Identification of Critical Node for the Efficient Performance in Manet

Shivashankar
Asst.Professor
Medical Electronics
Dr.Ambedkar Institute of Technology,
Bangalore 560 056, India

B.Sivakumar
Professor&HOD
Telecommunication Engg,
Dr.Ambedkar Institute of Technology

G.Varaprasad
Associate Professor
Computer Science Engg
B.M.S.College of Engineering
Bangalore 560 019, India.

***Abstract*— This paper considers a network where nodes are connected randomly and can fail at random times. The critical-node test detects nodes, whose failures are malicious behavior, disconnects or significantly degrades the performance of the network. The critical node is an element, position or control entity whose disruption, is immediately degrades the ability of a force to command, control or effectively conducts combat operations. If a node is critical node, then more attention must be paid to it to avoid its failure or removal of a network. So how to confirm critical nodes in the ad hoc network is the premise to predict the network partition. A critical node is the most important node within the entity of a network. This paper suggests methods that find the critical nodes of a network based on residual battery power, reliability, bandwidth, availability and service traffic type. The metrics for evaluation has been considered as packet delivery ratio, end-to-end delay and throughput.**

Keywords- Critical node; malicious; residual battery power; reliability; bandwidth; Mobile Ad hoc Network.

I. INTRODUCTION

Nodes in Mobile Ad hoc Networks (MANETs) are battery powered and hence have limited lifetime. Due to excessive utilization a node may die which can result in energy depletion problem and thereby affect overall network performance. Local rate of energy consumption based on application can be monitored. Thus early detection and avoidance of energy depletion problem is possible based on monitoring of power and remaining battery lifetime. As and when the rate of consumption based on the application returns to efficient levels, the mobile relay is released so that it can be made available for other critical nodes. This technique can be applied to any protocol used in MANETs such as DSDV, DSR, AODV, TORA etc.

In this work, we focus on maximizing avoidance of network partition, rather than after the network partition, then taking some remedial measures. We describe the critical nodes compensation approach to increase the network connectivity and improve packet delivery rate. First, we detect the critical nodes which may lead to the network partitioning. Secondly, propose the compensation algorithm to avoid the network partitioning. This approach described in this paper is built around the notion of a critical node in an ad hoc network. Our definition of a critical node is a node, whose failure or malicious behavior disconnects or significantly degrades the performance of the network. Once identified, a critical node can be monitored in terms of resource. If a node is not considered critical, this metric can be used to decide if the application or the risk environment warrant the expenditure of the additional resources required to monitor, diagnose, and alert other nodes about the problem. Determining the global network topology in a MANET gives the time delays of the diagnostic packets and the mobility of the nodes makes this task futile, but determining an approximation of this topology or subset of this topology, within a certain time frame may be useful.

An approximation of the network topology can still provide useful information about network the density, network mobility, critical paths, and critical nodes. Even with the uncertainty associated with correctly reconstructing the network topology for a given time period, this additional information can help to reduce the resources consumed to monitor all nodes in the absence of this information.

The node performing the test is referred to as the testing node and the node being tested is referred to as the node under test. Three steps are required to detect whether a testing node shares a critical link with its neighbor. First step is to temporarily modify the testing node's routing table to allow only one communication link to be operational at a time, while blocking communication through all others. The enabled communication link will be between the testing node and a node other than the node under test. Each communication link will be tested sequentially in this manner to determine if an alternative path to the link under test exists.

The responsibilities of a routing protocol include exchanging the route information, finding a feasible path to a destination based on criteria such as hop length, minimum power required and life time of the wireless link. Gathering information about the path breaks, mending the broken paths expending minimum processing power, bandwidth and utilizing the minimum bandwidth. Fig.1 shows the graphical view of identification of the critical node in the network.

If the critical node find in the network, then alternate path will be selected for the efficient network. The major challenges are:

A. Ability to Measure the Resource Availability

In order to handle the resources such as bandwidth efficiently and perform call admission control based on their availability, the MAC protocol should be able to provide an estimation of resource availability at every node.

B. Capability for Power Control

The transmission power control reduces the energy consumption at the nodes, causes a decreasing interference at neighboring nodes and increases frequency reuse.

C. Mobility

One of the most important properties of MANET is the mobility associated with the nodes. The mobility of the nodes results in frequent path breaks, packet, collisions, transient loops, stare routing information and difficulty in resource reservation. A good routing protocol should be able to efficiently solve all the above issues.

The rest of the paper is organized as follows. In section II, some previous work related to this paper and some applications are identified. In Section III, we present the different mechanisms with algorithms and full connectivity when the only randomness is due to random connections and there are no node failures. Section IV contains the simulation results, analyzing and comparison of different parameters and also it includes the discussion on the performance by the various protocols agents in our simulations. Finally, Section V concludes the paper.

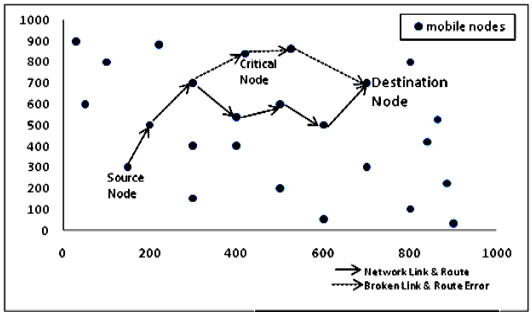


Figure 1. Critical Node representation in network.

II. Some of the Related Research Work

A. Critical Nodes Compensation Algorithm in Sparse Ad hoc Wireless network

Sparse ad hoc wireless networks [1] are an active application in recent years, though sparse environment often makes the network unconnected. However, most of the previous researches focus on connected networks where an end-to-end path exists between any two nodes in the network, therefore these technologies would not work well in sparse ad hoc networks, where restricted node communication radius can result in periods of intermittent connectivity. In this work, we develop a critical nodes compensation algorithm in order to prevent network from partitioning, thereby insure network connectivity and throughput.

But the drawback of previous studies is that they overlooked the importance of the service traffic flow [2] and non-articulation nodes. We propose a method that evaluates how important each node is based on service traffic flow and articulation node. Based on this evaluation, we can give priority to each node. In a complex network, it is useful for a network administrator to focus mainly on some high-ranked nodes, which are relatively important for security purposes.

B. Determining Node Priority Order Based on Traffic Volume

Assuming that there is a web server with a small amount of traffic volume and a backup server with huge amount of traffic volume, it is possible for the network administrator to value the web server because it needs to be alive all the time compared to backup server. In this case, the web server node is more important in spite of its low traffic volume [5].

C. Depth First Search Algorithm(DFS)

DFS was used to detect critical nodes in [3]. DFS is a centralized algorithm and can be also implemented in globalized distributed manner. The algorithms in [4] require that a node should be aware of global topology. In practice, this method is inefficient and involves a quadratic (in number of nodes) communication overhead. The node density is the average number of neighbor nodes of a node in the network. This value reflects the density of the network. The larger the value is, the denser the network is [6]. In this paper, we present a novel critical node detection algorithm for wireless ad hoc networks. It is an effective distributed localized algorithm, which greatly reduces communication overheads and the speed of detection. This is a distributed algorithm which adapts the dynamic topology adaptively, detects the critical node faster and more reliably, and decreases the detection overheads efficiently.

D. Bandwidth Balancing

The bandwidth balancing [7] solves the fairness problems suffered by long bandwidth in the networks. By constraining each node to take only a fraction of the available slots, bandwidth balancing can achieve a fair operation point when several nodes are performing large file transfers.

As routing protocols exchange routing data between nodes, as a result, they would maintain routing status in each node. Based on routing status, data packets are transmitted by mediated nodes along an established route to the destination [8]. M.K Rafsanjani, A Movaghar presents a scheme in which nodes do not need to exchange multiple messages to prove their identities [10]. However, most of the previous researches[11,9] focus on connected networks where an end to end path exists between any two nodes in the network, therefore these technologies would not work well in sparse ad hoc networks, where restricted node communication radius can result in periods of intermittent connectivity.

As routing protocols exchange routing data between nodes, as a result, they would maintain routing status in each node. Based on routing status, data packets are transmitted by mediated nodes along an established route to the destination [12]. In [13], the authors describe a distributed intrusion detection system for MANETs that consists of the local components data collection, detection and response and of the global components. Whereas their architecture is very promising and similar to the one we use in our paper, they

neglect the aspect how their local data collection should find out on incidents like dropped packets, concealed links, etc.

III. DESIGN AND IMPLEMENTATION

A. Bandwidth Constraint in MANET

Since the channel is shared by all nodes in the broadcast region (any reason in which all nodes can hear all other nodes), the bandwidth available per wireless link depends on the number of nodes and a traffic they handle. Thus only a fraction of the total bandwidth is available for every node. The control over head involved must be kept as minimal as possible.

Bandwidth efficiency can be defined as the ratio of the bandwidth used for actual data transmission to the total available bandwidth. The limited bandwidth availability also imposes a constraint on routing protocols in maintaining the topological information. Due to the critical nodes, maintaining consistence topological information at all the nodes involves more control over head which, in turn, results in more band width.

Available bandwidth calculation for the MANET:

Sufficient Bandwidth = $BW_{available} = \frac{Tidle}{T} \times W$ ------(1)

T=Sampling time window for calculating real time bandwidth.
T_{idle}= Time period when a mobile node in idle mode.
W= Maximum bandwidth for data transmission.

B. Location Dependent Contention

The load on the wireless channel varies with the number of critical nodes present in a given geographical region. This makes the contention for the channel high when the number of nodes increases. The high contention for the channel results in a high number of collisions and a subsequent wastage of bandwidth. A good routing protocol should have built in mechanism for distributing the network load uniformly across the network so that the information of regions where channel contention is high can be avoided.

C. Quick Route Reconfiguration

The unpredictable changes in the topology of the network require that the routing protocol be able to quickly perform route configuration in order to handle path break and subsequent packet losses because of critical nodes in the network.

D. Loop Free Routing

This is a fundamental requirement of any routing protocol to avoid unnecessary wastage of network bandwidth. In MANET, wireless network due to the random movement of critical nodes, transient loops may form in the route. A routing protocol should detect such critical nodes and take corrective actions.

E. Signal Strength Based Reliability

A node, N can measure signal strength of its active neighbors. The received signal strength is measured at physical layer and made available to the access of top layers.

$$R(\text{node}) = P(\text{new}) / [P(\text{old}) + P(\text{new})] \quad \ldots\ldots\ldots (2)$$

Where R(node) denotes node reliability and it will be a value between 0 and 1. Whatever new signal strength is more than before, R(node) approaches towards one and whatever new signal strength is less than before, R(node) approaches towards zero.

F. Reliability

The reliability of the real time data being transmitted can be enhanced by introducing a buffer of a fixed size calculated through monitoring the data transmitted by employing self-healing nodes.

G. Residual Battery Power

Power conservation in wireless ad hoc networks is a critical issue as energy resources are limited at the electronic devices used. Therefore to conserve battery energy of the nodes, there are various routing algorithms and schemes designed to select alternative routes. These algorithms and schemes are collectively known as 'power-aware routing protocols' and an example of a better choice of routes selected is one where packets get routed through paths that may be longer but that pass through nodes that have plenty of energy reserves. Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation. ..... (1)

H. Minimize Energy Consumed/Packet

This is one of the more obvious metrics. To conserve energy, we want to minimize the amount of energy consumed by all packets traversing from the source node to the destination node. That is, we want to know the total amount of energy the packets consumed when it travels from each and every node on the route to the next node. The energy consumed for one packet is thus given by the equation:

$$E = \sum_{i=1}^{k-1} T(n_i, n_{i+1}) \quad \text{---------- (3)}$$

In equation (1), n1 to nk are nodes in the route while T denotes the energy consumed in transmitting and receiving a packet over one hop. Then we find the minimum E for all packets. However, this metric has a drawback and i.e. nodes will tend to have widely differing energy consumption profiles resulting in early death for some nodes. Power aware routing schemes make routing decisions to optimize performance of power or energy related evaluation metric.

Excessively, conserving energy neglects power consumption at individual nodes, which speeds up network partition by draining batteries of the critical nodes in the network one by one. In effect, it shortens the network lifetime. On the other hand, overly conserving power expels energy consideration, which commits to paths with large number of hops and longer total distance. Consequently, the total energy dissipated is high and on average, the battery power decays faster. In effect, it also shortens the network lifetime. Energy efficiency is also an important design consideration due to the limited battery life of wireless node. Since, the network interface is a significant consumer of power, considerable research has been devoted to low power design of the entire

network protocol stack of wireless network in an effort to enhance energy efficiency.

All mobile should drain their power at equal rate as a minimal set of mobile exist such that their removal cause network to partition. Such node is called as a critical node. The route between these two partitions must go through one of these critical nodes. A routing procedure must divide the work among these nodes to maximize the life of the network. This problem is similar to load balancing problem. A packet to be routed through a path contains mobiles having grater amount of energy though it is not a shortest path. Delay is minimized as no congestion and nodes having less number of loads.

I. *Availability*

MANETs establishing trust relationships between the nodes in a decentralized fashion has been an important research issue for a long time. If the sender nodes accurately identify the legitimate nodes in the network, a robust routing can be provided while mitigating the effects of malicious nodes. Further, there is always a mutual interaction between a sender and its neighbor nodes during the communication. The scheme guarantees the availability of message as long as a legitimate path exists. Through simulations, we will show the efficiency of the scheme with respect to latency, availability and energy consumption in the presence of adversary.

J. *Residual Capacity*

Residual capacity at a node is the difference between the node's channel capacity and the sum of the bandwidth consumed by all contending flows of that node. It denotes the channel capacity that is not used and it constrains the rate that contending flows can acquire. To measure the residual capacity, each node in the network monitors the channel activity. The fraction of channel idle time during the past measuring period and the channel capacity, determine its residual capacity. The residual capacity at node k can be expressed as

$$R_k = \frac{T_{idle}}{T_P}(C_k) \qquad \text{----------(4)}$$

In equation(4), Ck is the channel capacity at node k; Tidle is the channel idle time during the last measuring period Tp. Larger Tp will give more accurate channel view but also longer response time for the source node to react to the change in the network. In this paper, Tp is set to 0.5 second.

IV. Simulation Setup and Result Discussion

Network Simulator (NS-2.33) has a very rich component library, which is compiled of two languages: C++ or Python is object oriented extension of TCL. First of all, we define the simulation in the 1,000 m×1,000 m region, random waypoint mobile model, the node number: 65; node original communication radius: 40m; according to the distance between compensation node and critical node, choose compensation transmission power; in order to maintain low-speed movement environment, node movement speed is not more than 2 m/s.

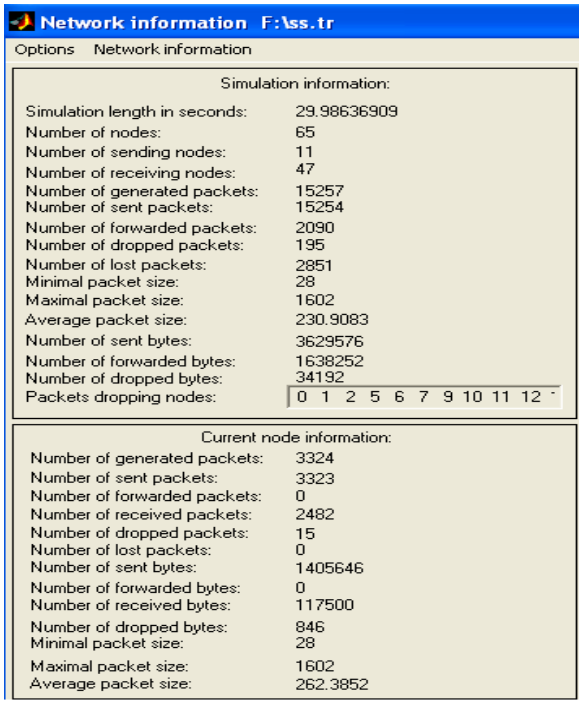
We choose two ad hoc network performance parameters: critical node number and network throughput. For our simulation, we used NS-2.33 with mobility extension. These extensions include the modeling of an IEEE 802.11/MAC.

Table 1 shows the simulation parameters used in the network setup for identifying the critical node and select the alternate path for maintaining the continuous efficient network connection in MANET.

TABLE 1. Simulation Parameters.

Simulation time	0-50 sec
Traffic type	TCP
Packet size	1460
Hello packet interval	2 sec
Node mobility	0 to 10 mts/sec
Frequency	1 Ghz
Channel capacity	2 M bps
Transmit power	2.0 Mw
Receiver power	2.0 Mw
Total number nodes	65
Communication system	MAC/IEEE 802.11G

TABLE 2. Overall network information with critical node and without critical node in MANET.



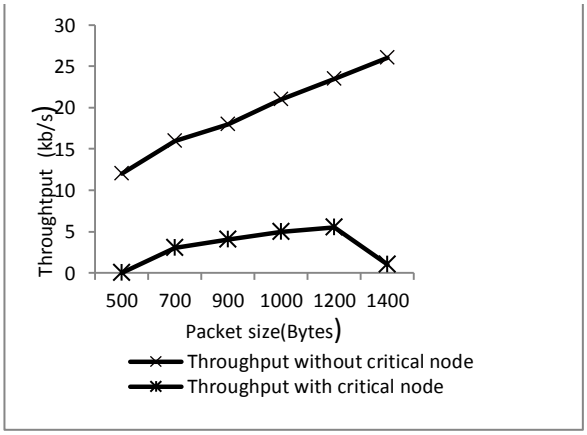


Figure 2. Throughput with and without critical node in MANET.

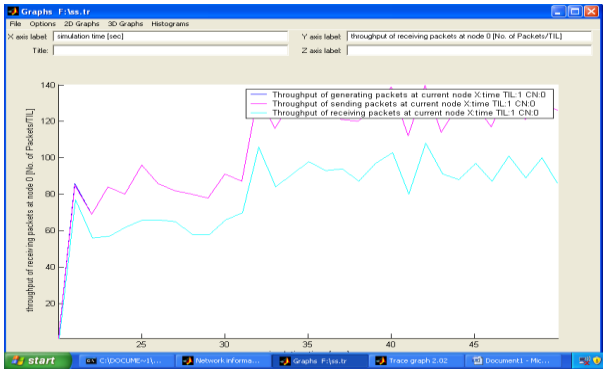


Figure 3. Throughput of receiving packets when there is critical node occurs during the transmission of data.

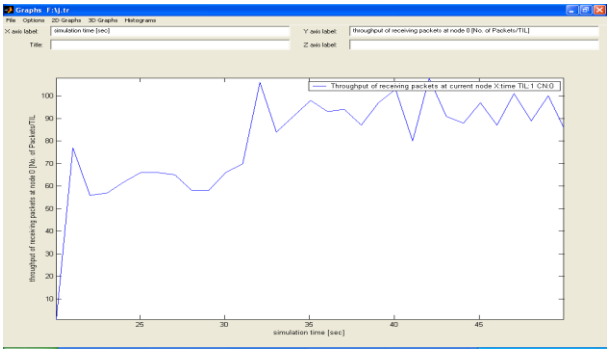


Figure 4. Throughput of receiving packets during the transmission of data.

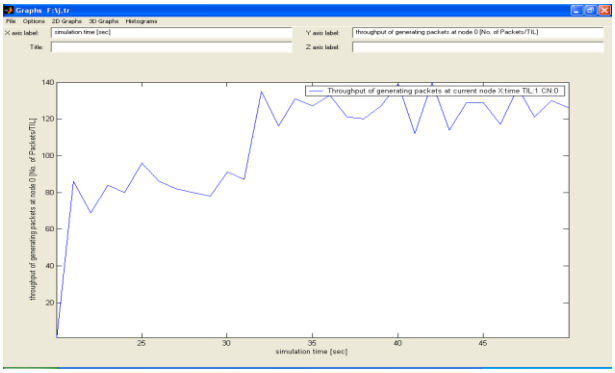


Figure 5. Throughput of generating packets at destination node.

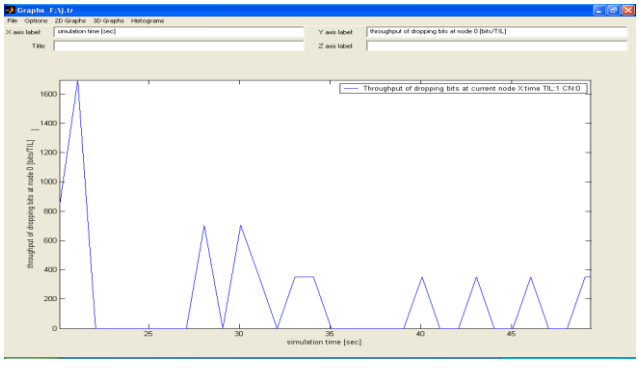


Figure 6. Throughput of dropping bits at destination node.

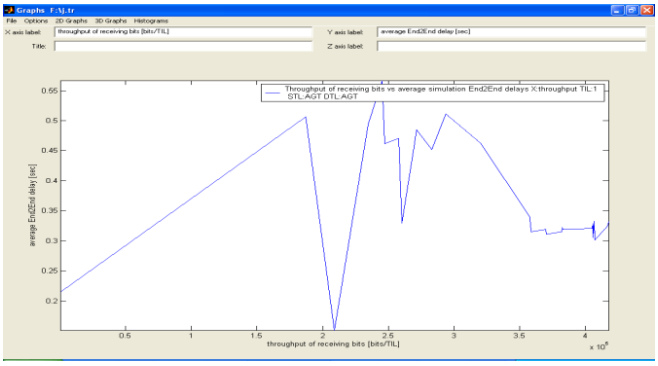


Figure 7. Average of end-to-end delay.

Figure-2 shows the throughput response of the MANET is 78% difference with and without critical nodes. In this paper, the performance analysis of MANET for different scenario as mention in Table-2 has been studied using trace graph. The first part of the table-2 shows more dropping packets, more number of lost packets in the presence of critical node as intermediate node. The second part of the table-2 shows that the improvements in MANET approximately 94% with more received packets, less dropped packets and less number of lost packets.

The figure-3 represents the throughput performance in MANET. The Y axis shows throughput of receiving packets at destination node in kilo bytes and the X axis shows simulation time in sec. The red line of the graph represents the best effort with 92% of the throughput. The green line of the graph shows the throughput of critical node presence and it is approximately 52% of the throughput. We start the best effort approximately started at 12 sec and going on until 50 sec. The presence of critical node in MANET, results in large delay. Since the delay has been increased, the throughput is gradually reduced. When the neighbor nodes are communicating with each other, the packets will move between source and destination and thus the throughput will be increased.

Figure-4 plots the receiving packets during the transmission time v/s simulation time after identified the critical node and alternate path has been selected. It shows the sum of numbers of all the intermediate nodes, receiving packets sent by the source node and number of received packets at the destination node. There is some packet losses (6% to 12%) for the rates of 78 to 90pkts/sec for both the schemes on some of the nodes. This may be due to insufficient bandwidth, less residual battery power and minimized energy consumed per packet. If these metrics are good, then throughput of the network will be increased.

Figure-5 shows the throughput of generating packets at any intermediate nodes v/s simulation time (sec).The graph reflects the simulation time for which an intermediate node in route generated packets. In other words, it depicts how long the route through the intermediate node was valid during the simulation after selected alternate path for the best efficiency.

The throughput for the proposed Networks as shown in figure-6, are calculated based on the distance. The throughput has dropped around 45.3%. The number of data packets dropped at any critical node present in the network. This is an important parameter because if the number of dropped packets increases, the throughput would decrease. Therefore the lower packets drop; lower would be delay in the network.

Figure-7 represents the average of end to end delay for both the schemes (with and without critical node). Though the nodes are at same distance from the route, they receive different bandwidth. This is the average delay of all the data packets. The delay different is 50% of the throughput of receiving bytes. It is calculated as the time taken between the generation of data packets and arrival of last bit of destination. There are possible delays caused by bandwidth, throughput, average number of node receiving delay between current and other node etc. This metric describes the packet delivery time. The lower end to end delay is the better application performance in MANET.

V. CONCLUSION

In this work, we develop a critical nodes compensation algorithm in order to prevent network from partitioning, thereby insure the network connectivity and throughput. Finally, we give simulation design and analysis of the critical nodes compensation algorithm using NS-2.33 model. Our simulation results show that the algorithm can effectively improve ad hoc networks performance. In addition, some time-critical applications may not be able to function properly in disconnected MANET as the end-to-end delay. However, there are lacks of full proof in theory and in practice. In these systems, nodes are subject to battery power, efficient bandwidth constraints and good throughput. The overall performance of the network is increased after detection of the critical node and selecting alternate path for the continuation of the same operation. By considering all the above metrics we come to a conclusion that while a network is set up, each node is leveled with a threshold value of energy. The node's energy is decreasing gradually as it is used in network connectivity. So the failure of critical node depends on less bandwidth, less residual battery power and poor throughput.

REFERENCES

[1] Shoudong Zou, Ioanis Nikolaidis and Janelle J. Harms "ENCAST: Energy–Critical Node Aware Spanning Tree for Sensor Networks", In Proceedings of the Communication Networks and Services Research Conference, pp.249-254, 2005.

[2] Michael Dion "Building in Reliability (BIR) with Critical Nodes", http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00493599

[3] Massimo Franceschetti and Ronald Meester, "Critical Node Lifetimes in Random Networks via the Chen–Stein Method", IEEE Transactions on Information Theory, vol.52, no.6, pp.2831-2837, June 2006.

[4] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos, "Detecting Critical Nodes for MANET Intrusion Detection Systems", In Proceedings of IEEE Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, pp.7-15, 2006.

[5] Vahid Tabatabaee and Leandros Tassiulas, "MNCM: A Critical Node Matching Approach to Scheduling for Input Buffered Switches with no Speedup", IEEE/ACM Transactions on Networking, Vol.17, no.1, pp.294-304, February 2009.

[6] Daisuke Kasamatsu, Norihiko Shinomiya and Tadashi Ohta, "A Broadcasting Method considering Battery Lifetime and Distance between Nodes in MANET", IEICE Transactions on Information and Systems, Vol. J91-B, No.4, pp.364-372, 2008

[7] Min Sheng, Jiandong Li and Yan Shi, "Critical Nodes Detection in Mobile Ad Hoc Network, ieeexplore.ieee.org/iel5/10777/33944/01620401.pdf.

[8] N.Komnios, D.Vergados and C. Douligeries. "Detecting unauthorized and compromised nodes in mobile adhoc network." Elseviewer Adhoc network,vol5,n0 3,pp.289-298,2007.

[9] Christian Bravo, Sonia A¨ıssa and Andr´e Girard, "Providing Quality of Service for Critical Nodes in Ad Hoc Networks", IEEE Vehicular Technology Conference, 2005.

[10] M.K Rafsanjani, A Movaghar, "Identifying monitoring nodes with selection of Authorized nodes in mobile Adhoc network",World Applied Sciences Journal,vol4,n03, pp.444-449,2008

[11] N.Komnios, D.Vergados and C. Douligeries, "Detecting Unauthorized and Compromised Nodes in Mobile Ad hoc Network," Adhoc Network(Elsevier), vol.5, no.3, pp.289-298, 2000.

[12] Yongguang Zhang, Wenke Lee, and Yi-An Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", ACM Wireless Networks, vol.9, no.5, pp.545-556, September 2003.