International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Hybrid Energy and Trust Efficient Reactive Routing Mechanism for MANETs

V. Vijayagopal, K.Prabu

Abstract: ***The facilitation of quality of service (QoS) under routing in Mobile Ad Hoc NETworks (MANETs) is a challenging issue due to its resource constraints, bandwidth sharing and topology dynamism. Moreover, security is considered as another complex issue of provisioning QoS as the prevalence of maliciousness nodes introduces all types of threats to the MANETs. In spite of a diversified number of mechanisms contributed for securing MANETs, majority of the solutions are potential in preventing some particular category of attacks or facilitate security by sacrificing the QoS cost. In this paper, Hybrid Energy and Trust Efficient Reactive Routing Mechanism (HETERRM) was proposed for ensuring trust-oriented QoS routing process that integrates QoS trust and social trust. This proposed HETERRM first relies on the process of mitigating maliciousness nodes by incorporating a trust mechanism that is capable in different packet forwarding misbehavior and reliable path discovery for facilitating trustworthy communication. This proposed HETERRM further aids in selecting the optimal forwarding node based on quality of channel, quality of link and residual energy to quantify the packet forwarding potential. The simulation experiments of the proposed HETERRM are conducted using ns-2 is evaluated using energy consumptions, packet delivery ratio and overhead.***

Keywords : Routing, QoS trust, Hybrid Markov Chain, Energy Efficiency, Social Trust

I. INTRODUCTION

The data delivery rate of ad hoc network is considered to be maximum under a high trust degree level of mobile nodes in the network [1]. However, the selfish nodes have the tendency to deny the act of packet forwarding for focusing on conservation of its energy in the network with a view to increase the longevity of the network [2]. The selfish nodes possess the characteristics of intentional dropping of packets that greatly degrades the performance of the network in terms of throughput, packet delay and energy consumptions [3]. The existence of selfish nodes needed to be detected through a continuous monitoring process that is facilitated through direct or neighborhood monitoring in the network [4]. Statistical Reliability factors are considered to be significant in determining the packet forwarding potential of the mobile nodes in the network with reduced energy consumptions in the network [5]. These statistical reliability factors are determined to be more predominant towards effective mitigation of selfish influence in the network [6]. Hence, an efficient mitigation approach that inspires the benefits of parametric distribution need to be formulated [7].

In this paper, an Extended Hyper Geometric Trust Factor-Based Markov Foresting Scheme (EHGTF-MFS) is contributed for effective forecasting of selfish node intent in the future such that the forwarding of packets through those specific malicious nodes is prevented. This proposed EHGTF-MFS incorporates the advantages of Hybrid Markov Chain and Enhanced Functional Link Network-based Grey Forecasting process for isolating selfish node behavior in ad hoc networks. This proposed EHGTF-MFS also includes Markov chain for quantifying the level of residual energy that is essential in modifying the forecasting value of enhancing the prediction accuracy. The simulation experiments of the proposed EHGTF-MFS scheme are conducted using throughput, detection rate, energy consumptions and packet latency by varying the number of CBR connection and selfish nodes in the network. research articles globally. All accepted papers should be formatted as per Journal Template. Be sure that Each author profile (min 100 word) along with photo should be included in the final paper/camera ready submission. It is be sure that contents of the paper are fine and satisfactory. Author (s) can make rectification in the final paper but after the final submission to the journal, rectybrid Markov Chaiification is not possible. In the formatted paper, volume no/ issue no will be in the right top corner of the paper. In the case of failure, the papers will be declined from the database of journal and publishing house. It is noted that: 1. Each author profile along with photo (min 100 word) has been included in the final paper. 2. Final paper is prepared as per journal the template. 3. Contents of the paper are fine and satisfactory. Author (s) can make rectification in the final paper but after the final submission to the journal, rectification is not possible.

II. RELATED WORK

In the recent past, a number of recent selfish node detection schemes contributed in the literature are discussed in this section. Initially, a selfish node detection approach using the merits of Exponential Reliability Coefficient was proposed for effective data dissemination through effective isolation of their impacts [8]. This proposed exponential reliability-based detection approach was determined to a significant in exploring all the dimensions that attribute.

Manuscript published on 30 September 2019.
***Correspondence Author(s)
V,Vijayagopal, Research Scholar, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India – 622104, Email: vijayagopal1976@gmail.com
K.Prabu, Associate Professor, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India – 622104,

Then, a two acknowledgement-based selfish node detection approach was proposed for effective isolation of intentional characteristics of the network [10]. Further, a selfish node detection scheme-based on continuous Bayes Theorem and prior probability was proposed for handling selfish node behavior in the network [11]. This continuous Bayes Theorem and prior probability-based selfish node detection schemes was determined to be superior in terms of packet delivery rate, throughput, total overhead and control overhead under a varying number of mobile nodes and selfish nodes in the network. [12], Furthermore, an Erlang Factor-based selfish node detection approach was proposed for determining the conditional probability that suits well for the effective isolation selfish intent from the network [13]. This Erlang Factor-based selfish node detection approach was also determined to be superior in terms of packet delivery rate, throughput, total overhead and control overhead under a varying number of mobile nodes and selfish nodes in the network. Finally, a Trust-based selfish node detection approach that utilizes the merits of conditional probability was proposed for effective isolation of selfish intent characteristics in the network [14]. This proposed conditional probability-based detection approach was also determined to a significant in exploring all the dimensions that attribute towards effective isolation of intentional characteristics of the network In addition, a significant contextual trust-based selfish nodes detection approach was contributed for eliminating the impacts of selfish behavior from the network [15]. This contextual trust-based selfish nodes detection approach was estimated to be excellent in terms of packet delivery rate, throughput, total overhead and control overhead under a varying number of mobile nodes and selfish nodes in the network.

III. AN EXTENDED HYPER GEOMETRIC TRUST FACTOR-BASED MARKOV FORESTING SCHEME (EHGTF-MFS)

In this proposed EHGTF-MFS scheme, the packet forwarding capability and residual energy of each mobile node is considered as input to the Grey Model GM (1,1). In the GM (1,1) model, a new data sequence $y^{(1)} = (y_1^{(1)}, y_2^{(1)}, ..., y_m^{(1)})$ from the input data sequence $y^{(1)} = (y_1^{(1)}, y_2^{(1)}, ..., y_m^{(1)})$ is derived using the method of one time accumulated generation operator expressed in Equation (1)

$$y^{(1)} = \sum_{j=1}^{m} y_j^{(0)} \quad (1)$$

Then the new data sequence $y^{(1)} = (y_1^{(1)}, y_2^{(1)}, ..., y_m^{(1)})$ is approximated based on the method of first order whitening differential function denoted in Equation (2)

$$\frac{dy^{(1)}}{dt} + ly^{(1)} = m \quad (2)$$

Where 'l' and 'm' refers to the development factor and control variable that guides the process of predicting selfish nodes.

Further, the predicted value $\hat{y}^{(1)}$ to the newly derived $y^{(1)} = (y_1^{(1)}, y_2^{(1)}, ..., y_m^{(1)})$ is determined based on the method of solving differential equation as specified in Equation (3) with initial condition satisfying $y_1^{(1)} = y_1^{(0)}$.

$$\hat{y}^{(1)} = (y_1^{(0)} - \frac{m}{l})e^{-l(m-1)} + \frac{m}{l} \quad (3)$$

The grey difference equation specified in Equation (4) is utilized for determining the value of 'l' and 'm' by satisfying the condition $y_1^{(1)} = y_1^{(0)}$.

IV. $$y^{(0)} + lI_k^{(1)} = m \quad (4)$$

V. Where the background value $I_k^{(1)}$ is computed based on Equation (5)

$$I_k^{(1)} = \delta * y_k^{(1)} + (1-\delta) y_{k-1}^{(1)} \quad (5)$$

In this context, the value of δ is assigned to 0.5 for effectiveness.

Thus, the value of l and m are estimated using the method of least squares by applying $n-1$ Grey difference equation as specified in Equation (6)

$$[l, m]^T = (G^T G)^{-1} G^T x \quad (6)$$

Where the value of x is represented as $x = [y_2^{(0)}, y_2^{(0)}, ..., y_m^{(0)}]^T$ with B is the $m \times 2$ matrix in which m corresponds to the number of elements in the data sequence with the first column varying from $[-I_2^{(1)}, -I_3^{(1)}, ..., -I_m^{(1)}]$ and second column consisting of m number of unity value.

Then the predicted value of $\hat{y}^{(0)}$ is determined based on Equation (7) by applying the inverse function of inverse one time accumulated generation operator

$$\hat{y}^{(0)} = y_m^{(1)} - y_{m-1}^{(1)} \equiv (1-e^l)(y^{(0)} - \frac{m}{l})e^{-l(m-1)} \quad (7)$$

In this proposed scheme EHGTF-MFS scheme, the value of $\hat{y}^{(0)}$ is modified to $\tilde{y}^{(0)}$ through the addition and subtraction of $\hat{r}_k^{(m)}$ based on Equation (8) for improving the flexibility in the process of forecasting.

$$\tilde{y}^{(0)} = \hat{y}^{(0)} + d_{flex} \hat{r}_k^{(m)} \quad \text{with } 1 \le k \le m \quad (8)$$

Retrieval Number: K23120981119/19©BEIESP
DOI: 10.35940/ijitee.K2312.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Where d_{flex} is the degree of flexibility (ranges from -1 to 1) based on which the value of $\hat{y}^{(0)}$ can be adjusted effectively. The value of d_{flex} is computed with the aid of Functional Link Network based on the hyperbolic tangent function specified in Equation (9) under the activation function that ranges from -1 to 1 respectively.

$$\tanh(I_k^{(m)}) = \frac{(e^{I_k^{(m)}} - e^{-I_k^{(m)}})}{(e^{I_k^{(m)}} - e^{I_k^{(m)}})} \quad (9)$$

Furthermore, the time period t_p of $\hat{y}^{(0)}$ is enhanced for more accuracy based on the Functional Link Network that derives value of t_p, with α as the bias of the output node.

In this proposed EHGTF-MFS scheme, the Mean Absolute Percentage Error (MAPE) is incorporated in the forecasting model in order to facilitate high prediction accuracy since it is considered as suitable for modeling prediction approach that can be considered as the time-series model. Thus MAPE (P_{MAPE}) of $y^{(0)}$ is determined for identifying the selfish activity of selfish nodes based on Equation (10)

$$P_{MAPE} = \frac{1}{n}\sum_{k=1}^{m}\frac{\left|y_k^{(0)} - \tilde{y}_k^{(0)}\right|}{y_k^{(0)}} \times 100\% \quad (10)$$

In this context, the mobile nodes are considered as selfish nodes when the value of P_{MAPE} is greater than 0.3 (fixed based on simulation experiments) Trust Efficient Reactive Routing Mechanism (HETERRM)

i) Quality of the link

The quality of the link is defined as the time duration for which a link between two mobile nodes persists (residual life of the link). In this proposed HETERRM, the quality of the link is estimated for minimizing the failure of the route in the highly reactive environment.The residual life of the link is comparatively easy to estimate by extracting the relative velocity between nodes and range of communication, even when the accurate prediction of wireless links in ad hoc networks is a complex issue. The determination of the quality of the link is initiated by estimating the relative velocity and distance between nodes.

$$Dist_{nodes(i,j)} = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (2)$$

Then, the quality of the link is determined based on the relative velocity ($R_{Vel} = Vel_A - Vel_B$) and Range of Communication (R_{Comm}) based on Equation (3)

VI. MATH

The experimental investigations of the proposed EHGTF-MFS scheme is facilitated through the series of simulations conducted using ns-2.31. The total terrain network area considered for the implementation of the proposed EHGTF-MFS scheme is 100x100 square meters with 200 mobile nodes randomly distributed throughout the entire network topology. The simulation time for the implementing the proposed EHGTF-MFS scheme is 250 seconds with the CBR of 40 packets per second under the packet size of 512 bytes. The pause time used for the implementation of the proposed EHGTF-MFS scheme is 30 seconds with MAC 802.11.

Initially, the predominace of the proposed EHGTF-MFS scheme is investigated using throughput, detection rate, total overhead and packet drop based on increasing number of mobile nodes in the network. Figure 1 and 2 depicts the significance of the proposed EHGTF-MFS scheme quantified using throughput and detection rate evaluated under a varying number of mobile nodes in the ad hoc network. The proposed EHGTF-MFS scheme confirmed a potential enhancement in throughput under varying mobile nodes of nearly 11%, 13% and 15% excellent to the existing TBIDT-DSN, SD-TBDEand EFBCRMapproaches. Likewise, the detection rate of the proposed EHGTF-MFS scheme under increasing mobile nodes is determined to be enhanced through a considerable margin of 9%, 13% and 17% remarkable to the existing TBIDT-DSN, SD-TBDEand EFBCRMapproaches. Likewise, Figure 3 and 4 exemplars the significance of the proposed EHGTF-MFS scheme quantified in terms of total overhead and packet drop evaluated under a varying number of mobile nodes in the ad hoc network. The proposed EHGTF-MFS scheme under increasing mobile nodes confirmed a potential reduction in total overhead of approximately 10%, 13% and 18% superior to the baseline TBIDT-DSN, SD-TBDEand EFBCRM approaches. Likewise, the packet drop rate of the proposed EHGTF-MFS scheme under increasing number of mobile nodes is also determined to be greatly minimized through a considerable margin of 9%, 14% and 17% remarkable to the existing TBIDT-DSN, SD-TBDEand EFBCRMapproaches. This predominance of the proposed EHGTF-MFS scheme in maximizing throughput and detection rate with minimized packet drop and total overhead under increasing number of mobile nodes is mainly due to the exact quantification of trust possessed by each interacting mobile nodes ensured by the computation of the Gwet Kappa Factor.

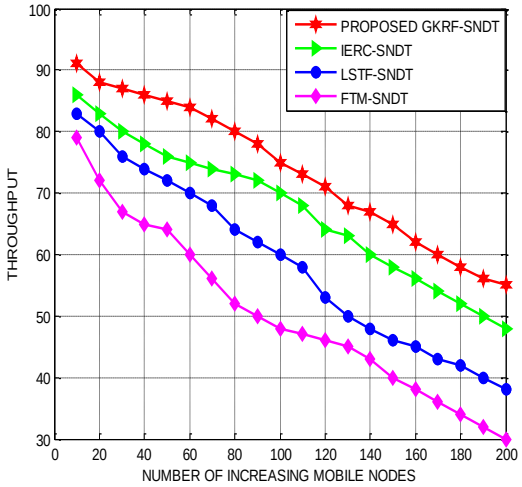

Figure 1: Proposed EHGTF-MFS scheme-throughput under different mobile nodes

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

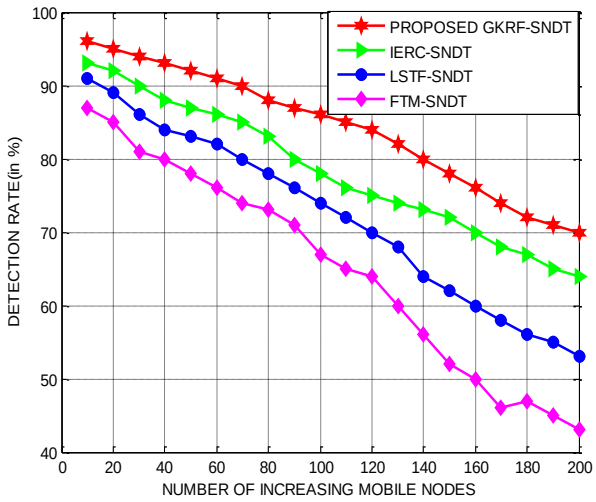

Figure 2: Proposed EHGTF-MFS scheme-detection rate under different mobile nodes

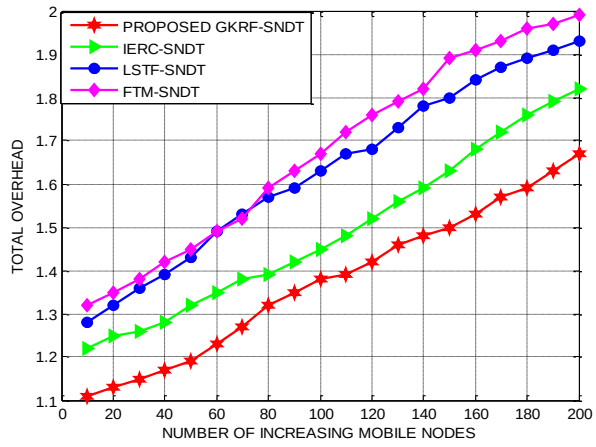

Figure 3: Proposed EHGTF-MFS scheme-total overhead under different mobile nodes

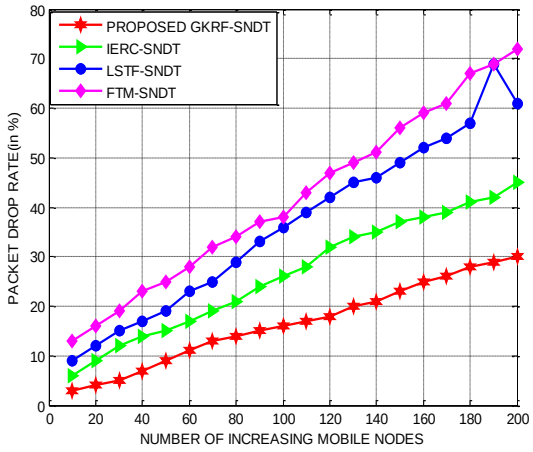

Figure 4: Proposed EHGTF-MFS scheme-packet drop under different mobile nodes

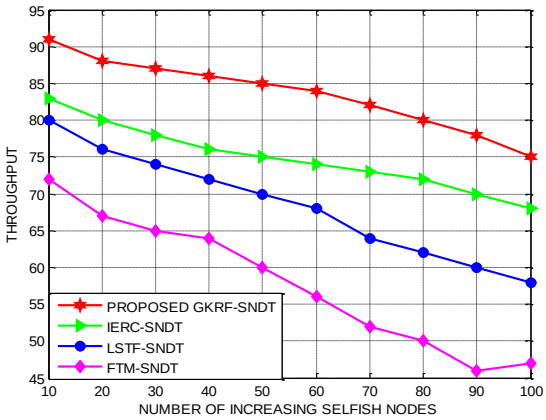

Figure 5: Proposed EHGTF-MFS scheme-throughput under different selfish nodes

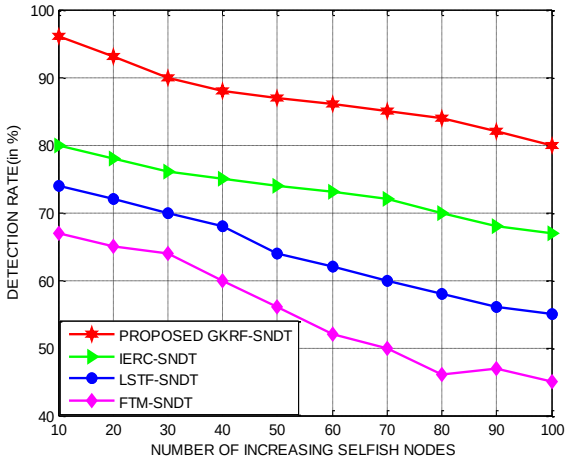

Figure 6: Proposed EHGTF-MFS scheme-detection rate under different selfish nodes

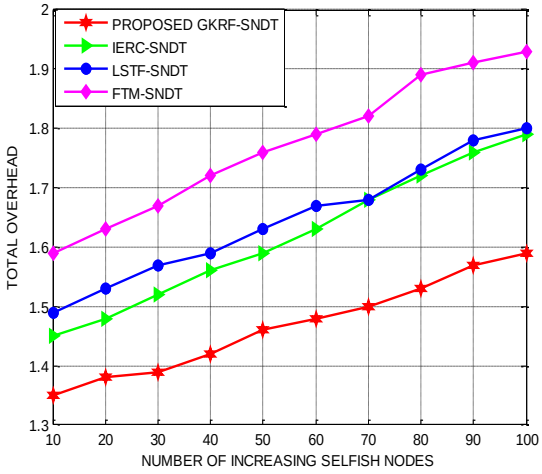

Figure 7: Proposed EHGTF-MFS scheme-total overhead under different selfish nodes

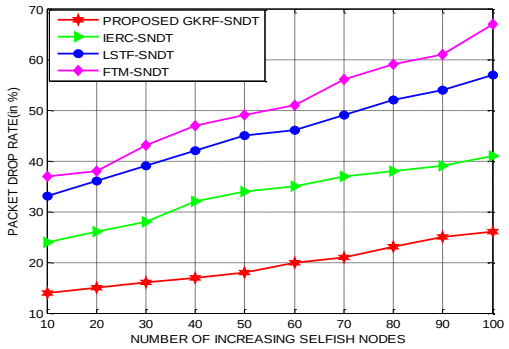

Figure 8: Proposed EHGTF-MFS scheme-packet drop under different selfish nodes

Furthermore, the role of the proposed EHGTF-MFS scheme is investigated using throughput, detection rate, total overhead and packet drop based on increasing number of selfish node intensity in the network. Figure 5 and 6 portrays the significance of the proposed EHGTF-MFS scheme quantified using throughput and detection rate evaluated under varying number of selfish nodes in the network topology. The proposed EHGTF-MFS scheme confirmed a potential enhancement in throughput of 13%, 16% and 18% remarkable to the existing TBIDT-DSN, SD-TBDEand EFBCRMapproaches. Likewise, the detection rate of the proposed EHGTF-MFS scheme is determined to be enhanced through a considerable margin of 10%, 14% and 19% remarkable to the existing TBIDT-DSN, SD-TBDEand EFBCRMapproaches.

Figure 7 and 8 depicts the significance of the proposed EHGTF-MFS scheme quantified in terms of total overhead and packet drop evaluated under varying number of selfish nodes in the network topology. The proposed EHGTF-MFS scheme confirmed a potential reduction in total overhead of approximately 12%, 14% and 16% superior to the baseline TBIDT-DSN, SD-TBDEand EFBCRM approaches. Likewise, the packet drop rate of the proposed EHGTF-MFS scheme is also determined to be greatly minimized through a considerable margin of 11%, 16% and 21% remarkable to the existing TBIDT-DSN, SD-TBDEand EFBCRMapproaches. This predominance of the proposed EHGTF-MFS scheme in maximizing throughput and detection rate with minimized packet drop and total overhead under increasing number of selfish is mainly due to the possibility of multi-perspective investigation assured by the Gwet Kappa Factor.

Figure 9: Proposed EHGTF-MFS-energy consumptions under vaying mobile nodes

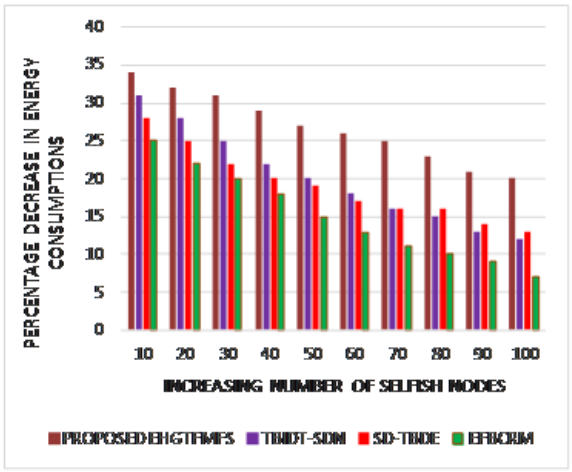

Figure 10: Proposed EHGTF-MFS-energy consumptions under varying selfish nodes

Finally, Figure 9 and 10 exemplars the performance of the proposed EHGTF using a percentage decrease in energy consumptions under an increasing rate of varying mobile nodes and selfish nodes in the network. The energy consumptions of the proposed EHGTF-MFS scheme under monotonically increasing number of mobile nodes is confirmed to be minimized by a greater margin of 7%, 10% and 12% excellent to the existing TBIDT-DSN, SD-TBDEand EFBCRMapproaches. In addition, the energy consumptions of the proposed EHGTF-MFS scheme under monotonically increasing number of selfish nodes are also determined to be significantly reduced through a significant level of 8%, 11% and 13% excellent to the existing TBIDT-DSN, SD-TBDEand EFBCRMapproaches.

V. CONCLUSION

This paper has presented a reliable EHGTF-MFS approach that estimates the predicted value through the enforcement of potent Grey Model that is potentially adjusted based on the application of the Enhanced Functional Link Network. This proposed EHGTF-MFS approach was presented using the merits of Markov chain for forecasting the probability of selfish intent in the mobile nodes in a precise manner. The simulation results and investigations of the proposed EHGTF-MFS mechanism confirmed a superior enhancement in energy consumptions, packet delivery rate and packet latency in the network. In the near future, it is also planned to formulate a fuzzy operator based selfish node detection scheme that explores the option of investigating the maximum dimension in mitigating them from the network

REFERENCES

1. Ryu, B., Choi, J., & Lee, S. (2013). Impact of node distance on selfish replica allocation in a mobile ad-hoc network. Ad Hoc Networks, 11(8), 2187-2202.
2. Lee, F. (2011). Routing in Mobile Ad hoc Networks. Mobile Ad-Hoc Networks: Protocol Design, 1(1), 23-31.
3. Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, & Kun-Lung Wu. (2012). Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network. *IEEE Transactions on Mobile Computing*, *11*(2), 278-291.

4. Zhu, J., & Wang, X. (2011). Model and Protocol for Energy-Efficient Research Scholar, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India - 622104
5. 2 Associate Professor, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India - 622104Routing over Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, 10(11), 1546-1557.
6. Eidenbenz, S., Resta, G., & Santi, P. (2008). The COMMIT Protocol for Truthful and Cost-Efficient Routing in Ad Hoc Networks with Selfish Nodes. IEEE Transactions on Mobile Computing, 7(1), 19-33.
7. Wang, Y., & Singhal, M. (2006). LSTOP: A Light-Weight Scalable Truthful Routing Protocol in MANETs with Selfish Nodes. *Ad-Hoc, Mobile, and Wireless Networks*, *1*(2), 280-293.
8. Wang, Y., Giruka, V. C., & Singhal, M. (2008). Truthful multipath routing for ad hoc networks with selfish nodes. *Journal of Parallel and Distributed Computing*, *68*(6), 778-789.
9. Sengathir, J., & Manoharan, R. (2015). Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs. Egyptian Informatics Journal, 16(2), 231-241.
10. Sengathir, J., & Manoharan, R. (2015). Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs. Egyptian Informatics Journal, 16(2), 231-241.
11. Kariya, S. L., & Panchal, B. B. (2012). Selfish Nodes Detection in MANETs: Acknowledgement Based Approach. *International Journal of Scientific Research*, *2*(5), 216-217.
12. Kshirsagar, V., Kanthe, A. M., & Simunic, D. (2014). Analytical approach towards packet drop attacks in mobile ad-hoc networks. 2014 IEEE International Conference on Computational Intelligence and Computing Research, 1(1), 45-54.
13. Lamba, G. K. (2016). Varying Number of Selfish Nodes based Simulation of AODV Routing Protocol in MANET using Reputation Based Scheme. *International Journal Of Engineering And Computer Science*, *1*(1), 56-63.
14. Janakiraman, S., & Rajendiran, M. (2016). An Erlang factor-based conditional reliability mechanism for enforcing co-operation in MANETs. Serbian Journal of Electrical Engineering, 13(2), 265-284.
15. Kshirsagar, V. H., Kanthe, A. M., & Simunic, D. (2017). Trust Based Detection and Elimination of Packet Drop Attack in the Mobile Ad-Hoc Networks. Wireless Personal Communications, 100(2), 311-320.
16. Kumar, S., & Dutta, K. (2018). Trust Based Intrusion Detection Technique to Detect Selfish Nodes in Mobile Ad Hoc Networks. *Wireless Personal Communications*, *101*(4), 2029-2052.

AUTHORS PROFILE

V.Vijayagopal, is a Research Scholar, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India – 622104.

K.Ptabhhu is an Assocaite Professor**,** PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India – 622104**.** He has two decade experience in teaching Ad hoc networks, image processing, etc. He has guided many research scholars towards their Ph.D