

Link Prediction Methods for Complex Illicit Networks: A Systematic Review

Hasini Balasuriya

hmabala02@louisville.edu

University of Louisville

Monica Gentili

University of Louisville

Naoru Koizumi

George Mason University

Systematic Review

Keywords: link prediction, illicit networks, dynamic networks, social network analysis

Posted Date: April 17th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-9431584/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License. [Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Link Prediction Methods for Complex Illicit Networks: A Systematic Review

Hasini Balasuriya^{1*}, Monica Gentili¹ and Naoru Koizumi²

^{1*}Department of Industrial & Systems Engineering, University of Louisville, Louisville, Kentucky, USA.

²Schar School of Policy and Government, George Mason University, Arlington, Virginia, USA.

Abstract

Illicit trades, organized crime, trafficking, and terrorism remain major threats to global security, yet the networks that sustain these activities are difficult to study because available data are typically secondary, incomplete, and strategically concealed. In such settings, link prediction becomes important for inferring missing or unobserved relationships from network structure and associated attributes. This paper presents a systematic review focused on link prediction in illicit networks. We synthesize the network representations, input features, models, and evaluation practices used across the existing literature, and critically examine how different link prediction methods have been adapted to the complex, covert, dynamic, and incomplete nature of illicit systems. The review shows that current studies span a wide range of illicit contexts and employ diverse methodological approaches, from similarity-based indices to graph neural networks and learning-based methods. However, the literature remains fragmented and is still dominated by static formulations, limited data settings, and evaluation strategies that do not fully reflect real-world investigative conditions. We identify major methodological and empirical gaps, including strong closed-world assumptions, and insufficient attention to robustness and uncertainty. The review concludes by outlining key directions for future research aimed at developing more realistic, interpretable, and operationally useful link prediction models for illicit-network analysis.

Keywords: link prediction, illicit networks, dynamic networks, social network analysis

1 Introduction

Illicit operations, including human trafficking, drug trafficking, organized crime, and terrorism, pose serious threats to global security, governance, and stability. Human trafficking alone affects around 27 million people globally, generating roughly \$236 billion each year from forced labor and sexual exploitation ([International Labour Organization 2024](#)). In addition to the aforementioned trafficking operations, several other profit-driven and politically motivated criminal markets, such as counterfeiting, arms smuggling, mafia syndicates, and terrorism, continue to fuel global instability and violence. According to the Global Financial Crime Report ([Nasdaq and Verafin 2024](#)), an estimated \$3.1 trillion in illicit funds circulated through the global financial system in 2023. Through frameworks like the UN Convention against Transnational Organized Crime (UNTOC) and the UN Sustainability Goals, the global community has explicitly committed to dismantling these illicit operations ([UNTOC 2024](#); [WHO 2024](#)). Hence, understanding the scale and nature of these illicit operations is essential for developing effective strategies to detect, prevent, and combat them.

Illicit networks comprise individuals or groups engaged in illegal activities for financial or material gain. They often use decentralized structures to ensure resilience and are designed to remain hidden with redundant connections and withstand disruption, unlike any other social network ([Logan et al. 2009](#); [Sparrow 1991](#)). Trafficking operations, at the same time, could be highly organized, often transnational, and involved in the illegal trade of humans, drugs, organs, wildlife, or other illicit goods ([Konrad et al. 2017](#); [Logan et al. 2009](#); [Wang et al. 2025](#); [Diviák 2022](#); [Sharkey et al. 2024](#)).

A growing body of qualitative research has shed light on the social context of criminal and trafficking networks, emphasizing how inequality, corruption, and limited opportunities facilitate their expansion ([Islam 2024](#); [Barrick et al. 2024](#); [Martin et al. 2023](#); [Russell 2018](#); [Morselli 2009](#); [Catino 2014](#)). This type of research highlights the psychological and social consequences of exploitation. They have also examined and documented grassroots interventions and gaps in local law enforcement ([Macaveiu et al. 2024](#); [Martin et al. 2024](#)). But they lack the quantitative rigor necessary for designing policies or large-scale disruption strategies. In response, many quantitative studies have focused on descriptive analyses of illicit network data, applying Operations Research (OR) methods and Social Network Analysis (SNA) to uncover hidden patterns and key structural characteristics ([Konrad et al. 2017](#); [Sharkey et al. 2024](#); [Dimas et al. 2022](#); [Wright et al. 2006](#)). By representing these networks as graphs, these tools allow researchers to identify critical structural patterns, such as (i) central actors or individuals who dominate information flow, using degree or betweenness centrality measures ([Ficara et al. 2020](#)), (ii) tightly knit clusters found using community detection methods ([Keskin et al. 2021](#); [Yang 2023a](#); [Isah et al. 2015](#)), and (iii) vulnerabilities that could disrupt the network’s operations by simulating the removal of central actors or connections to determine how the network might fragment under pressure ([Ficara et al. 2021](#)).

The main limitation of existing quantitative research on illicit networks is that it tends to remain descriptive, rather than capturing the dynamic nature of these networks. In reality, illicit networks are highly adaptive, continuously reorganizing in response to external pressures such as law enforcement interventions. Studying them

is further complicated by the fact that available data is typically sparse, fragmented, and incomplete, a consequence of the covert and hidden nature of these organizations (Diviák 2022; Dimas et al. 2022; Ficara et al. 2021). Addressing the challenges posed by limited and unreliable data is, therefore, critical for understanding both the scale and the adaptive behavior of illicit networks. However, primary data collection is extremely difficult, as individuals involved in such networks are incentivized to avoid detection, and the disclosure of information about their collaborators would compromise their operational secrecy (Diviák 2022; Dimas et al. 2022; Ficara et al. 2021).

To address this, *predictive tools in SNA* can be used to infer missing or potential information about network structure (Diviák 2022). Techniques such as link prediction and network reconstruction can help estimate unobserved relationships and recover parts of the network that are not captured in the available data. **Link prediction** plays a key role in understanding missing connections in a given network. It is a technique used to estimate the likelihood of a link existing or forming between two nodes based on the observed structure of the network (Liben-Nowell and Kleinberg 2003; Kumar et al. 2020; Arrar et al. 2024; Samad et al. 2020; Yang et al. 2015). For comprehensive insights into link prediction methods in general, you may refer to studies by Kumar et al. (2020), Yang et al. (2015), Arrar et al. (2024), and Samad et al. (2020), which provide a detailed overview of LP methods. Link prediction has been applied in many social network domains, such as co-authorship networks, recommender systems, and in biological networks and bioinformatics (Kumar et al. 2020; Samad et al. 2020), but it is under-explored in the context of illicit networks.

This paper investigates **the application of link prediction methods on illicit networks**. To the best of our knowledge, this is the first systematic review of studies focusing on LP methods in this context.

To guide this review, we address the following research questions:

- **RQ1:** How are illicit networks represented for link prediction, and what structural and attribute data are used as inputs?
- **RQ2:** Which link prediction methods have been applied to illicit networks, and how well do they match the structural and operational characteristics of these networks?
- **RQ3:** To what extent do existing studies account for the dynamic, multilayer, incomplete, and covert nature of illicit networks?
- **RQ4:** How are link prediction models in illicit networks evaluated, and to what extent do existing evaluation criteria reflect the specific challenges of illicit-network settings?
- **RQ5:** What key methodological, data, and evaluation gaps remain, and what directions should future research prioritize?

The rest of the paper is structured as follows: Section 2 outlines the systematic review methodology; Section 3 defines the LP problem; Section 4 includes a review of datasets and data types used for LP models, a critical review of existing LP models and discusses the evaluation criteria used to assess their performance; Section 5 discusses the findings; and Section 6 offers conclusions and four promising future research directions.

2 Research Methodology

This study was conducted as a systematic literature review of link prediction studies for illicit networks, using a structured review approach consistent with the methodology proposed by [Sauer and Seuring \(2023\)](#). The review was guided by clearly defined research questions, explicit search terms, predefined inclusion and exclusion criteria, and a staged study-selection process. Because the included studies varied substantially in the illicit domain, dataset, network representation, and prediction method, the evidence was synthesized qualitatively rather than through meta-analysis.

2.1 Search strategy

A literature search was conducted across Google Scholar, Scopus, IEEE Xplore, ScienceDirect, SpringerLink, Taylor & Francis Online, and Emerald Insight. Searches were conducted up to August 2025. The search strategy combined two concept groups: link-prediction terminology and illicit-network terminology. The link-prediction block included terms such as “link prediction,” “edge prediction,” “missing link,” “hidden link,” “future link,” “latent link,” and “link mining.” The illicit-network block included terms such as “illicit network,” “criminal network,” “crime network,” “covert network,” “dark network,” “trafficking network,” “terrorist network,” “mafia,” “drug trafficking,” “human trafficking,” “money laundering,” “counterfeit,” and “corruption.” Broader terms such as “link analysis” and “graph analysis” were used only during exploratory searching; however, studies were retained only when link prediction was a substantive analytical task.

2.2 Eligibility criteria

To ensure a focused and consistent review, the retrieved studies were then assessed using predefined inclusion and exclusion criteria. These criteria were used to determine which papers were sufficiently relevant to the aims of the review.

Table 1 summarizes the inclusion and exclusion criteria used for study screening.

2.3 Screening and study selection

Search results from the selected databases were merged, and duplicate records were removed. This process resulted in 75 unique candidate records. The study selection process was conducted in two stages using the eligibility criteria defined above. In the first stage, titles and abstracts were screened to exclude 21 records that were clearly outside the scope of the review, such as studies unrelated to illicit or crime-related networks and those focused on general network or link analysis without an explicit prediction task. In the second stage, the remaining 54 papers were assessed in full text against the full set of inclusion and exclusion criteria, including relevance to illicit-network link prediction, the presence of a substantive link prediction task, and the availability of sufficient methodological detail for comparison. 36 papers were excluded at this stage and the final review corpus comprised 18 studies. They are Kaza et al. (2007a), Kaza et al. (2007b), Berlusconi et al. (2016), Mahesar et al. (2016), Marciani et al. (2017), Bahulkar et al. (2018), Crandell and Korkmaz (2018), Lim et al. (2019),

Table 1 Inclusion and exclusion criteria used for study screening

Category	Criterion
Inclusion	Studies that explicitly addressed a link prediction task, including missing, hidden, latent, future, or hyperedge links.
Inclusion	Studies focused on illicit, criminal, covert, trafficking, terrorist, corruption, money-laundering, counterfeit, or related crime networks.
Inclusion	Primary empirical studies published as journal articles, conference papers, or preprints with accessible full text.
Inclusion	Studies reporting sufficient methodological detail on the dataset or application setting, network construction, and prediction method.
Inclusion	Studies written in English.
Exclusion	Studies on crime prediction, hotspot prediction, or incident forecasting without an explicit link prediction task.
Exclusion	Studies on link analysis, network analysis, community detection, or disruption analysis that only describe existing network structure.
Exclusion	Studies on network reconstruction where link prediction was not a main focus of the paper.
Exclusion	Studies outside illicit or crime-related applications.
Exclusion	Reviews, editorials, theses, duplicate records, and studies with insufficient methodological detail.

Su et al. (2019), Calderoni et al. (2020), Lim et al. (2020), Assouli et al. (2021), Qiao et al. (2021), Lopes et al. (2022), Ribeiro et al. (2023), Ahmadi et al. (2023), Aktas et al. (2023), and Yang (2023b).

2.4 Data extraction and synthesis

For each included study, data were extracted on the illicit application domain, dataset, network size or structure, node and edge definitions, input data types, link prediction method, and whether the prediction setting was static or temporal. We also recorded the main analytical objective of each study, modeling specificities, and evaluation criteria. These extracted elements directly support the structure of the review in the following sections, namely the analysis of datasets and data types, the evaluation of link prediction model classes, model evaluation criteria used, and the identification of methodological gaps and future research directions.

3 Link Prediction Problem Characterization

Link prediction is a method of identifying links between unconnected pairs of nodes in a given network. Researchers often work with datasets that may include temporal information or opt to consolidate data over a period of time to remove the temporal aspect. Depending on whether the temporal aspect of the network is considered, link prediction is categorized into static link prediction (SLP) and temporal link prediction (TLP). These two approaches differ in their assumptions, methodologies, and suitability for different types of networks. The earliest formal definition of link prediction was

provided in 2003 by Liben-Nowell and Kleinberg (2003). The problem can be defined as follows:

Link Prediction Problem (Static).

Given an undirected graph $G = (V, E)$ where V is the set of nodes and E is the set of edges, the link prediction problem aims to predict whether there is a link $e(u, v)$ between a pair of nodes u, v where $u \neq v$, $u, v \in V$, and $e(u, v) \notin E$ (Yang 2023b).

Figure 1 illustrates a simple static link prediction problem. In this example, node A connects to nodes B, C, and D, but B and C are not directly connected; their shared neighbor suggests a potential link. Static link prediction uses such structural properties from a single network snapshot to estimate the likelihood of missing connections like BC, CD, or BD. Temporal link prediction (TLP) considers a sequence of network

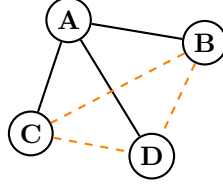


Fig. 1 An illustrative example of a static link prediction problem.

snapshots over time $(1, 2, \dots, T)$ to estimate the likelihood of links that may appear in the next state $T + 1$. As shown in Figure 2, the network evolves with changes in the connections among nodes. TLP uses these historical patterns to forecast future connections, capturing dynamics that static methods overlook. The dotted red edges in the figure illustrate anticipated links at time $T + 1$. The definition of TLP is as follows:

Temporal Link Prediction Problem.

Given a sequence of graph snapshots of G represented as $G_1, G_2, \dots, G_T$ over time stamps 1 to T , where each snapshot $G_t = (V, E_t)$, the temporal link prediction aims to predict the graph snapshot G_{T+1} at time $T + 1$ (Zhang et al. 2022).

The field of link prediction methods has evolved significantly and now includes a variety of approaches ranging from conventional statistical methods to advanced Machine Learning (ML) and Deep Learning (DL) models.

4 Evaluation of Literature

4.1 Overview of Existing Link Prediction Studies in Illicit Networks

Existing work on link prediction in illicit networks spans a range of domains, reflecting the diversity of criminal and covert structures. Broadly, these studies can be grouped into investigations of Mafia and organized crime, terrorist networks, drug trafficking, corruption, money laundering, and other crime-related contexts.

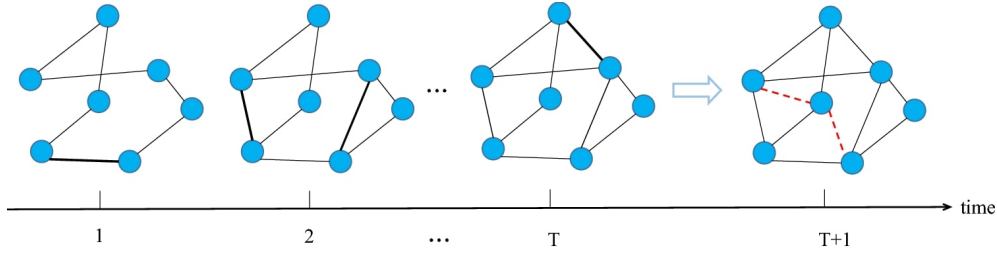


Fig. 2 An illustrative example of temporal link prediction (Zhang et al. 2022)

Organized crime and Mafia studies, such as those drawing on Italian anti-mafia operations, have used datasets built from judicial documents, meetings, and communication records. These works examine how similarity-based and embedding models can recover incomplete information and highlight short-path interactions within dense clusters (Calderoni et al. 2020; Bahulkar et al. 2018). In drug trafficking contexts, particularly the CAVIAR and Ndrangheta investigations, link prediction has been used to understand evolving connections and enhance community detection by uncovering intentionally hidden relationships (Bahulkar et al. 2018; Lim et al. 2020).

By predicting missing edges in known terrorist structures such as the September 11 hijacker network, LP has been applied to simulate incomplete intelligence and guide strategies for disintegration of networks through targeting critical nodes. Studies relying on global terrorism datasets further extend this line of work by proposing reliability metrics to identify strong candidate links between perpetrators, groups, or attacks (Su et al. 2019; Assouli et al. 2021).

Corruption and money-laundering investigations have leveraged LP to map ties between individuals, companies, and transactions in Spain, Brazil, and broader federal police datasets. These networks often encode multirelational interactions such as political scandals, financial exchanges, or criminal-personal ties, and studies have utilized LP to predict missing partnerships, classify relationships, and detect illicit financial flows (Yang 2023b; Lopes et al. 2022; Ribeiro et al. 2023). Similar work in general crime networks, using case records or arrest data, has focused on predicting whether individuals will engage in new incidents by combining social proximity with individual attributes (Crandell and Korkmaz 2018).

Other applications extend beyond traditional crime, such as counterfeit cigarette shipments in logistics networks. Here, time-series features of delivery patterns are combined with graph-based measures to train classifiers that identify high-risk packages, demonstrating the adaptability of LP beyond person-to-person criminal ties (Qiao et al. 2021).

Overall, these studies highlight both the breadth of domains where LP has been applied and the methodological diversity of approaches. Whether reconstructing incomplete Mafia data, disrupting terrorist cells, or tracing financial crime, the common goal is to exploit network structure, sometimes complemented by metadata or temporal information, to predict unobserved or future connections (Yang 2023b; Calderoni et al. 2020; Bahulkar et al. 2018; Lim et al. 2020; Su et al. 2019; Assouli

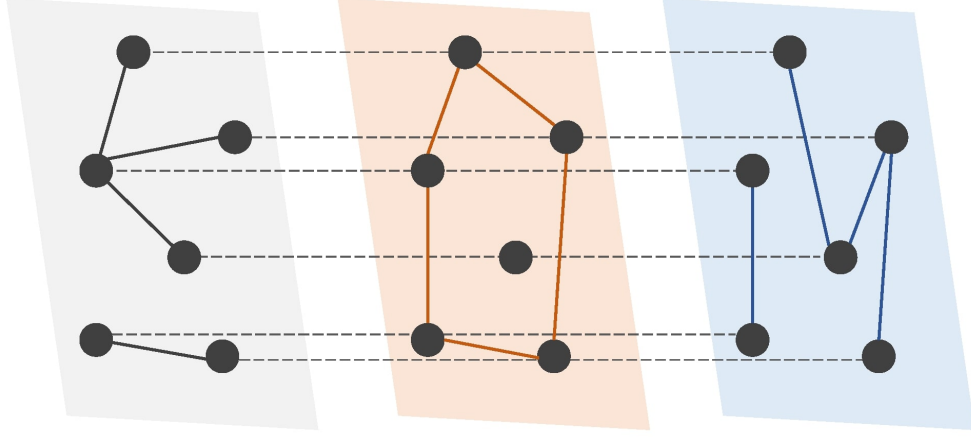


Fig. 3 A schematic illustration of a multiplex network consisting of three layers and six nodes. In this structure, the same set of nodes is present across all layers, with each layer capturing a different type of relationship between nodes. Additionally, interlayer links connect each node to its corresponding counterparts in the other layers (Yu et al. 2023)

et al. 2021; Lopes et al. 2022; Ribeiro et al. 2023; Crandell and Korkmaz 2018; Qiao et al. 2021).

4.2 Methods of Network Representation of Illicit Networks

In illicit network research, the design of nodes and edges of the network defines how link prediction can be applied. Nodes often represent individuals directly involved in illicit activity, such as suspects, offenders, or victims but can also extend to organizations, companies, locations, or digital entities like social media posts and darknet advertisements (Calderoni et al. 2020; Su et al. 2019; Ribeiro et al. 2023; Berlusconi et al. 2016). Broadening the definition of nodes acknowledges that illicit operations frequently involve intermediaries and non-human actors, particularly in financial crime and trafficking contexts.

Edges capture interactions or relationships between nodes, including communication, financial transactions, co-participation in criminal events, or movement across locations. They can be unweighted or weighted (e.g., by transaction amount), and in some cases classified into legal, criminal, or mixed ties to distinguish the nature of interactions (Su et al. 2019; Ribeiro et al. 2023). This flexibility allows illicit networks to reflect both the overt and covert ties that sustain criminal enterprises.

Beyond traditional pairwise connections, recent studies explore hypergraph modeling, which enables edges to link multiple nodes simultaneously. This is particularly useful for crime events influenced by overlapping spatial, temporal, and categorical factors. For example, UniMHe, a model developed by Aktas et al. (2023), introduces hyperedges that group crimes by shared context, such as location, crime type, or season, allowing models to capture higher-order interactions that standard graphs miss.

4.3 Flat vs. Multilayer Networks

The majority of the existing studies have only studied the networks as flat structures, but there are more advanced approaches to LP, which examine networks in a more complex manner, such as multilayer network-based LP. These methods extend the traditional single-layer analysis by considering interactions across multiple layers, thereby enabling richer and more nuanced predictions on illicit networks (Arrar et al. 2024).

Multi-layer networks (also referred to as multiplex networks) model systems where the same set of nodes interact through different types of relationships across multiple “layers” (Boccaletti et al. 2014). Each layer captures a distinct interaction, such as physical, social, or temporal ties, allowing interdependencies to be modeled explicitly. This design reveals insights missed in flat networks, where all ties are collapsed into one layer (Figure 3). For example, Yu et al. (2023) compares two criminal multiplex networks: a Canadian drug trafficking system and a Sicilian Mafia network. The Canadian network includes actors linked through drug transactions, business partnerships, organizational membership, and kinship ties, each represented in different layers. In the Mafia case, nodes are individuals, with one layer capturing in-person meetings and another recording phone communications. While this study addresses the broader challenge of network reconstruction, which is about recovering both missing nodes and links, it demonstrates how multilayer structures better represent the complex relational patterns of covert groups compared to flat networks.

4.4 Different Input Data Types to LP Models

In our analysis, we broadly categorize the input data types into two main groups based on their characteristics and content: (i) structural data and (ii) attribute data/metadata. These data often act as features in advanced link prediction models. Table 2 provides an overview of the datasets analyzed for link prediction in the reviewed studies, summarizing their network sizes, type of illicit activity, and indicating which datasets are publicly available.

4.4.1 Structural Data

Structural data forms the foundational layer of information in LP models and is derived from the topology of the network itself. It describes how nodes and edges are connected, capturing the structure of the network under study. Structural data can be further classified into two types: (i) node-specific and (ii) edge-specific. Common examples of node-specific structural data include features such as node labels, degree, or network distance. On the other hand, edge-specific data may involve features such as the level of connection, specific paths, or subgraph structures associated with a given link.

4.4.2 Attribute Data

Attribute data or metadata refers to supplementary information about nodes or edges that provides richer context than the network topology alone. Attribute data can also be classified into node attributes and edge attributes, each adding a distinct set of information to LP models. Node attributes describe properties of individual

entities within the network. These can include profiles, demographics such as sex, ethnicity, race, age, and gender (Samad et al. 2020; Ribeiro et al. 2023; Crandell and Korkmaz 2018), roles such as leader, recruiter, operative, broker, supplier, and distributor (Berlusconi et al. 2016; Yu et al. 2023), or characteristics relevant to the entities’ behavior or status such as criminal history, type of criminal activity, size of the criminal case, and location (Crandell and Korkmaz 2018; Berlusconi et al. 2016).

Edge attributes describe the properties of relationships between nodes. These may include interaction frequency (Ribeiro et al. 2023; Qiao et al. 2021; Berlusconi et al. 2016; Marciani et al. 2017; Ahmadi et al. 2023), types of relationships such as familial ties, professional collaborations, and illicit transactions (Su et al. 2019; Ribeiro et al. 2023), or edge weights that quantify the strength or significance of connections (Isah et al. 2015; Marciani et al. 2017).

There is another frequently used category of attribute data, which are derived attributes such as centrality measures (betweenness, closeness, degree) and similarity measures (local and global similarities), describing the topological characteristics of the nodes and edges of the network. These measures describe a network in a more quantifiable manner. Further description of these measures will be provided in Section 4.6.

4.5 Classification of link prediction methods in illicit networks

This section explores the major categories of link prediction methods applied to illicit networks. Most LP models reviewed fall into four broad classes: similarity-based methods, probabilistic and maximum likelihood models, dimensionality reduction techniques, and learning-based algorithms. Their classification is shown in Figure 4. Based on this taxonomy, a generic LP framework can be designed, where inputs may be graphs with or without features, and outputs are binary predictions of potential links using either classical or learning-based models (see Figure 5). Table 4 summarizes all reviewed studies, identifying the model used, its LP model category, and the study’s objective.

4.6 Similarity based methods

Similarity-based methods are one of the conventional methods of link prediction, which assign a score to each unconnected pair of nodes, estimating the likelihood of a link based on the structural similarity of the neighborhood that the two nodes share. These methods fall into three types: (i) local, (ii) global, and (iii) quasi-local. Local measures use only the immediate neighborhoods of nodes, while global measures consider the entire network. Quasi-local indices serve as a middle ground, balancing predictive accuracy with computational efficiency (Kumar et al. 2020). After computing similarity scores for all pairs, the task continues by ranking them in descending order. Pairs above a case-specific threshold are then predicted as new links. The following section reviews commonly used similarity-based methods and how they have been adapted for the illicit networks.

Table 2 A Summary of Illicit Network Datasets

Reference	Dataset Name	Type of Illicit Activity	# of Nodes	# of Edges	Data Availability
Ribeiro et al. (2023); Lopes et al. (2022)	Spanish corruption	Political Corruption Scandals	2695	N/A	Publicly available
Ribeiro et al. (2023); Lopes et al. (2022)	Brazilian corruption	Political Corruption Scandals	404	N/A	Publicly available
Ribeiro et al. (2023); Lopes et al. (2022)	Criminal intelligence network by Brazilian Federal police	Crime and Drug Trafficking	25,666	N/A	Publicly available
Ribeiro et al. (2023); Lopes et al. (2022)	Money laundering	Crime	1,126	N/A	N/A
Aktas et al. (2023)	Crime data from New York City (NYC) Open-Data	Crime	156,243	N/A	Publicly available
Ahmadi et al. (2023)	A burglary dataset from Israel National Police	Crime	23,380	42,604	N/A
Yang (2023b)	New York Police Department (NYPD) Arrests Data	Crime	245,867	312,453	Publicly available
Yang (2023b)	Chicago Crime Data	Crime	78,456	112,345	Publicly available
Qiao et al. (2021)	Counterfeit cigarettes criminality in China	Counterfeit Goods Trafficking	1,925	N/A	N/A
Lim et al. (2020), Bahulkar et al. (2018)	CAVIAR drug import syndicate	Drug Trafficking	42	N/A	Publicly available
Calderoni et al. (2020)	Montagna Meeting Graph	Crime	101	256	N/A
Calderoni et al. (2020)	Montagna Phone Call Graph	Crime	100	124	N/A
Assouli et al. (2021)	GTD terrorist dataset	Terrorism	50	239	N/A
Assouli et al. (2021)	RAND Database of Worldwide Terrorism Incidents (RDWTI)	Terrorism	100	189	N/A
Su et al. (2019)	September 11th hijackers' network	Terrorism	62	153	N/A
Crandell and Korkmaz (2018)	Albuquerque Police Dept. network	Crime	25,924	N/A	N/A
Berlusconi et al. (2016)	Crime cases of an Italian Mafia group	Crime	182	247	Publicly available

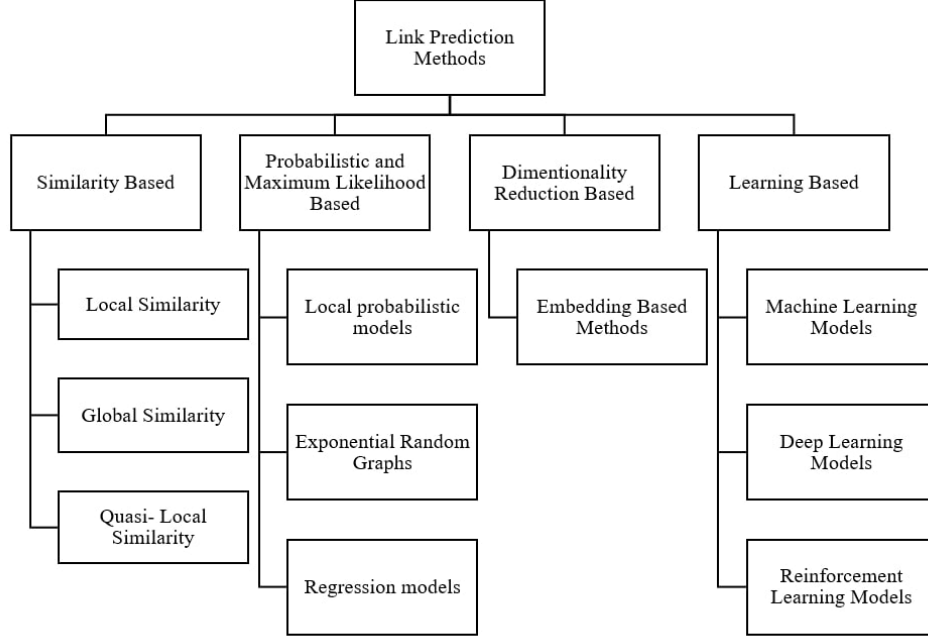


Fig. 4 Classification of Popular Link Prediction Methods used in Illicit Network Exploration

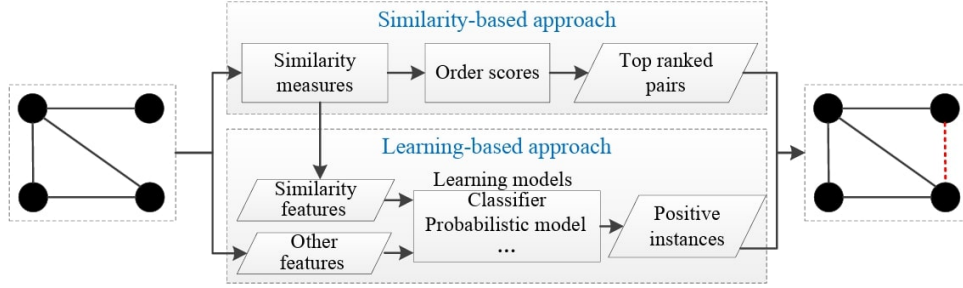


Fig. 5 Generic link prediction framework (Wang et al. 2014)

4.6.1 Local Similarity Measures

Local similarity measures rely on immediate neighborhoods to assess the likelihood of a missing or future link. Even though there are many similarity-based metrics in SNA, the reported few have been the most effective predictors for the illicit networks under study, due to their structural differences from other social networks.

Common Neighbors (CN):

$$S_{CN}(x, y) = |\Gamma(x) \cap \Gamma(y)| \quad (1)$$

where $\Gamma(\cdot)$ denotes the set of neighbors of node x and node y .

CN is one of the simplest metrics, counting the shared neighbors between two suspects x and y . Despite its simplicity, it remains a baseline in several studies. For example, [Bahulkar et al. \(2018\)](#) applied CN in their edge-augmentation process for the CAVIAR drug-trafficking network, showing it as a useful starting point before more advanced measures. They also proposed two modifications tailored to their dataset. The first, Common Neighbors Weighted by Calls, sums the total calls each suspect makes with shared neighbors, incorporating interaction intensity. More frequent calls with mutual contacts signal a stronger likelihood of hidden links. The second, Common Neighbors Weighted by Hierarchy, incorporates organizational structure by estimating a suspect’s rank through communication with supervisors. Large differences in such communication imply different hierarchy levels, reducing the chance of direct links, whereas similar patterns suggest comparable ranks and higher likelihood of direct ties. [Calderoni et al. \(2020\)](#) also applied CN and related measures to two Sicilian Mafia networks from the Montagna anti-mafia operation, covering meetings and phone calls among suspects. CN performed strongly on the denser meeting graph (Area Under the Receiver Operating Characteristic Curve, AUROC ≈ 0.94 to 0.95) but dropped to about 0.60 on the sparser phone-call graph, highlighting how its effectiveness depends heavily on network density and clustering.

Jaccard Coefficient (JC):

$$S_{JC}(x, y) = \frac{|\Gamma(x) \cap \Gamma(y)|}{|\Gamma(x) \cup \Gamma(y)|} \quad (2)$$

This ratio measures the proportion of common neighbors of x and y .

[Calderoni et al. \(2020\)](#) also analyzed the Jaccard index as a normalized measure, where it was noted that if node degrees are low or the network has only scattered common neighbors, Jaccard can lose discriminative power.

Adamic-Adar (AA):

$$S_{AA}(x, y) = \sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{1}{\log k_z} \quad (3)$$

This index sums the contributions of each common neighbor z of x and y , weighing them by $1/\log(k_z)$. Here, k_z is the degree of node z .

Adamic-Adar was likewise evaluated by [Calderoni et al. \(2020\)](#), where it often performed slightly better than Jaccard for sparse, highly compartmentalized cliques in the Mafia data. Part of the appeal was how Adamic-Adar penalizes high-degree nodes, thus prioritizing lower-degree nodes.

Resource Allocation (RA):

$$S_{RA}(x, y) = \sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{1}{k_z} \quad (4)$$

The similarity between two vertices x and y is computed in terms of resources sent from x to y through their common neighbors. It penalizes high-degree neighbors more than Adamic-Adar.

In [Su et al. \(2019\)](#), RA outperformed nearly 20 indices on the 9/11 hijackers’ network under incomplete data. By emphasizing low-degree neighbors (more directly than Adamic–Adar), it effectively exposed covert ties among hijackers with few visible connections. These hidden links supported interdiction strategies by identifying critical suspects, and adding RA-predicted edges sometimes produced a “comic effect” that magnified key actors and reshaped the network’s structure.

[Marciani et al. \(2017\)](#) evaluated a wide range of local similarity metrics on both a criminal-wiretap dataset and a corporate network. As part of their baseline comparison, the authors tested a total of 10 widely used local metrics, among which the most prominent include Common Neighbors, Jaccard Coefficient, Adamic–Adar, Preferential Attachment (PA), Resource Allocation, Salton Index (SI), Sørensen Index (So), Hub Promoted Index (HPI), Hub Depressed Index (HDI), and Leicht–Holme–Newman Index (LHN) ([Kumar et al. 2020](#)). From their experiments, the authors of [Marciani et al. \(2017\)](#) concluded that CN, AA, and PA delivered a comparatively strong performance in predicting links of the criminal network. Results showed that CN, AA, and PA performed particularly well in predicting links in criminal settings (see [Kumar et al. 2020](#) for formulae of the remaining indices). However, they noted that conventional indices rely too heavily on shared neighbor counts or degree-based weighting, which overlooks the role of brokers or intermediaries in criminal networks. To address these gaps, they proposed three new measures.

Broker Allocation (BA):

$$\Phi(x, y) = \sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{w_{x,z} + w_{z,y}}{w_z} \quad (5)$$

Here, $w_{x,z}$ and $w_{z,y}$ are the weights on the edges (x, z) and (z, y) , and w_z is the total weight of edges incident to z . This measure is aimed at revealing hidden ties mediated by “middleman” nodes. A larger value of $\Phi(x, y)$ suggests that x and y are likely to be indirectly connected through a broker z .

Relative Broker Allocation (RBA):

$$\Phi(x, y) = \frac{\sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{w_{x,z} + w_{z,y}}{w_z}}{\sum_{z \in \Gamma(x) \cap \Gamma(y)} w_z} \quad (6)$$

RBA extends BA by normalizing the sum of weighted contributions, so that the final score lies in the interval $(0, 1)$, making it straightforward to determine a threshold for identifying a hidden link.

Relative Resource Allocation (RRA):

$$\Psi(x, y) = \frac{\sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{1}{k_z}}{\sum_{z \in \Gamma(x) \cap \Gamma(y)} k_z} \quad (7)$$

This index adapts the standard Resource Allocation (RA) measure by normalizing each neighbor’s contribution. The role of the common neighbors z in bridging (x, y)

diminishes if z has many connections, since it will have fewer “resources” to allocate when linking x and y .

In their experiments, the authors found that these new measures achieved accuracy comparable to, and sometimes surpassed, that of well-established local measures. Most notably, BA proved capable of detecting connections hidden by mid-level intermediaries, which is particularly relevant for criminal/trafficking networks where such brokers may deliberately conceal direct ties (Marciani et al. 2017).

The Latent Link Prediction based on Internal and Local Links (LLPIL) model by Assouli et al. (2021) leverages bipartite projections to detect hidden links in criminal networks. It computes a connectivity score from shared neighbors’ edges and a reliability measure capturing consistency of interactions. By comparing the two, the model predicts links without relying on fixed thresholds, adapting instead to each node’s local structure.

Global Similarity Measures: Unlike local indices, global methods incorporate paths across the entire network. Calderoni et al. (2020) tested several global measures, including Katz Index and Personalized PageRank (PPR), to evaluate whether longer chains of interaction reveal hidden Mafia ties. The Katz Index aggregates all possible paths between nodes, penalizing longer ones with a damping factor β :

$$S_{\text{Katz}}(x, y) = \sum_{l=1}^{\infty} \beta^l \left| \text{paths}_{x,y}^{(l)} \right| \quad (8)$$

with its matrix form given as $S = (I - \beta A)^{-1} - I$, where $\beta < 1/\lambda_1$. In denser “meeting” networks Katz achieved higher AUROC value, as short walks effectively captured clustered collaborations, but performance dropped in the sparser phone-call graph.

PPR instead measures node importance relative to a source node s through a random walk with restart:

$$\pi_s = \alpha e_s + (1 - \alpha) A_e^T \pi_s \quad (9)$$

where α is the restart probability and A_e the row-stochastic adjacency matrix. Calderoni et al. (2020) found that both Katz and PPR outperformed local indices in denser subgraphs but lost accuracy in sparse settings dominated by a few hubs. Global indices thus offer strong predictive power when full network structure is available, but their computation can be difficult in decentralized illicit networks. Ultimately, the choice of index should depend on structural properties such as density, hierarchy, and presence of intermediaries, since these features dictate which measures best uncover hidden ties and inform law-enforcement strategies (Kumar et al. 2020).

4.7 Probabilistic and Maximum Likelihood Methods

Probabilistic approaches frame link prediction as estimating the probability of tie formation under a predefined network structure, such as community or hierarchical organization (Samad et al. 2020). Parameters are learned to assign probabilities to missing links, which are then ranked similar to similarity-based scores. While flexible, these models often require detailed node or edge attributes, involve complex parameter

tuning, and scale poorly to large networks. Maximum likelihood methods face similar challenges of complexity and computational burden, making them largely impractical for large or sparse illicit networks (Kumar et al. 2020; Arrar et al. 2024; Samad et al. 2020). As a result, applications in this domain have been limited.

A few studies illustrate these challenges. Crandell and Korkmaz (2018) applied logistic regression, combining demographic, case-level, and structural predictors to estimate the probability of an individual’s involvement in a case. Their results showed improved accuracy when network-derived features were included. Kaza et al. (2007b,a) extended this line of work by employing multivariate Cox regression survival analysis, which models the hazard of a new co-offending tie forming over time. This dynamic approach integrates individual attributes and facilitators (e.g., mutual acquaintances or shared resources) to capture the temporal progression of criminal ties. Overall, probabilistic and maximum likelihood methods demonstrate methodological rigor and temporal adaptability but remain underutilized in illicit network studies.

4.8 Learning-Based Methods

Learning-based approaches apply ML and DL to link prediction by combining structural and attribute information. In supervised ML, link prediction is framed as a binary classification problem where unconnected node pairs are represented by feature vectors and labeled as either positive or negative (Wang et al. 2014). Unsupervised approaches, in contrast, rely on representation learning such as node embeddings from algorithms like node2vec or graph neural networks (GNNs), to encode nodes into a low-dimensional space, with link likelihood determined by similarity between embeddings (Kumar et al. 2020; Arrar et al. 2024; Samad et al. 2020). These methods are powerful because they can capture complex structural patterns beyond simple heuristics.

Although no studies were found using standalone embedding-based models, embeddings have frequently been incorporated as features within ML frameworks. For example, Lopes et al. (2022) employed node2vec embeddings with classifiers such as logistic regression and k-nearest neighbors to predict hidden ties and classify relationship types in Brazilian criminal networks, showing that embedding-enhanced models improve accuracy even in sparse, noisy data. Similarly, Qiao et al. (2021) developed a machine learning framework to predict counterfeit cigarette shipments in China by constructing a directed logistics network of cities and shipment routes. They developed a comprehensive feature vector for each package, combining temporal delivery patterns with some centrality and similarity measures. Multiple classifiers were trained on these features, with logistic regression achieving the strongest performance. The study demonstrated the effectiveness of integrating structural and temporal data, though its reliance on a balanced dataset and limited sample size were key limitations.

Deep learning methods extend these ideas by directly learning from graph structures. Ribeiro et al. (2023) applied GraphSAGE, an inductive graph convolutional network, to corruption and money-laundering networks, highlighting its scalability to large and dynamic graphs. Yang (2023b) introduced CrimeGraphNet, a graph convolutional network (GCN)-based model tailored for criminal networks. It addressed data imbalance with weighted loss functions and incorporated side information (e.g., node and edge attributes), outperforming both similarity indices and standard GCNs.

Table 3 Summary of Learning-Based Models

Model	Embedding Type	Learning	Scalability	Reference
node2vec	Shallow	Supervised	High	(Lopes et al. 2022)
ML Classifiers	N/A	Supervised	High	(Qiao et al. 2021)
GraphSAGE	Deep	Supervised	High	(Ribeiro et al. 2023)
CrimeGraphNet	Deep	Supervised	High	(Yang 2023b)
TDRL-CNA	N/A	Reinforcement Learning	Medium	(Lim et al. 2019)

These studies illustrate how DL models can better exploit structural complexity and heterogeneity in illicit networks.

More recently, deep reinforcement learning (DRL) has been explored for link prediction. DRL combines RL’s decision-making with DL’s representation power, making it suitable for evolving, data-scarce criminal networks. Lim et al. (2019) proposed TDRL-CNA (Time-Evolving Deep Reinforcement Learning for Criminal Network Analysis), which simulated the evolution of a drug-trafficking network over time. By iteratively generating training data and integrating structural features such as common neighbors and Katz scores, it reduced dependence on large labeled datasets. However, its ability to capture nuanced contextual factors remained limited, which often involves learning about external factors related to the network.

In summary, learning-based methods have progressed from ML models using hand-crafted features to DL models leveraging embeddings and GNNs, and now to DRL frameworks tackling dynamics and data sparsity. Their strengths lie in adaptability and predictive accuracy, but challenges remain regarding interpretability, data requirements, and computational cost. This explains their growing but still selective adoption in illicit network analysis. A summary of learning-based models is provided in Table 3.

4.9 Temporal Link Prediction in Illicit Networks

Around 53% of the reviewed studies (Calderoni et al. 2020; Su et al. 2019; Assouli et al. 2021; Ribeiro et al. 2023; Crandell and Korkmaz 2018; Berlusconi et al. 2016; Aktas et al. 2023; Ahmadi et al. 2023) have focused their analysis on static link prediction. But there is also a growing trend in TLP methods in recent years, with the advancements of ML and DL techniques and concepts such as RL, which allows models to learn from limited data available (Lim et al. 2020; Lopes et al. 2022; Ribeiro et al. 2023; Qiao et al. 2021; Lim et al. 2019). These studies have adopted time-evolving network models to capture the dynamics of criminal interactions over multiple snapshots and predict future connections based on past trends.

A common approach among these works is to construct a sequence of network states over time, leveraging historical structural changes to make informed predictions about future links. For example, Lim et al. (2020) utilized a series of time-stamped

snapshots from a criminal network dataset (CAVIAR drug syndicate), capturing the evolution of relationships over 10 sequential time steps. Their model was trained on earlier snapshots and evaluated how well it could predict links appearing in the final time step.

Illicit networks are dynamic in nature, with relationships evolving over time as members join, leave, or alter their connections. TLP is often better suited for such networks because it can track these changes and predict future connections. Thereby, in future if research advances to streamline real-time data into these prediction models, the interdiction of these criminal networks could be accelerated and made efficient (Marciani et al. 2017).

There are a few obvious downsides to temporal LP techniques, such as these models being computationally demanding and highly reliant on large datasets for training. Advancements in RL would be a solution for some of these problems. Having said that, static LP is not completely to be ignored; these are very efficient models and simpler to implement, making them suitable for large-scale networks or cases where temporal data is sparse.

4.10 Evaluation Metrics in Illicit-Network Link Prediction

Across the reviewed studies, the most consistently used evaluation criteria are AUC (Area Under the ROC Curve), followed by precision, recall, and F1-score, while accuracy appears less central. Precision and recall are also emphasized because they directly reflect the trade-off between false positives (investigative noise) and false negatives (missed critical connections). Studies such as those by Su et al. (2019), Ahmadi et al. (2023), Lopes et al. (2022), and Ribeiro et al. (2023) consistently rely on combinations of AUC, precision, recall, and F1-score, often supplemented by **top- k evaluation**, where only the highest-ranked predicted links are assessed. This reflects a practical shift from global classification performance to prioritized link discovery, which aligns more closely with investigative use.

At the same time, several studies introduce evaluation *choices that deviate from standard social network link prediction*. A key example is the work by Berlusconi et al. (2016), where predicted links are not evaluated solely through statistical metrics but are **validated against external judicial evidence** and interpreted through a **reliability threshold** ($1 - \alpha$), linking predictions to evidentiary confidence. Similarly, Calderoni et al. (2020) emphasizes **robustness** under missing or noisy data, evaluating whether predictions remain stable when the observed network is incomplete, which is a defining property of illicit systems. Assouli et al. (2021) introduces a reliability-based weighting rule instead of fixed classification thresholds, while Aktas et al. (2023) frames evaluation through the precision–recall trade-off in hyperedge prediction, explicitly accounting for the cost of false positives in sparse settings.

5 Discussion

This review shows that link prediction in illicit networks is not a one-size-fits-all problem. Success depends on the network’s structure, size, density, and the types of relationships embedded in it. As a result, most studies take a case-by-case approach,

Table 4 Link-Prediction Studies, Models, and Their Taxonomic Category

Reference	Model	Category	Purpose
(Kaza et al. 2007b)	Cox proportional-hazards regression	Regression models	Identify attributes that facilitate new co-offending links.
(Kaza et al. 2007a)	Cox regression survival model	Regression models	Quantify effect of facilitators on future co-offending links.
(Berlusconi et al. 2016)	Similarity-based measures	Local similarity	Detect unobserved ties to guide investigations.
(Mahesar et al. 2016)	Similarity-based measures	Local similarity	Compare heuristics for predicting terrorist ties.
(Marciani et al. 2017)	Stream-adapted similarity based measures	Local similarity	Predict links in high-velocity streams.
(Bahulkar et al. 2018)	Edge augmentation via similarity based methods	Local similarity	Improve community detection by adding predicted edges.
(Crandell and Korkmaz 2018)	Logistic regression on SNA features	Regression models	Predict person-case links to aid policing.
(Lim et al. 2019)	FDRL-CNA deep-reinforcement learning	Reinforcement learning models	Improve link prediction in evolving criminal networks using SNA + meta-data.
(Su et al. 2019)	Resource-Allocation similarity	Local similarity	Recover hidden edges then target critical nodes.
(Calderoni et al. 2020)	Node2Vec and similarity based measures	Embedding-based methods	Evaluate accuracy & robustness with missing data.
(Lim et al. 2020)	ISNA-DRL (indexed-metric DRL)	Deep Reinforcement learning models	Embed node metadata in similarity indices to raise link-prediction precision.
(Assouli et al. 2021)	LLPIL reliability metric	Local similarity	Uncover latent/future offender-crime links for early-warning intelligence.
(Qiao et al. 2021)	ML Models with SNA features	Machine-learning models	Rank parcels by likelihood of counterfeit cigarettes.
(Lopes et al. 2022)	node2vec embeddings + LR/k-NN	Embedding-based methods	Recover hidden partnerships, classify edges, forecast transfers.
(Ribeiro et al. 2023)	GraphSAGE GNN	Deep-learning models	Recover missing links, classify tie types, predict money flow and future partnerships.
(Ahmadi et al. 2023)	Inductive & transductive GNN	Deep-learning models	Predict future co-offender links and connect new burglary cases to likely suspects.
(Aktas et al. 2023)	UniMHe hypergraph neural net	Deep-learning models	Predict location, crime-type and season hyperedges to expose spatio-temporal crime patterns.
(Yang 2023b)	CrimeGraphNet (GCN)	Deep-learning models	Predict hidden or missing criminal links.

tailored to the distinct hierarchies, strategies, and behaviors of each illicit group, factors that generic LP models often fail to capture.

Few studies apply multi-layer (or multiplex) approaches, though these can reveal richer insights into illicit enterprises. Their main obstacle is data scarcity: robust multi-layer models require multiple relationship types observed simultaneously, but researchers typically only access partial views such as call logs or single transaction

types. When such data are available, multi-layer and hypergraph-based models have shown clear potential to capture the interconnected nature of criminal operations.

Temporal link prediction offers another valuable dimension by modeling the formation, dissolution, or reappearance of ties over time. This dynamic perspective reveals how groups evolve or adapt strategically to evade law enforcement. Yet temporal data are even harder to obtain than static snapshots. Aggregating observations into one view is often necessary but suppresses important dynamics, such as seasonal alliances or intermittent collaborations, reducing predictive precision.

Methodologically, similarity-based indices such as Common Neighbors, Adamic-Adar, Resource Allocation, and Katz remain common. They are simple, effective on sparse networks, and provide useful baselines. However, they often fail to capture cross-layer dependencies or hidden structures in larger or more compartmentalized networks. Probabilistic and maximum likelihood models are rarely used, as they demand extensive parameter tuning and struggle with large or noisy datasets. In contrast, learning-based methods, from traditional ML to GNNs and reinforcement learning, show greater adaptability to the complexities of covert and evolving networks. Their limitation remains data scarcity, though reinforcement learning is particularly promising for smaller, incomplete datasets.

A common limitation in most LP studies is the **fixed-node or closed-world assumption**. Models are trained and evaluated transductively, meaning the set of actors is held constant, and the task reduces to predicting edges only among already observed nodes. For illicit networks, which often expand through recruitment or external partnerships, this is a serious gap. As a result, current predictions are inherently bounded by the observed set of participants and cannot anticipate the introduction of unseen collaborators.

In summary, advances in **multi-layer and temporal modeling** broaden the scope of LP research, but data limitations still constrain most studies to narrower, static analyses. Similarity-based methods remain reliable but insufficient for complex networks. Learning-based approaches represent the most promising frontier, balancing scalability with the flexibility needed to adapt to the unique characteristics of illicit networks.

When discussing about the **evaluation of link prediction methods** in illicit networks, it departs from conventional practice in two critical ways. First, AUC and ranking-based measures dominate in illicit-network link prediction because the data are inherently sparse and highly imbalanced, with far more non-links than true links. Under such conditions, accuracy becomes misleading because a model can achieve high accuracy by predicting non-links. AUC, in contrast, evaluates the model’s ability to rank true links higher than false ones, independent of a fixed threshold, making it more robust for incomplete and uncertain network data. Second, there is a clear move toward context-aware evaluation, where predictions are judged not only by statistical performance but also by their reliability, robustness, and investigative value. This highlights a fundamental limitation in the literature: many studies still rely on artificially constructed test settings, such as random edge removal or balanced samples, which may overestimate real-world performance. A rigorous evaluation in this

domain should therefore combine ranking performance, robustness analysis, temporal validation, and domain-grounded plausibility, rather than relying on a single metric.

6 Conclusion and Future Directions

This systematic review examined the state of link prediction research in illicit networks, covering methods ranging from classical statistical and similarity-based approaches to machine learning, graph neural networks, and reinforcement learning. Across the reviewed studies, link prediction emerged as a valuable but still underdeveloped tool for illicit-network analysis. Its promise is clear: when network data are fragmented, covert, and incomplete, link prediction can help recover hidden structure, identify plausible relationships, and support disruption strategies that would otherwise rely only on partial evidence.

The literature reveals a clear pattern. Most studies still rely on static or simplified graph formulations, even though illicit networks are dynamic, multilayered, strategic, and only partially observed. Only a few demonstrate robustness under the conditions that matter most in practice: missing data, severe class imbalance, sparse observations, and uncertainty about whether observed ties reflect the true operational structure of the network. Progress in predictive accuracy alone is not enough; what is needed are models that are credible under uncertainty, interpretable to domain experts, and useful in high-stakes investigative settings.

Therefore, future research should prioritize the following directions:

1. ***Incorporating Network Metadata:*** Beyond structural features, integrating contextual data such as demographics, criminal history, organizational roles, geographic information, or interaction types can improve prediction. These should be combined with graph-based measures to create richer feature representations or embeddings and then evaluated against strong structural baselines. Where metadata are high-dimensional or noisy, dimensionality reduction and feature selection will be essential.
2. ***Leveraging Reinforcement Learning and Advanced GNNs:*** Reinforcement learning is promising for small, noisy, and evolving datasets because it can refine predictions through iterative feedback. Its adaptive nature makes it particularly appealing for illicit networks, where relationships shift strategically over time. Combining reinforcement learning with advanced graph neural networks may further improve performance by joining expressive graph representations with sequential decision-making.
3. ***Developing Time-Aware and Multilayer Models:*** Dynamic GNNs, temporal embeddings, and snapshot-based methods can better capture the emergence, persistence, and dissolution of ties. Multilayer and multiplex formulations are also important because illicit actors often interact across multiple channels such as communication, finance, kinship, co-offending, and logistics. Future work should move beyond flat graph representations whenever the data allow it and should explicitly test how temporal and multilayer structure changes predictive performance.
4. ***Combining Real and Synthetic Data:*** Limited access to real illicit-network data remains one of the field’s main bottlenecks. Carefully generated synthetic

data, including simulation-based or Large Language Model-based generative AI approaches, may help expand training samples while preserving important structural properties. However, this should not be treated as a shortcut. Hybrid datasets must be validated against reserved real-world evidence to ensure that they do not introduce unrealistic patterns or inflate model performance.

5. ***Modeling Predictive Uncertainty***: A major gap in the current literature is the limited attention to uncertainty in link prediction outputs. In illicit networks, predictions are made under partial observability, noisy records, hidden actors, and ambiguous ties, yet models are often evaluated as if predictions were equally reliable. Future research should therefore move toward uncertainty-aware link prediction by estimating confidence, calibration, or prediction intervals around candidate links, and by distinguishing high-confidence inferences from speculative ones. This would make model outputs more realistic, more interpretable, and more useful for investigators and policymakers who must make decisions under risk.

For illicit networks, the central challenge is not only to infer missing ties, but to do so in a way that respects the hidden, adaptive, and uncertain nature of the system being studied. The most valuable future models will therefore be those that combine predictive strength with interpretability, robustness, temporal awareness, and explicit treatment of uncertainty. Advancing the field in this direction would move link prediction from a promising analytical technique to a more credible and operationally relevant tool for understanding and disrupting illicit networks.

Declarations

Funding

Applicable. Removed from the blinded manuscript.

Conflict of interest/Competing interests

The authors declare that they have no competing interests.

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Data availability

Not applicable.

Materials availability

Not applicable.

Code availability

Not applicable.

Author contribution

Applicable. Removed from the blinded manuscript.

References

- Ahmadi Z, Nguyen HH, Zhang Z, et al (2023) Inductive and transductive link prediction for criminal network analysis. *Journal of Computational Science* 72:102063
- Aktas MY, Alkulaib L, Lu CT (2023) Unimhe: Unified multi hyperedge prediction a case study on crime dataset. In: 2023 IEEE International Conference on Big Data (BigData), IEEE, pp 5134–5139
- Arrar D, Kamel N, Lakhfif A (2024) A comprehensive survey of link prediction methods. *The journal of supercomputing* 80(3):3902–3942
- Assouli N, Benahmed K, Gasbaoui B (2021) How to predict crime—informatics-inspired approach from link prediction. *Physica A: Statistical Mechanics and its Applications* 570:125795
- Bahulkar A, Szymanski BK, Baycik NO, et al (2018) Community detection with edge augmentation in criminal networks. In: 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), IEEE, pp 1168–1175
- Barrick K, Sharkey TC, Maass KL, et al (2024) Expanding our understanding of traffickers and their operations: A review of the literature and path forward. *Trauma, Violence, & Abuse* 25(3):2348–2362
- Berlusconi G, Calderoni F, Parolini N, et al (2016) Link prediction in criminal networks: A tool for criminal intelligence analysis. *PloS one* 11(4):e0154244
- Boccaletti S, Bianconi G, Criado R, et al (2014) The structure and dynamics of multilayer networks. *Physics reports* 544(1):1–122
- Calderoni F, Catanese S, De Meo P, et al (2020) Robust link prediction in criminal networks: A case study of the sicilian mafia. *Expert Systems with Applications* 161:113666
- Catino M (2014) How do mafias organize?: Conflict and violence in three mafia organizations. *European Journal of Sociology/Archives Européennes de Sociologie* 55(2):177–220
- Crandell I, Korkmaz G (2018) Link prediction in the criminal network of albuquerque. In: 2018 IEEE/ACM International Conference on Advances in Social Networks

- Analysis and Mining (ASONAM), IEEE, pp 564–567
- Dimas GL, Konrad RA, Lee Maass K, et al (2022) Operations research and analytics to combat human trafficking: A systematic review of academic literature. *PLoS one* 17(8):e0273708
- Diviák T (2022) Key aspects of covert networks data collection: Problems, challenges, and opportunities. *Social Networks* 69:160–169
- Ficara A, Cavallaro L, De Meo P, et al (2020) Social network analysis of sicilian mafia interconnections. In: *Complex Networks and Their Applications VIII: Volume 2 Proceedings of the Eighth International Conference on Complex Networks and Their Applications COMPLEX NETWORKS 2019* 8, Springer, pp 440–450
- Ficara A, Cavallaro L, Curreri F, et al (2021) Criminal networks analysis in missing data scenarios through graph distances. *PLoS one* 16(8):e0255067
- International Labour Organization (2024) Forced labour, modern slavery and trafficking in persons. <https://www.ilo.org/topics-and-sectors/forced-labour-modern-slavery-and-trafficking-persons>, accessed June 22, 2025
- Isah H, Neagu D, Trundle P (2015) Bipartite network model for inferring hidden ties in crime data. In: *Proceedings of the 2015 IEEE/ACM international conference on advances in social networks analysis and mining 2015*, pp 994–1001
- Islam F (2024) Human trafficking law enforcement over the victims and offenders: The perspective of anti-trafficking stakeholders. *Victims & Offenders* 19(8):1512–1540
- Kaza S, Hu D, Atabakhsh H, et al (2007a) Predicting criminal relationships using multivariate survival analysis. In: *Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains*, pp 290–291
- Kaza S, Hu D, Chen H (2007b) Dynamic social network analysis of a dark network: Identifying significant facilitators. In: *2007 IEEE Intelligence and Security Informatics*, IEEE, pp 40–46
- Keskin BB, Bott GJ, Freeman NK (2021) Cracking sex trafficking: Data analysis, pattern recognition, and path prediction. *Production and Operations Management* 30(4):1110–1135
- Konrad RA, Trapp AC, Palmbach TM, et al (2017) Overcoming human trafficking via operations research and analytics: Opportunities for methods, models, and applications. *European Journal of Operational Research* 259(2):733–745
- Kumar A, Singh SS, Singh K, et al (2020) Link prediction techniques, applications, and performance: A survey. *Physica A: Statistical Mechanics and its Applications* 553:124289

- Liben-Nowell D, Kleinberg J (2003) The link prediction problem for social networks. In: Proceedings of the twelfth international conference on Information and knowledge management, pp 556–559
- Lim M, Abdullah A, Jhanjhi N, et al (2019) Hidden link prediction in criminal networks using the deep reinforcement learning technique. *Computers* 8(1):8
- Lim M, Abdullah A, Jhanjhi N, et al (2020) Indexed metrics for link prediction in graph analytics. *International Journal of Advanced Computer Science and Applications* 11(5)
- Logan T, Walker R, Hunt G (2009) Understanding human trafficking in the united states. *Trauma, Violence, & Abuse* 10(1):3–30
- Lopes DD, Cunha BRd, Martins AF, et al (2022) Machine learning partners in criminal networks. *Scientific Reports* 12(1):15746
- Macaveiu C, Wong L, Guarcello L (2024) Factors, counter-trafficking programs, and geographical variations in human trafficking literature (2010–2022). *Journal of Human Trafficking* pp 1–22
- Mahesar A, Bhatti Z, Waqas A, et al (2016) Efficient link prediction method in dark networks analysis. *Sindh University Research Journal-SURJ (Science Series)* 48(1)
- Marciani G, Porretta M, Nardelli M, et al (2017) A data streaming approach to link mining in criminal networks. In: 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), IEEE, pp 138–143
- Martin L, Matthias C, Abeyta S, et al (2023) Mechanisms of recruitment into sex trafficking operations: a systematic review. *Global Crime* 24(4):239–262
- Martin L, Maass K, Barrick K, et al (2024) Identification of effective strategies to disrupt recruitment of victims in human trafficking: Qualitative data, systems modeling, survivors and law enforcement. Tech. rep., Final technical report, National Institute of Justice
- Morselli C (2009) *Inside criminal networks*, vol 8. Springer
- Nasdaq and Verafin (2024) 2024 global financial crime report. Technical report, Nasdaq, Inc., New York, NY, USA, URL <https://www.nasdaq.com/global-financial-crime-report>, includes data model and insights by Celent and Oliver Wyman
- Qiao LC, Wang JL, Gao BH, et al (2021) Utilizing link prediction approach to predict express-related counterfeit cigarette crime cases. In: 2021 IEEE 21st International Conference on Communication Technology (ICCT), IEEE, pp 328–332

- Ribeiro HV, Lopes DD, Pessa AA, et al (2023) Deep learning criminal networks. *Chaos, Solitons & Fractals* 172:113579
- Russell A (2018) Human trafficking: A research synthesis on human-trafficking literature in academic journals from 2000–2014. *Journal of human trafficking* 4(2):114–136
- Samad A, Qadir M, Nawaz I, et al (2020) A comprehensive survey of link prediction techniques for social network. *EAI Endorsed Trans Ind Networks Intell Syst* 7(23):e3
- Sauer PC, Seuring S (2023) How to conduct systematic literature reviews in management research: a guide in 6 steps and 14 decisions. *Review of Managerial Science* 17(5):1899–1933
- Sharkey TC, Keskin BB, Konrad R, et al (2024) Introduction to the special issue on analytical methods for detecting, disrupting, and dismantling illicit operations. *IISE Transactions* 56(3):221–223
- Sparrow MK (1991) The application of network analysis to criminal intelligence: An assessment of the prospects. *Social networks* 13(3):251–274
- Su Z, Ren K, Zhang R, et al (2019) Disrupting terrorist networks based on link prediction: A case study of the 9–11 hijackers network. *IEEE Access* 7:61689–61696
- UNTOC (2024) Un convention against transnational organized crime and the protocols thereto. <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>, accessed: 2025-06-23
- Wang P, Xu B, Wu Y, et al (2014) Link prediction in social networks: the state-of-the-art. *arXiv preprint arXiv:14115118*
- Wang Z, Li MH, Baxter P, et al (2025) Implementing large language model and retrieval augmented generation to extract geographic locations of illicit transnational kidney trade. *International Journal of Health Geographics* 24(1):1–25
- WHO (2024) Sdg target 5.2.1: Eliminate violence against women and girls. <https://www.who.int/data/gho/data/themes/topics/indicator-groups/indicator-group-details/GHO/sdg-target-5.2.1-eliminate-violence-against-women-and-girls>, accessed: 2025-06-23
- Wright PD, Liberatore MJ, Nydick RL (2006) A survey of operations research models and applications in homeland security. *Interfaces* 36(6):514–529
- Yang C (2023a) Crimegnn: Harnessing the power of graph neural networks for community detection in criminal networks. *arXiv preprint arXiv:231117479*
- Yang C (2023b) Crimegraphnet: Link prediction in criminal networks with graph convolutional networks. *arXiv preprint arXiv:231118543*

- Yang Y, Lichtenwalter RN, Chawla NV (2015) Evaluating link prediction methods. *Knowledge and Information Systems* 45:751–782
- Yu JZ, Wu M, Bichler G, et al (2023) Reconstructing sparse multiplex networks with application to covert networks. *Entropy* 25(1):142
- Zhang R, Wang Q, Yang Q, et al (2022) Temporal link prediction via adjusted sigmoid function and 2-simplex structure. *Scientific Reports* 12(1):16585