Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2022 3(1), 1149–1154

CDR/IPDR ANALYSER AND VISUALIZER: ENHANCING INVESTIGATIVE CAPABILITIES THROUGH COMMUNICATION DATA ANALYSIS

Prashant Kapri [1], Noopur Thanvi [1], Shubham Patane [1], Rashmi Thakur [1]

[1] Thakur College of Engineering & Technology, India

Corresponding Author

Prashant Kapri,
prashantkapri7@gmail.com

DOI
10.29121/shodhkosh.v3.i1.2022.6058

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Call Detail Records (CDRs) and Internet Protocol Detail Records (IPDRs) provide a wealth of metadata crucial for modern investigations. With increasing data volumes and complexities, law enforcement agencies (LEAs) require robust tools that can ingest, analyse, and visualize these records. This review paper explores the current landscape of CDR/IPDR analysis tools, their capabilities in criminal investigations, technological approaches for visual analytics, and the challenges associated with handling such sensitive data. Emphasis is placed on the development of an intuitive visualizer that supports multi-format uploads, communication link mapping, suspect prioritization, and exportable reports.

Keywords: CDR, IPDR, Criminal Investigation, Suspect Link Analysis, Behavioural Pattern Detection

1. INTRODUCTION

Communication metadata such as CDRs and IPDRs have become instrumental in modern policing, especially in criminal investigations, counter-terrorism, cybercrime, and intelligence gathering. Traditional manual methods of interpreting this data are not scalable for large datasets. Hence, automated CDR/IPDR analysers and visualizers are increasingly being adopted.

This paper reviews technologies and methodologies employed in the development of CDR/IPDR visual analytics tools and proposes a framework for an ideal system for use by LEAs and police departments.

How to cite this article (APA): Kapri, P., Thanv, N., Patane, S., and Thakur, R. (2022). CDR/IPDR Analyser and Visualizer: Enhancing Investigative Capabilities Through Communication Data Analysis. *ShodhKosh: Journal of Visual and Performing Arts, 3*(1), 1149–1154. doi: 10.29121/shodhkosh.v3.i1.2022.6058

2. LITERATURE REVIEW

2.1. CDR/IPDR BASICS

CDR (Call Detail Record): Contains metadata about telecommunication interactions – time, duration, sender/receiver numbers, cell towers, etc.

IPDR (Internet Protocol Detail Record): Tracks internet activity over IP – websites accessed, IP addresses, application types, and communication endpoints.

2.2. APPLICATIONS IN LAW ENFORCEMENT

CDR/IPDR analysis helps in:

Link Analysis: Determining networks of communication between suspects.

Behavioural Analysis: Identifying usage patterns, frequent contacts, and unusual activity.

Geo-Spatial Analysis: Tracking movement and location-based behaviour.

Suspect Prioritization: Identifying central figures in a criminal network using social network analysis.

2.3. EXISTING TOOLS AND SOLUTIONS

Several commercial and open-source platforms exist:

CallBox, Analyst’s Notebook, PenLink, VASCO: Allow LEAs to visualize and analyze call and internet data.

Maltego and i2 Analyst’s Notebook: Known for network mapping and entity resolution.

However, these tools are often expensive, require expert handling, and lack adaptability to regional data formats.

3. KEY FEATURES

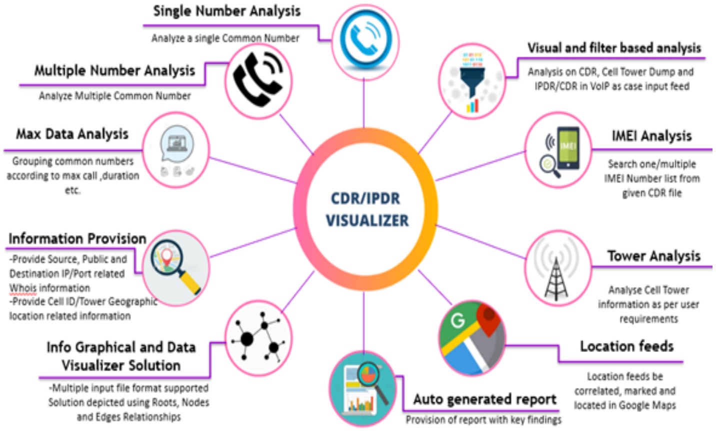
Single Number Analysis
Analyze a single Common Number
Multiple Number Analysis
Analyze Multiple Common Number
Max Data Analysis
Grouping common numbers according to max call ,duration etc.
Information Provision
-Provide Source, Public and Destination IP/Port related Whois information
-Provide Cell ID/Tower Geographic location related information
Info Graphical and Data Visualizer Solution
-Multiple input file format supported Solution depicted using Roots, Nodes and Edges Relationships
CDR/IPDR VISUALIZER
Visual and filter based analysis
Analysis on CDR, Cell Tower Dump and IPDR/CDR in VoIP as case input feed
IMEI Analysis
IMEI
Search one/multiple IMEI Number list from given CDR file
Tower Analysis
Analyse Cell Tower information as per user requirements
G
Location feeds
Location feeds be correlated, marked and located in Google Maps
Auto generated report
Provision of report with key findings

Figure 1 Features of CDR/IPDR

4. LIST OF FEATURES IN CDR MODULE

4.1. UPLOAD PAGE

- File Format Supported: XLSX, XLS, CSV, TXT, JSON and RTF.
- Multiple files supported in heterogeneous format (e.g.: XLSX+TXT+JSON)
- Maximum file upload size [Mongo db. Gridfs]:
- 2GB on 32-bit system
- Unlimited on 64-bit system

- 1 Lakh records processed in less than a minute.
- Multiple files from multiple operators supported (Airtel, Idea, Vodaphone, BSNL)
- Universal Data Table formats.
- Homogenous data after uploading (Predefined Headers are applied).
- GUI to map new header names to predefined headers.
- GUI to map new internal data headers to predefined internal headers.

DASHBOARD

- Summary of data in form of cards, graphs and map.
- Option to set preferences for cards.
- Interactive Graphs

NUMBER ANALYSIS (For Single as well as Multiple Numbers):

- View data: See unprocessed data.
- Master Filter Table:
- ▪ Filter by
- All Columns
- Date Range
- Duration
- Day / Night Calls
- Push SMS
- Remove Junk Calls
- Flagging Numbers by colour for criminal activity, In-radar/Suspect
- list and probable Suspect.
- Dynamically Filter data and use it in below submodules

SUMMARIZE DATA

- Max Caller Summary
- First and Last Call Summary
- First and Last Tower Locations
- Location History Per Suspect
- Interactive Graphs and Cell Tower Locations

SHOW PLOTS

- Show by Chart and Show by Column
- All Columns vs
- Sunburst Chart
- Pie
- Tree Map I
- Tree Map II
- Bar Plot
- Scatter Plot
- Stacked Bar Chart
- Horizontal Bar Chart
- Bubble Plot

- Line Plot

NODE ANALYSIS

- Interactive Graphical Nodes and edges relationships
- Make Root / Click and make root
- Search by Name or Number
- Filter minimum and maximum calls
- Find all paths between 2 parties
- Threshold slider for Node link duration

MAP ANALYSIS

- All tower locations
- Chronological line map connecting towers.
- Geo fencing

PATTERN ANALYSIS

- Find pattern in calls for each number
- Most probable associate using apriori algorithm
- Support for number found in pattern

IMEI ANALYSIS

- IMEI Change log
- IMSI Change log

TOWER ANALYSIS

- Tower location Slide show.
- Location History per suspect on basis of tower change.

QUICK ANALYSIS

- All summaries for unfiltered data
- Print report (PDF)
- Export report to Excel

SUSPECT ANALYSIS

- Find caller(s) in an area within the given time range.
  Search location by name
  Auto populate coordinates
- Frequency Based Suspect Analysis
  Call Frequency
  Call Duration
  Irregular Missed Calls
- Location Based Suspect Analysis
- Flag Criminals for Future Analysis
- Flag Suspects for Future Analysis

ADMIN

- Create, delete and update users.
- View other users file access and file export logs.

4.2. LIST OF FEATURES IN IPDR MODULE

UPLOAD PAGE

- Same as what we have in CDR module.

DASHBOARD

- Summary of data in form of cards, graphs and map.
- Option to set preferences for cards.
- Interactive Graphs

IP ANALYSIS:

- VIEW PERSONA:
- Master Filter Table
- Building User persona
- Finding Source ISP name and Address from Public Name
- Mapping Destination IP and Ports to it name and Address.

BUILD CORRELATION:

- Correlating user on the basis of Usage and Activity.
- Threshold Buffer to vary your Correlation analysis.
- Interactive Graph on the basis of Correlation.

DATA SUMMARY:

- Similar to CDR Module and Print Report, Export Feature Added.

SHOW PLOTS:

- Similar to CDR Module

NODE ANALYSIS:

- Interactive Graphical Nodes and edges relationships
- Make Root / Click and make root
- Threshold slider for Node link duration

5. CHALLENGES AND LIMITATIONS

- Privacy and Legal Restrictions: Stringent regulations on communication metadata handling.
- Data Quality Issues: Incomplete or inconsistent records from telecom providers.
- Scalability: Performance drops with millions of records if not optimized.
- Usability: Complex UI hampers adoption by non-technical officers.

6. FUTURE SCOPE

- AI-Driven Insights: Use of NLP and deep learning to infer hidden connections.
- Real-time Analysis: Streaming CDR/IPDR data from telecom operators.
- Cross-Border Investigations: Standardized data formats and APIs for international collaboration.
- Voice/SMS Content Analysis (Where Legal): Sentiment and context extraction from messages or transcripts.

7. CONCLUSION

The ability to analyse and visualize CDR/IPDR data effectively can dramatically enhance the investigative capabilities of law enforcement agencies. By integrating multi-format data ingestion, visual analytics, pattern recognition, and intelligent suspect ranking, such a system can provide critical insights into criminal networks. Developing an accessible, secure, and adaptable CDR/IPDR analyser and visualizer remains a priority for modern digital policing.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

R. Singh and N. Kaur, “Forensic analysis of CDR for criminal investigation,” International Journal of Computer Applications, vol. 168, no. 7, pp. 31–36, Jun. 2017.

A. Hussain et al., “CDR Analysis for Network Monitoring and Criminal Investigation,” Procedia Computer Science, vol. 78, pp. 428–434, 2016.

P. Angeline et al., “Crime Pattern Detection Using Call Detail Records,” Journal of Computer Science and Engineering, vol. 10, no. 2, pp. 45–52, 2019.

IBM i2 Analyst’s Notebook. [Online]. Available: https://www.ibm.com

Maltego Documentation. [Online]. Available: https://docs.maltego.com

V. Sharma, “Link Analysis Techniques in CDR for Criminal Network Investigation,” International Journal of Digital Crime and Forensics, vol. 12, no. 4, 2020.

S. Sharma, “Big Data Analytics in CDR Analysis for Security Agencies,” IEEE Access, vol. 8, pp. 132548–132561, 2020.

N. Jain et al., “Visual Analytics for Crime Link Detection,” Visual Informatics, vol. 3, no. 2, pp. 69–77, 2019.

D. Bansal, “A Review on Call Detail Record Analysis Tools,” IJERT, vol. 10, no. 1, Jan. 2021.

Telecom Regulatory Authority of India, “Guidelines on Call Detail Records (CDRs),” [Online].
Available: https://www.trai.gov.in