Efficient Replica Distribution by Determining Selfishness In MANET

Kanmani Govindaraj[1], R.Muthuvenkatakrishnan [2], A.Mani[3]

[1] *MTech , Department of CSE, PRIST University,*
Thanjavur, India

[1]kanmanigovindaraj@gmail.com

[23] *Assistant Professor, Department of CSE ,*
PRIST University, Thanjavur, India

[2]muthu.brillia@gmail.com , [3]inovic.mani@gmail.com

Abstract- In a mobile adhoc network (MANET), recovering selfish data is a pressurized work. The duplication method provides a desirable sketch to the mobile nodes, that's doesn't get post packets to other nodes. The nodes systems which act as selfishly to keep their resource are called selfish nodes: This method is used in distributed networks. Data duplication design for MANET many selfish nodes do not share out their replicas for the purpose of other nodes. These selfish nodes scrutinized by a credit risk score method or else data replication method which is organized by selfish node detection algorithm, and identifying with false alarm. The proposed method simulations and analytical assessment demonstrates that reduces the communication cost over the replica allocation scheme as the number of users' increases in network while achieving analogous data accessibility.

Index Terms: Replica allocation, selfish nodes, false alarm, degree of selfishness, credit risk

1. INTRODUCTION

A MANET is a self-organizing network which consists of wireless nodes without a fixed infrastructure. [12]. If the resource nodes and destination nodes are not in the coverage area, information is posted to the destination through other nodes which exist between two hosts. selfish nodes begin submissive stabbing and are usually a region consequence effect of a particular node planning at protecting their restricted amount of property or absolute selfishness [2].The network issues are important in a MANET, replica allocation is also a critical stage in mobile nodes which performs the larger network area [2] [11].

The self-seeking nodes are reacted by a risk-aware response mechanism based on revise resolution creation (RRC) which results in node separation, duplication distribution and direction-finding table recovery. In MANET Replica allocation are used to overcome the drawbacks of performance deficiency. It simulates all nodes allocate their disk area to reduce the congestion in network.

In Mobile Ad hoc Network (MANET), each node fulfills their service using their specific action in the network. There is no federal and circulated service, user defined service. Here arbitrary performance of network is the main issues which concern the data deliverance; it depends on coverage of neighbors and root link failure, each and every node works according to the successful request and response of data lines in the network distribution. This network distribution is determined by self seeking node performance according to the data duplication score which is calculated by the malicious node in destination coverage area. The replica allocation techniques in MANET is described as Static Access Frequency (SAF) [4], Dynamic Access Frequency and Neighbourhood (DAFN) [4] [11], and Dynamic Connectivity Based Grouping (DGBG) [4] failed to consider the selfish nodes. Therefore the selfish replica allocation considers the replica allocation techniques and false alarm mechanism. Mobile adhoc network each selfish node will calculate and collect information by send and transmit data from a normal flow of action more than discovered secret source by trusted nodes in a network.

2. PROBLEM DEFINITION

This section address the problem of handling selfishness nodes from the replica allocation perception in a MANET for example... a selfish node may not transmit data to other nodes. It also provides selfish node detection methods and to identify the false alarm concepts.

3. PROPOSED SYSTEM APPROACH

The proposed system approach provides self seeking nodes reliability of data transmitted over a network

3.1 Monitoring Nodes

The spectator is the progression of handling data transmission of the nodes in the mobile adhoc network. The interruption detection system comprises in looking up the nodes performance which behaving maliciously. The replica server accesses the data transmission of the network.

3.2 Node Behavioural States

The behavioural states of nodes as three types in mobile adhoc network from the perspective of constraints at memory space

Type-1 Selfish Node: These nodes are restricted in nature to send data rather receives and stores for its own purpose.

Type-2 Non Selfish Node: These nodes are opened to share memory space and resource from other nodes in a network.

Type-3 Partial Selfish Node: These nodes are using their memory space partially for resource by the other nodes. These nodes will accept or reject request based on their local status

3.3 Recognizing the Selfish Nodes

In MANET, the key constraint is that all nodes have to assist fully in terms of their property. A node wants to know if another node is creditable to distribute a memory space over in network. The node can be separate into three types based on their credit risk (CR). The CR can be described by

Credit risk=expected risk/expected value

And also the self seeking node is calculated by the data replication techniques.

$$\textbf{Data Replication}= \frac{\textbf{Number of successful request}}{\textbf{Number of successful and failed request}}$$

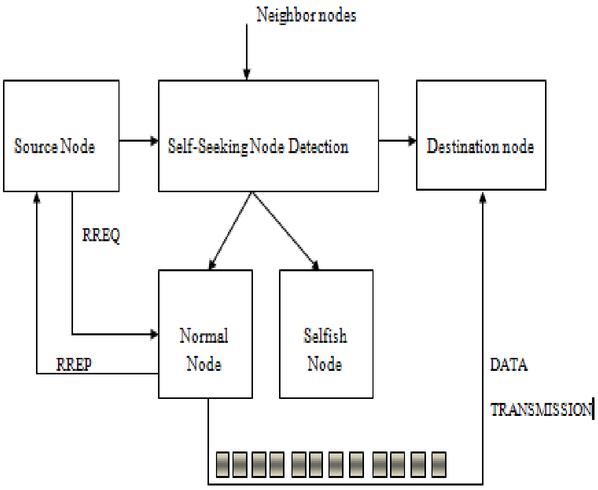
Data Replication (DR) value is known as quantity of self-centredness. The number of successful request is considered by amount of resources performed by node and the number of successful and failed request is considered by amount of memory spaces distributed.

Node selfish attribute classified into two sets
1) Node specific and
2) Query processing specific

Node specific method signifies to the number of successful request served by the nodes and it's calculated by packets send to the nearby malicious nodes. **Query processing specific** method symbolizes to the number of successful and failed request served by the node and its main focus in find out the self seeking node and reduces the congestion in network coverage area of MANET.

Credit risk scores are used to conclude the self-seeking behavior of nodes. Therefore every node is talented of identifying self-seeking nodes. Handling selfishness in a small network based on their node states and credit risk value

BLOCK DIAGRAM FOR SEEKING SELFISH NODES



ALGORITHM

Step 1: Each and every node in the network evaluates credit risk for allocating replica

Step 2: The source node implements the self-seeking node detection algorithm and find the node behaviour partial or full selfish present in the network

Step 3: The source transmits its data packet to the node which finds the query processing time
Step 4: Determine the expected node responds to the requested node or unexpected node responds to the requested node.

3.4 Discovering Selfish Nodes

The node with high credit risk score value is designated then the node is described as fully selfish node and the credit risk value is middling then the node is defined as partial selfish node. The credit risk value is less than the middling value then it is non selfish value. The replica allocation techniques are based on the SCF tree management. These tree forms relationship between the nodes but this does not have to conserve with other nodes in a network to maintain the friendship.

3.5 Relocating Memory Space

Reproduction distribution controls the essential node in each group plays of the mock-up allocator who distribute replicas to the group nodes based on the estimated access allocator at the duplication relocation time .The approximate access frequency time to enhance the solidity of the data accessibility.

Repositioning of reproduction management will address the two issues: first to ensure how fulfil a data request with minimum cost of time and the second issue how to improve request success ratio in network.

3.6 False Alarm Mechanism

The detection of the false alarm leads recovered performance in the overall network. The false alarm has been raised to reduce detection time of selfish node and identify the network dissemination. The false alarm can be handled using the overall selfishness alarm.

The false alarm may occur when detecting the node as selfish node that has low credit risk value due to network failure or traffic. The false alarm are used to detect selfish nodes in network are initiated by replica server. False alarm is a way to reduce the detection time and improve accuracy of the nodes

4. SIMULATION ANALYSIS

Simulation analysis model uses the network simulator NS-2 for evaluation [5].

A. *Simulation Parameters*:

To find the best routing among the self-seeking nodes in the network, this helps to transmit the data. Transmission range will be very high in non elfish nodes. The system parameter is used to adjust the node updates at all dispensation into connected node at every relocation period. Each node determines duplication distribution individual basis without any communication with other nodes; these things are used to perform the picture to provide best result.

Parameter	Value
Simulator	Ns2 - 2.3x
Number of nodes	50
Simulation Time	15 min
Packet Interval	0.01 sec
Simulation Landscape	1000 x 1000
Background Data Traffic	CBR
Packet Size	1000 bytes
Queue Length	50
Initial Energy	10 Joules
Transmission Range	100 Kbytes
Node Transmission range	250 m
Antenna Type	Omni directional
Mobility Models	Random-waypoint (0-30 m/s)
Routing Protocol	MCAST
MAC Protocol	IEEE 802.11

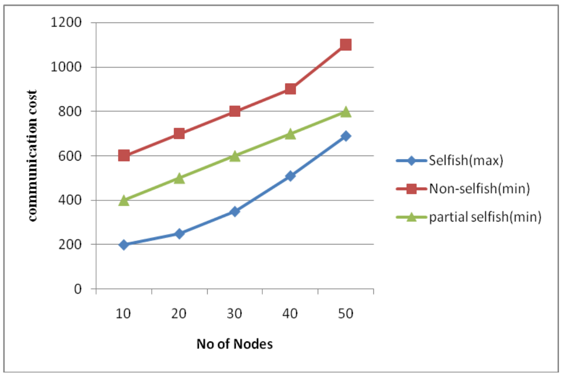
B. *Performance parameter*

- Communication cost
- Average query delay
- Data delivery rate

1. *Communication Cost*

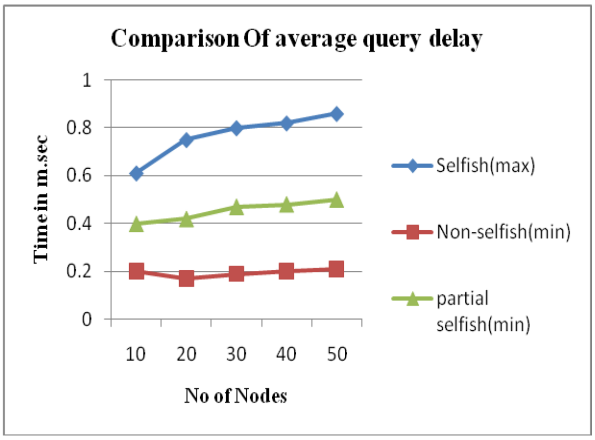
The communication cost is estimated by the total amount of data transmission for self-seeking node and simulated allocation. The issue of Communication cost increases as restricted recollection amount. It participate the information sharing and node detection process based on network topology. The communication path is most trusted transferring message path between the malicious and self-seeking nodes. This path is referred based on the data replication method or credit risk score values

.



2. *Average query Delay*

The average query delay process is the number of successive and the number failed request in data replication. The average query delay ratio is determined by time moved out to the send and transmitting nodes request and response process engaging with all successive uncertainty nodes states. Each node generates node states and time link by the other nodes.

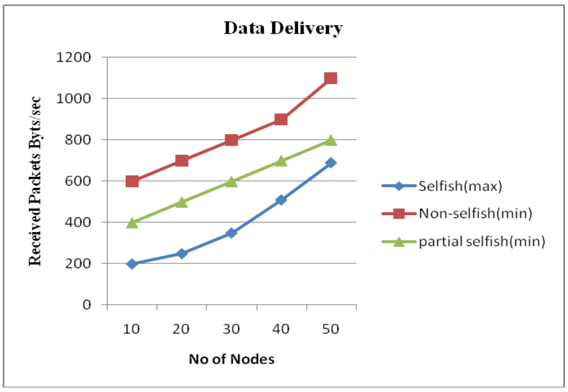


3. *Data Delivery Rate*

Data delivery ratio will address the two issues.

- Data delivery measures how to implement a data request with a minimum cost of time in mobile networks.
- It displays how to improve the successive request ratio while sending the information to other nodes because in MANET a data request and response can get failed easily due to network problem or congestion problem.

So that data delivery rate is stable with relocation period. It is propositional of the size of memory space expected. These node states represented by size of memory space and shared resources.



CONCLUSION

In this proposed system has addressed the problem of selfish node from the reproduction distribution perspective in a MANET as overall. This proposed system is accomplished for handling selfishness in a small network based on their node states and credit risk value or else calculating data replication value method. In MANET the self-seeking duplication share could reduce the overall data convenience and identify the false alarms. MANET calculates credit risk information on other connected nodes individually to measure the amount of self-seeking nodes. Since duplication share techniques used to decreases the communication cost, average query delay and data delivery detection time of self-seeking nodes. False alarm concept is the problem that the nodes are not transmitted to the destination not because of selfishness. The failure will occur due to network failure

REFERENCES

1. Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu, Fellow, IEEE, “Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network” IEEE Transactions On Mobile Computing, Vol. 11, No.2, February 2012.
2. E. Adar and B.A. Huberman, “Free Riding on Gnutella,” First Monday, vol. 5, no. 10, pp. 1-22, 2000.
3. 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.
4. 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.
5. R.F. Baumeister and M.R. Leary, “The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation,” Psychological Bull., vol. 117, no. 3, pp. 497-529, 1995.
6. J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, and J. Jetcheva, “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols,” Proc. ACM MobiCom, pp. 85-97, 1998.
7. G. Cao, L. Yin, and C.R. Das, “Cooperative Cache-Based Data Access in Ad Hoc Networks,” Computer, vol. 37, no. 2, pp. 32-39, Feb. 2004.
8. B.-G. Chun, K. Chaudhuri, H. Wee, M. Barreno, C.H. Papadimitriou, and J. Kubiatowicz, “Selfish Caching in Distributed Systems: A Game-Theoretic Analysis,” Proc. ACM Symp. Principles of Distributed Computing, pp. 21-30, 2004.

9. E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, “Managing and Sharing Servents’ Reputations in P2P Systems,” IEEE Trans. Knowledge and Data Eng., vol. 15, no. 4, pp. 840-854, July/Aug. 2003.
10. G. Ding and B. Bhargava, “Peer-to-Peer File-Sharing over Mobile Ad Hoc Networks,” Proc. IEEE Ann. Conf. Pervasive Computing and Comm. Workshops, pp. 104-108, 2004.
11. M. Feldman and J. Chuang, “Overcoming Free-Riding Behavior in Peer-to-Peer Systems,” SIGecom Exchanges, vol. 5, no. 4, pp. 41-50, 2005.
12. D. 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.
13. T. Hara, “Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility,” Proc. IEEE INFOCOM, pp. 1568- 1576, 2001.
14. 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.
15. 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.
16. S.U. Khan and I. Ahmad, “A Pure Nash Equilibrium-Based Game Theoretical Method for Data Replication across Multiple Servers,” IEEE Trans. Knowledge and Data Eng., vol. 21, no. 4, pp. 537-553, Apr. 2009.

AUTHOR PROFILE

Kanmani Govindaraj received her B.Tech degree in Information Technology from Bharathiyar College of Engineering and Technology, Pondicherry University, Karaikal, India in 2007. She is pursuing her **M.Tech** Degree in Department of Computer Science and Engineering, PRIST University, Thanjavur. She was a lecturer in the department of Information Technology, Rajalakshmi Institute of Technology, Anna University, Chennai. Her research interest includes distributed databases and mobile networks.

MuthuVenkataKrishnan.R , he received his M.E(Master of Engineering) Degree from the Department of Computer Science and Engineering Annamalai University in 2006. He is Working as an Assistant professors in PRIST UNIVERSITY and having more than 8 years of teaching experience. His research interests are Image processing and mobile computing.

A.MANI, MCA, M.Tech, (MBA) he received his M.Tech degree from Degree from the Department of Computer Science and Engineering PRIST UNIVERSITY Tanjavur. He is Working as an Assistant professors in PRIST UNIVERSITY. His research interests are System Software, Operating System and mobile computing