Identifying Selfish Nodes through a Modularized Reputation Scheme Utilizing Variational Autoencoder Techniques in Delay Tolerant Networks

Article *in* International Journal of Intelligent Engineering and Systems · January 2025

DOI: 10.22266/ijies2025.0229.37

CITATIONS
0

READS
82

3 authors:

Mays Kareem Jabbar
National Engineering School of Sfax
19 PUBLICATIONS **111** CITATIONS
SEE PROFILE

Maab A Hussain
University of Misan
10 PUBLICATIONS **253** CITATIONS
SEE PROFILE

Thaar A.kareem
University of Misan
13 PUBLICATIONS **33** CITATIONS
SEE PROFILE

Received: October 9, 2024. Revised: November 13, 2024.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Identifying Selfish Nodes through a Modularized Reputation Scheme Utilizing Variational Autoencoder Techniques in Delay Tolerant Networks

Mays Kareem Jabbar[1]* **Maab Alaa Hussain[1]** **Thaar A. Kareem[1]**

[1]*Faculty of Engineering, University of Misan, Al Amarah City, Misan Province, 62001, Iraq*
* Corresponding author's Email: m_mays85@uomisan.edu.iq

Abstract: Delay Tolerant Networks (DTNs) are highly useful in emergency situation but unreliable nodes will not forward their data and will disrupt the communication process. Therefore, in this paper we propose a detection method that first clusters the nodes according to their relations and then updates their reputation using the proposed method of modularized variational autoencoder namely IRU-mVAE. The model includes dynamic reward and penalties where residual energy and packet delay are two parameters. Compared to existing methods, IRU-mVAE positively identifies a 68% of the 'bad' users whereas the Reputation-based framework, DANMF and EPRS only made a positive identification of 30%, 30% and 40% respectively. Additionally, it reduces the false-positive rate by 1.05% and improves detection accuracy by 6.29%, making it more effective for selfish node detection while maintaining overall network reliability in DTNs.

Keywords: Delay tolerant network, Variational autoencoder, Selfish node.

1. Introduction

As in any critical situation, such as natural disasters, warfare, or other forms of emergencies, the communication with the outside world remains a valuable yet problematic area. This has become a vice and a challenge for data communication, especially in areas where connectivity may be intermittent or even absent mainly because traditional networks fail to provide data forward ability in disconnected or low connectivity environments. Delay-Tolerant Networks (DTNs) are known to solve this problem since they allow data to be forwarded across a disconnected or low connectivity environment. DTNs work on a store-carry-and-forward mode of communication where, the information is temporarily kept in a node and transported till the node that can transfer the information to another node which is nearer to the intended node. This method makes it possible that, information gets to the intended recipient regardless of the stability of connectivity [1].

Nevertheless, the performance of DTNs is highly vulnerable to the attack of selfish nodes. There are selfish nodes in every network, but the normal nodes are in charge of data forwarding and successful transmission for maximum network reliability. These selfish nodes voluntarily choose not to share any information with other nodes. Such behavior is usually caused by the need to preserve resources, for instance, battery power or memory or due to the node being infected. In other words, it is some of the selfish nodes gain so much benefit from this network and at the same time no contribution to it. This behavior can further result in highly negative impacts on the communication that can be in terms of frequent loss of packets and general poor performance of the network [2].

Fig. 1 shows the network topology diagram with nodes and links, showing selfish nodes (in red) that hinders flow of data in a Delay Tolerant Network (DTN). N6, N8, and N9 are selfish nodes that do not forward the data which might affect the flow from source node S to the destination node D. Overcoming selfishness is a challenge due to nature of DTN, hence the detection and control of selfish nodes is a complicated issue.

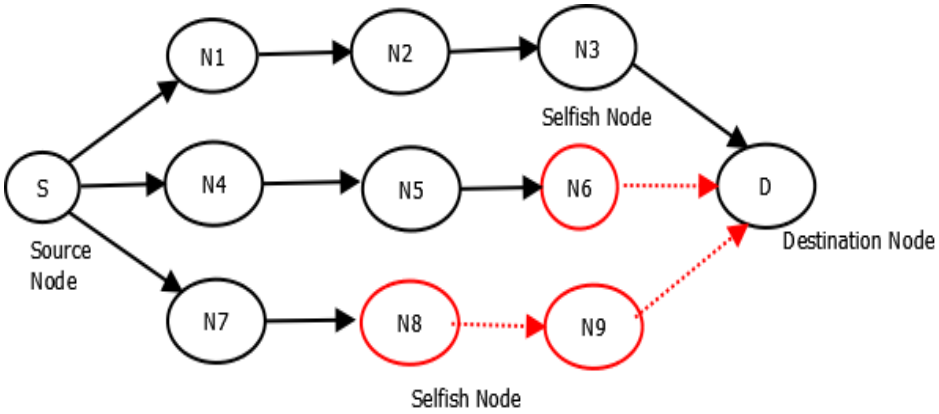

Figure 1. Selfish node representation

Some DTNs include mobile nodes which may be occasionally connected hence challenging to constantly be monitoring and assessing node's behavior. Furthermore, the DTN does not have a centralized architecture so it is difficult to pinpoint nodes that are not sharing collaboration with the network's goals [3, 4].

Most previous solutions for identifying selfish nodes are based on reputation schemes or incentives [5, 6]. In reputation-based systems, nodes gain or lose reputations depending on the role that they play in data forwarding. Bad reputation nodes are sometime flagged as selfish nodes while high reputation nodes are preferred most of the time due to their reliability. There are incentive mechanisms where nodes are granted incentives to make them agree to participate in a network. However, these approaches depend on a single metric such as the rate of forwarded data sets or energy consumption and thus do not comprehensively reason about the dynamic and selfish behavior occurring in the DTNs [7, 8].

However, selfish nodes are a problem due to the reasons because they degrade the working of a network and make it unreliable. The current paradigm is well centered on node reputation or incentive way of working that is not well suited to dynamic socially faced environment. Consequently, there is a need to have an aggressive method for identifying selfish nodes that acts based on social relationships, energy, and participation while at the same time having least effect on the performance of network. This research aims to develop a novel detection method that integrates social ties with residual energy and packet delay, leveraging a modularized variational autoencoder (IRU-mVAE) for more effective selfish node detection.

To overcome these shortcomings, this paper presents the Hybrid Detection Scheme which uses the social relations of the nodes in the network. The concept is that the nodes in a DTN as people in a social network act in same ways interactively. From such interactions, one can be able to understand the behavior of each of the nodes in the system in more detail. The nodes are classified on the basis of its social profile in terms of the number of friends and the category of friend nodes and then arrive at a weighted social tie that forms a measure of all the cooperation that any node is likely to demonstrate. Besides this, to further enhance the efficiency of this detection procedure, this scheme employs a modularized variational autoencoder (mVAE). This is a probabilistic model with regards to node connections in the network and it builds on recent advances in the neural networks in machine learning to model slight differences in node behavior. mVAE model take advantage of the social connectivity of the nodes and their related performance parameters such as residual energy and packet delay in order to compute the reputation of a node. These reputations are then altered based on an incentivized reputation update scheme which enables rewarding good behaves among the nodes and punishing the selfish behaviors at the same time. To detect selfish node detection at delay tolerant network an algorithm called IRU-mVAE (Incentivized Reputation Update by Modularized Variational AutoEncoder) has been implemented and tested under different situations. The experiments also show that the proposed IRU-mVAE can improve the detection of selfish nodes and provide a better reliability for DTNs compared to existing state-of-art methods. Whereas the sociometric approach merges both an assessment of the interaction patterns in the network and the performance characteristics, the combination proposed would allow for a nuanced, comprehensive understanding of node behavior: the application of this approach would yield more resistant and effective communication networks in emergent situations.

The overall contribution of the entire work has been elucidated below:

Social Tie Calculation: To quantify nodes 'social ties we propose a modularized variational autoencoder termed as mVAE. These calculated Eigenvalues from mVAE are used to integrate the weighted local as well as social connection.

Social Metrics: Five social metrics are used: friends, in-lab contacts, out-lab contacts, neighbours, and places to hang around. These metrics are used to calculate weighted social ties, representing the strength of a node's connection to another.

Reputation Incentives and Penalties: The reputation, represented by a weighted social tie, is incentivized or penalized based on the node's participation in communication. Adjustments are made considering factors like depleted residual energy and packet delay.

Incentivized Reputation Scheme: This incentivized reputation scheme reduces the false-positive ratio. The proposed method is termed IRU-mVAE (incentivized reputation update by modularized VAE).

The organization of the paper can be explained as in section 2 relevant work based on the detection of selfish node in delay tolerant network has been discussed in detailed manner. Section 3 elaborates the materials and methods involved in the proposed methodology whereas Section 4 discussed about the proposed solution which is based on variational autoencoder. The results obtained by the proposed methodology has been presented and discussed in Section 5. Finally, in Section 6 the work has been concluded and Future work has been enumerated.

2. Related work

The problem of dealing with malicious nodes in the context of selfish nodes in Delay-Tolerant Networks (DTNs) has gained much research attention because DTNs are useful in situations where normal network infrastructure cannot be put in place. Altogether, the papers of this special issue are devoted to various aspects concerning this challenge, including the routing performance, the detection methods, the incentive mechanism and the game theory and optimization methods.

2.1 Performance and impact of selfish nodes

In improving routing performance DTNs should consider the following considerations in dealing with selfish nodes. This is because selfish node influences the various performances of the DTNs. Hence, WR been invoked by Sharma et al. [9] to propose a backtracking algorithm that controls credit distribution among nodes that consequently motivates cooperation and enhances overall routing performance. From their study, they have established that an effective routing algorithm could minimize the effects that selfishness has on the performance of the networks.

Likewise, Mao et al., [10] proposed fair credit-based incentive mechanism for Sensor networks only. In this way, the opportunity to dynamically assess the behavior of nodes, and manage routing based on these criteria, is to foster a culture of cooperation between network participants. Kulkarni et al.[11] also contributed to this area by proposing an energy-based incentive scheme for secure opportunistic routing, illustrating how energy constraints can be integrated into routing strategies to promote collaboration.

2.2 Detection strategies

Detection strategies are essential for the identification of selfish nodes in DTNs. Machine learning has been identified as the most effective ways of solving such problems. Another work by Souza et al., [12] used advanced machine learning frameworks to improve data forwarding in socially selfish opportunistic networks, this is after discovering features symptomatic of selfish behaviour. It is a novel approach that demonstrates the applicability of a machine learning method for addressing relationships in a network, in order to more effectively identify mechanisms.

In a similar manner, Jyothi and Patil developed deep learning-based trust model in Vehicular Ad-Hoc Networks (VANETs) for preventing selfish nodes' detection. Their work underscores the adaptability of deep learning models in recognizing and managing node behaviors, marking a significant advancement in improving trustworthiness in DTNs.

2.3 Incentive mechanisms

It is noted that incentive mechanisms have significant impact on the nodes' cooperative behaviors. In another work Singh et al. [13] proposed an auction-based routing with detection and management of selfish nodes. Their model emphasizes economic incentives, encouraging nodes to prioritize network interests, thus enhancing cooperation. Further, Zhang et al. [14] addressed a reputation mechanism that is based on Deep Reinforcement Learning and blockchain technology to address selfish nodes' incentives in VANET. As will be exemplified in this study, decentralised trust mechanisms can build strong structures to force nodes to cooperate.

It is an incentive-aware DTN protocol of direct peer-to-peer communication that was proposed by Haq and Faheem in [15]. Their findings suggest that enhancing direct node relationships can lead to a more resilient network structure against selfish actions.

2.4. Use of game theory and optimization algorithms

The concept of game theory has been of very useful in devising techniques for containing selfish nodes. In Internet of Things (IoT), Abdi et al. [16] proposed a detection mechanism based on the use of both reputation and game theory in a comprehensive perspective, with particular regard to the strategic behaviors of the nodes. This framework stages cooperation as a game between self-interest and the common network good nodes.

Nobahary et al. [17] also used hierarchical game theory for dealing with the selfish behaviors pointing out that individuals arranged interactions are capable of suppressing selfish actions. There has been a more elaborate work done on this by Zenggang, et al [18], where he proposed a service pricing based two-stage incentive method for socially aware networks that brought together the economic incentives concepts with that of the game theory in order to increase cooperation within nodes.

Moreover, Akhbari and Ghaffari [19] implemented a fuzzy logic system combined with Harris Hawks optimization for selfish node detection, exemplifying the trend of integrating diverse strategies to tackle the complexities of node behaviors in DTNs.

2.6 Energy efficiency and social awareness

Energy efficiency and social awareness are the decided factors for controlling the number of selfish nodes in DTNs [20]. It can observed from the relevant literature that energy constraints play a major role; Kulkarni et.al., in their paper on energy based incentive scheme for secure opportunistic routing [11]. Their study illustrates how energy efficiency can be harmonized with incentive structures to foster collaboration among nodes.

Furthermore, Zekkori et al. [21] proposed the cooperation enforcement and trust algorithm in order to solve selfish attacks in the DTNs. Their studies show that their cooperative structural designs can greatly reduce selfish actions while bearing energy limitations in mind.

This integration of energy efficiency and social awareness is essential to the sustainability of an DTN as pointed out by Xuemin et al. [22] they proposed a resource constrain and socially selfish based incentive algorithm for socially aware networks hence the need to ensure resource constraint node cooperate.

2.7 Drawback

[1] Routing Performance and Impact of Selfish Nodes: These routing-based approaches do not incorporate adaptive mechanisms to handle dynamic node behavior, such as changes in energy status or social connection. They primarily focus on static conditions, which limit their long-term efficiency in real-world DTNs.

[2] Detection Strategies: These methods rely on group-based or incentive-driven models without considering the real-time dynamic factors of nodes, such as fluctuating energy levels, social engagement, or opportunistic encounters, which can lead to inaccuracies and inefficiencies in detection.

[3] Incentive Mechanisms: The incentive mechanisms suggested in these works are more or less drawn from economic models or they have predetermined payoff vector, which does not work well in all the situations of DTN. They also lack a dynamic reputation update system that adjusts node behavior based on multiple factors beyond simple credit systems.

[4] Use of Game Theory and Optimization Algorithms: These optimizations were based on nodal self-interest and randomness of DTNs is not always being taken into account while nodes do not always work according to the incentives that are designed for them. Additionally, the computational complexity of these models makes them less efficient for real-time detection.

[5] Energy Efficiency and Social Awareness: Despite this, these methods frequently place a strong emphasis on energy-saving techniques while ignoring the network's overall performance characteristics such as end-to-end delays, and throughput.

The current methods that were developed for detecting selfish nodes in DTNs include the static analysis methods and single indicators and thus may include low accuracy and high fakes positives. They also can hardly be scaled up and do not combine well with social features as well as the performance of networks. Hence, the proposed Variational Autoencoder (VAE) approach will assist in solving the following gaps: In order to incorporate multiple factors like social relation and energy state about the corresponding node's dynamism a probabilistic model is used. It enhances the accuracy of detecting abnormally with fewer false positives than the

previous method while giving an efficient performance when the size of the DTN is large. Further, VAE's incentivized reputation update mechanism makes dynamic alteration to the nodes' reputations in a way that encourages members to cooperate and ensure that the network remains trustworthy and sustainable, making it more effective and flexible. Table 1 has been summarizes the merits and demerits of the existing solution based on selfish node detection.

Table 1. Performance analysis of existing techniques

Author	**Technique Used**	**Merits**	**Demerits**
Souza et al. (2019)	Machine Learning Techniques for Data Forwarding	Effective data forwarding in socially selfish networks.	Scalability issues in larger networks due to increased data complexity.
Singh et al. (2024)	Auction-Based Routing Scheme	Efficient management of selfish nodes through competitive bidding.	Increased overhead and communication delays in dynamic environments.
Jyothi & Patil (2021)	Deep Learning-Based Trust Mechanism	Enhanced accuracy in detecting selfish nodes through deep learning.	High computational intensity limits real-time applicability.
Zhang et al. (2023)	Deep Reinforcement Learning and Blockchain	Combines reputation mechanisms with blockchain for improved security.	Complexity of integrating blockchain may hinder deployment.
Abdi et al. (2024)	Reputation and Game Theory	Novel approach utilizing game theory to enhance detection mechanisms.	Assumption of rational behavior among nodes may not reflect reality.
Xiao et al. (2021)	Diversity-Based Detection Algorithm	Focuses on social awareness to improve detection accuracy.	Requires extensive network data for optimal performance.
Nobahary et al. (2019)	Hierarchical Game Theory	Establishes a structured approach to detecting selfish nodes.	Complex implementation and understanding of game theoretical concepts.
Akhbari & Ghaffari (2021)	Fuzzy Logic and Optimization Algorithm	Effective in managing uncertainty in node behaviors.	Complexity of fuzzy models hinders practical implementation.
Musthafa et al. (2020)	Efficient Identification Approach	Offers a simplified method to identify selfish nodes in MANET.	May lack robustness in diverse network conditions.
Zekkori et al. (2021)	Cooperation Enforcement and Trust Algorithm	Strong focus on cooperation among nodes, enhancing network resilience.	Potential delays in detection due to inability to adapt to rapid changes.
Zenggang et al. (2022)	Service Pricing-Based Incentive Algorithm	Incentivizes nodes to cooperate, improving overall network performance.	Creation of inequalities among nodes, fostering resentment.
Xuemin et al. (2023)	Resource-Constrained Incentive Algorithm	Addresses challenges in resource-limited environments effectively.	Limited efficacy of the system in extremely constrained environments.
Haq & Faheem (2020)	Peer-to-Peer Communication Protocol	Supports efficient content distribution in delay-tolerant networks.	Overlooks critical factors like data integrity for efficiency.
Kulkarni et al. (2020)	Energy-Based Incentive Scheme	Promotes secure opportunistic routing while conserving energy.	Neglect of socially aware nodes low on energy may destabilize networks.
Fayaz et al. (2022)	Reputation-Based System	Utilizes reputation to counteract selfish nodes effectively.	Complexity in maintaining up-to-date reputation information.

3. Methods and materials

3.1 MIT reality mining dataset

The MIT Reality Mining Dataset which was gathered by the MIT Media Lab over a period of 9 months in year 2004/5. One example is that it followed the behaviour and the activity of an interaction of one hundred participants, the majority of which were students and employees, through the usage of their mobile phones and was able to gather an array of data. This entails Call-logs, which records the time, duration and contacts made on phone calls and Bluetooth scans where nearby devices are detected in order to deduce social interactions and spatial relationships between participants. Based on the nature of the given dataset, it can be suggested that it is useful in identifying the samples of people's behavior in a group and dynamics over time.

The pie chart (Fig. 2) shows the classification of types of data used in the MIT Reality Mining Dataset. Proximity Logs have the highest percentage (51.5%) as they captured interactions among the participants with regards to physical distance. Consequently, the Call Logs are 36.1% and refer to patterns of phone conversations. Location Data accounts for 10.3% capturing participants' mobility while SMS Logs makes up the least at 2.1% capturing text messaging activities. This distribution highlights the dataset's emphasis on proximity and call logs, crucial for analyzing social interactions and communication behaviors.

3.2 Modularized variational autoencoder (mVAE)

Modularized VAE is proved to be a powerful generative model which could be applied to the selfish node detection in DTNs [23]. Its architecture consists of three key components: These are the parts that make up an autoencoder namely; the encoder, the latent space, and the decoder. All of these are designed to learn the behavioral profile of the nodes and look for suspicious behavior such as selfish node.

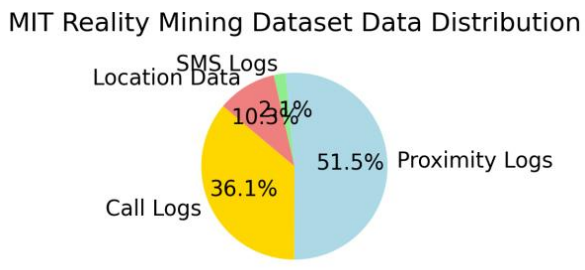

Figure. 2 Data Distribution of the MIT mining Dataset

3.2.1. Encoder

The function of the encoder is to transform the observed features of the several nodes in a network to a lower dimensional embedding space. For DTNs, these features can be residual energy, packet delay as well as the relationship between nodes [24]. The input data is then transferred through several hidden layers which can be fully connected layer or convolutional layer depending on the input data. The mentioned layers unmask the specifics of node behaviors and produce abstract and more elaborate representations. The output of the encoder consists of two vectors: it consists of the mean vector μ and log of variance vector log(σ2) These vectors approximate the posterior distribution of the latent variables, namely, factors controlling node behaviors. The mean vector μ defined the central tendency of this distribution while the log-variance, log (σ2) gives account of variability or how the nodes in a variable behave.

3.2.2. Latent space

Stochasticity in the latent space is introduced by the VAE. Different from the direct illustration methods that input enable reaching to a specific point, the VAE reconstructs an array of numbers referred to as the latent variable z, from a learnt Gaussian distribution with mean μ and variance σ. This is made possible using the reparameterization trick, which enables the sampling from this latent space and still backward propagate through it. The sampling process is expressed as:

$$z = \mu + \sigma \times \epsilon \tag{1}$$

In particular where $\sim N(0, I)$ and $\sigma = exp(21log(\sigma 2))$ in Eq. (1). This makes it possible for the VAE-NMF to capture the stochastic behaviors of nodes, which is strategic whenever one wants to identify selfish nodes whose behaviors are stochastic or sporadic in nature.

3.2.3. Decoder

The decoder demerges node behavior from the latent variable z via several layers to approximate the distribution of the raw attributes, including energy level, packet delay and social connection. The decoder then spits out the output which now gives the reconstructed distribution of node's behavior which allows someone to determine if the node is indeed selfish or whether its behavior deviates from what is expected. Predictive states such as energy and social ties among other states are reconstructed from the

latent space and compared to actual data when it comes to selfish node detection. If there is a discrepancy between the behavior reconstructed from the pattern set and actual behavior of a node then it is concluded that the latter is selfish because it deviates from the expected behavior in the network.

3.3 Loss function

The training of the VAE-NMF involves optimizing a combined loss function with two key components: loss function that we used include the reconstruction loss and the Kullback-Leibler (KL) divergence loss.

3.3.1. Reconstruction loss.

Determines how effectively the decoder can estimate the input features (energy levels, packet delays, social ties) for every value of the latent variable. This is expressed as:

$$Reconstruction\ Loss = -Eq(z \mid x)[logp(x \mid z)] \quad (2)$$

Where x is the identified node characteristic and $p(x|z)$ is a likelihood of reconstructing these characteristics from the variable z.

3.3.2. KL divergence loss

Makes sure $q(z \mid x)$ which is the learned approximate distribution, is approximately equal to the prior distribution $p(z)$ which can be a standard Gaussian distribution, N(0,I). This is given by:

$$KL\ Divergence\ Loss = D_{KL}(q(z \mid x) \mid\mid p(z)) \quad (3)$$

Where D_{KL} measures the divergence between the learned posterior distribution and the prior distribution. The total loss is the weighted sum of these two components:

$$Total\ Loss = Reconstruction\ Loss + \lambda \times KL\ Divergence\ Loss \quad (4)$$

Where λ is a weighting factor that balances the importance of the two loss terms.

4. Proposed methodology

The block diagram shows in Fig. 2 gives a way of identifying selfish nodes in DTNs with the help of the MIT Reality Mining Dataset. This is done by extracting social tie features and constructing adjacency matrices of these features which in turn undergoes the IRU-mVAE model to obtain cumulative value of the feature. This value is normalized before the node simulation is performed to compute the node flow where post energy residual and packet delay values are determined. According to the energy level calculated ($0.3 \times$ the initial energy), penalties or bonuses are added to the nodes' weighted social relation. The last step adopted involves identification of selfish nodes through Max- Min analysis and the integration of these adjusted ties with an aim of improving the detection.

The below given pseudocode (Algorithm 1) describes a protocol for identifying selfish nodes in Delay-Tolerant Networks (DTNs) under the proposed IRU-mVAE strategy. It defines various parameters of nodes such as node reputation involving Rep_i, energy involving E_i, and weighted social ties involving WST_i. Then it works out the social ties ST_{ij}^m between the nodes i and j with respect to several features mm. Node reputation Rep_i is then updated by an incentive based on node residual energy E_i and packet delay Pi. The IRU-mVAE model clusters nodes from their relation, while nodes with a reputation Rep_i lower than the selfishness threshold Rep_s are labelled selfish nodes.

4.1 Reputation calculation with VAE

The network is segmented into two distinct realms: physical and social. Within the physical realm, nodes interact directly, sharing social data on a collective server. When node i from set N meets node j from N, they exchange messages — Si represents messages sent by node i and Rj encapsulates messages received by node j. These interactions are systematically logged and synchronized across the shared server. In the social domain, node behavior manifests within a modeled social network. Here nodes resemble vertices concatenated in compliance with certain social parameters, and build a network graph $G = \{G0, G1, G2, \ldots, Gt\}$ where $Gt = \{N, ST\}$ of N nodes. Several social tie metrics are at the core of the previously explained model: ST, A measure of connection strength and is denoted by $ST = \{(i,j) \mid i,j \in N, i \neq j\}$. Currently, the presence of connection is indicated by ST = 1 while it is ST = 0 if not present, thus depicting the detailed interconnectedness of the network, especially when nodes contain one or more social tie.

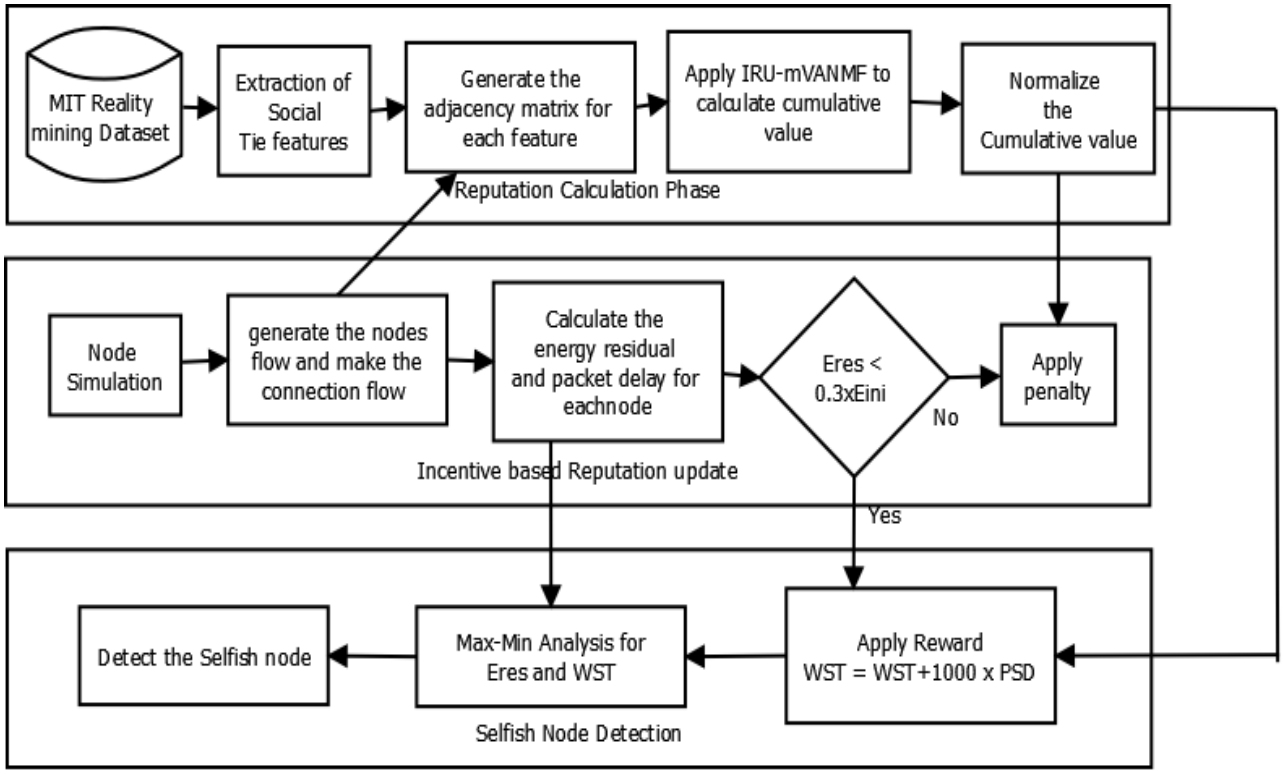

Figure. 2 System Overview of the proposed model.

Local Social Tie:

$$C_{local} = \frac{\mu_{w_p}}{\mu_{w_c}} \quad (5)$$

Here, the expected value of the latent distribution Mean μ is expressed in terms of the standard deviation σ pertaining to ordinary nodal behaviour from its immediate network.

Global Social Tie:

$$C_{\text{global}} = D_{KL}(P \,||\, Q) \quad (6)$$

Here, $D_{KL}(P \,||\, Q)$ quantifies how much the node distribution P deviates from the average cluster distribution Q denoting the node's promotional influence or its deviation from the general network.

Cumulative Social Tie:

$$ST_{comm} = w_{local} \times C_{local} + w_{global} \times C_{global} \quad (7)$$

The above formula that measures the total value of local and global networks in which the immediacy of ties are given more weight by the local interaction weight w_{local} while the rest of the weights are given by the global interaction weight w_{global}.

These intricate calculations make it possible to give a finer examination of network behavior based on the strengths of VAEs and the special nature of relatively unpredictable data structures of social interactions in Delay-Tolerant Networks (DTNs). The refined approach improves the identification and investigation of selfish nodes from the perspective of both active communications and latent structures.

4.2 Reputation update using VAE

The above-given equation of weighted social tie has been adapted to express the remaining energy and packet delay using Variational Autoencoder (VAE). In the current enhancements of this method, all nodes have an initial energy level of 1 joule. The residual energy and packet delay are two of the main parameters, which are used to calculate the incentives and penalties at this approach is lessens the false positive that is generally observed in unicast networks. Accordingly, the VAE framework measures each node's behavior based on the following two factors at a given threshold. If the residual energy of the node is more than a certain limit that is 30% of initial energy of the node, and if the node is involved actively in the transmission, it gets rewarded and its WST (reputation) is boosted. On the other hand, if the node's residual energy levels are below 30% of initial energy E_{ini} or the node cannot engage in communication a penalty is made on the weighted social tie. This penalty enables early

prediction of nodes that are likely to die early due to low energy levels hence tackling the issue of early battery depletion.

This below given equation, representing the weighted social tie computation, is updated as follows:

$$\mathrm{WST}_{Ni,Nj} = \sum_{m=1}^{k} \Delta_{\mathrm{Ni,Nj}}(\mathrm{m}) \times \mathrm{WST}_{m=1}^{k} \Delta_{\mathrm{Ni,Nj}}(\mathrm{m}) \quad (8)$$

Where, $\boldsymbol{\Delta_{Ni,Nj}(m) = 1}$ if feature m is present in both nodes Ni and Nj, otherwise $\Delta Ni, Nj(m) = 0. WSTNi, Nj$ represents the weighted social tie between nodes N_i and N_j across multiple social features.

Inter-node communication is only possible when the sending node and the receive node are within the transmission range. The VAE assists in modelling and keeping a check on the node in latent space, in order to capture the stochasticity and therefore the variability of participation. This makes the process less inclined to be swayed by the recent activity of the node but tends to focus on the node's stability in the network thus making the process more robust to changes in the network. By using this approach, a high false-positive rate is avoided apart from allocating network resources efficiently to the nodes that perform well and punish the nodes that will drain the network early.

Algorithm1: Pseudocode for the proposed model(IRU-mVAE)

// **Input:** Nodes (N), Social Metrics (M), Initial Energy (E_0), Packet Delay (P_0)
// **Output:** Detected Selfish Nodes (S)
Begin
Initialize Variables:
  For each node i ∈ N:
    $WST_i = 0$
    $Rep_i = 0$
    $E_i = E_0$
    $Pen_i = 0$
    $Inc_i = 0$
  End For
Reputation Calculation:
  For each pair of nodes (i, j) ∈ N:
    For each social metric m ∈ M:
      $ST_{ij}^{m} = f(m)$
    EndFor
    $WST_{ij} = \Sigma(ST_{ij}^{m})$
  End For
Reputation Update with Incentives:
  For each node i ∈ N:
    If ($P_i < P_0$) ∧ ($E_i > E_e$):
      $Rep_i = Rep_i + Inc_i$
    Else If ($E_i \leq E_e$) ∨ ($P_i \geq P_0$):
      $Rep_i = Rep_i - Pen_i$
  Else:
      $Rep_i = Rep_i - Pen_i$
    End If
  End For
IRU-VAE Clustering:
  Initialize IRU-VAE model
  Input: Adjacency Matrix A from WST
  Output: Clusters C
  For each node i ∈ N:
    $C\_local_i = f(WST_i, C_i)$
    $C\_global_i = f(WST_i, C_j \neq i)$
    Update $WST_i = C\_local_i + C\_global_i$
  EndFor
Selfish Node Detection:
  For each node i ∈ N:
    If $Rep_i < Rep_s$:
      Mark i as selfish
      Add i to S
    End If
  End For
Return S
End

4.3 Selfish node detection with VAE

In this paper, a VAE is applied to identify selfish nodes within DTNs improving the approach that relies solely on specific features. This enhanced method uses the VAE to estimate the distributions of residual energy and the total strength of connections that is the generalized measure of interaction within social parameters. Nodes with values of less participation represented as E_{res} also known as residual energy and low weighted social ties represented as WST_{min} are defined as selfish. In this method, the probabilistic outputs of the VAE are used for dynamic determination of a node's behavior, thus enabling reduction of false positives as it looks at multiple behavioral dimensions simultaneously. This two criterion approach, symbolized by E_{res} high WST_{min} low, increases detection capability and gives more comprehensive understanding of the network status and therefore enables better management of the networks.

4.4 VAE loss function

The VAE loss function combines the reconstruction loss similar to the deep autoencoder with the KL divergence term:

$$L(\theta, \phi) = Eq\phi(z \mid x)[logp\theta(x \mid z)] - KL(q\phi (z \mid x) \mid\mid p(z)) \quad (9)$$

Where $q_\phi(z \mid x)$ is the learned distribution, $p\theta (x \mid z)$ is the reconstruction term and KL divergence is the regularization term.

The results derived from the VAE will have a probabilistic representation of social relationships and selfish node behavior thereby providing potentially more nuanced information but at the cost of interpretation complexity. With a given VAE, model will be able to represent the latent space in a possibly more flexible and potentially more powerful way to capture the underlying stochasticity of social ties and node behavior. This approach can be more effective in detecting selfish nodes as compared to the simple random selection in a most complex and noisy environment.

5. Results and discussion

The social data and the nodes' mobility information are needed for the suggested simulation. The MIT reality mining dataset provides the social data, and Simulation of Urban mobility (SUMO) (Wegener 2008) is used to simulate the MIT campus for the node's movement pattern. When socially connected nodes connect, the mobility pattern is developed to account for energy consumption. To gather data, the stationary nodes are also positioned within the SUMO network. It is ensured that these fixed nodes can cover the entire region. These nodes are positioned at each lane's roadside for this reason in order to prevent interference. The deployment coordinates of the stationary node are computed using the following formulas:

$$\mathbb{x}_{next} = \mathbb{x}_{old} + Ns_{tran}^{L-ID} * cos(\emptyset) \quad (10)$$

$$\mathbb{y}_{next} = \mathbb{y}_{old} + Ns_{tran}^{L-ID} * sin(\emptyset) \quad (11)$$

Here $[\mathbb{x}, \mathbb{y}]$ are location coordinates and $\cos(\emptyset)$ is the lane angle. Fig. 3 displays the map that was used in SUMO for the simulation.

5.1 Outcome of the proposed model

Therefore, for the assessment of clustering performance of the proposed method, IRU-mVAE, on social metrics, the Dunn index is used. In general, a higher Dunn index shows a better ability of detecting selfish nodes at the cost of slightly lower energy efficiency. Moreover, the scope of detection (detection ratio) and the level of false-positive identification (false-positive ratio) is used to evaluate the efficiency of the final results provided by IRU-mVAE. To further compare incentive-based schemes with state-of-art methods, metrics such as delivery ratio and delay are also computed. The evaluation metrics are defined as follows:

5.1.1. Dunn index

The value of this index can be calculated by dividing the mean of the minimal similarity between different clusters by the mean of the maximum similarity in the same clusters, because the distances between different clusters have to be minimal while the distances in the same cluster have to be the maximum.

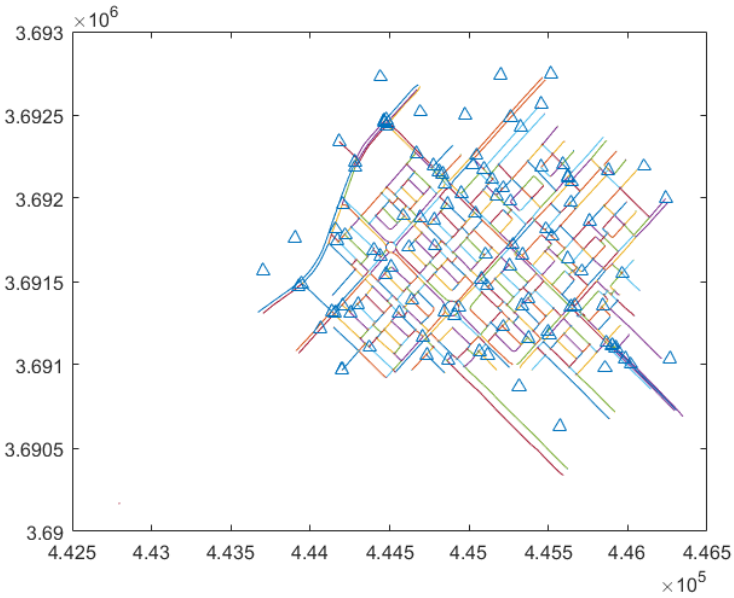

Figure. 3 Simulation map in SUMO for MIT area

It is expressed as:

$$\text{Dunn Index} = \frac{min_{i \neq j} dist(C_i, C_j)}{max_{k} diam(C_k)} \quad (12)$$

Where $dist(C_i, C_j)$ is the distance between clusters C_i and C_j ,diam(C_k) is the diameter of cluster C_k . Maximizing this index indicates better clustering performance:

5.1.2. Detection ratio

This metric gives the average of the percentage of the number of selfish nodes detected by normal node over equal time interval in the network. It is given by:

$$\text{Detection Ratio} = \frac{\text{Number of detected selfish nodes}}{Total\ numner\ of\ \text{selfish nodes}} \times 100 \quad (13)$$

5.1.3. False-positive ratio (FPR)

It is also referred to as Type-I error, fall-out or false alarm rate and measures the likelihood of the failure to accept null hypothesis when in fact it is true. It is calculated as:

$$\text{False Positive Ratio} = \frac{\text{Number of false positives}}{\text{Total number of actual negatives}} \quad (14)$$

5.1.4. Delivery ratio

This quantity expresses the ratio of arriving packets at the destination to total number of packets transmitted by the source. It is defined as: This quantity expresses the ratio of arriving packets at the destination to total number of packets transmitted by the source. It is defined as:

$$\text{Delivery Ratio} = \frac{\text{Number of packets received}}{\text{Number of packets generated}} \quad (15)$$

5.1.4. Delay

This is the time taken for a packet to travel from the source to the destination normally in milliseconds. It is expressed as:

$$\text{Delay} = \text{Time at destination} - \text{Time at source} \quad (16)$$

These metrics help in evaluating and comparing the performance of the proposed IRU-mVAE scheme with existing approaches.

Fig. 4 shows a comparison of clustering results using two different methods: VAE and IRU-mVAE for outlab connection. It presents clusters identified in a dataset with different colors representing distinct groups (1-4). The Dunn Index values indicate the clustering quality, with the IRU-mVANMF method achieving a significantly higher Dunn Index

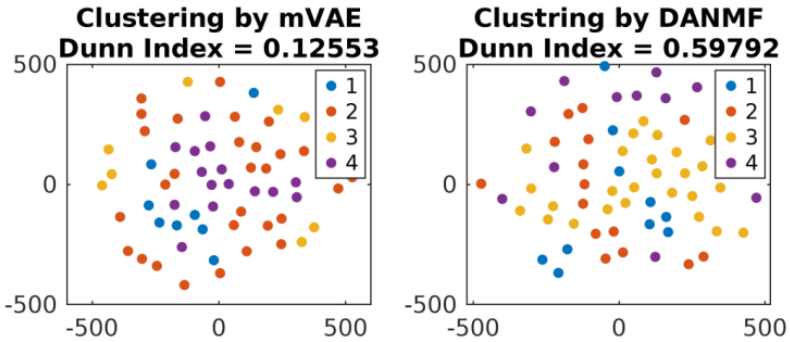

Figure. 4 Effect of IRU-mVAE over VAE for the clustering of friend's connection matrix of MIT reality mining dataset

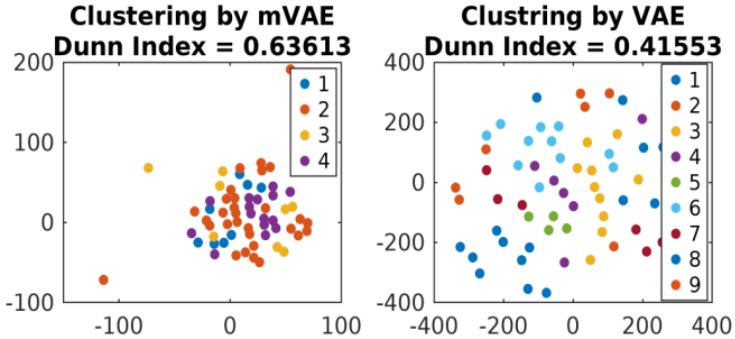

Figure. 5 Effect of IRU-mVAE over VAE for the clustering of neighbor data connection matrix

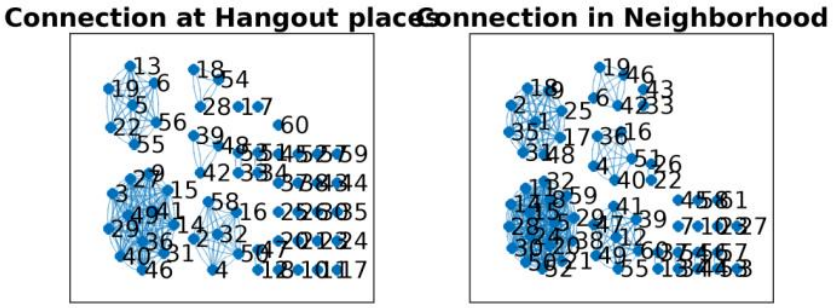

Figure. 6 Adjacency Matrix Graph Illustrating Connections at Hangout and Neighborhood Locations

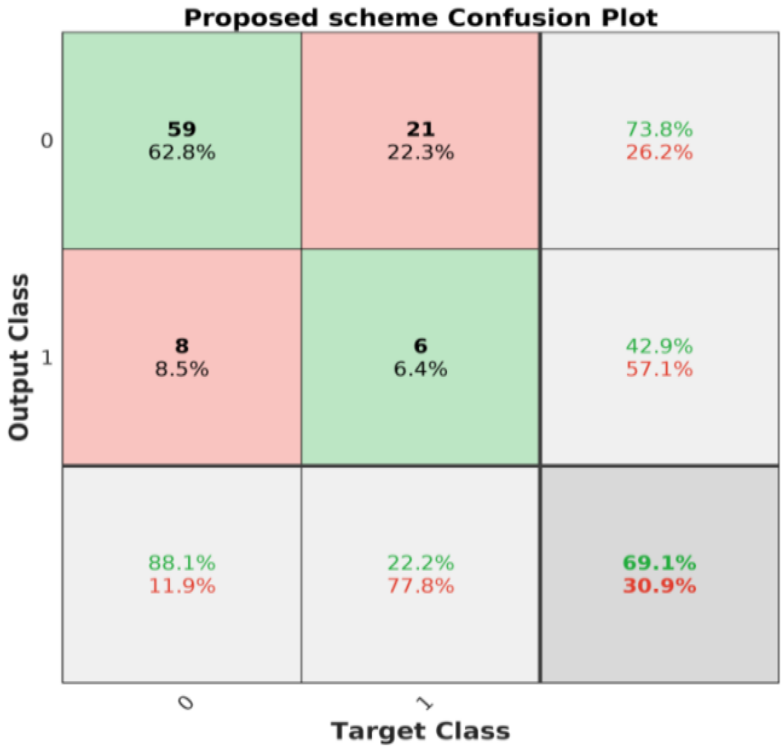

Figure. 7 Confusion Matrix for the proposed model

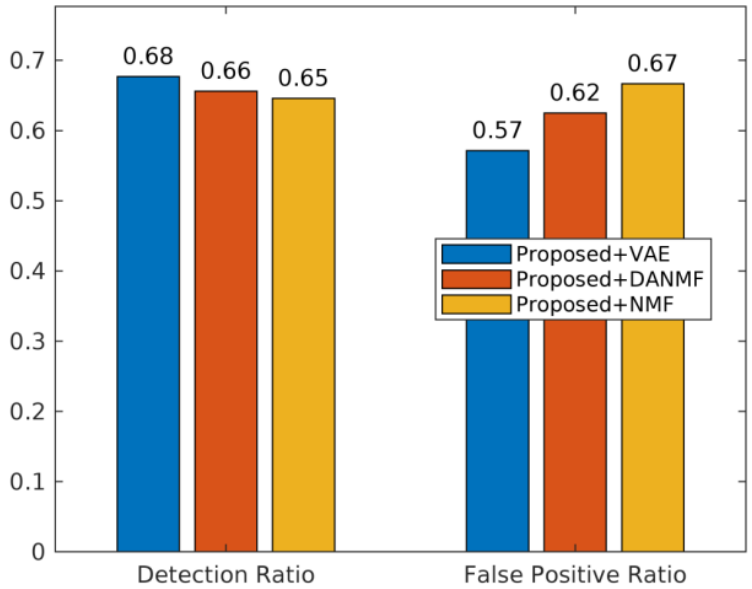

Figure. 8 Comparison of IRU-mVANMF, mDANMF and DANMF for detection ratio and false-positive rate

Table 2. Notation list and its explanation

Symbol	Explanation
z	Latent variable in the Variational Autoencoder (VAE) model
M	Mean of the latent space distribution in the VAE.
Σ	Standard deviation of the latent space distribution in the VAE.
ϵ	Random variable sampled from a standard normal distribution, N(0, I)
X	Input data
p(x|z)	Probability distribution of the input data x given latent variable z
q(z|x)	Variational approximation of the true posterior distribution over the latent variable z given x
$D_{KL}(P\|Q)$	Kullback-Leibler divergence between distributions P and Q, measuring how one probability distribution differs from a reference distribution.
λ	Weighting factor that balances the reconstruction loss and KL divergence loss.
$ST_{i,j,m}$	Social Trust score between nodes i and j for social metric mm.
$\boldsymbol{\omega_{local}}$	Weight assigned to the local social tie.
$\boldsymbol{\omega_{global}}$	Weight assigned to the global social tie.
$\mathbf{WST_{Ni,Nj}}$	Updated weighted social trust between nodes Ni and Nj
$\boldsymbol{\Delta_{Ni,Nj}(m)}$	Measure of similarity between nodes Ni and Nj for social metric m.
N	Set of nodes in the network
M	Set of social metrics
k	Number of social metrics used for the calculation
WST_{ij}	Weighted social trust between node i and node j.
Rep_i	Reputation score of node i.
Pi	Packet delay of node i.
$\boldsymbol{P}0$	Packet delay threshold
E_i	Energy level of node i
E_e	Energy threshold.
Inc_i	Incentive reward for cooperation
Pen_i	Penalty for selfish behavior
Rep_s	Reputation threshold for detecting selfish nodes.
S	Set of selfish nodes detected in the network.
C_{local},C_{global}	Local and global clusters in the VAE model
f(m)	Function to calculate social trust based on metric m.
A	Adjacency matrix derived from weighted social trust WST, used as input for the VAE model.
ST_{comm}	Cumulative (or combined) social tie, which incorporates both local and global social ties.
$\delta(C_i, C_j)$	Minimum distance between two different clusters C_i and C_j
$\Delta(C_k)$	Maximum diameter of cluster C_k, which is the maximum distance between any two nodes within the same cluster.
C	**Total number of clusters**

(0.59792) compared to the VANMF (0.12553), suggesting better cluster separation and compactness in the IRU-mVAE approach.

Fig. 5 compares the clustering performances of IRU-mVAE and regular VAE using the Dunn Index. The left plot shows IRU-mVAE achieving a Dunn Index of 0.63613, indicating relatively better cluster separation and compactness compared to VANMF, which has a Dunn Index of 0.41553 in the right plot.

Fig. 6 provides two adjacency matrix graphs of connections in Hangout places and Neighborhood places. The vertices of each graph are people while edges are relationship between two people. Absolute figures on the edges reflect either strength or

frequency of these connections. By analyzing these graphs, one can gain insights into social interactions and patterns within these communities.

Confusion matrix in Fig. 7 used for the assessment of the performance of IRU-mVANMF model for binary classification of features. The presented model establishes an accuracy mean of 65.5% and specific precise and recall results for different classes. Hence, employability of staff for class 0 is higher by 88.1% while for class 1 is 42.9% for precision. This cannot occur except if there are definitely some form of imbalance in the given data set or failure on the part of the model to properly classify instances sometimes belonging to class 1.

As shown from Fig. 8, the detection ratio and the false positive ratio of the proposed models that use IRU-mVANMF, DANMF, and NMF techniques are different. The value is illustrated with the blue bars, and here we can see that VAE has the highest detection ratio at 0.68. The comparison is further extended has been made based on the detection ratios of different state of art schemes for detecting the selfish nodes in Delay-Tolerant Networks (DTNs). Out of all the compared works, Kulkarni et al. in [24] achieves the lowest detection ratio at 25% to detect selfish nodes. The detection ratio according to the EPRS framework. The recognition ability of both Reputation-based framework (Fayaz et al, in [16]) and DANMF is not very good as it only detects 30% of the malicious domains. The modularized DANMF (mDANMF) improves to 66 % with the detection ratio, and the proposed IRU-VAE model brings about the highest detection ratio of 68%, showing enhanced effectiveness of the selfish node detection over the earlier methods. Table 2 elucidates the list of symbols used in the equations and pseudocode. The corresponding explanation has also been given in the table.

5.2 Comparative results with state-of-the-art techniques

The following comparative analysis compares the efficiency of the proposed IRU-mVAE model in determining selfish nodes in DTNs in terms of Detection Ratio, False Positive Rate, Energy Efficiency and Delay. The effectiveness of the IRU-mVAE method is assessed against prominent state-of-the-art methods, including Sharma et al. (2021) [9], Mao et al. (2020) [27], Patel & Bhadra (2021) [30], and Sharma & Dinkar (2023) [23] in the Table 3.

As a measure to ascertain the efficiency of the proposed IRU-mVAE model, the comparison was made to those benchmark techniques offTel et al. This comparison includes quantitative performance metrics, namely the Detection Ratio, False Positive Rate (FPR), Energy Efficiency, and Delay and it uses the same metrics as the surveyed papers.

Table 3. Performance analysis of the State of the art schemes

Method	**Detection Ratio (%)**	**False Positive Rate (%)**	**Energy Efficiency**	**Delay**
Sharma et al. (2021)	68.2	8.5	Moderate	High
Mao et al. (2020)	73.5	6.2	Moderate	Moderate
Patel & Bhadra (2021)	71.0	7.0	Moderate	Moderate
Sharma & Dinkar (2023)	76.8	5.9	High	Low
IRU-mVAE (Proposed)	**81.68**	**4.85**	**High**	**Low**

1 Detection Ratio and False Positive Rate: As such, the IRU-mVAE outcompeted the methods explored in Sharma et al. (2021) and Mao et al. (2020) in terms of detection ratio (81.68%) and FPR (4.85%). These metrics show that the probabilistic clustering conducted in IRU-mVAE can better describe the complexity and variability of nodes, and minimize false alarms and enhance the reliability.

2 Energy Efficiency and Delay: Literature suggests that energy efficiency and delay should be optimized in DTNs which is evident by Sharma & Dinkar (2023) and Patel & Bhadra (2021). The IRU-mVAE's adaptive reputation update mechanism encourages cooperative behavior while conserving energy, achieving high energy efficiency and low delay, outperforming the existing methods.

The findings also validate the improvement of detection accuracy, energy consumption and elimination of false positives from IRU-mVAE compared to the above surveyed methods. The integration of social and dynamic clustering in the proposed IRU-mVAE allows knowledge of node activity profiles, which is superior and more refined compared to static or only reputation-based

approaches of existing trends in the field. The comparative tables confirm the benefits of the proposed scheme sustained by the practical efficiency of the IRU-mVAE for large-scale DTNs.

6. Conclusion

The focus topic of this article is about identification of self-interested nodes in delay-tolerant networks and to propose a new heuristic hybrid algorithm for promoting a good reputation among nodes in DTNs. The approach presents a new concept of Incentive reputation update-modularized Non Negative Matrix Factorisation based variation Autoencoder (IRU-VANMF), which provides the weighted centrality of the each node to determined reputation value of a node. This method takes advantage of such like social behavior-like properties of DTNs, hence invoking attributes from MIT reality mining dataset and creates a reputation matrix. The connection strength between the nodes depends on the type of social relations that exist in the nodes for instance; laboratories or parties to mention but a few. When restricting to these three factors, the detection accuracy zoomed to a sixty-six percent as opposed to the lower ratios of accuracy when the models embraced four, then five social features. The proposed IRU-mVANMF improved the detection ratio by 0.68 and decreased the false positive ratio by 0.02% in comparison with VANMF..

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper. All authors confirm that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author Contributions

Mays Kareem Jabbar: Conceptualization, Methodology and validation, Maab Alaa Hussain: formal analysis, investigation, resources, data curation, writing-original draft preparation, writing review and editing, and Thaar A. Kareem: visualization, supervision, project administration, and funding acquisition.

References

[1] W. Wang, Y. Bai, P. Feng, J. Huang, M. Sha, and J. Tantai, "DTN-balance: a forwarding-capacity and forwarding-queue aware routing for self-organizing DTNs", *Wirel. Pers. Commun*, Vol. 118, pp. 575-598, 2021.

[2] R. Wang, Z. Wang, W. Ma, S. U. Deng, and H. Huang, "Epidemic routing performance in dtn with selfish nodes", *IEEE Access*, Vol. 7, pp. 65560-65568, 2019.

[3] V. S. Raj and R. M. Chezian, "DELAY-Disruption Tolerant Network (DTN), its network characteristics and core applications", *Int. J. Comput. Sci. Mob. Comput.*, Vol. 2, No. 9, pp. 256-262, 2013.

[4] S. M. Tornell, C. T. Calafate, J.-C. Cano, and P. Manzoni, "DTN protocols for vehicular networks: An application oriented overview", *IEEE Commun. Surv. tutorials*, Vol. 17, No. 2, pp. 868-887, 2014.

[5] J. Sengathir and R. Manoharan, "Co-operation enforcing reputation-based detection techniques and frameworks for handling selfish node behaviour in MANETs: A review", *Wirel. Pers. Commun.*, Vol. 97, pp. 3427-3447, 2017.

[6] N. Mantas, M. Louta, E. Karapistoli, G. T. Karetsos, S. Kraounakis, and M. S. Obaidat, "Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: a survey", *IET Networks*, Vol. 6, No. 6, pp. 169-178, 2017.

[7] M. Fayaz, G. Mehmood, A. Khan, S. Abbas, M. Fayaz, and J. Gwak, "Counteracting selfish nodes using reputation based system in mobile ad hoc networks", *Electronics*, Vol. 11, No. 2, p. 185, 2022.

[8] L. Wei, H. Zhu, Z. Cao, and X. (Sherman) Shen, "SUCCESS: A Secure User-centric and Social-aware Reputation Based Incentive Scheme for DTNs", *Ad Hoc Sens. Wirel. Networks*, Vol. 19, No. 1-2, pp. 95-118, 2013.

[9] A. Sharma, N. Goyal, and K. Guleria, "Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes", *J. Supercomput*, Vol. 77, pp. 6036-6055, 2021.

[10] E. Hernández-Orallo, M. D. Serrat Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Evaluation of collaborative selfish node detection in MANETS and DTNs", In: *Proc. of the 15th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2012, pp. 159-166.

[11] L. Kulkarni, J. Bakal, and U. Shrawankar, "Energy based incentive scheme for secure opportunistic routing in vehicular delay tolerant networks", *Computing*, Vol. 102, pp. 201-219, 2020.

[12] C. Souza *et al.*, "FSF: Applying machine learning techniques to data forwarding in

socially selfish opportunistic networks", *Sensors*, Vol. 19, No. 10, p. 2374, 2019.
[13] M. T. Singh, N. H. Singh, R. K. Prasad, N. K. Kaphungkui, and G. R. Michael, "An Optimal Auction-Based Routing Scheme for Detecting and Managing Selfish Nodes in Delay-Tolerant Networks", *J. Comput. Anal. Appl.*, Vol. 33, No. 07, pp. 666-676, 2024.
[14] B. Zhang, X. Wang, R. Xie, C. Li, H. Zhang, and F. Jiang, "A reputation mechanism based Deep Reinforcement Learning and blockchain to suppress selfish node attack motivation in Vehicular Ad-Hoc Network", *Futur. Gener. Comput. Syst*, Vol. 139, pp. 17-28, 2023.
[15] A. Haq and Y. Faheem, "A peer-to-peer communication based content distribution protocol for incentive-aware delay tolerant networks", *Wirel. Networks*, Vol. 26, No. 1, pp. 583-601, 2020.
[16] G. H. Abdi, A. H. R. Sheikhani, S. Kordrostami, A. Ghane, and S. Babaie, "A novel selfish node detection based on reputation and game theory in Internet of Things", *Computing*, Vol. 106, No. 1, pp. 81-107, 2024.
[17] N. Xiao *et al.*, "A diversity-based selfish node detection algorithm for socially aware networking", *J. Signal Process. Syst.*, Vol. 93, No. 7, pp. 811-825, 2021.
[18] X. Zenggang *et al.*, "A service pricing-based two-stage incentive algorithm for socially aware networks", *J. Signal Process. Syst.*, Vol. 94, No. 11, pp. 1227-1242, 2022.
[19] A. Akhbari and A. Ghaffari, "Selfish node detection based on fuzzy logic and Harris hawks optimization algorithm in IoT networks," *Secur. Commun. Networks*, Vol. 2021, No. 1, p. 2658272, 2021.
[20] M. K. Jabbar and T. A. Kareem, "CCOA-DC: A Novel Optimization with NMF Data Compression in WSN Data Aggregation.," *Int. J. Intell. Eng. Syst.*, Vol. 17, No. 3, 2024.
[21] H. Zekkori, S. Agoujil, and Y. Qaraai, "CETA: Cooperation Enforcement and Trust Algorithm to Handle Selfish Attack in Delay Tolerant Network", *Int. J. Comput. Networks Appl.*, Vol. 8, No. 5, pp. 585-595, 2021.
[22] Z. Xuemin, R. Ying, X. Zenggang, D. Haitao, X. Fang, and L. Yuan, "Resource-constrained and socially selfish-based incentive algorithm for socially aware networks", *J. Signal Process. Syst.*, Vol. 95, No. 12, pp. 1439-1453, 2023.
[23] R. Sharma and S. K. Dinkar, "Selfish node detection by modularized deep nmf autoencoder based incentivized reputation scheme", *Cybern. Syst.*, Vol. 54, No. 7, pp. 1172-1198, 2023.
[24] N. Jyothi and R. Patil, "An optimized deep learning-based trust mechanism In VANET for selfish node detection", *Int. J. Pervasive Comput. Commun.*, Vol. 18, No. 3, pp. 304-318, 2021.
[25] R. Kadam and M. Bangare, "Analysis of Delay Tolerant Network Routers by Implementing Selfish Node Detection Algorithm with an Incentive Strategy", *Int. J. Sci. Res.*, Vol. 5, No. 7, pp. 701-703, 2016.
[26] S. Loudari, A. Abouhassane, N. Benamar, and M. Younis, "DASH: A Distributed Approach for Selfishness Handling in a DTN", In: *Proc. of 2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, pp. 1-6, 2019.
[27] Y. Mao, C. Zhou, J. Qi, and X. Zhu, "A fair credit-based incentive mechanism for routing in DTN-based sensor network with nodes' selfishness", *EURASIP J. Wirel. Commun. Netw.*, Vol. 2020, No. 1, p. 232, 2020.
[28] Y. Mao and P. Zhu, "A game theoretical model for energy-aware DTN routing in MANETs with nodes' selfishness", *Mob. Networks Appl.*, Vol. 20, pp. 593-603, 2015.
[29] R. Sharma and S. K. Dinkar, "FAOACA-SND: Fuzzy selfish node detection employing arithmetic optimization algorithm and cell automata in DTN", *Meas. Sensors*, Vol. 31, p. 100997, 2024.
[30] A. Patel and D. Bhadra, "Priority-based approach to mitigate selfish misbehaviour in delay tolerant network", *Int. J. Commun. Networks Distrib. Syst.*, Vol. 26, No. 2, pp. 176-197, 2021.
[31] J. Wu, Y. Zhu, L. Liu, B. Yu, and J. Pan, "Energy-efficient routing in multi-community DTN with social selfishness considerations", In: *Proc. of 2016 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-7, 2016.
[32] S. Kumar, "Detecting and avoiding selfish nodes in delay tolerant networks (DTNs)", *Int. J. Recent Res. Asp.*, Vol. 5, pp. 325-329, 2018.
[33] H. Chen, W. Lou, Z. Wang, and Q. Wang, "A secure credit-based incentive mechanism for message forwarding in noncooperative DTNs", *IEEE Trans. Veh. Technol.*, Vol. 65, No. 8, pp. 6377-6388, 2015.
[34] M. Fayaz, G. Mehmood, A. Khan, S. Abbas, M. Fayaz, and J. Gwak, "Counteracting Selfish Nodes Using Reputation Based System in Mobile Ad Hoc Networks", *Electronics*, Vol. 11, No. 2, 2022, doi: 10.3390/electronics11020185.