International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET2310128

Identification and Mitigation of the Selfish Node and Its Behavior in WSN

Dr. Md. Sirajuddin[1], T. Nandini[2], Ch.Venkata Deepthi[3], K. Hemalatha[4], Ch. Karthik[5]

[1]Professor, Head of the Department, Information Technology, Kallam Haranadha Reddy Institute of Technology, Chowdavaram, Guntur (Dt), Andhra Pradesh, India

[2, 3, 4, 5]B. Tech Students, Department of Information Technology, Kallam Haranadha Reddy Institute of Technology, Chowdavaram, Guntur(Dt), Andhra Pradesh, India

ARTICLEINFO

Article History:

Accepted: 01 March 2023
Published: 30 March 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
203-210

ABSTRACT

In Wireless Sensor Network (WSN) communication, every node transmits data packets to further nodes and spend its resources like battery power, CPU time and memory. In ideal situation all the nodes forward packets to other nodes according to their requirements .Presence of selfish nodes is a very big issue in WSNs. A selfish node doesn't forward packets and utilize to its own profit but it is hesitating using personal resources for others. If such activities occurs within most of the nodes in the network, the network is disrupted. Selfish behavior detection and punishment is an essential requirement in wireless sensor networks. In our paper we have described an efficient algorithm for detection and punishment of a selfish node and the necessary action to be taken if the node is a critical node.

Keywords - WSN, Selfish node ,Critical node, Replica Allocation , Retransmission Numbers.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) and Mobile ad hoc networks (MANETs) are groups of mobile nodes which are accountable for swapping packets over a wireless transmission medium. The Wireless Sensor Network(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[1],[4]. 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. Mobile nodes are gathered in WSNs to exchange packets across a wireless transmission media. Since sending packets consumes additional energy and bandwidth, balanced nodes may try to increase their energy and bandwidth usage by obstinately refusing to send packets. Recently, much effort has been paid to the prevention, identification, and defense of selfishness among MANET and WSN nodes. A wireless sensor network (WSN) is made up of dispersed

autonomous sensors that monitor environmental or physical conditions such as temperature, pressure, sound, etc. while concurrently transmitting the information to a distant point over the network. Small volume, low power consumption, low cost, and dispersed, self-organizing features are advantages of WSN. Since it uses universal sensing, the WSN is considered one of the ten developing technologies of the future of life and has significant potential for use in a variety of fields, including disaster prediction, harsh environment nursing, industrial manufacturing procedure nursing, and other fields. Mobile ad hoc networks are popular and need little infrastructure. It doesn't require any additional fixed infrastructure and can be setup without a base station or specialized routers. When necessary, it can be established[7],[5]. With a MANET, each node serves as a router and keeps in touch with the other nodes. This network has multiple hops. There are numerous MANET applications available worldwide. For instance, they can be used during natural catastrophes and conflicts. Since it uses universal sensing, the WSN is considered one of the ten developing technologies of the future of life and has significant potential for use in a variety of fields, including disaster prediction, harsh environment nursing, industrial manufacturing procedure nursing, and other fields.Mobile ad hoc networks are popular and need little infrastructure. It doesn't require any additional fixed infrastructure and can be setup without a base station or specialized routers. When necessary, it can be established[7],[5]. With a MANET, each node serves as a router and keeps in touch with the other nodes. This network has multiple hops. There are numerous MANET applications available worldwide. For instance, they can be used during natural catastrophes and conflicts.A selfish enjoys all the resources of the network but it never gives away its own resources to other node . When most of the node behave like this disorder of network[5] happens. The selfish node utilizes the network resources like battery power , bandwidth etc. for its own profit. If such a selfish behavior happens in the network , the network seems to be inactive.

The data contained in the owner node is replicated to other nodes as well[6], a process known as replica distribution, to facilitate the accessibility of data between nodes. In The data present in memory space of one node copies to memory space of another node using the replica distribution technique. in order for the node to successfully send data to other nearby nodes. The CONFIDANT algorithm to deal with self-centered nodes[10], algorithm obtained reputation value and in use to eliminate network method to punish uncooperative nodes, method exists an issue of malicious nodes failure behavior. A flawed mechanism called the watchdog detects selfish nodes and transforms them into regular nodes. Before, all methods are extremely difficult to detect. In order to appropriate detect selfish nodes and punish the nodes of refused cooperation, this paper proposes a new approach for cooperation of node's selfish behavior mechanism . Wireless Sensor Networks (WSN) is like the eyes and ears of the Internet of Things. It is the bridge that connects the real world to the digital world. And it is also responsible for passing on the sensed real world values to the Internet (WSN is thus involved with the hardware communication). The Internet of Things in a broad sense is like a brain, it can both store the real world data (in cloud services or databases) and can also be used to monitor the real world parameters, make meaningful interpretation and even make decisions based on the sensed data and also, the node in WSN has limit resources to support the DISOT method but IoT is responsible for the data processing, manipulation and decision making and can done DISOT protocol to detect the selfish node.

II. RELETED WORK

In the case of moving data in a wireless sensor network, the network becomes inappropriately dysfunctional when a node turns selfish. Because of their selfish

character, the nodes are not helpful for moving data. A selfish node makes use of the resources available across the network for personal gain. When the majority of the network's nodes exhibit this behavior, the network may eventually become disrupted. In this section[1], it is investigated how self-centered nodes' attention to detail affects the superiority of service in MANETs and WSNs.

Features of Selfish nodes: A selfish node may change the route request and reply packets by changing the TTL value to the minimum probable value, or it may abandon the routing post. These are some characteristics of selfish nodes [1].

- It doesn't respond to or transmit hello messages: A selfish node may not respond to hello messages, making it difficult for other nodes to detect its presence when needed.
- Intentionally delay the RREQ packet: A self-centered node may intentionally delay the RREQ packet for as long as the highest upper limit time allows. It will undoubtedly get away from the steering techniques.
- Data packet abandonment: Selfish nodes may participate in mail routing but may choose not to broadcast data packets.

Many factors, including the necessary overall transmission power and the intermediate nodes' battery health, determine the price of a packet. Because the impact they have on the network turmoil will vary depending on their level of concentration, the approach to dealing with this self-centered conduct should be dependent on their concentration intensity in the network. Selfish nodes can provide challenges in both WSN and ad hoc networks [1]. The gradual loss of power is the main motivation for selfishness. The nodes' batteries go down over time, and restoring in a disaster- or battle-affected area is theoretically impossible.

In terms of enquiry distribution, the self-centered node is worried about reducing data accessibility and increasing communication costs [6]. There are several methods for finding selfish nodes, however they can't find the selfish nodes that don't share replicas with other nodes because they don't participate in packet forwarding. Selfish nodes can be identified by the ways as they assign replicas to other nodes. In a mobile ad hoc network, there are throughout replica allocation. Selfish nodes lessen the data availability of extra nodes in query processing. The selfish nodes don't mollify neighbor nodes by giving mandatory information to them. The nodes can be divided into three types [8] they are

1. Non selfish nodes
2. Fully selfish nodes
3. Partially selfish nodes

many approaches for identifying selfish nodes and reducing their impact. The amount of replica share mechanisms and the selfish nodes count as the main characteristics. To effectively handle selfish replica allocation, the selfish node identification algorithm takes into account partial selfishness and innovative replica allocation techniques.

Identifying key nodes in a network can help reduce the complexity of the NP computational issue that large-scale MANET reliability computation poses. It is computationally challenging to identify essential nodes in the first place [7]

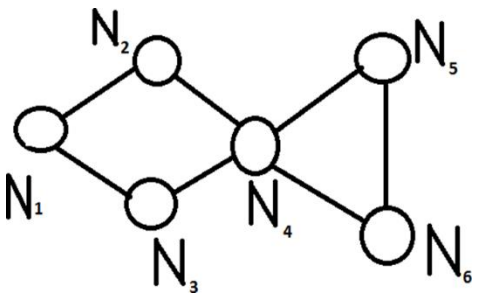

Figure 1 : Sample Topology G

The consequence of selfish nodes concentration [0-100%] on the various Quality of Service (QoS) parameters[1]. The QoS parameters is taken into contemplation are as follows:

- Throughput: Proportion of packets acknowledged by the target to the number of packets directed by the source.
- Hop count: Stated as the number of hops present between cause and goal.
- Packet dropped: Amount of packets abandoned by the routers for many reasons.
- Probability of Reachability: Division of probable accessible routes to the all likely routes among all different sources to all different destinations.

Thus with the rise in attentiveness of selfish nodes:

i. The average hop count may increase
ii. The packet drop rate may increase
iii. The average throughput may decline
iv. The probability of reach ability may decline

The paper gives an overview of replica allocation techniques[6]. 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 doesn't allocate information for other node's purpose is called selfish imitation allocation [6].

The selfish nodes assign data stuff that are highly retrieved by it and don't believe other nodes retransmission numbers (NAmax) in the period; Finally, it is judged whether retransmission numbers of node i to meet the equation (1), when it is satisfied the condition indicates that the node is a normal node, and if not, the node is a selfish node; continually repeating this process until the end of the result.

$$NA_i = \frac{\sum_{j=1}^{n} NA_i}{n} \qquad j=1, 2, \ldots\ldots n$$

Non selfish nodes assign their reminiscence space entirely for the use of additional nodes. Selfish nodes don't assign their reminiscence space for the use of other nodes. partly selfish nodes assign a least bit of their reminiscence space for the use of other nodes and residual for the advantage of personal node[9]. 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.

In Wireless sensor network, the characteristic data of nodes selfish behavior including throughput, delay time, retransmission numbers [3].

when an insufficient number of grouping packets are received at the destination node, so that the destination cannot reproduce the original packets forward by the source . The retransmission is basically alike with Automatic repeat request (ARQ) and it is the resending of packets which have been either dented or gone. It is a term that points to one basic mechanisms used by protocols working over a packet switched computer network to make available dependable communication.

III. PROPOSED SYSTEM

In the network where selfish behavior happens, are usually defective, there is no warranty that they will not holdup, break, or make the packets , or take them out of order. Protocols those offer trustworthy communication over those networks use a mixture of acknowledgments, retransmission of missing or broken packets, and checksums to provide that reliability. In this paper we are using retransmission number of nodes to detect a selfish node. Each node

itself retransmission numbers before successfully sending a packet(NAj , j=1,2,…n)and records of retransmission numbers(n) within a certain period (recordnum), using NAj and n to calculate the average retransmission numbers (NAi) of each node itself; after that looking for the maximum value of average

NA_{max}-NA_i< Threshold (1)

Threshold value depends on the amount of nodes present in the network. It varies according to the presence of nodes.

If NA_j =0 ,there is no successful packets forwarded toother nodes. It absorbs all the required packets for its own profit.

3.1. Punishing the selfish node and make the selfish node into cooperative nature

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 a network is disrupted , the nodes are not responsible for forwarding packets. In this technique all nodes are having data items of other nodes. where nodes N1; N2; N6 contain their memory space M1;

M2;...M6, respectively in figure 2. 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 , thememory space of selfish node doesn't 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.

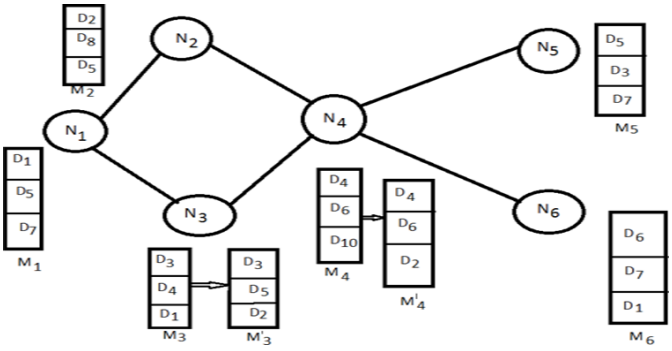

Figure 2 : Replica allocation to nodes in network G

j=1,2,…n)and records of retransmission numbers(n) within a certain period (recordnum), using NAj and n to calculate the average retransmission numbers (NAi) of each node itself; after that looking for the maximum value of average.

To overcome the selfish behavior of a node in a network G , replica allocation helps to make the selfish node cooperative with neighbor nodes and other nodes. If the selfish node becomes fully selfish node , the node doesn't 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.

3.1 Selfish node detection

The Wireless Mesh Network is modeled and the nodes in the network are deployed according to the architectural model. Numerous nodes will be participating in the MANET for forwarding and transmitting the data packets between the source and destination. All the nodes in MANET perform the routing function as mandatory and they must forward traffic, which other nodes sent to it. Among all the nodes, some of the nodes will behave selfishly; these types of nodes are called selfish nodes. Any node in MANET may act selfishly, which means using its limited resources only for its

own profit, since each node in a network has the resource constraints such as storage and battery limitations. This type of nodes likes to enjoy the profits provided by the resources of other nodes in the network. But it should not make its own resource accessible to others. These nodes intent to get the greatest benefits from the network while trying to preserve their own resources. The behaviors of the selfish nodes are shown below:

- Do not forward RREQ messages. This type of nodes does not forward the RREQ messages in MANET. It drops these packets to avoid being the route member for others.
- Do not forward data messages. This kind of selfish nodes will forward the messages, but it will not relay data messages and drop them. This misbehavior will impact the performance of MANET.
- Delayed forwarding RREQ messages. This kind of selfish nodes forwards the messages with a delay near the upper limit of timeout.
- Do not forward RREP messages. If this kind of selfish node exists in MANET, it will drop all RREP messages received by these nodes.

Existing explorations on selfish behaviors in a MANET mainly concentrates on network concerns. The main objective of this analysis is to enhance the performance of MANET by detecting these types of selfish nodes using RTBD technique. In this paper, the problem of selfishness is addressed by using record-based trust mechanism.

IV. EVALUATION

To get optimal results, detection mechanisms need the larger detecting rate . So the *Threshold* value is set to be 1 and the *recordnum* take 1500. The simulation process is done by MAT Lab . We arrange the nodes in a grid approach in the network. In this , one set of nodes is named as source (S) and another set of nodes is named as destination (D) as shown in figure 3. All the nodes forward packets to another nodes.

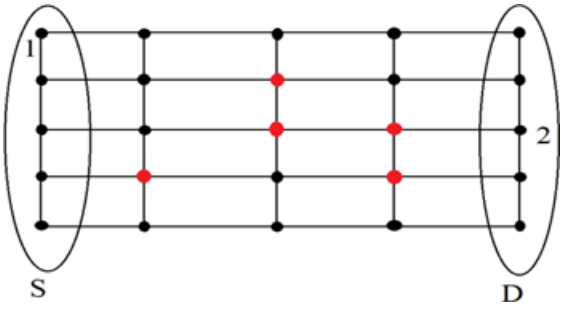

Figure 3: nodes are arranged in grid approach

The red dots are selfish nodes present in the network as shown in figure 3. When nodes from source(S) communicate data packets to nodes of destination(D) , it goes either through normal nodes or one or many selfish nodes. First time, one node of source(S) forward data packets to other nodes of destination(D) and check every possible path to reach at the destination node. Next time , 2nd node of source(S) forward packets to other nodes of destination(D) and check every possible path to reach at the destination node. This process continues for every node of source to destination and give the result of the selfish node present in the network in the form of retransmission number of each node. Performance of the selfish node present in the network as shown in figure 4.

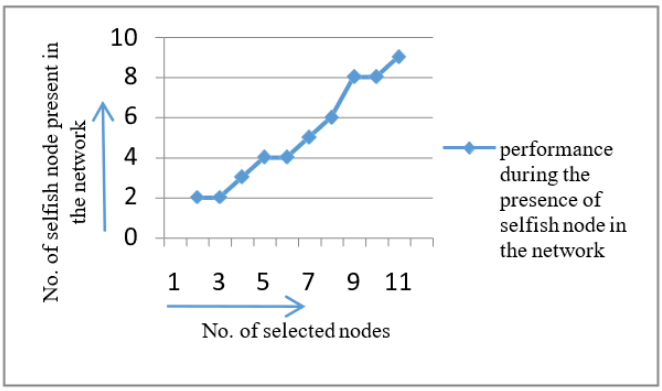

Figure 4 : performance analysis of selfish node vs. transmission of data in nodes.

In this figure 4, the result shows that when we transfer data between two nodes in every possible path for successful transmission , we found two selfish node. When we transfer data between five nodes, we found three selfish node present in the network.

For punishing the selfish node , simply change the strategy of the selfish node by replica allocation. In replica allocation , we use contention window (CW) for sharing of data items. We use 12 nodes where node 0 is the central coordinator node and remaining 11 nodes to build a 11 link simulation scenario.

V. CONCLUSION

We have designed an algorithm which will improve the detecting rate as well as improve the performance of the network .The selfish behavior of nodes results in deterioration of the performance of the whole network in the wireless sensor networks. The selfish node detection and punishment is very important issue and makes the nodes cooperative in nature in case of transferring data. When the selfish node becomes critical node , it will have a major impact on the network and the network is divided. To overcome the problem of network partitioning and forward packets between nodes successfully , replica allocation technique is used. Replica allocation technique gives better result for communication of data packets between nodes.

VI. REFERENCES

[1]. Shailender Gupta, C. K. Nagpal and CharuSingla, Impact of Selfish node Concentration in MANETs, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April, 2011.

[2]. Jerzy Konorski and RafałOrlikowski, A Framework for Detection of Selfishness in Multihop Mobile Ad Hoc Networks, Journal of Telecommunications & Information Technology, February,2009.

[3]. Bo Chen, Jian-Lin Mao, NingGuo, Guan-Hua Qiao, Ning Dai, An Incentive Detection Mechanism for cooperation of Nodes Selfish Behavior in Wireless Sensor Network , 25th Chinese Control and Decision Conference (CCDC), China, 2013.

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

[5]. Bo Wang , SohraabSoltani, Jonathan K. Shapiro, Pang-Ning Tan, Local Detection of Selfish Routing Behavior in Ad Hoc Networks, IEEE, Oct 2005

[6]. K.Indumathi, N.Jayalakshmi, S.Kartiga, Selfish node detection using replica allocation techniques and SCF Tree in MANET, IJARET, Mar 2013

[7]. Majid Ahmad,Durgesh Kumar Mishra, Critical Node Detection in Large Scale Mobile Ad hoc Networks, International Journal of Computer Applications ,Nov 2013.

[8]. Y. Yoo and D.P. Agrawal, “Why Does It Pay to be Selfish in a MANET,” IEEE Wireless Communication., Volume. 13, No. 6, December. 2006

[9]. Jae-Ho Choi Kyu-Sun Shim, Sang Keun Lee, and Kun- Lung Wu, Fellow, “Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network” IEEE Transaction on Mobile Computing, Volume 11, No.2, February 2012.

[10]. S. Buchegger, J. Y. Le Boudec, Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks), Proceedings of 3rd ACM International Sysposium on Mobile Ad Hoc Networking and Computing , 2002.

Cite this article as :

Harshwardhansinh K. Chauhan, Dr. Sheshang Degadwala, " Sensitivity Analysis of Project using Machine Learning , International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 10, Issue 2, pp.197-202, March-April-2023. Available at doi : https://doi.org/10.32628/IJSRSET2310128
Journal URL : https://ijsrset.com/IJSRSET2310128