Towards Fast Detection of Suspicious Bluetooth Trackers Using Anomaly Detection

Orobosa Ekhator — Portland State University

Dylan Conklin — Portland State University

Primal Pappachan — Portland State University

Roberto Yus — University of Maryland, Baltimore County

Motivation

Why?

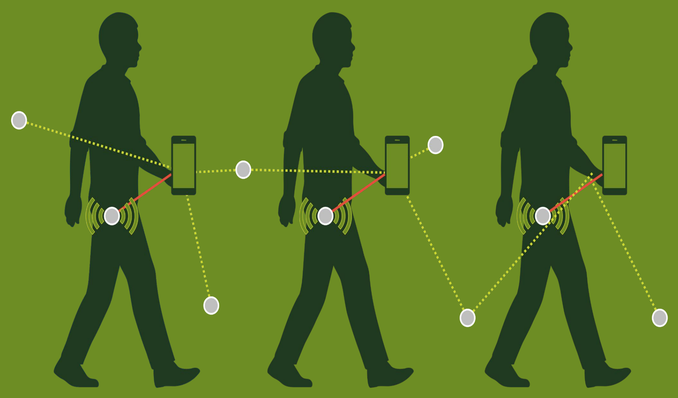
Bluetooth Low Energy (BLE) trackers are devices that can be used to locate lost items, but they are commonly misused for stalking because of their convenience and small size[1]. Such devices include AirTags, Tiles, SmartTags, PebbleBees and Chipolos.

Current Approaches

BLE tracking alert approaches do not adequately alert users, partially due to device incompatibilities and lack of manufacturer participation. Existing approaches [2, 3] addresses these problems, but have limitations because of the static time and distance thresholds used to determine risk.

How?

CBLOF introduces a data-driven anomaly detection method together with a gap thresholding mechanism to identify suspicious devices based on risk factors. Our model is able to detect these suspicious devices in 5 minutes.



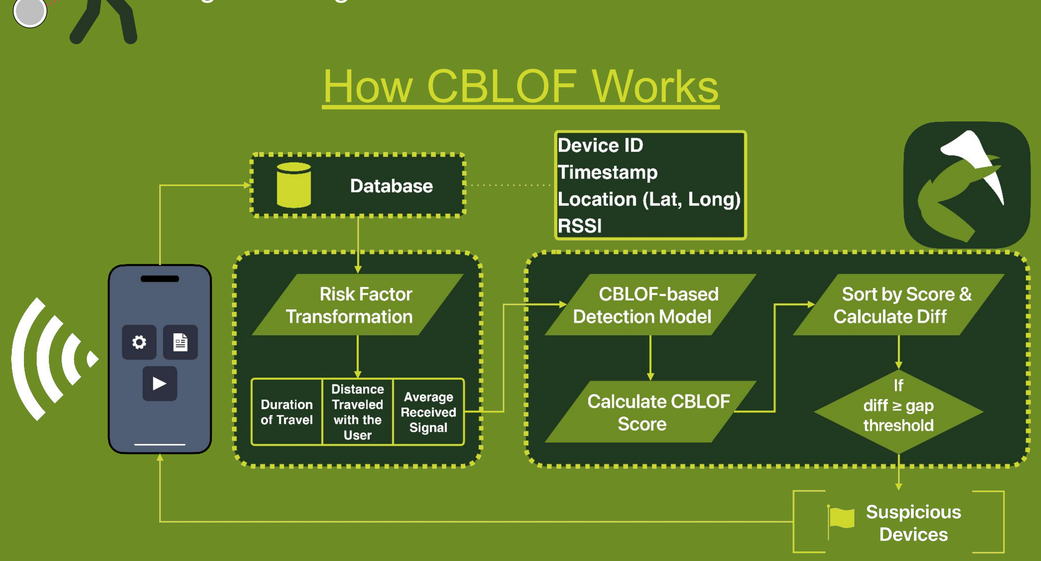
Risk Factors

Duration of travel: Measures the duration of time a device is near the user

Distance Travelled with User: The distance a device has travelled near the user

Average Signal Strength: Measures the device's average signal strength via RSSI

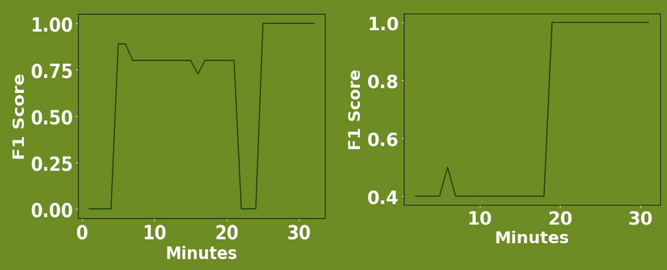
How CBLOF Works



1. Run the K-means Algorithm on risk factors to form k clusters.
2. Sort clusters by size in descending order:

   $| C1 | \geq | C2 | \geq \cdots \geq | Ck |$
3. Determine Large Clusters (LC) and Small clusters (SC) using alpha (α) and beta (β) parameters.
4. Calculate CBLOF scores for each device in LC and SC.
5. Sort CBLOF scores in descending order and calculate the differences between consecutive scores.
6. The anomaly boundary is set to the first instance where the difference exceeds the calibrated gap threshold (δ). Devices with scores above this boundary are classified as suspicious.

Results



Future Work

1. Evaluate the model's robustness across more diverse and large-scale scenarios
2. Explore different density-based clustering techniques, such as DBScan

References

[1] Heinrich. et al., "Please Unstalk Me: Understanding Stalking with Bluetooth Trackers and Democratizing Anti-Stalking Protection," PoPETs 2024.

[2] Heinrich. et al., "Airguard - Protecting Android Users from Stalking Attacks by Apple Find My Devices," ACM WiSec 2022.

[3] Briggs. et al., "BLE-Doubt: Smartphone-Based Detection of Malicious Bluetooth Trackers," IEEE SafeThings 2022.

Database and Internet Privacy Lab

Portland State UNIVERSITY