EAI Endorsed Transactions
on Energy Web

Research Article EAI.EU

Selfish Node Detection Scheme based on Bates Distribution Inspired Trust Factor for MANETs

Sengathir Janakiraman[1], M. Deva Priya[2,*]

[1]Department of Information Technology, CVR College of Engineering, Mangalpally, Vastunagar, Hyderabad, Telangana, India
[2]Department of Computer Science & Engineering, Sri Eshwar College of Engineering, Coimbatore, Tamilnadu, India

Abstract

The trustworthiness of mobile nodes is considered as the principal parameter for ensuring significant data dissemination in a Mobile Ad hoc NETwork (MANET). However, the selfish behaviour of nodes minimizes the trust by dropping a considerable amount of data packets in the network. The significant dropping of data packets by the selfish node introduces huge data overhead with increased latency and energy consumption, thus increasing the number of retransmissions. In this paper, Selfish Node Detection Scheme based on Bates Distribution Inspired Trust Factor (SNDS-BDITF) is propounded for predominant detection of selfish behaviour by investigating multiple levels of factors that contribute towards effective selfishness detection. The proposed SNDS-BDITF approach is also potent in enhancing the detection rate of selfishness by multi-perspective analysis of each monitored node's forwarding characteristics considering the benefits of other cooperating mobile nodes. The simulation results of the propounded SNDS-BDITF method are enhanced on an average by 16% and 14% when compared to the existing selfish node segregation mechanisms prevalent in the literature.

Keywords: Bates Distribution, Selfish behaviour, Trust Factor, Mean Packet Deviation, Variance, Standard Deviation

Received on 27 February 2020, accepted on 15 February 2023, published on 22 February 2023

Copyright © 2023 Sengathir Janakiraman *et al.*, licensed to EAI. This is an open access article distributed under the terms of the CC BY-NC-SA 4.0, which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/ew.v9i6.3065

1. Introduction

The trust possessed by each node in the Mobile Ad hoc Network (MANET) is considered as the essential parameter in enumerating the reliability of the nodes towards forwarding data packets [1]. MANET represents the category of ad hoc networks which is capable of changing the locations and configuring on the fly, since they comprise of nodes that are mobile and capable of establishing wireless connections to link several networks. MANET represents a decentralized network, wherein any node can join and leave with the influence of any predefined infrastructure in the network. The trustworthiness of nodes is greatly inclined by the selfishness of mobile nodes since they restrain the nodes from forwarding packets [2]. The intentional activity of selfish nodes is primarily due to its need for conserving energy that is essential for its existence in the network during routing [3]. Moreover, the presence of selfish nodes is found to gradually increase packet drop in the network [4]. Thus, the stringy selfish nodes need to be identified and removed from the network for ensuring predominant network performance [5]. Selfish node detection methods are propounded based on acknowledgement, token, incentive and game theory [6]. However, these contributed approaches possess the limitations of communication and computation overheads with high-energy utilization [7]. Further, Bates Distribution (BD) is determined to be significant which follows the property of continuous distribution for exploiting and exploring the inherent characteristics of mobile nodes during detection [8]. The value of BD is estimated to be predominant in selfish node detection since it is capable of exploring multiple levels of dependent factors that contribute to selfish node detection [9]. In addition, BD is also significant in removing the consistency level in the performance of mobile nodes [10]. This study can be possibly can be applied in any emergency situations such as distaster response, flooding, military vehicle monitoring and forest fire detection during which infrastructure cannot be established in the environment.

In this paper, a Selfish Node Detection Scheme based on Bates Distribution Inspired Trust Factor (SNDS-BDITF) is proposed for efficient identification and isolation of selfish nodes by exploring multi-perspective parameters that are responsible for the intentional activity. SNDS-BDITF deals with enhancing the degree of cooperation in the network with the view to minimize the degree of degradation of network performance. Simulations are conducted for enumerating the significance in terms of throughput, control and total overheads, and packet latency in order to assess the

significance of the propounded SNDS-BDITF over the baseline selfishness detection schemes.

The contribution can be completely realized in the environment during emergency events in which pre-defined insructure cannot be established. This study can be used for detecting the malicious as well as selfish nodes in the as hoc network environment for preventing the packet forwarding and energy depletion attack launched into the network imprlementation scenario. This proposed scheme not only detects the attack but determines the optimal paths through which the packets can be disseminated from the source to the destination.

2. Related Work

In this section, the latest works related to the recognition and segregation of selfish nodes are discussed with their merits and demerits.

Futuristic Trust Factor-based Semi-Markov Forecasting approach is propounded for recognizing and segregating selfish nodes [11]. This future forecasting approach is proposed for analysing and evaluating the impact of selfish nodes attributed in the sustainability of network lifetime. This futuristic trust parameter inspired selfish node detection is significant in framing the upper and lower limits of selfish node identification. The throughput of this approach is found to be maximum independent of the amount of selfish nodes existing in the network.

An evidence trust based selfish node identification is propounded by incorporating Trusted authority to identify the duplicate nodes formed by the adversary [12]. This evidence trust based selfish node detection approach employs enhanced self-centric friend tree for identifying selfish nodes. The data accessibility rate of this approach is identified to be maximum with reduced packet latency and routing overhead incurred during data dissemination.

An Erlang coefficient based conditional probabilistic scheme for effective selfish node detection is proposed with the view of investigating the conditional probability of interdependent events that influence malicious behaviour [13]. This conditional probability-based Erlang Coefficient parameter used in this approach is estimated to impact the determinants of selfish node characteristics in the network. This approach involves reduced energy, throughput and total overhead when compared to the evidence and future trust inspired forecasting approaches.

A cooperation inspired incentive approach is contributed for encouraging selfish nodes based on the trust evaluations [14] evaluations estimated over a time period. This type of evaluation in cooperation-based incentive helps in segregating selfish and cooperative nodes. The mobile nodes with lowest trust values are considered to be selfish on par with other collaborating nodes. Three different limits of mobile node co-operations are formulated for effectively categorising nodes as normal or selfish nodes.

A two-acknowledgement based selfishness identification approach is proposed for resolving the negative impacts of the nodes' stringy behaviour [15]. In this scheme, the acknowledgement packets are transmitted in the opposite sides of the established routing path. However, the main limitations are that only a reduced number of data packets are acknowledged through this detection mechanism. Throughput, energy consumption and packet latency of the two-acknowledgement scheme are determined to be more excellent than the cooperation incentive schemes. An Efficient security algorithm for detecting and isolating selfish nodes is proposed for reducing the cumulative amount of data overhead incurred in the process of data routing [16]. This security algorithm uses the concept of multiple level authentications in order to discriminate selfish nodes from cooperative nodes. The computation and communication complexity of this security algorithm is found to be very low in contrast to the acknowledgement mechanisms considered for study.

A couple based selfish node identification scheme is propounded for early detection of energy conserving stringent attackers in the network [17]. This detection scheme ensures that the selfish nodes use two levels of privacy such as source and sink level privacy by the process of flooding backbones in a predominant manner. This detection scheme is determined to be more significant than the existing cooperation enforcing approaches of the literature due to its incorporated dual level of mobile node monitoring. The detection rate is also confirmed to be superior than the compared evidence and cooperation enforcing approaches. A Secure Reputation Assisting Fully Selfish Node detection (SRA-FSND) is propounded for evaluating the influence of partial and fully selfish nodes [18]. This SRA-FSND scheme proves to focus on the Secure Hill Cipher Technique (SHCT) for ensuring effective memory space utilization in the network. This SRA-FSND approach is also estimated to enhance the fully selfish node elimination and detection times to the maximum level.

Distributed Detection of Selfish Nodes using Dynamic Associativity (DDSN-DA) is designed for reducing the degree of false detection in the selfish nodes of the network [19]. This DDSN-DA approach reduces the likelihood of a selfish mobile node entering a network in a distributed manner such that communication and computation overheads are minimized to the maximum level. The degree of trust and detection facilitated by this DDSN-DA scheme proves to be maximized during the process of categorizing mobile nodes into selfish and trustworthy.

An Exponential Reliability Factor based Selfish Node Detection Technique (ERF-SNDT) is propounded for effective detection and segregation of selfish nodes [20]. It is determined to reduce the packet drop and latency, energy and total overhead to a considerable level in contrast to the DDSN-DA and SRA-FSND mechanisms contributed to potential selfish node detection process. The rate of false positive rate of the proposed scheme is

seen to be maximum with reduced computation and communication overheads.

Yamini et al (2022) have proposed an Effective Trust Establishment-based Routing Evidence (ETERE) for creation as well as manipulation of illustrations of identified information. The basic idea of I-Trust is offering an intermittently Accessible Trusted Authority (ATA) to pass decision on node behaviour dependent on the collected routing indications with self and coordinate observation. Hackers or internal attackers who are aware of the security mechanism will not be able to take hold of the system. The mechanism offers improved routing efficiency, PDR and throughput.

Fayaz et al. [22] proposed a cooperation enforcement approach using a reputation strategy which explores the selfish and malicious characteristics of mobile nodes. It determined the value of reputation for saving the resources of other interacting mobile nodes and prevent mobile nodes from being detached from the network. The results of this reputation strategy proved its efficacy in minimized the normalized routing load with maximized packet delivery fraction under the presence of selfish and malicious nodes. It was also identified to detect and isolated selfish nodes at a faster rate. Chiejina et al. [23] proposed a trust management system using Dirichlet reputation for assessing the trust of nodes cooperating in the network. It was proposed with candour integrated into the different modes of operations, such that the network security is never compromised. It specifically employed Dirichlet probability distribution for computing the reputation of mobile nodes using the first and second-hand information. It calculated the trust values and cumulative reputations of mobile nodes using a two-dimensional candour reputation evaluation process. The results proved its efficiency in sustain the energy rate of the mobile nodes.

Sharma and Dinkar [24] have designed a reputation strategy using incentives which was determined by clustering the social features of cooperating mobile nodes depending on the computation of weighted social tie. This reputation mechanism depends on the strength of social connections and updates the social tie weight depending on the incentives provided as penalty and reward in the network. This strategy facilitated the incentive when the deviation between residual energy and packet delay is not realized. It penalized the node when the trade-off between energy and packet delay is maximized. It utilized the merits of modularized deep nonnegative matrix deep autoencoder for calculating the trust of mobile nodes using the social features. The experimental validation of this incentive approach confirmed better throughput and minimized delay for varying times of simulations. Rama Abirami & Sumithra [25] a routing mechanism which utilized a simplified neighbour credit value integrated with AODV for attaining maximized cooperation in the network. It was proposed with minimized false detection rate for preventing unnecessary isolation of selfish nodes from the network. It adopted a contextual parameters which aided in discriminating malicious node fromgenuine nodes of the network, The rate of detection facilitated by this approach was better than most of the incentive-based selfish isolation methodologies of the literature.

3. Proposed Selfish Node Detection Scheme based on Bates Distribution Inspired Trust Factor (SNDS-BDITF)

Selfish Node Detection Scheme based on Bates Distribution Inspired Trust Factor (SNDS-BDITF) is a vital numerical reliability factor-based alleviation scheme propounded for detection and isolation of selfish nodes from an ad hoc environment. The nodes that are selfish are recognized and quarantined using the following steps: a) Approximation of Mean Packet Deviation b) Computation of Variance and Standard Deviation (SD) for determining BDITF c) Detection and isolation of selfishness using calculated BDITF. Table 1 lists the notations involved.

Table 1: Nomenclature

Notation	Description
$PF_{(1)}, PF_{(2)}, PF_{(3)}, .., PF_{(S)}$	Quantity of Packets sent in all sessions
$PR_{(1)}, PR_{(2)}, PR_{(3)}, .., PR_{(S)}$	Quantity of Packets received in all sessions
$DROP_C^{PACKET}$	Amount of dropped packets
PR_C	Total Quantity of Packets sent in session ‘c’
PF_C	Total Quantity of Packets received in session ‘c’
$MDROP_C^{PACKET}$	Mean Packet Drop of a node in session ‘c’
T_VAR_{DETECT}	Total Variance experienced by a mobile node
$(BDITF)_{DETECT}$	Detected Bates Distribution Inspired Trust Factor

3.1 Approximation of Mean Packet Deviation

In the propounded SNDS-BDITF approach, an ad hoc network is considered, wherein the nodes are observed by their adjoining nodes for complete ‘s’ sessions. The quantity of packets sent and received by a node ‘i’ as observed by its neighbours in ‘s’ sessions are $PF_{(1)}, PF_{(2)}, PF_{(3)}, .., PF_{(S)}$ and $PR_{(1)}, PR_{(2)}, PR_{(3)}, .., PR_{(S)}$ correspondingly. The amount of dropped packets by a node as monitored by their neighbours in session ‘c’ is,

$$DROP_C^{PACKET} = PR_C - PF_C \quad (1)$$

The Mean Packet Drop of a node in a session 'c' as observed by its neighbours is,

$$\mathrm{MDROP}_{C}^{\mathrm{PACKET}} = \sum_{c=1}^{s} \frac{\mathrm{DROP}_{C}^{\mathrm{PACKET}}}{s} \quad (2)$$

3.2 Computation of Variance and Standard Deviation (SD) for determining BDITF

In this step, Standard deviation is utilized for determining the packet forwarding capacity of mobile nodes in the network. This SD is essential as it represents the value to which the packet forwarding rate of each mobile is getting changed from its mean original packet forwarding rate before its selfishness or malicious behavior. When the value of SD is low, then the packet forwarding rate is very clise to the mean value of the oritgnal forwarding rate before its selfishness or malicious behavior. On the other hand, the the packet forwarding rate is highly diverging from the mean value of the oritgnal forwarding rate before its selfishness or malicious behavior. Thus, depending Based on the values of 'PR_C' and '$\mathrm{MDROP}_{C}^{\mathrm{PACKET}}$', the Total Variance experienced by a mobile node in packet propagation is given by,

$$\mathrm{T\_VAR}_{\mathrm{DETECT}} = \sum_{C=1}^{S} \frac{(\mathrm{PR}_C - \mathrm{MDROP}_{C}^{\mathrm{PACKET}})}{S} \quad (3)$$

The BDITF computed based on Equations (3) and (4) is given by,

$$(\mathrm{BDITF})_{\mathrm{DETECT}} = \frac{S}{S-1}\left(1 - \frac{\sum_{C=1}^{S}(\mathrm{DROP}_{C}^{\mathrm{PACKET}} * \mathrm{PR}_C)}{\mathrm{T\_VAR}_{\mathrm{DETECT}}}\right) \quad (4)$$

At this juncture, the mean deviation refers to the statistical measure useful for comptung the mean deviation from the mean value of the observed or monitored determined from a mobile node either through direct and neighborhood interaction.

3.3 Identification and Segregation of Selfishness using Calculated BDITF

Once BDITF is computed for each mobile node, the process of identification and segregation of selfish node behaviour is commenced. The nodes with BDITF < 0.30 (got through simulation) are recognized as malevolent and are not involved in multicasting. The ensuing algorithm shows the steps involved in detecting and removing selfish nodes based on BDITF.

Algorithm

N - Quantity of mobile nodes in a network
GN - Collection of nodes on the routing path
SN - Source Node
DN - Destination Node

Establish routing paths by sending `RREQ' messages to nodes
Prepare nodes for communication by forwarding `RREP' messages
for each node (u) in GN with 't' transmission sessions
  Measure the number of dropped packets, difference between amount of packets obtained and forwarded by a node $\left(\mathrm{DROP}_{C}^{\mathrm{PACKET}} = \mathrm{PR}_C - \mathrm{PF}_C\right)$
  Calculate mean packet drop of a node in each session $\left(\mathrm{MDROP}_{C}^{\mathrm{PACKET}} = \sum\right)_{c=1}^{s} \frac{\mathrm{DROP}_{C}^{\mathrm{PACKET}}}{s}$
  Compute total variance for computing BDITF based on 'PR_C' and '$\mathrm{MDROP}_{C}^{\mathrm{PACKET}}$', $\left(\mathrm{T\_VAR}_{\mathrm{DETECT}} = \sum_{C=1}^{S} \frac{\mathrm{PR}_C - \mathrm{MDROP}_{C}^{\mathrm{PACKET}}}{S}\right)$
  Compute BDITF, $\mathrm{BDITF}_{\mathrm{DETECT}} = \frac{S}{S-1}\left(1 - \frac{\sum_{C=1}^{S}(\mathrm{DROP}_{C}^{\mathrm{PACKET}} * \mathrm{PR}_C)}{\mathrm{T\_VAR}_{\mathrm{DETECT}}}\right)$
  if (BDITF (u) < 0.30) then
    Declare node 'u' to be selfish
    Invoke Selfish_Node_Mitigation (u)
  else
    Declare node 'u' as reliable
  End /*if*/
End /*for*/
End

In the proposed SNDS-BDITF, the threshold of BDITF is considered to be 0.30 depending on the series of the simulation, as extreme amount of selfish node misbehaviour in the ad hoc network is detected at this point.

4. Simulation Experiments and Results

The performance of the proposed SNDS-BDITF is analysed by carrying out simulation using ns-2.31. A network topology of 100x100 square meters is taken. The simulation time is 100 seconds with Constant Bit Rate (CBR) traffic patterns of data. 100 mobile nodes are distributed randomly with a packet of size 512 bytes. The complete simulation was run for 30 times and the mean of the results is considered for plotting the graphs used for highlighting the performance of the proposed mechanism.

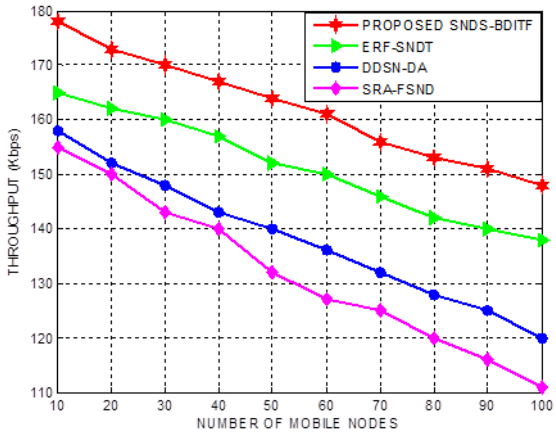

Figure 1. Throughput of SNDS-BDITF based on Number of Mobile Nodes

Primarily, the performance of the propounded SNDS-BDITF is investigated based on throughput, control overhead, total overhead and packet latency for increasing quantity of mobile nodes. Figures 1 and 2 exemplar the throughput and control overhead of the propounded SNDS-BDITF explored for increasing quantity of nodes respectively. The proposed SNDS-BDITF is inferred to offer increased throughput of 11%, 14% and 18% better than the ERF-SNDT, DDSN-DA and SRA-FSND approaches. Likewise, the control overhead of the propounded SNDS-BDITF is explored for varying quantity of nodes. The propounded SNDS-BDITF is established to reduce the control overhead to the maximum extent of 10%, 16% and 19% in contrast to the benchmarked schemes.

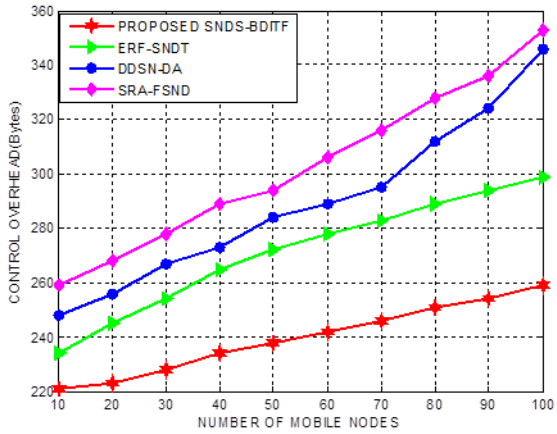

Figure 2. Control Overhead of SNDS-BDITF based on Number of Mobile Nodes

Figures 3 & 4 highlight the total overhead and packet latency of the propounded SNDS-BDITF explored for increasing quantity of nodes respectively. The propounded SNDS-BDITF is determined to reduce total overhead to an extreme degree of 10%, 13% and 18% in contrast to the ERF-SNDT, DDSN-DA and SRA-FSND schemes. In addition, the plots of packet latency of the proposed SNDS-BDITF is investigated for varying quantity of mobile nodes. The proposed SNDS-BDITF is determined to minimize the packet latency to a considerable extent of 14%, 19% and 22 in contrast to the standard approaches. This improvement in throughput and considerable reduction in the control and total overhead, and packet latency for increasing quantity of nodes is mainly owing to the characteristic property of Bates distribution that is significant in discovering the factors that induce selfish behaviour into the network.

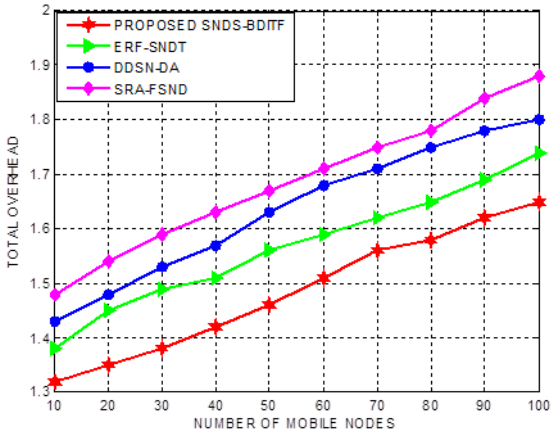

Figure 3. Total Overhead of SNDS-BDITF based on Number of Mobile Nodes

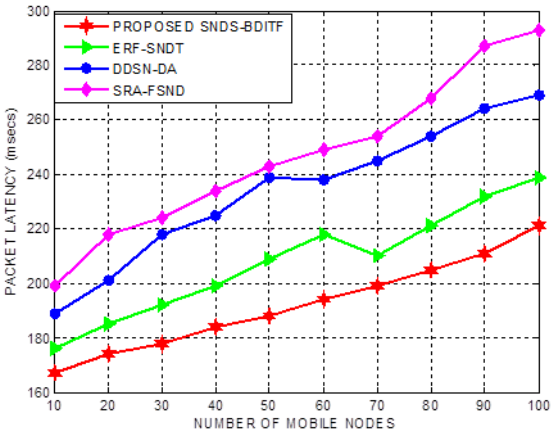

Figure 4. Packet Latency of SNDS-BDITF based on Number of Mobile Nodes

Furthermore, the performance of the propounded SNDS-BDITF is investigated based on throughput, control and total overhead, and packet latency for varying rate of selfish nodes. Figures 5 and 6 highlight the throughput and control overhead of SNDS-BDITF

explored for increasing number of selfish nodes. The propounded SNDS-BDITF is inferred to offer increased throughput at a maximum level of 13%, 17% and 21% in contrast to benchmarked approaches. Likewise, the control overhead of SNDS-BDITF is observed for increasing quantity of selfish nodes. The propounded SNDS-BDITF is proven to reduce the control overhead to a supreme extent of 12%, 15% and 18% when compared to standard schemes.

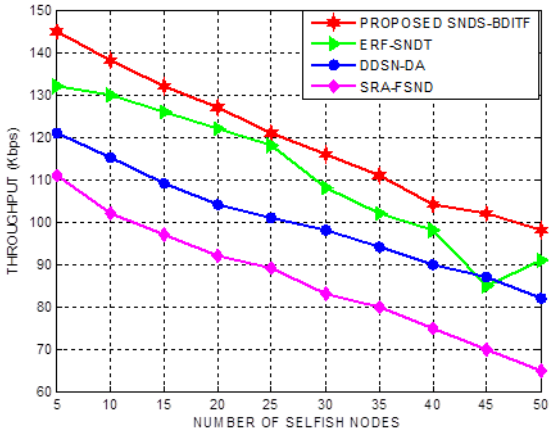

Figure 5. Throughput of SNDS-BDITF based on Number of Selfish Nodes

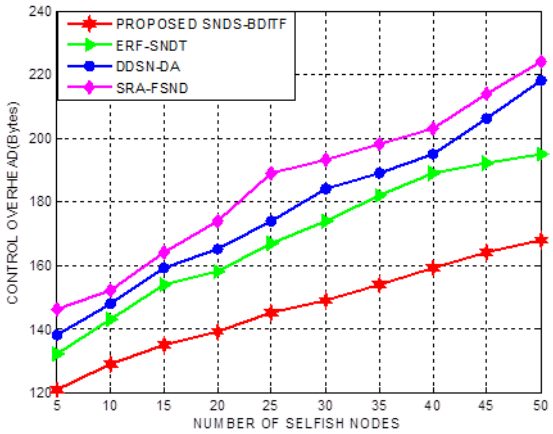

Figure 6. Control Overhead of SNDS-BDITF based on Number of Selfish Nodes

Figures 7 and 8 depict the total overhead and packet latency of the propounded SNDS-BDITF explored for increasing amount of selfish nodes work. The proposed SNDS-BDITF is determined to reduce total overhead to a greater extent of 9%, 12% and 16% when compared to standard schemes. Further, the packet latency of the propounded SNDS-BDITF is investigated for increasing number of selfish nodes. SNDS-BDITF is seen to minimize the packet latency considerably by 12%, 15% and 18% when compared to benchmarked approaches. This improvement in throughput and considerable reduction in the control overhead, total overhead and packet latency for increasing number of selfish nodes is primarily attributable to the inherent potential of Bates distribution which explores the exhaustive factors that induce selfish behaviour in the network.

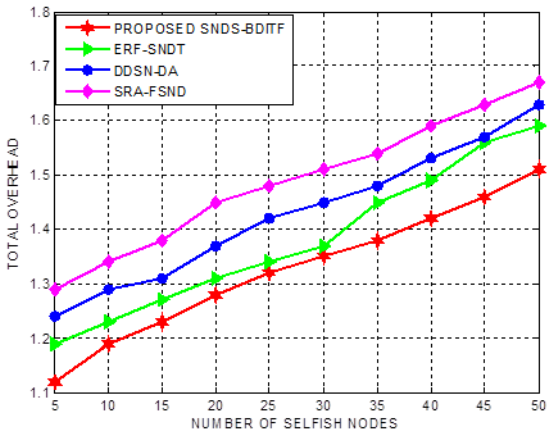

Figure 7. Total Overhead of SNDS-BDITF based on Number of Selfish Nodes

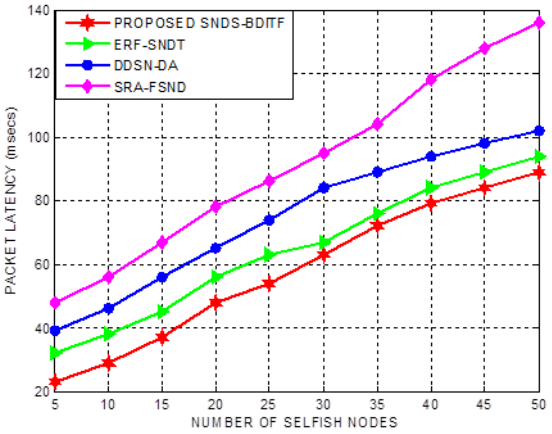

Figure 8. Packet Latency of SNDS-BDITF based on Number of Selfish Nodes

Finally, the detection rate of the propounded SNDS-BDITF is explored in terms of the percentage rise in identification rate for increasing quantity of mobile and selfish nodes (Figures 9 & 10). The percentage increase in the detection rate of the proposed SNDS-BDITF for increasing quantity of mobile nodes is proved to be 8%, 10% and 13% predominant when compared to standard approaches. Likewise, the percentage increase in the detection rate of the proposed SNDS-BDITF for increasing number of selfish nodes is also confirmed to be 8%, 10% and 12% better when compared to benchmarked methods.

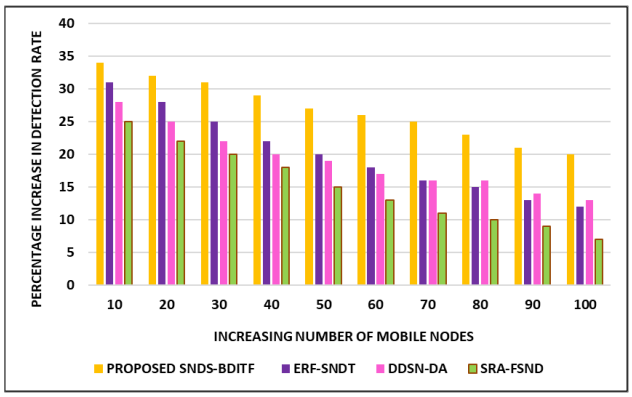

Figure 9. Percentage Increase in Detection Rate of SNDS-BDITF based on Number of Mobile Nodes

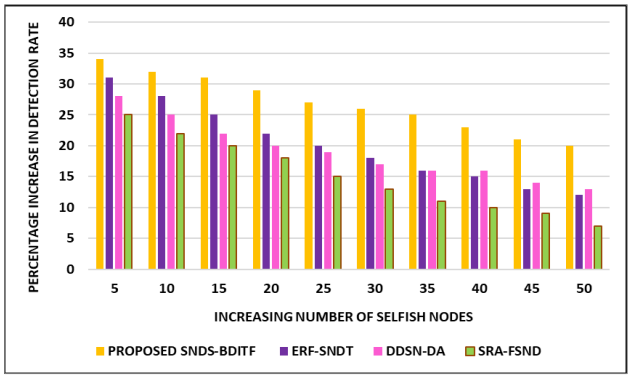

Figure 10. Percentage Increase in Detection Rate of SNDS-BDITF based on Number of Selfish Nodes

The analysis over the results of the proposed wcheme and the benchmarked schemes confirmed the following highlights such as, i) the proposed explored maximized number of influential factors during the process of trust estimation, ii) it considered three contexts such as past trust value of nodes, present behavior of nodes, and possible forecast of nodes' trust during trust evaluation, iii) It adopted a reactive approach which ideally isolated the malicious and selfish nodes from routing path rather than introducing route break in the network, iv) it is proposed as a multi-attribute decision making process which explores maximized number of factors during detection process.

In addition, the proposed SNDS-BDITF scheme and benchmarked schemes are explored based on throughput. Latency and routing overhead with selfish detection threshold value equal to 0.3, lesser than 0.3, and greater than 0.3 with different number of mobile nodes. The results from Figure 11 clearly proved that the proposed SNDS-BDITF scheme confirmed its excellent performance in throughput at 0.3, while the throughput at the values less than 0.3, and greater than 0.3 is comparatively less par than the baseline schemes.

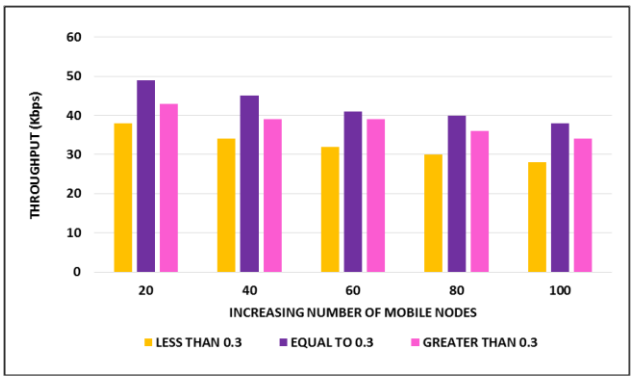

Figure 11. Throughput achieved by the proposed SNDS-BDITF with different selfish node detection values

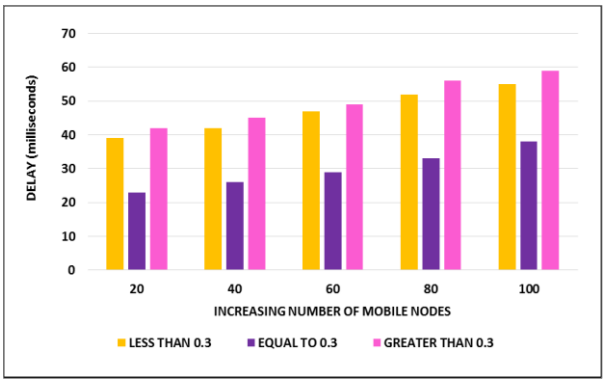

Figure 12. Throughput achieved by the proposed SNDS-BDITF with different selfish node detection values

In addition, Figure 12 depicts the delay incurred by the SNDS-BDITF scheme and the benchmarked approaches with selfish detection threshold value equal to 0.3, lesser than 0.3, and greater than 0.3 with different number of mobile nodes. The results confirmed that the proposed SNDS-BDITF scheme exhibited better performance in terms of minimized delay at the threshold detection value of 0.3, while the delay at the values less than 0.3, and greater than 0.3 is comparatively higher compared to the baseline schemes

5. Conclusion

Selfish Node Detection Scheme based on Bates Distribution Inspired Trust Factor (SNDS-BDITF) is presented as a reliable attempt for significant detection of selfish behaviour by exploring different levels of influential factors that contribute towards effective selfishness detection. The propounded SNDS-BDITF method is estimated to be superior in the effective detection of selfish nodes through multi-dimensional investigations of each monitored node and their attribute towards forwarding potential of other collaborating

mobile nodes. The simulation experiments and results of the proposed SNDS-BDITF approach is found to be outstanding in reducing the control overhead, total overhead and packet latency on average by 21%, 17% and 19% when compared to the other selfish node detection schemes taken for analysis. The detection rate of the propounded SNDS-BDITF approach is also confirmed to be improved by 13% in contrast to the selfish node detection schemes. In the future, it is intended to frame a significant selfish node identification scheme using Gwet Kappa reliability factor for analysing the process of detection.

References

[1] Wu LW, Yu RF. A threshold-based method for selfish nodes detection in MANET. In: Institute of Electrical and Electronics Engineers (IEEE). Proceedings of the International Computer Symposium (ICS2010); 16-18 Dec; Tainan: IEEE; 2010. p. 875-882.

[2] Crepeau C, Davis CR, Maheswaran M. A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes. In: IEEE Computer Society. Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07); 21-23 May; Niagara Falls, Ont., Canada: IEEE; 2007. Vol. 2, p. 19-26.

[3] Lakshmi S, Radha S. Selfish aware queue scheduler for packet scheduling in MANET. In: Institute of Electrical and Electronics Engineers (IEEE). Proceedings of the International Conference on Recent Trends in Information Technology (ICRTIT '12); 19-21April; Chennai, Tamil Nadu, India: IEEE. 2012. p. 343-348.

[4] Kurkure AM, Chaudhari B. Analysing credit-based ARAN to detect selfish nodes in MANET. In: Proceedings of the International Conference on Advances in Engineering & Technology Research (ICAETR-2014); 1-2 August; Unnao, Kanpur, India: IEEE; 2014. p. 1-5.

[5] Sengathir J, Manoharan R. Co-operation enforcing reputation-based detection techniques and frameworks for handling selfish node behaviour in MANETs: A review. Wireless Personal Communications. 2017; 97(3): 3427-3447.

[6] Gupta AK, Mandal JK, Bhattacharya. Mitigating selfish, blackhole and wormhole attacks in DTN in a secure, cooperative way. IJICS. 2017; 9(1/2):130-155.

[7] Valarmathi ML, Meenakowshalya A, Bharathi A. Robust Sybil attack detection mechanism for Social Networks-a survey. In: Proceedings of the 3rd International Conference on Advanced Computing and Communication Systems (ICACCS); 22-23 Jan; Coimbatore: IEEE. 2016. Vol. 1, p. 1-5.

[8] Konorski J. An idea bag strategy to discourage selfish behavior under random token MAC protocols for wireless LANs. In: In: Chaudhuri S., Das S.R., Paul H.S., Tirthapura S. (eds). Distributed Computing and Networking. Proceedings of the International Conference on Distributed Computing and Networking; 27-30 December; Guwahati, India: Springer, Berlin, Heidelberg. Lecture Notes in Computer Science; 2006. p. 582-593.

[9] Ramya N, Rathi S. Detection of selfish Nodes in MANET-a survey. In: Proceedings of the 3rd International Conference on Advanced Computing and Communication Systems (ICACCS); 22-23 Jan; Coimbatore: IEEE. 2016. Vol. 1, p. 1-5.

[10] Gupta AK, Bhattacharya I, Banerjee PS, Mandal JK. A co-operative approach to thwart selfish and black-hole attacks in DTN for post disaster scenario. In: Proceedings of the 4th International Conference of Emerging Applications of Information Technology; 19-21 December; Indian Statistical Institute, Kolkata. IEEE Computer Society1730 Massachusetts Ave., NW Washington, DC, United States: IEEE. 2014. p. 113-118.

[11] Sengathir J, Manoharan R. A futuristic trust coefficient-based semi-Markov prediction model for mitigating selfish nodes in MANETs. EURASIP Journal on Wireless Communications and Networking. 2015; 2015(1): 158.

[12] Gopal DG, Saravanan R. Selfish node detection based on evidence by trust authority and selfish replica allocation in DANET. International Journal of Information and Communication Technology. 2016; 9(4): 473-491.

[13] Manoharan R, Sengathir J. Erlang coefficient based conditional probabilistic model for reliable data dissemination in MANETs. Journal of King Saud University-Computer and Information Sciences. 2016; 28(3): 289-302.

[14] Wang W, Huang K, Zou Y. Cooperation incentive mechanism for selfish users based on trust degree. In: Zdravković M, Trajanović M, Konjović Z. Proceedings of the 6th International Conference on Information Science and Technology (ICIST); Society for Information Systems and Computer Networks; Belgrade, Serbia: IEEE. 2016. p. 204-209.

[15] Kariya SL, Panchal BB. Selfish nodes detection in MANETs: acknowledgement based approach. Int. J. Sci. Res. 2012; 2(5): 216-217.

[16] Sengathir J, Manoharan R. Security algorithms for mitigating selfish and shared root node attacks in MANETs. International Journal of Computer Network and Information Security. 2013; 5(10): 1.

[17] Sivashankari S, Raseen MM. A framework of location privacy and minimum average communication under the global eavesdropper. In: Proceedings of the International Conference on Current Trends in Engineering and Technology (ICCTET); 8 December; Ernakulam, India: IEEE. 2013. p. 392-395.

[18] Muthumalathi N, Raseen MM. Fully selfish node detection, deletion and secure replica allocation over MANET. In: Proceedings of the International Conference on Current Trends in Engineering and Technology (ICCTET); 8 December; Ernakulam, India: IEEE. 2013. p. 413-415.

[19] Tarannum R, Pandey Y. Detection and deletion of selfish MANET nodes-a distributed approach. In: Proceedings of the 1st International Conference on Recent Advances in Information Technology (RAIT); 15-16 March; Dhanbad, India: IEEE. 2012. p. 152-156.

[20] Sengathir J, Manoharan R. Exponential reliability factor based mitigation mechanism for selfish nodes in MANETs. Journal of Engineering Research. 2016; 1(4): 1-22.

[21] Yamini, K. A., Stephy, J., Suthendran, K., & Ravi, V. (2022). Improving routing disruption attack detection in MANETs using efficient trust establishment. Transactions on Emerging Telecommunications Technologies, 33(5).

[22] Fayaz, M., Mehmood, G., Khan, A., Abbas, S., Fayaz, M., & Gwak, J. (2022). Counteracting selfish nodes using reputation based system in mobile ad hoc networks. Electronics, 11(2), 185.

[23] Chiejina, E., Xiao, H., Christianson, B., Mylonas, A., & Chiejina, C. (2022). A robust Dirichlet reputation and trust evaluation of nodes in mobile ad hoc networks. Sensors, 22(2), 571.

[24] Sharma, R., & Dinkar, S. K. (2022). Selfish node detection by modularized deep NMF Autoencoder based Incentivized reputation scheme. Cybernetics and Systems, 3(4), 1-27.

[25] Rama Abirami, K., & Sumithra, M. G. (2018). Preventing the impact of selfish behavior under MANET using neighbor credit value based AODV routing algorithm. Sādhanā, 43(4), 12-24.