INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1397 - 1401
RECEIVED : 16/11/2016. PUBLISHED: 28/11/2016
November 28, 2016

ERADICATION OF SELFISH NODE IN MANET USING CSNA MECHANISM

[1]P.Vijayalakshmi, [2]P.Visvanathan,
[1]PG Scholar, Dept Of CSE, Ganadipathy Tulsi's Jain Engineering College, Vellore
[2]Asst Prof, Dept Of CSE, Ganadipathy Tulsi's Jain Engineering College, Vellore

Abstract:

A Mobile Ad hoc Network is an infrastructure less system of mobile node connected by wireless links. These mobile nodes act as an end system as well as a router. Most of the routing algorithms designed for MANET to forward every packet in the network. But in practice few of the nodes may act as the selfish nodes. Therefore, detecting these nodes is essential for network performance. In this paper, we present a new mechanism called Categorized Selfish Node Allowance (CSNA) to improve energy in wireless sensor networks to detect those selfish nodes. There is a possibility that because of less energy, the normal node will not respond to other nodes in the network. Since there is low energy for the node, there is a chance for the normal node to become dead when those nodes continuously respond to other nodes in the network. To avoid such situation, the normal node will act as selfish node. By calculating the energy for each node, the normal node will be differentiated from the selfish node.

Keywords : Ad hoc Network, Manet, Selfish Node, CSNA.

1. INTRODUCTION

MANET is the most relevant area of research mainly because of the various challenges that it poses to the existing protocols and architectures. MANETs are wireless infrastructure less, autonomous networks and self organizing networks. Owing to their inherit characteristics such as no centralized control and limited energy resources, MANETs are susceptible to various vigorous and flaccid attacks. Additionally, most of the routing protocols proposed for MANET operate on the hypothesis that all the nodes must cooperate in routing operations such as packet forwarding, route discovery and route maintenance process. MANET nodes are necessary to cooperate with other nodes in forwarding packets and delivery services. In MANETs, nodes are varied such as mobile phones, laptops and belong to different persons gathered in the same environmental area for some reasons. These nodes can communicate each other that an individual node unselfishly spends its inadequate resources for helping other nodes. Conversely, this cooperation leads towards in which each node consumes its insufficient resources, such as battery power. The limited energy resource can prompt nodes to avoid take part in network services for other nodes, whilst still enjoying the network service. The nodes display such activities are considered as selfish. Talreja and Jethani [2] proposed selfish node use the network for their individual communication but just reject to cooperate in forwarding packets for other nodes to facilitate save battery life. A selfish node would thus use the benefits provided by the resources of other nodes, but will not make available its own resources to help others. The selfish node does not cooperate jointly the normal node in the main reason for saving battery power. As a result we propose a Revival of Selfish node in clustered MANET.

2. RELATED WORK

Acknowledgement is authenticated by the node's public key and some encryption method. But the node does not received acknowledgment by two hops left node and it indict the one hop away node as selfish. The 2 ACK receivers, monitors the link periodically by maintaining the information about the no of data packets sent and the no of data packets does not acknowledged within the period. Samreen and Narasimha [1] explained 2ACK technique detects the misbehaving link but cannot decide the connected node in which nodes are misbehaving thus, PFC monitoring as to detect the misbehaving nodes once the misbehaving link is detected. Hernandez-Orallo [3] introduced Watchdogs to detect selfish nodes in computer networks. A watchdog is the collaborative approach. The analytical model is evaluating the detection time and cost of this collaborative approach. Watchdog can significantly reduce the overhead and decrease overall detection time. Also improve the accuracy. Hernandez-Orallo et al [7] proposed CoCoWa (Collaborative Contact-based Watchdog) method is a collaborative based on the diffusion of local selfish nodes alertness thus that information about selfish nodes is rapidly propagated. This approach reduces the time and increases the accuracy while detecting selfish nodes. Hussain et al [6] proposed selfish node detection which contains two major considerations. First, it focuses on the factors that induce appropriate nodes to act self-interestedly. Second, it proposed a slightly light-weight mechanism in terms of low energy consumption. This method consists of three main modules such as monitoring, data collection and detection. Tarannum and Pandey [11] explained detecting and removing the misbehaving node as well as improved the performance of the system by reentering the false detected node in network. This scheme consists of Data Gathering and Processing, Decision Making, and Response Operation. Gathering and Processing Module of the system collect data in two ways; first it locally runs a monitoring process to get the behavior information of neighbor nodes and secondly it exchanges this information with other nodes monitored information. This module is used as a data processing unit. Manchikalapudi et al [8] proposed that every node in the network monitors the activities of its neighbors and if any irregular action is detected it invokes an algorithm to conclude whether the assumed node is definitely selfish. This mechanism builds trust in the network by communications between some defense components. The components at each node are supervisor, aggregator, trust calculator and disseminator. Supervisor module monitors neighbors by passively listen to their communication. This module uses Passive Acknowledgement (PACK) mechanism that checks whether the neighbors really forward the packets or drops them. Aggregator module collects all the details of the communication that can be used to estimate the number of packets dropped. Trust calculator is determined by the percentage of packet dropped. The percentage is treated as fuzzy input variable and the output of the algorithm is trust level of a node.This technique is applicable for all nodes that are having data items of other nodes. When the data transmits from one node to other nodes, allocation of memory space of every node is responsible for communication. If one node is selfish in the network the memory space of selfish node doesn't take the data items of other neighbor. In favor of forwarding packets through the selfish nodes copy the data items of neighbor nodes into the memory space of selfish node explicitly and make the selfish node cooperative to other nodes.

3. PROPOSED METHOD

A lot of protocols are suggested to enforce corporation and to find misbehaving nodes. In network, two or three nodes can be easily identified and detected. Sometimes most of nodes act as selfish nodes and all nodes are detected and removed. Therefore, the remaining nodes will not perform well.The

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1397 - 1401
RECEIVED : 16/11/2016. PUBLISHED: 28/11/2016
November 28, 2016

existing scheme aims to Detect and Mitigate Selfish node (DMS) in MANETs. In this scheme, the selfish nodes do not co-operate other nodes. To overcome this problem, we propose Revival of Selfish nodes in clustered MANET. In this scheme, the selfish node cooperates with normal node. The node is acting s selfish because of saving the energy. If a selfish node is convinced about its necessity; selfish nodes automatically behave as the normal nodes. In this scheme, the base station sends a pilot message to the all nodes. Normal nodes will respond to the message.

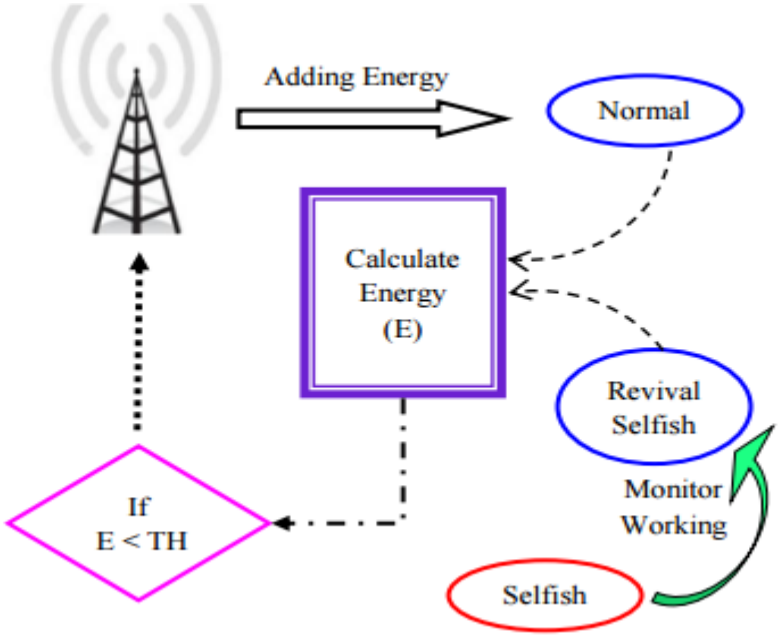

Fig.1. Revival of Selfish node Architecture

The selfish node does not respond. The normal nodes are combined together to form a cluster. Then base station is decided by the cluster head.The cluster head is selected based on energy. The node with highest energy is selected. The cluster members send information to the cluster head. The normal nodes send data from source to destination. The nodes are cooperating to all nodes; the residual energy is reduced automatically. If the residual energy is less than threshold, then the base station provides the energy. Therefore, the energy in the node doesn't get dried. So the normal nodes are not dead. Also, this process is monitored by the selfish node and the selfish nodes are converting to the good behavior node. Then the selfish nodes are cooperating to the all nodes. Fig 2 explains the process of Revival of selfish nodes. Initially the cluster is formed based on the distance and the cluster head is selected based on the node with high energy. The Data transmission nodes check the energy. If the energy is less than the threshold, the base station will add the energy. This process is monitored by selfish node and revival of selfishness then cooperates to all nodes in the networks.

4. RESULT ANALYSIS

The simulation analysis is performed using the network simulator. To ensure that the proposed scheme is more efficient than the existing scheme, we have performed simulations to assess some of the vital parameters. The parameters in the table 1 below show how the simulation experiments have been

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1397 - 1401
RECEIVED : 16/11/2016. PUBLISHED: 28/11/2016
November 28, 2016

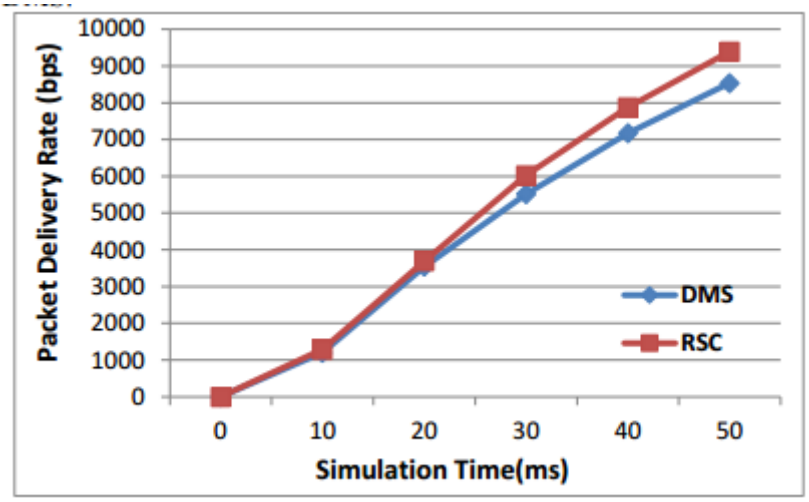

Fig.2. Packet Delivery Rate

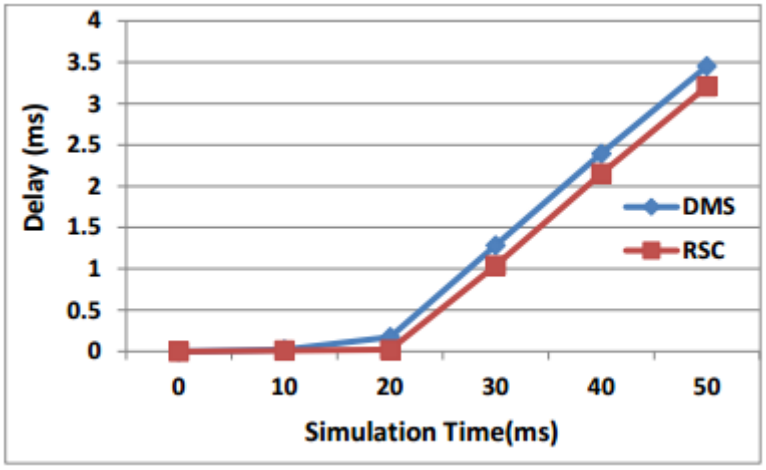

Fig.3. Average Delay

performed.The RSC routing performance is obtained by comparing it against the DMS protocols using the parameters packet delivery rate, throughput, loss and delay and residual energy.Throughput is the amount of data received by all the destinations in the network. The throughput is one of the main efficiency parameters used to assess the network.

CONCLUSION

This paper proposes Revival of Selfish nodes in clustered MANETs to encourage cooperation of the selfish node with the other nodes. A node generally behaves selfish in order to save its energy. When data transmission occurs, and when the energy of the node is below threshold, the base station automatically adds the energy. This process is monitored by selfish node and revival of selfishness then co-operates all nodes in the networks. Simulation results show that the proposed method has low packet loss ratio, packet delay and better packet delivery ratio, residual energy and throughput.

REFERENCES

[1] Samreen, S.; Narasimha, G., "An efficient approach for the detection of node misbehaviour in a MANET based on link misbehaviour," Advance Computing Conference (IACC), 2013 IEEE 3rd International, vol., no., pp.588, 592, 22-23 Feb. 2013.

[2] Talreja, R.; Jethani, V., "A vote based system to detect misbehaving nodes in MANETs," Advance Computing Conference (IACC), 2014 IEEE International, vol., no., pp.391, 394, 21-22 Feb. 2014.

[3] Hernandez-Orallo, E.; Serrat, M.D.; Cano, J.-C.; Calafate, C.T.; Manzoni, P., "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog," Communications Letters, IEEE, vol.16, no.5, pp.642, 645, May 2012.

[4] Djenouri D and N.Badache, "New approach for selfish nodes detection in mobile ad hoc networks," In Proceedings of the Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005., vol., no., pp. 288- 294, 5-9 Sept. 2005.

[5] Kargl F., A. Klenk, S. Schlott, and M. Weber, “Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks”, In Proceedings of the 1st European on Security in Ad-Hoc and Sensor Networks (ESAS 2004) Heidelberg, Germany, August 6, 2004.

[6] Hussain, M.A.; Nadeem, A.; Khan, O.; Iqbal, S.; Salam, A., "Evaluating network layer selfish behavior and a method to detect and mitigate its effect in MANETs," Multitopic Conference (INMIC), 2012 15th International, vol., no., pp.283,289, 13-15 Dec. 2012.

[7] Hernandez-Orallo, E.; Olmos, M.D.S.; Cano, J.; Calafate, C.T.; Manzoni, P., "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes," Mobile Computing, IEEE Transactions on, vol.14, no.6, pp.1162, 1175, June 1 2015.

[8] Manchikalapudi, V.; Yelisetti, S.; Surapaneni, R., "Detecting misbehavior nodes and trust levels in manets," Engineering Education: Innovative Practices and Future Trends (AICERA), 2012 IEEE International Conference on, vol., no., pp.1,4, 19-21 July 2012.

[9] Muthumalathi, N.; Raseen, M.M., "Fully selfish node detection, deletion and secure replica allocation over MANET," Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on, vol., no., pp.413, 415, 3-3 July 2013.