CHALLENGES IN DETECTING SELFISH NODES FOR MANETs - A SURVEY

[1]Sheethal Sunny, [2]Dr.Suriyakala.C.D

[1]Postgraduate Student, Toc H Institute of Science & Technology, Kochi
[2.] Professor, Toc H Institute of Science & Technology, Kochi

ABSTRACT

During the partition of network, mobile nodes in one network may not be able to access data hosted by nodes in other network. Most of the users at different places will assume that mobile nodes may co-operate fully in sharing their memory space. But some of the nodes may decide not to co-operate with other nodes. Such behavior of these selfish nodes may degrade in data accessibility or the performance the network. As the performance of the MANETS is highly dependent on collaboration of all nodes, detection of selfish node is unavoidable task in MANETS in order to improve the performance. This paper highlights a comparative study of different methods exists in survey to detect selfish nodes and proposes benefits of using the credit risk method to detect selfish node and collaborative watchdog technique to reduce the time of detection of selfish nodes, which also take care of avoiding the false alarm of detecting the selfish nodes. A performance study may be done later with MANET's different mobility pattern using suitable metrics like data accessibility, communication cost etc. with and without handling false alarm in selfish replica allocation.

Key words: MANETS, Selfish nodes, credit risk, watch dog

INTRODUCTION

In communication networks, MANETs have their design flaws and security concerns. One such issue is the existence of one or more selfish nodes within the network. Continuous change in topology of MANETs may result in network partition. When network partition occur mobile nodes in one network may not able to access data hosted by nodes in other network. Some of the nodes may decide not to co-operate with other nodes. Selfish nodes are the nodes within the network that wish to conserve its power, which results into denial of packets from other nodes, at the same time nodes attempt to send packets of their own to its neighbors . Selfish nodes can cause major negative impact in a MANET, by dropping packets to the point where no node can send any message, which results the entire network offline. The behavior of this selfish node may lead to decrease in data accessibility or the performance the network.

The selfish nodes, specifically the nodes continuously drop packets, in Mobile Ad Hoc Networks, may lead to disastrous effects within the MANET. If the system is a closed network, such as tracking vehicles within a particular area of land in military operations; the existence of selfish nodes could lead in losing a battle instead of winning. In open systems, usually selfishness only results in loss of data during transmission. If the network is designed correctly, the data can be retransmitted until a successful transmission. Although the data is eventually transmitted successfully, it will increase bandwidth utilization and extra power usage of each node within the path of the transmission.

Many studies were conducted on the Mobile Ad Hoc Networks and particularly on selfish node detection. In this paper we are describing the existing methods, comparison, and suggested solutions. In presentation Introduction section is followed by challenges involved in MANETS due to selfish nodes. Challenges in eliminating selfish nodes with the backup of related work in survey is described in the following section.

CHALLENGES IN ELIMINATING SELFISH NODES

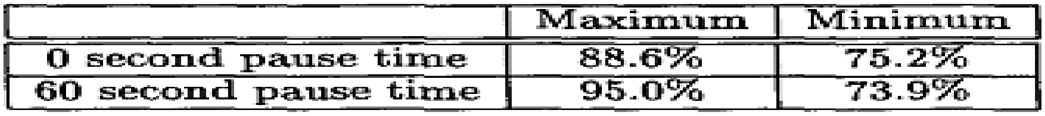
If we study the characteristics of selfish nodes, it may not participate in routing process or it may modify the Route Request and Reply packets by changing TTL value to smallest possible value. A selfish node may not respond to hello messages, hence other nodes may not be able to detect its presence when they need it and may delay the RREQ packet up to the maximum upper limit time. It will certainly avoid itself from routing paths. Also selfish nodes may participate in routing messages but may not relay data packets. The challenges involved here is

- *Tolerance:* If the threshold is too low in which to tolerate selfishness, then the error rate will be high due to an increased amount of discarded packets. If the threshold is too high, then there will be low error rate, but fewer nodes will be able to participate in routing because they will be seen as selfish.
- *Bandwidth*: Since bandwidth is limited within the MANET, retransmission must be kept at a minimal. Each node is responsible for sending data using the best possible path in order to reduce retransmission. Therefore, each node must be able to recognize when it has a selfish node as a neighbor and find an alternate path to send the data if one is available.
- *Power Consumption*: Each node is responsible for finding the best path to send the packet, but the node can't use too much power to determine the best path. Nodes are limited in amount of power available to them, therefore the more power used in finding a path results in a shorter life span for the node. If all nodes use a large amount of power trying to find the best path to route a packet, the network will eventually become unusable due to a large amount of isolated nodes.
- *Problem Formulation:* The algorithm proposed for detection and removal based upon the credit risk based algorithm. The main objective is to identify and isolate selfish nodes from the network. Through successful isolation, the MANET performance will be increased and will become more reliable.

Selfish node may not share its own memory space to store replica for the benefit of other nodes. Such a problem refers as the selfish replica allocation [1]. Through credit risk method a node can measure the degree of selfishness of another node, to which it is connected by one or multiple hops in a MANET. The leader is elected to avoid false alarm while identifying partial selfish node along with the novel replica allocation techniques. They are based on the concept of a self-centered friendship tree (SCF-tree) and its variation to achieve high data accessibility with low communication costs.

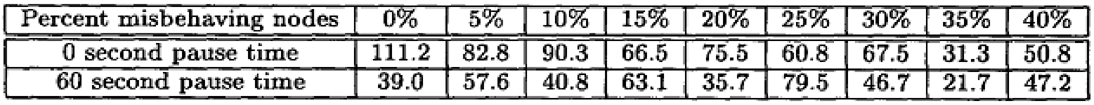
RELATED WORK/SURVEY

In order to mitigate bad effects of misbehaving MNs and to improve throughput in ad hoc network in presence of nodes that agree to forward packets but failed [S.Marti et.al,; 2000**]** proposed two techniques: watchdog and pathrater. Watch dog that identifies misbehaving nodes and pathrater that helps routing protocols avoid these nodes. Watchdog and pathrater are implemented at each node, to detect and mitigate, respectively, routing misbehaviors in MANETs. This paper based on reputation based algorithm, each node is responsible for either keeping track of other nodes, or obtaining the reputation from a centralized node on the network. This paper mainly focused selfish node detection based on packet forwarding and routing. However, our work mainly focused on the problem of selfish replica allocation [1]. Here authors evaluate the performance through throughput, overhead and Effects of watchdog false positives on network throughput. The two techniques increase throughput by 17% in a net- work with moderate mobility, while increasing the ratio of overhead transmissions to data transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the percentage of overhead transmissions from 12% to 24%.



	Maximum	Minimum
0 second pause time	88.6%	75.2%
60 second pause time	95.0%	73.9%

Table 1: Maximum and minimum network through- put obtained by any simulation at 40% misbehaving nodes with all features enabled. [S.Marti et.al,; 2000**]**



Percent misbehaving nodes	0%	5%	10%	15%	20%	25%	30%	35%	40%
0 second pause time	111.2	82.8	90.3	66.5	75.5	60.8	67.5	31.3	50.8
60 second pause time	39.0	57.6	40.8	63.1	35.7	79.5	46.7	21.7	47.2

Table 2: Comparison of the number of false positives between the 0 second and 60 second pause time simulations. Average taken from the simulations with all features enabled. [S.Marti et.al,2000**]**

T.Hara,2001 in his paper, author have discussed replica allocation in ad hoc networks to improve data accessibility. Authors proposed three replica allocation methods which take into account the access frequencies to data items and the network topology. In the SAF (Static Access Frequency) method, a mobile host allocates replicas with high access frequencies. In the DAFN method (Dynamic Access Frequency and Neighborhood), replicas are preliminary allocated based on the SAF method, and then the replica duplication is eliminated among neighboring mobile hosts. In the DCG (Dynamic Connectivity based Grouping) method, stable groups of mobile hosts are created, and replicas are shared in each group. Performance analysis is based on effects of the size of memory space, effects of the radio communication range, effects of the scattering access characteristics and effects of the relocation period. T.Hara [13] proposed data replication schemes in ad hoc networks. These schemes are based on the intuition that to improve data accessibility, replicating the same data near neighboring nodes should be avoided. However, this intuition may not be valid when the link failure probability is taken into consideration. Extensive performance evaluations demonstrate that the proposed schemes can provide high data accessibility. Proposed schemes are 1) Greedy Schemes 2) One-To-One Optimization (OTOO)

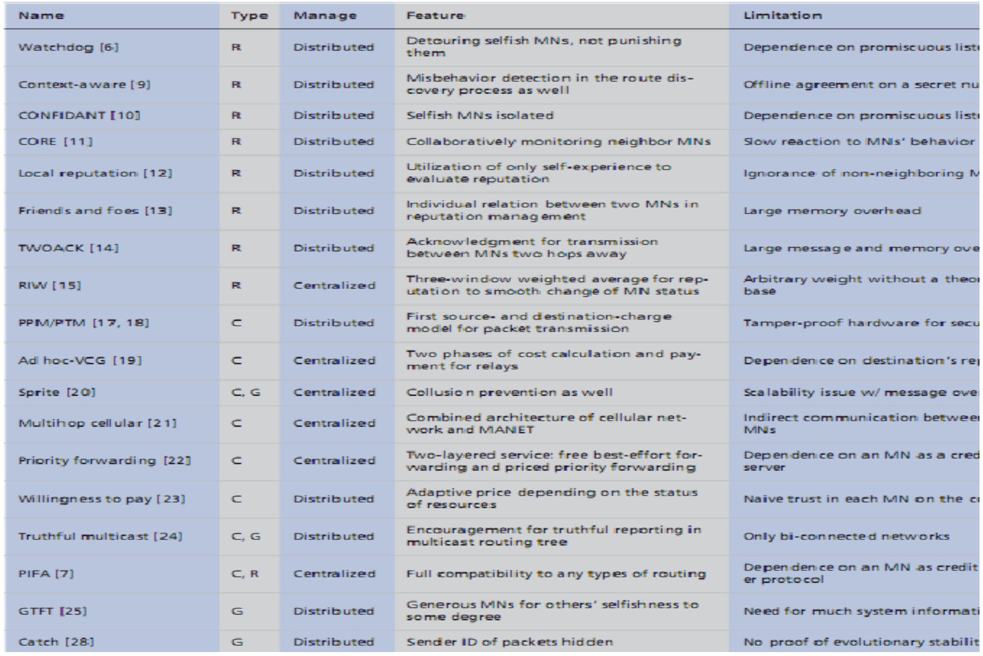
Scheme 3) Reliable Neighbor (RN) scheme. These schemes achieve a balance between data accessibility and query delay. Simulation results show that balance between these two metrics and provide satisfying system performance. In his extension work, the simulation results showed that the three extended methods work well in an environment where each data item is randomly updated and mobile users behave based on their schedules. The simulation results also showed that the three extended methods give poor performance when some data items have very low write frequencies and not high access frequencies. This drawback is due to that RWR is defined as the ratio of read frequencies to write frequencies. To address this problem by setting a threshold (lower bound) of access frequency to prevent mobile hosts from replicating data items with low access frequencies. But our work mainly address this problem by setting a threshold of access frequency to prevent mobile hosts from replicating data items with low access frequency through credit risk method. T.Hara et.al; 2006 suggests that data replication drastically improves data availability. However, since mobile hosts 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. In this paper consistency maintenance based on local conditions such as location and time need to be investigated and also attempts to classify different consistency levels according to requirements from applications and provides protocols to realize them. In this paper four different primitive consistency levels are mentioned. Global Consistency, Local Consistency, Time-Based Consistency, and Peer-Based Consistency and one combined consistency level. The simulation results showed that the three extended methods work well in an environment where each data item is randomly updated and mobile users behave based on their schedules. Since there is a trade-off relationship between the improvement of data accessibility and the reduction of traffic over network.

K.Paul and D.Weshoff [K.Paul et.al.; 2002] showed that security threats in a DSR based co-operative ad-hoc network and presented a context aware inference scheme for source node to blame and rate an accused node conclusively. This work, in particular, detects attacks on Dynamic Source Routing (DSR) protocol for ad-hoc routing by using shared secret between source and destination only.

K.Balakrishnan,J.Deng and P.K Varshney [K.Balakrishnan et.al.; 2005] in their work described technical literature to mitigate routing misbehavior. For performing network function consumes energy and other resources. Therefore, some network nodes may decide against cooperating with others. Providing these selfish nodes, also termed misbehaving nodes. To mitigate routing misbehavior, two network-layer acknowledgment-based schemes was proposed, termed the TWOACK and the S-TWOACK schemes, which can be simply added-on to any source routing protocol. The TWOACK scheme detects such misbehaving nodes, and then seeks to alleviate the problem by notifying the routing protocol to avoid them in future routes. It is a reputation based approach; nodes detect and then declare another node to be misbehaving. The S-TWOACK (Selective-TWOACK) scheme is a derivative of the basic TWOACK scheme, aimed at reducing the routing overhead caused by excessive number of TWOACK packets and achieves the performance improvement without any routing overhead but with some expected increase of false alarms. These schemes detect selfish node based preserved their own resources and also focused on packet forwarding. Through simulations authors have shown that, in a network where up to 40% of the nodes are misbehaving, the TWOACK scheme improves the end to-end packet delivery ratio from around 70% to almost 90% while increasing the overhead from 4% to 7%.

N. Laoutaris, O. Telelis, V. Zissimopoulos, and I. Stavrakakis[N. Laoutaris et.al.; 2006] suggests that individual nodes act selfishly, i.e., cater to the optimization of their individual local utilities. The main contribution of this paper is the derivation of equilibrium object placement. S.Y.Wu and Y.-T.Chang [S.Y. Wu et.al.; 2006] suggests dynamic replication schemes, try to overcome the problem by continuously maintaining statistics about access patterns and system workload so as to dynamically recalculate access cost and reconfigure the replication structure to adjust to the changes in access patterns. This is particularly desirable for mobile computing environments.

Y. Yoo and D.P. Agrawal[Y.Yoo et.al.; 2006] suggests that routing protocols for a mobile ad hoc network have assumed that all mobile nodes voluntarily participate in forwarding others packets. This was a reasonable, because all MNs in a MANET belonged to a single authority. 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 and reduce the performance degradation in MANETs, many studies have explored the use of both the carrot and the stick approaches by having reputation-based, credit-payment, and game theory schemes. In reputation schemes, each MN observes others behavior and uses the information in the routing process. Credit-payment schemes give credits to MNs as a reward for packet forwarding and all MNs need the credit in order to send their own packets. And in game theory based schemes model the forwarding process as a game whereby all rational MNs gradually determine their own optimal strategies. This paper summarizes three schemes and identifies their relative advantages. Table2 summarizes important features of selfishness prevention schemes introduced in this article.



Name	Type	Manage	Feature	Limitation
Watchdog [6]	R	Distributed	Detouring selfish MNs, not punishing them	Dependence on promiscuous liste
Context-aware [9]	R	Distributed	Misbehavior detection in the route discovery process as well	Offline agreement on a secret nu
CONFIDANT [10]	R	Distributed	Selfish MNs isolated	Dependence on promiscuous liste
CORE [11]	R	Distributed	Collaboratively monitoring neighbor MNs	Slow reaction to MNs' behavior
Local reputation [12]	R	Distributed	Utilization of only self-experience to evaluate reputation	Ignorance of non-neighboring M
Friends and foes [13]	R	Distributed	Individual relation between two MNs in reputation management	Large memory overhead
TWOACK [14]	R	Distributed	Acknowledgment for transmission between MNs two hops away	Large message and memory ove
RIW [15]	R	Centralized	Three-window weighted average for reputation to smooth change of MN status	Arbitrary weight without a theor base
PPM/PTM [17, 18]	C	Distributed	First source- and destination-charge model for packet transmission	Tamper-proof hardware for secu
Ad hoc-VCG [19]	C	Centralized	Two phases of cost calculation and payment for relays	Dependence on destination's rep
Sprite [20]	C, G	Centralized	Collusion prevention as well	Scalability issue w/ message ove
Multihop cellular [21]	C	Centralized	Combined architecture of cellular network and MANET	Indirect communication betweer MNs
Priority forwarding [22]	C	Centralized	Two-layered service: free best-effort forwarding and priced priority forwarding	Dependence on an MN as a cred server
Willingness to pay [23]	C	Distributed	Adaptive price depending on the status of resources	Naive trust in each MN on the c
Truthful multicast [24]	C, G	Distributed	Encouragement for truthful reporting in multicast routing tree	Only bi-connected networks
PIFA [7]	C, R	Centralized	Full compatibility to any types of routing	Dependence on an MN as credit er protocol
GTFT [25]	G	Distributed	Generous MNs for others' selfishness to some degree	Need for much system informati
Catch [28]	G	Distributed	Sender ID of packets hidden	No proof of evolutionary stabilit

Table 2. Selfishness prevention schemes [Y.Yoo et.al.; 2006]

N. Laoutaris, G. Smaragdakis, A. Bestavros, I. Matta, I.Stavrakakis[N. Laoutariset.al.; 2007] discussed that distributed on-demand caching enables loosely coupled groups of nodes to share their (storage) resources to achieve higher efficiencies and scalability. They have outlined an efficient emulation-based approach that allows individual nodes to decide autonomously whether they should stick to or secede from a caching group, based on whether or not their participation is beneficial to their performance compared to a selfish greedy scheme.

S.Bhuvaneshwari, Prof.M.Suguna[S.Bhuvaneshwari et.;al 2013] described that 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. As part of this 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. This in turn to increases the data accessibility and reduces average query delay. Author's shows through simulation result on average about 56 to 50 percent of the overall selfishness alarm are reduced by node selfishness.

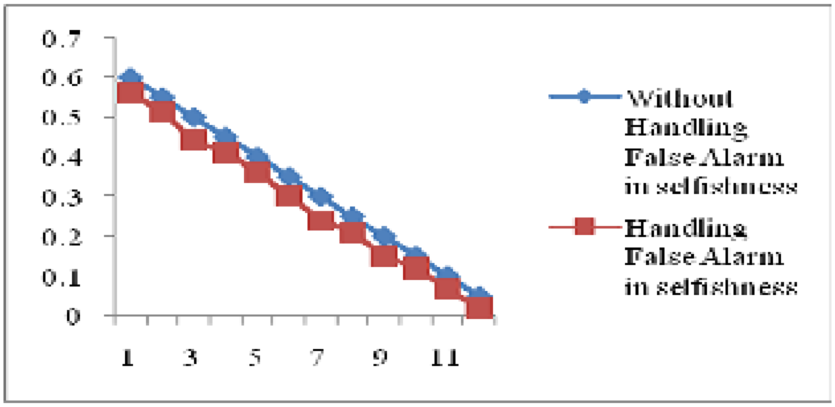
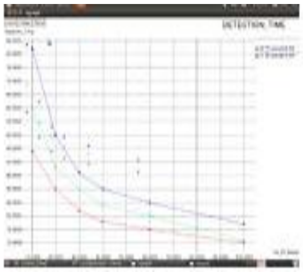


Fig 1.Comparison between with and without handling false alarm in selfish replica allocation. [S.Bhuvaneshwari et.;al 2013]

S. J. K. Jagadeesh Kumar, R. Saraswathi & R. Raja[S. J. K. Jagadeesh Kumar et.al.;2013] describes that in mobile ad hoc networks, nodes can move freely and link/node failures occur frequently. This leads to frequent network partitions, and it degrade the performance of data access in ad hoc networks. When the network partition occurs, mobile nodes in one network are not able to access data hosted by nodes in other networks. In mobile ad hoc network, 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 work, the impact of selfish nodes in a mobile ad hoc network from the perspective of replica allocation is examined.

They term this selfish replica allocation [1]. A combined credit risk method & collaborative watchdog is proposed to detect the selfish node and also apply the SCF tree based replica allocation method to handle the selfish replica allocation appropriately. The proposed method improves the data accessibility, reduces communication cost and average query delay and also to reduce the detection time and to improve the accuracy of watchdogs in the collaborative method. Extensive simulation shows [Fig.2-4] that the proposed strategies outperform existing representative cooperative replica allocation techniques in terms of data accessibility, communication cost, and query delay [S. J. K. Jagadeesh Kumar et.al.;2013]



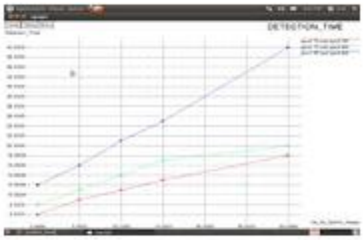


Fig 2.Evaluation depending on node

Fig 3. Evaluation based on selfish nodes

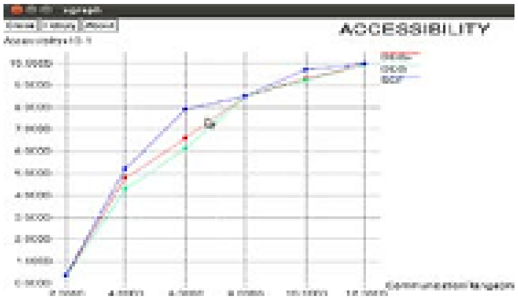


Fig 4 Accessibility [S. J. K. Jagadeesh Kumar et.al.;2013]

PROPOSED STRATEGY

From survey MANET's performance that degrades multi-hop communication requires collaboration among nodes which forward packets [9] one another. Most studies of ad hoc networks assume that nodes can be programmed to always perform this forwarding functionality. In commercial deployment of MANETs, however, some nodes may refuse to forward packets in order to conserve their limited resources (for example, energy), resulting in traffic disruption [8]. Nodes exhibiting such behavior are termed selfish. Selfishness is usually passive behavior. Additionally, malicious nodes may intentionally, and without concern about their own resources, attempt to disrupt network operations by mounting denial-of-service attacks or by actively degrading the network performance. Selfish and malicious behaviors are usually distinguished based on the node's intent. Network disruption is a side effect of the behavior of a selfish node, while disrupting the network is the intent of malicious nodes.

Network partitions can occur frequently, since nodes move freely in a MANET, causing some data to be often inaccessible to some of the nodes. Hence, data accessibility is often an important performance metric in a MANETs [5]. Data are usually replicated at nodes, other than the original owners, to increase data accessibility to cope with frequent network partitions. Data replication can simultaneously improve data accessibility and reduce query delay in MANET; the nodes have sufficient memory space to hold both all the replicas and the original data. A node may act selfishly by using its limited resource only for its own benefit, since each node in a MANET has resource constraints, such as battery and storage limitations. A node 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.

To mitigate this problem, survey suggest different approach like watch dog, path rather method[9], TWO ACK scheme and S-TWO ACK schemes[3], reputation scheme ,game theory based scheme and credit payment based scheme[15].

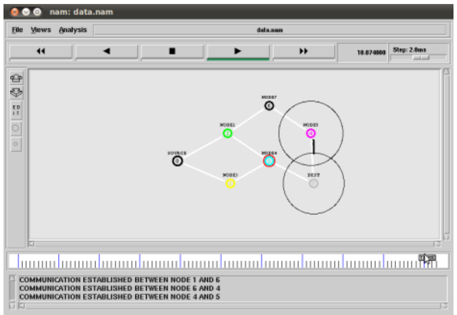
PROPOSED SOLUTION

By analyzing the above mention methods with respect to achieved results in survey, we have proposed a selfish node detection method and novel replica allocation techniques to handle the selfish replica allocation appropriately. To solve such problems we examine the impact of selfish nodes in a mobile ad hoc network from the perspective of replica allocation [1]. 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. For that every node in MANET calculates credit risk information of other connected nodes to measure the degree of selfishness. The proposed 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. We applied the notion of credit risk from economics to detect selfish nodes. Every node in a MANET calculates credit risk information on other connected nodes individually to measure the degree of selfishness. Since traditional replica allocation techniques failed to consider selfish nodes, we also proposed novel replica allocation techniques. And finally we propose a set of replica allocation techniques that use the self-centered friendship tree to reduce communication cost, while achieving good data accessibility. The simulations can be carried out using an object oriented network simulating tool called NS-2.

Develop a selfish node detection algorithm that considers partial selfishness and novel replica allocation techniques to properly cope with selfish replica allocation. For that every node in MANET calculates credit risk information of other connected nodes to measure the degree of selfishness. Every node in a MANET calculates credit risk information on other connected nodes individually to measure the degree of selfishness. Since traditional replica allocation techniques failed to consider selfish nodes, we also proposed novel replica allocation techniques like using the concept of SCF tree. The main challenges involved are recognizing the selfish replica allocation problem, detecting the fully or the partially selfish nodes effectively (credit risk method may be effective), allocating replica effectively and verify the proposed strategy. 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.

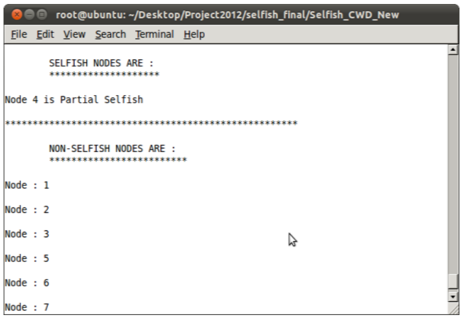
Detection of selfish node and reducing the time of detection is an unavoidable mechanism to be in cooperated in MANETs to improve performance. A number of solutions has been introduced to mitigate the unreliability problem like reputation based scheme, game theory based scheme etc. So we are proposing credit risk method [1] a node can measure the degree of selfishness of another node. From the simulations it is observed that the mobile ad-hoc networks will perform with AOMDV protocol and detecting the degree of selfishness of each node in networks through credit risk method. Through that analysis we can conclude that whether the node is partial selfish or non-selfish nodes.

As a future work, this method also indirectly support leader is elected to avoid false alarm [8] while identifying partial selfish node along with the novel replica allocation techniques. The performance of MANETs highly depended on watch dog [10] technique to reduce the time of detection of selfish nodes. They are based on the concept of a self-centered friendship tree (SCF-tree) and its variation to achieve high data accessibility with low communication cost in the presence of selfish nodes. Network simulator (NS-2) is used for the comparative study of MANETs different mobility pattern using suitable metrics like data accessibility, communication cost etc. with and without handling false alarm in selfish replica allocation. Few simulation results attached in Fig.5 & Fig.6



```
COMMUNICATION ESTABLISHED BETWEEN NODE 1 AND 6
COMMUNICATION ESTABLISHED BETWEEN NODE 6 AND 4
COMMUNICATION ESTABLISHED BETWEEN NODE 4 AND 5
```

Fig.5 selfish node detection


root@ubuntu: ~/Desktop/Project2012/selfish_final/Selfish_CWD_New
File Edit View Search Terminal Help

```
        SELFISH NODES ARE :
        ********************

Node 4 is Partial Selfish

*****************************************************

        NON-SELFISH NODES ARE :
        *************************

Node : 1

Node : 2

Node : 3

Node : 5

Node : 6

Node : 7
```

Fig.6 Detecting selfish and non selfish nodes in MANET through credit risk method

CONCLUSION

Detection of selfish node and reducing the time of detection is an unavoidable mechanism to be in cooperated in MANETs to improve performance. A number of solutions has been introduced to mitigate the unreliability problem like reputation based scheme, game theory based scheme etc. We are proposing credit risk method [1], which can measure the degree of selfishness of another node. This method also indirectly support leader is elected to avoid false alarm [8] while identifying partial selfish node along with the novel replica allocation techniques. The performance of MANETs highly depended on watch dog [10] technique to reduce the time of detection of selfish nodes. They are based on the concept of a self-centered friendship tree (SCF-tree) and its variation to achieve high data accessibility with low communication cost in the presence of selfish nodes. Network simulator (NS-2) is used for the comparative study of MANETs different mobility pattern using suitable metrics like data accessibility, communication cost etc. with and without handling false alarm in selfish replica allocation.

REFERENCE

[1] Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu"Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network" IEEE Transactions on mobile computing, vol. 11, no. 2,February 2012.

[2]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.

[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]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.

[5]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.

[6]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.

[7]N. Laoutaris, G. Smaragdakis, A. Bestavros, I. Matta, and I. Stavrakakis, "Distributed Selfish Caching," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 10, pp. 1361-1376, Oct. 2007.

[8]S.Bhuvaneshwari, Prof.M.Suguna,"Identifying and handling of false alarm in selfish replica allocation ,"Vol 2 Issue 4 April 2013 ISSN 2278-733X.

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

[10]S. J. K. Jagadeesh Kumar, R. Saraswathi & R. Raja," Improving the Performance of Mobile Ad Hoc Network using a Combined Credit Risk and Collaborative Watchdog Method," Global Journals Inc. (US)., Volume 13 Issue 6 Version 1.0 Year 2013.

[11]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.

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

[13]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.

[14]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.

[15]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, Dec. 2006.