QUALITY OF SERVICE TRANSMISSION IN NETWORK LEVELS

[1]K. SREELATHA, [2]Dr.T.SREEKALA,
[1]Research Scholar, [2]Associate Professor,
Department of Computer Science , VISTAS, Chennai,
[1]9994035658, [2] 9629333746
[1]sreelathak59@gmail.com, [2]sreekalatm@gmail.com

Abstract: In Wireless Sensor Network (WSN) sending data needed to be more secure. To provide security over data is a difficult process. The sensors are installed in the region called as the sensor field. WSNs require more attention towards data security and this is considered to be a major problem in this research. Quality of Service (QoS) are known as methods and procedures used to determine the quality of the network parameters. But implementing QoS is usually not an easy operation because of many network nodes. Several critical elements like energy protection, protocol design and architecture in WSNs are studied in detail. QoS supports problems related to security of data. The basic aim of QoS is to ensure that the network can deliver the intended outcomes where the proposed Network ID based Transmission Securing Protocol (NIDTSP) achieves effectiveness. The delay (latency), performance, energy consumption and error rate are considered to be the basic quality factors. It distinguishes the network traffic flows by processing packets in a distinct way. The patterns fulfil various tasks depending on the network traffic flow and the device site with QoS functionality. In order to guarantee a given degree of performance, it prioritizes distinct data flows. However, QoS is undermined by factors such as missing network data, reliability, and latency.

Keyword: QoS, network ID, security, latency, reliability, data traffic, energy consumption, and WSN.

1. Introduction

In WSN sending data needed to be more secure. To provide security over data is a difficult process. The sensors are installed in the region called as the sensor field. Environment provides data to sensors and transmits them via multi-hops to BS. BS which is also called the sink uses a satellite or internet connection to connect with the users. The development of multifunctional small smart sensors has been enabled with advancements in miniatures, particularly in microelectronic mechanical systems. The Multi-functional Tiny Smart Sensors (MTSE) are used in WSNs and are intended for the IQoSment its standard networks with WSNs. This permits WSNs to become a component of human lives.

The WSNs can be split into two primary categories based on their application such as tracking and monitoring said by (Singh 2019). The application comprises environmental monitoring both inside and outside. Apart from this node, human beings, animals and objects are tracked for various applications. Sensors can also be used in all kinds of physical contexts, including plain, subterranean, and under-sensing fields for collecting various forms of data. In each condition, depending on the environment, a sensor network is bound differently. However, WSNs continue to face a number of obstacles, including restricted power, bandwidth, and movement and with no central controller. Once the parameters of the network are correctly determine any networks performance incorporating WSNs may be measured, forecasted and enhanced. These network metrics include access, bandwidth, latency and error rate.

WSNs require more attention towards data security and this is considered to be a major problem in this research. Quality of Service (QoS) are known as methods and procedures used to determine the quality of the network parameters. But implementing QoS is usually not an easy operation because of many network nodes as proposed in (Ahmed 2016). Several critical elements like energy protection, protocol design and architecture in WSNs are studied in detail. QoS supports problems related to security of data. The basic aim of QoS is to ensure that the network can deliver the intended outcomes. The delay (latency), performance, energy consumption and error rate are considered to be the basic quality factors. It distinguishes the network traffic flows by processing packets in a distinct way. The patterns fulfil various tasks depending on the network traffic flow and the device site with QoS functionality. In order to guarantee a given degree of performance, it prioritizes distinct data flows. However, QoS is undermined by factors such as missing network data, reliability, and latency. The following tasks can be achieved through QoS.

- Offer high-level services in video, audio and pictures applications.
- Distinguish between different traffic networks and prioritize each class to organize network resources.
- Efficient utilization of network bandwidth.

The QoS process is divided into 4 network levels in WSNs – (i) identity (ii) path (iii) position, and (iv) privacy. Due to existing restrictions in WSN, it is a difficult task to secure the network level. In WSN, QoS Routing protocols and privacy based routing strategy are not preferred in the event of energy consumption and security attacks. Existing privacy schemes cannot give information on many forms of identification, route, location and data confidentiality.

Each sensor node must send its data to other nodes by a multi-hop routing network. Optimized power in WSNs is a key measure of performance since the minimum battery power in design-based sensor nodes is available. However, the formation of node clusters minimizes the number of nodes participating and thereby reduces energy consumption by picking a CH for each cluster. CH collects, combines and transmits data from its member nodes to sink using a single hop or multi-hop routing in cluster process.

The multi-hop routing gives the nodes an chance to observe the malicious activity in the WSN nodes. The design of safe routing protocols is the most critical problem for WSNs due to the presence of hostile nodes. These nodes may deliberately delete packets or misdirect messages along the route. It also redirects active packets from renowned sensor nodes with highly trusted CH for successful secured WSN routing. The CH should be picked in this case based on a high confidence to prevent a CH from attacking nodes.

In addition, member nodes must be isolated from other cluster members to reduce illegal activities and to prevent interference with network activities. Otherwise it will lead to a decrease of accuracy in confidence value. As already said, secure routing algorithms in the presence of attackers are a significant and tough problem in WSN. A security method must therefore be developed to safeguard network communication.

The secure routing algorithm can be created by considering two important strategies like firewall and Intrusion Detection System (IDS). Firewalls as well as IDS can be discovered by deploying attackers on network nodes. But attackers attempt to breach the safety procedures provided in firewalls and IDS with efficient technology. A trust-based safe routing protocol can be constructed employing keys, encryption and decryption techniques through user authentication. In order to provide better security, this procedure needs support for effective core generation, key distribution, control and rekeying methods. Authentication protocols were previously developed to improve user authentication. Many strategies for centralized key management and distributed key management procedures were suggested by researchers. Both Firewall and IDS are helpful for more efficient user authentication.

The first stage authentication is used in most authentication techniques like the user credentials like the name of the user, password, IP address and a captcha. Better key management techniques can also be used for the verification of decryption and encryption, use of nonce (number only used once) to improve security and also generate and send OTPs. QoS-aware multi-hop communications network using ID based secured routing protocol utilizes the technique of resembling and fragmentation. The network will be adjusted with the cluster nodes portion with respect to dynamic network scale size count and possess good flexibility and achievability. In this process initially the ID based secured routing has been established for enhancing the security. Here each online user is considered to be single data and they have been clustered to improve the data optimization.

2. Proposed Methodology

A connected graph G (V, E) is considered as model for sensor network, considering sensor nodes set as V, |V| = N and the sensor nodes count is N, and E represents the set of wireless links concerning the sensor nodes. To explore optimality of routing protocols, a set of directed physical wireless links are used in design routing models. Every node is accountable to monitoring and evaluates its neighbour‘s behavior. In particular, results of detection of trust calculations are used. Node i is an evaluating device in our paradigm, while node j is an assessing device. Confidence t of an arbitrary node comprises both direct confidence and indirect confidence

Routing charts are determined by path and packet transfer values. Selection of an optimum route on a weighted physical graph can be regarded as a routing problem through use of routing measure r. The routing measure r for our model is one of the trust metrics. Ideal routing can eventually generate all the optimal paths. In order to maximize the required service quality ideal path is defined based on the principle of security

Sensor nodes are normally extremely restricted with regard to power of computaion, energy, memory, and bandwidth. Therefore it is significantly challenging to design security mechanisms for WSNs. A lightweight method of calculating sensor node confidence values is proposed.

$$t(i,j)^{l} = \alpha \times dt(i,j)^{l} + \beta \times \frac{\sum_{(kkC_j=\neq i)}^{n} it(k,j)^{l}}{n-1}$$

where, t(i,j) is the trust value of node i with respect to node j, n indicates number of neighbors, while l refers to evaluation sequence number. kkC$_j$ is the recommended trust value of j node, it(i,j) is the previous trust value of j node. Weighed factors related to security policies are α and β. A greater α value indicates a stronger understanding of the sensor node in WSNs. Likewise, a higher value for β means more trustworthy in the process of trust assessment of suggestions offered by other nodes. Furthermore, the trust value ranges from 0 to 1.

In general, if the sensor nodes trust value is greater, then the data is said to be more confidential. With appropriate values of α and ß the effect of contradictory behavior attacks can be reduced. Since the neighbor on the network monitors the behavior of nodes, a malicious node can be easily identified. Comparing neighbor nodes with different ways, the direct trust and indirect trust combination can then be identified. The direct trust shall be calculated by

$$dt(k,j)^{l} = \gamma_1 \times dt_{p(j)}(i,j)^{l-1} + ids(i,j)^{l}$$

where γ_1, γ_2 are environmental factor that range from 2 to 5, $dt_{p(j)}(i,j)^{l-1}$ is node i's direct trust value with respect to node j, based on node j's previous well-behaved behavior, and $dt_{N(j)}(i,j)^{l-1}$ is node j's direct trust value for node i, based on node j's previous malevolent behavior. Exponential decay time factors of positive and negative assessments, respectively, are j1 and j2. ids (i, j)^l signifies an assessment of device j's current behavior using IDS and is given by

$$ids(i,j) = \begin{cases} p(j), \; for 0 < P(j) < 1 \\ 0, \qquad for\ uncertain \\ N(j), for -1 < N(j) < 0 \end{cases}$$

P(j) and N(j) denote positive and negative evaluations of device j's behavior, respectively. These standards should be based on the principle that gaining a better repute is highly challenging and gaining a negative one. If judgment for node behavior is not totally certain, the value of ids(i,j) should be set to zero.

In a cluster, collected data is sent to CH by cluster members. Furthermore, CH node collects data from nodes participated and sends it to sink (BS). If the BS is inside CHs range of transmission, CH sends collected data immediately to BS. Otherwise, it uses relay nodes to transfer data. Relay nodes must be carefully chosen in this case. Incorrect relay nodes selection may result in a network with a short lifespan.

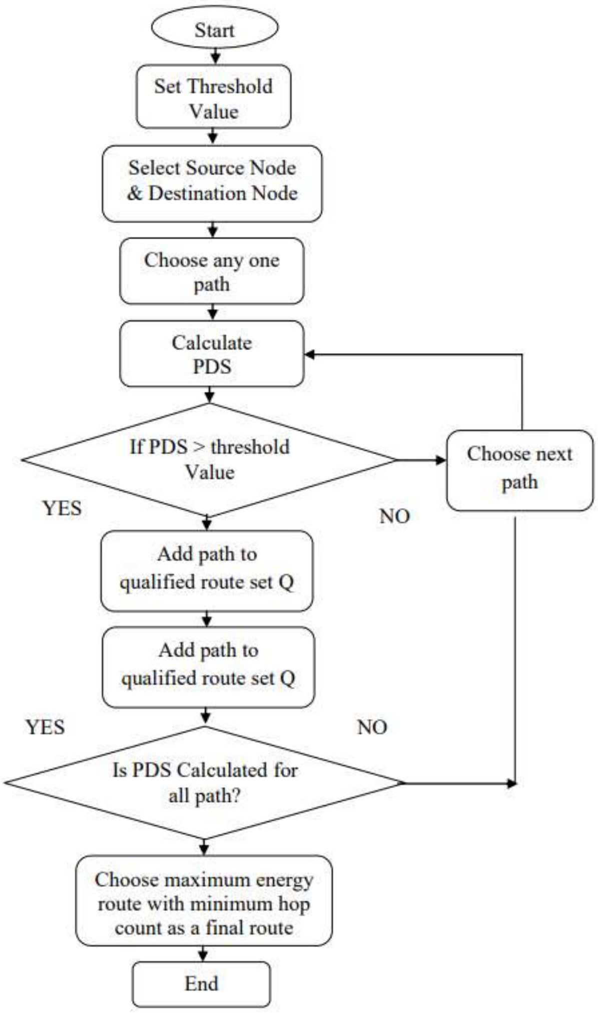
Start
Set Threshold Value
Select Source Node & Destination Node
Choose any one path
Calculate PDS
If PDS > threshold Value
Choose next path
YES
NO
Add path to qualified route set Q
Add path to qualified route set Q
YES
NO
Is PDS Calculated for all path?
Choose maximum energy route with minimum hop count as a final route
End

Figure 2.1 Flowchart of Trust Based Secure Routing Algorithm

A source node chooses a trustworthy path depends on value of path trust in this protocol. If the path trust value is higher than one path is larger then fewest hops to BS is chosen as the final route. Trust Based Secure Routing Algorithm is represented as flowchart in Figure 1.

3. Result and Discussion

Coverage area and energy consumption are the QoS metrics of performance that are considered while the algorithm is analyzed. The amount of energy used to transmit a packet from source to destination is largely established by the number of intermediate hops taken along the way. As the number of hops along a route upsurges, the amount of energy consumed will also be increased. The energy used during the initialization phase for test packets is also increased. Energy depends on the path chosen after the routing phase begins. Thus, the energy expended increases progressively depending on the path length before becoming saturated at a certain point. This is because there are the same numbers of intermediary nodes throughout the whole route from source to destination. The overall energy consumed for the intermediate hop and single hop transmissions are equal when transmitted normally (attack-free). When there is an attack-prone transmission, retransmission is required due to a lack of timely acknowledgement. The proposed NIDTSP is compared with the existing techniques namely Artificial Intelligence assisted QoS for WSN (AI-QoS) [21], and Industrial QoS (IQoS) [20].

Detection Probability

Various WSN domains employ the Probability of Detection (POD) concept to determine an inspection's capacity to find faults. The detection probability is given in Table 1 and Figure 2.

$$P_b = \exp[1\mu s\ (R(i) - D\ (i)]$$

Where, P_b = detection probability R(i) = detected targets (destination) D(i) = sum of all possible attacks.

Table 3.1. Comparison of Detection Probability

Algorithm/ Node Node	Existing Technique		Proposed Technique
	AI-QOS	IQOS	NIDTSP
200	69.3	58	83
300	70.5	58.7	83.9
400	74.7	59.7	84.6
500	76.8	60	85.1
600	78.2	61.7	85.3

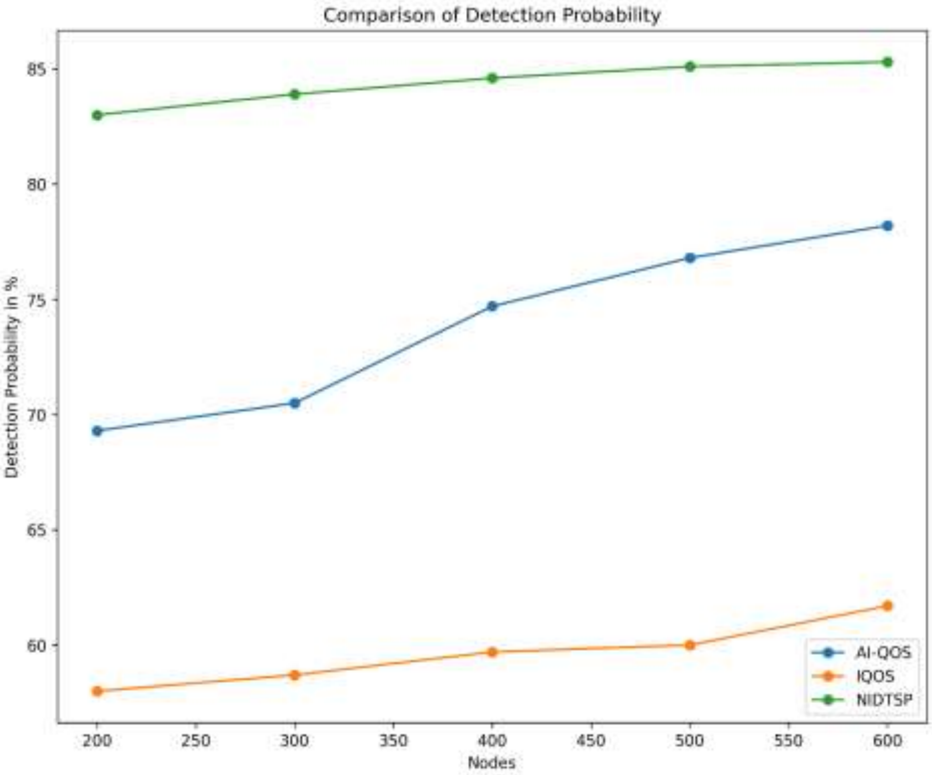

Figure 3.1. Comparison of Detection Probability

With assistance of trust score and trust identification, the inappropriate nodes are identified and it is illustrated in the Figure 2. The NIDTSP has highest detection probability for diverse count of nodes.

Packet Delivery Ratio

The packet delivery ratio (PDR), is a network metric, and it is the proportion of all packets transferred to total packets sent from source nodes to destination nodes. The PDR is given in Table 3 and Figure 4. The PDR calculation is as follows:

$$PDR = \frac{Recd_p}{Snd_p}$$

where $Recd_p$ - Received Packets by sink node and Snd_p - Sent Packets by node nodes.

Table 3.2. Comparison of PDR

Algorithm/ Node Node	Existing Technique		Proposed Technique
	AI-QOS	IQOS	NIDTSP
200	89	87	91
300	91	87.5	93
400	92	90	95
500	92.5	91	96
600	93	92	97

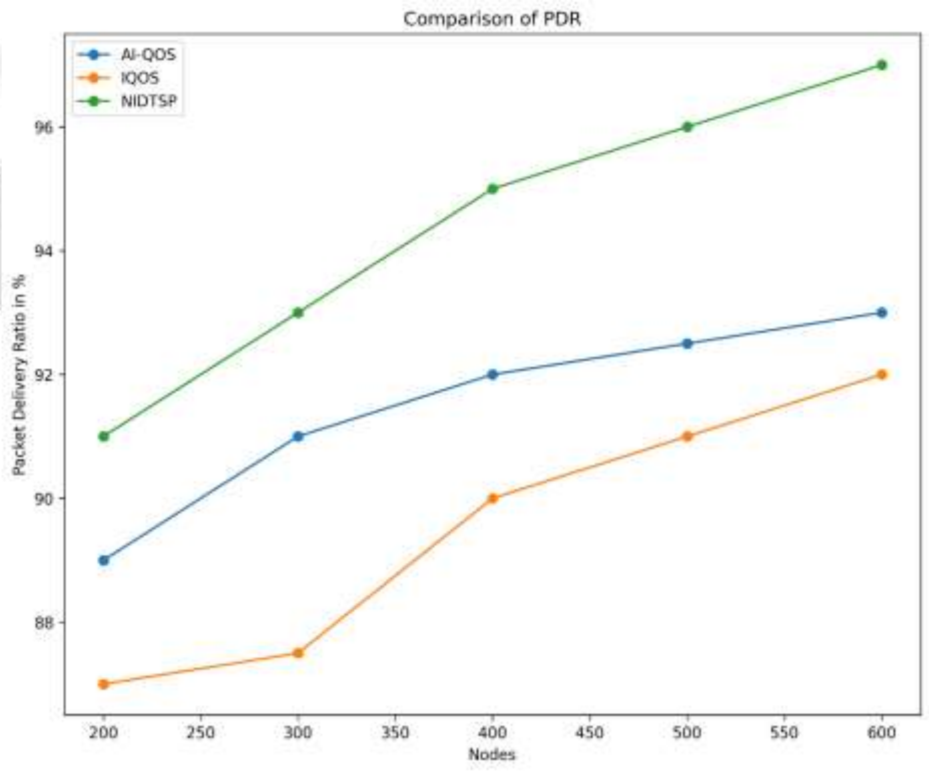

Figure 3.2. Comparison of PDR

With assistance of node management strategy and connection restoration, the inappropriate nodes are identified and it is illustrated in the Figure 4. The proposed approach has higher PDR for different count of node.

4. Conclusion

Nowadays, techniques of wireless communication and low cost wireless devices are improved a lot which paved a way to the development of WSN. In wireless communication systems, network and sensor are used to establish the communication known as wireless sensor network. It is applied in various applications because of its easier deployment and sensor node‘s multi-functionality. So, WSN is applicable in healthcare, tracking target, and monitoring environment. The results obtained indicate that the system proposed enhances the coverage area and decreases the energy consumption of the network. The proposed methods provide improvements in most of the factors and are validated. There are few other techniques and methods that can be considered to incorporate with the proposed methods. Grid-connected renewable energy systems was created and adjusted in future to estimate the effective data transmission among sensor nodes.

Reference

1. Ashish, A., Desai, A., &Sakadasariya, A. (2017, May). A review on energy efficient data centric routing protocol for WSN. In Trends in Electronics and Informatics (ICEI), 2017 International Conference on (pp. 430-434). IEEE.
2. Patil, S. S., Gudnavar, A., &Chandan, K. (2017, April). Energy efficient and reliable routing in densely distributed WSN. In Communication Systems, Computing and IT Applications
3. Ait Aoudia, F., Gautier, M., Magno, M., Berder, O., &Benini, L. (2017). A generic framework for modeling MAC protocols in wireless sensor networks. IEEE/ACM Transactions on Networking (TON), 25(3), 1489-1500.
4. Sabri A, Al-Shqeerat K, “Hierarchical cluster-based routing protocols for wireless sensor networks a survey”, Int J Comput Science 11(1):13, 2014.
5. Aldeer, M. M. (2013, December). A summary survey on recent applications of wireless sensor networks. In *2013 IEEE Student Conference on Research and Developement* (pp. 485-490). IEEE.
6. Potdar, M., Sharif, A., Potdar, V., & Chang, E. (2009, May). Applications of wireless sensor networks in pharmaceutical industry. In *2009 International Conference on Advanced Information Networking and Applications Workshops* (pp. 642-647). IEEE.
7. Xu, G., Shen, W., & Wang, X. (2014). Applications of wireless sensor networks in marine environment monitoring: A survey. *Sensors*, *14*(9), 16932-16954.
8. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd annual Hawaii international conference on system sciences* (pp. 10-pp). IEEE.
9. Younis, O., & Fahmy, S. (2004). HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on mobile computing*, *3*(4), 366-379.
10. Smaragdakis, G., Matta, I., & Bestavros, A. (2004, August). SEP: A stable election protocol for clustered heterogeneous wireless sensor networks. In *Second international workshop on sensor and actor network protocols and applications (SANPA 2004)* (Vol. 3).
11. Qing, L., Zhu, Q., & Wang, M. (2006). Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. *Computer communications*, *29*(12), 2230-2237.
12. Rathee, A., Kashyap, I., & Choudhary, K. (2015). Developed distributed energy-efficient clustering (DDEEC) algorithm based on fuzzy logic approach for optimizing energy management in heterogeneous WSNs. *International Journal of Computer Applications*, *115*(17), 14-19.
13. Saini, P., & Sharma, A. K. (2010, October). E-DEEC-enhanced distributed energy efficient clustering scheme for heterogeneous WSN. In *2010 First international conference on parallel, distributed and grid computing (PDGC 2010)* (pp. 205-210). IEEE.
14. Qureshi, T. N., Javaid, N., Khan, A. H., Iqbal, A., Akhtar, E., & Ishfaq, M. (2013). BEENISH: Balanced energy efficient network integrated super heterogeneous protocol for wireless sensor networks. *Procedia Computer Science*, *19*, 920-925.
15. Keshtgari, M., & Deljoo, A. (2011). A wireless sensor network solution for precision agriculture based on zigbee technology.
16. Hussain, R., Sahgal, J. L., Mishra, P., & Sharma, B. (2012). Application of WSN in rural development, agriculture water management. *International Journal of Soft Computing and Engineering (IJSCE)*, *2*(5), 68-72.
17. Correa-Hernando, E., Arranz, F. J., Diezma, B., Julia, E., Robla, J. I., Ruiz-Garcia, L., ... & Barreiro, P. (2011). Development of model based sensors for the supervision of a solar dryer. *Computers and electronics in agriculture*, *78*(2), 167-175.

18. Dong, X., Vuran, M. C., & Irmak, S. (2013). Autonomous precision agriculture through integration of wireless underground sensor networks with center pivot irrigation systems. *Ad Hoc Networks*, *11*(7), 1975-1987.
19. Milenković, A., Otto, C., & Jovanov, E. (2006). Wireless sensor networks for personal health monitoring: Issues and an implementation. *Computer communications*, *29*(13-14), 2521-2533.
20. Srinivasan, S., Ramesh, T. K., Paccapeli, R., & Fanucci, L. (2022). Industrial functional safety assessment for WSN using QoS metrics. *Heliyon*, *8*(11), e11255.
21. Osamy, Walid, Ahmed M. Khedr, Ahmed Salim, Ahmed A. El-Sawy, Mohammed Alreshoodi, and Ibrahim Alsukayti. "Recent Advances and Future Prospects of Using AI Solutions for Security, Fault Tolerance, and QoS Challenges in WSNs." *Electronics* 11, no. 24 (2022): 4122.