Modified Bates Distribution for Selfish Node Detection Technique in MANETs

Ramesh V[1] Sureshkumar C[2] Venkatakrishnan S[3]

[1] Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore 641 046, TN, India.
[2] Principal, J.K.K Nattraja College of Engineering and Tech, Komarapalayam, TN, India.
[3]Assistant Professor, Department of Computer Science, Annamalai University, TN, India

Abstract-

The noteworthy dropping of data packets by the selfish node presents tremendous information overhead with expanded inactivity and vitality utilizations by expanding the quantity of retransmissions This MBD-SNDT is proposed for consolidating it in the system for improving the level of participation in the system with the view to limit the level of debasement in arrange execution. The recreation tests are likewise directed for measuring the hugeness as far as throughput, control overhead, all out overhead and parcel idleness so as to assess the criticalness of the proposed MBD-SNDT over the thought about standard self-centeredness discovery plots The re-enactment investigations and consequences of the proposed MBD-SNDT approach is resolved to be upgraded on a normal by 12% and 10% better than the looked at selfish node confinement approaches existing in the literature.

Key words: Selfish nodes, Selfish Node Detection Technique, Throughput, packet delivery rate, Modified Bates Distribution

Introduction

The collaboration of the mobile nodes is measured dependent on its sending potential ascribed for their neighbouring nodes in the impromptu system. The transmission of information through the helpful mobile nodes decreases the level of hazard included the fitting information dispersal in the system. Be that as it may, the selfish qualities of versatile hubs forces negative impact over the system by dropping significant number of bundles instead of sending so as to ration the had vitality for its own reality . Further, the presence of selfish nodes in the system additionally presents most extreme number of retransmissions that expands the control overhead and all out overhead in the system that contribute towards greatest system execution debasement. Henceforth, the childish expectation of versatile hubs should be viable recognized for improving the pace of information dispersal in the impromptu system. Various narrow minded plan discovery approaches were propounded in the writing utilizing watch dog, and token for precise confinement process. In any case, the majority of them are not fit in investigating the elements of egotistical hubs in a multi-dimensional viewpoint.

This MBD-SNDT is proposed for joining it in the system for improving the level of collaboration in the system with the view to limit the level of debasement in organize execution. The re-enactment tests are additionally led for measuring the centrality as far as throughput, control overhead, complete overhead and parcel inactivity so as to assess the essentialness of the proposed MBD-SNDT over the analyzed standard selfishness detection discovery plans.

Related Work

The authors [1] surveyed the challenges and proposals to mitigate performance degradation and network partitioning in MANETs. Most of the works to mitigate selfish behavior may be classified into Incentive-Based Mechanism, Reputation-Based Mechanism and different mechanisms. The authors [2] outline self-configuring because the capability to adapt involuntary ally and dynamically to environmental changes. The problem of stimulating cooperation in self-organizing mobile unintended networks for civilian applications is self-addressed [3]. This approach uses the tamper resistant hardware module referred to as security module in every node. A credit-based protocol to stimulate cooperation among mobile nodes in packet forwarding so as to enhance the network performance by mitigating the ungenerous behavior have planned by [4].The authors [5] planned a good, economical and secure cooperation incentive mechanism for multihop wireless networks to thwart stinginess attacks and to stimulate node cooperation so as to enhance the network performance and fairness. The fairness is achieved by charging each the supply and destination nodes of the communication.

selfish node detection approach victimization cluster head was planned for managing name and dependableness of mobile nodes within the network [6].This cluster head-based name theme was firm to cut back the degree of routing overhead and energy consumptions compared to the watch dog-based cooperative contact approach. The agreeable identification assault is observant [7] the all the new section hub in organize, useful hub square measure convey between the neighbor nodes and subsequent nodes in course and within the event that aggressor hubs is acknowledge, at that time heavy to the all hubs through combination places. SHRCDM was planned for facilitating vital cooperation between the mobile nodes [8]. This SHRCDM motor-assisted in higher discrimination of mobile nodes so as to cooperative and ungenerous nodes for superior performance improvement within the network.

In this native trust factor-based ungenerous node detection approach, a number of the selected nodes square measure used for analyzing the characteristics of mobile nodes so as to see the degree of intentional behavior attributed by them towards the network. A gradable Location Aware Hash Table-based Selfish Node Detection Mechanism (HLAHT-SNDM) was contributed victimization native and world name price determined through continuous observation [9]. Finally, the Hash Table-based Selfish Node Detection Mechanism (SMPM-SNDT) was planned for effective foretelling in malicious activity supported the present standing of packet forwarding rate [10]. The SMPM-SNDT was calculable for implementing superior performance in terms of increased outturn, reduced total overhead and management overhead. . The outturn and detection rate of this cluster head-based name approach was conjointly determined to the most underneath any variety of ungenerous nodes within the network.

The proposed Technique (MBD-SNDT)

The proposed MBD-SNDT, the detection and isolation of selfish nodes include

1. Calculation of mean packet deviation,
2. Estimation of variance and standard deviation for computing MBD and
3. Detection and isolation misbehaviour node.

Mean Packet Drop

If the number of packets forwarded and received by each node 'i' is $PF_{(1)}, PF_{(2)}, ..., PF_{(s)}$ and $PR_{(1)}, PR_{(2)}, ..., PR_{(s)}$ respectively as monitored by each of its neighbours in's' sessions. The number of packets dropped by each mobile node as monitored by their neighbours in each session 'k' is

$$DROP_{PACKET(k)} = PR_{(k)} - PF_{(k)} \quad (1)$$

The mean packet drop is

$$MDROP_{PACKET(k)} = \sum_{k=1}^{s} \frac{DROP_{PACKET(k)}}{s} \quad (2)$$

Total variance

The total variance is

$$\text{T-}VAR_{DETECT} = \sum_{c=1}^{s} \frac{(PR_{(c)} - MDROP_{PACKET(c)})}{s} \quad (3)$$

The MBD computed based on (3) and (4) is

$$(BDITF)_{DETECT} = \frac{s}{s-1}\left(1 - \frac{\sum_{k=1}^{s}(DROP_{PACKET(k)} * PR_{(k)})}{T - VAR_{DETECT}}\right) \quad (4)$$

The mobile nodes identified by MBD value less than 0.35 (obtained from simulation) are detected as selfish node misbehaviour.

Proposed Algorithm

The following algorithm illustrates the steps involved in detecting selfish node misbehaviour using MBDand isolating them from the multicasting activity.

1. Let N be number of nodes.
2. GN – Group of nodes of the routing path, SN (source node) and DN (the destination node) respectively.
3. The mobile node which is ready for data transmission acknowledge SN by `RREP' message.
4. Let this algorithm step (6 -13) be executed for a node 'n' number of sessions for transmission.
6. For every node 'u' of GN in the routing path.
7. Estimate $DROP_{PACKET(k)} = PR_{(k)} - PF_{(k)}$
8. Compute $MDROP_{PACKET(k)} = \sum_{k=1}^{s} \frac{DROP_{PACKET(k)}}{s}$
9. Calculate $\text{T-}VAR_{DETECT} = \sum_{k=1}^{s} \frac{(PR_{(k)} - MDROP_{PACKET(k)})}{s}$

10. Estimate $(BDITF)_{DETECT} = \frac{s}{s-1}(1-\frac{\sum_{k=1}^{s}(DROP_{PACKET(k)} * PR_{(k)})}{T - VAR_{DETECT}})$

11. if (MBD(u) < 0.35) then

12. Node u is selfish node misbehaviour compromised

13. Call Selfish_Node_Attack-Mitigation (u)

14. Else

15. Node u is reliable

16. End if

17. End for

18. End.

Results

The predominance of the proposed MBD-SNDT is investigated based on simulation experiments conducted using ns-2.33. The potential of the proposed MBD-SNDT approach is compared with the existing SMPM-SNDT, HLAHT-SDNM and SHRCDM approaches using the packet delivery ratio, throughput, total overhead and energy consumptions under increasing number of mobile nodes and selfish nodes. The data traffic pattern used for implementation is Constant Bit Rate (CBR) data traffic. The simulation time used for the proposed MBD-SNDT is 300 seconds with pause time of 20 seconds.

Figure 1 and 2 exemplars the potential of the proposed MBD-SNDT approach using packet delivery ratio and throughput investigated under increasing rate of mobile nodes. The packet deliver ratio of the proposed MBD-SNDT approach is confirmed to be superior by 6%, 10%, 13% compared with the existing SMPM-SNDT, HLAHT-SDNM and SHRCDM approaches. Similarly, the throughput of the proposed MBD-SNDT approach is determined to be excellent by 9%, 11%, 14% compared with the existing SMPM-SNDT, HLAHT-SDNM and SHRCDM approaches.

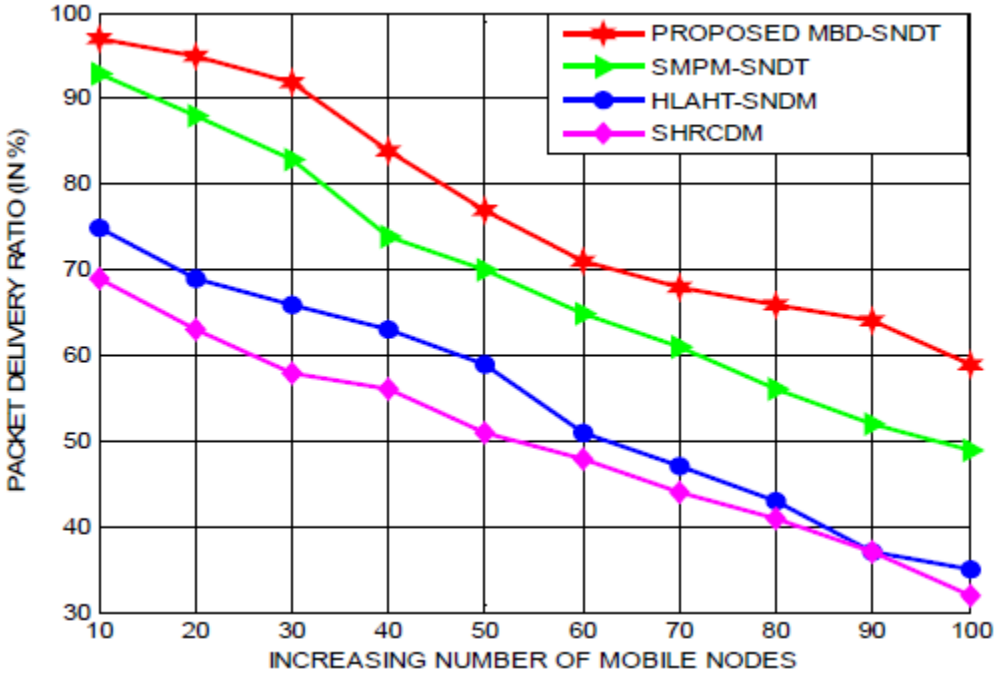

Figure .1 Performance of MBD-SNDT using packet delivery ratio under increasing mobile nodes

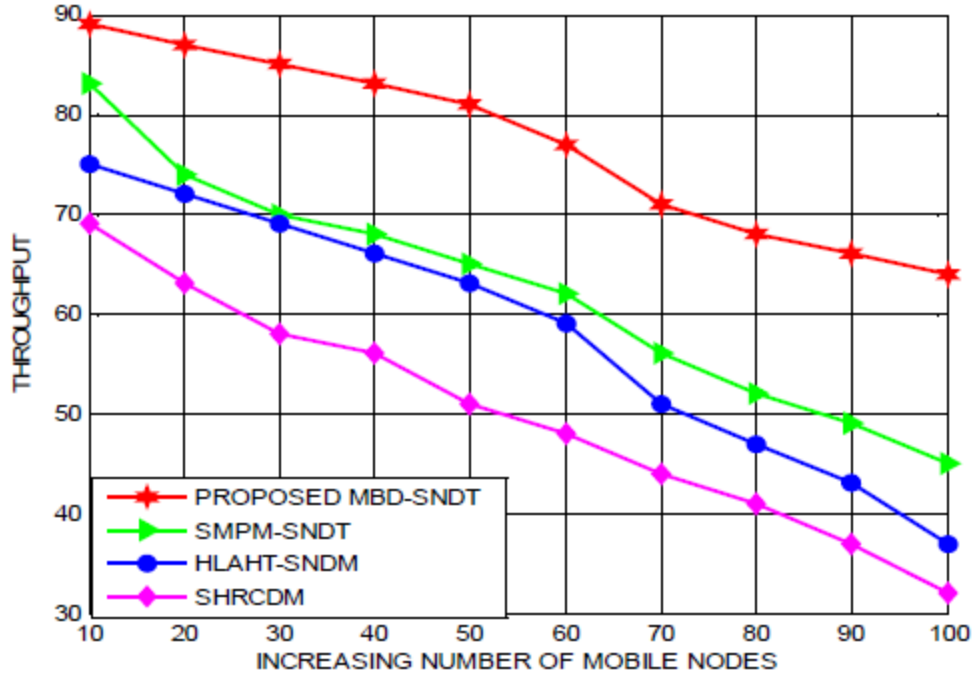

Figure .2 Performance of MBD-SNDT using throughput under increasing mobile nodes

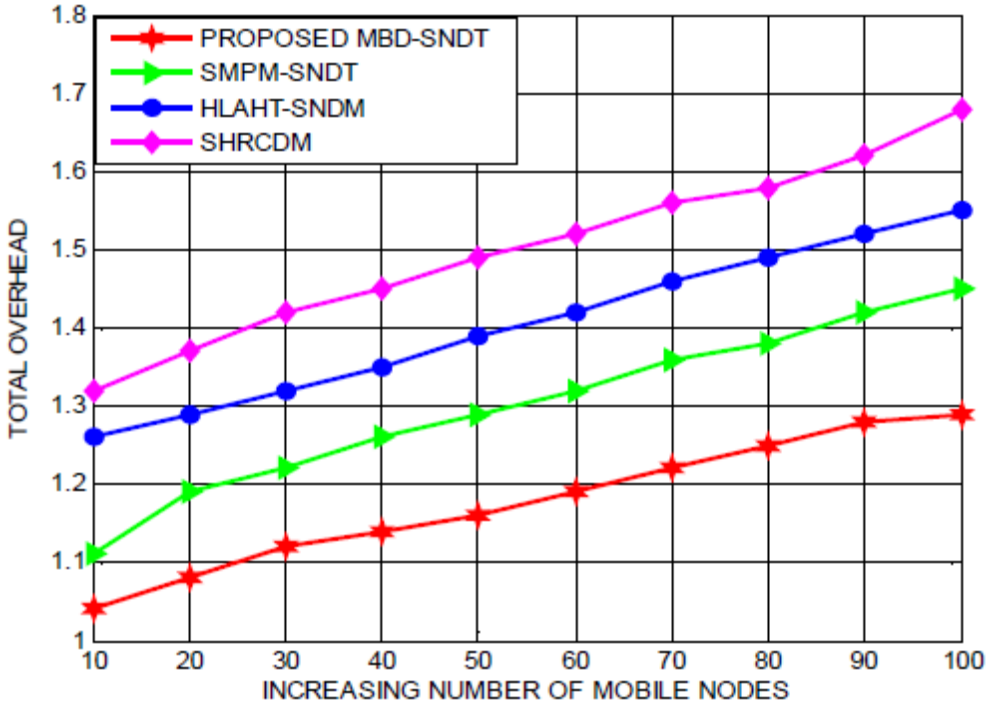

Figure.3 Performance of MBD-SNDT using packet delivery ratio under increasing mobile nodes

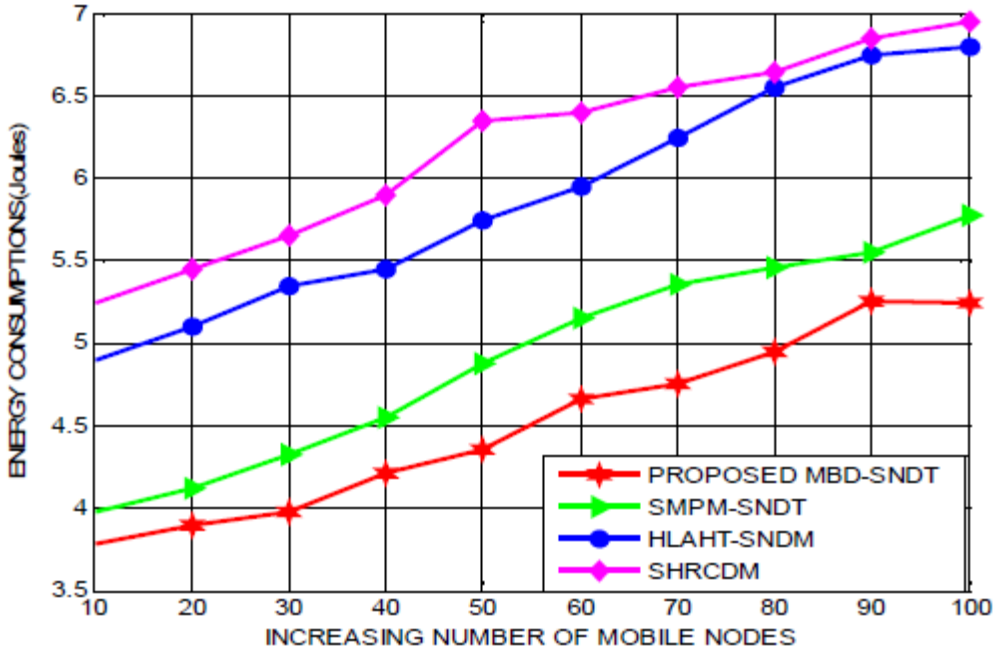

Figure. 4 Performance of MBD-SNDT using energy consumptions under increasing mobile nodes

Figure 3 and 4 unveils the significance of the proposed MBD-SNDT approach using total overhead and energy consumptions investigated under increasing rate of mobile nodes. The total overhead of the proposed is significantly minimized by 10%, 13% and 15% remarkable with the existing SMPM-SNDT, HLAHT-SDNM and SHRCDM approaches. Similarly, the energy consumptions of the proposed approach is determined to be excellently reduced by 8%, 10% and 13% compared with the existing SMPM-SNDT, HLAHT-SDNM and SHRCDM approaches.

Figure 5 and 6 quantifies the potential of the proposed SDITF-SNDT approach using packet delivery ratio and throughput investigated under increasing rate of selfish nodes. The packet delivery ratio of the proposed approach under increasing selfish nodes is confirmed to improve 9%, 13% and 16% excellent to the benchmarked SMPM-SNDT, HLAHT-SDNM and SHRCDM approaches. Similarly, the throughput of the proposed approach under increasing selfish nodes is determined to be excellent by 10%, 12% and 15% compared with the existing SMPM-SNDT, HLAHT-SDNM and SHRCDM approaches.

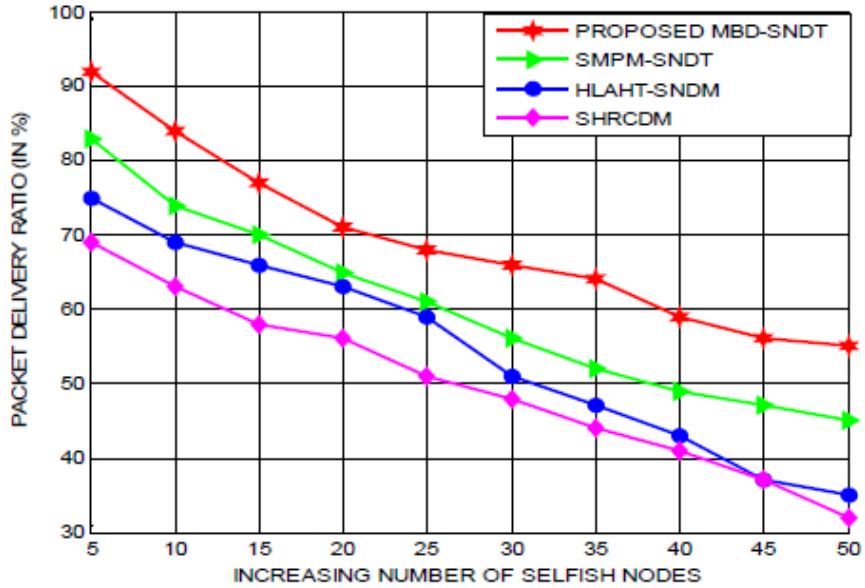

Figure. 5 Performance of MBD-SNDT using packet delivery ratio under increasing selfish nodes

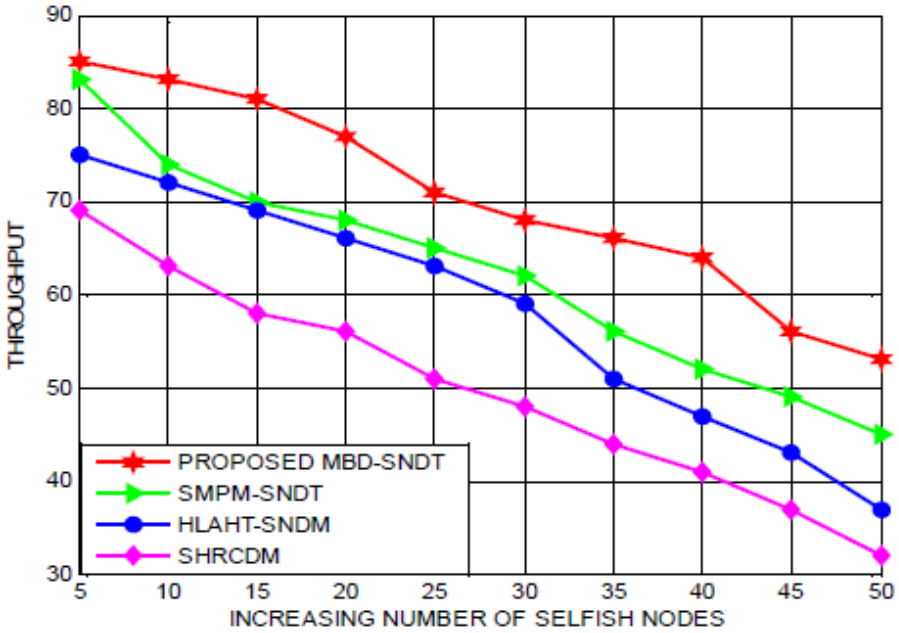

Figure. 6 Performance of MBD-SNDT using energy consumptions under increasing mobile nodes

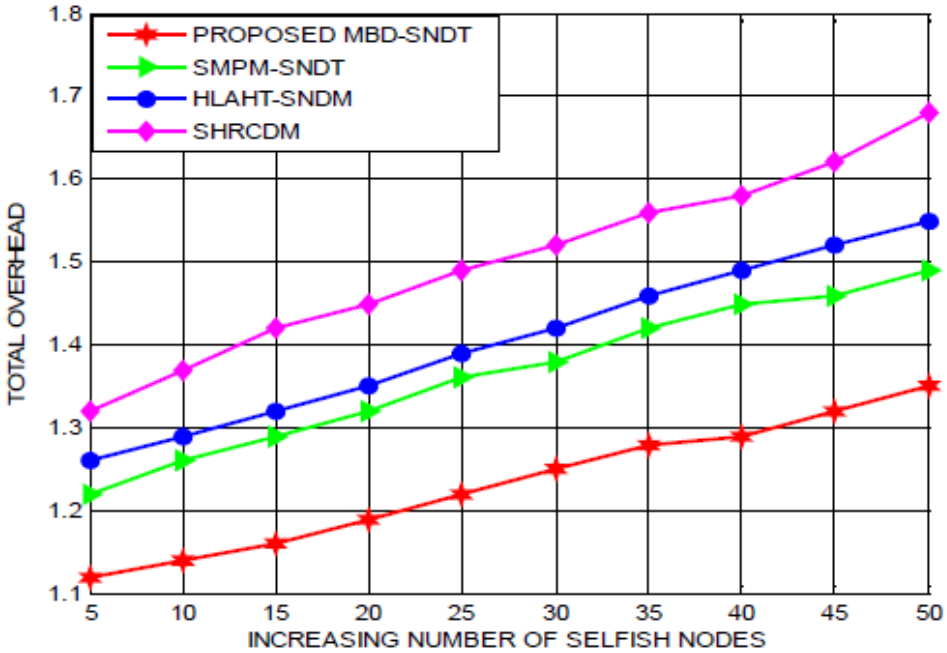

Figure. 7 Performance of MBD-SNDT using packet delivery ratio under increasing mobile nodes

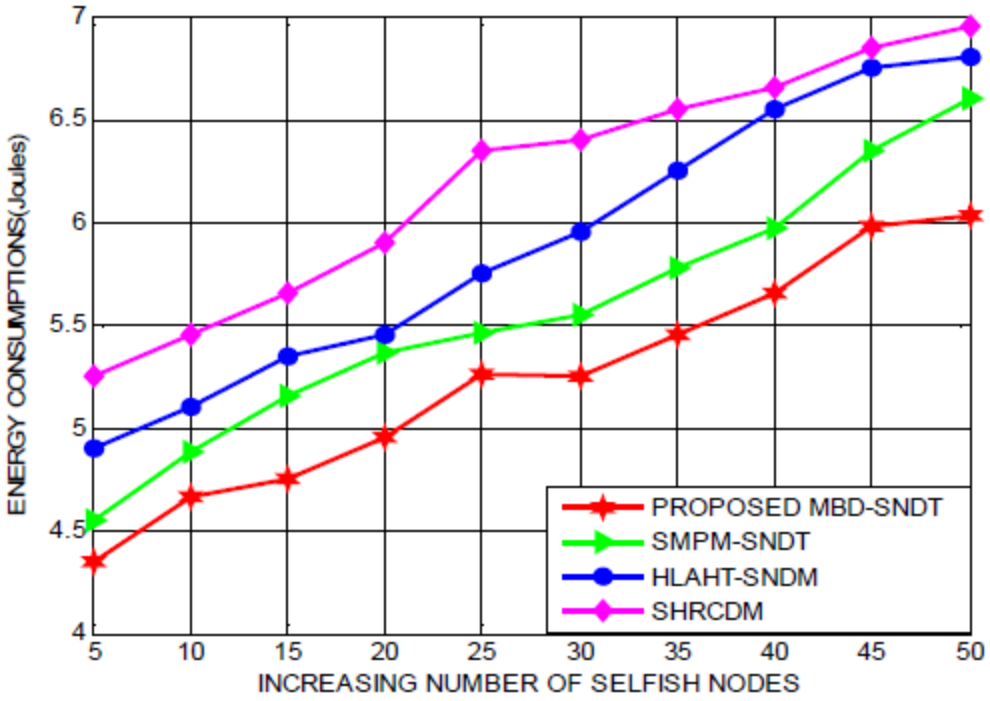

Figure. 8 Performance of MBD-SNDT using energy consumption under increasing mobile nodes

Figure 7 and 8 highlights the significance of the proposed MBD-SNDT approach using total overhead and energy consumptions investigated under increasing rate of selfish nodes. The total overhead of the proposed approach is determined to be significantly minimized by 10%, 13% and 16% remarkable to the existing SMPM-SNDT, HLAHT-SDNM and SHRCDM approaches. Similarly, the energy consumptions of the proposed approach is determined to be excellently reduced by 7%, 9% and 12% compared with the existing SMPM-SNDT, HLAHT-SDNM and SHRCDM approaches.

Conclusion

This proposed MBD-SNDT was presented using variance and mean packet forwarding rate for estimating the degree of influence induced by the selfish characteristics of mobile node towards the network such that accurate detection and isolation of selfish nodes can be imposed for enhancing the degree of network performance. The simulation experiments of the proposed MBD-SNDT confirmed a mean improvement rate of 19% and 17% in packet delivery and throughput with 20% and 12% minimized energy consumptions and routing overhead rate compared to the selfish nodes isolation approaches contributed in the literature. The mean rate in detection of the proposed was also determined to be improved by 18% superior on par with the compared selfish nodes isolation approaches.

References

[1] S.Tamilarasan and Dr.Aramudan (2011)A performance and Analysis of Misbehaving node in MANET using IDS" International Journal of Computer Science and Network Security VOL.11 No.5, May 2011,258-264 Communications on Applied Electronics, 3(5), 43-49.
[2] Aliu et al.] (2012). Optimizing Monitoring Requirements in Self-adaptive Systems International Conference on Exploring Modeling Methods for Systems Analysis and Design, 362-367.
[3] Buttyan et.al (2003). Self-Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing 2(1):52- 64.
[4] Zhang et al (2011). An Energy Efficient-Based AODVM Routing in MANET, International Conference on Information and Management Engineering Innovative Computing and Information, 66-72.
[5] Mahmoud, M.M.E.A., Shen, X.S. (2014) secure routing protocols. In: Security for Multi-hop Wireless Networks, pp. 63–93.
[6] Manzoni.P.et.al (2007) A Low-Complexity Routing Algorithm with Power Control for Self-Organizing Short-Range Wireless Networks, Wireless Personal Communications volume 41, pages407–425.
[7] Dr.E.Mohan, Dr.A.Annamalai (2018) Distributed Attack Detection For Wireless Sensor Networks, International Journal of Engineering & Technology, 7(6), 465-468.
[8] Sengathir, J., & Manoharan, R. (2013). A split half reliability coefficient based mathematical model for mitigating selfish nodes in MANETs. 2013 3rd IEEE International Advance Computing Conference (IACC), 2(1), 78-87.
[9] Ramya, K., & Kavitha, T. (2016). Deterring selfish nodes using hierarchical account-aided reputation system in MANET. 2016 International Conference on Computing technologies and Intelligent Data Engineering (ICCTIDE'16), 2(2), 34-45.
[10]Karthikayen, A et.al. (2018). A Skellam distribution inspired trust factor- based selfish node detection technique in MANETs. *Journal of Advanced in dynamical and control systems*, *10*(13), 940-949.