа пакетов сетевого трафика. Агенты взаимодействуют с сервером, передают ему перехваченные пакеты. Сервер обрабатывает полученные данные на предмет обнаружения сигнатур атак и выявления аномального поведения сетевых узлов, а также реагирует на происходящие события.

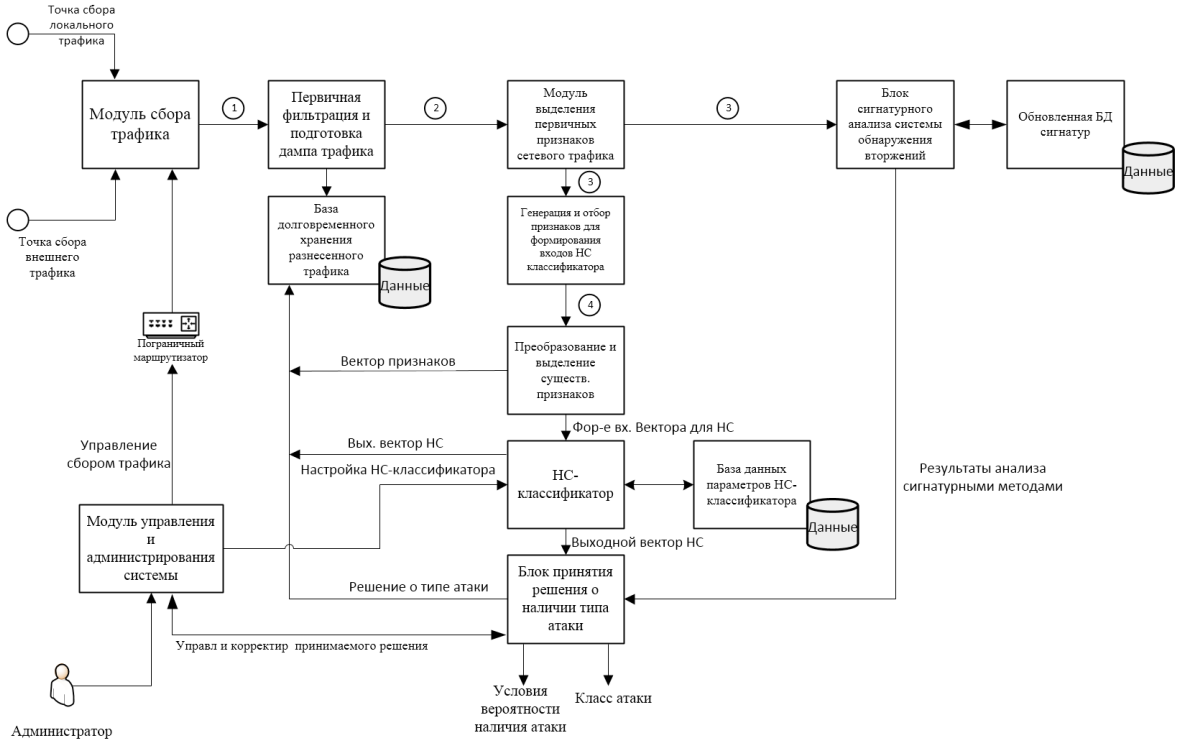

Рис. 4. Структурная схема системы обнаружения сетевых атак в беспроводной сенсорной сети промышленного мониторинга и управления на основе технологий искусственного интеллекта

Разработанная структурная схема WIDS изображена на рисунке 4.

В качестве входных используются данные, накапливаемые точками сбора локального и внешнего трафика. Из модуля сбора внутренний трафик сети предприятия и внешний трафик с пограничного маршрутизатора (1) поступает в блок первичной фильтрации и подготовки дампа. Далее собранная информация поступает в базу данных долговременного хранения предобработанного трафика, а также дамп трафика в формате PCAP-файлов (2) поступает в модуль выделения первичных признаков. Извлекаемые первичные признаки сетевого трафика по результатам анализа структуры кадров и пакетов протоколов соответствующего уровня (3) поступают от модуля выделения первичных признаков к модулю генерации и отбора признаков для формирования входов нейросетевого классификатора и к блоку сигнатурного анализа системы обнаружения атак, откуда в дальнейшем информация поступает в базу данных сигнатур и в блок принятия решения о наличии и типе атаки. Из модуля генерации и отбора признаков существующие признаки, полученные обработкой параметров сетевого соединения и анализа пакетов (4), поступают в модуль преобразования и выделения существенных признаков, который формирует вектор и направляет его в базу долговременного хранения разнесенного трафика, а также формирует входные вектора для модуля нейросетевого (НС) классификатора. Параметры работы модуля НС-классификатора задаются в модуле управления и администрирования системы, который осуществляет обмен данными с базой данных параметров НС-классификатора, передает выходной вектор НС-классификатора в базу долговременного хранения разнесенного трафика и блок принятия решения о наличии и типе атаки. Блоком решения о наличии и типе атаки формируются решения о классе атаки, условная вероятность наличия атаки.

3. Анализ эффективности нейросетевой системы обнаружения сетевых атак

Для оценки эффективности предложенных алгоритмов анализа сетевого трафика был использован набор данных, разработанный сообществом ученых из Саудовской Аравии и Иордании, с непосредственного одобрения авторов научной статьи: Iman Almomani, Bassam Al-Kasasbeh, Mousa ALAkhras [4]. В [4, 21] проводятся исследования с использованием протокола LEACH (Low-energy adaptive clustering hierarchy) – протокола MAC на основе TDMA, который реализует процедуру кластеризации и маршрутизации в беспроводных се-

тях датчиков. Цель LEACH – снизить потребление энергии, необходимое для создания и обслуживания кластеров, чтобы улучшить срок службы беспроводной сети датчиков. На основе данного протокола в [4] были созданы 4 алгоритма сетевых атак, имитирующих вторжение в беспроводную сенсорную.

Результирующий набор данных WSN-DS включает в себе девятнадцать параметрических значений – номинальных и категориальных переменных – и содержит 374661 запись.

В процессе предобработки набора категориальные переменные были заменены на численные, а классы, содержащие менее 1000 примеров, были удалены (Таблица 2).

Табл. 2

Параметры обучающей выборки WSN-DS

Тип атаки	Количество экземпляров
Черная дыра (Blackhole)	10049
Серая дыра (Grayhole)	14596
Переполнение (Flooding)	3312
Атаки по расписанию (TDMA)	6638
Нормальные экземпляры	340066

Алгоритма анализа сетевого трафика в виде укрупнённой блок-схемы представлен на рисунке 5.

Рис. 5. Блок-схема алгоритма

В качестве инструмента для генерации и селекции признаков [22,23] предлагается использовать нейросетевой автоэнкодер (NNA) с четырехслойной архитектурой и метод главных компонент (PCA).

Для построения классификатора, оперирующего параметрами исходного или сжатого пространства признаков, применяются:

Табл. 3

Параметры предобработки данных и параметры классификаторов

Параметры	Эксперимент						
	1	2	3	4	5	6	7
	MLP	**SVM**	**k-nn**	**RF**	**NNA + softmax**	**PCA + MLP**	**PCA + RF**
Генерация компактного вектора признаков	Нет					с помощью PCA отобрано 7 главных комп-т	с помощью PCA отобрано 12 главных комп-т
Архитектура НС блока сопоставления							
Размерность входного вектора	19						
Тип входного вектора	Вещественные числа, mean = 0, std = 1						
Размерность выходного вектора	5						
Тип выходного вектора	Вектор вещественных числе в диапазоне [-1; 1], характеризующий степень уверенности системы в наличии соответствующего вида атаки. Схема кодирования «один из» («one-hot»)						
Параметры классификатора	Количество нейронов по слоям: 19, 25, 5; Функции активации нейронов по слоям: гиперболический тангенс	Количество эпох: 1000	Количеств соседей k = 5	Количество случайных деревьев в комитете: 5	количество скрытых слоев 1 автокодировщика: 15, количество скрытых слоев 2 автокодировщика: 10.	мин количество компонент: 6; максимальное количество компонент: 10; минимальное количество нейронов: 6.	Количество случайных деревьев в комитете: 5
Постобработка выхода классификатора	Преобразования унитарного кода в номер класса				Softmax + унитарный код в номер класса	Преобразования унитарного кода в номер класса	

Табл. 4.

Усреднённые значения результатов классификации для обучающей выборки при перекрестной проверке с 10 прогонами

Характеристика	MLP	SVM	k-nn	RF	NNA + softmax	PCA + MLP	PCA + RF
Чувствительность	0,862	0,929	0,992	0,999	0,849	0,745	0,999
Специфичность	0,992	0,986	0,999	0,992	0,993	0,990	0,995
Точность	0,986	0,979	0,996	0,998	0,986	0,979	0,999

Табл. 5.

Усреднённые значения результатов классификации для тестовой выборки при перекрестной проверке с 10 прогонами

Характеристика	MLP	SVM	k-nn	RF	NNA + softmax	PCA + MLP	PCA + RF
Чувствительность	0,879	0,928	0,985	0,998	0,843	0,696	0,998
Специфичность	0,993	0,986	0,998	0,980	0,993	0,990	0,976
Точность	0,986	0,986	0,995	0,996	0,986	0,977	0,995

– нейронная сеть прямого распространения на основе многослойного персептрона (MLP);
– машина опорных векторов с регуляризацией (C-SVM);
– классификатор на основе k-ближайших соседей (k-NN);
– деревья решений на основе метода «случайный лес» (RF).

Параметры классификаторов представлены в таблице 3.

Основными параметрами, характеризующими качество классификации разработанных алгоритмов, являются: точность, чувствительность и специфичность, рассчитанные как усреднённые значения для тестовых выборок при использовании схемы процедуры k-кратного скользящего контроля.

Чувствительность (Sensitivity) – доля истинно-положительных случаев; специфичность (Specificity) – доля истинно-отрицательных случаев, которые были верно обнаружены моделью; корректность классификации (correctRate) – относительное количество верно классифицированных образцов по всем классам; абсолютное число ошибочно распознанных образцов (numError).

Исходная выборка после применения процедуры предобработки разбита на два типа: обучающая и тестовая в соотношении: 75 % отводится на обучающую выборку, а 25 % – на тестовую (Таблицы 4, 5).

Таким образом, наилучшие результаты по параметрам чувствительности и специфичности показали классификаторы: «классификатор k-ближайших соседей», «случайный лес» и «комбинация методов главных компонент и случайный лес». В данной работе с помощью методов нейросетевого анализа удалось добиться точности классификатора на тестовой выборке 0,996.

Заключение

Таким образом, исследованы возможности повышения эффективности функционирования системы обнаружения сетевых атак за счет применения алгоритмов нейросетевого анализа сетевого трафика в беспроводной сенсорной сети промышленного мониторинга и управления.

Разработана структурная схема системы обнаружения сетевых атак на основе алгоритмов интеллектуального анализа данных, а также алгоритм анализа сетевого трафика в беспроводной сенсорной сети в составе модуля системы обнаружения вторжений. С помощью реализованного модуля проведена оценка эффективности предложенного алгоритма анализа на натурных данных в системе промышленного мониторинга: с помощью методов нейросетевого анализа удалось добиться точности классификации типов сетевой активности на тестовой выборке 0,996.

Литература

1. *Greengard S.* The internet of things. – MIT press, 2015. – 232 p.
2. *Зараменских Е.П., Артемьев И.Е.* Интернет вещей. Исследования и область применения. – Издательство Инфра-М, 2017. – 188 с.
3. *Roth A.* Einführung und Umsetzung von Industrie 4.0. Grundlagen, Vorgehensmodell und Use Cases aus der Praxis. – Springer Gabler Verlag, Wiesbaden, 2016. – 272 p.

4. *Almomani I., Al-Kasasbeh B., Al-Akhras M.* WSN-DS: a dataset for intrusion detection systems in wireless sensor networks // Journal of Sensors. – 2016. – Т. 2016.
5. *Финогеев А.* Маршрутизация и защита данных в беспроводных сенсорных сетях. – Lambert Academic Publishing, 2016. – 96 с.
6. *Akyildiz I.F. et al.* Wireless sensor networks: a survey //Computer networks. – 2002. – Т. 38. – №. 4. – С. 393-422.
7. *Восков Л.С.* Беспроводные сенсорные сети и прикладные проекты // Автоматизация и IT в энергетике. – 2009. – № 2-3. – С. 44-49.
8. *Терентьев М.Н.* Беспроводные сенсорные сети: учебное пособие. – Издательство МАИ, 2008. – 95 с.
9. *Yick J., Mukherjee B., Ghosal D.* Wireless sensor network survey //Computer networks. – 2008. – Т. 52. – №. 12. – С. 2292-2330.
10. *Калачев А.В.* Аппаратные и программные решения для беспроводных сенсорных сетей. – НОУ “ИНТУИТ”, 2016. – 240 с.
11. *Pathan A.S.K., Lee H.W., Hong C.S.* Security in wireless sensor networks: issues and challenges. // 2006 8th International Conference Advanced Communication Technology. – IEEE, 2006. – Т. 2. – С. 1043-1048.
12. *Смирнова Е.В., Ромашкина Е.А., Пролетарский А.В.* Технология современных беспроводных сетей Wi-Fi. – МГТУ им. Н.Э.Баумана, 2017. – 448 с.
13. *Щербаков В.Б., Ермаков С.А.* Безопасность беспроводных сетей. Стандарт IEEE 802.11. – Издательство РадиоСофт, 2010. – 256 с.
14. *Pathan A.S.K.* Security of self-organizing networks: MANET, WSN, WMN, VANET. – CRC press, 2016. – 638 p.
15. *Chelli K.* Security issues in wireless sensor networks: Attacks and countermeasures // Proceedings of the World Congress on Engineering, London, U.K., – 2015. – Т. 1. – №. 20. – С. 1-3.
16. *Loo J., Mauri J.L., Ortiz J.H.* Mobile ad hoc networks: current status and future trends. – CRC Press, 2016. – 538 p.
17. *Sinha P. et al.* Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey // 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, Tamil Nadu, India, 2017. – С. 288-293.
18. IEEE 802.15.4-2003 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Available at: https://ieeexplore.ieee.org/document/1237559 (accessed March 26, 2019).
19. *Can O., Sahingoz O.K.* A survey of intrusion detection systems in wireless sensor networks // In the 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Istanbul, Turkey, 2015. – С. 1-6.
20. *Al-Dabbagh A. W., Li Y., Chen T.* An intrusion detection system for cyber attacks in wireless networked control systems //IEEE Transactions on Circuits and Systems II: Express Briefs. – 2017. – Т. 65. – №. 8. – С. 1049-1053.
21. *Almomani and B. Al-Kasasbeh.* Performance analysis of LEACH protocol under Denial of Service attacks //Proceedings of the 6th IEEE International Conference on Information and Communication Systems (ICICS ’15), Amman, Jordan, April 2015. – С. 292–297.
22. *Николенко С., Кадурин А., Архангельская Е.* Глубокое обучение. Погружение в мир нейронных сетей. – Издательство: Питер, 2018. – 480 с.
23. *Flach P.* Machine learning: the art and science of algorithms that make sense of data. – Cambridge University Press, 2012. – 410 p.

Васильев Владимир Иванович. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Профессор кафедры вычислительной техники и защиты информации, доктор технических наук, профессор. Количество печатных работ: более 100. Область научных интересов: интеллектуальные системы управления и защиты информации. E-mail: vasilyev@ugatu.ac.ru

Вульфин Алексей Михайлович. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Доцент кафедры вычислительной техники и защиты информации, кандидат технических наук. Количество печатных работ: более 50. Область научных интересов: интеллектуальный анализ данных и моделирование сложных технических систем. E-mail: vulfin.alexey@gmail.com

Картак Вадим Михайлович. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Заведующий кафедрой вычислительной техники и защиты информации, доктор физико-математических наук, доцент. Количество печатных работ: более 50. Область научных интересов: информационная безопасность, методы оптимизации. E-mail: kvmail@mail.ru

Кириллова Анастасия Дмитриевна. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Аспирант кафедры вычислительной техники и защиты информации. Количество печатных работ: 17. Область научных интересов: комплексный анализ и управление рисками кибербезопасности АСУ ТП промышленных объектов с использованием технологии когнитивного моделирования. E-mail: kirillova.andm@gmail.com

Миронов Константин Валерьевич. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Старший преподаватель кафедры вычислительной техники и защиты информации, PhD. Количество печатных работ: 20. Область научных интересов: применение распределенного реестра в системах промышленного интернета вещей с ограниченными вычислительными ресурсами. E-mail: mironovconst@gmail.com

System of attacks detection in wireless sensor networks of Industrial Internet of Things

V.I. Vasilyev[1], A.M. Vulfin[1], V.M. Kartak[1], A.D. Kirillova[1], K.V. Mironov[1]
[1] Ufa State Aviation Technical University, Ufa, Russia

Abstract. The aim of the study is to improve the performance of the network attack detection system through the use of neural network analysis algorithms for network traffic in a wireless sensor network of industrial monitoring and control. The tasks of developing a block diagram of a network attack detection system and intelligent network traffic analysis algorithms are being solved. The evaluation of the effectiveness of the proposed algorithm for analysis of field data was performed.
Keywords: *network attack detection system, wireless sensor networks, data mining*
DOI: 10.14357/20790279190409

References

1. *Greengard, S.* 2015. The internet of things. MIT Press. 232 p.
2. *Zaramenskih E. and I. Artemev.* 2017. Internet veshhej. Issledovanija i oblast' primenenija [Internet of Things. Research and scope]. Izdatel'stvo Infra-M. 188 p.
3. *Roth, A.* 2016. Einführung und Umsetzung von Industrie 4.0. Grundlagen, Vorgehensmodell und Use Cases aus der Praxis. Springer Gabler Verlag, Wiesbaden. 272 p.
4. *Almomani, I., B. Al-Kasasbeh and M. Al-Akhras*. 2016. WSN-DS: a dataset for intrusion detection systems in wireless sensor networks. Journal of Sensors, Vol. 2016.
5. *Finogeev, A.* 2016. Marshrutizacija i zashhita dannyh v besprovodnyh sensornyh setjah [Routing and data protection in wireless sensor networks]. Lambert Academic Publishing. 96 p.
6. *Akyildiz, I.F. et al.* 2002. Wireless sensor networks: a survey. Computer networks, 4(38): 393–422.
7. *Voskov, L.S.* 2009. Besprovodnye sensornye seti i prikladnye proekty [Wireless sensor networks and application projects]. Avtomatizacija i IT v jenergetike [Automation and IT in the energy sector], 2-3(2-3): 44–49.
8. *Terent'ev, M.N.* 2008. Besprovodnye sensornye seti: uchebnoe posobie [Wireless sensor networks]. Izdatel'stvo MAI. 95 p.
9. *Yick, J., B. Mukherjee and D. Ghosal.* 2008. Wireless sensor network survey. Computer networks, 12(52): 2292–2330.
10. *Kalachev, A.V.* 2016. Apparatnye i programmnye reshenija dlja besprovodnyh sensornyh setej [Hardware and software solutions for wireless sensor networks]. NOU "INTUIT". 240 p.
11. *Pathan, A.S.K., H.W. Lee and C.S. Hong.* 2006. Security in wireless sensor networks: issues and

challenges. 8th International Conference Advanced Communication Technology, ICACT 2006, 2: 1043–1048.
12. *Smirnova, E.V., E.A. Romashkina, A.V. Proletarskij*. 2017. Tehnologija sovremennyh besprovodnyh setej Wi-Fi [Technology of modern wireless networks Wi-Fi]. MGTU im. N.Je.Baumana. 448 p.
13. *Shherbakov, V.B., S.A. Ermakov*. 2010. Bezopasnost' besprovodnyh setej. Standart IEEE 802.11. [Wireless security. IEEE 802.11 standard.] Izdatel'stvo RadioSoft. 256 p.
14. *Pathan, A.S.K*. 2016. Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press. 638 p.
15. *Chelli, K*. 2015. Security issues in wireless sensor networks: Attacks and countermeasures. Proceedings of the World Congress on Engineering, London, U.K., 2015, 1: 1–3.
16. *Loo, J., J.L. Mauri and J.H. Ortiz*. 2016. Mobile ad hoc networks: current status and future trends. CRC Press. 538 p.
17. *Sinha, P. et al*. 2017. Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. IEEE International Conference on Signal Processing and Communication (ICSPC), Coimbatore, Tamil Nadu, India, 2017. 288–293.
18. IEEE 802.15.4-2003 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Available at: https://ieeexplore.ieee.org/document/1237559 (accessed March 26, 2019).
19. *Can, O., O.K. Sahingoz*. 2015. A survey of intrusion detection systems in wireless sensor networks. In the 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Istanbul, Turkey, 2015. 1–6.
20. *Al-Dabbagh, A.W., Y. Li, T. Chen*. 2018. An intrusion detection system for cyber attacks in wireless networked control systems. IEEE Transactions on Circuits and Systems II: Express Briefs, 8(65): 1049–1053.
21. *Almomani and B. Al-Kasasbeh*. 2015. Performance analysis of LEACH protocol under Denial of Service attacks. Proceedings of the 6th IEEE International Conference on Information and Communication Systems (ICICS '15), Amman, Jordan, April 2015. 292–297.
22. *Nikolenko, S., A. Kadurin, E. Arhangel'skaja*. 2018. Glubokoe obuchenie. Pogruzhenie v mir nejronnyh setej [Deep learning. Immersion in the world of neural networks]. Izdatel'stvo: Piter. 480 p.
23. *Flach, P.* 2012. Machine learning: the art and science of algorithms that make sense of data. Cambridge University Press. 410 p.

V.I Vasilyev. Doctor of Technical Science, Professor of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation;
E-mail: vasilyev@ugatu.ac.ru

A.M. Vulfin. PhD (Cand. of Sc.) Ass. Professor of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation;
E-mail: vulfin.alexey@gmail.com

V.M. Kartak. Doctor of Technical Science, Professor of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation;
E-mail: kvmail@mail.ru

A.D. Kirillova. Postgrad. Student of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation; E-mail: kirillova.andm@gmail.com

K.V. Mironov. PhD, Senior lecturer of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation; E-mail: mironovconst@gmail.com