Design of Wireless Sensor Networks Considering the Robustness of the Topology

Yu-Dong Tan*, Xiao-Qin Huang, Ye Cai, Yi Tan, and An-Gang Chen

College of Electrical and Information Engineering, Hunan University,
ChangSha, 410082 Hunan Province, China
yudongtan@126.com

Abstract. In wireless sensor networks, the sensor nodes are facing the random failure and the selective attacks all the time, which will cause partial or even entire network disintegrating. How to control the failures resulted from random failure or the selective attacks has become a hot topic in recent years. In this paper, we applied three matching models of capacity on three common kinds of wireless sensor network topology, and each model developed a profit function to defense cascading failures. Performances of the proposed matching models of capacity are evaluated using computer simulations. By studying the relationship between network investment and robustness, we find that NM model can defend against cascading failures better and requires a lower investment cost when higher robustness is required .The network performance analysis and the simulation results indicated that it can improve network robustness and invulnerability which are particularly important for the design of networks after applying this algorithm in the wireless sensor network.

Keywords: reliability, robustness, complex network**,** wireless sensor networks.

1 Introduction

In recent years, wireless sensor networks have attracted more and more related researchers for its advantages. Wireless sensor networks consist of large amounts of wireless sensor nodes to collect information from their sensing terrain, such as seismic and acoustic data [1-4]. People can spread the nodes in the high temperature, high humidity, harmful gases and other enemy controlled areas where our personnel can not reach, to achieve continuous real-time data acquisition in order to achieve unattended monitoring purposes. With the development of technology (system on a chip), integrating the sensor nodes into a micro-chip, like smart dust [5] and other micro-sensor networks will become the future trend of development. In the near future, it will be possible that hundreds or even thousands of sensor nodes form a network.

Different from traditional wireless networks, apart from the need for local information collection and data processing, the sensor nodes should also store and

* Corresponding author.

P. Sénac, M. Ott, and A. Seneviratne (Eds.): ICWCA 2011, LNICST 72, pp. 216–227, 2012.

forward integrate the data sent by other sensor nodes, and sensor nodes require mutual coordination and communication with each other and work together to complete complex work. Restricted by price and volume of the nodes, the wireless sensor network nodes have only a relatively limited signal processing capabilities, computing power and storage capacity. Sensor nodes of the network can be divided into different categories according to the sensing capability, computing power, energy, and etc. Thus the sensor networks can be divided into homogeneous sensor networks and heterogeneous sensor networks. Homogeneous sensor network is constituted by the same nodes (sensor nodes), and the heterogeneous sensor network is constituted by the different nodes including sensor nodes and sink nodes. The sensors monitor environmental variations then transmit observation results to a fusion center [6-9]. For example, seismic and acoustic datas are collected by several sensors and then transmitted to a sink node for joint processing to detect, classify, and track vehicles [6].Sink node also has the relatively strong processing power, storage capacity and communication capacity, for the use of connecting the wireless sensor network and the external networks. Sink nodes can be either an enhancement of the sensor nodes or only the particular gateway device with the wireless communication interface without monitoring functions to ensure the sink nodes have adequate energy and more memory and computing power. Regardless of sensor nodes or sink nodes, they only have relatively limited data processing and communication capabilities.The integrity of the original networks will be destroyed and other nodes will have more business burden for data transmission if some certain nodes fail. When the load of these nodes exceeds the capacity of their own or their operating environment deteriorate, these sensor nodes will also be out of service.

In the category of complex networks, the phenomenon has been abstracted into the two types of situations:(1) the breakdown of node is random, each node has the equal probability of breakdown; (2) selective attacks, with the purpose to attack the most connected nodes for destruction[10]. More processing and communication capabilities can be allocated to the nodes to avoid affecting the entire network connectivity due to breakdown of some nodes. Regardless of how much of the investment cost, the sensor network can reach a high robustness through allocating sufficient redundancy capacity to the nodes. But it is definitely improper in designing the network of reality. The designer must take robustness and economy of the sensor network into account simultaneously.

With the development of wireless sensor networks, the key issue of sensor network research is to allocate more investment cost to some critical nodes to ensure them have a higher reliability, thus enhance the sensor network robustness when the total investment cost of the sensor network is fixed, which means finding a balance between economy and reliability[11].

2 Robustness of the Complex Networks

The complex network theory has been for some time since first proposed by Barabási and Albert in 1998, but complex network theory and analysis method applied to

wireless sensor networks research are seriously rare and develop in slow progress. It is necessary to introduce a way of how to study wireless sensor network by complex network theory and analysis methods. The key of which lies in a successful modeling which is able to make complex network theory and analysis methods more suitable for the application of wireless sensor network in order to achieve the optimization of some certain network characteristics of wireless sensor network. The complex system theory study the large-scale network that exists in social system with the systemic perspective, such as internet, electricity networks, metabolic networks and protein networks, and etc. Watts and Strogatz revealed the small-world properties of complex network in 1998, and established a small world network model [12]. Barabási further revealed the complexity of many real-world networks with the degree distribution of power law form, called scale-free network [13], and established a scale-free network model. These pioneering works promote the complex networks research into a new era. Therefore, complex networks have recently attracted considerable attention in physics and other fields. Interestingly, many real-world networks share a certain number of common topological properties, such as small-world and scale-free properties [14-17] .

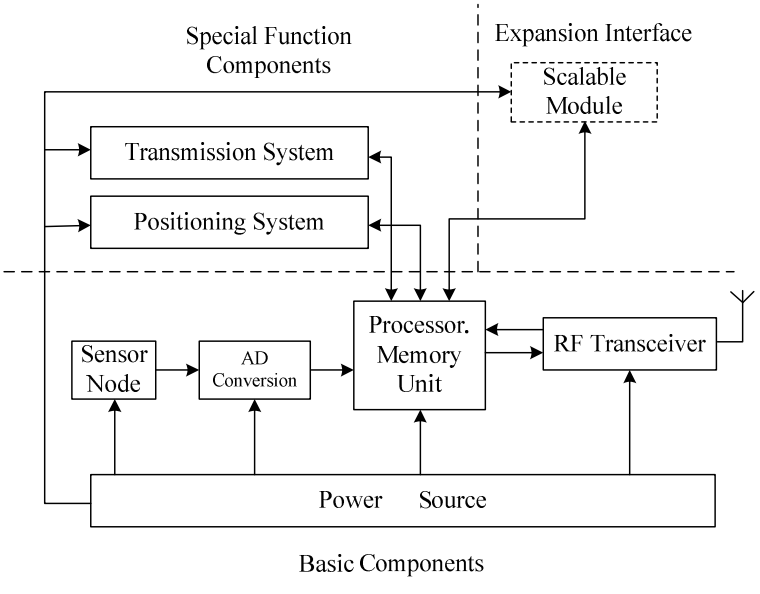

Fig. 1. Components of wireless sensor network node

Robustness refers to the malfunction avoiding ability of a network when a fraction of its constituents are damaged. The network robustness has been one of the most central topics in the complex network research [18]. In scale-free networks, the existence of hub nodes with high degrees has been shown to yield fragility to intentional attacks, while at the same time the network becomes robust to random failures due to the heterogeneous degree distribution [19–22]. Sensor network is a real

network, must have the characteristics of complex network. Study the dynamic behavior and complex networks' characteristics of wireless sensor network will have special significance for the development of sensor network. In different applications, the compositions of the wireless sensor network nodes are different [23]. But generally the core of node consist of three parts: the processing unit (CPU, memory unit, Embedded Operating System), communication unit and power management unit. The type of sensor node is determined by the kinds of physical signals monitored by the node [24].

Fig. 1 is hardware schematic diagram of the sensor node, the sensor node is a miniaturized embedded system [25], it is typically composed of data acquisition module, data processing and control module, communication module and power modules. These units are hold in a matchbox-sized module, some even smaller [26-27]. Because limited by the volume, sensor nodes are usually battery-powered, this greatly limits the energy of sensor nodes. In addition, as constrainted by the energy and volume, the processing power and storage capacity of the sensor nodes is limited [28-29]. The operating environment of sensor nodes is harsh, as a result, the entire network may collapse due to the breakdown of some nodes, because nodes prone to be lack of processing capacity or the destruction of nature to the nodes. And the anti-investigation actions of enemy will carry out the purpose of destruction to our sensor networks. People must overcome these problems into account when they construct a wireless sensor network. The most effective way is to increase investment cost of the sensor networks. But how to spend less investment cost for a maximum robustness? The researchers of complex networks have made some significative works in the topology robustness.

Network robustness [30-34] subjects to random or intentional attacks has been one of the most central topics in network safety. Therefore, failures on complex networks have been highly concerned and widely investigated. The network robustness has been one of the most central topics in the complex network research.

Each node (sensor or fusion center) of the wireless sensor network, its load such as seismic and acoustic data is either produced or transferred to other nodes, and it is possible that for the limited processing power and storage capacity, node is overloaded beyond the given capacity, which is the maximum data that the node can handle. The breakdown of the heavily loaded single node will cause the redistribution of loads over its neighboring nodes, and load is reassigned to bypass malfunctioning nodes which can trigger breakdowns of newly overloaded nodes. This process will go on until all the loads of the remaining nodes are below their capacities.The damage caused by failures can be quantified by the relative size of the largest connected component *G*, defined as following

$$G = N^{'} / N \tag{1}$$

Where N and $N^{'}$ are the numbers of nodes in the largest component before and after the failure, respectively. The integrity of a network is maintained if $G \approx 1$, while breakdown occurs if $G \approx 0$. The relative size *G* also represents the robustness of wireless sensor network against intentional attacks or random failure.

For wireless sensor network, the breakdown of some nodes is sufficient to collapse partial even the entire system. In the research of the failures, the following two issues are closely related to each other and of significant interests: one is how to improve the network robustness to failures, and the other particularly important issue is how to design manmade networks at a less cost. In most circumstances, a high robustness and a low cost are difficult to achieve simultaneously. The failure can be prevented by assigning extra capacities (processing power and storage capacity) to sensor nodes. Since the extending of sensor network capacity will bring economic and technique pressure, it is important to explore how to rationally allocate the limited capacity onto sensor nodes or sink nodes, and efficiently improve the robustness of sensor network. In general, one can split, at least conceptually, the total cost for the sensor networks into two different types: on one hand, there should be the initial construction cost to build a sensor network structure, another type of the cost is required to allocate extra capacities to sensor nodes or sink nodes of the given sensor network. For the latter, we need to spend more to have bigger memory sizes and processing power and so on for the server of sensor node which it can handles more data packets. In the present letter, we assume that the sensor network structure is given, (accordingly the construction cost is fixed), and focus only how to efficiently allocate limited resources of capacity to make sensor network more robust, which should be spent in addition to the initial construction cost. Assume that in a sensor network, the load of sensor node is l_i, we expect the capacity c_i of this sensor node should be an increasing function of l_i

$$c_i = \lambda_i \cdot l_i \tag{2}$$

Although it should be possible to find, via a kind of the variational approach, the optimal functional form of λ_i ، that sensor networks can indeed be made more robust while spending less cost.

For a given sensor network structure, we aim to increase *G* and decrease the cost, which will eventually provide us a way to achieve the high robustness and the low cost at the same time. In the present letter, for simplicity, we try to find a possible way of assigning the extra capacities. For the improvement of robustness of the network, based on the work [35], many models have been studied extensively. While for the design of manmade networks, Motter-Lai first proposed ML model, Wang et al, proposed a high-robustness and low-cost model (WK), H.J. Sun et al, also proposed a NM model to improve networks. In our research, we will apply ML,WK and NM model to the improvement of sensor networks' robustness[36]. Our results suggest that networks can indeed be made more robust while spending less cost.

3 Model

Among the previous works, ML model assumes the capacity c_i of node i be proportional to the initial load l_i as

$$c_i = \lambda_i \cdot l_i = (1+\alpha) \cdot l_i, i = 1,2,...,N, \tag{3}$$

Where $\alpha \geq 0$ is the control parameter representing the extra capacity. In WK model, Wang et al . set $\lambda(i)$ as

$$\lambda(i) = 1 + \alpha\theta(l_i / l_{\max} - \beta) \tag{4}$$

Where $\theta(x) = 0(1)$ for x¡0(¿0) is the Heaviside step function, $l_{\max} = \max(l_i)$ (i=1,2,3…N), and they use $\alpha \in [0,\infty)$ and $\beta \in [0,1]$ as two control parameters in the model. In ML model, λ has been a constant, which corresponds to the limiting case of $\beta = 0$ with the identification $\lambda = 1 + \alpha$ in the WK model. ML model raises a linear correlation between extra capacity and initial load, while WK model prefers to protect the highest-load nodes.

In the research of how to design robust manmade network, there is another capacity allocation model proposed by H.J. Sun. This model considered the betweenness distribution, the flow generation rate and the network structure in the process of network designment at the same time, the failures will be alleviated effectively. In the model, it is assumed that, at each time step, on average, μ packets are generated and the flow is forwarded along the shortest path. The betweenness B_i can be used to characterize the number of shortest paths between pairs of nodes that run through node i. The betweenness of node i can be defined as

$$B_i = \sum_{j,l \in N, j \neq l} \frac{n_{jl(i)}}{n_{jl}} \tag{5}$$

Where n_{jl} is the number of shortest paths connecting j and l, while $n_{jl}(i)$ is the number of shortest paths connecting j and l and passing through i. The model assumes the capacity of a node as the maximum load that the node can handle and is proportional to its initial load. Thus, the capacity allocation model is given as follows

$$\lambda_i = 1 + \alpha \frac{B_i}{\mu ND + \mu} \tag{6}$$

Where the capacity c_i of node i be proportional to its initial load l_i, α is a tolerance parameter, μ is the average flow generating rate, N is the size of network, D is the average shortest path length. As we know, in man-made networks, the capacity is severely limited by cost.

For convenience define the cost e as

$$e = \frac{1}{N} \sum_{i=1}^{N} (\lambda_i - 1) \tag{7}$$

In ML model, the cost is

$$e_{ML} = \frac{1}{N}\sum_{i=1}^{N}(\lambda_i - 1) = \alpha \tag{8}$$

In the WK model, the cost is

$$e_{WK} = \frac{1}{N}\sum_{i=1}^{N}(\lambda_i - 1) = \frac{1}{N}\sum_{i=1}^{N}\alpha \cdot \theta(\frac{l_i}{l_{\max}} - \beta) = \alpha \cdot \frac{N^{"}}{N} \tag{9}$$

Where $N^{"}$ is the number of nodes with initial load larger than $\beta l_{\max}$

In the NM model, the cost is

$$e_{NM} = \frac{1}{N}\sum_{i=1}^{N}(\alpha \frac{B_i}{\mu ND + \mu}) \tag{10}$$

Generally the number of nodes of a network is large, thus

$$e_{NM} = \frac{1}{N}\sum_{i=1}^{N}(\alpha \frac{B_i}{\mu ND}) \tag{11}$$

Because $\sum_{i=1}^{N} B_i = N(N-1)D$, the equation above can be simplified to

$$e_{NM} = \frac{1}{\mu N}\alpha \frac{\sum_{i=1}^{N} B_i}{ND+1} \approx \frac{\alpha}{\mu} \tag{12}$$

Apparently, when $\mu = 1$, the cost of our model is equal to ML model.

4 Simulation and Application

There are three kinds of common network topology in the wireless sensor network: (1) line structure based on chains, and the sensor nodes are connected in series on one or more chains in this network topology, while, users are connected at the end of the chains; (2) planar structure based on network, the wireless sensor network is connected into a network and very robust, which has a good flexibility; (3) hierarchical structure based on cluster, and this network topology possesses the naturally distributed processing ability, meanwhile, cluster head is the distributed processing center, and sensor nodes deliver the data to the cluster head, accordingly, the processing and fusion of the data is finished in the cluster head, then the results will be delivered through multi-hop by other cluster heads or directly delivered to the

users. In this letter, we will not only apply three matching models of capacity mentioned above, but also analyse the effect of the models on different network topology.

The final purpose of our research is to maximize the benefits within limited resources. The traditional method is to allocate larger capacity to the node with the largest degree or load, which may only obtain a tiny benefit even a negative one in some circumstance. Therefore, it is important to find the optimal strategy of capacity allocation in order to maximize the profit of the investment.

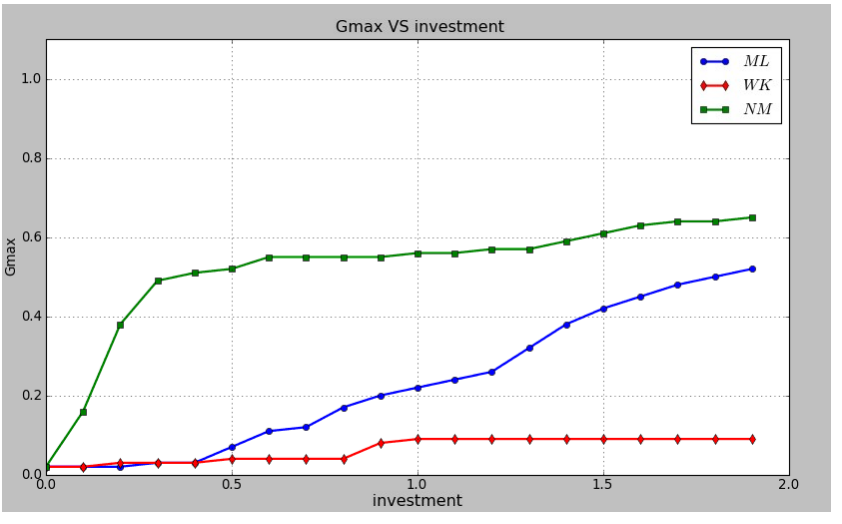

Fig. 2. The effects of ML,WK, NM on the topology of line structure based on chains

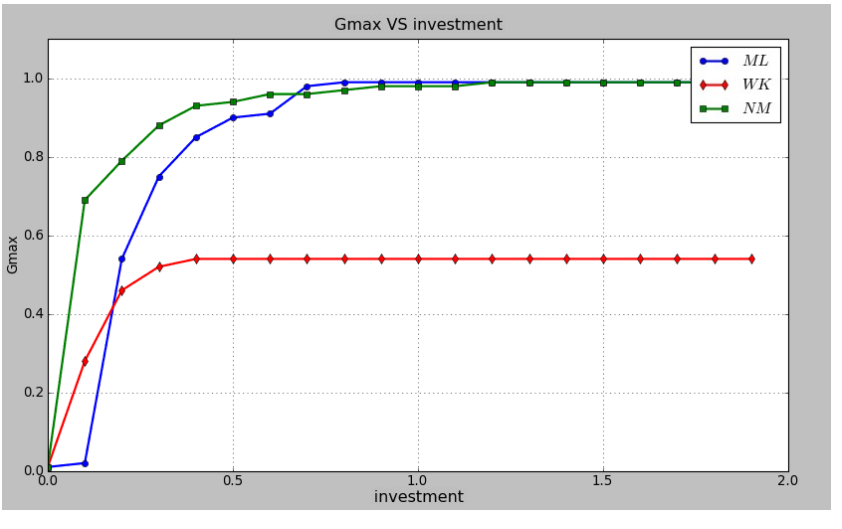

Fig. 3. The effects of ML,WK,NM on the topology of planar structure based on network

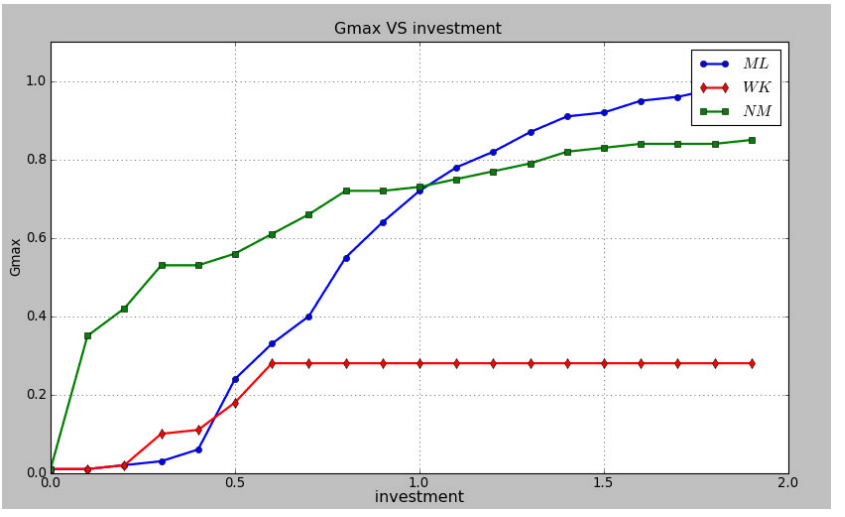

Fig. 4. The effects of ML,WK, NM on the topology of hierarchical structure based on cluster

In this paper, we call $G_{\max}$ and cost e as the income and the cost functions respectively. we illustrate how the models work in practice by considering three sensor network topologies: (1) line structure based on chains; (2) planar structure based on network;(3) hierarchical structure based on cluster. The tested sensor network is created according to the BA mode with network size N=1000, average degree <k>=4.

Here we focus on failures triggered by the removal of a single node, which is among those with higher load.

Figure 2 describes the effect of the models applied on three different sensor network topologys, abscissa is the investment for the nodes of wireless sensor network, vertical axis is $G_{\max}$, indicating flexibility of the network confronts deliberately attacks and random failures. The larger $G_{\max}$ is, the better the matching model of capacity is. Constructing a wireless sensor network according the strategy of this model can make the network get a higher robustness. In Figure 2, we can see that, applying ML, WK and NM to the construction of sensor network that is based on the topology of line structure based on chains. Therefore, the NM model get the highest profit, and the NM model has the best robustness against the failures. Figure 3 reveals that when the abscissa increase from 0 to 0.66, the effect of NM is better than ML and WK. However, when the abscissa increases from 0.66 to 1.2, the effect of ML is better than NM, and the effect of ML and NM is nearly the same lever at 1.0 when abscissa is larger than 1.2.This indicates that constructing wireless sensor network according to the topology of planar structure based on network can get a higher robustness.

Figure 4 reveals that when the abscissa increase from 0 to 1.02, the effect of NM is obviously better than ML and WK, but when the abscissa increase larger than 1.02, the effect of ML is better than WK and NM. To sum up the three figures above, we can find out that when allocating different investment on different topologys, the ML.

WK and NM can get different effects. But overall the effect of NM is better than ML and WK.

5 Conclusion

The main idea in our research is the same as in existing studies: in a highly heterogeneous wireless sensor network with a broad load distribution, nodes with large loads should be more protected by assigning large capacities such as processing power, storage capacity and communication capability. This study presents how to enhance robustness of the wireless sensor network by the way of allocating more capabilities to the important and hub nodes based on the concept of robustness of complex network. We proposed three matching models of capacity (ML, WK and NM) then applied these matching models of capacity on three common kinds of wireless sensor network topologies and compared the effects of these modes. Simulation results show that improves the robustness of the wireless sensor networks through allocating more processing and communication capabilities to the important and hub nodes is definitely feasible. Under the same network investment, applying the algorithm of NM model can get a higher robustness. we believe this work have its theoretical importance and potential application in designing wireless sensor networks from the point of economic view. It can also provide guidance in designing more robust artificial networks.

Acknowledgments. The authors would like to appreciate the financial support from the National Natural Science Foundation of China (No. 50977022) and Hunan Provincial Innovation Foundation For Postgraduate (No. CX2010B150).

References

1. Li, D., Wong, K.D., Yu, H.H., Sayeed, A.M.: Detection, classification, and tracking of targets. IEEE Signal Process. Mag. 19(3), 17–29 (2002)
2. Madden, S.R., Franklin, M.J., Hellerstein, J.M., Hong, W.: The design of an acquisitional query processor for sensor networks. In: Proceedings of the SIGMOD Conference, pp. 491–502. ACM Press, New York (2003)
3. Ma, Z.C., Sun, Y.N., Mei, T.: Survey on wireless sensors network. Journal on Communications 25(4), 114–124 (2004)
4. Almomani, I., Al-Akaidi, M., Reynolds, P., Ivins, J.: Architectural framework for wireless mobile adhoc networks. Computer Communications 30(1), 178–191 (2006)
5. Smart Dust, `http://robotics.eecs`; Berkeley, Edu/~pister/SmartDust/
6. Aldosari, S.A., Moura, J.M.F.: Detection in decentralized sensor networks. In: Proc. ICASSP, Montreal, QC, Canada, May 2004, pp. 277–280 (2004)
7. Chamberland, J.-F., Veeravalli, V.V.: Asymptotic results for decentralized detection in power constrained wireless sensor networks. IEEE J. Sel. Areas Commun. 22(6), 1007–1015 (2004)
8. Tsitsiklis, J.N.: Decentralized detection by a large number of sensors. Math. Control Signals Syst. 1(2), 167–182 (1988)

9. D'Costa, A., Ramachandran, V., Sayeed, A.M.: Distributed classification of Gaussian space-time sources in wireless sensor networks. IEEE J. Sel. Areas Commun. 22(6), 1026–1036 (2004)
10. Paul, G., Tanizawa, T., Havlin, H., et al.: Optimization of robustness of complex networks. Eur. Phys. J B 38, 187–191 (2004)
11. Albert, R., Jeong, H., Barabási, A.-L.: Error and attack tolerance of complex networks. J. Nature 406, 378–382 (2000)
12. Watt, D.J., Strogtz, S.H.: Collective dynamics of small-world networks. J. Nature 393, 440–442 (1998)
13. Barabási, A.L., Albert, R.: Emergence of scaling in random networks. J. Science 286(5439), 509–512 (1999)
14. Newman, M.E.J.: Model of the small world. Journal of Statistical Physics 101, 819–841 (2000)
15. Strogatz, S.H.: Exploring complex networks. Nature 410, 268–276 (2001)
16. Albert, R., Barabási, A.L.: Statistical mechanics of complex networks. Reviews of Modern Physics 74, 47–97 (2002)
17. Dorogovtsev, S.N., Mendes, J.F.F.: Evolution of networks. Advances in Physics 51, 1079–1187 (2002)
18. Schafer, M., Scholz, J., Greiner, M.: Proactive Robustness Control of Heterogeneously Loaded Networks. Phys. Rev. Lett. 96, 108701 (2006)
19. Holme, P., Kim, B.J., Yoon, C.N., Han, S.K.: Attack vulnerability of complex networks. Phys. Rev. E 65, 056109 (2002)
20. Zhao, L., Park, K., Lai, Y.C.: Attack vulnerability of scale-free networks due to cascading breakdown. Phys. Rev. E 70, 035101(R) (2004)
21. Motter, A.E.: Cascade Control and Defense in Complex Networks. Phys. Rev. Lett. 93, 098701 (2004)
22. Crucitti, P., Latora, V., Marchiori, M.: Model for cascading failures in complex networks. Phys. Rev. E 69, 045104(R)(2004)
23. Pister, K., Hohlt, B., Jeong, J., Doherty, L., Vainio, J.P.: Ivy-A sensor network infrastructure (EB/OL) (2003), http://www-bsac.eecs.berkeley.edu/projects/ivy
24. Corson, S., Macker, J., Batsell, S.: Architectural considerations for mobile mesh networking. Internet Draft RFC Version 2 (1996)
25. Warneke, B., Last, M., Liebowitz, B., Pister, K.S.J.: Smart dust: Communicating with a Cubic-millimeter computer. IEEE Computer Magazine 34(1), 44–51 (2001)
26. Tilak, S., Abu-Ghazaleh, N.B., Heinzelman, W.: A taxonomy of wireless micro-sensor network models. J. Mobile Computing and Communication Review 1(2), 1–8 (2002)
27. Li, J.Z., Li, J.B., Shi, S.F.: Concepts, issues and advance of sensor networks and data management of sensor networks. J. Journal of Software 14(10), 1717–1727 (2003)
28. Peters, L., Moerman, I., Dhoedt, B., Demeester, P.: Q-WEHROM: Mobility support and resource reservations for mobile senders and receivers. J. Computer Networks 50(6), 1158–1175 (2006)
29. Bonnet, P., Gehrke, J., Seshadri, P.: Querying the physical world. IEEE Personal Communication 7(5), 10–15 (2000)
30. Tanizawa, T., Paul, G., Cohen, R., Havlin, S., Stanley, H.E.: Optimization of network robustness to waves of targeted and random attacks. J. Phys. Rev. E 71, 047101 (2005)
31. Cohen, R., Erez, K., ben-Avraham, D., Havlin, S.: Resilience of the internet to random breakdowns. J. Phys. Rev. Lett. 85, 4626 (2000)

32. Cohen, R., Erez, K., ben-Avraham, D., Havlin, S.: Breakdown of the internet under intentional attack. J. Phys. Rev. Lett. 86, 3682 (2001)
33. Motter, E.A.: Cascade control and defense in complex networks. Physical Review Letters 93(9), 98701 (2004)
34. Newman, M.E.J.: The structure and function of complex networks. SIAM Review 45(2), 167–256 (2003)
35. Motter, A.E., Lai, Y.-C.: Cascade-based attacks on complex networks. J. Phys. Rev. E 66, 065102 (2002)
36. Wang, B., Kim, B.J.: A High Robustness and Low Cost Model for Cascading Failures. J. Europhys. Lett. 78, 48001 (2007)