IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Fault Detection Based on Round Trip Time in WSNs and Trust Value Based Correction

Jeethumol K Joy[1], Syamesh K G[2], Reshma Rajan[3], Saneesh P S[4]

M.Tech Student, Electronics and Communication, College of Engineering Kidangoor, Kottayam, India [1, 3, 4]

Assistant Professor, Electronics and Communication, College of Engineering Kidangoor, Kottayam, India [2]

Abstract: The Wireless Sensor Networks (WSNs) has many applications in our day today life. With the development of technologies it's uses also increases. But the chance of sensor node failure also increases. Hence for proper working of the system, detection and correction of such faulty node is essential. This paper deals with faulty node detection based on Round Trip Time.

Keywords: RTT, RTP, WSNs, Trust value.

I. INTRODUCTION

WSNs are networks with large number of sensor nodes deployed in a random pattern in a particular field or area to monitor the area. As in every network, WSNs also faces problems due to failure of the nodes in the network. A sensor node consists of a sensor, a processor, a radio transceiver and a power supply/ Battery. Failure of any of this units causes failure of the network. This paper deals with failure of the network due to malicious user attack. The malicious user or malicious node can be either dead or malfunctioning.

II. RELATED WORKS

The faulty sensor nodes detection suggested in [2] is based on comparisons between neighbouring nodes and dissemination of the decision made at each node. Malicious node cannot be detected using this algorithm. Cluster head failure recovery algorithm used in [3] includes transfer of cluster head and hence have data loss problem. Path redundancy technique to detect faulty sensor node is suggested in [4] and [5].

III.ROUND TRIP TIME

Round Trip Time(RTT)[1] is the time taken by a packet data to travel through a Round Trip Path(RTP)[1] and to come back to the sender node. Under normal condition, i.e., in the absence of any faulty node, each RTP value has a threshold RTT value. In the presence of a faulty node, the RTT value changes. The new RTT value is compared with the threshold value. By this comparison, the node common to the RTPs with higher RTT value is concluded as faulty node. The faulty node can be either dead(infinity RTT value) or malfunctioning(RTT value greater than the threshold value).

A. Round Trip Path

The fault detection is performed in a network with ten sensor nodes arranged in a circular topology. The RTPs are selected in such a way that each RTP contains three sensor nodes. And hence each node will be present in such three RTPs. To find whether a node is faulty, we have to compare only such three RTPs. If we form RTP with more than three nodes, a single node will be present as many RTPs as the number of nodes in the RTP. Hence comparison of all such RTPs is time consuming. So we select number of nodes as three for each RTP.

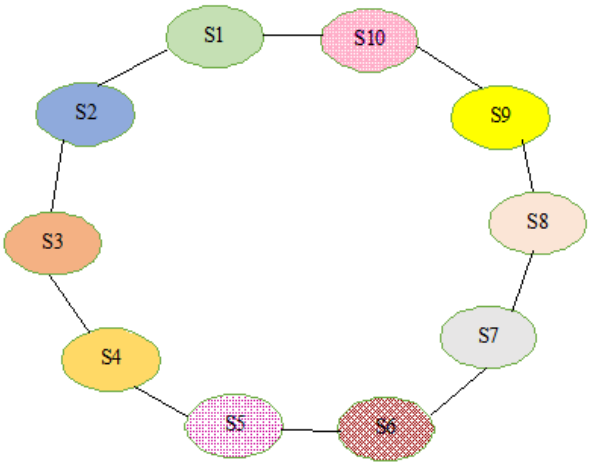

Fig. 1. Wireless Sensor Network with ten nodes

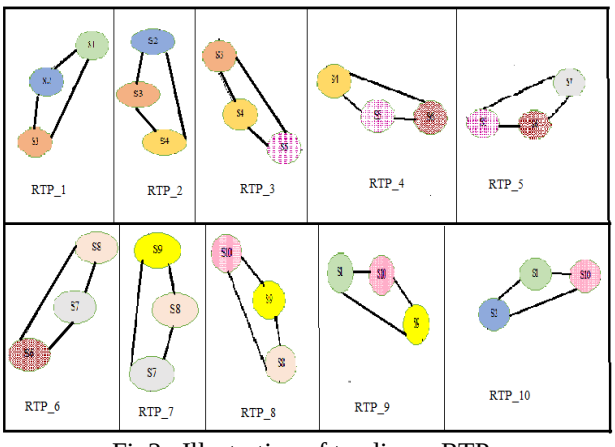

Fig2. Illustration of ten linear RTPs

DOI 10.17148/IJARCCE.2016.55180

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Figure 1 shows a network with ten sensor nodes and figure 2 shows the ten linear RTPs with three sensor nodes. A single node is present in three RTPs and comparison of such three RTPs is sufficient to detect the failure of a node.

B. Algorithm to Detect Failure Node

The threshold RTT value of RTP is calculated under normal condition. The RTT value in case of RTP_1 is the sum of delay time between each node pair, i.e., the taken from node 1 to 2 plus time from 2 to 3 plus time from 3 to 1. The RTT value in the presence of failure node is also calculated. The node common to the RTPs with RTT value greater than the threshold is detected as the faulty node.

In first stage, RTP_1 and RTP_2 are compared. If RTD time of RTP_2 is equal to threshold value and RTD of RTP_1 is greater than threshold, then S1 is malicious. If the RTD value is infinity, then S1 is dead else is malfunctioning. In second stage, RTP_2 and RTP_3 are compared provided RTD value of RTP_1 is greater than threshold. If RTD of RTP_2 is greater than threshold and RTP_3 is threshold, then S2 is malicious. If the RTD value is infinity, then S2 is dead else is malfunctioning.

In third stage, RTP_1, RTP_2 and RTP_3 are compared. If RTD value of all three RTPs are greater than threshold indicates that S3 is malicious. If the RTD value is infinity, then S3 is dead else is malfunctioning.

IV. CORRECTION

The proposed RTT based method detects the failure in the Wireless Sensor Network. Now, as we know, for the proper working of the network, the data from the failure node has to be discarded. But the network will not perform well by just discarding the data from such nodes. In order to overcome this, we have to find an alternate path for the data to be send through the faulty node. The alternate path is calculated based on the trust value[6].

The belief level one sensor node puts on another sensor node based on the behavior of previous observations is termed as trust value. The value ranges from 0 to 1. Trust value is of three types, direct trust, recommendation trust and indirect trust. Direct trust is calculated based on direct communication behaviors. The recommendations from third parties may not be always reliable. Hence filtered recommendations are termed as recommendation trust. Indirect trust are calculated when two nodes (sender and receiver) cannot send data directly, i.e., they are at multi-hop distance.

Here, since the nodes are at one-hop distance, we have to calculate only direct trust. Direct trust is calculated by considering communication trust, and energy trust. To calculate communication trust, we should know the behavior of sensor node. The communication channel between the nodes is subject to many factors and is not stable. Hence we cannot calculate communication trust based on previous observations. Therefore, we calculate it based on successful(s) and unsuccessful(f) packets.

$$T_{com}=(2b+u)/2$$

Where, b=s/(s+f+1), u=1/(s+f+1).

Energy is another important aspect for proper working of the sensor nodes. Each node is provided with a particular energy. When the energy level falls below a particular level, the node cannot be used in the network. The energy consumption of malicious node will be high. To calculate energy trust, we calculate the residual energy of nodes. The residual energy is dependent on the energy consumption rate. The energy consumption rate of malicious node is higher where as the rate of normal working nodes is steady. If the energy consumption rate is high, then the residual energy will be low and hence its energy trust will be less.

For every node, a threshold energy level is calculated. If the energy level of the node falls below this value, then the node becomes failure or can act as a malicious node. Hence the energy trust is calculated based on the residual energy.

$$T_{ene}= \begin{cases} 1-p_{ene}, & \text{if } E_{res} \geq \theta \\ 0, & \text{else} \end{cases}$$

Where T_{ene} is the energy trust and E_{res} is the energy consumption rate.

V. CONCLUSION

The failure detection based on RTT helps to detect the failure nodes in the Wireless Sensor Networks. This method is less time consuming compared to other fault detection mentioned in related works. This method can be tested in network with any number of nodes. The neighbor node with greater trust value is selected for the alternate path. Hence, the data is successfully transmitted throughout the network.

REFERENCES

[1] Ravindra Navanath Duche and Nisha P Sarwade, "Sensor Node Failure Detection Based on Round Trip Delay and Paths in WSNs", IEEE Sensor Journal, Vol.14. No.2, February 2014.

[2] M. Lee and Y. Choi, "Fault detection of wireless sensor networks," Comput. Commun., vol. 31, pp. 3469–3475, Jun. 2008.

[3] A. Akbari, A. Dana, A. Khademzadeh, and N. Beikmahdavi, "Fault detection and recovery in wireless sensor network using clustering," IJWMN vol. 3, no. 1, pp. 130–138, Feb. 2011.

[4] C.-C. Song, C.-F. Feng, C.-H. Wang, and D.-C. Liaw, "Simulation and experimental analysis of a ZigBee sensor network with fault detection and reconfiguration mechanism," in Proc. 8th ASCC, May 2011, pp. 659–664.

[5] A. Mojoodi, M. Mehrani, F. Forootan, and R. Farshidi, "Redundancy effect on fault tolerance in wireless sensor networks," Global J. Comput. Sci. Technol., vol. 11, no. 6, pp. 35-40, Apr. 2011.

[6] Jinfang Jiang, Guangie Han, Feng Wng, Lei Shu and Mohsen Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 26, no.5, May 2015.

[7] R. N. Duche and N. P. Sarwade, "Sensor node failure or malfunctioning detection in wireless sensor network," ACEEE Int. J. Commun., vol. 3, no. 1, pp. 57–61, Mar. 2012.

[8] H. Chan and A Perrig, "Security and privacy in sensor networks, Comput" vol. 36, no. 10, pp. 103–105, Oct. 2003.

[9] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical-based healthcare monitoring architecture in wireless heterogeneous sensor networks," IEEE J. Sel. Areas Commun., vol. 24, no. 7, pp. 400–411, May 2009.

[10] V. C. Gungor, L. Bin, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.