C3IT-2012

Transient Fault Tolerant Wireless Sensor Networks

Arunanshu Mahapatroa, Pabitra Mohan Khilar

*a, b National Institute Technology, Rourkela, India

Abstract

Intermittent and transient faults are the largest source of failure for sensor networks. In order to provide a method for detecting permanent, intermittent and transient faults, a distributed detection algorithm is developed. This algorithm uses repeated testing in discrete time and considers the case of system level faults. It subsumes several algorithms already reported in the literature. Simulation result shows that the false detection rate is well under control while maintaining high detection accuracy.

© 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of C3IT
Open access under CC BY-NC-ND license.

Keywords: Fault detection; WSN; transient faults.

1. Introduction

A considerable amount of research effort has been focused toward the development of algorithms to detect faults that may occur in sensor networks. However, this effort has been limited almost completely to the study of permanent faults in sensor networks. The problem of transient and intermittent fault detection has been largely overlooked. This paper attempts to fill this research gap by developing a complete fault detection framework which is shown to be robust in detecting permanent, intermittent and transient faults. Permanent faults are the ones that are continuous and stable in time and produce errors when they are fully exercised. An intermittent fault originates from inside the system when software or hardware is faulty. After their first appearance, they usually exhibit a relatively high occurrence rate and, eventually, tend to become permanent. On the other hand, transient faults caused by external agents like electromagnetic radiation, heat, etc. and normally, their adverse effects rapidly disappear. Since most malfunctions derive from transient faults, if they do not occur too frequently, removing the affected sensor nodes would not be the best solution for most systems [1]. By its nature, intermittent and transient faults will not occur consistently, which makes its diagnosis a probabilistic event over time [2]. Since the effect of fault is not always present, detection of intermittent and transient faults require repetitive testing at the discrete time contrary to single test requirement for permanent fault detection.

These issues motivate to explore a complete distributed fault detection algorithm for sensor networks. The specific contributions of this paper are listed below:
• Proposes a generic detection scheme that identifies permanent and intermittent faults with high accuracy by maintaining low time, message and energy overhead.
• Proposes a mechanism to discriminate intermittent from transient faults.

In this work, each sensor node makes a decision based on comparison between its own reading and readings of its 1-hop neighbours. The sensor node is detected as fault free if the sensor reading agrees with readings of more than \( T_h \) neighbours where \( T_h \) is a threshold.

The problem of identifying faulty nodes (crashed) in WSN has been studied in [4]. This article proposes the WINdiag diagnosis protocol which creates a spanning tree (ST) for dissemination of diagnostic information. Thomas et al. [5] have investigated the problem of target detection by a sensor network deployed in a region to be monitored. The performance comparison was performed both in the presence and in the absence of faulty nodes. Luo et al. [6] proposed a fault-tolerant detection scheme that explicitly introduces the sensor fault probability into the optimal event detection process where the optimal detection error decreases exponentially with the increase of the neighbourhood size. In [7] the authors present a distributed fault detection model that uses time redundancy to tolerate transient faults in sensing and communication. The fault detection accuracy of a detection model would decrease rapidly when the number of neighbour nodes to be diagnosed is small and the nodes failure ratio is high. In [8], the authors have addressed this problem by defining new detection criteria. Krishnamachari et al. have presented a Bayesian fault recognition model to solve the fault-event disambiguation problem in sensor networks [9]. In [10], the authors have proposed time redundancy to diagnose intermittent fault in sensing and communication of a sensor network. They assume that each sensor has at least 3 neighbouring nodes which may not be always possible for sparse networks.

2. System Model

The system under consideration accommodates \( n \) number of nodes. Each node occupies a position \((x, y)\) inside of a fixed geographic area \((l \times l \, m^2)\). Two nodes \( v_i \) and \( v_j \) are within transmission range \( R_{tx} \) if the Euclidean distance \( d(v_i, v_j) \) is less than \( R_{tx} \). The topology graph \( G = (V, E) \) consists of a set of vertices \( V \) representing the nodes of the network and the set \( E \) of undirected edges corresponding to communication links between nodes. The proposed model is based on the following realistic assumptions:

1. Faults may occur intermittently or may be permanent.
2. Faults are investigated only though tests based on comparisons of sensor reading between neighbouring nodes where test are scheduled at periodic time \( k.T \) (\( k = 1, 2, \ldots \)) for a fixed \( T \).
3. Test is not perfect; a fault is detected by the test with probability \( 1 - P_e \) and not detected with probability \( P_e \).
4. Links are symmetric, i.e., two nodes \( v_i \) and \( v_j \) can communicate using the same transmission power level.

The proposed model considers both hard and soft faults. If a node is hard faulty, the sensor node is unable to communicate. A soft faulty node continues to operate and communicate with altered behaviour. Both the hard and soft faults may appear intermittently.

3. Fault Detection Algorithm

This work follows the general principle of diagnosis algorithms where working nodes perform their own independent diagnosis of the system. Initially only permanent is assumed. However, this assumption is relaxed in the subsequent sections. The two performance metrics namely detection accuracy (DA) and false detection rate (FDR) are used to evaluate the performance of the proposed algorithm. DA is defined as the number of faulty sensor nodes detected to the total number of faulty sensor nodes in the network. FDR is defined as the ratio of number of fault free sensor nodes detected as faulty to total number of fault free nodes in the network.
3.1. Permanent Fault Detection

At each communication round each node broadcasts its own sensor reading. The detection algorithm uses timeout mechanism to detect hard faulty nodes. In the proposed model every node maintains a neighbour set $N$. The node $v_i$ declares node $v_j \in N_i$ as hard faulty, if $v_i$ does not receive the sensor reading from $v_j$ before $T_{out}$. $T_{out}$ should be chosen carefully so that the entire fault free nodes $v_j \in N_i$ connected by fault free channels $E_{ij}$ must report node $v_i$ before $T_{out}$. For each fault free sensor node its neighbouring fault-free sensor nodes have broadcasted similar sensor reading. Let $v_i$ be neighbour of $v_j$, $x_i$ and $x_j$ are the sensor readings of $v_i$ and $v_j$ respectively. In this work $x_i$ is similar to $x_j$ when $|x_i - x_j| < \delta$ where $\delta$ is application dependent. An arbitrary node $v_i$ receives the sensor reading from neighbouring nodes and form a set $\{E\} \subset \{N_i\}$ of nodes with similar reading $x$. Node $v_i$ then compares its own reading $x_i$ and take a decision on the basis of agreement and disagreement. The node $v_i$ is detected fault free if reading $x_i$ agrees with $x$ and the cardinality of set $\{E\}$ is greater than $T_h$ else $v_i$ is marked as possibly soft faulty. The optimal value for $T_h$ is $0.5(|N_i| - 1)$ [9] where $|N_i|$ is the number of 1-hop neighbours. This decision is then broadcasted.

Intermittent and Transient Fault Detection.

Once intermittent or transient fault is activated in a sensor node, faults are observable for a period before they disappear. Eventually, errors will reappear after fault disappearance duration either because of permanent faults or correlated intermittent faults. If a test is applied to a node and the node fails the test then three conclusions are possible: the node is either permanent faulty or intermittent faulty or transient faulty. In order to discriminate the type of fault, the test need to be applied in discrete time where the test is execution of permanent fault detection algorithm discussed earlier. This can be explained as follows:

- If a test is applied to a node with a transient fault and the node fails then the test may lead to reduction of system availability and impacting reliability.
- If a test is applied to a node with an intermittent fault and the node fails the test then the intermittent fault is detected. If the node passes the test, two conclusions are possible: (1) the node is fault-free, or (2) the circuit has an intermittent fault but the fault is not active at the time of test. If at any time in the repetition process, the fault appears, then the intermittent fault is detected.
- A node is detected as permanent (soft) faulty if the node fails consecutive tests.

In this work test are scheduled at periodic time $k.T$ ($k=1, 2, \cdots$) for a fixed $T$. As discussed earlier a node with intermittent fault, after the first fault appearance, it exhibit a relatively high occurrence rate. Thus this work assumes Weibull distribution for fault appearance duration and exponential distribution for fault disappearance duration. Without loss of generality exponential distribution is assumed for both fault appearance and disappearance duration for transient fault. Once the fault appears and detected by the applied test pattern, the identified node enters to observation stage. A node in observation stage is restricted from doing any network activities. Once the node has entered to observation stage, the inter fault appearance period $T_i$ ($i=0, 1, 2,\ldots$) is used to discriminate transient from intermittent fault. For intermittent faulty nodes it is expected that $T_{i+1}$ is less than $T_i$. In this work if $T_{i+1} < T_i$, then the algorithm increases the confidence level of being intermittent faulty (CL) by a factor 1. On the other hand, if $T_{i+1} \geq T_i$, then the algorithm reset the confidence level of being intermittent faulty to zero. The node is isolated if the confidence level crosses a predefined threshold $T_{h1}$. 
Algorithm 1.

Step 1: Test are scheduled at periodic time $k.T (k = 1, 2, \cdots)$ for a fixed $T$. Upon the first appearance of a fault the node enter to observation state.

Step 2: If $T_{i+1} < T_i$, then $CL=CL+1$.
If $T_{i+1} \geq T_i$, then $CL=0$.

Step 3: If $CL \geq T_{hi}$, then node is intermittent faulty and is isolated.

4. Performance Evaluation

In order to evaluate the performance of the proposed work, we chose to conduct an extensive set of simulations using the OMNET++ simulator. For simulation purpose a communication scenario has been generated with simulation parameters as summarized in Table 1, where nodes were randomly distributed. We chose random sets of 100 faulty nodes. For intermittent fault the mean value of fault appearance and disappearance duration is considered 50ms and 1 hour respectively. The fault disappearance duration is assumed to follow a Weibull distribution with increasing failure rate ($\beta = 1.5$). For transient fault the mean value of fault appearance and disappearance duration is considered 50ms and 10 hour respectively.

Table 1: Simulation Parameters

| Parameter      | Value                           |
|----------------|---------------------------------|
| Number of sensors | 1000                           |
| Network grid    | From (0, 0) to (1000, 1000)    |
| Sink           | At (75,150)                     |
| $T_{out}$       | 30µsec.                         |

Fig. 1. FDR for a scenario with only transient faults.

Fig. 1. shows the important performance measures for the fault detection algorithm. These results are obtained for a scenario where all faults are assumed to be transient. The key conclusion from this plot is that a better control over FDR is achieved with increase in $T_{hi}$. This work suggests $T_{hi} = 10$ such that intermittent fault is efficiently discriminated from transient fault. To validate this we choose a scenario where number of intermittent and transient faults is randomly chosen while maintaining total fault count equals to $n \times p$ where $p$ is the fault rate range from 0.05 to 0.3. The robustness of the detection algorithm to varying fault rates is analyzed by estimating DA and FAR. As expected and shown in Fig. 2 the detection accuracy decreases with increase in fault rate. An improvement in DA is observed for higher average node degree ($d$). Due to the expected high node degree in sensor networks, the proposed algorithm shows a better performance in regard to DA. Fig. 3 depicts the FDR at varying fault rate. For performance evolution we assume the number of intermittent and permanent faults do not change during
the simulation period. Note that this assumption does not mean that the detection algorithm is not adaptive to change in fault type and fault rate.

Fig. 2 DA with $d = 4$ and $d = 12$ for a network considering only intermittent and transient faults

Fig. 3 FDR with $d = 4$ and $d = 12$ for a network considering only intermittent and transient faults

5. Conclusions

We have proposed a robust fault detection algorithm for wireless sensor networks. The robustness of the detection algorithm in discriminating intermittent and transient faults in communication is investigated. This algorithm detects faults with high accuracy for a wide range of fault rate. Due to high detection accuracy, low false detection rate and reduced complexity the algorithm could be integrated to fault tolerant wireless sensor networks.

References

1. A. Bondavalli, S. Chiaradonna, F. Di Giandomenico, and F. Grandoni, “Threshold-Based Mechanisms to Discriminate Transient from Intermittent Faults,” IEEE Transactions on Computers, vol. 49, no. 3, pp. 230-245, Mar. 2000.
2. M. Barbata, A. Dahbura, and M. Malek, “The consensus problem in fault-tolerant computing,” ACM Computing Survey, vol. 25, pp. 171–220, June 1993.
3. A. Mahapatro and P. M. Khilar, “SDDP: Scalable Distributed Diagnosis Protocol for Wireless Sensor Networks,” International Conference on Contemporary, Springer, pp. 69-80, 2011.
4. T. Clouqueur, K. Saluja, and P. Ramanathan, “Fault tolerance in collaborative sensor networks for target detection,” IEEE Transactions on Computers, vol. 53, no. 3, pp. 320 – 333, mar. 2004.
5. X. Luo, M. Dong, and Y. Huang, “On distributed fault-tolerant detection in wireless sensor networks,” IEEE Transactions on Computers, vol. 55, no. 1, pp. 58 – 70, jan. 2006.
6. M.-H. Lee and Y.-H. Choi, “Fault detection of wireless sensor networks,” Computer Communications, vol. 31, no. 14, pp. 3469 – 3475, 2008.
7. P. Jiang, “A new method for node fault detection in wireless sensor networks,” Sensors, vol. 9, no. 2, pp. 1282–1294, 2009.
8. B. Krishnamachari and S. Iyengar, “Distributed bayesian algorithms for fault-tolerant event region detection in wireless sensor networks,” IEEE Transactions on Computers, vol. 53, no. 3, pp. 241 – 250, mar. 2004.
9. X. Xu, W. Chen, J. Wan, and R. Yu, “Distributed fault diagnosis of wireless sensor networks,” in 11th IEEE International Conference on Communication Technology, nov. 2008, pp. 148 –151.
10. P. Khilar and S. Mahapatra, “Intermittent fault diagnosis in wireless sensor networks,” in Information Technology, (ICIT 2007). 10th International Conference on, dec. 2007, pp. 145 –147.