International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Identifying Node Failures in Cellular Wireless Network Systems : A Probabilistic Approach

Gaddipathi Bharathi*[1], Nallabothula Bhujanga Chakrapani2
*[1]Associate Professor, Department of MCA , St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India
[2]PG Student, Department of MCA , St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

The main concept of this paper is to detect the node failures and the signal strength of the nodes. To find out these fail nodes we use two schemes, Binary Scheme and Non Binary Scheme. In Binary scheme, there are two ways one is send query and other one is receive query. In Binary scheme, the result will be in Zero's and One's, if the Node is active means result will be 1 and if when the node is in active means 0. In this Node A will send the status of Node B, Node B will send the status of Node C and Node C will send the status of Node D. But we cannot find the strength of each node in this binary scheme. For this reason we go for Non Binary Scheme, in this scheme we can check whether the node is in strong state or weak state to receive the signals. Same like in binary scheme Node A will send the strong or weak status of Node B, Node B will send the Strong or weak status of Node C and Node C will send the Strong or Weak status of Node D. Also while sending the files it will select the alternate path automatically for off and weak nodes. So by using the alternate nodes the files will reach the destination. And also by using the main node we can check the node status and we can check the file status also in those particular nodes.
Keywords: Node Failure Binary Scheme, Non Binary Scheme, Fault Management**.**

I. INTRODUCTION

Mobile wireless networks have been used for many mission critical applications, including search and rescue, environment monitoring ,disaster relief, and military operations. Such mobile networks are typically formed in an ad-hoc manner, with either persistent or intermittent network connectivity. Nodes in such networks are vulnerable to failures due to battery drainage, hardware defects or a harsh environment.

Node failure detection in mobile wireless networks is very challenging because the network topology can be highly dynamic due to node movements. Therefore, techniques that are designed for static networks are not applicable. Secondly, the network may not always be connected. Therefore, approaches that rely on network connectivity have limited applicability. Thirdly, the limited resources (computation, communication and battery life) demand that node failure detection must be performed in a resource conserving manner.

Node failure detection in mobile wireless networks assumes network connectivity. Many schemes adopt probe-and-ACK (i.e., ping) or heartbeat based techniques that are commonly used in distributed computing. Probe-and-ACK based techniques require a central monitor to send probe messages to other nodes. When a node does not reply within a timeout interval, the central monitor regards the node as failed. Heartbeat based techniques differ from probe-and-ACK based techniques in that they eliminate the probing phase to reduce the amount of messages. Several existing studies adopt gossip based protocols, where a node, upon receiving a gossip message on node failure information, merges its information with the information received, and then broadcasts the combined information. A common drawback of probe-and-ACK, heartbeat and gossip based techniques is that they are only applicable to networks that are connected. In addition, they lead to a large amount of network-wide monitoring traffic. In contrast, our approach only generates localized monitoring traffic and is applicable to both connected and disconnected networks.

.

II. EXISTING SYSTEM

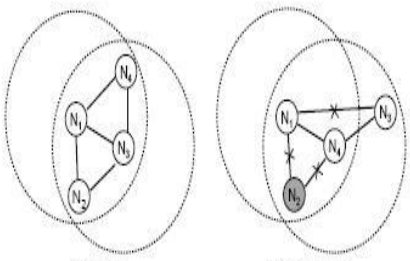
In Existing system, they use only the binary scheme to detect the node failure, so we can detect only the ON or OFF state of the nodes, we cannot find whether the node is strong or weak. In Existing system, there is no way to detect the weak node and to find the alternate node for the data transmission. Use Only Binary Scheme which gives Zero's or Ones, it will not show the weak or strong Status of nodes, in this there is no way to find alternative path for data transfer.

III. PROPOSED SYSTEM

In the Proposed system, the user can detect the node failures from main node by using two schemes one is binary scheme and other one is non-binary scheme. So by using these two schemes the user can get the ON - OFF and Wear -Strong status of the each nodes. After detecting the node failure we can find the alternative path to transfer the data during transmission. Uses both Binary and Non-Binary Scheme, user can check, both the on-off and weak-strong status, alternative path for node failures.

3.1 APPROACH

We use the example given below to discuss our approach.



At time t, all the nodes are alive, and node N1 can hear heartbeat messages from N2 and N3 (see Fig. 1(a)). At time t+1, node N2 fails and N3 moves out of N1's transmission range (see Fig. 1(b)). By localized monitoring, N1 only knows that it can no longer hear from N2 and N3, but does not know whether the lack of messages is due to node failure or node moving out of the transmission range. Location estimation is helpful to resolve this ambiguity: based on location estimation, N1 obtains the probability that N2 is within its transmission range, finds that the probability is high, and hence conjectures that the absence of messages from N2 is likely due to N2's failure; similarly, N1 obtains the probability that N3 is within its transmission range, finds that the probability is low, and hence conjectures that the absence of messages from N3 is likely because N3 is out of the transmission range. The above decision can be improved through node collaboration. For instance, N1 can broadcast an inquiry about N2 to its one-hop neighbors at time t + 1, and use the response from N4 to either confirm or correct its conjecture about N2. The above example indicates that it is important to systematically combine localized monitoring, location estimation and node collaboration, which is the fundamental of our approach.

The core building block of our approach is the means to calculate node failure probability. Suppose a node, A, hears the heartbeat packets from another node, B, at times $t - k\ldots, t(k \geq 0)$, but not at time t + 1. We next derive the probability that node B has failed at time t+1 given the fact that node A can no longer hear B at t+1. In the following, the node failure probability is for node B, and the packet loss probability is for the heartbeat packets from B to A at t + 1.

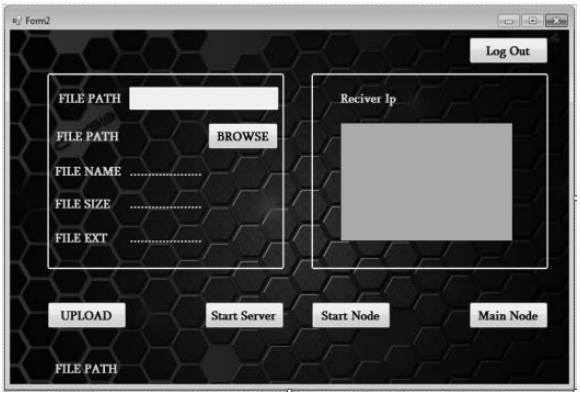
IV. MODULE DESCRIPTION

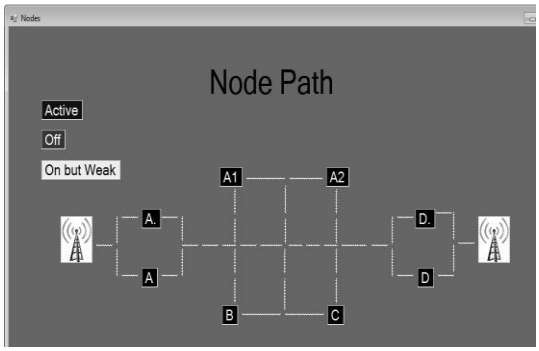
4.1Authentication Module

In this paper they are only two users one is sender and other one is receiver. Any user who wants to the share and receive the data by using this paper, must have to do registration in this project. After registration was done successfully they can login into this project by their user-name and password which they entered during registration process.

4.2 Share Data to Client

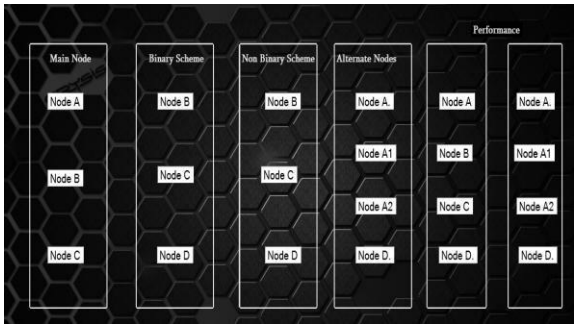
Sender must share the data to client only after getting the request from client but client cannot send a request directly to the sender before that they have to get the connection path by entering the IP address of the sender. After getting the request, the request contains the IP address of the client, so by using that IP the sender can share the data to multiple clients.





4.3 Binary Code Detection

Before sending the data the sender can check the status of each nodes by two schemes one is binary code and other one is non-binary code. In Binary code detection, the sender can check the ON or OFF status in the binary format (0's and 1's). If the node is in ON state means the result will be 1 and if the node is in OFF state means the result will be 0.



4.4 Non-Binary Code Detection

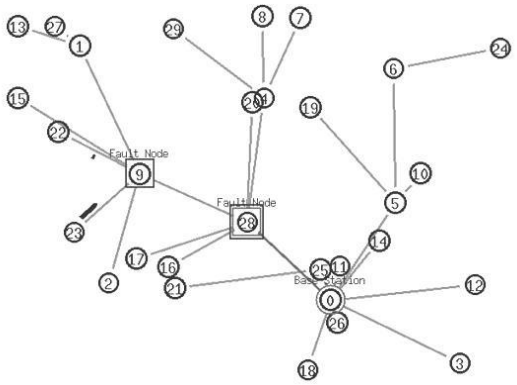
In Binary code detection, the sender can check the ON or OFF status in the binary format (0's and 1's). But Sender cannot check the Weak or Strong Status of the nodes. For that problem the sender go for Non-Binary code detection, by using this scheme the sender can check the strength of every nodes whether they are Strong or Weak to receive the data.

4.5 File Path in Router

Sender can view the path of the data which was shared by him in router. In this router the node which is expressed in blue color in active state, the node which is in red color is in off state and the node which is in yellow color is in on state but they are weak to receive and send the datas. Sender can view all this details of nodes during the transmission time.

4.6 Node Failure and Recover Path

In this module, the sender share a files there will be a checking for each node before they receiving the data. For example , checking will be done for Node A before the data reaches Node A, if the Node A is active and strong means the data will move through Node A or it will find a alternate node automatically and then data will move through that alternate node. This process will be done for each and very nodes.



4.7 Receive Data

In this module, the client will receive the data after passing by all the nodes successfully. By using the Admin Node the Sender can check the binary and non binary scheme for each nodes. Node A will send the binary and Non Binary results of Node B to Admin Node, Node B will send the binary and Non Binary results of Node C to Admin Node, Node C will send the binary and Non Binary results of Node C to Admin Node. And Also we can see the performance of each nodes while transmission.

V. CONCLUSION

In this approach, the sender can view both the binary and non binary result. So by using this, the sender can

check both the on/off state and also he can check the whether the node is strong or weak. And also the sender can view the path how the data which was send by sender is transmitted.

VI. REFERENCES

[1]. R. Badonnel, R. State, and O. Festor. Self-configurable fault monitoring in ad-hoc networks. Ad Hoc Networks, 6(3):458-473, May 2008.

[2]. P. Bahl and V. N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In Proc. of IEEE INFOCOM, 2000.

[3]. Y. Bar-Shalom, T. Kirubarajan, and X.-R. Li. Estimation with Applications to Tracking and Navigation. John Wiley & Sons, Inc., 2002.

[4]. D. Ben Khedher, R. Glitho, and R. Dssouli. Novel Overlay-Based Failure Detection Architecture for MANET Applications. In IEEEInternational Conference on Networks, pages 130-135, 2007.

[5]. C. Bettstetter. Smooth is Better than Sharp: A Random Mobility Model for Simulation of Wireless Networks. In Proc. of ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems, pages 19-27, New York, NY, USA, 2001.ACM.[7]

[6]. C. Bettstetter. Topology Properties of Ad Hoc Networks with Random Waypoint Mobility. ACM SIGMOBILE Mobile Computing and Communications Review, 7(3):50-52, 2003.

[7]. J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva.A Performance Comparison of Multi-Hop Wireless Ad hoc Network Routing Protocols. In Proc. of MobiCom, pages 85-97, New York, NY,USA, 1998. ACM.

[8]. T. D. Chandra and S. Toueg. Unreliable Failure Detectors for ReliableDistributed Systems. Journal of the ACM, 43:225-267, 1996.

[9]. I. Constandache, R. R. Choudhury, and I. Rhee. Towards Mobile PhoneLocalization without War-Driving. In Proc. of IEEE INFOCOM, March2010.

[10]. Y. Yi, M. Gerla, and K. Obraczka. Scalable Team Multicast in Wireless Ad Hoc Networks Exploiting Coordinated Motion. Ad Hoc Networks,2(2):171-184, 2004.