IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Detection of Greedy Nodes over Wireless Sensor Networks

Pritima Chhillar[*1]**, Ms. Smita**[2]**, Ms. Sunita**[3]

[*1,2,3] PDMCEW College, MDU, Rohtak, India

pritimachhillar@gmail.com

Abstract

Wireless Sensor Networks (WSNs) are ad-hoc networks, which consist of distributed devices using sensor nodes to collectively gather physical or environmental conditions at different places or sites. Sensor networks transmit data or information from different sensor nodes to a data repository on a server. The life span of the sensor network is limited to its left-over power. The wireless sensor nodes run through the batteries and since they are deployed in hostile environment their battery is usually un- chargeable and un-replaceable. There may exist some of the nodes do not forward the packets or data to other nodes in order to conserve their own resources such as energy, bandwidth and power. These types of nodes that act in a selfish manner to conserve their respective resources are called greedy nodes. This paper describes the various techniques to detect greedy nodes. It also discusses the key features of greedy nodes. The main goal of this paper is to propose a novel algorithm to detect such greedy nodes.

Keywords: Greedy nodes, Sensor nodes, Wireless Sensor Networks.

Introduction

Wireless Sensor Networks (WSNs) [1]-[2] have emerged as research areas with an overwhelming effect on practical application developments. They permit fine grain observation of the ambient environment at an economical cost much lower than currently possible. In hostile environments where human participation may be too dangerous sensor networks may provide a robust service. Sensor networks are designed to transmit data from an array of sensor nodes to a data repository on a server. WSN has potential to design many new applications for handling emergency, military and disaster relief operations that requires real time information for efficient coordination and planning.

Sensors are devices that give a measurable response when a change in a physical condition like temperature, humidity, pressure etc. occurs. WSNs may consist of different types of sensors such as seismic, magnetic, thermal, visual, infrared etc. to monitor a wide variety of ambient conditions. Though each individual sensor may have severe resource constraint in terms of energy, memory, communication and computation capabilities; large number of them may collectively monitor the physical world, disseminate information upon critical environmental events and process the information quickly.

The WSN provides an intelligent platform to gather and analyze data without human intervention as a result; they have a wide range of applications. The wireless sensor nodes are generally battery driven and due to their deployment in harsh or hostile environment their battery is usually un-chargeable and un-replaceable. Moreover, since their sizes are too small to accommodate a large battery, they are constrained to operate using an extremely limited energy budget.

A node in a network of this nature should aim to achieve the following main characteristics:

1) Low power consumption.
2) Low cost nodes that use cheap and commonly available batteries.
3) Small physical size to facilitate deployment.
4) Compliance to standards and regulations.
5) Single design for international markets.
6) Ability to maintain time synchronization with other nodes and hopping messages to destination.
7) Operate over wide temperature ranges especially for military applications or high temperature scenarios (i.e. a desert zones).
8) Fault tolerant.

Greedy Node

In forwarding the packets to other nodes costs extra energy and bandwidth which itself is a scarce resource in wireless sensor networks so, some of the nodes try to save their energy and bandwidth as much as possible by refusing to relay packets. Such non-cooperative behavior is called selfishness and such nodes are called selfish nodes or greedy nodes. Greedy nodes use the benefits provided by the resources of other nodes, but will not make available their own resources to help other nodes. They do not have the intention of damaging the network.

Types of Greedy Node

According to [3], there are three types of selfish or greedy nodes:

1) Selfish Node Type 1 (SN1) – These nodes cooperate in the DSR Route Discovery and Route Maintenance phases, but do not forward data packets.
2) Selfish Node Type 2 (SN2) – These nodes neither cooperate in the Route Discovery phase, nor in forwarding data packets. They only use their energy to transmit their own packets.
3) Selfish Node Type 3 (SN3) – These nodes act differently based on their energy levels.

Features of Greedy Node

Greedy nodes aim to extract maximum benefit from the network while trying to preserve their energy or battery life or bandwidth. A greedy node may or may not send the data packets in a proper way. It can do [4] any of the possible actions in the network:

1) It may switch off its power when it does not have active communication with other nodes in the network.
2) It may not forward all packets received from any of its surrounding neighboring nodes to its correct neighboring destinations.
3) Sometimes the node sends some packets and drops others.
4) When a request is passed, it does not forward the reply request on reverse route.

Related Work

Greedy Node Detection

The various techniques to handle greedy nodes can be classified into three main categories: reputation-based, credit-payment, and game theory-based techniques [5]. 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 [6].In credit-payment techniques [5], 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 [7] to increase the performance of the system.

Detection Techniques Description

1. Reputation based technique

In reputation based technique [6] a node receives one unit of credit for forwarding a message of another node and such credits are deducted from the sender or the destination. In this technique, a node monitors the transmission of a neighbour node in order to ensure that the neighbour node forwards others traffic. If the neighbour node does not forward others traffic, it is considered as greedy node and this uncooperative reputation is propagated throughout the network. Each node in the network runs the Confidant protocol, which observes the behaviour of neighbour nodes to detect misbehaviour such as dropping of packets. This protocol makes the nodes to run in a promiscuous mode. When the monitor finds any type of misbehaviour, it informs the reputation system, which has a table containing nodes and their respective ratings. If the number of times a node misbehaves exceeds a threshold value, the reputation system updates the node's rating. If a node's rating is below a threshold, it is considered as a malicious node. The reputation system maintains a list containing greedy nodes. When forwarding packets, nodes avoid next nodes on the list. When the reputation system detects a greedy node, it asks the trust manager to broadcast an alarm message on the network. Trust managers also receive alarms from other trust managers on the network. The path manager ranks the path according to the ratings of the nodes and deletes all paths that contain malicious nodes and discards route requests received from greedy nodes.

1.1. Watchdog mechanism

The watchdog [8] is one of the mechanisms which detect greedy nodes by running a misbehaving node locator on every host that maintains a buffer of recently sent packets. It overhears packets transmitted and compares it with the packets in the buffer to find if there is a match between the packets sent. If the packet has been sent from the buffer then watchdog removes the packet from the buffer. If there is any mismatch occurs and certain packets occupy the buffer for more than particular time, the watchdog increases a failure count for the node responsible for forwarding the packet. If the count increases the threshold value, the watchdog considers that host as a misbehaving node.

1.2. Pathrater method

A Pathrater [8] is a mechanism which maintains a rating for every host on the network. To choose a route that is considered to be reliable, it calculates a path metric by taking an average of the rating of the nodes on the paths and chooses the path with the highest metric.

If any node gets very low rating, it is considered as a greedy node and thus excluded from routing. It increases throughput by 17% in a network with moderate mobility and increases network throughput by 27%, with extreme mobility. Pathrater also has some drawbacks such as increasing overhead in the transmissions from 9% to 17% with moderate mobility. Pathrater is inefficient without the use of watchdog. Watchdog is necessary to be used in all the detection systems.

2. Credit-payment technique

Ad hoc-VCG [9] is one of the reactive routing protocols, which discovers the routing paths when a network node starts a session. Ad hoc-VCG uses a DSR like route discovery protocol which provides information about shortest paths to the destination node. The destination node calculates the shortest path and the VCG payments and sends this information back to the source. During the data transmission phase, the source sends packets along with electronic payments to the destination on the shortest path. Ad hoc-VCG is reliable against a single cheating node but it may fail in the presence of coalitions of nodes (coalition forming) which try to maximize their total payments. It provides truthfulness and assures cost efficiency.

3. Game theory based technique

Selfish nodes or greedy nodes are sometimes called as freeloaders [10] which get resources from the network but do not upload any resources to the network. Minimising the effects of freeloaders require the services of some external centralized authority. The inclusion of third party produces overhead in tracking, storing and processing the behaviour of other nodes. The algorithm called SLAC algorithm used to eliminate the use of external third party and minimises the overhead.

3.1. *SLAC algorithm*

It assumes that nodes want to use their abilities selfishly to increase their own utility in a greedy way. The algorithm [11] depends on Selfish Link and behaviour Adaptation to produce Cooperation (SLAC). According to the activities of each node, SLAC generates some measure of utility U (The number of files downloaded or jobs processed). Periodically each node (i) compares its performance against another node (j), selected from the network in a random way. If the utility Ui < Uj node then node i drops all current links to node j.

3.2. Generous TIT-FOR-TAT (GTFT) algorithm

The GTFT algorithm is used by the nodes to consider relay requests made by the neighbour nodes and to decide whether to accept or reject a relay request. It shows that GTFT [10] algorithm provide maintenance of Nash equilibrium in the network. For each node, the algorithm [12] defines the Normalized Acceptance Rate (NAR). It is the ratio of the number of successful relay requests generated by the node, to the number of relay requests made by the node. According to the NAR, selfishness can be decided.

Proposed Work

To detect and solve the problem of Greedy node over wireless sensor networks, we propose a greedy node detection algorithm that considers partial greediness and novel replication allocation techniques to properly cope up with greedy replication allocation.

The proposed algorithm will perform the following steps:

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 manner.

Conclusion and Future Work

Wireless Sensor Networks (WSNs) have been an active area of research over the past few years, because of their widespread application in military and civilian communications. These networks are highly dependent on the cooperation of all its nodes to perform networking functions. This makes it highly vulnerable to greedy or selfish nodes. This paper summarizes the key features of the greedy nodes that may exist in WSNs. This paper also presents some techniques of detecting selfish node behavior over WSNs. We will implement the proposed algorithm to solve the problem of greedy node over WSNs.

References

[1] F. Koushanfar, M. Potkonjak, A. Sangiovanni-Vincentelli, “Fault Tolerance in Wireless Sensor Networks”, Chapter 36, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems (Edited By Mohammad Ilyas and Imad Mahgoub), CRC Press, 2005. ISBN 0-8493-1968-4.

[2] Q. Wang, H.S. Hassanein and K. Xu, “A practical perspective on wireless sensor networks”, Chapter 9, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems (Edited By Mohammad Ilyas abnd Imad Mahgoub), CRC Press, 2005. ISBN 0-8493-1968-4.

[3] P. Michiardi and R. Molva, “Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks”, *Proc. of European Wireless Conference*, February 2002.

[4] S. Manju Priya, K.Thilagam, K.Rama, A.Jeevarathinam, K.Lakshmi, “A Novel approach for identifying greedy nodes in wireless sensor network by using EEGN algorithm”, IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 2928-293.

[5] 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.

[6] 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.

[7] 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.

[8] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad hoc Networks,” Proc. ACM MobiCom, pp. 255-265, 2000.

[9] L. Anderegg and S. Eidenbenz, “Ad Hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao, “Cooperation in Wireless Ad Hoc Networks,” Proc. IEEE INFOCOM, pp. 808-817, 2003.

[10] 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.

[11] 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.

[12] M.J. Osborne, An Introduction to Game Theory. Oxford Univ., 2003.