IMPROVEMENT OF DATA SHARING OVER MOBILE AD HOC NETWORK BASED ON SELF-STABILIZE REPLICA ALLOCATION

R. Varsha, Student

Miss R.Mercy, Assistant Professor

Abstract

In a mobile ad hoc network, disconnections occur frequently due to various factors like power failure, mobility of the nodes, atmosphere conditions etc. This result in data inaccessibility, thereby causing selfishness. The reply from source node holding a target data item may not reach its destination due to two reasons, disconnections and node selfishness. In a frequent time interval, replica allocation will be performed based on the Self Centered Friendship (SCF) tree of each node in order to avoid selfishness. The source node fail to assign replica to a particular node in which the destination node cannot tell its status, since their impacts are high, i.e., data inaccessibility. Faulty Root Alarm (FRA) occurs when a particular node and its sub SCF tree vanishes unexpectedly and a massive data loses arises. In this paper we develop and Faulty Root Alarm to retain all the replicas that will be accessible in the remaining networks and a Self-Stabilize Replica Allocation (SSRA) algorithm for data allocation based on selfishness. The SSRA technique decreases query delay, improves the efficiency and reduce communication cost.

Keywords— Mobile Ad hoc Network, Faulty Root Alarm, Self Stabilize Replica Allocation.

.

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) can be described as an autonomous collection of mobile nodes that communicate over relatively low capacity wireless links, without a centralized infrastructure. It is a peer-to-peer multihop mobile wireless network. MANETs find applications in diverse fields ranging from low-power military wireless sensor networks to large-scale civilian applications, and emergency search/rescue operations. A mobile peer-to-peer file sharing system is another interesting MANET application .Network partitions can occur frequently, since nodes move freely in a MANET, causing some data to be often inaccessible to some of the nodes causing data inaccessibility. Therefore data's are usually replicated at nodes, other than the original nodes, to increase data accessibility to cope with frequent network partitions.

Non-cooperative actions of mobile nodes are usually termed as selfishness, which is different from malicious behavior. Selfish nodes use the network for their own communication and refuse to cooperate in forwarding packets to other nodes which causes, increase the query processing time and overall power usage. A selfish node would utilize the benefits provided by the resources of other nodes, but will not make available its own resources to help others. They do not have the intention to damage the network.

In this paper we address the problem of faulty alarm which is a major issue while detecting selfish nodes in manet.i.e, when network disconnections occur, the node will identify it as selfish and not as network disconnection. This problem has been solved by providing an alarm when network disconnections occur. The technical contributions of this paper are summarized as follows:

- Faulty root alarm detection and handling.
- Self-Stabilize Replica Allocation.

The rest of this paper contained as follows: In Section 2, we review the related work. Section 3 presents our approach for the proposed strategy. Finally, Section 4 concludes the paper.

2. RELATED WORK

2.1 Selfishness Handling in Replica Allocation

Nodes move freely in manet due to frequent network partitions, causing some data to be often inaccessible to some of the nodes. Hence, data accessibility is often an important performance metric in a MANET. Such selfish behavior can potentially lead to a wide range of problems for a MANET. Data are usually replicated at nodes, other than the original owners, to increase data accessibility to cope with frequent network partitions. J. H. Choi et al report that the selfish node detection and reduce the effect of selfishness in data replica allocation over the network [1]. This consists of detecting selfish nodes based by building the SCF-tree based on the topology and allocating replica. At a specific relocation period, each node detects the selfish nodes based on credit risk scores. SCF-tree based replica allocation can minimize the communication cost, while achieving high data accessibility.

In this paper a sample topology of the nodes in the network and construction SCF-tree based on each nodes with different routes is described.

Selfish node detection was based on calculating a credit risk score and checking it with a threshold value to detect whether the node is selfish or not. The construction of SCF-tree is inspired by our human friendship management in the real world. In the real world, a friendship, which is a form of social bond, is made individually. As an example, although A and B are friends, the friends of A are not always the same as the friends of B. With the help of SCF-tree, Jae-Ho Choi aim to reduce the communication cost, while still achieving good data accessibility. After building the SCF-tree, a node allocates replica at every relocation period. When a node receives a data access request, it either serves the request by sending its original or replica if it holds the target data item or forward the request to its neighbors if it does not hold the target data item. Each node asks nonselfish nodes within its SCF-tree to hold replica when it cannot hold replica in its local memory space. Since the SCF-tree based replica allocation is performed in a fully distributed manner, each node determines replica allocation individually without any communication with other nodes. The problem arises when network disconnections occur in the network. The node will identify it as selfishness behavior. This has been named as false alarm.

2.2 Consistency Management Strategies For Data Replication

In Manet, data replication drastically improves data availability. However, since mobile host's mobility causes frequent network partitioning, consistency management of data operations on replicas becomes a crucial issue. In such an environment, the global consistency of data operations on replicas is not desirable by many applications. Thus, new consistency maintenance based on local conditions such as location and time need to be investigated.

T. Hara and S.K. Madria [6] attempts to classify different consistency levels according to requirements from applications and provides protocols to realize them and also report simulation results to investigate the characteristics of these consistency protocols in a manet.

In this paper[6] a quorum system based on dynamic quorums is used, where mobile hosts are dynamically grouped into quorums, thus, it is tolerant to unpredictable network topology change and node failures in MANETs. The consistency of data operations on replicas is hierarchically managed at two levels; among peers in each region and among proxies, calculates the sizes of quorums and dynamically constructs quorums with the calculated sizes, by using the information that is easily available

1. SCF-Tree: Self Centered Friendship Tree :This strategies are inspired by the real-world observations in economics in terms of credit risk and in human friendship management in terms of choosing one's friends completely at one's own discretion.

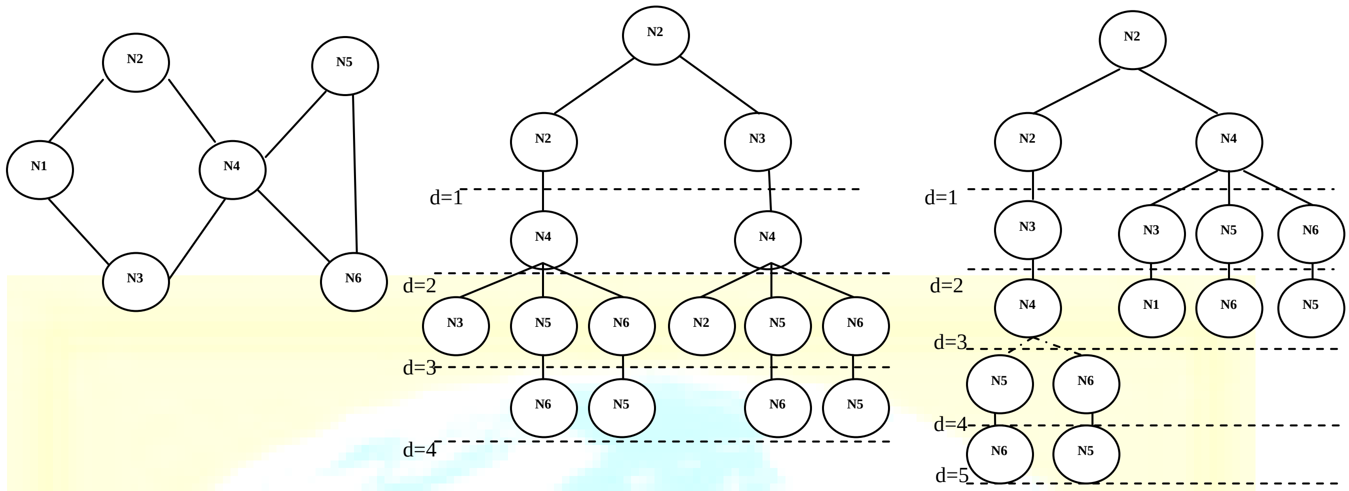
by proxies specifically, to calculate quorum sizes, each proxy uses the information on the total number of regions in the entire network and on the total number of peers having eachreplica in its responsible region. The problem arises during complex transactions in the network.

2.3 Selfishness in Manet

Routing protocols for a manet have assumed that all types of mobile nodes voluntarily participate in forwarding others' packets. This is a reasonable assumption because all MNs in a MANET belonged to a single authority. In the near future, however, a MANET may consist of MNs that belong to many different organizations since numerous civilian applications are expected to crop up. In this situation, some MNs may run independently and purposely decide not to forward packets so as to save their own energy. This could potentially lead to network partitioning and corresponding performance degradation. To minimize such situations in MANETs they have explored the use of both the carrot and the stick approaches by having reputation-based, credit-payment, and game theory schemes[7].

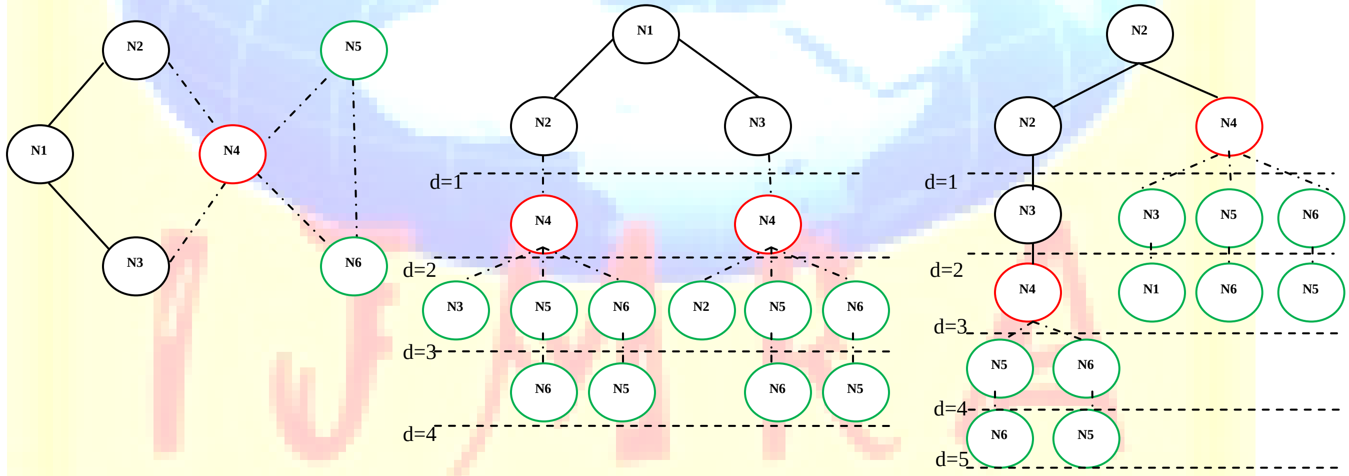
The techniques include reputation-based scheme to mitigate bad effects of misbehaving MNs that are selfish, malicious, broken, or over-loaded. Each MN runs two extensions on top of watchdog. The watchdog overhears neighbor MNs' transmission to check if neighbors are forwarding the packets correctly or not. If a neighbor repeats

any misbehavior more times than a predefined threshold value, the observer notifies the source node of this by sending a message. This information is collected by the watchdog located at each MN, which maintains a rating for every other MN. This rating is used in calculating the reliability of paths to avoid using misbehaving. In credit based scheme MNs provide service to other MNs receive virtual currency or credit, and MNs benefiting from the service are charged for it whereas game theory uses Generous Tit-For-Tat and multiple-GTFT are the first relay acceptance algorithms to use game theory in MANETs. GTFT is for the case where all requests are relayed by just one MN until they reach the destination, and m-GTFT is for when multiple relays exist between the source and the destination. These algorithms are for a node to balance the energy consumed for other MNs with the energy used by others for itself; and to find an optimal trade-off between blocking probability and power consumption. The work considers only binary behavioral states for selfish nodes from the network routing perspective: selfish or not (i.e., forwarding data or not). Note that selfish and nonselfish nodes perform the same procedure when they receive a data access request, although they behave differently in using their memory space.



(a) Sample topology G (b)SCF-tree of N1 (c)SCF-tree of N2

Fig A. Before Faulty Root Alarm



(a) Sample topology G (b)SCF-tree of N1 (c)SCF-tree of N2

Fig B. After Faulty Root Alarm

3. PROPOSEDSTRATEGY

Our strategy consists of identification and detection of FRA when network disconnections occur in the network and results in data inaccessibility. The alarm helps in identifying which all nodes are currently active in the network. When a particular node disappears from the network, their subs trees will also get disappear from the SCF tree and that data's will be inaccessible and results in a massive data loss.

The topology consists of a controller which is capable of identifying and maintaining the status of each nodes i.e., whether the nodes are in active or inactive stage. The controller sends requests each time to all the nodes in the network only to identify its status like a beehive to check which all nodes are active. If a node fails to reply, the server once again sends request to conform that particular node have failed, now is in inactive stage and disconnected from the network. Then the controller informs all other nodes regarding the failure of a particular node by providing an alarm named as FRA.

The FRA concept consists of rearranging the Self-centered friendship tree considering only the active nodes in the network. The concept can be explained in the following steps.

Step1. Identifying the inactive nodes in the network.

Step2. Sending FRA to all the nodes.

Step3. Modifying the SCF-tree by removing the inactive nodes and constructs the tree for each of the nodes.

The figure A and figure B represents the diagrammatic representation of SCF-tree before and after the Faulty root alarm. In figure B the red circle denotes the node that left the network due to disconnection. Due to its disconnection its sub- tree and the corresponding nodes will be inaccessible which is denoted by green circles and the dotted line connecting the nodes indicates, that particular path will be inaccessible. Thereby modifying the sub-tree with the available nodes.

After rearranging the SCF-tree, we also introduce a new data replica algorithm, SSRA algorithm to allocate the remaining nodes based on FRA and selfishness. It reallocates the data's that were present in the nodes that are excluded from the network due to disconnection.

Suppose each node has the capability of holding three packet data for network sharing. In the network collectively has m number of data equally distributed among n nodes. When FRA generates and p nodes disappear from SCF-tree of a particular node during disconnection such that the node as well as its sub-tree vanishes accordingly. 3n data's are equally distributed to each node in the network. So the available nodes will be n-p. Therefore data that were allocated to n nodes now must be allocated to n-p nodes. Here the SSRA algorithm consists of 3cases.

(i) When m=3(n-p), then all data is equally distributed to the remaining nodes. there is no need of additional memory space to be created.

(ii) m<3(n-p), then the data is allocate to the all nodes and the remaining memory is allocate the repeated data, so it increase the accessibility.

(iii) m>3(n-p), from 3(n-p) data is allocate the all the nodes and the controller request all the nodes to create the additional memory space for storing remaining data i.e., m-3(n-p).

From the above case if 3n data's are available, the number of non-allocated data can be observed using the equation as below.

No: of Non-allocated data = 3n-3(n-p).

Therefore the number of data's allocated in each node can be found out using the equation below.

Data's to be allocated in each of the available nodes= $\frac{m-3(n-p).}{n-p}$

The second case, where the memory assigned and data to be allocated are different in which the data to be allocated is less than the memory assigned. In that case additional free memory will be available. Third case consists of a condition in which data to be allocated will be greater than the memory assigned. In that case the data's available will be equally distributed and requires additional memory space for its allocation which will be handled by the controller by sending requests to each of the available nodes to share their memory space.

When the inactive nodes again become active, the same procedure follows by modifying the tree and allocating the data's efficiently.

4. CONCLUSION

From the networking view point we presented an approach for identification and handling of a faulty root alarm during data sharing where network disconnections occur frequently which could lead to could lead to overall poor data accessibility in a MANET. Node holding a target data item may not reach its destination due to disconnection, not its selfishness was the main problem in this paper. We proposed a self-stabilize replica allocation algorithm. This algorithm modifies the SCF tree by excluding the nodes that have disconnected from the network and data are reallocated based on the available nodes in the network. The nodes that have vanished from the network will be identified by the controller, who manages by sending request to identify the status of each of the nodes. After reallocation period the data allocation details of each node as statistics will be displayed to identify the location of where the data will be residing.

REFERENCES

[1] Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu," Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network",Proc. IEEE Transactions On Mobile Computing, Vol. 11, No. 2, 2012.

[2] H. Miranda and L. Rodrigues, "Friends and Foes: Preventing Selfishness in Open Mobile Ad hoc Networks,"Proc. IEEE Int'l Conf. Distributed Computing Systems Workshops ,pp. 440-445, 2003.

[3] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," Proc. IEEE Wireless Comm. and Networking, pp. 2137-2142 2005.

[4] S.-Y. Wu and Y.-T. Chang, "A User-Centered Approach to Active Replica Management in Mobile Environments," IEEE Trans.Mobile Computing,vol. 5, no. 11, pp. 1606-1619, 2006.

[5] V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao, "Cooperation in Wireless Ad Hoc Networks," Proc. IEEE Infocom,pp. 808-817, 2003.

[6] T. Hara and S.K. Madria, "Consistency Management Strategies forData Replication in Mobile Ad Hoc Networks,"IEEE Trans. Mobile Computing,vol. 8, no. 7, pp. 950-967, 2009.

[7] Y. Yoo and D.P. Agrawal, "Why Does It Pay to be Selfish in a MANET,"IEEE Wireless Comm.,vol. 13, no. 6, pp. 87-97, 2006.

[8] T. Hara, "Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility," Proc. IEEE INFOCOM,pp. 1568-1576,2001.

[9] S.-Y. Wu and Y.-T. Chang, “A User-Centered Approach to Active Replica Management in Mobile Environments,” IEEE Trans. Mobile Computing,vol. 5, no. 11, pp. 1606-1619, Nov. 2006.

[10] L. Yin and G. Cao, “Balancing the Tradeoffs between Data Accessibility and Query Delay in Ad Hoc Networks,”Proc. IEEE Int’l Symp. Reliable Distributed Systems,pp. 289-298, 2004.

[11] Y. Liu and Y. Yang, “Reputation Propagation and Agreement in Mobile Ad-Hoc Networks,”Proc. IEEE Wireless Comm. and Networking Conf.,pp. 1510-1515, 2003.

[12] N. Laoutaris, O. Telelis, V. Zissimopoulos, and I. Stavrakakis, “Distributed Selfish RepLication,” IEEE Trans. Parallel and Distributed Systems,vol. 17, no. 12, pp. 1401-1413, Dec. 2006.

[13] G. Ding and B. Bhargava, “Peer-to-Peer File-Sharing over Mobile Ad Hoc Networks,”Proc. IEEE Ann. Conf. Pervasive Computing and Comm. Workshops,pp. 104-108, 2004.

[14] M. Feldman and J. Chuang, “Overcoming Free-Riding Behavior in Peer-to-Peer Systems,”SIGecom Exchanges,vol. 5, no. 4, pp. 41-50, 2005.

[15] B.-G. Chun, K. Chaudhuri, H. Wee, M. Barreno, C.H. Papadimi-triou, and J. Kubiatowicz, “Selfish Caching in Distributed Systems:A Game-Theoretic Analysis,”Proc. ACM Symp. Principles of Distributed Computing,pp. 21-30, 2004.

[16] M. Li, W.-C. Lee, and A. Sivasubramaniam, “Efficient Peer-to-Peer Information Sharing over Mobile Ad Hoc Networks,”Proc. World Wide Web (WWW) Workshop Emerging Applications for Wireless and Mobile Access,pp. 2-6, 2004.

[17] P. Padmanabhan, L. Gruenwald, A. Vallur, and M. Atiquzzaman, “A Survey of Data Replication Techniques for Mobile Ad Hoc Network Databases,”The Int’l J. Very Large Data Bases,vol. 17, no. 5, pp. 1143-1164, 2008.

[18] K. Paul and D. Westhoff, “Context Aware Detection of Selfish Nodes in DSR Based Ad-Hoc Networks,”Proc. IEEE Global Telecomm. Conf.,pp. 178-182, 2002.

[19] J. Zhai, Q. Li, and X. Li, “Data Caching in Selfish Manets,” Proc.
Int’l Conf. Computer Network and Mobile Computing, pp. 208-217,2005.

Author's Detail :

Varsha.R doing her M.E in Computer Science and Engineering at PSN College of Engineering And Technology, Tirunelveli. She received her B.Tech in Computer Science from SIST Engineering College, Trivandrum in 2006. Her research interests include Networking, Web Development.

IJMRA