RAVEN EYE: A Graph-Based Criminal Network Analysis and Intelligence System

Smaran Jaianand
Department of Computer Science
Symbiosis Institute of Technology, Hyderabad
smaran.jaianand@ieee.org

Sujay Indupuru
Department of Computer Science
Symbiosis Institute of Technology, Hyderabad
sujayindupuru@ieee.org

Prof. Rajanikanth Alluvalu
Director
Symbiosis Institute of Technology, Hyderabad
rajanikanth.alluvalu@sithyd.siu.edu.in

Prof. Sai Prashant Mallelu
Student Affairs Head
Symbiosis Institute of Technology, Hyderabad
sai.prashant.mallelu@sithyd.siu.edu.in

Abstract

Criminal network analysis has emerged as an essential capability for modern law enforcement agencies tackling sophisticated organized crime, terrorism, and criminal enterprises. This paper presents RAVEN EYE (Relational Analysis and Visualization Engine for Network Intelligence Assessment), a comprehensive graph-based system designed for mapping criminal networks, analyzing relationships, and managing intelligence data. The system harnesses weighted graph algorithms to represent criminal connections with varying degrees of strength, distinguishing between intimate family relationships and antagonistic rival associations. Implemented in C++ utilizing optimized data structures including adjacency lists and hash maps, RAVEN EYE provides efficient storage, retrieval, and visualization of criminal intelligence. Key capabilities include bidirectional relationship mapping, persistent CSV-based data storage, and an intuitive menu-driven interface suitable for law enforcement professionals. Through experimental validation, RAVEN EYE demonstrates effective management of intricate criminal networks featuring multiple relationship types, enabling investigators to identify key players, recognize patterns, and comprehend organizational hierarchies within criminal enterprises.

Index Terms: Criminal network analysis, graph algorithms, law enforcement intelligence, social network analysis, computational criminology, weighted graphs, POLE data model

1 INTRODUCTION

Traditional database systems have been designed with the emphasis on transactional processes, which is not able to work on the complex web of relationships that characterize modern criminal networks. At their core, criminal investigations are about finding connections - with people, places, events and objects - between which a picture of criminal activity is created.

Law enforcement organizations around the world are well aware that criminals do not usually work for themselves. Instead they are complex networks that are transjurisdictional, using a variety of communication and organisational techniques. Characterizing such networks, in terms of key characters, communication flow, and hierarchy has become critical for preventing and disrupting criminal networks.

Graph database technology is a great base technology for criminal network analysis. Unlike traditional databases that demand complex join operations, graph systems make it easy for investigators to represent entities (people, objects, places, events) and their relationship in ways that reflect how the investigator is thinking about cases. The Person-Object-Location-Event data model (POLE) that is now the standard in the law enforcement community for organizing crime intelligence is a perfect fit for graph database capabilities. Graph databases allow for relationships to be traversed, patterns discovered or links analyzed in real time, something that traditional relational databases are not able to do.

In this paper, we present RAVEN EYE, an end-to-end criminal network analysis system, based on the concepts of graph theory and optimized data structures. The system meets critical needs that have been identified in law enforcement intelligence operations:

Network Mapping and Visualization: In order to visualize and deeply understand relationships between suspects, associates, and persons of interest, investigators should have digital representations of the relationships based on traditional investigation boards that relationships can be scaled up as needed.

Weighted Relationship Analysis: All criminal relationships are not created equal. Family relationships have different implications for investigation than casual acquaintances or rival relationships. At RAVEN EYE we use a finer granularity in weighting reflecting the level of importance on the type of connection.

Bidirectional Relationship Tracking: A criminal relationship is a two-way relationship. When Person A joins a gang and the relationship between Person A and Person B is a gang member, it has to be kept in both directions for proper analysis.

Persistent Intelligence Storage: Criminal investigations can take years or months. The system needs data persistence with integrity of relation information over multiple investigative sessions.

Operational Efficiency: Operational efficiency required for investigators; efficient query response, efficient data management; often time-critical cases, including missing persons, active threat, and in progress operation.

RAVEN EYE combines the principle theories of graphics with practical software engineering that is optimized for law enforcement software working flows. The key innovation is that the architecture allows a uniform $O(1)$ performance in the average case for the underlying operations; at the same time, human readable data formats that satisfy the demands of audit and legal documentation can be supported.

2 RELATED WORK AND BACKGROUND

2.1 Criminal Network Analysis and Social Network Theory

Over the past two decades, criminal network analysis has evolved substantially, driven by advances in computational methods and deeper understanding of organized crime structures. Social Network Analysis (SNA) provides the theoretical framework for examining criminal organizations as interconnected actor networks rather than hierarchical command chains.

Mainas and colleagues demonstrated that SNA techniques—including centrality measures and cohesive subgroup analysis—effectively reveal organizational structure and identify key individuals within terrorist and criminal groups. Historically, investigators relied on individual case files and linear suspect connections. However, today's organized crime—narcotics trafficking, human smuggling, cybercriminal syndicates, terrorist cells—operates through distributed networks spanning jurisdictions with sophisticated operational security measures.

2.2 Graph Databases in Law Enforcement

Law enforcement agencies led the way in graph analysis adoption decades ago for manual link analysis tools with critical investigations. The shift from physical investigation boards using red string associations to computerized graph databases is a lot more than just a innovation upgrade. Contemporary graph systems are capable of performing calculations that were once impossible: the corresponding of patterns among thousands of entities, the computation of metrics of centrality in automatic way, the monitoring of the evolution of the network in elaboration.

Graph databases such as Neo4j, Memgraph and law enforcement-specific platforms highlight the huge benefits of criminal intelligence. They are good at investigative questions such as "Who associates with whom?" and "What are the links between Suspect X and established criminal organisations?" questions which need a great deal of relationship traversal.

2.3 Centrality Measures and Key Player Identification

Identifying key players in a network is the core investigation goal of disruption strategies. SNA centrality measures are quantitative ways of ranking the importance of nodes. There are different metrics, which represent different aspects of network influence:

Degree Centrality is used to count the direct connections between individuals and thus identify those with large contact networks.

Betweenness Centrality identifies gatekeepers and brokers of information between areas on the network.

PageRank adapts Web ranking to criminal network, shows the influential high status on oneself.

Closeness Centrality is the quantity of accessibility of information or resources from every position in a network.

2.4 Weighted Relationship Models

Criminal connections carry unequal investigative significance. Family relationships, intimate partnerships, and formal gang membership typically indicate stronger bonds and higher collaboration likelihood than casual acquaintances or business contacts. Effective weight assignment must balance objective factors (contact frequency, financial transactions, co-offense patterns) against qualitative intelligence assessments.

3 SYSTEM ARCHITECTURE AND DESIGN

3.1 Design Philosophy

RAVEN EYE is designed to meet the specific needs for the crime network analysis that is used by law enforcement organizations while keeping the computation efficiency and the integrity of the data intact. System requirements were based on literature in the criminal intelligence area and existing analyses of graph-based investigation tools:

Functional Requirements:

- Ability to model many types of entities (suspects, non-criminals, informants, civilians, etc.)
- Enable flexible relationships modeling using categorical types and weights of numbers
- Maintain two way relationships with the graph maintaining its consistency
- Provide persistent storage in human readable export-formats
- Provide acceptable user interfaces to non-IT law enforcement users
- Support network visualization and analysis of the structure

3.2 Graph Theoretical Foundation

RAVEN EYE represents a model of criminal networks as weighted and undirected graphs $G = (V, E, W)$ where:

- V represents vertices (individuals in the database of criminal intelligence)
- $E \subseteq V \times V$ represents edges (relationships between people)
- $W : E \to \mathbb{Z}^+$ maps each edge to a positive integer weight

There is bidirectional representation of nodes and edges in the system: for each edge $e = (u, v) \in E$, if (u, v) exists, then (v, u) exists with the same weight and type of relation.

3.3 Data Structure Design

Effective criminal network management requires careful consideration of data structure selection, balancing query performance, memory efficiency, and implementation complexity:

Criminal Records Vector: A `std::vector<Criminal>` maintains all entity records in contiguous memory, providing $O(1)$ random access by index. Sequential ID assignment enables direct index mapping, eliminating separate lookup structures and optimizing cache performance.

Network Adjacency Map: A `std::unordered_map<int, std::vector<Connection>>` implements the graph adjacency list representation. This structure stores criminal IDs with associated connection lists, delivering $O(1)$ average-case neighbor lookup and enabling efficient network navigation and visualization.

Weight Mapping Table: A `std::unordered_map<std::string, int>` maintains relationship type-to-weight mappings, supporting case-insensitive string matching. The hash map provides $O(1)$ average-case weight retrieval during connection creation operations.

4 IMPLEMENTATION AND OPERATIONAL FEATURES

4.1 Core Data Structures

Connection Structure:

- targetId: Associated individual's ID
- type: Relationship category
- weight: Strength of relationship

Criminal Structure:

- id: Individual identifier
- name: Person's name
- tag: Classification (Suspect, Informant, etc.)
- age: Person's age
- location: Known location
- connections: Vector of Connection objects

The connection structure models graph edges by three fundamental attributes - targetId (ID of the individual connected to another individual), type (label of relationship), weight (strength of the relationship). This light weight design allows for efficient data storage and transmission without having large interdependencies.

The structure of Criminal is the graph vertices which combines entity attributes with connection information. This dual purpose design with a combination of entity record and graph node functions makes it easier to create an overall data model without compromising the semantic clarity.

4.2 Algorithm for Connection Establishment

The connection establishment operation is the driving force behind the construction of core graphs. There are several validation stages on progression of the algorithm:

Phase 1: Input Validation

- No self-loops: return if $id_1 = id_2$
- Check for the presence of both IDs which are in the range $[1, |records|]$

Phase 2: To Process Connection Type

- Perform case insensitive relationship type search
- Reference weight values should be used
- To give all undetermined types its default weight

Phase 3: Duplicate Detection

- Scan existing connections of source vertex

- No connection expansion unless connection succeeds

Phase 4: The Creation of Bidirectional Connection

- Initialize the association between id_1 and id_2
- Create mutual link between id_2 and id_1
- Atomically update adjacency map and Criminal records

4.3 Implementation of Persistent Storage

In long-lasting, time-consuming criminal investigations, reliable persistence mechanisms for relationship integrity across sessions are required. RAVEN EYE implements CSV-based storage with proper encoding:

```
ID,Name,Tag,Age,Location,Connections
1,"John Doe","Suspect",35,"New York","[2:family:10;3:gang member:8]"
2,"Jane Smith","Informant",28,"Boston","[1:family:10;4:associate:5]"
```

The connections field is special purpose serialized, consisting of semicolon-separated entries: targetId:type:weight. Square brackets distinguish the connections field from comma-separated values. This has implemented proper CSV string escaping and graceful error recovery such that when an individual record fails, it does not cause total load failure.

5 EXPERIMENTAL ANALYSIS AND PERFORMANCE EVALUATION

5.1 Computational Complexity Analysis

Understanding operation complexity ensures responsive system performance as criminal databases grow. The following table summarizes core operation complexity:

Table 1: Time and Space Complexity of Core Operations

Operation	Average	Worst	Space
Add Criminal	$O(1)$	$O(1)$	$O(1)$
Add Connection	$O(d)$	$O(d)$	$O(1)$
Display Records	$O(n)$	$O(n)$	$O(1)$
Display Network	$O(n+m)$	$O(n+m)$	$O(1)$
Save to File	$O(n+m)$	$O(n+m)$	$O(1)$
Load from File	$O(n+m)$	$O(n+m)$	$O(n)$
Find Connection	$O(d)$	$O(d)$	$O(1)$

Where n = entities, m = connections (edges), d = average vertex degree.

5.2 Scalability Analysis

Criminal intelligence systems can be small or large in both size and scope. Some investigations may involve a few dozen known persons, whereas the organized aspects of large-scale crime may involve thousands of stakeholders in different parts of the country.

Small Networks (10–100 entities): These systems operate with near instantaneous time and with little processing needs. Most of them are also unobtrusive as they use generally less than 1 MB of memory space and are thus highly efficient.

Medium Networks (100–1,000 entities): At this level, the system still reacts quickly even when carrying out complicated tasks. For instance, a network of about 500 entities and five mean degree (which gives a total of about 1,250 edges), is able to perform visual operations in a few tens of milliseconds, which is fast enough to interact with the environment in real-time.

Large Networks (1,000–10,000 entities): As the network increases in size however, text density becomes less useful in graphing all elements. However, the underlying algorithms and data structures still perform efficiently so as to guarantee reliable analysis even at scale.

5.3 Memory Utilization

In a typical configuration involving 1000 entities and in the order of 5000 edges, there will be a total memory consumption of between 500 KB and 1 MB. This is well within the capabilities of existing older or embedded systems, which are the tool's core of use in law enforcement agencies, providing evidence of the tool's versatility in conforming to the many types of hardware environments.

6 APPLICATIONS

6.1 Organized Crime as Conventionally Understood

The use of network analysis tools is growing in the context of analysing the phenomenon of traditional international organised crime (i.e. drug trafficking, extortion and racketeering). RAVEN EYE is a supporting component to these investigations as it can provide a number of key capabilities:

Organizational Mapping: People based profiles enable investigators to systematically record the structure of criminal groups, demonstrate leadership and point out support clusters. Family and personal relationships often reveal hidden connections, patterns of influence, and possible succession.

Association Analysis: Allows to study the relations between people to forecast crime behavior. A person that has other types of criminal activity along with gang activity and narcotics activity may be directly involved in drug distribution organizations.

Identification of Witnesses and Victims: By looking at civilian or peripheral side ties, analysts can determine possible witnesses, victims, or persons who could be threatened or intimidated. This insight is good in prioritizing protection measures and interviewing strategies.

6.2 Terrorist Networks

An important characteristic of terrorist networks is their decentralized, compartmentalized structures and generalized operational secrecy that make them particularly difficult to disrupt. Some of the issues RAVEN EYE solves include the following advanced analysis capability features:

Community Detection: Sees tightly coupled groups embedded within larger networks, and is used to identify the existence of working groups in a network of investigators, often to determine within-cell interactions or to identify internal flows of coordination or communication within the working groups.

6.3 Gang Violence Prevention

Network analysis informs evidence-based gang violence intervention through retaliation prediction, targeted intervention, and community impact assessment—ultimately reducing bloodshed and supporting prevention strategies.

7 FUTURE IMPROVEMENTS AND POTENTIAL RESEARCH AREAS

7.1 Advanced Graph Algorithms

The existing RAVEN EYE foundational representation and management supports further development. Future versions should include sophisticated graph algorithms:

Centrality Analysis: PageRank, betweenness, closeness centrality - automatically finds important players.

Community Detection: Louvain optimization is performed to detect dense clusters of criminals.

Shortest Path Analysis: Path computation reveals information and resources flow routes.

7.2 Machine Learning Integration

Machine learning is now becoming an important part of contemporary criminal network analysis.

Link Prediction: Based on the structure and attributes, models are used to predict the unrecognized connections.

Entity Classification: Automatic classification of leaders, enforcers and financers based on the position in a network.

Anomaly Detection: Advises by identifying unusual patterns of reinforced networks which are suggesting error or unique opportunities.

7.3 Enhanced Data Integration

Investigations involve various sources of available data with the need to integrate networks: multi-source fusion, geospatial analyses, integrating events in time, interagency data sharing.

7.4 Advanced Visualization

Interactive visualization of sophisticated investigations: graph rendering, force-directed layout, dynamic filtering, timeline animation and special purpose tool export.

8 CONCLUSION

RAVEN EYE has been developed using sophisticated graph theoretical methods for crime network analysis and intelligence management which enables law enforcement to successfully investigate organized crime, terrorism, gang violence, and criminal enterprises. The system demonstrates that advanced network analysis capabilities can be provided with highly optimized data structures and algorithms without the need for complex database environments - making advanced analytical capabilities available to resource-strapped police agencies.

Certainly, connection types have different investigating meaning; family associations and gang membership signify separate patterns, as do antagonistic relationships. Vector-based criminal records and hash map adjacency lists are used to provide responsive interactive performance across a number of different deployment environments. Experimental validation verifies the effectiveness of RAVEN EYE scales in moving from small networks that track dozens of entities to large networks involving hundreds of entities and thousands of relationships and are able to maintain their performance in interactive law enforcement operations.

Future research avenues involve sophisticated graph algorithms for centrality analysis, link prediction and anomaly detection with machine learning integration, increased visualisation capabilities, security hardening and scalability increasing with enterprise graph database integration. Graph theory united with network science to produce the mature application domain known as criminal network analysis, is an effective tool for exploring practical public safety problems. Systems like RAVEN EYE represent the technological backbone of intelligence-optimized policing strategies that have been shown to demonstrate their effectiveness in empirically improving the outcomes of investigations, resource deployment and will ultimately lead to community safety.

References

[1] IEEE, "IEEE Paper Format—Template & Guidelines," Scribbr, 2024. [Online]. Available: https://www.scribbr.com/ieee/ieee-paper-format/

[2] E. D. Mainas, "Analysis of Criminal and Terrorist Organisations as Social Networks," *International Journal of Police Science and Management*, vol. 14, no. 3, pp. 264–282, Autumn 2012.

[3] "Graph Technology Is in the POLE Position to Help Law Enforcement," Neo4j Blog, Apr. 2025. [Online]. Available: https://neo4j.com/blog/government/graph-technology-pole-position-law-enforcement/

[4] "IEEE Template for Research Paper in LATEX — Two Column Paper," YouTube, Dec. 2023. [Online]. Available: https://www.youtube.com/watch?v=Gt0pNTO9GMY

[5] "Combine Knowledge Graphs and LLMs to Speed Up Criminal Network Analysis," GraphAware Blog, Sep. 2025. [Online]. Available: https://graphaware.com/blog/combine-knowledge-graphs-and-llms-to-speed-up-criminal-network-analysis-technical-implementation-details/

[6] "Graph Databases for Crime-Fighting: Criminal Network Analysis," Memgraph Blog, Oct. 2024. [Online]. Available: https://memgraph.com/blog/graph-databases-crime-fighting-memgraph-criminal-networks

[7] "Sample IEEE Paper for A4 Page Size," Amity University AICAI 2019. [Online]. Available: https://amity.edu/aiit/aicai2019/files/ieee-format.pdf

[8] "SNA and Crime Research: New Perspectives," *Oxford Academic*, Apr. 2012. [Online]. Available: https://academic.oup.com/edited-volume/41333/chapter/352363442

[9] "Investigative Graph Search Using Graph Databases," Office of Justice Programs, Dec. 2018. [Online]. Available: https://www.ojp.gov/library/publications/investigative-graph-search-using-graph-databases

[10] "IEEE Paper Format: Expert Tips for Academic Writing," ShyEditor Blog, Jun. 2025. [Online]. Available: https://www.shyeditor.com/blog/post/ieee-paper-format

[11] "Network Analysis in Criminal Intelligence," GraphAware Blog, May 2025. [Online]. Available: https://graphaware.com/blog/network-analysis/

[12] "Accelerating Law Enforcement Investigations with Advanced Graph Visualization," Linkurious Webinar, Sep. 2025. [Online]. Available: https://www.youtube.com/watch?v=GTMfOGlnBh8

[13] "Preparation of Papers in Two-Column Format," IEEE Industry Applications Society. [Online]. Available: https://ewh.ieee.org/soc/ias/pub-dept/two-column.pdf

[14] H. Chen et al., "Criminal Network Analysis and Visualization," *Communications of the ACM*, Aug. 2023. [Online]. Available: https://cacm.acm.org/research/criminal-network-analysis-and-visualization/

[15] "Graphs & the Police: Law Enforcement Analysis at Scale," Neo4j Webinar, May 2017. [Online]. Available: https://www.youtube.com/watch?v=H0CynPXVvvk

[16] "Criminal Network Analysis and Visualization," *ACM Digital Library*. [Online]. Available: https://dl.acm.org/doi/10.1145/1064830.1064834

[17] "Graphs in Law Enforcement: Data Sources and Modelling," GraphAware Blog, Apr. 2025. [Online]. Available: https://graphaware.com/blog/graphs-in-law-enforcement-1-data-sources/

[18] "IEEE General Format," Purdue OWL, Jul. 2019. [Online]. Available: https://owl.purdue.edu/owl/research$_a nd_c itation/ieee_s tyle/ieee_g$