Design and Evaluation of a Failure Detection Algorithm for Large Scale Ad Hoc Networks Using Cluster Based Approach

[1]*Pabitra Mohan Khilar Email: pmkhilar@nitrkl.ac.in ,khilarpm@yahoo.com*
[2]*Jitendra Kumar Singh, Email: jitendrakumars@gmail.com ,*
[3]*Sudipta Mahapatra, Email: sudipta@iitkgp.ernet.in*

[1& 2] Department of Computer Science and Engineering, National Institute of Technology, Rourkela, India -769008
[3] Department of E & ECE, Indian Institute of Technology, Kharagpur, India - 721302

Abstract

In this paper we propose a scalable failure detection service for large scale ad hoc networks using an efficient cluster based communication architecture. Our failure detection service adapts the detection parameter to the current load of the wireless ad hoc network. The proposed approach uses a heartbeat based testing mechanism to detect failure in each cluster and take the advantage of cluster based architecture to forward the failure report to other cluster and their respective members. The simulation results show that this approach is linearly scalable in terms of message complexity and consensus time.

Keyword: ad hoc networks, Cluster, Failure Detector (FD), Heartbeat.

1. Introduction

Wireless ad hoc networks are extensively used in many applications such as monitoring the environment and for data gathering, due to their easy installation, inexpensive system resources, no need of any fixed infrastructure or centralized administration. Due to their unfavorable operational environment such systems are highly vulnerable to failures and thus leads to frequent topology change [12-14]. So one of the prerequisite for wireless ad hoc network is to provide efficient failure detection service to monitor the health of these system. In fact, failure detectors are basic building block for fault tolerance in such system. Failure detectors can detect failure of a node or part of the network and in this way it can help to take the necessary action for the correct operation of the system.

Any failure detector is characterized by two main properties: completeness (failure of a group member is eventually detected by every non faulty member) and accuracy (number of mistakes that a failure detector can make) [1]. The accuracy and completeness of a failure detector depends highly on the efficient & reliable communication. The development of an efficient failure detection service in wireless ad hoc network is more difficult than in traditional distributed system [7] due to two major problems such as **(i) Scalability** due to their large size and **(ii) Message loss** due to the high probability of message loss that may cause frequent false detection and make it difficult to let every non faulty node in the system be aware of detected failures. Consequently, it is impossible for a failure detection service to provide deterministic guarantees for completeness and accuracy.

The research on failure detection and monitoring in wireless adhoc networks and sensor networks are lagging behind in past. Recently, some of the approaches can be found in [6-7]. In order to address the above problems, this paper proposes a failure detection service based on the clustering of nodes in a wireless adhoc network. We show that the clustering is useful in handling these issues and in building scalable and robust ad hoc network.

The paper is organized as follows. Section 2 describes the system model, assumptions, and problem description. Section 3 describes cluster based communication architecture and

978-0-7695-3513-5/08 $25.00 © 2008 IEEE
DOI 10.1109/ICIT.2008.17

clustering algorithm. Section 4 covers the failure detection service algorithm. Section 5 describes the simulation model and shows simulation results. Section 6 describes the previous works. Finally section 7 concludes the paper.

2. System Description and Assumption

We assume that the wireless ad hoc network is a large connected network in which there are totally N nodes denoted by 1, 2, 3,…..,N. The nodes are distributed randomly in some physical domain. The nodes could be the hosts that become stationary after deployment. We assume that transmission range for each node is fixed and identical and link between two host is bi-directional. If host u is in the transmission range of another host v, then their must be a link between the two.

The system can be modeled as a communication graph G = {V, E}, where V={1,2,….N}, and E={(v1,v2): v1 is in transmission range of v2 and vice versa}. Assume d is the diameter of this communication graph. A cluster is a group of nodes in which one node is appointed as head of the cluster known as clusterhead (CH) and is given some responsibilities like maintenance of the cluster and detection of failed node in the cluster. Node who is responsible for forwarding message to neighbor clusters is known as gateway (GW) node. The order of a gateway node is number of neighbor cluster that the gateway node connects with. Node that is neither CH nor GW node is called ordinary node. Node that doesn't belong to any cluster is with status unselected. Otherwise it is with status selected. The physical degree of a node is the number of one-hop neighbors that the node connects with. The logical degree of a node is number of unselected number. A node with degree 1 is defined as boundary node and only neighbor of a boundary node is defined as indispansible node. A cluster is said to be an orphan cluster which has no connectivity to the rest of the network but the degree of the nodes in the cluster is greater than 0.

Host normally operates under promiscuous receiving mode and based on the exchange of a heartbeat message i.e., when a node sends the heartbeat message, all its immediate neighbor may hear this message, regardless whether or not they are the intended recipient of the message. It is assumed that the nodes are subjected to only crash fault i.e., they can not send or receive heartbeat messages.

3. Clustering

The failure detection algorithm coupled with suitable clustering algorithm make a very efficient failure detection service for wireless adhoc networks. We propose an efficient clustering technique to build a scalable failure detection service which executes in parallel in each cluster and detect failure of nodes. Clustering divides whole network into two level communication architecture namely intra-cluster and inter-cluster. Failure detection service executes in the intra- cluster level in each cluster. If a failure is detected in a local cluster, the detection information is forward to other clusters through inter-cluster communication hierarchy.

Two types of message overheads are required to maintain such as intra-cluster and inter-cluster. All members in a cluster are required to exchange intra-cluster heartbeat messages to maintain the cluster. However only CHs are responsible for inter-cluster communication in order to maintain the entire cluster based wireless ad hoc network. If the wireless ad hoc network is organized into k number of clusters and the number of members in cluster i is n_i, in worst case, the number of required intra-cluster maintenance overhead is n_i^2 and the number of required inter-cluster maintenance overhead in the cluster i is (k-1). Thus the total number of cluster maintenance overheads for the cluster i is n_i^2 +k-1 and the total number of required cluster maintenance overheads for the entire wireless ad hoc network is:

$$OH = \sum_{i=1}^{k} n_i^2 + k - 1 = \sum_{i=1}^{k} n_i^2 + k^2 - k$$

let $\mu = N/k$ be the mean value of the number of cluster members and

$$\sigma^2 = (1/k) \sum_{i=1}^{k} (n_i - \mu)^2 \text{ be}$$

the variance of the number of clusters. Then above equation can be written as

$$OH = N^2/k + k\sigma^2 + k^2 - k$$

From the above equation it is clear that to reduce the number of cluster maintenance overheads, we need to come with a clustering algorithm that can not only reduce the number of generated cluster but also reduce the variance of the cluster size.

Selecting the cluster head (CH) based on criteria such as indispensable status of the node and their logical degree has been proposed in [10]. However these two parameters do not address the stability issue of the clusters. Rather, the energy factor is more significant in deciding the stability of the cluster head. The proposed algorithm is an extension of [10] and selects a cluster head based on indispensable status, logical degree, energy factor which not only reduces cluster maintenance overhead, but also improves the stability of the cluster.

Using logical degree and energy reserve of a node we can calculate the quality of each node. In general, the quality of a node is given by:

$$Q_i = E_i + LD_i$$

Where Q_i is the quality of node i, E_i the energy reserve of node i, LD_i is the logical degree of node i. The node which is having highest quality value among its unselected neighbor will be the candidate for CH.

3.1 Algorithm Details

The modified algorithm for clustering is stated as follows:

For any unselected node v
{
If ((node v is an indispensable node)||(node v is the only node with highest quality Q_v among unselected neighbor)||(among unselected neighbor with same quality node v is with the smallest ID)
{ Update status to selected;
Regard itself as a CH;
Send an invite packet, invite(v) to all neighbors;}
On receiving an invite packet from neighboring node v
If (node u is an indispensable node)
Discard this packet;
Else
{Regards itself as an ordinary node;
Updates status to selected;
Sends a join packet, join (u,v) to join the cluster constructed by v;
If (more than one such packets are received)
Join the one with smallest ID;
Else
Joins sender with largest logical degree;
Regards itself as a gateway node;
}
On receiving a join packet sent from neighboring node u decreases the logical degree by 1;
}}

3.2 Backup Clusterhead

The disadvantage of the above approach is that CH itself may fail, hence it becomes necessary that the presence of leader is also need to be monitored and in case of its failure another node takes over the CH. We use the concept of deputy clusterhead to solve this problem. Because of the dense population of the network we assume that there must be a member nearer to CH who can cover the rest of the members i.e. in the transmission range of this member. We will choose this member as deputy clusterhead (DCH), who can monitor the leader as follows: (i) After every heartbeat interval, CH node sends a packet to the backup clusterhead, (ii) The packet contains information about each nodes in the group and its arrival indicates that the CH is up and running, (iii) The deputy clusterhead (DCH)

updates its database using data obtained from this packet, (iv) In case of absence of this packet indicating that the primary CH has failed, DCH assumes the role of the leader, (v) This change is multicast to the cluster members who update their database in order to change the communication path of the heartbeat messages, and (vi) The same is multicast to the other CHs through GWs who multicast it to there respective members.

4. Failure Detection Service

Failure detection is handled by using a heartbeat based mechanism within each cluster, in which each node periodically sends a heartbeat message to the CH of the cluster. To check the frequent false detection we are using an adaptive timeout based heartbeat mechanism, which makes the algorithm adaptive to network load and processing load. If the CH do not receive heartbeat message within timeout period from a node then the node is considered to have failed.

In adaptive timeout method concepts of freshness point is used. A freshness point is an estimation of the arrival date of the i^{th} heartbeat message from node v. In [5-6] authors have proposed a method to estimate accurately the arrival time of the heartbeat messages where the arrival time of the next heartbeat of a node is computed by averaging the n last arrival times.

4.1 Failure Detection Algorithm

In our failure detection algorithm each clusterhead maintains a heartbeat receive table for each member node. Clusterhead CH also stores the arrival time of last n heartbeat messages for each member node. Initially table has a fixed timeout period for each node. When a heartbeat from a particular member is received, a new freshness point is calculated using the arrival time of this heartbeat and previous heartbeat messages and new timeout period is set equal to this freshness point.

(i) In every heartbeat interval $\mathbf{T_{HB}}$ each member node sends a heartbeat message to the clusterhead.
(ii) If heartbeat from a particular member is received within the timeout period T_{TM}, clusterhead first saves the arrival time t of this heartbeat message according to its local clock. Then a new freshness point is calculated using the arrival time of this heartbeat and previous heartbeat messages and new timeout period is set equal to this freshness point.
(iii) If the heartbeat from a particular member is not received within the timeout period T_{TM} then that node is considered as failed by the CH. The CH broadcast the firm failure message containing ID of the node to the group.

When a gateway node GW receives this message it forwards this message to the clusterhead of the neighboring clusters. These CHs in turn forward this message to their members and neighboring CH. Because of the inherent broadcast capability of the ad hoc network nodes GW nodes over hear the failure message from the neighboring clusterhead, when neighbor CHs forward the failure message to their neighbor clusters. In this way GW node gets an implicit acknowledgement for the failure message it forwarded. Retransmission of the failure message occurs if it doesn't over hear the failure message from the intended recipient. This reduces the effect of message loss.

5. Simulation Results

5.1 Simulation Model

A simulator is designed in C language where grids are represented as a graph G(V,E). To model the random topology of the ad hoc networks, random graphs with k-connectivity were generated. The experiments were conducted for the networks of varying network sizes and maximum up to 100 nodes. The processing and communication delay are the random numbers generated by a random number generator in the range of 0.001 to 0.01

and 0.1 to 1.0 respectively. Network is clustered using the algorithm described above. To cope up with orphan clusters overlapping of the clusters are allowed. The experiments were conducted for study of the performance parameters such as local detection time, consensus time and message complexity defined in the following section.

5.2 Simulation Parameters

Here, we define the parameters used to evaluate the proposed failure detection service.
(i) Local Detection Time (LDT): It is the time that elapses from p's crash to the time when the clusterhead (CH) of p starts suspecting p permanently faulty.
(ii) Consensus Time (CT): It is the time that elapses from p's crash to the time at which all nodes in the network knows that p has been crashed.
(iii) Message Complexity: It is the number of messages exchanged among nodes to reach the consensus.

5.3Simulation Results

Figure 1 shows the local detection time versus the number of nodes in the network. Local detection time is almost independent of the number of nodes. This is because of one hop cluster formation algorithm in which the distance between a CH and its members are limited by maximum transmission range. So maximum propagation delay of a message is equivalent to maximum transmission range.

Figure 2 shows the number of messages versus the number of nodes. Message complexity i.e total number of message exchange increases linearly with the number of nodes. This shows that algorithm is linearly scalable.

Figure 3 shows the number of messages exchanged versus number of nodes. The consensus time also shows the linear growth with the number of nodes. This is because the distance between two CHs increases with increase in number of nodes.

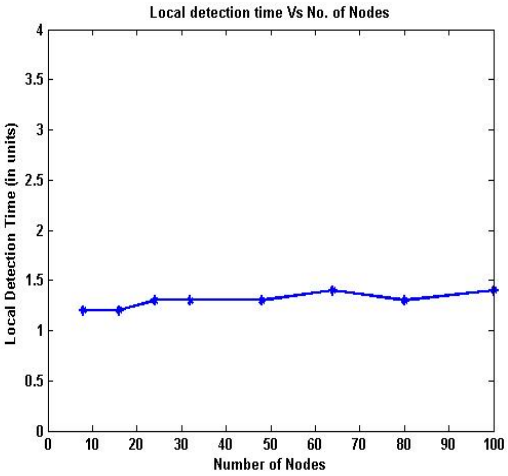

Figure 1. Local detection time graph

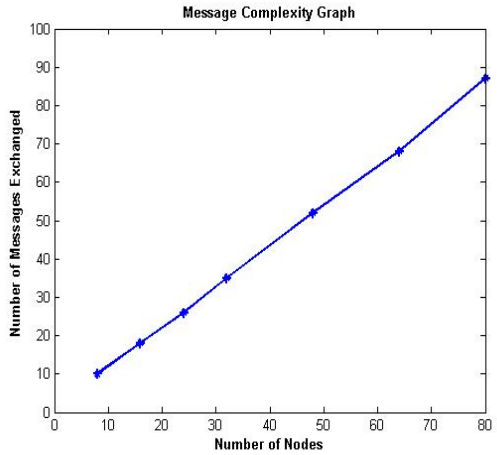

Figure 2. Message complexity graph.

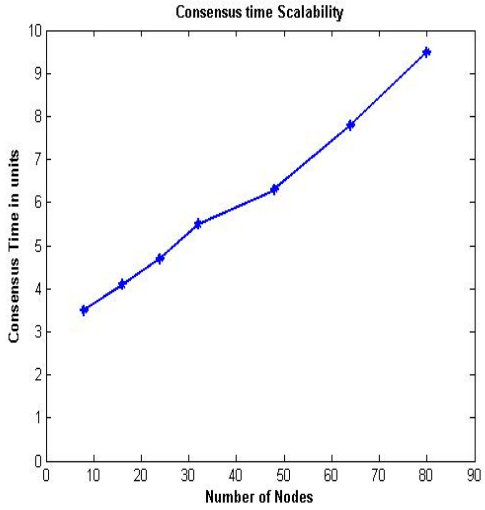

Figure 3. Consensus time scalability

6. Previous Works

Failure detectors were first introduced by Chandra and Toueg in [1]. Subsequent work has focused on different properties and classifications of failure detectors [2, 3, 4, 8, 9]. The failure detection algorithm proposed by authors Bertier, Marin and Sen in [5] is more adaptable to the current state of the network as their approach reduces the false detection and also improves the detection time. The previous algorithms including [5] assume a fully connected and fixed network topology which can not be used for wireless ad hoc network because it follows an arbitrary network topology. In [6], authors have proposed a heartbeat based and variant of the gossip style failure detector for wireless ad hoc network which adapts the detection parameters to the current load of the network such that the failure detection time is a function of previous heartbeat messages. However this approach lacks scalability and is not applicable to the large scale wireless ad hoc network. A cluster based failure detection protocol has been proposed by Ann et al in [7]. The drawbacks of this approach are poor clustering algorithm and large failure detection time.

7. Conclusions

Providing an efficient failure detector is necessary to provide a fault tolerant wireless adhoc network. In this paper we introduced an efficient failure detection service using an efficient clustering approach. Simulation results show that message complexity (bandwidth utilization) increases linearly with the number of nodes. Local detection time is independent of the number of nodes. This approach is linearly scalable in terms of consensus time.

References

1. T.D. Chandra and S. Toueg. *Unreliable failure detectors for reliable distributed systems*. JACM, 43(2):225-267, March 1996.

2. R.V. Renesse, and et. al., *A gossip-style failure detection service.* In Proc. of Int. Conf. on IFIP, 1998.

3. W.Chen and et. al., *On the Quality of Service of Failure Detectors.* In Proc. of 30th Int. Conf. on DSN, June 2000.

4. R.V. Renesse and et al., Hayden. *A Gossip Style Failure Detection Service.* In Proc of. Int. Conf. on IFIP, 1998.

5. M. Bertier and et. al. *Performance Analysis of Hierarchical Failure Detector.* In Proc. of the Int. Conf. on DSN, USA, June 2003

6. Mourad Elhadef and Azzedine Boukerche. ***A Gossip-Style Crash Faults Detection Protocol for Wireless Ad-Hoc and Mesh Networks*** **In Proc. of Int. Conf. IPCCC PP. 600-602, June 2007,**

7. Ann T. Tai and et. al., *Cluster-Based Failure Detection Service for Large-Scale Ad Hoc Wireless Network Applications.* In Proc. of Int. Conf. on DSN, Sep, 2004.

8. Christ Fetzer, and et. al., *An Adaptive Failure Detection Protocol*. In Proc. of the 8th IEEE Symp. on Dependable Computing 2001.

9. Michel Raynal. *A short introduction to failure detectors for asynchronous distributed system. ACM SIGACTs,* March 2005 Vol. 36.

10. Chih-Cheng Tseng and et. al., *Organizing Power Efficient Cluster Based Network Architectures for Wireless Ad Hoc Network.* In Proc. of **Int. Conf. on IPCCC** 2007.

11. Fatiha Djemili Tolba, and et. al., *A Stable Clustering Algorithm for Highly Mobile Ad Hoc Networks.* In Proc. of 2nd Intl. Conf. on System and Networks Communications 2007.

12. P.M.Khilar and S.Mahapatra, *A Hierarchical Approach to Fault Diagnosis in Large-Scale Self-Diagnosable Wireless Adhoc Systems*, Intl. Jourl. of TAIT, Vol.3 No. 4 (October-December 2007), pp. 25-44.

13. P.M.Khilar and S.Mahapatra, *Intermittent Fault Diagnosis in Wireless Sensor Network,* In Proc. of 10th Intl. Conf. on ICIT-2007 , Dec 17-20, NIT, Rourkela, India, pp. 145-147.

14. P.M.Khilar and S.Mahapatra, A Fault Diagnosis Algorithm for Wireless Sensor Networks", In proc. of 19th IASTED Intl. Conf on PDS, Nov. 19-21, 2007, Cambridge, Massachusetts, USA, pp. 443-447.