Received: October 2, 2017

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Hybrid Optimization Algorithm for Community and Fraud Detection in Complex Networks for High Immunity Towards Link and Node Failures

Ahuja Mini Singh[1*] **Singh Jatinder**[2]

[1]*Punjab Technical University, Punjab, India*
[2]*Sant Baba Bhag Singh University, Adampur, Jalandhar, India*
* Corresponding author's Email: ahujams0376@gmail.com

Abstract: The complex networks are offering a high resource of heterogeneous data and the proper and efficient analysis discovers the unknown information and relations in networks. Due to the huge number of users and non-familiar fraud detection system in complex networks, a lot of online frauds introduce to affects the networks. In this paper, we concentrate on both community and fraud detection to minimize the link and node failures in the complex networks. A hybrid optimization algorithm proposed for community and fraud detection in the complex networks (HCFD-Net). The first contribution is to detect the community based on fruit fly optimization algorithm with differential evolution (FOADE). The second contribution is that the fraud detection is achieved by contingency table terminology with multi-link metrics. The performance of the HCFD-Net is analyzed on different five real-world networks are Zachary's karate club, Bottlenose dolphins', American college football, American political books, and Amazon online purchase network. The simulation result shows that the proposed HCFD-NET perform very efficient than existing algorithms in terms of normalized mutual information (NMI) and network lifetime.

Keywords: Hybrid optimization, Community detection, Fraud detection, Fruit-fly optimization, Differential evolution, Contingency table.

1. Introduction

In modern studies, one of the major tasks is analyzed and identifying the network communities in the network. The temporal dynamics plays a vital role while integrating provides a better perceptive of network behavior [1-3]. Basically, the community relates the grouping of nodes with a cluster connected with many edges and cluster exists with few edges [4]. There are various domains such as power grids, browser, biological networks, sensor networks and social networks used by the complex networks [5]. Nowadays the attention goes on community structure important properties of complex networks [5, 6].

The determination of network community makes as to learn interaction among modules, prediction in unobserved connections, missing attribute values and inferring missing attribute values [7, 8].

For an example, data propagation is subjected by the group structure in the online social community [9-12]. The migration of humans or birds in the network have the capacity to spread the diseases across the globe [12]. The structure of grid community predicts the electricity supply system in fail propagation. The community structure is found by measuring the electric circuit with efficient layout [12, 13]. First source is the data regarding their attributes and the objects [14, 15]. We can identify the related objects and it belongs to which community using the users, authors, and known properties of proteins, publication history or social network profiles [11-14]. In this user forms the protein interact, friendships, and authors team [15]. The networks are becoming wider and wider since it is the period of information explosion. Thus, we required many effective community detection algorithms for analyzing the networks with millions of vertices [1-15].

Our contributions: A hybrid optimization algorithm proposed for Community and Fraud Detection in complex networks (HCFD-Net). The network is highly increased due to the less entrance cost and a large number of users, therefore,creates the online frauds. The fraud generates the fake accounts in the network and uses the other user information criminally by stealing their personal data. Many hackers are involved in performing malicious activities in the network and hence the social networking communities become less reliable and harmful for the younger generation. Hence our proposed work primarily deals with the fraud detection and analyzes the fault and illegal data acquisition behavior in the real data transaction.

The rest of the paper is organized as follows. The recent works related to our contribution is discussed in Section 2. The problem definition and proposed solution are given in Section 3. The details of proposed hybrid algorithms are described in Section 4 and corresponding simulation results with the performance comparisons are present in Section 5. Finally, the paper concludes in Section 6.

2. Related works

B. Baingana *et al.* [16] have presented an approach for joint tracking communities in time-varying networks for detecting anomalous nodes.

J. Yang *et al.* [17] have introduced communities from edge structure and node attributes (CESNA). This network size has a linear runtime so it is processed with high magnitude while compared with other approaches.

T. Ma *et al.* [18] have presented a loop edges delete (LED) algorithm. It is an efficient detection algorithm used for finding overlapping communities in the network based on structural clustering. This converts the network vertices to weights with the structural similarity.

A. Mahmood *et al.* [19] have proposed a community detection algorithm based on the information that each network community the geodesic space spanned by the different subspace.

J. Whang *et al.* [20] have introduced an algorithm using seed expansion approach for detecting efficient overlapping community. The algorithm is based on community metrics to find and expand the good seed nodes.

F. Zhang *et al.* [21] have proposed detection rules for analyzing social networks to generate the behavior features and changed this behavior features into fuzzy rules.

X. Zhou *et al.* [22] have proposed multi-objective discrete cuckoo search algorithm to discover communities in dynamic networks. An ordered neighbor list method is used to encode the location of the nest for population initialization.

D. Zhou *et al.* [23] have addressed particle swarm optimization (PSO) into community detection problem, and an algorithm based on new label strategy.

3. Problem definition and solution

C. Pizzuti *et al.* [24] have proposed a multi-objective genetic algorithm for community detection in complex networks (GA-Net) and presented an evolutionary multi-objective approach to uncover community structure. Z. Li *et al.* [25] have proposed a multi-agent genetic algorithm for large-scale networks (MAGA-Net) to overcome local optima problem. Other time consumption, the major problems affects the performance than existing algorithms, especially, community detection method utilizing multi-swarm fruit fly optimization algorithm (CDMFOA) [26], that are slow convergence of GA, unguided mutation, no guarantee of finding global maxima, difficult fine tuning of GA parameters, and long training time.

In this paper, we combine fuzzy based fraud detection system to the FOADE community detection algorithm. The main feature of any community is the relationship between their members. Due to these brand new technologies and communication devices available currently, this type of characteristic have been increasing in relevance and becoming more evident in networks.

The multi evolution metrics involved in contingency table terminology to optimize fraud detection such as misclassification rate (R_1), accuracy (R_2), true positive rate (R_3), false positive rate (R_4), specificity (R_5), positive predictive value (R_6), negative predictive value (R_7), false discovery rate (R_8), false discovery ratio(R_9) and alert rate (R_{10}). The fraud detection system, in our approach, is made immune to node and link failures. Hence this proposed hybrid community detection with the fraud detection system is efficient and reliable even under link and node failure strategies. The two different algorithms are used for community and fraud detection in complex networks to make the proposed work as a hybrid (HCFD-Net).

4. Hybrid optimization algorithm for community and fraud detection in complex networks (HCFD-Net)

In this section, we first define community detection metrics. Then we propose community

detection algorithm based on FOADE and describes fraud detection using contingency table terminology.

4.1 Metrics for community detection

Modularity of undirected with the un-weighted network is defined as the ratio of the difference between the actual and expected number of edges within the community. Modularity measures the positive effect of grouping nodes together in terms of taking into account existing edges between nodes. Consider an undirected network $G = (V, E)$ with $|E|$ edges and modularity(Q) is given by,

$$Q = \sum_{c_i \in C} \left[\frac{\left|E_{c_i}^{in}\right|}{|E|} - \left(\frac{2\left|E_{c_i}^{in}\right| + \left|E_{c_i}^{out}\right|}{2|E|} \right)^2 \right] \quad (1)$$

Where C is the set of all the communities, C_i is a specific community in C, $|E_{ci}^{in}|$ is the number of edges between nodes within the community C_i, and $|E_{ci}^{out}|$ is the number of edges from the nodes in the community C_i to nodes outside C_i. The modularity of directed network is given as follows:

$$Q = \sum_{c_i \in C} \left[\frac{\left|E_{c_i}^{in}\right|}{|E|} - \frac{\left(\left|E_{c_i}^{in}\right| + |E_{out,c_i}|\right)\left(\left|E_{c_i}^{in}\right| + |E_{c_i,out_i}|\right)}{|E|} \right] \quad (2)$$

Where $|E_{out,ci}|$ is the number of edges from the nodes outside the community C_i to the nodes in community C_i and $|E_{ci,outi}|$ is the number of edges from the nodes in the community C_i to the nodes outside C_i.

The modularity with a split penalty (Q_{sp}) is compute by subtracting modularity from the split penalty (S_p) which is the fraction of edges that connect nodes of different communities.

$$S_p = \sum_{c_i \in C} \left[\sum_{\substack{c_j \in C \\ c_j \neq c_i}} \frac{|E_{c_i,c_j}|}{2|E|} \right] \quad (3)$$

where $|E_{ci,cj}|$ is the number of edges from community C_i to C_j for unweighted networks or the sum of the weights of the edges for weighted networks.

The S_p of directed network is given by,

$$S_p = \sum_{c_i \in C} \left[\sum_{\substack{c_j \in C \\ c_j \neq c_i}} \frac{|E_{c_i,c_j}|}{|E|} \right] \quad (4)$$

Therefore, the modularity with a split penalty (Q_{sp}) of undirected and directed networks expressed in Eq. (5) and (6) respectively.

$$Q_{SP-UD} = \sum_{c_i \in C} \left[\frac{\left|E_{c_i}^{in}\right|}{|E|} - \left(\frac{2\left|E_{c_i}^{in}\right| + \left|E_{c_i}^{out}\right|}{2|E|} \right)^2 - \sum_{\substack{c_j \in C \\ c_j \neq c_i}} \frac{|E_{c_i,c_j}|}{2|E|} \right] \quad (5)$$

$$Q_{SP-D} = \sum_{c_i \in C} \left[\frac{\left|E_{c_i}^{in}\right|}{|E|} - \frac{\left(\left|E_{c_i}^{in}\right| + |E_{out,c_i}|\right)\left(\left|E_{c_i}^{in}\right| + |E_{c_i,out_i}|\right)}{|E|} - \sum_{\substack{c_j \in C \\ c_j \neq c_i}} \frac{|E_{c_i,c_j}|}{2|E|} \right] \quad (6)$$

To address the resolution limit problem in [25] and it is also quite intuitive to introduce community density into modularity, incorporating both the number of edges and the number of nodes in the communities and also Split Penalty.

The corresponding new metric, modularity density (Q_D) is computed form the Eq. (5) and (6) and Q_D of undirected and directed networks expressed in Eq. (7) and (8) respectively.

$$Q_D = \sum_{c_i \in C} \left[\frac{\left|E_{c_i}^{in}\right|}{|E|} d_{c_i} - \left(\frac{2\left|E_{c_i}^{in}\right| + \left|E_{c_i}^{out}\right|}{2|E|} d_{c_i} \right)^2 - \sum_{\substack{c_j \in C \\ c_j \neq c_i}} \frac{|E_{c_i,c_j}|}{2|E|} d_{c_i,c_j} \right] \quad (7)$$

$$Q_D = \sum_{c_i \in C} \left[\frac{\left|E_{c_i}^{in}\right|}{|E|} d_{c_i} - \frac{\left(\left|E_{c_i}^{in}\right| + |E_{out,c_i}|\right)\left(\left|E_{c_i}^{in}\right| + |E_{c_i,out_i}|\right)}{|E|} d_{c_i} - \sum_{\substack{c_j \in C \\ c_j \neq c_i}} \frac{|E_{c_i,c_j}|}{2|E|} d_{c_i,c_j} \right] \quad (8)$$

Where $|d_{ci}|$ is the internal density of community $|c_i|$ and the $|d_{ci,\,cj}|$ is the pair-wise density between community $|_{ci,}|$ and community c_j. Note that λ is un-weighted for both un-weighted and weighted networks and it is always $0 \leq \lambda \leq 1$. The analysis of the topological structure and reveal more detailed and hierarchical organization of complex network by tuning parameter λ.

4.2 Proposed community detection algorithm using FOADE

4.2.1. Summary of MFOA

Fruit fly algorithm (FOA) [26] is a new type optimization evolutionary algorithm. We introduce an idea of differential evolution after each iteration and propose fruit fly optimization algorithm based

on differential evolution (FOADE). The steps of MFOA are summarized as follows: (1) initialize fruit fly population (2) perform the mutation scheme by adding a random value to each fruit fly individual (3) compute the fitness function value of each individual according to the specific problem being analyzed (4) find out a fruit fly individual with maximal fitness value and save its location of current generation; meanwhile, make other fruit fly individuals fly toward this location and finally (5) perform the mutation scheme to population comprised of best individual in each generation until a predefined number of iteration is achieved.

4.2.2. Differential evolution

Differential evolution (DE) algorithm was proposed in [27] based on a joint group differences stochastic parallel algorithm, which has simple, less controlled parameters, robustness, and other characteristics.

In the selection, differential evolution algorithm uses one-way elimination mechanism greed in merit [34], differential evolution algorithm does not use the gradient information of function, has low demand indifferentiability, even in continuity, the advantages are obvious. The processing step of differential evolution algorithm is given in Fig. 1.

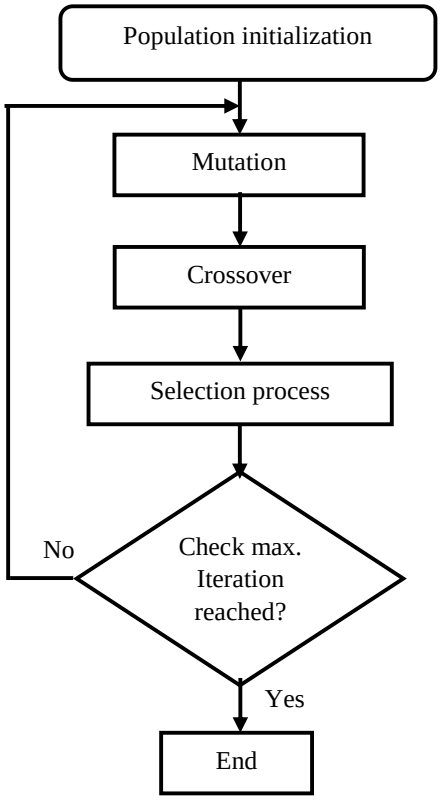

Figure.1 Processing steps of differential evolution

4.2.3. Fruit fly optimization algorithm based on differential evolution

The implementation step of our proposed FOADE is given in Fig. 2.

Population initialization- Determine population size *(P_s)* maximum iterations $I_{max,}$ including both differential evolution scaling factor (*F*), crossover probability (*CR*). Fruit fly populations' location X axis, Y axis. For a network $G = (V, E)$, where *V* is the vertex set with the number of it, *n*; and *E* is the edge set with the number of it, e. An individual can be represented as follows:

$$ind_j = \left\{c_{id_1,\ldots\ldots,}c_{id_i\ldots\ldots,}c_{id_n}\right\} \quad (9)$$

where ind_j represents the j^{th} individual in the population, c_{idi} means that the vertex *i* belongs to the community c_{idi} For instance, if $c_{id11=7}$, this means that the eleventh vertex is in the seventh community now.

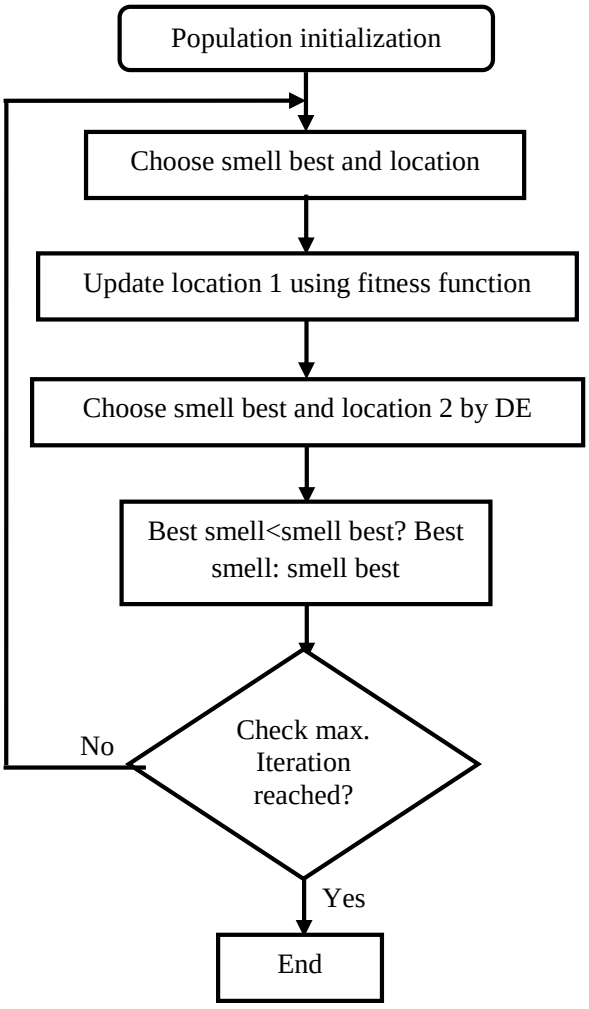

Figure.2 Processing steps of FOADE

Choose smell best and location- The traditional FOA [26] utilized to compute the smellbest. Because the value of best smell may change in different fruit fly population, so the smellbest is used to keep the best smell so as to have a comparison with the maximal smell concentration in the next fruit fly population.

$$smellbest = bestsmell \quad (10)$$
$$X_{axis} = X(bestindex) \quad (11)$$
$$Y_{axis} = Y(bestindex) \quad (12)$$

Update location- The obtained position initiated to compute the new fruit fly group's position. Then again perform the traditional FOA to compute a new fitness function and optimal location of a fruit fly.

Perform differential operation- The differential evolution operation performed in the optimal position in the previous step; the differential operations are a mutation, crossover, and select action. The mutation operation in each iteration, we randomly choose two different individuals based on the best position according to relation Eq. (13) and applied to a vector of the best individual scaled, we obtain the mutated individuals.

$$M_i(t) = X_{axis(t)} + F \times (X_{r_1}(t) - X_{r_2}(t)) \quad (13)$$

Where F is the scaling factor i.e. initialized at first step and $X_{r1,}$ X_{r2} is randomly choose two individual from total populations. Then to crossover the mutated individuals and populations of individuals currently in a discrete crossover manner, generating intermediate individuals to increase the diversity of the population, the process as follows,

$$C_{i,j}(t) = \begin{cases} M_{i,j}(t), r \le CR || j = rand \\ X_{i,j}(t), otherwise \end{cases} \quad (14)$$

Where r=*rand*(0,1) and $CR\epsilon$[0,1]. After crossing the middle of the individual with the current selection greedy individuals, compare their corresponding taste, if the current value of the individual has an excellent taste; choose it, otherwise retained, as follows,

$$X_i(t+1) = \begin{cases} X_i(t), f(X_i(t)) \le f(M_i(t)) \\ M_i(t), otherwise \end{cases} \quad (15)$$

where f(.) is the fitness function.

Table 1. Contingency table terminology

	Frauds	**Not frauds**	**Total**
Frauds	α^+	β^+	$\alpha^+ + \beta^+$
Not frauds	β^-	α^-	$\beta^- + \alpha^-$
Total	$\alpha^+ + \beta^-$	$\beta^+ + \alpha^-$	$\alpha^+ + \beta^+ + \alpha^- + \beta^-$

4.3 Fraud detection using contingency table terminology

Fraud detection models are what are more generally known as binary classifiers. The detection model will assign an example to either the positive or negative (P or N) classes, but it will not do so perfectly. This generates the four possible outcomes in the contingency table. "True" means a correct classification, and "False" means an incorrect classification.

- True Positive (α^+) – A correctly identified fraudulent transaction or victimized customer
- False Positive (β^+) – A transaction or customer incorrectly identified as a fraudulent transaction or victimized customer
- True Negative (α^-) – A correctly identified good transaction or non-victim customer
- False Negative (β^-) – A transaction or customer incorrectly identified as a good transaction or non-victim customer
- These outcomes add up as shown in table 1.

Evaluation metrics for binary classifiers derived from the contingency table include the following, and note that these can be computed on a unit basis. Misclassification rate (R_1),

$$R_1 = \frac{\beta^- + \beta^+}{\alpha^+ + \beta^- + \beta^+ + \alpha^-} \quad (16)$$

Accuracy (R_2),

$$R_2 = 1 - \frac{\beta^- + \beta^+}{\alpha^+ + \beta^- + \beta^+ + \alpha^-} \quad (17)$$

True positive rate (R_3),

$$R_3 = \frac{\alpha^+}{\alpha^+ + \beta^-} \quad (18)$$

False positive rate (R_4)

$$R_4 = \frac{\beta^+}{\beta^+ + \alpha^-} \quad (19)$$

Specificity (R_5)

$$R_5 = \frac{\alpha^+}{\beta^+ + \alpha^-} \quad (20)$$

Positive predictive value (R_6)

$$R_6 = \frac{\alpha^+}{\alpha^+ + \beta^+} \quad (21)$$

Negative predictive value (R_7)

$$R_7 = \frac{\alpha^-}{\alpha^- + \beta^-} \quad (22)$$

False discovery rate (R_8)

$$R_8 = \frac{\beta^+}{\beta^+ + \alpha^+} \quad (23)$$

False discovery ratio (R_9)

$$R_9 = \frac{\beta^+}{\alpha^+} \quad (24)$$

Alert rate (R_{10})

$$R_{10} = \frac{\beta^+ + \alpha^+}{\beta^+ + \alpha^+ + \beta^-} \quad (25)$$

Fraud detection models produce score instead of simply "positive" or "negative" classifications, a threshold value is set below which examples are considered "Negative" and above which they are considered "Positive."

5. Simulation

The Network Simulator (NS-2) is used to simulate the proposed hybrid optimized algorithm for community and fraud detection in complex networks (HCFD-Net). A 1000 meter x 1000 meter environment is used for 200 seconds of simulation time for simulation of the proposed algorithm. The simulated traffic is constant bit rate (CBR). In order to evaluate the performance analysis of the proposed HCFD-Net is compared with the known existing algorithms, GA-Net [24], and MAGA-Net [25] with the detection evolution metrics named as normalized mutual information (NMI) and given as follows,

$$NMI(P_1, P_2) = \frac{-2\sum_{i=1}^{cp1}\sum_{j=1}^{cp2} CM_{i,j}\log\left(\frac{CM_{i,j}N}{CM_{i.}CM_{.j}}\right)}{\sum_{i=1}^{cp1} CM_{i.}\log\left(\frac{CM_{i.}}{N}\right)+\sum_{j=1}^{cp2} CM_{.j}\log\left(\frac{CM_{.j}}{N}\right)} \quad (26)$$

The simulation parameters are given in table 2 and the real world networks given in table 3.

Table 2. Simulation parameters

Node mobility	10 m/s
Area Size	1000 X 1000 m
MAC	IEEE 802.11
Transmission Range	250m
Simulation Time	200 sec
Traffic Source	Constant Bit Rate (CBR)
Packet Size	1024 bytes
Rate	50Kbps

Table 3. Real world networks

Network structure	**Karate**	**Dolphins**	**Football**	**Political book**	**Amazon**
Number of nodes	100-500	100-500	100-500	100-500	100-500

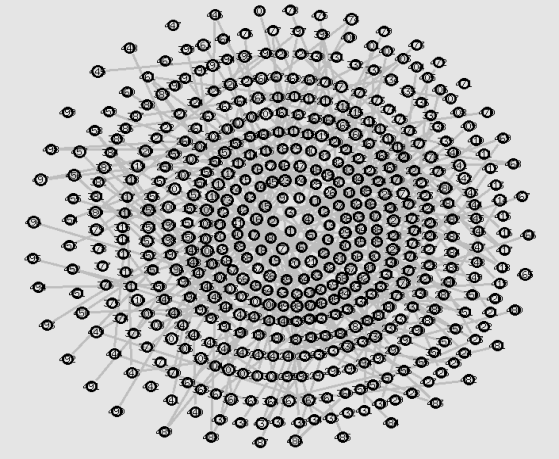

Figure.3 Input network at 0th simulation time

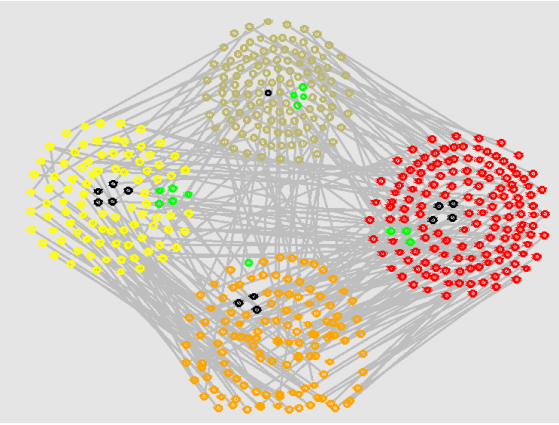

Figure.4 Complete 100% of partition due to λ = 0.90 at the simulation time 200 second

5.1 Simulations on real-world networks

In this subsection, we apply HCFD-Net on five real-world networks: Zachary's karate club network, Bottlenose dolphins' network, American college football network, American political books network, and Amazon online purchase network. Fig. 3, 4 shows the real partitions of karate club network and the detected results of proposed HCFD-Net. The input network of a karate club at the simulation time 0 second and we show the further result actions. Similarly, we perform five different networks.

5.2 Performance comparison

The NMI is used to compute the similarity of our partitions and the real ones. The computed NMI of our proposed HCFD-Net is compared with the existing algorithms, such as GA-Net [24], and MAGA-Net [25]. NMI is used to estimate the similarity between the detected communities and the true ones. We run all three algorithms independently in the Amazon network, and the comparisons of average values of NMI are shown in Fig. 5 to 9, respectively.

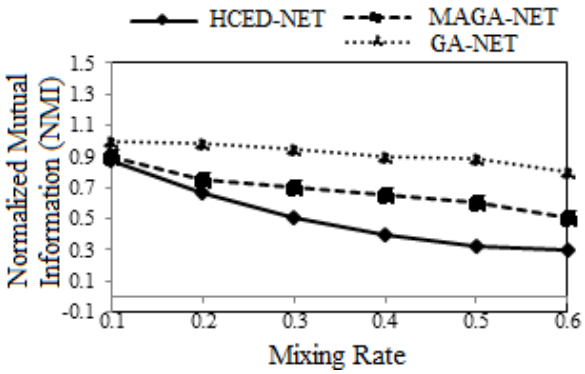

Figure.5 Performance comparison using computed NMI with three algorithms for Amazon network with mixing parameter range of 0.1 to 0.6 and the number of nodes as 100.

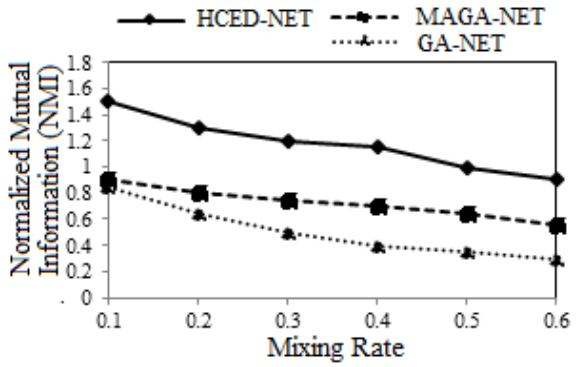

Figure.6 Performance comparison using computed NMI with three algorithms for Amazon network with mixing parameter range of 0.1 to 0.6 and the number of nodes as 200.

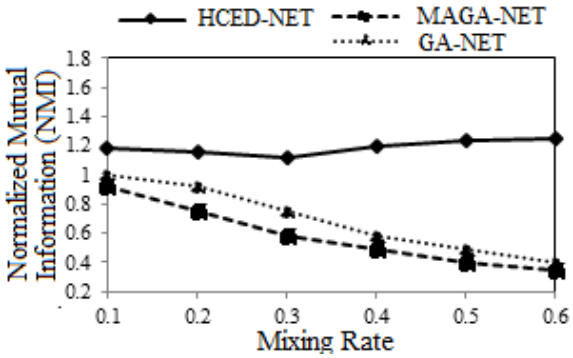

Figure.7 Performance comparison using computed NMI with three algorithms for Amazon network with mixing parameter range of 0.1 to 0.6 and the number of nodes as 300.

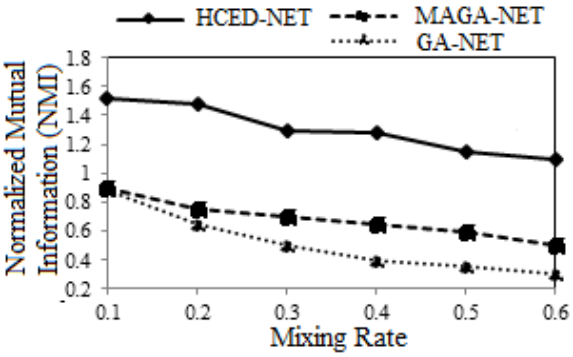

Figure.8 Performance comparison using computed NMI with three algorithms for Amazon network with mixing parameter range of 0.1 to 0.6 and the number of nodes as 400.

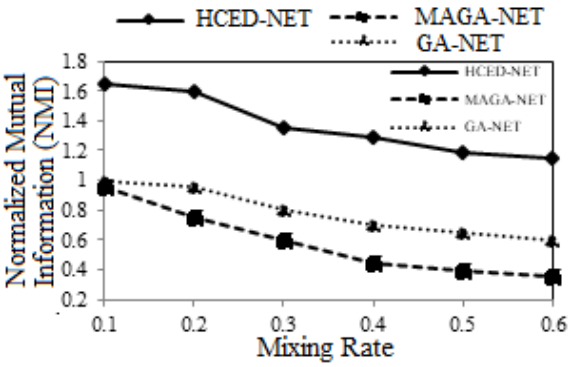

Figure.9 Performance comparison using computed NMI with three algorithms for Amazon network with mixing parameter range of 0.1 to 0.6 and the number of nodes as 500.

The major objective of our proposed HCFD-Net is the link and node failures that are analyzed by the network lifetime. It is computes, how long the nodes are performed in the network without failed. In this scenario, the network lifetime of different real time networks are analyzed by varying the number of nodes form 100 to 500. Fig. 10-14 shows network lifetime comparison of proposed HCFD-Net and

MAGA-Net.

The simulation results show that performance of proposed HCFD-Net can handle large complex network than the MAGA-Net and GA-Net, while HCFD-Net obtains good results with the size from 100 to 500. Changing the value of μ from 0.1 to 0.6 makes it much harder to detect communities, but HCFD-Net overcomes the difficulties and still has a good performance which comprehensively verifies the effectiveness of HCFD-Net.

All the above results show that HCFD-Net has a good performance. In terms of NMI, HCFD-Net can converge to the global optima with a small number of evaluations than MAGA-Net and GA-Net. For all five real networks, the network lifetime of proposed HCFD-Net is very high compare to the other existing algorithms.

6. Conclusion

In this paper, we have proposed the hybrid optimization algorithm for community and fraud detection in complex networks (HCFD-Net). The fruit fly optimization with the differential evolution can used to detect community by mixing parameter. The similarity of detected communities is analyzed by the computed NMI. Then, contingency table terminology with multiple link metrics utilized to detect the fraud in the network, which maximize the node, link failures and maximize network lifetime. The proposed hybrid algorithm applied on five different real world complex networks with 100 to 500 nodes for performance analysis. The simulation results show that the performance of proposed HCFD-Net is very efficient than existing detection algorithms. In future, the HCFD algorithm further enhanced by the DEEP community detection and it is applied for real-time complex network.

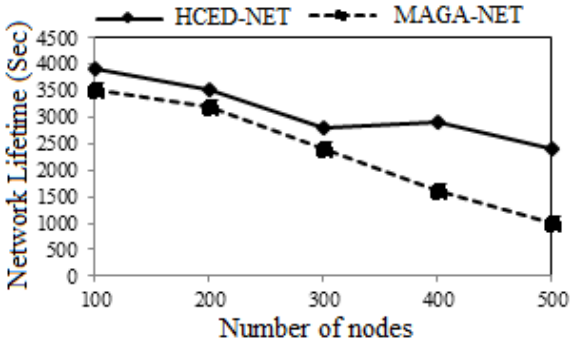

Figure.10 Number of nodes Vs Network lifetime (Sec) comparison of Karate club network

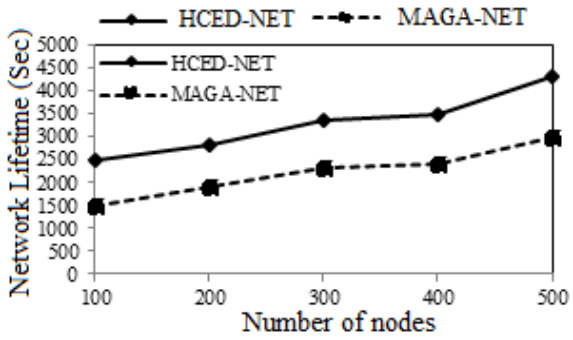

Figure.11 Number of nodes Vs Network lifetime (Sec) comparison of Dolphins network

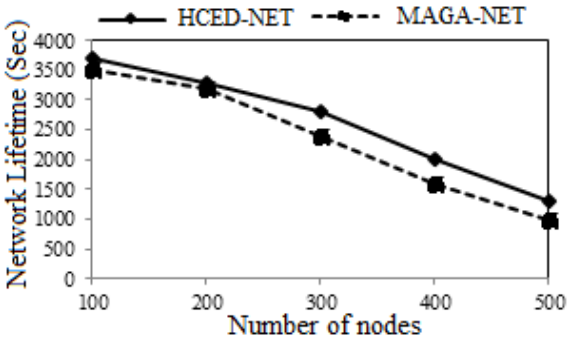

Figure.12 Number of nodes Vs Network lifetime (Sec) comparison of College football network

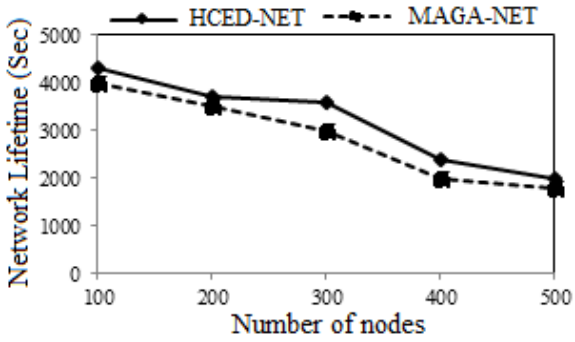

Figure.13 Number of nodes Vs Network lifetime (Sec) comparison of Political book network

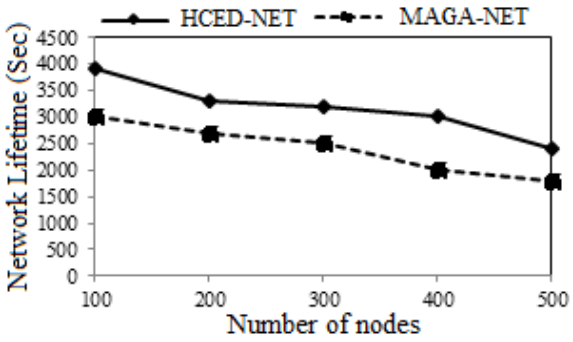

Figure.14 Number of nodes Vs Network lifetime (Sec) comparison of Amazon online purchasing network

References

[1] G. Thakur, A. Dress, R. Tiwari, S. Chen, and M. Thai, "Detection of local community structures

in complex dynamic networks with random walks", *IET Systems Biology*, Vol.3, No.4, pp.266-278, 2009.
[2] I. Morarescu and A. Girard, "Opinion Dynamics with Decaying Confidence: Application to Community Detection in Graphs", *IEEE Transactions on Automatic Control*, Vol.56, No.8, pp.1862-1873, 2011.
[3] Z. Chen, W. Hendrix, and N. Samatova, "Community-based anomaly detection in evolutionary networks", *Journal of Intelligent Information Systems*, Vol.39, No.1, pp.59-85, 2011.
[4] Z. Wu, Y. Lin, S. Gregory, H. Wan, and S. Tian, "Balanced Multi-Label Propagation for Overlapping Community Detection in Social Networks", *Journal of Computer Science and Technology*, Vol.27, No.3, pp.468-479, 2012.
[5] C. Lee and P. Cunningham, "Community detection: effective evaluation on large social networks", *Journal of Complex Networks*, Vol. 2, No.1, pp.19-37, 2013.
[6] Y. Li, G. Liu, and S. Lao, "A genetic algorithm for community detection in complex networks", *Journal of Central South University*, Vol.20, No.5, pp.1269-1276, 2013.
[7] M. Gong, L. Zhang, J. Ma, and L. Jiao, "Community Detection in Dynamic Social Networks Based on Multi objective Immune Algorithm", *Journal of Computer Science and Technology*, Vol.27, No.3, pp.455-467, 2012.
[8] Z. Yang, R. Algesheimer, and C. Tessone, "A Comparative Analysis of Community Detection Algorithms on Artificial Networks", *Scientific Reports*, Vol.6, pp.30750, 2016.
[9] S. Jin, P. Yu, S. Li, and S. Yang, "A Parallel Community Structure Mining Method in Big Social Networks", *Mathematical Problems in Engineering*, pp.1-13, 2015.
[10] C. Yin, S. Zhu, H. Chen, B. Zhang, and B. David, "A Method for Community Detection of Complex Networks Based on Hierarchical Clustering", *International Journal of Distributed Sensor Networks*, Vol.11, No.6, pp.849140, 2015.
[11] Y. Xing, F. Meng, Y. Zhou, M. Zhu, M. Shi, and G. Sun, "A Node Influence Based Label Propagation Algorithm for Community Detection in Networks", *The Scientific World Journal*, pp.1-13, 2014.
[12] S. Ríos and R. Muñoz, "Content Patterns in Topic-Based Overlapping Communities", *The Scientific World Journal*, pp. 1-11, 2014.
[13] W. Li, "A Constrained Power Method for Community Detection in Complex Networks", *Mathematical Problems in Engineering*, Vol. 2014, pp.1-6, 2014.
[14] D. Chen, Y. Dong, X. Huang, H. Chen, and D. Wang, "A Community Finding Method for Weighted Dynamic Online Social Network Based on User Behavior", *International Journal of Distributed Sensor Networks*, Vol.2015, pp. 1-10, 2015.
[15] L. Yang, J. Xin-sheng, L. Caixia, and W. Ding, "Detecting Local Community Structures in Networks Based on Boundary Identification", *Mathematical Problems in Engineering*, Vol. 2014, pp.1-8, 2014.
[16] B. Baingana and G. Giannakis, "Joint Community and Anomaly Tracking in Dynamic Networks", *IEEE Transactions on Signal Processing*, Vol.64, No.8, pp.2013-2025, 2016.
[17] J. Yang, J. McAuley, and J. Leskovec, "Community Detection in Networks with Node Attributes", In: *Proc. of 13th International Conf. On Data Mining, IEEE*, 2013.
[18] T. Ma, Y. Wang, M. Tang, J. Cao, Y. Tian, A. Al-Dhelaan, and M. Al-Rodhaan, "LED: A fast overlapping communities detection algorithm based on structural clustering", *Neurocomputing*, Vol.207, pp.488-500, 2016.
[19] A. Mahmood and M. Small, "Subspace Based Network Community Detection Using Sparse Linear Coding", *IEEE Transactions on Knowledge and Data Engineering*, Vol.28, No.3, pp.801-812, 2016.
[20] J. Whang, D. Gleich, and I. Dhillon, "Overlapping Community Detection Using Neighborhood-Inflated Seed Expansion', *IEEE Transactions on Knowledge and Data Engineering*, Vol.28, No.5, pp.1272-1284, 2016.
[21] F. Zhang, J. Li, F. Li, M. Xu, R. Xu, and X. He, "Community Detection Based on Links and Node Features in Social Networks", *Multi Media Modeling*, pp.418-429, 2015.
[22] X. Zhou, Y. Liu, and B. Li, "A multi-objective discrete cuckoo search algorithm with local search for community detection in complex networks", *Modern Physics Letters B*, Vol.30, No.7, pp.1650080, 2016.
[23] D. Zhou and X. Wang, "A Neighborhood-Impact Based Community Detection Algorithm via Discrete PSO", *Mathematical Problems in Engineering*, pp.1-15, 2016.
[24] C. Pizzuti, "A Multi objective Genetic Algorithm to Find Communities in Complex Networks", *IEEE Transactions on Evolutionary Computation*, Vol.16, No.3, pp.418-430, 2012.
[25] Z. Li and J. Liu, "A multi-agent genetic algorithm for community detection in complex

networks", *Physica A: Statistical Mechanics and its Applications*, Vol.449, pp.336-347, 2016.
[26] Q. Liu, B. Zhou, S. Li, A. Li, P. Zou, and Y. Jia, "Community Detection Utilizing a Novel Multi-swarm Fruit Fly Optimization Algorithm with Hill-Climbing Strategy", *Arabian Journal for Science and Engineering*, Vol.41, No.3, pp.807-828, 2015.
[27] H. Liu, H. Zhao, W. Li, and B. Liu, "Synthesis of Sparse Planar Arrays Using Matrix Mapping and Differential Evolution", *IEEE Antennas and Wireless Propagation Letters*, Vol.15, pp.1905-1908, 2016.
[28] W. Xiang, X. Meng, M. An, Y. Li, and M. Gao, "An Enhanced Differential Evolution Algorithm Based on Multiple Mutation Strategies", *Computational Intelligence and Neuroscience*, Vol. 2015, pp.1-15, 2015.