# Security Risk Assessment of the RabbitMQ Broker using Concurrent Stochastic Games

### Reply to the Editor and Reviewers' Comments
### Internet of Things Journal

Manuscript Id.: IOT-D-24-00184R1

We express our gratitude to the reviewers and the Editor-in-Chief of Internet of Things Journalfor their valuable comments and constructive suggestions during the first round of review. Their input has significantly contributed to the enhancement of our manuscript. In this revised version, we have addressed the various comments and provided detailed responses to the inquiries the Editor and Reviewers raised. Following the structure of the received email for revision, we have provided comprehensive answers to each question and comment. The modifications made to the updated manuscript are highlighted in blue.

## Comments from Reviewer #1

**Comment 1**: This is an interesting topic. A few questions need to be addressed through:

***Answer***: We sincerely appreciate the positive feedback and valuable comments provided, which have greatly contributed to the improvement of our contribution. With regard to the updated version, we firmly believe that we have effectively addressed the various concerns, as evidenced by the implemented changes.

**Comment 2**: RabbitMQ is NOT a protocol, it is a broker that supports multiple protocols including MQTT and AMQP. What is the actual protocol that is used?

***Answer***: You are correct that RabbitMQ is a message broker that supports multiple protocols, such as MQTT and AMQP. In our study, we specifically utilized the AMQP protocol implemented by RabbitMQ for communication purposes. We have updated the manuscript to reflect this information accurately. For instance, we removed the term protocol from the title. The new title is: ”Rigorous Security Analysis of RabbitMQ Broker with Concurrent Stochastic Games”

**Comment 3**: What does the protocol stack look like? (IETF layers) ?

***Answer**:* AMQP is defined by the Oasis Open Specifications Consortium standardized in ISO/IEC 19464:2014. However, AMQP 1.0 does utilize some functionalities and protocols aligned with the general IETF layering model. (1) Application Layer: This layer interacts with applications using client libraries and defines message format and semantics. It directly corresponds to the application layer in the IETF model. (2) Messaging Layer: This layer handles message routing, exchanges, queues, and bindings. It's similar to the application layer in the IETF model but with a stronger focus on message routing and distribution. (3) Framing Layer: This layer takes messages from the messaging layer and packages them into frames with specific headers and content data. It aligns with the transport layer in the IETF model, focusing on data structuring and encapsulation. (4) Transport Layer: This layer provides reliable and secure communication between peers (RabbitMQ servers). It typically uses TLS/SSL for encryption and TCP for reliable delivery, corresponding to the transport layer in the IETF model. (5) Wire Level: This layer defines the byte format on the network for each frame. It corresponds to the network layer in the IETF model, addressing low-level network communication details. These details are portrayed in the *Background section.*

**Comment 4**: What is the effect of network layer and latency on the mechanism?

***Answer**:* The impact of the network layer and latency deserves careful consideration. The network layer acts as the foundation for data transmission, impacting both performance and reliability. Notably, latency, the time it takes data to travel from one point to another, directly affects the mechanism's responsiveness and real-time capabilities.

In the discussion section, we have included two paragraphs that provide additional information regarding network and latency characteristics. These paragraphs delve into the specific details surrounding these aspects

**Comment 5**: Broker-based protocols like those supported by RabbitMQ are more suitable for core side communications. When enabling communication on the access side with smart devices, other protocols like CoAP are more convenient. This needs to be justified.

***Answer**:* We recognize ambiguities regarding the use of CoAP and RabbitMQ. To clarify their application, we've added clarifications to distinguish between these two types of protocols: device-side and core-side.

## Comments from Reviewer #2

**Comment 6**: The research summary effectively addresses the pressing issue of security threats in Internet of Things (IoT) architectures, emphasizing the importance of designing communication protocols with robust security measures.
The proposed approach, utilizing the Concurrent Stochastic Game (CSG) model to specify the behavior of the RabbitMQ protocol in IoT systems while considering potential data corruption attacks, offers a novel and promising solution to address security vulnerabilities. The implementation of the CSG model in the PRISM-games language for automated analysis, along with the use of reward Probabilistic Alternating Temporal Logic (rPATL) to model security requirements as game goals, demonstrates a systematic and rigorous approach to analyzing protocol behavior and security properties.
Empirical validation of the proposed approach through an industrial case study, focusing on data corruption attacks impacting sensed data in water dam infrastructure, adds practical relevance to the research and highlights potential real-world implications of security vulnerabilities in IoT systems.
The assessment of the RabbitMQ protocol's feasibility in relation to existing implementations of edge gateway software provides valuable insights into the protocol's performance and suitability for secure communication in IoT environments.

***Answer***: We are grateful for your positive assessment of our contribution, and we appreciate your comments that allow us to improve it. Regarding the revised version, we have a conviction that we have addressed the diverse concerns, which are substantiated by the implemented modifications.

**Comment 7**: I believe that incorporating relevant and recent academic sources could further strengthen your paper's validity and provide readers with more context and background on the topic. as follows. Genghis Khan shark optimizer, Geyser Inspired Algorithm;
Prairie dog optimization algorithm,
Dwarf mongoose optimization algorithm,
Gazelle Optimization Algorithm,
DETDO: An adaptive hybrid dandelion optimizer for engineering optimization,
A Global Best-guided Firefly Algorithm for Engineering Problems,
Lungs performance-based optimization.

***Answer***: We have made the necessary updates by incorporating the cited references obtained from the Academic library into the *related work* section, specifically focusing on the optimization techniques discussed in the research to calculate attack frequency with different accuracy:
1- Gang Hu, Yuxuan Guo, Guo Wei, Laith Abualigah, Genghis Khan shark optimizer: A novel nature-inspired algorithm for engineering optimization, Advanced Engineering Informatics, Volume 58, 2023, 102210, ISSN 1474-0346, https://doi.org/10.1016/j.aei.2023.102210.

2- Ezugwu, A.E., Agushaka, J.O., Abualigah, L. et al. Prairie Dog Optimization Algorithm. Neural Comput & Applic 34, 20017–20065 (2022). https://doi.org/10.1007/s00521-022-07530-9

3- Jeffrey O. Agushaka, Absalom E. Ezugwu, Laith Abualigah, Dwarf Mongoose Optimization Algorithm, Computer Methods in Applied Mechanics and Engineering, Volume 391, 2022, 114570, ISSN 0045-7825, https://doi.org/10.1016/j.cma.2022.114570.

4- Agushaka, J.O., Ezugwu, A.E. & Abualigah, L. Gazelle optimization algorithm: a novel nature-inspired metaheuristic optimizer. Neural Comput & Applic 35, 4099–4131 (2023). https://doi.org/10.1007/s00521-022-07854-6

5- Gang Hu, Yixuan Zheng, Laith Abualigah, Abdelazim G. Hussien, DETDO: An adaptive hybrid dandelion optimizer for engineering optimization, Advanced Engineering Informatics, Volume 57, 2023, 102004, ISSN 1474-0346, https://doi.org/10.1016/j.aei.2023.102004.

6- Zare, M., Ghasemi, M., Zahedi, A. et al. A Global Best-guided Firefly Algorithm for Engineering Problems. J Bionic Eng 20, 2359–2388 (2023). https://doi.org/10.1007/s42235-023-00386-2

7- Mojtaba Ghasemi, Mohsen Zare, Amir Zahedi, Pavel Trojovský, Laith Abualigah, Eva Trojovská, Optimization based on performance of lungs in body: Lungs performance-based optimization (LPO), Computer Methods in Applied Mechanics and Engineering, Volume 419, 2024, 116582, ISSN 0045-7825, https://doi.org/10.1016/j.cma.2023.116582.

**Comment 8**: Overall, the research makes a significant contribution to the field of IoT security by proposing a systematic approach to analyzing and addressing security threats in communication protocols.

However, providing more detailed information about the experimental setup, such as the specific methodologies used for the case study and the metrics evaluated, would enhance the comprehensiveness of the validation process.

***Answer****:* Thank you for your review and for acknowledging the significant contribution of our research in IoT security. We appreciate your suggestion to improve the comprehensiveness of the validation process by providing more detailed information about the experimental setup. In response to your feedback, we enhanced the manuscript by including a section *6.1. Experimental setup* used for the case study and elaborating on the metrics evaluated.

**Comment 9**: Additionally, discussing potential limitations and future research directions would further enrich the paper.

***Answer****:* We agree that addressing potential limitations and future research directions would significantly enrich the overall contribution of the research. In response to your feedback, we discussed our approach's potential limitations in the paper's conclusion and suggested promising avenues for future research.