Indian Journal of Science and Technology, *Vol 8(20), DOI: 10.17485/ijst/2015/v8i20/59236, August 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Communication based Clustering to Detect Selfish Nodes in MANET

D. Santhosh Kumari[1]* and K. Thirunadana Sikamani[2]

[1]Department of Electronics and Communication Engineering, St. Peter's University, Chennai - 600054, Tamil Nadu, India; kumari.stpeters@yahoo.in

[2]Department of Computer Science and Engineering, St. Peter's College of Engineering and Technology, Chennai - 600054, Tamil Nadu, India; thirumani.sikamani@gmail.com

Abstract

Objective: The main intent of this research is to detect the selfish node in Mobile Ad-hoc Networks (MANETs) and to select the Cluster Head (CH) based on the energy level and Node Communication Ratio (NCR). **Methods/Analysis:** In this paper, a new mechanism is developed to identify the selfish nodes in the communication network. Based on the level of energy and the Node Communication Ratio, the Cluster Head is selected. The cluster head in turn is used to contribute to the network within its infrastructure range. The sink node will be noticing the behavior of each and every communicating node in the network. **Results:** The communication based clustering has proved better performance in terms of packet delivery rate, packet loss rate, packet delay rate and better energy efficiency during data transmission. **Conclusion:** The simulation results show that this scheme has improved quality of service compared to the existing scheme 2Ack. This scheme can be applied in the areas of military operations, emergency and disaster management in order to ensure reliable data delivery on-the-move.

Keywords: Cluster Head, Clustering, Mobile Ad-hoc Network, Selfish Node

1. Introduction

In Mobile Ad-hoc Network (MANET), because of the dynamic nature, the ad hoc routing faces problems those are not present in wired networks. Particularly in MANETs where routes become obsolete frequently because of mobility and poor wireless link quality.

Watchdog and Pathrater is a mechanism proposed in[1] based on detects and exclude principle to deal with the selfish nodes. It uses Dynamic Source Routing implemented in[2] as base protocol. It has two components: Watchdog and Pathrater. The charge of Watchdog is to detect selfish nodes that do not forward packets. The Pathrater assigns different rating to the nodes based upon the feedback that it receives from the Watchdog. All the nodes in the network buffer every transmitted packet for some time. During this interval, the node places its wireless interface into the promiscuous mode in order to overhear whether the next node has forwarded the packet or not and ratings are developed. These ratings are then used to select routes consisting of nodes with the highest forwarding rate.

SORI protocol[3] is based on detect and exclude mechanism. It makes two records, the local evaluation record (First hand trust) and the overall evaluation record based on the reputation index given by the nodes about their neighbors. Every node in the network maintains tables of first and second hand trust of their neighboring nodes. Based on these tables the trust of a node is calculated and then action is taken against the selfish nodes.

2. Related Works

Confidant protocol[4] adds trust manager and reputation index to the Watchdog and Pathrater mechanism. Each node in the network maintains two lists to deal with the selfish nodes. The nodes which behave rationally are kept in the friends list and the nodes which drop the packets

*Author for correspondence

or tamper them are kept in the black list. These lists are exchanged by the neighboring nodes. Based on these list trust of a particular node is calculated. Whenever the trust value for a particular node falls below a certain threshold the protocol stops forwarding packets of that node.

CORE (Collaborative Reputation)[5] is a reputation based system. The limitation with CORE is that the most reputed nodes may become congested as most of the routes are likely to pass through them. The limitations of the monitoring system in networks with limited transmission power and directional antennas have not been addressed in CORE. Observation-based Cooperation Enforcement in Ad-hoc Networks (OCEAN)[6] is the improved version of DSR. OCEAN uses a monitoring system and a reputation system to identify malicious nodes. But OCEAN fails to deal with misbehaving nodes properly. These papers have addressed the black hole attack problem on unicast routing protocols.

Another acknowledgement based scheme similar to TWOACK scheme is proposed in[7]. This scheme detects the misbehaving link, eliminate it and choose the other path for transmitting the data. The main plan is to send 2ACK packet which is assigned a fixed route of two hops back in the opposite direction of the data traffic route and to reduce the additional routing overhead, a portion of the data packets will be acknowledged via a 2ACK packet. This scheme also consists of multicasting method by which sender can broadcast information of misbehaving nodes so that other nodes can avoid path containing misbehaving nodes and take another path for the data transmission. Even though routing overhead caused by transmission of acknowledgement packets is minimized, this scheme also suffers to identify the particular misbehaving node.

Mobile Agent Based Detection of Selfish Node (MADSN) in MANET is an approach implemented in[8] which uses a set of Mobile Agents (MA) that can move from one node to another node within a network. This will reduce network bandwidth consumption by moving the computation for data analysis to the location of the intrusion. The mobile agents travel through the network, gathering vital information is then processed by the mobile agent itself. As the computation overhead of our algorithm is less, the computation complexity of the mobile agent will be reduced. The computation is done by mobile agent when the source node notices that the destination node does not respond in correct time. Mobile Ad-hoc Network (MANET) is highly vulnerable to attacks due to the open medium, dynamically changing network topology, co-operative algorithm, lack of centralized monitoring and management point.

In[9] a new mechanism presented to detect selfish node. In this method, each node is expected to contribute to the network on the continual basis within a time frame. The nodes which fail will undergo a test for their suspicious behavior. This scheme is also based on monitoring node. A monitoring node hears a request from its neighboring node to forward a data packet; it will first check the time difference between last request and last action and status of the requestor.

In[10] the Predictive Re-Alignment Strategy for Agile Communication in Wireless Sensor Networks using the network simulator is proposed and simulated. From the results obtained through multiple simulations, it is understood that the performance of the PRS is much superior to that of the normal AODV. The outputs obtained showed a 78% difference between the conventional and the proposed scheme. Optimization of the PRS algorithm to compare with some of the recent mobility algorithms is under current research. Future works will aim at providing a clear cut application based strategy extended from the PRS with real-time implementation to support the simulation analysis of the same.

One of the efficient and prevalent usages of ad-hoc network is using clustering in such a network. In fact, sensor nodes might reduce overload communications. With this purpose, it was tried to deliver an algorithm[11] which prevents direct connection between all cluster heads and base station; instead, cluster heads should use other cluster heads near to the base station in order to transfer data to the base station; they were selected based on the factors such as cluster head distance with base station and distance among cluster heads. Also, in this proposed algorithm, routes are selected such that, the selected routes' length is almost equal and finally results in work load balance among cluster heads and decrease energy consumptions and increase network lifetime. In addition, time delay for data transfer to base station becomes level off in all routes.

An unequal clustering approach is proposed[12] in the networks for even energy distribution. It also reduces the overall energy consumption which in turn improves the network lifetime. The energy needed for entire operations for one round using the proposed method is lesser than that of LEACH, an equal clustering methodology.

The distribution of keys in an authenticated manner is a difficult task in MANETS and when a mobile node

leaves or joins generates new session key. The combination of Enhanced Distributed Weighted Clustering Routing Protocol (EDWCRP) and RSA has been proposed in [13] to secure multicast key distribution. Cluster Head maintains the group key and it also updates the group key whenever there is a change in the membership. A Secondary Cluster Head (SCH) is also elected to avoid the CH from becoming a bottleneck. Mobile nodes get authenticated using MD-5 hash authentication mechanism.

3. Communication based Clustering

The main objective of this project is to improve the routing in MANET by introducing the concept of Communication based clustering to detect Selfish Nodes (CCDS) in MANET. The behavior of the node is monitored depending on the reply messages from the nodes in the network. The Node Communication Ratio (NCR) is calculated based on the behavior of the nodes. If the value of NCR is found to be greater than 30%, it is a normal node which is able to send and receive information. If the value of NCR is found to be lesser than 30%, then the node is a selfish node. Depending upon the nodes in the network within its communication range the nodes are combined to form clusters in the network. The Cluster Head (CH) is selected for every cluster group with the node having high energy and highest communication ratio. If the node is found to be the cluster it sends the information to the cluster head and only through cluster head the information is send to the sink node. The Architecture of the proposed system is shown in Figure 1.

3.1 Node Communication Ratio

In the proposed work, the Node Communication Ratio (NCR) is calculated. The NCR is calculated depending upon the route request and route reply messages send within the communication network. For a node in the network, the NCR is calculated depending upon the difference between the number of route request message received to a particular node and the number of unsent route reply messages to the number of route request message received. The node communication ratio is calculated by

$$NCR = \left(\frac{P-R}{P}\right) * 100 \quad (1)$$

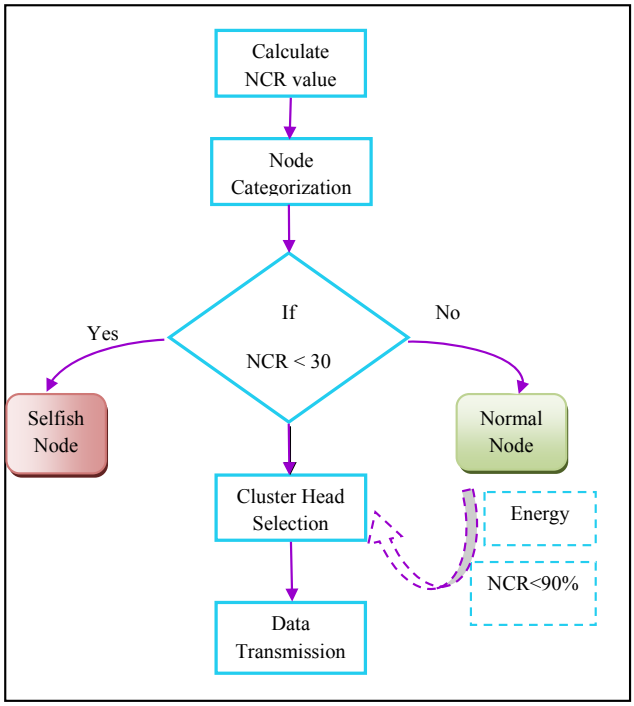

Figure 1. Architecture of the communication based clustering scheme.

where

P-> Get Route Request

R-> Not send Route Reply

$$R = P - Q \quad (2)$$

Q->Reply Route Request

3.2 Node Categorization Algorithm

The cluster is formed based on location of the node. The nodes that are communicated with in transmission range are grouped.

Then the Cluster Head is selected based on energy level and Node Communication Ratio. The energy level is compared with each node and the node with the higher energy as well as NCR with greater than 90% is selected. Finally data is transmitted from source to sink successfully.

The algorithm for node categorization is given in Table 1. This method is used effectively to increase packet delivery ratio. It reduces packet loss, network delay and energy consumption. Every node that communicates within its transmission range is grouped. Then CH is selected based on energy and NCR. The energy is higher compared to other nodes and those nodes with NCR >

Table 1. Node categorization algorithm

Step 1: Start

Step 2: Calculate NCR

Step 3: if NCR > 90%

That node is called efficient node

Step 4: Else if, 30% < NCR < 90%

That node is called Average Node

Step 5: Else NCR < 30%

That node is Selfish node

90% is selected. Finally data is transmitted from source to sink successfully. This proposed method has increased packet delivery rate, reduced packet loss, network delay and energy consumption.

4. Simulation Analysis

The simulation analysis of the proposed mechanism is analyzed using network simulator NS-2. Since it is possible to discreetly analyze the events in a network scenario, we use the NS-2 tool for the simulation of the CCDS scheme in a MANET. In order to assess the network performance we evaluate the packet delivery ratio, packet loss ratio and the delay performance of the network before and after adapting the proposed system. The simulation parameters for performance analysis are listed in Table 2.

4.1 Packet Delivery Rate

The Packet Delivery Rate (PDR) is the rate of the number of packets delivered to the destination to the total number of packets sent. It is given by the Equation 3.

$$PDR = \frac{\sum_0^n Packets\ Received}{\sum_0^n Packets\ Sent} \quad (3)$$

Figure 2 indicates that the proposed scheme CCDS has achieved higher packet delivery ratio when compared to that of the existing scheme DSR.

Table 2. Simulation parameters for performance analysis

Parameter	Value
Simulation Time	50 ms
Number of nodes	38
Routing protocol	DSR
Traffic model	CBR
Simulation Area	800 x 800
Transmission range	250m
Antenna Type	Omni antenna
Network interface Type	Wireless Phy
Channel Type	Wireless channel
Mobility Model	Random Way Point

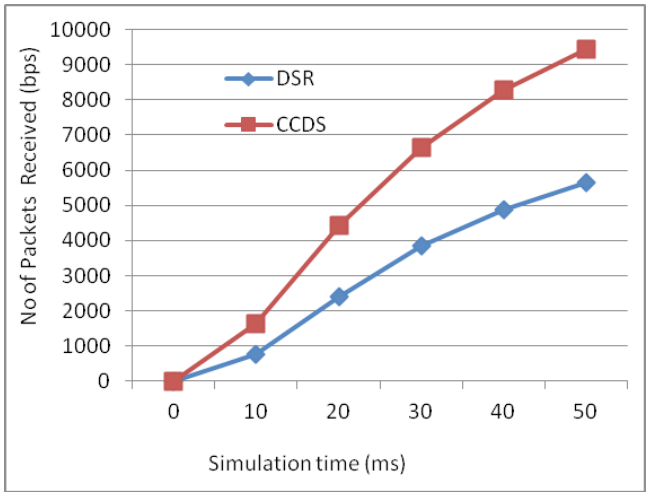

Figure 2. Packet delivery rate.

4.2 Packet Loss Rate

The Packet Loss Rate (PLR) is the rate of the number of packets lost to the total number of packets sent. It is given by the Equation 4.

$$PLR = \frac{\sum_0^n Packets\ Dropped}{\sum_0^n Packets\ Sent} \quad (4)$$

Figure 3 comparison analyses of CCDS with DSR. The proposed scheme provides better performance than the existing scheme.

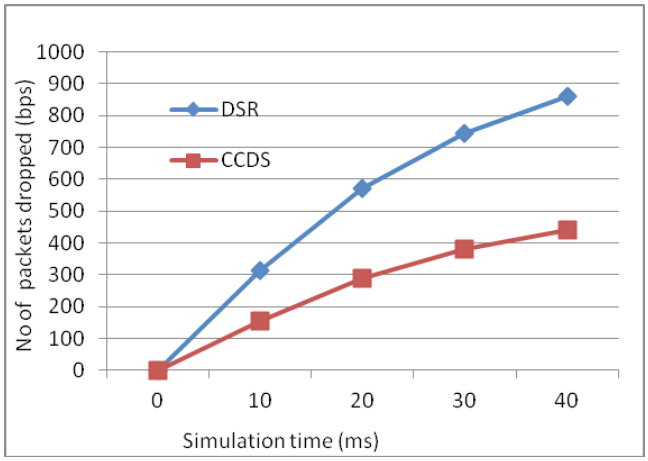

Figure 3. Packet loss rate.

4.3 Average Delay

Average Delay refers to the ratio of the time at which packets are sent to the packets that are received. It is given by the Equation 5.

$$Average\ Delay = \sum_{0}^{n} (Pkt\ Recvd\ Time - Pkt\ Sent\ Time) \quad (5)$$

Figure 4 indicates that the delay of the CCDS is low compared to the DSR scheme.

4.4 Energy Efficiency

The amount of energy remaining in a node at the current instance of time is called as residual energy. The energy efficiency is shown in Figure 5.

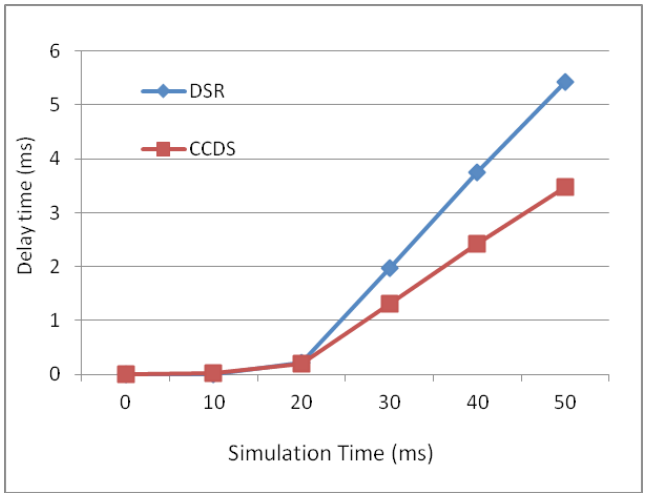

Figure 4. Delay rate.

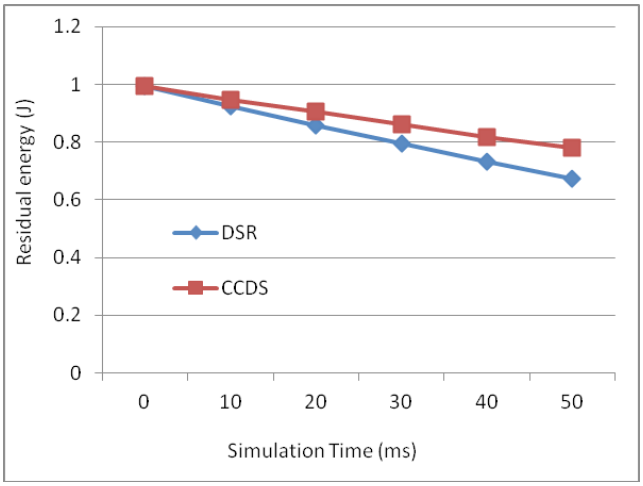

Figure 5. Energy efficiency.

Figure 5 shows that the residual energy of the network is high for the CCDS when compared with DSR.

5. Conclusion

In this paper, we proposed, designed and simulated the communication based clustering Concept to Detect Selfish Nodes (CCDS) in Mobile Ad-hoc Networks. We have introduced the new concept of node communication depending upon the route request and route reply messages send within the communication network. Comparing with the simulation results of DSR, the CCDS has proved better performance in terms of packet delivery rate, packet loss rate, packet delay rate and better energy efficiency during data transmission. This scheme can be applied in the areas of military operations, emergency and disaster management in order to ensure reliable data delivery on-the-move.

Future work aims at analysis of using the selfish node as a front node of data transmission instead of avoiding it in the network.

6. References

1. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in Mobile Ad-Hoc Networks. Proceedings of MobiCom; Boston. 2000.
2. Johnson DB, Maltz DA, Broch J. DSR: The dynamic source routing protocol for multihop wireless ad hoc networks. Ad Hoc Networking. 2001; 5:139–72.
3. Wu D, He Q, Khosla P. SORI: A secure and objective reputation - based incentive scheme for ad-hoc networks. IEEE

Transactions on Wireless Communications and Networking. 2004; 2:825–30. DOI: 10.1109/WCNC.2004.1311293.

4. Buchegger S, Le Boudec J-Y. Performance analysis of the CONFIDANT protocol on Mobile Ad-Hoc Networking and computing. Proceedings of 3rd ACM International Symposium; 2002.
5. Michiardi P, Molva R. Core: A collaborative reputation mechanism to enforce node cooperation in Mobile Ad-Hoc Networks. Proceedings of 6th IFIP Communications and Multimedia Security Conference; Portorosz, Slovenia. 2002. p. 107–21.
6. Bansal S, Baker M. Observation-based cooperation enforcement in ad-hoc networks. Networking and Internet Architecture; 2003. p.1–10. arXiv: cs/0307012.
7. Vijaya K. Secure 2Ack routing protocol in Mobile Ad-Hoc Networks. IEEE Region 10th Conference on TENCON; 2008. p. 1–7.
8. Roy DB, Chaki R. MADSN: Mobile agent based detection of selfish node in MANET. International Journal of Wireless and Mobile Networks. 2011; 3(4):225–35.
9. Azmi K, Abu Bakar, Irvine J. A scheme for detecting selfish nodes in MANET using OMNET++. IEEE Transactions on Wireless and Mobile Communications. 2010:410–4.
10. Vallapuram BM, Nair GP. Predictive re-alignment strategy for agile communication in wireless sensor networks. Int J Adv Sig Img Sci. 2015; 1(1):12–8.
11. Fanian F, Rafsanjani MK. A novel routing efficient algorithm based on clustering in WSNs. Indian Journal of Science and Technology. 2013; 16(12):5542–5.
12. Baranidharan B, Srividhya S, Santhi B. Energy efficient hierarchical unequal clustering in wireless sensor networks. Indian Journal of Science and Technology. 2014; 7(3):301–5.
13. Gomathi K, Parvathavarthini B. An enhanced distributed weighted clustering routing protocol for key management. Indian Journal of Science and Technology. 2015; 8(4):342–8.