Proceedings of the Annual General Donald R. Keith Memorial Conference
West Point, New York, USA
April 23, 2026
A Regional Conference of the Society for Industrial and Systems Engineering

A Mobility Analytics Framework for Pattern-of-Life Analysis

Gabriel Dabkowski, Andrew Farrant, Patrick Lichtner, Jonathan Mallon, Haixing Yan, and Julia Coxen

Department of Systems Engineering, United States Military Academy, West Point, NY 10996

Corresponding author's Email: gabriel.d.dabkowski.mil@army.mil

Author Note: The authors of this report are extremely grateful for the guidance and assistance from our sponsors at USASOC. Their professionalism and willingness to include us in a real-world exercise was not only professionally enriching, but allowed us to gain a firsthand understanding of the challenges Special Operations face in handling mobile app metadata. The views expressed herein are those of the authors and do not reflect the position of the United States Military Academy, the Department of the Army, or the Department of War.

Abstract: Mobile application metadata leakage presents significant risk to the Operational Security (OPSEC) of US Forces. This research develops a mobility analytics framework to demonstrate vulnerabilities exploited through Pattern-of-Life (PoL) analysis. Existing literature on PoL analysis, data exploitation, data inference, and Mobility Analysis (MA) establish the basis for the methodology that frames the data analysis within our prototype application. Stakeholder interviews and observations from a United States Army Special Operations Command (USASOC) training exercise informed model design and established a need for specific capabilities. The result is a decision support tool named "Freyja" capable of identifying irregular individual movement, geofencing Named Areas of Interests (NAIs), and supporting PoL analysis-based inference. These capabilities, combined with an emphasis on model usability, support training exercises and further inform personnel on OPSEC.

Keywords: Pattern-of-Life, Device Metadata, Mobile App Leakage

1. Introduction

Metadata leakage presents a substantial threat to the Operational Security (OPSEC) of US Forces by exposing sensitive information that can be exploited to infer activities, locations, and patterns of life. To mitigate this risk, US Forces must understand both the mechanisms and potential consequences of metadata exploitation in operational settings. USASOC can leverage Pattern-of-Life (PoL) analysis tools derived from metadata leakage to illustrate vulnerabilities to personnel, improve training, and convey OPSEC risk to force and mission. Prior to deployment, USASOC units often participate in validation exercises based on operational mission demands and requirements. These exercises are complex, multi-dimensional validations of expertise across a wide range of competencies, including OPSEC preservation in the face of metadata analysis. Validating forces face a simulated opposing force with the ability to apply advanced analytic techniques and Mobility Analysis (MA) to infer sensitive behaviors. This project pursues an improvement to PoL and MA tools to aid the opposing force and improve the quality of training for US Forces.

Data is a key requirement for actionable intelligence. PoL and MA tools source, analyze, and visualize data fuel intelligence. This project builds upon a body of knowledge and develops customized tools that reveal behavioral information about device users. Stakeholder engagements supported the model design observations made during an exercise and identified objectives with necessary functions established during functional analysis. The engagement improved the quality of training and displaying the risk of metadata leakage will educate US Forces on how to avoid risk in future operations.

Our team attended a USASOC exercise from the operations center and observed that commonly targeted metadata includes device IDs, device activity, and geospatial-temporal data. Access vectors for metadata exploitation appear due to vulnerabilities within Application Programming Interface (API) security and API keys. Network traffic provides additional access to sensitive metadata. Intercepted network traffic, through faulty transport layer security (TLS), and encryption by malicious Wi-Fi and Bluetooth sniffing, add to data risk (Nguyen, Carminati, & Ferrari, 2024). Higher-permission network-based approaches can triangulate device position based on cell tower data (Sivan, Bitton, & Shabtai, 2019). Application permissions collect data on devices to improve experience, but this data collection presents leakage risks by recording accelerometer data, gyroscopic information, and precise locational data (Degirmenci, 2020). These access vectors illustrate the basis of metadata exploitation, with the greatest vulnerability emerging from geospatial-temporal data due to the variety of exploitation methods associated with this data type.

The established data for PoL and MA models uses geolocation coordinates that are paired with temporal markers to build sequence analysis capabilities (Ashbrook & Starner, 2002). Entropy-based mobility metrics now serve as gateways to behavioral interpretation by "[quantifying] the amount of predictable structure in an individual's life using an entropy metric," with high-entropy lives harder to predict (Eagle & Pentland, 2005). Here, entropy denotes the degree of uncertainty in an individual's movement pattern, where higher entropy reflects greater variability and reduced predictability.

These models form the basis for user deanonymization and inference. Mobility Markov Chains (MMC) exploited the Points of Interest (POIs) to characterize the mobility of individuals, with some MMCs yielding 45% reidentification rate and work/home location pair identification of 67-70% (Gambs et al., 2014). Individuals with high entropy and irregularity distinguish themselves in a larger population, encouraging more scrutiny into those individuals. Inference can be so invasive into life as to infer "measures of friendship" or job satisfaction when incorporating activity and mobility metadata (Eagle & Pentland, 2005).

2. Methodology

2.1 Problem Definition

Our initial problem statement addressed USASOC's concerns regarding OPSEC threats from unsecured sensors and devices. The authors' consultations focused on metadata exploitation and analysis. We conducted interviews with seven stakeholders, including former USASOC intelligence officers, Special Operations forces, data scientists, targeting officers, and a direct support training director through interviews and exposure at a validation exercise. A redefined problem statement and functional hierarchy form the basis of solution design. The redefined problem statement is as follows: Develop and assess a framework for PoL analysis that presents actionable information through modeled adversarial exploitation capabilities and communicates resulting risk to US Forces.

2.2 Solution Design

This project resulted in the prototyping of a software application designed to visualize and evaluate device metadata that exposes potential operational risks within USASOC simulated operational environments. Stakeholder findings indicated that data analysts avoid overly complex models with higher startup cost and prefer models with intuitive workflow. As a result, this group designed a system with a workflow that enables a minimal learning curve to encourage analyst adoption.

The model ingests device telemetry through a mobile application that simulates access that high-level app permissions grant. The application tracks and forwards metadata, denoting both active user interaction as well as passive sensing. The data includes {lat, lon} pairings coupled with associated timestamps, app usage statistics, accelerometer data, altitude, orientation, and eighteen other fields of data collection.

Freyja's five primary analytical tabs guide users through a structured workflow from raw telemetry data to behavioral insight. Targeting officers and intelligence professionals can leverage Freyja to enrich their analysis, identify anomalous patterns of life, and reveal individuals whose behavior may indicate malicious or operationally relevant activity. The first stage of analysis focuses on identifying unusual mobility behavior using the Path Traversal Metric (PTM). This metric summarizes an individual device's daily mobility patterns by way of a composite metric measuring spatial coverage, distance traveled, and temporal entropy. Analysts can visualize one-to-many devices and examine how a device's daily mobility score deviates from its historical mean. Days that fall significantly outside the expected range from their respective baseline may indicate abnormal behavior and constitute subsequent flagging for further investigation (See Figure 1a).

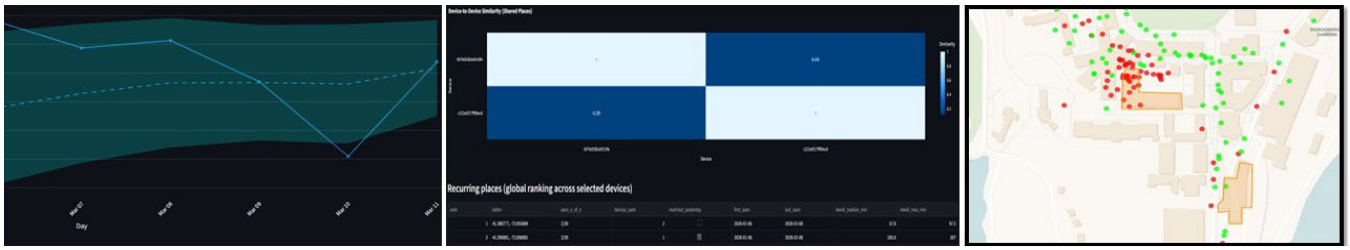
When the user identified the anomalous day, the user will then transition to the Device Locations tab for deeper inspection, focusing on the validation and authenticity of the collected metadata. The primary objective within this stage is to improve the authenticity of collected telemetry. The Device Locations tab provides analysts with several filtering controls designed to remove observations that are implausible or otherwise cluttering the dataset while preserving legitimate movement patterns. Analysts can configure three global filters: a minimum temporal separation between observations to prevent overly dense sampling, step distance that targets small positional fluctuations caused by GPS jitter, and a maximum speed threshold that filters impossibly fast movements that exist as outliers (See Figure 1b).

Following the cleansing of presumptively erroneous data from the telemetry dataset, the workflow continues into the Daily Mobility Summary tab, providing analysts with a consolidated view of an individual device's activity for a selected day. The system identifies key behavioral indicators such as total distance traveled, most likely wake-up and bed-down locations based on time-of-day clustering, and the device's most significant dwell locations. These locations are ranked by dwell time

and presented with arrival and departure timestamps. Additionally offered is Google Maps Streetview imagery of the locations ranking highest in dwell time, providing analysts an initial mental image to improve their inference capacity.

Working in tandem are the NAI Identification and NAI Geofencing tabs, which enable analysts to identify and evaluate locations of operational relevance across multiple devices. The NAI Identification tab compares movement patterns from selected devices, identifying locations visited by multiple devices. The NAI Geofencing tab allows analysts to build geofenced locations that aim to encapsulate overlapping behavioral patterns. Geographic boundaries fence named areas of interest (NAIs) that the system subsequently monitors for entry events, visit frequency and dwell durations for each device within the defined set. Repeated presence and extended dwell times within these geofenced areas can indicate meaningful behavioral patterns, allowing analysts to identify locations that may serve as shared meeting points and are worthy of physical surveillance (See Figure 1c).

The goal of Freyja is to provide analysts with different visualizations and means of understanding raw telemetry data. By structuring device metadata into interpretable metrics and visualizations, the system enables analysts to rapidly identify anomalous movement, automating the pipeline from raw data to identification of adversarial action. These analytical tools transform otherwise unstructured telemetry into insights that support PoL analysis and highlight OPSEC vulnerabilities.



(1a) (1b) (1c)

Figure 1. Frejya Tool Tabs. Pictured in Figure 1a: PTM, Figure 1b: Device Comparison by Location, Figure 1c: Geofenced NAIs

2.2.1 Optimal Coefficient of Jitter

The back-end application collects geospatial telemetry, recording device movement and metadata. The collected information significantly overrepresents both distance traveled and number of locations visited. This inflation occurs as a function of positional noise inherent to satellite-based navigation systems. Stakeholders identified that sources of error include satellite clock drift, orbital inaccuracy, receiver noise, and signal multipath. When uncorrected, these errors artificially inflate mobility metrics and degrade the reliability of downstream models that rely on these sources of data. This process uses a data source limited by the nature of the collected data pipeline which, by design, does not filter out jitter while collecting data. To better approximate true device movement and accurately represent authoritative behavior, the data incorporated into our models was processed through a series of filters designed to identify and remove suspected erroneous observations. Our filters include a sampling interval, targeting redundant high-frequency observations, a minimum step filter, targeting small movements below a user-defined threshold, and a max speed filter that flags and removes points that are impossibly fast (Chen, 2016).

Through iterative experimentation and validation, threshold values for each filter were tuned to minimize the presence of jitter while preserving legitimate mobility behavior. Because movement characteristics vary across modes of transportation, optimal threshold values were determined separately for walking/rucking, running, cycling, and vehicular travel. This filtering process produced a cleaned dataset specific to the inferred mode of travel that more accurately represents real-world device movement and serves as the foundation for the mobility and behavioral inference models that inform the targeting officers.

2.2.2 Path Traversal Metric

The PTM quantifies how extensively a device moves through space during a user-specified observation window. The PTM emphasizes the structure of movement, measuring traversal by concentration, transitions between grid squares, the uniqueness of that square and a normalized measure of distance traveled. The metric is designed to not solely reflect distance traveled but instead measure the pattern of transitions across spatial states, measuring behavioral complexity. Transition density, $H_{t,norm}$, spatial coverage, K, and normalized path length, D_{norm}, are integrated into a single composite metric (Equation 1) to reveal information about users similar to models in existing work (Schneider, 2013). Our PTM intends to balance structure and coverage and identify anomalous activity in contrast to respective device's historical precedent. The composite metric is a novel

approach towards identification of anomalous behavior, applying equations grounded in MA literature with additional parameters considered. PTM is defined by calculations with entropy, H, unique whatever, K, and distance, haversine equation.

$$PTM = \log(1+K) * (.25 + D_{Norm}) * (.5 + H_{t,Norm}) \quad (1)$$

2.3 Model Evaluation

The researchers measure user performance by comparing mean task completion times based on different categories of user (Expert, Expert-Trained, User-Trained, Novice). These categories represent varying levels of proficiency, allowing for analysis of how training and familiarity with the application impact performance.

To evaluate usability, the researchers implement a System Usability Scale (SUS) which measures perceived usability, effectiveness, efficiency, and user satisfaction. The surveys assess users with a Likert Scale based on their interaction with the model and produces an individual score for each user (Clark, 2021). The sample average of scores yields a system's SUS score. Usability can be evaluated based on this score, and more analysis on the confidence interval (CI) of the mean SUS score can produce greater insight into usability. In the context of this research, the SUS analysis was based on responses from research-group members who contributed to the generation of this model. SUS analysis results are subject to skew or bias when only a small number of users are evaluated (n<6) as the "CIs suffer from parameter bound violations and interval widths that confound mapping to adjective and other constructed scales," but this shortcoming can be avoided when using the expanded Bias Corrected and Accelerated (BCA) bootstrap CI with "comparable coverage and narrower or similar widths" (Clark, 2021).
The BCA methodology begins with a sample from a dataset. A bias correction factor, z_0 (Equation 2), quantifies bias of the sample. To account for skewness, the research group applied jackknife resampling (Equation 3) to calculate an acceleration factor *a* (Equation 4). These parameters are then used to adjust interval percentiles (Equation 5) which are used to construct bias corrected and accelerated confidence intervals (Equation 6) that more accurately reflect bias and skewness in our small sample size.

$$z_0 = \Phi^{-1}\frac{\left(\#\left(\hat{\theta}^{*b}<\hat{\theta}\right)\right)}{B} \quad (2) \qquad \bar{\theta}_{\cdot} = \frac{1}{n}\sum_{i=1}^{n}\hat{\theta}_{(i)} \quad (3)$$

$$a = \frac{\sum_{i=1}^{n}\left(\bar{\theta}_{\cdot}-\hat{\theta}_{(i)}\right)^3}{\left[\sum_{i=1}^{n}\left(\bar{\theta}_{\cdot}-\hat{\theta}_{(i)}\right)^2\right]^{3/2}} \quad (4) \qquad \alpha_1 = \Phi\left[z_0 + \frac{z_0+z_\alpha}{1-a(z_0+z_\alpha)}\right] \quad (5)$$

$$\left[\hat{\theta}_{(\alpha_1)}, \hat{\theta}_{(\alpha_2)}\right] \quad (6)$$

3. Results

3.1 Impact of Jitter Filtering on Positional Accuracy

To evaluate the effectiveness of the jitter filtering framework, the team collected a validation dataset using pre-determined routes of known distance. Team members carried mobile devices with data collection software during walking/rucking, running, biking and driving trials over routes whose ground-truth distances were independently established using Strava corroborated measurements. This provided a controlled means of comparing the raw distances reported by the telemetry stream against the cleaned distance produced after filtering. Because GPS jitter artificially inflates movement with the introduction of small false displacements and occasional positions jumps, the objective of this analysis was to determine whether the filtered trajectories more closely approximated the known route distance than the unfiltered data. Filter effectiveness was assessed by comparing the absolute error of the raw and cleaned distances estimated relative to ground truth for each activity trial. Let D_{gt} represent the ground truth distance, D_{Raw} the distance computed from unfiltered telemetry, and D_{clean} the distance computed after jitter filtering. Distance error was measured as the absolute difference between estimated and known distance. Improvement in positional accuracy was then quantified as the percentage reduction in error achieved by filtering. Summary statistics including mean absolute error and mean percent improvement were calculated separately for walking/rucking, running, biking, and driving to assess how filter performance varied across inferred modes of travel. The following equations detail the calculations the team used to assess effectiveness of the filter (See Equations 7-9).

$$E_{raw} = |D_{raw} - D_{gt}| \quad (7) \qquad E_{clean} = |D_{clean} - D_{gt}| \quad (8) \qquad Improvement(\%) = \frac{E_{raw} - E_{clean}}{E_{raw}} \times 100 \quad (9)$$

3.2 Model Usability Scoring

Six members of the group completed task evaluation consisting of three tasks: program setup, clean data, and identify key information. Tasks are further broken into 13 subtasks (ex: identify likely bed-down location, clean data using jitter filters, draw geofence around NAI 1, etc.). Completion time was recorded for each subtask with a cutoff of four minutes. Scores are categorized by user type and presented below in Table 1. A visualization of completion times is presented in Figure 2.

Table 1: Recorded Total Time of Task Completion Based on User Type

User Number	User Type	Total Time (Minutes)	SUS Score	Acceptability
1	Expert	4:55	92.5	Acceptable
2	Expert Trained	5:20	90.0	Acceptable
3	User Trained	7:50	72.5	Marginal
4	User Trained	6:00	55.0	Marginal
5	Novice	11:14	90.0	Acceptable
6	Novice	14:45	77.5	Marginal
		BCa CI	[55.0,91.1]	

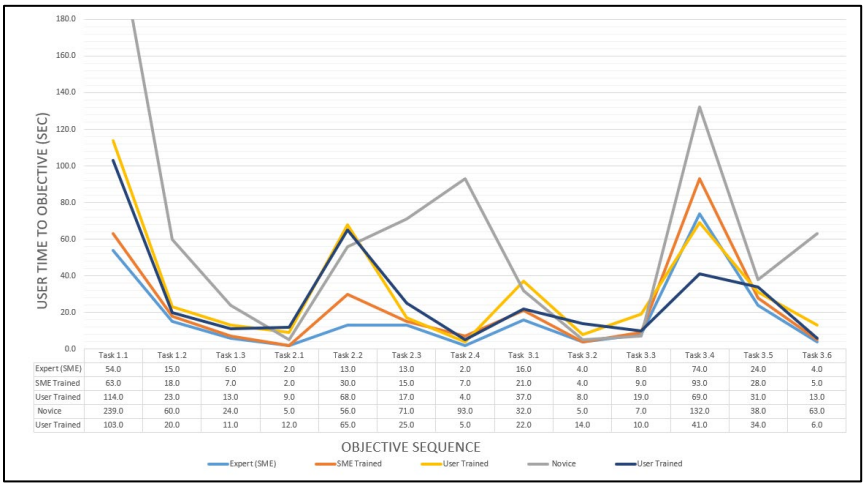


Figure 2. Task Completion Timesheet Graph

Time comparisons display that Expert-Trained took 8.5% longer to complete tasks than the Expert, the Users-Trained mean completion was 30% longer than the Expert-Trained, and the Novice mean time was 88% longer than the User-Trained mean. Following completion of task evaluation, all users participated in a SUS to record perceived usability of the system and raw scores with associated Acceptability Scale is present in Table 1.

The calculated SUS Score average when applying the BCA method is 79.58. This score is corrected for bias associated with small sample sizes ($n \leq 6$). The sample mean with a 95% CI of [55,91.07], translates to a "Good" on the adjective scale, and "Acceptable" on acceptability scale of perceived usability (Blattgerste, 2022). The width of the confidence interval limits its usefulness in precisely estimating a usability score. However, findings on task completion across user types suggest training appears to improve task efficiency for recommended Freyja prototype enhancements, and the documented SUS scores form a generally positive and acceptable level of perceived usability.

4. Conclusions and Future Work

This research demonstrates that mobile metadata can be transformed into operationally relevant PoL intelligence with direct implications for the US Army Special Operations Command. Drawing on stakeholder interviews, exercise observations, and building on established literature about mobility analysis, the authors developed Freyja, a prototype application designed to enhance inferential capacity on targeted behavioral mechanisms. The system applies user-defined jitter filters and variable thresholds to clean telemetry data for model analysis. The PTM then evaluates PoL across one-to-many devices to identify uncharacteristic behavior by comparing device activity between POIs. As a result, Freyja reduces error associated with noisy data while introducing enhanced capabilities for identifying and applying NAI theory.

Future work should evaluate the effectiveness of the PTM in differentiating between operational and non-operational days. In the current absence of predefined data, the PTM lacks demonstrated credibility in achieving its intended objective. A limitation of this model evaluation is the small sample size which restricts the strength of statistical takeaways. External validation in an operational environment would further support model refinement and improve system usability and user performance. Additionally, Freyja can be expanded by integrating new tools based on existing access vectors to include data from wearable devices, Bluetooth or Wi-Fi sniffing interfaces, and accelerometer data to visualize devices in space. All these tools can be tailored to target the specific needs of operational forces.

5. Citations and References

Blattgerste, Jonas, Jan Behrends, and Thies Pfeiffer. “A Web-Based Analysis Toolkit for the System Usability Scale.” In *Proceedings of the 15th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA ’22)*, 237–246. New York: Association for Computing Machinery, 2022. https://doi.org/10.1145/3529190.3529216

Chen, Xiao-Jian & Cui, Tingting & Fu, Jianhong & Peng, Jianwei & Shan, Jie. (2016). Trend-Residual Dual Modeling for Detection of Outliers in Low-Cost GPS Trajectories. Sensors. 16. 2036. 10.3390/s16122036.

Clark, Nicholas, Matthew Dabkowski, Patrick J. Driscoll, Dereck Kennedy, Ian Kloo, and Heidy Shi. “Empirical Decision Rules for Improving the Uncertainty Reporting of Small Sample System Usability Scale Scores.” *International Journal of Human–Computer Interaction* 37, no. 13 (2021): 1191–1206. https://doi.org/10.1080/10447318.2020.1870831

D. Ashbrook and T. Starner. (2016). "Learning significant locations and predicting user movement with GPS," *Proceedings of the Sixth International Symposium on Wearable Computers*, Seattle, WA, USA, 2002, pp. 101-108, doi: 10.1109/ISWC.2002.1167224.

Degirmenci, K. (2020). Mobile users’ information privacy concerns and the role of app permission requests. *International Journal of Information Management, 50*, 261–272. https://doi.org/10.1016/j.ijinfomgt.2019.05.010.

Eagle, N., (Sandy) Pentland, A. (2005). “Reality mining: sensing complex social systems.” *Pers Ubiquit Comput* **10**, 255–268. https://doi.org/10.1007/s00779-005-0046-3

Gambs, S., Killijian, M.-O., & Núñez Del Prado Cortez, M. (2014). *De-anonymization attack on geolocated data*. *Journal of Computer and System Sciences, 80*(8), 1597–1614. https://doi.org/10.1016/j.jcss.2014.04.024.

Nguyen, T. T. L., Carminati, B., & Ferrari, E. (2024). *MetaLeak: Assessing image metadata leakage in Android apps*. In *Proceedings of the 2024 21st ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)*. IEEE

Schneider, Christian & Belik, Vitaly & Couronné, Thomas & Smoreda, Zbigniew & Gonzalez, Marta C.. (2013). Unravelling daily human mobility motifs. Journal of the Royal Society, Interface / the Royal Society. 10. 20130246. 10.1098/rsif.2013.0246.

Sivan, N., Bitton, R., & Shabtai, A. (2019, September). *Analysis of location data leakage in the Internet traffic of Android-based mobile devices*. In *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)* (pp. 243-260). USENIX Association. https://www.usenix.org/system/files/raid2019-sivan.pdf.