A Stochastic Game for Privacy Preserving Context Sensing on Mobile Phone

WEI WANG, QIAN ZHANG
HONG KONG UNIV. OF SCI. & TECH.
Context Sensing on Smartphone

Smartphones equipped with a variety of sensors
Context Sensing on Smartphone

Smartphones equipped with a variety of sensors

- Locations
- Social activities
- Mobility mode
Context-Aware Applications on Today’s Smartphone

Siri®: Location-based reminder
Context-Aware Applications on Today’s Smartphone

Siri®: Location-based reminder

Moves®: Activity and location tracker
Context-Aware Applications on Today’s Smartphone

Siri®: Location-based reminder

Moves®: Activity and location tracker

AutoSilent®: Mute the phone when user is in a meeting
Context-Aware Applications: User Experiences and Privacy Issues

User Experiences

Personalized services
Context-Aware Applications: User Experiences and Privacy Issues

**User Experiences**

Personalized services

**Privacy Issues**

- Tracking
- Aggressive data collection
- Criminal intent

[Enck et al. OSDI ’10, MS survey’ 11]: People believe that the risks outweigh the benefits in many LBS.

[Consumer privacy bill of rights’12]: “Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones.”
Existing Privacy Preserving Techniques

Hide the exact location spot/sensing results by *spatial cloaking, data perturbation, etc.*

Strike a balance between *service quality* and *privacy protection*
Privacy Problem in Context Sensing

Dynamics of user behaviors

A user usually goes to grab sth to eat before seeing a doctor.

Correlation between contexts leaks info
Privacy Problem in Context Sensing

Dynamics of user behaviors
A user usually goes to grab sth to eat before seeing a doctor.

Real-time attacks
Pushing context-related ads/spam to users

Correlation between contexts leaks info
Adversaries adapt attacking strategies over time
The Target of Our Work

Analyze privacy protection for context sensing, and devise optimal strategies to preserve context privacy.
Contributions

1. Identify context privacy problem in consideration of context correlations and powerful strategic adversaries.

2. Devise an efficient learning algorithm to obtain optimal strategies.

3. Use real smartphone traces for evaluation.
Context Sensing Model

Smartphone User with
- Privacy-preserving middleware (e.g., MaskIt[Gotz et al. SIGMOD’12])
- Context-aware application

Context-aware application
- Extract contexts and provide services
Context Sensing Model

Smartphone User with

- Privacy-preserving middleware (e.g., MaskIt[Gotz et al. SIGMOD’12])
- Context-aware application

Context-aware application

- Extract contexts and provide services
- Leak info to adversary
User Model

- Encounter a set of contexts
  - Two-state Markov model
    [Kim et al. IEEE Perv. Comp. 11]

- Claim a set of sensitive contexts via a special app (Locaccino [UbiComp'10])

- Installed a privacy-preserving middleware
  Control the released data granularity of each sensor (MaskIt [SIGMOD'12])
User Model

- Encounter a set of contexts
  - Two-state Markov model
    [Kim et al. IEEE Perv. Comp. 11]

- Claim a set of sensitive contexts
  - via a special app (*Locaccino* [UbiComp’10])
User Model

- Encounter a set of contexts
  - Two-state Markov model [Kim et al. IEEE Perv. Comp. 11]

- Claim a set of sensitive contexts
  - via a special app (*Locaccino* [UbiComp’10])

- Installed a privacy-preserving middleware
  - Control the released data granularity of each sensor (*MaskIt* [SIGMOD’12])
Adversary Model

- A malicious attacker
  - Minimize user’s utility through a series of strategic attacks
  - Launch real-time attacks (e.g., spams)

- Know user’s Markov model

- Access the released sensing data via context-aware app
  - Retrieve a limited amount of data in a time slot
Context Privacy
Game Formulation
Problem Overview

A series of time slots
- User cares about the long-term utility: service quality and privacy loss
- Adversary minimizes user’s utility

In each time slot
- User chooses the released granularity of each sensor
- Adversary chooses a limited amount of data for retrieval

Modeled as a zero-sum stochastic game
Illustration of Stochastic Game

System state

Actions of players

\[ t \rightarrow t+1 \rightarrow \ldots \]
Illustration of Stochastic Game
Illustration of Stochastic Game
Illustration of Stochastic Game

System state → Actions of players → Stage playoffs of players

System state → Actions of players → Stage playoffs of players

Sum of discounted payoffs
System States

\[ S^t = \{ C^t, A^t \} \]

Current Context

Observed Attack
Result: fail/success

Sum of discounted payoffs
Players’ Actions

$$S^t = \{C^t, A^t\}$$

Current Context

Observed Attack
Result: fail/success

$$a^t_u = \{a^t_{u,1}, \ldots, a^t_{u,K}\}$$

Data Granularity

K sensors used by the app

$$a^t_a = \{a^t_{a,1}, \ldots, a^t_{a,K}\}$$

Effort on each sensor is limited

$$\sum_k a^t_{a,i} \leq L, \quad 0 \leq a^t_{a,i} \leq 1, \forall k$$

Stage playoffs of players

System state

Actions of players

Stage playoffs of players

System state

Actions of players

Sum of discounted payoffs
State Transitions

\[ S^t = \{ C^t, A^t \} \]

Current Context

\[ a^t_u = \{ a^t_{u,1}, \ldots, a^t_{u,K} \} \]

Data Granularity

\[ a^t_{a} = \{ a^t_{a,1}, \ldots, a^t_{a,K} \} \]

K sensors used by the app

Effort on each sensor is limited

\[
\Pr[S^{t+1} | S^t, a^t_u, a^t_a] = \Pr[A^{t+1} | A^t, a^t_u, a^t_a] \Pr[C^{t+1} | C^t] = \Pr[A^{t+1} | a^t_u, a^t_a] \Pr[C^{t+1} | C^t].
\]
Stage Payoff

\[ r_u(S^t, a^t_u, a^t_\alpha) = QoS(a^t_u) - \omega \cdot Pri(S^t) \]

Service Quality  Privacy Loss

System state

Actions of players

Stage playoffs of players

Sum of discounted payoffs
Stage Payoff

\[ r_u(S^t, a_u^t, a_{\alpha}^t) = QoS(a_u^t) - \omega \cdot Pri(S^t) \]

Service Quality

Sigmoid function of recognition accuracy

\[ 0 \rightarrow 1 \]

System state \rightarrow System state

Actions of players \rightarrow Actions of players

Stage playoffs of players \rightarrow Stage playoffs of players

Sum of discounted payoffs
Stage Payoff

\[ r_u(S^t, a^t_u, a^t_\alpha) = QoS(a^t_u) - \omega \cdot Pr(S^t) \]

Privacy Loss

Privacy loss = context sensitivity x attack result

the sum of the discounted differences between the prior belief and the posterior belief after observing current context

\[ Sens(c) = \sum_{t=0}^{\infty} \sum_{c^s \in C_s} \gamma^t \Pr[C^t = c_s | C^0 = c] - \Pr[C^t = c_s] \]

Discounted factor Posterior belief Prior belief

System state Actions of players System state Actions of players

Stage playoffs of players

Sum of discounted payoffs
Utility Function

\[ r_u(S^t, a_u^t, a_\alpha^t) = QoS(a_u^t) - \omega \cdot Pri(S^t) \]

- Delayed payoffs value less.
  - The smartphone users care more about the current context or near future contexts than the faraway future contexts.

\[ U_u = \mathbb{E}\left[ \sum_{t=0}^{\infty} \gamma^t r_u(S^t, a_u^t, a_\alpha^t) \right] \]

Discounted factor

- **Objective**: derive an *optimal defense policy* to maximize \( U_u \)
Learning Algorithm For Optimal Defense Policy
Minimax Equilibrium in the Context Privacy Game

User’s Policy
\[ \pi_u : S \mapsto \Delta(A_u) \]

Adversary’s Policy
\[ \pi_a : S \mapsto \Delta(A_a) \]

Probability distribution over action space

State value
\[ V^\pi(s) = \sum_{t=0}^{\infty} \gamma^t \mathbb{E}[r_u(S^t, a_u^t, a_a^t)|\pi_u, \pi_a, S^0 = s] \]

Utility
\[ V^\pi(s) = r_u(s, a_u^\pi, a_a^\pi) + \gamma \sum_{s' \neq s} \Pr[s'|s, a_u^\pi, a_a^\pi] V^\pi(s') \]

s as the initial state at t=0
Minimax Equilibrium in the Context Privacy Game

**Definition 2 (NE in Stochastic Game)** In a zero-sum stochastic game \( \Gamma \), a Nash Equilibrium (NE) point is an optimal strategy pair \( \pi^* = \{ \pi_u^*, \pi_a^* \} \), such that for all state \( s \in S \)

\[
V^{\pi^*}(s) \geq V^{\pi^a}(s), \tag{11}
\]

and

\[
V^{\pi^a}(s) \leq V^{\pi^u}(s), \tag{12}
\]

where \( \pi^a = \{ \pi_u, \pi_a^* \} \), \( \forall \pi_u \), and \( \pi^u = \{ \pi_u^*, \pi_a \} \), \( \forall \pi_a \).

Minimax Equilibrium

\[
V^{\pi^*}(s) = \max_{\pi_u} \min_{\pi_a} \left\{ r_u(s, a_u^\pi, a_a^\pi) + \gamma \sum_{s' \neq s} \Pr[s'|s, a_u^\pi, a_a^\pi] V^{\pi^*}(s') \right\}
\]
Efficient Minimax Learning Algorithm

- The cardinality of $S$ can be very large
  - Minimax $Q$-learning needs to solve $|S|$ bimatrix games

- Solve an equivalent problem instead
  - Eliminate $c$ in the learning process

$$V^\pi(s) = r_u(s, a^\pi) + \gamma \sum_{Ar'} \left( \Pr[Ar'|a^\pi] V^\pi(\text{Ar'}) \right)$$

$$\mathbb{E}_c [V^\pi_u(s)] = \mathbb{E}_c \left[ r_u(s, a^\pi) + \gamma \sum_{Ar'} \left( \Pr[Ar'|a^\pi] V^\pi(\text{Ar'}) \right) \right]$$
Evaluation
Setup

- **Dataset:**
  - Reality Mining Dataset from MIT
    - Transportation mode (driving, walking, stationary)
    - Location (cell granularity)
    - Proximity to each other (via Bluetooth)
    - Activities (calling, using apps)

- **Contexts:**
  - Locations of 91 users with at least 30 days of data
  - Randomly select a context as sensitive context

- **System parameters:**
  - Number of sensors: 3 (WiFi, GPS, Bluetooth) [Nath, MobiSys’12]
  - Power limitation of adversary: 2

- **Baselines:**
  - Fixed strategy
  - Myopic strategy

[http://reality.media.mit.edu/dataset.php]
Comparison with Baseline Schemes

- Gain of the proposed scheme comes from the consideration of future payoffs.
- For users with little privacy concerns, the impact of current actions on the future payoffs can be neglected.
- For users with low satisfaction threshold, high service quality is easily achieved with little privacy loss.
Convergence Speed

(a) Convergence speed of the proposed algorithm

(b) Convergence speed of the traditional learning algorithm

Reduce # of iterations by three orders of magnitude
Conclusions

- Consider the distinct features of the context privacy problem
  - Context dynamics and correlations
  - Powerful adversaries can adjust their attacking strategies

- Obtain the user’s optimal defense strategy efficiently
  - Formulate the interactive competition as a zero-sum stochastic game
  - Solve an equivalent problem with reduced dimensions

- Evaluate on real smartphone traces
  - It is worthwhile to consider current action’s impact on future payoffs
  - Provide some guidelines for context privacy preserving mechanisms
Any Question?
Thank you!

Wei Wang
gswwang@cse.ust.hk
Backup Slides
Real-time Attacks

Fixed attacking strategy
- Only valid for offline attacks, e.g., analyzing user’s personal information and preferences.

Real-time attacks
- Sell user’s sensing data to remote advertisement adversaries, who continuously push context-related ads or spam to users based on the user’s instant context information.
- In the real world, context-based ads or spam need to be delivered in real time (e.g., NAVTEQ or AdLocal by Cirius Technologies) as users may lose interest if the ads do not match current context.
- Adapt attacking strategies based on their observations of previous attacking results and context dynamics.
Stage Payoff

\[ r_u(S^t, a_u^t, a_a^t) = QoS(a_u^t) - \omega \cdot Pri(S^t) \]

equivalent service quality improvement caused by unit privacy loss

For all contexts

Access all raw data

Access no data

Adversary’s prior belief
Learning algorithm

1. Initialization
   1. $t \leftarrow 0$, $A_{r}^t = 0$;
   2. $\tilde{V}_t^t(A_r = 0) \leftarrow 1$, $\tilde{V}_t^t(A_r = 1) \leftarrow 1$;
   3. Initialize strategy pair $\pi^t$: two uniform distributions where $a_{u,i}^t = \frac{1}{K}$, $a_{a,i}^t = \frac{L}{K}$, $\forall i$;

2. Iteration
   4. repeat
   5. Select an action pair $\{a_{u}^t, a_{a}^t\}$ based on $\pi^t$;
   6. Update $A_{r}^{t+1}$ after both players take their actions $\{a_{u}^t, a_{a}^t\}$;
   7. Update equivalent state value $\tilde{V}_{t+1}^t(A_r)$ according to (18);
   8. Update optimal strategy $\pi^{t+1}$ according to (16) with updated state values;
   9. $t \leftarrow t + 1$;
10. until Converge