IEEE *Access*
Multidisciplinary : Rapid Review : Open Access Journal

Link Prediction in Time-Evolving Criminal Network With Deep Reinforcement Learning Technique

MARCUS LIM[ID]**[1], AZWEEN ABDULLAH**[ID]**[1], NZ JHANJHI**[ID]**[1],**
MUHAMMAD KHURRAM KHAN[ID]**[2], (Senior Member, IEEE), AND**
MAHADEVAN SUPRAMANIAM[ID]**[3]**
[1]School of Computing and IT (SoCIT), Taylor's University, Subang Jaya 47500, Malaysia
[2]Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh 11451, Saudi Arabia
[3]Research and Innovation Management Center, SEGi University and Colleges, Petaling Jaya 47810, Malaysia

Corresponding author: NZ Jhanjhi (noorzaman.jhanjhi@taylors.edu.my)

ABSTRACT The prediction of hidden or missing links in a criminal network, which represent possible inter-
actions between individuals, is a significant problem. The criminal network prediction models commonly
rely on Social Network Analysis (SNA) metrics. These models leverage on machine learning (ML) tech-
niques to enhance the predictive accuracy of the models and processing speed. The problem with the use of
classical ML techniques such as support vector machine (SVM), is the dependency on the availability of large
dataset for training purpose. However, recent ground breaking advances in the research of deep reinforcement
learning (DRL) techniques have developed methods of training ML models through self-generated dataset.
In view of this, DRL could be applied to other domains with relatively smaller dataset such as criminal
networks. Prior to this research, few, if any, previous works have explored the prediction of links within
criminal networks that could appear and/or disappear over time by leveraging on DRL technique. Therefore,
in this paper, the primary objective is to construct a time-based link prediction model (TDRL) by leveraging
on DRL technique to train using a relatively small real-world criminal dataset that evolves over time. The
experimental results indicate that the predictive accuracy of the DRL model trained on the temporal dataset
is significantly better than other ML models that are trained only with the dataset at specific snapshot in time.

INDEX TERMS Social network analysis, link prediction performance, deep reinforcement learning,
time-evolving network.

I. INTRODUCTION

A. BACKGROUND

Deep reinforcement learning (DRL) is a field of machine
learning (ML) which integrates the multi-layer representation
learning of neural networks as the value network within
the reinforcement learning (RL) framework. RL is a form
of ML technique, which usually involves the presence of
agents or programs that interact with the environment in
which it will go through a process of learning and adaptation
by evaluating points given continuously when tasks have been
completed [1]. This ML technique is not similar to supervised

The associate editor coordinating the review of this manuscript and
approving it for publication was Kim-Kwang Raymond Choo[ID].

and unsupervised ML techniques which are trained using
available dataset [2]. Deep neural network (DNN) or deep
learning (DL) is a ML technique that simulate the function
of neurons in the brain by learning feature representations
derived from large dataset through multiple processing lay-
ers to formulate a ML model. Thus, DL is able to remove
the reliance on predefined human crafted algorithms in the
construction of ML models [1], [3], [4]. The objective of the
application of DRL is to achieve self-learning capabilities in
ML to simulate general artificial intelligence [2].

Criminal network analysis (CNA) refers to tools and
techniques applied in the structural analysis of a criminal
network, which are developed based on the metrics and
models in the field of social network analysis (SNA) [5].

CNA will be able to provide a better knowledge of the relationships or links between key actors or nodes within the criminal network to improve the effectiveness of law enforcement agencies. Social networks are ubiquitous, such as collaborations within scientific communities, drug smuggling syndicates and even text messaging activities between participants in social media, e.g. WhatsApp, Instagram and Twitter. The structures of these network communities are depicted in the form of graphs, where the participants or actors of these communities are represented as nodes and the social interactions or relationships occurring between them are represented as edges or links. In the topological analysis of these network communities, the possibility of making precise prediction of the formation of new links, re-occurrence of previous links and disappearance of existing links is a predominant problem. Link prediction of this nature is useful in the anticipation of subsequent evolution in the behavioural patterns of these network communities. Link prediction based on SNA metrics can be formulated either from topological or content-based metrics of network-orientated domain. These topological and content-based metrics are categorised as neighbourhood, random-walk and Katz-based. Examples of typical neighbourhood-based metrics are common neighbour, Adamic–Adar and Jaccard index [6]. In the real world, the complexity of the link prediction problem is compounded by the evolving nature of the criminal network structure over time, which reflects the effect of temporal information on the activities within that domain. Such dynamic network, where the network topology varies over time, is referred to as time-evolving network [7].

B. PROBLEM DEFINITION

The link prediction problem in criminal networks has been attracting considerable interest recently and a number of methods, which leverage on the topological analysis of the graph structure of criminal networks, have been proposed. However, many of these approaches encounter two important limitations. Firstly, other than a few of the methods reviewed [7], [8], most of the proposed link prediction models designed do not consider the temporal dimension of evolving social networks. The network topology of real-world criminal syndicate evolves over time because of constant changes in the underlying environmental variables influencing criminal activities, thus providing a time series dataset. The analysis of these dataset shows that the events of the distant past have a less significant influence on the formation and disappearance of future links than the events that occur recently.

Secondly, in most criminal network domains, the ranking of nodes with high probability of interaction in the future with an identified node, has an important influence on the identification of possible future links of the identified node, has not been considered.

In this research, the effect of temporal information on the evolution of criminal networks are factored in the construction of the link prediction model with the following objectives:

Firstly, a link prediction model is developed and trained by incorporating information on the temporal characteristics of the social network dataset. In particular, this model will be an extension of the DRL CNA model proposed by Lim et al. [9] to include time awareness. The model will incorporate the weights of the edges that are formulated based on the factoring of features, such as rooted PageRank algorithm and Adamic–Adar SNA metrics, which are affected by the temporal characteristics of the network, into the link prediction method.

Secondly, a testing method that compares the performance of the proposed model with that of a few classical link prediction models in terms of its capability to rank nodes based on the proximity of the nodes to a selected node has been formulated. The predictive accuracy of links by DRL-CNA model is evaluated using the area under curve (AUC) scores and confusion matrix by comparing the TDRL-CNA model with the baseline DRL-CNA model.

The DRL technique adopted in the construction of the link prediction model will enable the model to be trained with self-generated dataset based on SNA metrics and models to compensate for the relatively small dataset of criminal networks. This technique is expected to overcome the limitations of classical ML models, which need to be trained with real-world dataset that is large enough to achieve an acceptable level of predictive accuracy.

C. DATASET

For the purpose of experiment evaluation, the 2002 Bali Bombing Operations Attack Series dataset obtained from UCINET [10]. The dataset in comma-separated-value(CSV) file format contains an 11-period history of the evolution of terrorist network groups was utilised. Each period of the dataset contains the number of nodes/actors and edges/links that exist between node-pairs at that point in time. The network dataset was the largest in the year 2002 prior to the bombing, which has 27 nodes and 205 edges/links.

II. RELATED WORK

The features required from the criminal network dataset for link prediction are based on two types, i.e. the structure of the network and the features of the nodes. In the case of social network, for example, Facebook members, the features of the nodes may be in the form of the subject of interest of the members, such as common purchasing habits. These structural data can be used alone. In [11], the authors conducted thorough research on various proximity measures and determined that methods that incorporate proximity measures can achieve significantly higher precision in link prediction than random classification models by a factor of more than 40. However, they observed that the precision achieved by these methods could be further improved. Meanwhile, Dash et al. [12] have successfully created a model to predict the occurrence of crimes by leveraging support vector regression techniques based on the time-series dataset of the city of Chicago. They highlighted the significance of node ranking based on temporal information in their predictive model.

In [13], Clauset et al. developed a link prediction model based on the hierarchical random graph. The iterative nature of community structure is represented in the form a tree, where the nodes of the graph are the leaves. The model designed was used to predict missing links from a few domains, such as the terrorist, metabolic and species interaction datasets. Their experimental results indicated that this model performed better than the models constructed based on the common neighbour and Jaccard indices.

In their research, Wang *et al.* [14] incorporated the distance metrics, the attributes of the nodes and a new feature formulated using a probabilistic model derived from the network dataset. Murata and Moriyasu [15] investigated the possible advantages of factoring multiple edges found in some datasets. In their model, the multigraph of a network is converted into a simple graph with the weight of the edges formulated from the number of related edges found within the multigraph. The results of their research indicated the predictive accuracy of weighted methods over non-weighted methods.

Potgieter *et al.* [16] specifically investigated link prediction incorporating temporal information. In their research, they experimented with the use of moving averages and SNA metrics, such as common neighbour and Katz indices. They leveraged on the Bayesian network methods to analyze the correlation between appearance of links and weights based on the SNA metrics.

In [17], the authors designed their model for the link prediction problem as a binary classification task. They extracted the historical information related to the activities within the network and the features of the nodes, which are then formulated as a feature matrix. The feature matrix is then input into a binary classification model based on logistic regression to predict the potential of future links between nodes.

In recent work, Huang and Liu [18] designed a link prediction model that factored in the time-evolving nature of the communication network dataset. Their research focussed on the surveillance aspect of the communication network traffic. In this domain, activities, such as phone calls and e-mails, may trigger other events. Their research indicated that their model, which factored in temporal information, i.e. time-aware, performed better than baseline models that omit the use of time-aware techniques. However, in [8], the authors demonstrated that the optimum results could be obtained by incorporating both techniques. The time-based link prediction method adopted by the authors utilised a two-step approach. In the first stage, a weighted static graph was derived by summarising the dynamic graph. In the second stage, the relational Bayes classification technique was incorporated. Their model was trained on a dataset of scientific collaborations.

RL refers to the ML technique where agents, usually in the form of programs designed to interact with the changing environment variables, will learn by completing tasks and will be awarded points upon successfully achieving predefined rules or objectives. The points achieved by the agent upon successful completion of tasks are labelled as rewards or positives; otherwise, the points are labelled as punishment or negative [19]. This form of ML is different from the typical approach employed in supervised learning models, which are trained on specifically identified domain datasets [20].

Anthony *et al.* [21] improved the performance of RL algorithms by combining imitation learning methods in the domain of the game of Hex. Their investigation was an extension to the pioneering research work on DRL by Silver et al. who develop the AlphaGo program which was designed to play the game of Go and can be applied to other domain [22].

Silver et al. successfully developed the AlphaGo program because of a breakthrough in formulating the DRL technique, which integrates deep neural network into the framework of RL. AlphaGo simulated human intuitive judgement and was able to master the board game of Go entirely by playing against a version of itself through DRL.

Silver et al. conducted further research on DRL by developing AlphaGo Zero, which was capable of self-learning by training on dataset simulated purely by self-play [23], based only on the basic rules of legal moves of the game. The DRL technique could be applied to other environments where the availability of large dataset becomes a limiting factor in the training ML models. This technique also overcame the requirement of domain-related programming rules to be handcrafted by humans.

The research work by Silver et al. have contributed significantly to the development of artificial general intelligence (AGI), as AlphaGo Zero was able to not only defeat the AlphaGo version but also master other 2-player board games such as Chess and Shogi.

Based on the review of related works, there is little evidence that DRL technique have been leveraged upon in the construction of link prediction model for criminal network that evolves over time. This research fills the gaps by investigating and proposing a time-evolving criminal network that leverages on the DRL to construct a link prediction model, which will exhibit better predictive performance than classical ML models.

III. MODELS

The link prediction problem can be considered a classification problem by labelling the appearance or disappearance of a link or edge between a pair of nodes as a binary classification of positive and negative edges, respectively. Therefore, the feature or attribute can be extracted for each pair of nodes as a multidimensional data record. The feature matrix of this multidimensional data record usually consists of SNA metrics, such as the common neighbour, Katz-based or walk-based indices, between nodes [24].

The feature matrix is formulated based on the SNA metrics (Table 1) for each node pair and edge within the criminal network, where $\varphi(i)$ refers to the nodes in the network that are neighbours of node i. k_i represents the degree of node i.

TABLE 1. Link prediction metrics [24].

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

$n_{ij}^{(t)}$ refers to the count of walks with length t of node pairs i and j. β is the discount factor used to compute the number of walks on a longer length.

For a graph, which is undirected and unweighted, G = (V,E) represents the network structure of a criminal network, where each link e = (u,v) denotes the relationship between u and v that occurred at a specific point in time $t(e)$ and $(u,v) \in E$. Given the times t and $t' > t$, we let G[t, t'] represent the subgraph of G, which comprises all of the links that have been timestamped between t and t', where four different times are denoted as t_0, t'_0, t_1 and t'_1 with the condition that $t_0 < t'_0 \leq t_1 < t'_1$ [25].

For a sample graph network G[t_0, t'_0], the link prediction model is expected to generate a list of edges, which are predicted to be added to the network G[t_1, t'_1] and do not exist in G[t_0, t'_0]. The periods [t_0, t'_0] and [t_1, t'_1] represent the training and test intervals, respectively. t_n denotes the given future time of graph G, where the edges are to be predicted using the trained model (Fig.1).

To test the algorithm's accuracy, a fraction of the observed edges E (80% of all edges) of some known relationship within the dataset is selected randomly as a training set, $E_{training}$. The remaining edges (20% of all edges) will serve as the testing set, E_{test}, to evaluate the predictive accuracy of the model with none of the information in this set are used for prediction. For training this model, $E = E_{training} \cup E_{test}$ and $E_{training} \cap E_{test} = \emptyset$.

The area under the receiver operating characteristic curve (AUC) is the metric used to evaluate the predictive precision of the model. The AUC metric is a standard metric, which indicates the probability that a randomly identified predicted edge (an edge in E_{test}) is given a higher score than a randomly selected non-existent edge (an edge found in U but not in E, where U represents the universal set that
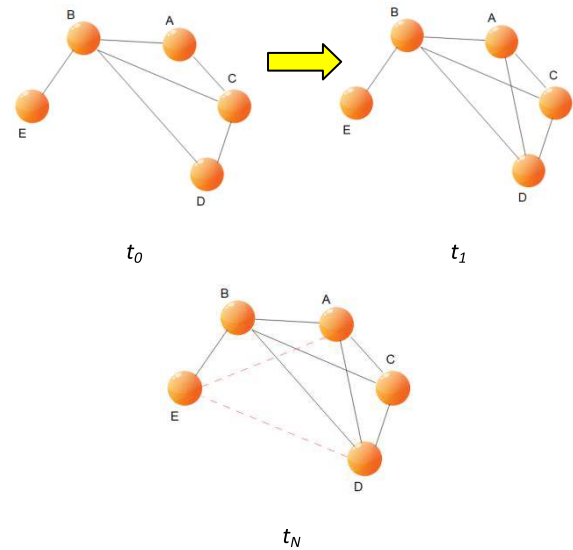

FIGURE 1. An example of proposed link prediction model trained with subgraph at time-stamp t_1 to t_2 and prediction made at t_N.

Algorithm 1: Heuristics evaluation method for link prediction accuracy
Input: Observed network G(V′,E′)

1: Select random edges for testing and create sub-graph; G′(V′,E″) = G(V′,E′) - random edges
2: Score some or all possible edges (V′² - E″) based on similarity index (SNA link prediction metrics)
3: E_{new} = pick k top ranked edges (edges score > 0.5)
4: Evaluate prediction method : effectiveness = |E_{new} ∩ (E′ - E″)| (by comparing predicted edges with random edges sampled)

Output: Accuracy metric of link prediction

FIGURE 2. Algorithm for evaluation of link prediction accuracy [16].

---

consists of all possible existing and non-existing edges) [26] (Fig.2). Given all possible independent comparisons n, the predictive precision of the model is represented by AUC = (n' + 0.5n'')/n, where n' denotes occurrences of predicted edges having a higher score and n'' denotes occurrences of predicted edges and non-existing edges with the same score [26].

If the dataset used has the properties of an independent and similar distribution from which all the scores are generated, then the AUC metric should be approximately 0.5. As a result, the extent to which the predictive accuracy of the model performs better than pure chance is represented by the degree that the AUC metric exceeds the score of 0.5.

For the construction of the TDRL link prediction model, deep neural network(DNN) performs the approximation function that inputs the initial instance of the network, S_0, and generate vectors containing probabilities of the existence of links. The SNA metrics for each node pair are used to compute the weights of these links based on the values of these probabilities. Then, the SNA neural network function

FIGURE 3. TDRL-CNA link prediction model for time-evolving network [9].
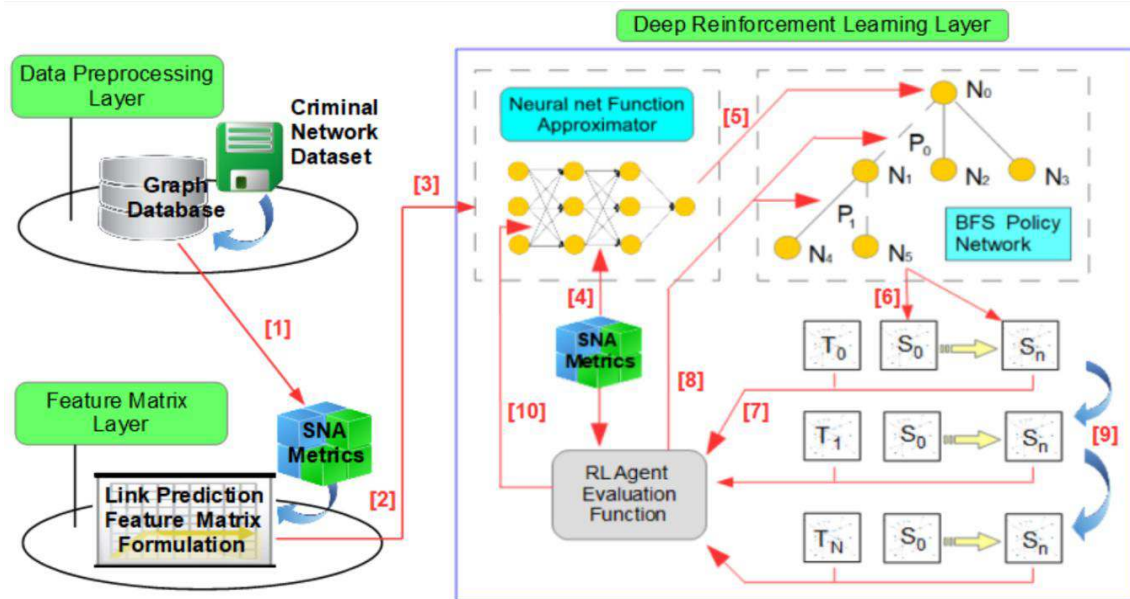
Notes:

[1] Criminal Network Dataset is mapped into SNA feature matrix for link prediction.

[2] The feature matrix serve as the input layer of the Value Network.

[3] The SNA feature matrix of the Common Neighbour, Jaccard, Adamic-Adar Metrics, serve as the input layer of the Value Network.

[4] 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. The SNA feature matrix will be factored in the data fusion weighted edges formulation process.

[5] The Breadth-First Search (BFS) Module perform the network path traversal initiated on the random node-pairs identified by the function approximator of the Value Network based on the probability of edge formation.

[6] 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 10-years test dataset (T_1 to T_{10}) to measure the degree of success in the link prediction.

[7] The link prediction result feed to the RL agent to access the prediction accuracy and calibrate hyper-parameters for subsequent link predictions.

[8] The SNA metrics weighted edges formulation process will generate the weights of the edges for node-pair based on the highest probability (P_0, P_1) of link formation or destruction.

[9] Performance metrics from each evaluation of time-interval test dataset (T_0 to T_{10}) is feedback to Function Approximator Neural Net to calibrate the weights parameters.

[10] Performance metrics from each evaluation of time-interval test dataset (T_0 to T_{10}) is feedback to Metadata Fusion Neural Net to calibrate the weights parameters.

approximator (Fig.3) is trained based on the patterns of the feature matrix computed from the probabilities of hidden edges from which values are estimated from SNA metric scoring derived entirely from self-simulated network instances using RL. These values, which represent hidden links with the highest probabilities, prioritise the traversal through the branches of the tree from root to leaf.

The proposed time-evolving link prediction (TDRL-CNA) model (Fig.3), which is an extension of the work [27] on the DRL-CNA link prediction model, will use a general-purpose breadth-first search (BFS) algorithm. The SNA link prediction metrics are formulated into a feature matrix as input to the RL policy network (Fig. 3) to compute the score of each instance of the simulated network during the link prediction process. The common SNA metrics selected to compute the feature matrix consist of neighbourhood, Katz and random walk based measures. The neural network function approximator (value network) which has a few layers of hidden neural network (Fig. 2), utilises SNA metrics to provide the weights represented as a vector of probability distributed over

sets of node pairs and edges. The DRL model will initiate its search from the node pair with the highest ranking. The scores achieved by the RL agent for each state of the network are then factored into the training of the value network to enhance its predictive accuracy by calibrating its hyper-parameters.

The value network contains parameters that have been calibrated through a training process utilising a dataset of network instances self-generated by RL. The BFS function is initiated on nodes with the highest probability of link formation estimated by the value network based on SNA index using a tree search algorithm. Then, the iterations of network instance are continuously simulated to compute an approximation of the value of instances. The BFS process will subsequently expand and traverse the network instances guided by probability of edges formation derived from the formulation of SNA indices.

In each BFS iteration simulation, the probability of edge formation is computed for each node-pair by the BFS policy network. Thereafter, during the rollout process, where the BFS traverses from root to leaf in each network instance in accordance with the default policy, the estimated values of each node computed from the previous phase by the network traversal process are calibrated to obtain the current result.

Every tree traversal process of a tree from root to leaf involves a sequential reconstruction of network instances simulated on self-scoring weighted edges. The tree search process commencing at the root node denotes the existing state, and each traversal to the next child node generates a snapshot of the network state from the current state due to the probable formation or cessation of an edge. A possible hidden edge predicted from current instance, S_1 to the next, S_2 is the result of an action by the agent in accordance with policy network to create the next instance, S_2.

The network structure after each iteration is constructed by identifying edges with the highest weight scores derived from the SNA metrics. At every end of a simulation process, the instance of the predicted network is evaluated against the original network structure extracted from the prior instance of the criminal network dataset. On the basis of the outcome of each evaluation, the cost function will recalibrate the hyper-parameters of the DNN to reduce errors in the prediction of edges in the next iteration(Fig.3).

IV. EXPERIMENT

For the purpose of this experiment, the 2002 Bali Bombing Operations Attack Series dataset from UCINET [10] that contains an 11-period history of the evolution of terrorist network groups was utilised. The proposed TDRL-CNA model is evaluated using the AUC metric, which is a commonly method employed to assess the accuracy of ML classification models.

A. EXPERIMENT SET-UP

To train both DRL-CNA and TDRL-CNA models, the dataset was transformed, whereby each instance that represents the presence or absence of a link was mapped to
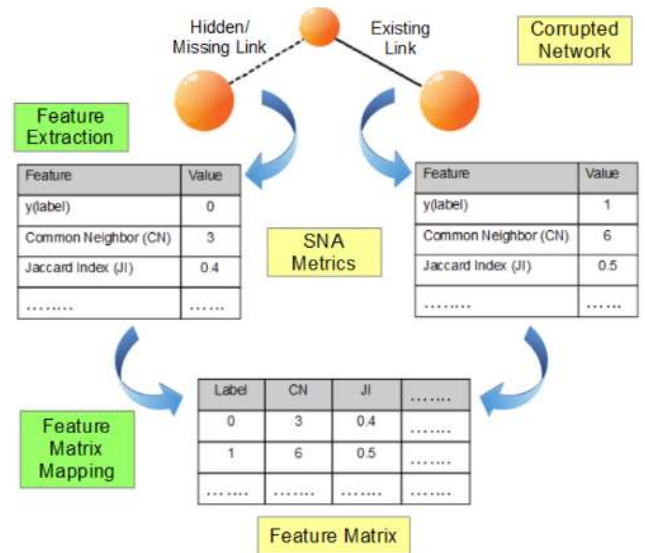

FIGURE 4. The feature matrix mapping process of Criminal network dataset [30].

a multidimensional feature space that follows the linear dependency assumed in the models. The task of link prediction to accurately predict future links or edges, which are not yet in existence in the current network topology, is commonly termed as positive link prediction.

1) FEATURE EXTRACTION AND MAPPING PROCESS

The SNA metrics for link prediction are extracted from the topological features of the criminal network and were mapped into a feature matrix to train the link prediction model. The actual node pair link at each timestamp was mapped to a multidimensional feature space with values from previous time-periods representing the presence or absence of the criminal link (Fig.4).

2) MODEL TRAINING

The feature matrix was input into the link prediction model for training and testing purposes (Fig.3). For the training set, the dataset was reduced, so there was an equal number of positive and negative instances (a link does not exist between two nodes). For each year, the number of positive instances was obtained. Then, negative instances were randomly selected until an equal number of positive and negative instances were derived. The trained models were used to predict the network for each instance, and these predictions were collected to construct the predicted network from the test dataset.

To predict negative links, i.e. links that will disappear from the model at a future point, the positive links predicted from the original feature matrix were used as input. Then, the label from the original feature matrix was inverted by replacing 0 with 1, and vice versa. New links were then predicted from the inverted feature matrix. The negative links were identified by inverting back the inverted feature matrix and comparing with the original matrix.

To predict both positive and negative links for a temporal dataset, the edges of node pairs were weighted according to
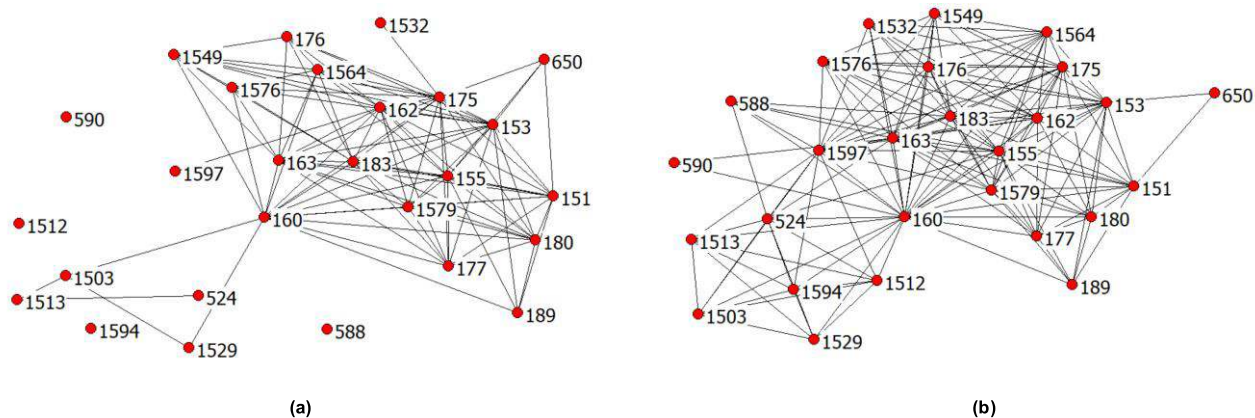
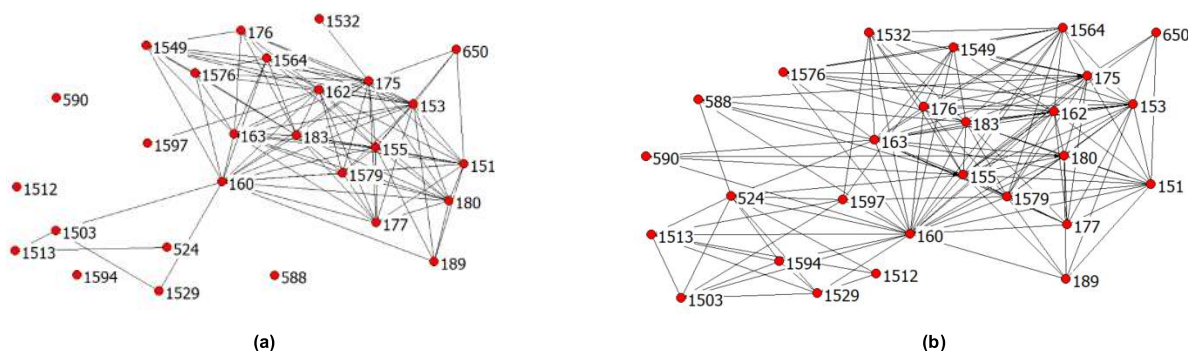**FIGURE 5.** (a) Year 2001 network topology (pre-bombing) (b) Year 2002 network topology.

FIGURE 6. (a) 2001 network topology (pre-bombing) (b) 2002 predicted network topology.
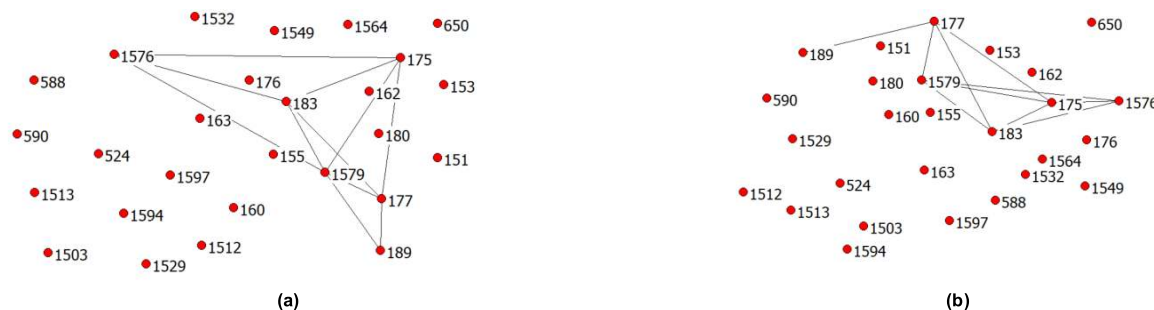

FIGURE 7. (a) Year 2005 network topology(post-bombing) (b) 2006 network predicted links.

the time that elapsed since the prior interaction between node pairs [29]. The time-elapsed metric was used as the weight of a specific edge and applied to a rooted PageRank algorithm on a weighted network to obtain the scores for each node [24]. The probability of being an edge can be predicted using the proposed TDRL-CNA model.

The evaluation process involves graphs with edges that contain temporal information. The Bali Bombing dataset used was segregated into two parts. The first part consists of the data collected from 1985 to 2001, before the 2002 bombing event in Bali. The second part consists of the data collected from 2003 to 2006, after the 2002 bombing event in Bali.

The dataset has been divided into two parts because the characteristics of the dataset before (pre-bombing) and after (post-bombing) the event are significantly different after major disruptions to the terrorist network because of the

arrests and/or deaths of key actors. The first part of the dataset, from 1985 to 2001 Fig.5(a), i.e. training dataset, is extracted to formulate the feature matrix for link prediction and 2002 Fig.5(b) dataset is used as the testing dataset to ascertain the performance accuracy of the prediction techniques of both models. The second part of the post-bombing dataset from the year 2003 to 2005 (Fig.7(a)) is used to train both models after major disruptions to the terrorist network. The 2006 dataset was used to test the predictive accuracy in post-bombing dataset.

B. EXPERIMENT RESULTS
The TDRL-CNA model Fig.6(b) managed to predict most of the edges that were supposed to appear in the network topology in the year of the bombing (Fig.5(b)). However, the model was unable to predict the edges that were supposed
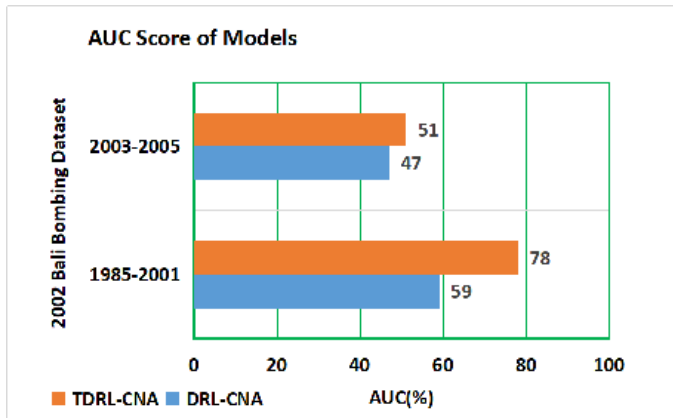
AUC Score of Models

Model	DRL-CNA	TDRL-CNA	Iterations
1985-2001	59	78	1500
2003-2005	47	51	1500

FIGURE 8. AUC scores of DRL-CNA and TDRL-CNA link prediction model.

to disappear in the 2002 network topology, e.g. edges for node pairs (155, 650) and (175, 650), which could be attributed to the nature of the terrorist network, where node 650 most probably represents an outlier. There are also edges that were supposed to appear but were not successfully predicted, such as the edges for node pairs (1512, 1597) and (1512, 1503), which could be attributed to the fact that node 1512 was a new node that only existed in the year before the bombing. This finding could also be attributed to the fact that the weights of the edges based on the time elapsed between node pairs in node 1512 are relatively small compared to that of other edges.

The prediction of edges using TDRL-CNA trained on the post-bombing dataset (year 2003–2005) (Fig. 7(b)) shows significant differences from the edges of the actual 2006 dataset. Edges for node pairs (151, 175) and (151, 183), which should appear for the 2006 predicted network topology Fig.7(b), did not appear.

However, the edge for node pair (189, 1579), which should still exist in the 2006 predicted network topology, was observed to have been removed. The inconsistency in the 2006 predicted network topology could be attributed to the massive disruption to the network because of factors other than the time elapsed between node pairs, such as the arrest and/or death of key actors.

The AUC values (Fig.8) indicate that the models trained on the pre-bombing event dataset Fig.5(a) have a higher predictive accuracy than the models trained on the post-bombing event dataset (Fig.7(a)). This finding could be attributed to the disruption to the terrorist network after the bombing event, which resulted in a massive reduction in the number of active nodes after the arrest and/or death of key actors. The AUC scores (Fig.8) also indicate that the TDRL-CNA model has higher predictive accuracy than the baseline DRL-CNA model.

The TDRL-CNA link prediction confusion matrix for the predicted network topology of the 2002 Bali Bombing (Table 2) yields a predictive accuracy of 0.704 ([88 + 0]/[88 + 34 + 0 + 3]).The accuracy score of the confusion matrix is reflective of the AUC score achieved (78%),

TABLE 2. TDRL-CNA link prediction confusion matrix for the predicted 2002 network topology.

NODE	ORIGINAL NUMBER OF EDGES	POSITIVE EDGES PREDICTED AS POSITIVE	POSITIVE EDGES PREDICTED AS NEGATIVE	NEGATIVE EDGES PREDICTED AS NEGATIVE	NEGATIVE EDGES PREDICTED AS POSITIVE
151	12	0	0	0	0
153	16	0	0	0	0
155	19	6	0	0	1
160	25	7	2	0	0
162	16	1	1	0	0
163	19	4	1	0	0
175	17	0	1	0	0
176	13	6	1	0	0
177	11	0	1	0	0
180	11	0	2	0	0
183	17	3	0	0	0
189	7	1	1	0	0
524	10	7	1	0	0
588	6	6	0	0	0
590	2	2	2	0	0
650	4	2	0	0	2
1503	7	4	0	0	0
1512	7	2	5	0	0
1513	7	4	0	0	0
1529	6	4	0	0	0
1532	9	7	1	0	0
1549	10	0	1	0	0
1564	13	2	1	0	0
1576	12	3	2	0	0
1579	14	4	0	0	0
1594	7	7	0	0	0
1597	18	6	11	0	0
TOTAL		88	34	0	3

which indicates that, although the TDRL-CNA model may not achieve a high link prediction accuracy score, the TDRL-CNA model trained on the temporal dataset is more accurate than the baseline DRL-CNA model trained on a specific timestamped dataset in the prediction of edges.

An analysis of the top 4 features contributing to the accuracy of the TDRL-CNA model trained (Fig.9) indicates that the number of common neighbours and the number of edges changed provide the most significant effect on the ranking of nodes identified for the tree search process in the prediction of the appearance and disappearance of edges over time.
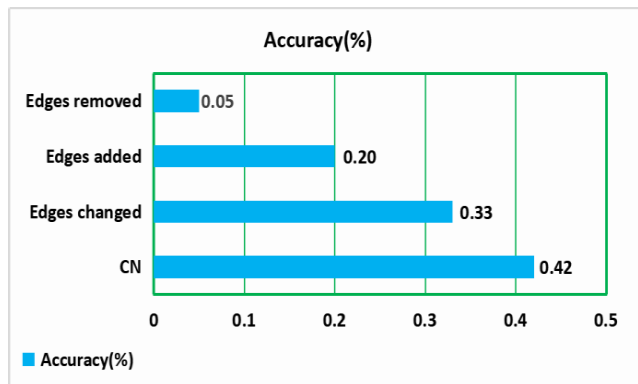
FIGURE 9. Analysis of features contributing to the TDRL-CNA model predictive accuracy.

TABLE 3. Topological statistics of features contributing to TDRL-CNA model accuracy.

Node	Original Number of Edges	Positive Edges Predicted as Positive	Positive Edges Predicted as Negative	Negative Edges Predicted as Negative	Negative Edges Predicted as Positive
151	12	0	0	0	0
153	16	0	0	0	0
155	19	6	0	0	1
160	25	7	2	0	0
162	16	1	1	0	0
163	19	4	1	0	0
175	17	0	1	0	0
176	13	6	1	0	0
177	11	0	1	0	0
180	11	0	2	0	0
183	17	3	0	0	0
189	7	1	1	0	0
524	10	7	1	0	0
588	6	6	0	0	0
590	2	2	2	0	0
650	4	2	0	0	2
1503	7	4	0	0	0
1512	7	2	5	0	0
1513	7	4	0	0	0
1529	6	4	0	0	0
1532	9	7	1	0	0
1549	10	0	1	0	0
1564	13	2	1	0	0
1576	12	3	2	0	0
1579	14	4	0	0	0
1594	7	7	0	0	0
1597	18	6	11	0	0
Total		88	34	0	3

The feature analysis (Fig.9) also indicates that feature learning based on the edges removed has the least significant effect on the predictive accuracy of the TDRL-CNA model. This finding could be attributed to the characteristics of the Bali Bombing dataset, where the number of nodes and edges removed prior to the bombing is small (Table 3).

V. CONCLUSION

The proposed TDRL-CNA link prediction model was constructed to identify the links or edges that might appear and disappear from the network over time. In the field of CNA, there seems to be little evidence that the proposed time-based link prediction model has been constructed leveraging on DRL. Although the link prediction model developed was successful in predicting the appearance of links over time, the prediction of negative links has not been precise, which could be attributed to the properties of the dataset selected for training. However, the TDRL-CNA model has been observed to provide higher predictive accuracy than the baseline DRL-CNA model when applied on a temporal dataset. This research has also found that DRL technique could be leveraged to train ML models in other domain areas where datasets are insufficiently large by simulating self-generated dataset built on the rules operating in that domain.

VI. FUTURE WORK

The trajectory of this research in the future will factor the incorporation of data fusion from data sources related to CNA, e.g. judicial judgements, death, arrests and phone tapping, to evaluate the effect of data fusion on the predictive accuracy of the link prediction model. It is expected that the inclusion of such peripheral information sources will contribute to the development of a link prediction model with better predictive accuracy, which can improve criminal network disruption operations by law enforcement agencies. Additionally, future plans will also include devising specific SNA in the formulation of weights to improve the precision of classification algorithms built into the TDRL-CNA model.

REFERENCES

[1] K. Yao, G. Zweig, M.-Y. Hwang, Y. Shi, and D. Yu, "Recurrent neural networks for language understanding," in *Proc. INTERSPEECH*, 2013.

[2] Y. Li, "Deep reinforcement learning: An overview," Sep. 2017, *arXiv:1701.07274*. [Online]. Available: https://arxiv.org/abs/1701.07274

[3] A. Hannun, C. Case, J. Casper, B. Catanzaro, G. Diamos, E. Elsen, R. Prenger, S. Satheesh, S. Sengupta, A. Coates, and A. Y. Ng, "Deep speech: Scaling up end-to-end speech recognition," 2014, *arXiv:1412.5567*. [Online]. Available: https://arxiv.org/abs/1412.5567

[4] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*. [Online]. Available: https://arxiv.org/abs/1409.1556

[5] J. Xu and H. Chen, "Criminal network analysis and visualization," *Commun. ACM*, vol. 48, no. 6, pp. 100–107, 2005.

[6] M. G. Campana and F. Delmastro, "Recommender systems for online and mobile social networks: A survey," *Online Social Netw. Media*, vol. 3, pp. 75–97, Oct. 2017.

[7] T. Almanie, R. Mirza, and E. Lor, "Crime prediction based on crime types and using spatial and temporal criminal Hotspots," 2015, *arXiv:1508.02050*. [Online]. Available: https://arxiv.org/abs/1508.02050

[8] U. Sharan and J. Neville, "Exploiting time-varying relationships in statistical relational models," in *Proc. 9th WebKDD 1st SNA-KDD Workshop Web Mining Social Netw. Anal.*, New York, NY, USA, 2007, pp. 9–15.

[9] A. A. Lim, N. Z. Jhanjhi, and M. Supramaniam, "Hidden link prediction in criminal networks using the deep reinforcement learning technique," *Computers*, vol. 8, no. 1, p. 8, 2019.

[10] S. P. Borgatti, M. G. Everett, and L. C. Freeman, *UCINET 6 for Windows: Software for Social Network Analysis*. Harvard, MA, USA: Analytic Technologies, 2002.

[11] D. Liben-Nowell and J. Kleinberg, "The link prediction problem for social networks," in *Proc. 12th Int. Conf. Inf. Knowl. Manage. (CIKM)*, New York, NY, USA, 2003, pp. 556–559.

[12] S. K. Dash, I. Safro, and R. S. Srinivasamurthy, "Spatio-temporal prediction of crimes using network analytic approach," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 1912–1917.

[13] A. Clauset, C. Moore, and M. Newman, "Hierarchical structure and the prediction of missing links in networks," *Nature*, vol. 453, no. 7191, pp. 98–101, 2008.

[14] C. Wang, V. Satuluri, and S. Parthasarathy, "Local probabilistic models for link prediction," in *Proc. 7th IEEE Int. Conf. Data Mining (ICDM)*, Oct. 2007, pp. 322–331.

[15] T. Murata and S. Moriyasu, "Link prediction of social networks based on weighted proximity measures," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI)*, Washington, DC, USA, Oct. 2007, pp. 85–88.

[16] A. Potgieter, K. April, R. Cooke, and I. Osunmakinde, "Temporality in link prediction: Understanding social complexity," in *Proc. Sprouts, Work. Papers Inf. Syst.*, 2007, vol. 7, no. 9.

[17] J. O'Madadhain, J. Hutchins, and P. Smyth, "Prediction and ranking algorithms for event-based network data," *ACM SIGKDD Explor. Newslett.*, vol. 7, no. 2, pp. 23–30, 2005.

[18] Z. Huang and D. Lin, "The time-series link prediction problem with applications in communication surveillance," *INFORMS J. Comput.*, vol. 21, no. 2, pp. 286–303, 2008.

[19] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. Riedmiller, A. K. Fidjeland, G. Ostrovski, S. Petersen, C. Beattie, A. Sadik, I. Antonoglou, H. King, D. Kumaran, D. Wierstra, S. Legg, and D. Hassabis, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, 2015.

[20] H. Li, N. Kumar, R. Chen, and P. Georgiou, "A deep reinforcement learning framework for Identifying funny scenes in movies," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2018, pp. 3116–3120.

[21] T. Anthony, Z. Tian, and D. Barber, "Thinking fast and slow with deep learning and tree search," Dec. 2017, *arXiv:1705.08439*. [Online]. Available: https://arxiv.org/abs/1705.08439

[22] D. Silver, J. Schrittwieser, K. Simonyan, I. Antonoglou, A. Huang, A. Guez, T. Hubert, L. Baker, M. Lai, A. Bolton, Y. Chen, T. Lillicrap, F. Hui, L. Sifre, G. van den Driessche, T. Graepel, and D. Hassabis, "Mastering the game of go without human knowledge," *Nature*, vol. 550, no. 7676, pp. 354–359, 2017.

[23] D. Silver, T. Hubert, J. Schrittwieser, I. Antonoglou, M. Lai, A. Guez, M. Lanctot, L. Sifre, D. Kumaran, T. Graepel, T. Lillicrap, K. Simonyan, and D. Hassabis, "A general reinforcement learning algorithm that masters chess, shogi, and go through self-play," *Science*, vol. 362, no. 6419, pp. 1140–1144, 2018, doi: 10.1126/science.aar6404.

[24] E. Budur, S. Lee, and V. S. Kong, "Structural analysis of criminal network and predicting hidden links using machine learning," Sep. 2015, *arXiv:1507.05739*. [Online]. Available: https://arxiv.org/abs/1507.05739

[25] P. J. Zufiria and I. Barriales-Valbuena, "Evolution models for dynamic networks," in *Proc. 38th Int. Conf. Telecommun. Signal Process. (TSP)*, Prague, Czech Republic, Jul. 2015, pp. 252–256.

[26] L. Wang, K. Hu, and Y. Tang, "Robustness of link-prediction algorithm based on similarity and application to biological networks," *Current Bioinf.*, vol. 9, no. 3, pp. 246–252, 2014.

[27] M. Lim, A. Abdullah, and N. Z. Jhanjhi, "Performance optimization of criminal network hidden link prediction model with deep reinforcement learning," *J. King Saud Univ.-Comput. Inf. Sci.*, Jul. 2019.

[28] U. Sharma and B. Minocha, "Link prediction in social networks: A similarity score based neural network approach," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies*, 2016, p. 90.

[29] N. Sett, S. R. Singh, and S. Nandi, "Influence of edge weight on node proximity based link prediction methods: An empirical analysis," *Neurocomputing*, vol. 172, pp. 71–83, Jan. 2016.

MARCUS LIM received the M.S. degree in business information system from the University of East London, in 2016. He is currently pursuing the Ph.D. degree in computer science with Taylors University.

AZWEEN ABDULLAH is currently working with Taylor's University. He is currently a Professional Development Alumni of Stanford University and MIT. His work experience includes 30 years as an academic in institutions of higher learning and as the Director of research and academic affairs at two institutions of higher learning, the Vice-President for educational consultancy services, 15 years in commercial companies as a Software Engineer, a Systems Analyst, and as a Computer Software Developer and a IT/MIS consultancy and training.

NZ JHANJHI received the Ph.D. degree in IT from UTP, Malaysia. He has great international exposure in academia, research, administration, and academic quality accreditation. He was with ILMA University, King Faisal University (KFU) for a decade. He is currently with Taylors University, Malaysia. He has 19 years of teaching and administrative experience. He has an intensive background of academic quality accreditation in higher education besides scientific research activities. He had worked a decade for academic accreditation. He received ABET accreditation twice for three programs from CCSIT, King Faisal University, Saudi Arabia. He also worked for National Commission for Academic Accreditation and Assessment (NCAAA), Education Evaluation Commission Higher Education Sector (EECHES) formerly NCAAA Saudi Arabia, for institutional level accreditation. He also worked for National Computing Education Accreditation Council (NCEAC).

Dr. Noor Zaman has awarded as top Reviewer 1% globally by WoS/ISI (Publons) recently. He has edited/authored more than 11 research books with international reputed publishers, received several research grants, and a great number of indexed research articles on his credit. He has supervised several postgraduate students, including master's and Ph.D. He is an Associate Editor of IEEE Access, Keynote speaker for several the IEEE international conferences globally, External examiner/evaluator for Ph.D. and master's for several universities, Guest editor of several reputed journals, a member of the editorial board of several research journals, and an active TPC member of reputed conferences around the globe.

MUHAMMAD KHURRAM KHAN is currently a Professor of cybersecurity with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia. He is one of the founding members of CoEIA. He has served as the Manager R&D, from 2009 to 2012. He, along with his team, developed and successfully managed Cybersecurity research program of CoEIA, which turned the center as one of the best centers of excellence in the region. He is a founder and the CEO of the Global Foundation for Cyber Studies and Research, an independent, non-profit, and non-partisan cybersecurity think-tank in Washington, DC, USA, which explores and addresses global cyberspace challenges from the intersecting dimensions of policy and technology. He has published more than 350 research articles in the journals and conferences of international repute. In addition, he is an Inventor of 10US/PCT patents. He has edited seven books/proceedings published by Springer-Verlag and IEEE. He has secured several national and international competitive research grants in the domain of Cybersecurity. He has played a Leading Role in developing BS Cybersecurity Degree Program and Higher Diploma in Cybersecurity, King Saud University. His research areas of interest are cybersecurity, digital authentication, the IoT security, cyber policy, and technological innovation management. Prof. Khurram Khan is a member of the IEEE Consumer Electronics Society, the IEEE Communications Society, the IEEE Technical Committee on Security and Privacy, the IEEE IoT Community, the IEEE Smart Cities Community, and the IEEE Cybersecurity Community; a Senior Member of the IACSIT, Singapore; a Fellow of the IET, U.K., BCS, U.K., and FTRA, South Korea. Moreover, he is one of the organizing chairs of more than five dozen international conferences and a member of technical committees of more than ten dozen international conferences. He has secured Outstanding Leadership Award at the 2009 IEEE International Conference on Networks and Systems Security, Australia.

Besides, he has received certificate of appreciation for outstanding contributions in Biometrics & Information Security Research at the AIT international Conference, Japan, in June 2010. He was awarded a Gold Medal for the Best Invention & Innovation Award at 10th Malaysian Technology Expo 2011, Malaysia. Moreover, in April 2013, his invention has received a Bronze Medal at 41st International Exhibition of Inventions at Geneva, Switzerland. In addition, he was awarded Best Paper Award from the *Journal of Network and Computer Applications* (Elsevier), in December 2015. He is the Vice Chair of IEEE Communications Society Saudi Chapter. He is a Distinguished Lecturer of the IEEE. He is the Editor-in-Chief of a well-reputed International journal *Telecommunication Systems* published by Springer for over 26 years with its recent impact factor of 1.707 (JCR 2019). Furthermore, he is on the editorial board of several international journals, including, the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, the IEEE COMMUNICATIONS MAGAZINE, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the *Journal of Network and Computer Applications* (Elsevier), IEEE ACCESS, the *IEEE Consumer Electronics Magazine*, *PLOS One*, *Electronic Commerce Research*, *IET Wireless Sensor Systems*, the *Journal of Information Hiding and Multimedia Signal Processing*, and the *International Journal of Biometrics*. He has also played role of the Guest Editor of several international journals of IEEE, Springer, Wiley, and Elsevier Science.

MAHADEVAN SUPRAMANIAM received the D.B.A. degree from the Twintech International University College of Technology, Malaysia, and the master's degree in software engineering from the University of Malaya. He serves as the Director of the Research and Innovation Management Centre, Institute of Graduate Studies, SEGi University and Colleges. His expertise include R&D Development and Policies, Enterprise Resource Planning, Computer Science & Security Systems, Business Process Management, and Integrated Technologies for industries. He has shared most of his experiences on his expertise area through public talks and has written many articles and books which have been published all over the world.

• • •