ISSN (Print) : 2320 – 3765
ISSN (Online):2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

Handling Selfishness in MANETs – A Survey

Gayathry S S[1], R N Gaur[2]

PG Student [Wireless Technology], Dept. of ECE, Toc H Institute of Science and Technology, Kochi, India[1]

Professor, Dept. of ECE, Toc H Institute of Science and Technology, Kochi, India[2]

ABSTRACT: A mobile ad hoc network (MANET) is an infrastructure-less network with self-configuring capability of mobile nodes connected wirelessly. 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 along with an increase in query delay. In the past, many people have worked on this selfish node problem, and proposed several methods to detect these selfish nodes. This paper provides a survey on different methods used to detect selfish nodes in MANETs. It also provides an overview on data replication in a mobile adhoc network, andcertain methods to handle selfishness occurring in this replica allocation process. It is being proposed to use a combined credit risk and collaborative watchdog method to improve the network performance by detecting such selfish nodes within a reduced time period.

KEYWORDS: MANETs, Selfish nodes, Replica allocation, Credit risk method, Watchdog method, Combined credit risk and watchdog method

I. INTRODUCTION

Mobile AdHoc networks (MANETs) or simply adhoc networks, comprise of nodes that move freely and dynamically self-organize into arbitrary and temporary network topology without any fixed infrastructure support. In a mobile ad hoc network, the mobility and resource constraints of mobile nodes may lead to network partitioning or performance degradation.The mobile nodes that are in radio range of each other can directly communicate, whereas others need the help of intermediate nodes to route their packets.

In MANET, each node acts as a router [2]. These nodes in the network are responsible for discovering a path to a particular node and forward the data to that node. Since the nodes in the network are capable of moving, the infrastructure of network will change rapidly.Dynamic topology of MANETs may result innetwork partition. When network partition occurs,mobile nodes in one network are not able toaccess data hosted by nodes in other network. Each node in the MANET will do forward the data to other node but some nodes will not forward the data packet to other nodes, and so they are called as selfish nodes. This selfish behavior of the network nodesmay lead to decrease in data accessibility or the performance the network. As the performance of MANETs highly depends on collaboration of all nodes, detection of selfish node is an essential task.

The existence of selfish nodes in a network results in a considerable decrease in the data accessibility, but the delay time will get increased. It is very important to prevent the deterioration of data accessibility at the point of network partition.So, there is a need to detect and eliminate these selfish nodes.

The organization of this paper is as follows. The following section II describes the behavioral modes of nodes in MANETs. Section III gives out different methods to detect selfish nodes in these networks. The next section describes data replication process and the methods to detect selfish nodes in replica allocation. The paper ends with an outlook on a fast and efficient method to handle selfishness problem in MANETs.

II. RELATED WORK

A. NODE BEHAVIOURALMODEL

MANETs are mobile wireless networks that are rapidly changing, unpredictable and have no fixed base stations or infrastructure design. There are two types of MANETs: closed and open MANETs. In a closed MANETs, all nodes

ISSN (Print) : 2320 – 3765
ISSN (Online):2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

participate and organize the network. In an open MANET, different mobile nodes with different goals hesitate to share their resources. In this case, selfish nodes are originated.These nodes will not be willing to forward packets and share their memory space for the benefit of other nodes [2]. The nodes in a mobile adhoc network can be classified into three types, such as:

- Non-selfish nodes: These nodes allocate their memory space completely for the purpose of other nodes.
- Fully selfish nodes: They never utilize their memory space for other nodes to store data.
- Partially selfish nodes: These nodes may act as both selfish and non-selfish nodes. Since they have a selfish behavior, they have to be considered as selfish; rather than non-selfish. The detection of these partially selfish nodes is complex.

The major characteristics of selfish nodes include the following:

- Do not participate in routing process
- Do not reply or send hello messages
- Intentionally delay the RREQ packet
- Dropping of data packet

B. SELFISH NODE DETECTION METHODS

A. 2ACK METHOD

The acknowledgement-based 2ACK scheme is suggested to mitigate the adverse effects of misbehaving nodes. The basic idea of TWOACK scheme is that, when a node forwards a data packet successfully over the next hop, the next-hop-link's destination node will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully. The 2ACK scheme is a network-layer technique to detectmisbehaving links and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route [12].

B. S-2ACK METHOD

Another acknowledgement-based scheme, termed as S-TWOACK is a derivative of the basic TWOACK scheme, aimed at reducing the routing overhead and achieves the performance improvement along with the problem of false-alarms due to genuine TWOACK packets lost. The Selective TWOACK (S-TWOACK) scheme is different from 2ACK. Mainly, each TWOACK packet in the S-TWOACK scheme acknowledges the receipt of a number of data packets, but a 2ACK packet in the 2ACK scheme only acknowledges one data packet. With such a change, the 2ACK scheme has easier control over the trade-off between the performance of the network and the cost as compared to the S-TWOACK scheme[12].

C. SECURE INTENSIVE PROTOCOL(SIP)

Secure Intensive Protocol is a credit-based method that uses the credit as the incentive to stimulatepacket forwarding. Here each mobile node has a security module and they deal with the security related functions. The credits of the node increases and decreases depending on the forwarding behaviorof the node. Whenever a node is initiating or forwarding a packet, first node will pass it to SIPmodule for processing. SIP is session based and consists of four phases, 1) Session Initiation 2) Session Key Establishment 3) Packet Forwarding And 4) Rewarding Phase. The advantages of the scheme are SIP is routing independent; it is session based rather than packet based; unauthorized access is not allowed. The disadvantage of SIP is that it implemented on hardware module so each node shouldpossess a hardware module[13].

C. CONFIDANT METHOD

The reputation-based CONFIDANT(Cooperation of Nodes, Fairness in Dynamic Ad Hoc Networks) method will detect the misbehavior nodes by monitoring the behavior of neighbor nodes and they will pass this information to all other nodes. The misbehavior node will not be punished as a result.Monitoring System, Reputation System, Trust Manager and Path Manager are the four modules involved in this CONFIDANT protocol, each having a specific task to perform. CONFIDANT protocol is an expansion of DSR protocol. Increase in throughput andlow overhead of extra message are major advantages of this protocol but it has a disadvantage is that, the node authentication is not checked [15].

D. CORE METHOD

The reputation-based CORE (Collaborative Reputation) Mechanism to detect the selfish nodes, improves the coordination among nodes. For this purpose, it makes use of reputation mechanism and collaborative monitoring. The basic components used in the CORE mechanism are 1) reputation table and 2) watchdog mechanism. The CORE mechanism will prevent the

ISSN (Print) : 2320 – 3765
ISSN (Online):2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

DOS attacks, it is impossible for a node to decrease another node's reputation maliciously because there is no negative rating spread between nodes. The CORE suffers from spoofing attacks, it cannot prevent colluding nodes from distributed negative reputation [15].

E. AD-HOC VCG

Ad hoc-VCG,named afterVickrey, Clarke, and Groves is a Truthful and Cost-Efficient reactive routing protocol for mobile ad hoc networks that is robust against individual selfishness of the communication nodes and is cost-efficient. This protocol first computes the most cost-efficient path and then routes the data packets from source to destination along this path. Ad hoc-VCG consists of the following two phases such as:-1) Route discovery 2) Data transmission. Route discovery includes payment computation whereas data transmission includes the act of making payments to the intermediate nodes. Ad hoc- VCG utilizes shortest path information to the destination node as in the case of DSR protocol. It is identical to credit-payment technique in which each node gives a credit to others, as a reward for data forwarding.This credit acquired is then used to send data to the others [4].

D. DATA REPLICATION IN MANETS

In mobile ad hoc networks (MANETs), since mobile nodes move freely, networkpartition may occur, where nodes in one partition cannot access data held by nodes in otherpartitions. Thus, data availability (i.e., the number of successful data accesses over the totalnumber of data accesses) in MANETs is lower than that in conventional wired networks. Datareplication has been widely used to improve data availability in distributed systems, and we willapply this technique to MANETs. By replicating data at mobile nodes which are not the ownersof the original data, data availability can be improved because there are multiple replicas in thenetwork and the probability of finding one copy of the data is higher. Also, data replication canreduce the query delay since mobile nodes can obtain the data from some nearby replicas.However, most mobile nodes only have limited storage space, bandwidth, and power, and henceit is impossible for one node to collect and hold all the data considering these constraints [7].

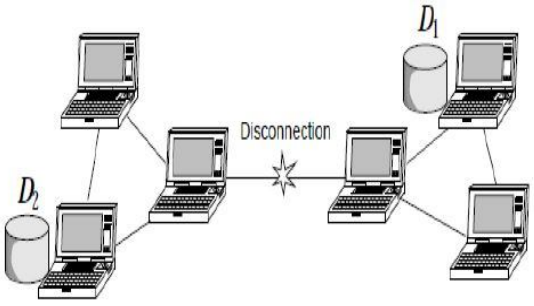


Fig 1: Network partitioning [7]

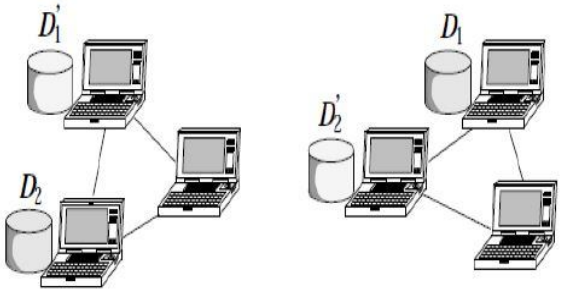


Fig 2: Effective data replication [7]

In Fig 1, if the radio link between two mobile hosts at the central part isdisconnected, the mobile hosts in the left-hand side and those in the right-hand side cannotaccess data items D1 and D2 respectively. In ad hoc networks, it is a very important issue toprevent deterioration of data accessibility at the point of network division. A possible solution isby replicating data items at mobile hosts which are not the owners of the original data. InFig 1, if the replicas of data items D1 and D2 are

ISSN (Print) : 2320 – 3765
ISSN (Online):2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

allocated at one of the mobile hosts in theopposite networks as shown in Fig 2, every mobile host can access both data items after thenetwork division.

E. REPLICA ALLOCATION METHODS

This section describes certain methods to allocate data replicas; in networks influenced by selfish nodes.

A. SAF METHOD

In SAF (Static Access Frequency) method, the nodes allocate replica of data items according to the access frequencies of that data items. Thus, this method allocates replicas with low overhead and low traffic. Mobile nodes with the same access frequencies to data items allocate the same replicas.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.

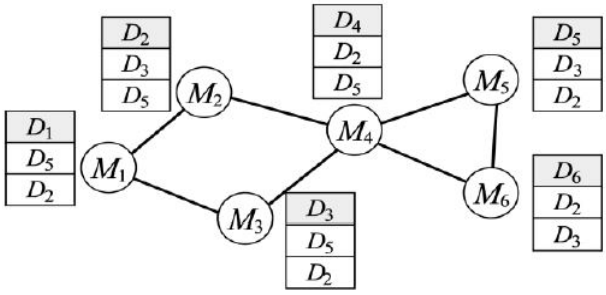


Fig 3: SAF method of replica allocation [6]

Fig 3 shows SAF method of replica allocation. In this, M1, M2 etc. are mobile nodes and thestraight lines between them denotes a wireless link. D1, D2 etc. are data items. The gray rectangles indicate original data, whereas the white indicates replicas allocated.

B. DAFN METHOD

The DAFN *(Dynamic Access Frequency and Neighborhood)*method was introduced in order to overcome the problem of replica duplication in the SAF method.In DAFN method, each mobile host first broadcasts both its id and access frequency at relocation period. The replicas will be allocatedin the same way as that of SAF method.Then, if there is replica duplication of a data item between two neighboring mobile hosts, the mobile host with the lower access frequency to the data item changes the replica to another replica.The node having high access frequency will store its replica,if two mobile nodes have the same data item.At each relocation period, the mobile nodes exchange information about replicas allocated in the memory space. So the overhead and the traffic are high compared with the SAF method.

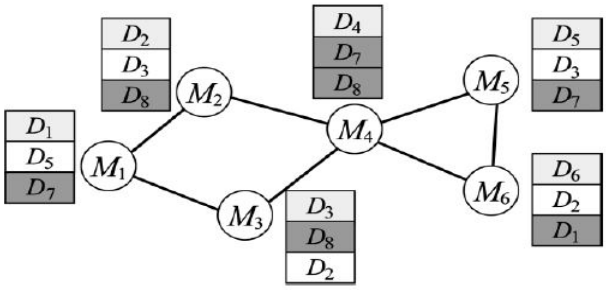


Fig 4: DAFN method of replica allocation [6]

Fig 4 shows DAFN method in which replica duplication of the data item, D8 takes place between ;M2 and M4,also duplication of D8 between M3 and M4, and also D7 between ;M4 and ;M5. Moreover, if the network topology changes during the execution of this method, the replica relocation cannot be done at mobile hosts over disconnected links.

C. DCG METHOD

Differing from the DAFN method that shares replicas among neighboring nodes, the DCG*(Dynamic Connectivity and Grouping)*method shares replica of data items in several groups of mobile nodes.The DCG method creates groups of mobile nodes that are bi-connected in an ad hoc network. The group is not being divided even if one mobile node is disconnected from the network. This DCG methodprovides high data accessibility and stability over nodes since many

ISSN (Print) : 2320 – 3765
ISSN (Online):2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

kinds of replicas can be shared. The network topologychanges rapidly during the execution of this method since it consists of three steps, such as 1) broadcasting host identifiers, 2) determining the replica allocation, and 3) notifying it to all hosts in the group, that makes this method to take the longest time among the three methods to relocate replicas. Here, the replica relocation cannot be done over disconnected links. Moreover, both the overhead and traffic are higher than the other two methods because,during each relocation period, mobile hosts exchange information and relocate replicas in a wide range.

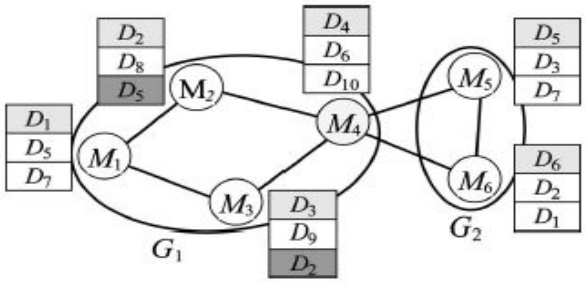
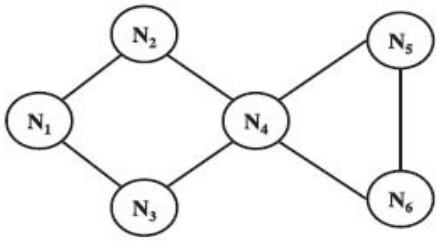


Fig 5: DCG method of replica allocation [6]

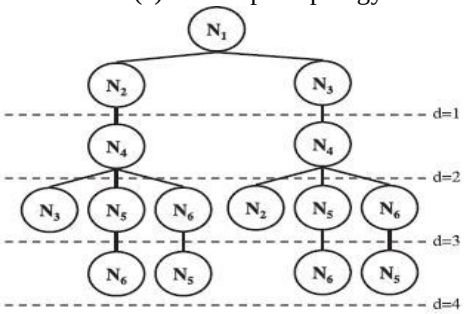
Fig 5 shows DCG method in which two groups G1 and G2 are created containing some mobile nodes. In this method, each mobile node broadcast its host id and its access frequency along with data items to other nodes. By using the broadcasting information every node identifies its bi-connected nodes. The access frequency of each group is calculated by adding the access frequencies of all the mobile nodes in that group. According to the overall access frequency of the group, replicas of data items are allocated till the memory of all mobile nodes in the group becomes full.

D. SCF-TREE BASED METHOD

With the measured degree of selfishness, a tree represents relationships among nodes in a MANET for replica allocation, called as SCF-tree. The SCF-tree resembles human friendship management in the real world. The SCF-tree-based replica allocation technique highlights because it can reduce the communication cost, with a considerable achievement on high data accessibility.



(a) A sample topology



(b) SCF-tree of node N1

Fig 6: SCF-tree based method of replica allocation [2]

ISSN (Print) : 2320 – 3765
ISSN (Online):2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

Fig 6(a) shows a sample topology including 6 nodes and Fig 6(b) illustrates the SCF-trees of N1 and N2. The SCF-tree may have multiple routes for some nodes from the root node, but the shortest path will be selected. At every relocation period, each node updates its own SCF-tree based on the network topology at that moment.

III. HANDLING SELFISHNESS IN REPLICA ALLOCATION OVER MANETS

A. CREDIT RISK METHOD

This SCF-tree based credit risk method is found to be the best among the other aforementioned replica allocation methods to handle selfish nodes [19].Each node detects selfishness and makes replica allocation at its own discretion, without forming any group so it reduces overhead. This method includes 3 steps;

- Detecting selfish nodes:

  Each host detects the selfish nodes dependingupon credit risk scores. The credit risk can be calculated as,

$$Credit\ Risk = \frac{Expected\ risk}{Expected\ value}$$

The CR score is updated accordingly during the query processing phase by measuring the degree of selfishness. A node wants to know if another node is believable, in order to share a memory space in a MANET.

- Building SCF-tree:

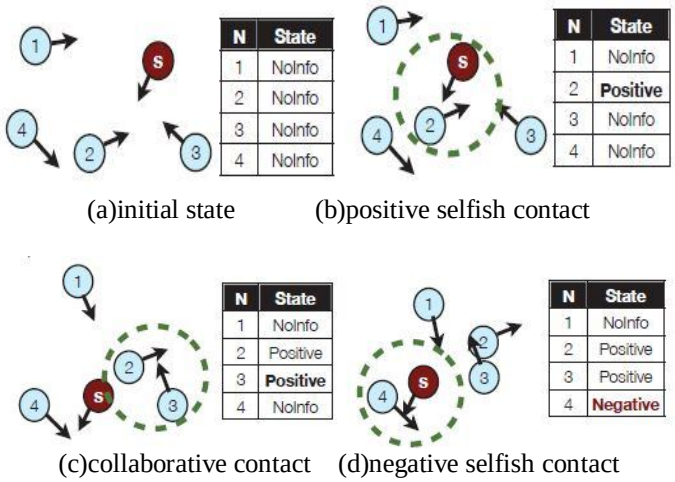
Each node makes its own topology graph and constructs its own SCF-tree by excluding selfish nodes. The SCF-tree based replica allocation techniques are inspired by human friendship management in the real world, where each person makes his/her own friends forming a web and manages friendship by himself/herself. He/she does not have to discuss these with others to maintain the friendship. The decision is solely at his/her discretion.

- Allocating replica effectively:

According to SCF-tree, each node allocates replica in a distributed manner. After building the SCF-tree, a node allocates replica at every relocation period. Each node asks non-selfish 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.

B. COLLABORATIVE WATCHDOG METHOD

Watchdog systems overhear wireless traffic and analysesit to decide whether neighbor nodes are behaving in a selfishmanner and also detects the selfish nodes in the networks. The nodes other than the selfish nodes in the network can be called as collaborative nodes. Collaborative watchdog indicates the presence of the selfish node to the source node. The source node then broadcasts the selfish information to all other nodes. When the watchdog detects a selfish node, it is marked as a *positive* detection (or a *negative*detection, if it is detected as a non-selfish node) or *noinfo*when dissatisfying both the above. This approach reduces the detection time and improves the precision by reducing the effect of both false positives and false negatives [3] [10].



(a)initial state (b)positive selfish contact

(c)collaborative contact (d)negative selfish contact

Fig 7: Collaborative watchdog method [3]

ISSN (Print) : 2320 – 3765
ISSN (Online):2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

Infigure 7, initially it is assumed that there is onlyone selfish node. At this stage, no node has information about the selfish node. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non-selfish node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it. So, from this stage, both nodes store information about this positive (or negative) detection. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative transmission of information that is provided by other nodes. This collaborative approach reduces the time and increases theprecision when detecting selfish nodes.

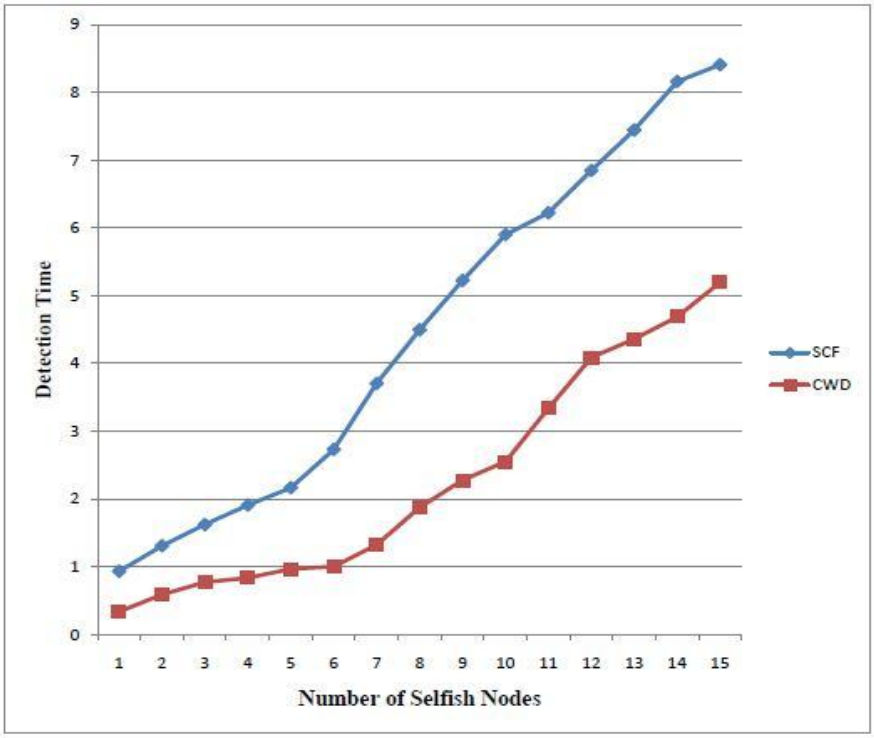


Fig 8: comparison between detection time of SCF-tree base method and watchdog method [11]

Fig 8 illustrates the graphical representation of the detection time of both SCF-tree based credit risk method and the collaborative watchdog method. It is clear that watchdog method takes much less time to detect the same selfish nodes.

C. COMBINED CREDIT RISK AND WATCHDOG METHOD

We applied the credit risk method to detect the selfish nodes and also proposed the collaborative watchdog method to reduce the detection time of those nodes [1] [21]. Every node in a MANET calculates credit risk information on other connected nodes individually so that it is used to measure the degree of selfishness. And then SCF-tree has been constructed with the backup of this credit-risk information. Since the various traditional replica allocation techniques, as described in section V were failed to consider the selfish nodes; in this paper, we propose the combined credit risk and watchdog methodto handle selfishness in replica allocation effectively.The combined credit risk and watchdog method works as follows:

- Recognizing the selfish replica allocation problem.
- Detecting the fully or the partially selfish nodes effectively.
- Applying collaborative watchdog method.
- Allocating replica effectively.

Finally, the credit risk method incorporates watchdog mechanism in it before building the SCF-tree to detect the selfishness in mobile adhoc networks fastly and effectively. This method includes the advantages of both credit risk method and watchdog method. Thus, the combination of credit risk and watchdog methods improves the data accessibility, reduces communication cost and average query delay and to improve the accuracy of watchdogs in the collaborative methodand also to reduce thedetection time.

ISSN (Print) : 2320 – 3765
ISSN (Online):2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

IV. CONCLUSION

This survey paper considers various methods to handle selfish nodes in MANETs. It deals with traditional replica allocation methods such as SAF, DAFN and DCG methods. From the above survey, we understood that SCF-tree based technique is the best among the above mentioned replica allocation techniques, and a combination of this credit risk and watchdog method detects the selfish nodes within much less amount of time.The proposed methodimproves the data accessibility, reduces communication cost and average query delay and also to reduce thedetection time and to improve the accuracy of watchdogs in the collaborative method.Detecting the false alarms in this technique can be considered as a future work.

REFERENCES

[1] 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
[2] Jae Ho Choi, Kyu Sun Shim, Sang Keun 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,pp.278-291,February 2012
[3] Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni, "CoCoWa: A Collaborative Contact-based Watchdog for Detecting Selfish Nodes",IEEE Transactions on Mobile Computing, DOI 10.1109/TMC.2014.2343627, 2014
[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] Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog", IEEE Communications letters, Vol. 16, no. 5, May 2012
[6] Takahiro Hara, Sanjay K. Madria, "Data Replication for Improving Data Accessibility in Ad Hoc Networks", IEEE transactions on mobile computing, Vol. 5, no. 11, November 2006
[7] T Hara, "Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility," Proc. IEEE INFOCOM, pp. 1568-1576, 2001
[8] ShailenderGupta,C. K. Nagpal and CharuSingla, "Impact of selfish node Concentration in manets", International Journal of Wireless & Mobile Networks (IJWMN), Vol. 3, No. 2, April 2011
[9] 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
[10] JosephinJeneba Y, Prabakaran T, "Detection of Selfish Node in Manet using a Collaborative Watchdog", international journal of engineering sciences & research Technology, ISSN: 2277-9655, May 2013
[11] Sheethal Sunny1, Dr.C.D.Suriyakala, "Performance Analysis of Selfish Nodes in Mobile Ad-hoc Networks", ISSN (Print) : 2320 – 3765, ISSN (Online): 2278 – 8875, Vol. 3, Issue 5, May 2014
[12] 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
[13] Yanchao Zhang, Wenjing Lou, Yuguang Fang, "SIP: A Secure Incentive Protocol against Selfishness in Mobile Ad Hoc Networks", IEEE Communications Society, 2004
[14] Kejun Liu, Jing Deng, Pramod K. Varshney, KashyapBalakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in manets", IEEE transactions on mobile computing, Vol. 6, no. 5, May 2007
[15] K.Sridevi, S.Kannan, S.Karthik, "A Survey on Selfish Node Detection Using Several Techniques in MANET", International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-I, Issue-I, December 2012
[16] J.Vijithanand, K.Sreerama Murthy, "A Survey on Finding Selfish Nodes in Mobile Ad Hoc Networks", J.Vijithanand et al,/ (IJCSIT) International Journal of Computer Science and Information Technologies, ISSN:0975-9646,Vol. 3 (6), 2012,5454-5461, 2012
[17] 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. 1606-161, Nov. 2006.
[18] Sagar D. Padiya, RakeshPandit, Sachin Patel, "A System for MANET to Detect Selfish Nodes Using NS2", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 1, Issue 2, November 2012
[19] Mr. RiteshDhanare, Dr. SunitaVarma, "Replica Allocation in MANETs for Eliminating Selfish Node", International Journal of Scientific & Engineering Research, ISSN 2229-5518,Volume 4, Issue 8, August 2013
[20] Y-Yoo and D P Agrawal,"Why does it pay to be selfish in a manet?", IEEE Wireless Communications, December 2006
[21] N.Muthumalathi, Dr.M.MohamedRaseen, "Fully Selfish Node Detection, Deletion And Secure Replica Allocation Over Manet", International Conference on Current Trends in Engineering and Technology, 2013