# An Experimental Analysis on Selfish Node Detection Measures and Methods

**Sumiti, Sumit Mittal**

*Abstract*: ***Mobile network is an open space network that suffers from various internal and external attacks. Selfish node is one such attack form that occurs in intermediate nodes. In this paper, the work behavior and characterization of selfish node is explored. The paper has presented three different algorithms called token based, agent based and watchdog methods to detect selfish node attack. The characteristics and the work behavior of these methods is provided in this paper. These methods are simulated on a mobile network. The analysis results shows that the token based method has achieved the better packet communication, byte communication ratio and reduced the communication loss. The watchdog and agent based method also performed better in terms of lesser communication delay.***

***Index Terms*: Mobile Network, Malicious Node, Selfish Node, Selfish Node Detection Method.**

## I. INTRODUCTION

A Mobile network is the infrastructure less networks which are not controlled by any centralized device. The nodes in the network are independent with individual specifications. The neighbour mobile nodes are responsible to generate the communication route by participating as intermediate node. These forwarders not only challenge the network security, but the workload on mobile nodes also increases. To improve the communication reliability, there is the requirement to observe the requirement and behaviour each individual node. The communication improvement can be achieved at the architecture level, routing level, authentication level or the security level. The resource adaptive evaluation can be regulated by the administrative authority to control the resource consumption. The positional, zonal and the application driven aspects are also analysed in a more critical network. Mobile networks can exist in open space or it can exist in indoor region. The application is driven restrictions can be defined at node, network and architecture level. One of the critical challenges in mobile network is in terms of intermediate participation nodes. These nodes can be some internal or external nodes. These nodes can affect the network performance, integrity and reliability. The nodes can either intentionally capture the valid communication contents or becomes the part of disruption because of own communication tasks. Because of this, there is the requirement to evaluate the reputation and performance of each node.

Various methods, measures and formulas are available to evaluate the node, network and route. The evaluation can be respective to some specific attack or can be generalized form. The paper has explored some of the methods and measures used by earlier researchers for selfish node detection. To identify the selfish node, the first requirement is to identify the misbehaving node in the network. Such kind of misbehaving nodes is called malicious node. Later on the dedicated check can be applied to identify the selfish node.

### A) Malicious Node:-

Any node which is acting abnormally and disrupt the communication is considered as malicious node. These malicious intermediate nodes either delay the communication or captures the delivering information. The abnormal communication frequency of some node, connectivity observation or the response time evaluation can be taken to identify the malicious status of a node. At first level, some authentication check can be applied to verify the node existence. If the node is internal and having a verified identity, then it is required to observe the behaviour to recognize it as malicious node.

### B) Selfish Node:-

Selfish node is one of the common forms of malicious node that captures the communication anonymously. A node that supports the selfish behaviour will not transfer the resources or data to other nodes.

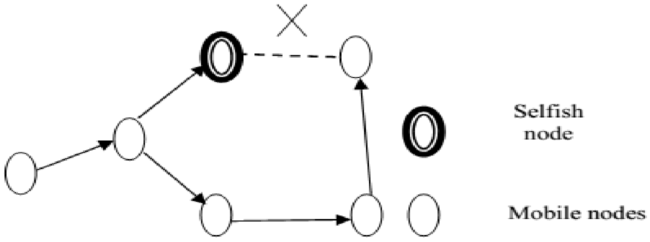

**Figure 1**: Selfish Node

The selfish behaviour of nodes is shown here in figure 1. The figure shows that, as the intermediate node act as selfish node, it stops forwarding the data packets or other information. When the neighbouring nodes of a node are listed and evaluated, the selfish node gives the positive response as of any other mobile node. But, as it gets the responsibility to act as intermediate forwarder, It accepts the communication but not forward it. In this way, all kinds of incoming packets are discarded by the selfish node to provide final delivery. Selfish node increases the packet drop and increases the communication delay.

**Revised Manuscript Received on June 22, 2019.**

**Sumiti,** Research Scholar, M. M. Institute of Computer Technology and Business Management, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala (Haryana), India.

**Dr. Sumit Mittal,** Professor, M. M. Institute of Computer Technology and Business Management, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala (Haryana), India.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

To improve the communication, integrity, it is required to resolve the selfish node problem at an earlier stage. In this paper some of the methods and measures of selfish node detection are explored.

Security in mobile network compromises because of various network attacks. Selfish node is one such attack that disrupts the communication by capturing the network traffic. In this paper, the characterization of selfish node and the countermeasures are presented. In this section, the exploration of network criticalities is provided. The selfish node and its behaviour are also described in this section. In section II, the work provided by earlier researchers is explained. In section III, some of the common methods for selfish node detection are described. Comparison between them is described in section IV. In section V, the conclusion of work is presented.

## II. LITERATURE REVIEW

Selfish node is the critical internal node attack that captures the communication and increases the communication loss. Various researchers have defined different methods for detection and prevent selfish node over the network. Some of the contributions of earlier researchers are discussed in this section. Wang et. al.[1][2] has identified the selfish node and generated a trustful multipath routing for a mobile network. Author defined work as an improvement to AOMDV protocol. Author also reduced the communication overhead over the balanced network. Das et. al. [3] has applied a new game theory scheme to detect the selfish node in mobile networks. Author used the least total cost factor on packet transmission to identify the cost effective path. The featured method identified the damaged path as well as identified the next available ranked path to ensure data delivery. Ramya et. al. [4]. Identified the issues and effects of selfish node on this dynamic network. The behavior of selfish node and detection method applied by different researchers was also identified by the author. A fuzzy based trust model for selfish node detection was provided by Ullah et.al. [5]. Author applied the neighbor node analysis to identify the cooperative behaviour of mobile nodes. Trust value based fuzzy functions are defined to categorize the node and the attack criticality. Based on the number of packet dropped and generated, seven different trust classes are defined. While performing the communication, the nodes with higher trust reputation and selected. Chakrabarti et. al. [6] has defined a two hops reputation analysis scheme to rate the node and to detect the selfish node dynamically for Delay Tolerant Network. A cooperative communication pattern analysis at node level is defined to select the forwarder. The trusted authority is defined to generate the reputation matrix for effective route formation. Das et. al. [7] has defined a method to observe the neighbor nodes based on available resources in terms of memory, bandwidth and battery power. A time scheduled analysis on communication traffic was defined to identify the attacker node in sensor network. Author applied different limits to recognize the fully and partial selfish node in the network. Chakrabarti et. al.[8] has defined a new observer based distributed method to detect the selfish node in Delay Tolerant Network. The observer node used the dynamic reputation scheme based on individual, group and periodic statistical observations applied on nodes. The performance evaluation was provided by the author to generate the secure communication path. The encrypted token analysis with reputation evaluation was provided by the author. Muthumalathi et. al.[9] has developed a selfish node detection algorithm based on non-cooperative action analysis. A secure hill cipher algorithm was applied at network nodes to reduce the communication cost. Author also utilized the memory usage and improved the communication throughput. Ciobanu et. al. [10] has defined a noval collaborative method based on content and context data analysis for selfish node detection. The neighbor node analysis was defined by the author through gossiping and identify the reliable intermediate node. The node level evaluation was defined for opportunistic routing in mobile network. Wei et. al. [11] has defined a method to analyze the neighbor node for assigning the node degree and to locate the punishing node. The total forwarding probability under energy and communication in rate parameters was defined by the author. These parameters were trained by using game theory method to generate the effective network route. Orallo et. al. [12] has setup a collaborative watchdog on a selective, effective node to monitor the covered region. The evaluation matrix was defined by the author based on the probabilistic estimation on neighbor nodes. The transient state analysis was defined to identify the most effective neighbor. Gunasekaram et. al. [13] has applied contention control method based on random backoff time analysis. The parameter specific evaluation for slot time was defined under communication statistics. Based on this observation, the misbehaving node are located and safe communication was performed by the author. Sharma et. al. [14] has refined a method to evaluate the selfish degree of each node for Delay Tolerant Network. The cooperative node evaluation for distributed network was defined by the author. The implicit and explicit communication parameters were considered to improve the accuracy of misbehaving node identification. Tarannum et. al. [15] has defined a distributed analysis method to detect the selfish node in mobile networks. The local and global communication statistics of neighbor node were processed and collaborative decision making was applied to generate the effective network path. The local reading and response was processed by the author to improve neighbor response. Saeed et. al. [16] has defined a cooperative communication analysis framework to identify the resource usage in the network. Author analyzed the unstructured network based on trust values and created an oversight preventive mechanism against selfish node attack. The evolved framework first ranked the trusted nodes and later on generated the preventive route in P2P network. Yokoyama et. al. [17] has categorized various security issues in reference to the selfish node attack. The node behavior was evaluated by the author with timeout and relay constraints. Author defined the countermeasure method to avoid the attacker nodes and to generate the preventive communication route. Djenouri et. al. [18] described a resource utilization based method to identify the selfish node in mobile networks. The node behavior along with packet forwarding was analyzed by the author. The potential threat analysis along with QoS (Quality of Service) was evaluated by the author. The security requirement and the attack mitigation methods were explored by the author. Author reduced the average power consumption and the delay. Hussain et. al. [19] has defined a performance measure to evaluate the resource consumption and network communication at node level and network level. Author defined the proactive method to observe the network behavior and highlight the abnormal behavior of nodes. A watchdog architecture was defined by the author list the critical nodes and to generate the preventive path. Jangra et.al. [20] has defined the authentication preserved reputation method to identify the attacker node and to generate the preventive path in mobile networks. A route reconstruction method based on the communication neighbor information was defined by the author. Sumiti et. al. [21] has defined the different routing approach under the network scenario and strength specification. And different routing constraints and challenges are explored. Sumiti et. al. [22] has defined nearest neighbor analysis to detect the selfish node in the active path and generate the secure path. Existing AODV protocol is modified and a new bit is taken to define the trustful status. This technique is able to detect almost 90% selfish nodes in the active path. Sumiti et. al. [23] has defined a Agent based technique for identifying the passive paths selfish nodes. The proposed technique is able to isolate selfish nodes easily and increase the security of network at a minor cost of overhead in coordinating nodes. Tamilarasi et. al. [24] has enhanced the security measure to detect the selfish node. Author also integrated the cryptographic algorithm to improve the authentication behavior and to reduce the energy consumption. The method improved the packet delivery ratio and reduced the routing overhead. Kashyap Balakrishnan et. al.[25] has define a TWOACK Technique to detect the selfish nodes. This technique improves the 20% packet delivery ratio in the network. P. Sankareswary et. al. [26] proposed the Multicast Ad-hoc on demand distance vector protocol. In this paper work is performed on RREQ method. In this paper packet delivery ratio is 25% and control overhead decreased 20.5%. Sandeep A. Throat et.al. [27] Proposed a opportunistic Routing protocol. This technique is proposed for non-forward data packets and this technique improves the 10% packet delivery ratio in the network.

## III. SELFISH NODE DETECTION

The researchers have already provided various methods to detect and prevent the selfish nodes in mobile network. In this section, some of the common attack detection methods are defined and discussed. These methods are categorized as token based method, agent based methods and watchdog method.

### 3.1 Token based Method

In this approach, some token[28] or incentive is distributed in the neighbor nodes to identify the selfish node. At the earlier stage, a RREQ is generated on the neighboring node to analyze the behavior of the nodes. The previous node here works as the monitor to observe the behavior of next intermediate node. In this method, the nodes are having the token with ID and status. As the next intermediate node sends the RREQ packets, the previous immediate node observe the behavior of communication. Based on this observation, the normal and selfish nodes are identified. The behavior information of nodes is also shared with the neighbor nodes using these tokens. The RREQ packet is communicated and relatively the node status is set. The node sends the RREQ packet and set the status of effective immediate neighbor. If the RREQ packets are node distributed by the node, then the status is set as red which means the node is not allowing forwarding and the node is selfish node. This process is repeated on all nodes in the path till the complete safe path is not formulated. The functional process for path generation using token based approach is provided in table 1.

**Table 1:** Algorithm for Token based Method

1. Set the source and destination for path generation
2. Destination D set the umpire node for observation
3. Umpire node forward list of neighbors to previous node
4. Previous node tally the list respective to own list and identify the interaction with received neighbor list
5. Perform interaction analysis to identify next umpire
6. The neighbor list is transferred to the adjacent umpire
7. Each time the interaction analysis is done to identify the effective neighbor
8. The process is repeated till the source node not occurs and the path is not formed.

Algorithm I provided the behaiovr of selection of the umpire node and to perform the analysis on the neighbor node. Each time, the neighbors are identified; the interaction analysis is done based on different parameters. The tokens are used to transmit this inform in secure way and to perform the analysis to generate the weights. The node with lesser weight or interaction is considered as the selfish node. This process is repeated from destination to source node till the complete safe path is not generated.

### 3.2 Agent based Method

The agent based approaches uses the external agents [29] to monitor the region. These agents are not actually participating in the communication. They only observe the nodes and take the decision on the node status based on the communication behavior of these nodes. The agents are able to collect the information of nodes and their neighbors in the network. In this method, at first the agents are placed in the network. These agents are placed to cover the region and the nodes. Once the agent roles are assigned, the agent start monitoring the nodes in the region. As the communication begin and the RREQ packet is sent to next intermediate node. The node level cooperation and communication is analyzed by the agent node. The network participation and activity analysis is performed to identify the cooperative behavior of nodes. The observation technique is applied by the agent to observe the node behavior for its neighbor nodes. Based on this analysis, the identification of normal and selfish node is performed.

The message count information is collected and maintained in the form of a table. The evaluation on this table information is done to identify the normal nodes. The range based analysis is applied to identify the selfish behavior of nodes. Once all the normal nodes in the path are done, whereas the safe path is generated over the network. The algorithm for agent based selfish node detection is provided in table 2.

**Table 2:** Algorithm for Agent based Method

1. Define the centralized controller node
2. Distribute the k agents in the network
3. Each agent identify the nodes in the coverage
4. Share the routing table amount the cover nodes
5. Find the current status of node
6. Observe the load and loss rate for each node
7. Apply threshold limit to identify the selfish and safe node
8. Agent will exclude the selfish node
9. Connect with other agents to generate the safe path

Table 2 has provided the algorithm for agent based selfish node detection and route generation. The algorithm shows that the agents are distributed in the network by a controller node. Each agent is having its coverage region. The node communication features are analyzed by these agent nodes. The load and loss rate are the key factors used to identify the selfish and normal nodes. Once all the normal nodes are identified in the region, the agent identifies the effective nodes over the path and generate the safe path.

### 3.3 Watchdog Method

The watchdog [31] based method is a behavior monitoring method in which a gateway based analysis is performed in the network nodes. The watchdog filters the nodes based on the node behavior and selects the nodes which are actually affecting the communication. In this method, the RREQ message is broadcasted while performing the communication between source and destination nodes. The receiver node accepts the route request from previous node and performs the test based on the available communication information. The monitoring is performed on all the activities held by the intermediate to identify the misbehavior or suspicious node. The watchdog method performs the neighbor specific test for certain period of time. The identification of suspicision node is identified by applying the threshold to the communication values. The node status is set 0 or 1 based on the normal and selfish nodes. The destination analysis based method is applied to identify the participation to the nodes and to generate the safe path in the network. The algorithm for watchdog based selfish node detection method is provided in table 3.

**Table 3:** Algorithm for Watchdog based Method

1. Set two nodes as selfish and 2 as malicious nodes
2. Find immediate neighbors for all nodes in the network
3. Initialize the watchdog system for monitoring then node behavior
4. Share the information of selfish nodes to every node
5. Perform watchdog based evaluation on NONINFO nodes to identify selfish node
6. The node that identify the selfish node set it as positive
7. If a node provide false information about selfish node, set it as Negative node
8. Perform reputation estimation based on watchdog and indirect information
9. Block all selfish nodes and generate safe route path between source and destination.

Table 3 has provided the method for selfish node detection using watchdog based approach. In this approach, two nodes are defined as the selfish nodes and malicious node. The watchdog system is enabled and the analysis is performed on the neighbor nodes. The neighbor list is generated and the communication features are analyzed by the nodes. The response of the nodes is analyzed to identify the selfish and safe nodes. Once all safe nodes are identified, the safe route is generated between the source and destination nodes.

## IV. RESULTS

The methods discussed in the previous sections are experimented in NS2 environment by generating a scenario with mobile nodes. The network is defined with the specification of selfish nodes. The communication is performed between the node pair. The AODV protocol is considered for routing and to perform data delivery. The handling of the selfish node is token based, agent based and watchdog methods. The parameters considered to generate the network scenario are provided in table 4.

**Table 4:** Network Scenario

| Properties | Value |
|---|---|
| Network Size | 3000x2000 mtr |
| Number of Nodes | 49 |
| Simulation Time | 100 sec |
| Protocol | AODV |
| Energy model | Yes |
| MAC Protocol | 802.11 |
| Topology | Random |
| Packet Size | 512 Byte |

The network is established in larger network area with specification of 49 nodes. The communication is performed for 100 seconds and the attack handling is done using token based, agent based and watchdog methods. The comparative evaluation of these methods is done using packet communication, packet loss, bytes and packet delay parameters. In this section, the comparative results are provided using graphs.

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

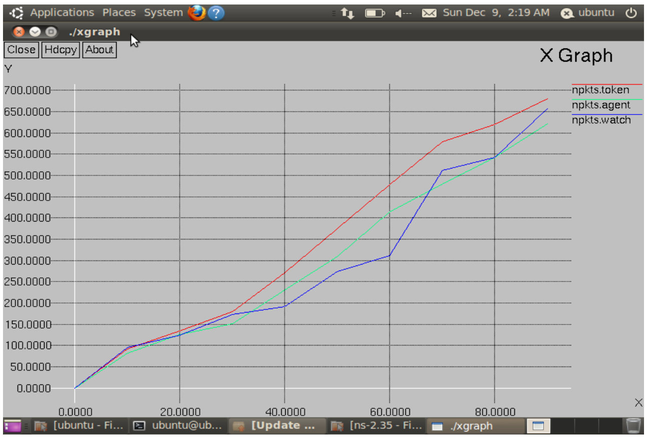

**Figure 2:** Packet Communication Analysis

Figure 2 has provided the comparative analysis of token based, agent based and watchdog methods using packet communication parameter. In this figure, x axis represents the simulation time and y axis represents the number of packets successfully communicated. The figure 2 shows that the packet communication using token based method is slightly better than agent based and watchdog methods. The packet communication parameter represents the communication throughput. Based on this parameter, the effectiveness of communication method is analyzed. The results show that the token based method provided the better results than other two methods.

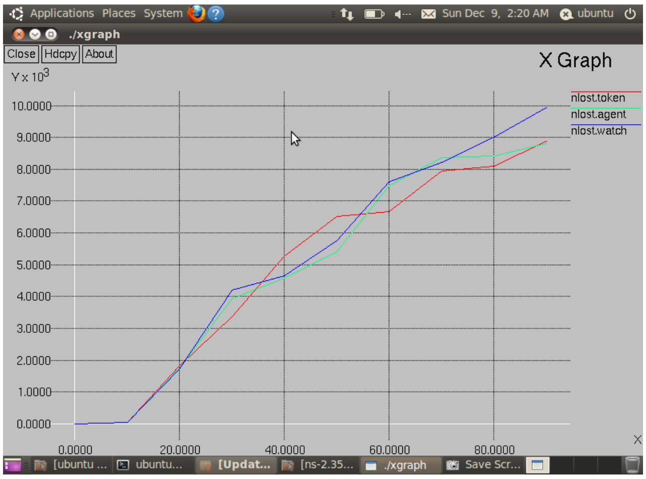

**Figure 3:** Packet Loss Analysis

Figure 3 has provided the analysis of the token based, agent based and watchdog methods using packet loss parameter. The packet loss occurs in the network because of the existence of selfish node. As the selfish node accepts the packet, it does not forward to next neighbor and the loss occur. The figure 3 shows that the communication loss is almost same earlier. But later, as the communication performed, the token based method works more effectively and the communication loss decreases. Whereas the communication loss in case of watchdog method is increasing in same ratio constantly.

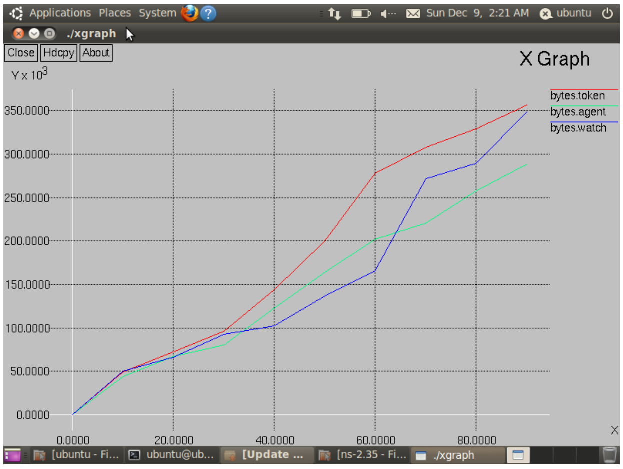

**Figure 4:** Byte communication Analysis

The byte communication is the parameter to observe the communication effectiveness is a network. If the network is infected by selfish node attack, then the byte communication over the network is also affected. The figure 4 is showing the byte communication in the network. In this figure, x axis shows the simulation time and y axis shows the bytes communicated in the network. The comparative results show that the byte communication in case of token based method is higher than agent based and watchdog methods.

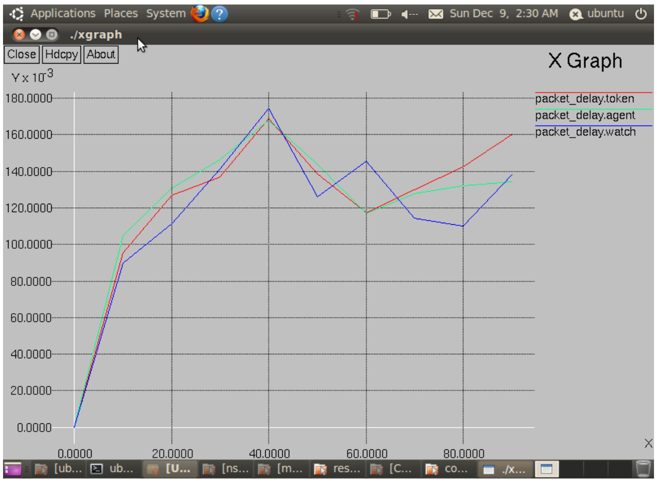

**Figure 5:** Packet Delay Analysis

The communication delay represents the time taken to deliver the packet between the source and destination. The higher delay affects the efficiency of the communication. The figure 5 shows that the earlier the delay of all methods is same. But as the communication performed, the delay in case of watchdog method is reduced. The watchdog method performed better than other methods in terms of packet delay. The comparative analysis of these three methods in numerical form is provided in table 5. Table clearly shows that the token based method has performed better among all these methods with higher packet delivery ratio and lesser packet loss and communication delay.

**Table 5:** Comparative analysis of all methods

| | Token Based | Agent based | Watch-dog |
|---|---|---|---|
| Packet Transmission Ratio | 64.13% | 59.13% | 61.23% |
| Byte Transmission | 68.89% | 53.55% | 67.19% |
| Packet loss | 35.87% | 40.87% | 38.77% |
| Packet Delay | 160.13ms | 137.58ms | 139.02ms |

## V. CONCLUSION

Selfish node can act in different forms and with different characterization in mobile networks. In this paper, an exploration to the Selfish node and its working behavior is provided. The paper also provided the three different algorithms to recognize three different forms of selfish nodes. The existing token based, agent based and watch dog methods are discussed with their relevant approaches. These methods are also simulated in a random mobile network in existence of selfish nodes. The comparative results are obtained in terms of packet communication, bytes communications, packet loss and delay parameters. The result shows that the token based method provided the effective results for packet communication, byte communication and packet loss parameters. Whereas, the results of packet delay are mixed and the delay in case of watchdog and agent based is better than token based method.

## APPENDIX

It is optional. Appendixes, if needed, appear before the acknowledgment.

## ACKNOWLEDGMENT

## REFERENCES

1. Yongwei Wang, Venkata C. Giruka, Mukesh Singhal, Truthful multipath routing for ad hoc networks with selfish nodes, Journal of Parallel and Distributed Computing, Volume 68, Issue 6, June 2008, Pages 778-789
2. Yongwei Wang, Mukesh Singhal, On improving the efficiency of truthful routing in MANETs with selfish nodes, Pervasive and Mobile Computing, Volume 3, Issue 5, October 2007, Pages 537-559
3. Debjit Das, Koushik Majumder, Anurag Dasgupta, Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory, Procedia Computer Science, Volume 54, 2015, Pages 92-101
4. N. Ramya and S. Rathi, "Detection of selfish Nodes in MANET - a survey," 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, 2016, pp. 1-6
5. Z. Ullah, M. S. Khan, I. Ahmed, N. Javaid and M. I. Khan, "Fuzzy-Based Trust Model for Detection of Selfish Nodes in MANETs," 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, 2016, pp. 965-972.
6. C. Chakrabarti, S. Chakrabarti and A. Banerjee, "A dynamic two hops reputation assignment scheme for selfish node detection and avoidance in delay tolerant network," 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, 2015, pp. 345-350.
7. S. K. Das, B. J. Saha and P. S. Chatterjee, "Selfish node detection and its behavior in WSN," Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on, Hefei, 2014, pp. 1-6.
8. C. Chakrabarti, A. Banerjee and S. Roy, "An observer-based distributed scheme for selfish-node detection in a post-disaster communication environment using delay tolerant network," Applications and Innovations in Mobile Computing (AIMoC), 2014, Kolkata, 2014, pp. 151-156.
9. N. Muthumalathi and M. M. Raseen, "Fully selfish node detection, deletion and secure replica allocation over MANET," Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on, Coimbatore, 2013, pp. 413-415.
10. R. I. Ciobanu, C. Dobre, M. Dascalu, S. Trausan-Matu and V. Cristea, "Collaborative selfish node detection with an incentive mechanism for opportunistic networks," 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), Ghent, 2013, pp. 1161-1166.
11. Wang Xing-Wei, D. P. Qu and M. Huang, "Selfish nodes detection mechanism and stimulation mechanism over mobile peer-to-peer networks," 2012 7th IEEE Conference on Industrial Electronics and Applications (ICIEA), Singapore, 2012, pp. 1030-1034
12. 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," in IEEE Communications Letters, vol. 16, no. 5, pp. 642-645, May 2012.
13. R. Gunasekaran, V. Rhymend Uthariaraj, R. Sudharsan, S. Sujitha Priyadarshini and U. Yamini, "Detection and prevention of selfish and misbehaving nodes at MAC layer in mobile ad hoc networks," Electrical and Computer Engineering, 2008. CCECE 2008. Canadian Conference on, Niagara Falls, ON, 2008, pp.
14. A. Sharma, D. Singh, P. Sharma and S. Dhawan, "Selfish nodes detection in delay tolerant networks," Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), 2015 International Conference on, Noida, 2015, pp. 407-410.
15. R. Tarannum and Y. Pandey, "Detection and deletion of selfish MANET nodes-a distributed approach," Recent Advances in Information Technology (RAIT), 2012 1st International Conference on, Dhanbad, 2012, pp. 152-156.
16. S. Saeed, I. Zubair and M. H. Islam, "Detection of selfish nodes in peer-to-peer networks," 2009 First International Conference on Networked Digital Technologies, Ostrava, 2009, pp. 504-507.
17. Shin Yokoyama, Y. Nakane, O. Takahashi and E. Miyamoto, "Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods," 7th International Conference on Mobile Data Management (MDM'06), 2006, pp. 95-95.
18. D. Djenouri and N. Badache, "New approach for selfish nodes detection in mobile ad hoc networks," Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005., 2005, pp. 288-294
19. Hussain, A. Nadeem, O. Khan, S. Iqbal and A. Salam, "Evaluating network layer selfish behavior and a method to detect and mitigate its effect in MANETs," Multitopic Conference (INMIC), 2012 15th International, Islamabad, 2012, pp. 283-289.
20. A. Jangra, Shalini and N. Goel, "e-ARAN: Enhanced Authenticated Routing for ad hoc networks to handle selfish nodes," Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on, Nagapattinam, Tamil Nadu, 2012, pp. 144-149
21. Sumiti and Sumit Mittal, “Characterization of Routing Approaches in Mobile Network: A Study,” International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 4, Issue 10, October 2014, pp. 108-111.
22. Sumiti and Sumit Mittal, “Detecting Selfish Node over the Active Path using Neighbor Analysis based Technique,” International Journal of Science and Research (IJSR), Volume 4, Issue 3, March 2015, pp. 1295-1298.
23. Sumiti and Sumit Mittal, “Identification Technique for all Passive Selfish Node Attacks In a Mobile Network,” International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS), Volume 3, Issue 4, April 2015, pp. 46-51.
24. M. Tamilarasi and T. V. P. Sundararajan, "Secure enhancement scheme for detecting selfish nodes in MANET," 2012 International Conference on Computing, Communication and Applications, Dindigul, Tamilnadu, 2012, pp. 1-5.
25. Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney, “TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Wireless Communication and Networking Conference, 2005, ISBN: 0-7803-8966-2.

26. P. Sankareswary, R. Suganthi and G. Sumathi, "Impact of Selfish Nodes in Multicast Ad Hoc on demand Distance Vector Protocol," International Conference on Wireless Communication and Sensor Computing, (ICWCSC), IEEE, 2010, INSPEC Accession Number: 11140332.
27. Sandeep A. Throat and P. J. Kulkarni, "Opportunistic Routing in Presence of Selfish Nodes for MANET," Wireless Personal Communication, Springer, 2015, Volume 82, issue 2,pp. 689-708.
28. Jebakumar Mohan Singh Pappaji Josh Kumar, Ayyaswamy Kathirvel, Namaskaram Kirubakaran, Perumal Sivaraman, "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT", EURASIP Journal on Wireless Communications and Networking, pp 1-11, 2015
29. Radhika Garg, Sanjay Kumar, Sangeeta Malik, Deepak Goyal, Dr. Pankaj Gupta, An Agent Based Approach to Avoid Selfish Node Dynamically in Mobile Networks, International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, pp 49-53, September 2012
30. Pavithra SL, Prema P. Efficient Detection Of Selfish Node In Manet Using A Colloborative Watchdog. International Journal of Engineering Research and Applications. 2016 Jan 1;6(4):43-5.
31. A. Meeran, N. Praveen A and K. Ratheesh T, "Enhanced system for selfish node revival based on watchdog mechanism," 2017 International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, 2017, pp. 332-337.

## AUTHORS PROFILE

**Sumiti** is completed P.G. in Computer science and Application from Maharshi Dayanand University, Rohtak, Haryana, India and M.phil in CSA from M.M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India. She is a Ph.D Scholar at Maharishi Markandeshwar University. Her research interest includes MANET Security.

**Dr. Sumit Mittal** received his Doctorate & Master's from Kurukshetra University, Kurukshetra. Presently, he is working as Professor & Principal at M.M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India. Two scholars awarded their Ph.D degree under his supervision and currently 8 scholars are ongoing. He has more than 40 publications in International/ National Journals and Conferences. He has chaired number of technical sessions in International/National Conferences. He is a life member of Computer Society of India, senior member of Universal Association of Computer and Electronics Engineers and member of The IAENG Society of Computer Science, Middle East Association of Computer Science and Engineering, Computer Science Teachers Association, Institute for Computer Science, Social Informatics and Telecommunications Engineering. His research area includes Cloud Computing, Computer Architecture, Wireless communication and Distributed Environments.