IDENTIFYING AND HANDLING OF FALSE ALARM IN SELFISH REPLICA

S.Prabhavathi[1], Ms.R.Bharathi[2]
M.Tech CSE[1], Assistant Professor/CSE[2]
PRIST University, Puducherry-605007.India

ABSTRACT

A MANET is a multi hop mobile wireless network that has neither a fixed infrastructure nor a central server. Each node in a MANET acts as a router, and communicates with each other. A selfish node is one that tries to utilize the network using its limited resource only for its own benefit, since each node in a MANET has resource constraints, such as battery and storage limitations, it would like to enjoy the benefits provided by the resources of other nodes, but it may not make its own resource available to help others. Such selfish behavior can potentially lead to a wide range of problems for a MANET. Consequently, data accessibility in ad hoc networks is lower than that in the conventional fixed networks. There are several data replication techniques are involved to minimize the performance degradation. Due to selfishness and mobility of the node, they decide to cooperate partially or not at all, along with other nodes for resource sharing. In this paper, the leader is elected to avoid the false alarm in identifying the selfish nodes for selfish node detection algorithm that considers partial selfishness and novel replica allocation techniques to properly cope with selfish replica allocation. In turn it increases the data accessibility and reduces average query delay.

Keywords: mobile ad hoc network, selfish nodes, selfish replica allocation

1. INTRODUCTION

A mobile ad-hoc network (MANET) is a selfconfiguring infrastructure less network of mobile devices connected by wireless links. Ad hoc is Latin and means "for this purpose". A large variety of MANET applications have been developed. For example, a MANET can be used in special situations, where installing infrastructure may be difficult, or even infeasible, such as a battlefield or a disaster area. A mobile peer-to-peer file sharing system is another interesting MANET application. The conventional protocols in MANETs such as WRP, DSDV, AODV and DSR assume that all the nodes are cooperative and whenever a node receives a request to relay traffic, it always does so truthfully.

However the experience has shown that as the time passes there is a tendency in the nodes in an ad hoc network to become selfish.

The selfish nodes are not malicious but are reluctant to spend their resources such as CPU time, memory and battery power for others. The problem is especially critical when with the passage of time the nodes have little residual power and want to conserve it for their own purpose. Thus in MANET environment there is a strong motivation for a node to become selfish.

The characteristics of selfish nodes as follows:

i) Do not participate in routing process: A selfish node drops routing messages or it may modify the Route Request and Reply packets by changing TTL value to smallest possible value.

ii) Do not reply or send hello messages: A selfish node may not respond to hello messages, hence other nodes may not be able to detect its presence when they need it.

iii) Intentionally delay the RREQ packet: A selfish node may delay the RREQ packet up to the maximum upper limit time. It will certainly avoid itself from routing paths.

iv) Dropping of data packet: A selfish nodes may participate in routing messages but may not relay data packets

The major reason for such behavior is low residual battery power. It may here be clarified that a selfish node is not malicious and doesn't intend to involve itself in the network damaging activities such as content alteration, spoofing etc. It normally restrains itself from the activities of the other nodes which do not bring any benefit to it.

Data are usually replicated at nodes, other than the original owners, to increase data accessibility to cope with frequent network partitions, replication can simultaneously improve data accessibility and reduce query delay, i.e., query response time, if the mobile nodes in a MANET together have sufficient memory space to hold both all the replicas and the original data.

For example, the response time of a query can be substantially reduced, if the query accesses a data item that has a locally stored replica. However, there is often a trade-off between data accessibility and query delay, since most nodes in a MANET have only limited memory space. For example, a node may hold a part of the frequently accessed data items locally to reduce its own query delay. However, if there is only limited memory space and many of the nodes hold the same replica locally, then some data items would be replaced and missing. Thus, the overall data accessibility would be decreased. Hence, to maximize data accessibility, a node should not hold the same replica that is also held by many other nodes. However, this will increase its own query delay. It can be avoided through replication technique.

The partially selfish node should be taken into account, in addition to the fully selfish nodes to properly handle the selfish replica allocation problem. The credit risk is calculated from several selfishness features to measure the degree of selfishness. The leader is elected to avoid the false alarm while identifying the partial selfish node along with the novel replica allocation

techniques. They are based on the concept of a selfcentered friendship tree (SCF-tree) and its variation to achieve high data accessibility with low communication cost in the presence of selfish nodes.

2) EXISTING SYSTEM

The impact of selfish nodes in a mobile ad hoc network from the perspective of replica allocation, consists of three parts,

i) Detecting selfish nodes

a) Building the SCF (Self-centered friendship) tree.

b) Allocating replica

ii) At a specific period, or relocation period, each node executes the following procedures,

a) Each node detects the selfish nodes based on credit risk scores.

i) node specific

ii) query processing-specific

b) Each node makes its own (partial) topology graph and builds its own SCF-tree by excluding selfish nodes. c) Based on SCF-tree, each node allocates replica in a fully distributed manner.

2.1) DRAWBACKS OF EXISTING SYSTEM

Mobile nodes do not collaborate fully in terms of sharing their memory space. Replication can simultaneously improve data accessibility and reduce query delay, i.e., query response time, if the mobile nodes in a MANET together have sufficient memory space to hold both all the replicas and the original data.

Selfishness in replica allocation is that they do not share its own memory space to store replica for the benefit of other nodes.

To overcome it the selfish node is detected based on credit risk value and self centered friendship tree is constructed by excluding the selfish node for novel replica allocation.

The drawback here is there may be a chance of having false alarm in selfish replica allocation, that is, the particular node credit risk value may be low due to network failure o traffic.

3) PROPOSED SYSTEM

In a proposed system at a specific period, or relocation period, each node executes the following procedures:

a) Each node detects the selfish nodes based on credit risk scores.

b) The Leader is elected to avoid false alarm in detecting selfish node.

c) Each node makes its own (partial) topology graph and builds its own SCF-tree by excluding selfish nodes.

d) Based on SCF-tree, each node allocates replica in a fully distributed manner.

The CR score is updated accordingly during the query processing phase. Borrow the

notion of credit risk from economics to effectively measure the "degree of selfishness." In economics, credit risk is the measured risk of loss due to a debtor's nonpayment of a loan. A bank examines the credit risk of an applicant prior to approving the loan. The measured credit risk of the applicant indicates if he/she is creditworthy. A node wants to know if another node is believable, in the sense that a replica can be paid back, or served upon request to share a memory space in a MANET. With the measured degree of selfishness, propose a novel tree that represents relationships among nodes in a MANET, for replica allocation, termed the SCF-tree. The SCF-tree models human friendship management in the real world. The key strength of the SCF-tree-based replica allocation techniques is that it can minimize the communication cost, while achieving high data accessibility. This is because each node detects selfishness and makes replica allocation at its own

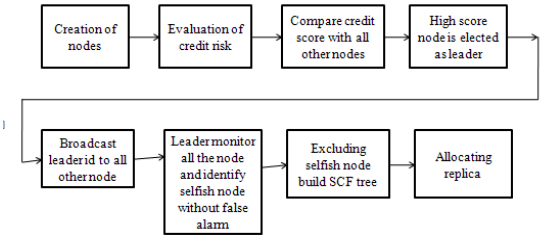


Figure 1. Architecture for handling falseness in identifying selfish node.

The node will be created dynamically and the each node energy level is monitored that is, their credit risk value is calculated based upon their query request response value. Then the node with high credit score value is elected as leader by comparing all the other nodes to monitor the other node to avoid the false alarm in identifying the selfish node for novel replica allocation technique.

3.1 IMPLEMENTATION

The number of mobile nodes is set to 40. The movement pattern of nodes follows the random waypoint model, where each node remains stationary for a pause time and then it selects a random destination and moves to the destination. After reaching the destination, it again stops for a pause time and repeats this behavior. The default number of selfish nodes is set to be 70 percent of the entire nodes in simulation, based on the observation of a real application. Set 75 percent of selfish nodes to be type-3 (i.e., partially selfish) and the remaining to be type-2 (i.e., fully selfish). Type-3 nodes consist of three groups of equal size. Each group uses 25, 50 and 75 percent of its memory space for the selfish area Type-2 nodes will not accept replica allocation requests from other nodes in the replica allocation phase, thus being expected to create significant selfishness alarm in

query processing. Type-3 nodes will accept or reject replica allocation requests according to their local status, thereby causing some selfishness alarms in subsequent query processing. When a node Ni makes an access request to a data item (i.e., issuing a query), it checks its own memory space first. The request is successful when Ni holds the original or replica of the data item in its local memory. If it does not hold the original or replica, the request will be broadcast. The request is also successful when Ni receives any reply from at least one node connected to Ni with one hop or multiple hops, which holds the original or replica of the targeted data item. Otherwise, the request, or query processing, fails. When a node Ni receives a data access request, it either 1) serves the request by sending its original or replica if it holds the target data item (the data may go through multiple hops before reaching the requester), or 2) forward the request to its neighbors if it does not hold the target data item. Define three types of behavioral states for nodes from the viewpoint of selfish replica allocation.

i) Type-1 node: The nodes are non-selfish nodes. The nodes hold replicas allocated by other nodes within the limits of their memory space.

ii) Type-2 node: The nodes are fully selfish nodes. The nodes do not hold replicas allocated by other nodes, but allocate replicas to other nodes for their accessibility.

iii) Type-3 node: The nodes are partially selfish nodes. The nodes use their memory space partially for allocated replicas by other nodes. Their memory space may be divided logically into two parts: selfish and public area. These nodes allocate replicas to other nodes for their accessibility. The detection of the type-3 nodes is complex, because they are not always selfish. In some sense, a type-3 node might be considered as non-selfish, since the node shares part of its memory space. Considered it as (partial) selfish, because the node also leads to the selfish replica allocation problem. The selfish and nonselfish nodes perform the same procedure when they

receive a data access request, although they behave differently in using their memory space.

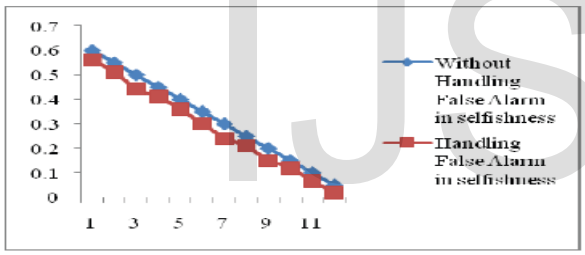
Partial selfish nodes will accept or reject replica allocation requests according to their local status, thereby causing some selfishness alarms in subsequent query processing.

The credit score will be calculated for each and every node and it is compared.

The node which has high credit risk value is elected as leader; the credit risk is calculated based upon the query request response, to handle the false alarm in detecting the selfish nodes.

The false alarm may occur when detecting the node as selfish node that has low credit risk value due to network failure or traffic.

After identifying the Selfish nodes without any false alarm the self-centered friendship tree is constructed by excluding the selfish nodes and replica is allocated.



Graph 3.1. Comparison between with and without handling false alarm in selfish replica allocation.

On average about 56 to 50 percent of the overall selfishness alarm are reduced by node selfishness, not disconnections and in parallel it increases the data accessibility and reduces average query delay which is graphically depicted manually and plotted using MSExcel and shown

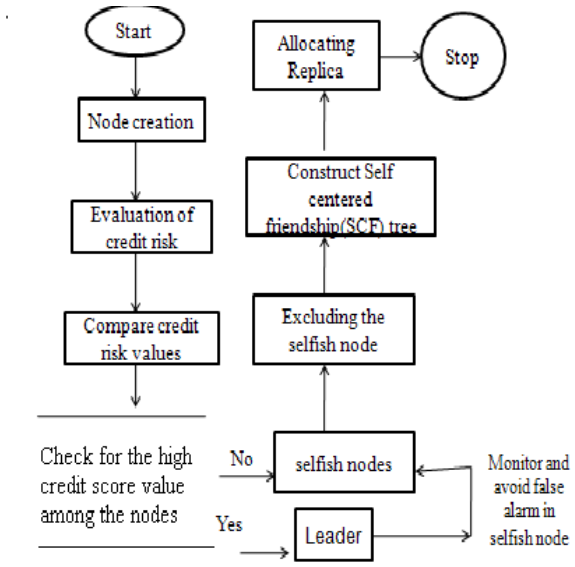


Figure 2. DFD for electing leader and allocating replica.

4) CONCLUSION

The problem addressed here are selfish nodes from the replica allocation perspective. Term this problem selfish replica allocation. The proposed selfish node detection method and novel replica allocation techniques are used to handle the selfish replica allocation appropriately. The notion of credit risk is applied to detect selfish nodes. Every node in a MANET calculates credit risk information on other connected nodes individually to measure the degree of selfishness. The node with high credit Score is elected as leader and it will broadcast the message about its id, and monitor all the other nodes and avoid false alarm in detecting selfish nodes. So, that without any falseness in detecting selfishness the selfish node are excluded and

SCF tree will be constructed and replica will be allocated The proposed strategies outperform existing replica allocation techniques in terms of data accessibility, communication cost, and query delay. In future Plan to identify and handle false alarms in selfish replica allocation, on different mobility pattern.

5) REFERENCES

[1] C.E. Perkins and P. Bhagwat,(1994) 'Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers' Proc. ACM SIGCOMM '94, pp. 234-244.

[2] C.E. Perkins and E.M. Royer,(1999) 'Ad Hoc on Demand Distance Vector Routing,' Proc. IEEE Workshop Mobile Computing Systems and Applications, pp. 90-100.

[3] C.R. Lin and M. Gerla, (1995) 'A distributed architecture for multimedia in a multihop dynamic packet radio network,' Proc. IEEE Globecom'95, pp.1468-1472.

[4] D.B. Johnson,(1994) 'Routing in Ad Hoc Networks of Mobile Hosts,' Proc. IEEE Workshop Mobile Computing Systems and Applications, pp. 158- 163.

[5] D. Johnson, D. A. Maltz, (1996) 'Dynamic source routing in ad hoc wireless networks,' in Mobile Computing (T. Imielinski and H. Korth, eds.), Kluwer Acad. Publ.

[6] E. Adar and B.A. Huberman, (2000) 'Free Riding on Gnutella' First Monday, vol. 5, no. 10, pp. 1-22

[7] E. Cohen and S. Shenker, (2002) 'Replication Strategies in Unstructured Peer-to-Peer Networks' Proc. ACM SIGCOMM, pp. 177-190

[8] Hyun injin kim, jon M.peha, Carnegie mellon university(2008),'Detecting selfish behavior in a cooperative commons',research show,IEEE span.

[9] Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu. (2012) 'Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network' IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 2

[10] Noman Mohammed, Hadi Otrok, Lingyu Wang,Mourad Debbabi, and Prabir Bhattacharya, (2011) 'Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET'IEEE transactions on dependable and secure computing, VOL. 8, NO. 1