An Improved Integrated Energy and Trust-based Routing Mechanism for MANETs

V. Vijayagopal, K. Prabu

Abstract*: The degree of packet dissemination among the mobile nodes of the network depends on the reliability of each individual mobile node attributed towards the benefits of the other interacting nodes in forwarding activity. However, the selfish intent of selfish nodes in the network reduces the performance in terms of packet forwarding rate. Thus, the influence of selfish intent in the network need to be minimized to the maximum level by introducing a predominant isolation process. In this paper, a Gwet Kappa Reliability Factor-based Selfish Node Detection Technique (GKRF-SNDT) scheme is proposed for superior detection of selfish nodes in the network. This proposed GKRF-SNDT scheme inherently derives the advantages of Gwet Kappa Reliability Factor for quantifying the degree of trust possessed by each mobile nodes interacting in the network. The experimental investigations of the proposed GKRF-SNDT scheme confirmed a superior throughput rate of 18% with reduced energy consumptions of 21% compared to the existing selfish intent isolation approaches.

***Index Terms*: Gwet Reliability Factor, Selfish Nodes, Mobile Nodes, Data Dissemination.**

I. INTRODUCTION

The cooperation of the mobile nodes is quantified based on its forwarding potential attributed for the sake of their neighboring nodes in the ad hoc network [1]. The transmission of data through the cooperative mobile nodes reduces the degree of risk involved the appropriate data dissemination in the network [2]. However, the selfish characteristics of mobile nodes imposes negative influence over the network by dropping considerable number of packets rather than forwarding in order to conserve the possessed energy for its own existence. Further, the existence of selfish nodes in the network also introduces maximum number of retransmissions that increases the control overhead and total overhead in the network that contribute towards maximum network performance degradation. Hence, the selfish intent of mobile nodes need to be effective detected for improving the rate of data dissemination in the ad hoc network [3]. A number of selfish intent detection approaches were propounded in the literature using watchdog, path rater and token for accurate isolation process [4-6]. But, most of them are not capable in exploring the factors of selfish nodes in a multi-dimensional perspective. These selfish intent mitigation approaches have the shortcomings of incurring high communication overhead during the process of implementation [7]. Furthermore, Gwet Kappa Relaibility Factor is considered as the key reliability estimator that can catergorise the normal mobile nodes from malicious selfish nodes in the network [8]. Hence, the selfish node detection using Gwet Kappa Factor becomes indispensable for ensuring maximum performance in the network.

In this paper, a Gwet Kappa Reliability Factor-based Selfish Node Detection Technique (GKRF-SNDT) scheme is proposed for superior detection of selfish nodes in the network. This proposed GKRF-SNDT scheme utilizes the key characteristics of exploring multiple levels of selfish intent detection-oriented decision parameters that are derived from the monitoring activity of the mobile nodes in the network. The simulation experiments of the proposed GKRF-SNDT scheme are conducted using throughput, detection rate, total overhead and packet drop rate under varying degree of mobile nodes and selfish nodes of the network for quantifying its predominace over the benchmarked selfish intent detection approaches.

The remaining sections of the paper are structured as follows. Section 2 highlights the significances of the existing selfish intent detection works contributed in the literature over the recent decade. Section 3 describes the detailed view on the implementation process of the proposed GKRF-SNDT scheme with its associated algorithm. Section 4 portrays the details of the simulation experiments and results of the proposed GKRF-SNDT scheme conducted using throughput, detection rate, total overhead and packet drop rate analysed under varying degree of mobile nodes and selfish nodes of the network. Section 5 highlights the major contributions of the proposed GKRF-SNDT scheme with its future plan of research.

II. RELATED WORK

In this section, the most recent works contributed in the literature over the past decade towards the detection and isolation of selfish nodes are detailed with its merits and limitations. Initially, a colloborative scheme for selfish node detection was proposed for spreading the awareness of maliciousness in the entire network for preventing its influence towards the other cooperating nodes of the network [9].

Manuscript published on 30 September 2019
* Correspondence Author

V.Vijayagopal*, Research Scholar, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai – 622104, Tamilnadu, India. Email: vijayagopal1976@gmail.com

Dr. K.Prabu, Associate Professor, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai – 622104, Tamilnadu, India.Email: kprabu.phd@gmail.com.

This collaborative selfishness detection detection utilized an analytical approach for evaluating the detection time and incurred overhead of the network.

This collaborative selfishness detection detection approach used a mean and max approximation method of computation depending on the degree of selfishness in the network. This collaborative selfishness detection detection approach was determined to be potent in reducing the detection time and comprehensive routing overhead. Then, a watchdog-based collaborative contact approach was contributed for diffusing the awareness of local selfish intent whenever they come into interaction with the other cooperating mobile nodes of the network [10]. This watchdog-based collaborative contact approach was determined to minimize the time and precision degree involved in the process of detecting selfish nodes. The degree of selfish intent awareness was also determined to be maximum compared to the earlier colloborative selfish node detection approaches. A selfish node detection approach using cluster head was proposed for managing reputation and reliability of mobile nodes in the network [11]. This cluster head-based reputation scheme was determined to reduce the degree of routing overhead and energy consumptions compared to the watchdog-based collaborative contact approach. The throughput and detection rate of this cluster head-based reputation approach was also determined to the maximum under any number of selfish nodes in the network.

Further, an Exponential Reliability Coefficient-based Selfishness Detection Scheme (ERC-SDS) was proposed using the past historical data derived from the mobile nodes either through direct and indirect monitoring process [12, 15]. This ERC-SDS aided in devising two different upper and lower thresolds for facilitating the process of selfish node detection. The total overhead and energy consumptions of this ERC-SDS was determined to highly minimized on par with the collaborative watchdog-based selfish node detection approaches. Then, a two hop acknowledgement-based selfishness detection approach was contributed using the details derived from the routes during the forward and backward routing process [13,16]. The overhead incurred during the process of routing is greatly reduced compared to the ERC-SDS approach since the number of retransmissions is phenomenally minimized based on the process of hybrid monitoring. The total overhead and energy consumptions of this two hop acknowledgement-based selfishness detection approach was also determined to highly minimized on par with the collaborative watchdog-based selfish node detection approaches.

Furthermore, Fuzzy Trust Method for Selfish Node Detection Technique (FTM-SNDT) was proposed using the benefits of Fuzzy analyser for distinguishing the charateristics of mobile nodes into normal and selfish nodes [14]. This proposed FTM-SNDT used a fuzzy function for categorizing mobile nodes into various classes depending on the forwarding potential of each monitored mobile nodes. This proposed FTM-SNDT was estimated to be potential in preventing the degradation of the network performance by rapid isolation of selfishness from the ad hoc network. The The total overhead and energy consumptions of this FTM-SNDT was determined to highly minimized on par with the ERC-SDS and two hop acknowledgement-based selfish node mitigation approaches.

III. Gwet Kappa Reliability Factor-based Selfish Node Detection Technique (GKRF-SNDT) scheme

This GKRF-SNDT scheme faciltates the detecion process through the computation of Energy-Aware Gwet Kappa Reliability Factor (EA-GKRF) which quantifies the stability of the link that exists between multicast group leader and the downstream nodes or between the link established between the multicast group leader and the downstream nodes. This link stability quantification based detection is achieved using three steps viz., a) Computation of energy-based neighborhood stability, b) Computation of link loss-aware neighbour stability and c) Estimation of individual path lifetime stability and d) Computation of Energy-Aware Gwet Kappa Reliability Factor (EA-GKRF).

a) Computation of energy-based neighborhood stability

In GKRF-SNDT scheme, let us consider an ad hoc network in which each core group leader ‘i’ possess an intial energy E_i. In this context, $E_r(i)$ and $NP_f(i)$be the residual energy and number of packets forwarded by each core group leader ‘i’ with $E_{m(p)}$ and $E_u(i)$ as the maximum energy necessary for forwarding unit number of packet and energy consumed by them respectively.

Then the energy consumption factor of core group leader ‘i’is given by

$$E_u(i) = \frac{E_r(i) - E_{m(p)} \times NP_{f(i)}}{E_i} \qquad (1)$$

b) Computation of link loss-aware neighbour stability

In this step, the neighbourbood stability of each core group leader ‘i’ is measured based on an significant parameter called link loss.This link loss is measured in terms of signal to noise ratio which is proportional to the bit error ratio (BER). Hence the link loss-aware neighbour stabilityLS_{ns} is

$$LS_{ns} = \frac{NP_{f(i)}}{Md^2 m} \quad (2)$$

Where‘ M_d^2 ’ is the mean distance between the group leader with the downstream nodes or upstream nodes with ‘m’ as the mobility constant. If the movement of mobile nodes is atmost constant with m=1 then,

$$LS_{ns} = \frac{NP_{f(i)}}{Md^2} \quad (3)$$

c) Estimation of individual path lifetime.

The stability of each path depends on the number of mobile nodes ‘n’ in a routing path and amount of energy required $C_{j,j+1}$ for sustaining the path stability.Then path stability $P_s$is

$$P_s = \sum_{i=1}^{n} C_{j,j+1(t)} \quad (4)$$

Based on the path stability P_s, the optimal path stability is calculated using OP_s based on minimum path stability min_{PS} through

$$OP_s = \frac{min_{PS}}{P_s} \qquad (5)$$

d) Computation of EA-GKRF for selfish node detection

The overall stability quantifying factor EA-GKRF is calculated based on the weighted sum of stabilities defined in (1), (2) and (5) is

$$EPPF = \alpha E_u(i) + \beta LS_{ns} + \gamma OP_s \qquad (6)$$

If the computed EA-GKRF value is identified to be less than 0.4, then the core group leader is said to be selfish in nature and hence isolated from multicast routing.

The following algorithm 1 illustrates the steps involved in detecting selfish nodes using the proposed GKRF-SNDT scheme for isolating them from the multicasting activity.

Algorithm 1- Energy-Aware Gwet Kappa Reliability Factor based Selfish Intent Mitigation Mechanism

```
1. Let the number of nodes in the network be N.
2. GN – Group of Nodes of the routing path, in which two significant nodes are labeled as SN (Source Node) and DN (Destination Node) respectively.
3. Set of nodes in the routing path can be established by sending `RREQ' message by the SN to all other nodes in the network.
4. Mobile node which are ready for data transmission replies to the source node by `RREP' message.
5. Let this algorithm step (6 -15) be executed for a node say, u, which belongs to the list GN, that uses ‘t’ number of sessions for transmission.
6. For every node ‘u’of GN in the routing path.
7.  Estimate the energy consumption factor of core group leader ‘i’ using intial energy $E_i$, residual energy $E_r(i)$, number of packets forwarded $NP_f(i)$, maximum necessary energy $E_{m(p)}$ through $E_u(i) = \frac{E_r(i) - E_{m(p)} \times NP_{f(i)}}{E_i}$
8.  Compute link loss-aware neighbour stability $LS_{ns}$ for each core group leader ‘i’ based on link loss using $LS_{ns} = \frac{NP_{f(i)}}{Md^2m}$
9.  Estimate minimum path stability $min_{PS}$ based ‘n’ mobile nodes ‘n’ in a routing path and $C_{j,j+1}$ cost of energy utilized using $OP_s = \frac{minp_S}{P_s}$
10. Compute overall stability quantifying factor EA-GKRF based on the weighted sum of stabilities using
    $EA - GKRF = \alpha E_u(i) + \beta LS_{ns} + \gamma OP_s$
11. if (EA-GKRF(u) < 0.40) then
12. node u is Selfish Node
13. Call Selfish Node Mitigation (u)
14. Else
15. node u is reliable.
16. End if
17. End for
```

Thus, the threshold detection point of selfish nodes is determined to be 0.4 since considerable number of selfish nodes are detected through the enforcement of this point (determined based on simulations).

IV. SIMULATION RESULTS AND DISCUSSION

The experimental investigations of the proposed GKRF-SNDT 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 GKRF-SNDT scheme is 1000 x1000 square meters with 200 mobile nodes randomly distributed throughout the entire network topology. The simulation time for the implementing the proposed GKRF-SNDT 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 GKRF-SNDT scheme is 30 seconds with MAC 802.11.

Initially, the predominace of the proposed GKRF-SNDT 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 GKRF-SNDT scheme quantified using throughput and detection rate evaluated under varying number of mobile nodes in the ad hoc network. The proposed GKRF-SNDT scheme confirmed a potential enhancement in throughput under varying mobile nodes of nearly 11%, 13% and 15% excellent to the existing IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches. Likewise, the detection rate of the proposed GKRF-SNDT scheme under increasing mobile nodes is determined to be enhanced through a considerable margin of 9%, 13% and 17% remarkable to the existing IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches. Likewise, Figure 3 and 4 exemplars the significance of the proposed GKRF-SNDT scheme quantified in terms of total overhead and packet drop evaluated under varying number of mobile nodes ine the ad hoc network. The proposed GKRF-SNDT scheme under increasing mobile nodes confirmed a potential reduction in total overhead of approximately 10%, 13% and 18% superior to the baseline IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches. Likewise, the packet drop rate of the proposed GKRF-SNDT 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 IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches. This predominance of the proposed GKRF-SNDT 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.

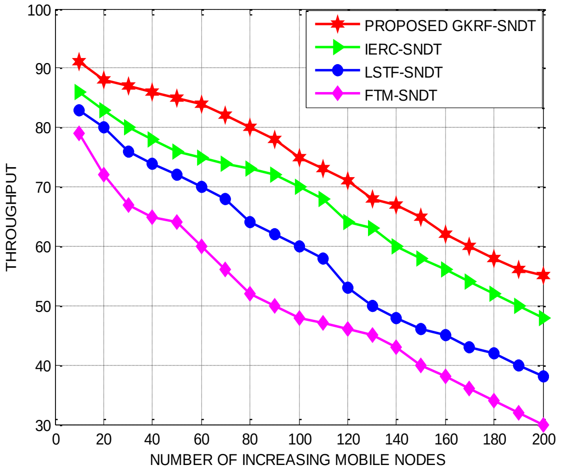

Figure 1: Proposed GKRF-SNDT scheme-throughput under different mobile nodes

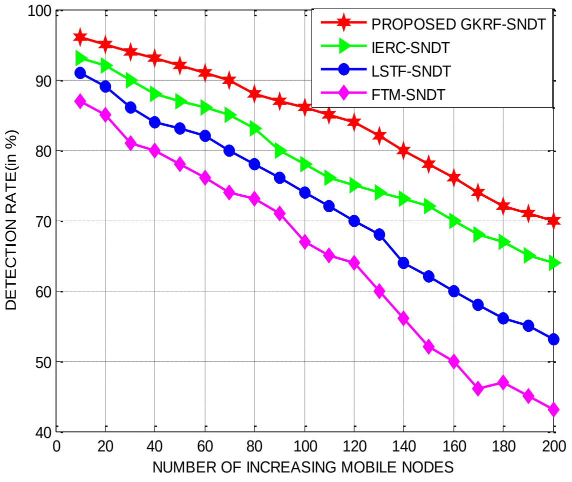

Figure 2: Proposed GKRF-SNDT scheme-detection rate under different mobile nodes

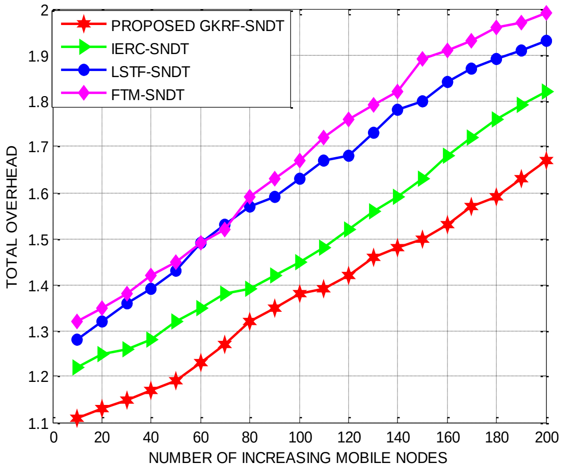

Figure 3: Proposed GKRF-SNDT scheme-total overhead under different mobile nodes

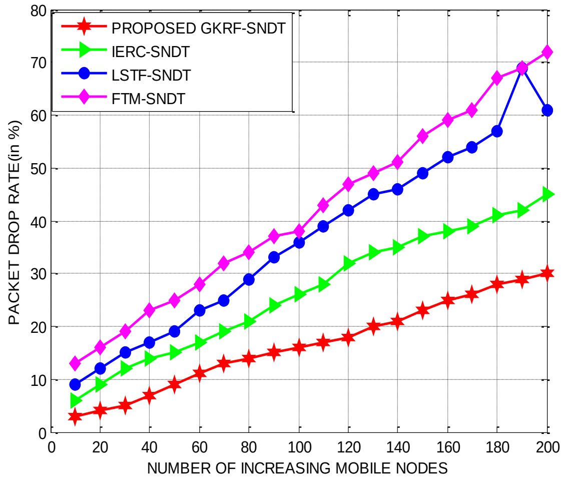

Figure 4: Proposed GKRF-SNDT scheme-packet drop under different mobile nodes

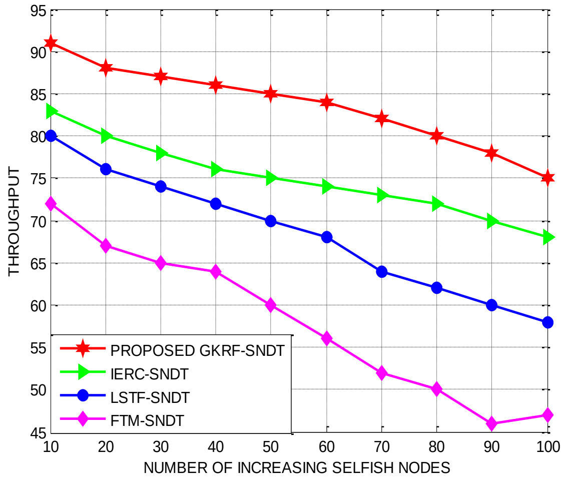

Figure 5: Proposed GKRF-SNDT scheme-throughput under different selfish nodes

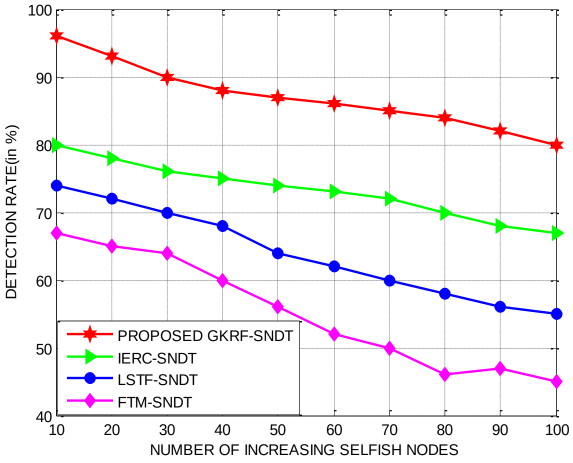

Figure 6: Proposed GKRF-SNDT scheme-detection rate under different selfish nodes

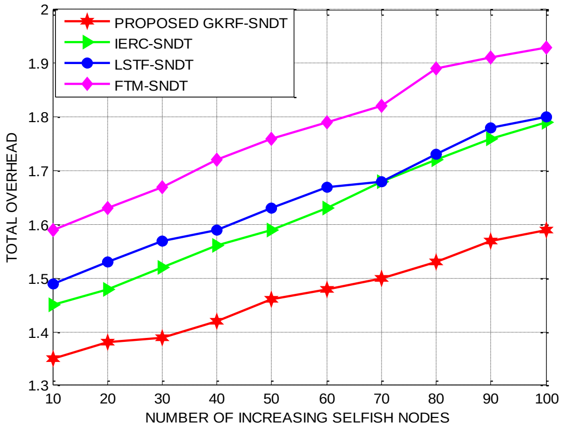

Figure 7: Proposed GKRF-SNDT scheme-total overhead under different selfish nodes

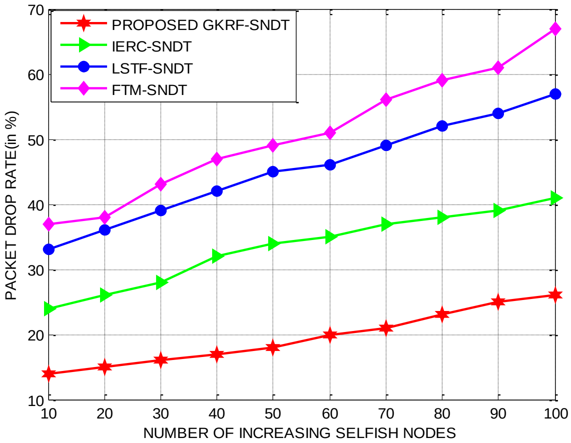

Figure 8: Proposed GKRF-SNDT scheme-packet drop under different selfish nodes

Furthermore, the role of the proposed GKRF-SNDT 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 GKRF-SNDT scheme quantified using throughput and detection rate evaluated under varying number of selfish nodes in the network topology. The proposed GKRF-SNDT scheme confirmed a potential enhancement in throughput of 13%, 16% and 18% remarkable to the existing IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches. Likewise, the detection rate of the proposed GKRF-SNDT scheme is determined to be enhanced through a considerable margin of 10%, 14% and 19% remarkable to the existing IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches.

Figure 7 and 8 depicts the significance of the proposed GKRF-SNDT scheme quantified in terms of total overhead and packet drop evaluated under varying number of selfish nodes in the network topology. The proposed GKRF-SNDT scheme confirmed a potential reduction in total overhead of approximately 12%, 14% and 16% superior to the baseline IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches. Likewise, the packet drop rate of the proposed GKRF-SNDT scheme is also determined to be greatly minimized through a considerable margin of 11%, 16% and 21% remarkable to the existing IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches. This predominance of the proposed GKRF-SNDT 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.

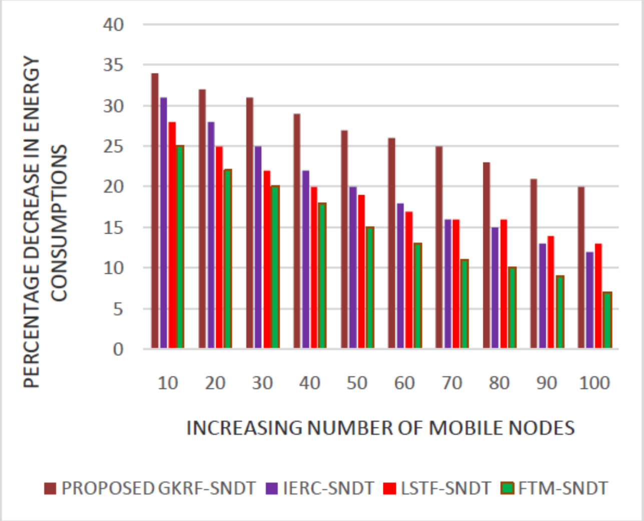

Figure 9: Proposed GKRF-SNDT scheme-energy consumptions under different number of mobile nodes

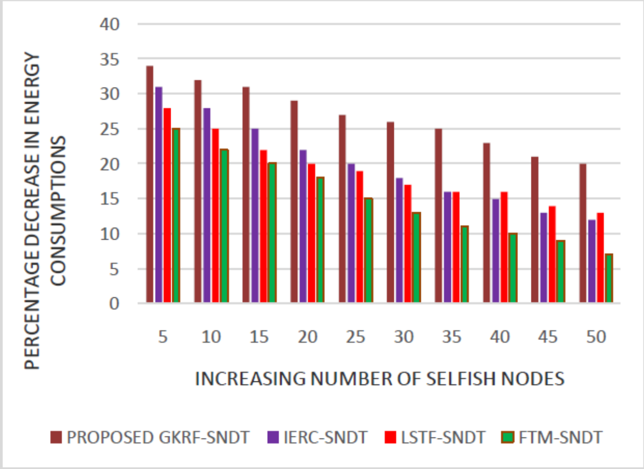

Figure 10: Proposed GKRF-SNDT scheme-energy consumptions under different number of selfish nodes

Finally, Figure 9 and 10 highlights the plots for the decrease in the energy consumptions of the proposed GKRF-SNDT scheme investigated under diversified number of mobile nodes and selfish nodes existing in the network. The energy consumptions of the proposed GKRF-SNDT 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 IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches. In addition, the energy consumptions of the proposed GKRF-SNDT 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 IERC-SNDT, LSTF-SNDT and FTM-SNDT approaches.

V. CONCLUSIONS

The proposed GKRF-SNDT scheme was presented as a reliable selfish node prevention approach that concentrates on the quantification of the trust inherently existing in each mobile nodes for categorizing normal nodes from malicious nodes. This proposed GKRF-SNDT scheme incorporated the advantages of Gwet Kappa Trust Factor for differentiatng the role of selfish nodes from the normal cooperating mobile nodes. This proposed GKRF-SNDT scheme also possessed the capability of determining a detection threshold that aided in appropriate and maximum number of detection in the selfish nodes. The experimental investigations of the proposed GKRF-SNDT scheme confirmed a superior throughput rate of 18% with reduced energy consumptions of 21% compared to the existing selfish intent isolation approaches. As the plan of future, it is also decided to devise a Fleiss Kappa-based selfish node detection approach for analysing multiple parameters in the detection of malicious intent that degrades the performance in the network.

REFERENCES

1. Yang, Y., Qiu, X., Meng, L., & Gao, Z. (2011)., “An Emotion-driven Negotiation Mechanism of Selfish Nodes in the MANETs”, *Journal of Electronics & Information Technology*, *33*(6), 1294-1300.
2. Serrat-Olmos, M. D., Hernandez-Orallo, E., Cano, J., Calafate, C. T., & Manzoni, P. (2012)., “Accurate detection of black holes in MANETs using collaborative bayesian watchdogs”, *2012 IFIP Wireless Days*, *2*(1), 23-34.
3. Djenouri, D., & Badache, N. (2010)., “A gradual solution to detect selfish nodes in mobile ad hoc networks”, *International Journal of Wireless and Mobile Computing*, *4*(4), 264-275.
4. Yongwei Wang, & Singhal, M. (2005)., “A light-weight solution for selfish nodes problem considering battery status in wireless ad-hoc networks”, *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005*, *2*(1), 67-78.
5. 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.
6. Waqas, A., & Mahmood, H. (2017)., “A Game Theoretical Approach for Topology Control in Wireless Ad Hoc Networks with Selfish Nodes”, *Wireless Personal Communications*, *96*(1), 249-263.
7. Umar, R., & Mesbah, W. (2017), “Throughput-efficient coalition formation of selfish/altruistic nodes in ad hoc networks: a hedonic game approach”, *Telecommunication Systems*, *67*(1), 95-111.
8. Yang, Y., Guo, S., Qiu, X., & Meng, L. (2011)., “A Service Negotiation Model for Selfish Nodes in the Mobile Ad Hoc Networks”, *2011 IEEE International Conference on Communications (ICC)*, *2*(1), 25-35.
9. Hernández-Orallo, E., Olmos, M. D., Cano, J., Calafate, C. T., & Manzoni, P. (2013)., “A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs”, *Wireless Personal Commn.*, *74*(3), 1099-1116.
10. Hernandez-Orallo, E., Olmos, M. D., Cano, J., Calafate, C. T., & Manzoni, P. (2015)., “CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes”, *IEEE Transactions on Mobile Computing*, *14*(6), 1162-1175.
11. 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*, *2*(1), 34-46.
12. Sengathir, J., & Manoharan, R. (2015)., “Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs”, *Egyptian Informatics Journal*, *16*(2), 231-241.
13. Kariya, S. L., & Panchal, B. B. (2012)., “Selfish Nodes Detection in MANETs: Acknowledgement Based Approach”, *International Journal of Scientific Research*, *2*(5), 216-217.
14. Ullah, Z., Khan, M. S., Ahmed, I., Javaid, N., & Khan, M. I. (2016)., “Fuzzy-Based Trust Model for Detection of Selfish Nodes in MANETs”, *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, *1*(1), 45-56.
15. Sengathir, J., & Manoharan, R. (2014)., “Laplace Stleltjes Transform based Conditional Survivability Coefficient Model for mitigating Selfish Nodes in MANETs”, *Egyptian Informatics Journal*, *15*(3), 149-157.
16. C, D. Nesan., & V, Saravannan. (2018)., “Improved Exponential Reliability Coefficient Based Reputation Mechanism for Isolating Selfish Nodes in Mobile Ad hoc Network”, *International Journal of Computer Sciences and Engineering*, *6*(6), 206-212.

AUTHORS PROFILE

Mr. V.Vijayagopal received his M.Sc and M.Phil from Madurai Kamaraj University, Madurai, India. Now doing his Ph.D research in Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India. His Research interested is Adhoc Networks, MANET. He has published more than 5 technical papers at various National / International Conferences and Journals.

Dr. K. Prabu received his MCA and M.Phil from Annamalai University, Chidambaram, India. He received his Ph.D Degree in Computer Applications from Manonmaniam Sundaranar University, Tirunelveli, India. He is now working as an Associate Professor in PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India. He is a Reviewer of 06 National/International Journals. His Research interested is Adhoc Networks, Wireless Networks & Mobile Computing, and Wireless Sensor Networks. He has published more than 75 technical papers at various National / International Conferences and Journals. He is a life member of ISTE, IACSIT, IAENG, and also senior member of IASED, and IRED.