ISSN 2782-2001
Системы анализа
и обработки данных
том 85, № 1, 2022, с. 109–120

http://journals.nstu.ru/vestnik
Analysis and data
processing systems
Vol. 85, No. 1, 2022, pp. 109–120

ИНФОРМАТИКА,
ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
И УПРАВЛЕНИЕ

INFORMATICS,
COMPPUTER ENGINEERING
AND MANAGEMENT

УДК 621.391.812.4 DOI: 10.17212/2782-2001-2022-1-109-120

Метод цифровых водяных символов для совершенствования объектов на базе кластеров и значения восприятия*

П.М. ШОНАЗАРОВ[1,a], Ф.Т. ХОЛОВ[2,b], Б.Б. САИДОВ[1,c]

[1] *454080, РФ, г. Челябинск, пр. Ленина, 86, Южно-Уральский государственный университет*
[2] *634050, РФ, г. Томск, пр. Ленина, 40, Томский государственный университет систем управления и радиоэлектроники*

[a] *shonazarov1991@gmail.com* [b] *fozil_1990-90@mail.ru* [c] *mathem.1994@mail.ru*

Одна из наиболее важных проблем в области IoT – ограничения ресурсов, такие как источник питания, вычислительная мощность, объем памяти, диапазон беспроводной связи и ширина полосы беспроводной связи. Беспроводная маршрутизация с низкой пропускной способностью требует нескольких шагов для достижения пункта назначения. Интернет вещей (Internet of things, IoT) – это технология, которая состоит из набора объектов, подключенных через Интернет, и собирает информацию, генерируемую датчиками; IoT – это устройства, которые подключены в сеть и доступны «любому и ко всему» в любое время и в любом месте. Примерами таких устройств могут быть датчики температуры, датчики движения, датчики сердечного ритма, датчики энергопотребления и т. д. Например, датчик температуры может быть встроен в термостат, показатель количества потребляемой электроэнергии в домах и датчик уличного движения на светофоре. В этой статье предлагается схема, основанная на хрупком водяном знаке и улучшенной кластеризации, чтобы разрешить конфликт между безопасностью и ограниченными ресурсами уровня восприятия. Для повышения безопасности мы разрабатываем стратегию стохастического позиционирования, основанную на алгоритме кластеризации, чтобы вычислить положение, встроенное во временную динамику измерения данных. Таким образом, уязвимости безопасности, создаваемые стационарной встроенной ситуацией, могут не только эффективно устраняться, но и приводить к нулевому нарушению данных. Результаты исследований показывают, что предложенный алгоритм может эффективно обеспечивать интеграцию «недорогих» данных, а также снизить энергопотребление и увеличить время жизни сети.

Ключевые слова: интернет вещей, IoT, цифровая маркировка, цифровые водяные знаки, безопасность, передача данных, множественная маршрутизация, алгоритм кластеризации, временная динамика

* *Статья получена 03 сентября 2021 г.*

ВВЕДЕНИЕ

Одной из основных проблем в интернете вещей (IoT) является безопасность и конфиденциальность. Быстрое принятие IoT как неотъемлемой части повседневной жизни и открытость вызывает обеспокоенность в отношении безопасности независимых объектов, которые имеют функцию обмена данными для выполнения личных или коллективных задач [1–3]. Интернет вещей – это технология, которая состоит из набора объектов, связанных через Интернет, и собирает информацию, генерируемую датчиками. Все датчики отправляют информацию в контрольные блоки назначения для принятия решений на основе этой информации. Вполне возможно, что в ближайшем будущем будет большой объем взаимосвязей между компьютерами и другим электронным оборудованием, которые взаимосвязаны и обмениваются информацией через Интернет, тем самым уменьшая вмешательство человека [4–7].

В этой статье мы в основном рассматриваем защиту данных восприятия и беспроводные сенсорные сети (WSN) как уровень восприятия IoT. Беспроводные сенсорные сети организованы большим количеством микродатчиков с ограниченной вычислительной мощностью и малым зарядом батареи для формирования самоорганизующейся сети в беспроводной связи. Предложенный алгоритм водяного знака обеспечивает целостность данных и может эффективно предотвращать различные атаки, вызванные вредоносными узлами. Кроме того, предложенный алгоритм эффективно решает недостатки существующих технологий, такие как энергопотребление. Данный алгоритм сохраняет больше энергии, чем алгоритмы LSB и MultiMark, повышает эффективность аутентификации и безопасность, обеспечивает обратимое извлечение водяного знака.

Одной из наиболее важных проблем в области IoT являются ограничения ресурсов, такие как источник питания, вычислительная мощность, объем памяти, диапазон беспроводной связи и ширина полосы беспроводной связи. Беспроводная маршрутизация с низкой пропускной способностью требует нескольких шагов маршрутизации для достижения пункта назначения. Низкая вычислительная мощность и ограничения памяти на устройствах IoT требуют максимально возможной оптимизации процесса маршрутизации. Низкая пропускная способность связи создает ограничение: размер прямых пакетов должен быть небольшим. Из-за дефицита энергоснабжения будет трудно решить, какой узел будет двигаться дальше, потому что беспроводная связь будет определять потребление энергии устройствами IoT [8, 9]. На рис. 1 показана структура мониторинга энергии на основе интернета вещей.

Рис. 1. Структура IoT на уровне восприятия

Fig. 1. The structure of the IoT at the perception level

Уровень восприятия также указывается в этой форме. Этот простой уровень узлов сталкивается с серьезными проблемами безопасности, которые привлекают внимание большинства исследователей. Главная особенность функции уровня восприятия состоит в том, чтобы понимать информацию. Восприятие информации основано на приложениях IoT, которые генерируют информацию из физического мира. Таким образом, уровень восприятия является основной проблемой в области IoT.

1. ТЕХНОЛОГИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Информация о восприятии играет важную роль в качестве связующего звена между IoT и реальным миром, состоящим из данных о восприятии и данных о местоположении. Раскрытие данных о восприятии может привести к раскрытию важной информации по всей сети, что приведет к непоправимым последствиям. Чтобы устранить недостатки традиционных методов аутентификации интеграции данных, исследователи внедрили технологию цифровых водяных знаков (ЦВЗ) в WSN для защиты целостности данных [9]. Технология ЦВЗ широко используется для защиты информации об авторских правах и интеграции контента цифровых мультимедийных произведений (изображений, аудио и видео и т. д.) [10]. По сравнению с традиционной технологией шифрования технология ЦВЗ имеет четыре преимущества:

1) ЦВЗ использует легкие вычисления, что приводит к низкому энергопотреблению;

2) информация о водяных знаках напрямую интегрируется в данные без дополнительных затрат на сетевую связь и емкость хранилища узлов в WSN;

3) методы шифрования теряют свое действие после дешифрования, но ЦВЗ остаются как неотъемлемая часть носителя и всегда могут гарантировать безопасность данных [11–15];

4) технология ЦВЗ может значительно уменьшить сквозную задержку, вызванную технологией шифрования.

В этой статье также используется кластеризация для сенсорной сети. Кластеризация относится к группированию выборок или наблюдений в классы похожих объектов. Кластер – это набор выборок, которые похожи друг на друга и отличаются от других выборок кластера. Кластеризация не пытается прогнозировать, оценивать или классифицировать выборки. Вместо этого алгоритмы кластеризации стремятся разбить все выборки на подгруппы или кластеры так, чтобы сходство между выборками в максимальном кластере и сходство с выборками в другом кластере было минимальным.

Кластеризация важна для интеллектуального анализа данных, группировки, принятия решений и машинного обучения, включая интеллектуальный анализ данных, поиск информации, сегментацию изображений и классификацию шаблонов. Кроме того, в тех случаях, когда базовых знаний о данных и принятии решений (статистических моделях) мало, кластеризация может дать предположения о данных.

Следует отметить, что кластеризация процессов является тематической в том смысле, что сходные наборы данных для разных задач часто классифицируются как разные кластеры. Это делает кластеризацию сложной проблемой, и поэтому только один алгоритм не подходит для решения каждой проблемы кластеризации. Кластеризация также может использоваться в качестве шага предварительной обработки для извлечения классов шаблонов.

Благодаря функциям контратаки цифровую маркировку можно разделить на хрупкую маркировку и стойкую маркировку [16]. Хрупкая маркировка не устойчива к изменениям и может использоваться для защиты авторских прав. Хрупкая маркировка очень чувствительна к манипуляциям, и любое изменение в носителе может привести к неадекватной маркировке, которая может быть использована для проверки данных [17]. В этой статье мы представляем хрупкую технику маркировки. Предложенный алгоритм динамически вычисляет внедренную позицию сигнала, используя время сбора данных от узлов датчиков, что не только повышает безопасность, но также экономит энергию и проверку данных в реальном времени.

2. ПРЕДЛАГАЕМЫЙ ПЛАН

По сравнению с проводными сетями WSN, развертываемые в жестких условиях, подвергаются большей угрозе, и, кроме того, протокол общедоступной связи, принятый WSN, увеличивает риск физических манипуляций. Воспринимающий узел обладает вычислительной мощностью и ограниченными энергетическими ресурсами, что увеличивает недостаток при разработке протоколов безопасности. Мы суммируем основные модели атак на пять категорий.

1. Манипулирование пакетами: злонамеренный узел добавляется к пакетам WSN и отправляет манипулированные пакеты, что в некоторых случаях может иметь очень серьезные последствия.

2. Подделка пакетов: злонамеренный узел, добавленный в WSN, продолжает отправлять поддельные пакеты другим узлам, значительно увеличивая сетевой трафик и, таким образом, тратя всю энергию WSN.

3. Выборочный транспорт: злонамеренный узел, добавленный в WSN, удаляет частичные пакеты и передает некоторые пакеты в пункт назначения. Потеря информации может привести к плохой ситуации, когда узел приемника не может предоставить правильный ответ.

4. Распределение пакетов: злонамеренный узел, добавленный в WSN, передает пакеты, отправленные один или несколько раз, на другие узлы, вызывая перегрузку и потерю энергии.

5. Задержка при передаче: злонамеренный узел, добавленный в WSN, доставляет пакеты позже заданного времени, что приводит к тому, что узел приемника покидает пакеты.

3. МЕТОД ИССЛЕДОВАНИЙ

В настоящей статье представлена новая стратегия защиты целостности данных WSN, основанная на хрупких методах цифровой разметки. Этот алгоритм сначала делит данные зондирования на группы одинакового размера (количество, которого не могут достичь данные зондирования) по отношению к определителю; создает последовательность SN для каждой группы и помещает ее в группу с целью определения функции удаления или добавления групп. Цифровая запись была получена с помощью хэш-функции (HASH) через ключ K, групповые данные и серийный номер группы. Чтобы предотвратить повторную атаку, алгоритм помещает текущую группу в предыдущую группу,

а затем объединяет все группы с цифровой маркировкой. Предлагается алгоритм, основанный на хрупкой цифровой разметке, для защиты данных датчиков от вышеуказанных категорий моделей атак. Предложенный алгоритм использует признаки, которые являются хрупкой маркировкой, чувствительной к модификации. После изменения данных хоста отметка печати исчезает. Вредоносные узлы не могут эффективно извлекать реальные данные без предварительного знания алгоритмов маркировки. Манипулирование данными и подмена данных схожи, и их можно рассматривать как вредоносные данные, генерируемые вредоносными узлами. Предложенный алгоритм вводит порядковый номер пакета SN, который используется для определения местоположения добавленных или удаленных пакетов. Алгоритм маркировки состоит из трех процессов, а именно: создание цифрового знака, внедрение цифрового знака и извлечение цифрового знака, как показано на рис. 2. На первом этапе каждый узел датчика собирает данные датчика и выдает цифровой сигнал в соответствии с алгоритмом хрупкой маркировки. Затем разметка объединяется с данными датчика по заранее заданному правилу, чтобы сформировать пакет данных, который передается на узел приемника через узел передачи.

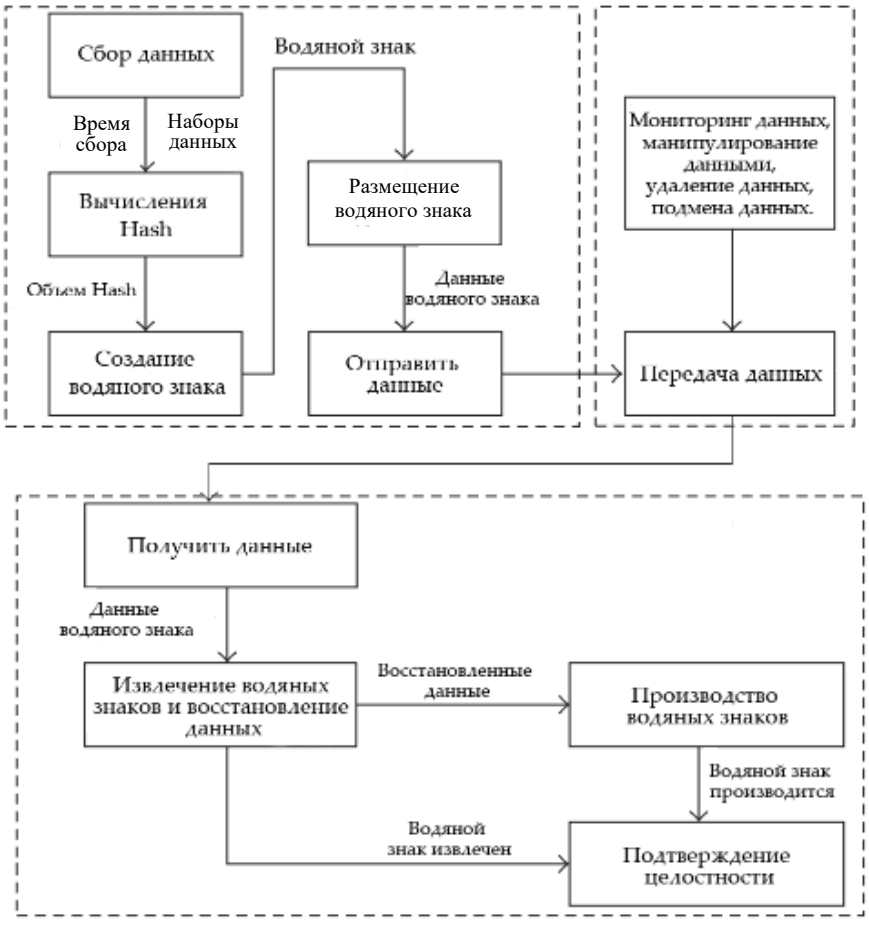

Рис. 2. Модель реализации предложенного алгоритма хрупкой маркировки

Fig. 2. An implementation model of the proposed fragile marking algorithm

Пакет может столкнуться с ненадежной передачей и различными типами атак. Затем узел приемника принимает данные, извлекает водяной знак и обнаруженные данные в соответствии с предопределенным правилом.

Существует также общий процесс кластеризации для беспроводной сенсорной сети.

1. Отображение шаблонов, которые обычно включают выделение или извлечение атрибута.

2. Определение метрики оценки аналогично определению области данных.

3. Процесс кластеризации или группировки.

4. Суммирование данных при необходимости.

5. Проверка системы.

На рис. 3 показаны первые три шага этого процесса, включая обратную связь с результатами кластеризации на первых двух шагах.

Шаблоны представляют количество классов, количество доступных выборок, а также количество, тип и масштаб объектов в алгоритме кластеризации. Обратите внимание, что часть этой информации не контролируется пользователем.

Рис. 3. Процесс кластеризации для беспроводной сенсорной сети

Fig. 3. The clustering process for a wireless sensor network

Выбор функций – это процесс определения подмножества наиболее эффективных функций кластеризации и извлечения функций, процесс изменения некоторых существующих функций и создания новых функций. Оба этих метода предназначены для достижения правильного набора функций и повышения эффективности кластеризации.

Близость выборок обычно измеряется функцией расстояния между парой входных шаблонов. Простой критерий измерения, такой как евклидово расстояние, обычно используется, чтобы показать несоответствие между двумя образцами, а другие критерии оценки также могут быть использованы для определения концептуального сходства между образцами [5].

4. РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

Моделирование было проведено в среде MathLab 2017a. Результаты моделирования показаны на рис. 4. Этот рисунок наглядно демонстрирует превосходство предложенного алгоритма с точки зрения пропускной способности по сравнению с методами Multi-Marker и LSB. Встраивание с самой низкой разметкой битов (LSB), представленное в [19, 20], не только ограничивает емкость встраивания, но также нарушает целостность данных, что крайне опасно для высокоточных приложений. Метод множественных меток в [18] может гарантировать точность данных, но количество пустых символов ограничено, что уменьшает емкость разметки.

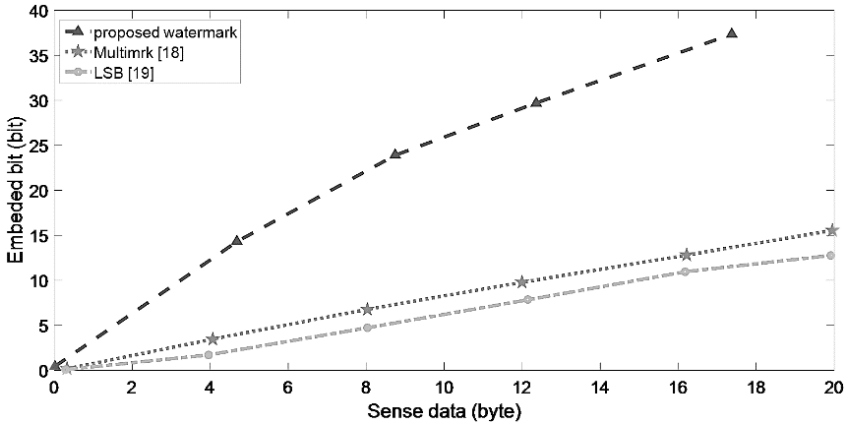

Рис. 4. Водяной знак встроенной емкости

Fig. 4. A built-in tank watermark

На рис. 5 показана диаграмма энергопотребления, которая четко показывает, что предлагаемый алгоритм сохраняет больше энергии, чем алгоритмы LSB и MultiMark.

На рис. 6 показано количество узлов для беспроводной сенсорной сети. Видно, что предлагаемый способ на основе кластеризации и водяного знака имеет больше узлов.

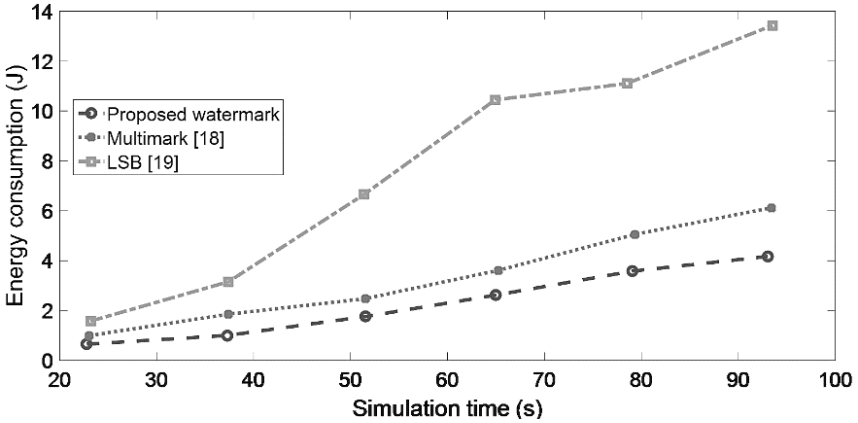

Рис. 5. Диаграмма энергопотребления

Fig. 5. A power consumption diagram

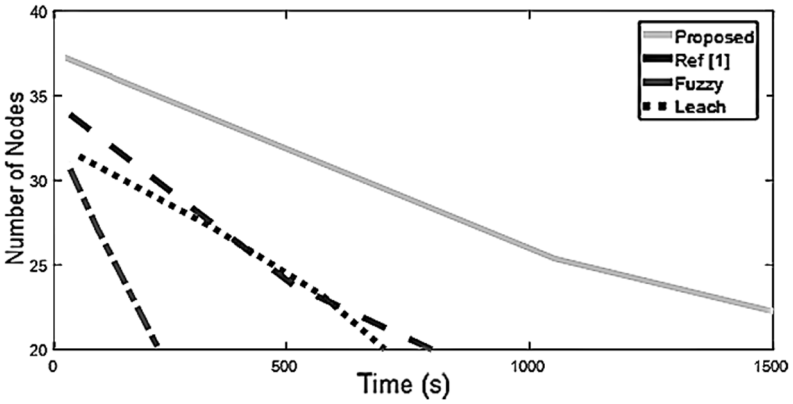

Рис. 6. График количества узлов

Fig. 6. Graph of the number of nodes

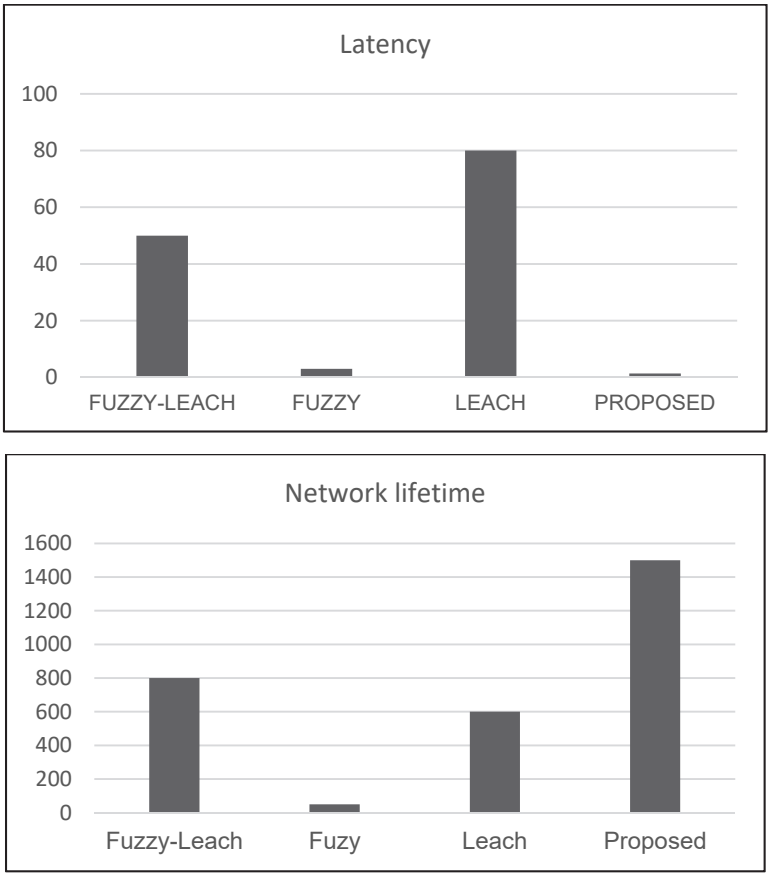

Рис. 7. Диаграмма задержки и времени жизни сети

Fig. 7. Network latency and lifetime diagram

График задержки и времени жизни сети показан на рис. 7. Результаты показывают, что предлагаемый способ имеет меньшую задержку и более длительный срок службы WSN.

ЗАКЛЮЧЕНИЕ

В этой статье представлен усовершенствованный алгоритм цифровой разметки, а также новый алгоритм кластеризации для интеграции данных уровня восприятия IoT, улучшения энергопотребления и времени жизни сети. Предложенный алгоритм может эффективно предотвращать различные атаки, такие как спуфинговые атаки, атаки с пересылкой пакетов, атаки с манипулированием пакетами, атаки с повторением пакетов и атаки с задержкой пакетов из-за вредоносных узлов. Кроме того, предлагаемый алгоритм эффективно устраняет недостатки существующих технологий. Это не только упрощает вычислительную сложность и повышает эффективность и безопасность, но также обеспечивает обратимое извлечение из маркировки и поиска без данных.

СПИСОК ЛИТЕРАТУРЫ

1. *Tolibovich K.F., Aleksandrovich S.A., Mahmadnazarovich S.P.* A new algorithm watermark for improving objects based on clusters and perceptions // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – Yekaterinburg, Russia, 2020. – P. 520–523. – DOI: 10.1109/USBEREIT48449.2020.9117762.

2. Blockchain for IoT security and privacy: the case study of a smart home / A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram // 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). – Kona, HI, USA, 2017. – P. 618–623. – DOI: 10.1109/PERCOMW.2017.7917634.

3. *Dorri A., Kanhere S.S., Jurdak R.* Towards an optimized blockchain for IoT // 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). – Pittsburgh, PA, USA, 2017. – P. 173–178.

4. Fuzzy comprehensive evaluation method for energy management systems based on an internet of things / Y. Li, Z. Sun, L. Han, N. Mei // IEEE Access. – 2017. – Vol. 5. – P. 21312–21322. – DOI: 10.1109/ACCESS.2017.2728081.

5. *Yuan D., Kanhere S.S., Hollick M.* Instrumenting wireless sensor networks a survey on the metrics that matter // Pervasive and Mobile Computing. – 2017. – Vol. 37. – P. 45–62. – DOI: 10.1016/j.pmcj.2016.10.001.

6. *Lee I., Lee K.* The internet of things (IoT): applications, investments, and challenges for enterprises // Business Horizons. – 2015. – Vol. 58 (4). – P. 431–440. – DOI: 10.1016/j.bushor.2015.03.008.

7. *Jeba N., Kamala V.* A survey on routing protocols for internet of things // International Journal of Advanced Research in Science, Engineering and Technology. – 2016. – Vol. 3 (5). – P. 1993–1996.

8. Review of the present technologies concurrently contributing to the implementation of the internet of things (IoT) paradigm: RFID, green electronics, WPT and energy harvesting / L. Roselli, C. Mariotti, P. Mezzanotte, F. Alimenti, G. Orecchini, M. Virili, N.B. Carvalho // 2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet). – San Diego, CA, 2015. – P. 1–3. – DOI: 10.1109/WISNET.2015.7127402.

9. *Maghfur H.* A state of the art review on the internet of things (IoT) // Buletin Inovasi ICT and Ilmu Komputer. – 2015. – Vol. 2 (1).

10. *Bouaziz M., Rachedi A.* A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology // Computer Communications. – 2016. – Vol. 74. – P. 3–15. – DOI: 10.1016/j.comcom.2014.10.004.

11. *Truong C., Römer K.* Efficient geocasting to multiple regions in large-scale wireless sensor networks // 37th Annual IEEE Conference on Local Computer Networks. – Clearwater Beach, FL, 2012. – P. 453–461. – DOI: 10.1109/LCN.2012.6423661.

12. *Fei C., Kundur D., Kwong R.H.* Analysis and design of secure watermark-based authentication systems // IEEE Transactions on Information Forensics and Security. – 2006. – Vol. 1 (1). – P. 43–55. – DOI: 10.1109/TIFS.2005.863505.

13. Digital watermarking and steganography / I. Cox, M. Miller, J. Bloom, J. Fridrich. – Morgan Kaufmann, 2007.

14. Watermarking security: a survey / L. Pérez-Freire, P. Comesaña, J.R. Troncoso-Pastoriza, F. Pérez-González // Transactions on Data Hiding and Multimedia Security I. – Berlin; Heidelberg: Springer, 2006. – P. 41–72. – DOI: 10.1007/11926214_2.

15. *Li W., Song H., Zeng F.* Policy-based secure and trustworthy sensing for internet of things in smart cities // IEEE Internet of Tings Journal. – 2018. – Vol. 5 (2). – P. 716–723. – DOI: 10.1109/JIOT.2017.2720635.

16. *Li W., Song H.* ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks // IEEE Transactions on Intelligent Transportation Systems. – 2016. – Vol. 17 (4). – P. 960–969. – DOI: 10.1109/TITS.2015.2494017.

17. *Anbuchelian S., Lokesh S., Baskaran M.* Improving security in Wireless Sensor Network using trust and metaheuristic algorithms // Proceedings of the 3rd International Conference on Computer and Information Sciences, ICCOINS 2016. – Kuala Lumpur, Malaysia, 2016. – P. 233–241. – DOI: 10.1109/ICCOINS.2016.7783220.

18. *Feng J., Potkonjak M.* Real-time watermarking techniques for sensor networks // Security and Watermarking of Multimedia Contents V. – SPIE, 2003. – P. 391–402. – DOI: 10.1117/12.479736.

19. *Guo H., Li Y., Jajodia S.* Chaining watermarks for detecting malicious modifications to streaming data // Information Sciences. – 2007. – Vol. 177 (1). – P. 281–298.

20. *Kamel I., Juma H.* Simplified watermarking scheme for sensor networks // International Journal of Internet Protocol Technology. – 2010. – Vol. 5 (1). – P. 101–111.

Шоназаров Парвиз Махмадназарович, аспирант кафедры инфокоммуникационных технологий Южно-Уральского государственного университета, г. Челябинск. E-mail: shonazarov1991@gmail.com

Холов Фозил Толибович, аспирант кафедры защиты информации Томского государственного университета систем управления и радиоэлектроники. E-mail: Fozil_1990-90@mail.ru

Саидов Бехруз Бдридинович, аспирант кафедры инфокоммуникационных технологий Южно-Уральского государственного университета, г. Челябинск. E-mail: mathem.1994@mail.ru

Shonazarov Parviz M., postgraduate student at the Department of Infocommunication Technologies, South Ural State University, Chelyabinsk. E-mail: shonazarov1991@gmail.com

Kholov Fozil T., postgraduate student at the Department of Information Security, Tomsk State University of Control Systems and Radioelectronics. E-mail: Fozil_1990-90@mail.ru

Saidov Bekhruz B., postgraduate student at the Department of Infocommunication Technologies, South Ural State University, Chelyabinsk. E-mail: mathem.1994@mail.ru

DOI: 10.17212/2782-2001-2022-1-109-120

The method of digital watermarking for improving objects based on clusters and perception values[*]

P.M. SHONAZAROV [1,a], *F.T. KHOLOV* [2,b], *B.B. SAIDOV* [1,c]

[1] *South Ural State University, 86 Lenin Prospekt, Chelyabinsk, 454080, Russian Federation*
[2] *Tomsk State University of Control Systems and Radioelectronics, 40 Lenin Prospekt, Tomsk, 634050, Russian Federation*

[a] *shonazarov1991@gmail.com* [b] *fozil_1990-90@mail.ru* [c] *mathem.1994@mail.ru*

Abstract

One of the most important IoT concerns is resource constraints such as power supply, processing power, memory capacity, wireless range, and wireless bandwidth. Low bandwidth wireless routing requires multiple routing steps to reach a destination. The Internet of things (Internet of things, IoT) is a technology that consists of a set of objects that are connected via the Internet

[*] *Received 03 September 2021.*

and collect information generated by sensors. IoT devices are devices that are networked and accessible to anyone and everything anytime and anywhere. Examples of such devices include temperature sensors, motion sensors, heart rate sensors, energy consumption sensors, etc. For example, a temperature sensor can be built into a thermostat, an indicator of the amount of electricity consumed in homes, and a traffic sensor at a traffic light. This article proposes a scheme based on fragile watermarking and improved clustering to resolve the conflict between security and limited perceptual resources. To improve security, we are developing a stochastic positioning strategy based on a clustering algorithm to compute the position embedded in the temporal dynamics of the data measurement. Thus, security vulnerabilities created by a stationary embedded situation can not only be effectively addressed but also result in zero data disturbance. Our research results show that the proposed algorithm can effectively integrate low-cost data, as well as reduce power consumption and increase network life.

Keywords: Internet of Things, IoT, digital marking, digital watermarking, security, data transmission, multiple routing, clustering algorithm, temporal dynamics

REFERENCES

1. Tolibovich K.F., Aleksandrovich S.A., Mahmadnazarovich S.P. A new algorithm watermark for improving objects based on clusters and perceptions. *2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, Yekaterinburg, Russia, 2020, pp. 520–523. DOI: 10.1109/USBEREIT48449.2020.9117762.

2. Dorri A., Kanhere S.S., Jurdak R., Gauravaram P. Blockchain for IoT security and privacy: the case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, USA, 2017, pp. 618–623. DOI: 10.1109/PERCOMW.2017.7917634.

3. Dorri A., Kanhere S.S., Jurdak R. Towards an optimized blockchain for IoT. *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Pittsburgh, PA, USA, 2017, pp. 173–178.

4. Li Y., Sun Z., Han L., Mei N. Fuzzy compre-hensive evaluation method for energy management systems based on an internet of things. *IEEE Access*, 2017, vol. 5, pp. 21312–21322. DOI: 10.1109/ACCESS.2017.2728081.

5. Yuan D., Kanhere S.S., Hollick M. Instrumenting wireless sensor networks a survey on the metrics that matter. *Pervasive and Mobile Computing*, 2017, vol. 37, pp. 45–62. DOI: 10.1016/j.pmcj.2016.10.001.

6. Lee I., Lee K. The internet of things (IoT): applications, investments, and challenges for enterprises. *Business Horizons*, 2015, vol. 58 (4), pp. 431–440. DOI: 10.1016/j.bushor.2015.03.008.

7. Jeba N., Kamala V. A survey on routing protocols for internet of things. *International Journal of Advanced Research in Science, Engineering and Technology*, 2016, vol. 3 (5), pp. 1993–1996.

8. Roselli L., Mariotti C., Mezzanotte P., Alimenti F., Orecchini G., Virili M., Carvalho N.B. Review of the present technologies concurrently contributing to the implementation of the internet of things (IoT) paradigm: RFID, green electronics, WPT and energy harvesting. *2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, San Diego, CA, 2015, pp. 1–3. DOI: 10.1109/WISNET.2015.7127402.

9. Maghfur H. A state of the art review on the internet of things (IoT). *Buletin Inovasi ICT and Ilmu Komputer*, 2015, vol. 2 (1).

10. Bouaziz M., Rachedi A. A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology. *Computer Communications*, 2016, vol. 74, pp. 3–15. DOI: 10.1016/j.comcom.2014.10.004.

11. Truong C., Römer K. Efficient geocasting to multiple regions in large-scale wireless sensor networks. *37th Annual IEEE Conference on Local Computer Networks*, Clearwater Beach, FL, 2012, pp. 453–461. DOI: 10.1109/LCN.2012.6423661.

12. Fei C., Kundur D., Kwong R.H. Analysis and design of secure watermark-based authentication systems. *IEEE Transactions on Information Forensics and Security*, 2006, vol. 1 (1), pp. 43–55. DOI: 10.1109/TIFS.2005.863505.

13. Cox I., Miller M., Bloom J., Fridrich J. *Digital watermarking and steganography*. Morgan Kaufmann, 2007.

14. Pérez-Freire L., Comesaña P., Troncoso-Pastoriza J.R., Pérez-González F. Watermarking security: a survey. *Transactions on Data Hiding and Multimedia Security I*. Berlin, Heidelberg, Springer, 2006, PP. 41–72. DOI: 10.1007/11926214_2.

15. Li W., Song H., Zeng F. Policy-based secure and trustworthy sensing for internet of things in smart cities. *IEEE Internet of Tings Journal*, 2018, vol. 5 (2), pp. 716–723. DOI: 10.1109/JIOT.2017.2720635.

16. Li W., Song H. ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 2016, vol. 17 (4), pp. 960–969. DOI: 10.1109/TITS.2015.2494017.

17. Anbuchelian S., Lokesh S., Baskaran M. Improving security in Wireless Sensor Network using trust and metaheuristic algorithms. *Proceedings of the 3rd International Confer-ence on Computer and Information Sciences, ICCOINS 2016*, Kuala Lumpur, Malaysia, pp. 233–241. DOI: 10.1109/ICCOINS.2016.7783220.

18. Feng J., Potkonjak M. Real-time watermarking techniques for sensor networks. *Security and Watermarking of Multimedia Contents V*. SPIE, 2003, pp. 391–402. DOI: 10.1117/12.479736.

19. Guo H., Li Y., Jajodia S. Chaining watermarks for detecting malicious modifications to streaming data. *Information Sciences*, 2007, vol. 177 (1), pp. 281–298.

20. Kamel I., Juma H. Simplified watermarking scheme for sensor networks. *International Journal of Internet Protocol Technology*, 2010, vol. 5 (1), pp. 101–111.

Для цитирования:

Шоназаров П.М., Холов Ф.Т., Саидов Б.Б. Метод цифровых водяных символов для совершенствования объектов на базе кластеров и значения восприятия // Системы анализа и обработки данных. – 2022. – № 1 (85). – С. 109–120. – DOI: 10.17212/2782-2001-2022-1-109-120.

For citation:

Shonazarov P.M., Kholov F.T., Saidov B.B. Metod tsifrovykh vodyanykh simvolov dlya sovershenstvovaniya ob"ektov na baze klasterov i znacheniya vospriyatiya [The method of digital watermarking for improving objects based on clusters and perception values]. *Sistemy analiza i obrabotki dannykh = Analysis and Data Processing Systems*, 2022, no. 1 (85), pp. 109–120. DOI: 10.17212/2782-2001-2022-1-109-120.