Singaporean Journal of Scientific Research

Singaporean Journal of Scientific Research(SJSR)
Issue of International Journal of Applied Sciences (IJAS)
Vol.7.No.2 2015 Pp.416-420
available at :www.iaaet.org/sjsr
Paper Received : 29-09-2015
Paper Accepted: 27-10-2015
Paper Reviewed by: 1.Prof. Cheng Yu 2. Dr.M. Akshay Kumar
Editor : Dr. Chu Lio

A STUDY ON DETECTION OF SELFISH NODES AND PROVIDING HIGH PERFORMANCE IN MANET

M.Senthil
Associate Professor, Head of the Dept. of CSE
DEAN (School of Computing)
Christ College of Engineering & Technology,
Pondicherry, India

S.Banu
M.Tech, Dept. of CSE, Christ College of Engg. & Tech.,
Pondicherry, India

V.Suganya
M.Tech, Dept. of CSE, Christ College of Engg. & Tech.,
Pondicherry, India

D.Suganya
M.Tech, Dept. of CSE, Christ College of Engg. & Tech.,
Pondicherry, India

Abstract

In mobile ad-hoc networks the co-operation of all mobile nodes is very important in order to preserve the network performance. The mobile nodes should voluntary cooperate in order to work properly to and to achieve the high data transmission to greater extend. But some nodes they could not able to cooperative with the other nodes. That is some nodes will not forward the data to the other nodes in the network, some nodes will replica the data within it, some nodes can change the data and send the wrong data packet to other and many more fake process in the network. It is all because of the selfish behavior of those nodes. And thus that kind of nodes is called as the selfish node which seems to have any one of the selfish behavior as mentioned above. Those selfish nodes could not pave the way to construct a system with energy efficiency and load balancing also. Consequently the overall network performance could be seriously affected. The optimal method is recommended for constructing a network in to provide the network performance.

Keywords: Mobile nodes, selfish nodes, selfish behavior, network performance.

1. INTRODUCTION

Wireless network enables communication between computers using standard network protocols, without network cabling. These networks use radio waves or microwaves as a communication medium. These networks are widely used nowadays because of their great advantages over a wired network.

Wireless Networks can be classified into two main categories:

- Fixed Infrastructure Wireless networks
- Infrastructure less Wireless Networks

1.1 A Fixed Infrastructure Wireless network

It provides communication among wireless nodes through the Access Point (AP), not directly. The access points also works as a bridge.

1.2 An Infrastructure less Wireless Network.

It does not have any fix infrastructure for the communication. Each node can communicate directly with other node and there is no requirement of the access point. An important thing about these networks is that these networks do not have routers, the wireless nodes work as routers. These networks don't have any fixed or static topology.

A mobile ad hoc network is an autonomous collection of mobile devices such as laptops mobiles etc. They communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure.

This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications. Application scenarios include, but are not limited to: emergency and rescue operations, conference or campus settings, car networks, personal networking, etc.

A mobile Ad hoc network consists of mobile nodes that use wireless transmission for communication. MANET is an infrastructure less wireless network. In these types of networks the nodes can move from one place to another. The motion of the mobile nodes may be random or periodical. Thus, these networks have no fixed infrastructure, no fixed configuration and other controlling device such as router etc.

The setup or deployment of these networks is very easy because these networks don't have a fixed infrastructure or a fixed topology also they have a very less setup time. The routers are free to move randomly. They plays important role in real life applications such as military applications, home applications etc.

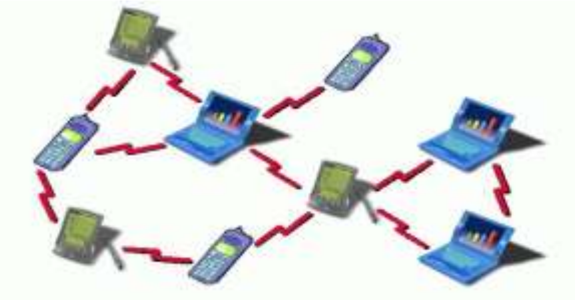

Figure 1: MANET

The basic technologies that are considered as the core for collaborative types of networks are mobile ad-hoc networks (MANETs). Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide services and applications in contexts such as mobile ad hoc networks. The cooperation on these networks is usually contact based. Mobile nodes can directly communicate with each other if a contact occurs (that is, if they are within communication range). Supporting this cooperation is a cost intensive activity for mobile nodes. But the major drawback is the selfishness of nodes. The overall network performance could be seriously affected by the selfish behavior of nodes.

2. SELFISH NODE DETECTION METHODS:

2.1 MOTIVATION OR INCENTIVE BASED APPROACH

This Motivation or incentive based approach tries to motivate nodes to actively participate in the forwarding activities if that node fails to take part in the data transmission. This approach is usually based on virtual currency and/or game theory models.

This approach has a disadvantage that all nodes should be provided with large amount of energy to carry out the data transmission. So this approach does not able to provide the energy efficient system.

2.2 THE DETECTION AND EXCLUSION APPROACH

The detection and exclusion approach is a straight-forward way to cope with selfish nodes. This approach eliminates the particular node in the network. This provides the disadvantage that load in the network cannot be balanced if that node is fully eliminated from that network and also routing process cannot be done properly if so the node is entirely taken from the network.

2.3 2ACK METHOD

The acknowledgement-based 2ACK scheme is suggested to mitigate the adverse effects of misbehaving nodes. The basic idea of TWOACK scheme is that, when a node forwards a data packet successfully over the next hop, the next-hop-link’s destination node will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully.

The 2ACK scheme is a network-layer technique to detect misbehaving links and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

2.4 S-2ACK METHOD

Another acknowledgement-based scheme, termed as S-TWOACK is a derivative of the basic TWOACK scheme, aimed at reducing the routing overhead and achieves the performance improvement along with the problem of false-alarms due to genuine TWOACK packets lost. The Selective TWOACK (S-TWOACK) scheme is different from 2ACK. mainly, each TWOACK packet in the S-TWOACK scheme acknowledges the receipt of a number of data packets, but a 2ACK packet in the 2ACK scheme only acknowledges one data packet. With such a change, the 2ACK scheme has easier control over the trade-off between the performance of the network and the cost as compared to the S-TWOACK scheme.

2.5 SECURE INTENSIVE PROTOCOL:

Secure Intensive Protocol is a credit-based method that uses the credit as the incentive to stimulate packet forwarding. Here each mobile node has a security module and they deal with the security related functions. The credits of the node increases and decreases depending on the forwarding behavior of the node. Whenever a node is initiating or forwarding a packet, first node will pass it to SIP module for processing.

SIP is session based and consists of four phases, 1) Session Initiation 2) Session Key Establishment 3) Packet Forwarding And 4) Rewarding Phase. The advantages of the scheme are SIP is routing independent; it is session based rather than packet based; unauthorized access is not allowed. The disadvantage of SIP is that it implemented on hardware module so each node should possess a hardware module.

2.6 CORE METHOD

The reputation-based CORE (Collaborative Reputation) Mechanism to detect the selfish nodes, improves the coordination among nodes. For this purpose, it makes use of reputation mechanism and collaborative monitoring. The basic components used in the CORE mechanism are 1) reputation table and 2) watchdog mechanism. The CORE mechanism will prevent the DOS attacks, it is impossible for a node to decrease another node's reputation maliciously because there is no negative rating spread between nodes. The CORE suffers from spoofing attacks; it cannot prevent colluding nodes from distributed negative reputation.

2.7 WATCHDOG MECHANISM

The watch dog is a technique used to detect the misbehaving and selfish nodes. It overhears wireless traffic and analyze whether the neighbor node is having the selfish behavior by using the local watchdog. Here in this method we have to appoint the watch dog for all nodes in the network that acquires lots of energy and also the transmission of data is not so accurate and thereby performance of the system is being reduced. The watchdog technique can fail by giving false positive or false negative which degrades the system performance of the system by relaying only to local watchdog. It also takes much time to detect. So in order to overcome this problem it uses a method called collaborative contact based watchdog method.

2.8 COCOWA METHOD

It has two methods they are:
LOCAL WATCHDOG METHOD:
The Local Watchdog has two functions: the detection of selfish nodes and the detection of new contacts. The local watchdog can generate the following events about neighbor nodes PosEvt (positive event) when the watchdog detects a selfish node, NegEvt (negative event) when the watchdog detects that a node is not selfish, and No DetEvt (no detection event) when the watchdog does not have enough information about a node.

2.9 DIFFUSION METHOD IN COCOWa:

The Diffusion module has two functions: the transmission as well as the reception of positive (and negative) detections. A key issue of the approach is the diffusion of information. As the number of selfish nodes is low compared to the total number of nodes, positive detections can always be transmitted with a low overhead. When the diffusion module receives a new contact event from the watchdog, it transmits a message including this information to the new neighbor node. When the neighbor node receives a message, it generates an event to the network information module with the list of these positive (and negative) detections. This method has a disadvantage that it does not concentrate on data transmission accuracy and energy efficiency.

3. FALSE ALARM METHOD WITH NODE REPLACEMENT ALGORITHM

The false method is the best method for detection of selfish node in the network. This method undergoes three steps for detection. First step focus on calculating the distance between the nodes and finds the shortest path to reach the data from source to destination is made. In second step the behavior of the nodes is taken into account and that node is the abnormal behavior node is termed as the selfish node. And then the node replacement algorithm is used and thereby the selfish node is replaced by the adjacent node in the network. This is achieves the energy efficiency and performance in the system and load can also be balanced in the network.

CONCLUSION

The false alarm method along with node replacement algorithm proves as the best method for detection and approaching the selfish node and also achieves the load balancing, energy efficiency feature in the system and the main advantage is that this method has data transmission accuracy to great extent.

REFERENCES

[1] E. Hern_andez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate,and P. Manzoni, “Improving selfish node detection in MANETsusing a collaborative watchdog,” IEEE Comm. Lett., vol. 16, no. 5,pp. 642–645, May 2012

[2] CoCoWa: A Collaborative Contact BasedWatchdog for Detecting Selfish NodesEnrique Hern_andez-Orallo, Member, IEEE, Manuel David Serrat Olmos, Juan-Carlos Cano,Carlos T. Calafate, and Pietro Manzoni, Member, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 6, JUNE 2015

[3] A Combined Credit Risk and Collaborative Watchdog Method for Detecting Selfish Node over Mobile Ad-Hoc Network, International Journal of Advanced Research in Computer Science and Software Engineering, S.J.K. Jagadeesh Kumar R. Saraswathi Volume 2, Issue 11, November 2012

[4] E. Hern_andez-Orallo, M. D. Serrat, J.-C. Cano, C. M. . Calafate,and P. Manzoni, “Improving selfish node detection in MANETsusing a collaborative watchdog,” IEEE Comm. Lett., vol. 16, no. 5,pp. 642–645, May 2012

[5] E. Hern_andez-Orallo, M. D. Serrat Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, “Evaluation of collaborative selfish node detection in MANETS and DTNs,” in Proc. 15th ACM Int. Conf. Modeling, Anal.

[6] F. Kargl, A. Klenk, M. Weber, and S. Schlott, “Sensors for detectionof misbehaving nodes in MANETs,” in Proc.15ACMTNT.CONF.modelling.anal.