# Detection of Selfish Nodes Through Reputation Model In Mobile Adhoc Network - MANET

**Muruganantham Ponnusamy[a], Dr. A. Senthilkumar[b], and Dr.R.Manikandan[c]**

[a]Deputy Registrar, Indian Institute of Information Technology, Kalyani, West Bengal, India
[b]Associate Professor, Department of ECE, Kings Engineering College, Chennai, India.
[c]Co-Ordinator& Head, Department of CS, The QuaideMilleth College for Men, Chennai, India

**Article History**: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

**Abstract:**The nodes are placed in open environment and moves randomly from one place to other are vulnerable to security threats in Mobile Adhoc Network (MANET). Therefore the node reputation and energy efficient model is applied in MANET that reduces the inconvenience created by selfish nodes and removes from the system during routing operation. The reputed and energy efficient nodes are identified from the network and the data transmission takes on reliable routes. However in this reputation scheme the malicious nodes are non co-operative with each other.-The reputed nodes are detected through the analysis of communication ratio between the nodes. The simulation result for the proposed model is discussed here and shows the efficiency achieved is better.

**Keywords*:*** Reputation Ratio; Energy Factor; Selfish nodes; MANET.

## 1. Introduction

MANETs comes under ad-hoc network here the nodes moves independently from one location to other characterised with self-organizing abilities (Khan, B. U. I., 2013). Node mobility is one of the primary features of MANET due to dynamic nature and it works under the principle of decentralized system architecture i.e. the tasks are performed at a temporary time interval. Decentralized architecture is defined as that the mobile nodes will not rely on any other nodes for initiation of tasks and performing the same (Raghunandan, G. H., 2017). MANET can be applied in a variety of applications such as military field, medical field, weather monitoring, indoor applications etc. Execution of tasks in a timely manner is significant for the consequences of reliable transmission of data even if the link strength is not so good during communication (Almazyad, A. S. 2018).

Cooperative event of forwarding of packets is presently used method for ensuring the reliability of time-dependent tasks. However, the process of forwarding of packets in MANET is a crucial task due to its mobility nature. If the middle relaying nodes are not chosen properly during the route-set up between source and destination then the possibilities of link failures will be high (Abirami, K. R., 2018). Additionally link failures causes more packet losses that simultaneously increases the events of retransmission process this greatly effects the utility factor of throughput and energy for the strategy of packet forwarding (Bisen, D., 2018).

The nodes in the MANET are self-controlled and it usually operated with limited energy and memory capacity. This makes a node to become self centered and that way it only participates in communication when it brings the node more benefits for its interest than cost (Khan, B. U. I., 2014). The possibility of occurrence of self centered nodes set in the middle of other decisive networking constituent leads to distraction of the generally message and network performance from both security and energy point (Rajesh, M. 2018). Therefore, the trust model is necessary for designing the reliable link routes for processing the packet forwarding approach.

## 2. Related Works

Many works related to the study of reputation and trust models as well as related to false nodes identification and removal of same has been discussed in (Sonekar, S. V., 2020) that introduced a distinct approach of computation termination of selection of Cluster Head (CH) process and on the basis of Finite State Machines (FSM) mechanism a security concept can be employed for identification and mitigation of threats in MANET. Mechanized security approach is discussed in (Mir, R. N. 2020) that is enrolled here for the safety measures of transmission of data which is routed using distributed routing protocol for MANET. Consequences of related study are examined however it still lags in the scope of simulation validation improvement for securing the data that travels over the MANET system.

A research work (Fu, Y., 2019) was carried out for improving the reliability and security measures of AODV routing protocols by implementing strong routing and security measures. This work actively performs against black hole attacks but not other attacks are considered. Performance of security aspects in terms of reputation for DSR (Menaka, R 2020) routing protocols are evaluated in MANET environment. Local positioning model (Monakhov, Y. M., 2019) was proposed in MANET to identify the intruder node. The intruder node tries to stop the normal operation and creates latency problem during routing. Security approach of authentication mechanism (Amin, U., 2018) was proposed for providing communication security as well as proper routing for data transmission in MANET. This process takes very less computation time for node validation process for the nodes which are ready to join in the network.

Game-based Reputation and Trust Scheme (GRTS) (Khan, B. U. I., 2020) was proposed for packet-forwarding process in an intelligent manner. This policy is the combined form of node interactions and forwarding packets and this is formulated with the systematic philosophy in a MANET scenario. This approach considers both possibilities of packet drops and reward factor. Reward factor is considered for the assessment of node reputation. Thereby the self-centred nodes are identified in the network and packet forwarding pattern is carried out for routing the data's reliably.

## 3. Proposed Model

Selfish Node Removal using Reputation Model (SNRRM) is proposed here. The node reputation is determined in order to remove the selfish nodes from routing. The reputation calculation of each node is done through the node's current energy level and its communication ratio. The source node 'S' is set and destination 'D' is set and the communication begins with the sender node. If both 'S' and 'D' falls under the communication range the node checks only for 'S' reputation value, if matches the transmission process is done and the updates the system. If both 'S' and 'D' not falls under the communication range then 'S' sends control packets to its neighbours and waits for reply messages. Here the reputation checks are bit complex since the selfish nodes are not easily replies to the sent messages. Therefore the communication ratio between the nodes is computed through the sent request message and the received replied message.

### 3.1 Communication Ratio ($C_R$)

Communication ratio between nodes is calculated on basis of the request and reply routing messages that transmits to each other within their communication network. For a node the $C_R$ is computed by taking the difference between the count of Path reQuest ($P_Q$) message received to the specific node and the count of unsent Path Reply ($P_R$) messages with respect to received '$P_Q$' message. Therefore $C_R$ is calculated using equation 1.

$$C_R = \left( \frac{P_Q - P_R}{P_Q} \right) X\, 100 \qquad (1)$$

where $P_Q$ denotes the count of request message that sent from the node 'S' and $P_R$ denotes the number of reply message received by the node 'S'.

### 3. 2 Energy Factor

Once the neighbor nodes are identified then the energy values for each node is checked along with the '$P_R$' message. The energy with high value is considered as one of the metric for the selection of next relay node. The process of selecting the node with high communication ratio and with the highest energy is selected in the sequence of routing. The nodes presented in the route are selected forwards the sensed information from 'S' to the destination node 'D'. The threshold energy is set and the energy values of the nodes are compared with the threshold values.

The higher energy values of the node compared to the threshold is selected and this process is continued till the data is reached to the destination. $E_{left}$represents the leftover energy and T denotes time taken and is shown in equation 2.

$$E_{left} = \left( \frac{E_{Initial} - E_{Current}}{T} \right) \qquad (2)$$

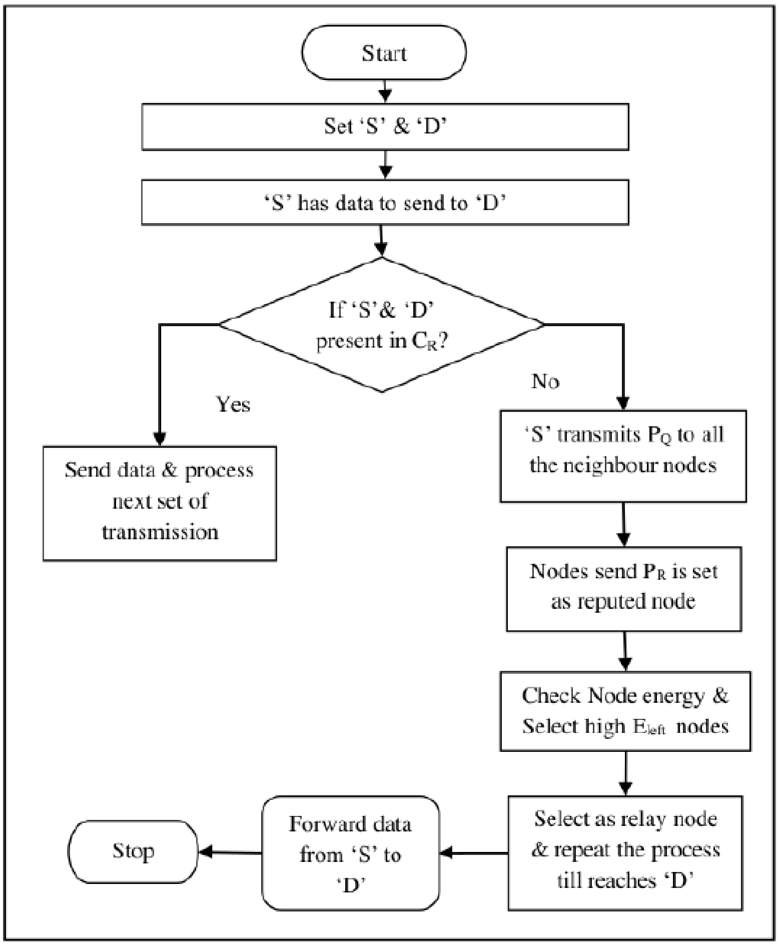
Start
Set 'S' & 'D'
'S' has data to send to 'D'
If 'S'& 'D' present in $C_R$?
Yes
No
Send data & process next set of transmission
'S' transmits $P_Q$ to all the neighbour nodes
Nodes send $P_R$ is set as reputed node
Check Node energy & Select high $E_{left}$ nodes
Select as relay node & repeat the process till reaches 'D'
Forward data from 'S' to 'D'
Stop

**Figure 1: Flowchart of SNRRM**

**Algorithm**

Steps involved in the mechanism proposed can be constrained to many smaller operations as listed.

1: 'S' and 'D' nodes are set.

2: Check communication range for 'S' and 'D'

3: If 'S' and 'D' falls under single-hop communication the data can be send easily.

4: If 'S' and 'D' not falls under the communication range

5: then 'S' sends '$P_Q$' message to its neighbours

6: Nodes that respond to the '$P_Q$' message of 'S' considered as reputed nodes.

7: Now check energy values of reputed nodes

8: Calculate energy threshold and pick higher residual energy node

9: Repeat the process till it reaches the 'D'

10: End.

The flowchart for SNRRM is shown in figure 1. Once the reputed and energy efficient nodes are selected from the sender 'S' to the receiver 'D', the data can be forwarded through this reliable and reputed route. This process can easily identify the reputed nodes and reduces the computational complexity.

## 4. **Results and Discussion**

Network Simulator tool of version 2.35 is used here for simulating the proposed SNRRM method and existing GRTS protocol. NS2 has its own advantages and validating with this tool makes the protocols more

Computational efficient. It has simple scalability factor by using tool command language. The simulation area is taken here in the dimensions of 1000X800 m deployed with 100's of nodes.

The parameters taken for analysing the proposed scheme are Packet Rate Delivered (PRD), Reputation Ratio and Energy Consumption.

### 4.1 Packet Rate Delivered

The rate of packets that is delivered over the channel to the destination is calculated by taking the difference between the rates of sent packets and receiving packets.PRD is calculated using equation 3, n represents number of nodes.

$$PRD = \frac{\sum_0^n PktRcv(n) - \sum_0^n PktSent(n)}{Time} \qquad (3)$$

The packet rates that are delivered to the destination are shown in figure 2 for both the proposed SNRRM scheme and conventional GRTS method. It is proved that the SNRRM proposed scheme achieves better delivery rates when compared with conventional GRTS method.

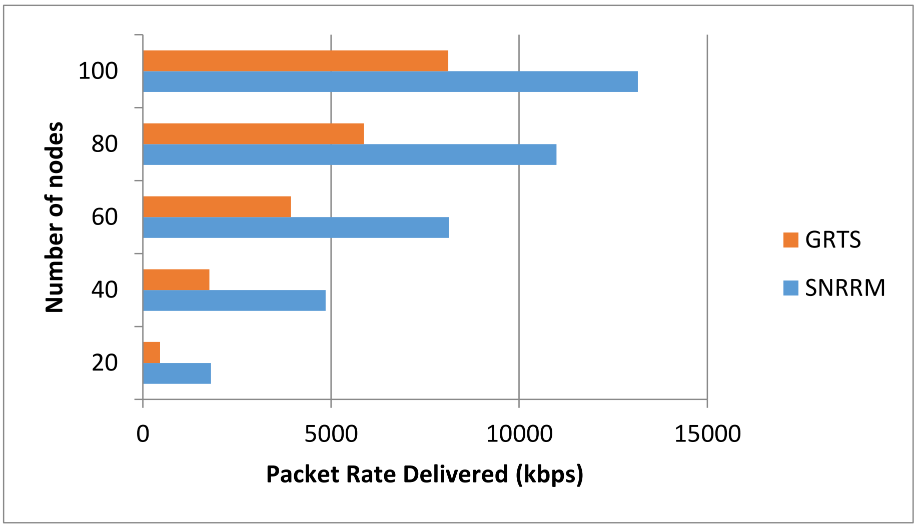

**Figure 2: Packet Rate Delivered**

### 4.2 Node Reputation Ratio

The average reputation ratio is calculated for all the neighbor nodes in order to detect the number of reputed nodes that presented in the data routing path. To check whether the neighbor node is selfish or not; the path request and path replies count are measured accurately with respect to their packet rates. The average reputation ratio for the proposed SNRRM scheme is 0.34 and for conventional GRTS the obtained average reputation ratio is 0.23. Therefore the achieved average reputation ratio of SNRRM scheme is high and hence it has high packet delivered rates.

Figure 3 shows that node reputation ratio for both SNNRM and GRTS schemes and proved that SNRRM is better in terms of selecting reputed nodes.

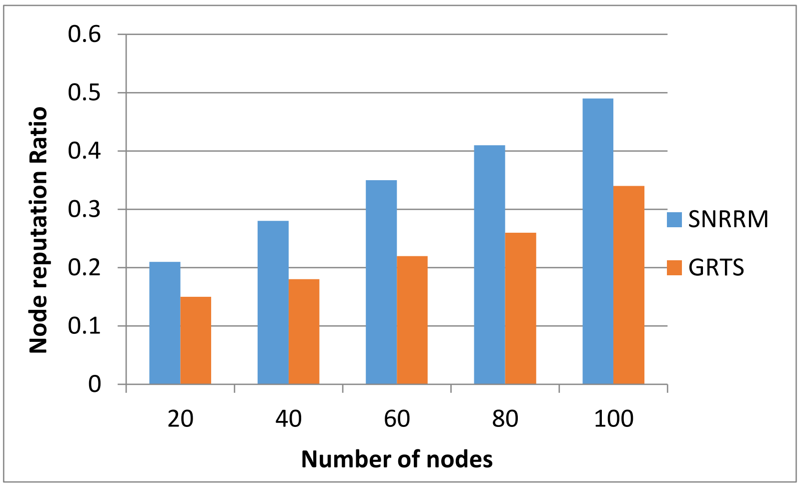

**Figure 3: Node Reputation Ratio**

### 4.3 Residual Energy

The energy value that is remained in the node for the further transmission of certain level of data packets for the next set of routing process is said to be residual energy. The node's energy level is commonly spent for the process of sensing and relaying the information.

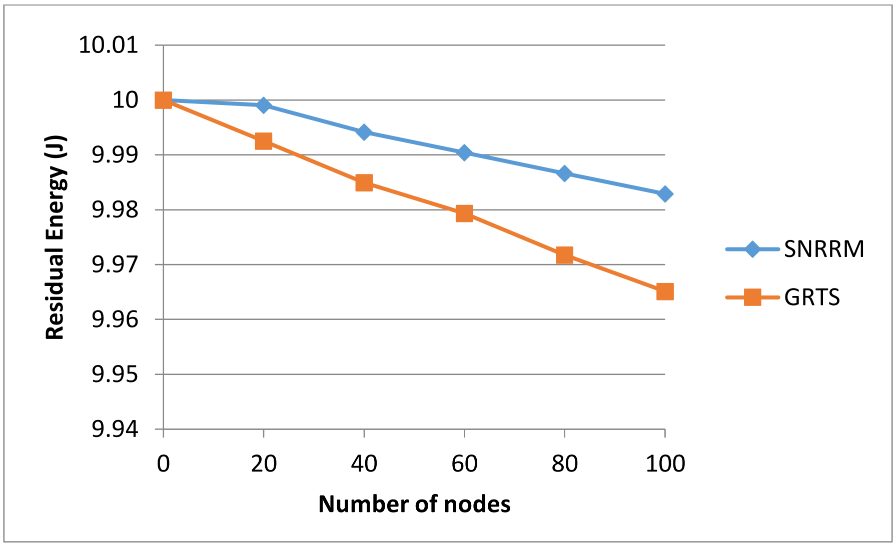

**Figure 4: Residual Energy**

The residual energy obtained for both proposed SNRRM and conventional GRTS scheme is shown in figure 4. The proposed protocol consumes less energy in comparison with conventional GRTS since the data's are processed high energy level nodes.

## 5. Conclusion

Selfish node removal using reputation model is proposed and the results are analysed. Here the selfish node that causes inconvenience during routing is removed from the system during routing operation. The reputed and energy efficient nodes are identified from the network and the data transmission takes on reliable routes. In this reputation scheme the selfish nodes are not co-operative with each other and hence the reputed nodes are detected through the analysis of communication ratio between the nodes. The simulation result for the proposed model is discussed here and shows the efficiency achieved is better in terms of reputation ratio and delivery rates.

## References

*1.* Almazyad, A. S. (2018). *Reputation-based mechanisms to avoid misbehaving nodes in ad hoc and wireless sensor networks. Neural Computing and Applications*, *29*(9), *597-607.*

2. Abirami, K. R., &Sumithra, M. G. (2018). *Preventing the impact of selfish behavior under MANET using Neighbor Credit Value based AODV routing algorithm*. *Sādhanā, 43(4), 1-7*

3. Amin, U., & Shah, M. A. (2018, September). *A novel authentication and security protocol for wireless adhoc networks.* In *2018 24th International Conference on Automation and Computing (ICAC)* (pp. 1-5). IEEE.

4. Arunkarthikeyan, K. and Balamurugan, K., 2020, July. Performance improvement of Cryo treated insert on turning studies of AISI 1018 steel using Multi objective optimization. In 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE) (pp. 1-4). IEEE.

5. Aroulanandam, V.V., Latchoumi, T.P., Bhavya, B., Sultana, S.S. (2019). Object detection in convolution neural networks using iterative refinements. Revue d'Intelligence Artificielle, Vol. 33, No. 5, pp. 367-372. https://doi.org/10.18280/ria.330506

6. Bhasha, A.C. and Balamurugan, K., 2020, July. Multi-objective optimization of high-speed end milling on Al6061/3% RHA/6% TiC reinforced hybrid composite using Taguchi coupled GRA. In 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE) (pp. 1-6). IEEE.

*7.* Bisen, D., & Sharma, S. (2018). *Fuzzy based detection of malicious activity for security assessment of MANET. National Academy science letters, 41(1), 23-28.*

8. Chinnamahammad Bhasha, A., Balamurugan, K. Fabrication and property evaluation of Al 6061 + x% (RHA + TiC) hybrid metal matrix composite. SN Appl. Sci. **1,** 977 (2019). https://doi.org/10.1007/s42452-019-1016-0

9. Deepthi, T. and Balamurugan, K., 2019. Effect of Yttrium (20%) doping on mechanical properties of rare earth nano lanthanum phosphate (LaPO4) synthesized by aqueous sol-gel process. Ceramics International, 45(15), pp.18229-18235.

10. Garikipati P., Balamurugan K. (2021) Abrasive Water Jet Machining Studies on AlSi$_7$+63%SiC Hybrid Composite. In: Arockiarajan A., Duraiselvam M., Raju R. (eds) Advances in Industrial Automation and Smart Manufacturing. Lecture Notes in Mechanical Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-15-4739-3_66

11. Gowthaman, S., Balamurugan, K., Kumar, P.M., Ali, S.A., Kumar, K.M. and Gopal, N.V.R., 2018. Electrical discharge machining studies on monel-super alloy. Procedia Manufacturing, 20, pp.386-391.

*12.* Fu, Y., Li, G., Mohammed, A., Yan, Z., Cao, J., & Li, H. (2019, August). *A study and enhancement to the security of MANET AODV protocol against black hole attacks. In 2019 IEEE SmartWorld, Ubiquitous Intelligence &Computing,pp. 1431-1436). IEEE.*

*13.* Khan, B. U. I., Anwar, F., Olanrewaju, R. F., Pampori, B. R., & Mir, R. N. (2020). *A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission with Optimized Network Operations in Futuristic Mobile Adhoc Networks. IEEE Access, 8, 124097-124109.*

*14.* Khan, B. U. I., Olanrewaju, R. F., Anwar, F., Najeeb, A. R., &Yaacob, M. (2018). *A survey on MANETs: architecture, evolution, applications, security issues and solutions. Indonesian Journal of Electrical Engineering and Computer Science, 12(2), 832-842.*

*15.* Khan, B. U. I., Olanrewaju, R. F., Anwar, F., & Shah, A. (2014). *Manifestation and mitigation of node misbehaviour in adhoc networks. Wulfenia Journal, 21(3), 462-470.*

*16.* Mir, R. N. (2020, January). *Secure distributed routing in mobile ad hoc networks using proactive secret sharing. In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 459-463). IEEE.*

*17.* Dr. R. Manikandan, Dr Senthilkumar A. Dr Lekashri S. AbhayChaturvedi. *"Data Traffic Trust Model for Clustered Wireless Sensor Network." INFORMATION TECHNOLOGY IN INDUSTRY 9.1 (2021): 1225–1229. Print.*

*18.* Menaka, R., Mathana, J. M., Dhanagopal, R., &Sundarambal, B. (2020, March). *Performance evaluation of DSR protocol in MANET untrustworthy environment. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 1049-1052). IEEE.*

*19.* Monakhov, Y. M., Monakhov, M. Y., &Telny, A. V. (2019, November). *Method for local positioning of the node violating information security in mobile networks intrusion detection systems. In 2019 Dynamics of Systems, Mechanisms and Machines (Dynamics) (pp. 1-7). IEEE.*

*20.* Mir, R. N. (2020, January). *Secure distributed routing in mobile ad hoc networks using proactive secret sharing. In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 459-463). IEEE.*

21. Ranjeeth, S., Latchoumi, T.P., Sivaram, M., Jayanthiladevi, A. and Kumar, T.S., 2019, December. Predicting Student Performance with ANNQ3H: A Case Study in Secondary Education. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 603-607). IEEE.

*22.* Raghunandan, G. H., Chaithanya, G. H., &Hajare, R. (2017, February). *Independent robust mesh for mobile adhoc networks. In 2017 4th International Conference on Electronics and Communication Systems (ICECS) (pp. 125-128). IEEE.*

*23.* Rajesh, M. (2018). *A review on excellence analysis of relationship spur advance in wireless ad hoc networks. International Journal of Pure and Applied Mathematics, 118(9), 407-412.*

*24.* Dr.G.Suresh, Dr.A.Senthil Kumar, Dr.S.Lekashri, Dr.R.Manikandan. (2021). *Efficient Crop Yield Recommendation System Using Machine Learning For Digital Farming. International Journal of Modern Agriculture, 10(01), 906 - 914. Retrieved from http://www.modern-journals.com/index.php/ijma/article/view/688*

*25.* Sonekar, S. V., Pal, M., Tote, M., Sawwashere, S., &Zunke, S. (2020, March). *Computation termination and malicious node detection using finite state machine in mobile adhoc networks. In 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 156-161). IEEE.*