System and Method for Context-Aware Social Interaction Based on Shared Transit Routes

Technical Field

This invention relates to mobile computing systems that enable asynchronous and privacy-preserving social interaction. It focuses on device-local sensor fusion, semantic reflection matching, and dual-consent mechanisms for users who share physical space within public transit infrastructure. In addition, the invention provides concrete improvements in mobile device efficiency by reducing processor cycles and energy consumption through optimized on-device computation.

Introduction and Background of the Invention

Social discovery applications such as Tinder, Bumble, and Hinge rely on user-declared location data and server-mediated profile browsing to facilitate interaction. While not strictly proximity-based in the sense of real-time device-to-device detection, these systems require periodic internet connectivity and location sharing. This raises persistent concerns regarding privacy, energy consumption, and reliance on continuous connectivity. Moreover, they are ill-suited for infrastructure-limited environments such as underground public transport, where network access is unavailable and real-time interaction is impractical.

In addition, conventional systems prioritize synchronous engagement, requiring users to be discoverable and willing to interact in real time. They provide limited support for retrospective or memory-based encounters, and typically lack mechanisms for private, dual-consent reconnection after an event has passed.

This invention addresses those limitations by enabling asynchronous, context-aware, privacy-preserving social interaction using on-device computation. It passively captures co-location metadata, stores it locally in encrypted form, and allows semantic matching of user-submitted reflections at a later time. User identity and contact potential are disclosed only after mutual consent, enabling

delayed engagement and secure, server-free interaction suitable for dynamic or disconnected environments.

Summary of the Invention

The invention provides a system and method for enabling asynchronous, privacy-preserving social interaction using mobile devices equipped with multimodal sensors, including Bluetooth Low Energy (BLE), GPS, WiFi, and inertial motion components.

The system detects co-location events within predefined spatial and temporal thresholds and stores associated metadata locally in encrypted form. Users may later submit reflections in natural language, which are processed into semantic embeddings using transformer-based or equivalent lightweight language models optimized for on-device execution. Similarity between embeddings is determined using one or more vector distance metrics, and matches exceeding a configurable threshold trigger a dual-consent workflow in which identity and communication are revealed only upon mutual opt-in.

This architecture supports local-only computation and data retention, ensuring that user information remains private and functional even in disconnected environments such as underground transit. Efficiency is further achieved through quantization, pruning, and other model optimization techniques that reduce energy consumption on resource-constrained devices. Privacy is enhanced by optional mechanisms, including noise injection to the embedding process and automatic expiration of unmatched reflections.

By combining spatiotemporal sensing, semantic matching, and a consent-gated reveal process, the invention delivers a technical improvement over prior art systems that rely on continuous connectivity, centralized servers, or real-time broadcast visibility.

Introduction to the Detailed Description

The following description provides a detailed explanation of the invention's components, workflows, and interactions. Each figure corresponds to a subsystem or interaction flow and is cross-referenced by element identifiers. Together, these figures illustrate how the system initializes, detects co-location, logs moments, captures reflections, performs semantic matching, and manages consent and privacy.

Detailed Description of the Invention

Figure 1: Initialization and Permission Workflow

The system begins when the user signs in and grants permissions (location, Bluetooth, motion). These permissions activate background sensing services: GPS/WiFi for geofencing, BLE for proximity detection, and motion sensors for activity recognition. All outputs are processed by a local encryption module and stored securely on-device

Figure 2: Convergence Detection and Event Logging

While users are in transit, the system monitors for co-presence. A co-location detector checks whether users share the same geofence for a minimum duration. Optionally, if either user opens the app, this serves as an intent signal. Qualified encounters are logged as "Moments" with time, location, and anonymized metadata.

Figure 3: Reflection Interface for User Input

At a later time, users may open the app and receive prompts to create reflections. The reflection interface auto-fills contextual data (time, location) and allows user entry of descriptive tags and free text. Submitted reflections are saved locally for subsequent semantic processing.

Figure 4: Semantic Matching and Consent Workflow

When multiple users submit reflections, the system compares metadata and semantic embeddings. If alignment exceeds threshold criteria, both users are notified. Identity and communication are enabled only when both confirm via the dual-consent "Loop Back" mechanism. Unconfirmed matches expire automatically after a set period.

Figure 5: Privacy Control and Data Management

Users can opt out at any time, which deletes all local data. Otherwise, reflections are subject to auto-expiration and anonymized archiving. Privacy controls therefore balance user autonomy with system continuity.

Natural Language Processing Pipeline (NLP) for Semantic Matching

- Tokenization and Normalization
- Embedding Generator (e.g MobileBERT)
- Vector Storage
- Cosine Similarity Engine
- Match Threshold Decision Logic

Reflections are tokenized and normalized, transformed into embeddings using MobileBERT or similar models, and stored in a local vector index. The system then calculates cosine similarity between current and stored vectors. Matches are flagged if similarity exceeds a tunable threshold, triggering the consent workflow described in figure 4. Embedding generation leverages quantization when hardware supports it, optimizing for execution on mobile processors with 4GB RAM.

Algorithms and Pseudocode

Dynamic Threshold Adjustment Algorithm

```
function adjust_threshold(embedding_density, user_feedback):
    base_threshold = 0.80
    if embedding_density > HIGH_DENSITY:
        base_threshold += 0.05    # tighten to reduce false positives
    if embedding_density < LOW_DENSITY:
        base_threshold -= 0.05    # loosen to capture sparse matches
    if user_feedback == "false_positive":
        base_threshold += 0.02
    if user_feedback == "missed_match":
        base_threshold -= 0.02
    return clamp(base_threshold, 0.70, 0.95)
```

Differential Privacy Noise Injection for Embeddings

```
function add_dp_noise(embedding_vector, epsilon):
    noise_scale = 1.0 / epsilon
    for i in range(len(embedding_vector)):
        noise = random_laplace(0, noise_scale)
        embedding_vector[i] += noise
```

```
return embedding_vector
```

Hardware Requirements and Efficiency Constraints

The system is optimized for mobile execution on devices with at least 4 GB of RAM and ARM-based processors supporting ML acceleration. Reflection embeddings of up to 50 words can be generated in approximately 150 ms using quantized transformer models. Matching operations run asynchronously to avoid UI latency. Lightweight fallback models are supported for devices with lower resources.

Non-Transitory Computer-Readable Medium

Software instructions configured to perform the following operations are stored on a non-transitory computer-readable medium:

- Passive sensing of transit-based events using multimodal sensors
- Encryption and local storage of convergence metadata
- Prompting users to submit memory-based reflections
- Converting text input to embeddings via NLP models
- Matching embeddings via vector distance metrics
- Managing consent and initiating communication only upon dual opt-in
- Executing privacy-preserving data management, including optional differential privacy

Technical Advantages Over Prior Art

- No Real-Time Discoverability: System does not broadcast user presence.
- Fully On-Device: All inference, storage, and matching occur locally.
- Semantic NLP Matching: Reflections are compared using embeddings, not rigid metadata.

- Consent-Gated Identity Reveal: Profiles are unblurred only after mutual consent.
- Offline Operability: Works in disconnected environments such as subway tunnels.
- Modular Fault Tolerance: Supports delayed input and failed matches.
- Differential Privacy Optionality: Optional noise injection strengthens privacy.
- False Positive Suppression: Multi-factor validation reduces spurious matches.
- Partial Match Handling: Expiration, feedback, and persistence controls.
- Mobile Device Efficiency: The invention reduces processor cycles and battery drain via quantization, pruning, and efficient on-device inference.

Independent Claim 1

1. A system for privacy-preserving asynchronous social interaction, comprising:
    - at least one wireless sensor configured to detect spatiotemporal proximity between mobile devices, the wireless sensor selected from the group consisting of Bluetooth Low Energy (BLE), Global Positioning System (GPS), WiFi, and inertial motion sensors,
    - a local memory storing encrypted, anonymized metadata representing co-location events,
    - a natural language processing (NLP) module configured to:

generate semantic embeddings from user-submitted reflections using a transformer-based or equivalent embedding model, and

compute similarity between embeddings to identify matches exceeding a threshold,

- dual-consent module configured to initiate identity disclosure and enable communication only upon mutual opt-in by both users within a predefined consent window.

Independent Claim 2

2. A computer-implemented method for privacy-preserving asynchronous social interaction, the method comprising:

- detecting spatiotemporal proximity between at least two mobile devices using at least one wireless sensor,
- storing metadata representing the detected proximity in encrypted form on a local memory,
- receiving user-submitted reflections comprising natural language input,
- generating embeddings from the reflections using a transformer-based or equivalent embedding model,
- comparing the embeddings to stored embeddings to determine similarity,
- and revealing user identity and enabling communication only upon mutual confirmation from both users within a predefined consent window.

Dependent Claims

3. The system or method of claim 1 or 2, wherein the similarity is determined using a vector distance metric selected from the group consisting of cosine similarity, Euclidean distance, or Manhattan distance.
4. The system or method of claim 1 or 2, wherein the threshold for similarity is dynamically adjusted based on embedding density or user feedback.
5. The system or method of claim 1 or 2, wherein the NLP module applies quantization or pruning to the embedding model to optimize execution on mobile hardware.
6. The system or method of claim 1 or 2, further comprising a differential privacy module configured to inject calibrated noise into the embeddings prior to similarity comparison.
7. The system or method of claim 1 or 2, wherein anonymized status notifications are displayed for unmatched reflections within the consent window.

8. The system or method of claim 1 or 2, wherein stored reflections are automatically deleted after expiration of the consent window unless extended by the user.
9. The system or method of claim 1 or 2, wherein proximity detection requires simultaneous satisfaction of spatial and temporal thresholds.
10. A non-transitory computer-readable medium storing instructions that, when executed by a mobile device, perform the steps of the method of claim 2.

Abstract

A system and method for asynchronous, privacy-preserving social interaction within transit and similar environments is disclosed. Mobile devices equipped with multimodal sensors, including Bluetooth Low Energy (BLE), GPS, WiFi, and motion components, detect co-location events within defined spatial and temporal thresholds. Metadata representing these events is stored locally in encrypted form. Users may later submit natural language reflections, which are converted into semantic embeddings using lightweight models optimized for on-device execution. The system compares embeddings using similarity metrics to identify potential matches. A dual-consent mechanism ensures that user identity and communication are revealed only when both parties opt in within a predefined consent window. Optional privacy-preserving features include differential privacy noise injection, automatic expiration of unmatched reflections, and model quantization to improve device efficiency. By combining spatiotemporal sensing, semantic reflection matching, and consent-gated identity disclosure, the invention enables offline-compatible social discovery that improves privacy, efficiency, and scalability