Node-failure Tolerance of Topology in Wireless Sensor Networks

Liang-Min Wang[1], Jian-Feng Ma[2], and Yuan-Bo Guo[3]

(Corresponding author: Liang-Min Wang)

The Computer School, Jiangsu University, Zhenjiang, 212013, China[1]
Key Laboratory of Computer Network and Information Security of Education Ministry,[1,2]
Xidian University, Xi'an Shaanxi, P.R. China, 710071
School of Electronic Technology, Engineering University of PLA, Zhengzhou, 450004, China[3]
(Email: liangminwang@hotmail.com)

(Received March. 08, 2006; revised Apr. 24, 2006, and accepted June 12, 2007)

Abstract

Three basic questions are presented and answered in researching on node-failure topology in wireless sensor network. First, what is the definition of node-failure tolerance? Second, how to evaluate this tolerance ability? Third, which type of topologies is more efficient in tolerating node-failure?

Keywords: Intrusion tolerance system, tolerance ability, wireless sensor networks

1 Introduction

Wireless sensor networks usually were deployed in remote and hostile surroundings, and people cannot attend the sensor nodes. When some nodes are failure, such as batteries exhausted, hardware faulted and intrusion from attackers, these unattended nodes cannot be changed or repaired. The failure nodes may lead to network partition which decreases the cover ratio, reduces the availability of the network and even produces network failure. So network topology should tolerate node-failure to avoid network partition. We think the following three questions should be answered when researching node-failure tolerance of wireless sensor networks.

1) What is the definition of node-failure tolerance for topology in WSN?

2) How to evaluate the tolerance abilities of topologies?

3) Which topologies are more efficient than the others in tolerating failure nodes?

2 Review

The existing research [2, 3, 4, 5] on tolerance topologies for WSN is concentrated on finding multiply connected network with minimum energy by using power control. But we argue that it is not the truth.

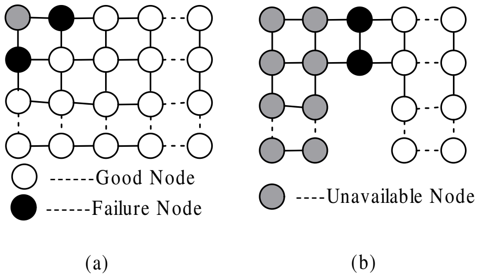

Figure 1: Effect of node-failure on availability of WSN

Considering graph G with grid structure in Figure 1, we regard a point of intersection as a sensor node, and denote the number of the sensors as n, i.e. $\|V\| = n$.

Firstly, the node-connectivity of graph Figure 1(a) is 2, but it can tolerate 3 or more failure nodes when n are big enough. After 2 black nodes are deleted from Figure 1(a), the gray node becomes isolate, and the connected graph is divided into two partitions. According to the existing work [2, 3, 4, 5], graph (a) can only tolerate 1 failure nodes. But 3 unavailable nodes in Figure 1(a) have less effect on the large-scale sensor networks. Thus the number of failure nodes that topologies can tolerate is not equivalent to the node-connectivity of the graph.

Secondly, the graphs in Figure 1(a) and Figure 1(b) are 2-connected, but the availability of the entire network is significantly different after 2 black nodes are deleted. When 2 black nodes are deleted, only three nodes are not available in Figure 1(a), but more than 50% nodes are unavailable in Figure 1(b). That is to say, although node connectivity of these two graphs is 2, one can tolerate 2 failure nodes, but the other cannot.

Now we conclude that fault-tolerance topology is not the same concept as multiply connected graph, and using multiply connectivity to evaluate tolerance ability is not appropriate.

3 Tolerating Node-Failure

We think that the effect on the availability of the network taken by the failure nodes should be considered defining node-failure tolerance for topologies of wireless sensor network. We describe the tolerance ability of G as the number of nodes which are deleted without the effect on availability of the network.

Definition 1. *Graph $G = (V, E)$ is connected, where $\|V\| = n$. After $k(n)$ nodes are deleted, the residual graph has r connected component, which are $G_1 = (V_1, E_1), G_2 = (V_2, E_2), \sharp G_r = (V_r, E_r), 1 \leq r \leq k(n) + 1$. Then the node number of maximum connected component is $A_{k(n)} = max(|V_1|, |V_2|, \sharp|V_r|)$, and the cover rate of available nodes is denoted as $C_{k(n)}$. If it satisfies*

$$\lim_{n\to\infty} C_{k(n)} = \lim_{n\to\infty} \frac{A_{k(n)}}{n} = 1. \qquad (1)$$

Then we call graph G can tolerate $k(n)$ failure nodes.

4 Tolerance of Fault and Intrusion

We use an extension network model with Bernoulli nodes uniform distributing in a unit area to describe topologies for WSN. In this model, an additional assumption is introduced to graph G(V, E) that all nodes are elected as heads independently with probability p for some constant$0 < p \leq 1$[6]. Flat and hierarchical topologies of wireless sensor network can be illustrated by graph over Bernoulli nodes. In flat topologies, $p = 1$, all nodes are heads. In hierarchical topologies, $0 < p < 1$, there are $n \times p(n)$ heads in the network.

In fact, node failure of WSN falls into two classes, one is fault caused by error, and the other is intrusion brought by attack. Because Error happens at random, but attack is hostile and selective[1], so fault happens in all nodes with the same probability, but intrusion happens only in the head nodes for their important roles in the hierarchy topology of wireless sensor network. Let the Bernoulli probability of the network model be $p(n)$, then fault happens in all the nodes, but intrusion only attack these $n \times p(n)$ heads.

If the failure node number is $k(n)$, we write the number of failure heads as $k_1(n)$ and the number of failure ordinary nodes as $k_2(n)$.

$$k(n) = k_1(n) + k_2(n). \qquad (2)$$

$p_1(n)$ is denoted as the failure-head ratio of all the failure nodes:

$$p_1 n = \frac{k_1(n)}{k(n)}. \qquad (3)$$

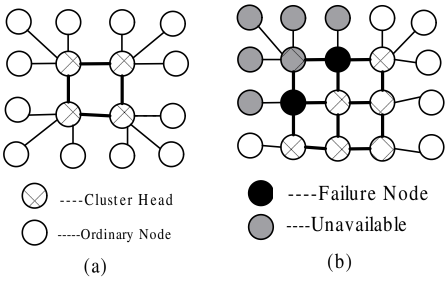

Figure 2: Hierarchy topology

If node-failure is fault, then $p_1(n) = p(n)$. If node-failure is intrusion, then $p_1(n) = 1$. From Definition 1, we can define fault tolerance and intrusion tolerance as the maximum number of tolerating failure nodes, which is the standards to evaluate tolerance abilities of topologies.

Definition 2. *$G = (V, E)$ is the network module with Bernoulli nodes, where $\|V\| = n$ and the active probability is$p(n)$. If $k(n)$ nodes are arbitrarily selected, in which $k(n) \times p_1(n)$ nodes are heads, where $p_1(n)$is defined by Equations (2) and (3). If graph G can tolerate these $k(n)$ failure nodes, we call G can tolerate $k(n)$ fault nodes when $p_1(n) = p(n)$, and we call G can tolerate $k(n)$ intrusion nodes when $p_1(n) = 1$.*

Definition 3. *$G = (V, E)$ can tolerate$k(n)$ fault nodes. When $A(n)$ nodes are deleted from G, where $m(n) = \Omega(k(n))$, the ratio of available nodes $C_m(n)$ satisfies:*

$$\lim_{n\to\infty} C_{k(n)} = \lim_{n\to\infty} \frac{A_{k(n)}}{n} \neq 1. \qquad (4)$$

Then we call$G$ is $\theta(k(n))$ fault tolerance, also call fault tolerance of G is $\theta(k(n))$, write as $FTOL = \theta(k(n))$.

Definition 4. *$G = (V, E)$ can tolerate $k(n)$ intrusion nodes. When $m(n)$ nodes are deleted fromG, where $m(n) = \Omega(k(n))$, the ratio of available nodes $C_m(n)$ satisfies Equation (4). Then we call G is $\theta(k(n))$ intrusion tolerance, also call intrusion tolerance of Gis $\theta(k(n))$, written as $ITOL = \theta(k(n))$.*

In Definition 3 and 4, the symbol Ω and θ are described by the following equation: $f(n) = \theta(g(n)) \Leftrightarrow$.

Exist constant c_1, c_2 and n_0, such that $c_1 \times g(n) \leq f(n) \leq c_2 \times g(n)$, where$n > n_0$.

5 Tolerance of Hierarchy Topology

There are n nodes in the network model with Bernoulli probability $p(n)$, which means each node has probability $p(n)$ to be cluster, then there are $n \times p(n)$ cluster, and each cluster has a head and average $\frac{1}{p(n)-1}$ ordinary nodes, as shown in Figure 2(a). If an ordinary node is

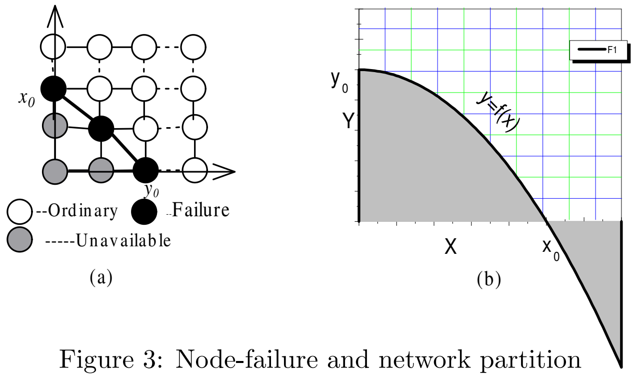

Figure 3: Node-failure and network partition

failure, then only a node is unavailable. If a head is failure, then the head and its $\frac{1}{p(n)-1}$ ordinary nodes are unavailable. If some heads are failure, they may make some other heads partitioned, then the failure heads and their ordinary nodes, the partitioned heads and their ordinary nodes are unavailable, As shown in Figure 2(b), black failure nodes make a head gray, then all the ordinary neighbors of these black or gray heads are unavailable.

Let $F_f(n)$ be the unavailable nodes brought by $k_1(n)$ heads. To attack the network, attackers try their best to make $F_f(n)$ reach the biggest value. In Figure 3(a), $k_1(n)$ black failure nodes form a connected curve and divide the network to two parts. Then the number of unavailable gray nodes reaches the biggest value. We treat $F_f(n)$ as the maximum area of shading region in Figure 3(b), and we compute the maximum of $F_f(n)$ with restriction of Equation (5).

$$\begin{aligned} F_f(n) &= \int_{x=0}^{x_0} f(x)dx \\ k_1(n) &= \oint ds. \end{aligned} \tag{5}$$

Then the maximum of $F_f(n)$:

$$F_f(n) = \frac{k_1^2(n)}{\pi}. \tag{6}$$

From Equations (2) and (6), $A_k(n)$ residual nodes is available.

$$A_k(n) = n - (\lfloor F_f(n) \times (\frac{1}{p(n)} - 1) \rfloor + k_2(n)). \tag{7}$$

If Equation (1) is true, the topology can tolerate $k(n)$ failure nodes. From Equations (7) and (1):

$$k(n) = \begin{cases} c_2 \times n^{1-\varepsilon_1}, & p_1(n) = 0 \\ y, & p_1(n) \in (0,1) \\ c_1 \times n^{\frac{1}{2}-\varepsilon_1} \cdot p^{\frac{1}{2}}(n), & p_1(n) = 1. \end{cases} \tag{8}$$

Where

$$y = min\Big(c_1 \cdot \frac{p^{\frac{1}{2}}(n)}{p_1(n) \cdot n^{\frac{1}{2}-\varepsilon_2}}, c_2 \cdot \frac{1}{1-p_1(n)} \cdot n^{1-\varepsilon_1}\Big)$$

and $p_1(n)$ is defined by Equation (3), c, ε_1 and ε_2 are constants, ε_1 and $\varepsilon_2 \in (0, \frac{1}{2}]$. Now Theorem is proved.

Theorem 1. *$G = (V, E)$ is a network model with Bernoulli nodes, in which each node has probability $p(n)$ to be cluster head, and each failure node is a head with probability $p_1(n)$. Then the network topology can tolerate $\theta(k(n))$ failure nodes, where $\theta(k(n))$ is defined by Equation (8).*

Corollary 1. *In hierarchical structure of WSN topology, let the probability of head be c, then fault tolerance decreases with c, but intrusion tolerance increases with c.*

Proof. From Equation (8), in this structure:

$$\begin{aligned} FTOL &= \theta(c^{-\frac{1}{2}} \cdot n^{\frac{1}{2}-\varepsilon}). && (9) \\ ITOL &= \theta\big((c \cdot n)^{\frac{1}{2}-\varepsilon}\big). && (10) \end{aligned}$$

Where ε is a very small constant, and $\varepsilon_2 \in (0, \frac{1}{2}]$. From Equations (9) and (10):

$$\begin{aligned} \frac{dFTOL(c)}{dc} &= \theta\Big(-\frac{1}{2}c^{-\frac{3}{2}} \cdot n^{\frac{1}{2}-\varepsilon}\Big) < 0 \\ \frac{dITOL(c)}{dc} &= theta\Big(c \cdot n^{-\frac{1}{2}+\varepsilon}\Big) > 0. \end{aligned}$$

□

6 Related Work

The popular researching on tolerance of WSN topology is looking for k-connected graph with minimum energy consumed that is far away from our work. The earlier paper [1] studies tolerance of wired network, in which the residual wired links after some nodes are deleted are used to evaluate the tolerance ability of the topologies. And it conclude that the topology whose wired links are centralized in minority nodes, has better fault tolerance, but less intrusion tolerance. This conclusion is consistent with our corollary.

7 Conclusion

We point out that the node-failure tolerance of WSN topologies is not the same as the connectivity of graphs, and present the definition of tolerating k failure nodes. Then the tolerance of fault and intrusion tolerance are presented in network model with Bernoulli nodes to evaluate the tolerance ability. Finally, fault and intrusion tolerance of hierarchical topology are studied, and the rules of fault and intrusion tolerance with head ratio of hierarchical topology are achieved.

Acknowledgments

This work was supported by the National Natural Science Foundation of China 60703115 and 60503012, Natural Science Foundation of Jiangsu Province BK2007560, Postdoctoral Science Foundation of China 20070420955, Postdoctoral Science Foundation of Jiangsu 0702003B and Talent Foundation of Jiangsu University 07JDG080.

References

[1] R. Albert, H. Jeong, and A. L. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 27, pp. 378–382, 2000.

[2] E. Chen, and S. H. Son, "A fault tolerant topology control in wireless sensor networks," *ACS/IEEE International Conference on Computer Systems and Applications*, pp. 57–69, Cairo, Egypt, Jan. 2005.

[3] X. Jia, D. Kim, S. Makki, et al., "Power assignment for k-connectivity in wireless ad hoc networks," *24th Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2005*, pp. 213–222, Miami, Florida, USA, 2005.

[4] N. Li, and J. C. Hou, "FLSS: A fault-tolerant topology control algorithm for wireless networks," *proceedings of the 10th annual international conference on Mobile computing and networking MobiCOM04*, pp. 275–286, Sep. 2004.

[5] E. Santi, "Topology control in wireless ad hoc and sensor networks," *ACM Company Surveys*, vol. 37, no. 2, pp. 164–194, 2005.

[6] P. j. Wan and C. W. Yi, "Asymptotic critical transmission range for connectivity in wireless ad hoc networks with bernouli nodes," *proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing (MOBIHOC 2004)*, pp. 1–8, Tokyo, Japan, 2004.

Liang-min Wang was born in 1977. He received his B. S. degree in computational mathematics in Jilin University in 1999, and obtained his M. E in computer application from Jiangsu University in 2003, and received his Ph.D. degree in cryptology from Xidian University. Now he is a instructor of Jiangsu University and his research interests include intrusion tolerance and security protocol.

Jian-feng Ma received his B. S. degree in mathematics from Shaaxi Normal University (Xi'an) in 1985, and obtained his M. E. and Ph. D. degrees in computer software and communications engineering from Xidian University (Xi'an) in 1988 and 1995 respectively. Since 1995 he has been with Xidian University as a instructor, associate professor and professor. Prof. Ma is a member of the executive council of the Chinese Cryptology Society and a member of the Ministry of Education Expert Committee for Discipline Development (China). His research interests include information security, coding theory and cryptography.