IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 5 (Jul. - Aug. 2013), PP 07-13
www.iosrjournals.org

Selfish Node Detection in Replica Allocation over MANETs

A. Kishore Kumar[1], Surya Bahadhur[2]

M.Tech Scholar, Dept. of CSE, Madanapalle Institute of Technology and Sciences, Madanapalle, JNTUA[1]
Assistant professor, Dept. of CSE, Madanapalle Institute of Technology and Sciences, Madanapalle, JNTUA[2]

Abstract: *MOBILE ad hoc networks (MANETs) have attracted a lot of attention due to the popularity of mobile devices and the advances in wireless communication technologies. A MANET is a peer-to-peer 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. In a mobile ad hoc network, the mobility and resource constraints of mobile nodes may lead to network partitioning or performance degradation. Several data replication techniques have been proposed to minimize performance degradation. Most of them assume that all mobile nodes collaborate fully in terms of sharing their memory space. In reality, however, some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes. These selfish nodes could then reduce the overall data accessibility in the network. In this paper, we examine the impact of selfish nodes in a mobile ad hoc network from the perspective of replica allocation. We term this selfish replica allocation. In particular, we develop a selfish node detection algorithm that considers partial selfishness and novel replica allocation techniques to properly cope with selfish replica allocation. The conducted simulations demonstrate the proposed approach outperforms traditional cooperative replica allocation techniques in terms of data accessibility, communication cost, and average query delay.*

Index Terms*: Mobile ad hoc networks, selfish nodes, router, replica allocation.*

I. Introduction

A MANET is a collection of autonomous mobile users to communicate over relatively bandwidth constrained wireless links. The nodes are mobile and the network topology between nodes may change rapidly and unpredictably at any time. The network is decentralized which does not having central server or controller, where all nodes must be discovering the topology and delivering messages to other nodes. The application for MANETs is different ranging from small and static networks that are constrained by power sources, to large-scale highly mobile dynamic networks. these network protocols design is a complex issue. However efficient distributed algorithms are needed for MANETs to determine organization of network, scheduling of link, and routing. MANETs are divided into two categories: closed and open in the work. In a closed MANET, all nodes voluntarily participate in and organize the network. in an open MANET individual nodes may have different objectives. In this case, some nodes can be selfish to preserve their own resources.

MANET (Mobile ad hoc network) is dynamic networks populated by mobile stations. Stations in MANETs are usually laptops or mobile phones. These devices feature Bluetooth or Wi-Fi network interfaces and communicate in a decentralized manner. Mobile ad hoc networks are composed of a set of communicating devices able to spontaneously interconnect without any pre-existing infrastructure for it. Devices in specific range can communicate in a point-to-point fashion. More and more people are interested in mobile ad hoc networks.

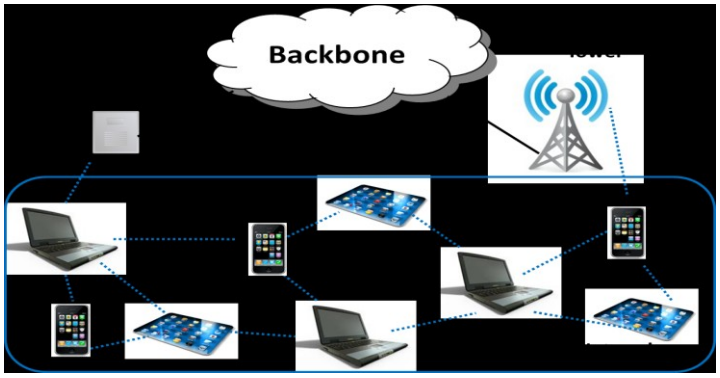

Figure.1. MANET

Mobile networking is one of the most important technologies supporting pervasive computing. Mobility is a vital feature of MANET. Because of the high cost and lack of flexibility of such networks, experimentation is generally achievable through simulation. During the last years, advances in both hardware and software techniques have resulted in mobile hosts and wireless networking common and diverse. Generally there are two different approaches for enabling wireless mobile units to communicate with each other:

1. Infrastructure-Based network: Wireless mobile networks usually been based on the cellular concept and depend on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the stable network infrastructure.

2. Infrastructure less network: In infrastructure less approach there is no central administration for the entire network. The mobile wireless network is infrastructure less in manner commonly known as a mobile ad hoc network (MANET). A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing stationary network infrastructure.

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies.

Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power and availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources.

In ad hoc networks devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes.

This information is sensitive. So there may be occurred malicious attacks running on it. In routing protocols, there are two types of threats. External attackers are first threat, which injecting routing information, replaying or distorting routing information, and inefficient routing which causes retransmission. The second and most severe threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures.

The provision of systematic approaches to evaluate the impact of such threats on particular routing protocols remains an open challenge today. Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks. The active attacks are further classified into internal attacks and external attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques. Internal attacks are from internal nodes which are difficult to identify because those are actually authorized nodes and part of the network.

1.1 Characteristics: Mobile Ad hoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes directly communicate which are reside in the radio range, where as intermediate node is needed to communicate two nodes which are not residing the radio range to route their packets. MANETs are fully distributed and it does not need any infrastructure at any place. So that MANETs are robust and exile.

Main characteristics of MANETs:

- Wireless communication done.
- Nodes act as both hosts and routers.
- No need of infrastructure and decentralized network.

1.2 States of Node Behavior:

In MANETs each mobile node has limited local memory space for data. Every node acts as a data provider of several data items and also a data consumer. Each node local memory space holds the data item replicas which are relocated in specific period. There are m nodes (n_1, $n_{2,}$….$n_{m)}$ and no central server determines the Access Frequency of Nodes and allocation of replica in memory space. In open MANET any node freely joins and organizes.

The work considers only binary behavioral states for selfish nodes from the network routing perspective: selfish or not (i.e., forwarding data or not). It is also necessary to further consider the partial selfish behavior to handle the selfish replica allocation. So, nodes are three types in selfish replica allocation view. The nodes which divided into three types are following.

Type-1 node: non-selfish nodes are type-1 node. These nodes provide memory space within limits to hold replicas allocated by other nodes.

Type-2 node: fully selfish nodes are type-2 node. These nodes do not provide memory space to hold replicas allocated by other nodes.

Type-3 node: partially selfish nodes are type-3 node. These nodes partially provide memory space to hold replicas allocated by other nodes. This memory space logically divided into two parts: selfish and public area.

Non selfish nodes allocate their memory space. Selfish nodes do not allocate their memory space for the purpose of other nodes. Partially selfish nodes allocate minimum portion of their memory space for the purpose of other nodes and remaining for the benefit of own node.

Minimising the effects of selfish nodes will be important to increase the data accessibility between the nodes. The replica allocation techniques such as Static Access Frequency (SAF)[2], Dynamic Access Frequency and Neighbourhood (DAFN)[2][3], and Dynamic Connectivity-based Grouping (DCG)[2] failed to consider the selfish nodes, Hence improvements have to be made in replica allocation techniques that consider selfish replica allocation. The friendship manner replication has to be done in relocation period (The time gap between each replica allocation) produce the new technique called SCF-tree based replica allocation [1]. Various techniques have been proposed to handle the problem of selfish behavior from the network perspective. As described in, techniques handling selfish nodes can be classified into three categories, they are following,

Reputation-Based Techniques: Each node observes the behaviors of others and uses the acquired information for routing.

Credit-Payment Techniques: Each node gives a credit to others, as a reward for data forwarding . The acquired credit is then used to send data to others.

Game Theory-Based Techniques: It assumes that all rational nodes can determine their own optimal strategies to maximize their profit. The game theory-based techniques want to find the Nash Equilibrium point to maximize system performance.

All the above techniques focused on packet forwarding in between the selfish nodes. The work introduced several trust models and trust management schemes in a MANET that can help mitigate selfishness in a MANET. Although the work introduces several schemes for the detection of selfish nodes, the work also focuses on the selfish behavior from the network perspective, such as dropping or refusing to forward packets. Note that traditional detection techniques in a network domain cannot be directly applied to the selfish replica allocation problem, since they mainly make a binary decision: selfish or not, that is, forwarding data or not. However, we need to consider the partial selfish behaviors into account in the selfish replica allocation problem. In the pioneering work, some effective replica allocation techniques are suggested, those are following,

Static Access Frequency (SAF) Method: In SAF method, the nodes allocate replica of data items according to the access frequencies of that data items. Mobile nodes with the same access frequencies to data items allocate the same replica. A mobile node can access data items held by other connected mobile hosts, and it is more possible to share different kinds of replica among them. The SAF method causes low data accessibility when many mobile hosts have the similar access characteristics hence some of the data items to be duplicated in many nodes.

Dynamic Connectivity Based Grouping Method (DCG): The DCG method shares replicas in larger groups of mobile hosts than DAFN. At every relocation period, each mobile host broadcasts its host identifier. After all mobile hosts complete the broadcasts; every host knows the connected mobile hosts and the network topology from the received host identifiers. In each set of mobile hosts connected to each other, the mobile host with the lowest host identifier suffix executes an algorithm to find bi-connected components with the network topology known by received messages.

Even if a mobile host belongs to more than one bi-connected component, it can only belong to one group in which the corresponding bi-connected component was found first. By grouping mobile hosts as bi-connected components, the group is not divided even if one mobile host disappears from the network or one link is disconnected in the groups. Thus, it is assumed that the group has high stability affected, unless they were in sleep mode and also if the selected routes are via specific host, the battery of this host will be exhausted quickly.

Dynamic Connectivity-Based Grouping with Detection (DCG +): The technique combines DCG with our detection method. Initially, groups of nodes are created according to the DCG methodology. Subsequently, in each group, selfish nodes are detected based on our detection method. For the detection, each node in a group sends its nCR scores to the coordinator with the lowest suffix of node identifier in the group.

The coordinator excludes selfish node(s) from the group for replica allocation. As a result, only non-selfish nodes form a group again. The replica allocation is only performed within the final group without any selfish nodes. After replica allocation, the coordinator shares the information of replica allocation with group members for the subsequent selfishness detection. In particular, selfish nodes are determined to be selfish only when all other nodes in the group agree with the node's selfishness. The other approaches to determine selfishness, including the agreement of 1) at least one and 2) the majority of nodes.

Dynamic Access Frequency and Neighbourhood (DAFN): The algorithm of this method is as follows:
1) At a relocation period, each mobile host broadcasts its host identifier and information on access frequencies to data items. After all mobile hosts complete the broadcasts, from the received host identifiers; every host shall know its connected mobile hosts.
2) Each mobile host preliminary determines the allocation of replicas based on the SAF method.
3) In each set of mobile hosts which are connected to each other, the following procedure is repeated in the order of the breadth first search from the mobile host with the lowest suffix (i) of host identifier (Mi). When there is duplication of a data item (original/replica) between two neighbouring mobile hosts, and if one of them is the original, the host which holds the replica changes it to another replica.

If both of them are replicas, the host whose access frequency value to the data item is lower than the other one changes the replica to another replica. When changing the replica, among data items whose replicas are not allocated at either of the two hosts, a new data item replicated is selected where the access frequency value to this item is the highest among the possible items. This eliminates replica duplication among neighbouring hosts. The above procedure is executed every relocation period. Overhead and traffic is much higher than SAF.

II. Selfish Node Detection And Replica Allocation

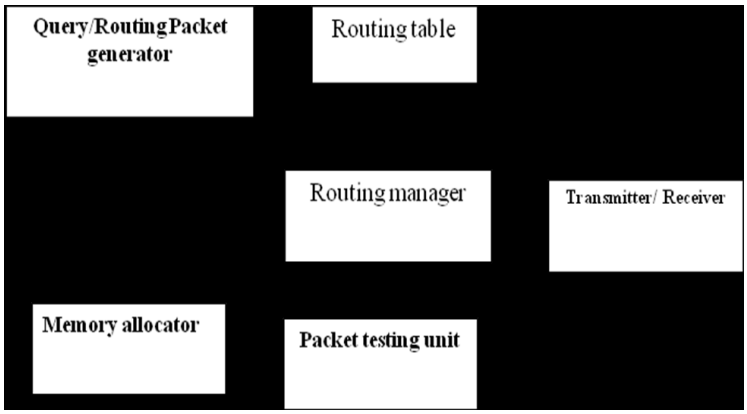

Figure.2. Routing Protocol.

Routing packet generator creates the routing packets and broadcast it to all nodes. Whenever routing packet received in node, then node allocate memory to source node by memory allocator and updating information. And normal transmission will be there.

Whenever source gets doubt then it make query packet by query packet generator and transmitting it. Whenever that particular node (which is mentioned in query packet) receives query packet, node replies back to source node. Source node tests the reply items by packet testing unit. If replied items having any correction then it will fix that node as selfish node. Routing manager controls the whole block.

Path Finding:

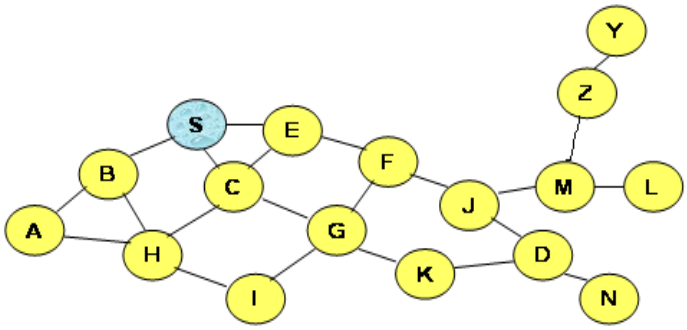

Figure.3. Route or Path Discovery from S to D.

Initially all nodes collecting the data about neighbor nodes. The network monitors having the detailed information of neighbor nodes such as Routing table. It provides the connection information to Route manager.

The AODV Routing protocol and Dynamic Source Routing (DSR) both techniques are used to find paths from source node to destination node for transmitting packets. All possible paths are found by these techniques in network but packet transmission done through only shortest path in a network. Route request (RREQ) and route reply (RREP) are forwarded in between nodes to communicate. Intermediate nodes also used RREQ RREP to communicate with source and destination nodes.

Detecting Selfish Node:

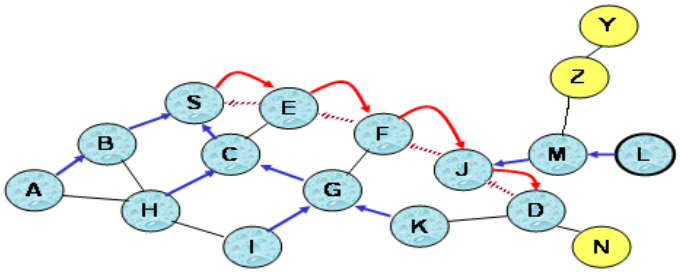

Figure.4. Packet sending from S to D.

Figure 4 shows packet transmission from S node to D node represented with thick red line which route is shortest among all possible routes. If any node behaves like selfish node, then it is not ready to transmit packets to other node. This cause may fail the communication. So in network selfish node detection is needed for efficient communication by applying "degree of selfishness" formula for each node.

We 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. We take a similar approach. 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.

The notion of extended credit risk can be described by the following equation to find integrated degree of selfishness for all connected nodes:

$$xCR_i^k = nCR_i^k * \left(\frac{H_i^k}{max\ H_i}\right)^2, \text{where } 0 \leqslant \alpha \leqslant 1$$

Each node calculates xCR score for each of the nodes to which it is connected. Each node shall estimate the "degree of selfishness" for all of its connected nodes based on the score. First, selfish features may lead to the selfish replica allocation problem were both expected value and expected risk are determined.

Replica Allocation: The SCF-tree based replica allocation techniques are inspired by human friendship management in the real world, where each person makes his/her own friends forming a web and manages friendship by himself/herself. He/she does not have to discuss these with others to maintain the friendship. The decision is solely at his/her discretion. After building the SCF-tree, a node allocates replica at every relocation period.

Algorithm:

1. Initialize :
    1. Initialize node memory(in pkt)
    2. Initialize the update timer
2. Send request for allocate replica
3. If node selfish
    1. Give wrong reply or no response
4. If not
    1. Send correct reply
5. If reply is received by originator
    1. Process the reply
    2. And make the route
6. If timer is triggered
    1. Send the query for checking
7. If node is correspond node then sends the query reply
8. Originator checks the query reply
    1. And forms the SCF tree
    2. And allocates priority and replica according to the tree

III. Implementation

Figure.5 represents how selfish node was found and how it was detected. Figure.5.a contains different nodes in network. In those source and destination nodes are needed to connect with each other through packet sending. Initially the shortest paths are finding in between the source and destination nodes. Those searching signals are represented with green circles in diagram. Figure.5.b shows particular shortest path was founded and represented by red colored signals. Through that shortest path, source node sends packets to the destination node.

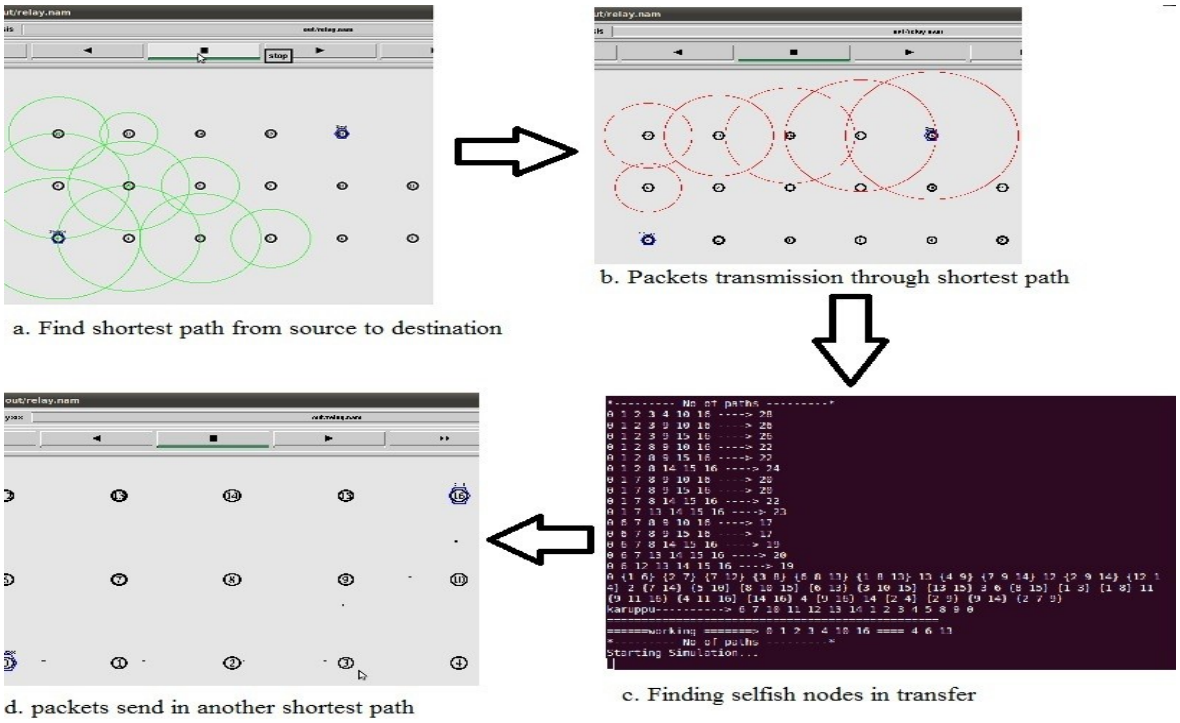

Figure.5. Snapshots of selfish node detection.

If the transmissions are done perfectly then the network graph shows linear transmission lines. If any breaks found in transmission lines, it is the signal of occurring selfish nodes. That selfish node are extracted when path founding among all nodes. Figure.5.c. shows number of paths in network and selfish nodes of network also in detail. Network simulation is performed to found selfish nodes. If any path contains selfish node, through that

path packets are not transmitted. Then the network founds another route or path from source to destination node. That path show in figure.5.d with dotted lines, which is also one of the shortest path.

IV. Related Work

The related work introduces the cooperative caching-based data access methods, including Cache Path, Cache Data, and Hybrid. Differing from all the above-mentioned replica allocation or caching techniques, we consider selfish nodes in a MANET. The work proposes Conquer, a broker-based economic incentive model for mobile peer-to-peer networks. Although the work considers free riders to host data in mobile peer-to-peer networks, it assumes that all peers are trusted and they do not cheat. Some strategies for handling selfish behavior have been proposed In the research field of distributed databases. However, these works cannot be directly applied to a MANET, since they did not consider the constraints such as the bandwidth limitation for the detection of selfish nodes and system failures due to frequent node disconnections of a MANET.

V. Conclusion

In this paper we illustrated the problem of selfish replica allocation in MANETs. Our SCF+ procedure is based on the SCF technique [5]. Our work is motivated by the observation that the existing SCF technique may suffer from poor system performance, because it loses the original distance information between nodes when building the SCF tree. To cope with this limitation, we measure the degree of selfishness by considering both node distance and selfish behaviour in an integrated manner. In addition, we propose a novel node levelling technique that utilizes the memory space of all connected nodes, including selfish nodes as well. In our proposed strategy, nodes prefer to allocate replicas to near, non-selfish nodes, even though faraway nodes are not necessarily selfish. An important consequence of this strategy is that risky and faraway nodes, which are likely to disconnect frequently, are effectively measured. Through a simulation, we confirm the efficacy of our strategy in terms of data accessibility, query delay, and communication cost. We are currently working on the impact of data updates and different moving patterns on our scheme. We also plan to improve the current levelling technique by considering the frequency of disconnections and/or the weighted ratio of total number of items and average of shared memory space.

References

[1]. Jae-Ho Choi, Kyu-Sun Shim, "Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network" SangKeun Lee, and Kun-Lung Wu, Fellow, IEEE.2012.

[2]. L. Anderegg, S. Eidenbenz, "Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents", in: Proceedings of ACM MobiCom, 2003, pp. 245–259.

[3]. J. Broch, D.A. Maltz, D.B. Johnson, Y. Chun Hu, J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols", in: Proceedings of ACM MobiCom, 1998, pp. 85–97.

[4]. G. Cao, L. Yin, C.R. Das, "Cooperative cache-based data access in ad hoc networks", IEEE Computer 37 (2) (2004) 32–39.

[5]. Shailender Gupta, C. K. Nagpal and Charu Singla, "IMPACT OF SELFISH NODE CONCENTRATION IN MANETS" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011.

[6]. Yang Zhang, Student Member, IEEE, Liangzhong Yin, Jing Zhao, and Guohong Cao, Fellow, IEEE, "Balancing the Tradeoffs between Query Delay and Data Availability in MANETs", IEEE Transactions On Parallel And Distributed Systems.

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

[8]. T. Hara and S.K. Madria, "Data Replication for Improving Data Accessibility in Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1515-1532, Nov. 2006.

[9]. L.J. Mester, "What's the Point of Credit Scoring?" Business Rev.pp. 3-16, Sept. 1997.

[10]. Y. Liu and Y. Yang, "Reputation Propagation and Agreement in Mobile Ad-Hoc Networks," Proc. IEEE Wireless Comm. And Networking Conf., pp. 1510-1515,

[11]. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," Proc. ACM MobiCom, pp. 255-265, 2000.

[12]. L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao, "Cooperation in Wireless Ad Hoc Networks," Proc. IEEE INFOCOM, pp. 808-817, 2003.

[13]. Hales, "From Selfish Nodes to Cooperative Networks – Emergent Link-Based Incentives in Peer-to-Peer Networks," Proc. IEEE Int'l Conf. Peer-to-Peer Computing, pp. 151-158, 2004.

[14]. 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.

[15]. L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad Hoc Networks with Selfish Agents," Proc. ACM MobiCom, pp. 245-259, 2003.

[16]. 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.

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

[19]. G. Ding and B. Bhargava, "Peer-to-Peer File-Sharing over Mobile Ad Hoc Networks," Proc. IEEE Ann. Conf. Pervasive