УДК 004.056

В.И. Васильев, В.Е. Гвоздев, Р.Р. Шамсутдинов

Обнаружение аномалий в системах промышленного Интернета вещей на основе искусственной иммунной системы

Проведен анализ актуальности обеспечения безопасности беспроводных сенсорных сетей. Для обнаружения аномалий в таких сетях предложено использование механизмов искусственной иммунной системы (ИИС). С целью обучения и оценки эффективности системы использован тестовый набор данных о сетевых соединениях WSN-DS. Проведены вычислительные эксперименты, осуществлено сравнение полученных результатов при использовании в ИИС в качестве меры близости косинусного расстояния, Евклидовой меры и расстояния Хэмминга. Показано, что разработанная система демонстрирует высокую эффективность при использовании расстояния Хэмминга.

Ключевые слова: искусственная иммунная система, информационная безопасность, обнаружение аномалий, WSN-DS, беспроводные сенсорные сети.
DOI: 10.21293/1818-0442-2021-24-4-40-45

Стремительное развитие и широкое применение систем промышленного Интернета вещей (Industrial Internet of Things, IIoT) приводит к увеличению рисков нарушения кибербезопасности промышленных объектов. Так, 20% респондентов, опрошенных Лабораторией Касперского [1], в качестве одной из главных киберугроз определяют атаки на IIoT, а утечки данных и атаки на цепочки поставок считают наиболее опасными по 15% респондентов. 55% опрошенных выделили использование IIoT в качестве одного из главных факторов, влияющих на кибербезопасность АСУ ТП, но только 14% компаний внедрили инструменты детектирования сетевых аномалий и 19% – средства мониторинга сети и трафика. По данным CheckPoint [2], 67% предприятий уже столкнулись с инцидентами безопасности, связанными с IoT-устройствами. IIoT-сети становятся всё более сложными, а решения для обеспечения их безопасности остаются далеко позади.

Нарушение безопасности IIoT может привести к несанкционированному распространению защищаемой информации, возникновению угроз жизни и здоровью людей в результате аварий на промышленных предприятиях или деструктивного воздействия на IIoT-устройства в медицинских учреждениях.

Одной из ключевых уязвимостей систем IIoT является широкое применение беспроводных сетевых технологий, в частности, в беспроводных сенсорных сетях (Wireless Sensor Network, WSN), нередко используемых в IIoT. WSN характеризуются высокой степенью уязвимости, обусловленной их распределённостью, открытостью и ограниченностью ресурсов сенсорных узлов [3].

С целью обнаружения сетевых атак в информационных системах в последнее время все чаще предлагается применение механизмов искусственных иммунных систем (ИИС). ИИС способны обнаруживать неизвестные атаки, демонстрируют высокую производительность и низкое число ошибок 1-го и 2-го рода [4, 5]. В данной работе рассматривается применение ИИС для обнаружения аномалий в WSN. Под аномалиями при этом понимаются отклонения от нормального поведения, вызванные попытками несанкционированного доступа к данным, изменения протоколов обмена и передачи данных и т.п.

Анализ современного состояния исследований

В [6] проанализированы протоколы маршрутизации, применяемые в WSN, основные атаки, такие как Sinkhole, Blackhole, Byzantine Attack и др., а также основные проблемы исследований в области беспроводных сенсорных сетей.

В [7] проанализированы функциональные особенности WSN и наиболее распространенные типы атак. В качестве защиты от вредоносных или скомпрометированных узлов предлагается использовать адаптивное взаимодействие элементов системы, основанное на анализе поведения соседних узлов.

В [8] подчеркивается высокая уязвимость сенсорных узлов WSN, возможность злоумышленников нанести большой ущерб при успешной компрометации узла; определены уязвимости алгоритмов обмена аутентификационной информацией. Во избежание компрометации узла авторы предлагают дополнить существующий алгоритм новой схемой обмена аутентификационной информацией. Оценка BAN-логикой, а также проведённые оценки производительности и защищённости показывают эффективность предложенной схемы.

В [9] предлагается адаптивный иммуноинспирированный энергоэффективный кроссслойный протокол маршрутизации (Adaptive Immune-inspired Energy-Efficient Cross-layer Routing protocol (AIEECR)). Данный протокол используется для выбора наиболее эффективного маршрута передачи данных на базовую станцию от каждого центра кластера (Cluster Head). Производительность предложенного подхода сравнивается с другими методами, результаты экспериментов демонстрируют эффективность предлагаемого авторами метода.

В [10] предложено использование алгоритма муравьиной колонии для повышения уровня защищенности сенсорной сети. Вопросы обеспечения безопасности WSN подробно рассматриваются в [11–13].

С целью обучения систем обнаружения аномалий и оценки их эффективности используются различные наборы данных. В [14] подробно описан WSN-DS – один из таких наборов, преимуществом которого является то, что он основан на протоколе LEACH – одном из наиболее широко используемых иерархичных протоколов маршрутизации в беспроводных сенсорных сетях. Этот набор содержит около 370 тыс. строк, включает 4 вида атак: Blackhole, Grayhole, Scheduling, Flooding. Каждая запись WSN-DS содержит 18 параметров. Этот набор данных служит основой для построения различных систем обнаружения атак и использован в данной работе.

В [15] для обнаружения вторжений в WSN используется модель, основанная на применении генетических алгоритмов и градиентного бустинга. Оценка эффективности системы проводилась с применением набора данных WSN-DS. Предложенный подход позволил выявить 97,8% атак.

В [16] для анализа WSN-DS использовался случайный лес (СЛ) в сравнении с искусственной нейронной сетью (ИНС), где точность обнаружения атак с помощью СЛ составила 97,2%, ИНС – 95,8%.

В [17] авторы также анализируют вышеуказанный набор данных с применением таких классификаторов, как машина опорных векторов, J48, СЛ, наивный Байесовский классификатор (НБК), ИНС. Наилучшую точность обнаружения атак продемонстрировал случайный лес – 99,7% верно выявленных атак.

В [18] используется алгоритм бэггинга (Bagging algorithm) для построения ансамбля деревьев решений C4.5. Система обучена распознаванию атак, представленных в WSN-DS, выявлено 98,4% атак.

Проанализированные выше работы демонстрируют высокую точность обнаружения известных атак на примере рассматриваемого набора данных, однако постоянное возникновение новых атак обусловливает актуальность разработки системы, способной выявлять в том числе неизвестные атаки. Кроме того, с целью повышения производительности систем актуальным остается вопрос уменьшения пространства параметров.

Искусственные иммунные системы (ИИС) демонстрируют высокий уровень обнаружения неизвестных атак при низком уровне ошибок, способны постоянно самообучаться в процессе анализа. ИИС также применяются для решения задачи обнаружения атак в беспроводных сенсорных сетях. В рассматриваемых ниже работах для оценки эффективности используются другие наборы данных, отличные от WSN-DS, однако это не является критичным для сравнения методологий.

В [19] предлагается многоуровневая система обнаружения вторжений для WSN на основе иммунной теории. Система включает блоки: B-клеток, T-клеток, дентритных клеток и базофилов. Здесь B-клетки проводят первичный анализ данных, они формируются только на этапе обучения системы. Система не способна постоянно обучаться. Для измерения расстояния между векторами используется алгоритм битового сопоставления. Сравнения с другими метриками не произведено. Дальнейший анализ данных производится дентритными клетками, в случае выявления аномалии передается сигнал блоку T-клеток, который осуществляет реакцию, изолирует аномальный узел, не участвует в анализе. Блок базофилов в работе пока не реализован.

В [20] предложен алгоритм глубокого обучения и дентритных клеток (Deep Learning and Dendritic Cell Algorithm, DeepDCA). Для оценки эффективности применяется набор данных BoT-IoT. В работе реализовано сжатие пространства параметров, применяется самоорганизующаяся ИНС, осуществляющая первичную обработку данных и категорирование входного сигнала на сигналы об опасности и о безопасном состоянии. Дальнейший анализ осуществляется дендритными клетками. Представлены результаты сравнения с такими классификаторами, как k-ближайших соседей, машина опорных векторов, многослойный перспетрон, НБК. DeepDCA продемонстрировал наилучшую точность обнаружения. Однако в данной работе речь идет об обнаружении только известных атак с опорой на первичные сигналы опасности от ИНС.

В [21], как и в предлагаемом подходе, используются алгоритмы негативной селекции для обеспечения толерантности системы к нормальному состоянию, клональной селекции, обеспечивающей адаптивность системы, возможность ее постоянного самообучения. В моделировании использован протокол LEACH, проанализированы следующие виды атак: Resource depletion, Sinkhole, Wormhole, Sybil, Selective forwarding attack. Обнаружение строится с использованием теории опасности.

В первую очередь члены и центры кластера в WSN обнаруживают изменения своих собственных свойств, извлекают ключевые данные и получают информацию о сигналах среды, оценивают риск. В случае опасности член кластера передает соответствующий сигнал опасности центру кластера, объединяющего несколько сигналов опасности, переводящих их узлу-приемнику. Узел-приемник вычисляет степень риска, область риска запрашивает представления антигенов. Узлы датчиков опасной зоны собирают информацию о сетевом трафике для формирования антигенов. После этого узел-приемник проводит анализ на предмет вторжения. Подобный алгоритм создает дополнительную нагрузку на членов и центры кластера.

Искусственная иммунная система

ИИС имитирует работу естественной иммунной системы человека, способной обнаруживать неизвестные организму чужеродные патогены. Адаптивная составляющая иммунитета основывается на функционировании так называемых лимфоцитов – иммунных клеток, отвечающих за приобретенный иммунитет.

В ИИС нет необходимости подробного моделирования каждого вида лимфоцитов по отдельности, достаточно выделить основные функции. Для обучения ИИС достаточно данных о нормальном пове-

дении анализируемой системы. Первичное обучение заключается в генерации формальных лимфоцитов – точек-детекторов, обнаруживающих аномалии в пределах заданного от них расстояния. С целью исключения ошибочного определения нормального состояния системы как аномального проводится процедура отрицательного отбора или негативной селекции, которая заключается в удалении из числа детекторов всех тех, что «реагируют» на данные о нормальном состоянии системы.

Адаптивность ИИС обеспечивается реализацией алгоритма клональной селекции, а также периодическим обновлением набора детекторов. Клональная селекция заключается в многократном клонировании с некоторой случайной мутацией (искажением) детектора, выявившего угрозу. Данный механизм позволяет более эффективно обнаруживать аномалии, подобные уже выявленным ранее, обеспечивая постоянное самообучение системы. Необходимо отметить, что каждый такой клон также подвергается процедуре отрицательного отбора для обеспечения толерантности к нормальному состоянию системы. Клоны заменяют собой «худшие» детекторы, т.е. выявившие наименьшее число аномалий.

С целью периодического обновления детекторов каждому из них устанавливается некоторое время жизни, по истечении которого, если детектор не обнаружил аномалий, он уничтожается, вместо него генерируется новый случайный детектор, также подвергаемый негативной селекции. Если детектор обнаружил аномалию, время его жизни значительно увеличивается.

Процедура анализа данных заключается в вычислении расстояния между анализируемым вектором и каждым вектором-детектором: если хотя бы одно значение меньше порогового, считается, что соответствующий детектор выявил аномалию.

Результаты вычислительных экспериментов

Предлагаемая система предполагает формирование отдельных узлов-снифферов, что не требует дополнительных ресурсов членов кластера. Она, в отличие от проанализированных выше [19–21], не основывается на теории опасности. Анализ проводится постоянно обновляемым набором детекторов с реализацией алгоритмов негативной селекции, клональной селекции на основе различных метрик, что позволяет системе автоматически дообучаться на основе выявленных в процессе анализа аномалий, оставаясь толерантной к нормальному состоянию.

Система, помимо выявления известных атак, позволяет обнаруживать также ранее неизвестные атаки. Реализовано сжатие пространства параметров WSN-DS, сравнение мер близости векторов, используемых в процессе анализа.

В рамках предыдущего исследования [3] авторами настоящей статьи была проведена оценка эффективности применения искусственной иммунной системы для выявления аномалий в беспроводных сенсорных сетях на основе WSN-DS с использованием расстояния Хэмминга в качестве меры близости между векторами, однако не были рассмотрены другие критерии.

Рассмотрим косинусную меру, описываемую формулой

$$\cos\phi = \frac{\sum_{i=1}^{n} x_i y_i}{\sqrt{\sum_{i=1}^{n} x_i^2}\sqrt{\sum_{i=1}^{n} y_i^2}}. \quad (1)$$

В этой формуле x_i и y_i – компоненты векторов параметров сравниваемых шаблонов детекторов, n – размерность этих векторов. Соответственно, чем более похожи векторы, тем ближе значение косинуса к единице, если они менее похожи – к нулю.

Также было рассмотрено Евклидово расстояние, вычисляемое как

$$d(x,y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}. \quad (2)$$

Набор данных был предварительно обработан таким образом, чтобы значения всех параметров лежали в диапазоне [0; 1] с точностью до сотых. Флаговые значения были оставлены без изменений; значения, кодирующие номера узлов, были переведены в вышеуказанный диапазон. Все остальные значения были также равномерно распределены в вышеуказанном диапазоне, их нормализованные значения были вычислены следующим образом:

$$c = \frac{p}{\max(p_i)}, \quad (3)$$

где p – значение параметра до нормализации; $\max(p_i)$ – максимальное среди всех возможных значений данного параметра до нормализации.

Были проведены вычислительные эксперименты, которые показали, что эффективность ИИС при использовании меры расстояния на основе (1) оказалась крайне низкой. Поэтому был проведен следующий анализ. Нормализованный набор данных был разделен на подмножество данных о нормальном состоянии системы и подмножество данных об аномалиях. Затем для каждого вектора данных о нормальном состоянии был найден максимально похожий вектор данных об аномалиях с использованием косинусной меры. Оказалось, что более чем для 65% таких пар векторов значение косинуса превышает 0,98, для более чем 80% – 0,95, хотя число идентичных строк между двумя подмножествами менее 0,01%. Таким образом, подмножества трудноразделимы косинусной мерой.

Эффективность ИИС при измерении расстояния по критерию (2) оказалась более высокой. Анализ вначале проводился по всем 18 нормализованным параметрам. С целью улучшения производительности было принято решение уменьшить число анализируемых параметров.

Для каждого вектора данных о нормальной активности был найден ближайший вектор множества данных об аномалиях, вычислен и записан модуль разности по каждому параметру (координате). Затем была найдена сумма этих модулей отдельно по каждому параметру, после чего они были ранжированы

по наибольшему значению полученной суммы, как представлено в таблице.

Ранжированные параметры

Номер параметра	Наименование параметра	Сумма модулей разности
1	ID	10 706 270
4	Who_CH	9 286 618
2	Time	5 407 324
12	Rank	2 720 009
5	Dist_To_CH	1 762 264
13	DATA_S	1 733 408
16	dist_CH_To_BS	1 014 887
7	ADV_R	733 664
14	DATA_R	556 365
18	Consumed Energy	442 674
17	send_code	259 555
15	Data_Sent_ To_BS	199 383
9	JOIN_R	18 551
6	ADV_S	16 398
10	SCH_S	4 316
11	SCH_R	2 529
3	Is_CH	544
8	JOIN_S	147

При проведении анализа сначала учитывались все параметры, затем их число постепенно уменьшалось. Как показали результаты, при использовании первых 9 ранжированных параметров сохраняется высокая эффективность обнаружения, как это представлено на рис. 1. При дальнейшем уменьшении их количества эффективность обнаружения аномалий заметно снижается.

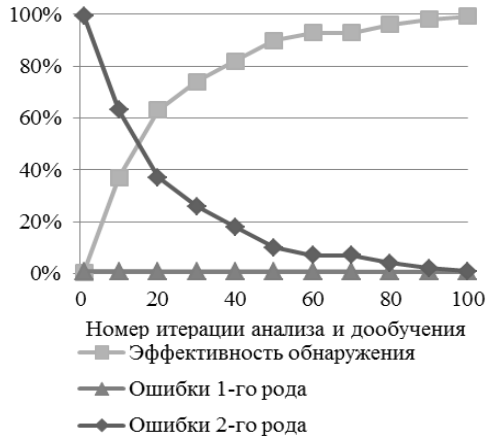

Рис. 1. Эффективность ИИС с использованием Евклидова расстояния

Отметим, что динамика обучения ИИС при использовании Евклидовой меры схожа с динамикой, наблюдаемой при использовании расстояния Хэмминга, представленной рис. 2.

Таким образом, использование и расстояния Хэмминга, и Евклидова расстояния позволяет обнаруживать как известные, так и неизвестные аномалии с высокой точностью и низким количеством ошибок, однако скорость вычисления расстояния Хэмминга, как показывает практика, более чем в 5 раз превышает скорость вычисления Евклидова расстояния.

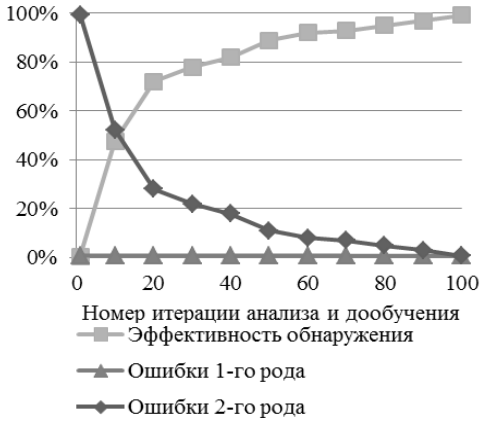

Рис. 2. Эффективность ИИС с использованием расстояния Хэмминга [3]

Достигнутый показатель точности распознавания при этом составляет 99,2%, что превышает аналогичные показатели, приведенные в работах [15, 16, 18–21]. В качестве примечания следует отметить, что алгоритм СЛ, использованный в [17], обеспечивает сходные показатели точности, однако не позволяет обнаруживать неизвестные атаки.

Заключение

Применение систем промышленного Интернета вещей значительно увеличивает риски нарушения кибербезопасности. По данным CheckPoint [2], 67% предприятий уже столкнулись с инцидентами безопасности, связанными с IoT-устройствами. Широкое использование беспроводных соединений, в том числе беспроводных сенсорных сетей, делает системы IIoT более уязвимыми.

Для выявления аномалий в информационных системах целесообразно применение искусственных иммунных систем, имитирующих работу естественной иммунной системы человека. Ключевые алгоритмы ИИС:

– отрицательный отбор – обеспечивает толерантность ИИС к нормальному состоянию системы;

– клональная селекция – осуществляет дообучение системы в процессе её функционирования;

– обновление детекторов – обеспечивает адаптивность системы и повышает вероятность обнаружения неизвестных атак.

Оценка эффективности разработанной системы в ходе экспериментов осуществлялась с использованием набора данных WSN-DS [14], содержащего около 370 тыс. строк, 4 вида атак на WSN. Было проведено сравнение работы ИИС на основе трёх мер расстояния между векторами: косинусного, Евклидова расстояния и расстояния Хэмминга. Результаты вычислительных экспериментов показали невысокую эффективность применения косинусной меры для анализируемого набора данных и высокую точность обнаружения при использовании Евклидовой меры и расстояния Хэмминга. Наибольшее быстродействие при этом демонстрирует ИИС, основанная на вычислении расстояния Хэмминга.

В целом применение ИИС демонстрирует высокую эффективность обнаружения аномалий в беспроводных сенсорных сетях.

Работа выполнена при поддержке гранта РФФИ № 20-37-90024.

Литература

1. Лаборатория Касперского: распространение умных устройств в промышленности повлечёт за собой смену подхода к киберзащите [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-rasprostranenie-umnih-ustroistv-v-promishlennosti-povlechyot-za-soboi-smenu-podhoda-k-kiberzaschite, свободный (дата обращения: 13.03.2021).

2. Check Point IoT Protect [Электронный ресурс]. – Режим доступа: https://www.checkpoint.com/downloads/products/cp-iot-security-solution-brief.pdf, свободный (дата обращения: 13.03.2021).

3. Vasilyev V. Providing Information Security on the Base of Artificial Immune System for Industrial Internet of Thing / V. Vasilyev, R. Shamsutdinov // Advances in Intelligent Systems Research. – 2020. – Vol. 174. – P. 212–217.

4. Tarakanov A.O. A Comparison of Immune and Genetic Algorithms for Two Real-Life Tasks of Pattern Recognition / A.O. Tarakanov, Y.A. Tarakanov // Int. J. of Unconventional Computing. – 2004. – Vol. 1.4. – P. 357–374.

5. Tarakanov A.O. A Comparison of Immune and Neural Computing for Two Real-Life Tasks of Pattern Recognition / A.O. Tarakanov, Y.A. Tarakanov // Lecture Notes in Computer Science. – 2004. – Vol. 3239. – P. 236–249.

6. Saini V. WSN Protocols, Research challenges in WSN, Integrated areas of sensor networks, security attacks in WSN / V. Saini, J. Gupta, K.D. Garg // European Journal of Molecular & Clinical Medicine. – 2020. – Vol. 7, Iss. 3. – P. 5145–5153.

7. Ovasapyan T. Security Provision in WSN on the Basis of the Adaptive Behavior of Nodes [Электронный ресурс] / T. Ovasapyan, D. Moskvin // Proceedings of the 4th World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). – Режим доступа: https://ieeexplore.ieee.org/document/9210421, свободный (дата обращения: 05.03.2021).

8. An Authentication Information Exchange Scheme in WSN for IoT Applications / S. Yang, Y. Shiue, Z. Su, I. Liu, C. Liu // IEEE Access. – 2020. – Vol. 8. – P. 9728–9738.

9. Yarde P. Adaptive immune-inspired energy-efficient and high coverage cross-layer routing protocol for wireless sensor networks / P. Yarde, S. Srivastava, K. Garg // IET Communications. – 2020. – Vol. 14, Iss. 15. – P. 2592–2600.

10. Iwendi C. ACO based key management routing mechanism for WSN security and data collection [Электронный ресурс] / C. Iwendi, Z. Zhang, X. Du // 2018 IEEE International Conference on Industrial Technology (ICIT). – 2018. – P. 1935–1939. – Режим доступа: https://ieeexplore.ieee.org/document/8352482, свободный (дата обращения: 05.03.2021)

11. Kavitha T. Security Vulnerabilities in Wireless Sensor Networks: a survey / T. Kavitha, D. Sridharan // Journal of Information Assurance and Security. – 2010. – Vol. 5. – P. 31–44.

12. Dimitrievski1 A. Security Issues and Approaches in WSN [Электронный ресурс] / A. Dimitrievski, V. Pejovska, D. Davcev. – Режим доступа: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.6190&rep=rep1&type=pdf, свободный (дата обращения: 06.06.2021).

13. Furtak J. Security techniques for the WSN link layer within military IoT [Электронный ресурс] / J. Furtak, Z. Zieliński, J. Chudzikiewicz // 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). – 2016. – P. 233–238. – Режим доступа: https://ieeexplore.ieee.org/document/7845508, свободный (дата обращения: 02.03.2021)

14. Almomani I. WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks [Электронный ресурс] / I. Almomani, B. Al-Kasasbeh, M. AL-Akhras // Journal of Sensors. – 2016. – Vol. 2016. – Режим доступа: https://www.hindawi.com/journals/js/2016/4731953, свободный (дата обращения: 01.03.2020).

15. A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks / M. Alqahtani, A. Gumaei, H. Mathkour, M. Maher Ben Ismail // Sensors (Basel). – 2019. – Vol. 19. – P. 1–20.

16. An Effective Classification for DoS Attacks in Wireless Sensor Networks [Электронный ресурс] / T.-T.-H. Le, T. Park, D. Cho, H. Kim // 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). – 2018. – P. 689–692. – Режим доступа: https://www.researchgate.net/publication/327065277_An_Effective_Classification_for_DoS_Attacks_in_Wireless_Sensor_Networks, свободный (дата обращения: 06.09.2021).

17. Alsulaimanand L. Performance evaluation of machine learning techniques for DOS detection in wireless sensor network / L. Alsulaimanand, S. Al-Ahmadi // International Journal of Network Security & Its Applications (IJNSA). – 2021. – Vol. 13, No. 2. – P. 21–29.

18. Dong R.-H. An Intrusion Detection Model for Wireless Sensor Network Based on Information Gain Ratio and Bagging Algorithm / R.-H. Dong, H.-H. Yan, Q.-Y. Zhang // International Journal of Network Security. – 2020. – Vol. 22, No. 2. – P. 218–230.

19. Alaparthy V. A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory / V. Alaparthy, S. Morgera // IEEE Access. – 2018. – Vol. 6. – P. 47364–47373.

20. DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System / S. Aldhaheri, D. Alghazzawi, L. Cheng, B. Alzahrani, A. Al-Barakat // Applied Sciences. – 2020. – Vol. 10. – P. 1909–1932.

21. Xiao X. A Danger Theory Inspired Protection Approach for Hierarchical Wireless Sensor Networks / X. Xiao, R. Zhang // KSII Transactions on Internet and Information Systems. – 2019. – Vol. 13, No. 5. – P. 2732–2753.

Васильев Владимир Иванович
Д-р техн. наук, проф. каф. вычислительной техники и защиты информации (ВТиЗИ) Уфимского государственного авиационного технического университета (УГАТУ)
Карла Маркса ул., 12, г. Уфа, Россия, 450008
Тел.: +7-917-350-11-39
Эл. почта: vasilyev@ugatu.ac.ru

Гвоздев Владимир Ефимович
Д-р техн. наук, профессор каф. технической кибернетики (ТК) УГАТУ
Карла Маркса ул., 12, г. Уфа, Россия, 450008
Тел.: +7-917-369-27-73
Эл. почта: wega55@mail.ru

Шамсутдинов Ринат Рустемович
Аспирант каф. ВТиЗИ УГАТУ
Карла Маркса ул., 12, г. Уфа, Россия, 450008
Тел.: +7-927-950-84-13
Эл. почта: shrr2019@yandex.ru

Vasilyev V.I., Gvozdev V.E., Shamsutdinov R.R.

Network Anomaly Detection Based on Artificial Immune System for Industrial Internet of Things

The paper analyzes the relevance of ensuring the security of wireless sensor networks (WSN), proposes the use of an artifi-

cial immune system (AIS) to detect anomalies in such networks. A dataset on WSN connections called WSN-DS was used to train and evaluate the efficiency of proposed system. Computational experiments were conducted with the use of the cosine distance, Euclidean measure and Hamming distance in the AIS. The system demonstrated the highest efficiency when using Hamming distance measure.

Keywords: Artificial Immune System, Information Security, Anomaly Detection, WSN-DS, Wireless Sensor Networks.
DOI: 10.21293/1818-0442-2021-24-4-40-45

References

1. *Laboratoriya Kasperskogo: rasprostranenie umnyh ustrojstv v promyshlennosti povlechyot za soboj smenu podhoda k kiberzashchite* [Kaspersky Lab: the proliferation of smart devices in the industry will lead to a change in the approach to cyber defense]. Available at: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-rasprostranenie-umnih-ustroistv-v-promishlennosti-povlechyot-za-soboi-smenu-podhoda-k-kiberzaschite, free (Accessed: March 13, 2021) (in Russ.).

2. Check Point IoT Protect, CheckPoint Software Technologies LTD. Available at: https://www.checkpoint.com/downloads/products/cp-iot-security-solution-brief.pdf, free (Accessed: March 13, 2021).

3. Vasilyev V., Shamsutdinov R. Providing Information Security on the Base of Artificial Immune System for Industrial Internet of Thing, *Advances in Intelligent Systems Research*, 2020, vol. 174, pp. 212–217.

4. Tarakanov A.O., Tarakanov Y.A. A Comparison of Immune and Genetic Algorithms for Two Real-Life Tasks of Pattern Recognition, *International Journal of Unconventional Computing*, 2004, vol. 1.4, pp. 357–374.

5. Tarakanov A.O., Tarakanov Y.A. A Comparison of Immune and Neural Computing for Two Real-Life Tasks of Pattern Recognition, *Lecture Notes in Computer Science*, 2004, vol. 3239, pp. 236–249.

6. Saini V., Gupta J., Garg K.D. WSN Protocols, Research challenges in WSN, Integrated areas of sensor networks, security attacks in WSN, *European Journal of Molecular & Clinical Medicine*, 2020, vol. 7, iss. 3, pp. 5145–5153.

7. Ovasapyan T., Moskvin D. Security Provision in WSN on the Basis of the Adaptive Behavior of Nodes, *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, UK, 2020, pp. 81–85. Available at: https://ieeexplore.ieee.org/document/9210421, free (Accessed: March 05, 2021).

8. Yang S., Shiue Y., Su Z., Liu I., Liu C. An Authentication Information Exchange Scheme in WSN for IoT Applications, *IEEE Access*, 2020, vol. 8, pp. 9728–9738.

9. Yarde P., Srivastava S., Garg K. Adaptive immune-inspired energy-efficient and high coverage cross-layer routing protocol for wireless sensor networks, *IET Communications*, 2020, vol. 14, iss. 15, pp. 2592–2600.

10. Iwendi C., Zhang Z., Du X. ACO Based Key Management Routing Mechanism for WSN Security and Data Collection, *2018 IEEE International Conference on Industrial Technology (ICIT)*, 2018, pp. 1935–1939. Available at: https://ieeexplore.ieee.org/document/8352482, free (Accessed: March 05, 2021).

11. Kavitha T., Sridharan D. Security Vulnerabilities In Wireless Sensor Networks: A Survey, *Journal of Information Assurance and Security*, 2010, vol. 5, pp. 31–44.

12. Dimitrievski A., Pejovska V., Davcev D. Security Issues and Approaches in WSN. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.6190&rep=rep1&type=pdf, free (Accessed: June 06, 2021).

13. Furtak J., Zieliński Z., Chudzikiewicz J. Security techniques for the WSN link layer within military IoT, *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp. 233–238. Available at: https://ieeexplore.ieee.org/document/7845508, free (Accessed: March 02, 2021).

14. Almomani I., Al-Kasasbeh B., AL-Akhras M. WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks, *Journal of Sensors*, 2016, vol. 2016. Available at: https://www.hindawi.com/journals/js/2016/4731 953, free (Accessed: March 01, 2021).

15. Alqahtani M., Gumaei A., Mathkour H., Maher Ben Ismail M. A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks, *Sensors (Basel)*, 2019, vol. 19, pp. 1–20.

16. Le T.-T.-H., Park T., Cho D., Kim H. An Effective Classification for DoS Attacks in Wireless Sensor Networks, *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2018, pp. 689–692. Available at: https://www.researchgate.net/publication/327065277_An_Effective_Classification_for_DoS_Attacks_in_Wireless_Sensor_Networks, free (Accessed: September 06, 2021).

17. Alsulaimanand L., Al-Ahmadi S. Performance Evaluation of Machine Learning Techniques for DOS Detection in Wireless Sensor Network, *International Journal of Network Security & Its Applications (IJNSA)*, 2021, vol.13, no. 2, pp. 21–29.

18. Dong R.-H., Yan H.-H., Zhang Q.-Y. An Intrusion Detection Model for Wireless Sensor Network Based on Information Gain Ratio and Bagging Algorithm, *International Journal of Network Security*, 2020, vol. 22, no. 2, pp. 218–230.

19. Alaparthy V., Morgera S. A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory, *IEEE Access*, 2018, vol. 6, pp. 47364–47373.

20. Aldhaheri S., Alghazzawi D., Cheng L., Alzahrani B., Al-Barakat A. DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System, *Applied Sciences*, 2020, vol. 10, pp. 1909–1932.

21. Xiao X., Zhang R. A Danger Theory Inspired Protection Approach for Hierarchical Wireless Sensor Networks, *KSII Transactions on Internet and Information Systems*, 2019, vol. 13, no. 5, pp. 2732–2753.

Vladimir I. Vasilyev
Doctor of Science in Engineering, Professor,
Department of Computing and Information Security
Ufa State Aviation Technical University
12, Karl Marx st., Ufa, Russia, 450008
Phone: +7-917-350-11-39
Email: vasilyev@ugatu.ac.ru

Vladimir E. Gvozdev
Doctor of Science in Engineering, Professor,
Department of Technical Cybernetics,
Ufa State Aviation Technical University
12, Karl Marx st., Ufa, Russia, 450008
Phone: +7-917-369-27-73
Email: wega55@mail.ru

Rinat R. Shamsutdinov
Postgraduate student,
Department of Computing and Information Security,
Ufa State Aviation Technical University
12, Karl Marx st., Ufa, Russia, 450008
Phone: +7-927-950-84-13
Email: shrr2019@yandex.ru