

Privacidad en aplicaciones móviles

Guía Práctica

Contexto

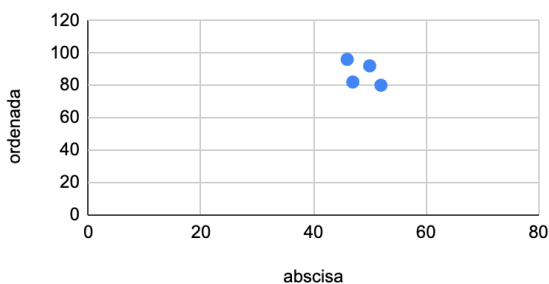
Ahora que ya conocemos cómo medir la privacidad de posiciones, nos preguntamos qué estrategia podríamos utilizar para aumentar la privacidad, de tal forma que las aplicaciones puedan reconocer tus ubicaciones para recomendarte lugares, pero sin reconocer tus puntos de interés.

La estrategia que usaremos para esto es: **agregar ruido a las posiciones**. Esto podemos entenderlo como perturbar “levemente” las posiciones de un usuario, y podemos hacerlo por ejemplo sumando o restando una cantidad aleatoria pequeña a cada coordenada.

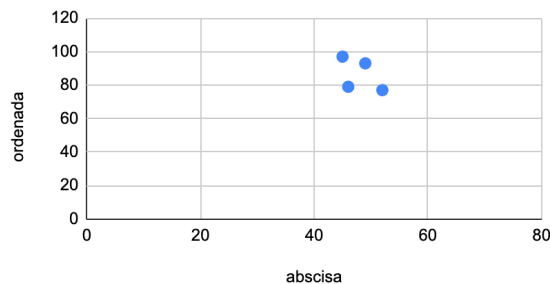
Por ejemplo si consideramos la posición $(x, y) = (50, 90)$ de un usuario y le aplicamos un ruido leve de 2 metros a cada coordenada, obtenemos una posición con ruido $(x_r, y_r) = (52, 88)$.

Esta estrategia busca un equilibrio entre entregar a una aplicación una ubicación “lo suficientemente precisa” para indicarte una ruta para ir a algún lugar, y al mismo tiempo “lo suficientemente alterada” para que no reconozca tus puntos de interés.

Consideremos ahora a modo de ejemplo, un conjunto de 4 posiciones de una usuaria y apliquemos a cada posición esta estrategia. A continuación se muestran estos dos gráficos, uno con las posiciones Sin Ruido, y otra con las posiciones Con ruido.



Posiciones sin ruido



Posiciones con ruido

Es posible notar que las posiciones son relativamente similares, solo que en el segundo gráfico alteramos levemente las posiciones originales. Las varianzas de las posiciones de estos dos casos son las siguientes.

	Sin ruido	Con ruido
Varianza X	7,6	10,0
Varianza Y	59,7	99,7

Actividad 1

Según el contexto dado anteriormente, responde las siguientes preguntas:

- 1) ¿Cuáles son los niveles o “valores” de privacidad en cada caso?
- 2) Al comparar ambos valores ¿En qué caso se tiene mayor privacidad?
- 3) Recordando el criterio de varianza visto en la clase, cuyo límite para reconocer puntos de interés es de $10^2 = 100$. ¿Es posible reconocer puntos de interés en cada caso?, ¿en cuáles?
- 4) Considerando que las posiciones sin ruido y con ruido son similares, ¿mejora la privacidad con ruido permitiendo el correcto funcionamiento de aplicaciones que usan la información de la posición de sus usuarias?

Solucionario

-
- Act. 1**
1. Sabemos que el nivel de privacidad viene dado por la suma de las varianzas del eje X y el eje Y.
Por lo tanto, tenemos los siguientes niveles de privacidad:

$$P = Var_X + Var_Y = 7,6 + 59,7 = 67,3$$

$$P_r = Var_X + Var_Y = 10 + 99,7 = 109,7$$
-
2. Si comparamos los valores de los niveles de privacidad, claramente las posiciones con ruido tienen mayores niveles de privacidad, que las que no tienen ruido.
-
3. Inspirandonos en lo visto para el caso de la circunferencia de radio 10 m, mientras se tengan varianzas menores a $10^2 = 100$ es suficiente para reconocer puntos de interés similares a una casa.
En este caso observamos que la varianza de la usuaria sin ruido es menor que 100, por lo tanto se puede reconocer un punto de interés. Al agregarle ruido, su varianza pasa a ser mayor que 100, por lo que no es posible reconocer un punto de interés.
-
4. Si mejora la privacidad al agregarle ruido a las posiciones, pues notamos cómo aumenta la varianza en ambas coordenadas: lo suficiente para que no se reconozcan puntos de interés, y lo necesario para que aún pueda funcionar la aplicación.
-