An improved selfish node detection in the mobile Adhoc network with the consideration of malicious nodes present in the network

[1]Angeline Prasanna, [2]R.Asha

[1]*Head and Assistant Professor, CA and IT Department, Kamadhenu Arts and Science College, Sathyamangalam, Erode – 638503*

[2]*Mphil Scholar, CA and IT Department, Kamadhenu Arts and Science College, Sathyamangalam, Erode – 638503.*

[1]ashamphil15@gmail.com

Abstract

Objective/Background: The main goal of this work is to identify and remove the selfish nodes present in the mobile adhoc networks to improve the packet transmission rate considerably with the help of local watch dogs which would also communicated with the other nodes present in the environment.

Method/Statistical analysis: Communication based selfish node detection methodology is introduced in this work to prevent the high resource consumption cost in the network based on sharing the selfish node details with other nodes present in the environment. This communication would be established in case of establishment of communication between the nodes.

Findings: The experimental tests were conducted in the NS2 simulator environment with varying number of genuine nodes and the selfish nodes. The performance evaluation conducted were proves that the proposed methodology provides better result than the existing approach in terms of improved accuracy rate level.

Application/Improvements: From the findings it can proved that the proposed research work provides better performance results.

Keywords: Selfish nodes, Local watch Dog, Communication, packet transmission

1. Introduction

Mobile Adhoc network is an infrastructure less network where there would not presence of established communication between the different number of nodes. The route to transfer the packets would be established whenever it is required to transfer the packets. The route establishment might change often due to mobility of different number of nodes in the environment which might move from one location to another location often. The transfer of packet between different number of nodes required to have an connection establishment between the nodes to complete the successful transmission of packets. The transmission and reception of packet often requires to have well defines path between different number of nodes which nearest to each other.

The cooperative network is the one type of network which make ease of process of transferring packets between source to destination by finding the well defined cooperative nodes between them. The successful transmission of packets highly depends on the high cooperation among the number of nodes. Generally cooperation between number of nodes are established by contacting them. This cooperation enables mobile nodes to communicate with each other directly through which fast transmission of packet can be done. The nodes with minimum distance ie., neighbouring nodes are allowed to establish the communication between each other. However this cooperation between different types of nodes is required to spend multiple resources to reach the destination which is cost sensitive process.

Some of the nodes might refuses to transfer the packet which are received from the sender node to preserve their resources to save their cost which is called the selfishness behaviour of nodes. That is selfishness is defined as the refusing to transfer the packets between number of nodes to save their resources. This selfish behaviour might lead to hight packet lose rate which need to be concerned more to detect and remove it from the environment for the successful transmission of packets. The packet lose might cause the overall network failure due to corruption present in the received data.

It is essential to detect and remove the selfish nodes present in the environment to improve the performance of the network. One of the general approaches to detect and find the selfish behaviour of nodes are local watch dogs. Local watch dogs are the mechanism to detect and prevent the selfishness behaviour present in the environment. Each and every node would have their own local watch dogs to monitor and find the selfish behaviour of the nodes present in the wireless environment. Local watch dogs need to be monitor the whole environment continuously to predict the overall network behaviour performance.

Finding of selfish nodes needs to have high resource consumption and high level details of the nodes present in the mobile Adhoc environment. The less details present about the nodes present in the mobile Adhoc network might lead to the failure of detection of selfish in the environment. These problem needs to be concentrated more to improve the performance of detection of selfish nodes present in the environment in terms of packet loss rate. This finding process of selfish nodes would be done periodically to keep the mobile Adhoc network in the secured manner.

The main contribution of this work is given as: detecting of selfish nodes by transmitting the packet with the neighbouring nodes and predict the packet loss rate. Share the selfish information with the neighboring nodes whenever the communication established between them. The overall research of this detects the selfish nodes optimally and results with the reduced packet loss rate.

Allen B et al [1] introduced new methodology for detecting the selfish nodes present in the environment with the consideration of the transmission of multiple packets across the multiple nodes present in the mobile Adhoc network. By forwarding the multiple packets through multiple nodes, this methodology detects the variation present among the multiple packets that are transferred. Based on the variation, the network environment finds the selfish nodes with the help of analysis of the time stamp present in the various nodes. The game theory is used to predict the network malicious behaviour in terms of the multiple nodes processing output. The game theory applied in this work attempts to find the various nodes that are hiding their capacity of transferring the data. The overall result of this work leads to the better detection of selfish nodes.

Zhaoyu Gao et al [2] discussed the security issued that may arise while transferring the packets between different number of nodes in terms of the collaboration. The collaboration establishment between different numbers of nodes required to share their identity information where there is an possibility of collaboration might occur. This collaboration of the network nodes between is found by sharing the radio network transmission signals. Radio transmission signals that are transmitted across the different nodes would sense the variation present in the network nodes based on which selfish behavior would be predicted.

Ruiliang Chen et al [3] proposed a transmission oriented authentication mechanism in which the radio signal features would be monitored to predict the malicious present in the network environment. The strong adversary based network nodes would attempt to change the behavior of the monitoring packets which would be analyzed based on the signal strength. The strength might lead to the deficiency of construction of signals based on the transmitter location. The weaker signals can be overcome by strengthening the radio signals with the help of smoothening process. The smoothening process leads to the efficient reconstruction of signals and avoids the malicious signals efficiently.

Yao Liu et al [4] introduced the new methodology which attempts to share the packets across the multiple nodes based on the authentication mechanism which ensures the security for the sender who transfer their data. This authentication mechanism avoids the selfish nodes present in the environment considerably by transferring the packets across the multiple nodes in the secured manner. The authentication enables the users to avoid transmitting of signals through the selfish nodes in which the nodes capacity transfer would be increased in the efficient manner. These efficient reconstructions of signals are done by using the radio transmitting signals which would attempt to avoid the various malicious nodes present in the environment.

Beibei Wang et al [5] introduced the new mechanism for establishing the collaboration among the different sensor nodes in terms of the mobility across the nodes. This collaboration is achieved by sharing the resources in terms of the different user requirement. The network requirement sharing is achieved by establishing the communication between the number of nodes. And also this methodology attempts to avoid the collaboration control among the different types of nodes in terms of the various collaborative networks. This mechanism also increased the throughput value by finding and removing the malicious nodes. This process enables the various controlling strategies in terms of the most collaborative methods. The primary users of the network enable the methodology to prevent the different malicious attacks.

2. Communication based selfish node detection

Selfishness is the behavior of refusing to transmit the packets to other nodes which are received from the sender nodes. Selfishness behavior of nodes present in the mobile Adhoc network leads to more computational cost and increases the packet loss rate considerably. The transmission and reception of different types of packets needs to concerned more to reduces the packet loss rate considerably.

Selfish node detection in the mobile Adhoc network is the more complex process which requires high level data about the selfish node in order decide whether it is selfish node or not. Many of the nodes present in the environment fails to predict the selfish node behavior because of less availability of resources. This problem is overcome in this work by introducing the new methodology called the communication based selfish node detection in which the resource wastage is reduced considerably by transferring the selfish node information with multiple nodes.

The overall flow of this work is given as follows:

- Find the selfish node based on the packet transmission rate by using local watch dog
- Communicating the selfish node information with neighboring nodes
- Updating the local watch dog data base

The above flow is discussed detailed in the following sub sections and the architecture is given in figure 3.

A. SELFISH NODE DETECTION

Initially network formation is done by using the network simulation environment in which multiple network nodes would be created. In addition to that number of collaborative nodes and the malicious nodes would be created. The selfish node would be formed with the number of network nodes in terms of the various configuration parameters. In this work, the sender node would attempt to transfer the packets to the destination through various number of nodes. Whenever the sender node attempt to transfer the packet, the local watch dog of that particular node would start to monitor the behavior of other nodes present in the environment to predict the malicious behavior. This is done by monitoring and comparing the number of packets that are transmitted and the number of received across the various mobile network nodes. The selfish nodes present in the environment would refuses to transfer the packet to destination to save their resources which will increase the packet loss rate. The local watch dog will find the variation between the number of packets transmitted and the number of packets received with the concern of packet flow direction.

If the selfish node was found by the local watch dog than the database of selfish node information would be updated in order to prevent the future transmission of packets through the selfish nodes. The selfish node detection behavior is indicated by using the three types of states which are listed as follows:

- PosEvent
- NegEvent
- NoDetEvent

PosEvent: PosEvent is used to indicate the successful detection of selfish nodes present in the environment. Whenever the local watch dog of the particular node detects the selfish node then the local watch dog status would be updated as the PosEvent. Thus the future transmission of packets to the particular selfish node would be prevented in future through which the packet loss rate would be reduced considerably.

NegEvent: NegEvent is used to indicate the selfish node is found as non malicious node. This situation might occur in case of presence of less detailed information about the selfish node. This case of negative detection of the selfish node would increase the packet loss rate in which selfish nodes would not be eliminated from the network.

NoDetEvent: NoDetEvent is used to indicate the incapability of detection of selfish node behavior because of less availability of resources and the missing values of information about the selfish node present in the environment. This NoDetEvent indicates the incapability of local watch dogs to detect the selfish node which might increase the packet loss rate considerably.

Thus the local watch dog status would be updated as like above mentioned attribute values in which selfish nodes are found based on packet transmission and reception rate. The nodes present in the network environment wouldn't transfer the packets to selfish nodes present in the network environment to prevent the packet loss rate.

However, nodes with NoDetEvent and NegEvent would to continue to transfer the packet through the selfish nodes which would lead to the packet loss rate.

Communicating the information about the selfish nodes with the other present in the network environment would lead to considerable network failure which needs to be prevented by informing the network node information to other nodes present in the network. The transferring selfish node information to the other nodes present in the network environment might lead to the high computational cost and thus requires high amount of resources to be spent. The selfish node information communication with other nodes with less computational cost leads is discussed detailed in the following sub section.

B. Communicating selfish node information to other nodes

The selfish node information would be communicated with other nodes in the environment whenever the contact is established between the different network nodes present in the environment. Consider there are three nodes namely 1, 2, and S reside in the network model. S is an selfish node which cannot predict the selfish node behavior of other nodes present in the environment. When node 1 transmits packet to selfish node, its local watch dog might predict the selfish node behavior in terms of various network nodes present in the environment. Then local watch dog will update the database and the network information would be communicated with other nodes. This is done whenever the communication is established. When the node 1 attempts to transfer the packets to node 2 present in the network environment then the local watch dog update would transfer the details to the node 2's local watch dog.

This communication based network sharing might lead to the update of the network details present in the network environment in terms of various nodes. This communication would occur whenever the new packets to be transmitted. The local watch dog information would be updated based in the various network learning parameters.

However this contact cannot always established for the packet transmission. Thus he probability of occurrence of neighboring node would be updated based on the various network learning parameters. These neighboring nodes would be contacted whenever the resources are available and there is packets to be transmitted. These network sharing leads to the efficient transmission of packets across various nodes in terms of the large volumes of packet transmission.

C. Updating local watch dog status

Whenever the node finds the selfish then it will stop the monitoring process and will continue the data transmission without predicting the presence of selfish nodes. These updation local watch dogs status would required to have in case of presence of new selfish nodes in the environment. However sometime genuine nodes may act as the malicious nodes which need to preserved in case of presence of various selfish nodes.

This problem is resolved by introducing periodic updation of local watch dog data base which attempts to update the status of nodes periodically. This updation further requires to be spending some resources present in the network environment in terms of presence of various network nodes.

3. Experimental results

The experimental tests were conducted in the network simulation environment with presence of various number of nodes. The performance evaluation were conducted in terms of parameters called the detection time and the diffusion time which is calculated and evaluated detailed in the following sub sections:

A. Detection time

Detection time is the computation time which is consumed to detect the selfish nodes present in the environment in terms of various number of nodes. The detection time should be less for the proposed methodology for the better performance of system. The detection time performance evaluation were illustrated in figure 1.

In figure 1, detection time evaluated for the proposed methodology in terms of varying number of nodes are illustrated. In the x axis number of nodes is given whereas in the y axis detection time in seconds are given. From this graph, it can be proved that the proposed methodology provides better result than the existing approach in terms of the reduced detection time.

B. Diffusion time

Diffusion time is defined as the total time taken to combine and update the varying selfish node values present in the different nodes local watch dogs database together. The diffusion should be less to prevent the nodes to transfer the packets to the selfish nodes. The graphical representation of the diffusion time is given in figure 2, diffusion time evaluated for the proposed methodology in terms of varying number of nodes is illustrated. In the x axis number of nodes is given whereas in the y axis diffusion time in seconds are given. From this graph, it can be proved that the proposed methodology provides better result than the existing approach in terms of the reduced diffusion time.

Figure 1. Detection Time

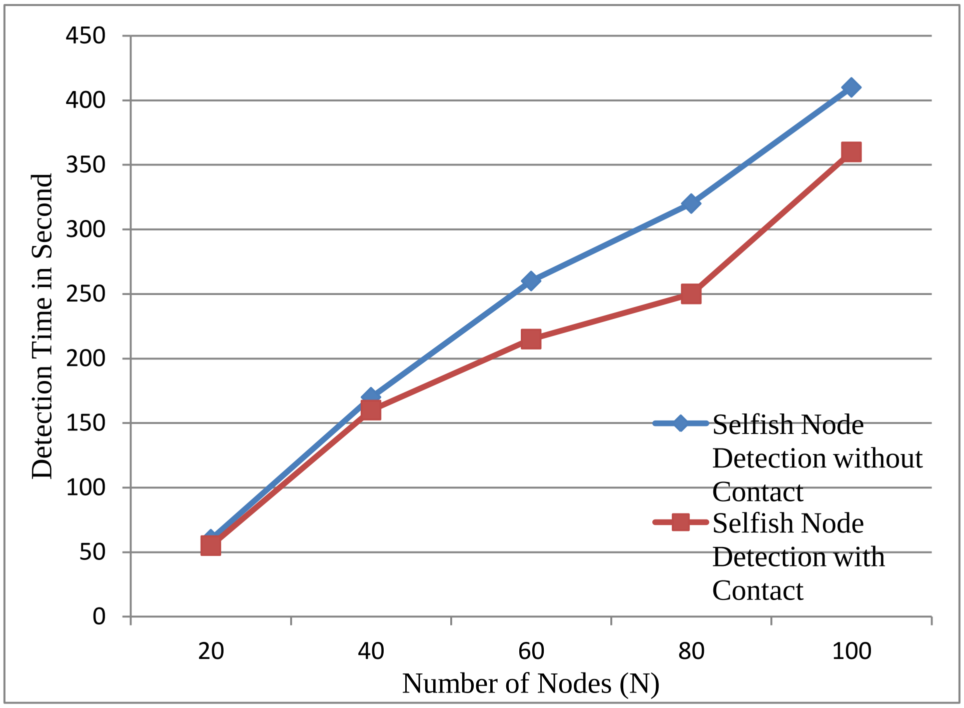


Figure 2. Diffusion Time

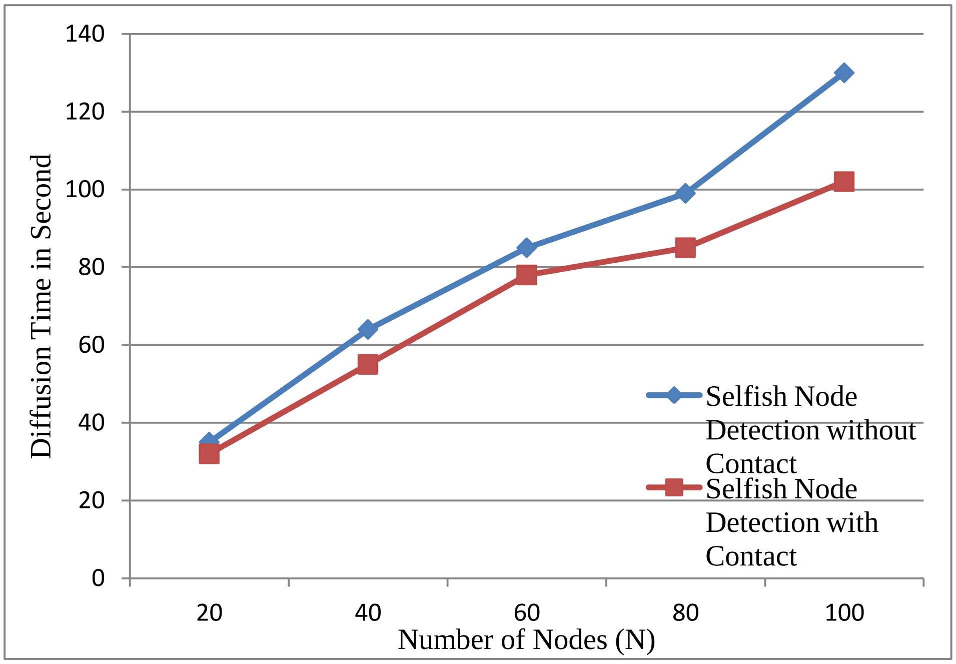
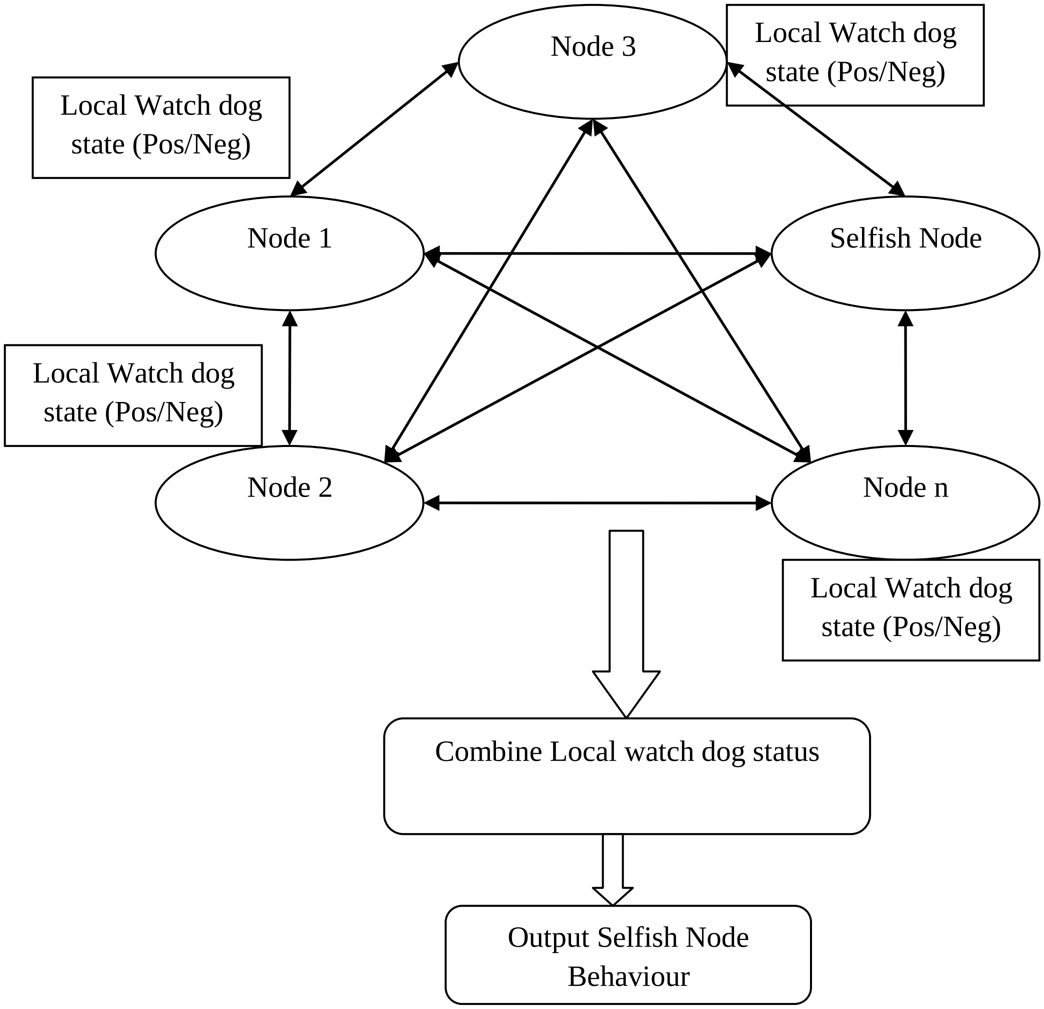


Figure 3. Architecture Diagram


Node 3
Local Watch dog state (Pos/Neg)
Local Watch dog state (Pos/Neg)
Node 1
Selfish Node
Local Watch dog state (Pos/Neg)
Node 2
Node n
Local Watch dog state (Pos/Neg)
Combine Local watch dog status
Output Selfish Node Behaviour

4. Conclusion

Selfish node detection plays a key role in the mobile Adhoc network which requires to spend more computational resources for detecting the selfish nodes. In this work communication based selfish node detection is introduced which founds an selfish node present in the network with less computational cost and reduced usage of resources. This selfish node detection needs to be handled with more concern for providing the secured environment for transferring packets among different number of nodes. The experimental tests were conducted in the network simulator environment from which it is proved that the proposed methodology provides better result than the existing approach in terms of better computational time and diffusion time.

5. Reference

1. A.B. MacKenzie, S.B. Wicker. Stability of Multipacket slotted aloha with selfish users and perfect information. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. USA, 2003, 30, 1583-1590.
2. Zhaoyu Gao, Shanghai Jiao, Shanghai China, Haojin Zhu, Shuai Li, Suguo Du. Security and Privacy of Collaborative spectrum Sensing in Cognitive Radio Networks, Wireless Communications. *IEEE*. 2012; 19(6), 106-112.
3. Ruiliang Chen, Jung-Min Park, Reed.Defense against Primary User Emulation Attacks in Cognitive Radio Networks.Selected Areas in Communications. *IEEE.* 2008; 26(1), 25-37.
4. Yao Liu, Peng Ning, Huaiyu Dai. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. Security and Privacy (SP), 2010 IEEE Symposium. 2010, USA, 286-301.
5. Beibei Wang, K.J.R Liu, T.C. Clancy. Evolutionary cooperative spectrum sensing game: How to collaborate?. Communications, *IEEE Transactions*. 2010; 58(3), 890-900.