NEXUS: Using Geo-fencing Services without revealing your Location

Michael Guldner, Torsten Spieldenner*, René Schubotz
German Research Center for Artificial Intelligence (DFKI)
(* Saarbrücken Graduate School of Computer Science)
66123 Saarbrücken, Germany
Email: {firstname.lastname}@dfki.de

Abstract—While becoming more and more present in our
every day lives, services that operate on users’ locations or
location trajectories suffer from general fear of misappropri-
ation of the transmitted location data. Several works have
investigated of how to cope with this drawback. Respective
systems claim location-privacy, i.e. keeping users’ locations
secret, by employing anonymisation techniques concerning a
user’s identity, or by obfuscating the transmitted location.
These approaches lead to a degrade of quality-of-service and
can be vulnerable to de-anonymisation attacks, or allow to
learn at least the approximate location of a user. Focusing on
the application domain of geo-fencing, we present as remedy a
protocol that is based on homomorphic encryption of a user’s
location. The protocol provably provides full location-privacy
by non-exposure of the users’ location data, while producing
exact geo-fencing results. We provide a detailed definition of
the protocol, show its applicability in an actual geo-fencing
application, and show that the resulting system fulfills all
security properties we see for a location-privacy preserving
system.

Keywords—location-based service; geo-fencing; data privacy;
location privacy

I. INTRODUCTION

Location-based services [1], [2] are information services
accessible with mobile devices through the mobile network.
They utilise the ability to access, store and analyse real-time
geographic information from mobile devices, and, in turn,
provide service offerings such as orientation and localisation,
navigation, search, identification or checking [3].

Despite considerable user uptake, e.g., in real-time social
systems [4], [5] or travel-related applications [6], [7], and
promising potentials in commerce [8] or smart cities [9],
[10], widespread adoption of location-based services is im-
peded by specific concerns regarding location privacy [11]
and general fear of misappropriation [12].

These qualms hold in particular for location-tracking
services [13], i.e. location-based services that capture or
predict users’ location trajectories. One prime example of
location-tracking services is geo-fencing, a class of location-
based services that trigger actions or fire events whenever
mobile devices enter or exit virtual perimeters set up for
geographical areas known as geo-fences.

Clearly, a straight-forward approach to avoid misappropri-
iation of users’ location data, are client-based approaches
that perform all processing of location information locally
on the mobile device. But not only can entirely client-
based approaches come with several drawbacks [14], they
moreover require mobile devices to constantly perform com-
putations against geo-fences locally, using processing power
and draining battery of the device.

This paper is therefore concerned with designing a pro-
tocol for network- and cloud-based privacy-preserving geo-
fencing services that provably does not leak any location
information to any party that is involved with the geo-
fencing evaluation.

Towards this end, we present NEXUS (Non-Exposure
User location privacy System), a protocol for multi-party
geo-fencing evaluation that employs an asymmetric, ho-
omorphic encryption scheme to satisfy non-exposure of
the users location, non-exposure of the geo-fences, and
computational correctness of the geo-fencing evaluation. The
presented approach has been prototypically implemented,
being efficient enough to be employed in actual geo-fencing
applications.

The remainder of this paper is organised as follows: Sec-
tion II discusses the related literature on privacy preservation
in location-based services. System assumptions, an advers-
sarial model, as well as properties that a location-privacy
preserving system should fulfill, are described in Section III.
Our NEXUS protocol for location privacy-preserving geo-
fencing evaluation is presented in Section IV, along with
an algorithm that, based on the NEXUS protocol, correctly
evaluates rectangular-shaped geo-fences; the fulfillment of
the previously stated location-privacy properties is discussed
subsequently. We conclude with summary and future work
in Section VII.

II. RELATED WORK

The available literature on location privacy preservation
techniques is vast, and can be categorised into four working
principles. We briefly outline the underlying key ideas and
refer the interested reader to representative works in each
category.

Regulation: Legal frameworks [15] governing collection,
processing and distribution of individuals’ location infor-
mation have been established in most nations. However,
regulation itself cannot prevent invasion of privacy, often
lags behind new technology and innovations, and might stifle location-aware applications.

**Policy-based approaches** [16], [17] address the definition of trust-based mechanisms for proscribing certain uses of location information. These mechanisms are often highly complex and of questionable practicality for highly dynamic location-aware environments. More importantly, policy systems rely on extratechnological pressures to ensure privacy policies are adhered to.

**Anonymisation** approaches rely on the notation of k-anonymity, i.e. a node is made indistinguishable from at least \( k - 1 \) other nodes, to prevent location privacy invasion. Popular techniques for achieving k-anonymity are location cloaking [18], [19], controlled flooding [20] or obfuscation [21], to name a few. Pseudonymisation [22], a variation of anonymisation, assigns persistent but non-identifying pseudonyms to individuals. Anonymisation is by far the most popular approach to (location) privacy preservation, however, it presents a barrier to authentication and personalisation, deliberately degrades quality-of-service, and exhibits vulnerabilities to de-anonymisation [23].

**Secure multi-party computations** (SMPC) enables parties to jointly compute an arbitrary agreed function of their private inputs with the computation results guaranteed to be correct. Prior works investigate multi-party computational geometry [24], [25], [26], privacy-preserving proximity detection in a two-party setting [27], privacy-preserving algorithms for determining fair multi-party rendez-vous points [28] or nearest-neighbor queries [20]. Although closest to our approach, we are not aware of secure multi-party protocols for privacy-preserving geo-fencing.

### III. System, Adversary and Requirements

In the following, we model a geo-fencing system and a privacy-invading adversary. Ensuing, the privacy properties that our solution should satisfy are outlined.

**System Model.** We assume the existence of a set of mobile nodes \( \mathcal{M} \), a geo-fencing service \( \mathcal{G} \), and a set of nodes \( S \) subscribed to geo-fencing events generated by \( \mathcal{G} \).

Each node \( M_i \in \mathcal{M} \) may periodically publish its location information in the form \((M_i, \mathcal{E}(\mathbf{L}))\) to the geo-fencing service \( \mathcal{G} \), where \( \mathbf{L} \in \mathbb{R}^2 \) specifies \( M_i \)'s current location and \( \mathcal{E}(\mathbf{L}) \) denotes a representation of \( \mathbf{L} \) suitable for our concerns.

The service \( \mathcal{G} \) manages a number of geo-fences, each of which is a tuple of the form \((\mathbf{F}, S' \subseteq S)\). We denote a geo-fence's boundary with \( \mathbf{F} \), and restrict ourselves to rectangles on the \( \mathbb{R}^2 \) plane, thus \( \mathbf{F} = \{A, B, C, D\} \). The set \( S' \) contains the nodes subscribed to the geo-fencing events for \((\mathbf{F}, S' \subseteq S)\) as generated by \( \mathcal{G} \).

Upon receiving a tuple \((M_i, \mathcal{E}(\mathbf{L}))\), \( \mathcal{G} \) determines if \( M_i \) is inside or outside of any eligible geo-fence \((\mathbf{F}, S')\) by evaluating

\[
f(\mathcal{E}(\mathbf{L}), \mathbf{F}) = \begin{cases} 1, & \mathbf{L} \in \mathbf{F} \\ 0, & \mathbf{L} \notin \mathbf{F} \end{cases}
\]

using solely \( \mathcal{E}(\mathbf{L}) \) and \( \mathbf{F} \).

Based on \( f(\mathcal{E}(\mathbf{L}), \mathbf{F}) \), \( \mathcal{G} \) issues notifications to the subscribers in \( S' \). Hence, a subscriber \( s \in S' \) is informed about whether or not a mobile node \( M_i \in \mathcal{M} \) is within the geo-fence to which \( s \) was subscribed, however, \( s \) has no knowledge about the particular geo-fence itself.

**Adversary Model.** Attacking the system as modeled above, the adversary primarily intends to break a mobile node’s location privacy. That is, the adversary will try to systematically and secretly record any \( M_i \)'s current or past location for later use.

We assume that mobile nodes in \( \mathcal{M} \) publish their locations correctly, and that they cannot be physically tracked by the adversary. Secondly, we assume \( \mathcal{G} \) and nodes in \( S \) to be semi-honest, i.e. these nodes run the protocol exactly as specified but may try to learn as much as possible about the locations of nodes in \( \mathcal{M} \). Finally, we consider the adversary to be computationally bounded.

**Privacy Properties.** The properties that we intend to provide for a geo-fencing system in the presence of privacy-invading adversaries are given as follows:

(P1) **Location Non-Exposition.** No party must be must able to obtain \( M_i \)'s current or past location from interaction or observation.

(P2) **Location Privacy Preservation.** No party must be able to learn or deduce \( M_i \)'s current or past location from interaction or observation.

(P3) **Computational Correctness.** Semi-honest parties are guaranteed to produce the correct outputs.

(P4) **Network Assistedness.** Since completely client-oriented approaches present several drawbacks [14], some information about a mobile nodes’ locations must be published to a remote party to not leave all crucial computations to the clients (in our case, the mobile nodes).

To the best of our knowledge, no previous study has investigated properties (P1) - (P4) in our context. As outlined before, regulation and policy-based systems rely on extratechnological pressures to ensure privacy; anonymisation-based approaches certainly violate (P1) and (P3) and exhibit vulnerabilities with respect to (P2); SMPC approaches do not yet address geo-fencing services at all.

### IV. Protocol Specification and Implementation

Obviously, encryption seems to be a suitable way to represent \( \mathbf{L} \) to \( \mathcal{G} \). The chosen encryption scheme needs to
provide certain characteristics to allow evaluation of $f$ solely based on $\mathcal{E}(\mathbf{L})$.

For this, in the following, we first provide some basics about cryptography and homomorphic encryption. Ensuing, we introduce our Non-Exposure User location privacy System (NEXUS) protocol for geo-fencing services, based on a homomorphic public key encryption scheme. Finally, we provide an overview of our prototype implementation and detail on how to perform geo-fence containment tests within the constraints of our chosen encryption system.

**Preliminaries.** A conventional encryption scheme consists of the following functions:

- **Key generation function** generates a symmetric encryption and decryption key $ek$ or an asymmetric key pair $(pk, sk)$ based on some parameter.
- **Encryption function** $\mathcal{E}_k(x)$ outputs a ciphertext from plaintext $x$ using a key $k$.
- **Decryption function** $\mathcal{D}_k(x)$ outputs a plaintext from ciphertext $x$ using a key $k$.

For any plaintext $x$, one has $\mathcal{D}_{ek}(\mathcal{E}_k(x)) = x$ for symmetric schemes and $\mathcal{D}_{ek}(\mathcal{E}_k(x)) = x$ for asymmetric encryption schemes.

In addition, homomorphic encryption [30], [31] features characteristics

$$\mathcal{E}_k(m_1) \odot \mathcal{E}_k(m_2) = \mathcal{E}_k(m_1 \cdot m_2)$$

In other words, a homomorphic encryption scheme enables specific computations on ciphertexts and generates encrypted results which, when decrypted, match the results of operations performed on the respective plaintexts.

We will in the following show that homomorphic encryption is thus suitable to evaluate $f$ in Equation (1) solely by the provided $\mathcal{E}_k(\mathbf{L})$, as required. As homomorphic encryption requires to encrypt all operands with the same key (cf. Equation (2)), the chosen encryption scheme must be a public key encryption scheme, as otherwise, parties that need to encrypt values during the process could use the symmetric key to decrypt $\mathcal{E}_k(\mathbf{L})$.

**Protocol.** Our protocol is based on a public key infrastructure (PKI) and a suitable homomorphic encryption scheme. We do not rely on the geo-fencing service $\mathcal{G}$ acting as a trusted third party (TTP), but rather on the collaboration of $\mathcal{G}$ and a certificate authority and evaluation service $\mathcal{A}$ taking the role to provide network assistedness. Hence, we extend our system model as indicated in Figure 1. The protocol then is as follows:

1. The certificate authority $\mathcal{A}$ generates a public-private key pair $(pk, sk)$ and shares $pk$ on demand with every other party.
2. Each $M_i$ may periodically send information about its location $\mathbf{L}$ in the form $(M_i, \mathcal{E}_\mathbf{pk}(\mathbf{L}))$ to $\mathcal{G}$.
3. $\mathcal{G}$ can not decrypt $\mathcal{E}_\mathbf{pk}(\mathbf{L})$ or any results of homomorphic computations based on $\mathcal{E}_\mathbf{pk}(\mathbf{L})$, but instead homomorphically computes an (encrypted) intermediate result $\mathbf{R}$ as

$$\mathbf{R} = f_\mathcal{G}(\mathcal{E}_\mathbf{pk}(\mathbf{L}), \mathbf{F})$$

with $f_\mathcal{G}$ being a function that homomorphically operates on $\mathcal{E}_\mathbf{pk}(\mathbf{L})$, and $\mathbf{F}$ the boundary of a geo-fence $(\mathbf{F}, S')$ as defined in Section III. $\mathcal{G}$ can encrypt $\mathbf{F}$ with $pk$ for homomorphic operations, where necessary.
4. $\mathcal{G}$ passes $\mathbf{R}$, the ID of the mobile node $M_i$, and the set of subscription nodes $S'$ that are to be invoked based on the evaluation result to $\mathcal{A}$.
5. $\mathcal{A}$ then evaluates $\mathbf{L} \in \mathbf{F}$ by an evaluation function $f_A$, such that

$$\mathbf{L} \in \mathbf{F} \iff f_A(\mathbf{R}) = \text{true}$$

$\mathcal{A}$ can decrypt $\mathbf{R}$ with $sk$, where necessary. By this, $f$ as given in Equation (1) is computed as

$$f(\mathcal{E}_\mathbf{pk}(\mathbf{L}), \mathbf{F}) = [f_A \circ f_\mathcal{G}](\mathcal{E}_\mathbf{pk}(\mathbf{L}), \mathbf{F})$$

6. $\mathcal{A}$ will invoke the respective subscriber $s \in S'$ with the result of the evaluation and the ID of the mobile node $M_i$.

**Implementation.** We base our implementation of above protocol on the Paillier encryption scheme. Implementation details concerning key generation, encryption, and decryption functions are found in [32]. Paillier features homomorphic addition:

$$\mathcal{E}_k(m_1) \oplus \mathcal{E}_k(m_2) = \mathcal{E}_k(m_1 + m_2), \quad (4)$$

and pseudo-homomorphic multiplication of a ciphertext by an unsigned integer $u$:

$$\mathcal{E}_k(m)^u = \mathcal{E}_k(u \ast m), \quad (5)$$

with $+$ and $\ast$ being arithmetic addition and multiplication.

Moreover, using Equations (4) and (5), we can homomorphically subtract by adding a negated ciphertext.

$$\mathcal{E}_k(m_1) \ominus \mathcal{E}_k(m_2) = \mathcal{E}_k(m_1) \oplus \mathcal{E}_k(m_2)^{-1} = \mathcal{E}_k(m_1 - m_2), \quad (6)$$
In our implementation, every position is a two dimensional vector consisting of a longitude and latitude value, which we indicate by indices $lon$ and $lat$. We determine if a position $L$ is inside a rectangle by testing perpendicular projection (see Figure 2) as follows:

$$0 \leq \overrightarrow{AL} \cdot \overrightarrow{AB} \leq \overrightarrow{AB}^2 \land 0 \leq \overrightarrow{AL} \cdot \overrightarrow{AD} \leq \overrightarrow{AD}^2 \quad (7)$$

Upon receiving a tuple $(M_i, \mathcal{E}_{pk}(L))$, $\mathcal{G}$ computes for a rectangular geo-fence $F = \{A, B, C, D\}$ the terms of Equation (7) as

$$R = \{\overrightarrow{AB}^2, \overrightarrow{AD}^2, \mathcal{E}_{pk}(\overrightarrow{AL} \cdot \overrightarrow{AB}), \mathcal{E}_{pk}(\overrightarrow{AL} \cdot \overrightarrow{AD})\},$$


$\mathcal{G}$ has to calculate $\mathcal{E}_{pk}(\overrightarrow{AL} \cdot \overrightarrow{AB})$ and $\mathcal{E}_{pk}(\overrightarrow{AL} \cdot \overrightarrow{AD})$ homomorphically due to encrypted $L$. For this, $\mathcal{G}$ encrypts $F$ with the shared public key $pk$. One can show that with Equations (4), (5) and (6), definition of dot product, and component-wise computation, it holds that

$$\mathcal{E}_{pk}(\overrightarrow{AL}_{lat}) = \mathcal{E}_{pk}(L_{lat}) \odot \mathcal{E}_{pk}(A_{lat}),$$

similar for longitude components, and with that

$$\mathcal{E}_{pk}(\overrightarrow{AL} \cdot \overrightarrow{AB}) = \mathcal{E}_{pk}(\overrightarrow{AL}_{lat}) \overrightarrow{AB}_{lat} \oplus \mathcal{E}_{pk}(\overrightarrow{AL}_{lon}) \overrightarrow{AB}_{lon},$$

and similar for $\mathcal{E}_{pk}(\overrightarrow{AL} \cdot \overrightarrow{AD})$.

The calculated values $R$ are then sent to the certificate authority and evaluation service $A$ along with the node ID $M_i$ and the subscription nodes $S'$ of the actions to trigger. $A$ decrypts the encrypted results with the secret key $sk$, evaluates Equation (7) as $f_A$, and invokes the corresponding subscribers.

**Performance evaluation.** For our performance evaluation deployment, we implemented $\mathcal{G}$ and $A$ as Python applications with Flask\(^1\) as backend Web-server. Same holds for the prototype client that we used for testing. Parties communicate with HTTP requests. For the homomorphic cryptography, we used the n1analytics/python-paillier Python library\(^2\). On a workstation (Linux, i5-2520M at 2.50GHz, 16GB RAM), we measured evaluation times of an average 323 milliseconds (1000 executions, network lag not included) per evaluation of $f_A \circ f_G$ with a 2048-bit Paillier key. The measured time is in the ranges suitable for an execution that is perceived “uninterrupted” by users [33]. Thus, we consider NEXUS practicable for actual application.

**V. DISCUSSION AND RESULTS**

The goal must be, that by our architecture and protocol, the security properties (P1) to (P4) can never be violated by a semi-honest adversary.

Adversaries, in our presented architecture the geo-fencing service $\mathcal{G}$, certificate authority and evaluation service $A$, and subscriptions $S$, could try to obtain $M_i$’s secret location $L$ directly (violating (P1)), which would require them to be in possession of both the encrypted location $\mathcal{E}_{pk}(L)$ and the secret key $sk$ to decrypt $L$.

Or they could try to approximate $L$ by observing evaluation of geo-fences $(F, S')$. For this, they would either need to learn about both $F$ and the outcome of $f(\mathcal{E}_{pk}(L), F)$ (Equation (1)). Or they need to know about the set $S' \subseteq S$ that is registered to a geo-fence $(F, S')$. Observing then if any $s \in S'$ was invoked as a result of an evaluation would allow to deduct the evaluation outcome against a geo-fence boundary $F$.

In the following, we show that by employing the protocol as described in Section IV, none of these attacks are possible, and by this, the security properties (P1) to (P4) as stated in Section III are always fulfilled:

**Location Non-Exposition (P1):** The geo-fencing service $\mathcal{G}$ only receives the encrypted location $\mathcal{E}_{pk}(L)$ from a mobile node $M_i$. $\mathcal{G}$ is not in possession of the private key $sk$ to decrypt the data, nor does it need to decrypt any value by exploiting the homomorphic characteristics of the Paillier system as described in IV. $\mathcal{G}$ can thus at no point obtain $L$ directly. The Authority service $A$, though in possession of the private key $sk$, never receives any encrypted location $\mathcal{E}_{pk}(L)$ from neither $M_i$ nor $\mathcal{G}$. Thus, $A$ does at no point obtain information about $L$. Subscribers in $S$ receive neither $sk$ nor the encrypted location $\mathcal{E}_{pk}(L)$. (P1) is by this always satisfied.

**Location-privacy Preservation (P2):** With $\mathcal{G}$ defining the geo-fences $(F, S')$, it is clearly in knowledge about both $F$ and $S'$. $\mathcal{G}$ is not in possession of $sk$ and by this can not decrypt the evaluation result and invoke any of the subscriptions $S'$ based on it. $\mathcal{G}$ can thus neither obtain, nor observe the result of an evaluation for a geo-fence $(F, S')$.

$\mathcal{G}$ does not disclose information about geo-fence boundaries $F$ to any party, and in particular no information about to which geo-fence $(F, S')$ subscriptions $s \in S'$ are

---

\(^1\)http://flask.pocoo.org/
\(^2\)https://github.com/n1analytics/python-paillier
registered. \( A \) by this can never observe for which geo-fence \((F, S')\) it decrypted the evaluation result. To retrieve \( L \) from the decrypted values \( AL \cdot AB \) and \( AL \cdot AD \), \( A \) would need knowledge about the geo-fence boundary \( F = \{A, B, C, D\} \), which is never disclosed by \( G \).

Subscribers in \( s \in S \) receive the result of an evaluation, but do not have knowledge about the geo-fence boundary \( F \), as \( F \) is not disclosed by \( G \). By this, a subscriber can not observe the location of a mobile node by observing its own invocation.

None of the transmitted data or computational intermediate results are stored during the process. By this, (P2) is always fulfilled.

**Computational Correctness (P3):** None of the parties willingly provides wrong data during the process, as we assume all participants to be semi-honest. Correctness of computations during the evaluation is moreover ensured by the homomorphic characteristics of the chosen Paillier encryption scheme. We have shown the correct computation of a containment check of \( L \) against a rectangle based on the Paillier homomorphism in Section IV. (P3) is by this always fulfilled.

**Network Assistedness (P4):** Mobile nodes do not receive geo-fences from \( G \) and by this can not perform geo-fencing evaluation computations on their own. They need to provide some information to a third party, in this case, \( \mathcal{E}_{pk}(L) \) to \( G \), which performs the evaluation with the help of \( A \). As shown above, information exchanged during this process is not sufficient for any other party to violate (P1) to (P3), and (P4) is always fulfilled.

VI. Future Work

We have in this paper limited ourselves to rectangular geo-fence shapes. For future work, we plan to investigate how to evaluate containment of a users’ position in arbitrarily shaped geo-fences within the possible mathematical operations as imposed by the encryption schemes.

Geo-fences are defined independently. This allows for parallel evaluation of multiple geo-fences. We plan to do further research on highly scalable large-scale distributed setups of several instances of geo-fencing and evaluation services, employing capabilities of latest Infrastructure-as-a-Service and virtual container management systems.

We moreover see in the proposed solution a promising approach to realise general purpose validation tasks in distributed IoT environments, similar to works on homomorphic privacy preserving multi party computations as for example presented in [34]. In fact, while we focused on the geo location validation as use-case in this paper, we see promising application opportunities for every kind of numerical computations or validations, like for example factory process sanitary monitoring in an Industrie 4.0 scenario, general sensor analysis in a Smart City environment, and other.

VII. Conclusion

In this paper, we have presented NEXUS (Non Exposure User location privacy System), a novel protocol for geo-fencing systems that ensures location privacy based on non-location exposure by employing a homomorphic encryption scheme.

In the paper, we have presented the following contributions to the topic:

Based on a list of properties for location-privacy preserving geo-fencing schemes, we have developed a protocol for a geo-fencing system that, unlike existing approaches, does not rely on anonymisation or obfuscation of the user. Instead, it utilises characteristics of homomorphic encryption. This allows to perform the evaluation entirely on encrypted location data. We have shown that by our protocol, provably, the correct result of the geo-fencing evaluation can be computed. The location of the client is kept entirely secret to all parties involved with the evaluation process.

The presented protocol was implemented in a prototype application for rectangular geo-fences based on the Paillier encryption system [32]. The prototype performed the computation in time ranges that allow for an actual applicable system.

Acknowledgement

The work in this paper was funded by financial means of the German Federal Ministry for Economic Affairs and Energy (BMWi) in the project GUIDED AL under the support code 01MD16010C, and by the Federal Ministry of Education and Research of Germany in the project Hybr-iT under support code 01IS16026A.

References


