Cumhuriyet Üniversitesi Fen Fakültesi
Fen Bilimleri Dergisi (CFD), Ciltl:36 , No:3 Özel Sayı (2015)
ISSN: 1300-1949

Cumhuriyet University Faculty of Science
Science Journal (CSJ), Vol.36 , No:3 Special Issue (2015)
ISSN: 1300-1949

Discovery of black holes in complex networks

Mina HASHEMİNİK[1,*], Alireza MİRZAEİ[2], Hamed MOHSENİ[3]

[1]*Department of computer, Qazvin Branch, Islamic Azad University, Qazvin, Iran; Email:*

[2]*Young Researchers and Elite Club, Qazvin Branch, Islamic Azad University, Qazvin, Iran*

[3]*Department of computer, Damavand Branch, Islamic Azad University, Damavand, Iran*

Received: 01.02.2015; Accepted: 05.05.2015

Abstract. Networks are vital in today's world. Design and configuration of networks have made the special considerations necessary for its various aspects such as security, integrity, scalability and cost. Malicious nodes on the network must be identified to enhance the resistance of network. Thus, detection of malicious nodes is critical in the networks .The concepts are presented in this article such as cross talking and black holes and studied networks are under the influence of random and targeted attacks. Also some algorithms have been developed to assess the vulnerability value and networks analysis against random and targeted failures in terms of establishment and detection of black holes and measurement of cross talking value in order to analyze the complex networks by help of above mentioned implications. The proposed strategies will allow us to design the networks and to reduce the threshold to secure them for all modes of problems (targeted and random).

Keywords: computer networks, complex networks, cross talking, black hole, failure rate.

1. INTODUCTION

In recent years, more attention has been paid to the study of complex networks. The systems include a dozen of basic components with bilateral connections. These systems are usually displayed with graph which forms individuals, graph nodes and dependencies between people such as friendship, kinship, business, common interests etc. The more complex of network, the more nodes and edges between them and they can be examined via network analysis.

A variety of complex networks ranged from random graph to networks with free scale degree distribution and small world have been reviewed and analyzed in this article. The purpose of this paper is to provide the indicators to assess the vulnerability and increase of the reliability and robustness of the networks through the development of strategies that do not require knowledge about the degree of nodes or global information in network and its structure.

Both nodes in the network may communicate with each other, if this connection is safe, so it will not be a threat to the network. But if the connection between two nodes is unsafe, the connection may be detriment to the network and even the network is compromised. We ourselves define the conception of these safe and unsafe connections for the network. If, after defining the connections, both nodes that do not have a safe connection with each other, they establish a connection with each other and influence each other, we say that both nodes interact with each other unintentionally. We call this unwanted interplay as cross talking. There are nodes in the network which are dangerous for the network. Being dangerous is meant the same unwanted effect on other network nodes; we call such nodes as black hole. The black holes themselves cause the cross talking and lead the other nodes of network to be involved and

* Corresponding author. *Email address*: *Mina_hasheminik@yahoo.com*

Special Issue: The Second National Conference on Applied Research in Science and Technology

become a black hole. Since the black hole destroys any input agent without leaving a trace of the failure, it will try to discover the agents in the networks as quick as possible in order to save the other agents. This is possible by preventing the contact with the black holes.

Search on black holes issues has recently attracted the attention of many researchers [1-5]. Since the concept of black holes has not been investigated in the complex networks, the purpose of this paper is to examine them in the complex networks to create an incentive to conduct the new researches in this field. The location of the nodes is important in the wireless networks or Interconnection Networks, but no matter the geographic location of the nodes in the complex networks.

For example, in the case of wireless sensor networks, Chong has studied the problem in [6] from a security perspective that the nodes have been expanded in a dangerous environment and they should be able to detect the intrusion. In [7]Cerpa and Estring stressed on the importance of the problem of detection of failure in the network. They benefited from the viewpoint of their own topology.

In [8] Kleinberg has dealt with question of recognition of a failure in a wired network. The failure has been described in the network as following: the network is divided into different groups after failure that their number depends on the disabled edges. In the article [9], Shrivastava has presented the randomized algorithms and failure to detect the disruption of network using a set of directory nodes to monitor the linear failures in the network. This work has been done on the paper [8]. Also in [10] Ritter has selected a source node and displays a message on the network. If Border nodes lose the message more than a specified number, they recognize the failure in the network through the source nodes.

The most recent detection algorithm of failure is provided by Barooah [11]. He has overcome many problems associated with previous solutions. The proposed algorithm is DSSD actually perceived as an abbreviation of Distributed Source Separation Detection. This algorithm is able to detect the failure in a distributed way. Two protocols namely ER-CD and LR-CD are provided to improve the algorithm [12]. The first is an improved detection protocol that offers the energy efficiency and more power against the attacks of disguise and impersonation. The next protocol is a detection protocol of the failure for source position where ER-CD is very heavy. This lightweight protocol ascends the position of failure detection algorithm with the power against the identity change attacks with Computations and memory low costs.

In a network, the information state of all nodes is the same at the outset and the overall network topology is determined, but the nodes do not know anything about the number and location of black holes. Thus, the detection of black holes is crucial until the other nodes of network know them in order not to establish such connection with such nodes. In this study, it has tried to attack the complex network. Number of edges in the network is destroyed due to this attack. Then 2 algorithms are used to identify the black holes in some complex networks using the cross talking rate.

According to the new criteria, it was concluded that the rate of cross talking is increased with increasing the degree of a node in the network so that the degree reaches a certain amount. But after that value, the increase in degree causes the reduced cross-talking rate. The results on the artificial graphs as well as also on the real world graph are done using MATLAB programming language.

In this paper in the second part, the various forms of cross talking and problems are described in the complex networks. In the second part, a new method is provided to detect the black hole nodes. And simulation results have been discussed in the Section three. And in the last section summary and conclusions is provided.

2. THE PROPOSED SOLUTİON

Since computer networks have infiltrated in our life substantially and via the networks, we have established the connection with many people for whom that there is no data and their work and life, the security and reliability of networks is a critical issue. In this section, we try to introduce the basic concepts used in the proposed method. For example, consider a network with **N** nodes. Each of these nodes may be problematic and passes its problem to other nodes. If the network is able to secure the nodes against each other, then we show 2secured nodes against each other by creating an edge between them.

The challenges of network monitoring are provided in the many articles [6-7]. But so far none of the solutions have been proposed and used about the complex networks. Algorithm Proposed in this paper is used for the detection of black hole nodes in the complex networks. We use the cross talking rate to obtain the cross talking in each node. We have calculated the cross talking that is created by node **u** in the interval **(t, t+dt)** with the Weibull distribution. It has been shown experimentally and theoretically that the Weibull distribution is a suitable approximation for the distribution of favorable lifespan probability.

2.1. Analytic evaluation of the proposed method

Burtoni (1964) has introduced some of the Weibull distribution applications. We also consider the time of cross talking created by a node as a random variable x in a similar case in this project. Then its density function is as follows:

$$f_X(t) = \begin{cases} 0, & X < 0 \\ \frac{k}{\theta\Theta}\left(\frac{x}{\theta\Theta}\right)^{k-1} e^{-\left(\frac{x}{\theta\Theta}\right)^k}, & X \geq 0 \end{cases} \quad (1)$$

In which k>0 is the form parameter and θ>0 scale parameter.

Its cumulative distribution function is as follows:

$$F_X(t) = \begin{cases} 0 \quad , & X < 0 \\ 1 - e^{-\left(\frac{x}{\theta\theta}\right)^k}, & X \geq 0 \end{cases} \quad (2)$$

So using the density function, we obtained the u node cross talking rate with respect to relations (1) and (2):

$$\lambda_X^u(x) = \frac{f_X(t)}{1-F_X(t)} = \frac{\frac{k}{\theta\Theta}\left(\frac{x}{\theta\Theta}\right)^{k-1} e^{-\left(\frac{x}{\theta\Theta}\right)^k}}{1-\left(1-e^{-\left(\frac{x}{\theta\Theta}\right)^k}\right)} = \frac{k}{\theta\Theta}\left(\frac{x}{\theta\Theta}\right)^{k-1} \quad (3)$$

In the cross talking created between node u and other nodes that are not connected to it, We consider the parameter k as node u , Because the Weibull distribution density function for k> 1 increases along with the increase of k And it reaches the maximum level then it starts to decline. We consider the parameter θ as $\frac{1}{\overline{d_v}}$ that:

$$\overline{d_v} = \frac{\sum_{v \notin \aleph_u} d_v}{N} \quad (4)$$

$\aleph_u$ is the neighbors of u node within the network and N as vertices of the network.

Also cross talking rate for the entire network is also obtained through total rates of cross talking of all network nodes:

$$\Lambda\Lambda_X^N(t) = \sum_{u\in N} \lambda_X^u(t) \quad (5)$$

Since the first graph is a tree, we consider the threshold value for the tree. Each tree is N-1 has an edge, so the mean degree of each vertex is equal to:

$$\frac{2(\mathrm{N}-1)}{\mathrm{N}} \quad (6)$$

We consider this value as the degree of each node, and locate it in the cross talking rate of each node. The number of nodes that are not connected to each network node is equal to:

$$(\mathrm{N}-1)-\frac{2(\mathrm{N}-1)}{\mathrm{N}} = \frac{\mathrm{N}^2-3\mathrm{N}-2}{\mathrm{N}} \quad (7)$$

At formula of cross talking rate of each node we will have:

$$\mathrm{K}=\frac{2(N-1)}{N} \quad (8)$$

And

$$\frac{1}{\boldsymbol{\theta}} = \frac{2(N-1)(N^2-3N-2)}{N^3} \quad (9)$$

So we have:

$$\lambda_X^u(x) = \frac{4(N-1)^2(N^2-3N-2)}{N^4}\left(\frac{2x(N-1)(N^2-3N-2)}{N^3}\right)^{\frac{N-2}{N}} \quad (10)$$

As a result:

$$\Lambda\Lambda_X^N(t) = \sum_{u\in N} \lambda_X^u = \mathrm{N}\frac{4(N-1)^2(N^2-3N-2)}{N^4}\left(\frac{2x(N-1)(N^2-3N-2)}{N^3}\right)^{\frac{N-2}{N}} \quad (11)$$

Then in the network, delta values will be as follows:

$$\delta_N=\lambda_X^u(x) = \frac{4(N-1)^2(N^2-3N-2)}{N^4}\left(\frac{2x(N-1)(N^2-3N-2)}{N^3}\right)^{\frac{N-2}{N}} \quad (12)$$

And

$$\Delta_N=\Lambda\Lambda_X^N(t) = \mathrm{N}\frac{4(N-1)^2(N^2-3N-2)}{N^4}\left(\frac{2x(N-1)(N^2-3N-2)}{N^3}\right)^{\frac{N-2}{N}} \quad (13)$$

then in each network with N node, we get to the delta values via insertion instead of N. In the end, we compare its cross talking rate with desired threshold limit for detecting a black-hole, so as we have for node u:

$$\lambda_X^u(x) > \delta_N \quad (14)$$

When the node u is considered a black hole. Also, if we have for the entire network:

$$\Lambda\Lambda_X^N(t) > \Delta_N \quad (15)$$

Then the network N will be at risk.

2.2. Description of the proposed method

Firstly the intended network is considered a graph as an input (algorithm 1, line 1), Then we get its corresponding adjacency matrix. We consider a person as the master node that is the network administrator. Then, the whole network is divided into equal clusters by the master node

(Algorithm 1, line 5) Master node selects the node with the highest safety as a directory of cluster in each category, (Algorithm 1, lines 6-11).

Algorithm1. Clustering and electing leader

Input: G(V, E), N, x, C // network with edges and vertex.
Input: C, N, t // C: number of clusters, N: number of nodes, t: time.

Output: AN = $[an_a]$, MN = $[mn_m]$ // AN: set of alone nodes, MN: set of malicious node.
01: Divide network into C clusters.
02**: Repeat**
03: Send Question MSG about nodes in cluster to all.
04: Run Answer () as per nodes in cluster.
05: **For** all nodes in each cluster:
06: EL (i) ← No MSG +.
07: **End For**
08: Elect node with max EL (i) as a leader.
09: $\delta=\frac{4(N-1)^2(N^2-3N-2)}{N^4}\left(\frac{2t(N-1)(N^2-3N-2)}{N^3}\right)^{\frac{N-2}{N}}$ // δ: node threshold.
10: Δ = N * δ. // Δ: network threshold.
11: **For** each leader
12: Send Question MSG about leader to all.
13: Run Answer () as per nodes.
14: d (i) ← No MSG +,
15: $\lambda=\frac{d}{\theta\Theta}\left(\frac{t}{\theta\Theta}\right)^{d-1}$, // calculate cross talk rate of node.
16: $\theta=\left(\frac{\sum_{v\notin\aleph} d_v}{N}\right)^{-1}$ // θ: avg degree of non-neighbor nodes.
17: **If** λ> δ **then**
18: Add leader to MN set.
19: **End If**

20**:** **End For**
21: **Until** λ <= δ
22: **For** each leader

23: Run Algorithm2.
24: **End For**
25: Λ = ΣλC. // calculate cross talk rate of network.
26**: If Λ> Δ then**
27: Risk for network.
28**: End If**

Function1. Answer

01**: If** have a direct connection with other node then
02: Send MSG + to sender.
03: **Else**
04: Send MSG- to sender.
05: **End If**

Algorithm2. Leader code

01: Send Cluster Information MSG to all nodes in cluster
02**: For** all nodes in cluster
03: Update information.
04**: If** a node is disconnected **then**
05: Add node to AN set.
06: **End If**
07**: End For**
08: Send Question MSG about all nodes to nodes in cluster.
09: Run Answer () as per nodes in cluster.
10: **For** each node in cluster:
11: d (i) ← No MSG +,
12: $\lambda=\frac{d}{\theta}(\frac{t}{\theta})^{d-1}$ // calculate cross talk rate of node.
13: $\theta=(\frac{\sum_{v\notin N} d_v}{N})^{-1}$ // θ: avg degree of non-neighbor nodes.
14**: If** $\lambda > \delta$ **then**
15: Add leader to MN set.

16: **End If**
17**: End For**
18: $\lambda C=\sum_{v\in C}\lambda_v$. // Calculate cross talk rate of cluster

The next step is to update the information of nodes by the Supervisor. So every directory node sends a message to its members so called clustered information after the election of clusters directories (algorithm 2). Each node calculates the number of its safe connections in every iteration of this method. Connection Status of each member of the cluster is checked relative to the desired directory in each cluster. If the node is not connected to the directory, we introduce it as an isolated node (algorithm 2, lines 4-6).

The discovery phase begins on the first iteration after this process. But in the next iterations, it is necessary that the master node chooses a new directory for the cluster, if the directory node is a black hole node due to network changes (Algorithm 1, line 19). Each directory sends any messages to all members of its cluster in the early stages of discovery stage. The directory asks every node's opinion about the other nodes network security with these messages (algorithm 2, line 8). Each normal node in the cluster is required to respond to it after receiving the message (function 1). Directory node has a number to as the security value of required node for each node at the end of each round of messages exchange.

Each directory node is able to detect the black hole node whit in the network having information of network nodes by comparing the value of cross talking of cluster nodes associated with the desired threshold value. Master node also identifies the directory nodes of the black hole by mentioned method.

Master node is able to identify the risk in the network after detecting the black hole nodes in the network by comparing the value of entire network cross talking with threshold limit of the network cross talking (algorithm 1, lines 23-25).

3. SİMULATİON THEOREMS

Various artificial networks is intended as a small world, free scale with Barabasy-Albert algorithm and Erdush-Renay random graph as input. We have used the real data from the social network Face-book and the network graph Enron Email to final implementation and impact of attacks. Artificial graphs are connected, directionless, weightless and dynamic. Dynamism of a network is meant: always edges are added to the network and number removed from the network due to network attacks. 2012 MATLAB simulation environment and two random and targeted attacks have been used to attack the network.

3.1. Simulation results

In this section, we describe the function of cross talking rate with its variables. As you can see in Figure 1, cross talking rate also increases with increase of anode degree until it reaches a maximum value and then it begins to decline. Thus, when the degree of node increases, the likelihood of unsafe connection of the node also increases As far as the number of nodes safe connections is more than unsafe connections. From now on, the number of safe connections will increase and cross talking rate decreases with the increase of node degree. The value of node cross talking rate is equal to zero in two modes. The first is when the node is isolated and is not dangerous to the network due to lack of any node. And the second mode occurs when the degree of a node is full, i.e. it has a safe connection to all network nodes.

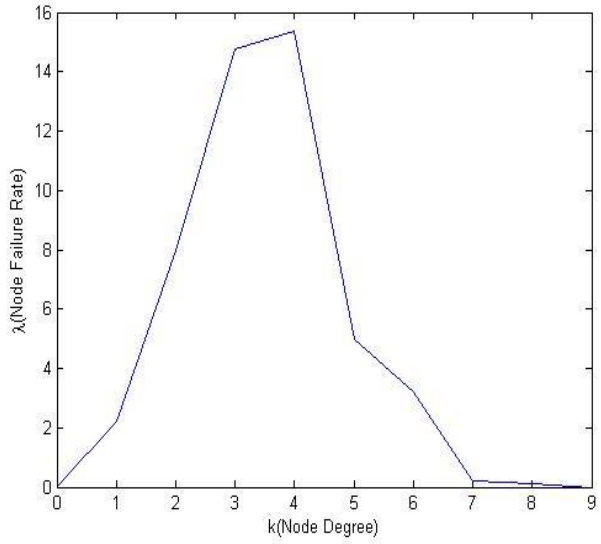

Figure 1: cross talking rate changes of the node based on changes in the degree of that node

The degree of a node is not the only factor in the rate of cross talking. As we saw in equation (3), another factor will influence such as the degree of non-neighboring nodes. Node cross talking rate changes is shown in Figure 2 based on changes of total non-neighboring nodes degrees in the intended node to understand this concept. This factor also has a direct connection with cross talking rate of the same node of node degree.

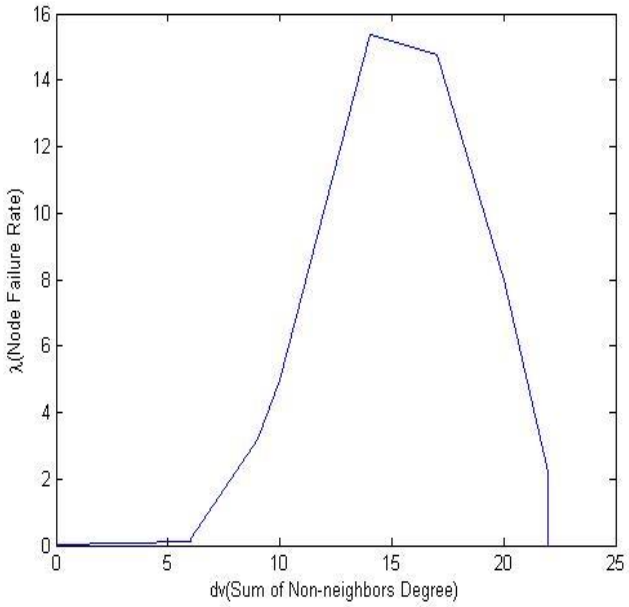

Figure 2: cross talking rate changes of the node based on changes in the total degrees of non-neighboring nodes

In this article, some sentences have been used that ultimately lead to the loss of network edges and reduction of their number. Both figures 3 and 4 show the result of edge removal in order to study the impact of these attacks on Cross talking rate of the entire network. The result of repeated attacks to the intended graph shown in Figure 3 and this is shown as an average in Figure 4. As it is marked in both figures as well, the entire network failure rate increases to reach a maximum value by increasing the number of edges deleted. Then it starts to decline, this is when the graph is dismissed as far as the graph is completely discrete and network failure rate reaches zero.

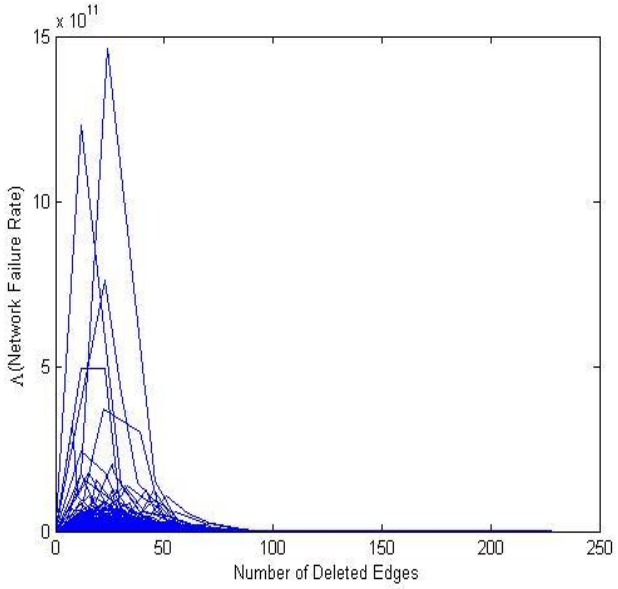

Figure 3: impact of number of edges deleted on network failure rate

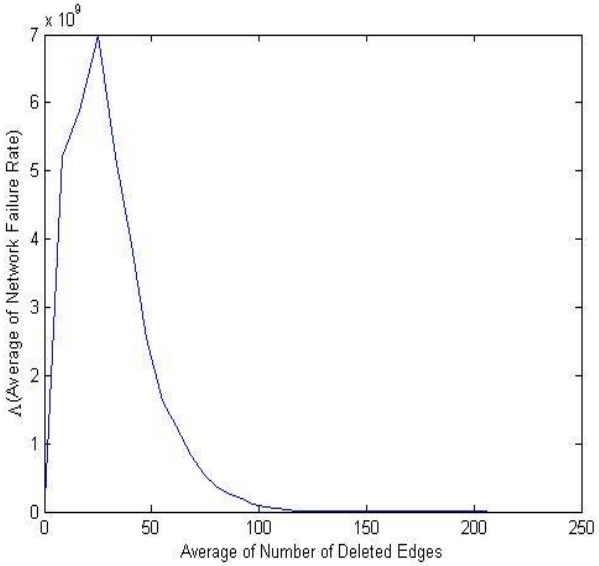

Figure 4: Mean impact of deleted edges on the network failure rate

4. SUMMARY AND CONCLUSİONS

The cross talking is the tendency of two nodes for unwanted interaction impact on each other. We use the failure rate to gain the cross talking for each node. If the failure rate is higher than its threshold, the node is malicious. Black hole is a malicious node that causes the transformation of other existing nodes into one destructive node in the network as well. Network is at risk when the network failure rate exceeds the threshold value.

We have introduced a new method of detection with new criteria for identifying the black hole nodes in the network and benchmarked its performance quality in this article. At first, the concept of complex networks, sophisticated network attacks and challenges are described for more learning and better understanding the issue. Then the proposed method is investigated and we have provided the used criteria and the proposed detection algorithm and the results from simulation on artificial and natural graphs.

Erdush-Renay structured graph is most vulnerable against the attacks of the black hole, according to the obtained results. But the pace of algorithm implementation on this graph has been more than rest and it wastes the less time. Enron email natural network graph has a great strength and it is considered a powerful network structurally.

REFERENCES

[1] C. Cooper, R. Klasing, and T. Radzik, "Locating and Repairing Faults in a Network with Mobile Agents," *Theoretical Computer Science*, vol. 411, no. 14, pp. 1638-1647, 2010.

[2] J. Chalopin, S. Das, A. Labourel, and E. Markou, "Black Hole Search with Finite Automata Scattered in a Synchronous Tours," *In Distributed Computing*, Springer Berlin Heidelberg, pp. 432-446, 2011.

[3] J. Chalopin, S. Das, A. Labourel, and E. Markou, "Tight Bounds for Scattered Black Hole Search in a Ring," *Structural Information and Communication Complexity. Springer Berlin Heidelberg*, pp. 186-197, 2011.

[4] S. Dobrev, P. Flocchini, G. Prencipe, and N. Santoro, "Searching For a Black Hole in Arbitrary Networks: Optimal Mobile Agent Protocols," *in: Proceedings of the twenty-first annual symposium on Principles of distributed computing*. ACM, 2002.

[5] W. Shi, "Black Hole Search with Tokens in Interconnected Networks," *Stabilization, Safety, and Security of Distributed Systems. Springer Berlin Heidelberg*, pp. 670-682, 2009.

[6] C. Y. Chong, and S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," *in: proceedings of IEEE*, vol. 91, no. 8, pp. 1247-1256, 2003.

[7] A. Cerpa, and D. Estrin, "ASCENT: Adaptive Self-configuring Sensor Networks Topologies," *mobile computing, IEEE transactions on*, vol.3, no. 3, pp.272-285, 2004.

[8] J. Kleinberg, "Detecting a Network Failure," *Internet Mathematics*, vol. 1, no. 1, pp. 37-55, 2004.

[9] N. Shrivastava, S. Suri, and C. D. Tpth, "Detecting Cuts in Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 2, pp. 1-25, 2008.

[10] H. Ritter, R. Winter, and J. Schiller, "A Partition Detection System for Mobile Ad-hoc Networks," *in: Proceedings of IEEE Conference on Sensor and Ad-hoc Communications and Networks (SECON)*, pp. 489-497, 2004.

[11] P. Barooah, "Distributed Cut Detection in Sensor Networks," *Decision and Control, 2008. CDC 2008. 47th IEEE Conference on*. IEEE, pp. 1097-1102, 2008.

[12] M. Won, S. M.George, and R. Stoleru, "Towards Robustness and Energy Efficiency of Cut Detection in Wireless Sensor Networks," *Ad Hoc Networks*, vol. 9, no. 3, pp. 249-264, 2010.

[13] L. Chun-Ping, L. Yu-Rong, H. Da-Ren, and Z. Lu-Jin," A Formula of Average Path Length for Unweighted Networks," *Communications in Theoretical Physics*, vol. 50, no. 4, 1017, 2008.

[14] A. Perisic, and C. T. Bauch, "Social Contact Networks and Disease Eradicability Under Voluntary Vaccination," *PLOS Computational Biology*, vol. 5, no. 2, e. 1000280, 2009.

[15] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Efficiency of Scale-Free Networks: Error and Attack Tolerance," *Phys. A, Statistical Mechanics and its Applications*, vol. 320, pp.622-642, 2008.

[16] I. Simonsen, L. Buzna, K. Peters, S. Bornholdt, and D. Helbing, "Dynamic Effects Increasing Network Vulnerability to Cascading Failures," *Phys. Rev. Lett*, vol. 63, no. 3, pp. 283-420, 2008.

[17] D. Centola, "Failure in Complex Social Networks," *Journal of Mathematical Sociology*, vol. 33, no. 1, pp. 64-68, 2008.

[18] S. Dobrev, N. Santoro, and W. Shi, "Scattered Mobile Agents Searchin for a Black Hole in an Unoriented Ring Using Tokens," *International Journal of Foundations of Computer Science*, vol. 19, no. 6, pp. 1355-1372, 2008.

[19] P. Flocchini, D. Ilcinkas, and N. Santoro, "Ping Pong in Dangerous Graphs: Optimal Black Hole Search with Pure Tokens," *In Distributed Computing. Springer Berlin Heidelberg*, pp. 227-241, 2008.

[20] D. Centola, "Failure In Complex Social Networks," *Journal of mathematical sociology*, vol. 33, no.1, pp. 64-68, 2008.

[21] J. Wu, H. Z. Deng, Y. J. Tan, and D. Z. Zhu, "Vulnrability of Complex Networks Under Intentional Attack With Incomplete Information," *Phys. A*, vol. 40, no. 11, pp. 2665-2671, 2007.