

Node Failure Detection in both Wired and Wireless Sensor Network Using Binary and Non-Binary Schemes

Amulya C N¹, Rajeshwari B S², Sowmya R³, Lavanya K⁴, Kavya K⁵

8th Sem Students, CSE, JVIT, Bidadi, India ^{1,2,3,4}

Assistant Professor, Department of CSE, JVIT, Bidadi, India ⁵

Abstract: The main objective of this paper is node failure detection. To do this there are Binary Scheme and Non Binary Scheme. In Binary scheme, result will be one if Node is active and result will be zero if Node is not active. But main problem with binary scheme is we cannot check the signal strength. So 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. In the proposed system we are designing the scheme which can be used for both wired and wireless sensor network. If the node is in active state the data can be transferred else checks for the alternate route.

Key Terms: 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. RELATED WORK

- a) Adaptive Fault Detection Approaches for Dynamic Mobile Networks proposed by D. Liu et al. In this approach they have used probe-and-ACK [5], [12], [19] technique to detect Node Failure. The main drawback of this paper is they require central monitor which causes additional overhead.
- b) A Failure Detection Service for Large-Scale Dependable Wireless Ad-Hoc and Sensor Networks proposed by M. Elhadeif et al. This work proposes a gossip based protocols [12], [24] for detecting the node failures. But the major drawback of this paper is it suites only for connected network.
- c) A distributed monitoring mechanism for wireless sensor networks proposed by C.-F. Hsin et al. This paper uses localized monitoring for node failure detection. It is not suitable for mobile networks since it does not consider that failure to hear from a node might be due to node mobility instead of node failure.
- d) Self-configurable fault monitoring in ad-hoc networks proposed by R. Badonnel et al. This work proposes a two-state Markov model for node failure detection. This is not applicable for wireless network.

e) RADAR: An in-building RF-based user location and tracking system proposed by P. Bahl et al. The proliferation of mobile computing devices and local-area wireless networks has fostered a growing interest in location-aware systems and services. In this paper we present RADAR, a radio-frequency (RF)-based system for locating and tracking users inside buildings. RADAR operates by recording and processing signal strength information at multiple base stations positioned to provide overlapping coverage in the area of interest. It combines empirical measurements with signal propagation modeling to determine user location and thereby enable location-aware services and applications. We present experimental results that demonstrate the ability of RADAR to estimate user location high degree of accuracy.

III. PROPOSED WORK

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.

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 $t - k \dots, t(k \geq 0)$, 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

A) System Construction

In the first module, we develop the system with the required entities to evaluate and show the performance of our proposed model. We develop Six Nodes by naming it Node A, Node B, Node C, Node D, Node E and Node F. Then Source Node, Network node showing the information of the network and the Network status indicating node. We consider the problem of detecting network failure by the nodes of a wireless network. We assume that there is a specially designated node in the network, which we call the *source node*. The source node may be a base station that serves as an interface between the network and its users. Since a failure may or may not separate a node from the source node, we distinguish between two distinct outcomes of a failure for a particular node.

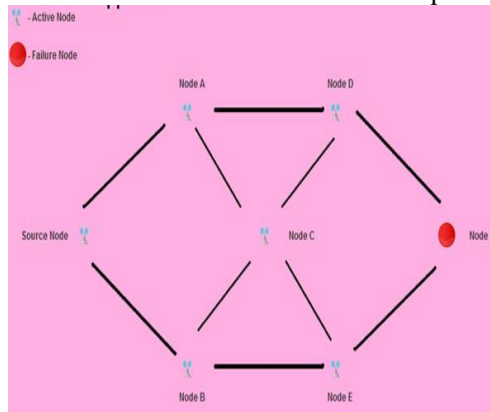


Fig 1: System Construction

B) Calculating Failure

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 , 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 $t + 1$. For ease of exposition, we omit superscripts and simply use p_d (death) and p_c (communication failure) to represent the above two probabilities; the meaning is we hope clear from the context. In the basic case, a node sends a single heartbeat packet at each time. When node A cannot hear from B, one of the following conditions must hold: node B has failed; node B is not failed but A is out of the transmission range of B; or node B has not failed and A is in the transmission range of B, but the packet sent from B is lost.

C) Binary Feedback Scheme

Suppose that a node, A, no longer hears from another node, B, at time $t+1$. In the binary feedback scheme, A calculates the conditional probability p that B has failed. Let denote a pre-defined detection threshold. If p is larger than the

threshold, then A has a high confidence that B has failed. To reduce the risk of false alarms, A broadcasts to its neighborhood an inquiry message about B (along with its own calculated probability p). In order to avoid multiple nodes broadcast inquiry messages about B, we assume A starts a timer with a random timeout value, and only broadcasts a query message about B when the timer times out and A has not heard any query about B. In this case, only the node has the lowest random timeout value will broadcast a query message about B; the other nodes refrain from sending an inquiry about B.

D) Non-binary Feedback Scheme

The binary feedback scheme does not fully utilize the information from other nodes because the responses from other nodes are binary (i.e., 0 or 1). The non-binary feedback scheme differs from the binary version in that A first gathers non-binary information from its neighbors and then calculates the conditional probability that B has failed using all the information jointly. Specifically, when A suspects B has failed, A broadcasts to its neighbors an inquiry about B. Again, to avoid multiple nodes broadcast inquiry messages about B, we assume A waits for a random amount of time, and only broadcasts a query message about B when it has not heard any other query about B. Each neighbor that hears A's query responds to A its information on B.

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.

REFERENCES

- [1] NS-3. [ONLINE]. AVAILABLE: [HTTPS://WWW.NSNAM.ORG/](https://www.nsnam.org/), AUG. 2014.
- [2] R. Badonnel, R. State, and O. Fester, "Self-configurable fault monitoring in ad-hoc networks," *Ad Hoc Netw.*, vol. 6, no. 3, pp. 458–473, May 2008.
- [3] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RFbased user location and tracking system," in *Proc. IEEE INFOCOM*, 2000, pp. 775–784.
- [4] Y. Bar-Shalom, T. Kirubarajan, and X.-R. Li, *Estimation with Applications to Tracking and Navigation*. Hoboken, NJ, USA: Wiley, 2002.
- [5] D. Ben Khedher, R. Glitho, and R. Dssouli, "A novel overlaybased failure detection architecture for MANET applications," in *Proc. IEEE Int. Conf. Netw.*, 2007, pp. 130–135.
- [6] C. Bettstetter, "Smooth is better than sharp: A random mobility model for simulation of wireless networks," in *Proc. ACM Int. Workshop Modeling, Anal. Simul. Wireless Mobile Syst.*, New York, NY, USA, 2001, pp. 19–27.
- [7] C. Bettstetter, "Topology properties of ad hoc networks with random waypoint mobility," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 7, no. 3, pp. 50–52, 2003.
- [8] 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. 4th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw.*, New York, NY, USA, 1998, pp. 85–97.
- [9] T. D. Chandra and S. Toueg, "Unreliable failure detectors for reliable distributed systems," *J. ACM*, vol. 43, pp. 225–267, 1996.
- [10] I. Constandache, R. R. Choudhury, and I. Rhee, "Towards mobile phone localization without war-driving," in *Proc. IEEE 29th Conf. Inf. Commun.*, Mar. 2010, pp. 2321–2329.
- [11] K. Dantu, M. H. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. S. Sukhatme, "Robomote: Enabling mobility in sensor networks," in *Proc. IEEE/ACM 4th Int. Symp. Inf. Process. Sens. Netw.*, 2005, pp. 404–409.
- [12] M. Elhadef and A. Boukerche, "A failure detection service for large-scale dependable wireless ad-hoc and sensor networks," in *Proc. Int. Conf. Availability, Rel. Security*, 2007, pp. 182–189.
- [13] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proc. ACM Conf. Appl., Technol., Archit. Protocols Comput. Commun.*, 2003, pp. 27–34.
- [14] I. Gupta, T. D. Chandra, and G. S. Goldszmidt, "On scalable and efficient distributed failure detectors," in *Proc. ACM Symp. Principles Distrib. Comput.*, 2001, pp. 170–179.
- [15] C.-F. Hsin and M. Liu, "A distributed monitoring mechanism for wireless sensor networks," in *Proc. 1st ACM Workshop Wireless Security*, Dec. 2002, pp. 57–66.
- [16] L. Hu and D. Evans, "Localization for mobile sensor networks," in *Proc. 10th Annu. Int. Conf. Mobile Comput. Netw.*, 2004, pp. 45–57.
- [17] J.-H. Huang, S. Amjad, and S. Mishra, "CenWits: A sensor-based loosely coupled search and rescue system using witnesses," in *Proc. 3rd Int. Conf. Embedded Netw. Sens. Syst.*, 2005, pp. 180–191.
- [18] J. Jubin and J. Tornow, "The DARPA packet radio network protocols" *Proc. IEEE*, vol. 75, no. 1, pp. 21–32, Jan. 1987.
- [19] D. Liu and J. Payton, "Adaptive fault detection approaches for dynamic mobile networks," in *Proc. IEEE Consum. Commun. Netw. Conf.*, 2011, pp. 735–739.
- [20] M. B. McMickell, B. Goodwine, and L. A. Montestruque, "Micabot: A robotic platform for large-scale distributed robotics," in *Proc. IEEE Int. Conf. Robot. Autom.*, 2003, pp. 1600–1605.
- [21] M. Natu and A. Sethi, "Adaptive fault localization for mobile, adhoc battlefield networks," in *Proc. IEEE Mil. Commun. Conf.*, Atlantic City, NJ, USA, Oct. 2005, pp. 814–820.
- [22] I. Rhee, M. Shin, S. Hong, K. Lee, S. J. Kim, and S. Chong, "On the levy-walk nature of human mobility," *IEEE/ACM Trans. Netw.*, vol. 19, no. 3, pp. 630–643, Jun. 2011.
- [23] S. Rice, *Mathematical Analysis of Random Noise*, Bell Telephone Laboratories, 1944.
- [24] N. Sridhar, "Decentralized local failure detection in dynamic distributed systems," in *Proc. IEEE Symp. Rel. Distrib. Syst.*, 2006, pp. 143–154.
- [25] Y. Yi, M. Gerla, and K. Obraczka, "Scalable team multicast in wireless ad hoc networks exploiting coordinated motion," *Ad Hoc Netw.*, vol. 2, no. 2, pp. 171–184, 2004.
- [26] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful," in *Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun.*, 2003, vol. 2, pp. 1312–1321