Data Fusion-Link Prediction for Evolutionary Network with Deep Reinforcement Learning

Marcus Lim[1], Azween Abdullah[2], NZ Jhanjhi[3]
School of Computer Science and Engineering (SCE)
Taylor's University, Selangor, Malaysia

***Abstract*—The sophistication of covert activities employed by criminal networks with technology has been proven to be very challenging for criminal enforcement fraternity to cripple their activities. In view of this, law enforcement agencies need to be equipped with criminal network analysis (CNA) technology which can provide advanced and comprehensive intelligence to uncover the primary members (nodes) and associations (links) within the network. The design of tools to predict links between members mainly rely on Social Network Analysis (SNA) models and machine learning (ML) techniques to improve the precision of the model. The primary challenge of constructing classical ML models such as random forest (RF) with an acceptable level of accuracy is to obtain a large enough dataset to train the model. Obtaining a large enough dataset in the domain of criminal networks is a significant problem due to the stealthy and covert nature of their activities compared to social networks. The main objective of this research is to demonstrate that a link prediction model constructed with a relatively small dataset and dataset generated through self-simulation by leveraging on deep reinforcement learning (DRL) can contribute towards higher precision in predicting links. The training of the model was further fused with metadata (i.e. environment attributes such as criminal records, education level, age and police station proximity) in order to capture the real-life attributes of organised crimes which is expected to improve the performance of the model. Therefore, to validate the results, a baseline model designed without incorporating metadata (CNA-DRL) was compared with a model incorporating metadata (MCNA-DRL).**

Keywords*—*Metadata; time-series network; social network analysis; criminal network; deep reinforcement learning

I. Introduction

Currently, members of organised crimes often work together to form a resilient and flexible structure to execute their covert and stealthy activities [1]. The CNA tools are mainly constructed based on social network analysis (SNA) models and metrics [2]. SNA which combines knowledge of graph theory and the discipline of social science [3] is a common method employed to analyse the criminal network to uncover hidden structural relationships and key players in criminal syndicates [4,5]. These SNA applications also have a graphical interface that provides a comprehensive visual topological analysis of domain with network orientated dataset [6]. Most social media e.g. Snapchat, Twitter and Facebook recommend relationships using the SNA models based on the likelihood of associations or links of common interest [7].

In the topological analysis of criminal network, environmental factors that can affect the evolving formations of links between participants of the network have to be taken into consideration [8]. These factors such as criminal records, education level, age and family background (Fig. 1) are known as metadata. They provide further circumstantial information that may affect structural patterns of a criminal network over a period of time [9].

Criminal networks tend to exhibit a high likelihood of having unknown links or relationships as criminal activities usually operate in covert and stealthy nature [11]. The incomplete and inconsistent database captured during law enforcement procedures could have been done deliberately by criminals or unintentional human mistakes [12]. In such circumstances, the SNA methods of predicting probable existence or non-existence of links or relationships in criminal networks provide critical information that determines whether attempts to disrupt criminal activities can be successful (Fig. 1).

The prediction of links using SNA metrics is usually based on the structure of the network and supported by information on the contents of the nodes [13].

The link prediction model developed in this research (Fig. 1) leverages on DRL to achieve self-learning and generated datasets which can be combined with smaller domain datasets [14, 15] for ML training. The deep learning (DL) algorithm within the model would reduce reliance on specific human programmed algorithms when formulating an ML function [16-18]. The self-learning ability leverages on reinforcement learning (RL) whereby ML is achieved through recursive trial and error based on a system of rules operating in a domain where points are awarded when each task is successfully completed and deducted as punishments for failure [19].

The model developed in this research may encounter certain limitations in that it is constructed based on relatively small dataset which is a common attribute of criminal or terrorist networks compared to social networks such as Twitter, Instagram and Pinterest. The relatively small dataset may have an impact on the predictive performance of some classical supervised machine learning models being trained.

A. Structure of Paper

Our research paper consists of six sections with Section I is the introduction, Section II is a review of other research works involving evolutionary social network, ML models and implications of metadata fusion. In Section III, an explanation of the proposed and baseline models developed together with

the methodology of training is provided. Section IV provides information on the properties of the dataset, set-up of the experiments and a discussion of the results of the experiments. The research conclusion is discussed in Section V and Section VI explores the trajectory for subsequent research work.

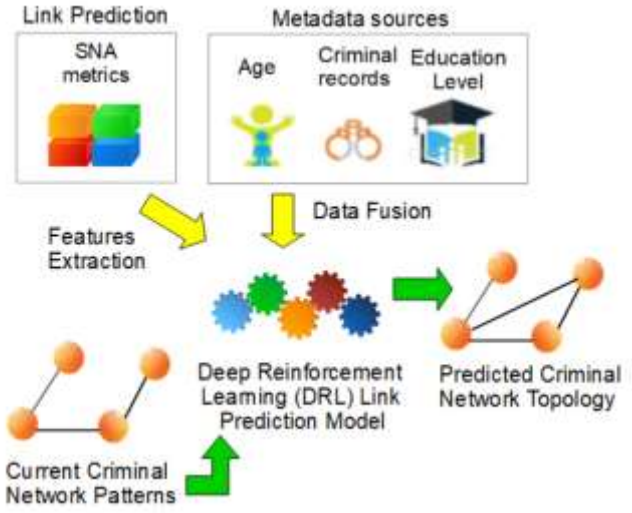

Fig. 1. MCNA-DRL Model to Predict Links for Evolutionary Criminal Network [10].

II. Related Work

In [13] Budur E. et al. developed an SNA model to predict hidden or missing links in a criminal network. The authors explained that the problem with real-world criminal dataset is that it is relatively small compared to social network dataset to effectively trained classical ML models. They leveraged upon the gradient boosting machine (GBM) ML algorithm and trained with a large dataset of about 1.5 million nodes and 4 million links by combining a few datasets. The large dataset is expected to capture the real-world nature of the criminal network with better precision. In their experiment, their proposed model managed to perform with higher predictive accuracy compared with models developed in prior works which performed with a smaller dataset. The authors did state that predictive accuracy could be improved if a time series dataset was used as it will better represent the properties of real-world criminal syndicates [20].

In [21], S. K. Dash et al. developed an SNA model to predict hotspot crime location by fusing crime data with metadata attributes such as police station proximity, education quality and emergency service call to improve the quality of the prediction. The model leveraged upon the supervised machine technique of support vector machine (SVM) which was trained on a dataset with feature extracted from environmental, social factors related to crime prediction. The data fusion was found to have improved the prediction quality of the model.

In [22], Bliss C. A. et al. proposed a link prediction model with Covariance Matrix Adaptation Evolution Strategy as link weights which ensemble 16 neighbourhood and similarity indices and leveraged on an evolutionary computing algorithm. The link prediction model, combining 16 SNA metrics, leveraged on evolutionary computing and trained with Twitter reciprocal reply network (RNN) dataset, was found to perform better than other supervised learning models such as SVM constructed from SNA metrics derived independently and in isolation. They also suggested future research to include geospatial features and community structure in a time-evolving network,

Sarvari, H. et al. [23] used SNA techniques such as centrality measures, PageRank and clustering coefficient to gain insight into the organisation of criminal community by constructing a large scale graph from a smaller dataset, for example, email address of criminals. The techniques of SNA analysis of large constructed social graph information were are able to provide a more detail profiling of criminals. Further research was suggested to incorporate the profile linking social graph from Facebook to other social networking media, e.g. Google+ and Twitter to derive a considerably complete profile of the scammers.

A recent breakthrough was achieved by Silver et al. [24] where an ML program that they developed with DRL, AlphaGo, demonstrated super-human performance by defeating the world's top grandmaster from China in the board game of Go, which has more permutation possibilities than all the atoms in the known universe. The feat was achieved with a combination of Monte Carlo tree search (MCTS) algorithm, which replicated the intuitive judgement capability of human to narrow the search scope to board patterns with the highest likelihood of success.

In the subsequent trajectory of their research on DRL, Silver et al. enhanced their AlphaGo program by developing AlphaGo Zero which was able to self-learn using dataset generated via self-play against prior versions of itself [25]. AlphaGo Zero was provided only with the basic domain rules of the game and was able to defeat AlphaGo after 3 days of self-learning. The DRL algorithm developed had reduced the reliance on incorporating human-crafted domain knowledge to achieve predictive performance. Therefore the DRL model had opened up possibilities of applying the algorithm to train other ML models with a relatively small real-world dataset.

In [26]. Lim, Marcus et al. have incorporated findings from the research work of Silver et al., and leveraged upon the algorithm of DRL to construct a link prediction in the domain of criminal network with a relatively small snapshot dataset combined with a self-generated dataset. The research yielded some positive results indicating DRL algorithm could be used to construct predictive models with adequate precision when trained with self-generated dataset in accordance with domain rules.

From the related works reviewed, there is little evidence that both DRL and metadata fusion technique have been incorporated into the field of link prediction for a dynamic criminal network structure which changes over time. This research is expected to fill the gaps by investigating the manner DRL and metadata fusion can be integrated to train a model to predict with better precision on a more diverse evolutionary graph-based dataset such as a terrorist network.

III. Models and Methodology

A. Proposed MCNA-DRL Model

The problem of predicting the formation or disappearance of edges in a network is treated as a binary classification task in ML modelling process.The data fusion DRL link prediction CNA (MCNA-DRL) model (Fig. 2) was developed as an extension of the research done by Marcus Lim et al. [27] using the MCTS model in the link prediction process.

The DL algorithm of the MCNA-DRL model has a significant influence on the overall performance of the model as it relies on the optimisation of parallel processing with graphics processing unit (GPU). The predictive accuracy of the MCNA-DRL model is assessed with the area under curve (AUC) scores [28].

The DL which functions as the value network for RL approximates a vector of a probability distribution (Fig. 3), computed from the SNA metrics as weights based on structural features of the nodes (vertex) and links (edges). In the formulation of the feature matrix (Fig. 2), metadata such as the count of criminal records, age and education levels are derived as weights in the training of the neural network. The metadata formulated weighted edges will approximate the output values provided by the neural network to rank node pairs based on the likelihood that links (edges) are predicted to form or disappear. The MCTS algorithm will perform the tree traversal commencing from the edges that achieved the top raking scores. The aggregated predicted scores computed from every state of a completed network traversal is then fed back to the value network to recalibrate the model's hyper-parameters to improve the precision of the prediction in the next iteration (Fig. 2).

B. Methodology

The classical SNA metrics (Table I) to predict the links are calculated for every pair of nodes and formulated as a feature matrix for the purpose of training the link prediction model [29]. During the features learning process, the DL (neural network) algorithms are trained to predict the probable edges as a classification of positive or negative edges (Fig. 2). An edge that is predicted to form in the next instance is tagged as a positive label or is tagged as a negative label if it disappears.

The SNA metrics are computed for each edge of the node pair of the criminal network where $\varphi(i)$ represents the neighbouring nodes in the network of node i. k_i refers to the degree of node i. $n_{ij}^{(t)}$ represents the number of walks of length t for each pair of nodes i and j. β denotes the discount factor for the computation of walks of longer length.

During testing, the prediction of links is made for every sample node pair based on the score aggregated from an array with multiple SNA feature metrics (Fig. 2).

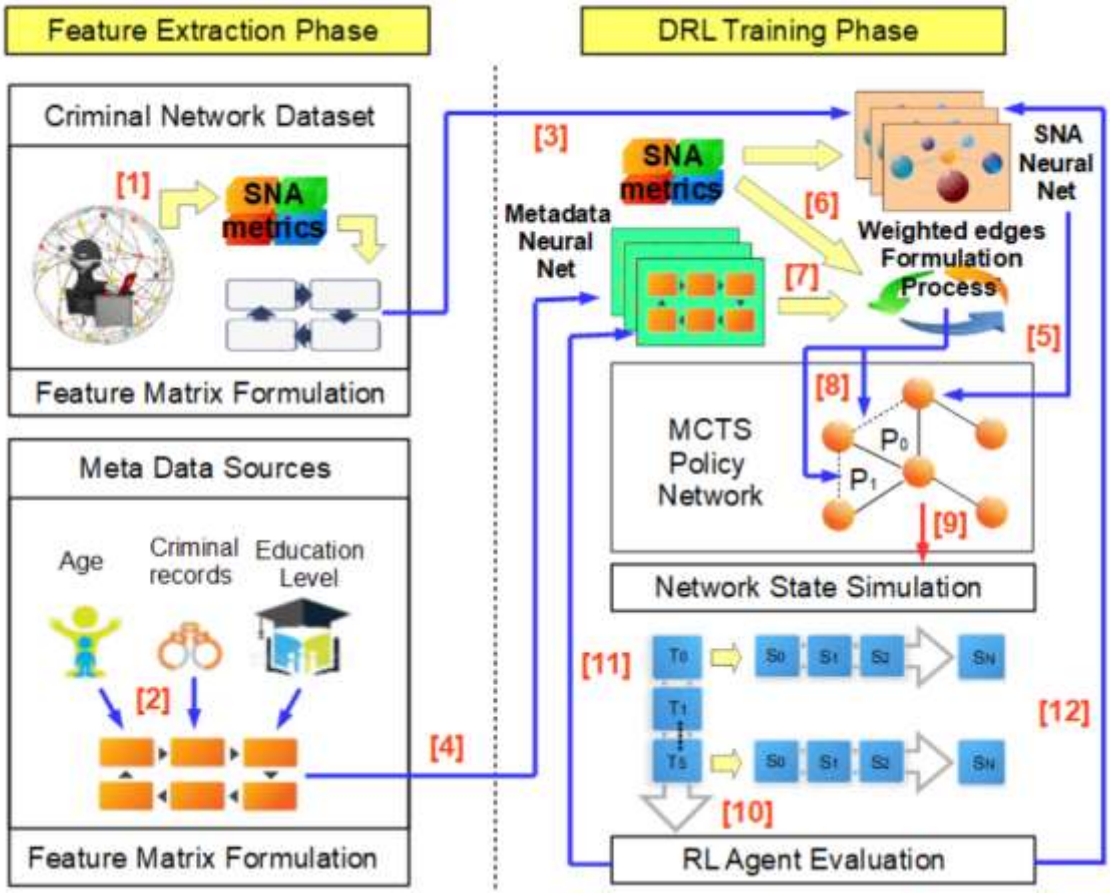

Fig. 2. Proposed MCNA-DRL Model for Link Prediction [10].

TABLE I. SNA METRICS FOR LINK PREDICTION [13]

Metrics	Definition
Common neighbour	$S_{xy} = \lvert \varphi(x) \cap \varphi(y) \rvert$
Jaccard Index	$S_{xy} = \frac{\lvert \varphi(x) \cap \varphi(y) \rvert}{\lvert \varphi(x) \cup \varphi(y) \rvert}$
Hub Index	$S_{xy} = \frac{\lvert \varphi(x) \cap \varphi(y) \rvert}{\min(k_x, k_y)}$
Preferential Attachment index	$S_{xy} = k_x \text{ x } k_y$
Adamic-Adar Index	$S_{xy} = \sum_{z \in \varphi(x) \cap \varphi(y)} \frac{1}{\log k_z}$
Katz	$S_{xy} = \sum_{t=1}^{\infty} \beta^t . n_{xy}^{(t)}$

In the MCNA-DRL model, the DL algorithm is an approximation function that is received as inputs of the first state of the network, S_0, and it computes the vectors indicating the likelihood of the existence or non-existence of the edges. The probability values derive from these vectors serve as weights of these edges in the link prediction process.

The SNA neural network (Fig. 2) learns from the values of these weights, and the value network generates the estimated measures via self-simulation using the SNA metric scoring by leveraging on the RL technique.

The MCTS network traversal commence at the root node, and the traversal to the following node creates a new state from the present network state based on the likelihood of an edge being formed or removed. A probable edge identified from the present state, S_1 to the subsequent state, S_2 is due to any action taken by the agent is based on the binary classification rules of evaluation will then be fed back to both the value and policy networks where a cost function will then calibrate the hyper-parameters again to enhance the predictive performance in the next iteration.

Notes (Fig. 2):

1) The Criminal Network dataset is mapped into SNA feature matrix for link prediction.

2) Metadata features is to a multi-dimensional feature matrix.

3) The SNA feature matrix of the Common Neighbour, Jaccard, Adamic-Adar Metrics, serve as the input layer of the value network.

4) The metadata feature matrix input such as the score of crime records, age and education level are processed to be processed by metadata data fusion value network. The SNA metrics of Hub Index and Preferential Attachment index functions as weights for the hidden layer 1 and hidden layer 2 respectively of the function approximator value Network.

5) The SNA metric function approximator identifies node-pairs with the highest likelihood of link formation or destruction.

6) The SNA feature matrix will also be factored in the data fusion weighted edges formulation process.

7) The output from .metadata fusion neural net is processed data fusion weighted edges formulation algorithm.

8) MCTS module simulates the network instance generation commencing on random node-pairs sorted by the links most likely to form or disappear (P_0, P_1) derived by The SNA metrics weighted edges formulation process.

9) The States, S_0 to S_N denote networks reconstructed with the identified hidden links at the end of each simulated link prediction rollout. The States generated are evaluated against the 5 test dataset instances (T_0 to T_5) to measure the degree of success in the link prediction.

*10)*The evaluation score from a prior instance is feedback to recalibrate the policy and value network to reduce errors in the next iteration.

*11)*The predictive performance evaluation score from time-elapsed training dataset (T_0 to T_5) by the RL is used to recalibrate the metadata fusion neural network.

*12)*The predictive performance evaluation score from time-elapsed training dataset (T_0 to T_5) by the RL is used to recalibrate the SNA neural network function approximator.

The AUC metric is used to evaluate both the MCNA-DRL and baseline CNA-DRL models. The AUC metric may have values from 0 to 1, where a score of 1 achieved by a model represents the best predictive precision.

C. Time-Evolving Network

In this research, both the MCNA-DRL model and the baseline CNA-DRL model is trained using the Madrid bombing time-series dataset based on the Rooted PageRank [28] algorithm. Every node pair is ranked based on the weights derived in accordance to the elapsed time between the present instance and the next instance of prediction process, Given a pair of nodes x and y with a common node, z that may exist between these nodes, the probability of a traversal commencing from x to y is represented as [30]:

$$P(x,y) = (1-\alpha)\frac{w(x,y)}{\sum_{z \in \varphi(x)} w(x,z)} + \begin{cases} \alpha \text{ if } y \text{ is the central node} \\ 0 \text{ if otherwise} \end{cases} \quad (1)$$

The time factor is formulated in Rooted PageRank as a weight with the time interval being a probability scaled in accordance with the distance between a pair of nodes.

The time-evolving network can be used to model social groups with structural configurations that change over time [30]. The structural configuration that varies over time may be caused by actors (nodes) joining or dropping out of the network as time passes.

D. Metadata Fusion

The fusion of metadata is the technique of combining various data sources derived from the external factors of the environment, which may have an impact on the features extracted to train a predictive model. Metadata in the context of

a criminal network that could have an impact on the behaviour of actors (nodes) to participate or exit from the network over time are criminal records, age, education level and family background [31]. In the construction of the MCNA-DRL model (Fig. 2), the number of criminal records, age and education level are factored as weights to train the metadata fusion DL value network. The value computed by the metadata fusion DL is factored in the calculation of the weights to rank the edges based on the likelihood to change in the next instance. The feature matrix extracted from the metadata and factored as weight is computed as follows [31]:

$$v_k = \sum_i w_{ki} x_i + b_i \quad (2)$$

with *v* representing the feature vector of the DL layers, *w* refers to the weight of every time-elapsed, *k*, for node *i* with *b* indicating the related bias. The bias is recalibrated at the completion of every training cycle.

The SNA metrics is combined linearly with the metadata weight index (2) in the formulation of the feature matrix for training the DL. Linear combination is used to simplify the resource hungry computation process. The combined weights index are used for making the actual prediction during the prediction process period. The combined index computed for every node pair would allow prediction to be made using alternative combination of parameters while reducing greatly the computation resource required by the technique. The first set of model parameters used as input to the DL is derived in random from parameter space for every prediction iteration.

IV. Experiments and Results

The terrorist network dataset of the Madrid train bombing in 2004 is a time-series dataset containing 20 time periods from the years 1985 to 2006 involving some 55 nodes (actors) [32] (Fig. 3, 4). The proposed MCNA-DRL model and CNA-DRL models are evaluated based on the AUC score which is a typical technique adopted to evaluate the precision of the classification models [13].

For the purpose of this experiment, only the dataset from the years 1998 to 2003 was used before the 2004 bombing event which was an exceptional event not reflective of the normal factors affecting the structural changes of the network.

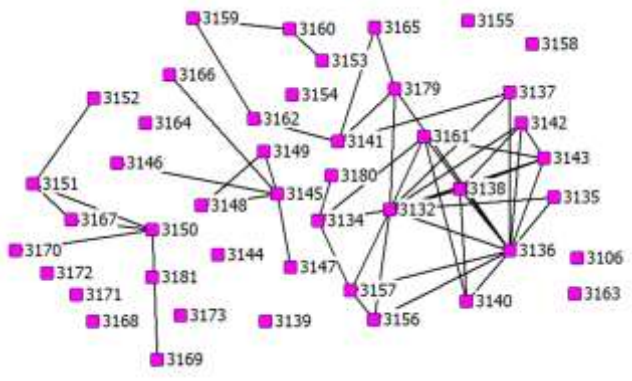

Fig. 3. Actual Criminal Network at Time-Stamp T_{2002}.

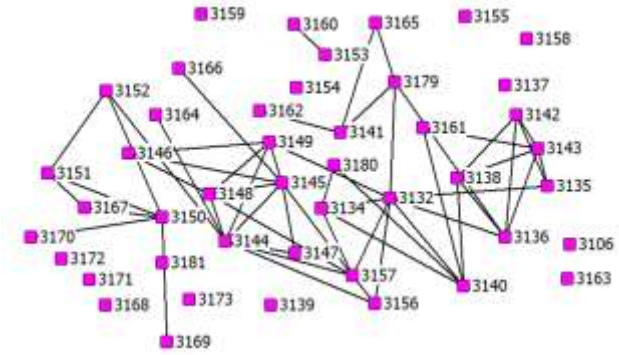

Fig. 4. Actual Criminal Network at Time-Stamp T_{2003}.

A. Experiment Set-up

To train the CNA-DRL and MCNA-DRL models, the dataset is formulated into a feature matrix whereby each state of the network represents the formation or cessation of an edge. The original node pair edge at each state is mapped onto a feature matrix with values from a prior time snapshot where a criminal link comes into existence or disappear (Fig. 2).

The Madrid bombing dataset segregated randomly into two (2) subset with a ratio of 75%:25% was used for training and testing respectively. The training set is extracted from the years 1998 to 2002 to build the feature matrix and used for training both the models. The number of positive links denoting the formation of new links in the next time step is obtained. The negative edges denoting cessation of the existing links in the next time step are then randomly chosen to match the number of positive links.

The performance evaluation score from the time-elapsed training dataset is fed back to the neural network to recalibrate the hyper-parameters using a cost function to minimise the error in prediction by both models in the next instance. The prediction of links is then simulated with the trained models which have been recalibrated on the test dataset (Fig. 5 and 6).

B. Results and Discussion

The MCNA-DRL model was able to correctly predict more edges (Fig. 5) that were supposed to appear in the topology of the year 2003 network than the CNA-DRL model (Fig. 6) when compared to the original terrorist network topology at T_{2003} (Fig. 4).

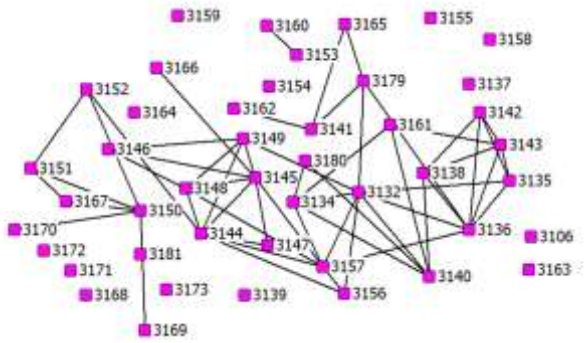

Fig. 5. Predicted Network by MCNA-DRL Model at Time-Stamp T_{2003}.

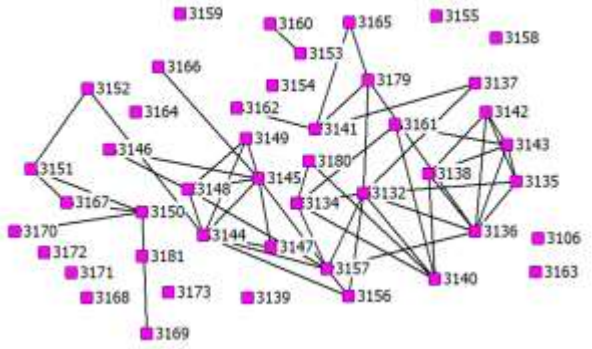

Fig. 6. Predicted Network by CNA-DRL Model at Time-Stamp $T_{2003.}$

The CNA-DRL model did not predict four new edges, i.e. node pairs (3146, 3149), (3144, 3164), (3132, 3149) and (3150, 3152) correctly. The CNA-DRL model did not correctly predict four edges that should have disappeared, i.e. node pairs (3134, 3161), (3132, 3137), (3137, 3141) and (3136, 3157) (Fig. 6) compared to the actual network in year 2002 (Fig. 3).

The MCNA-DRL model did not correctly predict one new edge, i.e. node pairs (3144, 3164) and two edges that should have disappeared, i.e. node pairs (3134, 3161)(3136, 3157) (Fig. 6) compared to the actual network at the year 2002 (Fig. 3).

Comparing the predicted terrorist network structure the year 2003, the results of the experiment indicate that the MCNA-DRL model (Fig. 6) which incorporates weights derived from the metadata incorrectly predicted five edges less than the CNA-DRL model (Fig. 5). Therefore, the features of metadata data sources factored as weights, attributed by the metadata formulation process seem to have contributed to the higher predictive precision of the MCNA-DRL model. This could be because of the incorporation of the metadata which captures the real-life environmental features of the terrorist network.

The AUC scores of the MCNA-DRL prediction model (Fig. 7) that factor in the metadata as weights achieved a higher AUC score than the CNA-DRL prediction model which did not incorporate metadata fusion by a score of 0.09 (Tables II).

The overall better performance of the MCNA-DRL model could be attributed to the fact that metadata provides other co-related environmental information that may strengthen or weaken the relationships between the nodes over time. This information improves the likelihood of identifying edges which can reduce the scope of the search performed by the MCTS algorithm.

The results also demonstrated that both models, constructed by leveraging on DRL, achieved predictive precision with the AUC scores above 0.5 (Fig. 8). This predictive precision was achieved despite the original dataset being relatively small compared to the most social networks as the models were further trained with self-simulated instances by RL.

The results of the experiment conducted are consistent with the investigation on DRL by Lim, Marcus et al. who constructed a criminal network link prediction model and trained on a snapshot dataset [27]. The current research represents an extension of the work done by the same research team [27] which made comparison of the DRL technique with classical GBM, SVM and RF techniques for link prediction models that were also trained on relatively small dataset which is characteristics of most criminal network (Table III). The comparisons made indicate that the classical models generally need to be trained on relatively larger dataset to achieve a better predictive accuracy than the DRL model that could be trained with the domain dataset and self-generated dataset.

Comparisons are also made with the time-evolving link prediction model (TDRL-CNA) model by Lim, Marcus et al. [28] which did not incorporate metadata fusion (Table III). While the TDRL-CNA model performance seems to peak after 1500 iterations, the MCNA-DRL model still managed to achieve a marginal improvement in the predictive accuracy by incorporating metadata after extended training iterations.

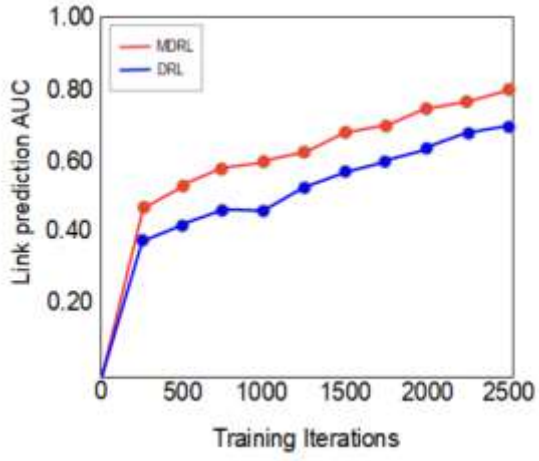

Fig. 7. AUC Score for the MCNA-DRL and CNA-DRL Link Prediction Models for Madrid Bombing Terrorist Network.

TABLE II. AUC SCORES OF MCNA-DRL LINK PREDICTION MODEL AND CNA-DRL MODELS

Dataset	AUC	Time-score(Hr)	Iterations
MCNA-DRL	0.79	4.3	2500
CNA-DRL	0.70	3.9	2500

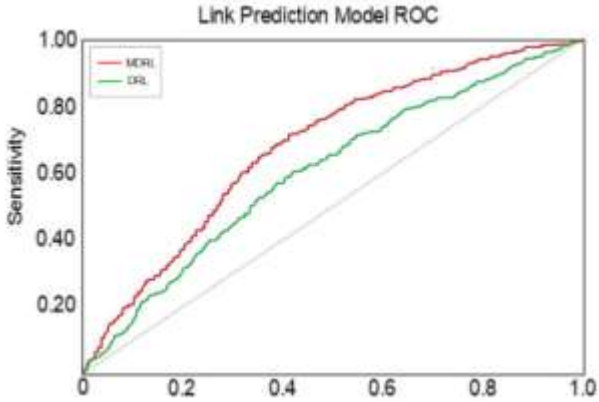

Fig. 8. ROC Curve of Link Prediction Model.

TABLE III. COMPARISON OF DRL LINK PREDICTION MODELS FROM RELATED RESEARCH WORKS

Model	MCNA-DRL	TDRL-CNA	DRL-CNA
ML technique	DRL with metadata fusion	DRL	DRL
Tree search ranking algorithm	MCTS	Breadth first search	Depth first search
SNA metrics	classical	classical	classical
Dataset	20 time-periods	11 time-periods	snapshot
Maximum nodes	55	27	62
Training time-score (hour)	4.3	Not available	1.2
Training iterations	2500	1500	1500
AUC Score	0.79	0.78	0.73
Authors	Current work	[28]	[27]

V. CONCLUSION

The results from this research was able to demonstrate that a model can be trained for the purpose of link prediction with a combination of metadata, relatively smaller dataset and self-generated dataset by leveraging on DRL. These results are evidenced by the AUC score of 0.79 and 0.70 achieved respectively by the MCNA-DRL and CNA-DRL models (Tables II). However, further experiments may need to be conducted to confirm if models constructed with DRL can achieve a better predictive performance than classical supervised ML models if a large scale dataset is used.

VI. FUTURE WORK

The future direction of this research will consider developing a new SNA metric and network search algorithm based on evolutionary computing to further improve the precision of the MCNA-DRL model. The performance of the search algorithm based on evolutionary computing will be compared with the MCTS model. The new SNA metric, will be indexed with metadata weights and is expected to further enhance predictive precision of the model as current findings indicate that models incorporating metadata are more reflective of real-world characteristics.

REFERENCES

[1] Duijn, Paul AC, Victor Kashirin, and Peter MA Sloot. "The relative ineffectiveness of criminal network disruption." Scientific reports 4: 4238, 2014.

[2] Taha, Kamal, and Paul D. Yoo. "A system for analyzing criminal social networks." In Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015, pp. 1017-1023. 2015.

[3] Qazi, Nadeem, and BL William Wong. "Behavioural & tempo-spatial knowledge graph for crime matching through graph theory." In 2017 European Intelligence and Security Informatics Conference (EISIC), pp. 143-146. IEEE, 2017.

[4] Kumar, Arunima S., and Raju K. Gopal. "Data mining based crime investigation systems: Taxonomy and relevance." In 2015 Global Conference on Communication Technologies (GCCT), pp. 850-853. IEEE, 2015.

[5] Giorgos Cheliotis, Associate Professor National University of Singapore. "Social Network Analysis", 2014.

[6] Thangamuthu, Mr AP, Mr G. Vadivel, and Mrs A. Priyadharshini. "Detecting Criminal Method using Data Mining.", 2019.

[7] Campana, Mattia G., and Franca Delmastro. "Recommender systems for online and mobile social networks: A survey." Online Social Networks and Media 3 : 75-97, 2017.

[8] Potgieter, Anet, Kurt A. April, Richard JE Cooke, and Isaac O. Osunmakinde. "Temporality in link prediction: Understanding social complexity." Emergence: Complexity & Organization (E: CO) 11, no. 1 : 69-83, 2009.

[9] Huang, Zan, and Dennis KJ Lin. "The time-series link prediction problem with applications in communication surveillance." INFORMS Journal on Computing 21, no. 2 : 286-303, 2009.

[10] Lim, Marcus, Azween Abdullah, N. Z. Jhanjhi, and Muhammad Khurram Khan. "Situation-Aware Deep Reinforcement Learning Link Prediction Model for Evolving Criminal Networks." IEEE Access 8 : 16550-16559, 2019.

[11] Dijkstra, L. J., Andrei V. Yakushev, P. A. C. Duijn, A. V. Boukhanovsky, and Peter MA Sloot. "Inference of the Russian drug community from one of the largest social networks in the Russian Federation." Quality & Quantity 48, no. 5 : 2739-2755, 2014.

[12] Spapens, Toine. "Macro networks, collectives, and business processes: An integrated approach to organized crime." European Journal of Crime, Criminal Law and Criminal Justice 18, no. 2 : 185-215, 2010.

[13] Budur, Emrah, Seungmin Lee, and Vein S. Kong. "Structural analysis of criminal network and predicting hidden links using machine learning." arXiv preprint arXiv:1507.05739, 2015.

[14] Li, Haoqi, Naveen Kumar, Ruxin Chen, and Panayiotis Georgiou. "A deep reinforcement learning framework for Identifying funny scenes in movies." In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 3116-3120. IEEE, 2018.

[15] Bahdanau, Dzmitry, Jan Chorowski, Dmitriy Serdyuk, Philemon Brakel, and Yoshua Bengio. "End-to-end attention-based large vocabulary speech recognition." In 2016 IEEE international conference on acoustics, speech and signal processing (ICASSP), pp. 4945-4949. IEEE, 2016.

[16] Zeiler, Matthew D., and Rob Fergus. "Visualizing and understanding convolutional networks." In European conference on computer vision, pp. 818-833. Springer, Cham, 2014.

[17] Chen, Xi-liang, Lei Cao, Chen-xi Li, Zhi-xiong Xu, and Jun Lai. "Ensemble network architecture for deep reinforcement learning." Mathematical Problems in Engineering, 2018.

[18] Duan, Yan, Xi Chen, Rein Houthooft, John Schulman, and Pieter Abbeel. "Benchmarking deep reinforcement learning for continuous control." In International Conference on Machine Learning, pp. 1329-1338. 2016.

[19] Yao, Kaisheng, Geoffrey Zweig, Mei-Yuh Hwang, Yangyang Shi, and Dong Yu. "Recurrent neural networks for language understanding." In Interspeech, pp. 2524-2528. 2013.

[20] Sharan, Umang, and Jennifer Neville. "Exploiting time-varying relationships in statistical relational models." In Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 workshop on Web mining and social network analysis, pp. 9-15. 2007.

[21] Dash, Saroj Kumar, Ilya Safro, and Ravisutha Sakrepatna Srinivasamurthy. "Spatio-temporal prediction of crimes using network analytic approach." In 2018 IEEE International Conference on Big Data (Big Data), pp. 1912-1917. IEEE, 2018.

[22] Bliss, Catherine A., Morgan R. Frank, Christopher M. Danforth, and Peter Sheridan Dodds. "An evolutionary algorithm approach to link prediction in dynamic social networks." Journal of Computational Science 5, no. 5 : 750-764. 2014.

[23] Sarvari, Hamed, Ehab Abozinadah, Alex Mbaziira, and Damon Mccoy. "Constructing and analyzing criminal networks." In 2014 IEEE Security and Privacy Workshops, pp. 84-91. IEEE, 2014.

[24] Silver, David, Julian Schrittwieser, Karen Simonyan, Ioannis Antonoglou, Aja Huang, Arthur Guez, Thomas Hubert et al. "Mastering the game of go without human knowledge." nature 550, no. 7676 : 354-359. 2017.

[25] Silver, David, Thomas Hubert, Julian Schrittwieser, Ioannis Antonoglou, Matthew Lai, Arthur Guez, Marc Lanctot et al. "A general reinforcement learning algorithm that masters chess, shogi, and Go through self-play." Science 362, no. 6419 : 1140-1144. 2018.

[26] Lim, Marcus, Azween Abdullah, N. Z. Jhanjhi, and Mahadevan Supramaniam. "Hidden link prediction in criminal networks using the deep reinforcement learning technique." Computers 8, no. 1 : 8. 2019.

[27] Lim, Marcus, Azween Abdullah, and N. Z. Jhanjhi. "Performance optimization of criminal network hidden link prediction model with deep reinforcement learning." Journal of King Saud University-Computer and Information Sciences, 2019.

[28] Lim, Marcus, Azween Abdullah, N. Z. Jhanjhi, Muhammad Khurram Khan, and Mahadevan Supramaniam. "Link Prediction in Time-Evolving Criminal Network With Deep Reinforcement Learning Technique." IEEE Access 7 184797-184807. 2019.

[29] Özcan, Alper, and Şule Gündüz Öğüdücü. "Multivariate temporal link prediction in evolving social networks." In 2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), pp. 185-190. IEEE, 2015.

[30] Casteigts, Arnaud, Paola Flocchini, Walter Quattrociocchi, and Nicola Santoro. "Time-varying graphs and dynamic networks." International Journal of Parallel, Emergent and Distributed Systems 27, no. 5 : 387-408. 2012.

[31] Satpathy, S., and A. Mohapatra. "A data fusion based digital investigation model as an effective forensic tool in the risk assessment and management of cyber security systems." In The 7th international conference on computing, communications and control technologies. 2009.

[32] Borgatti, S.P., Everett, M.G. and Freeman, L.C. 2002. Ucinet for Windows: Software for Social Network Analysis. Harvard, MA: Analytic Technologies.Vol.1.2002.