March-April 2020
ISSN: 0193-4120 Page No. 1282 - 1286

Optimizing the Life Time of Wireless Sensor Networks by Using Clustering and Genetic Algorithms

[1]Chigicherla Bharath Kumar Reddy, [2]R. Sheeja

[2]Assistant Professor, [1,2]Department of Computer Science and Engineering,
Saveetha School of Engineering, Saveetha Institutions of Medical and Technical Sciences,
Chennai, India

Article Info
Volume 83
Page Number: 1282 - 1286
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 14 March 2020*

Abstract

The communication between the master and the slave can be made through the wireless sensor network WSN. The WSN can be used in various resources for the data communication. Maximum numbers of protocols are communicating between the receiver and transmitter with the help of the WSN. For the communication the main sources is the energy consumption is act as the major part. Genetic algorithm can be implemented for the optimization which can increases the efficiency. Various applications are available for the optimization technique. The algorithm are selected based on the manner such as the less energy dissipation, uses the less number of nodes. The grouping of the routing system which can lead some disadvantages such as the node replacement, network failure. The increase the lifetime of grouping the router which can able to communicate to the other end in the specific distance. The target can be covered over less period of time. The optimization can achieve the large target medium and the use of less number of nodes. The simulation can be made using the optimization method which can result the proper communication between the two targets. Comparison has been made between the genetic algorithm and Radom deployment.

Keywords: *Transmission Time, Delivery Ratio, Genetic Algorithm, Throughput.*

1. Introduction

The data transmission can be made through the network communication. The communication between the transmitter and the receiver can be done through nodes. The node can transfer the data to the neighbor node. There is an intermediate node between the transmitter and the receiver. The intermediate node can receive and transmit the data to the next node. Several times some issues are raised such as the data is not communicate to the next node. Delays are getting raised to communicate the data. So to avoid this kind of problem the alternate way is used for the data path communication. For the alternate path they use the relay. The relay can operate act as the switch if the one path is not properly communicate to the node the another path can communicate the data to the next node. Due to the raise in the delay the energy consumption is increased. The nodes can also have the data of the large distance separate node. This can be used for the better performance for the data communication.

The multi hub communication also implemented in the network routing system. Data path can be created in two different sections.

The section is not linked to each other, this section can carries the separate data and the second section can carries the separate the data. When the data starts to communicate from the master to slave, it is get decrypted for the secured data transmission. Decrypted data is not able fetched by the unauthorized person. When the data is received by target it is get encrypted. The multi hub is mainly is used for the purpose to avoid the data traffic. If the data traffic occurs data to reach the target is difficult, at this time the multi hub can changes the data path for the fast data transmission. A sensor node network is provided in which seven sensor node are get connected to the each other. These nodes can monitor the humidity, temperature, pressure the sensed parameters are in the digital form. Each sensor node can contain the microcontroller, TX and RX module. The data which is sensed are stored in the data memory. The data can be communicated to the neighbor node. The network is sink is used which is the sensor node that can collects the information of the sensor network can transmit the data to the server. It uses the constant power when there is any increase in the delay. Connections are made if the server and the objects are linked in the same line. The access of the WSN can be made in which the network sink as act as the gate.

2. Literature Survey

Jayaram Pradhan et., al., proposed the data communicates through the network layer from the transmitter to receiver. In WSN the security is not much effective. The data transfer between the nodes is highly efficient. Due to the lack of security in the communication path. The hackers can easily enter the main section by attacking the various layer of protocols in WSN. The AODV system faces the security issues when the discovery process took place. So the users get fear to use the network layer for the communication. In this paper they propose the NL-IDS system. In which it can detects the black hole of the person who fetching the data from the nodes. The node trust of the sensor layer can be calculated based upon the black holes. The watchdog timer is used to calculate the deviation of the each node at specific period of time. The overall deviation can be calculated to find out the average value. Each node can carry the past and the present data. The NL-IDS system can easily find out the affected node and it get replaced by the other node. The node can carry the information of the next node. The simulation can be made using the MATLAB to calculate the NL-IDS. This method can gives the high accuracy and efficiency with false alarm rate. [1]

Colin C. Murphy et., al., proposed the internet can plays a vital role in the every person life. All the confidential data can be handling in the internet. The data are getting stored in the database. The data can be easily hacked by the unauthorized person or by the hackers. The Internet of things which can plays the major role in the network part. The data can be uploaded and viewed in the IOT. The data can be transferred through the node. The router has the several nodes, the nodes are get interlinked to form the communication network. Hackers can create a malicious data pack at the neighborhood node. The data can be attacked by the malicious data pack. To avoid the hacking of the data in this paper they proposes the COTS devices which act as the communication protocol in which the data transfer can be made more confidential manner. The data in the path is more standard in which can be undetected by the hackers. The WSN which use the particular protocol for the data extracting if the protocol does not match it detects the malicious data. In further the ZIGBEE based data transmission it can communicate the data at fast rate. The ZIGBEE can be interlinked with ISM which can act as the head of the network. The COTS devices are installed to detect the malicious data in the node connection. [2]

Haruo Yokota et., al., proposed in wireless sensor network the data communication can made through the node to node transfer. Using the nodes the hackers can creates the malicious data in each node when the data reaches the node it subjected to the malicious attack. It can create a uncertainty condition and it affects the environment by creating false alarm. To avoid these problems in this paper they proposes the detecting of the abnormal node. The abnormal node can be detected by using two methods spatial temporal ST and multivariate attribute MVA of sensor correlations. The ST sensor data are get gathered in the separate medium and it makes cross comparison is made between the node streams and the sensors. The threshold value is compared with the cross comparison. The MVA data and the ST cross comparison data can be interlinked together to reduce the abnormal nodes. This method can avoid the false alarm system can safeguard the node data from the malicious attack. The data can be in the standardized path. So the unauthorized person cannot able to create a attack in the node path to fetches the data. [3]

Houbing Song et., al., proposed when compared to the other network system the wireless sensor network WSN which has the lack of security. Data communication can be made through the communication protocols. As the WSN system implied the use of various protocols can

be increased. The increased protocols are mainly for the security purpose. These protocols can make the network layer more complex and it consume high amount of energy. To avoid this kind of problems in this paper they propose the knowledge based context aware approach. It can detect the malicious nodes present in the network layer. In the network layer knowledge based is in the base station, the knowledge based can accumulate all the data of the nodes. Nodes are connected in the form of cluster, the cluster head node which can block the malicious nodes in which data repetition appeared. Base station can affect the network layer this can be avoided by minimizing the security protection. [4]

$$d_{ij} = 1 - \frac{\left(x_i - \overline{x_i}\right)'\left(x_j - \overline{x_j}\right)}{\sqrt{\left(x_i - \overline{x_i}\right)'\left(x_i - \overline{x_i}\right)}\sqrt{\left(x_j - \overline{x_j}\right)'\left(x_j - \overline{x_j}\right)}}$$

Nei Kato et., al., proposed the WSN can extended the application in the field of the medical. The sensor can be setup in the body in which can reads the body parameters of the patient regularly. The sensed data whose resources are get limited. Environmental condition and the malicious attack can create a false data in which the false alarm is generated. If the false data of the patient can be transfer to the doctor, so based upon the false data the treatment is made which can affects the health of the patient. To make the WSN safe and secured in this paper they proposes the Bayesian network model based sensor network in which can prevents the data attack by the malicious node. This method can reads the training sets of the sensor data it can make the system process more accurate. The collection all the sensor data is avoided in this method. It can avoid the inaccuracy of data. The data base is maintained in which they collects the all the false alarm generated in the process. The number of false alarm generated is calculated and the performance is compared with the other methods. It can provide the better accuracy. [5]

Sunho Lim et., al., proposed the WSN has the lack of security in the physical protection and the co-ordination. The network protocols can be easily hacked by the unauthorized person. The DOS attack which is the denial of service attack which can affect the main server of the network layer or the current data communication path to fetches the data. To make the network layer more secured in this paper they propose the SCAD method. The SCAD can create check point in the communication between each nodes. The checkpoints are counter measured for the forward data transfer technique. The checkpoint can detect the malicious node in the network layer The simulation has been made to detect the performance by using the countermeasure technique the PDR can be detected which is the packet delivery ratio. The consumption of the energy is less compared to the other safety methods. The accuracy can be increased by the use of the counter measure. [6]

G.S Binu et., al., proposed compared to the wired sensor network, the wireless sensor network is not much secured due to the lack of security. The WSN can extend the application in the traffic monitoring, military. Due to the security defects they are not much used in these fields. The data is broadcast at the time of transmission the attackers can create the security nodes can fetches the data. Selective forwarding attack can target the network layer can stops the traveling of the data forwarding, the data leakage can occurs at the place. In this paper they propose the energy efficient detection algorithm which can detect the forward attacking of the data packets. This method can provide the accurate data security. The checkpoint can detect the malicious node in the network layer. The simulation has been made to detect the performance by using the countermeasure technique the PDR can be detected which is the packet delivery ratio. Malicious node can be detected in the network layer with the help of the energy efficient algorithm. It consumes less amount of power. The false alarm is reduced and the value is get recorded in the database. [7]

M. Rajesh et., al., proposed WSN can be applied in the field of the border security, radar surveillance etc., For the border security applications the data security in the network communication is more important. There are several types of attack to fetches the data in the communication layer. The false injection attack can attack the nodes of the data it is the dangerous attack in the network protocol. RSS, ECC are employed for the prevention of the false data injection in the communication path. The paper proposes the trusted parameter it can separate the node into two different mode malicious node and the non malicious node. The non malicious node can be used in the forward data transmission packet to the server. The simulation is made in the NS2 and energy consumption is also minimum. [8]

$$\frac{\pi^{n/2} r^n}{\Gamma\left(\frac{n}{2}+1\right)}$$

Donghui Li et., al., proposed Easy attack by the environment conditions, consumption of power, poor hardware constructions and the lack of security data. These drawbacks in the WSN can be overcome with implementing the paper. This paper proposes the novel

trust routing protocol method it gathers the number of attributes of the sensor network such as the energy, data, and communication. The use the sliding window method to detect the malicious node in the network layer. The nodes can be interlinked to from the communication to secure the information in the path by use of this method. The time consumption can be reduced up to 7% and the data packets can be increased up to 12%. [9]

Guruprasanna et., al., proposed the MANET which is the mobile ad-hoc network it has the various node for the data transfer. The malicious node are get created and attack the data in the other nodes. So to detect the malicious node in this paper they proposes the CBDS method which is the co-operate in active bait discovery method which use the Reverse mapping technique to create a effective to route to transfer the data from the node to the target and it avoid the data loss. Establishment of route can be made by the Dynamic source routing scheme.

Table 1: Differences between our work and previous works

Routing protocols	Main characteristics
Q-Routing	Considering the minimal delivery time to learn the best paths.
AdaR	Considering residual energy, hop count, aggregated ratio, and link reliability to learn an optimal routing strategy.
ATP	Considering metrics for energy-aware load balancing and congestion-aware routing to build an adaptive spanning tree.
FROMS	Considering hop costs to learn the best paths to multiple sinks.
QELAR	Considering residual energy and energy distribution among a group of nodes to learn the best paths.
DACR	Considering the knowledge on reliability and delay to learn the best paths.
FTIEE	Dividing nodes into clusters with different sizes and using RL to choose cluster heads; Taking the data retransmission scheme.
MRL-SCSO	Considering residual energy and buffer length to learn the best paths; Taking the sleep scheduling scheme.
RLBR	Considering the factors such as residual energy, link distance, and hop count to learn the best paths; Taking the schemes such as data packet carrying feedback and transmit power adjusting.

AdaR: adaptive routing; ATP: adaptive tree protocol; FROMS: feedback routing for optimizing multiple sinks; RLBR: reinforcement-learning-based routing protocol.

3. Proposed System

We propose a game-theory based clustering approach for wireless sensor networks. A game-theoretic model is built for CH selection. This paper adopts data replication to reduce possible network disconnection. The selection of a candidate CH is discussed under a second price sealed auction. Simulation results show that the throughput of the sink can still be guaranteed if any CH fails to work.

The proposed system incorporates both horizontal and vertical classification using linear regression. The sensor node locations correspond to the (x, y) co-ordinates. In case of horizontal classification, the line of regression is y = mx ? c where ‘y’ is the output variable that depends upon ‘x’.

4. Conclusion

In this paper they mainly propose the optimization of the secure data in the network protocol. The data can be transmitted from the source node and reaches the target. At the time of the data transmission the hackers can attack the node path and fetches the data. To avoid that they use the genetic algorithm which can make the data more optimized and secured the node from the attack of the malicious node. The processing time is less and the requirement of the additional path is made and energy consumption is also less. [10]

References

[1] NL-IDS: Trust Based Intrusion Detection System for Network layer in Wireless Sensor Networks Umashankar Ghugar, Jayaram Pradhan IEEE 2018.

[2] Analyzing the Vulnerability of Wireless Sensor Networks to a Malicious Matched Protocol Attack George D. O'Mahon, Philip J. Harris, Colin C. Murphy IEEE 2018.

[3] Abnormal-Node Detection Based on Spatio-Temporal and Multivariate-Attribute Correlation in Wireless Sensor Networks Nesrine Berjab, Hieu Hanh Le, Chia-Mu Yu, Sy-Yen Kuo, Haruo Yokota IEEE 2018.

[4] Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensor Networks Amjad Mehmood, Akbar Khanan, Muhammad Muneer Umar, Salwani Abdulla,

Khairul Akram Zainol Ariffin, Houbing Song IEEE 2018.

[5] Threshold Tuning-Based Wearable Sensor Fault Detection for Reliable Medical Monitoring Using Bayesian Network Model Haibin Zhang, Jiajia Liu, Nei Kato IEEE 2018.

[6] A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation Cong Pu, Sunho Lim IEEE 2018.

[7] Energy Efficient Detection-Removal Algorithm for Selective Forwarding Attack In Wireless Sensor Networks T.R Sreelakshmi, G.S Binu IEEE 2018.

[8] False Data Injection Prevention in Wireless Sensor Networks using Node-level Trust Value Computation B. Sreevidya, M. Rajesh IEEE 2018.

[9] A Comprehensive Trust-Aware Routing Protocol with Multi-Attributes for WSNs Boyuan Sun, Donghui Li IEEE 2018.

[10] A novel approach to avoid malicious attack to enhance network in WSN BY Guruprasanna Electronics and communication, MVJ College of engineering, Bengaluru, India in 2017

[11] Hussain, A., Manikanthan, S.V., Padmapriya, T. Nagalingam M. Wireless Networks (2019). https://doi.org/10.1007/s11276-019-02121-4 Genetic algorithm based adaptive offloading for improving IoT device communication efficiency, Wireless Networks, 2019.