A Modified Skellam Distribution - Based 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 , 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 trust of mobile nodes within the network is taken into account because the potential factor that requires to be investigated for facilitating predominant network performance. This network performance influencing trust is degraded by the presence of intentionally behaving selfish nodes that doesn't forward data packets to their neighborhood cooperative mobile nodes. These selfish nodes reduce the packet forward activity counting on its own energy state for conserving its energy so as to measure active within the network. Here, a Modified Skellam Distribution -based Selfish Node Detection Technique (MSD-SNDT) is proposed for enforcing effective and efficient detection and isolation of selfishly behaving mobile nodes from the network. The simulation experiments is conducted for quantifying the excellence of the proposed MSD-SNDT approach in terms of packet delivery, throughput, total overhead and energy consumptions under varying numbers of mobile nodes and selfish nodes within the network.

Key Words: Selfish nodes, Selfish Node Detection Technique, Throughput, packet delivery rate, Modified Skellam Distribution

Introduction

In Mobile Ad hoc Network (MANET), the dependability of the portable hubs towards bundle sending is resolved to be fundamental substance for guaranteeing predominant parcel sending rate .This unwavering quality of versatile hubs is affected by their egotistical conduct towards information sending movement so as to stay dynamic in the system. Huge number of essential applications, specially appointed explicit attributes, dynamic topology and absence of incorporated control in impromptu systems brought about difficulties and worries as for protection and security of the information and directing data. The remote idea of system with innate unique topology is fundamental explanation of security related concerns. Foundation less systems administration and absence of brought together control influences the foundation and reviving of security related data. The presence of narrow minded hubs in the system step by step expanding the directing overhead since the bundles are dropped by the versatile hubs instead of sending them. Skellam circulation is considered as the most intense dissemination that models the parameters utilized for narrow minded hub identification as the discrete irregular variable so as to examine them for accomplishing prevalent discovery. Skellam dispersion is likewise considered for evaluating the specific measurement about the negative effect forced by the egotistical hubs under directing. In this way, a narrow minded hub discovery and disconnection approach that relies upon Skellam dispersion is basic for precise improvement in the exhibition of the system as far as parcel conveyance and throughput.

This proposed MSD-SNDT uses the key advantages of Skellam Distribution for guaranteeing potential childish recognition process.

Literature review

At first, an selfish node identification conspire utilizing vitality level and proportion of node correspondence was propounded for recognizing the malevolent narrow minded movement of the portable hubs in the system [1]. This vitality level and proportion of hub correspondence based egotistical hubs location approach was evaluated to improve the pace of identification with the end goal that the childish purpose of the versatile hubs is forestalled to the greatest degree.

Community guard dog [2] approach and a systematic model that assesses time of identifying the narrow minded hubs, they have expanded the work incase egotistical hub builds a mean-max estimate for attainable computation.A convention on-request multi-way steering [3]in portable specially appointed systems, the proposed framework is plausible and adaptable to locate the briefest way to transmit the information bundles in a protected technique with vindictive hub identification. The agreeable identification assault is observing [4] the all the new section hub in organize, helpful hub are convey between the neighbor hubs two sequent hubs in course and in the event that aggressor hubs is recognize, at that point disturbing to the all hubs through combination places.

A vigorous agreeable trust [5] establishing plan for conveying the bundles safely and dependably in multi-bounce courses, in the plan deciding the trust for every hub, In direct hub trust is by MAC layer and recycled hub is by suggestion of the neighboring hubs so as to recognize and send parcels, this is powerful on the bogus data of vindictive hubs. Likewise, Distributed Detection of Selfish Nodes utilizing Dynamic Associativity (DDSN-DA) was proposed for decreasing the level of bogus discovery in the narrow minded hubs of the system [7]. The level of trust and recognition encouraged by this DDSN-DA plot was end up being augmented during the way toward sorting versatile hubs into narrow minded and dependable. At long last, an Exponential Reliability Factor-based Selfish Node Detection Technique (ERF-SNDT) was proposed for potential identification and confinement of childish hubs in the system [8]. This ERF-SNDT approach was resolved to decrease the bundle drop, vitality utilizations, parcel idleness and all out overhead to the impressive level contrasted with the DDSN-DA and SRA-FSND approaches added to potential narrow minded hub recognition process. The pace of bogus

positive pace of this proposed ERF-SNDT approach was resolved to be most extreme with decreased overhead in calculation and correspondence of the system.

At long last, the Semi-Markov Process Mechanism utilizing Selfish Node Detection Technique (SMPM-SNDT) was proposed for successful guaging in malevolent movement dependent on the present status of parcel sending rate [6]. The SMPM-SNDT was evaluated for upholding unrivaled execution as far as improved throughput, decreased complete overhead and control overhead[9].

Modified Skellam Distribution -based Selfish Node Detection Technique (MSD-SNDT)

The MSD-SNDT is developed in this research for detecting selfish nodes.
MSD-SNDT, follow three steps viz., 1) Computing mean deviation, 2) Computing MSD and 3) Detection of such nodes.

Mean packet deviation

The deviation in the number of packets received to the number of packet forwarded by each mobile node to their neighbors as recommended through neighbor-based interaction in each session 'c' is

$$DEVIATION_{PACKET(c)} = PR_{(c)} - PF_{(c)} \quad (1)$$

$PF_{(1)}, PF_{(2)}, ..., PF_{(s)}$ and $PR_{(1)}, PR_{(2)}, ..., PR_{(s)}$ define packet forwarded and packet received respectively by each of its neighbors in 's' sessions.

Packet forwarding capability identified by their neighbor is

$$P_{PFC(c)} = \frac{PF_{(c)}}{PR_{(c)}} \quad (2)$$

The mean packet deviation is given by

$$MDEV_{PACKET(c)} = \sum_{c=1}^{s} \frac{DEVIATION_{PACKET(c)}}{s} \quad (3)$$

Calculation of variance and standard deviation for computing MSD

$$STD_{DETECT} = P_{PFC(s)} * (1 - P_{PFC(s)}) \quad (4)$$

$$VARIANCE_{DETECT} = \sum_{c=1}^{s} (MDEV_{PACKET(c)} - DEVIATION_{PACKET(c)})^2 \quad (5)$$

Then MSD computed based on (4) and (5) is

$$MSD_{DETECT} = \frac{s}{s-1}\left(1 - \frac{\sum_{c=1}^{s} STD_{DETECT}}{VARIANCE_{DETECT}}\right) \quad (6)$$

Detection and isolation of selfish nodes misbehavior using computed MSD

The mobile nodes found with MSD value less than 0.35 are identified as selfish nodes and isolated.

Algorithm for the proposed MSD-SDNT

The following algorithm illustrates the steps involved in detecting selfish nodes using MSD

Proposed Algorithm:

1. Let N be number of nodes.
2. Let GN be group node (GN), in which SN is source node and DN is destination node.
3. Set of nodes in the routing path can be established by sending `RREQ' message by the NS to all other nodes in the network
4. Mobile node responds to the source node by `RREP'.
5. Let this algorithm step (6 -14) be executed for a node say, k, which belongs to the list GN, that uses‘t’ number of sessions for transmission.
6. For every node ‘k’of GN in the routing path.
7. Determine deviation using equation 1.
8. Compute packet forwarding capability using equation 2.
9. Calculate, mean deviation using equation 3.
10. Using equation 4 and 5 determine STD and VARIANCE respectively.
11. Compute MSD using equation 6.
12. if (MSD(k) < 0.35) then
13. node k is selfish node misbehavior compromised
14. Call Selfish_Node_-Mitigation (k)
15. Else
16. node k is reliable.
17. End if
18. End for
19. End for.

The threshold of the proposed MSD-SNDT approach is determined to be 0.35 based on simulations in which maximum number of selfish nodes is identified from the network with optimal performance improvement in the network.

Results and Discussions

The superior role of the proposed MSD -SNDT scheme is investigated using simulation experiments conducted using ns-2.31. The simulation time for the implementation is 100 seconds with the CBR traffic pattern of data. The number of mobile nodes in the network is 100 distributed in a random manner with the size bytes of 512 packets.

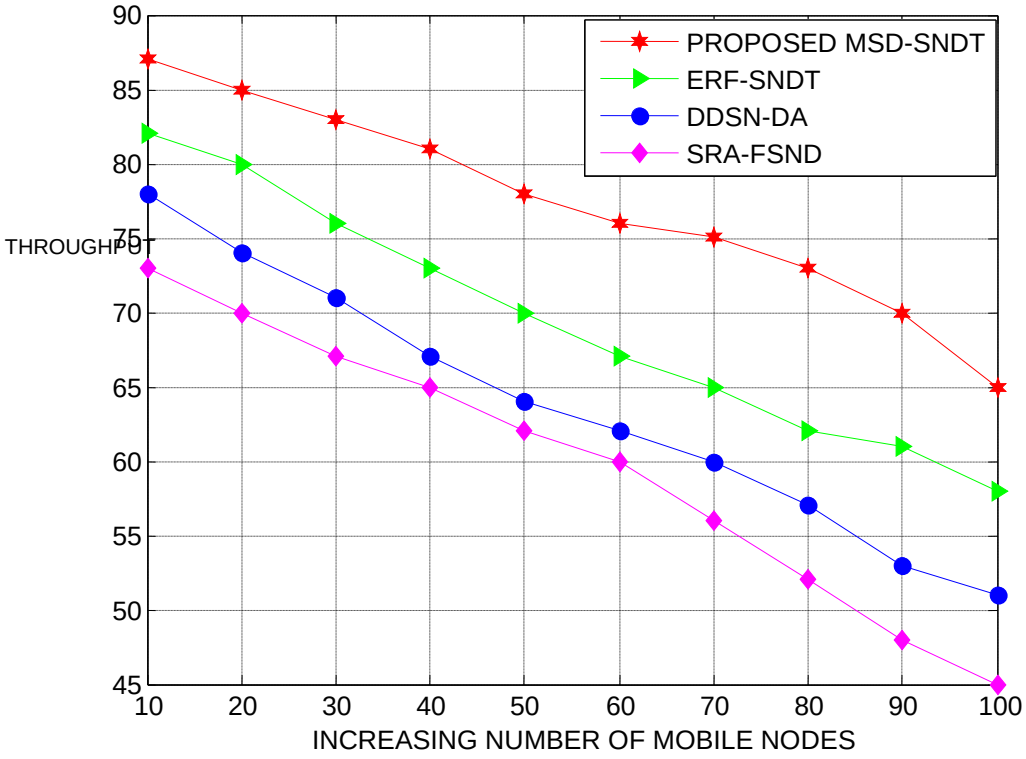
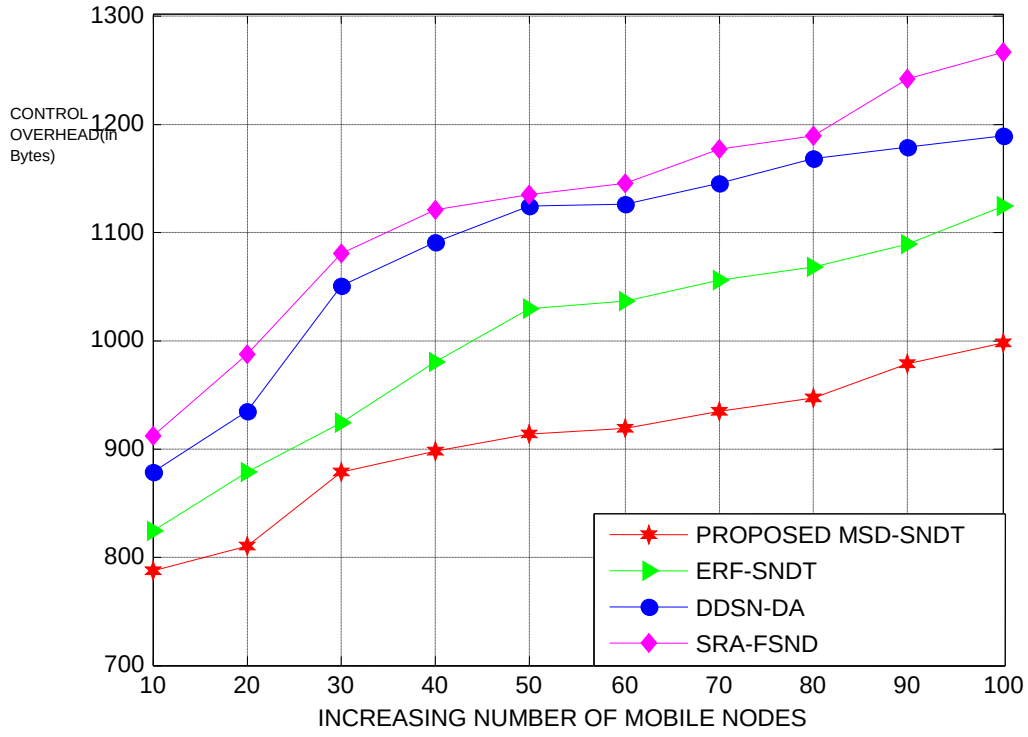


Figure 1: Performance of MSD-SNDT-throughput-different mobile nodes

Figure 1 models the throughput of the proposed MBD-SNDT plot investigated under an alternate number of versatile hubs in the system. The proposed MBD-SNDT is deduced to expand the throughput to a most extreme degree of 11%, 13% and 18% better than the analyzed ERF-SNDT, DDSN-DA and SRA-FSND approaches. Figure 2 depicts the control overhead of the MBD-SNDT conspire investigated under an alternate number of portable hubs in the system. The proposed MBD-SNDT is demonstrated to limit the control overhead to a most extreme degree of 10%, 14% and 18% better than looked at ERF-SNDT, DDSN-DA and SRA – FSND

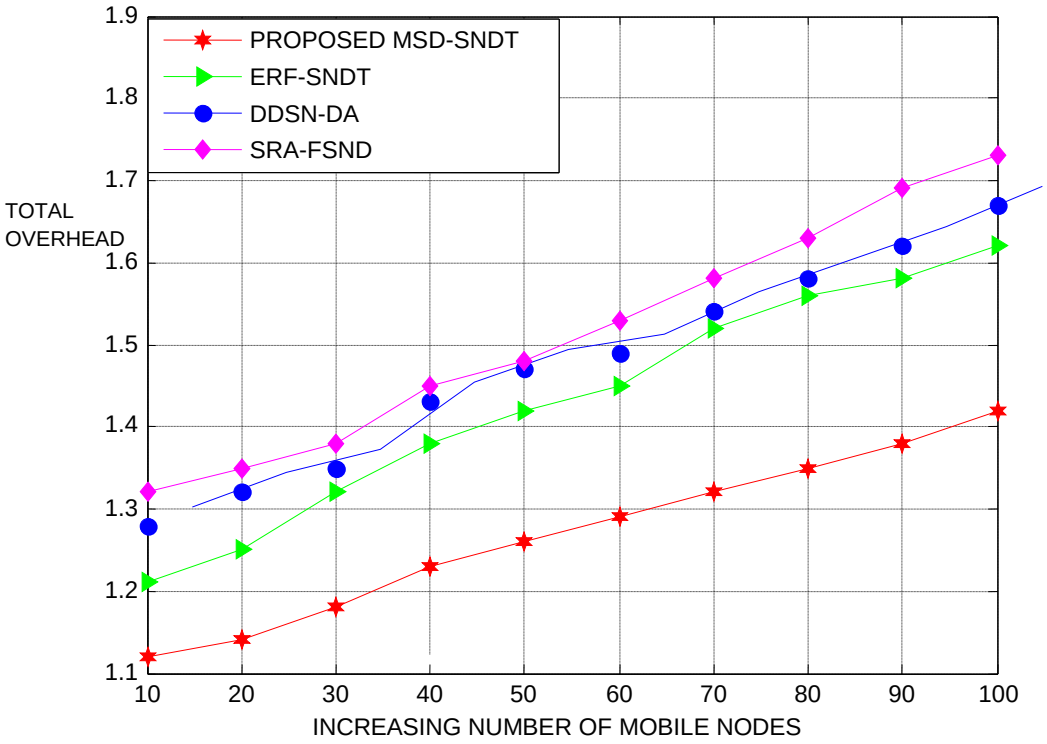


.

Figure 2: Performance of MsSD-SNDT-control overhead-mobile nodes

Figure 3 features the complete overhead of the proposed MBD-SNDT plot investigated under an alternate number of portable hubs in the system. The proposed MBD-SNDT is resolved to lessen complete overhead to a greatest degree of 9%, 12% and 18% better than the thought about ERF-SNDT, DDSN-DA and SRA-FSND approaches. Figure 4 presents the plots in the bundle dormancy of the proposed MBD-SNDT conspire researched under an alternate number of versatile hubs in the system. The proposed

MBD-SNDT is resolved to limit the bundle idleness to an impressive degree of 12%, 18% and 21 better than the analyzed ERF-SNDT, DDSN-DA and SRA-FSND.



.

Figure 3: Performance of MSD-SNDT-total overhead-different nodes

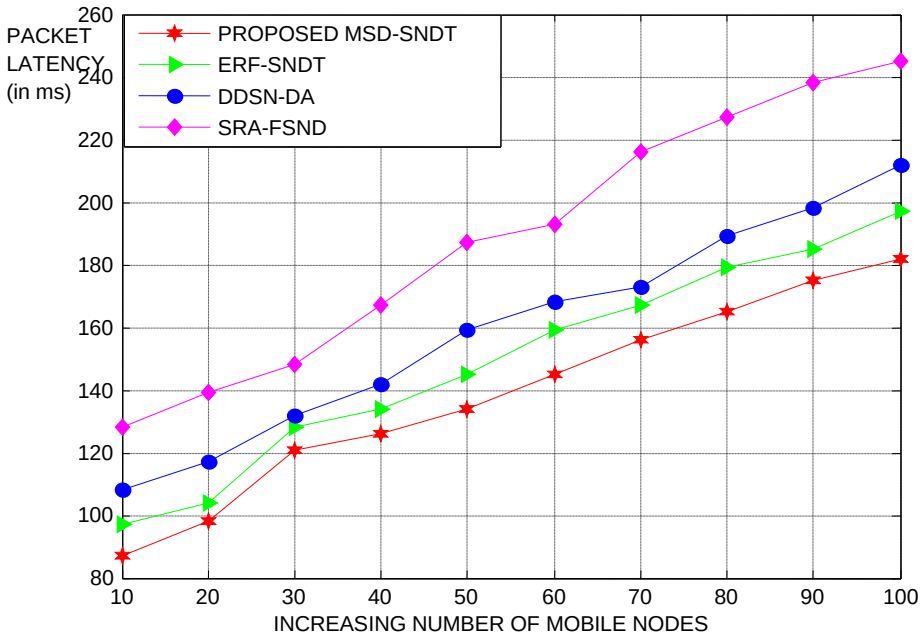


Figure 4: Performance of MSD-SNDT-packet latency-sdifferent mobile nodes

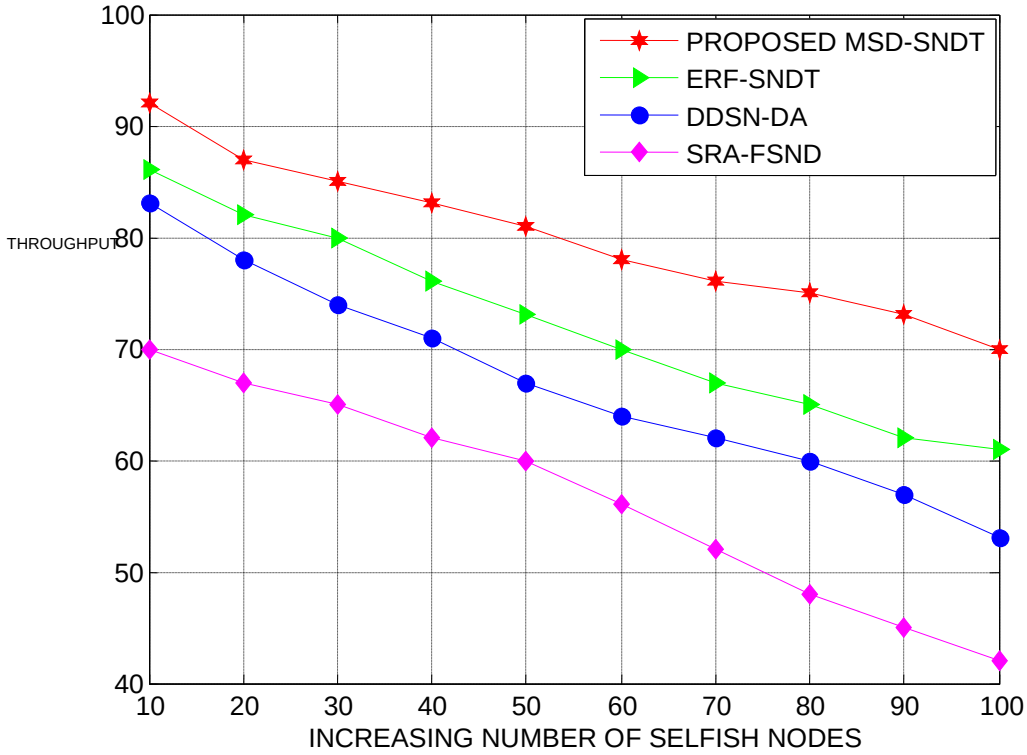


Figure 5: Performance of MSD-SNDT-throughput-different selfish nodes

Figure 5 features the throughput of the proposed MBD-SNDT conspire investigated under an alternate number of egotistical hubs in the system. The proposed MBD-SNDT is derived to expand the throughput to a most extreme degree of 11%, 15% and 19% better than the looked at ERF-SNDT, DDSN-DA and SRA-FSND approaches. Similarly, Figure 6 models control overhead of the proposed MBD-SNDT plot investigated under an alternate number of egotistical hubs in the system. The proposed MBD-SNDT is demonstrated to limit the control overhead to a greatest degree of 11%, 14% and 16% better than the analyzed ERF-SNDT, DDSN-DA and SRA-FSND approaches.

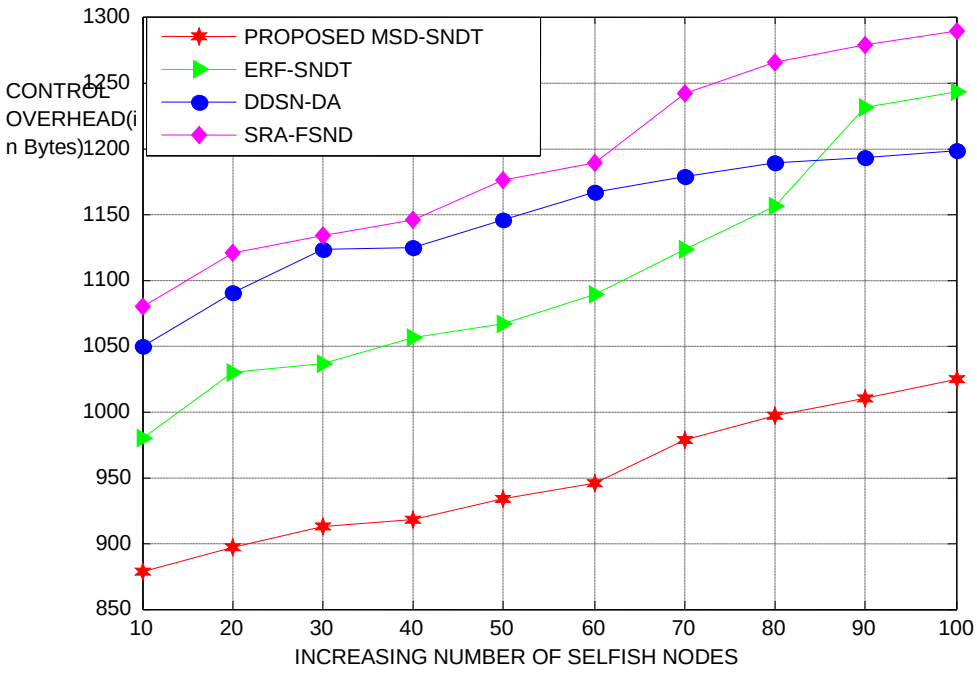


Figure 6: Performance of MSD-SNDT-control overhead-selfish nodes

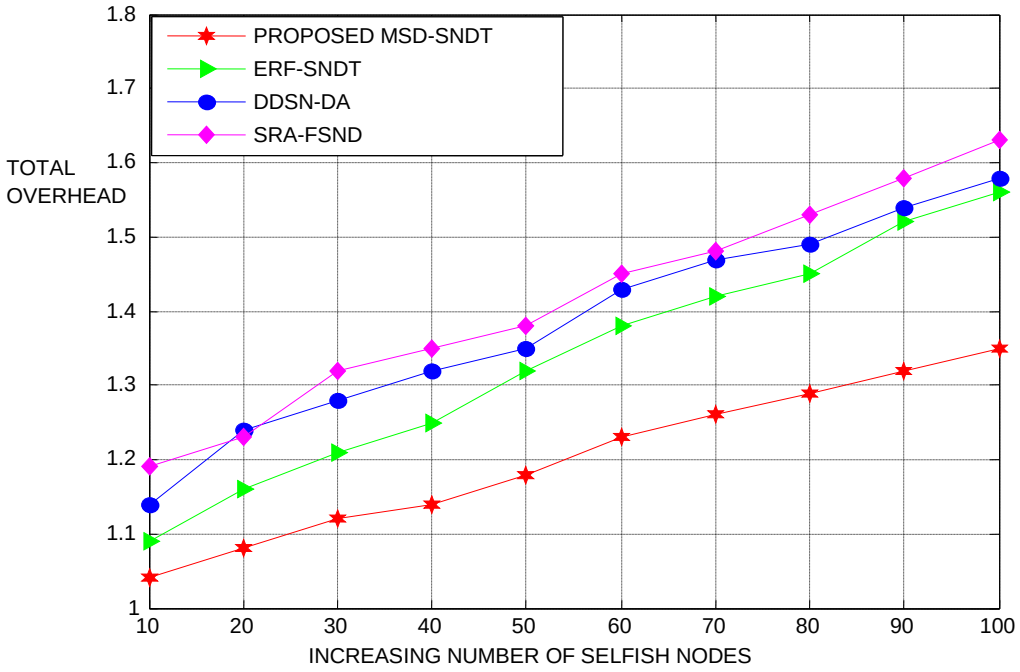


Figure 7: Performance of MSD-SNDT-total overhead-different selfish nodes

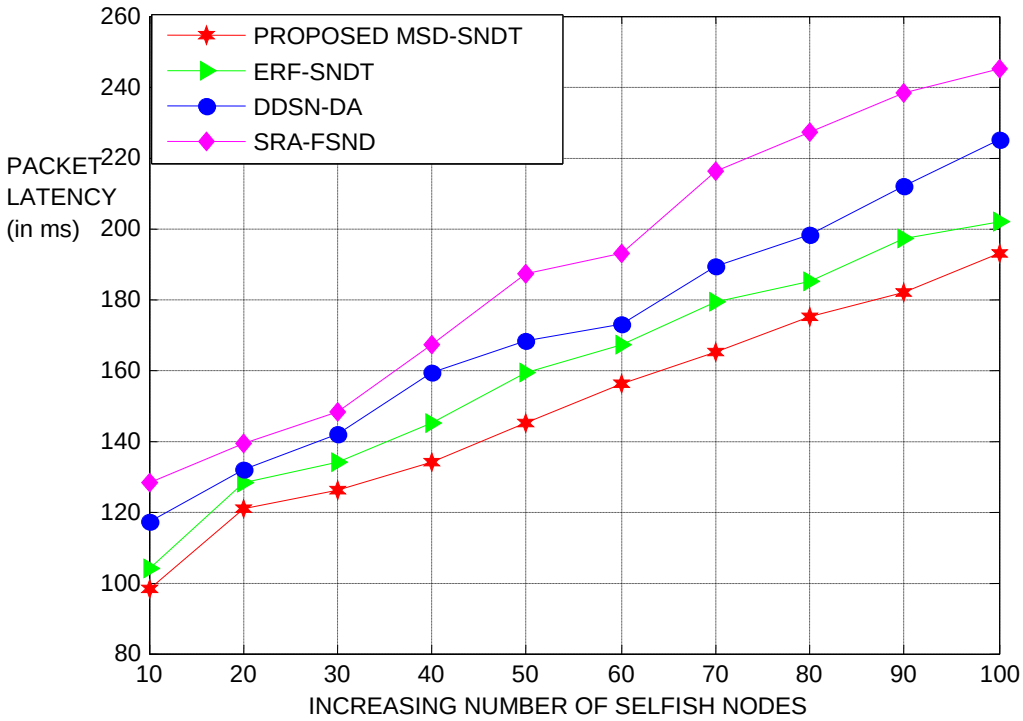


Figure 8: Performance of MSD-SNDT-packet latency-different selfish nodes

Figure 7 portrays the proposed MBD-SNDT is resolved to diminish all out overhead to a most extreme degree of 9%, 12% and 16% better than the looked at ERF-SNDT, DDSN-DA and SRA-FSND approaches. Figure 8 reveals the proposed MBD-SNDT is resolved to limit the parcel inertness to a significant degree of 12%, 15% and 18% better than the analyzed ERF-SNDT, DDSN-DA and SRA-FSND approaches.

5. Conclusions

The MSD-SNDT was introduced as a solid endeavor for critical recognition of narrow minded conduct by investigating various degrees of powerful factors that contribute towards compelling self-centeredness location. This proposed approach was additionally evaluated to be unrivaled in the successful identification of childish hubs through the multi-dimensional examination of each observed portable hubs' and its trait towards the sending capability of other working together versatile hubs. The reenactment tests and aftereffects of the proposed

MSD-SNDT approach was resolved to be astounding in decreasing the control overhead, absolute overhead and parcel dormancy on normal by 19%, 15% and 17% dominating than the narrow minded node location plans utilized for investigation. The location pace of the proposed MSD-SNDT approach was likewise affirmed to be upgraded by 12% phenomenal to the looked at narrow minded hub recognition plans.

References

[1] Santhos kumara et.al . (2015). " Revial of selfish nodes in clustered MANET" *International Journal of Advancesin Engineering and Technology* , *8*(3), 412-419.
[2] Hernández-Orallo et al (2015). A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes, *IEEE Transactions on Mobile Computing*, *14*(6), 1162-1175.
[3] Hui-xia et.al. (2013). Trust prediction and trust- based source routing in mobile ad hoc networks. *Adhoc Networks*, *11*(7), 2096-2114.
[4] Dr.E.Mohan, Dr.A.Annamalai "Distributed Attack Detection For Wireless Sensor Networks " *International Journal of Engineering & Technology***,** Volume 7 ,issue 6, 465-468 , 2018, *(*ISSN: 2227-524X).
[5] C.Zouridaki et al. (2005). A quantitative trust establishment framework for reliable data packet delivery in MANETs, Proceedings of ACM SASN, *2005*, 1-10.
[6] Sengathir, J., & Manoharan, R. (2015).A futuristic trust coefficient-based semi-Markov prediction model for mitigating selfish nodes in MANETs. *EURASIP Journal on Wireless Communications and Networking*, *2015*(1), 45-67.
[7] Tarannum, R.et.al .Detection and deletion of selfish MANET nodes distributed approach. *2012 1st International Conference on Recent Advances in Information Technology* , *2*(3), 45-56.
[8]Sengathir, J., & Manoharan, R. (2016). Exponential reliability factor based mitigation mechanism for selfish nodes in MANETs. *Journal of Engineering Research*, *4*(1), 67-78.
[9]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.