International Journal of Knowledge Based Computer Systems
6 (2), December 2018, 31-37
http://www.publishingindia.com/ijkbcs/

Isolating Selfish Nodes and Analyzing Performance of Ad-Hoc Network Using Perfect Information Game Theory

Samara Mubeen
Department of Information Science and Engineering, J.N.N. College of Engineering,
Shimoga, Karnataka, India. Email: samaramubeen@jnnce.ac.in

Abstract: Base stations are not required for the flow of information between different nodes. Nodes spontaneously get connected for transfer of information in the Ad-hoc network. Energy is the important resource used in the transfer of information from the one node to the other node. To preserve the energy, the nodes behave selfishly. These selfish nodes will stop the forwarding the information to the next node in the network by which the performance of the entire network degrades. To identify selfish nodes and isolate them from the network, perfect information game theory is used. Performance of the network is found out with and without using game theory approach for static and dynamic Ad-hoc network. The parameters considered to measure performance are throughput and End-to-End delay. Ns2 simulator is used for implementation.

Keywords: End-to-End delay, Energy, Ns2 simulator, Packet delivery ratio, Perfect information game theory, Selfish nodes.

I. Introduction

In Ad-hoc network transfer of information from one node to another is done without infrastructure. Forwarding of the information is done using the energy of the nodes. More energy is spent on the forwarding the information, than energy spent in receiving of the information. Some nodes in Ad-hoc network will not forward the information to preserve the energy resource, as a result the performance of the entire network falls down. Some method should be adopted for identification of such types of nodes. Perfect information game theory is used for eliminating the selfish nodes in the Ad-hoc network.

A. Classification of Different Types of Nodes in Ad-Hoc Network

The nodes in the Ad-hoc network are classified into different categories. The overloaded nodes lack CPU cycles, buffer space or available network bandwidth to forward packets, broken nodes prevent forwarding the packets as they have software fault, malicious nodes drop packets and will launches denial of service attack, selfish nodes do not forward other nodes packet and will maximize the benefit at the expense of all others.

B. A Game Theory

An applied mathematics that is used in the social sciences, most notably in economics, as well as in biology is a branch called as game theory. Game theory attempts to mathematically capture behavior in strategic situations, or games. There are different types of games theory concepts. They are cooperative or non-cooperative, symmetric or asymmetric, zero-sum or non-zero-sum, simultaneous and sequential and meta games. In this paper perfect information game theory is used for eliminating selfish nodes from the network.

Section II of the paper consist of literature survey, Section III consist of design and implementation of the proposed model, Section IV result and finally Section V conclusion.

II. Literature Survey

Good Neighbor Node Detection Technique in MANETS Using QOS GNDA (Pallavi Patil [1]). Mobile Ad-hoc network are wireless network which are characterized by dynamic typologies and have no fixed infrastructure. If malicious node is present in the network causing treat to the security data. Good Neighborhood node detection algorithm is used to find good nodes.

Impact of selfish node concentration in MANET [5], resource such as battery power, CPU time and memory is spend for forwarding of data packets. The node which utilizes the network resource for its own profit is called selfish nodes. If the network has large number of such nodes it may lead to disruption of network. Impact of selfish nodes on the quality of MANET is considered in this paper.

Effect of selfish nodes behavior on efficient topology design [6], the selfish node if present in the network how it will impact the overall connectivity and energy consumption in the resulting

typologies. Game theory is used to analyze it. Nash equilibrium is used to study and evaluate the efficiency of the network. A method is proposed with modified algorithm based on better response dynamic.

Mathematical model for the detection of selfish nodes in MANET [7]. The router is used for forwarding traffic. A mathematical model is used to detect selfish nodes using the probability density function. Bayes theorem and prior probability is used in the proposed model.

A Novel defense scheme against selfish node attack in MANET [8], in this paper major issue in wired and wireless network is the security is considered. A new intrusion detection system algorithm is proposed against selfish node attack. IDS algorithm identifies the behavior of selfish node also and increases the performance of the network by 92% and 0% infection rate from attack.

Performance analysis of selfish node aware routing protocol for mobile Ad-hoc networks [9], an individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources is known as selfish nodes. This will affect the performance of the network. AODV+2 ACK model is used to detect routing misbehavior and to overcome their adverse effect. The idea of this model is to search two-hop ACK packets in the opposite direction of the routing path. The simulation study in this paper brings higher performance than existing AODV.

In this paper [2] an Ad-hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure Ad-hoc On Demand Distance Vector Routing (AODV) is a novel algorithm for the operation of such networks. Every mobile host operates as a specialized router, and routes are obtained as needed (i.e., on-demand) with little or no reliance on periodic advertisements. New routing algorithm is quite suitable for a dynamic self-starting network, as required by users wishing to utilize Ad-hoc networks.

Fast internet and formation of wireless technologies provide significant impact on Internet and Communication Technologies [3]. They support of one of famous technique known as Ad-hoc network. Ad-hoc networks are assortment of mobile nodes connected by wireless links and also receiving attention in the scientific community. Ad-hoc networks, routes may be disconnected due to dynamic movement of nodes. The route selection and topology combination is very difficult and challenging issue. To overcome this good neighbor nodes in the network method is adopted which will avoid bad nodes is the network.

This paper [4] tells about wireless Ad-hoc network consisting of a group of wireless nodes which can dynamically self-organize themselves into a temporary topology to form a network without using any existing infrastructure. Node mobility is one of the significant factors that decreases the performance of Ad-hoc networks and restricts network stability. In this work, we propose a method for identifying set of reliable adjacent nodes in the network and extend the capabilities of AODV routing protocol. Simulation results show that the approach used is better than the traditional AODV routing protocol.

Mobile Ad-hoc networking has been an active research area for several years. To stimulate cooperation among selfish mobile nodes, is not well addressed yet. In this paper [10], Sprite, a simple, cheat-proof, credit-based system for stimulating cooperation among selfish nodes in mobile Ad-hoc networks. This system provides incentive for mobile nodes to cooperate and report actions honestly.

III. Design and Implementation of Proposed Model

The proposed model is designed and implemented for isolating selfish nodes in Ad-hoc network. Perfect information game theory is used for the implementation of the model. Perfect information game theory, is a non-cooperative game theory which focus on agents who make their own individual decisions without coalition.

Forwarding of the information from one node to other is done by the waste of energy which is spent in receiving and forwarding of the information. They are classified into normal nodes and selfish nodes. The normal nodes transfer the information until the information reaches the final destination node whereas the selfish nodes will pretend to act like normal node until threshold energy value is met, after that they will start forwarding the information.

A. Block Diagram of Behavior of Selfish Node in Ad-Hoc Network

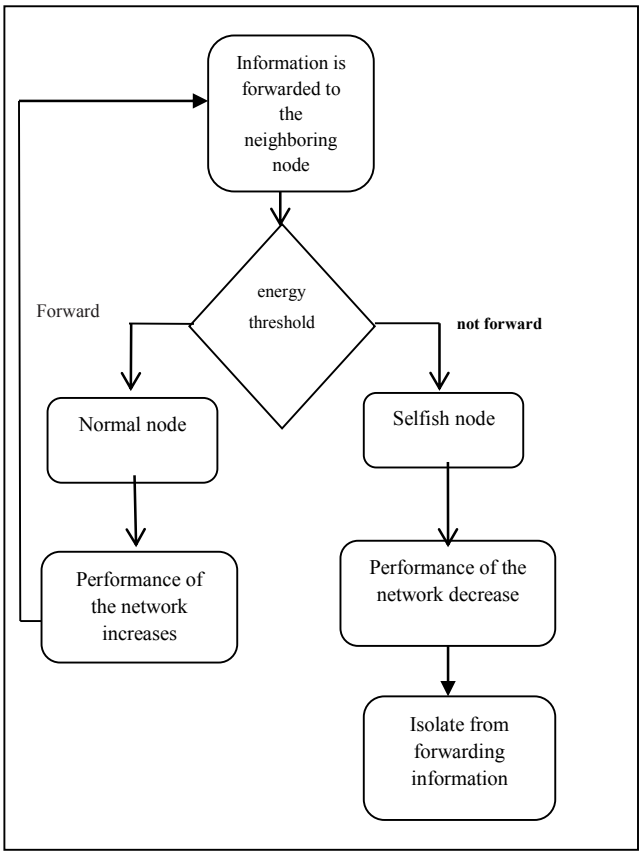

Fig. 1: Block Diagram of Selfish Node in Ad-Hoc

The block diagram shown in the Fig. 1 shows the effect of selfish node in the Ad-hoc network. Source node starts forwarding the information to the neighboring node. The neighboring node checks the energy of itself with threshold energy which is fixed. Based on this the selfish node will decide whether to forward the information or not. The normal nodes will not put such condition when forwarding of the information is done.

B. Implementation of Proposed Model Using Perfect Information Game Theory

The game tree in Fig. 2 gives the information when to forward the information in the Ad-hoc network. The tree starts with main node which is the normal node. The values in the edges of the tree give the value of the payoff. Two cases are considered in this decision tree. First case when both nodes are normal nodes and second case when one node normal node and the other node is selfish node.

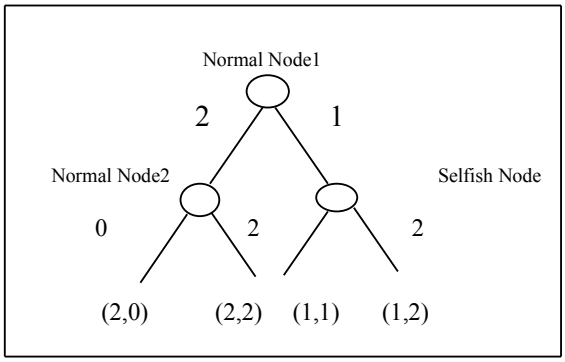

Fig. 2: Game Tree for Node Forwarding the Information Nodes in the Ad-Hoc Network

i. Case 1: Both Nodes Are Normal:

When both the nodes are normal, i.e., if one node is the source node and the other node is the neighboring node to which forwarding of the information is done. The normal node 1 forward the information to the normal node 2 who payoff value is 2. The normal node 2 has two decisions to make. If the payoff is zero it means the energy is totally exhausted and node will not participate in forwarding of the information. If the payoff value is 2 it means that it is ready to forward the information to next node. So the (2,2) is Nash equilibrium where the information is forwarded to next node.

ii. Case 2: One Node is Normal Node and Other Node is Selfish Node

When one node is normal node and the other node is selfish node. The normal node payoff value is 1 and next node is the selfish node. The selfish node take two decision to forward the information when the payoff value is 2 but the normal node 1 pay is less compared to the selfish node payoff so it is not Nash equilibrium. When the payoff value is 1 of the normal node 1 and payoff value of selfish node is 1. Here also Nash equilibrium is not met as the payoff value are (1,1) of the normal node 1 and selfish node. So the normal node 1 will not forward the information to the selfish node in the Ad-hoc network.

IV. Algorithm Using Perfect Information Game Theory for Isolating Selfish Nodes

This section has two algorithms. For sender node when checking energy in the nodes during transmitting and second algorithm is written for receiving packet and checking for energy is done for all nodes.

A. Algorithm 1: Sender Module

The algorithm 1 is used for sender module implementation. Firstly the energy is set for all nodes and threshold value is being specified. The node is checked whether the node is destination or not. If the node is neighboring node the information is forwarded and it checks whether the energy of the node is less than threshold energy if so other path is found out else forward the information. This process is being repeated until the node reaches the destination node.

Algorithm 1: Sender Module to Avoid Selfish Node

Step 1. Set the energy to all the nodes.

Step 2. Set the threshold value specifically for all nodes.

Step 3. Start the simulation.

Step 4. If the Nn(current node) = Nd(destination node)

Step 5. Packet forwarded to neighboring nodes.

Else go to step 8.

Step 6. If the energy of node is less than threshold energy.

Step 7. Compute the other path.

Else go to step 6.

Step 8 . Forward the data packet to neighboring node.

Step 9. If the Nn(current node)=Nd(destination node)

Step 10. End the process.

Else go to step 4.

B. Algorithm 2: Receiver Module

The algorithm 2 is the receiver module. Firstly, the energy is set for all nodes and threshold value is being specified here in order to isolate the selfish node if present. Then the node is checked whether the node is destination or not. Then packet is being forwarded and it checks whether the energy of the node is less than threshold energy if so, then compute the other path, else receive the information to be forwarded. This process is being repeated until the node reaches the destination node.

Algorithm 2: Receiver Module to Avoid Selfish Node

Step 1. Set the energy to all the nodes.

Step 2. Set the threshold value specifically for all nodes.

Step 3. Start the simulation.

Step 4. If the Nn(current node) = Nd(destination node)

Step 5. Packet forwarded to neighboring nodes.

Else go to step 8.

Step 6. If energy of node is less than the threshold energy.

Step 7. Compute the other path for receiving.

Else go to step 6.

Step 8. Receive the data packet.

Step 9. If the Nn(current node) =Nd(destination node)

Step 10. End the process.

Else go to step 4.

V. Result and Analysis

Result and analysis is carried on for different cases studies. There are mainly two cases considered. The Case Study 1 deals about the comparison of static and dynamic topology without the application of game theory. The network performance is observed by calculating the throughput and End-to-End delay. The Case Study 2 deals about the comparison of static network with and without the perfect information game theory approach.

A. Case Study 1: Comparison of Static and Dynamic Topology without Game Theory

In this case study the comparison is done between static and dynamic nodes in the Ad-hoc network without using game theory. The throughput and End-to-End delay is calculated.

In the graph, grey line refers to dynamic and the black line refers to static network topology respectively. Graph x-axis refers to number of selfish nodes and y-axis refers to throughput. Throughput keeps on decreasing both in static and dynamic Ad-hoc network as the number of selfish nodes increases.

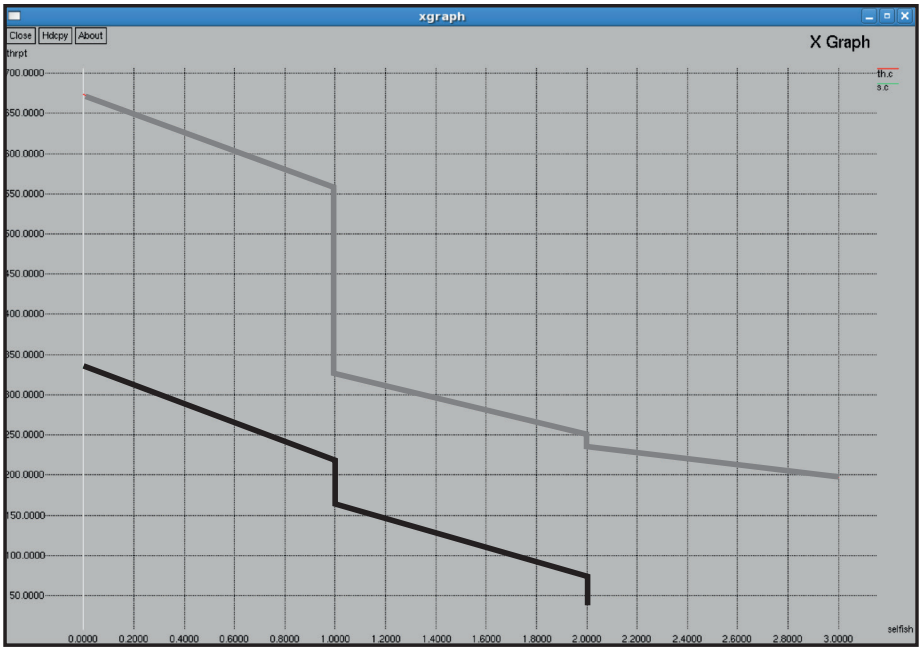

Fig. 3: Graph of Throughput Static V/S Dynamic

End-to-End delay refers to the time taken for a packet to be transmitted across a network from source to destination. The Fig. 4 here illustrates the End-to-End delay in static and dynamic network topology and the grey line indicates the dynamic topology End-to-End delay graph and black line indicates the static topology End-to-End delay.

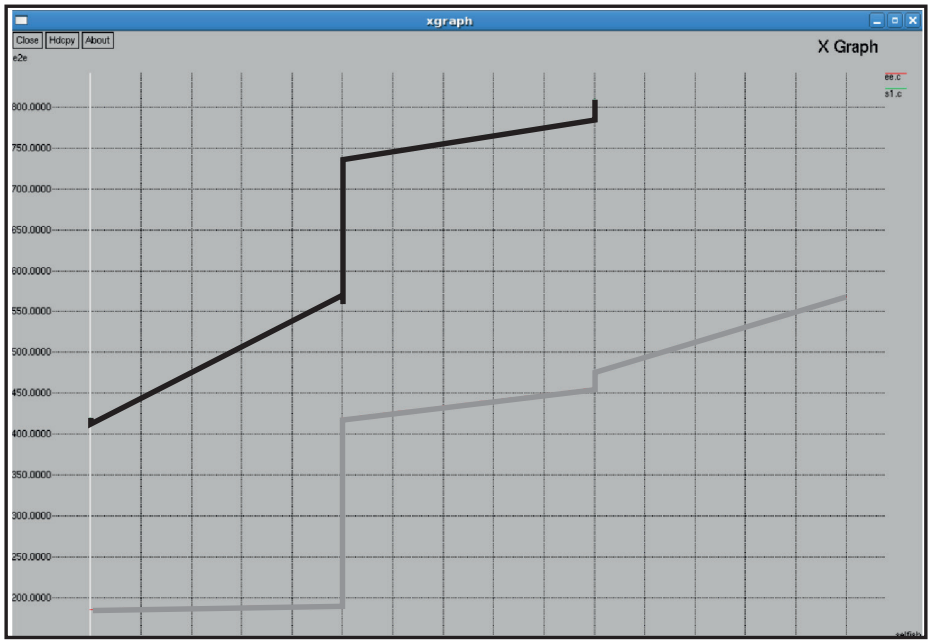

Fig. 4: Graph of End-to-End Delay Static V/S Dynamic

B. Case Study 2: Comparison of Static with and without Game Theory Application Respectively

In this case study, static and dynamic network topology with the application of game theory is simulated using Ns2 simulator. The throughput and End-to-End delay is calculated. The Table II is shown for static network with and without the application of the perfect information game theory.

TABLE I: TABLE OF COMPARISON WITH STATIC NETWORK AND DYNAMIC NETWORK WITHOUT GAME THEORY

	Throughput		End-to-End Delay	
Number of Selfish Node	Selfish Node=1	Selfish Node=2	Selfish Node=1	Selfish Node=2
Static without Game Theory	225	250	558	775
Dynamic without Game Theory	554	75	198	452

TABLE II: COMPARISON OF STATIC NETWORK WITH AND WITHOUT THE APPLICATION OF GAME THEORY

	Throughput		End-to-End Delay	
Number of Selfish Node	Selfish Node=1	Selfish Node=2	Selfish Node=1	Selfish Node=2
Static without Game Theory	102.065	53.476	430.725	717.237
Static with Game Theory	120.098	90.033	314.251	650.492

The throughput for static network with game theory and without game theory is shown in Fig. 5. Where grey line refers to throughout of static network without the application of perfect information game theory and the black line refers to static network with the application of the perfect information game theory respectively. Graph x-axis refers to number of selfish nodes and y-axis refers to throughput.

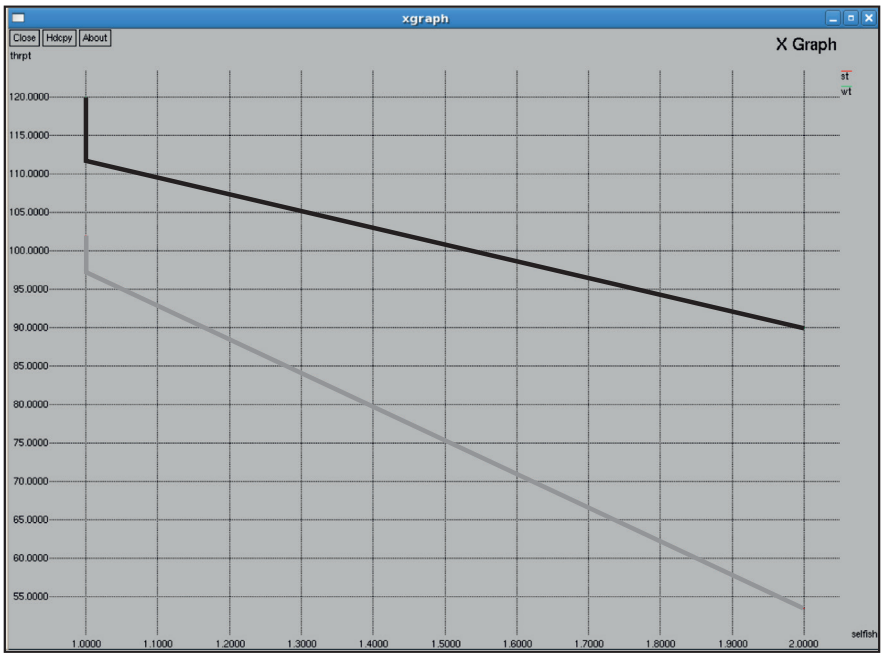

Fig. 5: Graph of Static Network of Throughput with and without the Application of Game Theory

With the application of game theory it can be observed that there will be increase in the throughput as shown in the graph. Hence, better network performance.

The Fig. 6 here illustrates the End-to-End delay in static network with and without the application of the perfect information game theory. The grey line indicates the static network with the application of game theory End-to-End delay graph is obtained and black line indicates the static network End-to-End delay without the application perfect information game theory.

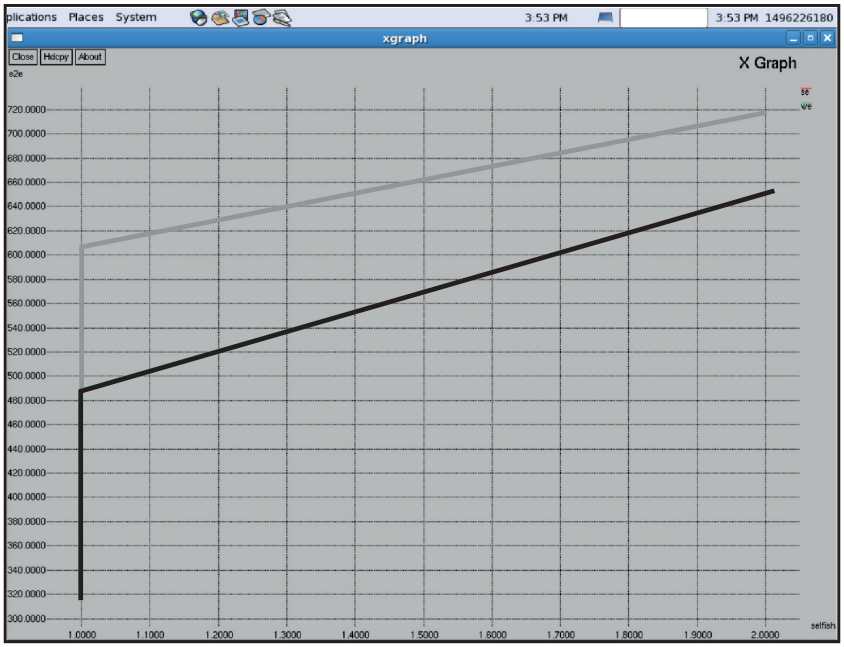

Fig. 6: Graph of End-to-End Delay Static V/S Dynamic

The x-axis in the Fig. 6 is number of selfish node and y-axis refers to the End-to-End delay. End-to-End delay is also referred to as one-way delay. By applying the game theory, there will be decrease in the End-to-End delay as compared with the graph of without applying game theory of Case Study 1.

VI. Conclusion

This paper uses the game theory concept perfect information game theory for isolating the selfish nodes from the Ad-hoc network. The performance of the Ad-hoc network is found for the static as well as dynamic network for normal behavior and also for the selfish behavior of the nodes. By using game theory concept the performance of the Ad-hoc network is improved in both types of Ad-hoc network static and dynamic.

Future Scope: Energy can be allocated dynamically to the nodes and eliminating the selfish nodes using the concept of game theory.

References

1. P. Patil, "Good neighbour node detection technique in Manets using QOS GNDA," *International Journal of Innovative Research in Engineering and Management (IJIREM)*, vol. 2, no. 3, pp. 43-48, May 2015.
2. C. E. Perkins, and E. M. Royer, "Ad-hoc on demand distance vector routing," *Second IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, IEEE, 1999.
3. U. Singh, B. V. R. Reddy, and M. N. Hoda, "GNDA: Detecting good neighbor nodes in Adhoc routing protocol," *Second International Conference on Emerging Applications of Information Technology (EAIT),* pp. 235-238, IEEE, 2011.
4. T. R. Reddy, and N. Sobharani, "Selective on-demand protocol for finding reliable nodes to form stable paths in ADHOC networks," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET),* vol. 1, no. 5, pp. 21-24, 2012.
5. S. Gupta, C. K. Nagpal, and C. Singla, "Impact of selfish node concentration in MANETs," *International Journal of Wireless and Mobile Networks (IJWMN),* vol. 3, no. 2, pp. 29-37, April 2011.
6. R. S. Komali, A. B. MacKenzie, and R. P. Gilles, "Effect of selfish node behavior on efficient topology design," *IEEE Transactions on Mobile Computing*, vol. 7, no. 9, pp. 1057-1070, September 2008.
7. Md. A. K. Akhtar, and G. Sahoo, "Mathematical model for the detection of selfish nodes in MANETs," *International Journal of Computer Science and Informatics (IJCSI)*, vol. 1, no. 3, pp. 25-28, n.d.
8. G. Soni, and K. Chandravanshi, "A nobel defence scheme against selfish node attack in MANET," *International Journal on Computational Science and Applications (IJCSA)*, 2013. Available: arXiv:1307.3638
9. T. V. P. Sundararajan, and A. Shanmugam, "Performance analysis of selfish node aware routing protocol for mobile ad hoc networks," *Computer Networks and Internet Research Journal*, vol. 9, no. 1, pp. 1-9, Delaware, USA, July 2009.
10. S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," *Proc. INFOCOM*, March-April 2003.