Оценивание вероятности дублирования сообщений в системе промышленного Интернета вещей

М.С. Балакшин, К.А. Польщиков

Белгородский государственный национальный исследовательский университет, Белгород

Аннотация: Статья посвящена разработке оригинальной математической модели процесса передачи информационных пакетов и подтверждений в системе промышленного Интернета вещей, применение которой позволяет оценить вероятность дублирования сообщений, отправляемых в центр управления производственным процессом. Результаты вычислительных экспериментов показали, что использование разработанной модели дает возможность обосновать выбор максимального числа повторных передач, при котором вероятность дублирования сообщений не превышает заданные допустимые значения при текущем уровне битовых ошибок.
Ключевые слова: промышленный Интернет вещей, телеметрические данные, управление производственным процессом, дублирование сообщений, повторные передачи, интенсивность битовых ошибок, сенсорные устройства, сервер, вероятностный граф.

В настоящее время технологии Интернета вещей (Internet of Things, IoT) активно применяются в самых различных сферах [1 – 3], в частности, на производственных предприятиях для удаленного мониторинга и превентивного управления технологическими процессами [4,5]. IoT-системы, функционирующие в целях контроля производственных процессов, строятся в рамках концепции промышленного Интернета вещей (Industrial Internet of Things, IIoT) [6, 7]. К числу распространенных стандартов, регламентирующих работу таких системы, относится протокол прикладного уровня MQTT [8] и его модификация MQTT-SN, адаптированная для сенсорных сетей [9, 10]. Указанные протоколы для доставки телеметрических данных регламентируют использование сервера как промежуточного устройства, к которому подключаются устройства-клиенты. В качестве таких клиентов в IIoT-системе применяются сенсорные устройства, которые осуществляют измерение контролируемых параметров и отправку на сервер соответствующих телеметрических сообщений, а также

IoT-устройства центра управления производственным процессом, на которые эти сообщения передаются из сервера.

Для повышения вероятности доставки сообщений IIoT-системе используются повторные передачи искаженных или потерянных данных. Однако при этом возможно дублирование передаваемых сообщений, которое снижает качество мониторинга контролируемых параметров и может привести к некорректному управлению производственным процессом. Анализ научно-технических публикаций показал, что вопросам оценивания вероятности дублирования сообщений в IIoT-системах уделяется недостаточное внимание, что определяет актуальность исследований, результаты которых представлены в данной работе.

В целях оценивания вероятности дублирования сообщений в системе промышленного Интернета вещей предлагается воспользоваться математическим аппаратом вероятностных графов, который позволяет учесть все возможные состояния моделируемого процесса и вероятности переходов из одних состояний в другие [11, 12]. На рисунке 1 представлен вероятностный граф процесса передачи информационных пакетов и подтверждений из сенсорного устройства на сервер в соответствии с протоколом MQTT-SN.

Начальное состояние моделируемого процесса обозначено вершиной «B». В этом состоянии установлены сетевые подключения устройств-клиентов к серверу, и начинается передача пакета PUBLISH из сенсорного устройства на сервер. Из состояния «B» моделируемый процесс может перейти в состояние корректного приема пакета PUBLISH сервером. Это состояние обозначено вершиной «S1». Вероятность перехода в состояние «S1» можно оценить по формуле:

$$P1 = 1 - \left(L1 \cdot BER \right), \qquad (1)$$

где $L1$ – битовая длина пакета PUBLISH; BER – интенсивность битовых ошибок в беспроводных каналах, соединяющих сенсорные устройства с сервером.

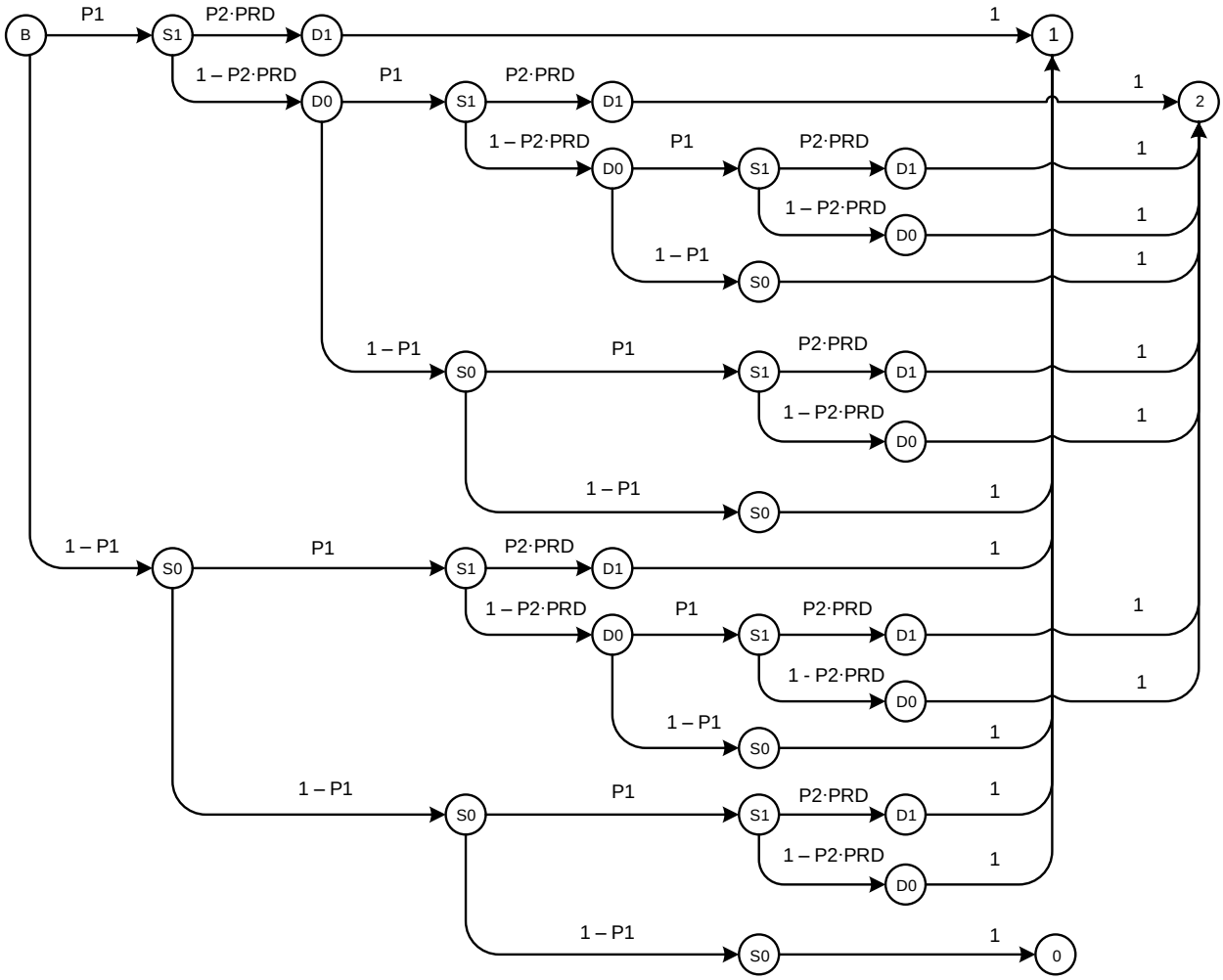

Рис. 1. Вероятностный граф процесса передачи информационных пакетов и подтверждений из сенсорного устройства на сервер в соответствии с протоколом MQTT-SN

После корректного приема пакета PUBLISH сервер отправляет на сенсорное устройство пакет-подтверждение PUBACK. Если это подтверждение будет корректно и своевременно принято сенсорным

устройством, то из вершины «S1» осуществится переход в вершину «D1». Вероятность корректного приема пакета-подтверждения PUBACK сенсорным устройством равна:

$$P2 = 1 - (L2 \cdot BER), \quad (2)$$

где $L2$ – битовая длина подтверждающего пакета PUBACK.

Допустим, вероятность того, что подтверждающий пакет PUBACK будет принят сенсорным устройством своевременно, т.е. до момента срабатывания таймера повторной передачи, равна PRD. Тогда вероятность перехода в вершину «D1» равна произведению $P2 \cdot PRD$. Если же подтверждающий пакет PUBACK не будет корректно принят сенсорным устройством или будет принят после срабатывания таймера повторной передачи, то моделируемый процесс перейдет в вершину «D0». Вероятность такого перехода равна $(1 - P2 \cdot PRD)$.

Возможно также, что пакет PUBLISH не будет корректно принят сервером, тогда из начальной вершины «B» моделируемый процесс перейдет в вершину «S0». Вероятность такого перехода равна $(1 - P1)$. Из вершины «S0» моделируемый процесс может перейти в вершину «S1», если число повторных передач, выполненных сенсорным устройством, меньше установленного значения $Nretry$, и отправленный дубликат пакета PUBLISH будет корректно принят сервером.

В конечном итоге моделируемый процесс завершается переходом в одно из трёх состояний: «1» – сообщение доставлено на сервер без дублирования; «2» – сообщение доставлено на сервер с дублированием; «0» – сообщение на сервер не доставлено. Ветви графа, которые содержат лишь одну вершину «S1», оканчиваются вершиной «1». Те ветви графа, которые содержат более одной вершины «S1», оканчиваются вершиной «2». Наконец,

в графе имеется ветвь, которая не содержит ни одной вершины «S1». Эта ветвь оканчивается вершиной «0».

Вероятность дублирования сообщений в процессе их доставки из сенсорного устройства на сервер – это вероятность перехода из вершины «B» к вершине «2». Эту величину можно оценить по формуле:

$$PDUBL1 = 1 - PONCE - PNOT, \quad (3)$$

где $PONCE$ – вероятность доставки сообщения на сервер без дублирования; $PNOT$ – вероятность того, что после $Nretry$ повторных передач сообщение не будет доставлено на сервер.

Значение величины $PNOT$ можно вычислить с помощью выражения:

$$PNOT = (1 - P1)^{Nretry+1}. \quad (4)$$

Чтобы оценить вероятность доставки сообщения на сервер без дублирования, следует воспользоваться выражением:

$$\begin{aligned} PONCE &= P1 \cdot P2 \cdot PRD + P1 \cdot (1 - P2 \cdot PRD) \cdot (1 - P1) \cdot (1 - P1) + \\ &+ (1 - P1) \cdot P1 \cdot P2 \cdot PRD + (1 - P1) \cdot P1 \cdot (1 - P2 \cdot PRD) \cdot (1 - P1) + \\ &+ (1 - P1) \cdot (1 - P1) \cdot P1 \cdot P2 \cdot PRD + (1 - P1) \cdot (1 - P1) \cdot P1 \cdot (1 - P2 \cdot PRD) = \\ &= P1 \cdot \left[(1 - P1)^{Nretry} \cdot (1 + Nretry \cdot (1 - P2 \cdot PRD)) + P2 \cdot PRD \cdot \sum_{i=0}^{Nretry-1} (1 - P1)^i \right]. \end{aligned} \quad (5)$$

Выражения (1) – (5) могут быть использованы также для оценивания вероятности дублирования сообщений в процессе их доставки из сервера на IoT-устройство центра управления. Тогда формула для оценивания результирующего значения вероятности дублирования сообщений в IIoT-системе в целом (т.е. в процессе их доставки из сенсорного устройства на IoT-устройство центра управления) имеет вид:

$$PDUBL = 2PDUBL1 - PDUBL1^2. \quad (6)$$

Разработанная модель была использована при проведении вычислительных экспериментов для исследования зависимости вероятности

дублирования сообщений от значений параметров передачи данных в IIoT-системе. Исходные данные для вычислительных экспериментов: $L1=256$ бит; $L2=128$ бит; $PRD=1$.

В результате вычислений по формулам (1) – (6) получены кривые зависимости вероятности дублирования сообщений от интенсивности битовых ошибок в беспроводных каналах IIoT-системы при различных значениях $Nretry$ (рисунок 2).

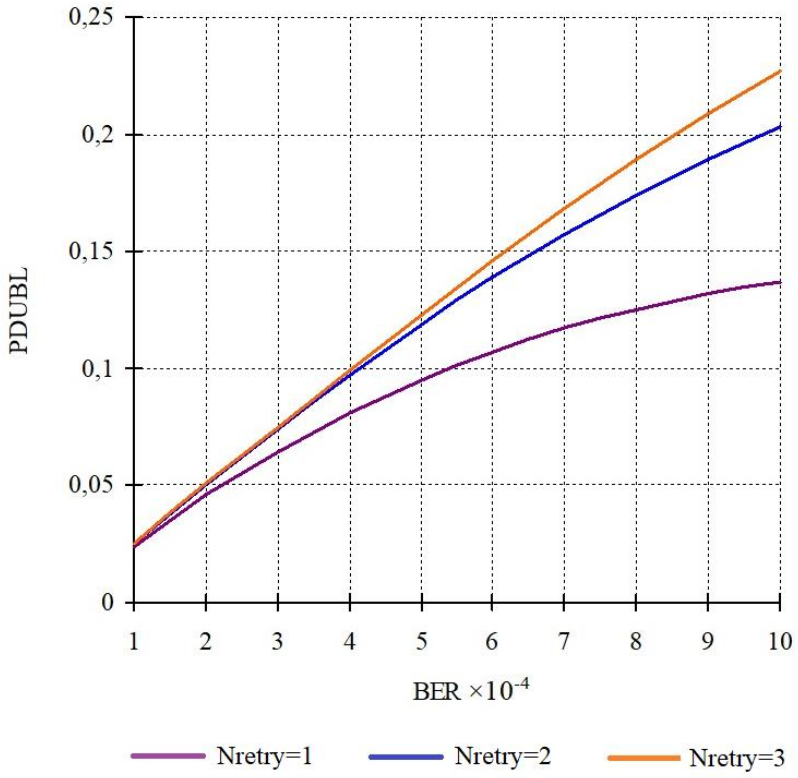

Рис. 2. Кривые $PDUBL(BER)$ при $Nretry=1, 2, 3$

Анализ рисунка 2 подтверждает предположение, что с ростом интенсивности битовых ошибок и разрешенного числа повторных передач в IIoT-системе увеличивается вероятность дублирования сообщений.

Таким образом, разработана модель процесса передачи информационных пакетов и подтверждений из сенсорного устройства на IoT-

устройство центра управления производством. Передача данных в рамках моделируемого процесса осуществляется в соответствии с протоколом MQTT-SN. Модель позволяет оценить вероятность дублирования сообщений в IIoT-системе и адекватно отражает зависимость этой величины от уровня битовых ошибок в беспроводных каналах и разрешенного числа повторных передач. Использование разработанной модели дает возможность выбрать такое число $Nretry$, при котором величина $PDUBL$ не превышает заданные допустимые значения при текущем уровне битовых ошибок.

Литература

1. Грачев В.М., Грачева Н.В. Технология интернет вещей и перспективы ее внедрения в растениеводстве // Инженерный вестник Дона. 2024. № 2. URL: ivdon.ru/uploads/article/pdf/IVD_79__1y24_grachev_gracheva.pdf_6a3da63ba4.pdf.

2. Васфиев Р.И., Орешникова Ю.С., Сафаров И.М. Система управления "Умного дома" в рамках концепции "Интернета вещей" // Инженерный вестник Дона. 2021. № 6. URL: ivdon.ru/uploads/article/pdf/IVD_67__5_Oreshnikova.pdf_55098e7067.pdf.

3. Yaser M.J., Polshchykov K.A., Polshchikov I.K. Algorithm for ensuring the minimum power consumption of the end node in the LoRaWAN network. Periodicals of Engineering and Natural Sciences. 2023. Vol. 11. No. 4. pp. 168-174.

4. Sari A., Lekidis A., Butun I. Industrial Networks and IIoT: Now and Future Trends. Industrial IoT. 2020. URL: doi.org/10.1007/978-3-030-42500-5_1.

5. Liu Y., Kashef M., Lee K. B., Benmohamed L., Candell R. Wireless Network Design for Emerging IIoT Applications: Reference Framework and Use Cases. Proceedings of the IEEE. 2020. Vol. 107. No. 6. pp. 1166-1192.

6. Chalapathi G.S.S., Chamola V., Vaish A., Buyya R. Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing: A Review and Future Directions. Advances in Information Security. 2021. Vol 83. URL: doi.org/10.1007/978-3-030-57328-7_12.

7. Torres P.M.B., Spencer G., Lopes P., Santos F. Industrial IoT Platforms Enabling Industry 4.0 Digitization Towards Industry 5.0. Lecture Notes in Mechanical Engineering. 2024. URL: doi.org/10.1007/978-3-031-61575-7_1.

8. Yeh C.-S., Chen S.-L., Li I.-C. Implementation of MQTT protocol based network architecture for smart factory. Journal of Engineering Manufacture. 2021. Vol. 235(13). pp. 2132-2142.

9. Palmese F., Redondi A.E.C., Cesana M. Adaptive Quality of Service Control for MQTT-SN. Sensors. 2022. Vol. 22(22). pp. 8852.

10. da Rocha H., Monteiro T.L., Pellenz M.E., Penna M.C., Alves Junior J. An MQTT-SN-Based QoS Dynamic Adaptation Method for Wireless Sensor Networks. Advances in Intelligent Systems and Computing. 2020. Vol. 926. URL: doi.org/10.1007/978-3-030-15032-7_58.

11. Jameel J.Q., Mahdi T.N., Polshchykov K.A., Lazarev S.A., Likhosherstov R.V., Kiselev V.E. Development of a mathematical model of video monitoring based on a self-organizing network of unmanned aerial vehicles. Periodicals of Engineering and Natural Sciences. 2022. Vol. 10(6). pp. 84-95.

12. Polshchykov K.O., Lazarev S.A., Kiseleva E.D. Mathematical Model of Multimedia Information Exchange in Real Time Within a Mobile Ad Hoc Network. International Journal of Computer Science and Network Security. 2018. Vol 18. No. 6. pp. 20-24.

References

1. Grachev V.M., Gracheva N.V. Inzhenernyj vestnik Dona, 2024. № 2. URL: ivdon.ru/uploads/article/pdf/IVD_79__1y24_grachev_gracheva.pdf_6a3da63ba4.pdf.

2. Vasfiev R.I, Oreshnikova Yu.S., Safarov I.M. Inzhenernyj vestnik Dona, 2021, №6. URL: ivdon.ru/uploads/article/pdf/IVD_67__5_Oreshnikova.pdf_55098e7067.pdf.

3. Yaser M.J., Polshchykov K.A., Polshchikov I.K. Periodicals of Engineering and Natural Sciences. 2023. Vol. 11. No. 4. pp. 168-174.

4. Sari A., Lekidis A., Butun I. Industrial IoT. 2020. URL: doi.org/10.1007/978-3-030-42500-5_1.

5. Liu Y., Kashef M., Lee K. B., Benmohamed L., Candell R. Proceedings of the IEEE. 2020. Vol. 107, No. 6. pp. 1166-1192.

6. Chalapathi G.S.S., Chamola V., Vaish A., Buyya R. Advances in Information Security. 2021. Vol 83. URL: doi.org/10.1007/978-3-030-57328-7_12.

7. Torres P.M.B., Spencer G., Lopes P., Santos F. Lecture Notes in Mechanical Engineering. 2024. URL: doi.org/10.1007/978-3-031-61575-7_1.

8. Yeh C.-S., Chen S.-L., Li I.-C. Journal of Engineering Manufacture. 2021. Vol. 235(13). pp. 2132-2142.

9. Palmese F., Redondi A.E.C., Cesana M. Sensors. 2022. Vol. 22(22). pp. 8852.

10. da Rocha H., Monteiro T.L., Pellenz M.E., Penna M.C., Alves Junior J. Advances in Intelligent Systems and Computing. 2020. Vol. 926. URL: doi.org/10.1007/978-3-030-15032-7_58.

11. Jameel J.Q., Mahdi T.N., Polshchykov K.A., Lazarev S.A., Likhosherstov R.V., Kiselev V.E. Periodicals of Engineering and Natural Sciences. 2022. Vol. 10(6). pp. 84-95.

12. Polshchykov K.O., Lazarev S.A., Kiseleva E.D. International Journal of Computer Science and Network Security. 2018. Vol 18. No. 6. pp. 20-24.

Дата поступления: 25.06.2024

Дата публикации: 3.08.2024