Fault and Intrusion Tolerance of Wireless Sensor Networks

Liang-min Wang[1], Jian-feng Ma[1], Chao Wang[1], Alex Chichung Kot[2], *Senior Member, IEEE*

[1] Xidian University.
Key Laboratory of CNIS of
Education Ministry
Xi'an Shaanxi, 710071, P.C. China.
{liangminwang, ejfma} @hotmail.

[2] Nanyang Technological University
School of Electrical and Electronic
Engineering,
639798, Singapore
eackot @ ntu. edu.sg

Abstract

The following three questions should be answered in developing new topology with more powerful ability to tolerate node-failure in wireless sensor network. First, what is node-failure tolerance of topologies? Second, how to evaluate this tolerance ability? Third, which type of topologies is more efficient in tolerating node-failure? Without giving the answers, the existing work regards fault-tolerance topology as the multiply connected graph, and use the connectivity of the graph as the standard to evaluate tolerance ability. In this paper, we argue that fault tolerance of topologies is not equivalent to the connectivity of multiply connected graph by illustrating two concrete examples. Then the definition of node-failure tolerance is presented. According fault and intrusion, the two sources of failure nodes, we define fault tolerance and intrusion tolerance as the standards to evaluate the tolerance ability of topologies, and analyze the tolerance performance of hierarchical structure of wireless sensor network by using these standards. Finally, the function relation between hierarchical topology and its tolerance abilities of fault and intrusion is obtained, and an obvious corollary is that fault tolerance increase with the ratio of cluster head hierarchical structure, but with the intrusion tolerance decreasing.

I. INTRODUCTION

WIRELESS sensor networks usually were deployed in remote and hostile surroundings, and people cannot attend the sensor nodes in bad environmental. 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 sensor network and even produces network failure. So network topology should tolerate node-failure to avoid network partition.

In k-connected graph, the residual graph is still connected after deleting arbitrarily selected k-1 nodes, i.e., k-connected graph can tolerate k-1 failure nodes. Considering the tolerance ability of multi-connected graph, some literatures [1-5] about fault-tolerance topology of wireless sensor networks are emerging, in which the problem of developing fault-tolerance topology is treated as looking for multiply connected graph. They produce k-connected network with energy- optimization to tolerate k-1 failure nodes by power control.

However, there are three problems in these power control algorithms. First, it is difficult to find the k-connected graph with minimum power, which is proved to be NP-hard even in 2-dimenision [6]. Second, some methods are proposed recently for achieving approximate optimum solution [1-5] of k-connected graphs with minimum power, but the networks gotten in these methods are so dense that radio interference and power consume are increased rapidly [7]. Thirdly, the value of k is very little in these approximate optimum k-connected graphs gotten from the existing methods for the above two reasons. Generally, $k<5$. That is to say, the topology can only tolerate 4 failure nodes. It is too little for plenty of fault nodes produced in large scale distributed sensor network or the selected intrusion nodes by the enemies.

In early time, literature [8] focus on the topology tolerance of some wired networks, in which the authors delete the failure nodes from the network and study the

Manuscript received November 13, 2005. This work was supported by the the significant Research Program of National Natural Science Foundation of China under grant 90204012, and National Natural Science Foundation of China 60503012, 60573035 and 60573036.

available links of the residual sub-graph, they regard the number of available links as the standard to evaluate the tolerance ability. By researching on exponential network and scale-free network, Albert [8] thinks that the exponential network whose majority links are concentrated on the small number of nodes has better fault tolerance and less intrusion tolerance, while the scale-free network in which every node has the similar number of links has less fault tolerance but better intrusion tolerance.

In summary, there is still no concept of node-failure tolerance of topology, and no standard to evaluate the tolerance ability, in that we cannot know which topology has better tolerance. We think the following three questions should be answered when researching node-failure tolerance of wireless sensor networks.

- What is the definition of node-failure tolerance for topology in WSN?
- How to evaluate the tolerance abilities of topologies?
- Which topologies are more efficient than the others in tolerating failure nodes?

In this paper, we focus on giving the answer of these questions. In section 2, we point out the deference between multiply connected graph and node-failure tolerance topology by illustrating two examples, then define node-failure tolerance of topology for WSN as the ratio of available sensor nodes over all the nodes of network, and then define the degree of fault-tolerance and intrusion tolerance to evaluate the tolerance ability for fault nodes and intrusion nodes respectively. In section 3, we study WSN topologies with hierarchic structure by using Bernoulli node model, and draw the Theorem 1. In section 4, we get some corollaries of the Theorem 1, which describe the tolerance abilities of hierarchic topologies with deference parameters. Then we point out the similarities and differences between our work and related work. In the end we summarize this paper in section 5.

II. FAULT TOLERANCE AND INTRUSION TOLERANCE

This section describes network model and some related concepts, then illustrates the deference between multiply connected graph and node-failure tolerance topology, and defines what is a topology tolerating k node-failure. In the end, the Bernoulli node model is adopted to describe hierarchic topologies, and fault tolerance and intrusion tolerance is defined over this model to evaluate the tolerating ability of topologies.

A. Network Model and Related Concept

Graph G=(V, E) denotes the topology of wireless sensor network, in which V is the set of nodes and E is the set of wireless links between two nodes. In this paper, we regard communication between nodes are bidirection, so the edges in the graph are directionless. If G′ is the subgraph of G and there is a way between two arbitrarily selected nodes, where G′=(V′, E′) and V′ $\subseteq$ V, then G′ is a ***connected subgraph*** of G. If G consists of l connected subgraph, which are $G_1=(V_1, E_1)$, $G_2=(V_2, E_2)$, … $G_l=(V_l, E_l)$, then we call $G_1, G_2, \ldots G_l$ is the connected component of G respectively. Let G′=(V′, E′) be a ***connected component*** of G, obviously $V' \in \{V_1, V_2, \ldots, V_l\}$, if V′ satisfies

$$|V'|=\max\{|V_1|, |V_2|, \ldots, |V_l|\} \quad (1)$$

Then G′ is the maximum connected component of G. we define C as the ***cover rate*** of subgraph G′ over graph G:

$$C=\frac{|V'|}{|V|} \quad (2)$$

In this paper, we use cover rate to evaluate the availability of the wireless sensor network.

If G has only a connected component, the G is a connected graph. If there is k no-joint ways between two arbitrarily selected nodes and these ways have no same nodes between each other, then G is k-connected. If G is k-connected, then the residual subgrah is still connected after $(k-1)$ nodes are deleted. If there is a set of k nodes, when all the nodes of the set are deleted, the residual subgraph is not connected, then we call the node connectivity of G is k.

B. Node-failure Tolerance

The existing research on tolerance topologies for wireless sensor network is concentrated on finding multiply connected network with minimum energy by using power control. But we argue that the tolerance ability of topologies is not equivalent to connectivity of multiply connected graph. In the following we give two examples to show the differences between these two concepts.

Considering graph G with grid structure, we regard a point of intersection as a sensor node, and denote the number of the sensors as n, i.e. $|V|=n$, the communication radius as r and the length of the grid edge as a, and all these parameters satisfy:

$$r/\sqrt{2} \le a \le r \quad (3)$$

In Fig.1, the connectivity of graph (a) is 2. When two black nodes are deleted, the gray node becomes isolate, and the connected graph are divided into two partitions. According to the existing work[1-5], graph (a) can only tolerate one failure nodes. When $n\to\infty$, $3/n \to 0$, thus 3 unavailable nodes in Fig.1 (a), just as in Fig.1 (b), have less

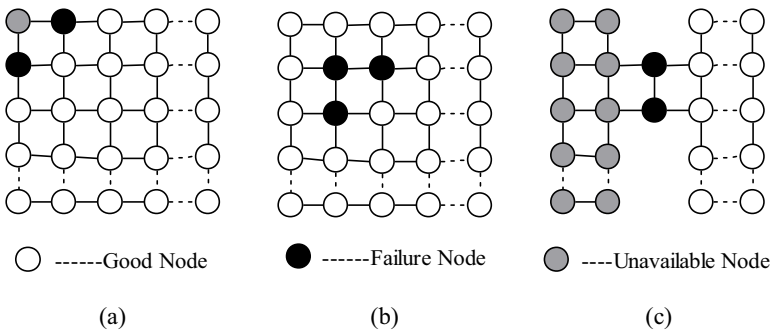


Fig.1 Effect of Node-failure on Availability of WSN (a) Two failure nodes make network partition and 3 sensor nodes unavailable; (b) Three failure nodes but network connected; (c) Two failure nodes make network partition and half of the sensor nodes unavailable

effect on the large-scale sensor networks. That is to say, the topologies in Fig.1 (a) and Fig.1 (b) can tolerate 3 or more failure nodes, although the connectivity of them is 2.

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

From above analysis, we can draw our conclusion that fault-tolerance topology is not the same concept as multiply connected graph, and using multiply connectivity to evaluate tolerance ability is not appropriate. Researching node-failure tolerance for topologies of wireless sensor network, we should consider the effect on the availability of the network taken by the failure nodes. In this paper, we use the cover rate of the available sensor nodes of the maximum connected component over the whole network to denote network availability.

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 $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$, … $G_r = (V_r, E_r)$, $1 \le r \le k(n) + 1$. Then the node number of maximum connected component is $A_k(n)=\max(|V_1|, |V_2|, \ldots |V_r|)$, and the cover rate of available nodes is denoted as $C_k(n)$. If $C_k(n)$ satisfies

$$\lim_{n\to\infty} C_k(n) = \lim_{n\to\infty} \frac{A_k(n)}{n} = 1 \tag{4}$$

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

Definition1 defines the concept of graph G which can tolerate $k(n)$ failure nodes, where G is a class of topologies and $k(n)$ is a function of all the nodes number n. The definition shows the tolerance ability of the topologies whose structure is G, and the tolerance ability is described by the number of nodes which are deleted without the effect on availability of the network.

C. Fault-tolerance and Intrusion-tolerance

Network topologies for WSN fall into two classes: one is flat structure, and the other is hierarchic structure. Flat structure is produced by power control algorithm [9], in which the sensor nodes are peer-to-peer; Hierarchic structure is achieved by clustering algorithm, such as LEACH[10], HEED[11], CEC[12]. In Hierarchic structure, some sensor nodes are selected as cluster heads, and the others are ordinary nodes. Ordinary nodes only collect data. Heads not only collect data, but forward packages.

In this paper, we use an extension network with Bernoulli nodes uniform distributing in a unit area to describe topologies for WSN. We introduce an additional assumption to the graph G(V, E) that all nodes are elected as heads independently with probability p for some constant $0 < p \le 1$. These nodes are referred to as Bernoulli nodes with the parameter p. 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, $0 < p < 1$, each node has probability p to be selected as cluster heads.

In fact, node failure of WSN falls into two classes, one is fault caused by error, and the other is intrusion brought by attack. Error happens at random, so the fault probability of each sensor node has the same value. But attack is hostile and selective, so the intrusion probability of each node is different. The node has greater probability to be intruded when it has an important role on the whole network, such as cluster head. In that, 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 $n \cdot p(n)$ heads.

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

$$k(n) = k_1(n) + k_2(n) \tag{5}$$

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

$$p_1(n) = \frac{k_1(n)}{k(n)} \tag{6}$$

If node-failure is fault, then $p_1(n) = p(n)$. If node-failure is intrusion, then $p_1(n) = 1$. From these rules and definition 1, we can define fault tolerance and intrusion tolerance, which are 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 $k(n)\cdot p_1(n)$ nodes are heads, where $p_1(n)$ is defined by equation(5) and equation(6). If graph G can tolerate these $\boldsymbol{k}(n)$ failure nodes, we call G can tolerate $\boldsymbol{k}(n)$ fault nodes when $p_1(n)=p(n)$, and we call G can tolerate $\boldsymbol{k}(n)$ intrusion nodes when $p_1(n)=1$.

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

$$\lim_{n\to\infty} C_m(n) = \lim_{n\to\infty} \frac{A_m(n)}{n} \neq 1 \tag{7}$$

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

The symbol Ω and θ are described by equation (8) and (9).

$f(n)= \theta(g(n))$

$\Leftrightarrow$ Exist constant c_1, c_2 and n_0, such that c_1

$$g(n) \le f(n) \le c_2 g(n), \text{ where } n>n_0 \tag{8}$$

$f(n)= \Omega(g(n))$

$\Leftrightarrow$ Exist constant c, and n_0, such that

$$f(n) \ge c\, g(n), \text{ where } n>n_0 \tag{9}$$

Definition 4: G=(V, E) can tolerate $k(n)$ intrusion nodes. When $m(n)$ nodes are deleted from G, where $m(n)=\Omega(k(n))$, the ratio of available nodes $C_m(n)$ satisfies equation(7). Then we call G is $\theta(k(n))$ intrusion tolerance, also call intrusion tolerance of G is $\theta(k(n))$, written as ITOL=$\theta(k(n))$.

Definition 2 illustrate the difference between tolerating fault nodes and intrusion node, and definition 3 and definition 4 give the two concepts of fault tolerance and intrusion tolerance to evaluate the abilities of topologies to tolerate fault or intrusion, in which the tolerance abilities are described as the maximum number of tolerating failure nodes.

III. TOLERANCE ABILITY OF HIERARCHY TOPOLOGY

This section uses the network model with Bernoulli nodes to study the fault tolerance and intrusion tolerance of hierarchical topology of wireless sensor network. There are n nodes in the network model and each node has probability $p(n)$ to be a head. That is to say, there is $n \cdot p(n)$ heads in the model. In the hierarchical structure, cluster heads compose the backbone network, which take charge of forwarding packages. The other nodes join the cluster whose head has shortest distant from them, then each head has average $(1/p(n)-1)$ ordinary neighbor nodes. The head and the joined ordinary nodes compose a cluster, as shown in Fig.2.

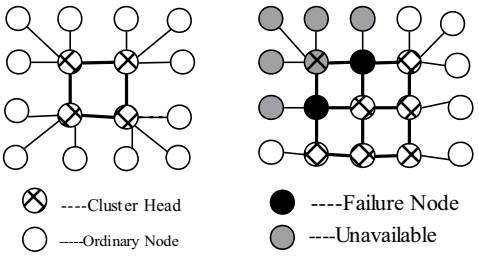


Fig.2 Hierarchy Topology (a) Cluster Structure; (b) Effect of Failure Heads

The node-failure effect on the whole network is different. If ordinary node is failure, then only is the node itself unavailable. If the head is failure, not only is the head itself unavailable, but also the ordinary nodes joined in this cluster, the unavailable heads and their neighbors, which are gray in Fig.2 (b).

From equation (5), $k_1(n)$ is the number of failure heads. Let $F_f(n)$ be the unavailable nodes brought by these $k_1(n)$ heads. To get most unavailable nodes, i.e., to make $F_f(n)$ reach the biggest value, $k_1(n)$ black failure nodes should form a connected curve which divides the network to two parts, just as shown in Fig.3 (a). Then the gray nodes are not available and the network cover rate is decreased. We compute $F_f(n)$ as the maximum area of shading region in Fig.3 (b), in which the length of edge $f(x)$ is $k_1(n)$. Thus we should compute the maximum of $F_f(n)$ with restriction of $k_1(n)$.

$$F_f(n) = \int_{x=0}^{x0} f(x)dx \tag{10}$$

$$k_1(n) = \oint ds \tag{11}$$

Then the maximum of $F_f(n)$:

$$F_f(n) = \frac{k_1^2(n)}{\pi} \tag{12}$$

Thus the residual $A_k(n)$nodes is available.

$$A_k(n) = n - \left(\left\lfloor F_f(n) \cdot \left(\frac{1}{p(n)} - 1\right) \right\rfloor + k_2(n) \right) \tag{13}$$

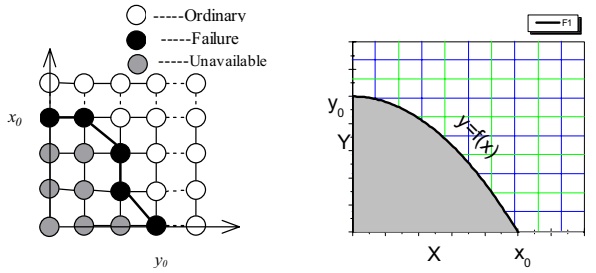
So we can conclude that the topology can tolerate $k(n)$ failure nodes when equation (4) is true.

$$k(n) = \begin{cases} c_2 \bullet n^{1-\varepsilon_1} & p_1(n) = 0 \\ \min\left(c_1 \bullet \frac{p^{1/2}(n)}{p_1(n)} \bullet n^{1/2-\varepsilon_2},\ c_2 \bullet \frac{1}{1-p_1(n)} \bullet n^{1-\varepsilon_1} \right) & p_1(n) \in (0,1) \\ c_1 \bullet p^{1/2}(n) \bullet n^{1/2-\varepsilon_1} & p_1(n) = 1 \end{cases} \tag{14}$$

Where $p_1(n)$ is defined by equation(6), c, ε_1 and ε_2 are constants, $\varepsilon_1, \varepsilon_2 \in (0, \frac{1}{2}]$.

Then we get our conclusion:

Theorem1: 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 (14).



(a) (b)

Fig.3 Node-failure and Network Partition (a) $k_1(n)$ nodes are deleted, network is divided into two or more connected components; (b)Curves $f(x)$ partitions the shading area $F_f(n)$.

IV. ANALYSIS AND DISCUSSION

This section analyzes the tolerance ability of hierarchical structure with $p(n)$ in some different case, and points out the similarities and difference between this paper and some related work.

A. Analysis on Tolerance of WSN Hierarchy

Firstly, flat structure is considered. If $p(n)$=1, all the nodes are heads, then $p_1(n)$=1. For the value of ε_1 and ε_2 could be very small, then we can get Corollary 1 from Theorem 1.

Corollary 1: Fault tolerance and intrusion tolerance of flat structure of WSN are equivalent, they satisfies:

$$\mathrm{ITOL} = \mathrm{FTOL} = \theta(n^{1/2-\varepsilon}) \tag{15}$$

Where ε is constant, and $\varepsilon \in (0, \frac{1}{2}]$.

The value of fault tolerance and intrusion tolerance are equal in flat structure, and then there is only a black real line in Fig.4 which denotes tolerance of flat structure.

Secondly, we consider the hierarchical structure has only m heads, where m is constant and $m < n$. Fault tolerance and intrusion tolerance of this structure is shown in Fig.4 (b), where fault tolerance is greater than that of flat structure, but the intrusion tolerance is less than that of flat structure.

Corollary 2: G=(V, E) is a network model with Bernoulli nodes, in which each node has probability $p(n)$ to be cluster head. If there is only m heads, m is a constant and $m < n$, i.e. $p(n) = m/n$, then

$$\mathrm{FTOL} = \theta(m^{-1} \bullet n^{1-\varepsilon}) \tag{16}$$

$$\mathrm{ITOL} = \theta(m^{1/2-\varepsilon}) \tag{17}$$

Where ε is a very small value, and $\varepsilon \in (0, \frac{1}{2}]$.

Thirdly, we consider the case with Bernoulli probability $p(n) = c$, where c is constant, and $0 < c < 1$. Corollary 3 gives tolerance of fault and intrusion in this situation.

Corollary 3: G=(V, E) is a network model with Bernoulli nodes, in which each node has probability $p(n)$ to be cluster head. If $p(n) = c$, c is a constant and $0 < c < 1$, then fault tolerance of this topology is

$$\mathrm{FTOL} = \theta(c^{-1/2} \cdot n^{1/2-\varepsilon}) \tag{18}$$

and intrusion tolerance of this topology is

$$\mathrm{ITOL} = \theta((c \cdot n)^{1/2-\varepsilon}) \tag{19}$$

ε is a very small constant in equation (18) and (19), and $\varepsilon \in (0, \frac{1}{2}]$.

From (18)

$$\mathrm{FTOL}'(c) = \theta(-\frac{1}{2} c^{-3/2} \cdot n^{1/2-\varepsilon}) < 0 \tag{20}$$

That is to say, fault tolerance decreases with c. As shown in Fig.4 (c), the function curve with bigger value of c is lower than that with smaller c.

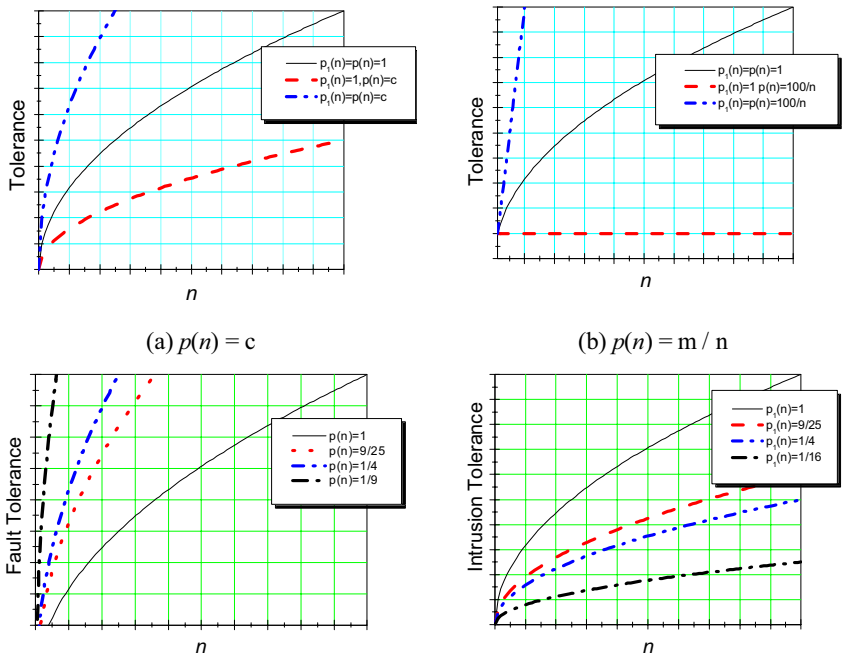
From (19)

$$\mathrm{ITOL}'(c) = \theta(c \cdot n^{-1/2+\varepsilon}) > 0 \tag{21}$$

We can see that intrusion tolerance increases with c. As shown in Fig.4 (d), the function curve with bigger value of c is higher than that with smaller c value.

Now Corollary 4 is achieved.

Corollary 4: 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.



(a) $p(n)$ = c (b) $p(n)$ = m / n

(c) Fault ($p_1(n) = p(n)$) (d) Intrusion ($p_1(n)$ =1)

Fig.4 Tolerance of Hierarchy Topology (a)In flat structure, $p(n) = p_1(n) = 1$, fault tolerance is equal to intrusion tolerance; but $p(n) = c \neq 1$, fault tolerance of hierarchical structure is not equal to intrusion tolerance. (b)Fault tolerance of network with 100 heads is bigger than that of flat structure, but intrusion tolerance is less. (c)Fault tolerance decreases with $p(n)$ increasing. (d) Intrusion tolerance increases with $p(n)$ increasing.

B. Comparison of Related Work

Some algorithms for k-connected graph with minimum energy consumed are presented in literature [1-5], in which fault and intrusion are not distinguished. The authors of these papers didn't give the definition of fault tolerance, and regard k-connected as k-tolerated. They didn't consider the relation between different topologies and their tolerance. In this paper, we argue that connectivity of the graph is not the same as tolerance of WSN topologies, and looking for k-connected topologies is not a good way for fault tolerance because of its increasing communication interference and poor tolerance ability.

Reference [8] studies the complex network, in which the residual wired links after some nodes are deleted are used to evaluate the tolerance ability of the topologies. They use statistic to research fault tolerance and intrusion tolerance of two different networks, and get some relations between topology structure and its fault and intrusion tolerance. But it doesn't give the accurate definition of topology tolerance, and the relations of topology and its tolerance are qualitatively described.

This paper deals with the wireless sensor network, and the number of available residual sensors is used to evaluate the tolerance of the topologies. The ability of fault or intrusion tolerance is divided in the network model with Bernoulli nodes. In the end we get the tolerance of hierarchy topology in this model, and discuss the related fault tolerance and intrusion tolerance in some situation, some conclusions are consistent with that of reference [8].

TAB. 1 SIMILARITIES AND DIFFERENCE OF RELATED WORK

Related Work	Network	Method	Fault or Intrusion	Definition	Evaluation Standard	Relation between Tolerance and Topology
Reference [1-3]	Wireless network	Deduction	Fault	No	Graph connectivity	No
Reference [4-5]	WSN	Deduction	Fault	No	Graph connectivity	No
Reference [8]	Wired network	Statistic	Distinguished	No	Available residual links	Qualitative description
Our paper	WSN	Deduction	Distinguished	Defined	Available residual sensor nodes	Quantitative function

In literature [8], the topology whose links are centralized in minority nodes has better fault tolerance, but less intrusion tolerance. In our conclusion, the topology that has less cluster heads has better fault tolerance, but less intrusion tolerance. In the hierarchical structure, cluster heads are less, links are more centralized in minority nodes. This consistence provides a proof for the efficiency of our theorem. Table 1 lists the sameness and difference among this paper and these related work.

V. CONCLUSION

This paper points out that the node-failure tolerance of WSN topologies is not the same as the connectivity of graphs, and defines tolerating k failure nodes according to the ratio of available nodes of all the sensor nodes. Then we tell the difference between fault tolerance and intrusion tolerance by using network model with Bernoulli nodes. Finally, we study fault tolerance and intrusion tolerance of hierarchical topology by this Bernoulli network model, and the functions of fault and intrusion tolerance with head ratio of hierarchical topology are achieved. In our future work, these functions will help us to devise the WSN topologies on the concrete demand of fault or intrusion tolerance. For the instant case, it can be used to devise power control algorithm to satisfy tolerance demand when sensor nodes are distributed in a field with constant area, or comput the appropriate number of sensors to satisfy tolerance demand in concrete area.

REFERENCE

[1] Xiaohua Jia, Dongsoo Kim, Sam Makki, et al. Power Assignment for k-Connectivity in Wireless Ad Hoc Networks. In 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005), Miami, Florida, USA.

[2] Ning Li, Jennifer 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), September, 2004.

[3] Xiang-yang Li, Peng-jun Wan, Yu Wang, et al. Fault Tolerant Deployment and Topology Control in Wireless Networks. In Proc. 4th ACM Intl. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc03), Annapolis, MD, 2003.

[4] Yong Chen, Sang H. Son, A Fault Tolerant Topology Control in Wireless Sensor Networks. ACS/IEEE International Conference on Computer Systems and Applications, Cairo, Egypt, January 2005.

[5] Hwajung Lee, SEEMLESS: Distributed Algorithm for Topology Control of Survivable Energy Efficient Multihop Wireless Sensor Networks Using Adjustable Transmission Power. Proc. 6th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD 2005), Baltimore, Maryland, May 23 - May 25, 2005.

[6] G Calinescu, Peng-jun Wan, et al. High Connectivity with Minimum Total Power in Wireless Ad Hoc Networks, Ad Hoc Now, 2003.

[7] Peng-jun Wan, Chih-wei 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), Tokyo, Japan, 2004.

[8] Reka Albert, Hawoong Jeong, Albert-Laszlo Barabasi, Error and Attack Tolerance of Complex Networks. Nature, Vol. 406(27): 378-382, 2000.

[9] Paolo Santi, Topology Control in Wireless Ad Hoc and Sensor Networks. ACM Comp. Surveys (to appear2005).

[10] W Heinzelman, A Chandrakasan, and H. Balakrishnan. An application-specific protocol architecture for wireless micro-sensor network. IEEE Trans on Wireless Communication. 2002,1(4): 660-670.

[11] Ossama Younis, Sonia Fahmy. HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks. IEEE Transactions on Mobile Computing, vol. 03, no. 4, pp. 366-379, October 2004.

[12] Ya Xu, Solomon Bien, Yutaka Mori, et al. Topology Control Protocols to Conserve Energy in Wireless Ad Hoc Networks. Center for Embedded Networked Computing. Technical Report 0006, University of California. January 2003.