

<http://ansinet.com/itj>

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Connection Stability Analyze Based on LEACH Algorithm for Mobile Ad Hoc Network

¹Xuejun Wu, ¹Minghua Zhou, ²Limin Meng, ²Jingyu Hua, ¹Kai Zhou and ¹Ting Wu

¹College of Science, Zhejiang University of Technology, Hangzhou, 310032, China

²College of Information Engineering, Zhejiang University of Technology, Hangzhou, 310032, China

Abstract: The invulnerability of mobile ad hoc network is very important to the routing protocol. This study presents a mathematically tractable model of node motion to derive a precise relationship between mobility and connection stability. We improve the first order energy consumption model with dynamic clustering first and then build an incidence matrix to depict the connectivity of the network nodes in a dynamic network model. Finally, this study simulates the network invulnerability related to time. As a result, it validates the high invulnerability of the dynamic clustering ad hoc networks.

Key words: Energy consumption model, dynamic clustering, tractable model, invulnerability, incidence matrix

INTRODUCTION

A multi-hop wireless ad hoc network is a collection of nodes that communicate with each other without any established infrastructure or centralized control. Each of these nodes is a wireless transceiver that transmits and receives at a single frequency band which is common with each other. However, they are limited by their transmitting and receiving capabilities. Therefore, they cannot directly reach all of the nodes in the network as most of the nodes are outside the direct range. In such a situation, one of the possibilities for the information transmission between two nodes that are not in the range to have a direct communication is to use other nodes in the network (Johnson, 1994).

To investigate the impact of mobility on network operation, previous work has relied mainly on simulations with mobility models that describe the manner in which nodes move through space (Hill, 2003). These mobility models typically aim to provide an accurate description of the behavior of a network consisting of pedestrians or moving vehicles. It is unlikely that a single mobility model can be applied to all types of networks and for this reason, new mobility models are being continuously developed. It has proven to be very difficult to analyse the relationship between these mobility models and the network connectivity due to the many parameters affecting the network operation, such as node speed, pause time, node density and transmission range (Tillett *et al.*, 2002).

The performance of mobile ad hoc networks is highly sensitive to changes in node-to-node connections (communication links) caused by node movement. The kind of link instability has proven very difficult to analyse

mathematically, so previous work has relied heavily on simulation. In this study, we present a mathematically tractable model of node motion and node damage, the different rates of damaged nodes, the inconstant velocity model and uses it to derive a precise relationship between mobility and connection stability (Wadaa *et al.*, 2003). We further investigate connection stability in multi-hop communication and discover some underlying properties of previously proposed mobility metrics. In particular, we demonstrate that link duration has a strong invariant relationship with the stability of multi-hop connections for a wide range of mobility models and thus is an excellent mobility metric (Krishnan and Starobinski, 2003).

We approach the problem as follows. Firstly, we set up a relatively simple and mathematically tractable mobility model. Then we develop an analytic expression for connective stability to depict the connectivity of the network nodes in a dynamic network model in multihop communication. Finally, this paper brings forward a determinant algorithm of the network connectivity and a calculate method (Heinzelman *et al.*, 2000). We simulate the damage situation of the dynamic ad hoc network through random trials and quantification ally calculates the ratio of the network invulnerability, which related to time. As a result, it validates the high invulnerability of the mobile ad hoc network.

ENERGY CONSUMPTION MODEL

A sensor uses its energy to carry out three main actions: acquisition, communication and data processing. Although varying according to the monitoring type, the power consumption to perform the data acquisition is not very important. The communications consume model is shown in Fig. 1.

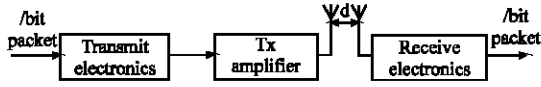


Fig. 1: Communication power consumption model in MANET

The communications consume model is shown in Fig. 1, to transmit a message of l bits over a distance of d meters, the energy that transmitter consumes is given by:

$$E_{Tx} = \begin{cases} E_{elec} + \epsilon_{fs} d^2 & d < d_0 \\ E_{elec} + \epsilon_{amp} d^4 & d \geq d_0 \end{cases} \quad (1)$$

where, E_{elec} , l , d and ϵ_{amp} denote energy of electronic signals; size of a message, distance between transmitter and receiver; and amplification factor, respectively. In addition, d_0 , M and d_{toBS} represent the limit distance over which the transmission factors change their value, the size of the area and the distance to the base station.

To receive a message of l bits, the receiver consumes:

$$E_{Rx}(l) = E_{elec} \times l \quad (2)$$

When there are N nodes in MANET, the optimal number of the Cluster-Heads (CHs) (Jung *et al.*, 2007):

$$k_{opt} = \frac{\sqrt{N} \sqrt{\epsilon_{fs}} M}{\sqrt{2\pi} \sqrt{\epsilon_{amp}} d_{toBS}^2} \quad (3)$$

Generally, we have $E_{elec} = 50$ nj/bit, $\epsilon_{amp} = 0.0013$ pj/bit/ m^4 and $\epsilon_{fs} = 10$ pj/bit/ m^2 .

DYNAMIC CLUSTERING ALGORITHMS

One of the most common clustering algorithms, the dynamic clustering technique, aims at assigning each pattern data set to the cluster having the nearest centroid. The basic steps of clustering are (Ali *et al.*, 2009):

- Step 1:** All nodes are assigned a cluster number between 1 and k randomly, k is number of cluster desired which can be computed from Eq. 3
- Step 2:** Find the cluster center of each cluster
- Step 3:** For each node, find the cluster center that is closest to the node. Assign the node to the cluster whose center is closest to it
- Step 4:** Re-compute the cluster centers with the new assignment of nodes
- Step 5:** Repeat Steps 3 and 4 till clusters do not change or within a fixed number of times

Dynamic clustering algorithms employ an iterative approach to group the node into a predefined k number of clusters by minimizing a cost function (Ranjan and Khalil, 2007):

$$\zeta = \sum_{i=1}^n \|d_i - C_j\|^q \quad (4)$$

where, C_j is the center of j th cluster and is the center nearest to node object d_j , n is the number of elements in node set, q is an integer which defines the nature of the distance function. For numeric valued nodes sets, a cluster center is represented by the mean value of each attribute and the mean value is computed over all objects belonging to the cluster.

ALGORITHM FOR INVULNERABILITY ANALYZE

To simulate the movement of the nodes in the mobile ad hoc network, we set up a ad hoc network scenario. There are N nodes in this scenario. Let $(x_i(t), y_i(t))$, $v_i(t)$ $\theta_i(t)$ be the coordinate, the velocity and the moving direction of mobile node i at time t . In our approach, these initial parameters are set with random. We assume a free space propagation model, where the received signal strength solely depends on its distance to the transmitter. These nodes are limited by their transmitting and receiving capabilities. Therefore, they cannot directly reach all of the nodes in the network as most of the nodes are outside the direct rang (Heinzelman *et al.*, 2002). In such a scenario, if two nodes can communicate with each other, the distance between these two nodes cannot exceed R . At arbitrary time t , the coordinate of the node i can be represented by Eq. 5 and the distance between node i and node j can be represented by Eq. 6.

$$\begin{cases} x_i(t) = x_i(t-1) + v_i(t)\cos\theta_i(t) \\ y_i(t) = y_i(t-1) + v_i(t)\sin\theta_i(t) \end{cases} \quad (5)$$

$$l_{ij}(t) = \sqrt{(x_j(t) - x_i(t))^2 + (y_j(t) - y_i(t))^2} \quad (6)$$

The algorithm for invulnerability analyze has very important senses to the research on mobile ad hoc network. But it has proven to be difficult to analyze mathematically. In this section, we can use graphic to represent the link and nodes in the networks. Thus we change the stability problem to the graphic problem. In the graphic problem, we can use the connective matrix to depict the connectivity of the network nodes in a dynamic network model (Camp *et al.*, 2002). We defined connective matrix as $D(t) = (d_{ij}(t))_{N \times N}$, the element in this matrix should satisfied in Eq. 7.

$$d_{ij}(t) = \begin{cases} 1 & l_{ij}(t) \leq R \\ 0 & l_{ij}(t) > R \end{cases} \quad (7)$$

We denoted $D^{(i)}(t)$ as the i th power of the matrix $D(t)$. Therefore, the connective matrix can be represented by Eq. 8.

$$D'(t) = \sum_{i=1}^{\infty} D^{(i)}(t) \tag{8}$$

Where, $D^{(m)}(t) = (d_{ij}^{(m)}(t))_{N \times N}$ if $d_{ij}^{(m)} = 0$ in this matrix, it means that node i cannot reach node j within m hops ($i \neq j, m \geq 1$). The graphic is not connectively if and only if there exist element $d'_{ij}(t) = 0, i \neq j$ in matrix $D'(t)$.

Therefore, we denote $X(t)$ as the number of nonzero elements in the $D'(t)$ and it can be used as a new index to estimate network invulnerability (Bianchi, 2000; Michierdi and Molva, 2003).

In mobile ad hoc network, we randomly choose $r\%$ nodes and damaged their communication ability to other nodes in the network to research the invulnerability in the scenario. Once the node which labeled i is damaged, the elements in the connective matrix will be changed, they should stratify Eq. 9.

$$d_{im}(t) = 0 (m \neq i) \tag{9}$$

It shows the node i can not communicate with other nodes in the network. It forms a new matrix $D'_n(t) = \sum_{i=1}^{\infty} D_n^{(i)}(t)$ based on $D'(t)$. We also denote $X_n(t)$ as the number of nonzero elements in $D'(t)$ to estimate network invulnerability when $k\%$ nodes are damaged. We define the invulnerability index K as Eq. 10.

$$K(t) = \frac{X(t)}{X_n(t)} \tag{10}$$

The algorithm diagram is shown in Fig. 2.

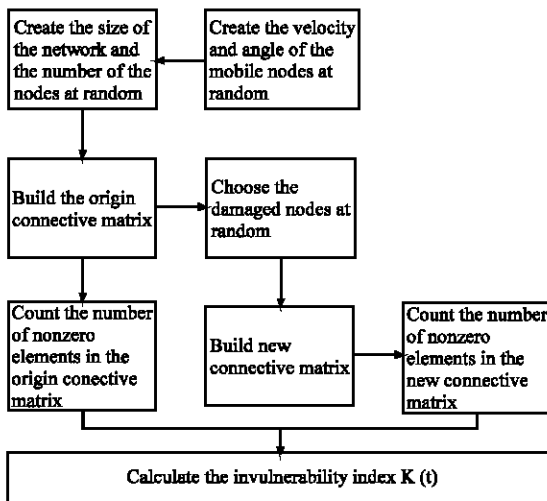


Fig. 2: Algorithm diagram for invulnerability analyze

SIMULATIONS

We use MATLAB to simulate the Energy Consumption Model. When the number of the nodes in sensor filed is growing, more CHs are needed. In dynamic clustering model our simulation models a network of 926 mobile nodes placed randomly within a 1000×1000 M area. From Eq. 3, we find that when there are 45 CHs in the sensor filed, the cost of energy consumption is the least. Using dynamic clustering model, we assign all the nodes in sensor filed into 45 classes, there are 45 classes shown in Fig. 3.

In ad hoc network, nodes are moving with time. In our simulation, we assume that the velocity of the nodes is in the interval (0.2 m sec^{-1}) with a normal distribution and the angle of the move is in the interval (0.2 m sec^{-1}) with a normal distribution. When the rate of damaged nodes is 10%, the result is given by Fig. 4.

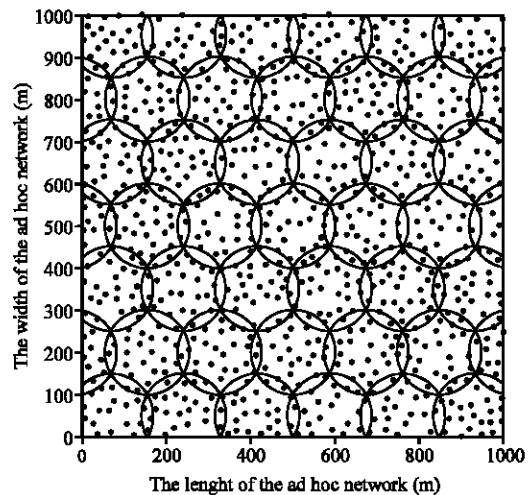


Fig. 3: Simulation of the dynamic clustering model

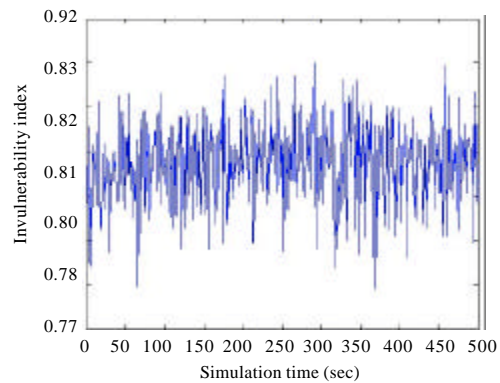


Fig. 4: The invulnerability index changed with the time when $r = 10\%$

From Fig. 4, it validates the high invulnerability of the mobile ad hoc network. The mobility has little impact on invulnerability index. When the rate of the damaged nodes is 10%, the invulnerability index fluctuations at interval 0.8 ± 0.01 .

When the rate of damaged nodes is 20%, the result is given by Fig. 5. When the rate of the damaged nodes is 20%, the invulnerability index fluctuations at interval 0.66 ± 0.02 .

In this mobile ad hoc network, we assume the maximum distance between two nodes which they can communicate with each other is 100 M. It's just one tenth of the length of the network area. Our simulation models different rates of damaged nodes in the network. We assume that if two nodes can communicate with each other they cannot exceed 2 hops. The damage rate vary from 0-100%, the invulnerability index is presented by Fig. 6.

From Fig. 6, we can find that if 10% nodes are damaged in the ad hoc network, the invulnerability index

will be reduced by 20%; if 20% nodes are damaged, the invulnerability index will be reduced by 38.75%, many communication requests will be denied.

In further, we discuss the maximum hops is not a constant to research the relationship between invulnerability index with maximum hop and rate of the damaged nodes in the network. The hops which two nodes can communicate with each other they cannot exceed is varied from 2 to 6 hops and the damage rate vary from 0-100%, the invulnerability index is shown in Fig. 7.

From Fig. 7, we can find that both the maximum hops and the rate of the damaged nodes in the network will have an effect on invulnerability index. The rate of the damaged nodes has a great effect on invulnerability index, while the maximum has a little effect.

For performance evaluations, this paper simulation our method and other methods that have been proposed in literature with the rate of the damaged nodes is 10%, it is shown in Fig. 8.

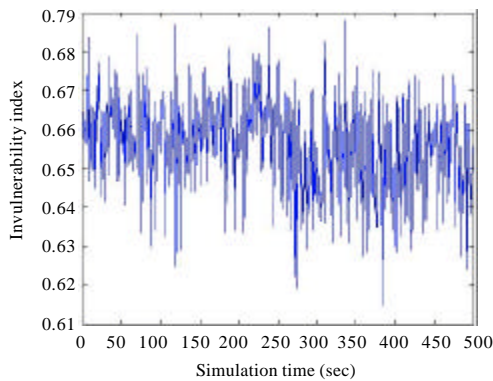


Fig. 5: The invulnerability index changed with the time when $r = 20\%$

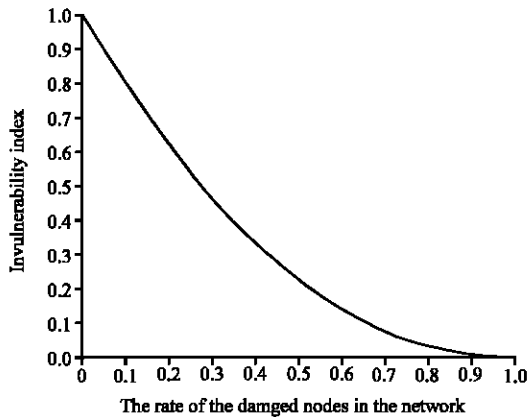


Fig. 6: The relationship between the rate of the damage nodes and the invulnerability index

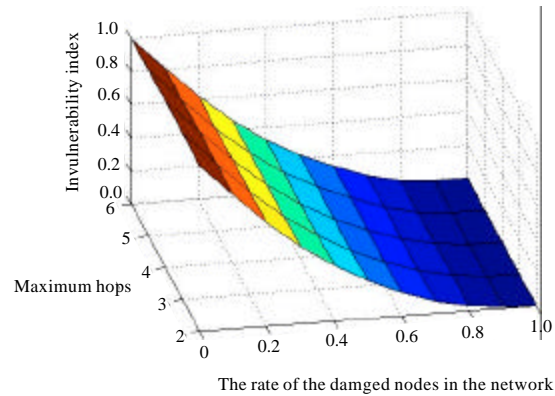


Fig. 7: The relationship between invulnerability indexes with maximum hop and rate of the damaged nodes in the network

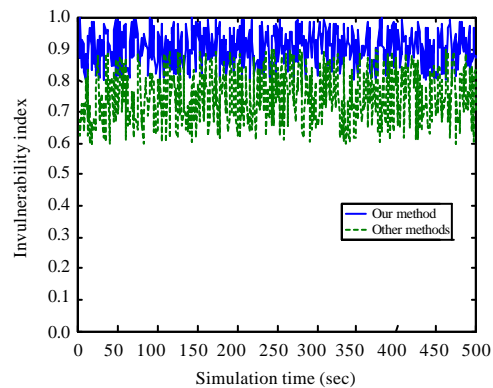


Fig. 8: The simulation of our method and other methods

From Fig. 8, we can find that our method is better than other methods that have been proposed in literature.

CONCLUSIONS

We have proposed an energy-aware routing algorithm for MANET which can also run efficiently under best-effort traffic. We have improved the first order energy consumption model with dynamic clustering; based on the clustering, we present a mathematically tractable model of node motion and nodes damage, the different rates of damaged nodes, the inconstant velocity model and use it to derive a precise relationship between mobility and connection stability. We present a new index to estimate network invulnerability and then build an incidence matrix to depict the connectivity of the network nodes in a dynamic network model. Finally, we simulate the damage situation of the dynamic ad hoc network through random trials and quantification ally calculates the ratio of the network invulnerability, which related to time. As a result, it validates the high invulnerability of the mobile ad hoc network.

ACKNOWLEDGMENT

The study is supported by the National Natural Science Foundation of China (60872020) and Zhejiang Provincial NSF undergrant No. Y1090645.

REFERENCES

- Ali, S.A., N. Sulaiman, A. Mustapha and N. Mustapha, 2009. K-means clustering to improve the accuracy of decision tree response classification. *Inform. Technol. J.*, 8: 1256-1262.
- Bianchi, G., 2000. Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE J. Sel. Areas Commun.*, 18: 3-3.
- Camp, T., J. Boleng and V. Davies, 2002. A survey of mobility models for ad hoc network research. *Wireless Commun. Mobile Comput.*, 2: 483-502.
- Heinzelman, W.R., A. Chandrakasan and H. Balakrishnan, 2000. Energy-efficient communication protocol for wireless sensor networks. *Proceedings of 33rd Annual Hawaii International Conference on System Sciences*, Jan. 4-7, IEEE Xplore Press, USA., pp: 1-10.
- Heinzelman, W.R., A.P. Chandrakasan and H. Balakrishnan, 2002. An application specific protocol architecture for wireless microsensor networks. *IEEE Trans. Wireless Commun.*, 1: 660-670.
- Hill, J., 2003. System architecture for wireless sensor networks. Ph.D Thesis, UC Berkeley.
- Johnson, D.B. 1994. Routing in ad hoc network of mobile hosts. *Proceeding of the IEEE Workshop on Mobile Computing Systems and Applications*, Dec. 8-9, IEEE Computer Society, Washington, DC, USA., PP: 158-163.
- Jung, E., S.H. Lee, J.W. Choi and Y.J. Park, 2007. A cluster head selection algorithm adopting sensing-awareness and sensor density for wireless sensor networks. *IEICE Trans. Commun.*, 90: 2472-2480.
- Krishnan, R. and D. Starobinski, 2003. Message-efficient selforganization of wireless sensor networks. *Proceedings of the Wireless Communications and Networks*, March 16-20, New Orleans, Louisiana, USA., pp: 1-6.
- Michierdi, P. and R. Molva, 2003. A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile adhoc networks. *Proceeding of Wiopt03*, March 03, Sophia Antipolis, France, pp: 3-5.
- Ranjan, J. and S. Khalil, 2007. Clustering methods for statistical analysis of genome databases. *Inform. Technol. J.*, 6: 1217-1223.
- Tillett, J., R. Rao and F. Sahin, 2002. Cluster-head identification in ad hoc sensor networks using particle swarm optimization. *Proceedings of the IEEE International Conference on Personal Wireless Communications*, Oct. 23-25, Singapore, pp: 201-205.
- Wadaa, A., S. Olariu, L. Wilson, K. Jones and Q. Xu, 2003. On training a sensor network. *Proceedings of the International Symposium on Parallel and Distributed Processing*, April 22-26, Nice France, pp: 22-26.