Компьютерные инструменты в образовании, 2021
№ 1: 58–67
УДК: 004.056
http://cte.eltech.ru
doi:10.32603/2071-2340-2021-1-59-68

КОМБИНИРОВАННЫЙ ПОДХОД К ВЫЯВЛЕНИЮ АНОМАЛИЙ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ НА ПРИМЕРЕ СИСТЕМЫ УПРАВЛЕНИЯ ВОДОСНАБЖЕНИЕМ*

Мелешко А. В.[1], младший научный сотрудник, ✉ meleshko.a@iias.spb.su
Шулепов А. А.[2], аспирант, ✉ aoshyleo@gmail.com
Десницкий В. А.[1], кандидат технических наук, доцент, ✉ desnitsky@comsec.spb.ru
Новикова Е. С.[1,2], кандидат технических наук, доцент, ✉ novikova@comsec.spb.ru

[1]Федеральное государственное бюджетное учреждение науки
«Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
14-я линия В.О., д. 39, 199178, Санкт-Петербург, Россия
[2]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В. И. Ульянова (Ленина), ул. Профессора Попова, 5, корп. 3, 197376, Санкт-Петербург, Россия

Аннотация

Статья описывает подход к выявлению аномалий применительно к беспроводным сенсорным сетям (БСС). Он основан на комбинировании методов визуального анализа данных и методов машинного обучения. Данный подход апробирован на примере БСС управления водоснабжением. Для проверки разработаны программно-аппаратный прототип системы и программная модель для генерации необходимых наборов данных для формирования моделей детектирования и их тестирования. Проведенные эксперименты показали высокое качество детектирования, что показывает применимость комбинированного подхода для выявления аномалий к использованию на практике.

Ключевые слова: *аномалия, детектирование, машинное обучение, визуальный анализ.*

Цитирование: Мелешко А. В., Шулепов А. А., Десницкий В. А., Новикова Е. С. Комбинированный подход к выявлению аномалий в беспроводных сенсорных сетях на примере системы управления водоснабжением // Компьютерные инструменты в образовании. 2021. № 1. С. 58–67. doi: 10.32603/2071-2340-2021-1-59-68

1. ВВЕДЕНИЕ

В настоящее время широкое распространение получают различные индустриальные киберфизические системы и сети Интернета вещей, осуществляющие мониторинг параметров окружающей среды, пользователей разнообразных технических устройств

* Работа выполнена в СПб ФИЦ РАН при финансовой поддержке Российского Фонда Фундаментальных Исследований (проект 19-07-00953).

и объектов живой и неживой природы. Подобные системы мониторинга, как правило, функционируют в условиях не доверенного, не надежного окружения и подвержены атакующим воздействиям, способным привести к компрометации таких систем, их устройств, сервисов и данных [1].

Потенциально возможные несанкционированные воздействия на сенсоры БСС способны приводить к катастрофическим последствиям, связанным с нарушением бесперебойного функционирования системы, задержками в получении или искажениями собираемых в процессе мониторинга критически важных данных. Такие атаки могут приводить также к нарушениям процессов уведомления оператора системы о выявленных инцидентах безопасности и последующем принятии решений по реагированию на них. В частности, в случае системы управления водоснабжением прямые или опосредованные воздействия на сенсоры уровня воды способны в конечном счете приводить к критически важным переполнениям резервуаров воды, затоплениям, обмелениям, сбоям в поставках потребителям, а также возможным связанным с этим повреждениям элементов программно-аппаратной и физической инфраструктуры системы. В результате возникает необходимость разработки модельно-методического аппарата для эффективного детектирования подобных атак. Своевременное выявление атак на сенсоры системы будет способствовать оперативному реагированию на подобные инциденты, в том числе в части переключения режимов работы и использования альтернативных схем водоснабжения.

В работе проведено моделирование системы управления водоснабжением с использованием натурного и имитационного моделирования. Для детектирования применяются методы интеллектуального и визуального анализа данных, комбинирование которых позволяет не только более точно контролировать состояние системы, но и отслеживать и проверять функционирование самой модели мониторинга.

Атаки на датчики беспроводных сенсорных сетей, как правило, выражаются в злонамеренном искажении показаний одного или нескольких сенсоров, изменении количества выдаваемой информации или ее периодичности. При этом зачастую сам факт воздействия оказывается скрытым от оператора сети и используемых автоматизируемых средств защиты. Поэтому наиболее естественным представляется детектирование таких атак путем выявления различных аномальных значений, возникающих на множестве признаков, формируемых узлами сети динамически. При этом целесообразно ориентироваться как на выявление значимых отклонений от ожидаемых показаний сенсоров, так и на несогласованность между значениями различных сенсоров или даже групп сенсоров.

К элементам новизны проведенной работы можно отнести предложенный способ комбинирования частных методов машинного обучения и визуального анализа данных, которые позволили достичь повышенных показателей качества детектирования, а также способ построения графика состояния системы во времени. Достижимость установленных значений показателей качества подтверждается экспериментально на тестовых наборах данных, полученных в процессе моделирования. В частности, комбинирование методов интеллектуального и визуального анализа данных нацелены на повышение полноты детектирования атак, включая ранее неизвестные разновидности известных атак.

2. ОБЗОР ЛИТЕРАТУРЫ

В настоящее время проблематика безопасности различных интеллектуальных и автоматизированных киберфизических систем и сетей в различных областях приложения представляется чрезвычайно актуальной [2]. Как показывает анализ литературы,

современные работы по обнаружению аномалий в киберфизических системах и БСС базируются на использовании методов машинного и глубокого обучения [2–4]. При этом выбор и формирование наборов признаков, выбор методов обучения и их параметров, исследуемые классы атак оказываются зависящими от семантики конкретной области применения.

Wang и др. [3] предложили алгоритм детектирования атак на сенсоры в БСС на основе внедрения виртуального сенсора и использования модели ошибок в показаниях сенсоров и истории их измерений для выявления несоответствий между показаниями сенсоров, когда такие несоответствия можно интерпретировать как атаки.

В качестве технической системы, функционирующей в целях контроля и управления процессами водоснабжения, в [5] описана реализованная БСС для мониторинга качества воды. При этом используются 12 сенсоров различных видов загрязнения и другие характеристики. Используя модель детектирования аномалий ADWICE, путем кластеризации на основе образцов данных, описывающих состояния незагрязненной воды, авторы построили обучающую модель и протестировали ее на данных, описывающих состояния загрязнений.

Визуализация данных может существенно улучшить процессы как исследования данных, так и контроля объектов за счет представления данных в понятно и легко воспринимаемой форме. В научной литературе представлено множество подходов, в основе которых лежат методы визуализации многомерных данных, целью которых является выявление аномалий различного вида — злонамеренных или случайных [6, 7]. Например, Shi и др. [8] представили подробный обзор методов визуального анализа для обнаружений аномалий в поведении людей на основе анализа событий в сети, финансовых транзакций, социальных взаимодействий и данных о перемещениях. Джи и др. [9] исследовали различные методы визуализации, применяемые для обнаружения аномальной активности непосредственно в сетевом трафике. Однако существует не так много работ, в которых решается задача обнаружения аномалий на основе графического представления данных от физических сенсоров.

3. МОДЕЛИРОВАНИЕ ПРОЦЕССОВ УПРАВЛЕНИЯ ВОДОСНАБЖЕНИЕМ

Для моделирования работы системы управления водоснабжением используется программно-аппаратный прототип, а также программный эмулятор, имитирующий работу системы на тестовом сценарии и позволяющий сгенерировать наборы показаний сенсоров [10].

Разработанный программно-аппаратный прототип, использованный в работе, имеет два резервуара — верхний и нижний. Вода перетекает из верхнего резервуара в нижний под действием силы тяжести. Управляемый кран играет роль затвора дамбы, по сути, разделяющей резервуары. После наполнения второго резервуара закрывается кран, и вода посредством насоса перекачивается в первый резервуар. При этом вода по одну сторону дамбы уходит, а с другой стороны прибавляется. Сенсоры измеряют уровень воды в резервуарах, а также потоки перетекаемой или перекачиваемой воды. В каждом резервуаре три сенсора уровня воды и один сенсор давления, показывающие наполненность резервуара. В нижнем резервуаре расположен управляемый насос и сенсор потока воды, поступающей от насоса. Между резервуарами находится управляемый кран и сенсор потока воды между резервуарами. В качестве элементов управления используются: контроллер Arduino UNO — для считывания показаний сенсоров и Raspberry PI — для их обработки и организации мониторинга показаний через web-интерфейс. Развернутый

на одноплатном компьютере Web-сервер построен с использованием языка программирования Python, библиотек Django, ngnix и используется для подключения и просмотра показаний сенсоров и состояния исполнительных элементов.

Для возможности генерации большего количества возможных состояний системы и ускорения процессов моделирования и тестирования различных сценариев и атак также был разработан программный эмулятор системы, позволяющий генерировать последовательности ее состояний. С его помощью можно не только формировать различные наборы состояний системы, но также и моделировать атакующие воздействия нескольких видов.

Как результат работы эмулятора суммарно было получено семь наборов данных, содержащих записи нормального функционирования системы и атак. При этом было смоделировано пять классов атак. Временная продолжительность каждого набора данных — 1 час работы системы (7200 строк сформированного набора данных). Значения полученного набора данных представляют собой отсортированные по времени показания сенсоров устройств сети и состояния ее актуаторов (исполнительных элементов), полученные с интервалов времени в 1 сек. Атаки можно разделить на следующие пять классов: (1) атака на сенсоры уровня воды; (2) атака, направленная на искажение общего объема воды в резервуарах; (3) атака на сенсоры потока воды между резервуарами; (4) модифицированная атака на сенсоры потока воды; атака, являющаяся комбинацией атак (3) и (4).

4. КОМБИНИРОВАННЫЙ ПОДХОД К ВЫЯВЛЕНИЮ АНОМАЛЬНЫХ ДАННЫХ

Предложенный в настоящей работе подход к выявлению аномальных данных для системы управления водоснабжением включает: модель на основе методов машинного обучения с учителем, модель визуального анализа данных от сенсоров, комбинирование интеллектуального и визуального анализа данных.

Особенностью предлагаемого подхода является сочетание методов машинного обучения и методов визуального анализа. Главной задачей является создание методики, которая позволит понять поведение системы во время атаки, с одной стороны, и, с другой стороны, выполнить экспресс-оценку и валидацию модели машинного обучения в контексте функционирования контролируемой системы. В первом случае визуализация позволяет оператору интерпретировать результаты работы методов машинного обучения для того чтобы понять, каким образом атака влияет на параметры системы, и оценить их изменения в контексте истории работы системы. Во втором случае визуализацию можно рассматривать как способ контроля и валидации эффективности моделей машинного обучения, независимый от типа модели, и, возможно, как средство выявления новых видов аномалий, которые остались необнаруженными используемыми аналитическими моделями.

Модель детектирования, базирующаяся на методах машинного обучения, включает 5 бинарных классификаторов для каждого типа атаки и один обобщенный — мультиклассификатор, направленные на отнесение образцов анализируемых данных к одному из 5 классов атак. Использованы следующие 7 методов машинного обучения с учителем: AdaBoost-классификатор, Случайный Лес, Байесовский классификатор, Логистическая регрессия, Линейный классификатор на основе метода опорных векторов (SVM), Деревья решений и Ridge-классификатор. Серия экспериментов на тестовых наборах данных позволила выбрать наиболее эффективные методы обучения и значения их параметров.

Для визуализации данных с различных датчиков одновременно авторы использовали подход, предложенный в [6], согласно которому состояние системы, описываемое множеством показаний датчиков в некоторый момент времени, рассматривается как точка в многомерном пространстве. Такое решение позволяет представить функционирование системы в виде траектории точки в многомерном пространстве. Исследование, выполненное авторами ранее [6], показало, что применение методов снижения размерности, таких как PCA или t-SNE [11], позволяет выявлять различные изменения в поведении системы и строить паттерны ее функционирования. Полученные результаты позволили авторам предположить, что площадь между точками, расположенными последовательно, можно использовать как меру изменения поведения системы, и построить график этих значений для контроля состояния системы. Таким образом, алгоритм предварительной обработки данных и их последующей визуализации описывается следующим образом:

1) выполнить снижение размерности исходных данных для их отображения в двумерное пространство, например, методом PCA;
2) выбрать размер скользящего окна для выбора последовательности точек, включая текущую;
3) применить триангуляцию Делоне над выбранным набором точек для вычисления меры изменения состояния системы (если количество точек больше 2, в противном случае вычислить эвклидово расстояние между двумя точками);
4) построить линейный график меры изменения в функционировании системы, на котором по оси Y откладывается вычисленная мера для текущего состояния, а по оси X — временная метка.

5. РЕАЛИЗАЦИЯ, ЭКСПЕРИМЕНТЫ И ДИСКУССИЯ

Реализация классификаторов проведена с использованием средств библиотеки scikit-learn. Использованные в рамках экспериментов наборы данных представляют собой записи состояния системы управления водоснабжением в определенный момент времени, то есть записи показаний сенсоров системы и состояний её актуаторов — анализируемых признаков. Подбор наилучших параметров для каждого из методов проведен с использованием компонента GridSearch. Кроме того, учитывались зависимости результата классификации от каждого из имеющихся признаков. По результатам экспериментов можно выделить наилучшие методы для каждого входного набора данных, обладающие наивысшими значениями правильности, f-меры и обеспечивающими минимальное время детектирования (таблица 1).

Для оценки способа визуализации использовались те же наборы данных. Была выполнена серия экспериментов для определения размера окна для выбора последовательности точек, для которых вычисляется мера изменения состояния системы. Были исследованы результаты визуализации при размере окна, равного 2, 3, 4 и 10 точкам. И, хотя графики для всех вариантов предобработки данных довольно похожи, можно сказать, что использование триангуляции по n точкам как способ вычисления меры изменения состояния системы позволяет сформировать более явные графические признаки аномалий и атак по сравнению с мерой изменения, вычисляемой как эвклидово расстояние между двумя точками. Поэтому минимальный рекомендуемый размер скользящего окна равен 3.

Эксперименты также показали, что для различных атак характерны различные графические паттерны, которые отличаются как по диапазону изменения значений меры плотности распределения точек на плоскости, так и наличием выбросов. Некоторые атаки явно видны без выполнения каких-либо дополнительных механизмов пост-обработки,

Таблица 1. Наилучшие методы машинного обучения и их параметры точности и f–меры

Название атаки	Лучший метод	Правильность	F-1 мера
Искажение уровня воды в одном резервуаре (атака 1)	SVM	99 %	0.99
Искажение общего объема воды в резервуарах (атака 2)	SVM	100 %	1.0
Искажение показаний сенсора потока воды при закрытом кране (атака 3)	Деревья решений	100 %	1.0
Искажение показаний сенсора потока воды при открытом кране или включенном насосе (атака 4)	Деревья решений	100 %	1.0
Подмена показаний потока воды (атака 5)	Деревья решений r	99 %	0.95
Все перечисленные атаки	Деревья решений	99 %	0.99

другие же требуют применения дополнительных механизмов пост-обработки полученных данных, связанных с применением фильтров на основе скользящего среднего или медианы, или переключения на логарифмическую шкалу для графического представления полученных значений меры изменения состояния системы. Для примера, атака класса 1 явно видна на обоих графиках с линейной и логарифмической шкалами, однако аномалия более очевидна при применении медианного фильтра с окном фильтрации, равным 60 точкам (рис. 1). Состояние системы в момент атаки класса 2 не отличается значительно от состояния системы в нормальном режиме работы независимо от применяемых механизмов пост-обработки данных. Однако в моменты начала и завершения атаки явно видны точки-выбросы (рис. 2). Этот признак специфичен для атаки данного класса. Следовательно, можно сделать вывод о том, что предложенный способ визуализации данных выглядит многообещающим как для мониторинга состояния системы, так и для анализа результатов применения моделей.

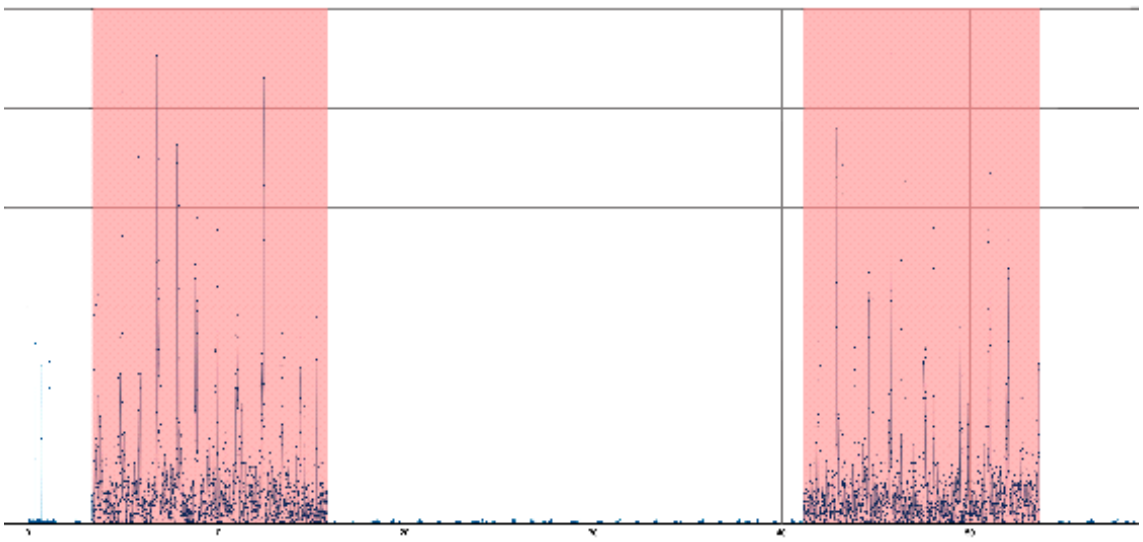

Рис. 1. Визуализация состояния системы в момент атаки класса 1, периоды времени, когда система находится под атакой, выделены цветом фона графика

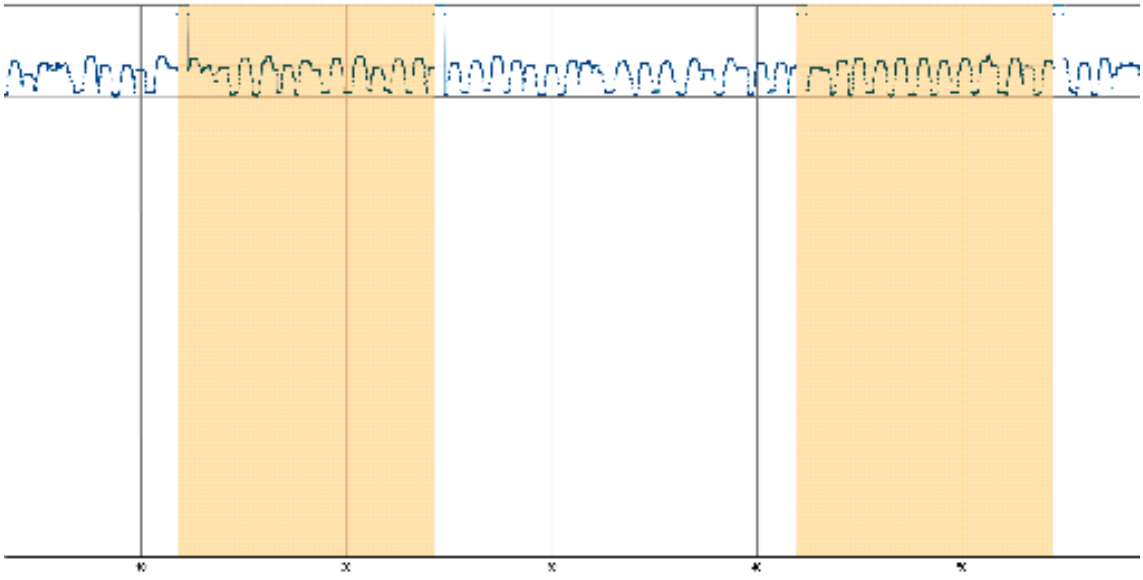

Рис. 2. Визуализация состояния системы в момент атаки класса 2, периоды, когда система находится под атакой, выделены цветом фона графика

Однако очевидно, что он требует разработки дополнительных механизмов предварительной и последующей обработки значений меры изменения состояния системы для более явного выделения признаков изменений в ней.

6. ЗАКЛЮЧЕНИЕ

В работе предложен комплексный подход к детектированию аномалий в беспроводных сенсорных сетях управления водоснабжением с использованием методов машинного обучения и визуального анализа данных. Применимость подхода подтверждена эмпирически на серии экспериментов. Полученные в результате экспериментов значения показателей правильности и f1-меры имеют высокие значения на объединенном датасете со смешанными данными с одновременным присутствием аномалий нескольких видов. Это позволило не только установить факт наличия аномалии, но также и определить ее разновидность. Исследование методов визуального анализа позволило установить наиболее подходящие для этого средства и формы отображения данных, а также их ограничения.

Кроме того, предложены два способа комбинированного использования построенных классификаторов и средств визуального анализа, которые целесообразно применять на практике: использование визуализации в качестве экспресс-оценки состояния сети оператором с последующим применением машинных классификаторов и в качестве средств апостериорной валидации построенных классификаторов.

В качестве направления дальнейшей работы планируется применение методов кластеризации и одноклассовой классификации как средств, возможно, менее точной идентификации злонамеренных воздействий, но применимых для повышения эффективности детектирования ранее неизвестных видов атак.

Другое возможное направление будущей работы связано с проработкой дополнительных способов обработки данных для их графического представления. К выбору методов следует подходить очень осторожно, для того чтобы избежать чрезмерной адаптации

способа визуализации к конкретным видам атак и сохранить возможность выявления ранее неизвестных аномалий.

Список литературы

1. *Левшун Д. С., Гайфулина Д. А., Чечулин А. А., Котенко И. В.* Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация. 2020. Т. 19, № 5. С. 1050–1088. doi: 10.15622/ia.2020.19.5.6
2. *Shin J., Baek Y., Eun Y., Son S. H.* Intelligent sensor attack detection and identification for automotive cyber-physic systems // Proc. 2017 IEEE Symposium Series on Computational Intelligence (SSCI). Honolulu, HI, USA, 2017. P. 1–8. doi: 10.1109/SSCI.2017.8280915
3. *Wang R., Song H., Jing Y., Yang K., Guan Y., Sun J.* A Sensor Attack Detection Method in Intelligent Vehicle with Multiple Sensors // Proc. 2019 IEEE International Conference on Industrial Internet (ICII). Orlando, FL, USA, 2019. P. 219–226. doi: 10.1109/ICII.2019.00047
4. *Inoue J., Yamagata Y., Chen Y., Poskitt C. M., Sun J.* Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning // Proc. 2017 IEEE International Conference on Data Mining Workshops (ICDMW). New Orleans, LA, USA, 2017. P. 1058–1065. doi: 10.1109/ICDMW.2017.149
5. *Raciti M., Cucurull J., Nadjm-Tehrani S.* Anomaly Detection in Water Management Systems, J. Lopez, R. Setola, and S. D. Wolthusen, eds. // Critical Infrastructure Protection. Heidelberg, Berlin: Springer, 2012. Vol. 7130. P. 98–119. doi: 10.1007/978-3-642-28920-0_6
6. *Novikova E., Bestuzhev M., Kotenko I.* Anomaly Detection in the HVAC System Operation by a RadViz Based Visualization-Driven Approach. S. Katsikas et al., eds. // Computer Security. CyberICPS 2019, SECPRE 2019, SPOSE 2019, ADIoT 2019. 2020. Vol. 11980. P. 402–418. doi: 10.1007/978-3-030-42048-2_26
7. *Herr D., Beck F., Ertl T.* Visual Analytics for Decomposing Temporal Event Series of Production Lines // Proc. 22nd International Conference Information Visualisation (IV). Fisciano, Italy, 2018. P. 251–259. doi: 10.1109/iV.2018.00051
8. *Shi Y., Liu Y., Tong H., He J., Yan G., Cao N.* Visual Analytics of Anomalous User Behaviors: A Survey // IEEE Transactions on Big Data, 2015. Vol. 14, no. 8. P. 1–20. doi: 10.1109/TBDATA.2020.2964169
9. *Ji S. Y., Jeong B. K., Jeong D. H.* Evaluating visualization approaches to detect abnormal activities in network traffic data // Int. J. Inf. Secur., 2020. Vol. 20. P. 331–345. doi: 10.1007/s10207-020-00504-9
10. *Meleshko A., Desnitsky V., Kotenko I.* Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems // IOP Conference Series: Materials Science and Engineering, 2019. Vol. 709. P. 1–7.
11. *van der Maaten L. J. P., Hinton G. E.* Visualizing High-Dimensional Data Using t-SNE // Journal of Machine Learning Research, 2008. Vol. 9, no. 11. P. 2579–2605.

Поступила в редакцию 10.02.2021, окончательный вариант — 11.03.2021.

Мелешко Алексей Викторович, младший научный сотрудник Лаборатории проблем компьютерной безопасности СПб ФИЦ РАН, ✉ meleshko.a@iias.spb.su

Шулепов Антон Андреевич, аспирант кафедры информационных системы СПбГЭТУ «ЛЭТИ» им. В. И. Ульянова (Ленина), ✉ aoshyleo@gmail.com

Десницкий Василий Алексеевич, кандидат технических наук, доцент, старший научный сотрудник Лаборатории проблем компьютерной безопасности СПб ФИЦ РАН, ✉ desnitsky@comsec.spb.ru

Новикова Евгения Сергеевна, кандидат технических наук, доцент, старший научный сотрудник Лаборатории проблем компьютерной безопасности СПб ФИЦ РАН, ✉ novikova@comsec.spb.ru

Computer tools in education, 2021
№ 1: 58–67
http://cte.eltech.ru
doi:10.32603/2071-2340-2021-1-59-68

Integrated Approach to Revelation of Anomalies in Wireless Sensor Networks for Water Control Cases

Meleshko A. V.[1], Junior Researcher, ✉ meleshko.a@iias.spb.su
Shulepov A. A.[2], Postgraduate, ✉ aoshyleo@gmail.com
Desnitsky V. A.[1], PhD, Associate Professor, ✉ desnitsky@comsec.spb.ru
Novikova E. S.[1,2], PhD, Associate Professor, ✉ novikova@comsec.spb.ru

[1]St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS) St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS)
39, 14th Line V. O., 199178, Saint Petersburg, Russia.
[2]Saint Petersburg Electrotechnical University «LETI»
5, building 3, st. Professora Popova, 197376, Saint Petersburg, Russia

Abstract

This article describes an approach to revelation of anomalies for Wireless Sensor Networks (WSN). It is based on the integration of visual data analysis techniques and data mining techniques. Feasibility of the approach has been confirmed on a demo case for WSN water management scenario. For verification we developed a software/hardware prototype of the network and a software model to generate the necessary data sets for the establishment of detection models and their investigation. The experiments carried out have shown a high quality of detection, which shows the applicability of the integrated approach to revelation of anomalies for use in practical cases.

Keywords: *anomaly, detection, machine learning, visual analysis.*

Acknowledgements: *The work is performed in SPC RAS and supported Russian Foundation for Basic Research (project 19-07-00953).*

Citation: A. V. Meleshko, A. A. Shulepov, V. A. Desnitsky, and E. S. Novikova, "Integrated Approach to Revelation of Anomalies in Wireless Sensor Networks for Water Control Cases," *Computer tools in education*, no. 1, pp. 58-67, 2021 (in Russian); doi: 10.32603/2071-2340-2021-1-59-68

References

1. D. Levshun, D. Gaifulina, A. Chechulin, and I. Kotenko, "Problemnye voprosy informatsionnoi bezopasnosti kiberfizicheskikh sistem" [Problematic Issues of Information Security of Cyber-Physical Systems], *Informatics and automation*, vol. 19, no. 5, pp. 1050–1088, 2020 (in Russian); doi: 10.15622/ia.2020.19.5.6
2. J. Shin, Y. Baek, Y. Eun, and S. H. Son, "Intelligent sensor attack detection and identification for automotive cyber-physic systems," in *Proc. 2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, Honolulu, HI, USA, 2017, pp. 1–8; doi: 10.1109/SSCI.2017.8280915
3. R. Wang, H. Song, Y. Jing, K. Yang, Y. Guan, and J. Sun, "A Sensor Attack Detection Method in Intelligent Vehicle with Multiple Sensors," in *Proc. 2019 IEEE International Conference on Industrial Internet (ICII)*, Orlando, FL, USA, 2019, pp. 219–226; doi: 10.1109/ICII.2019.00047

4. J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, “Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning,” in *Proc. 2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, New Orleans, LA, USA, 2017, pp. 1058–1065; doi: 10.1109/ICDMW.2017.149
5. M. Raciti, J. Cucurull, and S. Nadjm-Tehrani, “Anomaly Detection in Water Management Systems,” J. Lopez, R. Setola, and S. D. Wolthusen, eds., *Critical Infrastructure Protection*, Heidelberg, Berlin: Springer, vol. 7130, pp. 98–119, 2012; doi: 10.1007/978-3-642-28920-0_6
6. E. Novikova, M. Bestuzhev, and I. Kotenko, “Anomaly Detection in the HVAC System Operation by a RadViz Based Visualization-Driven Approach,” S. Katsikas et al., eds., in *Computer Security. CyberICPS 2019, SECPRE 2019, SPOSE 2019, ADIoT 2019*, vol. 11980, 2020, pp. 402–418; doi: 10.1007/978-3-030-42048-2_26
7. D. Herr, F. Beck, and T. Ertl, “Visual Analytics for Decomposing Temporal Event Series of Production Lines,” in *Proc. 22nd International Conference Information Visualisation (IV)*, Fisciano, Italy, 2018, pp. 251–259; doi: 10.1109/iV.2018.00051
8. Y. Shi, Y. Liu, H. Tong, J. He, G. Yan and N. Cao, “Visual Analytics of Anomalous User Behaviors: A Survey,” *IEEE Transactions on Big Data*, vol. 14, no. 8, pp. 1–20, 2015; doi: 10.1109/TBDATA.2020.2964169
9. S. Y. Ji, B. K. Jeong, and D. H. Jeong, “Evaluating visualization approaches to detect abnormal activities in network traffic data,” *Int. J. Inf. Secur.*, vol. 20, 331–345, 2020; doi: 10.1007/s10207-020-00504-9
10. A. Meleshko, V. Desnitsky, and I. Kotenko, “Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems,” *IOP Conference Series: Materials Science and Engineering*, vol. 709, pp. 1–7, 2019.
11. L. J. P. van der Maaten and G. E. Hinton, “Visualizing High-Dimensional Data Using t-SNE,” *Journal of Machine Learning Research*, vol. 9, no. 11, pp. 2579–2605, 2008.

Received 10-02-2021, the final version — 11-03-2021.

Alexey Meleshko, Junior Researcher Laboratory of Computer Security Problems of SPC RAS, ✉ meleshko.a@iias.spb.su

Anton Shulepov, Postgraduate of Information Systems Department of Saint Petersburg Electrotechnical University «LETI», ✉ aoshyleo@gmail.com

Vasily Desnitsky, PhD, Associate Professor, Senior Researcher Laboratory of Computer Security Problems of SPC RAS, ✉ desnitsky@comsec.spb.ru

Evgenia Novikova, PhD, Associate Professor, Senior Researcher Laboratory of Computer Security Problems of SPC RAS, ✉ novikova@comsec.spb.ru