International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume - 2, Issue - II ISSN (Online): 2454- 1966

Research Manuscript Title

Divergence Based Selfish Nodes Detection Approach in MANET

SATHYA.P [#1], **Mrs.C.SUGUNA** [*2],

[#1] PG Scholar, [*2] Assistant Professor

Department of CSE, College, V.S.B Engineering College, Karur, Tamilnadu, India,

E-mail: ***sathyamoorthysathya75@gmail.com, mcsuguna@gmail.com***

JUNE – 2016

www.istpublications.com

Divergence Based Selfish Nodes Detection Approach in MANET

SATHYA.P [#1], **Mrs.C.SUGUNA** [*2],

[#1] PG Scholar, [*2] Assistant Professor

Department of CSE, College, V.S.B Engineering College, Karur, Tamilnadu, India,

E-mail: ***sathyamoorthysathya75@gmail.com, mcsuguna@gmail.com***

ABSTRACT

Mobile Ad hoc network consists of multiple mobile nodes in the network, where the nodes would move in different direction based on which new path would be established. The collaborative network is the one where the multiple nodes may communicate with other to share resources, thus there is no need to get permission for data access. However, this existing work may lack to detect the selfish behaviour nodes in case of presence malicious monitoring node. The compromise between the selfish node and monitoring would prevent the detection the ration of selfish node detection. This is overcome in the proposed methodology by introducing the technique called Divergence based Malicious Monitoring Node Detection (DMMND) technique which attempts to find the malicious monitoring nodes present in collaborative MANET environment by predicting the divergence present in the usual behaviour. The divergence is calculated by using the methodology called the Kullback-Leibler divergence (KI divergence) which could identify the malicious monitoring nodes accurately. The experimental conducted was proved that the proposed methodology can predict the selfish behaviour of nodes more accurately than the existing approaches.

Keywords: MANNETs,selfish nodes,DMMND,KI divergence

1. INTRODUCTION

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs.

Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network. A Mobile Ad Hoc Network (MANET) is a continuously self configuring, infrastructure-less network of mobile devices connected without wires. Ad Hoc is Latin & means “for this purpose” Each device in a MANET is free to move independently in any direction and will change its links to other devices frequently. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger internet. They may contain one or multiple & different transceivers between nodes. This results in a highly dynamic autonomous topology.

The mobile Ad hoc networks are different from internet in two major ways. The first is that the hosts in this network are resource-constraint.MANET nodes are typically distinguished by their limited power, processing & memory resources as well as high degree of mobility. In such networks, the wireless nodes may dynamically enter the network as well as leave the network. Due to the limited transmission range of wireless network nodes, multiple hopes are usually needed for a node to exchange information with any other node in the network.

2. RELATED WORKS

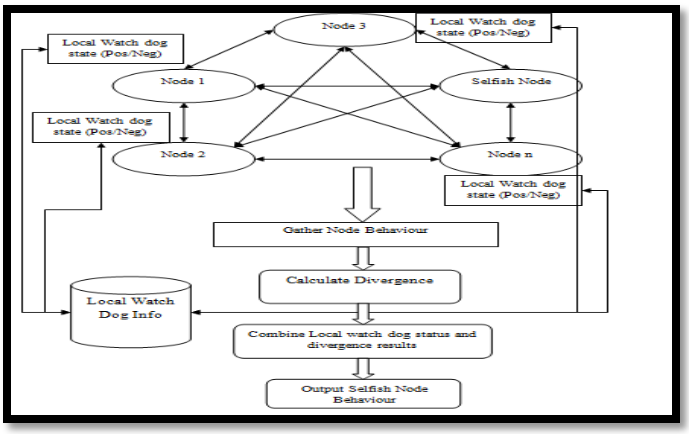
Many approaches have been proposed to detect selfishnodes have been proposed. For example, Jim Solomon Raja.,et al [1] suggested that analysed a process of finding the malicious nodes present in the mobile Adhoc environment in terms of selfish behaviour. This survey discusses a various techniques which focus on finding the selfish behaviour of the nodes that are present in the environment in terms of their packet forwarding behaviour. Senthilkumar Subramaniya.,et al [2] introduced the novel approach for detecting the selfish nodes present in the distributed environment. This is achieved by maintaining the record and trust based method which will create the table and stores the packet transmission rate. Dipali Koshti., et al [3] suggested that conducted a survey analysis to find the better algorithm that is used to find the malicious nodes in the efficient manner. Mechanism and procedures of various protocols has been studied and discussed in the efficient manner. The main protocols that has been compared for which can find the malicious node in the efficient manner are AODV and DSR protocols. Both of these protocols works with the consideration of forward packet transfer behaviour. Hongxun Liu.,et al [4] suggested that introduced the novel mechanism for the detecting the malicious behaviour of selfish nodes in the mobile Adhoc environment. This novel mechanism will maintain the hardware cache storage in the each and every nodes present in the environment. The hardware cache will store the every innovative packet that is transferred through the corresponding node. The detection mechanism will compare the original packet with the hardware cache stored packet information to find the divergence of both packets.

3. SYSTEM DESIGN

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. One could see it as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering. If the broader topic of product development blends the perspective of marketing, design, and manufacturing into a single approach to product development.

3.1Existing System

Cooperative networking is currently receiving significant attention as an emerging network design strategy for future mobile wireless networks. Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide services and applications in contexts such as vehicular ad hoc networks (VANETs) or mobile social networks. Existing work introduces Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish nodes in the network. The goal of this approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives.It is based on the combination of a local watchdog and the diffusion of information when contacts between pairs of nodes occur. A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them). Assuming that there is only one selfish node, the figure shows how initially no node has information about the selfish node. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non selfish node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it; so, from that moment on, both nodes store information about these positive (or negative) detections. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative transmission of information that is provided by other nodes.


Local Watch dog state (Pos/Neg)
Node 3
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)
Gather Node Behaviour
Calculate Divergence
Local Watch Dog Info
Combine Local watch dog status and divergence results
Output Selfish Node Behaviour

.

Fig 1: System architecture

3.2 Proposed System

The main problem resides in the existing methodology is the presence of number of malicious monitoring nodes (MMN) in the environment. The malicious MMN can lead to the cause the prevention process of detecting selfish nodes where the number of packet loss might also get increased. The malicious behaviour of monitoring nodes needs to be avoided as soon as possible to decrease the packet loss rate.One way to detect the malicious behaviour of monitoring node is to identification of behaviour changes present in the monitoring node activities. These changes can be predicted by constructing the matrix in which the behaviour of monitoring node can be indicated in different time periods. From this matrix, the variation of behaviour would be calculated between different time periods. The divergence would be calculated from this behaviour changes. The node with unusual divergence would be predicted as malicious node. The operation of KI divergence is given as follows:

In this work, Kullback-Leibler divergence (KL divergence) is used to identify the malicious monitor effectively where in existing work monitoring nodes are considered as trust worthy. In this work, the accessibility matrix for the monitoring nodes and its behaviour in difference time scenarios will be built. In this matrix information about the type of service functions that are supported by the monitoring node will present. From that behaviour matrix, divergence will be calculated. In our work divergence is calculated by using the KL divergence which is a popular measure for a similarity between two probability distributions. The KL-divergence is defined as,

$$\mathrm{KL}\ [p \parallel q] = \int p(x) \log \frac{p(x)}{q(x)}\,\mathrm{dx}$$

Where p and q are two discrete sequences described by two patterns with N samples. This KL-divergence is the technique robust with respect to quantitative similarities identified in the output patterns of other legitimate system processes. This technique is more effective than the existing paper.

4. SYSTEM IMPLEMENTATION

4.1 Network Model

The network is modelled as a set of N wireless mobile nodes, with C collaborative nodes, M malicious nodes and S selfish nodes (N = C + M + S). Our goal is to obtain the time and overhead that a set of D <= C nodes need to detect the selfish nodes in the network.

4.2 Cocowa Model

The local watchdog is modelled using three parameters: the probability of detection p_d, the ratio of false positives pf_p, and the ratio of false negatives pf_n. The first parameter, the probability of detection (p_d), reflects the probability that, when a node contacts another node, the watchdog has enough information to generate a PosEvt or NegEvt event. This value depends on the effectiveness of the watchdog, the traffic load, and the mobility pattern of nodes. For example, for opportunistic networks or DTNs where the contacts are sporadic and have low duration, this value is lower than for MANETs. Furthermore, the watchdog can generate false positives and false negatives. A false positive is when the watchdog generates a positive detection for a node that is not a selfish node. A false negative is generated when a selfish node is marked as a negative detection. In order to measure the performance of a watchdog, these values can be expressed as a ratio or probability: pf_p is the ratio (or probability) of false positives generated when a node contacts a non-selfish node, and pf_n is the ratio (or probability) of false negatives generated when a node contacts a selfish node. Using the previous parameters we can model the probability of generating local PosEvt and NegEvt events when a contact occurs:

- PosEvt event: the node contacts with the selfish node and the watchdog detects it, with probability $p_d(1 - pf_n)$. Note that a false positive can also be generated with probability $p_d . pf_p$.
- NegEvt event: the node contacts with a non-selfish node and detect it with probability $p_d\ (1 - pf_p)$. A false negative can also be generated when it contacts with the selfish node with probability $p_d . pf_n$.

The diffusion module can generate indirect events when a contact with neighbour nodes occurs. Nevertheless, a contact does not always imply collaboration, so we model this probability of collaboration as pc. The degree of collaboration is a global parameter, and it is used to reflect that either a message with the information about the selfish node is lost, or that a node temporally does not collaborate (for example, due to a failure or simply because it is switched off). In real networks, full collaboration (pc = 1) is almost impossible. Finally, the probability of generating the indirect events are the following:

4.3 Attacker Model

Malicious nodes attempt to attack the CoCoWa system by generating wrong information about the nodes. Thus, the attacker model addresses the behaviour or capabilities of these malicious nodes. A malicious node attack consists of trying to send a positive about a node that is not a selfish node, or a negative about a selfish node, with the goal of producing false positives and false negatives on the rest of nodes. In order to do this, it must have some knowledge about the way CoCoWa works. The effectiveness of this behaviour clearly depends on the rate and precision that malicious nodes can generate wrong information. Malicious nodes are assumed to have communications hardware similar to the rest of nodes, so they can hear all neighbour messages in a similar range than the rest of nodes. Nevertheless, the attacker could use high-gain antennas to increase its communications range and thus disseminate false information in a more effective manner.

The behaviour of malicious nodes is modelled from the receiver perspective, which is based on the probability of receiving wrong information about a given node when a contact with a malicious node occurs (that is, it receives a Negative about the selfish node, and a Positive about the other nodes). We denote this behaviour as the maliciousness probability pm. Below we detail several aspects that can affect this probability:

4.4 Calculating Divergence factor of nodes

One way to detect the malicious behaviour of monitoring node is to identification of behaviour changes present in the monitoring node activities. These changes can be predicted by constructing the matrix in which the behaviour of monitoring node can be indicated in different time periods. From this matrix, the variation of behaviour would be calculated between different time periods. The divergence would be calculated from this behaviour changes. The node with unusual divergence would be predicted as malicious node. The operation of KI divergence is given as follows:

In this work, Kullback-Leibler divergence (KL divergence) is used to identify the malicious monitor effectively where in existing work monitoring nodes are considered as trust worthy. In this work, the accessibility matrix for the monitoring nodes and its behaviour in difference time scenarios will be built. In this matrix information about the type of service functions that are supported by the monitoring node will present. From that behaviour matrix, divergence will be calculated. In our work divergence is calculated by using the KL divergence which is a popular measure for a similarity between two probability distributions. The KL-divergence is defined as,

Where p and q are two discrete sequences described by two patterns with N samples. This KL-divergence is the technique robust with respect to quantitative similarities identified in the output patterns of other legitimate system processes. This technique is more effective than the existing paper.

4.5 Detection Of Selfish Node

The goal is to obtain the detection time (and overhead) of a selfish node in a network. This model takes into account the effect of false negatives. False positives do not affect the detection time of the selfish node, so pf_p is not introduced in this model. Using λ as the contact rate between nodes, we can model the network using a 4D continuous time Markov chain (4DCTMC). For modelling purposes, the collaborative nodes are divided into two sets: a set with D destination nodes, and a set of E = C - D intermediate nodes.

4.6 Evaluating False Positives

We now develop a model for evaluating the effect of false positives. This model evaluates how fast a false positive spreads in the network (the diffusion time). Thus, in this case, a greater diffusion time stands for a lower impact of false positives. The diffusion time is similar to the detection time of true positives described in the previous section, and it can be obtained in a similar way. Following the same process that in the previous model for the false negatives, we have a 4D-CMTC with the same states (d_p, d_n, e_p, e_n), but in this case $c_p = d_p + e_p$ represents the number of nodes with a false positive, and $c_n = d_n + e_n$ the number of nodes with a (true) negative detection. We can derive expressions similar to 4 and 5, for the case of false positives. In this case, R_{fP} represents the rate of a false positive, and it is derived in a similar way:

$$R_{fp} = \lambda(\delta_{Pdpfp} + \max(pc(cp - \gamma cn) + Mpm, 0))/\theta$$

and R_n represents the rate of negative detection:

$$R_n = \lambda(S_{pd}\left(1 - P_{fp}\right) + \max(P_c\left(\gamma c_n - c_p\right) - M_{pm}, 0))/\theta$$

Using these expressions, the transition rates (qij) of the generator matrix Q are similar to expression 3, substituting R_P and Rf_n by Rf_p and R_n, respectively. Finally, using Equations (6) and (7) described in our previous model, we can obtain the diffusion time and the overhead.

4.7 Performance Evaluation

Finally in this module the performance of the existing and the proposed approaches were illustrated and evaluated. In the existing method the selfish attack detection technique, COCOWA is implemented. But in this method it detects the selfish nodes if there is one selfish secondary user is present and also cant provide accurate detection in case of presence of more number of malicious users. In the proposed system, KI divergence mechanism is implemented. Compared to the existing system, there is high detection accuracy is achieved in the proposed system.

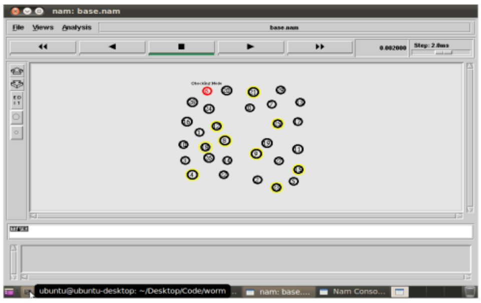
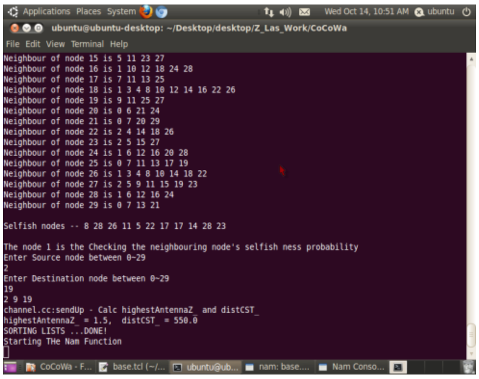
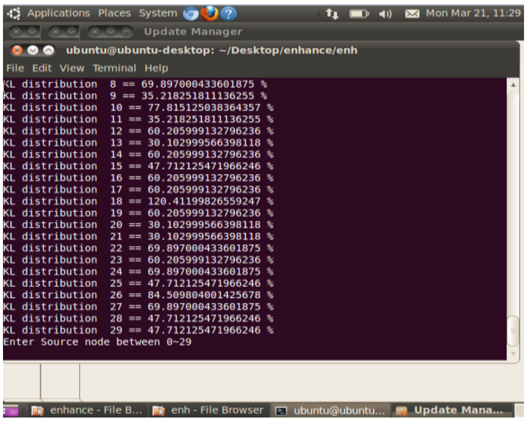


Fig 2 a)node creation


Applications Places System
Wed Oct 14, 10:51 AM
ubuntu
ubuntu@ubuntu-desktop: ~/Desktop/desktop/Z_Las_Work/CoCoWa
File Edit View Terminal Help
CoCoWa - F...
base.tcl (~/...
ubuntu@ub...
nam: base....
Nam Conso...

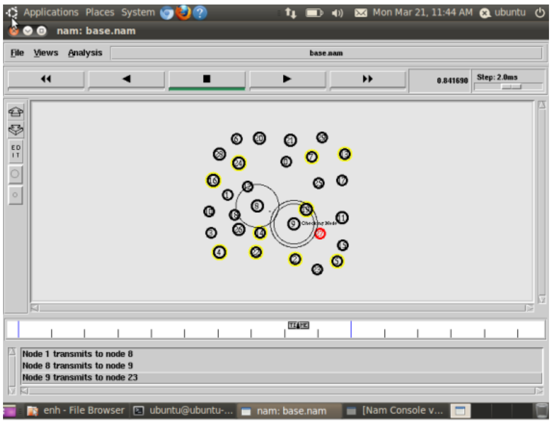
```
Neighbour of node 15 is 5 11 23 27
Neighbour of node 16 is 1 10 12 18 24 28
Neighbour of node 17 is 7 11 13 25
Neighbour of node 18 is 1 3 4 8 10 12 14 16 22 26
Neighbour of node 19 is 9 11 25 27
Neighbour of node 20 is 0 6 21 24
Neighbour of node 21 is 0 7 20 29
Neighbour of node 22 is 2 4 14 18 26
Neighbour of node 23 is 2 5 15 27
Neighbour of node 24 is 1 6 12 16 20 28
Neighbour of node 25 is 0 7 11 13 17 19
Neighbour of node 26 is 1 3 4 8 10 14 18 22
Neighbour of node 27 is 2 5 9 11 15 19 23
Neighbour of node 28 is 1 6 12 16 24
Neighbour of node 29 is 0 7 13 21

Selfish nodes -- 8 28 26 11 5 22 17 17 14 28 23

The node 1 is the Checking the neighbouring node's selfish ness probability
Enter Source node between 0~29
2
Enter Destination node between 0~29
19
2 9 19
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
Starting THe Nam Function
```

Fig 2 b) selfish node detetion between two nodes


Applications Places System
Mon Mar 21, 11:29
Update Manager
ubuntu@ubuntu-desktop: ~/Desktop/enhance/enh
File Edit View Terminal Help
enhance - File B...
enh - File Browser
ubuntu@ubuntu...
Update Mana...

```
KL distribution  8 == 69.897000433601875 %
KL distribution  9 == 35.218251811136255 %
KL distribution  10 == 77.815125038364357 %
KL distribution  11 == 35.218251811136255 %
KL distribution  12 == 60.205999132796236 %
KL distribution  13 == 30.102999566398118 %
KL distribution  14 == 60.205999132796236 %
KL distribution  15 == 47.712125471966246 %
KL distribution  16 == 60.205999132796236 %
KL distribution  17 == 60.205999132796236 %
KL distribution  18 == 120.41199826559247 %
KL distribution  19 == 60.205999132796236 %
KL distribution  20 == 30.102999566398118 %
KL distribution  21 == 30.102999566398118 %
KL distribution  22 == 69.897000433601875 %
KL distribution  23 == 60.205999132796236 %
KL distribution  24 == 69.897000433601875 %
KL distribution  25 == 47.712125471966246 %
KL distribution  26 == 84.509804001425678 %
KL distribution  27 == 69.897000433601875 %
KL distribution  28 == 47.712125471966246 %
KL distribution  29 == 47.712125471966246 %
Enter Source node between 0~29
```

Fig 2 c) calculate Kullback-Leibler (KL divergence)



Node 1 transmits to node 8
Node 8 transmits to node 9
Node 9 transmits to node 23

Fig 2 d) secure to send data packet

5. CONCLUSION

This work proposes CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, false negatives and malicious nodes. CoCoWa is based on the diffusion of the known positive and negative detections. When a contact occurs between two collaborative nodes, the diffusion module transmits and processes the positive (and negative) detections. Analytical and experimental results show that CoCoWa can reduce the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced overhead (message cost). This reduction is very significant, ranging from 20 percent for very low degree of collaboration to 99 percent for higher degrees of collaboration. Regarding the overall precision we show how by selecting a factor for the diffusion of negative detections the harmful impact of both false negatives and false positives is diminished.Finally, using CoCoWa we can reduce the effect of malicious or collusive nodes. If malicious nodes spread false negatives or false positives in the network CoCoWa is able to reduce the effect of these malicious nodes quickly and effectively. Additionally, we have shown that CoCoWa is also effective in opportunistic networks and DTNs, where contacts are sporadic and have short durations, and where the effectiveness of using only local watchdogs can be very limited.

6.REFERENCES

[1] Jim Solomon Raja.D, Immanuel John Raja.J,"A Survey On Selfishness Handling In Mobile Ad Hoc Network", International Journal Of Emerging Technology And Advanced Engineering Website (Issn 2250-2459, Volume 2, Issue 11, November 2012)

.[2]SenthilkumarSubramaniyan,William Johnson, Karthikeyan Subramaniyan," A Distributed Framework For Detecting Selfishnodes In MANET Using Record- And Trust-Based Detection (RTBD) Technique", Subramaniyan Et Al. EURASIP Journal On Wireless Communications And Networking (2014).

[3] Dipali Koshti, Supriya Kamoji," Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September(2011).

[4] Hongxun Liu, José G. Delgado-Frias, and Sirisha Medidi," Using A Cache Scheme To Detect Selfish Nodes In Mobile Ad Hoc Networks",(IASTED,July 2007).

[5] Julien Freudiger, David C. Parkes," On Non-Cooperative Location Privacy: A Game-Theoretic Analysis" IEEE(2011).

[6] Hang Hu, Youyun Xu," Optimal Strategies For Cooperative Spectrum Sensing In Multiple Cross-Over Cognitive Radio Networks" IEEE(2009).

[7] P. Saravanan, S. Chitra," Selfish Nodes in MANET: Impact on Security and QoS", (International Journal of Computer Applications (0975 – 8887) Volume 66– No.1, March 2013).

[8] John A. Stine And Gustavo De Veciana,"A Paradigm For Quality-Of-Service In Wireless Ad Hoc Networks Using Synchronous Signaling And Node States" IEEE(2006).

[9]E.Hern_AndezOrallo,M.D.Serrat,J.Cano,C.M.T.Calafate,P.Manzoni,"Improving Selfish Node Detection In Manets Using A Collaborative Watchdog," IEEE(2012).

[10] J.Hortelano,J.C.Ruiz,P.Manzoni,"Evaluating The Usefulness Of Watchdogs For Intrusion Detection In Vanets,"IEEE(2010).

[11] Y. Li, G. Su, D. Wu, D. Jin, L. Su, L. Zeng, "The Impact Of Node Selfishness On Multicasting In Delay Tolerant Networks," IEEE(2011).

Authors:

Ms. P.Sathya - Received the Bachelor Degree in Information Technology from Chettinad College Of Engineering And Technology in 2014. Currently she is doing Master of Engineering in Computer Science at V.S.B Engineering College, Karur under Anna University of India. Her research interests include Data Mining and Network security.

Mrs.C.Suguna,Assistant Professor Department of CSE, VSB Engineering College, Karur. Her area of research is Network Security and She has published many papers in National and International Conferences and Journals.

I.