**RESPONSE TO REVIEWERS’ COMMENTS RECEIVED FOR OUR SUBMISSION “***A Novel Blockchain Structure for Wireless Sensor Networks Based on IOTA Tangle*” (**Manuscript ID:** electronics-1758170)

**ROUND 1**

The authors thank the anonymous reviewers for the in-depth scrutiny, and valuable feedback and suggestions, which have improved the quality of the paper. In the following, we provide responses to the reviewers’ comments. The sentences highlighted in blue font are the new additions in the revised manuscript. These changes have been incorporated into our revised manuscript.

**REVIEWER 1**

**Reviewer 1, Comment 1:***-The paper although interesting, is related to a topic that has already been thoroughly studied and investigated. The standardization of this class of protocols is already very advanced and at least some indications should be provided.*

**Authors’ Response:**

This paper is related to the current hot topics of blockchain and IOTA, but mainly focuses on the network topology solution for WSNs. The proposed topology is inspired by IOTA and is designed according to the characteristics of WSNs. To the best of our knowledge, this is the first paper that proposes a new topology called the Fishing Net Topology (FNT) based on IOTA Tangle to Wireless Sensor Networks.

**Reviewer 1, Comment 2:**  
*-There is no related work section, which is just summarized in the introduction. This could be ok for a short conference paper, but definitely not for a full-length journal version with no page limitation. The authors should provide a full section explaining the novelty of their approach.*

**Authors’ response:**

Due to the lack of literature on related work, the manuscript provides only the relevant background. We found no existing solutions similar to our study, so we added an introduction to the literature on IOTA performance analysis, which we hope will be helpful. This study only draws on two validation and attachment ideas of nodes from the IOTA Tangle; other parts are not relevant and cannot be directly compared with IOTA.

Added Section 2.5, Related Work, line 126~146.

Since the lack of literature on the application of the IOTA Tangle to WSNs, studies on the simulation of the IOTA Tangle are presented here, which reflect some of the shortcomings of the Tangle and the barriers to its application in WSNs.

In [26], the researchers have analyzed actual transaction data published by the IOTA Foundation and compared it with theoretical data in the literature. They reconstructed 96 Tangles from the dataset. By analyzing their dimensions, in-degree distribution, cumulative weight, and transaction confirmation delay, they concluded that the actual transaction confirmation delay was very high. At the same time, they believed that the three influencing factors namely the transaction arrival rate, the Tip Selection Algorithm (TSA), and the intervention of the Coordinator (COO) caused the performance of the actual results to be far from the simulation results. In addition, the computation of cumulative weights was complex and inefficient that ultimately affecting the tip selection and the performance of the entire network.

In [28], researchers described the structure and characteristics of the Tangle. They use computer simulations to analyze the evolution of cumulative weights and tip counts over time, resulting in a formula for the average tip count. They conclude that the growth of cumulative weights follows an exponential growth during the adoption phase, followed by a linear phase with the slope of *λ*. The TSA did not affect this result when *α* was small and this significantly impacted the growth of cumulative weights for larger *α*. Due to the uncertainty of tip selection, the internal structure of the Tangle was also uncertain.

**Reviewer 1, Comment 3:**   
*-The fonts in figures 7 and 8 need to be improved.*

**Authors’ response:**

The font has been increased, and the size of other pictures has been appropriately increased.

**Reviewer 1, Comment 4:***-The novelty and major contribution of the research need properly described.*

**Authors’ response:**

Revised Section 2.6, summary, line 147~167 to describe novelty and contribution.

Summary

As one of the technological foundations of IoT, WSNs have a more straightforward structure than IoT. WSNs are used to collect and provide data, and IoT technology is used to analyze the data collected from the Internet and present the information for user access [32]. WSN devices are mainly various types of sensors, while IoT devices include sensors and more complex devices. There are many devices in IoT that can generate a large number of small transactions. Bitcoin can only process seven transactions per second, and Ethereum can process 14 transactions per second [6]. This performance cannot meet IoT requirements, so IOTA Tangle is proposed as a blockchain technology designed for IoT data transmission and security needs.

The differences between IoT and WSNs determine that IOTA Tangle is not the best solution for WSNs. WSN needs a new blockchain technology that is more suitable for it, so we propose a new blockchain technology based on the IOTA Tangle idea for WSNs, called Fishing Net Topology (FNT). In Tangle, two old transactions are approved by a new transaction. FNT draws on this dual authentication idea to design a new network topology for the packets generated by WSNs, making them more secure and faster to transmit and store the data. To address the computational power deficiency of WSN nodes and the difference with IoT devices, the proposed FNT simplifies the TSA in Tangle and removes the computation of cumulative weights that consume computational power, so that WSNs nodes do not need to perform complex computations and meet the energy-saving and lightweight requirements of WSNs.

**Reviewer 1, Comment 5:***-Another point that is very lightly treated but that should require more input is on the issues and cost of implementing these types of solutions.*

**Authors’ response:**

Rewritten Section 5, Conclusion and Recommendation, lines 349~413.

Added line 381~387.

In applying FNT, a reasonable rate should be calculated to save costs depending on the demand for WSNs. The cost of implementing FNT is mainly in the network service. FNT has no additional demand on the hardware of WSN nodes, so there is no additional cost. Higher network speed and bandwidth lead to more expenses, and the selection of the best rate in FNT is to refer users to choosing network services to reduce expenses. FNT aims to reduce the computation of WSN nodes while providing a secure and reliable data storage and transmission solution.

**Reviewer 1, Comment 6:***-I hope to read something about the practical application of the approach. A Section of applicability of the proposed solution is required in this manuscript.*

**Authors’ response:**

Rewritten Section 5, Conclusion and Recommendation, lines 349~413.

Added line 370~380.

The application scenario of FNT is shown in Figure 2. In WSNs, many sensor nodes are deployed in a specific environment for collecting and sensing data. Each sensor node should upload packets to the gateway at a preset time interval. The size of the FNT is also specified according to the user's demand for the size of the WSNs, so its rate is preset. In the gateway, the submitted packets are attached to the FNT. Each packet needs to be validated against the data of its two Tips, also previously submitted packets. Since it is not attached by other packets, it is temporarily called Tips. Packets that pass the two Approvers validation become general FNT nodes. As more and more packets are attached to the FNT and verified by more and more packets, the authenticity of the data in the whole network is guaranteed. Users can access the FNT and its data stored in the gateway and more operations through the Internet.

**REVIEWER 2**

The paper “A Novel Blockchain Structure for Wireless Sensor Networks Based on IOTA Tangle” presents an interesting and timely topic. However, unfortunately, the paper is not ready to be accepted in the Journal.

**Reviewer 2, Comment 1:***-The main weakness is the lack of a thorough comparison between the proposal and IOTA. Furthermore, considering the complexity of the p2p networks, the paper needs to provide strong results and formal simulations in different scenarios and with different assumptions. Likewise, these results should also provide a security analysis that explains how the proposal does not compromise security. I suggest the authors study the following works: https://doi.org/10.1109/IVS.2018.8500557 https://doi.org/10.1109/ACCESS.2020.3040875, and https://doi.org/10.1109/ACCESS.2020.3006078, to get a reference for evaluating their proposal.*

**Authors’ response:**

This paper draws on two validation ideas from IOTA, which are not directly related to IOTA and have different uses, so a quantitative comparison of the two is not directly relevant to the proposed technique in this paper. However, we have added a comparison of the two in terms of structure and algorithms.

IOTA is used for transaction processing in IoT, and its security mechanism is to use nodes to authenticate each other. While WSN has fewer functions than IoT, and the sensor nodes are not as powerful and computationally capable as IoT devices, the security mechanism of IOTA directly applied to WSN will impose an additional load on the sensor nodes, while FNT learns the verification ideas of IOTA, but removes the complex algorithms in it that do not need to be used in WSN, and designs a simpler network topology for WSN. FNT also requires new security mechanisms, which is the future direction of improvement.

Added a paragraph in section 2.4, line 118~121.

In Tangle, each transaction has its initial weight and cumulative weight. The cumulative weight is the sum of the weights of all the transactions that have directly or indirectly approved that transaction [26]. As more and more transactions are submitted and approved, the cumulative weight of a transaction increases.

A new structure comparison image is added in section 4.1, and a new figure comparison of cumulative weights is added. The three articles mentioned have been cited.

Added line 275~276, Figure 7.

Figures 7a and 7b show a comparison of the structure of FNT and Tangle, with FNT being more concise and straightforward.

A picture containing background pattern

Description automatically generated

Figure 7. Structure Comparison of FNT and Tangle.

Added line 286~22, Figure 8.

Chart, histogram, scatter chart

Description automatically generated

Figure 8. Comparison of the Cumulative Weights of the Nodes in FNT and Tangle.

Taking a network with a rate of 6, 100 nodes as an example, Figure 8a and 8b show the cumulative weights of each node under the two structures of FNT and Tangle, respectively. The trend of the cumulative weights in the figures also reflects the difference between the two structures. FNT has a more straightforward structure, so the trend of the cumulative weights is stable. While Tangle has a complicated structure, the cumulative weight trend is unstable. The above examples are only used to compare the differences between the two structures. FNT does not use cumulative weights.

**Reviewer 2, Comment 2:***-Another important point is the lack of state of the art. Currently, there are several proposals for blockchain (or distributed ledger) architectures. The authors should review a few of them. Otherwise, the paper should only focus on improving IOTA, which should be clearly stated in the title.*

**Authors’ response:**

Thank you for the observation. However, the main focus of this proposed work is different. The network topology proposed in this paper is inspired by the IOTA Tangle structure but has different functions and uses. Therefore, it is not an improvement of IOTA.

**Reviewer 2, Comment 3:***-Statement on line 39, “IOTA performs well**with complex architectures for IoT, but WSNs are different from IoT because WSNs have a relatively simple architecture.” needs a reference that demonstrates how and why IoTA performs well.*

**Authors’ response:**

Line 40~41, modified to "IOTA is designed for IoT, but WSNs are different from IoT because WSNs have a relatively simple architecture [5], [7]."

**Reviewer 2, Comment 4:***-Statement on line 74, “The Internet of Things (IoT) is a network infrastructure based on radio frequency identification (RFID) technology, and WSNs [10].” is too simplistic. IoT systems are complex systems with several components, not just RFID, and WSN. They include several other elements such as Edge gateways, LowPowerNetworks, etc*

**Authors’ response:**

Line81~84, modified to “Internet of Things (IoT) is a network infrastructure consisting of uniquely identifiable interoperable connected objects that communicate and exchange data with other devices and systems using technologies such as Radio Frequency Identification (RFID) technology and WSNs [14].”

**Reviewer 2, Comment 5:***-After reading Section 2.1 WSN and 2.2 IoT, their differences are not clear. Therefore, I will suggest a table comparing both at the end of the section.*

**Authors’ response:**

In Sections 2.1 and 2.2, we introduced WSN and IoT, respectively. WSN serves as a foundation for IoT, and IoT contains WSN, so it is difficult to compare the two. In general, technologies designed for IoT may be available for WSN, but those designed for WSN may not be available for IoT. we believe that Tangle, as a technology designed for IoT, may be somewhat incompatible and wasteful if applied directly to WSN. We have added a clarification of the difference between the two in section 2.6.

Added line 149~150, “WSNs are used to collect and provide data, and IoT is used to analyze the data collected from the Internet and present the information for user access [32].”

**Reviewer 2, Comment 6:***-Similarly, the authors should provide a table summarizing the differences between traditional block-based blockchains and IoTA types.*

**Authors’ response:**

Tables comparing blockchain and IOTA have been added in section 2.4. Table 1. Added line 120~123.

|  |  |  |
| --- | --- | --- |
| Table 1. Comparison of Some Features of Traditional Blockchain and IOTA Tangle [5] [27] [29] [30] [31]. | | |
| Features | Blockchain | IOTA Tangle |
| Decentralized | Yes | Yes |
| Distributed | Yes | Yes |
| Tamper-proof | Yes | Yes |
| Scalability | Low | High |
| Latency | High | Low |
| Security | Yes | Yes |
| Mining Process | Yes | No |
| Transaction Fee | Yes | No |
| Processing Time | Long | Short |
| Suitable Transaction Type | General Transactions | Small Transactions |
| Transaction Validation | Miner | Self-validation |
| Throughput | Low | High |
| Resource Requirements | High | Low |

Table 1 compares some of the characteristics of the traditional blockchain with the IOTA Tangle. IOTA Tangle is a technology based on blockchain, so it also includes some features of blockchain. Some blockchain features that are unsuitable for IoT have been improved to meet the needs of a large number of small transactions in IoT.

**Reviewer 2, Comment 7:***-Also, the authors should talk about smart contracts, as it has been highlighted in the current literature as one of the most useful properties of blockchain technology for applications on the IoT and thus WSN.*

**Authors’ response:**

Smart contracts will appear in future research plans for security models to improve FNT security. This paper is limited to the proposed network topology, and a more complete and comprehensive solution is still under research.

**REVIEWER 3**

**Reviewer 3, Comment 1:***-The abstracts introductory portion is too long as there is no quantitative results shown in the results portion of the abstract. Readers expect to see more detail of the methodology, results, and conclusion in the abstract. The abstract need to be greatly improved. The abstract does not show that the authors achieved much as there is no numerical justification to back the author’s claims or results of comparative analysis to show superior performance.*

**Authors’ response:**

Thank you for the comment. Although we would like to include as much content as possible in the abstract, we cannot show more details in the abstract due to the word limit. But we have described what has been suggested in the Introduction section. We have also reviewed recent articles published in MDPI Electronics and have aligned the abstract to be worded in a similar manner.

Line 6~8, “As the foundation of IoT, WSNs also need a similar solution.” Modified to “WSNs as one of the core technologies of IoT, and the two have a lot in common in terms of applications. Many solutions for IoT applications can be referenced by WSN applications.”

**Reviewer 3, Comment 2:***-In the introduction, the authors should explain why they did it (motivation) discussing the possible outcome. Readers are primarily interested in the motivation and outcome of your research. Therefore, a good introduction should contain:*

*a.       What is the problem to be solved?*

*b.      Are there any existing solutions?*

*c.       Which is the best?*

*d.      What is the main limitation of the best and existing approaches?*

*e.       What do you hope to change or propose to make it better?*

*f.       How is the paper structured?*

**Authors’ response:**

We have already included the following in the introduction of the manuscript (no modifications):

a. Designing a network topology for WSN data storage, based on blockchain and IOTA.

b. No existing solution.

c. It is difficult to conclude which one is the best, because there is no comparable object.

d. WSNs are limited by computing power and require lightweight solutions.

e. Design new network topologies to meet lightweight requirements.

f. The sixth paragraph describes the structure of the article.

**Reviewer 3, Comment 3:***-Please clearly highlight how your work advances the field from the present state of knowledge and you should provide a clear justification for your work which should be stated at the end of literature review/ related works. The impact or advancement of the work can also appear in the conclusion.*

**Authors’ response:**

Added Section 2.5, Related Work. Revised section 2.6, summary. Line 126~167. Since there is no existing research on the application of the IOTA-based network topology proposed in this paper in WSNs, an overview of the performance of IOTA is added here, reflecting some of the shortcomings of IOTA. This study only draws on two verification and additional ideas in the IOTA Tangle, other parts are irrelevant, so no existing cases are found for comparison.

Related Work

Since the lack of literature on the application of the IOTA Tangle to WSNs, studies on the simulation of the IOTA Tangle are presented here, which reflect some of the shortcomings of the Tangle and the barriers to its application in WSNs.

In [26], the researchers have analyzed actual transaction data published by the IOTA Foundation and compared it with theoretical data in the literature. They reconstructed 96 Tangles from the dataset. By analyzing their dimensions, in-degree distribution, cumulative weight, and transaction confirmation delay, they concluded that the actual transaction confirmation delay was very high. At the same time, they believed that the three influencing factors namely the transaction arrival rate, the Tip Selection Algorithm (TSA), and the intervention of the Coordinator (COO) caused the performance of the actual results to be far from the simulation results. In addition, the computation of cumulative weights was complex and inefficient that ultimately affecting the tip selection and the performance of the entire network.

In [28], researchers described the structure and characteristics of the Tangle. They use computer simulations to analyze the evolution of cumulative weights and tip counts over time, resulting in a formula for the average tip count. They conclude that the growth of cumulative weights follows an exponential growth during the adoption phase, followed by a linear phase with the slope of *λ*. The TSA did not affect this result when *α* was small and this significantly impacted the growth of cumulative weights for larger *α*. Due to the uncertainty of tip selection, the internal structure of the Tangle was also uncertain.

Summary

As one of the technological foundations of IoT, WSNs have a more straightforward structure than IoT. WSNs are used to collect and provide data, and IoT technology is used to analyze the data collected from the Internet and present the information for user access [32]. WSN devices are mainly various types of sensors, while IoT devices include sensors and more complex devices. There are many devices in IoT that can generate a large number of small transactions. Bitcoin can only process seven transactions per second, and Ethereum can process 14 transactions per second [6]. This performance cannot meet IoT requirements, so IOTA Tangle is proposed as a blockchain technology designed for IoT data transmission and security needs.

The differences between IoT and WSNs determine that IOTA Tangle is not the best solution for WSNs. WSN needs a new blockchain technology that is more suitable for it, so we propose a new blockchain technology based on the IOTA Tangle idea for WSNs, called Fishing Net Topology (FNT). In Tangle, two old transactions are approved by a new transaction. FNT draws on this dual authentication idea to design a new network topology for the packets generated by WSNs, making them more secure and faster to transmit and store the data. To address the computational power deficiency of WSN nodes and the difference with IoT devices, the proposed FNT simplifies the TSA in Tangle and removes the computation of cumulative weights that consume computational power, so that WSNs nodes do not need to perform complex computations and meet the energy-saving and lightweight requirements of WSNs.

**Reviewer 3, Comment 4:***-The authors mentioned WSNs but did not mention some of its challenges, such as security, lifespan of wireless nodes, etc. The authors should look for recent works on these aspects to cite. An example of such recent literature which the authors can consult amongst others is:*

*-Data Security in Wireless Sensor Networks: Attacks and Countermeasures. Lecture Notes in Networks and Systems, Vol. 140. Springer, Singapore, pp. 173-186, 2021. DOI: 10.1007/978-981-15-7130-5\_13*

**Authors’ response:**

Added a new paragraph describing the WSN challenge and citing the mentioned article. Section 2.1, line 74~79. The article mentioned has been cited.

WSNs face many challenges due to the limitations of node processor performance, wireless network, and physical environment [11]. Sensor nodes are deployed in unattended environments and are susceptible to accidental damage [12]. The use of wireless networks for communication leads to their vulnerability to network attacks. Common attacks against WSNs include Denial of Service, Jamming attack, Hello Flood attack, Black Hole attack, and Sybil attack [12], [13].

**Reviewer 3, Comment 5:***-Related works section was not presented thus the lack of identification of research gap. The authors should add this section as normally, it’s the gaps in work of others that the authors are expected to fill. Therefore, at the end of your review section state the problems in this field with appropriate reference and tell readers which one your work addresses.*

*The authors should consult and cite papers related to WSNs, IoT, Smart cities such as:*

*(i)                 Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks, in IEEE Access, vol. 9, pp. 72326-72341, 2021, doi: 10.1109/ACCESS.2021.3079708*

*(ii)               Recent Trends in IoT and Its Requisition with IoT Built Engineering: A Review. In: Rawat, B., Trivedi, A., Manhas, S., Karwal, V. (eds) Advances in Signal Processing and Communication. Lecture Notes in Electrical Engineering, Vol. 526. Springer Singapore, 2019. DOI: 10.1007/978-981-13-2553-3\_2*

*(iii)             An Integrated IoT System Pathway for Smart Cities. International Journal on Emerging Technologies, Vol. 11(1), pp. 1–9, 2020.*

*(iv)             IoT Based Smart Digital Electric Meter for Home Appliances. 2020 International Conference on Decision Aid Sciences and Application (DASA), Sakheer, Bahrain, pp. 708-713, 2020. DOI: 10.1109/DASA51403.2020.9317062.*

*(v)               Internet of Things: Energy, Industry, and Healthcare. Book published by CRC Press, Taylor and Francis, pp. 1-330, 2021. DOI: 10.1201/9781003140443.*

*Available online: https://www.routledge.com/Internet-of-Things-Energy-Industry-and-Healthcare/Rana-Salau-Sharma-Tayal-Gupta/p/book/9780367686529*

**Authors’ response:**

Added Section 2.5, Related Work. Revised section 2.6, summary. Line 126~167. The three articles mentioned have been cited.

Related Work

Since the lack of literature on the application of the IOTA Tangle to WSNs, studies on the simulation of the IOTA Tangle are presented here, which reflect some of the shortcomings of the Tangle and the barriers to its application in WSNs.

In [26], the researchers have analyzed actual transaction data published by the IOTA Foundation and compared it with theoretical data in the literature. They reconstructed 96 Tangles from the dataset. By analyzing their dimensions, in-degree distribution, cumulative weight, and transaction confirmation delay, they concluded that the actual transaction confirmation delay was very high. At the same time, they believed that the three influencing factors namely the transaction arrival rate, the Tip Selection Algorithm (TSA), and the intervention of the Coordinator (COO) caused the performance of the actual results to be far from the simulation results. In addition, the computation of cumulative weights was complex and inefficient that ultimately affecting the tip selection and the performance of the entire network.

In [28], researchers described the structure and characteristics of the Tangle. They use computer simulations to analyze the evolution of cumulative weights and tip counts over time, resulting in a formula for the average tip count. They conclude that the growth of cumulative weights follows an exponential growth during the adoption phase, followed by a linear phase with the slope of *λ*. The TSA did not affect this result when *α* was small and this significantly impacted the growth of cumulative weights for larger *α*. Due to the uncertainty of tip selection, the internal structure of the Tangle was also uncertain.

Summary

As one of the technological foundations of IoT, WSNs have a more straightforward structure than IoT. WSNs are used to collect and provide data, and IoT technology is used to analyze the data collected from the Internet and present the information for user access [32]. WSN devices are mainly various types of sensors, while IoT devices include sensors and more complex devices. There are many devices in IoT that can generate a large number of small transactions. Bitcoin can only process seven transactions per second, and Ethereum can process 14 transactions per second [6]. This performance cannot meet IoT requirements, so IOTA Tangle is proposed as a blockchain technology designed for IoT data transmission and security needs.

The differences between IoT and WSNs determine that IOTA Tangle is not the best solution for WSNs. WSN needs a new blockchain technology that is more suitable for it, so we propose a new blockchain technology based on the IOTA Tangle idea for WSNs, called Fishing Net Topology (FNT). In Tangle, two old transactions are approved by a new transaction. FNT draws on this dual authentication idea to design a new network topology for the packets generated by WSNs, making them more secure and faster to transmit and store the data. To address the computational power deficiency of WSN nodes and the difference with IoT devices, the proposed FNT simplifies the TSA in Tangle and removes the computation of cumulative weights that consume computational power, so that WSNs nodes do not need to perform complex computations and meet the energy-saving and lightweight requirements of WSNs.

**Reviewer 3, Comment 6:***-The authors need to discuss the results in the Tables better. The reason why the proposed technique performs better has not been explained. A block diagram or flowchart of the steps or method would be helpful.*

**Authors’ response:**

Updated the table 2 in section 4.3. Added line 334~348.

Table 2. The Waste Rates Under the Different Rates and Number of FNT Nodes.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| WR | S=100 | S=1000 | S=10,000 | S=100,000 | S=1,000,000 |
| r=5 | 16.2791% | 10.6700% | 10.0674% | 10.0067% | 10.0007% |
| r=6 | 18.1548% | 9.4203% | 8.4432% | 8.3443% | 8.3344% |
| r=10 | 32.1429% | 8.6538% | 5.3785% | 5.0380% | 5.0038% |
| r=15 | 51.0549% | 11.9210% | 4.2667% | 3.4275% | 3.3428% |
| r=20 | 65.1786% | 17.3729% | 4.2240% | 2.6752% | 2.5175% |
| r=25 | 74.7097% | 23.8835% | 4.7388% | 2.2809% | 2.0282% |
| r=30 | 81.0897% | 30.7512% | 5.6302% | 2.0779% | 1.7079% |
| r=50 | 92.3846% | 55.0000% | 11.6071% | 2.1739% | 1.1187% |
| r=100 | 98.0100% | 83.1356% | 33.2215% | 5.1478% | 0.9852% |
| r=120 | 98.6130% | 87.6753% | 41.6959% | 7.0010% | 1.1168% |
| r=150 | 99.1101% | 91.7631% | 52.7646% | 10.2910% | 1.4275% |
| r=200 | 99.4987% | 95.2043% | 66.5268% | 16.7362% | 2.1867% |
| r=500 | 99.9198% | 99.2040% | 92.5725% | 55.5011% | 11.1605% |
| r=600 | 99.9443% | 99.4461% | 94.7246% | 64.2388% | 15.2818% |
| r=700 | 99.9591% | 99.5926% | 96.0704% | 70.9763% | 19.6909% |
| r=800 | 99.9687% | 99.6879% | 96.9642% | 76.1599% | 24.2439% |
| r=900 | 99.9753% | 99.7533% | 97.5865% | 80.1737% | 28.8196% |
| r=1000 | 99.9800% | 99.8001% | 98.0363% | 83.3139% | 33.3222% |

Due to space limitations, this table only shows some combinations of rates and packets number. As can be seen in Table 2, the more the number of packets, the lower the waste rate for the same rate. However, a higher rate does not result in a lower waste rate for the same number of packets. At a rate of 10, the waste rate decreases as the number of packets increases, from 32.1429% at 100 packets to 5.0038% at one million packets, and will continue to decrease. When there are one million packets, the lowest waste rate occurs between 50 and 120, which is about 0.9852%. At this point, the waste rate is already below 1%. Such a combination of rate and number of packets is considered optimal, as its waste rate is minimal. More accurate optimal rates, which are not shown in the table, require further calculations between 50 and 120.

In summary, having an optimal rate for different numbers of packets can minimize the waste of the network. Thus, when establishing FNT, predicting the number of packets that may be generated based on the size of the WSNs can help users determine an optimal rate so that users can choose the most appropriate WSNs plan based on actual demand and budget.

Added line 318~320 in section 4.3, formula 6.

We use an example with a rate of 5 and 100 FNT nodes inserted to show the calculation process for the waste rate data shown in the subsequent figures and tables. The waste rate obtained in this case is 16.2791%.

Diagram, schematic

Description automatically generated

**Reviewer 3, Comment 7:***-There is no comparison of results with the existing works in this paper. This should be added for readers to see how your proposed method performs relative to other works.*

**Authors’ response:**

As there is currently no research on the application of the IOTA-based network topology proposed in this paper to WSNs. This study only draws on two verification and supplementary ideas in the IOTA Tangle, so no existing cases are found for comparison.

**Reviewer 3, Comment 8:**

*-The authors should structure the paper into abstract, introduction, literature review/related works, methodology, results and discussion, and conclusion.*

**Authors’ response:**

The titles have been changed.

**Reviewer 3, Comment 9:**

*-I was hoping to see more results and discussion as more results could be presented to make the work much appreciable. The authors are encouraged to reduce the plagiarism of the paper.*

**Authors’ response:**

Rewritten Section 5, Conclusion and Recommendation, lines 349~413.

We have checked the paper thoroughly for plagiarism and there is none. All parts of this article that refer to the work of others have been cited, and are in sections 1,2. The main part of the article, sections 3,4,5, does not refer to any existing work, and all images and figures in the article are drawn using PowerPoint and Python Matplotlib. The formulas are derived by ourselves, and the data in the tables and figures are also calculated from the formulas.

**Reviewer 3, Comment 10:**

*-The Limitations of the proposed study need to be discussed before conclusion.*

**Authors’ response:**

Rewritten Section 5, Conclusion and Recommendation, lines 349~413.

Based on the technical background of WSNs, IoT, Blockchain, and IOTA Tangle, we proposed Fishing Net Topology (FNT). FNT meets the energy-saving and lightweight requirements of WSNs. This paper elaborates on the structure, algorithm, and features of FNT. The comparison with Tangle and the experimental analysis of the waste rate of the FNT for different rates and the number of FNT nodes conclude that choosing a reasonable rate can significantly reduce waste and computation. FNT improves on two shortcomings of IOTA Tangle. First, it discards the complex tip selection algorithm and uses only a simple calculation of the node index to find tips and attach them. Second, the calculation of cumulative weights is not required in FNT. These improvements allow FNT to save computations and costs.

The FNT waste rate for different rates and number of packets is shown in the figures and tables. At the same rate, the higher the number of packets, the lower the overall waste rate, and eventually, the trend will stabilize, as waste will persist. Calculating the optimal rate for the different number of packets of FNT is critical, and the choice of different rates can lead to a dramatic change in the result. We used the waste rate calculation formula and calculated the waste rate of some FNTs shown in Table 2, from the maximum waste rate close to 100% to a minimum of less than 1%. We can see that under the same packet number, as the rate increases, the waste rate decreases gradually to the minimum value and then starts to increase. We can get the minimum value of the waste rate, and the corresponding rate is the optimal rate.

The application scenario of FNT is shown in Figure 2. In WSNs, many sensor nodes are deployed in a specific environment for collecting and sensing data. Each sensor node should upload packets to the gateway at a preset time interval. The size of the FNT is also specified according to the user's demand for the size of the WSNs, so its rate is preset. In the gateway, the submitted packets are attached to the FNT. Each packet needs to be validated against the data of its two Tips, also previously submitted packets. Since it is not attached by other packets, it is temporarily called Tips. Packets that pass the two Approvers validation become general FNT nodes. As more and more packets are attached to the FNT and verified by more and more packets, the authenticity of the data in the whole network is guaranteed. Users can access the FNT and its data stored in the gateway and more operations through the Internet.

In applying FNT, a reasonable rate should be calculated to save costs depending on the demand for WSNs. The cost of implementing FNT is mainly in the network service. FNT has no additional demand on the hardware of WSN nodes, so there is no additional cost. Higher network speed and bandwidth lead to more expenses, and the selection of the best rate in FNT is to refer users to choosing network services to reduce expenses. FNT aims to reduce the computation of WSN nodes while providing a secure and reliable data storage and transmission solution.

During the design of FNT, we took inspiration from the DAG structure of the IOTA Tangle and made many structural design attempts. Some of these solutions achieve higher network utilization but lack security, while others are faster processing but lack scalability. After comparison, we chose the current FNT structure. The FNT structure starts with one initial node, and each subsequent layer has one more node than the previous one until it reaches a preset rate value and completes the initialization. We need to verify each node twice to improve security so the FNT structure is obtained. In the Formal Network, to enable each FNT node to be approved twice, it can be noticed that one FNT node position is wasted every two layers. This means that not every layer is operating at the maximum rate. Despite the waste, this approach can effectively improve packet security. In addition, the main challenge we face is how to measure the performance of FNT. We have calculated the waste in the network through formula derivation and program simulation. There should also be more measures that need to be improved in future studies.

FNT relies on a stable and lightweight security mechanism. When a new FNT node is attached, it must approve its Tips. The approval process requires first determining the operational and security status of the sensor nodes, and second the authenticity of the data contained in the packet. This requires creating a data model to estimate the range of data the sensor may acquire, which relies on historical sensing data from the environment in which the sensor is located. In future research, we plan to create this security model based on machine learning. The model will use a series of algorithms and historical data analysis to determine the authenticity of the data in the nodes to avoid polluting the entire dataset with data generated by malicious nodes. Therefore, in future work, we need to develop and validate a security model for data validation to improve the security of using FNT. There is also a need to evaluate the performance of FNT from more perspectives and add more metrics. We also need to identify the problems and improve them through practical applications.

**Reviewer 3, Comment 11:**

*-Some of the challenges encountered during the course of the study can be highlighted and future recommendations can be added at the end of the conclusion. Retitle conclusion as conclusion and recommendation.*

**Authors’ response:**

Rewritten Section 5, Conclusion and Recommendation, lines 349~413. Retitled.

Added line 388~400.

During the design of FNT, we took inspiration from the DAG structure of the IOTA Tangle and made many structural design attempts. Some of these solutions achieve higher network utilization but lack security, while others are faster processing but lack scalability. After comparison, we chose the current FNT structure. The FNT structure starts with one initial node, and each subsequent layer has one more node than the previous one until it reaches a preset rate value and completes the initialization. We need to verify each node twice to improve security so the FNT structure is obtained. In the Formal Network, to enable each FNT node to be approved twice, it can be noticed that one FNT node position is wasted every two layers. This means that not every layer is operating at the maximum rate. Despite the waste, this approach can effectively improve packet security. In addition, the main challenge we face is how to measure the performance of FNT. We have calculated the waste in the network through formula derivation and program simulation. There should also be more measures that need to be improved in future studies.

**Reviewer 3, Comment 12:**

*-The results and discussion section is very weak. The authors should endeavor to improve on this section. In the section of selection of local minima, what criteria did the authors used. Also what priors did the authors consider? What is the minimum and the maximum values? If these are suitable, do they work for different types of speeches or features were extracted?*

**Authors’ response:**

Rewritten Section 5, Conclusion and Recommendation, lines 349~413.

Based on the technical background of WSNs, IoT, Blockchain, and IOTA Tangle, we proposed Fishing Net Topology (FNT). FNT meets the energy-saving and lightweight requirements of WSNs. This paper elaborates on the structure, algorithm, and features of FNT. The comparison with Tangle and the experimental analysis of the waste rate of the FNT for different rates and the number of FNT nodes conclude that choosing a reasonable rate can significantly reduce waste and computation. FNT improves on two shortcomings of IOTA Tangle. First, it discards the complex tip selection algorithm and uses only a simple calculation of the node index to find tips and attach them. Second, the calculation of cumulative weights is not required in FNT. These improvements allow FNT to save computations and costs.

The FNT waste rate for different rates and number of packets is shown in the figures and tables. At the same rate, the higher the number of packets, the lower the overall waste rate, and eventually, the trend will stabilize, as waste will persist. Calculating the optimal rate for the different number of packets of FNT is critical, and the choice of different rates can lead to a dramatic change in the result. We used the waste rate calculation formula and calculated the waste rate of some FNTs shown in Table 2, from the maximum waste rate close to 100% to a minimum of less than 1%. We can see that under the same packet number, as the rate increases, the waste rate decreases gradually to the minimum value and then starts to increase. We can get the minimum value of the waste rate, and the corresponding rate is the optimal rate.

The application scenario of FNT is shown in Figure 2. In WSNs, many sensor nodes are deployed in a specific environment for collecting and sensing data. Each sensor node should upload packets to the gateway at a preset time interval. The size of the FNT is also specified according to the user's demand for the size of the WSNs, so its rate is preset. In the gateway, the submitted packets are attached to the FNT. Each packet needs to be validated against the data of its two Tips, also previously submitted packets. Since it is not attached by other packets, it is temporarily called Tips. Packets that pass the two Approvers validation become general FNT nodes. As more and more packets are attached to the FNT and verified by more and more packets, the authenticity of the data in the whole network is guaranteed. Users can access the FNT and its data stored in the gateway and more operations through the Internet.

In applying FNT, a reasonable rate should be calculated to save costs depending on the demand for WSNs. The cost of implementing FNT is mainly in the network service. FNT has no additional demand on the hardware of WSN nodes, so there is no additional cost. Higher network speed and bandwidth lead to more expenses, and the selection of the best rate in FNT is to refer users to choosing network services to reduce expenses. FNT aims to reduce the computation of WSN nodes while providing a secure and reliable data storage and transmission solution.

During the design of FNT, we took inspiration from the DAG structure of the IOTA Tangle and made many structural design attempts. Some of these solutions achieve higher network utilization but lack security, while others are faster processing but lack scalability. After comparison, we chose the current FNT structure. The FNT structure starts with one initial node, and each subsequent layer has one more node than the previous one until it reaches a preset rate value and completes the initialization. We need to verify each node twice to improve security so the FNT structure is obtained. In the Formal Network, to enable each FNT node to be approved twice, it can be noticed that one FNT node position is wasted every two layers. This means that not every layer is operating at the maximum rate. Despite the waste, this approach can effectively improve packet security. In addition, the main challenge we face is how to measure the performance of FNT. We have calculated the waste in the network through formula derivation and program simulation. There should also be more measures that need to be improved in future studies.

FNT relies on a stable and lightweight security mechanism. When a new FNT node is attached, it must approve its Tips. The approval process requires first determining the operational and security status of the sensor nodes, and second the authenticity of the data contained in the packet. This requires creating a data model to estimate the range of data the sensor may acquire, which relies on historical sensing data from the environment in which the sensor is located. In future research, we plan to create this security model based on machine learning. The model will use a series of algorithms and historical data analysis to determine the authenticity of the data in the nodes to avoid polluting the entire dataset with data generated by malicious nodes. Therefore, in future work, we need to develop and validate a security model for data validation to improve the security of using FNT. There is also a need to evaluate the performance of FNT from more perspectives and add more metrics. We also need to identify the problems and improve them through practical applications.

**Reviewer 3, Comment 13:**

*-How does your paper vary with/what is the difference with this paper and yours: A blockchain-empowered authentication scheme for worm detection in wireless sensor network.* [*https://www.sciencedirect.com/science/article/pii/S2352864822000566*](https://www.sciencedirect.com/science/article/pii/S2352864822000566)

**Authors’ response:**

Thank you for recommending this new article, which focuses on a security model and provides us with a reference for designing a security model for FNT in the future. Our article mainly proposes a new packet/message network topology to facilitate data storage and transmission for WSNs. Although the security model is not the focus of this particular work, it lays the foundation for designing a robust security model for WSN in future.

**Reviewer 3, Comment 14:**

*-Lastly, no comparison of results was presented with other state-of-the-art methods which have used machine learning techniques*

**Authors’ response:**

We did not find a similar solution, so we cannot compare. However, your suggestion does point to our next research plan, where we plan to design a machine learning based security model for FNT to improve the security of FNT.

**Reference**

[5] Bhandary, M.; Parmar, M.; Ambawade, D. A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), 2020, pp. 827–832. https://doi.org/10.1109/ICCES48766.2020.9137858.

[6] Shabandri, B.; Maheshwari, P. Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle. In Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), 2019, pp. 1069–1075. https://doi.org/10.1109/SPIN.2019.8711591.

[7] Khalil, N.; Abid, M.R.; Benhaddou, D.; Gerndt, M. Wireless sensors networks for Internet of Things. In Proceedings of the 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014, pp. 1–6. https://doi.org/10.1109/ISSNIP.2014.6827681.

[11] Zia, T.; Zomaya, A. Security Issues in Wireless Sensor Networks. In Proceedings of the 2006 International Conference on Systems and Networks Communications (ICSNC’06), 2006, pp. 40–40. https://doi.org/10.1109/ICSNC.2006.66.

[12] Salau, A.O.; Marriwala, N.; Athaee, M. Data security in wireless sensor networks: attacks and countermeasures. In Mobile radio communications and 5G networks; Springer, 2021; pp. 173–186.

[13] Du, X.; Chen, H.h. Security in wireless sensor networks. IEEE Wireless Communications **2008**, 15, 60–66. https://doi.org/10.1109/MWC.2008.4599222.

[14] Hassan, W.H.; et al. Current research on Internet of Things (IoT) security: A survey. Computer networks **2019**, 148, 283–294.

[26] Guo, F.; Xiao, X.; Hecker, A.; Dustdar, S. Characterizing IOTA Tangle with Empirical Data. In Proceedings of the GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1–6. https://doi.org/10.1109/GLOBECOM42002.2020.9322220.

[27] Silvano,W.F.; Marcelino, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. Future generation computer systems **2020**, 112, 307–319.

[28] Kusmierz, B.; Staupe, P.; Gal, A. Extracting tangle properties in continuous time via large-scale simulations. Technical Report. working paper **2018**, pp. 2018–08.

[29] Hao, Y.; Li, Y.; Dong, X.; Fang, L.; Chen, P. Performance Analysis of Consensus Algorithm in Private Blockchain. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), 2018, pp. 280–285. https://doi.org/10.1109/IVS.2018.8500557.

[30] Zhou, Z.; Li, R.; Cao, Y.; Zheng, L.; Xiao, H. Dynamic Performance Evaluation of Blockchain Technologies. IEEE Access **2020**, 8, 217762–217772. https://doi.org/10.1109/ACCESS.2020.3040875.

[31] Fan, C.; Ghaemi, S.; Khazaei, H.; Musilek, P. Performance Evaluation of Blockchain Systems: A Systematic Survey. IEEE Access **2020**, 8, 126927–126950. https://doi.org/10.1109/ACCESS.2020.3006078.

[32] Worlu, C.; Jamal, A.A.; Mahiddin, N.A. Wireless sensor networks, internet of things, and their challenges. International Journal of Innovative Technology and Exploring Engineering **2019**, 8, 556–566.

[33] Nghia, M. TangleSimulator. https://github.com/minh-nghia/TangleSimulator, 2018.