Detecting Misbehaving and Selfish Nodes in the Network using Watchdog Mechanism

K. Naveen Kumar[1], Assistant Prof. K. Sriprasadh[2]

[1]P.G student, Thirumalai Engineering College, kilambi, kanchipuram, Tamil Nadu, India.
[2]Asst Prof. CSE, Thirumalai Engineering College, kilambi, kanchipuram, Tamil Nadu, India.

Abstract— *The nodes in a wireless network may misbehave at times. This misbehavior needs to be monitored in order to avoid sudden failure of network. The watch dog mechanism has been sufficiently studied to address the issue of malice node detection, in Mobile Adhoc Networks (MANETs). A Collaborative Contact based Watchdog (CoCoWa) is collaborated with information diffusion in the proposed work. This combination strategy analyses all the nodes in a network and provides the information update regarding the selfishness of the specific nodes to other nodes and routing protocols to enable performance oriented transmission. Once the selfish node is detected by the watch dog, it is marked as selfishness positive node else the node is marked as negative selfish node. For enabling this fool proof approach, true neighbors, fake neighbors, their probability of relationships with each other is analyzed. The evaluation of the viability of the proposed work is made in terms of detection efficiency, detection accuracy of both malicious and selfish nodes. Apart from these, the strategy is proved to be simple yet effective.*

Keywords— ***Wireless Networks, MANET, Selfish Nodes, Watch Dog, Information Diffusion, Performance analysis***.

I. INTRODUCTION

In the past few decades, Mobile Adhoc Networks (MANET) has been widely addressed because of high usage of mobile devices. To be specific, the MANET is the set of mobile nodes setup in a wireless multihop network without a determined infrastructure. This type of network is dynamic in nature that are totally independent from fixed organizations.

It has the following features

- Self-created
- Self-organized
- Highly dynamic
- Capable to reconfigure

In this environment, the mobile nodes are moving randomly without any centralized administration. The message transmission between two distant nodes can happen only by relay through the intermediate nodes in the network.

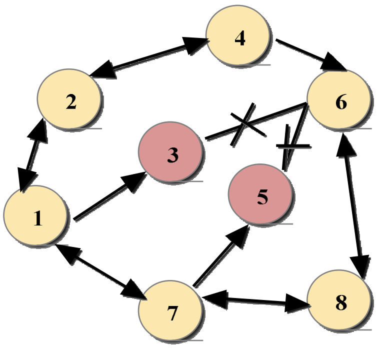

Fig.1: Selfish nodes

Fig 1 describes the working of selfish nodes in the network. Node 3 and node 5 is the selfish nodes as they don’t forward the packets they receive. The threats associated with selfish nodes can be dangerous to the trust of the concerned network and security of data. When the data is transferred from one mobile node to another node in a particular network, someone may hack or perform some malicious activities in the network. During the information transfer or when the services are offered to a user, the user may face delay reception of data. The information delivery to the destination node becomes delayed. These scenarios are considered as malicious activities or selfish activities. In DTNs, selfish nodes can seriously degrade the performance of packet transmission. For example, in two-hop relay schemes, if a packet is transmitted to a selfish node, the packet is not retransmitted, therefore being lost. Thus the co-operation of nodes is mandatory to work in the MANETs. The network design strategy adopted can be modified to accomplish this, however the precautions to know the presence of selfish nodes also becomes necessary. This co-operation can be described in terms of the contact. The contact is the relationship that a node have with the other nodes during the presence of communication range. Tough it has been known that, node co-operation is expensive, it has to be attained to sustain the reputation or trust of the network. In the earlier works, it has been provided with

- Incentive based methods and

- Detection and Exclusion strategies

For these enable stimulation of nodes in the network to actively participate in the routing of packet forwarding process. And our work does not focus to isolate or exclude the selfish node but only to detect them positively without false alarms.

This paper proposes CoCoWa as a collaborative contact-based watchdog to reduce the time delay in packet transmission through the nodes of the network and to improve the selfish nodes detection efficiency. Here, the harmful effects of false positives, false negatives and malicious nodes are reduced. The proposed work combines the CoCoWa mechanism with the diffusion of the known positive and negative detections. The work focusses to obtain the less detection time (and overhead) of a selfish node in a network.

The advantages of the proposed system are

- It takes less detection time (and overhead) of a selfish node in a network.
- It reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, false negatives and malicious nodes.
- If the collaboration approach was not used, CoCoWa can reduce the overall detection time with respect to the original detection time
- Reduced overhead (message cost).

The following part of the paper is organized as follows. The prior works related to the selfish node detection mechanisms are discussed with their methodologies and challenges associated with the anomalies detection and information updates of those systems in section II. Section III gives a detailed information on the proposed Collaborative Contact based Watchdog (CoCoWa) with the diffusion strategy and their working. Section IV gives the evaluation which is supported by the simulation screen shots. The concluding words are provided in section V.

II. RELATED WORK

Hernandez-Orallo, et al [1] suggested an analytical prototype to find the selfish nodes with the help of watch dog in the Mobile Adhoc Network (MANET). The model used contact dissemination over the identified selfish nodes collaboratively with the watch dog. Their metrics were evaluated in terms of detection time and cost of implementation. Also in the next work [2] studied the selfish nodes using watch dog with respect to diffusion. Their metrics were evaluated in terms of diffusion time and overhead of implementation. The work focused on the false positives and false negatives. *Li, et al* [3] evaluated the selfish behavior of the nodes of Delay Tolerant Networks (DTN). The work evaluated the factors affected due to the presence of selfish node. 3-D continuous time markov chain based message delivery was undertaken. The study concluded that the size of the multicast also decide the performance of the system. *Mahmoud and Shen* [4] proposed a secure cooperation incentive protocol for avoiding the disruption due to riding attacks, to stop the denial of payment and to minimize the overhead. For this purpose, public key operations and light weight hashing operations were utilized. Along with the performed operations, hash chains and keyed hash values were applied. The results presented had reduced overhead during transmission and proper accuracy.

Passarella and Conti [5] presented an analytical model to describe the relation between individuals and aggregates assuming a heterogeneous network. The aggregate inter-contact time statistics was determined. *Serrat-Olmos, et al* [6] proposed an integrated approach to identify the black holes and selfish nodes in the MANET. A set of watchdogs were utilized for the improvement of individual as well as collective performance of the network. There was minimum time requirement to detect the selfish node with maximum accuracy. *Gupta, et al* [7] summarized the impacts of selfish nodes in a Mobile Adhoc Network. The presence of selfish node in a network would degrade the efficiency of the network and ultimately the whole network would fail stated by the proposed work. The concentration of selfish nodes were illustrated along with the factors influenced by the nodes. *Padiya, et al* [8] reviewed on the novel and existing methodologies for the detection of selfish nodes in the MANET. The work gave a scope for new findings for the existing challenges. *Han, et al* [9] studied different trusted approaches of Wireless Sensor Networks (WSN) in detail. The work had compared and analyzed various parameters of the study and presented the requirement for a robust approach for the WSNs. *Dias, et al* [10] presented a novel co-operative watch dog based system for detecting the misbehaving nodes in Vehicular delay Tolerant Networks (VDTN). Thus the identification was carried out for increasing the overall network performance, probability of bundle delivery. The resources were effectively utilized. *Ataie, et al* [11] suggested a new idea to deal with the problem of selfish nodes in mobile Adhoc networks. A Cooperation Enforcement, Malice Detection and Energy Efficient Mechanism for Mobile Adhoc Network (CEMDEEM) was introduced for identification and isolation of energy based classical selfish nodes as well as malice behaving nodes. The work investigated the network by introducing a group of selfish nodes. The Dynamic Source Routing (DSR) Protocol was executed and the performance results were recorded. The work showed optimal performance in the presence of up to 40 selfish nodes. *Wahab, et al* [12] proposed a two phase model for treating the misbehaving node in Vehicular Adhoc Network (VANET). The model utilized Quality of Service Optimized Link State Routing (QoS-OLSR) Protocol. The work focused on

- Identification of misbehaving vehicles that crossed the speed range stipulated
- Promoting co-operation of selfish nodes during cluster formation
- Detection of malice nodes after cluster formation
- Dempster- Shafer was used for the co-operative watch dog model

The concept proved good for VANET with decreased false negatives and increased detection probability. Also the Quality of Service and stability was also maintained.

Sengathir, et al [13] reviewed and categorized the existing solution proposed in various works for selfish node detection. The misbehaviour was found to be the result of current condition instead of its future or past history. The study elaborated on the benefits and shortcomings of the markovian models. Nikmaram [14] worked out on the following objectives

- Evaluation of misbehaving node detection using current acknowledgement methodology.
- Design and development of misbehaving node detection using the acknowledgement strategy
- Provided energy efficiency
- Performance analysis of the proposed methodology

Akhtar and Sahoo [15] proposed an innovative mathematical model for the classification of nodes based on their misbehavior. Each node was graded based on the level of misbehavior. The degree of tolerance towards misbehavior was predefined so that, the nodes that misbehave was easily identified. The messages was displayed as a course of action against misbehavior. Thus, after effective classification of misbehaving nodes, the list of nodes prone to misbehave were sent to the routing protocol to avoid choking of data.

However the demerits of the existing system was listed as follows

- There is no selfishness prevention mechanism is present.
- The packet delivery rates become seriously degraded.
- The number of packet losses is increased by 500 percent when the selfish node ratio increases from 0 to 40 percent.

III. PROPOSED METHOD

In the proposed system, a new scheme for detecting selfish nodes is established as Collaborative Contact based Watchdog (CoCoWa) integrated with the information diffusion mechanism. It combines local watchdog detections and the dissemination of this information to the whole network. A common technique to detect this selfish behavior of a node is to monitor the network using local watchdogs. These watch dogs points out the selfish and misbehaving nodes and the information on the list of selfish nodes are diffused to all the other nodes in the network to beware before transferring data to that node. The information is updated regarding the status of the nodes in the whole network. Thus with the help of all these modules, the selfish nodes are detected successfully.

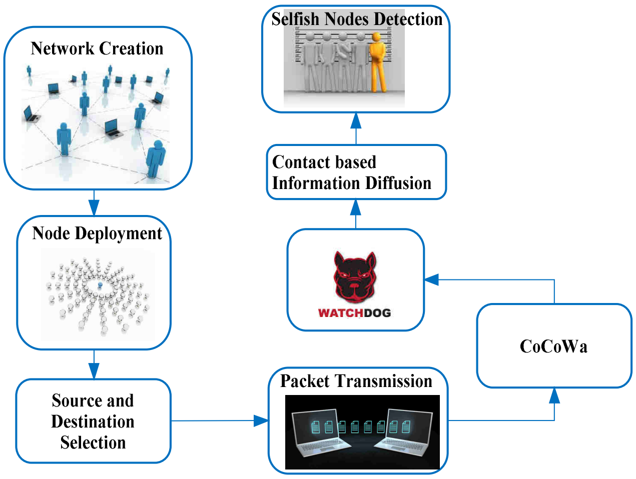

Fig.2:Generalized architecture of the proposed System

The modules of the proposed system is divided into five sub modules such as

- Network Creation
- Packet Transmission
- Local Watchdog
- Diffusion
- Information Update
- Selfish node Prediction

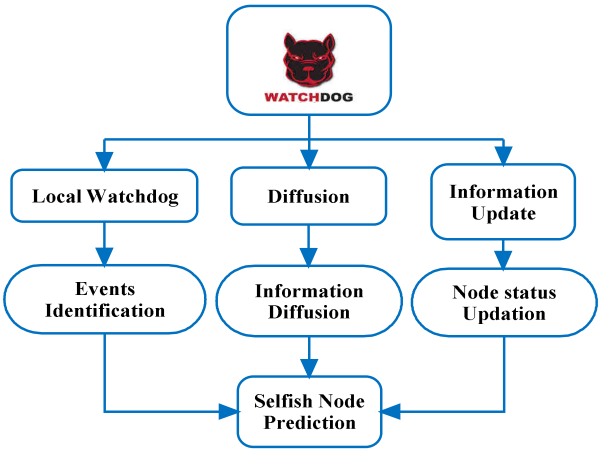

Fig.3: Proposed Flow of Watchdog Mechanism

The modules are described in detail

1. Network Creation:

Network creation is first and fore most step for wireless communication. Here, in this work the network nodes are deployed over an area dynamically. The source node and destination nodes are determined in this module.

2. Packet Transmission:

After the node deployment in the network the packet or file is chosen to transfer from the source node to destination node. Since the transmission is through wireless networks, it carried over to the destination via a chosen communication channel.

3. Local Watchdog:

Watch dog proposed in the current work has the duty to monitor the presence of selfish node and has to report accordingly. Each node is assigned with the local watch dog, which can overhear the packets transceived by its neighbors in order to detect anomalies, such as the ratio between packets received to packets being retransmitted. By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfish (or not). It is based on the combination of a local watchdog and the diffusion of information when contacts between pairs of nodes occurs. A contact are defined as an opportunity of transmission between a pair of nodes. The Local Watchdog of the proposed work has two functions: the detection of selfish nodes and the detection of misbehaving nodes. In order to perform its function effectively, they are designed to generate event based on the occurrence of the selfish nodes. The relationship, a node have with other normal nodes and misbehaving nodes is vital to identify the selfish nodes in a MANET. This with ease the work of proper routing possibility without channelizing the data to the selfish nodes. The local watchdog can generate the following events with regard to the neighboring nodes:

- PosEvt (positive event): when the watchdog detects a selfish node, it gets initiated
- NegEvt (negative event) : when the watch dog detects that a node is not selfish, this event is generated
- NoDetEvt (no detection event) when the watchdog does not have enough information about a node.

4. Diffusion:

A key issue of our approach is the diffusion of information. This is the novelty of the proposed work to be appended with the CoCoWa approach. The Diffusion module has two functions such that

(i) The transmission as well as the reception of information regarding positive (and negative) detections.

(ii) The routing protocol is also kept informed about the malicious nodes in the network to avoid forwarding data to those nodes. 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.

5. Information Update:

Updating or consolidating the information is the vital need of the work to serve the purpose of the objective. A node can have the following internal information about other nodes: No Info state, Positive state and Negative state.

- No Info state : means that the module has no information about that particular node,
- Positive state: denotes that the module believes that that particular node is selfish,
- Negative state: means that the module believes that that particular node is not selfish.

6. *Selfish node Prediction*

Finally, after the identification, diffusion and updation of the malicious node in a network, the system can easily predict the selfish nodes by based on

- the node behaviors in the network
- states of the nodes in the network
- events of the nodes in the network

IV. PERFORMANCE ANALYSIS

The performance evaluation has been done by simulating two or three machines process in real-time means over an virtual environment. Here we use machines as node instead of mobile phones. Evaluation of the selfish node detection through the wide nodes in the network enables the improved node specific recognition process. The network created is evaluated with the CoCoWa and diffusion modules. The proposed system is evaluated with the Java coding run over MySQL database. The efficiency of the proposed system is evaluated based on the following metrics namely

- Accuracy
- Computational Complexity
- Detection Time
- Malicious Node detection efficiency
- Node Event Detection Accuracy

Let us discuss these parameters with the help of graphical illustrations.

1. Accuracy:

Accuracy is defined as the ratio of the sum of true positive and true negative values to the total number of frequent patterns. True positive value denotes the number of correct frequent patterns that are identified and true negative value denotes the number of incorrect frequent patterns. Mathematically, the accuracy is given by the following equation.

$$\text{Accuracy} = \frac{\sum \text{TP} + \sum \text{TN}}{\sum \text{Total frequent patterns}}$$

Fig.4 provides the comparative results of the existing and proposed CoCoWa based diffusion method. Thus the graph shows the improved accuracy in detecting the selfish nodes in the network.

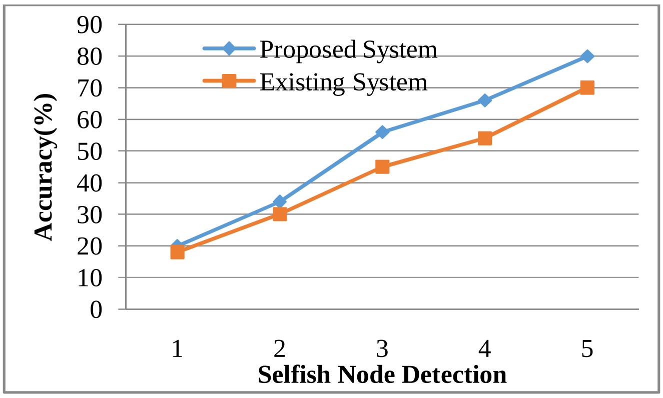

Fig.4: Accuracy analysis of the proposed system with the existing System

2. Computational Complexity:

The computations involved to attain the purpose , that is to detect the selfish nodes present in the network is found to be less. Hence the complexity of the system is low. This simple scheme of evaluation of the MANET in terms of misbehavior is graphically illustrated in Fig. 5. Thus our system outperforms the existing systems with reduced computational complexity.

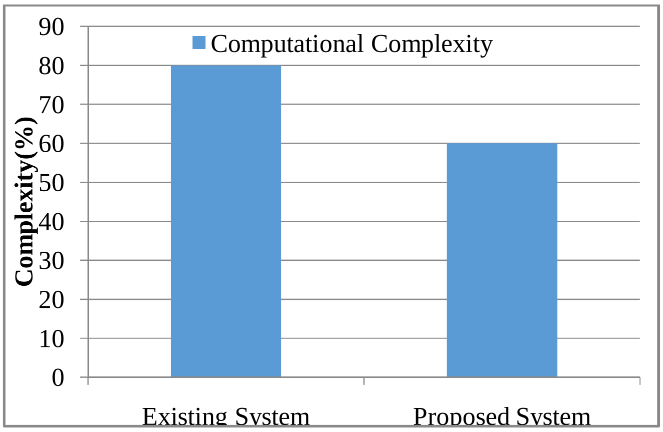

Fig.5 Computational complexity analysis of the proposed system with the existing System

3. Detection Time:

The execution time is defined as the time spent by the proposed CoCoWa based diffusion for finding the selfish node distributed in the wireless networks. The execution time of the proposed CoCoWa based diffusion is compared with the execution time of the existing methods. Figure.6 shows the execution time analysis of the proposed CoCoWa based diffusion and existing methods. From the comparison results, it is clearly evident that the execution time of the proposed CoCoWa based diffusion is lower than the execution time of the existing methods.

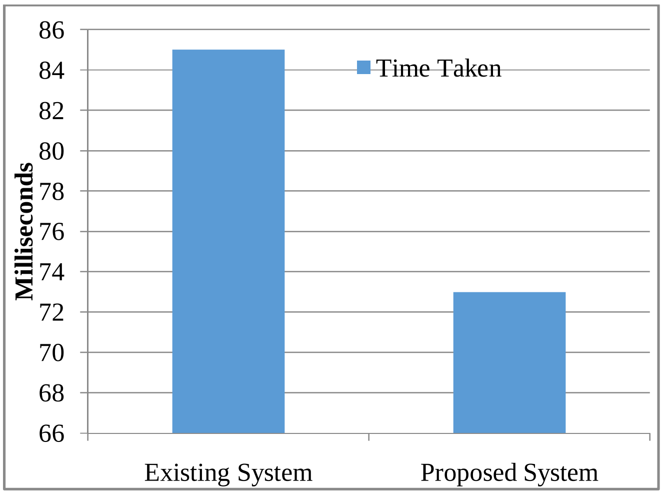

Fig.6: Detection time comparison of the proposed system with the existing System

4. Malicious Node Detection Efficiency:

The effectiveness at which the proposed strategy detects the malicious node in the wireless network is known as the efficiency of malicious node detection. Fig. 7 provides the analysis of the efficiency of CoCoWa based diffusion method and that of the existing methods.

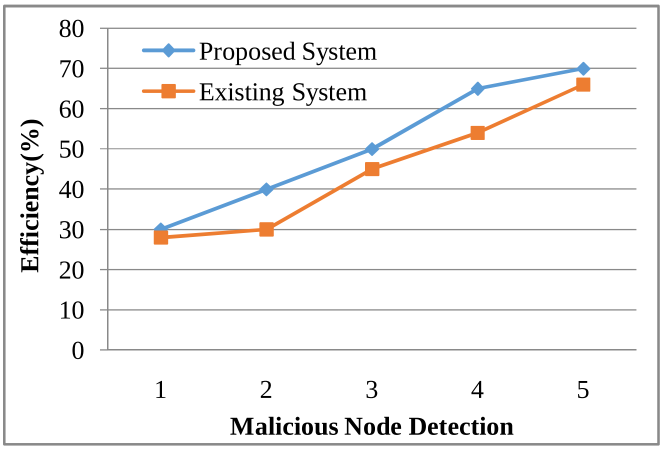

Fig.7: Malicious Node Detection time comparison efficiency

5. Node Event Detection Accuracy:

The false alarms given by the proposed solution is negligible. Thus the accuracy of detecting the node event is optimally good rather than the existing approaches which may creace false detection, which may result in disruption of network. Fig. 8 depicts the comparative analysis of the existing and proposed CoCoWa based diffusion method.

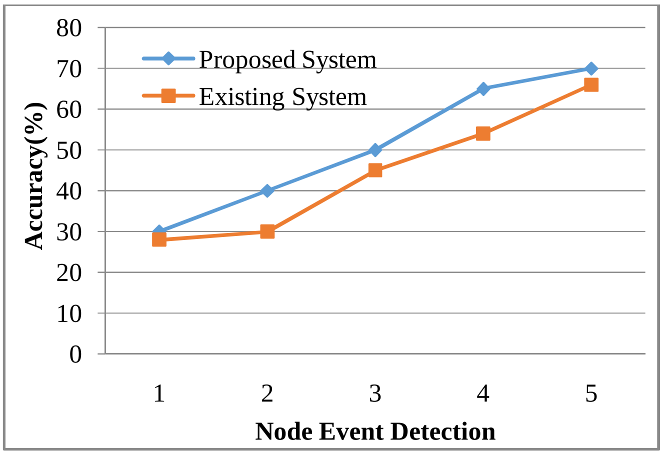

Fig.8: Node Event Detection accuracy comparison of the proposed system with the existing System

V. CONCLUSION AND FUTURE WORK

In the proposed work, the relationship or contact that a node have with the other neighboring nodes are exploited to address the issue of selfish nodes in the network. Each node is assigned with the local watch dog to monitor and report their misbehavior against the packet transmission in the network. The information diffusion strategy is also integrated to give the benefit of information update to the whole network to avoid delay in packet transmission with the blame of the presence of selfish nodes. Based on the event identification and node status updation, the selfish nodes can be predicted. This methodology is proved to outperform the earlier approaches with the simulations performed to evaluate the performance. Thus, the proposed system have greater selfish node detection accuracy, node event detection accuracy, malicious node detection. Also, it takes less time for detection with the help of this new approach with less computational complexity.

REFERENCES

[1] E. Hernandez-Orallo, M. D. Serrat, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Improving selfish node detection in MANETs using a collaborative watchdog," IEEE Communications Letters, vol. 16, pp. 642-645, 2012.

[2] E. Hernández-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 Proceedings of the 15th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, 2012, pp. 159-166.

[3] Y. Li, G. Su, D. O. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," IEEE Transactions on Vehicular Technology, vol. 60, pp. 2224-2238, 2011.

[4] M. E. Mahmoud and X. S. Shen, "Esip: Secure incentive protocol with limited use of public-key cryptography for multihop wireless networks," IEEE Transactions on Mobile Computing, vol. 10, pp. 997-1010, 2011.

[5] A. Passarella and M. Conti, "Characterising aggregate inter-contact times in heterogeneous opportunistic networks," in NETWORKING 2011, ed: Springer, 2011, pp. 301-313.

[6] M. D. Serrat-Olmos, E. Hernández-Orallo, J.-C. Cano, C. T. Calafate, and P. Manzoni, "A collaborative bayesian watchdog for detecting black holes in MANETs," in Intelligent Distributed Computing VI, ed: Springer, 2013, pp. 221-230.

[7] S. Gupta, C. Nagpal, and C. Singla, "Impact of selfish node concentration in manets," International Journal of Wireless & Mobile Networks, vol. 3, 2011.

[8] S. Padiya, R. Pandit, and S. Patel, "Survey of innovated techniques to detect selfish nodes in MANET," International Journal of Computer Networking, vol. 3, pp. 221-30, 2013.

[9] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in Wireless Sensor Networks: A survey," Journal of Computer and System Sciences, vol. 80, pp. 602-617, 2014.

[10] J. A. Dias, J. J. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," IEEE Transactions on Industrial Electronics, vol. 62, pp. 7929-7937, 2015.

[11] E. Ataie, A. Movaghar, and M. Bastam, "A Cooperation Enforcement, Malice Detection and Energy Efficient Mechanism for Mobile Ad hoc Networks," International Journal of Sensors Wireless Communications and Control, vol. 3, pp. 78-84, 2013.

[12] O. A. Wahab, H. Otrok, and A. Mourad, "A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles," Computer Communications, vol. 41, pp. 43-54, 2014.

[13] J. Sengathir, R. Manoharan, and R. R. Kumar, "Markovian process based reputation mechanisms for detecting selfish nodes in MANETs: A survey," in Fifth International Conference on Advanced Computing (ICoAC), 2013 2013, pp. 217-222.

[14] M. Nikmaram, "An energy efficient acknowledgement-based method for selfish node detection and avoidance in open MANET," Universiti Teknologi Malaysia, Faculty of Computing, 2014.

[15] A. K. Akhtar and G. Sahoo, "Classification of selfish and regular nodes based on reputation values in MANET using adaptive decision boundary," 2013.