International Journal of Computer Networks and Communications Security

VOL. 3, NO. 2, FEBRUARY 2015, 27–32
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

A Fault Tolerant Approach for WSN Chain Based Routing Protocols

Ahmad Jalili[1], Sajad Homayoun[2] and Manijeh Keshtgary[3]

[1, 2] PhD Student in IT, School of Computer Engineering & IT, Shiraz University of Technology, Iran

[3] Assistant Professor, School of Computer Engineering & IT, Shiraz University of Technology, Iran

E-mail: [1]a.jalili@sutech.ac.ir, [2]s.homayoun@sutech.ac.ir, [3]keshtgari@sutech.ac.ir

ABSTRACT

Wireless Sensor Networks (WSNs) have been applied in variety of industrial, medical and military applications. There are many routing protocols proposed for WSNs to deal with challenges such as energy depletion and latency of data transmission from nodes to base station. Recently, researchers have focused on Chain-based protocols. CCBRP (Chain-Chain Based Routing Protocol) tries to decrease both energy consumption and latency time, but it has some challenges such as randomness in choosing of chain leaders and not supporting of any fault tolerant mechanism. Due to energy depletion and mobility of nodes, nodes failure is unavoidable in WSNs. However, few protocols considered fault tolerant mechanisms while fault tolerant routing is a critical task in WSNs in dynamic environments to improve network reliability. In this paper, we aim to employ fault tolerant mechanism in CCBRP. We propose an approach to prevent early failures of chains in wireless sensor grid networks. The approach is modeled by Markov chain and the results show more reliability for our approach than simple CCBRP.

Keywords: *WSNs, CCBRP Routing Protocol, Fault Tolerant Systems, Markov Chain.*

1 INTRODUCTION

One of the applications of WSNs is environment monitoring such as monitoring weather, physical or chemical conditions in an area [1, 2].

A sensor node has limited energy (battery) and it is very difficult to recharge them so the node can be faulty due to loss of power or other physical defects such as circuit malfunction, processor failure and unavailable radio links. Therefore, Fault tolerant property is an important issue in WSNs.

Grid-based deployment is an attractive approach for moderate to large-scale coverage oriented deployment due to its simplicity and scalability [3]. There are some applications for grid-based networks such as military and agriculture.

There are many routing protocols in ad-hoc environments but few of them have any idea to make the network more reliable. They usually concentrate on one of two important issues: 1) Energy conservation and 2) Data delivery time reduction. Some protocols such as Chain-Chain Based Routing Protocol (CCBRP) try to focus on both energy and data delivery time in parallel. These protocols are appropriate in environment where sensor nodes are positioned as a grid and there are several chains in WSNs [4].

Moreover, chain based routing protocols show more optimized results in large-scale WSN based applications. For instance, CCM (Chain-Cluster based mixed routing) is another protocol [5] that proposes a routing algorithm which tries to make the best use of LEACH and PEGASIS, and provide improved performance.

In general, chain based algorithms divide network into chains and the process of data transmission has two phases of chain routing and cluster routing.

Since chain based algorithms try to optimize energy consumption and decrease delay, there are many researches related to routing protocols in WSNs. However, few of them considered missing of nodes (and fault toleration mechanism) that is an important issue in WSNs. The network will fail if a chain is unable to deliver its data to the base station (however it depends on the definition of failure in

the network). A fault tolerant design enables a system to continue its intended operation, possibly at a reduced level, rather than failing completely, when some part of the system fails [6].

In this article, we add fault tolerant mechanism to CCBRP by replacing failed nodes with another node and deliver data to the base station.

The rest of this paper is organized as follows: Section 2 covers a brief review on related works. Section 3 describes some preliminaries. The details of our proposed fault tolerant approach are explained in section 4. Section 5 provides a performance evaluation on proposed approach and section 6 concludes the paper.

2 RELATED WORK

In This section, a brief review on prior studies related to fault tolerant routing protocols are presented. A fault-tolerant clustering protocol in WSNs is proposed in [7]. It is a run-time recovery mechanism based on participation of healthy gateways to detect and handle faults in faulty gateways. The proposed protocol runs in two phases of detection and recovery. It uses Status messages for detecting faults and once the gateways find a fault, the next step is to identify the type of faults and allocate other sensors to replace the failed gateway node. In clustering protocols, each cluster needs a high-energy node called gateway as cluster-head. However, sometimes there is no high-energy node available and all nodes are the same. Therefore, fault-tolerant clustering is impossible in these situations.

Hazarath [8] proposed the first Fault Tolerant Trajectory Clustering (FTTC) that is a technique for selecting cluster heads in WSNs based on traffic.

Missing of the nodes located near base stations or cluster heads is a main issue in WSNs (because of energy depletion etc.). Hazarath tried to extend network lifetime by introducing a method for selecting of cluster heads. Their method aims to increase the lifetime of nodes located near base stations or cluster heads. The algorithm selects the cluster heads based on traffic and rotates periodically. The proposed algorithm has no idea for network recovery and there is no fault tolerant mechanism for nodes other than cluster heads.

In [9], Samia and Shreen introduced an approach where fault tolerant is consolidated for chain based routing protocols. They proposed two techniques of fault detection and recovery in chain based routing protocols. Fault detection mechanisms are the same for both techniques. Each sensor node in every chain identifies whether its successor neighbor in its chain is faulty by NOTIFY messages and READY messages. However, they proposed two different strategies for fault recovery phase. The first technique overcomes faults through passing faulty node and uses its successor instead. The second technique chooses a backup node from its closest neighboring chain (to the base station). However, the reliability of proposed protocol is not evaluated.

3 PRELIMINARIES

This section describes a review on an efficient routing protocol called CCBRP (Chain-Chain based routing protocol). CCBRP achieves both minimum energy consumption and minimum delay [3]. It divides the WSN into a number of chains; and it uses Greedy algorithm to construct each of the chains as in PEGASIS. Each chain contains a number of sensor nodes, the number of chains and sensor nodes in each chain depend on the number of sensor nodes in the WSN under consideration.

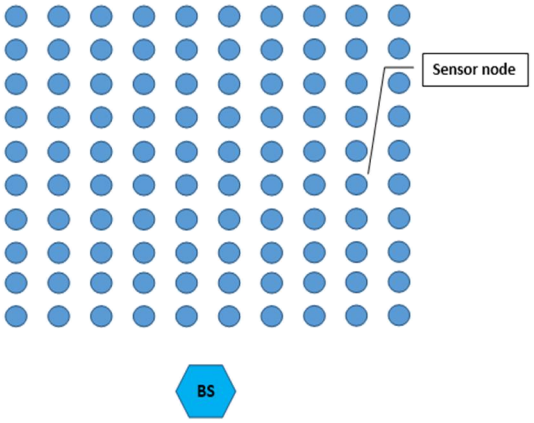


Fig. 1. 100 Sensor nodes in WSNs, divided into 10 chains each chain contains 10 sensor nodes.

To illustrate the CCBRP, consider a WSN with N sensor nodes distributed in a 2-dimension area having a size of L(m)×L(m). If N is 100 nodes and each chain has 10 sensor nodes, there are ten chains as shown in Fig. 1.

The CCBRP protocol forms each of the partitioned chains using Greedy algorithm and runs in two phases. The first phase starts by randomly select a leader for each chain (Chain Leader: CL), and then each CL sends a token message to the two ends of its chain to notify them. Afterwards, each end node in chain simultaneously starts sending its data to its closet neighbor node, the neighboring nodes receive data and fuse its data along with the received data and send to the next node in the chain and so on. This process repeats until the data has reached all the CL nodes.

The second phase of CCBRP starts after all the CL nodes have received all the data from their chain nodes. These CL nodes form a chain (using Greedy algorithm) and randomly choose a CL for the newly formed chain. Then the randomly chosen leader sends a token message to the two ends of the newly formed chain. Thereafter, each of the two nodes at the two ends of the formed chain of leaders simultaneously starts sending its data to its closest neighboring node. The neighboring nodes receive the sent data, merge their data with the received data, and send to the next neighboring nodes and so on. This process of sending data is repeated until all the data of the WSN received by the leader node of the chain of CLs. After the node leader of leaders received the data, it merges them with its own and sends them to the BS. Fig. 2 illustrates the data transmission for the proposed CCBRP.

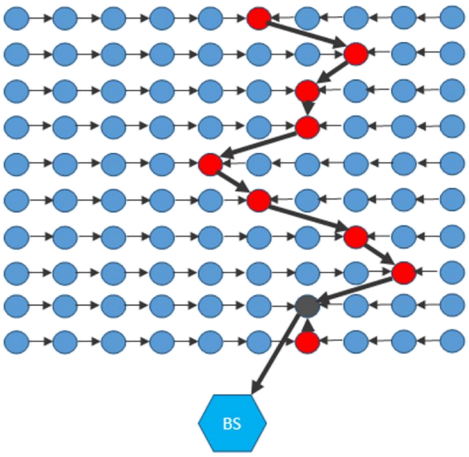


Fig. 2. Data transmission in CCBRP protocol

4 PROPOSED FAULT TOLERANT APPROCH

Reliability R (t) of a system at time t is the probability that the system operates without failure in the interval [0; t], given that the system was performing correctly at time 0[10]. λ is the failure rate that is the expected number of failures per unit time. During the useful life phase of the system, failure rate function is assumed to have a constant value λ. Then, the reliability of the system varies exponentially as a function of time: $R(t) = e^{-\lambda t}$.

This section presents the proposed strategies for supporting fault tolerant feature in CCBRP. As mentioned, CCBRP works in two phases. In phase one, the protocol chooses Chain Leaders (CL) in a random manner and hence other nodes in the same chain direct their data to the CL. Each CL tries to send data to the next CL and finally the data expected to receive by BS. As mentioned earlier, CCBRP randomly chooses CLs. Accordingly, this randomness can cause some problems in such cases in which a chain leader located too far to the next CL and CLs are not in the transmit range of each other. In this paper when a CL cannot find the next CL (because of such reasons as long distance, node failure, energy depletion etc.), nearest node will be considered as the CL of the next chain. The process of choosing replacement has two possibilities; 1) The CL is located in the middle of the chain and 2) it is located in the left or right fringes of the network.

4.1 Reliability Analysis for Middle Node CL (MNCL)

In this section, the reliability of a CL that located in the middle of a chain is modeled by Markov chain. As shown in Fig. 3, if CL1 cannot find CL2, CL1 tries to select one of its closest neighbors (they are Hot Spare) in the next chain as CL2 and direct data to it. The four states Markov chain of a MNCL is shown in Fig. 4, and table I describes each state.

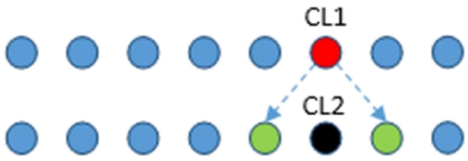


Fig. 3. Middle Node Chain Leader (MNCL)

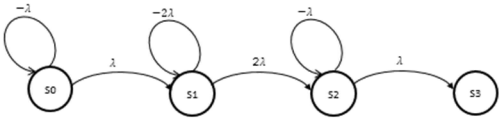


Fig. 4. Markov chain of MNCL

Table 1: States Description of Figure 4

State	Situation	Description
S0	Operational	CL1 successfully finds CL2
S1	Operational	CL2 failed and CL1 successfully choose a neighbor as CL2
S2	Operational	CL2 failed and first closest neighbor failed, so CL1 successfully choose a neighbor as CL2
S3	Failed	CL2 failed, both closest neighbors of CL1 failed

The transition matrix is shown in Figure 5.

$$\frac{d}{dt}\begin{bmatrix}P_0\\P_1\\P_2\\P_3\end{bmatrix}=\begin{bmatrix}-\lambda & 0 & 0 & 0\\ \lambda & -2\lambda & 0 & 0\\ 0 & 2\lambda & -\lambda & 0\\ 0 & 0 & \lambda & 0\end{bmatrix}\begin{bmatrix}P_0\\P_1\\P_2\\P_3\end{bmatrix}$$

Fig. 5. The transition matrix for Figure 4

And the differential equations which describe the fault tolerance CCBRP Markov is shown in Figure 6.

$$\begin{cases}\dfrac{dP_0(t)}{dt}=-\lambda P_0(t)\\ \dfrac{dP_1(t)}{dt}=\lambda P_0(t)-2\lambda P_1(t)\\ \dfrac{dP_2(t)}{dt}=2\lambda P_1(t)-\lambda P_2(t)\\ \dfrac{dP_3(t)}{dt}=\lambda P_2(t)\end{cases}$$

Fig. 6. The differential equations of Figure 5

Where $P_i(t)$ denotes the probability of being in state 1 at time t, and $\frac{dP_i(t)}{dt}$ represents the first order derivative of$P_i(t)$. The above simultaneous differential equations are solved by Laplace transforms as Figure 7.

$$\begin{cases}sP_0(s)-P_0(0)=-\lambda P_0(s)\\ sP_1(s)-P_1(0)=\lambda P_1(s)-2\lambda P_1(s)\\ sP_2(s)-P_2(0)=2\lambda P_1(s)-\lambda P_2(s)\\ sP_3(s)-P_3(0)=\lambda P_2(s)\end{cases}$$

Fig. 7. The solved differential equations

Where P3(s), P2(s), P1(s), and P0 (s) are the Laplace transforms of p3 (t), p2 (t), p1 (t), and p0 (t), respectively. We assume that the system starts out in perfect shape at time t = 0, and so, p3 (0) = 1, and p2 (0) = p1 (0) = p0 (0) = 0. The Laplace transforms can be written as:

$$\begin{cases}P_0(s)=\dfrac{1}{s+\lambda}\\ P_1(s)=\dfrac{\lambda}{(s+\lambda)(s+2\lambda)}\\ P_2(s)=\dfrac{2\lambda^2}{(s+\lambda)^2(s+2\lambda)}\end{cases}$$

Fig. 8. The transformation of Laplace

Fig. 9 shows solved differential equations where Pi(t) denotes the probability of being in state 1 at time t.

$$\begin{aligned}&P_0(t)=e^{-\lambda t}\\ &P_1(t)=e^{-\lambda t}-e^{-2\lambda t}\\ &P_2(t)=-2\lambda^2e^{-\lambda t}-2\lambda^2e^{-2\lambda t}+2\lambda^2te^{-\lambda t}\\ &P_3(t)=1-(P_0(t)+P_1(t)+P_2(t))\\ &=1-(2e^{-\lambda t}-e^{-2\lambda t}-2\lambda^2e^{-\lambda t}+2\lambda^2e^{-2\lambda t}+2\lambda^2te^{-\lambda t})\end{aligned}$$

Fig. 9. Laplace transformation for MNCL

Finally, the reliability of MNCL for one chain in fault tolerance CCBRP protocol when transmit data is shown in equation (1).

$$R_{MNCL}=1-P_3(t)=(2e^{-\lambda t}-e^{-2\lambda t}-2\lambda^2e^{-\lambda t}+2\lambda^2e^{-2\lambda t}+2\lambda^2te^{-\lambda t}) \quad (1)$$

4.2 Reliability Analysis for the Fringe Nodes CL (FNCL)

Fig. 10 shows a FNCL in a chain. Here, one closest neighbor (Hot Spare) from next chain selected as replacement of CL2.

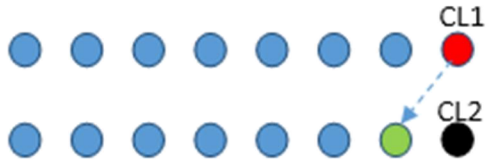


Fig. 10. Fringe Node Chain Leader (FNCL)

Fig. 11 shows the Markov chain of a FNCL and Table II describes the states.

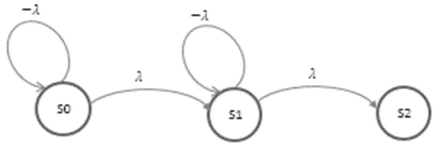


Fig. 11. Markov chain of a FNCL

Table 2: States Description of Fig.10

State	Situation	Description
S0	Operational	CL1 successfully finds CL2
S1	Operational	CL2 failed and CL1 successfully choose the closest neighbor as CL2
S2	Failed	CL2 failed and the closest neighbor failed

Solved differential equations is shown in Fig. 12 where Pi(t) denotes the probability of being in state 1 at time t.

$$P_0(t) = e^{-\lambda t}$$
$$P_1(t) = \lambda t e^{-\lambda t}$$
$$P_2(t) = 1 - (e^{-\lambda t} + \lambda t e^{-\lambda t})$$

Fig. 12. Laplace transformation for FNCL

Finally, reliability of a chain FNCL in fault tolerant CCBRP is as equation (2).

$$R_{FNCL} = 1\text{-}P_2(t) = (e^{-\lambda t} + \lambda t e^{-\lambda t}) \qquad (2)$$

4.3 Reliability Analysis of WSN

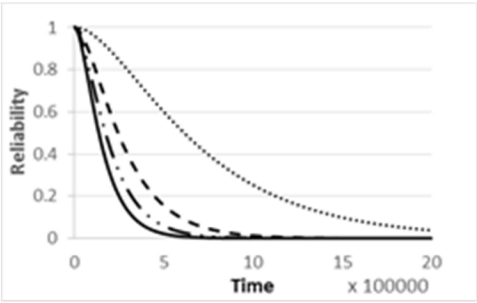
There are different definitions of reliability in a network. For example, one defines network failure as the failure of a single chain as inability to make a connection to the next chain. Others may define failure of the network after failing of threshold number of nodes. In this paper, failure is defined as inability of a CL to send its chain data to the next CL. Consequently, since chains located in a serial manner, the reliability of a WSN is the multiplication of all CLs reliabilities (CL reliability is either MNCL or FNCL) as shown in Equation (3):

$$R_{total} = R_{12} * R_{23} * R_{34} * \ldots * R_{(n-1)n} \qquad (3)$$

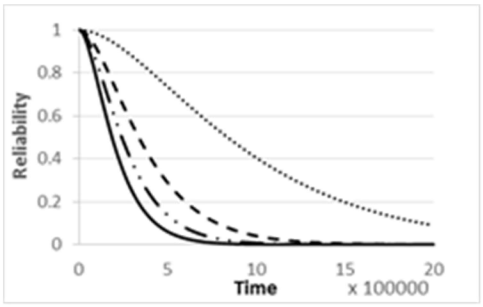
We assume each node in a chain can successfully deliver its data to the CL. In other words, if a node (other than CL) failure occurs, the protocol can handle it by the mechanisms proposed in [8].

5 PERFORMANCE EVALUATION

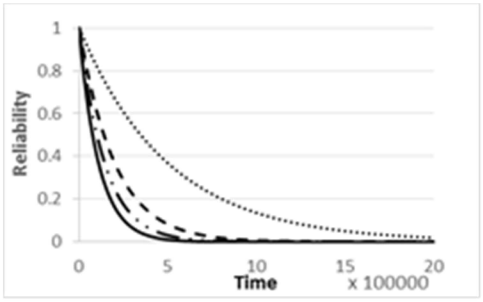
In this section, the reliability of each FNCL and MNCL is calculated by equations (1) and (2), and the reliability of simple CCBRP is achieved by calculating $R(t) = e^{-\lambda t}$. Figure 13 shows the results for different λ values.



(a)



(b)



(c)

Fig. 13. The reliability of a) MNCL b) FNCL c) simple CCBRP. For different λ values.

As Fig. 13 (c) shows, it is clear that MNCL and FNCL approaches are more reliable than simple CCBRP for different λ values.

5.1 Case Study

Consider a WSN consist of 100 nodes is organized in 10 chains as in Fig. 14. The first phase of CCBRP (random selection of CLs) has done and CLs of each chain is marked.

The reliability of the WSN is according to equation (4).

$$R_{total} = R_{12} * R_{23} * R_{34} * R_{45} * R_{56} * R_{67} * R_{78} * R_{89} * R_{910} \qquad (4)$$

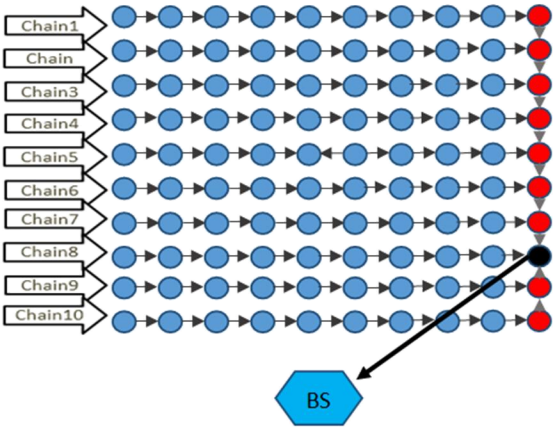


Fig. 14. A typical WSN with 10 chains

Rij shows the reliability for CL node located in chain i. Depending on CL type (MNCL or FNCL) the Rij must be replaced with either RMNLC or RFNLC.

For comparing proposed approach to simple CCBRP, we consider a network in which all chain leader (CL) nodes are FNCL (because FNCLs have less spare than MNCLs), hence the worst reliability of our approach is expected. Fig. 14 shows that the reliability of proposed approach is higher than simple CCBRP for considered case. In other words, it is more reliable than simple CCBRP even in situations in which all CLs are located in the fringes (the worst case).

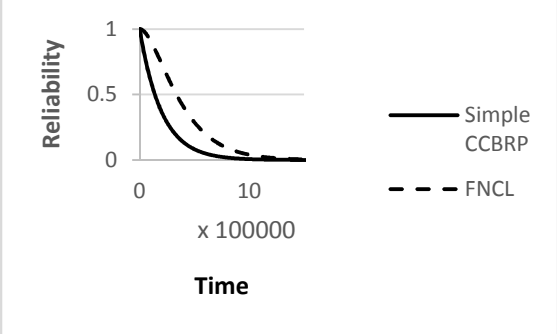


Fig. 15. Reliability of FNCL and simple CCBRP

6 CONCLUSION

Failing of sensor nodes is unavoidable in WSNs due to a variety of reasons including power depletion, circuit malfunction, processor failure and unreliable radio links. There are many routing protocols in ad-hoc environments, but few of them have any idea for making more reliable networks. They usually tried to focus on energy conservation or reducing data delivery time. CCBRP is a chain-based protocol that tries to decrease both energy consumption and data delivery time. It does not support any fault tolerant mechanism. In this paper, we aimed to reach higher reliability and prevent network partitioning by proposing a fault tolerant approach to inhibit early failures of chains in wireless sensor grid networks. The approach is modeled by Markov chain and the results shows that CCBRP by using MNCL and FNCL is more reliable.

7 REFERENCES

[1] Akyildiz I. F., Su W., Sankarasubramaniam Y. and Cayircl E., A survey on sensor networks, in: Proceedings of the IEEE Communication Magazine, Vol. 40, pp. 102-114, August 2002.

[2] Ilyas M. and Mahgoub I., Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, in: Proceedings of the CRC Press, London, Washington, D.C., 2005.

[3] Sharma, A. K. (2010). Comparative study of energy consumption for wireless sensor networks based on random and grid deployment strategies.

[4] Ali S. and Refaay S., Chain-Chain Based Routing Protocol, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, pp. 1694-0814, May 2011.

[5] Tang F., You I., Guo S., Guo M, MaA Y., chain-cluster based routing algorithm for wireless sensor networks, J Intell Manuf, 2012.

[6] Johnson and B. W. Fault-Tolerant Microprocessor-Based Systems, IEEE Micro, Vol. 4, Issue 6, pp. 6-21, 1984.

[7] Gupta G. and Younis M., Fault-Tolerant Clustering of Wireless Sensor Networks, Proc. IEEE Wireless Comm. and Networking Conf. Vol. 3, pp.1579–1584,2003.DOI: http://dx.doi.org/10.1109/WCNC.2003.1200622.

[8] Hazarath M., A Fault Tolerant Trajectory Clustering (FTTC) for selecting cluster heads in wireless sensor networks, International Journal of Computational Intelligence Research (IJCIR), Vol. 6, Issue 3, pp. 359-372, 2010.

[9] Samia A. Ali and Shreen K. Refaay, Chain Based Fault Tolerant Routing Protocols. Network Protocols and Algorithms Vol. 4. Issue 3, pp. 79-103, 2012.

[10] Dubrova E., Fault-Tolerant Design, Springer, 2013.