www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 1967-1970

IMPLEMENTATION OF SCFT ALGORITHM TO DETECT AND SOLVE GREEDY NODES IN WIRELESS SENSOR NETWORKS

Pritima Chhillar*, Ms. Smita,

Student, M. Tech
P.D.M. College of Engg. for Women, B'Garh, Haryana
pritimachhillar@gmail.com

Assistant Professor
P.D.M. College of Engg. for Women, B'Garh, Haryana

ABSTRACT

A Wireless Sensor Networks (WSNs) is a dynamic wireless network which consists of a network of sensor nodes, in which each node communicate and has to rely on others to relay its data packets. Since the sensor nodes are normally constrained by battery and computing resources, therefore some nodes may choose, not to cooperate by refusing to do so while still using the network to forward their packets. Greedy nodes avoid themselves from being asked to forward data packets and hence conserve the resources for their own use. The resources in WSN are limited like energy and bandwidth which motivate nodes to reduce their energy consumption. Detection these malicious nodes is a real challenge in WSNs. In this paper we propose a Self-Centered Friendship tree (SCFT) algorithm to detect and remove greedy nodes from the network. In this paper, we focus on the detection phase and tried to improve the rate of packet loss due to existence of greedy nodes. Simulation results that this algorithm is highly effective and can reliably detect and remove greedy nodes.

Keywords: *wireless sensor network, sensor nodes, greedy node, self-centered friendship tree.*

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consists of individual nodes that are able to interact with their environment by sensing or controlling physical parameter; these nodes have to collaborate in order to fulfil their tasks as usually, a single node is incapable of doing so; and they use wireless communication to enable this collaboration [1]. The features in WSN that make it different from other network; self-organize, low power, low memory, low bandwidth for communication, large-scale nodes, self-configurable, wireless, infrastructure-less. Therefore, WSN design must encounter these features in order to provide a reliable network. However each sensor node is equipped with its own sensor, processor and transceiver, so it has the ability of sensing, data processing and communicating with each other.

WSNs [2] may consist of many different types of sensors such as seismic, magnetic, thermal, visual, infrared, acoustic and radar, capable to monitor a wide variety of ambient conditions. A sensor node observes the condition values of a certain area like temperature, sound, vibration, pressure, movement or pollutants. The measured values are then forwarded to a data collection point that is in charge of their further processing. WSNs rely on collaborative work of large number of sensors. For this reason, they are deployed densely throughout the area where they monitor specific phenomena and communicate with each other and with one or more sink nodes that interact with a remote user. WSN are prone to failure and malicious user attack because it is physically weak, a normal node is very easy to be captured to become a malicious node or by inserting a malicious node in the network. The malicious or greedy nodes try to disrupt the operation of the network by fabricating or adding extra packets; they may mislead the operation of packet forwarding or will try to consume the resources of the nodes by making them believe that the packets are legitimate. The greedy node in order to preserve their energy or battery will not cooperate in the network operation resulting in the malfunction of the network operation.

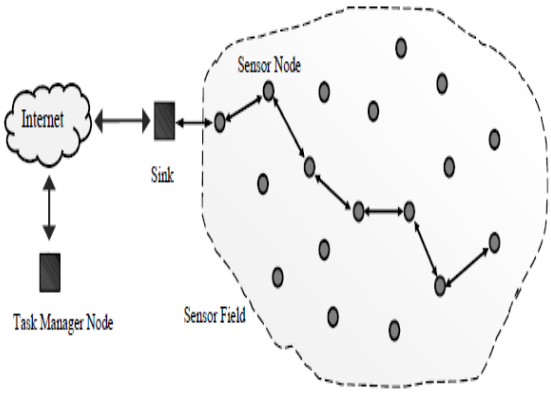
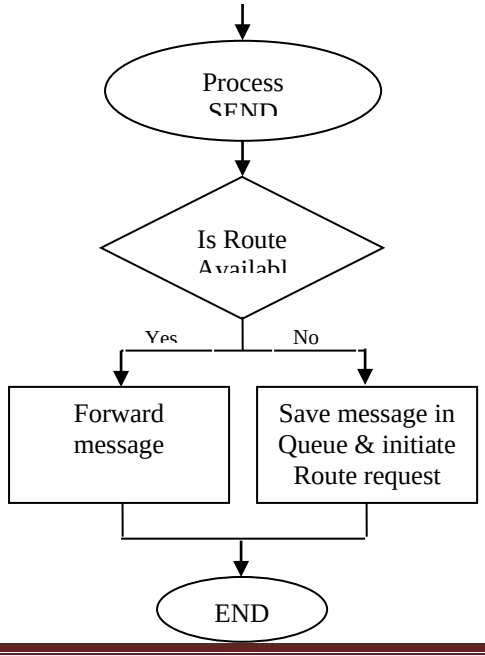


Figure 1. Components of Wireless Sensor Network

II. EXISTING WORK

The various techniques to handle greedy nodes can be classified into three main categories: reputation-based, credit-payment, and game theory-based techniques [4]. In the reputation-based, a large number of schemes belong to this category, with different implementations. One advantage of such schemes could be their quick convergence in detecting node misbehavior, especially in a large ad hoc network, due to increased information regarding a particular node's behavior. However, this approach has some drawbacks: they often assume that nodes that send reputation information about their peers are themselves trustworthy; and they are subject to collusion among nodes that misreport reputation information [5].In credit-payment techniques [4], every node gives a credit to other nodes, as a reward for forwarding the data. The acquired credit is then used to send data to others. The game theory-based techniques presume that all the nodes can determine their own optimal strategies to increase their profit. The game theory-based technique finds the Nash Equilibrium point [6] to increase the performance of the system. In this paper, we will discuss SCFT algorithm for detection and removal of greedy nodes



Flow Diagram

III. SIMULATION OF EXISTING WORK

Simulation is done using NS-2 (Network Simulator). Simulation of the existing work is performed over 13 nodes. Nodes in the network are placed at random places. In this scenario, there is a source node and many destination nodes that will broadcast the data to other nodes in the route after receiving it. When a greedy node comes in the route, it may or may not forward the packets. This leads to the loss of packets and these nodes can also terminate the network connection. The red color of the greedy nodes shows the failure of the network link or connection.

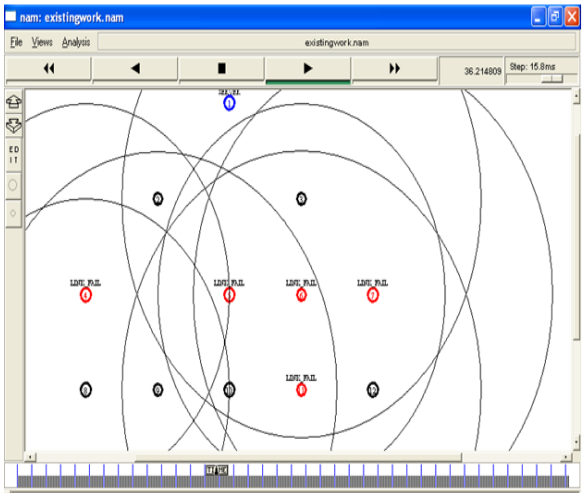


Figure 2. Greedy nodes terminates the network connection

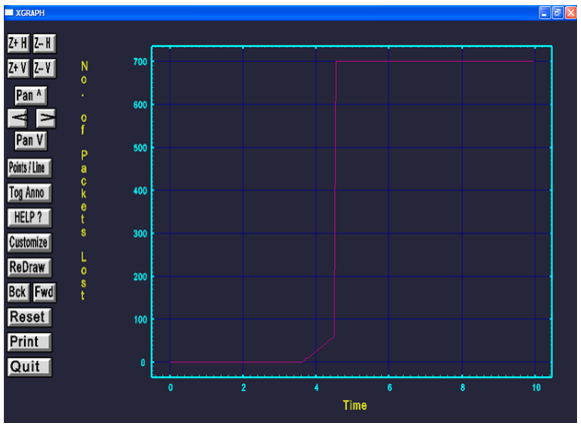


Figure 3. Number of packets lost over time

IV. PROPOSED ALGORITHM

The SCFT algorithm performs the following steps[3]:

1) Detect the greedy nodes.
2) Build the self-centered friendship (SCF) tree.
3) Allocating replication at a specific period or relocation period, each node executes the following procedure:-
   i. Each node detects the greedy node based on credit risk access.
   ii. Each node makes its own topology graph and built

it own SCF tree by excluding the greedy node.

iii. Based on SCF tree, each node allocates replication in a fully distributed mann

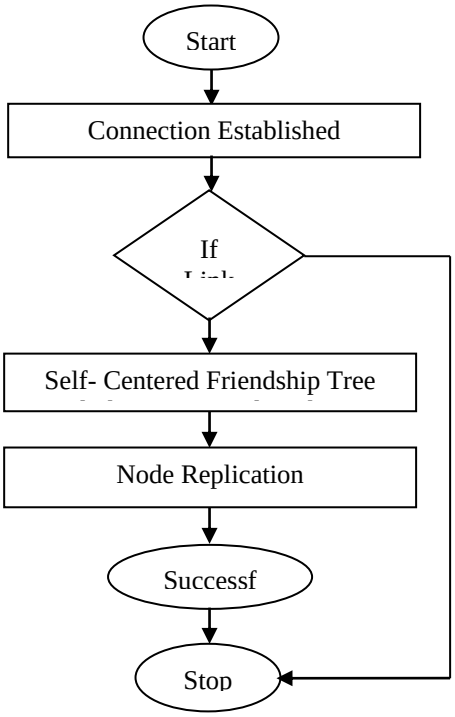


Figure 4. Flow chart of proposed algorithm

Main Algorithm(S, D, CR, SCFT, NC)
/*S is the source node and D is the destination node, */
/* CR is the credit risk factor */
/*SCFT is the Self-Centred Friendship Tree and NC is the child node */

{

1. Find all the nodes that occur in path between source and the destination. These nodes are representing by Node List (1 to N).
2. for i=1 to N
3. {
   IF (CREDIT RISK (CR) < THRESHHOLD VALUE)
   Show exist node is Greedy node.
   Else
   Node is not greedy node.
   }
4. for (first node to last node)
5. {

Contd ..

6. if (servers == SCFT) SCFT is root node.
7. else if (length of SCFT > NC)
8. then (move == xyz)
9. else fix the location of SCFT }
10. if (SCFT is allocated replication to NC)
11. SFCT store Unique Ids of each node.
12. {
13. if (unique id of each NC is available)
14. SCFT perform recovery and connection re-established.
15. else reconstruct SCFT and again perform replication.
16. }}}}

Proposed Algorithm

V. SIMULATION OF PROPOSED ALGORITHM

Due to existence of multiple greedy nodes in the network, they drop the packets and terminate the connection in order to conserve their own battery. energy of a node becomes less than the threshold energy, it changes its color. The low energy node is added in critical node list and another node with high energy is searched. The low energy nodes are replaced with high energy nodes in the network.

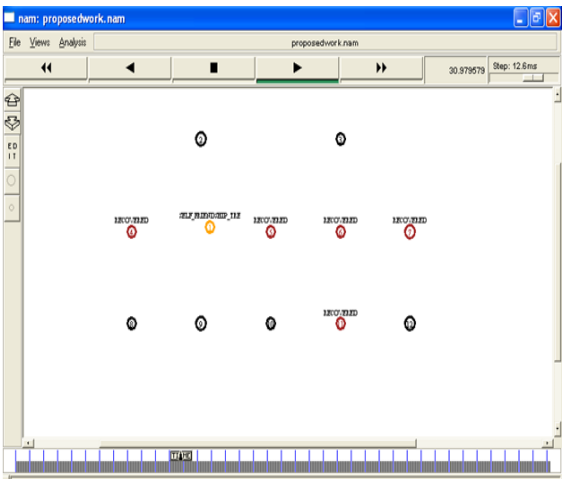


Figure 5. Nodes are recovered to re-establish the network connection

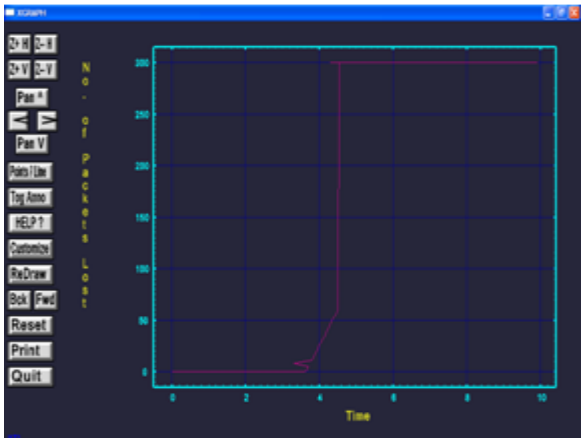


Figure 6. Number of packets lost over time

VI. COMPARISON OF EXISTING WORK WITH PROPOSED ALGORITHM

The comparison of the simulation results of existing work and proposed work shows that the number of packets lost have been decreased by a sufficient amount in the proposed work.

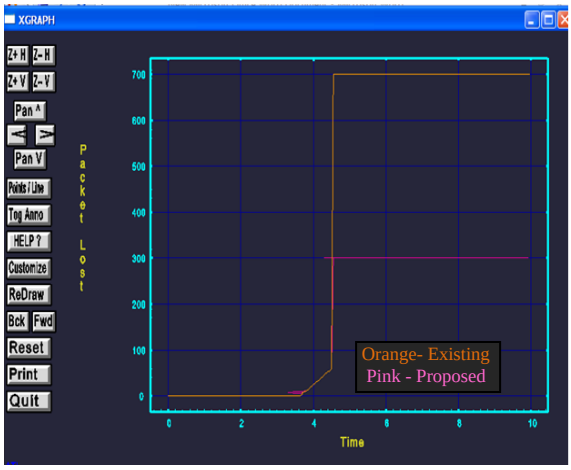


Figure 7. Number of packets lost over time

REFERENCES

[1] Stephan Olariu, "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University.

[2] S. Megerian and M. Potkonjak (2003) "Wireless Sensor Networks", Wiley Encyclopedia of Telecommunications. Wiley-Interscience, New York, January 2003

[3] Pritima Chhillar, Smita, Sunita, "Detection of Greedy Nodes over Wireless Sensor Networks" International Journal of Engineering Sciences & Research Technology (IJESRT), April 2013 ISSN: 2277-9655, 828-831.

[4] 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.

[5] Y.Liu and Y. Yang,"Reputation Propagation and Agreement in Mobile Ad-Hoc Networks," Proc. IEEE Wireless Comm. And Networking Conf., pp. 1510-1515, 2003.

[6] 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.