Indian Journal of Science and Technology, Vol 8(36), DOI: 10.17485/ijst/2015/v8i36/83183, December 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Efficient and Robust Token based DME Algorithm in MANET

B. Gopinathan[1*], S. Subramanian[2] and R. Nedunchezhian[3]

[1]Department of CSE, Adhiyamaan College of Engineering, Hosur - 635109, Tamil Nadu, India; gopinathanme@gmail.com
[2]Karpagam University, Coimbatore - 641021, Tamil Nadu, India; drsraju49@gmail.com
[3]Kalaignar Karunanidhi Institute of Technology, Coimbatore – 641402, Tamil Nadu, India; rajuchezhan@gmail.com

Abstract

In Mobile Adhoc Network mutual exclusion is the important research area, here nodes are waiting for the critical resources. The mutual exclusion allows the mobile nodes to split the resources among each other. Formation of the quorum is needed in order to deliver the data with general intermediate nodes between each other. During the communication, for data transmission between quorum that will use an arbitrator that is common to both the regions. The main objective of an arbitrator is to grant permission to the incoming requests in order to enter into the Critical Section (CS) by forwarding incoming requests to the node that will consist of the token, which in turn will reduce the response time, Synchronization delay and message complexity.

Keywords: Critical Section, Mutual Exclusion, Synchronization

1. Introduction

Mutual exclusion defines the need of knowing that no two parallel nodes are in the critical section at the same time. Parallel nodes should be clocked simultaneously to obtain the split resources. If more than one node is in the critical section it leads to breaking of unity. If there are no fixed infrastructure means, then the mobile devices communicate over wireless links and cooperate in a distributed manner, a mobile ad-hoc network is an independent collection of mobile devices. A critical section is the part of a program that accesses the shared resources. It leads to Distributed Mutual Exclusion (DME), if more than one node wishes to enter CS for accessing the critical resources simultaneously.

Methods for DME problem can be categorized into two groups, based on the Way of selection of node to enter in CS, are described below:

- Token-based algorithms.
- Permission-based algorithms.

In permission based algorithm, if the node needs to enter the CS must collect the permission from all other participating nodes. In the later algorithm, nodes which itself has token is allowed in CS and then the token is passed in other nodes in the network. In the proposed algorithm, two types of tokens i.e.

- Primary token.
- Secondary token.

In the mutual exclusion algorithm proposed by Lamport[4], when a node needs to enter in its CS, it sends the request to neighbor nodes and it waits for responses. When the node moves out from its CS, it sends a release message to neighbor nodes. This algorithm needs 3*(N-1) messages per CS entry. Singhal, et al.[8] suggested that a quorum needs not to consult other quorums that are not currently present for CS look ahead technique was introduced to decrease the message complication. Dynamic information sets, consists of Info set and Status set, to keep the set of quorums that are presently involved in RICART AND AGARWAL[11] introduced a distributed mutual exclusion algorithm which needs 2*(N-1)messages per CS entry.

The time a node enters the CS, it sends the request message to neighbor nodes of the network and waits for

*Author for correspondence

the reply message. If it receives the bond from all of these nodes, it enters the CS Response Time is calculated using Lamport clocks. Maekawa[5] has proposed the algorithm that needs c*(√N) messages has to enter into the critical section. It uses a logical structure, which has a collection of nodes involved with each of the nodes and this in turn has a set of node has a non-null intersection with every set of node involved in each of the nodes. It allows each of the nodes, which to access its CS, to have the permission only from the each member of the set of nodes involved into it.

Singhal[7] increased the performance of the Suzuki and Kazami algorithm, till N messages are in heavy loads. In this method, the heuristic method used to select which the nodes of a system, that are possibly holding or to have the token, the so token request message is sent only to those nodes other than to all the neighbor nodes. When token returns to the requester along the reverse link, it avoids the cycle.

2. Proposed Methodology

In the proposed algorithm, the token based approach is implemented at the quorum level. This algorithm comprises two classes of tokens namely Primary token and Secondary token. The primary token is kept as a unique identifier in the network and it is circulated between two quorums through the arbitrator. The Secondary token is generated by the nodes which itself primary token.

3. The Principle of Proposed Algorithm

3.1 Request Sending Phase

When node Ni interest to enter into the CS means times it will first set the timestamp request Ts to the current time CT and sends the request message back to CS to the nodes which will be present in the info_set as well as to arbitrator and wait for a response message.

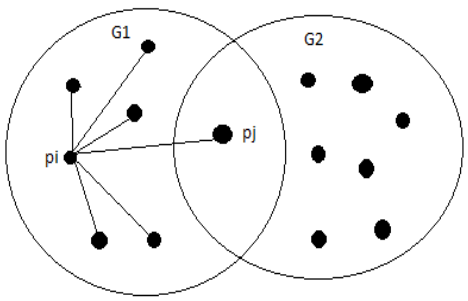

Figure 1. Requesting for token.

3.2 Request Receiving Phase

The receiving request message from the node Ni, here the arbitrator will pass the primary token to node Ni, if it is not presented in the CS. If any other nodes except the arbitrator are receiving a request from the node Ni then, it will send the response message to the node Ni if it is not present in CS or have high priority otherwise the node will store the received request in Request queue Rq.

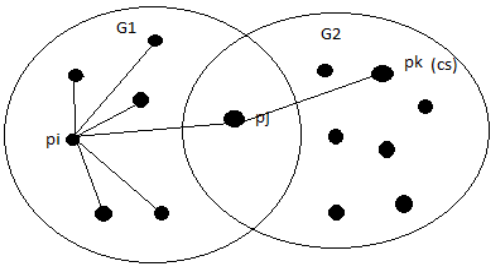

Figure 2. Forwarding request message.

4. Each request in the queue that is granted according to the following set of rules

If there is no node present in the CS means, then the primary token is assigned to the requesting to the requesting node. If more than one node interested in entering into CS means the arbitrator sends a secondary token to the node Ni and then place the Request Queue for the current node. Here, we, the higher priority node is requested. If the node Ni is the development of the primary token, then it will reduce the queue length by the previous CS.

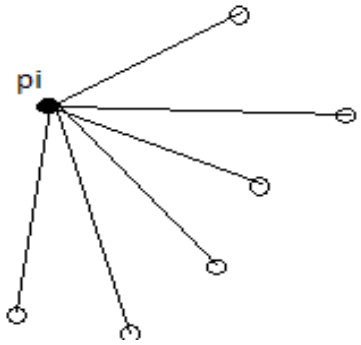

Figure 3. Releasing the CS.

5. Performance

We performed the comparative evaluation of the proposed algorithm, Distributed Mutual Exclusion. It is deployed on the permission and the token based algorithms by using MATLAB Simulator. These algorithms were used by creating networks randomly, it pick a different number of the nodes.

We use the three performance metrics used for comparison are: Response Time, Synchronization Delay and the Message Complexity. Here, we compare the delay with microseconds with a next hop by the other node. Each time the node will pick different hop to the forwarded request to the arbitrator. Then, it will check the delay value in each hop that is taken from the node in order to forward the request.

Then, it considering the message complexity in both of the cases. It will show the comparison of the number of messages passed by each node in a single hop. And,

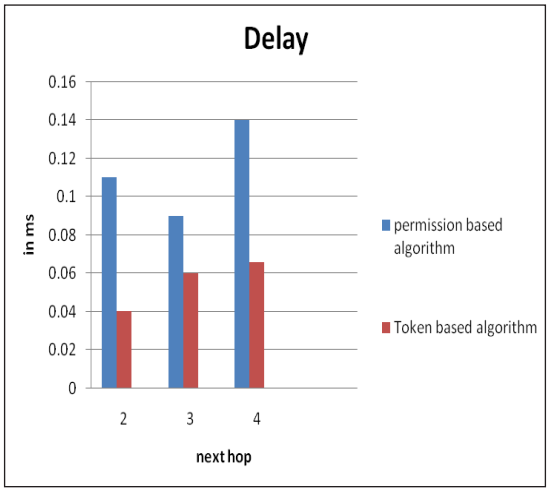

Figure 4. Delay vs next hop graph.

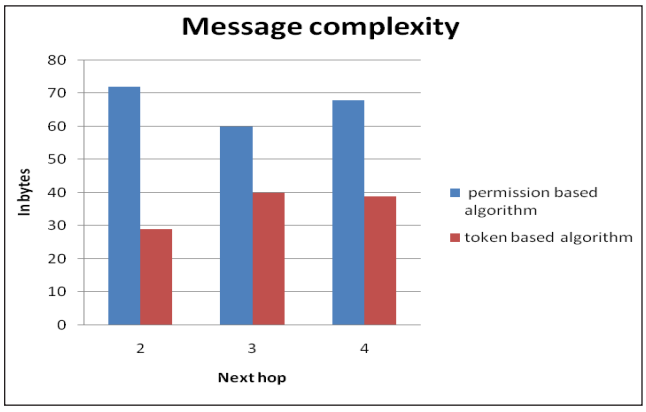

Figure 5. Message complexity vs next hop graph.

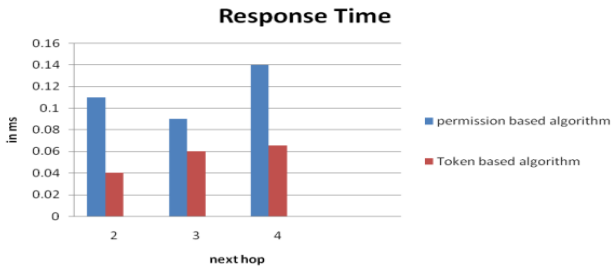

Figure 6. Response time vs next hop graph.

then the Response Time is considered, each hop by hop. It will check the response time taken by each node and also check which path useless response time.

6. Conclusion

The Mobile Adhoc Network does not have any fixed infrastructure and it is a type of wireless network here, the mobile nodes can move independently in any direction. The distributed mutual exclusion admits the mobile nodes to allocate resources between each other. Therefore, they have proposed a distributed group mutual exclusion algorithm that is based on the tokens for permissions and quorum for getting request communication. The proposed algorithm achieves the high concurrency, low response time and synchronization delay and also reduces the message complexity.

7. References

1. Derhab A, Badache N. A distributed mutual exclusion algorithm over multi - routing protocol for mobile ad hoc networks. International Journal of Parallel, Emergent and Distributed Systems. 2008; 23(3):197–18.
2. Sanders BA. The Information Structure of Distributed Mutual Exclusion Algorithms. ACM Transactions on Computer Systems. 1987; 5(3):284–99.
3. Ricart G, Agrawala AK. An optimal algorithm for mutual exclusion in computer networks. Communication of the ACM. 1981; 24(1):9–17.
4. Suzuki I, Kasami T. A distributed mutual exclusion algorithm. ACM Transactions on Computer Systems. 1985; 3(4):344–49.
5. Raymond K. A tree-based algorithm for distributed mutual exclusion. ACM Transactions on Computer Systems. 1989; 7(1):61–77.
6. Lamport L. Time, clocks, and the ordering of events in a distributed system. Magazine Communications of the ACM. 1978; 21(7):558–65.

7. Maekawa M. An algorithm for mutual exclusion in decentralized systems. ACM Transactions on Computer System. 1985; 3(2):145–59.
8. Singhal M, Manivannan D. A distributed mutual exclusion algorithm for mobile computing environments. Proceedings Intelligent Information Systems, IIS' 97, Grand Bahama Island, 1997; 557–61.
9. Singhal M. A heuristically-aided algorithm for mutual exclusion in distributed systems. IEEE Transactions on Computers. 1989; 38(5):651–62.
10. Chang YI, Singhal M, Liu MT. A fault tolerant algorithm for distributed mutual exclusion. Proceedings of 9th IEEE Symposium on Reliable Distributed Systems, Huntsville. AL. 1990; 146–54.
11. Parameswaran M, Hota C. A Novel Permission-based Reliable Distributed Mutual Exclusion Algorithm for MANETs. 2010 IEEE 7th International Conference on Wireless and Optical Communications Networks (WOCN), Colombo. p. 1–6.
12. Wu W, Cao J, Yang J. A fault tolerant mutual exclusion algorithm for mobile ad hoc networks. Pervasive and Mobile Computing. 2008; 4(1):139–60.