Journal of Engineering and Applied Sciences 9 (6): 231-236, 2014
ISSN: 1816-949X

Selfish Node Detection and its Behavior in WSN

Sujit Kumar Das, Bidyut Jyoti Saha and Pinaki Sankar Chatterjee
School of Computer Engineering, KIIT University, Bhubaneswar, India

Abstract: Now-a-days, selfish nodes is a huge problem in WSNs. In Wireless Sensor Network (WSN) communication, every node forwards the data packets to neighboring nodes and use up its battery power, bandwidth and memory space. All the nodes transmits packets to other nodes, according to their necessities in the ideal situation. Presence of selfish node in the network creates data communication failure and nodes do not transmits packets and utilize the network resources for its own profit but it refuses to share their personal resources for other nodes. Due to presence of selfish node in the network, the network is defective and the data communication between nodes is disrupted. It is an important issue to timely detect a selfish node and its behavior in wireless sensor networks. In this study, researchers have proposed an algorithm for detection of a selfish node in a given network topology.

Key words: WSN, selfish node, retransmission numbers, transmits, bandwidth

INTRODUCTION

Wireless Sensor Networks (WSNs) and Mobile Ad hoc Networks (MANETs) are collection of mobile nodes which are held responsible for transmitting packets over a wireless transmission medium. The WSN is the construction of nodes, from a few to several hundreds or even thousands where each node is associated with single or several sensors (Gupta *et al*., 2011; Sun *et al*., 2005). Each such sensor network node has characteristically several parts: A radio transceiver with an internal antenna or linking to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, regularly a battery or an embedded form of energy reaping. WSNs are gatherings of mobile nodes swapping packets over a wireless transmission medium. Since, packet transferring charges extra energy and bandwidth, balanced nodes may attempt to gather energy and bandwidth by greedily refusing to dispatch packets. Prevention, recognition and justification of selfishness among MANET and WSN nodes have recently received extensive attention. A Wireless Sensor Network (WSN) is made of spread sovereign sensors to check physical or environmental circumstances, like temperature, pressure, sound, etc and simultaneously the data is passed in the course of the network to a major location. WSN has the benefits of minor volume, little power consumption, small cost and dispersed, self-organizing features. Since, a universal sensing technology, the WSN is measured to be 1 of the 10 evolving technologies of the future living which has great likely for many applications, such as military investigation, industrial manufacture procedure nursing, environment nursing, disaster prediction, medical attention and harsh environment nursing and other fields.

Mobile ad hoc networks are widely used and they are infrastructure less. It can be installed without base station and dedicated routers and do not rely on extraneous fixed infrastructure. It can be established when it is required (Ahmad and Mishra, 2013; Wang *et al*., 2006). Each node in MANET, works as a router and maintain communication with other nodes. It is a multi-hop network. There are many MANET application in the world, for example it can be used in natural disasters, battle fields, etc. Due to presence of the selfish node MANET is affected during communication of data packets in case of accessibility of data. In these network, the nodes have limited battery power and bandwidth and each node needs the assistance of others for packet forward.

A selfish node uses all the network resources but it never gives away its own resources to other node. The network is disordered when most of the node behave like selfish node happens (Wang *et al*., 2006). The selfish node utilizes the network property like battery power, bandwidth, etc., for its own profit. If such a selfish behavior happens in the network, the network seems to be inactive.

Retransmission numbers of nodes happens due to unsuccessful packets received at the destination nodes. It is basically similar with automatic repeated request and it is responsible for resending of grouping of packets of nodes due to unreachable grouping of packets at the

Corresponding Author: Sujit Kumar Das, School of Computer Engineering, KIIT University, Bhubaneswar, India

destination nodes. Every data items of each node is responsible for forwarding data packets to neighboring nodes. Retransmission numbers of nodes occur due to lack of grouping packets received at the destination node. So that, the source node retransmits the data packets to destination node until the original grouping is reached at the destination node.

In order to proper detection of selfish nodes, this study proposes a new approach for cooperation of node's selfish behavior mechanism.

RELETED WORK

When a node becomes selfish in a network, the network does not properly work in order of relocating data in wireless sensor network. The nodes are not supportive in nature in case of relocating data because of selfish behavior.

A selfish node utilizes the total network resources for its individual profit. When these behavior happens among most of the nodes in the network, it may finally escort to disruption of network. The influence of selfish nodes create attention on the lead of service in MANETs and WSNs (Gupta *et al*., 2011). Features of selfish nodes are defined by Gupta *et al*. (2011):

- A selfish node discard routing messages or it may change the route request and reply packets by altering TTL value to minimum probable value
- A selfish node does not reply to hello messages, so that other nodes may not be capable to detect its existence when they want it
- A selfish node delay the RREQ packet up to the highest upper limit time. It will definitely escape itself from steering ways
- Selfish nodes may be the part of the routing messages but may not broadcast data packets

The cost of a packet is decided by numerous parameters, such as essential overall transmission power and the battery status of the intermediate nodes. The method to deal with this selfish behavior should be dependent on their concentration intensity in the network because of the impact they have on the network commotion will be different at different level of their concentration.

The difficulty of selfish nodes can be similar in ad hoc networks and WSN (Gupta *et al*., 2011). The major purpose for the selfishness is the deduction of power with time. As the time passes away, the nodes consume their battery power and in a disaster hit area or battle field area restoring is not technically feasible.

The selfish node is concerned to lower data accessibility and create high communication cost in terms of inquiry dispensation (Indumathi *et al*., 2013). Various selfish node discovery approaches are there to identify the nodes which do not contribute in packet forwarding but they fall short to detect the selfish nodes which does not allot replica for the reason of further nodes. The methods are able to detect selfish nodes, as assigning replica to other nodes. The methods are divided like detecting the selfish nodes and decreasing the effect of that nodes in mobile ad hoc network. The major attributes are counted, as the selfish nodes and number of replica share techniques. The selfish node detection algorithm that considers partial selfishness and novel replica allocation techniques to properly cope with selfish replica allocation.

The consequence of selfish nodes concentration (0-100%) on the various Quality of Service (QoS) parameters (Gupta *et al*., 2011). The QoS parameters is taken into contemplation are as follows:

- Throughput is defined, as proportion of packets acknowledged by the target to the number of packets directed by the source
- Hop count is stated, as the number of hops present between source and destination
- Packet dropped is defined, as amount of packets abandoned by the routers for many reasons
- Probability of reachability is defined, as division of probable accessible routes to the all likely routes among all different sources to all different destinations

Thus, behavior of network with the rise in consideration of selfish nodes:

- Due to selfish node the average hop count may increase
- Due to selfish node the packet drop rate may increase
- Due to selfish node the average throughput may decline
- Due to selfish node the probability of reach ability may decline

The study gives an overview of replica allocation techniques (Indumathi *et al*., 2013). The elasticity causes regular network partition, hence data accessibility in WSN and ad hoc networks is lesser than the fixed networks. The nodes which are not enthusiastic to broadcast packets and reveal their remembrance space are called self-centered nodes. The selfish node that does not allocate information for other node's purpose is called selfish replica allocation (Indumathi *et al*., 2013).

The selfish nodes assign data stuff that are highly retrieved by it and do not believe other nodes throughout

replica allocation. Selfish nodes lessen the data availability of extra nodes in query processing. The selfish nodes do not mollify neighbor nodes by giving mandatory information to them. The nodes can be divided into 3 types they are (Yoo and Agrawal, 2006):

- Non selfish nodes
- Fully selfish nodes
- Partially selfish nodes

Non selfish nodes behave like a normal node and allocate their memory space entirely for the use of another nodes. Non selfish node forwards packets to neighboring nodes successfully.

Fully selfish nodes do not allocate their memory space for the use of other nodes. Fully selfish node does not forward packets at all to other nodes. Partially selfish nodes allocate a smallest amount of their memory space for the use of other nodes and remaining for the benefit of own node (Buchegger and Le Boudec, 2002). Diminishing the property of selfish nodes will be significant to surge the data availability between the nodes. Replica allocation procedures are employed to lower communication cost while achieving good data availability.

To decrease the hop count and to increase the percentage of reachability of packets for transmission of packets in WSN due to selfish behavior of node, replica allocation technique is very efficient for cooperating the selfish node to other nodes. The replica allocation technique is used to make the selfish node cooperative in nature to other nodes. When the data transmits from one node to another nodes, sharing of memory space of each node is responsible for transmission. If one node is selfish in the network, the memory space of selfish node does not take the data items of other neighbor. For forwarding packets through the selfish nodes, simply copy the data items of neighbor nodes into the memory space of selfish node explicitly and make the selfish node cooperative to other nodes.

To overcome the selfish behavior of a node in a network, replica allocation helps to make the selfish node cooperative with neighbor and other nodes. If the selfish node becomes fully selfish node, the node does not forward any packets to other nodes. For cooperation, the selfish node makes replica of other neighbor nodes and store the data items into its memory space.

In wireless sensor network, the characteristic data of nodes selfish behavior including throughput, delay time, retransmission numbers (Chen *et al*., 2013).

To improve the accessibility of data between nodes, the data present in owner node is replicated to other nodes, as well known as replica distribution (Indumathi *et al*., 2013). In the replica distribution technique, the data present in memory space of one node copy to memory space of another node. So that, the node transfers data to other neighboring nodes successfully. The confidant algorithm to arrangement with selfish nodes (Buchegger and Le Boudec, 2002), the algorithm achieved the reputation value and in use to remove network method to punish non-cooperative nodes, the method exists a problem of malicious nodes failure behavior. Watchdog mechanism is a faulty mechanism for detection of selfish node and become the selfish node into normal node. Previously, all the algorithms are very much complex to detect selfish node and its behavior and the main problem is that making the selfish node into cooperative.

For handling the selfish node, simply modify the approach of the selfish node by replica allocation (Choi *et al*., 2012). In replica allocation, Contention Window (CW) is used for sharing of data items.

PROPOSED SYSTEM

The presence of selfish node creates a defective network, there is no assurance that they will not delay, split or make the packets or take them out of order. The protocols those put forward truthful communication over those networks use a combination of acknowledgments, retransmission of missing or broken down packets and checksums to provide that reliability.

Here, each node connected to other nodes and shares their data items for transferring of data packets to neighboring nodes and the cost is assigned to every linked node. Dijkstra's algorithm is used to find the shortest path from source to destination node. But, presence of the selfish node creates huge network failure. The original grouping of data packets are forwarded from source node can not reach at the destination node and some of the packets are missing or total packets are missed at the destination node. So, retransmission numbers of node occur between these nodes.

In this study, researchers are considering retransmission number of nodes to detect a selfish node. Each node itself retransmits data packets before successfully sending a packet (ND_j, j = 1, 2....n) and records of retransmission numbers (n) within a certain period (recordnum). By using ND_j and n, researchers calculate the average retransmission numbers (ND_i) of each node itself. After that calculate for the maximum value of average retransmission numbers (ND_{max}) in the period. Finally, it is judged whether retransmission numbers of node i to meet the Eq. 1, when it is satisfied the condition indicates that the node is a selfish node and if not the node is a non-selfish node and then repeating the process until the end of the result:

$$ND_i = \frac{\sum_{j=1}^{n} ND_j}{n},\ j = 1, 2.....n$$

$$\text{Decision} = ND_i/ND_{max} \quad \text{Decision}<\text{Threshold} \tag{1}$$

Threshold value is between 0-1. The threshold value is categorized to detect 3 types of selfishness of a node in a network. For finding better result, researchers set threshold value 0.8 is maximum for detecting partially selfish node. Researchers have taken 0.8 as an experimental value:

- If decision <0.8, then it is called as partially selfish node
- If decision >0.8 and <0.9, then it is called as fully selfish node
- If decision >0.9, then it is called as non-selfish

Proposed algorithm

Detection of selfish node algorithm:

Selfish_Node_ Detection (ND_{max}, ND_i)

// ND_{max} = Maximum average retransmission numbers within a certain period //
//j=1, 2....n //
1. For (each linked node N_k in G)//decision = ND_i/ND_{max}//
2. If (decision<$Threshold_{low}$)
3. N_k is marked as fully selfish
4. Else if ($Threshold_{high}$>decision>$Threshold_{low}$)
4. N_k is marked as partially selfish
5. Else
6. N_k is marked as non-selfish

Here from step 1-11, determines whether the node is a partially selfish node or is a fully selfish node or it is a normal node, according to the judgment of retransmission numbers of each nodes by the formula given in Eq. 1.

EVALUATION

Specifications: Matlab 2012a; Operating System Windows 8 (64-bit); Processor Intel (R) Core (TM) i5-3360M CPU@ 2.80GHz, 2801 MHz, 2 Core (s), 4 Logical Processor; Installed Memory (Ram) 8.00 GB.

To get the best result, detection mechanisms require the larger detecting rate. So, the threshold value is set to be between 0-1. The simulation process is done by Matlab. Researchers consider group of data packets that are sent to other neighbor nodes are constant, i.e., 200 packets and this is the maximum average retransmission numbers by every node. Researchers make the sample topology network G of Fig. 1 into matrix form and assign their cost into the matrix. Then, researchers have given source node and destination node and apply Dijkstra's algorithm. Then, researchers have found the shortest path from source to destination node from Fig. 1 and also find the path and the cost of the path. Here, researchers convert (Fig. 1) network into the matrix G given as:

$$G = \begin{vmatrix}
0\,2\,0\,4\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0; \\
0\,0\,4\,0\,9\,0\,3\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,1\,5\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,1\,0\,0\,0\,6\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,2\,2\,3\,4\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,2\,7\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,2\,0\,0\,0\,5\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,3\,0\,0\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,5\,7\,0\,0\,0\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,5\,6\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,2\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,2\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,4\,5\,6\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,2\,0\,0\,3\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,3\,0\,8\,0\,0\,0; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,3; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,10; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,4; \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0
\end{vmatrix}$$

After finding the shortest path, researchers are applying Eq. 1 to every node in the path between source and destination node and find out the presence of selfish node in the network. This process continues to check every related nodes.

From the observation, researchers can identify the node as a selfish node or non-selfish node by taking threshold value with the average retransmission numbers and maximum average retransmission numbers of the node as given in Eq. 1.

By the average retransmission number of nodes researchers are calculating the threshold values of each node and categorizing them as fully selfish (red), partially selfish (yellow) and non-selfish (green) as shown in Fig. 2.

In Fig. 3, researchers have shown the implementation result of maximum average retransmission number, average retransmission number of given 20 nodes. Researchers are finding the shortest path between [Node 1-8] and showing the behavior of all the nodes present in the given shortest path.

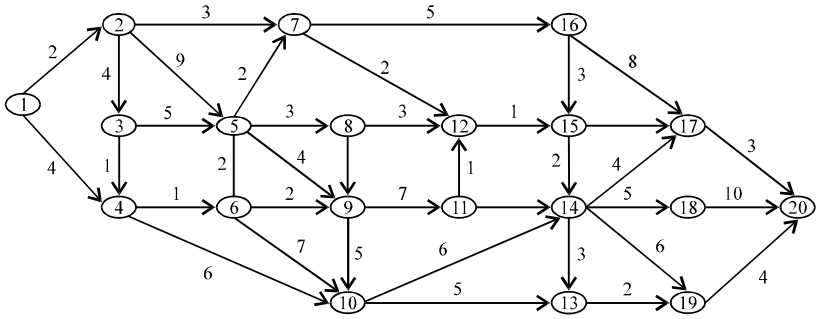

Fig. 1: Sample topology G

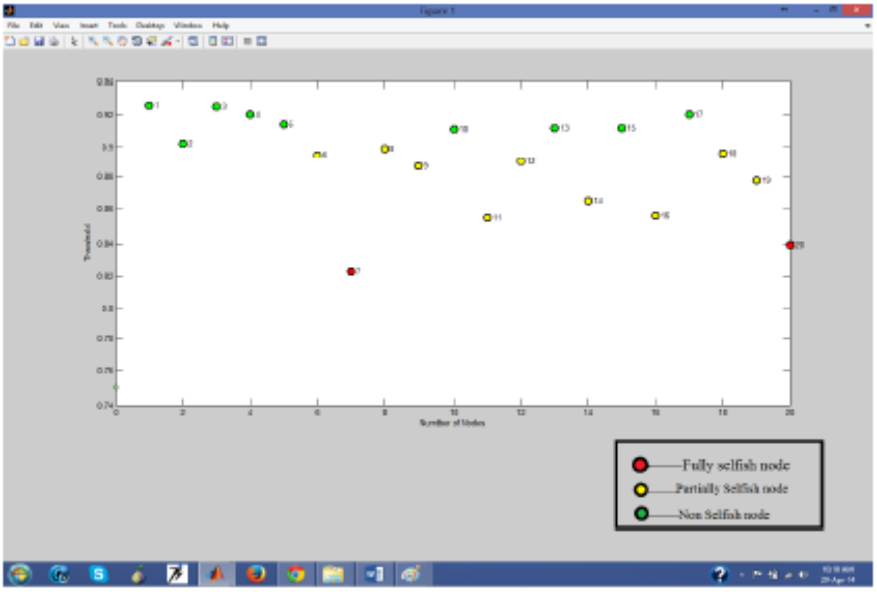

Fig. 2: Number of nodes vs. threshold

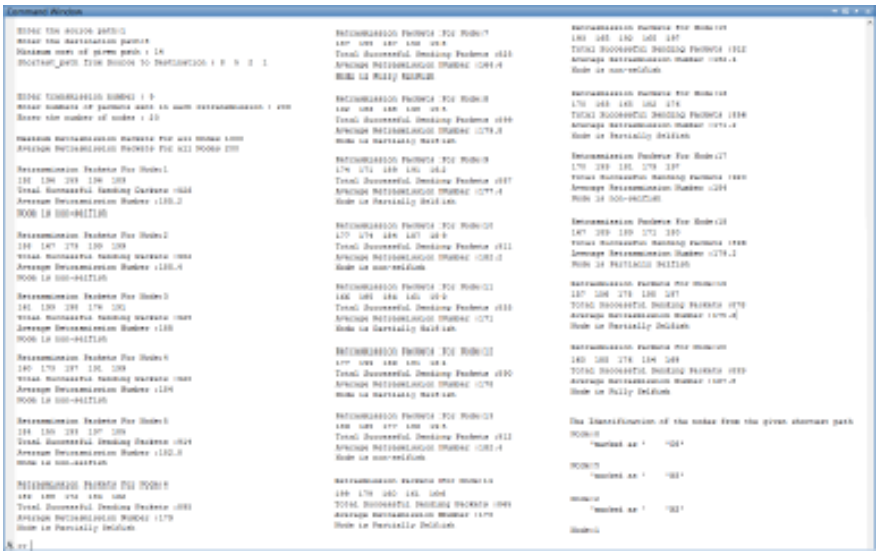

Fig. 3: Implementation result

Shortest path from source node 1 to destination node 8 from the Dijkstra's algorithm is given as shortest path from source to destination: 1, 2, 5 and 8.

In Fig. 2, researchers have shown which node is fully selfish or partially selfish or non-selfish of the network G given in Fig. 1. It is decided by Eq. 1. Comparing with threshold value.

Retransmission number can not be zero, otherwise it will give the empty detection graph and detection rate is zero. Retransmission number starts from 1 to onwards.

CONCLUSION

The algorithm that researchers have designed improve the detecting rate in the network. The selfish behavior creates the network failure and degrades the performance of the whole network in the wireless sensor networks due to non-cooperative nature to other nodes. The selfish node timely detection is very important issue for proper management of data communication in the network. The selfish node gives major impact on the network and the network is disrupted. To overcome the problem of selfish node and its behavior in WSN, researchers have to make the selfish node into cooperative nature for forwarding data packets to other nodes.

REFERENCES

Ahmad, M. and D.K. Mishra, 2013. Critical node detection in large scale mobile ad hoc networks. Int. J. Comput. Appl., 82: 34-38.

Buchegger, S. and J.Y. Le Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 9-11, 2002, Lausanne, Switzerland, pp: 226-236.

Chen, B., J.L. Mao, N. Guo, G.H. Qiao and N. Dai, 2013. An incentive detection mechanism for cooperation of nodes selfish behavior in wireless sensor networks. Proceedings of the 25th Chinese Control and Decision Conference, May 25-27, 2013, Guiyang, China, pp: 4021-4024.

Choi, J.H., K.S. Shim, S. Lee and K.L. Wu, 2012. Handling selfishness in replica allocation over a mobile ad hoc network. IEEE Trans. Mobile Comput., 11: 278-291.

Gupta, S., C.K. Nagpal and C. Singla, 2011. Impact of selfish node concentration in manets. Int. J. Wireless Mobile Networks, 3: 29-37.

Indumathi, K., N. Jayalakshmi and S. Kartiga, 2013. Selfish node detection using replica allocation techniques and SCF-tree in manet. Int. J. Adv. Res. Eng. Technol., 1: 78-82.

Sun, L.M., J.Z. Li, Y. Chen and H.S. Zhu, 2005. Wireless Sensor Networks. Tsinghua University Press, Beijing, China.

Wang, B., S. Soltani, J. Shapiro and P.N. Tan, 2006. Local detection of selfish routing behavior in ad hoc networks. J. Interconnection Networks, 7: 133-145.

Yoo, Y. and D.P. Agrawal, 2006. Why does it pay to be selfish in a MANET? IEEE Wireless Commun., 13: 87-97.