Universidad del Bío-Bío, Chile

Facultad de Ciencias Empresariales

Departamento de Sistemas de Información

Protocolos Delimitadores de Distancia Conscientes de la Privacidad de Ubicación en Redes Ad-Hoc Inalámbricas

Tesis presentada por
Cristián Molina Martínez
para obtener el grado de Magíster en Ciencias de la Computación

Dirigida por:
Dr. Cristian Durán, Universidad del Bío-Bío, Chile
Dr. Patricio Galdames, Universidad del Bío-Bío, Chile

2017

Dedicado a todos aquellos que influyeron en el desarrollo de esta Tesis y a mi familia.

Agradecimientos

Mis agradecimientos a mis directores de tesis Dr. Cristian Durán y Dr. Patricio Galdames, por su participación en la concreción de muchas de las ideas que permitieron la finalización de este trabajo. Y al profesor Dr. Pedro Rodríguez quien ha colaborado con la formación del tema y la propuesta de esta tesis.

Mis mayores agradecimientos a aquellos que con sus palabras han permitido la finalización de esta etapa de mi vida, Arq. María Paz Molina, Ing. Brunny Troncoso y Dr. Christian Vidal. Una conversación, por breve que sea, puede cambiar la dirección de una vida.

También mi eterno agradecimiento al grupo humano que formó parte de mis estudios en el Magister en Ciencias de la Computación. A mis profesores, Dra. Mónica Caniupán, Dra. Alejandra Segura, Dr. Clemente Rubio y aquellos que ya he mencionado por su aporte en mi desarrollo y conocimiento. A mis compañeros, todos aquellos que formaron parte de este ciclo de estudio e hicieron agradable y provechoso el entorno de estudio, por su colaboración y aporte. Y a la persona anónima que trabaja para que otros puedan estudiar.

Finalmente, no puedo dejar de mencionar a mis estudiantes del Departamento de Ingeniería Eléctrica y Electrónica del la Universidad del Bío Bío, quienes fueron la inspiración para iniciar esta etapa de estudio en mi vida.

Abstract

The existing location verification techniques are designed based on two assumptions: *1*) nodes are willing to disclose their exact location, and *2*) nodes allow them to be located as accurately as possible. These assumptions are unsuitable for applications where a user deliberately reduces the resolution of its location to protect privacy or security. This research is part of the area of wireless networks and considers the scenario where a user wishes that its location, defined by a spatial region, be verified by a verifier but ensuring that this region is not refined beyond a range set by the user. The following types of attacks are considered, which allow verifiers to check if the user is within the region declared by him: the attack area setting broadcasting and distance bounding attack. Different procedures are studied to protect the spatial region declared by a user against attacks to verify the user's location within their declared region, presenting their weaknesses and strengths with respect to the user. Within which is presented a procedure based on two cloaking regions and a metric based on the entropy to define the satisfaction of the protection requirements. This work culminates with a proposed protocol "Distance Bounding Protocol Aware of Location Privacy" or "Verification Protocol Cloaking Region" which mitigates the possible refinement of the user's location to a tolerance level defined by this and it enables the verifier complete the verification process location with a margin of desired error.

Keywords Location privacy, Cloaking region, Attack of refinement, Broadcasting attack, Attack distance delimitation, Demarcation of distance, Wireless transmission, Estimated distance, Setting the coverage area.

Resumen

Las técnicas de verificación de ubicación existentes están diseñadas bajo dos supuestos: *1*) los nodos están dispuestos a dar a conocer su ubicación exacta, y *2*) los nodos permiten que sean localizados con la mayor precisión posible. Estos supuestos son inadecuados para aplicaciones de localización encubierta donde un usuario reduce deliberadamente la resolución de su ubicación para proteger su privacidad o seguridad. Este trabajo de investigación se enmarca en el área de redes inalámbricas y considera el escenario donde un usuario desea que su ubicación, definida por una región espacial, sea comprobada por un verificador pero garantizando que esta región no sea refinada mas allá de un rango fijado por el usuario. Se consideran los siguientes dos tipos de ataques, que permiten al verificador comprobar si el usuario se encuentra dentro de la región por él declarada: el ataque de ajuste del área de cobertura de transmisión y el ataque de delimitación de distancia. Se estudian diferentes procedimientos para proteger la región espacial declarada por un usuario frente a los ataques para comprobar la ubicación del usuario dentro de su región declarada, presentando sus debilidades y fortalezas respecto del usuario. Presentando, finalmente, un procedimiento en base a dos regiones de encubrimiento y una métrica en base a la entropía para definir la satisfacción de los requerimientos de protección. Se culmina este trabajo proponiendo un "Protocolo Delimitador de Distancia Consciente de la Privacidad de Ubicación" o "Protocolo de Verificación de Regiones de Encubrimiento", el cual mitiga el posible refinamiento de la ubicación del usuario a un nivel de tolerancia definido por este y permite al verificador concluir el proceso de verificación de ubicación con un margen de error deseado.

Palabras Clave Privacidad de ubicación, Región de encubrimiento, Ataque de refinamiento, Ataque cobertura de transmisión, Ataque de delimitación distancia, Delimitación de distancia, Transmisión inalámbrica, Estimación de la distancia, Ajuste del área de cobertura.

Indice General

Indice de Figuras

Indice de Tablas

Nomenclatura y Acrónimos

Nomenclatura

V	—	Nodo verificador.
P	—	Nodo a prueba (prover).
U	—	Región máxima requerida por V (región útil para fines de verificación). Esta región tiene un radio r_u, que P debe satisfacer.
r_u	—	Radio de U.
R	—	Región de encubrimiento.
r	—	Radio de R, con $r \leq r_u$.
O	—	Centro de R.
R_{priv}	—	Región de encubrimiento privada, sólo conocida por P.
r_{priv}	—	Radio de R_{priv}, con $r_{priv} \leq r_u$.
O_{priv}	—	Centro de R_{priv}.
R_{pub}	—	Región de encubrimiento pública, entregada por P a V.
r_{pub}	—	Radio de R_{pub}, con $r_{pub} \leq r_{priv}$.
O_{pub}	—	Centro de R_{pub}.
C	—	Corona circular. Región determinada por V dentro de la cual se encuentra P, previa al refinamiento de R.
r_{ci}	—	Radio interior de C.
r_{ce}	—	Radio exterior de C.
g_c	—	Grosor de C, $g_c = r_{ce} - r_{ci}$.
R_F	—	Región de encubrimiento refinada, $R_F = C \cap R$.
R_{Fpriv}	—	Región de encubrimiento privada refinada, $R_{Fpriv} = C \cap R_{priv}$.
R_{Fpub}	—	Región de encubrimiento pública refinada, $R_{Fpub} = C \cap R_{pub}$.
d_{VP}	—	Distancia real entre el nodo V y el nodo P.
d_{VO}	—	Distancia real entre el nodo V y O.
d_{max}	—	Distancia máxima entre el nodo V y la frontera de R.
$\widetilde{d}_{VP}$	—	Distancia entre el nodo V y el nodo P estimada por V.
$\widetilde{d}_{VPmin}$	—	Distancia mínima entre el nodo V y el nodo P estimada por V.
$\widetilde{d}_{VPmax}$	—	Distancia máxima entre el nodo V y el nodo P estimada por V.
δ	—	Retardo en la respuesta de P.
Λ	—	Límite superior de intervalo de tiempos donde se selecciona el retardo δ.
c	—	Velocidad de propagación de la onda electromagnética en el medio de comunicación.

t_d	—	Tiempo que demora el P en responder al desafío recibido de V.
t_m	—	Tiempo total que mide V desde el envió de su desafío hasta la recepción de la respuesta de P.
t_p	—	Tiempo de propagación de la señal de comunicación entre los dos usuarios, V y P.
$t_{(r)}$	—	Tiempo en que la señal de comunicación recorre la distancia r.
Δ_{min}	—	Distancia mínima entre V y R, es decir $\Delta_{min} = d_{VO} - r$.
Δ_{max}	—	Distancia máxima entre V y R más la distancia recorrida por un mensaje durante un tiempo Λ, es decir $\Delta_{max} = d_{VO} + r + \Lambda r$.
W_t	—	Potencia de transmisión de la señal de Radio Frecuencia.
W_r	—	Potencia de recepción de la señal de Radio Frecuencia.
W_{Vt}	—	Potencia de transmisión de la señal de Radio Frecuencia de V.
W_{Prm}	—	Potencia de recepción mínima de P para considerar una comunicación válida.
τ	—	Factor de tolerancia aceptado por P para el refinamiento, $\tau \in [0, 1]$.
$d_{(\delta)}$	—	Distancia que recorre la señal de comunicación en un tiempo δ.
$\overrightarrow{r_{[VP]}}$	—	Vector de módulo igual a la distancia r y dirección igual al vector del nodo V al nodo P.
$\overrightarrow{d_{(\delta)[VP]}}$	—	Vector de módulo igual a la distancia que recorre la señal de comunicación en un tiempo δ y dirección igual al vector del nodo V al nodo P.
Υ_A	—	Métrica definida como la razón entre el área no refinada de la región R_{priv} y el área de la región R_{priv}.
Υ_H	—	Métrica definida como la razón entre la entropía del área no refinada de la región R_{pub} y la entropía del área de la región R_{priv}.
ρ	—	Delta de potencia a considerar sobre el nivel mínimo de recepción para que una comunicación sea válida.
$\Upsilon_{H\rho}$	—	Métrica definida como la razón entre la entropía del área no refinada de la región R_{pub} y la entropía del área de la región R_{priv}, donde el nivel de potencia ρ reemplaza al retardo δ.
$W_{(r)}$	—	Delta de potencia de la señal de comunicación para recorrer la distancia r y aún ser considerada válida.
N_v	—	Número máximo de veces que P permite a V ejecutar el protocolo DBP en un tiempo T_v.
T_v	—	Tiempo en el cual P permite ejecutar sólo N_v veces el protocolo DBP a V.

Acrónimos

AAC	—	Ataque de ajuste del Area de Cobertura.
$ABAC$	—	Ataque Basado en el ajuste del Area de Cobertura.
$ABED$	—	Ataque Basado en la dElimitación de la Distancia.
AED	—	Ataque de dElimitación de la Distancia.
DBP	—	Protocolo delimitador de distancia (Distance Bounding Protocol).

$DBPALP$	—	Protocolo delimitador de distancia consciente de la privacidad de ubicación (Distance Bounding Protocol Aware of Location Privacy).
$FMCW$	—	Frecuencia modulada de onda continua (Frequency Modulated Continuous Wave).
LBS	—	Servicios basados en la ubicación (Location Based Services).
$LDIS$	—	Servicios basados en la ubicación (Location Dependent Information Services).
MAC	—	Message Authentication Code.
$NS-3$	—	Network Simulator - 3.
RF	—	Radio Frecuencia.
$RFID$	—	Identificación en Radio Frecuencia (Radio Frequency IDentification).
$SBMD$	—	Solución en Base a un retardo igual a la Máxima Distancia.
$SBIR$	—	Solución en Base a un Intervalo de Retardos posibles.
$SBMDcDRE$	—	Solución en Base a un retardo igual a la Máxima Distancia con Dos Regiones de Encubrimiento.
$SBIRcDRE$	—	Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento.
$SBIRcDREyE$	—	Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento y uso de Entropía.

Capítulo 1

Introducción

1.1. Introducción

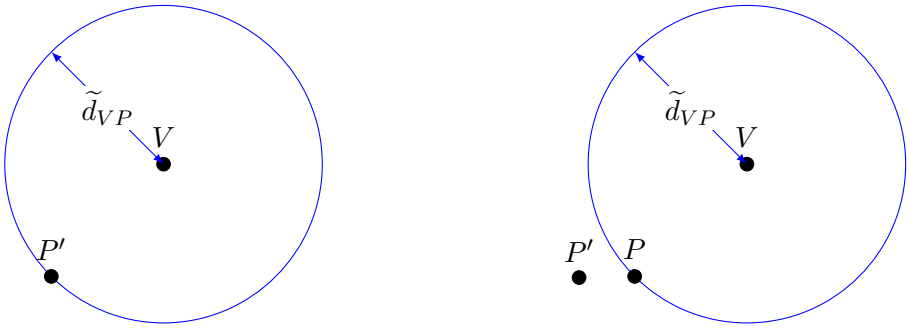
Diversas aplicaciones y protocolos están basados en la ubicación precisa de los usuarios que operan dispositivos de comunicación inalámbrica. Por ejemplo, los servicios basados en la ubicación, conocidos por sus siglas en inglés LBS (Location Based Services) o LDIS (Location Dependent Information Services), necesitan de la ubicación de los usuarios para proporcionarles información específica con respecto a su ubicación. Como ejemplos de estos servicios; un usuario que llega a un aeropuerto y busca el hotel más cercano a su ubicación [6, 21, 25, 44]; o una persona que requiere el ingreso a una instalación de seguridad, a esta se le puede solicitar una clave de ingreso y, además, se le puede solicitar que verifique su ubicación, si los datos de ubicación no corresponden es probable que la persona esté siendo suplantada. Además, están los protocolos de enrutamiento para redes ad hoc móviles que utilizan la posición de los usuarios para descubrir y construir una ruta de comunicación entre estos [24, 26, 29, 34, 35, 40].

Desafortunadamente, la liberación de la ubicación levanta una serie de inquietudes respecto a la seguridad y privacidad de los usuarios. Por ejemplo, visitas frecuentes a lugares como centros médicos o bares pueden permitir, a personas no autorizadas (de forma anónima), concluir información sobre el estado de salud o el estilo de vida de una persona. Estas inquietudes han motivado un significativo esfuerzo en investigación [12, 13, 17, 18, 22, 50–53, 53, 54]. Entre las diversas técnicas investigadas, la más práctica parece ser la denominada "encubrimiento de la ubicación" (location cloaking) [22, 50–53, 53, 54].

La técnica de encubrimiento de la ubicación permite a un usuario reducir la resolución de su ubicación para mitigar los riesgos de privacidad y seguridad. En esta técnica, el usuario hace pública un área geográfica, denominada "región de encubrimiento", que incluye su ubicación exacta y que debe satisfacer una serie de requerimientos de anonimato [22, 50, 51], privacidad [52] o seguridad [53, 53, 54]. Sin embargo, esta estrategia tiene un impacto significativo en aplicaciones basadas en la ubicación de los usuarios. Estas aplicaciones podrían sufrir de pérdida de eficiencia en el cómputo computacional [15]; otras simplemente podrían no funcionar con una menor resolución.

Un ejemplo de este último caso son los servicios de verificación de ubicación basados en la ejecución de protocolos de delimitación de distancia o DBP (Distance Bounding Protocols) [7]. Un DBP determina una estimación de la distancia entre dos usuarios denominados usuario verificador y usuario a prueba. El protocolo verificador de ubicación es principalmente ejecutado

por dos usuarios inalámbricos; el usuario a prueba, denotado como P, indica estar ubicado en una posición precisa; en cambio, el usuario verificador, denotado como V, tiene como rol verificar si la posición señalada es probablemente correcta. Para ello V y P intercambian mensajes, lo que le permite a V estimar su distancia con P y así comprobar si la posición declarada por P cae en una región circular centrada en su posición y de radio igual a la distancia determinada por medio del intercambio de mensajes. Si este es el caso se asume que la posición declarada por P es la correcta, en caso contrario se indica que la afirmación es falsa. Ambos escenarios posibles se muestran en la Figura 1.1.



(a) Posición declarada por P (P') es la correcta.

(b) Posición declarada por P (P') es incorrecta.

Figura 1.1: Estimación por parte de V de su distancia con P para comprobar si la posición declarada por P cae en una región circular centrada en su posición y radio igual a la distancia $\widetilde{d}_{VP}$.

1.1.1. Motivación del Trabajo de Investigación

En este trabajo de investigación se propone estudiar el escenario en el cual el usuario a prueba (P) está dispuesto a liberar una región de encubrimiento que lo contenga, pero no su posición exacta, para realizar un protocolo de delimitación de distancia con un usuario verificador (V). Se supone que tanto V como P no poseen antenas adaptativas o direccionales que les permitan a ambos inferir la dirección de llegada de un paquete, que tanto V como P conocen los medios de los cuales dispone el otro y los protocolos utilizados, Figura 1.2. Dentro de este escenario surge la pregunta, ¿cómo el usuario verificador V puede verificar que el usuario a prueba P se encuentra dentro de la región de encubrimiento declarada por este último, sin que V obtenga más detalles de la posición de P que aquellos hechos públicos con la región de encubrimiento?.

Este problema es desafiante ya que las técnicas de delimitación de distancia actuales intentan determinar la distancia precisa entre P y V. Esto podría permitir a V determinar que P se encuentra dentro de una región de menor tamaño incluida dentro de su región de encubrimiento R, como se muestra en la Figura 1.3. En la Figura 1.3, V determina una distancia $\widetilde{d}_{VP}$ a el usuario P; con lo cual se puede decir que P no se encuentra más allá de una distancia $\widetilde{d}_{VP}$ de V, ya que P puede estar utilizando alguna técnica de protección y no se puede asegurar que P no este a una distancia menor.

Este trabajo de investigación ha identificado dos tipos de ataques que permiten a V verificar la posición de P dentro de la región de encubrimiento: el ataque de ajuste del área de cobertura

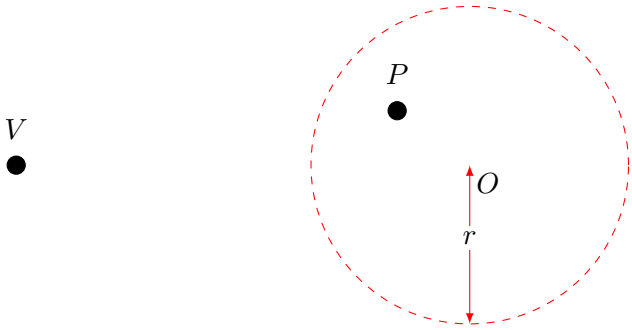


Figura 1.2: Escenario de estudio propuesto. P entrega a V la región de encubrimiento de centro O y radio r.

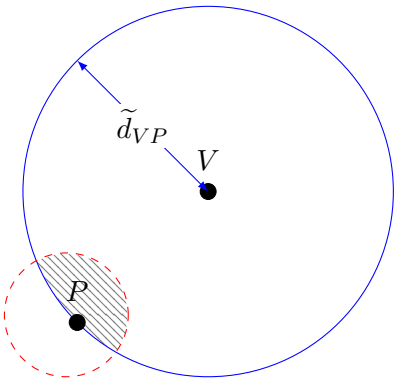


Figura 1.3: Reducción por parte de V del área de la región de encubrimiento (área encerrada por circunferencia segmentada) donde P podría encontrarse (la región achurada).

de una transmisión inalámbrica y el ataque de delimitación de distancia entre V y P.

En el primer ataque, representado en la Figura 1.4, V reduce el área de la región de encubrimiento de P, donde este podría encontrarse, mediante el ajuste de su rango de transmisión (potencia de transmisión) con el fin que este rango intersecte a la región de encubrimiento entregada por P. El usuario V envía un mensaje a P aumentando su potencia de transmisión hasta que recibe una respuesta de él. El conocimiento del medio en el cual se realiza la transmisión, de la atenuación de la señal física utilizada para transmitir el mensaje y del nivel de recepción requerido por P para responder un mensaje, permiten a V determinar su distancia $\widetilde{d}_{VP}$ a P. Con lo cual se puede decir que P no se encuentra más allá de una distancia $\widetilde{d}_{VP}$ de V, ya que P puede estar utilizando alguna técnica de protección y no se puede asegurar que P no este a una distancia menor.

La pregunta que surge en este contexto es; ¿cómo P podría saber que la potencia de transmisión utilizada por V cubre completamente la región de encubrimiento de P, si P desconoce detalles de la ubicación de V?. El conocimiento de la potencia mencionada permitiría proteger la región de encubrimiento.

En el segundo ataque, representado en la Figura 1.5, el usuario V mide el tiempo que

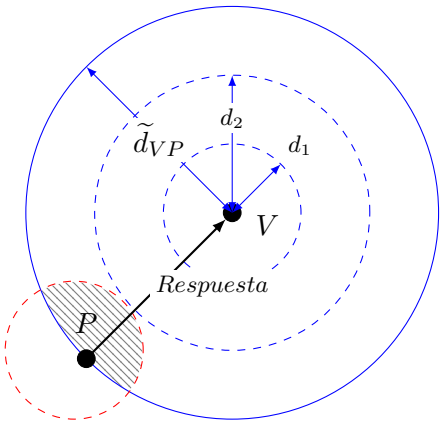


Figura 1.4: Ataque basado en el ajuste del área de cobertura de una transmisión inalámbrica (la región achurada es el área de la región de encubrimiento donde se podría encontrar P).

transcurre desde que envía un mensaje a P hasta que recibe una respuesta de él. Este cálculo de tiempo, más el conocimiento de la velocidad de la señal física utilizada para transmitir los mensajes y el tiempo que demora P en responder, le permite a V determinar su distancia a P. Con lo cual se puede decir que P no se encuentra más allá de una distancia $\widetilde{d}_{VP}$ de V, ya que P puede estar utilizando alguna técnica de protección y no se puede asegurar que P no esté a una distancia menor.

Se podría pensar que P pudiera retardar la transmisión de su mensaje para hacer parecer a V que está ubicado más lejos de lo que realmente está. Sin duda que esta es la opción a considerar, pero la pregunta que surge es ¿cuánto debe retardar P el envío de su respuesta a V?. Si el tiempo es muy corto, V podría reducir el área de la región de encubrimiento de P donde este podría encontrarse. Por el contrario, si tal tiempo fuese muy largo, V estimaría una distancia a P que pudiese ser inútil para fines prácticos de verificación de ubicación.

En este trabajo de investigación se proponen un conjunto de contramedidas que permiten al usuario a prueba P participar de un proceso de delimitación de distancia con un usuario verificador V, pero garantizando que exista un balance que permita:

(a) Que el grado de reducción del área de la región de encubrimiento en la cual se puede encontrar P no supere un nivel de tolerancia establecido por P.

(b) Que la distancia determinada por V al usuario P no sea superior a una cota máxima determinada por V para fines de verificación.

Estos requerimientos antagónicos imponen el diseño de un nuevo tipo de DBP que sea consciente de la privacidad del usuario. Este protocolo debe considerar las siguientes salidas (a diferencia de los tradicionales DBP que consideran sólo dos):

1. El usuario V concluye una distancia a P que es útil para fines de verificación. El grado de reducción del área de la región de encubrimiento en la cual se puede encontrar P estuvo dentro de los rangos tolerables por P.

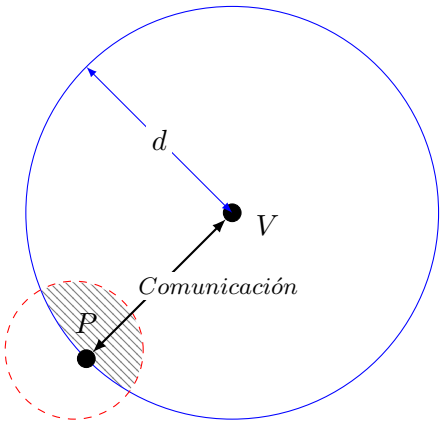


Figura 1.5: Ataque basado en la delimitación de la distancia entre V y P (la región achurada es el área de encubrimiento donde se podría encontrar P).

2. El usuario V concluye que no es posible que P esté dentro de su región de encubrimiento.
3. El usuario V concluye que P no está en una región útil para fines de verificación.
4. Tanto V como P pueden cancelar la ejecución completa del protocolo ya que pueden considerar que las exigencias de distancia útil y grado de reducción del área de la región de encubrimiento de P superan los valores máximos deseados.

Las salidas 1 y 2 corresponden a aquellas que entrega un DBP tradicional. Sin embargo, los requerimientos de privacidad y de distancia útil imponen salidas alternativas como 3 y 4.

1.1.2. Justificación del Trabajo de Investigación

Como ya se ha mencionado en párrafos anteriores; *"la liberación de la ubicación levanta una serie de inquietudes respecto a la seguridad y privacidad de los usuarios. Por ejemplo, visitas frecuentes a lugares como centros médicos o bares pueden permitir concluir información sobre el estado de salud o el estilo de vida de una persona"*. Esta inquietud hace que los DBP tradicionales sean inviables en un contexto de privacidad de ubicación.

El párrafo anterior por si sólo entrega una justificación para proteger la privacidad y seguridad de los usuarios y la justificación de este trabajo de investigación. En esta investigación, esto se traduce en minimizar la reducción del área de las regiones de encubrimiento utilizadas para proteger la privacidad y seguridad de los usuarios.

A diferencia de trabajos anteriores, esta investigación pretende proteger a un usuario que quiere participar de un proceso de verificación de ubicación de la reducción del área de su región de encubrimiento por sobre un valor tolerable.

1.2. Preliminares

En este capítulo se presentan los conceptos básicos necesarios para comprender el "Protocolo Delimitador de Distancia Consciente de la Privacidad de Ubicación del usuario" (DBPALP,

Distance Bounding Protocol Aware of Location Privacy) propuesto. Se comienza con algunos conceptos relevantes, entropía, refinamiento y utilidad de la distancia. Luego, se introduce al ámbito de los protocolos delimitadores de distancia (DBP) y los procedimientos identificados para que el usuario verificador V pueda verificar que el usuario a prueba P se encuentra dentro de la región de encubrimiento declarada por este último; el ataque basado en el ajuste del área de cobertura de una transmisión inalámbrica y el ataque de delimitación de distancia entre V y P.

1.2.1. Conceptos Relevantes

A continuación algunos conceptos que resultan relevantes para el resto del trabajo de investigación.

Entropía de la región

La entropía es utilizada desde mediados del siglo XX como una medida de la información. Más específicamente, la entropía es utilizada como medida de probabilidad de ocurrencia.

Para una región cualquiera R_q, formada por q subregiones S_i, la entropía queda definida en función de la probabilidad p de ocurrencia de un evento en cada subregión por la ecuación 1.1.

$$H(R_q) \;=\; -\sum_{i}^{q} p(S_i)\;\log_n(\;p(S_i)\;) \tag{1.1}$$

Para el caso que el evento sólo pueda asumir uno de dos estados, como es el caso en estudio (en cada subregión el usuario sólo puede estar presente o ausente), la entropía binaria define mejor la situación, ecuación 1.2.

$$H_b(R_q) \;=\; -\sum_{i}^{q} [\; p(S_i)\;\log_2(\;p(S_i)\;) \;+\; (\;1-p(S_i)\;)\;\log_2(\;1-p(S_i)\;)\;] \tag{1.2}$$

La entropía $H_b(R_q)$ es una medida de la cantidad de información de la región R_q. Mientras más cerca del máximo de la función de entropía este al valor de $H_b(R_q)$, que para $H_b(R_q)$ será igual al número de subregiones (q), mayor será la cantidad de información en la región y más cerca de la homogeneidad se encuentra la distribución de probabilidades, que es el caso asumido para este trabajo de investigación.

Refinamiento del área de la región de encubrimiento

En este trabajo de investigación el concepto de *"Refinamiento del área de la región de encubrimiento"* se entiende como: la reducción del área de la región de encubrimiento a una región cuya área es menor al área de la región de encubrimiento inicial y está incluida dentro de la región de encubrimiento inicial.

Refinamiento de la región de encubrimiento

En este trabajo de investigación el concepto de *"Refinamiento de la región de encubrimiento"* se entiende como: la reducción del área de la región de encubrimiento a una región cuya entropía

es menor a la entropía de la región de encubrimiento inicial.

Para este trabajo de investigación se considera que la distribución de probabilidades que describe la posibilidad que un usuario ocupe un lugar dentro de una región es homogénea. Esto se traduce en la equivalencia de los conceptos de refinamiento de la región de encubrimiento y de refinamiento del área de la región de encubrimiento para el caso de una región de encubrimiento. Para el resto de este trabajo ambos conceptos se tratan como equivalentes, a menos que se mencione lo contrario.

Utilidad de la distancia

En el proceso de delimitación de la distancia entre los usuarios V y P, el usuario V requiere que la distancia estimada por él le permita verificar que P se encuentre a una distancia prudentemente útil de la región de encubrimiento R. Por ejemplo, si P no responde a los mensajes de V, V estimaría que P se encuentra fuera de su rango de trabajo o que no está dispuesto a participar de un protocolo para verificar la distancia entre ambos.

Lo anterior se traduce en las siguientes consideraciones; *1*) Las distancias estimadas por V en el proceso de verificación de la distancia entre los usuarios V y P deben estar dentro del radio de servicio de las comunicaciones de V y *2*) Las restricciones de distancia informadas a P no deben proporcionar información de la posición de V ni de las fronteras del servicio de comunicaciones de V.

Para este trabajo de investigación las anteriores consideraciones se traducen en una región útil U de forma circular, de radio r_u y centro en el centro de la región de encubrimiento R de P.

1.2.2. Delimitadores de Distancia

Como ya se ha mencionado, un DBP es principalmente ejecutado por dos usuarios inalámbricos, el primer usuario denotado como P (usuario a prueba) indica estar ubicado en una posición precisa. En cambio, el segundo usuario denotado como V (usuario verificador) tiene como rol verificar si la posición señalada es probablemente correcta. Para ello V y P intercambian mensajes, lo que le permite a V estimar su distancia con P y así comprobar si la posición declarada por P cae en una región circular centrada en su posición y de radio igual a la distancia determinada por medio del intercambio de mensajes. Si este es el caso, se asume que la posición declarada por P es la correcta, en caso contrario se indica que la afirmación es falsa.

La distancia entre los usuarios P y V es estimada por medio de la ecuación 1.3.

$$\widetilde{d}_{VP} \;=\; c \quad \frac{t_m \;-\; t_d}{2} \tag{1.3}$$

Donde c es la velocidad de propagación de la onda electromagnética en el medio de comunicación, t_m es el tiempo total que mide el usuario V desde que envía su desafío hasta la recepción de la respuesta de P y t_d es el tiempo que demora el usuario P en responder al desafío recibido de V.

El elemento esencial de un DBP consiste del desafío de un solo bit y la rápida respuesta de un solo bit. En la práctica, se utiliza una serie de k intercambios rápidos de bits, el número k representa un parámetro de seguridad. Cada vez que P recibe un bit de desafío de V, envía su bit de respuesta lo más inmediatamente posible. Lo que hace este enfoque muy práctico es que

la electrónica de hoy en día puede manejar fácilmente tiempos de unos pocos nanosegundos, y la luz sólo puede viajar unos 30 [cm] durante un nanosegundo.

Protocolo DBP de Brands and Chaum

S. Brands and D. Chaum, en 1993, presentaron inicialmente el Protocolo Delimitador de Distancia (DBP, Distance Bounding Protocol). Este protocolo utiliza una serie de intercambios rápidos de bits, cuyo número es determinado por el parámetro de seguridad k elegido. El tiempo de retardo para la recepción de las respuestas de P permite al verificador V calcular una cota superior de la distancia entre V y P. El protocolo se muestra en la Figura 1.6.

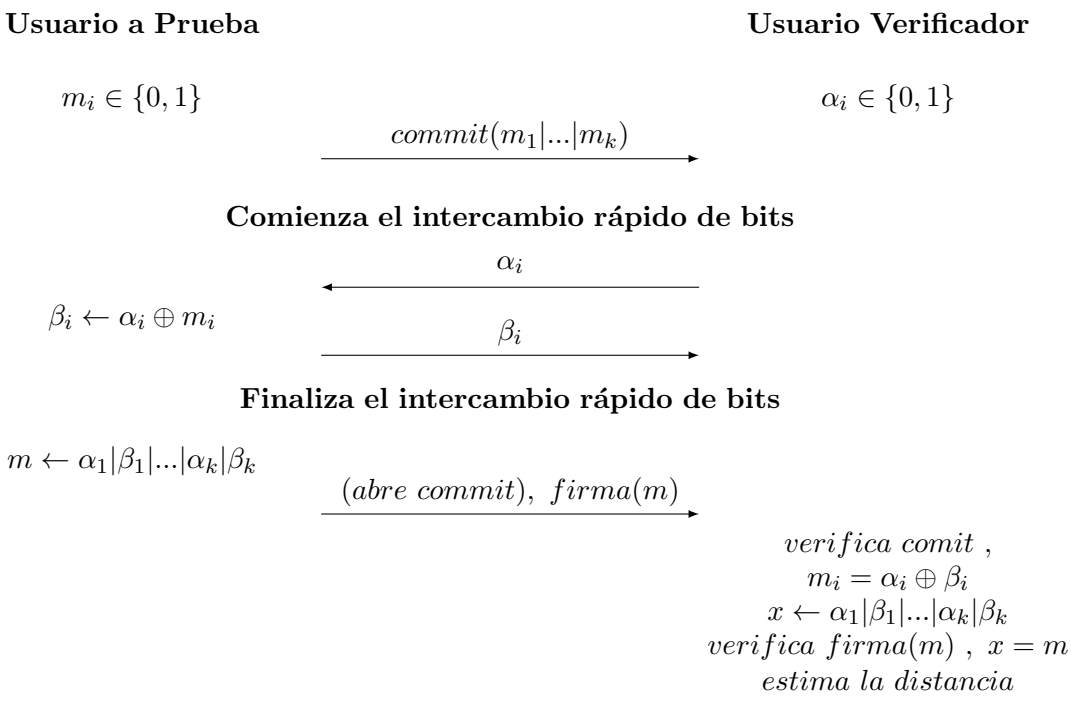


Figura 1.6: Protocolo DBP de Brands and Chaum.

El protocolo DBP de Brands and Chaum se describe a continuación.

(a) P genera aleatoriamente k bits m_i. Mientras, V genera aleatoriamente k bits α_i.

(b) P envía la concatenación de los k bits m_i $(m_1|\cdots|m_k)$, en forma segura, a V.

(c) Comienza un intercambio rápido de bits entre V y P.

(d) V envía un bit α_i a P. Y V responde inmediatamente enviando el bit $\beta_i \leftarrow \alpha_i \oplus m_i$.

(e) Finaliza el intercambio rápido de bits entre V y P.

(f) P envía a V la información para descifrar la concatenación de los k bits m_i.

(g) P concatena los $2k$ bits α_i y β_i en x $(x \leftarrow \alpha_1|\beta_1|\cdots\alpha_k|\beta_k|)$.

(h) P envía x firmado con su clave secreta a V.

(i) V verifica si los bits $\alpha_i \oplus \beta_i$ corresponde a los bits m_i.

(j) V verifica si la firma de P es correcta.

(k) Si todo es correcto, V calcula una cota superior de la distancia a P utilizando el máximo retardo estimado.

En la Figura 1.6 se puede observar que el usuario P debe calcular la operación XOR de dos bits. Es importante que el usuario P realice el menor número de operaciones posibles durante el intercambio rápido de bits y la operación XOR se puede realizar de manera muy eficiente en hardware. Esto para mantener el retardo de procesamiento lo más pequeño posible. Luego, para obtener una alta precisión se requiere que ambos usuarios dispongan de hardware dedicado para el protocolo DBP.

Protocolo DBP de Hancke and Kuhn

El protocolo de Brands y Chaum no ha sido diseñado para hacer frente a los errores de bits durante la fase de intercambio rápido de bits. Un único error de bit puede causar el fracaso del protocolo. Esto puede ser un problema significativo en entornos ruidosos, como los entornos de la identificación en radio frecuencia, RFID (Radio Frequency IDentification).

Hancke y Kuhn proponen el primer protocolo delimitador de la distancia remoto dedicado a redes RFID, el cual se puede ampliar fácilmente para hacer frente a los errores en la transmisión de bits. En comparación con el protocolo de Brands y Chaum, sólo tiene dos fases (una fase lenta y otra fase rápida), la tercera fase de la firma de mensajes no es necesaria. Este es un protocolo sencillo y rápido. El protocolo se muestra en la Figura 1.7.

El protocolo DBP de Hancke and Kuhn se describe a continuación.

(a) Tanto P como V disponen de una clave secreta K y una función seudoaleatoria $h(K, N)$.

(b) V genera un string impredecible N_V y N bits C_i.

(c) V le envía a P el string N_V.

(d) Ambos P y V calculan dos secuencias de n bits, R^0 y R^1, con la función seudoaleatoria $h(K, N_V)$

(e) Comienza un intercambio rápido de bits entre V y P, n intercambios de bits.

(f) V envía un bit C_i a P. Y V responde inmediatamente enviando el bit $R_i^{C_i}$.

(g) Finaliza el intercambio rápido de bits entre V y P.

(h) V verifica si los bits recibidos son correctos.

(i) Si todo es correcto, V calcula una cota superior de la distancia a P.

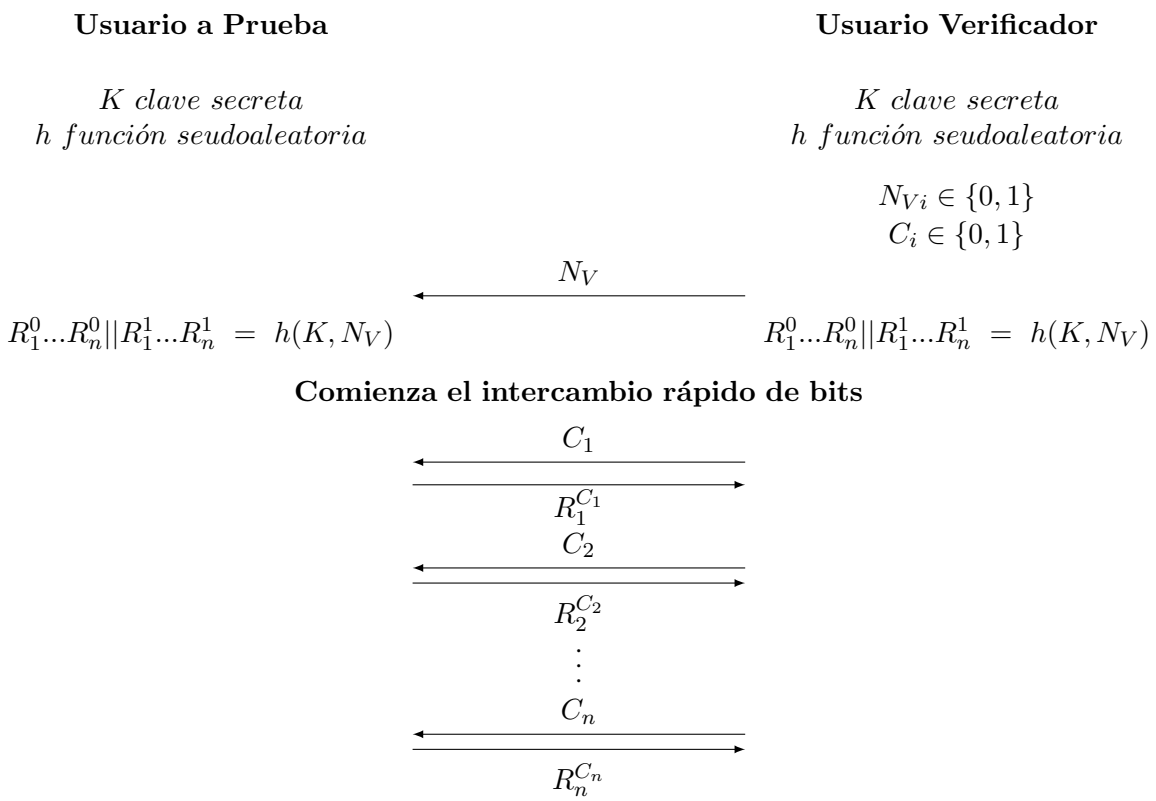


Figura 1.7: Protocolo DBP de Hancke and Kuhn.

1.2.3. Ataque de Delimitación de la Distancia

En el Ataque de dElimitación de la Distancia (AED) el usuario V mide el tiempo que transcurre desde que envía un mensaje de desafío a P hasta que recibe una respuesta de él. Este cálculo de tiempo, más el conocimiento de la velocidad de la señal física utilizada para transmitir los mensajes y el tiempo que demora P en responder, le permite a V determinar su distancia a P.

La distancia entre los usuarios P y V es estimada por medio de la ecuación 1.4.

$$\widetilde{d}_{VP} = c \quad \frac{t_m - t_d}{2} \tag{1.4}$$

$$t_m = 2\, t_p + t_d \tag{1.5}$$

Donde c es la velocidad de propagación de la onda electromagnética en el medio de comunicación, t_p es el tiempo de propagación de la señal de comunicación entre los dos usuarios,

t_m es el tiempo total que mide el usuario V desde que envía su desafío hasta la recepción de la respuesta de P y t_d es el tiempo que demora el usuario P en responder al desafío recibido de V.

Con este ataque V puede estimar un círculo, de radio $\widetilde{d}_{VP}$ y centro en si mismo, en el cual se debería encontrar P. Esto se muestra en la Figura 1.8.

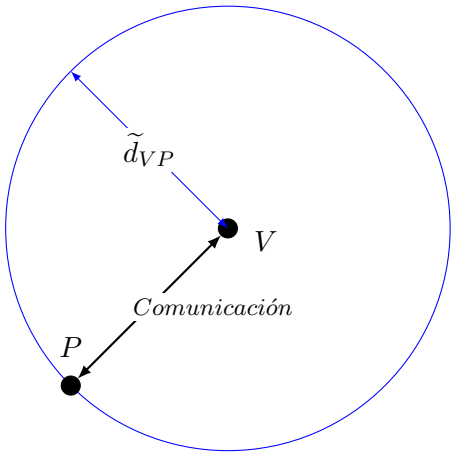


Figura 1.8: Determinación de la distancia entre V y P, por medio del ataque AED. V realiza un intercambio rápido de bits con P, *Comunicación*, para determinar la distancia, $\widetilde{d}_{VP}$, entre ambos.

1.2.4. Ataque de Ajuste del Area de Cobertura

En el Ataque de ajuste de Area de Cobertura (AAC) el usuario V ajusta su potencia de transmisión para determinar el límite del nivel de potencia al cual P responde a un desafío suyo. Por ejemplo, el usuario V envía un mensaje de desafío a P aumentando gradualmente su potencia de transmisión hasta que recibe una respuesta de P. El conocimiento de esta potencia, de la atenuación de la señal de comunicación durante la transmisión del mensaje y el nivel de recepción requerido por P para responder un mensaje, le permite a V determinar su distancia a P.

La distancia entre los usuarios P y V es estimada utilizando algún modelo de propagación de la señal electromagnética utilizada en la comunicación entre los usuarios. Para el modelo en espacio libre la potencia recibida es estimada por la ecuación 1.6, de la cual se deriva la estimación de la distancia entre los usuarios, ecuación 1.7.

$$W_r = \frac{1}{\xi} \frac{W_t}{d^2} \tag{1.6}$$

Donde ξ es una constante, d la distancia entre el nodo de transmisión y el nodo de recepción, W_t es la potencia de transmisión y W_r es la potencia de recepción.

$$\widetilde{d}_{VP} = \sqrt{\xi \frac{W_{Vt}}{W_{Prm}}} \tag{1.7}$$

Para la ecuación 1.7; ξ es una constante, W_{Vt} es la potencia de transmisión de la señal del desafío enviado por V y W_{Prm} es la potencia mínima requerida por P para recibir un mensaje válido.

Con este ataque V puede estimar un círculo, de radio $\widetilde{d}_{VP}$ y centro en si mismo, en el cual se debería encontrar P. Esto se muestra en la Figura 1.9, donde d_1 y d_2 son ejemplos de distancias equivalentes a rangos de transmisión donde P no ha respondido el desafío de V.

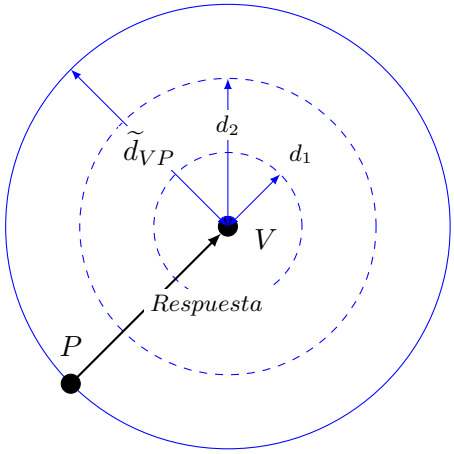


Figura 1.9: Determinación de la distancia entre V y P, por medio del ataque AAC. V realiza un aumento gradual de la potencia de transmisión del mensaje a P para determinar la distancia, $\widetilde{d}_{VP}$, entre ambos.

1.2.5. Tipos de Refinamientos

Dentro de esta investigación se pueden distinguir dos tipos de refinamientos de la región de encubrimiento R, refinamiento por arriba y refinamiento por abajo. Estos se diferencian por la ubicación del área de la región R, con respecto al usuario verificador V, en la cual se determina que no es factible que se encuentre el usuario a prueba P. Estos se podrían presentar en forma individual o combinada dentro de un proceso de refinamiento de una región de encubrimiento R.

Refinamiento por Arriba

En el refinamiento por arriba, V determina que P no se puede encontrar en un área de la región R cuya ubicación en relación al centro O de la región R es, principalmente, opuesta a su ubicación. En la Figura 1.10 se presenta un refinamiento por arriba.

En la Figura 1.10, P entrega una región de encubrimiento R a V, área encerrada por la circunferencia de linea segmentada de radio r. Luego, V, por medio de algún procedimiento, determina que P no se puede encontrar fuera del área de color y reduce la región R a una región de encubrimiento refinada R_F, área achurada, igual a la intersección de la región R con el área de color. La región R ha sido refinada por arriba, V puede asegurar que P no se encuentra en el área de R que permanece en blanco, la más lejana a V.

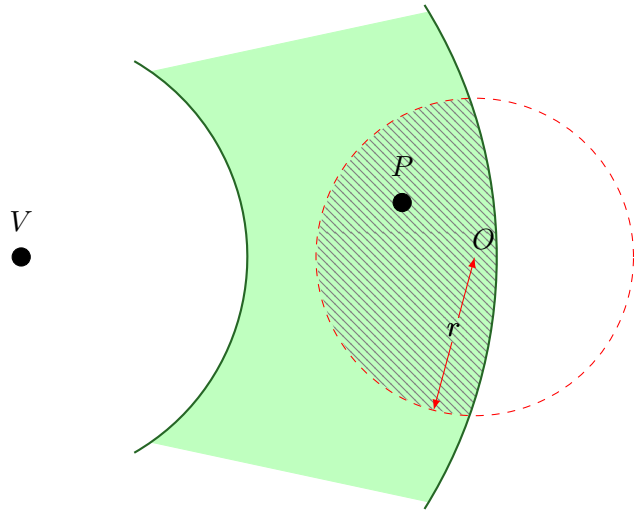


Figura 1.10: Refinamiento por arriba.

Refinamiento por Abajo

En el refinamiento por abajo, V determina que P no se puede encontrar en un área de la región R que enfrenta a su ubicación. En la Figura 1.11 se presenta un refinamiento por abajo.

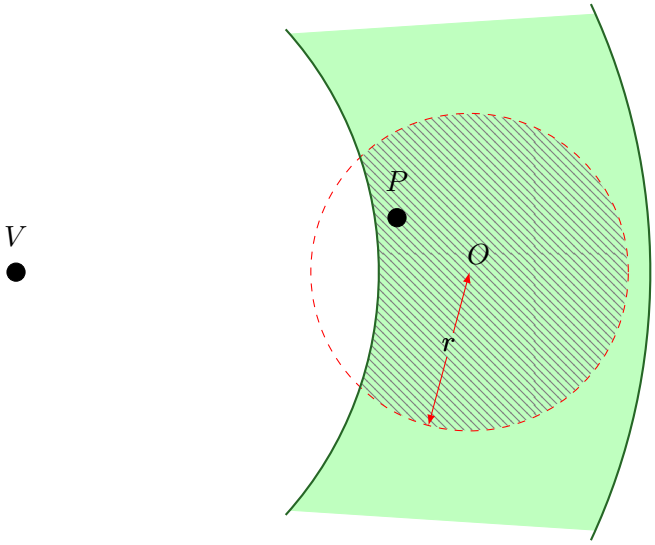


Figura 1.11: Refinamiento por abajo.

En la Figura 1.11, P entrega una región de encubrimiento R a V, área encerrada por la circunferencia de línea segmentada de radio r. Luego, V, por medio de algún procedimiento, determina que P no se puede encontrar fuera del área de color y reduce la región R a una región de encubrimiento refinada R_F, área achurada, igual a la intersección de la región R con el área de color. La región R a sido refinada por abajo, V puede asegurar que P no se encuentra en el área de R que permanece en blanco, la más cercana a V.

En la Figura 1.12 se presenta un refinamiento combinado, refinamiento por abajo y por arriba presentes dentro de un proceso de refinamiento de una región de encubrimiento R.

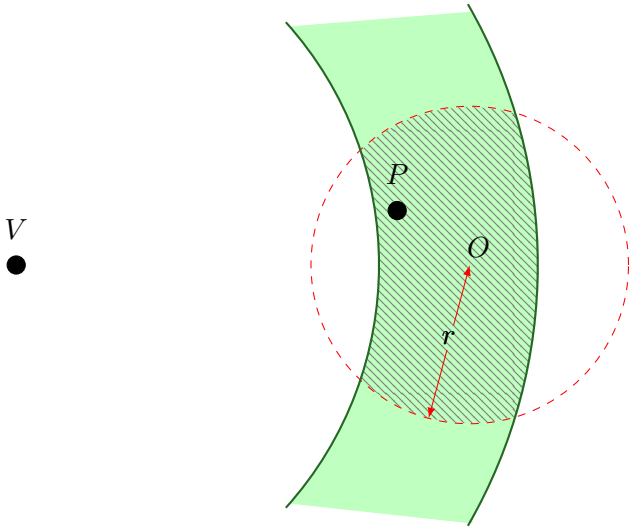


Figura 1.12: Refinamiento combinado, refinamiento por abajo y por arriba.

1.3. Hipótesis y Objetivos del Trabajo de Investigación

1.3.1. Hipótesis

La hipótesis planteada para el inicio de este trabajo de investigación es la siguiente :

"Es posible definir un protocolo de delimitación de distancia que considere los requerimientos de tolerancia del refinamiento de la región de encubrimiento exigidos por el usuario a prueba P y la utilidad de la distancia estimada por el usuario verificador V ."

1.3.2. Objetivos

Los objetivos planteados para el inicio de este trabajo de investigación son presentados a continuación.

Objetivo General

- Desarrollar un protocolo de delimitación de distancia que considere los requerimientos de tolerancia del refinamiento de la región de encubrimiento exigidos por el usuario a prueba P y la utilidad de la distancia estimada por el usuario verificador V .

Objetivos Específicos

- Desarrollar un protocolo de delimitación de distancia que permita crear una región de encubrimiento protegida frente a refinamientos por ajuste del área de cobertura y por

delimitación de distancia entre un usuario a prueba P estático y un usuario verificador V estático.

- Desarrollar un protocolo de delimitación de distancia que permita crear una región de encubrimiento protegida frente a refinamientos por ajuste del área de cobertura y por delimitación de distancia entre un usuario a prueba P estático y un usuario verificador V móvil.
- Desarrollar un protocolo de delimitación de distancia que permita crear una región de encubrimiento protegida frente a refinamientos por ajuste del área de cobertura y por delimitación de distancia entre un usuario a prueba P móvil y un usuario verificador V móvil.
- Desarrollar simulaciones de los protocolos de delimitación de distancia propuestos, en un simulador como el NS-3, considerando diversos modelos de propagación de señal y con diversos modelos de movilidad para los usuarios.
- Modificar los protocolos anteriores para minimizar la posibilidad que el usuario a prueba P trate de validar una ubicación falsa y desarrollar simulaciones de los algoritmos modificados, considerando diversos modelos de propagación de señal y con diversos modelos de movilidad para los usuarios, si es posible.

1.4. Alcance de la Investigación

Este trabajo de investigación busca desarrollar protocolos de delimitación de distancia que minimicen la probabilidad que la región de encubrimiento de un usuario a prueba (P) sea refinada, por sobre un nivel de tolerancia, cuando un usuario verificador (V) pretenda determinar la localización del usuario P en un proceso de delimitación de distancia y permitan concluir el proceso de verificación de ubicación con la menor incertidumbre posible.

Estos protocolos deben garantizar un balance que permita: *1*) Que el grado de refinamiento de la región de encubrimiento no supere un nivel de tolerancia establecido por P. *2*) Que la distancia determinada por V al usuario P no sea superior a una cota máxima determinada por V para fines de verificación.

Estos protocolos deben soportar las siguientes condiciones de usuarios: *1*) usuario estático y usuario verificador estático, *2*) usuario estático y usuario verificador móvil, *3*) usuario móvil y usuario verificador estático, *4*) usuario móvil y usuario verificador móvil.

Estos protocolos deben considerar los siguientes dos tipos de procedimientos para que el usuario verificador V pueda verificar que el usuario a prueba P se encuentra dentro de la región de encubrimiento declarada por este último: el ataque de ajuste del área de cobertura de transmisión y el ataque de delimitación de distancia.

En el escenario para este trabajo de investigación el usuario a prueba P está dispuesto a liberar una región de encubrimiento que lo contenga, pero no su posición exacta, para realizar un protocolo de delimitación de distancia con un usuario verificador V. Se supone que tanto V como P conocen los medios de los cuales dispone el otro y los protocolos utilizados; no poseen antenas adaptativas o direccionales que les permitan a ambos inferir la dirección de llegada de un paquete, sólo poseen antenas omnidireccionales; y el escenario en que se encuentran V y P es ideal, la propagación de las señales es perfecta.

1.5. Estado del Arte

El problema de la delimitación segura de distancia y verificación de ubicación en redes ad hoc inalámbrica fue inicialmente investigado por Brands y Chaum [7]. Estos autores proponen un protocolo donde una entidad llamada usuario verificador (V) determina un límite superior de la distancia a un nodo seleccionado como el usuario a prueba (P). En este protocolo, varios mensajes de desafío son enviados por el usuario verificador y cada uno es inmediatamente respondido por el usuario a prueba, quedando la distancia estimada por el tiempo en recibir la respuesta. Esta distancia se obtiene multiplicando la velocidad de una onda electromagnética por el tiempo que le toma a un desafío retornar al usuario verificador, su RTT (Round-Trip delay Time). Este enfoque funciona si el usuario a prueba se comporta correctamente. Si el usuario verificador sabe que el usuario a prueba que realizó la transposición de bits en la fase de intercambio rápido de bits está cerca y que sabe la clave privada del protocolo, puede estar seguro que este contacto es único.

Hancke y Kuhn [20] proponen el primer protocolo delimitador remoto dedicado a redes RFID (Radio Frequency IDentification). El protocolo de Brands y Chaum y sus derivados no han sido diseñados para hacer frente a los errores de bits durante la fase de intercambio rápido de bits. Un único error de bit puede causar el fracaso del protocolo. Esto puede ser un problema significativo en entornos ruidosos, como los entornos de la RFID. Hancke y Kuhn ofrecen un protocolo delimitador de la distancia que se puede ampliar fácilmente para hacer frente a los errores en la transmisión de bits. En comparación con el protocolo de Brands y Chaum, solo tiene dos fases (una fase lenta y fase rápida), la tercera fase de la firma de mensajes requerida por el protocolo de Brands y Chaum no es necesaria. Este es un protocolo sencillo y rápido, pero sufre de una alta probabilidad de éxito de ataques de algún adversario.

De los dos protocolos anteriores se han derivado los dos grupos principales en los que se pueden clasificar los Protocolos Delimitadores de Distancia. Entre estas derivaciones se pueden mencionar las siguientes:

El protocolo MAD (Mutual Authentication with Distance-Bounding) de Capkun et al. [8] es propuesto dentro del proyecto SECTOR (SECure Tracking Of node encounteRs), el cual es un conjunto de protocolos para la verificación segura entre nodos. El protocolo MAD se deriva ligeramente del protocolo de Brands y Chaum. Se han modificado sus propiedades para permitir la determinación mutua de la distancia entre nodos y para evitar el uso de la firma electrónica.

Sastry et al. [41] expresan que el tiempo de procesamiento en el usuario a prueba P al recibir un mensaje de desafío no es despreciable con respecto al tiempo de propagación cuando se utiliza una señal de radiofrecuencia (RF). Estos autores proponen el protocolo Echo, donde el tiempo de procesamiento del usuario a prueba P es tomado en cuenta. Los mensajes de desafío son enviados a través de una interfaz RF, en cambio, las respuestas a estos desafíos son transmitidas a través de una interfaz de ultrasonido.

Singelee et al. [42] señalan que los protocolos de delimitación de distancia basado en señales ultrasónicas son vulnerables a ataques de "agujeros de gusano", y proponen sólo el uso de señales de RF. En este ataque la señal de comunicación es retransmitida, ocupando un medio diferente al original, para indicar que el usuario a prueba se encuentra más cerca o más lejos de lo que realmente está. Estos autores también dan recomendaciones sobre cómo modificar un protocolo de delimitación de distancia como el de Brands y Chaum para que pueda ser resistente al ataque denominado "fraude terrorista". En este ataque el usuario a prueba se colude con un tercero

para indicar al usuario verificador que se encuentra más cerca de lo que realmente está.

El protocolo de Singelée et Preneel [43] es un protocolo mejorado de delimitación distancia, basado en el protocolo MAD de Capkun et al., para canales ruidosos. Este ofrece una reducción sustancial (aproximadamente 50 %) en el número de rondas de comunicación en comparación con el protocolo Hancke y Kuhn. La idea principal es utilizar códigos binarios para corregir errores de bits que se producen durante los intercambios rápidos de bits.

El protocolo de Tu et Piramuthu [48] es un protocolo que tiene como objetivo reducir la probabilidad de éxito de un ataque en la fase de desafío/respuesta como parte de un ataque de relevo. El protocolo es adecuado para redes RFID. Este protocolo es resistente a los ataques de fraude terrorista y aunque se reduce la probabilidad de un ataque de fraude de la mafia, la vulnerabilidad sigue existiendo.

Capkun et al. [10] proponen un protocolo de verificación de ubicación basado en interfaces de RF y de ultrasonidos para evitar el problema del tiempo de procesamiento en el usuario a prueba. Para evitar los ataques afectos al uso de interfaces de ultrasonido, los autores asumen que el usuario verificador es una estación móvil encubierta. Más tarde, Rassmussen et al. [38] muestran la factibilidad de implementar un protocolo de delimitación de distancia sólo con interfaces de red de RF, el cual es capaz de recibir, procesar y transmitir señales RF en menos de 1 nanosegundo. Estudios de este tipo de ataques y propuestas para enfrentarlos también se presentan en [14, 16, 47].

El protocolo de Nikov et Vauclair [33] ha sido diseñado para ser ligero y no interactivo, sé adaptada a las ejecuciones periódicas que están en conformidad con la naturaleza de la proximidad de medición a los dispositivos móviles. Por el contrario, es sensible a ruido electrónico y, por tanto, requeriría el uso de un código de control HMAC (Keyed-Hash Message Authentication Code) o encriptación AES (Advanced Encryption Standard).

El protocolo de Munilla et Peinado [32] es propuesto para disminuir la probabilidad de éxito de ataques como el ataque de fraude de distancia, el ataque de relevo y el fraude terrorista; y para reducir el tiempo medio para completar el protocolo. La modificación consiste en introducir desafíos vacíos. Una modificación de este protocolo es presentada por Kim et Avoine [27] dende se establecen dos tipos de desafíos: desafíos aleatorios y desafíos predefinidos.

El protocolo Swiss-knife [28] es propuesto para abordar la seguridad, la privacidad, la sobrecarga computacional y la tolerancia a fallos. Derivado del protocolo de Hancke y Kuhn, se basa en el protocolo de MAP1 (Mutual Authentication Protocol one) de Bellare y Rogaway [4] y en la variante MAP1.1 propuesta por Guttman et al. [19].

El protocolo Poulidor de Trujillo-Rasua et al. [46] es el primer protocolo de delimitación distancia basado en grafos, este resiste los fraudes de mafia y terrorista. Su objetivo es un protocolo que proporciona un buen compromiso entre estos dos ataques, sin sacrificar memoria.

Los protocolos de Benfarah et al. [5] hacen uso de la tecnología TH-UWB (Time-Hopping Ultra Wide Band). Denominados, protocolo A (secret TH sequences) y protocolo B (secret mapping code). Su objetivo es mejorar la protección frente al ataque de fraude de la mafia en un entorno real (con ruido electrónico).

El protocolo de Reid et al. [31, 39] presenta el primer protocolo de delimitación distancia con clave simétrica para radiofrecuencia, efectivo contra ataques de fraude de la mafia y de fraude terroristas. En su trabajo se ha tenido en cuenta el hecho que estos dispositivos son sensibles al ruido, añadiendo un mensaje firmado en la fase de intercambio rápido de bits.

Aún cuando en este trabajo se asume que el usuario verificador no está coludido con otros

usuarios es relevante conocer otros temas existentes de localización.

Para delimitar la ubicación de un usuario inalámbrico se han propuesto diversas técnicas basadas en múltiples verificadores que trabajan en colaboración [9, 11, 42, 49]. Por ejemplo, Capkun et al. [9] propusieron un "esquema de multilateración" para comprobar si la ubicación reclamada por el usuario a prueba es cierta. Liu et al. [30] argumentan que los protocolos existentes, o bien requieren interfaces de red especiales y/o necesitan la colaboración de otros usuarios en sus cercanías. Estos autores, proponen un protocolo de verificación de usuario a usuario para redes dispersas, la cual se apoya en una red de satélites.

Ranganathan et al. [36] proponen un nuevo esquema de capa física diseñado específicamente para un protocolo de delimitación de distancia en escenarios de baja potencia y corto alcance. La capa física combina frecuencia modulada de onda continua (FMCW) y la comunicación de retrodispersión. El uso de la comunicación de retrodispersión permite un bajo consumo de energía en el usuario a prueba. Debido al uso de la capa física para delimitación de distancia se puede desacoplar este proceso del retardo en el usuario a prueba, permitiendo la realización de la mayoría de los protocolos de delimitación de distancia desarrollados en el pasado. El sistema ofrece fuertes garantías de seguridad contra fraudes de distancia, mafia y terrorista.

Todos los enfoques anteriores asumen un escenario de espacio libre, pero Abumansoor et al. [2] proponen un protocolo de verificación de ubicación para redes vehiculares ad hoc donde los vehículos no tienen una línea visual directa.

Rasmussen et al. [37] señalan que todos los protocolos de delimitación propuestos poseen fuga de información de distancia y de ubicación de los usuarios a prueba y del usuario verificador hacia oyentes externos. Esta pérdida de la privacidad de ubicación viene a través de la medición de los tiempos de llegada de los mensajes. Este problema difiere de este trabajo de investigación, ya que en el trabajo de Rasmussen et al. se asume que el usuario a prueba ofrece su ubicación exacta y el adversario no es el usuario verificador, sino que un usuario externo al protocolo que está escuchando el tráfico generado como producto de la ejecución de un protocolo de delimitación distancia. Además, la solución propuesta por Rasmussen et al. tiene la intención de evitar que el adversario conozca toda la información sobre la ubicación del usuario a prueba y del usuario verificador. En lugar de ello, en este trabajo de investigación, al usuario a prueba no le importa hacer pública una región encubierta que incluye a su posición real.

En el contexto de enrutamiento geográfico, Xu. et al. [54] muestran que el ataque de cobertura de transmisión puede refinar la región de encubrimiento de un objetivo y proponen un protocolo de enrutamiento que impide este ataque. Sin embargo, su enfoque difiere de esta propuesta de investigación en dos aspectos. *1*) En el trabajo de Xu. et al. se asume que la región de encubrimiento de cada nodo se conoce y la decisión tomada por un receptor para enviar un paquete requiere determinar si la intensidad de la señal del paquete recibido cubre completamente la región de encubrimiento del receptor. Por el contrario, en el enfoque de este trabajo de investigación se muestra que esta condición es necesaria pero no suficiente para evitar un ataque de refinamiento y se busca proponer una nueva técnica que la evite o bien la mitigue. *2*) En el trabajo de Xu. et al. no se tiene en cuenta que un ataque de delimitación de distancia puede aún refinar exitosamente la región encubrimiento de un receptor a pesar que el ajuste del área de cobertura de transmisión pueda fallar.

La idea de utilizar retardo de tiempo se ha propuesto antes para proveer comunicación anónima en redes móviles inalámbricas. Huang et al. [23] introduce el concepto de periodo de silencio. En este período de tiempo, los usuarios no pueden optar por revelar su antigua o su

nueva MAC (Message Authentication Code) con el fin de prevenir un ataque de correlación MAC. Estos ataques intentan recuperar parte de una secuencia de cifrado MAC ya empleada y comparar las secuencias generadas con la secuencia de cifrado real.

En la línea de implementación de los protocolos delimitadores Abu-Mahfouz y Hancke [1] discute la posibilidad de implementar los protocolos delimitadores de distancia dentro de la industria de RFID y de las aplicaciones de localización en tiempo real; lo que requiere de un énfasis en aspectos tales como fiabilidad, seguridad, comunicación en tiempo real y eficiencia energética. En la misma dirección de valoración de la implementación de los protocolos delimitadores de distancia Avoine et al. [3] propone una metodología para comparar razonablemente los protocolos delimitadores a pesar de sus diversas propiedades. Este documento presenta una metodología basada en conceptos del campo de la toma de decisiones, la que permite una comparación multi-criterio de los protocolos delimitadores de distancia.

Tippenhauer et al. [45] presenta la primera realización completa de un sistema de intercambio rápido de bits para la delimitación de distancia. Este sistema consiste en una radio UWB (Ultra-Wideband) y una placa FPGA (Field-Programmable-Gate-Array) con el procesamiento digital implementado; este alcanza una precisión de 7[cm] a 5[cm] y un retardo de procesamiento en el usuario a prueba menor a 100[ns].

Las principales diferencias de los trabajos mencionados en los párrafos anteriores con este trabajo de investigación son las siguientes: en todos los trabajos la información disponible sobre los usuarios es mayor a la disponible en este trabajo, por ejemplo, el usuario a prueba conoce una región donde se encuentra el usuario verificador; en la mayoría de los trabajos el usuario a prueba entrega su posición exacta, a diferencia de este trabajo, donde se entrega una región en la cual se encuentra el usuario a prueba; en la mayoría de los trabajos el adversario es un tercer usuario, mientras en este trabajo los usuarios participantes son honestos y a las vez adversario; y para la mayoría de los trabajos la precisión en la determinación de la posición exacta del usuario a prueba es relevante.

Capítulo 2

Formalización del Problema

En este capítulo se entrega la formalización del problema a estudiar en este trabajo de investigación. Se comienza presentando el problema en su forma más general, formalización del problema, Sección 2.1. Se continúa con las condiciones que restringen el entorno del problema y definen el resto de esta investigación, Sección 2.2. Y se finaliza este capítulo con la justificación de las condiciones planteadas para esta investigación, Sección 2.3.

2.1. El Problema

En el párrafo siguiente se formaliza el problema a investigar, en su forma general. Esta formalización presenta la base sobre la cual se define el entorno de estudio para el resto de este trabajo de investigación.

" Se cuenta con 2 nodos: V el nodo verificador y P el nodo a prueba. V desea conocer una cota práctica de su distancia a P, cuando se permite a P declarar una región de encubrimiento R en reemplazo de su posición exacta. La cota práctica requerida por V impone que R tenga un área máxima que P debe satisfacer. Por su parte P aceptará participar del proceso de cálculo de la distancia práctica siempre que el tamaño del área requerida por V sea superior, o al menos igual, que el área aceptable por P. La región de encubrimiento R es un área que incluye la posición real de P, y que cumple ciertas restricciones de seguridad, privacidad de ubicación, etc, impuestas por P. P desea participar de este proceso de cálculo de la distancia práctica, bajo la condición que V no refine su área de encubrimiento más allá de un factor de tolerancia $\tau \in [0, 1]$ ".

La Figura 2.1 describe el escenario propuesto. En esta figura, por simplificación, se asume un escenario ideal en un espacio 2D y regiones circulares. La región de encubrimiento R es el área circular centrada en el punto O y de radio r. La cota máxima requerida por el usuario V es el radio r_u, el cual define la región circular U con centro en el punto O, satisfaciéndose que $r \leq r_u$. El usuario P se encuentra incluido en la región de encubrimiento R y el usuario V se encuentra fuera, como caso particular y no excluyente, de la región R.

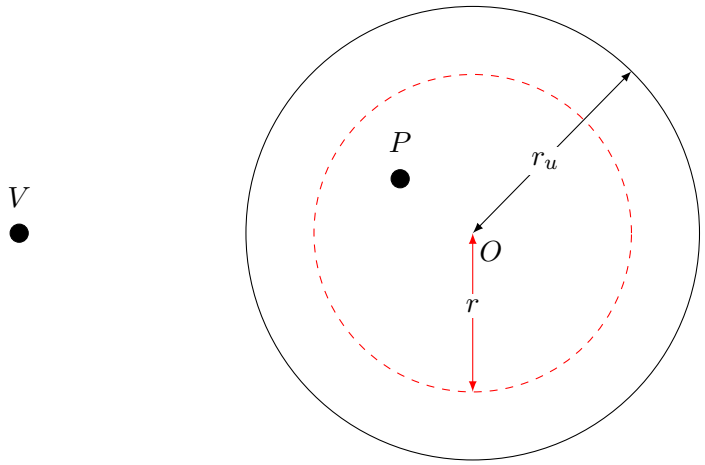


Figura 2.1: Escenario propuesto. Con la región de encubrimiento R, circunferencia de radio r y centro O, y la región útil para fines de verificación U, circunferencia de radio r_u y centro O.

2.2. Entorno de Estudio del Problema

El entorno en el cual se estudia el problema de este trabajo de investigación, presentado en la Figura 2.1, tiene como base la formalización del problema presentada en la sección anterior, Sección 2.1.

Dos usuarios, el usuario a prueba P y el usuario verificador V, desean participar en un protocolo delimitador de distancia (DBP). Cada usuario conoce su posición exacta y esta es secreta para el resto. El usuario P desea entregar una región de encubrimiento R, que lo contenga, en lugar de su ubicación precisa y el usuario V desea verificar que P se encuentre dentro de una cota práctica de la distancia sin entregar su posición.

Para el trabajo de investigación el adversario para el desarrollo del protocolo deseado es el usuario V, éste es quien trata de refinar la región de encubrimiento del usuario P. No se considera la participación de terceros usuarios que se puedan coludir con alguno de los dos usuarios o realizar un ataque coludido entre terceros.

El usuario P impone para el área de la región R ciertas características; restricciones de seguridad, privacidad de ubicación, etc.; con el fin que estas disminuyan la resolución de su ubicación. Estas restricciones no son relevantes de mencionar, pues no es objetivo de este trabajo de investigación el construir las regiones de encubrimiento. La distribución de probabilidades para la probabilidad que un usuario ocupe un lugar dentro de una región se considera homogénea, por lo cual la entropía de la región esta relacionada en forma directa con el área de esta.

El usuario V le impone al procedimiento una restricción práctica a la distancia, la cual se traduce en un radio r_u en torno al centro O de la región R. Esta cota máxima requerida por V a P forma una región U de área circular.

El escenario es ideal en un espacio 2D, con regiones circulares y propagación de las señales electromagnéticas en forma perfecta, es decir, de radio circular y sin shadowing. La región de encubrimiento R es un área circular centrada en O y radio r.

Ambos usuarios, P y V, conocen los medios utilizados para la comunicación y los protocolos

involucrados en el procedimiento. Los medios utilizados para la comunicación permiten la medición y control de los tiempos de comunicación y de la potencia de la señal electromagnética de comunicación. No se considera el uso de antenas adaptativas o direccionales que permitan a ambos usuarios inferir la dirección de llegada de un mensaje.

Los procedimientos utilizados para la estimación de la distancia por parte del usuario V son: el Ataque Basado en el ajuste del Area de Cobertura de una transmisión inalámbrica (ABAC) y el Ataque Basado en la dElimitación de Distancia (ABED) entre V y P.

El usuario P está dispuesto a participar en el protocolo DBP si el área de su región de encubrimiento no es refinada más allá de un factor de tolerancia $\tau \in [0, 1]$. Mientras que el usuario V está dispuesto a participar en el protocolo DBP si se respeta su cota práctica de la distancia entre V y P.

El procedimiento debe considerar las siguientes salidas:

1. El usuario V concluye una distancia a P que es útil para fines de verificación. El grado de refinamiento de la región de encubrimiento estuvo dentro de los rangos tolerados por P.
2. El usuario V concluye que no es posible que P esté dentro de su región de encubrimiento.
3. El usuario V concluye que P no está en una región útil para fines de verificación.
4. Tanto V como P pueden cancelar la ejecución completa del protocolo ya que pueden considerar que las exigencias de distancia útil y grado de refinamiento de la región de encubrimiento de P supera los valores máximos deseados.

El presente trabajo de investigación no considera relevantes para el estudio las fronteras de las regiones involucradas ni una región de encubrimiento de radio cero.

2.3. Justificación del Entorno Problema

La idealización del entorno del problema tiene su justificación en el comienzo del estudio de un problema, para poder estudiar un problema real hay que tener una referencia en la cual compararse. Al tratarse este trabajo de investigación sobre la propuesta de un nuevo problema, es relevante comenzar con el desarrollo del punto de referencia.

La inclusión de sólo dos usuarios en el proceso también se justifica por ser este trabajo de investigación el estudio sobre la propuesta de un nuevo problema. La inclusión de terceros usuarios participantes en otros tipos de ataques queda para trabajos futuros.

La idealización de una distribución de probabilidades homogénea no conlleva problemas en la determinación de un protocolo delimitador de distancia consciente de la privacidad de ubicación, el cual no pueda ser modificado fácilmente si se considera una distribución de probabilidades no homogénea, ya que la distribución de probabilidades no homogénea afecta principalmente la creación de las regiones de encubrimiento. Punto que no es de interés en este trabajo de investigación.

El imponer una restricción práctica a la distancia viene de la necesidad de no esperar una respuesta a un desafío un tiempo superior al rango de transmisión.

La utilización de regiones circulares y radiación circular perfecta de la señal de comunicación tiene su base en la utilización generalizada de antenas omnidireccionales en los dispositivos móviles.

El no considerar relevantes para la investigación las fronteras de las regiones involucradas dentro del estudio, es debido a que las regiones pueden definirse como el área del círculo de un determinado radio o como el área dentro de una circunferencia de un determinado radio. Tampoco se considera relevante una región de encubrimiento de radio cero, ya que esto significa que se está entregando la ubicación exacta.

Capítulo 3

Solución al Ataque Basado en la Delimitación de la Distancia

En este capítulo se presentan diferentes formas de enfrentar un Ataque Basado en la dElimitación de la Distancia (ABED). Se comienza presentando el procedimiento más elemental en la Sección 3.1, y describiendo sus debilidades, las cuales llevan a la propuesta del siguiente procedimiento en la Sección 3.2. Con el mismo análisis se presentan nuevas propuestas en las secciones 3.3 y 3.4, finalizando con el procedimiento que se propone para el protocolo delimitador de distancia consciente de la privacidad de ubicación, Sección 3.5.

En el ABED el usuario verificador V actúa como el adversario que ataca la región de encubrimiento R para refinarla. V mide el tiempo que transcurre desde que envía un mensaje al usuario a prueba P hasta que recibe una respuesta de este. Este cálculo de tiempo, más el conocimiento de la velocidad de la señal física utilizada para transmitir los mensajes y el tiempo que demora P en responder, le permite a V determinar su distancia a P.

Los procedimientos presentados en este capítulo para enfrentar el ataque ABED se basan en el retardo de la transmisión del mensaje de respuesta, por parte de P, al desafío enviado por V. Esto con el fin que V determine una ubicación de P más lejana de lo que realmente esta es.

3.1. Retardo en Base a la Máxima Distancia

En la Solución en Base a un retardo igual a la Máxima Distancia (SBMD) P retarda su respuesta al desafío de V un tiempo δ equivalente a la distancia máxima entre su posición y la frontera de la región de encubrimiento R, $d_{(\delta)}$ en la Figura 3.1. La elección de un retardo equivalente a la distancia máxima, nace de la necesidad que con el retardo δ se pueda alcanzar la frontera de la región R para cualquier posición de V. Con esto se crea una zona de protección de R frente a intentos de refinamiento por parte de V, zona cuya frontera es la circunferencia en línea continua con centro en P y radio $d_{(\delta)}$ en la Figura 3.1.

Como se puede observar en la Figura 3.1 el vector de la máxima distancia d_{max}, vector entre P y la frontera de la región R con máxima magnitud, siempre pasará por el centro O de la región R y siempre será mayor o igual al radio de la región R, r, y menor o igual al diámetro de esta. Es decir, $r \leq d_{max} \leq 2r$. El usuario V puede utilizar este conocimiento para realizar un ataque ABED donde a la distancia estimada entre V y P con el retardo utilizado por P,

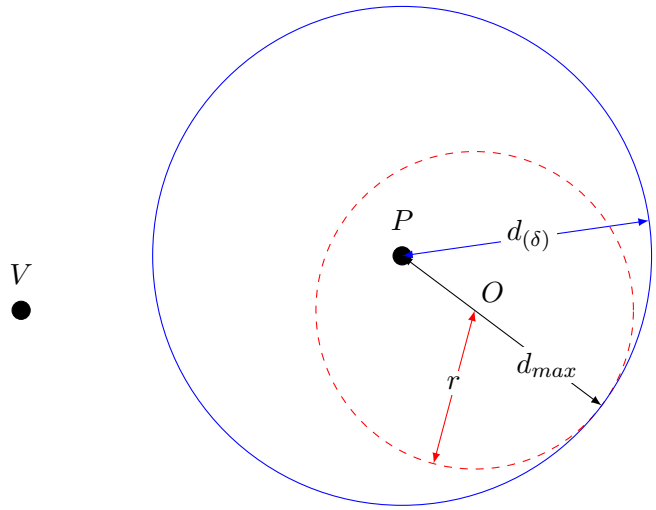


Figura 3.1: Máxima distancia d_{max} utilizada para retardar respuesta al desafío de un ataque ABED. La frontera de R en línea segmentada y la circunferencia que genera el retardo δ en torno a P en línea continua.

$\widetilde{d}_{VP}$, se le puede incorporar la resta del radio de R que es conocido por V, r, ya que el retardo siempre incorporará el tiempo en recorrer este radio. Luego, la distancia máxima estimada queda expresada por la ecuación 3.1.

$$\widetilde{d}_{VPmax} \;=\; \widetilde{d}_{VP} \;-\; r \tag{3.1}$$

Donde; $\widetilde{d}_{VP} = c(t_m - t_d)/2$, c es la velocidad de propagación de la onda electromagnética utilizada en el medio de comunicación, t_m es el tiempo total que mide el usuario V desde que envía su desafío hasta la recepción de la respuesta de P y t_d es el tiempo que demora el usuario P en responder al desafío recibido de V.

El ataque ABED que considera un retardo $\delta = t_{d_{max}}$ como parte adicional del ataque generará una región C, denominada corona circular, en la cual se debe encontrar P. En general, C tiene la forma de una corona circular centrada en V o la forma de un círculo, centrado en V, si el radio interno de la corona circular es cero. Esto se puede observar en la Figura 3.2.

La corona circular C es función de los retardos posibles, ecuación 3.2. Esta queda definida por la posición de V, como su centro, por su radio interno, r_{ci}, y por su radio externo, r_{ce} (ecuaciones 3.3 y 3.4), que además definen la frontera interior y exterior de C.

$$\delta \;\in\; [\; t_{(r)} \;,\; t_{(2r)} \;] \tag{3.2}$$

Donde, $t_{(r)}$ es el tiempo que demora la señal electromagnética utilizada en recorrer la distancia r y $t_{(2r)}$ es el tiempo que demora la señal electromagnética utilizada en recorrer la distancia $2r$.

$$r_{ci} \;=\; \widetilde{d}_{VPmin} \;=\; \widetilde{d}_{VP} \;-\; 2r \tag{3.3}$$

$$r_{ce} \;=\; \widetilde{d}_{VPmax} \;=\; \widetilde{d}_{VP} \;-\; r \tag{3.4}$$

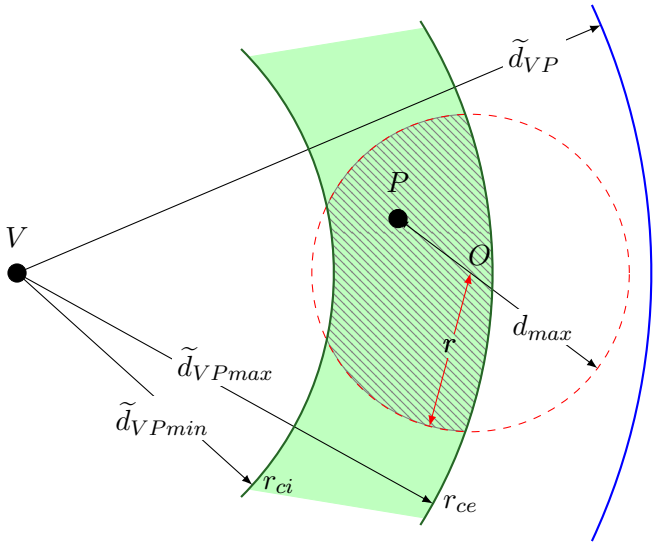


Figura 3.2: Ataque ABED considerando un retardo δ equivalente a una distancia máxima d_{max} de P a la frontera de su región de encubrimiento. La región C en color y la región R_F achurada.

La frontera interna de C se determina por la distancia estimada con el ataque ABED, $\widetilde{d}_{VP}$, a la cual se le resta el diámetro de la región R, ya que $\delta_{maximo} = 2r$ y P se encuentra dentro de R pues se supone honesto. Mientras, la frontera externa de C se determina por la distancia estimada con el ataque ABED, $\widetilde{d}_{VP}$, a la cual se le resta el radio de la región R, ya que $\delta_{minimo} = r$.

Como se observa en la Figura 3.2, la intersección de esta región C, región en color, con la región de encubrimiento R, círculo segmentado, determina un área de R en la cual se encuentra P, área achurada. Esta área es la región de encubrimiento refinada R_F.

Procedimiento frente al ataque ABED

Con referencia a la Figura 3.2, la participación de P en el procedimiento de verificación de distancia con el ataque ABED incrementado con δ equivalente a d_{max} se describe a continuación:

(a) El usuario P determina la región de encubrimiento R, enviándole a un tercero confiable los requerimientos para la creación de la región y espera su respuesta.

(b) Al recibir la región R, P determina el nivel de refinamiento τ y el retardo δ equivalente a d_{max}.

(c) P determina; con R, τ y δ; el nivel de refinamiento máximo posible de su región R para decidir si continua con el protocolo DBP.

(d) P entrega la región R a V. Y espera los desafíos del intercambio rápido de bits.

(e) Al recibir un desafío de V, P retarda su respuesta un tiempo δ.

Con referencia a la Figura 3.2, la participación de V en el procedimiento de verificación de distancia con el ataque ABED incrementado con δ equivalente a d_{max} se describe a continuación:

(a) V recibe la región R de P.

(b) V determina si la región R está dentro de la cota práctica de la distancia. Para saber si continua con el protocolo DBP.

(c) Si la cota práctica de la distancia es satisfecha, V comienza el intercambio rápido de bits. Si la cota práctica de la distancia no es satisfecha, se lo comunica a P y termina el procedimiento.

(d) Al recibir la respuesta de P a su desafío, V determina la distancia $\widetilde{d}_{VP}$ con el tiempo medido t_m.

(e) Con $\widetilde{d}_{VP}$ y el radio r, de la región R, V determina la distancia $\widetilde{d}_{VPmax} = \widetilde{d}_{VP} - r$, la que corresponde al radio externo de la corona circular, frontera exterior de la región C.

(f) Con $\widetilde{d}_{VP}$ y el radio r, V determina la distancia $\widetilde{d}_{VPmin} = \widetilde{d}_{VP} - 2r$, la que corresponde al radio interno de la corona circular, frontera interior de la región C.

(g) Con las regiones R y C, V determina la región R_F en la cual se podría encontrar P. $R_F = C \cap R$.

(h) Con los cálculos anteriores V verifica si P se encuentra en el interior de R.

Análisis del estudio de la solución

La elección de un retardo δ equivalente al tiempo de desplazamiento de la onda electromagnética para la distancia máxima d_{max} dentro de un intervalo posible $[r \leq, 2r]$, conlleva a un grosor máximo de la corona circular C, $g_c = \widetilde{d}_{VPmax} - \widetilde{d}_{VPmin}$, conocido e igual para toda condición posible de P y V, idéntico al radio r de la región R.

Lo expresado en el párrafo anterior implica que siempre se tendrá refinamiento de la región R; ya que el grosor máximo de C, g_c, es siempre menor que el diámetro de la región R, $2r$. Resultando en un menor refinamiento cuando P y V se encuentran cercanos. Esta es una situación no deseada para un protocolo delimitador de distancia consciente de la ubicación, DBPALP.

3.2. Retardo seleccionado sobre un Intervalo de Retardos Posibles

Se desea mejorar la capacidad de enfrentar el refinamiento de la región R por parte de V. Para esto se modifica la forma de seleccionar el retardo δ, con el fin de obtener un grosor de la corona circular C, g_c, mayor que el diámetro de la región R y así disponer de algún intervalo de retardos δ que aseguren que no habrá refinamiento posible.

En la Solución en Base a un Intervalo de Retardos posibles (SBIR) P retarda su respuesta al desafío de V un tiempo δ aleatorio seleccionado dentro de un intervalo $[0, \Lambda]$, donde Λ es un valor conocido tanto por P como por V.

Dado que el retardo mínimo es cero, $\delta = 0$, ya no se puede restar el radio de R, o un retardo mínimo, para determinar la frontera exterior de la región C. Para asegurar que se cubre toda la región R, con el retardo δ, en el tiempo Λ la señal electromagnética debe poder recorrer la máxima distancia posible entre P y la frontera de R, es decir, el diámetro de la región $(2r)$.

El ataque ABED que considera un retardo $\delta \in [0, \Lambda]$ como parte adicional del ataque genera una región C, corona circular, en la cual se debe encontrar P.

La intersección de la región C con la región de encubrimiento R determina el área de R en la cual se encuentra P. Esta área es la región de encubrimiento refinada R_F.

Para determinar si es posible un refinamiento de la región de encubrimiento se requieren las fronteras de la corona circular C, el radio externo $r_{ce} = \widetilde{d}_{VPmax}$ y el radio interno $r_{ci} = \widetilde{d}_{VPmin}$. Figura 3.3.

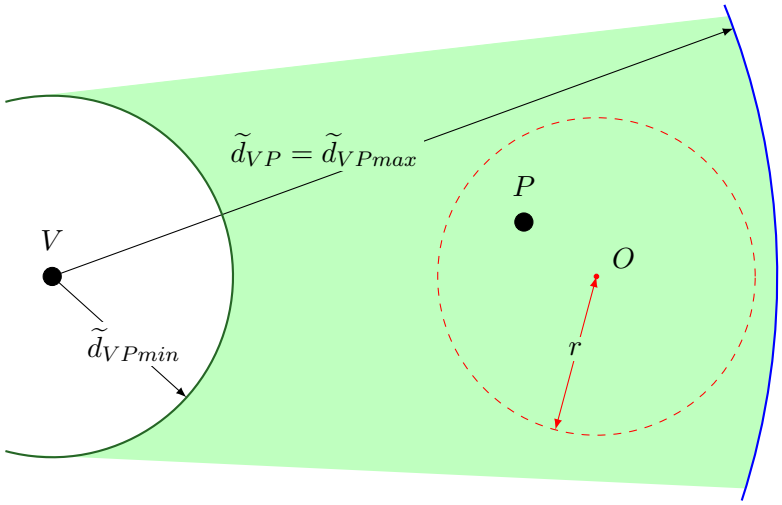


Figura 3.3: Fronteras de la corona circular C, región de color, para el procedimiento con retardo entre [0 , Λ].

Fronteras de la Corona Circular

Las fronteras de la corona circular C quedan definidas por sus radios, las ecuaciones vectoriales que definen estos son las ecuaciones 3.5 y 3.6, con referencia a las Figuras 3.3 y 3.4.

Para la frontera exterior de la región C.

$$r_{ce} = \widetilde{d}_{VPmax} = | \overrightarrow{VO} + \overrightarrow{OP} + \overrightarrow{d_{(\delta)[VP]}} | \tag{3.5}$$

Para la frontera interior de la región C.

$$r_{ci} = \widetilde{d}_{VPmin} = | \overrightarrow{VO} + \overrightarrow{OP} + \overrightarrow{d_{(\delta)[VP]}} - \overrightarrow{d_{(\Lambda)[VP]}} | \tag{3.6}$$

Donde, $\overrightarrow{VO}$ es el vector de la distancia entre V y O, $\overrightarrow{OP}$ es el vector de la distancia entre O y P, $\overrightarrow{d_{(\delta)[VP]}}$ es el vector de la distancia que recorre la señal electromagnética en el tiempo δ con la dirección del vector de la distancia entre V y P, y $\overrightarrow{d_{(\Lambda)[VP]}}$ es el vector de la distancia que recorre la señal electromagnética en el tiempo Λ con la dirección del vector de la distancia entre V y P. Estos se pueden observar en la Figura 3.4.

Las ecuaciones 3.5 y 3.6 junto con la frontera de la región R permiten determinar el refinamiento de esta.

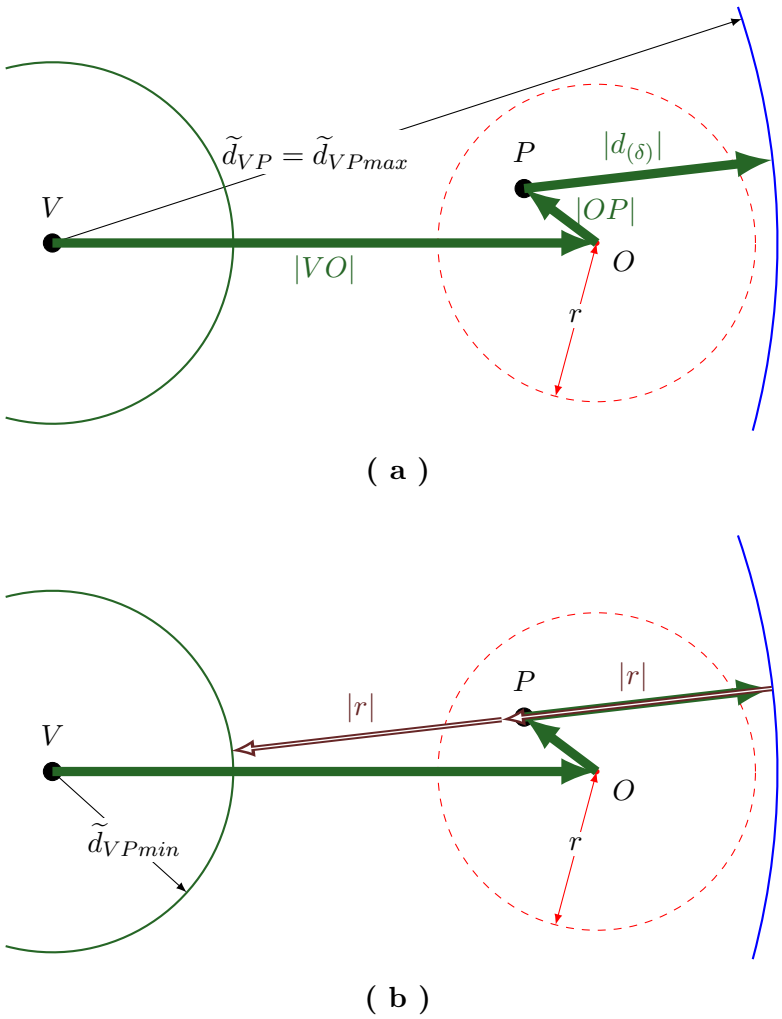


Figura 3.4: Vectores que determinan las fronteras de la corona circular, con radios $\widetilde{d}_{VPmin}$ y $\widetilde{d}_{VPmax}$. (a) frontera exterior y (b) frontera interior. Procedimiento con retardo en intervalo [0 , Λ].

Refinamiento por arriba

El refinamiento por arriba ocurre sobre la frontera exterior de la corona circular. Es decir, cuando alguna parte de la frontera de la región R se encuentra más lejana de V que la frontera exterior de la región C. Luego, ocurrirá un refinamiento por arriba de la región R si se cumple la siguiente desigualdad de distancias, ecuación 3.7, con referencia a la Figura 3.4.a.

$$| \overrightarrow{VO} + \overrightarrow{OP} + \overrightarrow{d_{(\delta)[VP]}} | < | \overrightarrow{VO} + \overrightarrow{r_{[VO]}} | \tag{3.7}$$

Con,

$$\begin{aligned} | \overrightarrow{d_{(\delta)[VP]}} | &\in [\, 0 \,,\, \Lambda \,] \\ | \overrightarrow{OP} | &\in [\, 0 \,,\, r \,] \end{aligned} \tag{3.8}$$

Ya que se desconoce la posición de V, interesa estudiar la ubicación de V que produzca el máximo refinamiento de la región R. Para tener un refinamiento por arriba máximo para alguna ubicación de V se requiere que el término izquierdo de la ecuación 3.7 sea mínimo, la frontera exterior de C se encuentre lo más cerca de V que sea posible y más cerca que alguna parte de la frontera de la región R. Es decir, $\overrightarrow{OP}$ debe tener la dirección opuesta a la dirección de $\overrightarrow{VO}$ y de $\overrightarrow{VP}$, los vectores deben estar en el mismo eje. Remplazando estas condiciones en la ecuación 3.7 se tiene la ecuación 3.9.

$$| \overrightarrow{VO} | - | \overrightarrow{OP} | + | \overrightarrow{d_{(\delta)[VP]}} | < | \overrightarrow{VO} | + | \overrightarrow{r_{[VO]}} | \tag{3.9}$$

La "recta crítica" de esta ecuación para las incógnitas $|\overrightarrow{OP}|$ y $|\overrightarrow{d_{(\delta)[VP]}}|$ es representada en la Figura 3.5. En esta, el valor de $|\overrightarrow{OP}|$ está limitado al intervalo $[-r, r]$, donde el signo negativo significa una dirección inversa al vector, y el valor de $|\overrightarrow{d_{(\delta)[VP]}}|$ es mayor que cero. La "recta crítica" divide el plano en dos áreas, la zona achurada es la combinación de valores que no permiten el refinamiento de la región R y la zona de color es la combinación de valores que permiten el refinamiento de esta región para alguna posición de V.

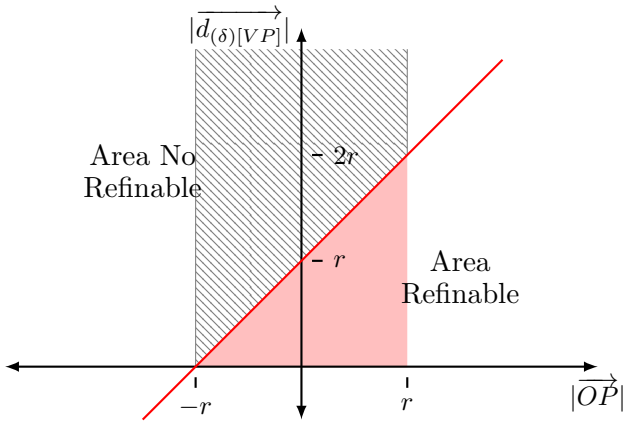


Figura 3.5: Curva crítica de la desigualdad para determinar el máximo refinamiento por arriba. Procedimiento con retardo en intervalo [0 , Λ].

Refinamiento por abajo

El refinamiento por abajo ocurre bajo la frontera interior de la corona circular. Es decir, cuando alguna parte de la frontera de la región R se encuentra más cercana de V que la frontera interior de la región C. Luego, ocurrirá un refinamiento por abajo de la región R si se cumple la siguiente desigualdad de distancias, ecuación 3.10, con referencia a la Figura 3.4.b.

$$| \overrightarrow{VO} + \overrightarrow{OP} + \overrightarrow{d_{(\delta)[VP]}} - \overrightarrow{d_{(\Lambda)[VP]}} | > | \overrightarrow{VO} - \overrightarrow{r_{[VO]}} | \tag{3.10}$$

Con,

$$\begin{aligned} | \overrightarrow{d_{(\delta)[VP]}} | &\in [\ 0\ ,\ \overrightarrow{d_{(\Lambda)[VP]}}\ ] \\ | \overrightarrow{OP} | &\in [\ 0\ ,\ r\ ] \end{aligned} \tag{3.11}$$

Ya que se desconoce la posición de V, interesa estudiar la ubicación de V que produzca el máximo refinamiento de la región R. Para tener un refinamiento por abajo máximo para alguna ubicación de V se requiere que el término izquierdo de la ecuación 3.10 sea máximo, la frontera interior de C se encuentre lo más lejos de V que sea posible y más lejos que alguna parte de la frontera de la región R. Es decir, $\overrightarrow{OP}$ debe tener la misma dirección que la dirección de $\overrightarrow{VO}$ y de $\overrightarrow{VP}$, los vectores deben estar en el mismo eje. Remplazando estas condiciones en la ecuación 3.10 se tiene la ecuación 3.12.

$$| \overrightarrow{VO} | + | \overrightarrow{OP} | + | \overrightarrow{d_{(\delta)[VP]}} | - | \overrightarrow{d_{(\Lambda)[VP]}} | > | \overrightarrow{VO} | - | \overrightarrow{r_{[VO]}} | \tag{3.12}$$

La "recta crítica" de esta ecuación para las incógnitas $|\overrightarrow{OP}|$ y $|\overrightarrow{d_{(\delta)[VP]}}|$ es representada en la Figura 3.6. En esta, el valor de $|\overrightarrow{OP}|$ está limitado al intervalo $[-r, r]$, donde el signo negativo significa una dirección inversa al vector, y el valor de $|\overrightarrow{d_{(\delta)[VP]}}|$ es mayor que cero y menor que Λ. La "recta crítica" divide el plano en dos áreas, la zona achurada es la combinación de valores que no permiten el refinamiento de la región R y la zona de color es la combinación de valores que permiten el refinamiento de esta región para alguna posición de V.

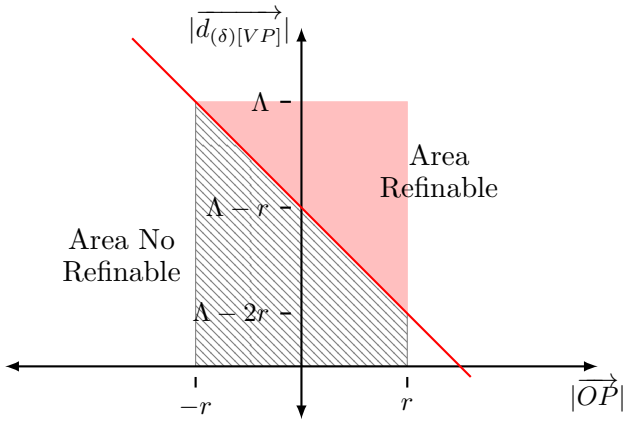


Figura 3.6: Curva crítica de la desigualdad para determinar el máximo refinamiento por abajo. Procedimiento con retardo en intervalo [0 , Λ].

Intervalos de Refinamiento

La combinación de las condiciones de refinamiento, para las incógnitas $|\overrightarrow{OP}|$ y $|\overrightarrow{d_{(\delta)[VP]}}|$, estudiadas anteriormente se resumen en la Figura 3.7.

Del análisis para la obtención de la Figura 3.7 se concluye que la elección de un retardo δ dentro de un intervalo conocido, $[0, \Lambda]$, conlleva múltiples posibilidades sobre el refinamiento de la región R. Estas son:

(a) Si el retardo cumple con $\delta \leq t_{(2r)}$, existe posibilidad de refinamiento por arriba.

(b) Si el retardo cumple con $\delta > t_{(2r)}$ y $\delta < \Lambda - t_{(2r)}$, no habrá refinamiento posible.

(c) Si el retardo cumple con $\delta \geq \Lambda - t_{(2r)}$, existe posibilidad de refinamiento por abajo.

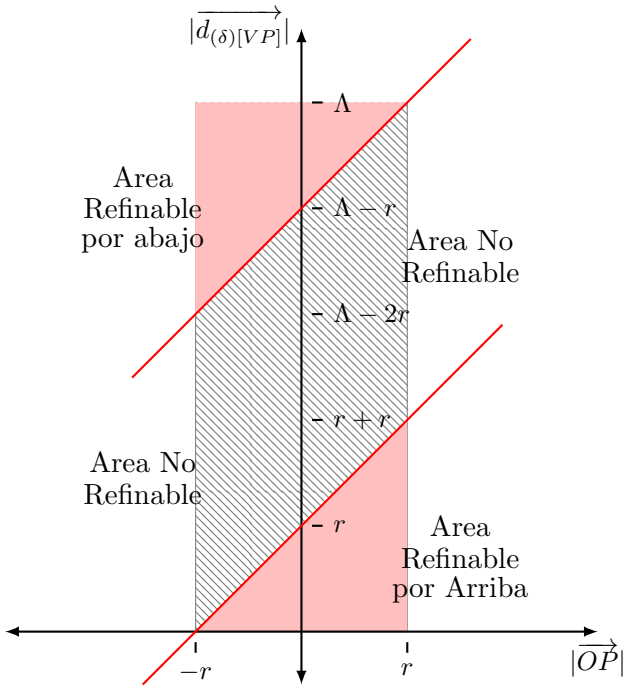


Figura 3.7: Combinación de curvas críticas de desigualdades para determinar el máximo refinamiento por arriba y abajo. Procedimiento con retardo en intervalo [0 , Λ].

Por lo cual, para un valor de $\Lambda \leq t_{(4r)}$ siempre existirá la posibilidad de refinamiento de la región R. Y para $\Lambda > t_{(4r)}$ existirá un intervalo interior de valores para δ en los cuales no habrá refinamiento posible, Figura 3.8.

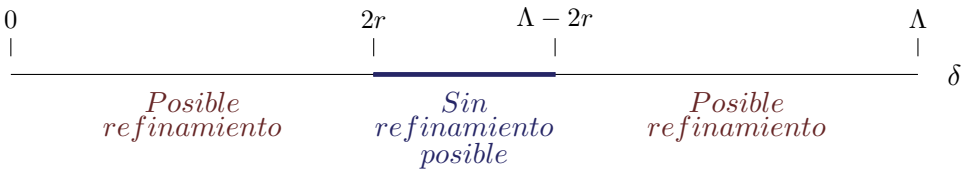


Figura 3.8: Intervalo genérico de valores posible para retardo Λ, con intervalo de valores con los cuales no habrá refinamiento de R.

Procedimiento frente al ataque ABED

Con referencia a la Figura 3.3, la participación de P en el procedimiento de verificación de distancia con el ataque ABED incrementado con δ dentro del intervalo $[0, \Lambda]$, se describe a continuación:

(a) El usuario P determina la región de encubrimiento R, enviándole a un tercero confiable los requerimientos para la creación de la región y espera su respuesta.

(b) Al recibir la región R, P determina el nivel de refinamiento τ y el retardo δ aleatoriamente dentro del intervalo $[0, \Lambda]$.

(c) P determina; con R, τ y δ; el nivel de refinamiento máximo posible de su región R para decidir si continua con el protocolo DBP.

(d) P entrega la región R a V. Y espera los desafíos del intercambio rápido de bits.

(e) Al recibir un desafío de V, P retarda su respuesta un tiempo δ.

Con referencia a la Figura 3.3, la participación de V en el procedimiento de verificación de distancia con el ataque ABED incrementado con δ dentro del intervalo $[0, \Lambda]$, se describe a continuación:

(a) V recibe la región R de P.

(b) V determina si la región R esta dentro de la cota práctica de la distancia. Para saber si continua con el protocolo DBP.

(c) Si la cota práctica de la distancia es satisfecha, V comienza el intercambio rápido de bits. Si la cota práctica de la distancia no es satisfecha, se lo comunica a P y termina el procedimiento.

(d) Al recibir la respuesta de P a su desafío, V determina la distancia $\widetilde{d}_{VP}$ con el tiempo medido t_m.

(e) Con $\widetilde{d}_{VP}$, V determina la distancia $\widetilde{d}_{VPmax} = \widetilde{d}_{VP}$, la que corresponde al radio externo de la corona circular, frontera exterior de la región C.

(f) Con $\widetilde{d}_{VP}$ y el retardo Λ, V determina la distancia $\widetilde{d}_{VPmin} = \widetilde{d}_{VP} - d_{(\Lambda)}$, la que corresponde al radio interno de la corona circular, frontera interior de la región C.

(g) Con las regiones R y C, V determina la región R_F en la cual se podría encontrar P. $R_F = C \cap R$.

(h) Con los cálculos anteriores V verifica si P se encuentra en el interior de R.

Análisis del estudio de la solución

Para este procedimiento se obtienen mejores niveles de protección de la privacidad de ubicación para valores altos de Λ. El intervalo de retardos donde no es posible el refinamiento es mayor mientras mayor sea el valor de Λ.

Considerando la cota práctica requerida por V que limita la región R, no es deseable un valor de Λ muy distinto del diámetro de la región R, lo que implica entrar a una zona donde existe la posibilidad de refinamiento para todo retardo δ posible. Como ya se mencionó, esta es una situación no deseada para un protocolo delimitador de distancia consciente de la ubicación, DBPALP.

Si se considera la elección de retardos cercanos a "0", esta selección conlleva a un refinamiento por arriba y a un incremento del nivel de refinamiento posible, incluso a la determinación precisa de la ubicación en un caso extremo, ya que un retardo inferior a la distancia máxima de P a la frontera de R no protege a R, completamente, en toda posible ubicación de V.

3.3. Dos Regiones de Encubrimiento con Retardo seleccionado en Base a la Máxima Distancia

Para enfrentar las debilidades de la solución anterior, SBIR, se desea disponer de un intervalo de retardos que entregue mayor incertidumbre sobre los límites posibles del retardo δ, respetando lo más posible el concepto de la cota práctica. Para esto se consideran dos regiones de encubrimiento; una región pública que determina el límite superior de los retardos posible y otra región privada que determina el retardo δ como la distancia máxima entre el usuario P y la frontera de la región.

Más específicamente, en la Solución en Base a un retardo igual a la Máxima Distancia con Dos Regiones de Encubrimiento (SBMDcDRE) el usuario P considera la existencia de dos regiones de encubrimiento, una región pública R_{pub} y otra región privada R_{priv}. La región R_{priv} cumplirá con los requisitos de privacidad de ubicación requeridos por P, estará contenida íntegramente en la región R_{pub} y no se dará a conocer al usuario V. La región R_{pub} será la región de encubrimiento entregada a V para la ejecución del protocolo DBP. Además, en el procedimiento P retarda su respuesta al desafío de V un tiempo δ equivalente a la distancia máxima entre el usuario P y la frontera de la región R_{priv}.

Dado que el retardo mínimo posible es cero, $\delta = 0$, cuando P decide no tener una región R_{priv}, no se puede restar el radio de R_{pub}, o un retardo mínimo, para determinar la frontera exterior de la región C. Además, como el retardo δ es la distancia máxima entre el usuario P y la frontera de la región R_{priv}, se asegura cubrir con el retardo toda la región R_{priv} para cualquier posición de V.

El ataque ABED que considera un retardo δ igual a la distancia máxima entre el usuario P y la frontera de la región R_{priv} como parte adicional del ataque, genera una región C, corona circular, en la cual se debe encontrar P.

La intersección de esta región C con la región de encubrimiento R_{pub} determina un área de R_{pub} en la cual se encuentra P, esta área es la región de encubrimiento refinada R_{Fpub}. Y la intersección de esta región C con la región de encubrimiento R_{priv} determina un área de R_{priv} en la cual se encuentra P, esta área es la región de encubrimiento refinada R_{Fpriv}.

El usuario V conocerá la región R_{Fpub} y desconocerá la región R_{Fpriv}. Es decir, V desconocerá si ha refinado le región de encubrimiento privada de P, R_{priv}.

Para determinar si es posible un refinamiento de las regiones de encubrimiento se requieren las fronteras de la corona circular C, el radio externo $r_{ce} = \widetilde{d}_{VPmax}$ y el radio interno $r_{ci} = \widetilde{d}_{VPmin}$.

Fronteras de la Corona Circular

Las fronteras de la corona circular C quedan definidas por sus radios, las ecuaciones vectoriales que definen estos son presentadas en las ecuaciones 3.13 y 3.14, con referencia a las Figuras 3.9 y 3.10.

Para la frontera exterior de la región C.

$$r_{ce} = \widetilde{d}_{VPmax} = | \overrightarrow{VO_{priv}} + \overrightarrow{O_{priv}P} + \overrightarrow{d_{(\delta)[VP]}} | \tag{3.13}$$

Para la frontera interior de la región C.

$$r_{ci} = \widetilde{d}_{VPmin} = | \overrightarrow{VO_{priv}} + \overrightarrow{O_{priv}P} + \overrightarrow{d_{(\delta)[VP]}} - 2\,\overrightarrow{r_{pub[VP]}} | \tag{3.14}$$

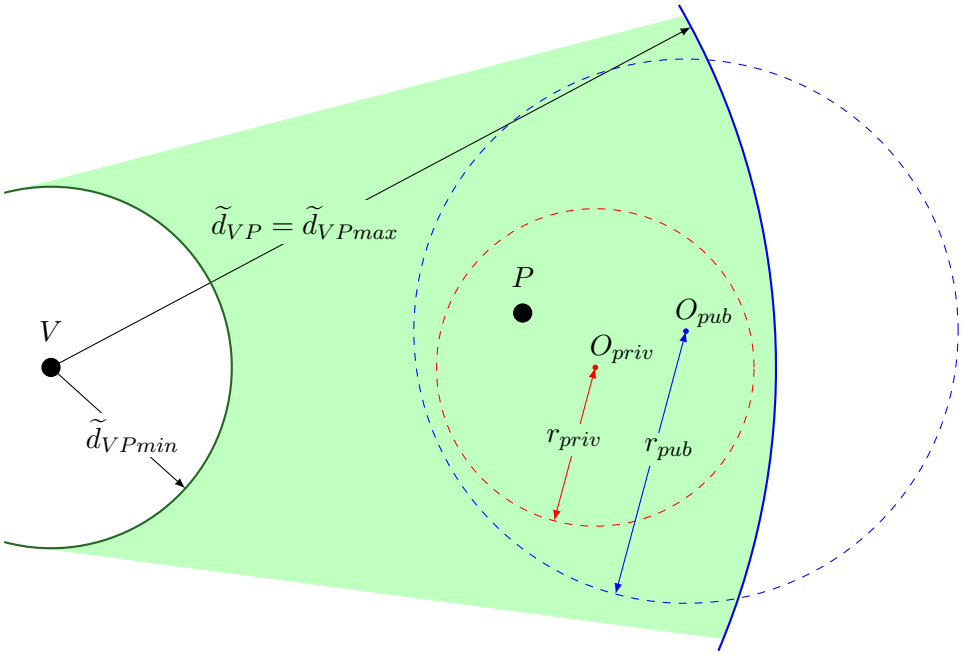


Figura 3.9: Corona circular y sus fronteras, para el procedimiento con dos regiones de encubrimiento con retardo $\delta = t_{(d_{maxpriv})}$.

Donde, $\overrightarrow{VO_{priv}}$ es el vector de la distancia entre V y O_{priv}, $\overrightarrow{O_{priv}P}$ es el vector de la distancia entre O_{priv} y P, $\overrightarrow{d_{(\delta)[VP]}}$ es el vector de la distancia que recorre la señal electromagnética en el tiempo δ con la dirección del vector de la distancia entre V y P, y $\overrightarrow{r_{pub[VP]}}$ es el vector del radio r_{pub} de la región de encubrimiento pública con la dirección del vector de la distancia entre V y P. Estos se pueden observar en la Figura 3.10.

Las ecuaciones 3.13 y 3.14 junto con las fronteras de las regiones R_{priv} y R_{pub} permiten determinar el refinamiento sobre estas regiones.

Refinamiento por arriba

El refinamiento por arriba ocurre sobre la frontera exterior de la corona circular. Luego, ocurrirá un refinamiento por arriba de la región R_{priv} si se cumple la siguiente desigualdad de distancias, ecuación 3.15 con referencia a la Figura 3.10.a, la cual relaciona la fronteras exterior de C con la frontera de R_{priv}.

$$| \overrightarrow{VO_{priv}} + \overrightarrow{O_{priv}P} + \overrightarrow{d_{(\delta)[VP]}} | < | \overrightarrow{VO_{priv}} + \overrightarrow{r_{priv[VO_{priv}]}} | \tag{3.15}$$

Con,

$$\begin{aligned} d_{maxpriv} &= | \overrightarrow{O_{priv}P} + \overrightarrow{r_{priv[O_{priv}P]}} | \\ | \overrightarrow{d_{(\delta)[VP]}} | &= d_{maxpriv} \\ | \overrightarrow{O_{priv}P} | &\in [\ 0\ ,\ r_{priv}\ ] \\ d_{maxpriv} &\in [\ r_{priv}\ ,\ 2r_{priv}\ ] \end{aligned} \tag{3.16}$$

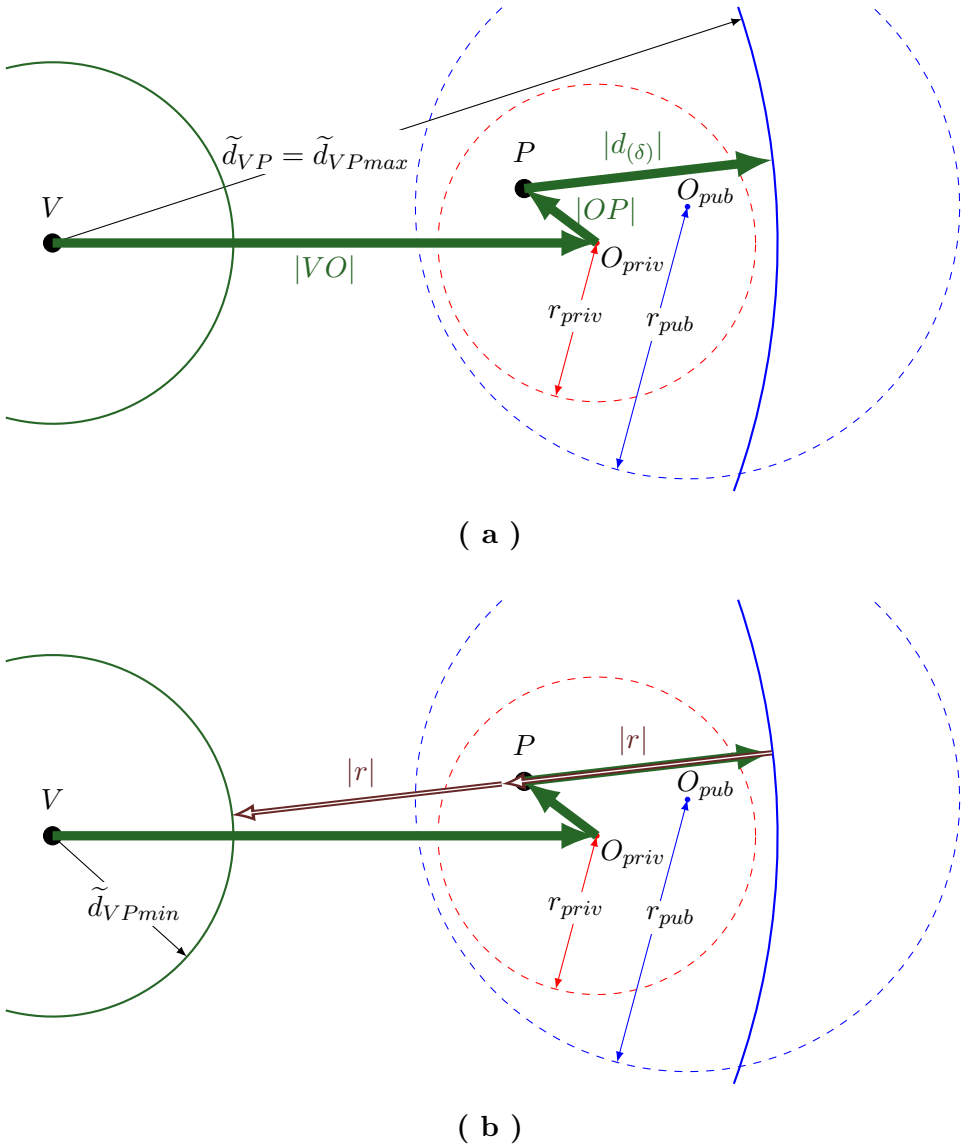


Figura 3.10: Vectores que determinan las fronteras de la corona circular. (a) frontera exterior y (b) frontera interior. Dos regiones de encubrimiento con retardo $\delta = t_{(d_{maxpriv})}$.

Ya que se desconoce la posición de V, interesa estudiar la ubicación de V que produzca el máximo refinamiento de la región R. Para tener un refinamiento por arriba máximo para alguna ubicación de V se requiere que el término izquierdo de la ecuación 3.15 sea mínimo, la frontera exterior de C se encuentre más cerca de V que alguna parte de la frontera de R_{priv}. Es decir, si δ equivale a una distancia $d_{maxpriv}$ y $\overrightarrow{O_{priv}P}$ tiene la dirección opuesta a la dirección de $\overrightarrow{VO_{priv}}$ y a la de $\overrightarrow{VP}$, los vectores deben estar en el mismo eje. Bajo estas condiciones,

$$\begin{aligned} \overrightarrow{d_{(\delta)[VP]}} &= -\overrightarrow{O_{priv}P} + \overrightarrow{r_{priv[VP]}} \\ &= -\overrightarrow{O_{priv}P} + \overrightarrow{r_{priv[VO_{priv}]}} \end{aligned} \tag{3.17}$$

Remplazando las ecuaciones 3.17 en la ecuación 3.15 y simplificando $\overrightarrow{O_{priv}P}$, se tiene la ecuación 3.18.

$$| \overrightarrow{VO_{priv}} + \overrightarrow{r_{priv[VO_{priv}]}} | < | \overrightarrow{VO_{priv}} + \overrightarrow{r_{priv[VO_{priv}]}} | \tag{3.18}$$

La desigualdad de la ecuación 3.18 nunca se cumplirá. Por lo cual, no hay posibilidad que exista refinamiento por arriba de la región R_{priv} para cualquier condición de los usuarios V y P, de las regiones R_{priv} y R_{pub}, y del retardo $\delta = t_{(d_{maxpriv})}$.

Refinamiento por abajo

El refinamiento por abajo ocurre bajo la frontera interior de la corona circular. Luego, ocurrirá un refinamiento por abajo de la región R_{priv} si se cumple la siguiente desigualdad de distancias, ecuación 3.19 con referencia a la Figura 3.10.b, la cual relaciona la frontera interna de C con la frontera de R_{priv}.

$$| \overrightarrow{VO_{priv}} + \overrightarrow{O_{priv}P} + \overrightarrow{d_{(\delta)[VP]}} - 2\,\overrightarrow{r_{pub[VP]}} | > | \overrightarrow{VO_{priv}} - \overrightarrow{r_{priv[VO_{priv}]}} | \tag{3.19}$$

Con,

$$\begin{aligned} d_{maxpriv} &= | \overrightarrow{O_{priv}P} + \overrightarrow{r_{priv[O_{priv}P]}} | \\ | \overrightarrow{d_{(\delta)[VP]}} | &= d_{maxpriv} \\ | \overrightarrow{O_{priv}P} | &\in [\ 0\ ,\ r_{priv}\ ] \\ d_{maxpriv} &\in [\ r_{priv}\ ,\ 2r_{priv}\ ] \\ r_{priv} &\in [\ 0\ ,\ r_{pub}\ ] \end{aligned} \tag{3.20}$$

Ya que se desconoce la posición de V, interesa estudiar la ubicación de V que produzca el máximo refinamiento de la región R_{priv}. Para tener un refinamiento por abajo máximo para alguna ubicación de V se requiere que el término izquierdo de la ecuación 3.19 sea máximo, la frontera interior de C se encuentra más lejos de V que alguna parte de la frontera de R_{priv}. Es decir, $\overrightarrow{O_{priv}P}$ debe tener la misma dirección que la dirección de $\overrightarrow{VO_{priv}}$ y de $\overrightarrow{VP}$, los vectores deben estar en el mismo eje. Reemplazando estas condiciones en la ecuación 3.19 se tiene la ecuación 3.21.

$$| \overrightarrow{VO_{priv}} | + | \overrightarrow{O_{priv}P} | + | \overrightarrow{d_{(\delta)[VP]}} | - | 2\,\overrightarrow{r_{pub[VP]}} | > | \overrightarrow{VO_{priv}} | - | \overrightarrow{r_{priv[VO_{priv}]}} | \tag{3.21}$$

La "recta crítica" de esta ecuación para las incógnitas $|\overrightarrow{O_{priv}P}|$ y $|\overrightarrow{d_{(\delta)[VP]}}|$ es representada en la Figura 3.11. En esta, el valor de $|\overrightarrow{O_{priv}P}|$ está limitado al intervalo $[-r_{priv}, r_{priv}]$, donde el signo negativo significa una dirección inversa al vector, y el valor de $|\overrightarrow{d_{(\delta)[VP]}}|$ al intervalo $[\ d_{maxpriv}\ ,\ 2r_{priv}\ ]$. La "recta crítica" divide el plano en dos áreas, la zona achurada es la

combinación de valores que no permiten el refinamiento de la región R_{priv} y la zona de color es la combinación de valores que permiten el refinamiento de esta región para alguna posición de V.

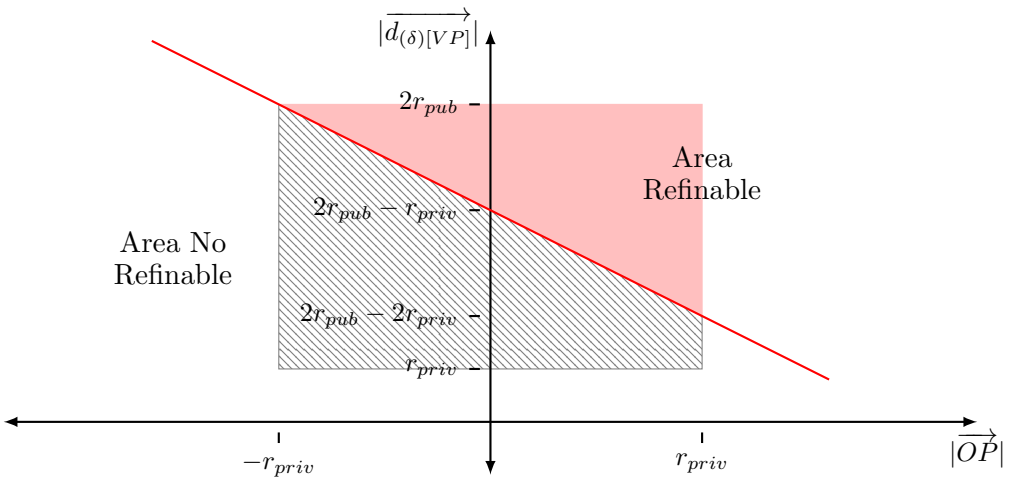


Figura 3.11: Curva crítica de la desigualdad para determinar refinamiento por abajo. Dos regiones de encubrimiento con intervalo de retardo $\delta = t_{(d_{maxpriv})}$.

Se evalúan los "puntos críticos" de la desigualdad de la ecuación 3.21 para los mínimos y máximos de $|\overrightarrow{O_{priv}P}|$ y $|\overrightarrow{d_{(\delta)[VP]}}|$.

Para el mín($|\overrightarrow{O_{priv}P}|$) $= 0 \longrightarrow$ mín($|\overrightarrow{d_{(\delta)[VP]}}|$) $= r_{priv}$;

$$r_{pub} = r_{priv}$$

Para el máx($|\overrightarrow{O_{priv}P}|$) $= r_{priv} \longrightarrow$ máx($|\overrightarrow{d_{(\delta)[VP]}}|$) $= 2r_{priv}$;

$$r_{pub} = 2\, r_{priv}$$

Luego, para la desigualdad de la ecuación 3.19 se tienen las siguientes condiciones que relacionan los radios r_{priv} y r_{pub};

$$\begin{aligned} r_{pub} &< r_{priv} && \text{; Este caso no puede ocurrir.} \\ r_{pub} &> 2r_{priv} && \text{; No habrá refinamiento.} \\ r_{priv} &< r_{pub} < 2r_{priv} && \text{; Hay posibilidad que exista refinamiento.} \end{aligned}$$

Para tener un refinamiento por abajo máximo, considerando el intervalo en la cual existe la posibilidad de refinamiento ($r_{priv} < r_{pub} < 2r_{priv}$) y con relación a la ecuación 3.19 y la Figura 3.10, se requiere que $\overrightarrow{VO_{priv}}$ y $\overrightarrow{O_{priv}P}$ tengan la misma dirección y la frontera interior de la corona circular sea una recta y no una circunferencia (V se encuentre a una distancia infinita de O_{priv}). Esta situación se puede observar en la Figura 3.12, donde la zona de color es el área de la región R_{pub} en la cual V determina que P no se puede encontrar.

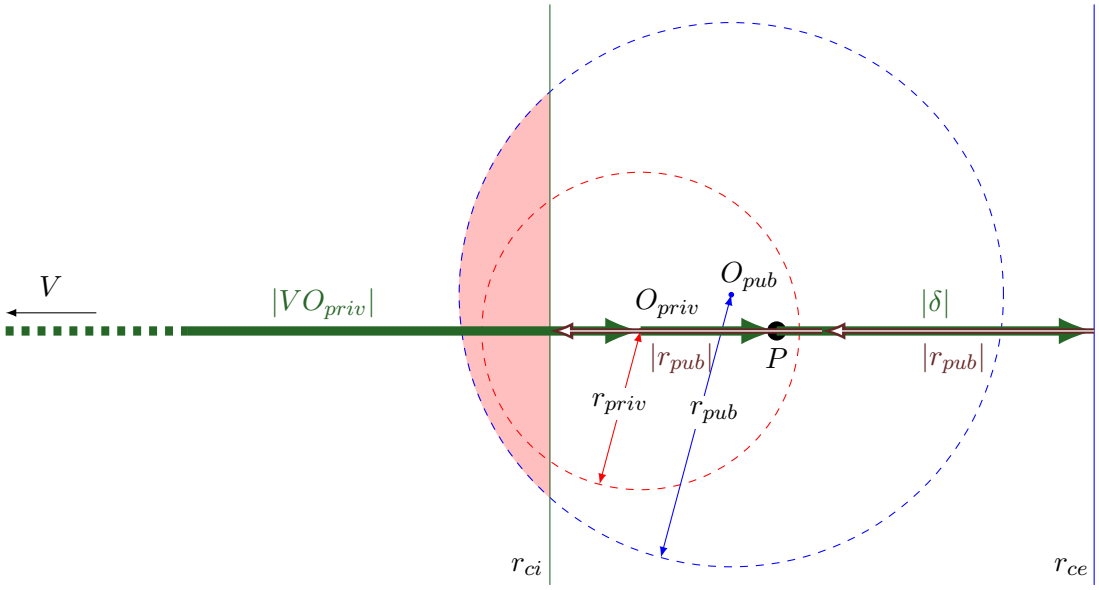


Figura 3.12: Condición para máximo refinamiento por abajo con ataque ABED. Dos regiones de encubrimiento con intervalo de retardo $\delta = t_{(d_{maxpriv})}$.

Refinamiento adicional

Al seleccionar un retardo de forma determinística, retardo $\delta = t_{(d_{max})}$, se le entrega al usuario V información adicional que se puede utilizar para realizar un nuevo nivel de refinamiento.

El nuevo nivel de refinamiento nace del hecho de seleccionar un retardo equivalente a d_{max}. En este, el usuario V se pregunta si los puntos de la región R_{Fpub}, en los que se ha determinado que el usuario P se puede encontrar, permiten un retardo a la frontera exterior de C.

Lo anterior se puede observar en la Figura 3.13, donde se estudia el caso para el eje que atraviesa V y O_{pub}; es claro que para poder producir un retardo que llegue al punto $P2$, el usuario P se debe encontrar más cerca de $P2$ que el punto medio entre $P2$ y $P1$, $P3$. Esto debido a que R_{priv} no puede ser mayor que R_{pub}.

Con este ataque se determina que los puntos entre la línea continua gruesa, en la Figura 3.13, y la región en color no pueden contener a P.

Procedimiento frente al ataque ABED

La participación de P en el procedimiento de verificación de distancia con el ataque ABED incrementado con; dos regiones de encubrimiento y $\delta = t_{(d_{maxpriv})}$; se describe a continuación:

(a) El usuario P determina las regiones de encubrimiento R_{priv} y R_{pub}, enviándole a un tercero confiable los requerimientos para la creación de las regiones y espera su respuesta.

(b) Al recibir las regiones R_{priv} y R_{pub}, P determina el nivel de refinamiento τ y el retardo $\delta = t_{(d_{maxpriv})}$.

(c) P determina; con R_{pub}, R_{priv}, τ y δ ; el nivel de refinamiento máximo posible de su región R para decidir si continua con el protocolo DBP.

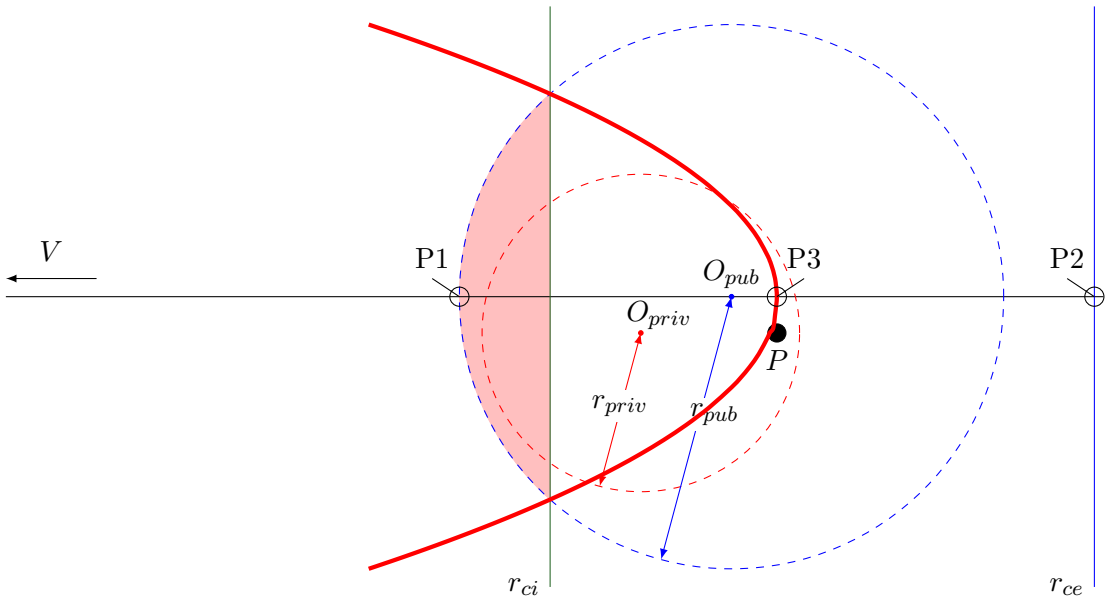


Figura 3.13: Segundo nivel de refinamiento para condición para máximo refinamiento por abajo. Dos regiones de encubrimiento con intervalo de retardo $\delta = t_{(d_{maxpriv})}$.

(d) P entrega la región R_{pub} a V. Y espera los desafíos del intercambio rápido de bits.

(e) Al recibir un desafío de V, P retarda su respuesta un tiempo δ.

La participación de V en el procedimiento de verificación de distancia con el ataque ABED incrementado con; dos regiones de encubrimiento y $\delta = t_{(d_{maxpriv})}$; se describe a continuación:

(a) V recibe la región R_{pub} de P.

(b) V determina si la región R_{pub} esta dentro de la cota práctica de la distancia. Para saber si continua con el protocolo DBP.

(c) Si la cota práctica de la distancia es satisfecha, V comienza el intercambio rápido de bits. Si la cota práctica de la distancia no es satisfecha, se lo comunica a P y termina el procedimiento.

(d) Al recibir la respuesta de P a su desafío, V determina la distancia $\widetilde{d}_{VP}$ con el tiempo medido t_m.

(e) Con $\widetilde{d}_{VP}$, V determina la distancia $\widetilde{d}_{VPmax} = \widetilde{d}_{VP}$, la que corresponde al radio externo de la corona circular, frontera exterior de la región C.

(f) Con $\widetilde{d}_{VP}$ y el radio r_{pub}, V determina la distancia $\widetilde{d}_{VPmin} = \widetilde{d}_{VP} - 2r_{pub}$, la que corresponde al radio interno de la corona circular, frontera interior de la región C.

(g) Con las regiones R_{pub} y C, V determina la región R_{Fpub} en la cual se podría encontrar P. $R_{Fpub} = C \cap R_{pub}$.

(h) Con las regiones R_{Fpub} y C, V determina los puntos de R_{Fpub} que no pueden tener un retardo que alcance la frontera exterior de C y los utiliza para refinar R_{Fpub}.

(i) Con los cálculos anteriores V verifica si P se encuentra en el interior de R_{pub}.

Análisis del estudio de la solución

Para este procedimiento se logra eliminar el refinamiento por arriba, obteniéndose un buen beneficio en comparación con los procedimientos anteriores. Pero, la existencia de información disponible para V en la metodología de selección del retardo δ proporciona un refinamiento adicional al refinamiento por abajo, esta solución muestra ser bastante perjudicial en el incremento del área refinada de R_{priv} para P.

3.4. Dos Regiones de Encubrimiento con Retardo sobre un Intervalo de Retardos Posibles

Para enfrentar las debilidades de las soluciones anteriores se desea la mayor incertidumbre en el intervalo de valores posibles para el retardo δ y no se desea entregar información sobre la forma de seleccionar el retardo. La selección del retardo no debe ser determinística y los límites de la selección deben ser desconocidos para V.

Para cumplir con lo anterior, en la Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento (SBIRcDRE) los límites del intervalo se escogen en función de la región de encubrimiento privada R_{priv}, considerando como restricción superior la región de encubrimiento pública R_{pub} debido a la cota práctica requerida por el usuario V.

En este procedimiento el usuario P considera la existencia de dos regiones de encubrimiento, una región pública R_{pub} y otra región privada R_{priv}. La región R_{priv} cumplirá con los requisitos de privacidad de ubicación requeridos por P, estará contenida íntegramente en la región R_{pub} y no se dará a conocer al usuario V. La región R_{pub} será la región de encubrimiento entregada a V para la ejecución del protocolo DBP y cumplirá con unos requisitos relajados de privacidad de ubicación comparados con los requeridos por P para la región R_{priv}. Además, en el procedimiento P retarda su respuesta al desafío de V un tiempo δ aleatorio seleccionado dentro de un intervalo de tiempos obtenidos del intervalo equivalente de distancias $[d_{maxpriv}, 2r_{priv}]$. Es decir, del intervalo expresado en la ecuación 3.22.

$$[\ d_{maxpriv}\ ,\ 2r_{priv}\ ] \quad \longrightarrow \quad \delta\ \in\ [\ t_{(d_{maxpriv})}\ ,\ t_{(2r_{priv})}\ ] \tag{3.22}$$

El ataque ABED que considera un retardo $\delta\ \in\ [\ t_{(d_{maxpriv})}\ ,\ t_{(2r_{priv})}\ ]$ como parte adicional del ataque, genera una región C, corona circular, en la cual se debe encontrar P.

La intersección de esta región C con la región de encubrimiento R_{pub} determina un área de R_{pub} en la cual se encuentra P, R_{Fpub}. Y la intersección de esta región C con la región de encubrimiento R_{priv} determina un área de R_{priv} en la cual se encuentra P, R_{Fpriv}.

El usuario V conocerá la región R_{Fpub} y desconocerá la región R_{Fpriv}. Es decir, V desconocerá si ha refinado la región de encubrimiento privada de P, R_{priv}.

Para determinar si es posible un refinamiento de las regiones de encubrimiento se requieren las fronteras de la corona circular C, el radio externo $r_{ce} = \widetilde{d}_{VPmax}$ y el radio interno $r_{ci} = \widetilde{d}_{VPmin}$.

Fronteras de la Corona Circular

Las fronteras de la corona circular C quedan definidas por sus radios, las ecuaciones vectoriales que definen estos son presentadas en las ecuaciones 3.23 y 3.24, con referencia a las Figuras 3.14 y 3.15.

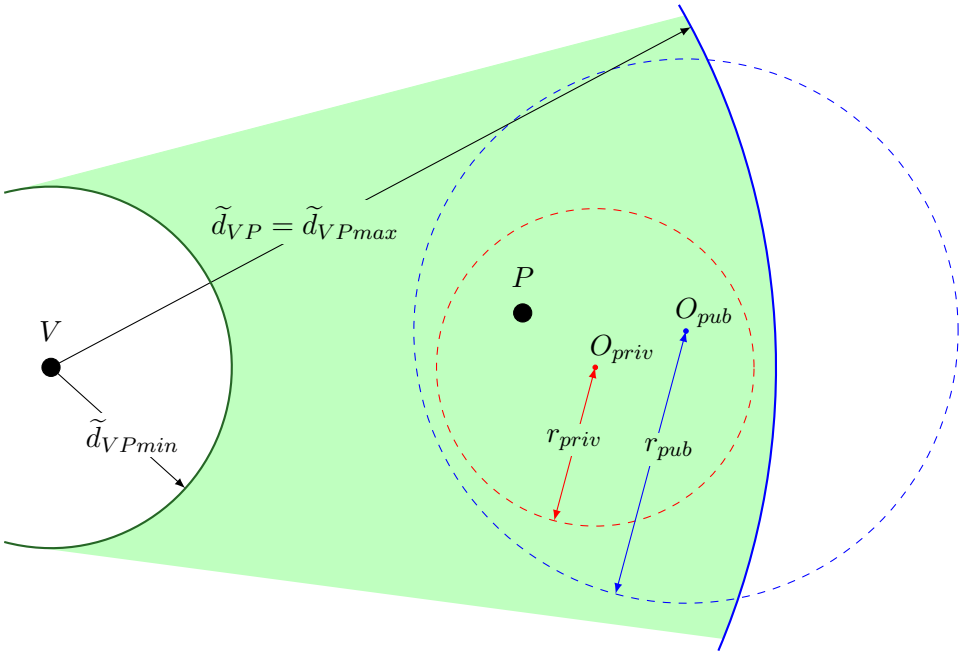


Figura 3.14: Corona circular y sus fronteras, para el procedimiento propuesto. Dos regiones de encubrimiento con intervalo de retardo, $\delta \in [\, t_{(d_{maxpriv})} \,,\, t_{(2r_{priv})} \,]$.

Para la frontera exterior de la región C.

$$r_{ce} = \widetilde{d}_{VPmax} = | \overrightarrow{VO_{priv}} + \overrightarrow{O_{priv}P} + \overrightarrow{d_{(\delta)[VP]}} | \tag{3.23}$$

Para la frontera interior de la región C.

$$r_{ci} = \widetilde{d}_{VPmin} = | \overrightarrow{VO_{priv}} + \overrightarrow{O_{priv}P} + \overrightarrow{d_{(\delta)[VP]}} - 2\, \overrightarrow{r_{pub[VP]}} | \tag{3.24}$$

Donde, $\overrightarrow{VO_{priv}}$ es el vector de la distancia entre V y O_{priv}, $\overrightarrow{O_{priv}P}$ es el vector de la distancia entre O_{priv} y P, $\overrightarrow{d_{(\delta)[VP]}}$ es el vector de la distancia que recorre la señal electromagnética en el tiempo δ con la dirección del vector de la distancia entre V y P, y $\overrightarrow{r_{pub[VP]}}$ es el vector del radio r_{pub} de la región de encubrimiento pública con la dirección del vector de la distancia entre V y P. Estos se pueden observar en la Figura 3.15.

Las ecuaciones 3.23 y 3.24 junto con las fronteras de las regiones R_{priv} y R_{pub} permiten determinar el refinamiento sobre estas regiones.

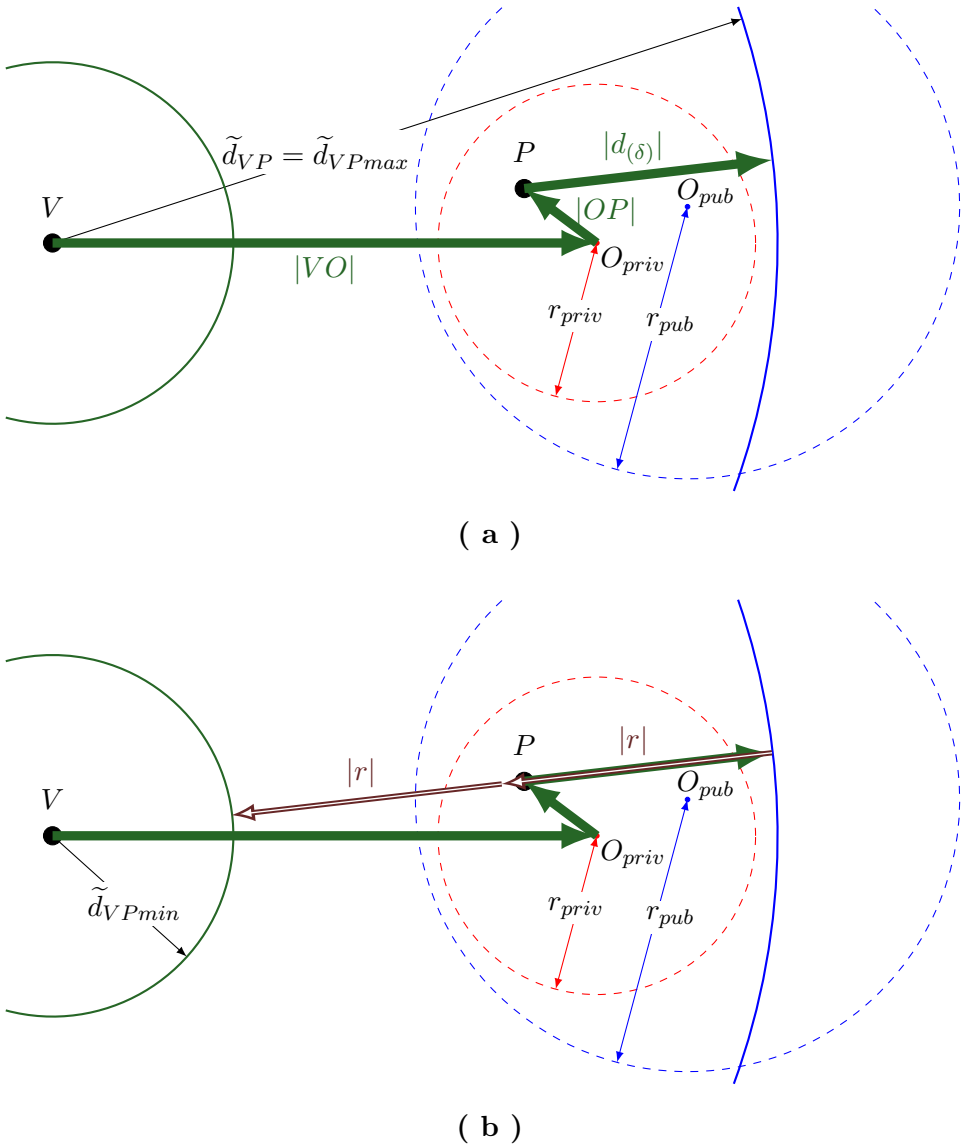


Figura 3.15: Vectores que determinan las fronteras de la corona circular. (a) frontera exterior y (b) frontera interior. Dos regiones de encubrimiento con intervalo de retardo, $\delta \in [\, t_{(d_{maxpriv})} \,,\, t_{(2r_{priv})} \,]$.

Refinamiento por arriba

El refinamiento por arriba ocurre sobre la frontera exterior de la corona circular. Luego, ocurrirá un refinamiento por arriba de la región R_{priv} si se cumple la siguiente desigualdad de distancias, ecuación 3.25 con referencia a la Figura 3.15, la cual relaciona la frontera exterior de C con la frontera de R_{priv}.

$$| \overrightarrow{VO_{priv}} + \overrightarrow{O_{priv}P} + \overrightarrow{d_{(\delta)[VP]}} | < | \overrightarrow{VO_{priv}} + \overrightarrow{r_{priv[VO_{priv}]}} | \tag{3.25}$$

Con,

$$\begin{aligned} d_{maxpriv} &= | \overrightarrow{O_{priv}P} + \overrightarrow{r_{priv[O_{priv}P]}} | \\ | \overrightarrow{d_{(\delta)[VP]}} | &\in [\ d_{maxpriv}\ ,\ 2r_{priv}\ ] \\ | \overrightarrow{O_{priv}P} | &\in [\ 0\ ,\ r_{priv}\ ] \\ d_{maxpriv} &\in [\ r_{priv}\ ,\ 2r_{priv}\ ] \end{aligned} \tag{3.26}$$

Ya que se desconoce la posición de V, interesa estudiar la ubicación de V que produzca el máximo refinamiento de la región R. Para tener un refinamiento por arriba máximo para alguna ubicación de V se requiere; un retardo δ mínimo y que el término izquierdo de la ecuación 3.25 sea mínimo, la frontera exterior de C se encuentre más cerca de V que alguna parte de la frontera de R_{priv}. Es decir, si δ equivale a una distancia $d_{maxpriv}$ y $\overrightarrow{O_{priv}P}$ tiene la dirección opuesta a la dirección de $\overrightarrow{VO_{priv}}$ y a la de $\overrightarrow{VP}$, los vectores deben estar en el mismo eje. Bajo estas condiciones,

$$\begin{aligned} \overrightarrow{d_{(\delta)[VP]}} &= -\overrightarrow{O_{priv}P} + \overrightarrow{r_{priv[VP]}} \\ &= -\overrightarrow{O_{priv}P} + \overrightarrow{r_{priv[VO_{priv}]}} \end{aligned} \tag{3.27}$$

Remplazando las ecuaciones 3.27 en la ecuación 3.25 y simplificando $\overrightarrow{O_{priv}P}$, se tiene la ecuación 3.28.

$$| \overrightarrow{VO_{priv}} + \overrightarrow{r_{priv[VO_{priv}]}} | < | \overrightarrow{VO_{priv}} + \overrightarrow{r_{priv[VO_{priv}]}} | \tag{3.28}$$

La desigualdad de la ecuación 3.28 nunca se cumplirá. Por lo cual, no hay posibilidad que exista refinamiento por arriba de la región R_{priv} para cualquier condición de los usuarios V y P, de las regiones R_{priv} y R_{pub}, y del retardo δ dentro de su intervalo $[\ t_{(d_{maxpriv})}\ ,\ t_{(2r_{priv})}\ ]$.

Refinamiento por abajo

El refinamiento por abajo ocurre bajo la frontera interior de la corona circular. Luego, ocurrirá un refinamiento por abajo de la región R_{priv} si se cumple la siguiente desigualdad de distancias, ecuación 3.29 con referencia a la Figura 3.15, la cual relaciona la frontera interior de C con la frontera de R_{priv}.

$$| \overrightarrow{VO_{priv}} + \overrightarrow{O_{priv}P} + \overrightarrow{d_{(\delta)[VP]}} - 2\ \overrightarrow{r_{pub[VP]}} | > | \overrightarrow{VO_{priv}} - \overrightarrow{r_{priv[VO_{priv}]}} | \tag{3.29}$$

Con,

$$\begin{aligned} d_{maxpriv} &= | \overrightarrow{O_{priv}P} + \overrightarrow{r_{priv[O_{priv}P]}} | \\ | \overrightarrow{d_{(\delta)[VP]}} | &\in [\ d_{maxpriv}\ ,\ 2r_{priv}\ ] \\ | \overrightarrow{O_{priv}P} | &\in [\ 0\ ,\ r_{priv}\ ] \\ d_{maxpriv} &\in [\ r_{priv}\ ,\ 2r_{priv}\ ] \\ r_{priv} &\in [\ 0\ ,\ r_{pub}\ ] \end{aligned} \tag{3.30}$$

Ya que se desconoce la posición de V, interesa estudiar la ubicación de V que produzca el

máximo refinamiento de la región R_{priv}. Para tener un refinamiento por abajo máximo para alguna ubicación de V se requiere que el término izquierdo de la ecuación 3.29 sea máximo, la frontera interior de C se encuentre más lejos de V que alguna parte de la frontera de R_{priv}. Es decir, $\overrightarrow{O_{priv}P}$ debe tener la misma dirección que la dirección de $\overrightarrow{VO_{priv}}$ y de $\overrightarrow{VP}$, los vectores deben estar en el mismo eje. Remplazando estas condiciones en la ecuación 3.29 se tiene la ecuación 3.31.

$$| \overrightarrow{VO_{priv}} | + | \overrightarrow{O_{priv}P} | + | \overrightarrow{d_{(\delta)[VP]}} | - | 2\ \overrightarrow{r_{pub[VP]}} | > | \overrightarrow{VO_{priv}} | - | \overrightarrow{r_{priv[VO_{priv}]}} | \quad (3.31)$$

La "recta crítica" de esta ecuación para las incógnitas $|\overrightarrow{O_{priv}P}|$ y $|\overrightarrow{d_{(\delta)[VP]}}|$ es representada en la Figura 3.16. En esta, el valor de $|\overrightarrow{O_{priv}P}|$ está limitado al intervalo $[-r_{priv}, r_{priv}]$, donde el signo negativo significa una dirección inversa al vector, y el valor de $|\overrightarrow{d_{(\delta)[VP]}}|$ al intervalo $[\ d_{maxpriv}\ ,\ 2r_{priv}\ ]$. La "recta crítica" divide el plano en dos áreas, la zona achurada es la combinación de valores que no permiten el refinamiento de la región R_{priv} y la zona de color es la combinación de valores que permiten el refinamiento de esta región para alguna posición de V.

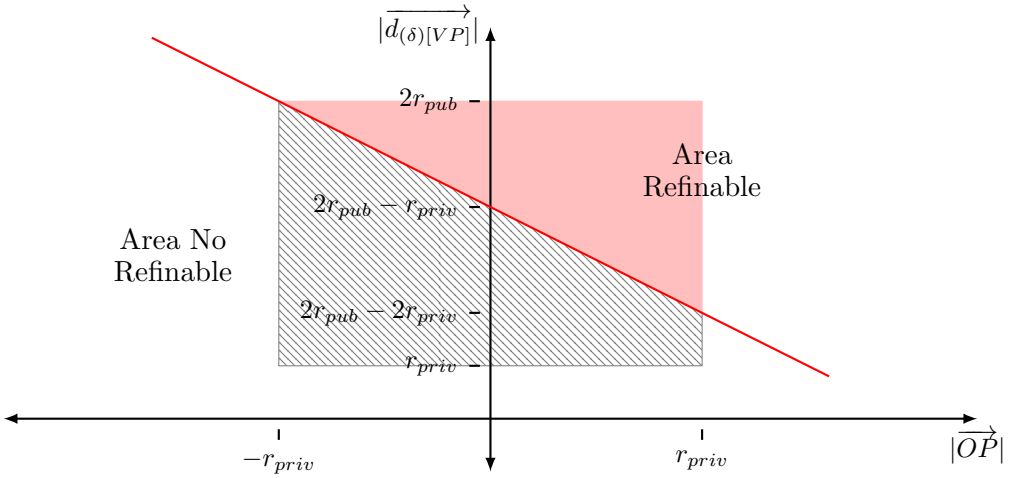


Figura 3.16: Curva crítica de la desigualdad para determinar el máximo refinamiento por abajo. Dos regiones de encubrimiento con intervalo de retardo, $\delta \in [\ t_{(d_{maxpriv})}\ ,\ t_{(2r_{priv})}\ ]$.

Se evalúan los "puntos críticos" de la desigualdad de la ecuación 3.31 para los mínimos y máximos de $|\overrightarrow{O_{priv}P}|$ y $|\overrightarrow{d_{(\delta)[VP]}}|$.

Para el mín($|\overrightarrow{O_{priv}P}|$) $= 0 \longrightarrow$ mín($|\overrightarrow{d_{(\delta)[VP]}}|$) $= r_{priv}$;

$$r_{pub} = r_{priv}$$

Para el máx($|\overrightarrow{O_{priv}P}|$) $= r_{priv} \longrightarrow$ máx($|\overrightarrow{d_{(\delta)[VP]}}|$) $= 2r_{priv}$;

$$r_{pub} = 2\ r_{priv}$$

Luego, para la desigualdad de la ecuación 3.29 se tienen las siguientes condiciones que relacionan los radios r_{priv} y r_{pub};

$$\begin{aligned} r_{pub} &< r_{priv} && \text{; Este caso no puede ocurrir.} \\ r_{pub} &> 2r_{priv} && \text{; No habrá refinamiento.} \\ r_{priv} &< r_{pub} < 2r_{priv} && \text{; Hay posibilidad que exista refinamiento.} \end{aligned}$$

Para tener un refinamiento por abajo máximo, considerando el intervalo en la cual existe la posibilidad de refinamiento ($r_{priv} < r_{pub} < 2r_{priv}$) y con relación a la ecuación 3.29 y la Figura 3.15, se requiere que $\overrightarrow{VO_{priv}}$ y $\overrightarrow{O_{priv}P}$ tengan la misma dirección y la frontera interior de la corona circular sea una recta y no una circunferencia (V se encuentre a una distancia infinita de O_{priv}). Esta situación se puede observar en la Figura 3.17, donde la zona de color es el área de la región R_{pub} en la cual V determina que P no se puede encontrar.

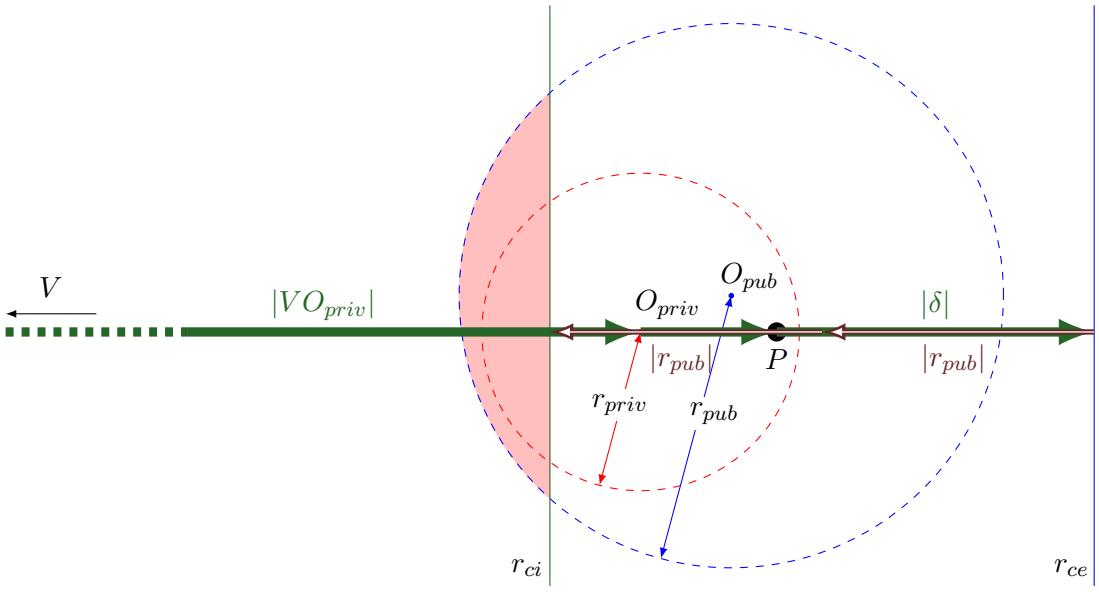


Figura 3.17: Condición para máximo refinamiento por abajo con ataque ABED. Dos regiones de encubrimiento con intervalo de retardo, $\delta \in [\, t_{(d_{maxpriv})} \,,\, t_{(2r_{priv})} \,]$.

Las regiones determinadas por el refinamiento, tanto de R_{priv} como R_{pub}, quedan definidas por el área de un segmento circular de un círculo, área de color en la Figura 3.18.

Esta área del segmento circular puede ser calculado por medio de alguna de las siguientes ecuaciones; 3.32, 3.34 o 3.33.

$$Area\ segmento\ circular\ (r, \alpha) = \frac{r^2 \cdot (\alpha - sen(\alpha))}{2} \tag{3.32}$$

o,

$$Area\ segmento\ circular\ (s, h) = \frac{h}{6\ s} \cdot (3\ h^3 + 4\ s^2) \tag{3.33}$$

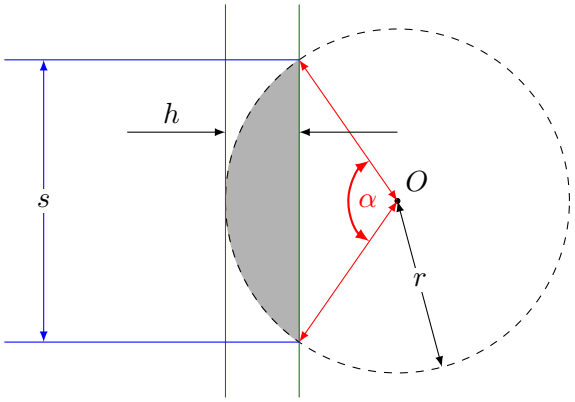


Figura 3.18: Segmento circular (en gris) de un círculo.

con,

$$r \;=\; \frac{h}{2} \;+\; \frac{s^2}{8\;h}$$

Es decir,

$$Area\ segmento\ circular\ (r,h) \;=\; \frac{32\;h^2\;r \;-\; 13\;h^3}{12\;\sqrt{2\;h\;r \;-\; h^2}} \tag{3.34}$$

Esta condición de máximo refinamiento posible permite determinar una métrica para que el usuario P decida si participa en el protocolo delimitador de distancia consciente de la ubicación, con la certeza que sus requerimientos de seguridad serán satisfechos.

Métrica para el Protocolo

Considerando la condición de máximo refinamiento posible, situación reflejada en la Figura 3.17, se define la métrica Υ_A como la razón entre el área no refinada de la región R_{priv} y el área de la región R_{priv}, ecuación 3.35.

$$\Upsilon_A\ (P,\delta,R_{pub},R_{priv}) \;=\; \frac{Area\ privada\ no\ refinada\ (P,\delta,R_{priv},R_{pub})}{Area\ privada\ (r_{priv})} \tag{3.35}$$

Esta métrica, junto al factor de tolerancia τ, permite al usuario P decidir si participa en el protocolo delimitador de distancia consciente de la ubicación. P participará en el protocolo DBP si se cumple la ecuación 3.36.

$$\Upsilon_A \geq \tau \tag{3.36}$$

Procedimiento frente al ataque ABED

La participación de P en el procedimiento de verificación de distancia con el ataque ABED incrementado con; dos regiones de encubrimiento, δ dentro del intervalo $[\ t_{(d_{maxpriv})}\ ,\ t_{(2r_{priv})}\ ]$ y métrica Υ_A; se describe a continuación:

(a) El usuario P determina las regiones de encubrimiento R_{priv} y R_{pub}, enviándole a un tercero

confiable los requerimientos para la creación de las regiones y espera su respuesta.

(b) Al recibir las regiones R_{priv} y R_{pub}, P determina el nivel de refinamiento τ y el retardo δ aleatoriamente dentro del intervalo [$t_{(d_{maxpriv})}$, $t_{(2r_{priv})}$].

(c) P determina si $\Upsilon_A\ (P, \delta, R_{priv}, R_{pub}) \geq \tau$, para decidir si continua con el protocolo DBP.

(d) P entrega la región R_{pub} a V. Y espera los desafíos del intercambio rápido de bits.

(e) Al recibir un desafío de V, P retarda su respuesta un tiempo δ.

La participación de V en el procedimiento de verificación de distancia con el ataque ABED incrementado con; dos regiones de encubrimiento, δ dentro del intervalo [$t_{(d_{maxpriv})}$, $t_{(2r_{priv})}$] y métrica Υ_A; se describe a continuación:

(a) V recibe la región R_{pub} de P.

(b) V determina si la región R_{pub} esta dentro de la cota práctica de la distancia. Para saber si continua con el protocolo DBP.

(c) Si la cota práctica de la distancia es satisfecha, V comienza el intercambio rápido de bits. Si la cota práctica de la distancia no es satisfecha, se lo comunica a P y termina el procedimiento.

(d) Al recibir la respuesta de P a su desafío, V determina la distancia $\widetilde{d}_{VP}$ con el tiempo medido t_m.

(e) Con $\widetilde{d}_{VP}$, V determina la distancia $\widetilde{d}_{VPmax} = \widetilde{d}_{VP}$, la que corresponde al radio externo de la corona circular, frontera exterior de la región C.

(f) Con $\widetilde{d}_{VP}$ y el radio r_{pub}, V determina la distancia $\widetilde{d}_{VPmin} = \widetilde{d}_{VP} - 2r_{pub}$, la que corresponde al radio interno de la corona circular, frontera interior de la región C.

(g) Con las regiones R_{pub} y C, V determina la región R_{Fpub} en la cual se podría encontrar P. $R_{Fpub} = C \cap R_{pub}$.

(h) Con los cálculos anteriores V verifica si P se encuentra en el interior de R_{pub}.

Análisis del estudio de la solución

Para este procedimiento se logra eliminar el refinamiento por arriba con la entrega de un mínimo de información en la metodología de selección del retardo δ, la cual no permite el refinamiento adicional visto en el procedimiento anterior.

La utilización de este procedimiento no modifica el intercambio rápido de bits del DBP, las modificaciones que conllevan mayor costo de cálculo se realizan previo al intercambio rápido de bits, lo cual no altera la esencia del DBP.

El procedimiento propuesto entregará una protección segura de la ubicación, un nivel de refinamiento máximo τ del área de la región de encubrimiento R_{priv} seleccionado como resolución de la ubicación antes de iniciar el protocolo DBP, para una mayor cantidad de regiones de encubrimiento R_{priv} que los procedimientos anteriores.

3.5. Dos Regiones de Encubrimiento con Retardo sobre un Intervalo de Retardos Posibles Modificado

La métrica para determinar la participación en el protocolo DBP del procedimiento anterior, Sección 3.4, se basa en el porcentaje de refinamiento del área de la región de encubrimiento R_{priv}. El valor de esta métrica se vuelve más negativo para la participación del usuario P cuando el radio de la región de encubrimiento R_{priv} se acerca más al radio de la región de encubrimiento R_{pub}, el porcentaje del área de la región R_{priv} refinada es mayor.

Si se considera que el usuario V desconoce si ha refinado o no la región R_{priv} al finalizar el protocolo DBP, aún cuando haya refinado la región R_{pub}, se puede considerar que la región R_{Fpub} es una buena sustituta de la región R_{priv} si satisface los mismos requerimientos utilizados para obtener la región R_{priv}. Bajo este criterio se puede modificar la métrica del procedimiento anterior para mejorar su desempeño.

En la Solución en Base a un Intervalo de Retardos con Dos Regiones de Encubrimiento y uso de Entropía (SBIRcDREyE) se modifica la métrica Υ_A del protocolo anterior, Sección 3.4.

Métrica para el Protocolo

Considerando que la entropía de una región es una medida de la cantidad de información de dicha región y que la condición de máximo refinamiento posible, situación reflejada en la Figura 3.19, se define la métrica Υ_H como la razón entre la entropía del área no refinada de la región R_{pub} y la entropía del área de la región R_{priv}, ecuación 3.37.

$$\Upsilon_H\ (P, \delta, R_{pub}, R_{priv}) \ = \ \frac{H\ (\ Area\ pública\ no\ refinada\ (P, \delta, R_{pub}, R_{priv})\ )}{H\ (\ Area\ privada\ (r_{priv})\ )} \tag{3.37}$$

Ya que la probabilidad que el usuario P ocupe un punto dentro de la región de encubrimiento privada R_{priv} se ha considerado igual para todo punto de esta, para este trabajo de investigación la razón entre las entropías es equivalente a la razón de las áreas de las regiones.

$$\Upsilon_H\ (P, \delta, R_{pub}, R_{priv}) \ = \ \frac{Area\ pública\ no\ refinada\ (P, \delta, R_{pub}, R_{priv})}{Area\ privada\ (r_{priv})} \tag{3.38}$$

Esta métrica, junto al factor de tolerancia τ, permite al usuario P decidir si participa en el protocolo delimitador de distancia consciente de la ubicación. P participará en el protocolo DBP si se cumple la ecuación 3.39.

$$\Upsilon_H \geq \tau \tag{3.39}$$

Procedimiento frente al ataque ABED

La participación de P en el procedimiento de verificación de distancia con el ataque ABED incrementado con; dos regiones de encubrimiento, δ dentro del intervalo $[\ t_{(d_{maxpriv})}\ ,\ t_{(2r_{priv})}\ ]$ y métrica Υ_H; se describe a continuación:

(a) El usuario P determina las regiones de encubrimiento R_{priv} y R_{pub}, enviándole a un tercero confiable los requerimientos para la creación de las regiones y espera su respuesta.

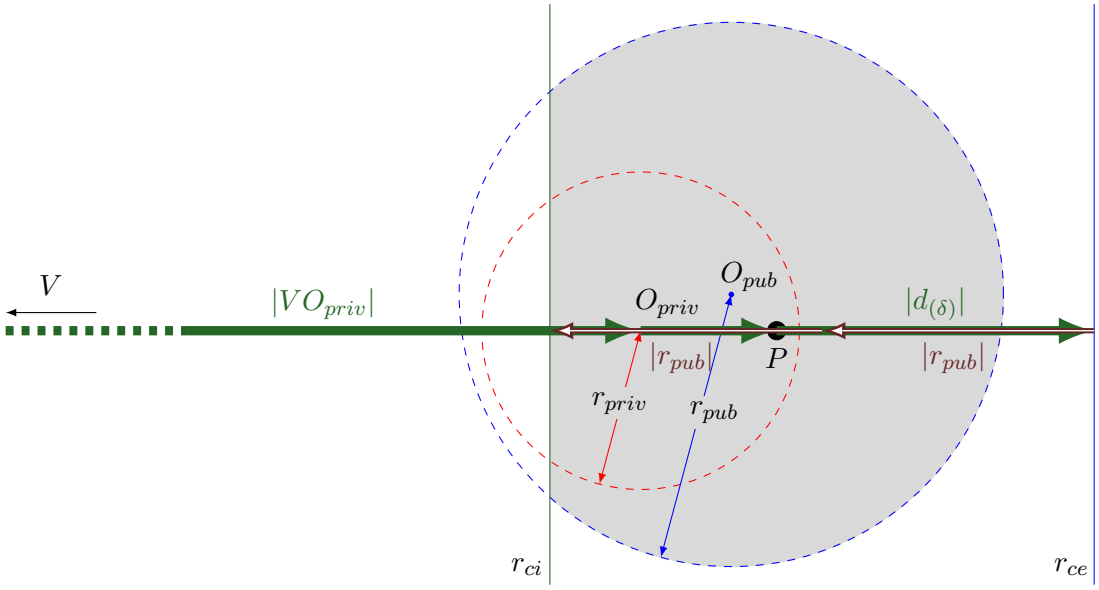


Figura 3.19: Condición para máximo refinamiento con ataque ABED para el procedimiento propuesto con dos regiones de encubrimiento, intervalo de retardo $\delta \in [\, t_{(d_{maxpriv})} \,,\, t_{(2r_{priv})} \,]$ y métrica Υ_H.

(b) Al recibir las regiones R_{priv} y R_{pub}, P determina el nivel de refinamiento τ y el retardo δ aleatoriamente dentro del intervalo $[\, t_{(d_{maxpriv})} \,,\, t_{(2r_{priv})} \,]$.

(c) P determina si $\Upsilon_H(P, \delta, R_{priv}, R_{pub}) \geq \tau$, para decidir si continua con el protocolo DBP.

(d) P entrega la región R_{pub} a V. Y espera los desafíos del intercambio rápido de bits.

(e) Al recibir un desafío de V, P retarda su respuesta un tiempo δ.

La participación de V en el procedimiento de verificación de distancia con el ataque ABED incrementado con; dos regiones de encubrimiento; δ dentro del intervalo $[\, t_{(d_{maxpriv})} \,,\, t_{(2r_{priv})} \,]$ y métrica Υ_H; se describe a continuación:

(a) V recibe la región R_{pub} de P.

(b) V determina si la región R_{pub} esta dentro de la cota práctica de la distancia. Para saber si continua con el protocolo DBP.

(c) Si la cota práctica de la distancia es satisfecha, V comienza el intercambio rápido de bits. Si la cota práctica de la distancia no es satisfecha, se lo comunica a P y termina el procedimiento.

(d) Al recibir la respuesta de P a su desafío, V determina la distancia $\widetilde{d}_{VP}$ con el tiempo medido t_m.

(e) Con $\widetilde{d}_{VP}$, V determina la distancia $\widetilde{d}_{VPmax} = \widetilde{d}_{VP}$, la que corresponde al radio externo de la corona circular, frontera exterior de la región C.

(f) Con $\widetilde{d}_{VP}$ y el radio r_{pub}, V determina la distancia $\widetilde{d}_{VPmin} = \widetilde{d}_{VP} - 2r_{pub}$, la que corresponde al radio interno de la corona circular, frontera interior de la región C.

(g) Con las regiones R_{pub} y C, V determina la región R_{Fpub} en la cual se podría encontrar P. $R_{Fpub} = C \cap R_{pub}$.

(h) Con los cálculos anteriores V verifica si P se encuentra en el interior de R_{pub}.

Análisis del estudio de la solución

Como se puede apreciar el procedimiento sólo cambia en la determinación de la métrica, Υ_H por Υ_A. La métrica Υ_H $(P, \delta, R_{pub}, R_{priv})$ requiere determinar si el área no refinada R_{Fpub} satisface los requerimientos para sustituir a la región R_{priv}. Para este caso de estudio, el considerar el área de R_{pub} en lugar del área de R_{priv} conlleva un menor refinamiento desde el punto de vista del usuario P, por lo cual una mayor participación total en el protocolo.

El procedimiento propuesto entregará una protección segura de la ubicación, un nivel de refinamiento máximo τ de la región de encubrimiento R_{priv} seleccionado como resolución de la ubicación antes de iniciar el protocolo DBP, para mayor cantidad de regiones de encubrimiento R_{priv} que el procedimiento de la Sección 3.4. Esto lo convierte en el mejor procedimiento estudiado para un protocolo delimitador de distancia consciente de la ubicación, DBPALP.

Capítulo 4

Solución al Ataque Basado en el Ajuste del Area de Cobertura

En este capítulo se entrega una forma de enfrentar un Ataque Basado en el ajuste del Area de Cobertura (ABAC). Se comienza describiendo la atenuación de una señal electromagnética en la Sección 4.1 y se finaliza con la presentación del procedimiento propuesto para enfrentar el ataque ABAC basado en el procedimiento propuesto para enfrentar el ataque ABED, en la Sección 3.5.

En el ABAC el usuario verificador V actúa como el adversario que ataca la región de encubrimiento R para refinarla. V controla la potencia de emisión de la señal electromagnética de comunicaciones para determinar el nivel de potencia para el cual el usuario P responde la comunicación. Este nivel de potencia más el conocimiento del nivel de potencia recibida mínima al cual responde P, le permite a V determinar su distancia a P.

El procedimiento presentado en este capítulo para enfrentar al ataque ABAC se basa en la consideración de un delta de potencia ρ, a considerar sobre el nivel mínimo de potencia de recepción del dispositivo del usuario P, para considerar válido un mensaje. Esto con el fin que V determine una ubicación de P más lejana de lo que realmente esta es.

4.1. Propagación de una Señal Electromagnética

El escenario de este trabajo de investigación es ideal en un espacio 2D, con regiones circulares y propagación de las señales electromagnéticas en forma perfecta, es decir, de radio circular y sin shadowing, y no se considera el uso de antenas adaptativas o direccionales que permitan a ambos usuarios inferir la dirección de llegada de un mensaje.

Bajo estas condiciones, la radiación electromagnética tiene una atenuación equivalente a la de una propagación esférica perfecta en un espacio 3D. Considerando el modelo en espacio libre, para la propagación esférica la potencia se atenúa según la siguiente relación, ecuación 4.1.

$$W_r = \frac{1}{\xi} \quad \frac{W_t}{d^2} \tag{4.1}$$

Donde ξ es una constante, dependiente del entorno de transmisión, d la distancia entre el nodo de transmisión y el nodo de recepción, W_t es la potencia de transmisión y W_r es la potencia

de la señal a la distancia d. La gráfica de esta ecuación se presenta en la Figura 4.1, donde se considera $\xi = 1$ y $W_r = 1$ a una distancia $d = 1$, para simplicidad y generalización de la gráfica.

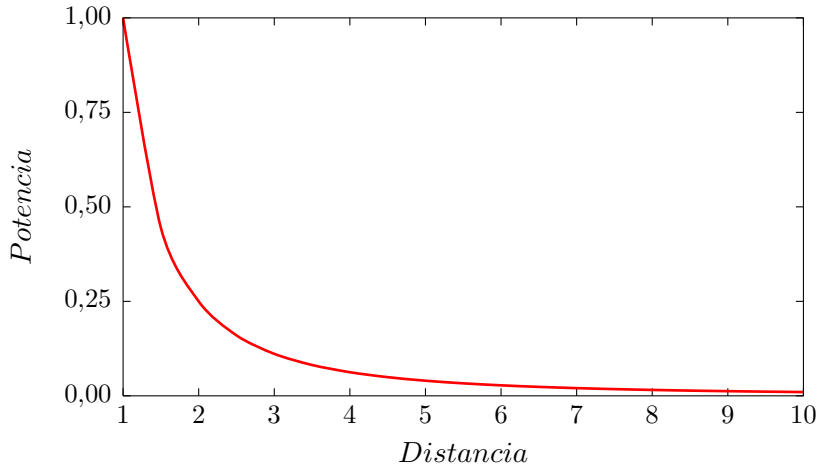


Figura 4.1: Atenuación de la potencia transmitida en base a la distancia recorrida por la señal de comunicación.

La ecuación 4.1, visualizada en la Figura 4.1, indica que un nivel de potencia se atenúa con el cuadrado de la distancia al centro del emisor.

Este efecto de atenuación se puede observar en la Tabla 4.1. Para un nodo que recibe un nivel de potencia de "1.1" de un nodo origen a diferentes distancias (10, 100, 1000 y 10000), la distancia desde su posición requerida para atenuar un delta de nivel de potencia de "0.1" es diferente para las distintas distancias entre los nodos. Es decir, para unos nodos separados una distancia "10"se requerirá de una distancia de "0.49"desde el nodo receptor para atenuar una potencia de "0.1", mientras que para una separación entre nodos de "100"se requerirá de una distancia de "4.88"(48.81 para una de separación de 1000 y 488.09 para una separación de 10000).

Tabla 4.1: Atenuación de un delta de potencia en la distancia. Delta de potencia de 0.1 sobre 1.

Potencia Recibida	Distancia del origen	Potencia en el Origen	Potencia Objetivo	Distancia de atenuación
1,1	10	110	1	0.49
1,1	100	11 000	1	4.88
1,1	1 000	1 100 000	1	48.81
1,1	10 000	110 000 000	1	488.09

Bajo el escenario propuesto para este trabajo de investigación y la diversidad de resultados posibles en el cálculo de la distancia de atenuación para un nivel de potencia de la señal de

comunicaciones, no es factible determinar un delta de potencia ρ útil para desarrollar un protocolo delimitador de distancia consciente de la privacidad de ubicación. La determinación de un delta de potencia ρ útil requiere de mayor cantidad de información, un requisito que se ha limitado en este trabajo de investigación.

4.2. Solución Propuesta

Como se ha determinado en la Sección 4.1, bajo el escenario propuesto para este trabajo de investigación no es factible determinar un delta de potencia ρ útil para desarrollar un protocolo DBP consciente de la privacidad de la ubicación y como no es aceptable la inclusión de mayor información sólo para enfrentar el ataque ABAC, alterando las condiciones propuestas para el problema, se plantea la siguiente modificación a las condiciones del problema. Para continuar con el estudio del problema se considera para el resto de esta investigación que el proceso de determinación de un delta de potencia ρ es ajeno al procedimiento a desarrollar, implementado por una entidad externa confiable. Además, para el resto de la investigación no se considera la información que se pudiera obtener del conocimiento del delta de potencia ρ.

Procedimiento propuesto

En el ataque ABAC el usuario V controla la potencia de la señal electromagnética de comunicaciones que utiliza para enviar los mensajes al usuario P y mide esta para determinar a que nivel de potencia de la señal transmitida recibe una respuesta de P. Esta medición de potencia, más el conocimiento del nivel mínimo de potencia de recepción que requiere P para considerar válida una comunicación, le permite a V determinar su distancia a P. Se podría pensar que P pudiera responder a un nivel superior de potencia y no al mínimo para hacer parecer a V que está ubicado más lejos de lo que realmente está.

La consideración de un delta de potencia, ρ, a sumar a la mínima potencia requerida para responder un mensaje es la opción a considerar, la pregunta a responder ¿cuál es la potencia a la que P debe responder un mensaje?. Esta pregunta es equivalente a la pregunta realizada para enfrentar un ataque ABED, ¿cuánto debe retardar P el envío de su respuesta a V?. Si el delta de potencia es muy pequeño, V podría refinar la región de encubrimiento de P. Por el contrario, si tal delta de potencia fuese muy grande, V estimaría una distancia a P que pudiese ser inútil para fines prácticos de verificación de ubicación.

Ambos enfoques, retardo - ataque ABED y delta de potencia - ataque ABAC, generan una región de protección sobre la región de encubrimiento, que es la misma para ambos ataques. Ya que en ambos casos se usan variables, el tiempo en uno y la potencia de transmisión en el otro, que son transformadas a sus equivalentes de distancia y los resultados de dichas transformaciones deben ser distancias iguales. Esto se puede observar en la Figura 4.2.

En la Figura 4.2, O_{priv} es el centro de la región de encubrimiento privada de radio r_{priv}, O_{pub} es el centro de la región de encubrimiento pública de radio r_{pub}, $\overrightarrow{d_{(\delta)}}$ es el vector de distancia equivalente al tiempo δ, $\overrightarrow{d_{(\rho)}}$ es el vector de distancia equivalente al uso de un delta de potencia ρ, $\widetilde{d}_{VP}$ es la distancia a P estimada por V, c es la velocidad de propagación de la onda electromagnética en el medio de comunicación, t_m es el tiempo total que mide el usuario V desde que envía su desafío hasta la recepción de la respuesta de P, t_d es el tiempo que demora

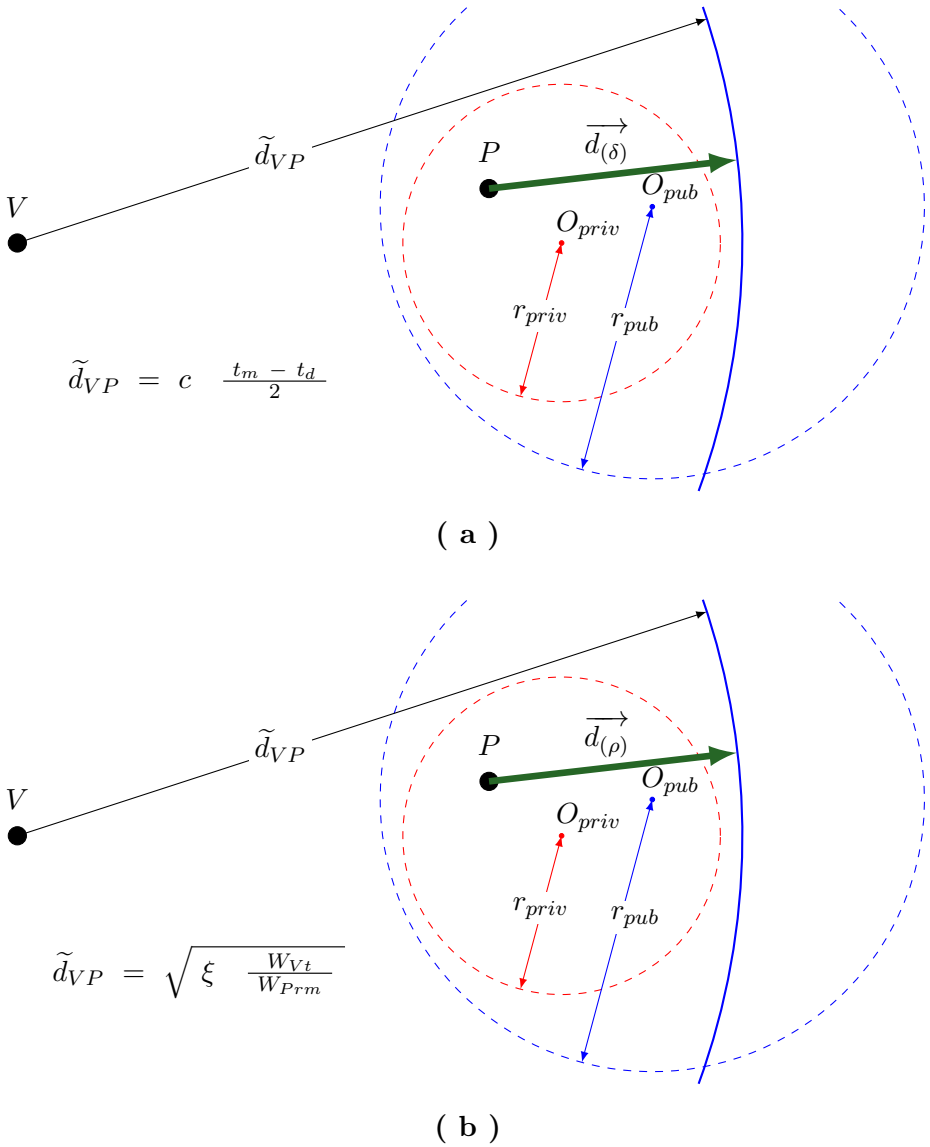


Figura 4.2: Similitud de los ataques ABED y ABAC. (a) Ataque ABED y (b) Ataque ABAC.

el usuario P en responder al desafío recibido de V, ξ es una constante, W_{Vt} es la potencia de transmisión de la señal del desafío enviado por V y W_{Prm} es la potencia mínima requerida por P para recibir un mensaje válido.

Entonces, para determinar la distancia que debe cubrir el delta de potencia son válidas todas las consideraciones de refinamiento realizadas en el Capítulo 3. Por lo cual, el procedimiento más adecuado es el uso de dos regiones de encubrimiento propuesto en la Sección 3.5.

Delta de Nivel de Potencia

Para esta investigación se ha considerado que el delta de potencia ρ es determinado por una entidad externa confiable. Para que esta entidad pueda determinar un delta de potencia ρ, adecuado, con el cual proteger la región de encubrimiento del usuario P, debe poseer información adicional a la que dispone el usuario P.

La determinación del delta de potencia ρ por una entidad externa queda definida, según la ecuación 4.1, por; la distancia entre los usuarios a prueba P y verificador V, la potencia de recepción mínima de señal requerida por el usuario P, la distancia que debe permitir el delta de potencia ρ, y las características del medio por el cual se transmite la señal.

Con la información mencionada la entidad externa puede determinar la potencia de transmisión, del usuario V, para que se reciba la mínima potencia de recepción a una distancia equivalente a la suma de la distancias entre usuarios, V y P, y la distancia que debe permitir el delta de potencia ρ. Con esta nueva potencia de transmisión se puede determinar la potencia que recibe el usuario P y con esta el delta de potencia sobre el mínimo de potencia de recepción, que sería el delta de potencia ρ.

Métrica para Protocolo DBP

Considerando que la entropía de una región es la medida de la cantidad de información que dispone la región y la condición de máximo refinamiento posible, situación reflejada en la Figura 4.3, se define la métrica $\Upsilon_{H\rho}$ como la razón entre el área no refinada de la región R_{pub} y el área de la región R_{priv}, ecuación 4.2, simplificación de la métrica definida en la Sección 3.5 para las condiciones de esta investigación.

$$\Upsilon_{H\rho}\ (P, \rho, R_{pub}, R_{priv}) \ = \ \frac{Area\ p\acute{u}blica\ no\ refinada\ (P, \rho, R_{pub}, R_{priv})}{Area\ privada\ (r_{priv})} \tag{4.2}$$

Esta métrica, junto al factor de tolerancia τ, permite al usuario P decidir si participa en el protocolo delimitador de distancia consciente de la ubicación. P participará en el protocolo DBP si se cumple la ecuación 4.3.

$$\Upsilon_{H\rho} \geq \tau \tag{4.3}$$

La única diferencia con la métrica definida anteriormente, Υ_H, es el uso del parámetro ρ en lugar de δ, potencia en lugar de tiempo para determinar distancia.

Procedimiento frente al ataque ABAC

La participación de P en el procedimiento de verificación de distancia con el ataque ABAC incrementado con; dos regiones de encubrimiento, ρ dentro del intervalo $[\ W_{(d_{maxpriv})}\ ,\ W_{(2r_{priv})}\ ]$ y métrica $\Upsilon_{H\rho}$; se describe a continuación:

(a) El usuario P selecciona las regiones de encubrimiento R_{priv} y R_{pub}, le envía a un tercero confiable los requerimientos para la creación de las regiones y espera su respuesta.

(b) Al recibir las regiones R_{priv} y R_{pub}, P determina el nivel de refinamiento τ y el delta de potencia rho aleatoriamente dentro del intervalo $[\ W_{(d_{maxpriv})}\ ,\ W_{(2r_{priv})}\ ]$ (el delta de potencia ρ por medio de una entidad externa confiable).

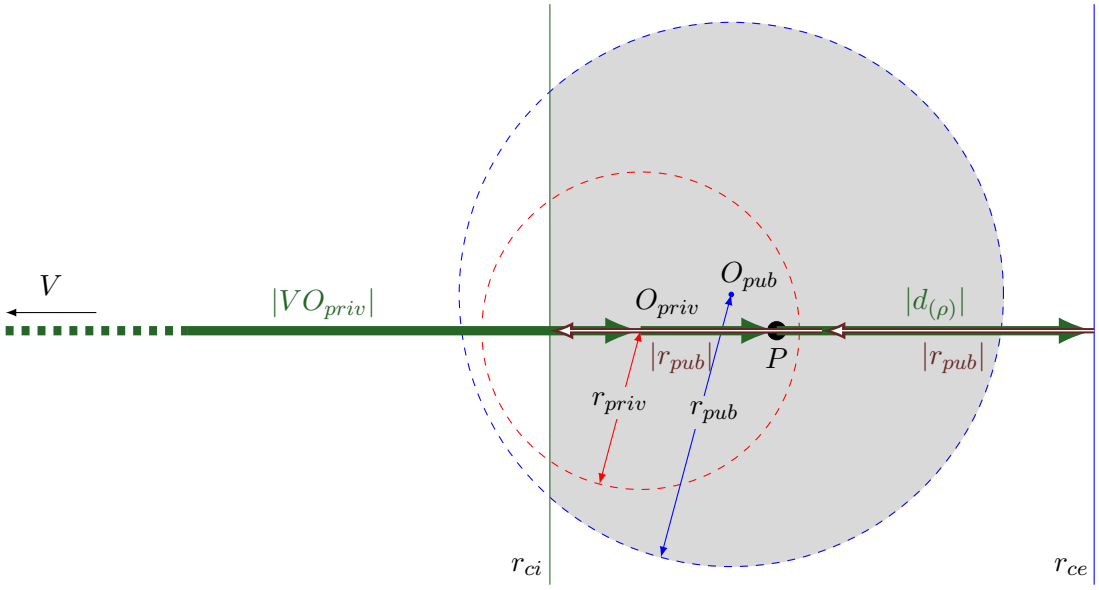


Figura 4.3: Condición para máximo refinamiento con ataque ABAC para el procedimiento propuesto. Dos regiones de encubrimiento con intervalo de potencia, $\rho \in [\, W_{(d_{maxpriv})} \,,\, W_{(2r_{priv})} \,]$.

(c) P determina si $\Upsilon_{H\rho}(P, \delta, R_{priv}, R_{pub}) \geq \tau$, para decidir si continua con el protocolo DBP.

(d) P entrega la región R_{pub} a V. Y espera los desafíos del intercambio rápido de bits.

(e) En las siguientes comunicaciones con V, P responde sólo si el nivel de potencia de la señal de comunicaciones tiene una potencia superior a ρ sobre el nivel mínimo de recepción.

(f) Al recibir un desafío de V, P responde sólo si el nivel de potencia de la señal de comunicaciones tiene una potencia superior a ρ sobre el nivel mínimo de recepción.

La participación de P en el procedimiento de verificación de distancia con el ataque ABAC incrementado con; dos regiones de encubrimiento, ρ dentro del intervalo $[\, W_{(d_{maxpriv})} \,,\, W_{(2r_{priv})} \,]$ y métrica $\Upsilon_{H\rho}$; se describe a continuación:

(a) V recibe la región R_{pub} de P.

(b) V determina si la región R_{pub} está dentro de la cota práctica de la distancia. Para saber si continua con el protocolo DBP.

(c) Si la cota práctica de la distancia es satisfecha, V comienza el intercambio rápido de bits. Si la cota práctica de la distancia no es satisfecha, se lo comunica a P y termina el procedimiento.

(d) Al recibir la respuesta de P a su desafío, V determina la distancia $\widetilde{d}_{VP}$ con el nivel de potencia de transmisión medido W_{Vt}.

(e) Con $\widetilde{d}_{VP}$, V determina la distancia $\widetilde{d}_{VPmax} = \widetilde{d}_{VP}$, la que corresponde al radio externo de la corona circular, frontera exterior de la región C.

(f) Con $\widetilde{d}_{VP}$ y el radio r_{pub}, V determina la distancia $\widetilde{d}_{VPmin} = \widetilde{d}_{VP} - 2r_{pub}$, la que corresponde al radio interno de la corona circular, frontera interior de la región C.

(g) Con las regiones R_{pub} y C, V determina la región R_{Fpub} en la cual se podría encontrar P. $R_{Fpub} = C \cap R_{pub}$.

(h) Con los cálculos anteriores V verifica si P se encuentra en el interior de R_{pub}.

Análisis del estudio de la solución

El procedimiento propuesto entregará una protección segura de la ubicación, un nivel de refinamiento τ de la región de encubrimiento R_{priv}, seleccionada como resolución de la ubicación antes de iniciar el protocolo DBP. Como ya está demostrado en el estudio de las soluciones presentadas para enfrentar un ataque ABED; considerando que ambos enfoques, retardo - ataque ABED y delta de potencia - ataque ABAC son equivalentes.

Capítulo 5

Hacia un Protocolo Delimitador de Distancia Consciente de la Privacidad de Ubicación

En este capítulo se presenta el protocolo delimitador de distancia consciente de la privacidad de ubicación (DBPALP, Distance Bounding Protocol Aware of Location Privacy). En la Sección 5.1 se presenta el protocolo para el escenario de dos usuarios estáticos. Se finaliza el capítulo con un análisis preliminar para los casos con usuario móvil, considerados trabajos futuros de investigación, Sección 5.2.

5.1. Protocolo para Usuario a Prueba y Usuario Verificador Estáticos

La determinación de las regiones de encubrimiento (R_{priv} y R_{pub}) y del delta de potencia sobre el nivel mínimo de recepción (ρ) requieren de información que no es conocida por los usuarios para este trabajo de investigación. Por lo cual se considera que tanto la determinación de las regiones de encubrimiento y la determinación del delta de potencia son realizados por terceras entidades confiables que disponen de la información necesaria.

Determinación de las regiones de encubrimiento

La determinación de las regiones de encubrimiento, R_{priv} y R_{pub}, requiere de información adicional para asegurar los criterios de privacidad y seguridad impuestos por el usuario P. Para el caso de este trabajo de investigación se considera que una tercera entidad confiable dispondrá de dicha información; por ejemplo, la probabilidad que el usuario este en una determinada ubicación.

Con esta información y con los requerimientos de privacidad y seguridad impuestos por P a sus regiones la tercera entidad puede determinar las regiones y enviarlas a P. Esto como es presentado en el Capítulo 3.

Determinación del delta de potencia

La determinación de un nivel de potencia a considerar sobre el nivel mínimo de recepción, ρ, requiere de información que no esta disponible para el usuario P. Para este trabajo de investigación se considera que una tercera entidad confiable dispondrá de dicha información; por ejemplo, entre la información no disponible se encuentra la distancia precisa entre los usuario P y V.

Con esta información adicional y con la distancia a cubrir con el delta de potencia, determinada por P, la tercera entidad puede determinar el delta de potencia ρ. Esto como es presentado en la Sección 4.2.

Protocolo propuesto

A continuación se presenta el protocolo delimitador de distancia consciente de la privacidad de ubicación (DBPALP) propuesto para dos usuarios estáticos. En este se consideren los dos ataques estudiados como procedimientos para que el usuario V estime su distancia al usuario P, el Ataque Basado en el ajuste del Area de Cobertura de una transmisión inalámbrica (ABAC) y el Ataque Basado en la dElimitación de Distancia (ABED).

El protocolo se describe a continuación y se presenta en la Figura 5.1.

(a) El usuario P determina los criterios de privacidad y seguridad para las regiones de encubrimiento, R_{priv} y R_{pub}. Con estos solicita a una tercera entidad confiable la formación de ambas regiones.

(b) El usuario P determina el nivel de refinamiento τ.

(c) El usuario P, con la información de las regiones R_{priv} y R_{pub}, selecciona aleatoriamente la distancia que define el retardo δ y el delta de potencia ρ sobre el intervalo $[\, d_{maxpriv} \,,\, 2r_{priv} \,]$.

(d) El usuario P determina el retardo δ y solicita a una tercera entidad confiable el delta de potencia ρ para satisfacer la distancia seleccionada.

(e) El usuario P determina si $\Upsilon_H \ (P, \delta, R_{pub}, R_{priv}) \geq \tau$. Para saber si continua con las comunicaciones con V.

(f) El usuario P determina si $\Upsilon_{H\rho} \ (P, \rho, R_{pub}, R_{priv}) \geq \tau$. Para saber si continua con las comunicaciones con V.

(g) En las siguientes comunicaciones con V, P responde sólo si el nivel de potencia de la señal de comunicaciones tiene una potencia superior a ρ sobre el nivel mínimo de recepción.

(h) P entrega la región R_{pub} a V.

(i) V determina si la región R_{pub} esta dentro de la cota práctica de la distancia. Para saber si continua con el protocolo DBP.

(j) Mediante un ataque ABED V determina la región C_δ, corona circular en la cual se debe encontrar P, durante el cual P retarda su respuesta un retardo δ.

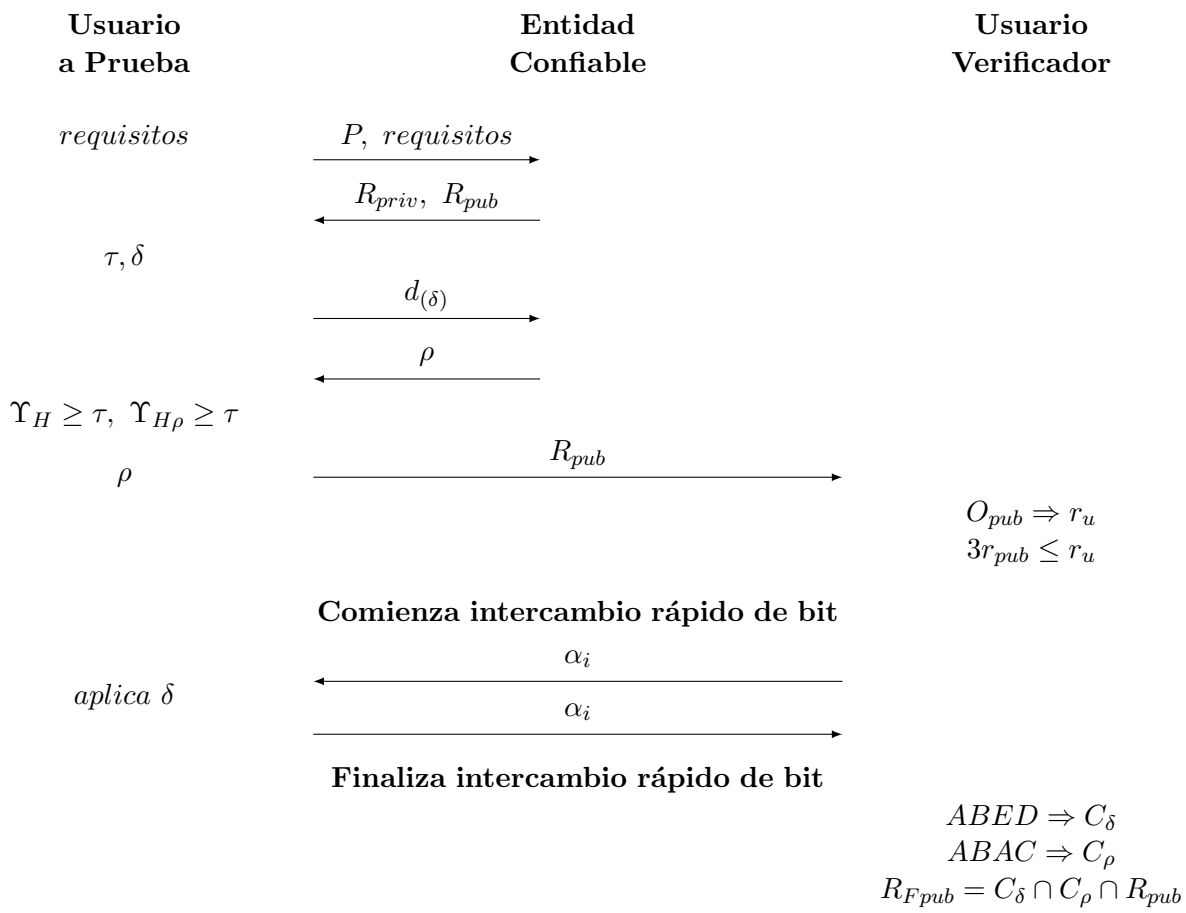


Figura 5.1: Protocolo delimitador de distancia consciente de la privacidad de ubicación (DBPALP, Distance Bounding Protocol Aware of Location Privacy), para usuario P estático y usuario V estático.

(k) Mediante un ataque ABAC V determina la región C_ρ, corona circular en la cual se debe encontrar P.

(l) Con las regiones R_{pub}, C_δ y C_ρ, V determina la región R_{Fpub} en la cual se podría encontrar P, $R_{Fpub} = C_\delta \cap C_\rho \cap R_{pub}$, para verificar la ubicación de P a una distancia útil.

5.2. Hacia un DBPALP con Usuario Móvil

5.2.1. Caso para Usuario a Prueba Estático y Usuario Verificador Móvil

En este escenario se considera que el usuario P esta estático dentro de su región de encubrimiento R_{priv}, mientras el usuario V cambia de posición en el entorno.

Al considerarse el uso de un DBPALP desarrollado para usuarios estáticos la movilidad de V conlleva la determinación exacta de la posición de P, esto al poder realizarse múltiples

refinamientos. Por ejemplo, si V pudiera circunvalar la región R_{pub} realizando refinamientos se tendría el caso que se muestra en la Figura 5.2.

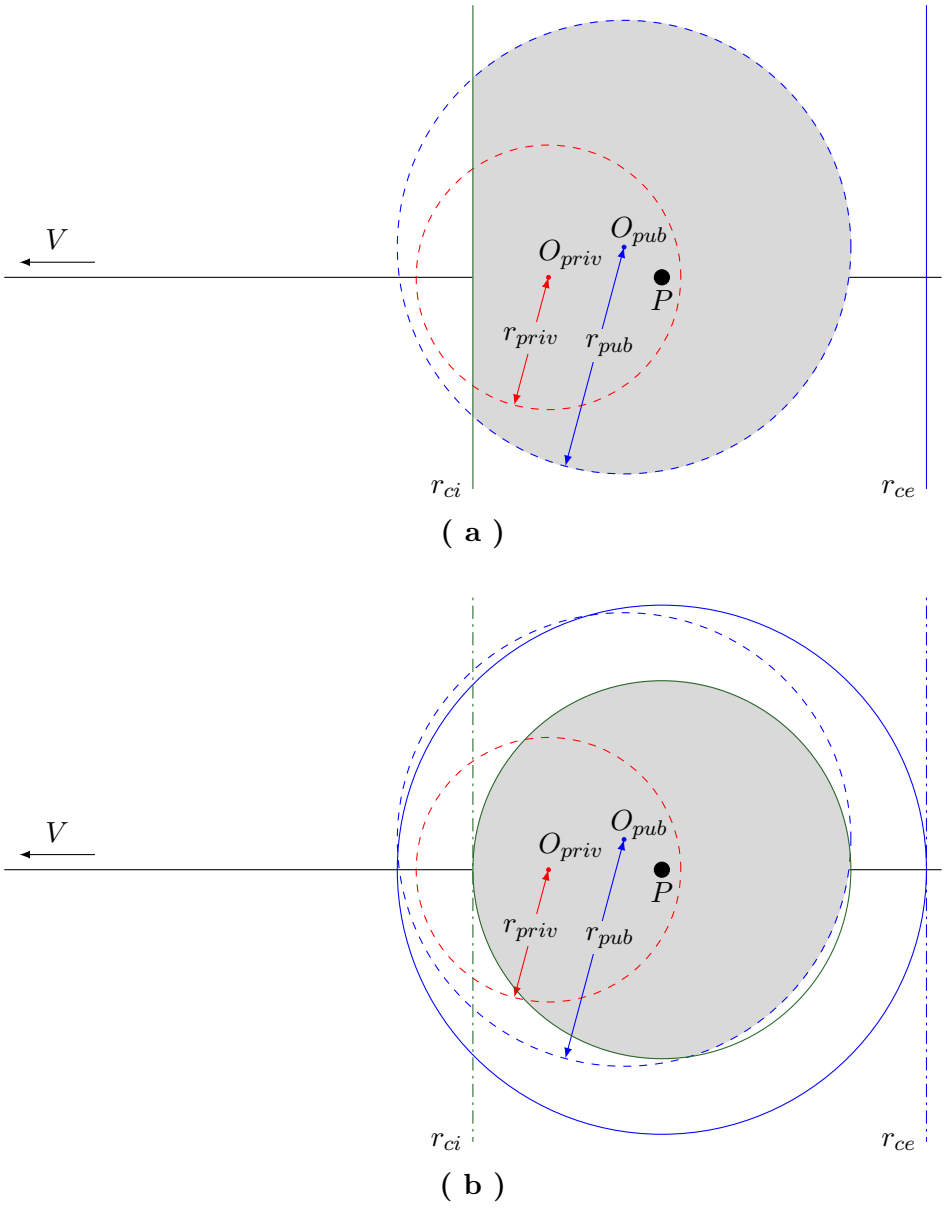


Figura 5.2: Condición para máximo refinamiento para procedimiento con usuario V móvil. (a) Primer refinamiento. (b) Múltiples refinamientos.

La Figura 5.2.a presenta el primer refinamiento y la Figura 5.2.b presenta el resultado de múltiples refinamientos si V circunvaliza a R_{pub} generando las fronteras de refinamiento, expresadas como circunferencias de líneas continuas, las cuales generan la región C que permite determinar la región refinada R_F (área gris). Más aún, en un segundo nivel de refinamiento, se puede determinar la posición exacta de P ya que ambas fronteras son circunferencias formadas

con centro en P.

La situación puede verse peor aún, pues ambas fronteras en forma de circunferencia quedan determinadas por solo tres posiciones de V, Figura 5.3, sólo una circunferencia toca en un solo punto a cada una de las fronteras. Es decir, si se mantiene el protocolo de la Sección 5.1 la posición exacta de P es determinada.

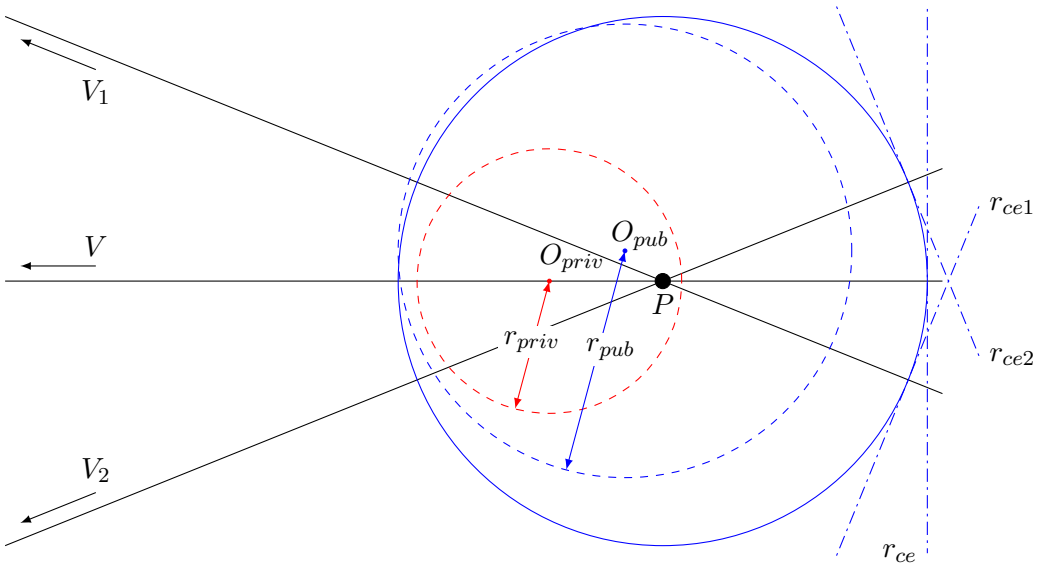


Figura 5.3: Triangulación de posición para procedimiento con usuario V móvil.

Para evitar que se determinen las fronteras circulares de C con exactitud se debe modificar el protocolo para variar aleatoriamente el valor del retardo δ y del nivel de potencia ρ, sobre valores en torno a los inicialmente determinados y dentro de sus intervalos permitidos, durante las comunicaciones en el protocolo DBP con el mismo usuario V. Además, se debe considerar un límite al número de veces, N_v, en que el protocolo DBP se ejecuta en un determinado tiempo, T_v, con un usuario V.

5.2.2. Caso para Usuario a Prueba Móvil y Usuario Verificador Estático

En este escenario se considera que el usuario P se mueve dentro de su región de encubrimiento R_{priv} a una velocidad y dirección desconocidas por el usuario V, mientras V se considera estático en algún punto del entorno.

La movilidad de P implica que el refinamiento del área de encubrimiento realizado por V sólo tiene validez por un instante de tiempo, nada le asegura a V que P no se mueva a un área en la cual se ha considerado que P no se puede encontrar. La información recolectada por V en refinamientos anteriores no puede ser considerada confiable.

Entonces, dado que el protocolo sería válido en un instante de tiempo, el protocolo propuesto en la Sección 5.1 sería útil para el escenario del usuario P móvil y el usuario V estático, con la consideración que los refinamientos sucesivos de la región de encubrimiento pierden validez para realizar un refinamiento más profundo de la región de encubrimiento, ya que en esta investigación el protocolo es utilizado por V sólo para verificar la ubicación de P dentro de la región de

encubrimiento, R_{pub}.

5.2.3. Caso para Usuario a Prueba Móvil y Usuario Verificador Móvil

En este escenario se considera que el usuario P se mueve dentro de su región de encubrimiento R_{priv} a una velocidad y dirección desconocidas por el usuario V, mientras el V cambia de posición en el entorno.

La movilidad de P implica que el refinamiento del área de encubrimiento realizado por V sólo tiene validez por un instante de tiempo, nada le asegura a V que P no se mueva a un área en la cual se ha considerado que P no se puede encontrar. La información recolectada por V en refinamientos anteriores no puede ser considerada confiable.

La movilidad de V conlleva la posibilidad de realizar un refinamiento de la región de encubrimiento mediante las metodologías mencionadas en la Subsección 5.2.1. La validez de la información obtenida estará sujeta a la velocidad del movimiento de P. Como, en este trabajo de investigación la velocidad de movimiento no esta restringida, el refinamiento del área de encubrimiento realizado por V sólo tiene validez por un instante de tiempo, nada le asegura a V que P no se mueva a un área en la cual se ha considerado que P no se puede encontrar. La información recolectada por V en refinamientos anteriores no puede ser considerada confiable.

Entonces, dado que el protocolo sería válido en un instante de tiempo, el protocolo propuesto en la Subsección 5.1 sería útil para el escenario del usuario P móvil y el usuario V móvil, con la consideración que los refinamientos sucesivos de la región de encubrimiento pierden validez para realizar un refinamiento más profundo de la región de encubrimiento, ya que en este trabajo de investigación el protocolo es utilizado por V sólo para verificar la ubicación de P dentro de la región de encubrimiento, R_{pub}.

Capítulo 6

Simulaciones Computacionales

En este capítulo se presenta un estudio computacional, en base al método de Montecarlo, del desempeño de las soluciones propuestas. Teniendo como métrica para comparar el desempeño de todas las soluciones el Porcentaje de Participaciones del usuario a prueba P en el intercambio rápido de bits. Se comienza entregando el entorno del estudio de desempeño del protocolo delimitador de distancia consciente de la privacidad de ubicación (DBPALP) en la Sección 6.1, describiendo las condiciones del estudio. Se continúa presentando el experimento realizado en la Sección 6.2. Luego, se presentan los resultados obtenidos del estudio y su análisis en las Secciones 6.3 y 6.4, finalizando con un estudio de casos particulares, Sección 6.5.

El programa se desarrolla en Lenguaje C y se corre sobre Windows 7 Enterprise, en un computador Samsung Notebook NP470R5E con Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz.

6.1. Entorno del Estudio de Desempeño del DBPALP

El estudio computacional del desempeño de las soluciones propuestas, en base al método de Montecarlo, se realiza para el protocolo delimitador de distancia consciente de la privacidad de ubicación propuesto en el caso de usuario a prueba P estático y usuario verificador V estático.

Las soluciones, ya presentadas en el Capítulo 3, son las siguientes;

- SBMD ; Solución en Base a un retardo igual a la Máxima Distancia.
- SBIR ; Solución en Base a un Intervalo de Retardos posibles.
- SBMDcDRE ; Solución en Base a un retardo igual a la Máxima Distancia con Dos Regiones de Encubrimiento.
- SBIRcDRE ; Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento.
- SBIRcDREyE ; Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento y uso de Entropía.

Para relacionar adecuadamente los estudios de las diferentes soluciones en la Tabla 6.1 se presentan las equivalencias de algunos conceptos y variables. El más relevante para el estudio de

desempeño es el concepto de cota útil, descrito en capítulos anteriores, del cual se presentan tres rangos en la Tabla 6.1; por ejemplo, si para la solución SBMD se considera una cota útil igual a $6r_{priv}$, para la solución SBIRcDREyE se tendría una cota útil equivalente de $6r_{priv}$ / $3r_{pub}$. Este concepto, cota útil, limita algunos parámetros dentro de las diferentes soluciones para la realización de una correcta comparación de las soluciones.

Tabla 6.1: Equivalencia de conceptos y parámetros en el estudio de desempeño de las diferentes soluciones.

Parámetro	Parámetros Equivalentes				
	SBMD	SBIR	SBMDcDRE	SBIRcDRE	SBIRcDREyE
Región de Encubrimiento	R	R	R_{priv}	R_{priv}	R_{priv}
Radio de la R. de E.	1	1	1	1	1
Cota Util	$3r$	$3r$	$3r_{pub}$ / $3r_{priv}$	$3r_{pub}$ / $3r_{priv}$	$3r_{pub}$ / $3r_{priv}$
	4,3r	4,3r	$3r_{pub}$ / 4,3r_{priv}	$3r_{pub}$ / 4,3r_{priv}	$3r_{pub}$ / 4,3r_{priv}
	$6r$	$6r$	$3r_{pub}$ / $6r_{priv}$	$3r_{pub}$ / $6r_{priv}$	$3r_{pub}$ / $6r_{priv}$
τ	1	1	1	1	1

R. de E. : Región de Encubrimiento.

La métrica utilizada para comparar el desempeño de todas las soluciones es el Porcentaje de Participaciones del usuario a prueba P en el intercambio rápido de bits. Es decir, cuando el usuario a prueba P decide participar en el protocolo delimitador de distancia (DBP) y no sólo porque comienza a participar del protocolo delimitador de distancia consciente de la privacidad de ubicación (DBPALP), el cual incluye el protocolo DBP, Sección 5.1.

Los parámetros utilizados en los experimentos son aquellos que están presentes en al menos una de las soluciones propuestas para lograr un DBPALP. Estos son los siguientes;

- r_{priv} ; radio de la región de encubrimiento privada.
- $O_{priv}(x, y)$; centro de la región de encubrimiento privada.
- r_{pub} ; radio de la región de encubrimiento pública.
- $O_{pub}(x, y)$; centro de la región de encubrimiento pública.
- Λ ; límite superior de intervalo de tiempos donde se selecciona el retardo δ.
- τ ; factor de tolerancia aceptado por P para el refinamiento.
- $V(x, y)$; posición del usuario verificador V.
- $P(x, y)$; posición del usuario a prueba P.
- $d_{(\delta)}$; distancia recorrida en el retardo δ.

6.2. Diseño del Experimento

El experimento computacional del desempeño de las soluciones determina el promedio de cada métrica evaluadora, para un número de experimentos que permiten la convergencia de este. Los parámetros involucrados en las soluciones son determinados seudoaleatoriamente.

Los parámetros utilizados en los experimentos y sus rangos de variación, para los estudios de las diferentes soluciones, se presentan en la Tabla 6.2.

Tabla 6.2: Parámetros utilizados en los experimentos.

Parámetro	Rango de Variación				
	SBMD	SBIR	SBMDcDRE	SBIRcDRE	SBIRcDREyE
r_{priv}	1	1	1	1	1
$O_{priv}(x, y)$	$(0, 0)$	$(0, 0)$	$(0, 0)$	$(0, 0)$	$(0, 0)$
r_{pub}	-	-	$]r_{priv}, 2r_{priv}[$	$]r_{priv}, 2r_{priv}[$	$]r_{priv}, 2r_{priv}[$
$O_{pub}(x, y)$	-	-	$Tal\ que\ R_{priv} \in R_{pub}$		
Λ	-	$[3r_{priv}, 6r_{priv}]$	-	-	-
τ	$[0, 1]$	$[0, 1]$	$[0, 1]$	$[0, 1]$	$[0, 1]$
$V(x, y)$	$([0, -10r_{priv}], 0)$		$([x_{pub}, x_{pub} - 10r_{priv}], y_{pub})$		
$P(x, y)$	$\in R_{priv}$	$\in R_{priv}$	$\in R_{priv}$	$\in R_{priv}$	$\in R_{priv}$
$d_{(\delta)}$	d_{max}	$]0, \Lambda[$	d_{max}	$]d_{max}, 2r_{priv}[$	$]d_{max}, 2r_{priv}[$

Las variaciones de los parámetros utilizados en los experimentos para los estudios de las diferentes soluciones se presentan en la Tabla 6.3. La combinación de estos rangos entrega la cantidad de experimentos realizados, los que son presentados en la última fila de la tabla, en el orden de los millones.

La métrica utilizada para comparar el desempeño de todas las soluciones es el Porcentaje de Participaciones del usuario a prueba P en el intercambio rápido de bits. Además, se presentan dos métricas adicionales; El Número de Refinamientos y el Area Promedio Refinada. Estas son definidas a continuación.

- Porcentaje de Participaciones : Número de participaciones de P en el intercambio rápido de bits sobre el número de experimentos.
- Número de Refinamientos : Número de experimentos en que hay refinamientos sobre el número de participaciones de P en el intercambio rápido de bits.
- Area Promedio Refinada : Area refinada sobre el número de participaciones de P en el intercambio rápido de bits sobre el área de encubrimiento privada.

Por costo computacional, el estudio del desempeño de la solución SBMDcDRE solo ha incluido el efecto del segundo refinamiento, mencionado en la Sección 3.3, para la determinación de la participación completa en el protocolo, no se ha incluido en la determinación de la región de encubrimiento refinada R_F. Por lo mencionado, los resultados para esta solución son sólo presentados como datos referenciales y no se profundiza en ellos.

Tabla 6.3: Variaciones de los parámetros utilizados en los experimentos.

Parámetro	Rango de Variación				
	SBMD	SBIR	SBMDcDRE	SBIRcDRE	SBIRcDREyE
r_{priv}	1	1	1	1	1
$O_{priv}(x, y)$	1	1	1	1	1
r_{pub}	-	-	10	10	10
$O_{pub}(x, y)$	-	-	1 000	1 000	1 000
Λ	-	10	-	-	-
τ	100	100	10	10	10
$V(x, y)$	1 000	1 000	100	100	100
$P(x, y)$	10 000	1 000	1 000	1 000	1 000
$d_{(\delta)}$	1	10	1	10	10
Experimentos $[10^6]$	1 000	1 000	1 000	10 000	10 000

6.3. Resultados del Estudio de las Soluciones

Los resultados del estudio computacional de desempeño de las cinco soluciones analizadas se presentan en las Tablas del Anexo A, en este se encuentran dos tipos de tablas por solución estudiada; una de ellas presenta las métricas Porcentaje de Participaciones y Número de Refinamientos, la otra presenta la métrica Area Promedio Refinada. Como ejemplo de estas se presenta la Tabla 6.4, en esta se entregan los resultados de la solución SBIRcDREyE.

En los dos tipos de Tablas del Anexo A se incluyen alguno de los siguientes parámetros;

- La razón entre los radios de las regiones de encubrimiento pública y privada, r_{pub}/r_{priv}.
- Cantidad de experimentos, que es la cantidad de combinaciones de diferentes valores de los parámetros que se involucran en cada solución propuesta estudiada.
- Cantidad de participaciones del usuario a prueba P en todo el protocolo DBPALP.
- El porcentaje de las participaciones del usuario a prueba P en todo el protocolo DBPALP, porcentaje de la cantidad de participaciones sobre la cantidad de experimentos.
- Cantidad de refinamientos del área de encubrimiento en los experimentos realizados.
- El porcentaje de los refinamientos, porcentaje de la cantidad de participaciones en las cuales hubo refinamiento sobre la cantidad de experimentos.
- El área promedio refinada en los experimentos realizados.

Los resultados del estudio computacional de las cinco soluciones analizadas, presentados en las Tablas del Anexo A, se grafican en las Figuras 6.1, 6.2 y 6.3. En estas se presentan; los porcentajes de participación en función de la razón de los radios de las regiones de encubrimiento pública

Tabla 6.4: Resultados del estudio de desempeño por Montecarlo de la solución SBIRcDREyE.

Razón	Experimentos	Participaciones		Refinamientos	
rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]
1.909091	10 000 000 000	10 000 000 000	100,00	0	0,00
1.818182	10 000 000 000	10 000 000 000	100,00	0	0,00
1.727273	10 000 000 000	10 000 000 000	100,00	0	0,00
1.636364	10 000 000 000	9 999 907 874	100,00	0	0,00
1.545455	10 000 000 000	9 983 245 678	99,83	12 042 772	0,12
1.454545	10 000 000 000	9 881 088 116	98,81	137 133 090	1,37
1.363636	10 000 000 000	9 410 917 072	94,11	595 713 117	5,96
1.272727	10 000 000 000	8 054 597 437	80,55	1 355 431 596	13,55
1.181818	10 000 000 000	6 182 387 327	61,82	1 988 612 451	19,89
1.090909	10 000 000 000	4 148 455 784	41,48	2 363 058 223	23,63

y privada en la Figura 6.1, los porcentajes de refinamiento sobre el número de participaciones en función de la razón de los radios de las regiones de encubrimiento pública y privada en la Figura 6.2, y las áreas promedio refinadas en función de la razón de los radios de las regiones de encubrimiento pública y privada en la Figura 6.3.

6.4. Análisis de los Resultados

La solución SBMD sólo tiene una razón de radios (r_{pub}/r_{priv}) igual a uno ya que no poseen región de encubrimiento pública. Esta solución muestra un mal desempeño global, presentando una baja participación en el DBP como parte del protocolo DBPALP, 26.48 % como se puede observar en la Figura 6.1, y una presencia de refinamiento de 100 % de los casos en que participa en el DBP, Figura 6.2.

La solución SBIR se presenta en función de la relación del límite superior del intervalo de selección del retardo, Λ, con la razón de radios (r_{pub}/r_{priv}). Esta solución presenta el peor resultado de participación, 12.9 % como se puede observar en la Figura 6.1, esto ocurre debido a que la peor situación de refinamiento se da en los extremos del intervalo de retardos posibles y en las condiciones del estudio los extremos se encuentran relativamente cercanos. En cuanto a la presencia de refinamiento, lo cual se puede observar en la Figura 6.2, no presenta un mejor desempeño promedio que la solución SBIRcDRE y un peor desempeño general que la solución SBIRcDREyE, 61.5 % al 25.6 % de refinamiento.

La solución SBIRcDRE presenta un mejor desempeño en la participación en el protocolo DBPALP que las dos soluciones anteriores, 32.9 % a 97.7 % como se puede observar en la Figura 6.1. En las peores condiciones de operación, razón de radios igual a la unidad, su comportamiento converge a las prestaciones de la solución SBMD. Esto es de esperar, ya que se dispondría de dos regiones de encubrimiento idénticas. En cuanto a la presencia de refinamiento,

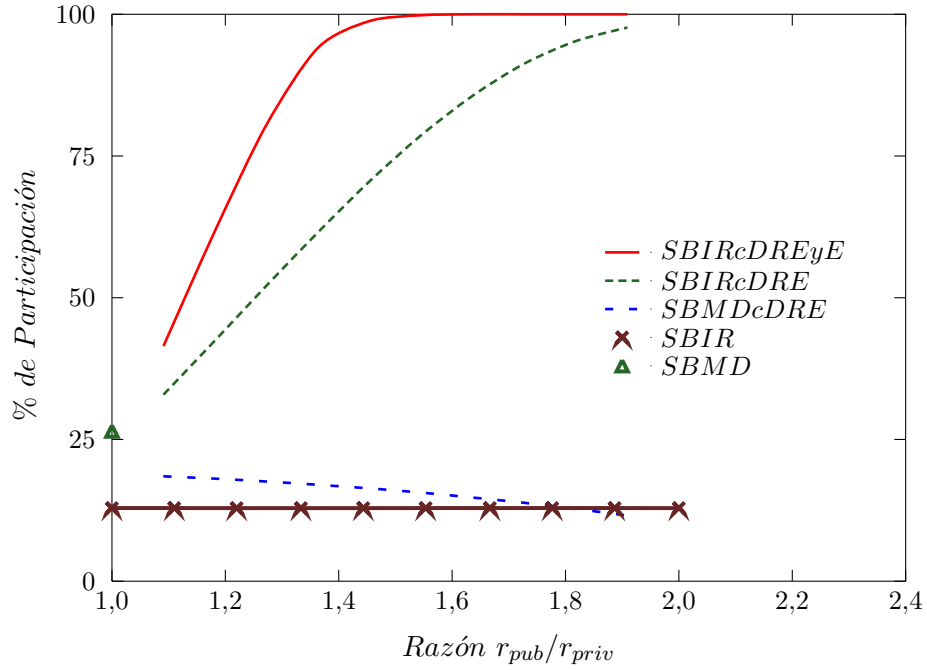


Figura 6.1: Gráfica de la participación completa en el protocolo DBPALP, por parte de los usuarios, del estudio de desempeño por Montecarlo de las soluciones.

Figura 6.2, sólo presenta un mejor desempeño general que la solución SBMD, pero en las condiciones de operación en que la razón de radios se aproxima a dos también llega a presentar mejores condiciones que la solución SBIR, 89.4 % al 3 % de refinamiento.

La solución SBIRcDREyE presenta el mejor desempeño en la participación en el protocolo DBPALP, 41.5 % a 100 % como se puede observar en la Figura 6.1. En las condiciones de operación en que la razón de radios es mayor o igual a $\sqrt{2}$; la participación es cercana, si no igual, al 100 %. Esto es congruente con lo demostrado en la Sección 3.4, donde se demuestra que no habrá refinamiento si $r_{pub} > 2r_{priv}$. En las peores condiciones de operación, razón de radios igual a la unidad, su comportamiento converge a las prestaciones de la solución SBMD. Esto es de esperar, ya que se dispondría de dos regiones de encubrimiento idénticas. En cuanto a la presencia de refinamiento, Figura 6.2, también presenta el mejor desempeño general, 57 % al 0 % de refinamiento. Y, al igual que para su desempeño de participación, en las peores condiciones de operación su comportamiento converge a las prestaciones de la solución SBMD.

6.5. Estudio de Casos Particulares

El estudio computacional de casos particulares de las soluciones propuestas tiene las mismas bases que el estudio computacional anterior, Sección 6.1. En este estudio de casos particulares se realiza el análisis de las soluciones para variaciones específicas de algunos de los parámetros de las soluciones.

Las soluciones estudiadas, ya presentadas en el Capítulo 3, son las siguientes;

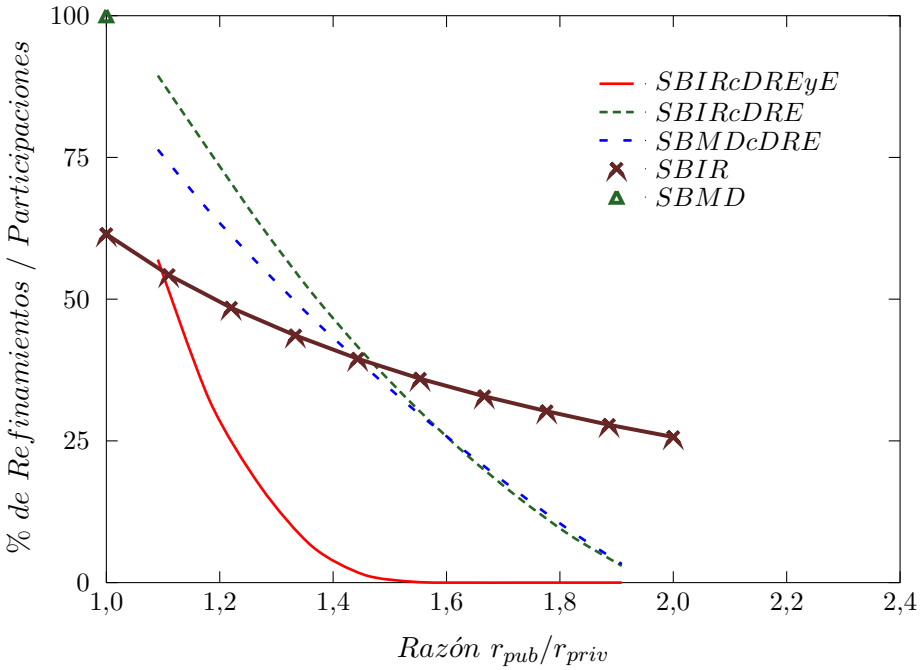


Figura 6.2: Gráfica del número de refinamientos sobre el número de participaciones en el protocolo DBPALP, del estudio de desempeño por Montecarlo de las soluciones.

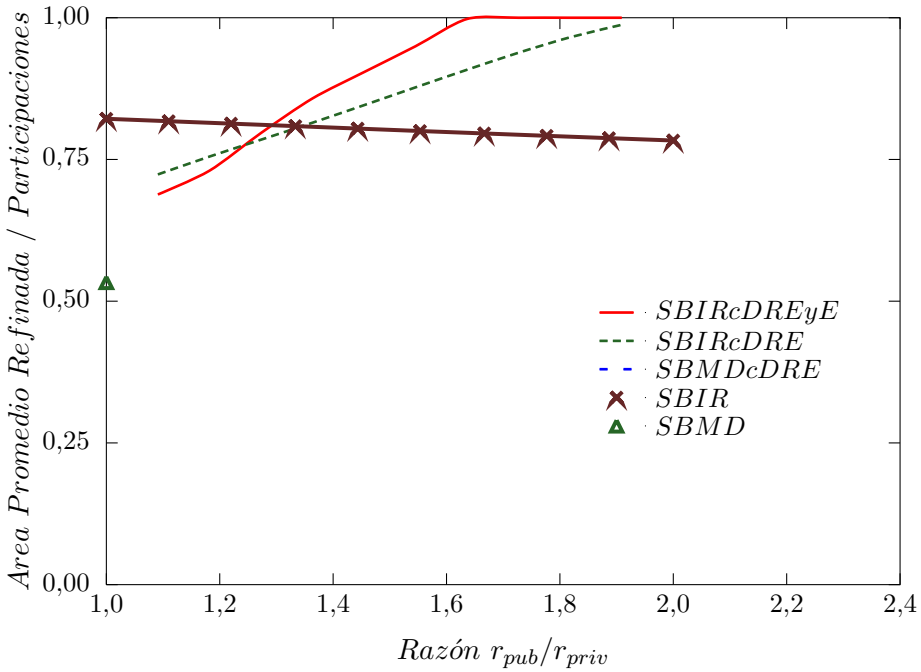


Figura 6.3: Gráfica del área promedio refinada sobre el número de participaciones en el protocolo DBPALP, del estudio de desempeño por Montecarlo de las soluciones.

- SBMD ; Solución en Base a un retardo igual a la Máxima Distancia.
- SBIR ; Solución en Base a un Intervalo de Retardos posibles.
- SBIRcDRE ; Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento.
- SBIRcDREyE ; Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento y uso de Entropía.

Al igual que en el estudio previo, los parámetros utilizados en los experimentos son aquellos que están presentes en al menos una de las soluciones propuestas para lograr un DBPALP. Estos son los siguientes;

- r_{priv} ; radio de la región de encubrimiento privada.
- $O_{priv}(x, y)$; centro de la región de encubrimiento privada.
- r_{pub} ; radio de la región de encubrimiento pública.
- $O_{pub}(x, y)$; centro de la región de encubrimiento pública.
- Λ ; límite superior de intervalo de tiempos donde se selecciona el retardo δ.
- τ ; factor de tolerancia aceptado por P para el refinamiento.
- $V(x, y)$; posición del usuario verificador V.
- $P(x, y)$; posición del usuario a prueba P.
- $d_{(\delta)}$; distancia recorrida en el retardo δ.

Los parámetros utilizados en los experimentos y sus rangos de variación son los mismos que en el estudio anterior y están presentados en la Tabla 6.2. Los parámetros estudiados como casos particulares y las variaciones específicas de estos se presentan en la Tabla 6.5

Tabla 6.5: Parámetros variados en el estudio de Casos Particulares y sus variaciones específicas.

Parámetro	Rango de Variación			
τ	25 %	250 %	75 %	
Distancia entre V y O_{pub}	0.5 r_{pub}	r_{pub}	2 r_{pub}	3 r_{pub}

El experimento computacional del desempeño de las soluciones determina el promedio de cada métrica evaluadora, para un número de experimentos que permiten la convergencia de este. Los parámetros no fijados para este estudio involucrados en las soluciones son determinados seudoaleatoriamente.

Las métricas utilizadas para comparar el desempeño de todas las soluciones son; Porcentaje de Participaciones del usuario a prueba P en el intercambio rápido de bits, el Número de Refinamientos y el Area Promedio Refinada. Ya presentadas enla Sección 6.2.

6.5.1. Resultados del Estudio Particular de las Soluciones

Los resultados del estudio computacional de desempeño de las cuatro soluciones analizadas se presentan en las Tablas del Anexo B. En este se encuentran las tablas con los resultados de las variaciones específicas de τ, Tablas B.1 a la B.4, y las tablas con los resultados de las variaciones de la posición del usuario V con respecto al centro O_{pub} de la región R_{pub}, Tablas B.5 a la B.8. Los gráficos de este estudio se presentan en el Anexo C.

En los dos tipos de Tablas del Anexo B se incluyen alguno de los siguientes parámetros;

- El Factor de Tolerancia τ.
- La distancia entra el usuario V y el centro O_{pub} de la región R_{pub}.
- La razón entre los radios de las regiones de encubrimiento pública y privada, r_{pub}/r_{priv}.
- Cantidad de experimentos, que es la cantidad de combinaciones de diferentes valores de los parámetros que se involucran en cada solución propuesta estudiada.
- Cantidad de participaciones del usuario a prueba P en todo el protocolo DBPALP.
- El porcentaje de las participaciones del usuario a prueba P en todo el protocolo DBPALP, porcentaje de la cantidad de participaciones sobre la cantidad de experimentos.
- Cantidad de refinamientos del área de encubrimiento en los experimentos realizados.
- El porcentaje de los refinamientos, porcentaje de la cantidad de participaciones en las cuales hubo refinamiento sobre la cantidad de experimentos.
- El área promedio refinada en los experimentos realizados.

Como ejemplo de estas, a continuación las Tablas 6.6 y 6.7, en estas se presentan los resultados de la solución SBIRcDREyE.

6.5.2. Análisis de los Resultados del Estudio Particular

Los resultados del estudio particular se muestran congruentes con los resultados del estudio de desempeño de las soluciones, las soluciones SBIRcDRE y SBIRcDREyE se muestran notoriamente mejores que las soluciones SBMD y SBIR. En particular la solución SBIRcDREyE se muestra mejor que todas las soluciones estudiadas.

En relación a las soluciones SBMD y SBIR; es de destacar el mal desempeño que presentan al tener un factor de tolerancia τ exigente, es decir, cercano a uno.

Tabla 6.6: Resultados del estudio de desempeño con variación del factor de tolerancia de SBIRcDREyE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento y uso de Entropía).

Factor de	Razón	Experimentos	Participaciones		Refinamientos		Area Promedio
Tolerancia	rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]	Refinada
0.25	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
0.25	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
0.25	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
0.25	1.636364	10 000 000	10 000 000	100.00	0	0.00	1.00
0.25	1.545455	10 000 000	10 000 000	100.00	6 639	0.07	0.954314
0.25	1.454545	10 000 000	10 000 000	100.00	159 848	1,.60	0.905329
0.25	1.363636	10 000 000	10 000 000	100.00	695 519	6.95	0.852976
0.25	1.272727	10 000 000	10 000 000	100.00	2 047 977	20.48	0.772209
0.25	1.181818	10 000 000	9720316	97.20	3 668 005	36.68	0.700324
0.25	1.090909	10 000 000	6626497	66.26	3 876 003	38.76	0.700739
0.5	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
0.5	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
0.5	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
0.5	1.636364	10 000 000	10 000 000	100.00	0	0.00	1.00
0.5	1.545455	10 000 000	10 000 000	100.00	14 220	0.14	0.951884
0.5	1.454545	10 000 000	10 000 000	100.00	128 853	1.29	0.912417
0.5	1.363636	10 000 000	9 902 409	99.02	790 971	7.91	0.843967
0.5	1.272727	10 000 000	9 235 021	92.35	1 663 004	16.63	0.803267
0.5	1.181818	10 000 000	9 720 316	63.72	1 931 024	19.31	0.787855
0.5	1.090909	10 000 000	6 626 497	31.30	1 630 020	16.30	0.804220
0.75	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
0.75	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
0.75	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
0.75	1.636364	10 000 000	10 000 000	100.00	0	0.00	1.00
0.75	1.545455	10 000 000	10 000 000	100.00	12205	0.12	0.946094
0.75	1.454545	10 000 000	9 877 586	98.77	137 075	1.37	0.908676
0.75	1.363636	10 000 000	9 422 623	94.22	537 348	5.37	0.875988
0.75	1.272727	10 000 000	6 165 688	61.65	696 070	6.96	0.876133
0.75	1.181818	10 000 000	3 209 193	32.09	586 605	5.86	0.889033
0.75	1.090909	10 000 000	1 080 564	10.80	381 210	3.81	0.901514

Tabla 6.7: Resultados del estudio de desempeño con variación de la distancia entre V y P de SBIRcDREyE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento y uso de Entropía).

Distancia entre V y P	Razón rpub/rpriv	Experimentos Cantidad	Participaciones Cantidad	[%]	Refinamientos Cantidad	[%]	Area Promedio Refinada
0.5 r_{pub}	1.909091	10 000 000	10 00 0000	100.00	0	0.0	1.00
0.5 r_{pub}	1.818182	10 000 000	10 000 000	100.00	0	0.0	1.00
0.5 r_{pub}	1.727273	10 000 000	10 000 000	100.00	0	0.0	1.00
0.5 r_{pub}	1.636364	10 000 000	10 000 000	100.00	0	0.0	1.00
0.5 r_{pub}	1.545455	10 000 000	9 988 800	99.88	0	0.0	1.00
0.5 r_{pub}	1.454545	10 000 000	9 842 070	98.42	2 482	0.02	0.966180
0.5 r_{pub}	1.363636	10 000 000	9 376 263	93.76	104 229	1.04	0.913340
0.5 r_{pub}	1.272727	10 000 000	8 060 308	80.60	574 232	5.74	0.847643
0.5 r_{pub}	1.181818	10 000 000	6 124 498	61.24	1 245 625	12.45	0.760252
0.5 r_{pub}	1.090909	10 000 000	4 172 476	41.72	1 599 663	15.99	0.680280
r_{pub}	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
r_{pub}	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
r_{pub}	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
r_{pub}	1.636364	10 000 000	9 999 668	99.99	0	0.00	1.00
r_{pub}	1.545455	10 000 000	9 995 126	99.95	0	0.00	0.993675
r_{pub}	1.454545	10 000 000	9 864 829	98.64	77	0.40	0.938145
r_{pub}	1.363636	10 000 000	9 397 731	93.97	40 730	3.42	0.881252
r_{pub}	1.272727	10 000 000	8 072 931	80.72	1 086 931	10.86	0.824874
r_{pub}	1.181818	10 000 000	6 083 356	60.83	1 787 955	17.87	0.751297
r_{pub}	1.090909	10 000 000	4 157 714	41.57	2 237 433	22.37	0.698924
2 r_{pub}	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
2 r_{pub}	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
2 r_{pub}	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
2 r_{pub}	1.636364	10 000 000	9 999 893	99.99	0	0.00	1.00
2 r_{pub}	1.545455	10 000 000	9 981 972	99.81	5 116	0.05	0.964569
2 r_{pub}	1.454545	10 000 000	9 902 504	99.02	85 857	0.85	0.917221
2 r_{pub}	1.363636	10 000 000	9 447 135	94.47	505 303	5.05	0.867922
2 r_{pub}	1.272727	10 000 000	8 088 944	80.88	1 318 775	13.18	0.808903
2 r_{pub}	1.181818	10 000 000	6 163 545	61.63	2 029 643	20.29	0.738812
2 r_{pub}	1.090909	10 000 000	4 124 438	41.24	2 423 219	24.23	0.688761
3 r_{pub}	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
3 r_{pub}	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
3 r_{pub}	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
3 r_{pub}	1.636364	10 000 000	10 000 000	100.00	0	0.00	1.00
3 r_{pub}	1.545455	10 000 000	9 984 455	99.84	10 791	0.10	0.954038
3 r_{pub}	1.454545	10 000 000	9 878 952	98.78	128 220	1.28	0.908643
3 r_{pub}	1.363636	10 000 000	9 328 763	93.28	599 357	5.99	0.856337
3 r_{pub}	1.272727	10 000 000	7 932 587	79.32	1 428 476	14.28	0.793921
3 r_{pub}	1.181818	10 000 000	6 205 871	62.05	2 071 275	20.71	0.734761
3 r_{pub}	1.090909	10 000 000	4 156 474	41.56	2 440 264	24.40	0.688414

Conclusiones

Esta investigación se ha enfocado en el estudio de las bases para definir un protocolo delimitador de distancia consciente de la privacidad de ubicación (DBPALP, Distance Bounding Protocol Aware of Location Privacy). Además de la formalización del problema, los aspectos básicos relevantes para la implementación del protocolo son los procedimientos por los cuales el usuario verificador V puede verificar que el usuario a prueba P se encuentra dentro de la región de encubrimiento declarada por este último; el ataque de ajuste del área de cobertura de transmisión y el ataque de delimitación de distancia.

El cumplimiento de los objetivos propuestos al iniciar esta investigación se describe a continuación.

- Se ha desarrollado un protocolo de delimitación de distancia que permite crear una región de encubrimiento protegida frente a refinamientos por ajuste del área de cobertura y por delimitación de distancia entre un usuario a prueba P estático y un usuario verificador V estático. Este protocolo cumple con las condiciones de estudio impuestas para el refinamiento por delimitación de distancia, pero se han modificado las condiciones de estudio para desarrollar la verificación por área de cobertura.

- No se han desarrollado protocolos de delimitación de distancia que permitan crear una región de encubrimiento protegida frente a refinamientos por ajuste del área de cobertura y por delimitación de distancia para las siguientes características de usuarios; entre un usuario a prueba P estático y un usuario verificador V móvil, entre un usuario a prueba P móvil y un usuario verificador V estático y entre un usuario a prueba P móvil y un usuario verificador V móvil.

- Se ha desarrollado un estudio computacional, basado en el método de Montecarlo, para estudiar el desempeño del protocolo con ambos usuarios estáticos. La solución propuesta se ha mostrado bastante robusta en un rango bastante amplio de sus parámetros y bastante superior a las demás soluciones estudiadas.

- No se han modificado los protocolos desarrollados, considerando que el usuario a prueba P actúa honestamente, para minimizar la posibilidad que el usuario a prueba P trate de validar una ubicación falsa, por disponibilidad de tiempo.

Los principales aportes de los estudios realizados en esta investigación se describe a continuación.

- Se ha formalizado el problema para implementar un protocolo de delimitación de distancia, que minimice la probabilidad que la región de encubrimiento de un usuario a prueba (P) sea refinada, más allá que un factor de tolerancia τ impuesto por P, por un atacante o usuario verificador (V), frente a un ataque basado en la delimitación de la distancia o un ataque basado en el ajuste del área de cobertura.
- Se ha estudiado el ataque basado en la delimitación de la distancia y propuesto una solución para implementar un protocolo de delimitación de distancia, que minimice la probabilidad que la región de encubrimiento de un usuario a prueba (P) estático sea refinada, más allá que un factor de tolerancia τ impuesto por P, cuando el atacante o usuario verificador (V) es estático.
- Se han definido dos métricas, relacionadas con el área de la región de encubrimiento, que permiten al usuario a prueba (P) asegurar que sus condiciones mínimas impuestas para participar de un protocolo de delimitación de distancia se cumplan si este participa, en forma completa, de dicho protocolo. Una de ellas basada en el área de la región de encubrimiento privada y otra basada en la entropía de la región de encubrimiento privada.
- Se ha estudiado el ataque basado en el ajuste del área de cobertura y se ha determinado la imposibilidad de presentar una solución para implementar un protocolo de delimitación de distancia, bajo las condiciones de estudio propuestas, que minimice la probabilidad que la región de encubrimiento de un usuario a prueba (P) estático sea refinada cuando el atacante o usuario verificador (V) es estático.
- Se ha propuesto un protocolo de verificación de ubicación que minimiza la probabilidad que la región de encubrimiento de un usuario a prueba (P) estático sea refinada, más allá que un factor de tolerancia τ impuesto por P, cuando el atacante o usuario verificador (V) es estático, bajo condiciones de estudio modificadas.

Trabajos Futuros

Los trabajos futuros relacionados con el tema de esta investigación se presentan a continuación.

- Se ha desarrollado un algoritmo de delimitación de distancia que permite crear una región de encubrimiento protegida frente a refinamientos por ajuste del área de cobertura y por delimitación de distancia entre un usuario a prueba P estático y un usuario verificador V estático, en el cual se considera un factor de tolerancia que determina si el usuario a prueba P continua con el protocolo o lo abandona. Sería de interés el estudio del protocolo sin la condición de término del factor de tolerancia.
- Desarrollar el estudio del protocolo de delimitación de distancia que permita crear una región de encubrimiento protegida frente a refinamientos por ajuste del área de cobertura y por delimitación de distancia entre un usuario a prueba P estático y un usuario verificador V móvil.

- Desarrollar el estudio del protocolo de delimitación de distancia que permita crear una región de encubrimiento protegida frente a refinamientos por ajuste del área de cobertura y por delimitación de distancia entre un usuario a prueba P móvil y un usuario verificador V móvil o estático.
- Desarrollar un estudio para modificar el protocolo propuesto para minimizar la posibilidad que el usuario a prueba P trate de validar una ubicación falsa.
- Desarrollar un estudio para determinar nuevas formas de obtener un delta de potencia para el protocolo de delimitación de distancia desarrollado que permite crear una región de encubrimiento protegida frente a refinamientos por ajuste del área de cobertura entre un usuario a prueba P estático y un usuario verificador V estático.
- Desarrollar un estudio sobre la utilización del protocolo propuesto en los diferentes escenarios que han llevado a las modificaciones, en aras de enfrentar diferentes ataques, del protocolo original de delimitación de distancia.

Bibliografía

[1] A. Abu-Mahfouz y G. P. Hancke. Distance bounding: A practical security solution for real-time location systems. *IEEE transactions on industrial informatics*, 9(1):92–102, 2013.

[2] Osama Abumansoor y Azzedine Boukerche. A secure cooperative approach for nonline-of-sight location verification in vanet. *Vehicular Technology, IEEE Transactions on*, 61(1):275–285, 2012.

[3] G. Avoine, S. Mauw, y R. Trujillo-Rasua. Comparing distance bounding protocols: A critical mission supported by decision theory. *Computer Communications*, 67:92–102, 2015.

[4] Mihir Bellare y Phillip Rogaway. Entity authentication and key distribution. En *Advances in Cryptology—CRYPTO'93*, págs. 232–249. Springer, 1994.

[5] Ahmed Benfarah, Benoit Miscopein, Jean-Marie Gorce, Cédric Lauradoux, y Bernard Roux. Distance bounding protocols on th-uwb radios. En *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, págs. 1–6. IEEE, 2010.

[6] Chatschik Bisdikian, Jim Christensen, John Davis II, Maria R Ebling, Guerney Hunt, William Jerome, Hui Lei, Stéphane Maes, y Daby Sow. Enabling location-based applications. En *Proceedings of the 1st international workshop on Mobile commerce*, págs. 38–42. ACM, 2001.

[7] Stefan Brands y David Chaum. Distance-bounding protocols. En *Advances in Cryptology—EUROCRYPT'93*, págs. 344–359. Springer, 1994.

[8] Srdjan Čapkun, Levente Buttyán, y Jean-Pierre Hubaux. Sector: secure tracking of node encounters in multi-hop wireless networks. En *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, págs. 21–32. ACM, 2003.

[9] Srdjan Čapkun y Jean-pierre Hubaux. Secure positioning in wireless networks. En *IEEE Journal on Selected Areas in Communications*. Citeseer, 2006.

[10] Srdjan Capkun, Kasper Bonne Rasmussen, Mario Cagalj, y Mani Srivastava. Secure location verification with hidden and mobile base stations. *Mobile Computing, IEEE Transactions on*, 7(4):470–483, 2008.

[11] Jerry T Chiang, Jason J Haas, y Yih-Chun Hu. Secure and precise location verification using distance bounding and simultaneous multilateration. En *Proceedings of the second ACM conference on Wireless network security*, págs. 181–192. ACM, 2009.

[12] Chi-Yin Chow y Mohamed F Mokbel. Enabling private continuous queries for revealed user locations. En *Advances in Spatial and Temporal Databases*, págs. 258–275. Springer, 2007.

[13] Chi-Yin Chow, Mohamed F Mokbel, y Xuan Liu. A peer-to-peer spatial cloaking algorithm for anonymous location-based service. En *Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems*, págs. 171–178. ACM, 2006.

[14] Cas Cremers, Kasper B Rasmussen, Benedikt Schmidt, y Srdjan Capkun. Distance hijacking attacks on distance bounding protocols. En *Security and Privacy (SP), 2012 IEEE Symposium on*, págs. 113–127. IEEE, 2012.

[15] Patricio Galdames y Ying Cai. Efficient processing of location-cloaked queries. En *INFOCOM, 2012 Proceedings IEEE*, págs. 2480–2488. IEEE, 2012.

[16] Sébastien Gambs, Cristina Onete, y Jean-Marc Robert. Prover anonymous and deniable distance-bounding authentication. En *Proceedings of the 9th ACM symposium on Information, computer and communications security*, págs. 501–506. ACM, 2014.

[17] Gabriel Ghinita, Panos Kalnis, y Spiros Skiadopoulos. Mobihide: a mobilea peer-to-peer system for anonymous location-based queries. En *Advances in Spatial and Temporal Databases*, págs. 221–238. Springer, 2007.

[18] Gabriel Ghinita, Panos Kalnis, y Spiros Skiadopoulos. Prive: anonymous location-based queries in distributed mobile systems. En *Proceedings of the 16th international conference on World Wide Web*, págs. 371–380. ACM, 2007.

[19] Joshua D Guttman, F Javier Thayer, y Lenore D Zuck. The faithfulness of abstract protocol analysis: Message authentication. En *Proceedings of the 8th ACM Conference on Computer and Communications Security*, págs. 186–195. ACM, 2001.

[20] Gerhard P Hancke y Markus G Kuhn. An rfid distance bounding protocol. En *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, págs. 67–73. IEEE, 2005.

[21] Andy Harter, Andy Hopper, Pete Steggles, Andy Ward, y Paul Webster. The anatomy of a context-aware application. *Wireless Networks*, 8(2/3):187–197, 2002.

[22] Haibo Hu y Jianliang Xu. Non-exposure location anonymity. En *Data Engineering, 2009. ICDE'09. IEEE 25th International Conference on*, págs. 1120–1131. IEEE, 2009.

[23] Leping Huang, Kanta Matsuura, Hiroshi Yamane, y Kaoru Sezaki. Enhancing wireless location privacy using silent period. En *Wireless Communications and Networking Conference, 2005 IEEE*, tomo 2, págs. 1187–1192. IEEE, 2005.

[24] David B Johnson y David A Maltz. Dynamic source routing in ad hoc wireless networks. En *Mobile computing*, págs. 153–181. Springer, 1996.

[25] Rui Jose y Nigel Davies. Scalable and flexible location-based services for ubiquitous information access. En *Handheld and Ubiquitous Computing*, págs. 52–66. Springer, 1999.

[26] Brad Karp y Hsiang-Tsung Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. En *Proceedings of the 6th annual international conference on Mobile computing and networking*, págs. 243–254. ACM, 2000.

[27] Chong Hee Kim y Gildas Avoine. Rfid distance bounding protocol with mixed challenges to prevent relay attacks. En *Cryptology and Network Security*, págs. 119–133. Springer, 2009.

[28] Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, y Olivier Pereira. The swiss-knife rfid distance bounding protocol. En *Information Security and Cryptology–ICISC 2008*, págs. 98–115. Springer, 2009.

[29] Young-Bae Ko y Nitin H Vaidya. Location-aided routing (lar) in mobile ad hoc networks. *Wireless Networks*, 6(4):307–321, 2000.

[30] Fuyu Liu, Georgiana Hamza-Lup, Kien Hua, et al. Using broadcast to protect user privacy in location-based applications. En *GLOBECOM Workshops (GC Wkshps), 2010 IEEE*, págs. 1561–1565. IEEE, 2010.

[31] Aikaterini Mitrokotsa, Christos Dimitrakakis, Pedro Peris-Lopez, y Julio C Hernandez-Castro. Distance bounding protocol and mafia fraud attacks over noisy channels. *Communications Letters, IEEE*, 14(2):121–123, 2010.

[32] Jorge Munilla y Alberto Peinado. Distance bounding protocols for rfid enhanced by using void-challenges and analysis in noisy channels. *Wireless communications and mobile computing*, 8(9):1227–1232, 2008.

[33] Ventzislav Nikov y Marc Vauclair. Yet another secure distance-bounding protocol. *IACR Cryptology ePrint Archive*, 2008:319, 2008.

[34] Guangyu Pei, Mario Gerla, y Tsu-Wei Chen. Fisheye state routing: A routing scheme for ad hoc wireless networks. En *Communications, 2000. ICC 2000. 2000 IEEE International Conference on*, tomo 1, págs. 70–74. IEEE, 2000.

[35] Charles E Perkins y Elizabeth M Royer. Ad-hoc on-demand distance vector routing. En *Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications*, pág. 90. IEEE Computer Society, 1999.

[36] Aanjhan Ranganathan, Boris Danev, y Srdjan Capkun. Low-power distance bounding. *arXiv preprint arXiv:1404.4435*, 2014.

[37] Kasper Bonne Rasmussen y Srdjan Čapkun. Location privacy of distance bounding protocols. En *Proceedings of the 15th ACM conference on Computer and communications security*, págs. 149–160. ACM, 2008.

[38] Kasper Bonne Rasmussen y Srdjan Capkun. Realization of rf distance bounding. En *USENIX Security Symposium*, págs. 389–402. 2010.

[39] Jason Reid, Juan M Gonzalez Nieto, Tee Tang, y Bouchra Senadji. Detecting relay attacks with timing-based protocols. En *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, págs. 204–213. ACM, 2007.

[40] Elizabeth M Royer y Charles E Perkins. Multicast operation of the ad-hoc on-demand distance vector routing protocol. En *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, págs. 207–218. ACM, 1999.

[41] Naveen Sastry, Umesh Shankar, y David Wagner. Secure verification of location claims. En *Proceedings of the 2nd ACM workshop on Wireless security*, págs. 1–10. ACM, 2003.

[42] Dave Singelee y Bart Preneel. Location verification using secure distance bounding protocols. En *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*, págs. 7–pp. IEEE, 2005.

[43] Dave Singelée y Bart Preneel. Distance bounding in noisy environments. En *Security and Privacy in Ad-hoc and Sensor Networks*, págs. 101–115. Springer, 2007.

[44] Mike Spreitzer y Marvin Theimer. Providing location information in a ubiquitous computing environment (panel session). ., 27(5), 1994.

[45] N. O. Tippenhauer, H. Luecken, M. Kuhn, y S. Capkun. Uwb rapid-bit-exchange system for distance bounding. *Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2015, June.

[46] Rolando Trujillo-Rasua, Benjamin Martin, y Gildas Avoine. The poulidor distance-bounding protocol. En *Radio Frequency Identification: Security and Privacy Issues*, págs. 239–257. Springer, 2010.

[47] Rolando Trujillo-Rasua, Benoit Martin, y Gildas Avoine. Distance bounding facing both mafia and distance frauds. *Wireless Communications, IEEE Transactions on*, 13(10):5690–5698, 2014.

[48] Yu-Ju Tu y Selwyn Piramuthu. Rfid distance bounding protocols. En *First International EURASIP Workshop on RFID Technology*, págs. 67–68. Citeseer, 2007.

[49] Adnan Vora y Mikhail Nesterenko. Secure location verification using radio broadcast. *Dependable and Secure Computing, IEEE Transactions on*, 3(4):377–385, 2006.

[50] Tao Xu y Ying Cai. Exploring historical location data for anonymity preservation in location-based services. En *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.

[51] Toby Xu y Ying Cai. Location anonymity in continuous location-based services. En *Proceedings of the 15th annual ACM international symposium on Advances in geographic information systems*, pág. 39. ACM, 2007.

[52] Toby Xu y Ying Cai. Feeling-based location privacy protection for location-based services. En *Proceedings of the 16th ACM conference on Computer and communications security*, págs. 348–357. ACM, 2009.

[53] Toby Xu y Ying Cai. Location cloaking for safety protection of ad hoc networks. En *INFOCOM 2009, IEEE*, págs. 1944–1952. IEEE, 2009.

[54] Toby Xu y Ying Cai. Lsr: A location secure routing protocol for ad hoc networks. En *Mobile Adhoc and Sensor Systems (MASS), 2010 IEEE 7th International Conference on*, págs. 176–185. IEEE, 2010.

Glosario

***Area Refinada* :** Area incluida en el área de una región de encubrimiento, resultante de un proceso de refinamiento, en la cual el usuario verificador V no puede negar la presencia del usuario a Prueba P.

***Ataque Basado en el Ajuste del Area de Cobertura* :** El Ataque Basado en el ajuste del Area de Cobertura ($ABAC$) es un ataque que tiene como base el ataque de ajuste de área de cobertura al cual se le adiciona una característica adicional, que permite un ataque más profundo, basada en información del protocolo utilizado.

***Ataque Basado en la Delimitación de la Distancia* :** El Ataque Basado en la dElimitación de la Distancia ($ABED$) es un ataque que tiene como base el ataque de delimitación de la distancia al cual se le adiciona una característica adicional, que permite un ataque más profundo, basada en información del protocolo utilizado.

***Corona Circular del Ataque* :** Es la región donde un ataque basado en la delimitación de la distancia, que considera informaci[on adicional como parte incremental del ataque, determina que el usuario a prueba P se puede encontrar. Esta región, en general, tiene la forma de una corona circular con centro en el usuario verificador V.

***Cota Util* :** Rango de distancia, entregado por el usuario verificador V al usuario a prueba P, que restrige las dimensiones de una región de encubrimiento. Es dependiente de la utilida de la distancia para V. En esta investigación se traduce en el radio de una circunferencia con centro en el centro de la región de encubrimiento declarada por P.

***Entropía de una Región* :** La entropía de una región R, $H(R)$, es el valor medio ponderado de la cantidad de información de las diversas subregiones en las cuales se puede dividir la región R. $H(R) = -\sum p(x_i) \log_k p(x_i)$.

***Método de Montecarlo* :** Los métodos de Montecarlo (o experimentos de Montecarlo) son una clase de algoritmos computacionales que se basan en el muestreo aleatorio repetitivo para obtener resultados numéricos. Su idea esencial es utilizar la aleatoriedad para resolver problemas que pueden ser deterministas.

***Privacidad* :** La privacidad es la habilidad de un individuo o grupo para aislar la información sobre sí mismos, y por lo tanto expresarse de manera selectiva. El dominio de la privacidad parcialmente se superpone a la seguridad (confidencialidad), que puede incluir los conceptos de uso adecuado, así como la protección de la información.

Refinamiento **:** Proceso por el cual un usuario verificador V determina que un ususario a prueba P no se encuentra en parte de una región de encubrimiento.

Región de Encubrimiento **:** Región en la cual se encuentra el usuario a prueba, P, y cumple con las características deseadas por P que difuminan su ubicación dentro de esta región.

Región de Encubrimiento Privada **:** Región de encubrimiento que se encuentra incorporada en una región de encubrimiento pública. Esta es conocida por el usuario a prueba P y desconocida por el usuario verificador V.

Región de Encubrimiento Pública **:** Región de encubrimiento que es entregada por el usuario a prueba, P, al usuario verificador, V, para participar en un protocolo delimitador de distancia consciente de la privacidad de ubicación.

Región Refinada **:** Región resultante de un proceso de refinamiento, en la cual el usuario verificador V no puede negar la presencia del usuario a Prueba P.

Seguridad **:** La seguridad es el grado de resistencia o protección contra el daño. La seguridad incluye los conceptos de protección de la información y uso adecuado de ésta (confidencialidad, integridad y disponibilidad de la informalción).

Shadowing **:** Es el fenómeno de Desvanecimiento por Sombra que se produce cuando la línea de vista se obstruye debido a los obstáculos que pueden estar en el trayecto de propagación: montañas, árboles, construcciones hechas por el hombre, etc.

Usuario a Prueba **:** El usuario a prueba P es un usuario que desea participar en un protocolo delimitador de distancia entregando una región de encubrimiento en lugar de su posición precisa.

Usuario Verificador **:** El usuario verificador V es un usuario que desea participar en un protocolo delimitador de distancia verificando que el usuario a prueba P se encuentra dentro de la región de encubrimiento declarada por este último.

Utilidad de la Distancia **:** Es el concepto referido al valor útil de la distancia que pueda estimar el usuario verificador V, en un proceso de validación de la ubicación del usuario P dentro de su región de encubrimiento. Por ejemplo, el usuario V no puede esperar un tiempo extremadamente grande la respuesta del usuario P, tampoco puede participar de un proceso cuando la región de encubrimiento se sale de su rango transmisión.

Apéndice A

Tablas de Resultados de Estudio de Desempeño

A continuación se presentan las Tablas de Resultados del estudio computacional, en base al método de Montecarlo, del desempeño de las soluciones propuestas. Estas representan el estudio sobre el protocolo propuesto en el caso de usuario a prueba P estático y usuario verificador V estático.

Las Tablas A.1 a A.9 presentan el estudio de desempaño general de las soluciones propuestas.

Tabla A.1: Resultados del estudio de desempeño por Montecarlo de SBIRcDREyE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento y uso de Entropía).

Razón	Experimentos	Participaciones		Refinamientos	
rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]
1.909091	10 000 000 000	10 000 000 000	100,00	0	0,00
1.818182	10 000 000 000	10 000 000 000	100,00	0	0,00
1.727273	10 000 000 000	10 000 000 000	100,00	0	0,00
1.636364	10 000 000 000	9 999 907 874	100,00	0	0,00
1.545455	10 000 000 000	9 983 245 678	99,83	12 042 772	0,12
1.454545	10 000 000 000	9 881 088 116	98,81	137 133 090	1,37
1.363636	10 000 000 000	9 410 917 072	94,11	595 713 117	5,96
1.272727	10 000 000 000	8 054 597 437	80,55	1 355 431 596	13,55
1.181818	10 000 000 000	6 182 387 327	61,82	1 988 612 451	19,89
1.090909	10 000 000 000	4 148 455 784	41,48	2 363 058 223	23,63

Tabla A.2: Resultados del estudio de desempeño por Montecarlo de SBIRcDRE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento).

Razón	Experimentos	Participaciones		Refinamientos	
rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]
1.909091	10 000 000 000	9 765 921 665	97,66	290 247 112	2,90
1.818182	10 000 000 000	9 527 473 100	95,27	794 441 439	7,94
1.727273	10 000 000 000	9 128 787 361	91,29	1 364 944 079	13,65
1.636364	10 000 000 000	8 563 568 813	85,64	1 923 447 112	19,23
1.545455	10 000 000 000	7 867 320 332	78,67	2 433 808 992	24,34
1.454545	10 000 000 000	7 055 101 943	70,55	2 847 821 823	28,48
1.363636	10 000 000 000	6 157 053 858	61,57	3 139 388 389	31,39
1.272727	10 000 000 000	5 215 432 861	52,15	3 284 482 290	32,84
1.181818	10 000 000 000	4 245 537 532	42,46	3 230 421 377	32,30
1.090909	10 000 000 000	3 291 374 836	32,91	2 943 173 577	29,43

Tabla A.3: Resultados del estudio de desempeño por Montecarlo de SBMDcDRE (Solución en Base a un retardo igual a la Máxima Distancia con Dos Regiones de Encubrimiento).

Razón	Experimentos	Participaciones		Refinamientos	
rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]
1.909091	1 000 000 000	115 726 217	11,57	3 843 087	0,38
1.818182	1 000 000 000	127 588 788	12,76	11 723 184	1,17
1.727273	1 000 000 000	138 295 147	13,83	21 922 565	2,19
1.636364	1 000 000 000	147 455 139	14,75	33 852 784	3,38
1.545455	1 000 000 000	156 284 390	15,63	47 322 597	4,73
1.454545	1 000 000 000	163 722 251	16,37	62 571 592	6,26
1.363636	1 000 000 000	170 013 761	17,00	79 153 501	7,92
1.272727	1 000 000 000	175 792 621	17,58	98 005 748	9,80
1.181818	1 000 000 000	180 910 552	18,09	118 396 527	11,84
1.090909	1 000 000 000	184 954 885	18,50	141 334 286	14,13

Para el análisis de la tercera solución, no se considera el segundo refinamiento.

Tabla A.4: Resultados del estudio de desempeño por Montecarlo de SBIR (Solución en Base a un Intervalo de Retardos posible).

Razón	Experimentos	Participaciones		Refinamientos	
rpub/rpriv	Cantidad (Lambda)	Cantidad	[%]	Cantidad	[%]
1 (6,00)	1 000 000 000	128 949 470	12,89	33 131 377	3,31
1 (5,66)	1 000 000 000	128 968 100	12,90	35 882 008	3,59
1 (5,33)	1 000 000 000	128 962 940	12,90	38 966 546	3,90
1 (5,00)	1 000 000 000	128 963 140	12,90	42 421 836	4,24
1 (4,66)	1 000 000 000	128 969 790	12,90	46 378 490	4,64
1 (4,33)	1 000 000 000	128 936 380	12,89	50 928 211	5,09
1 (4,00)	1 000 000 000	128 920 690	12,89	56 218 811	5,62
1 (3,66)	1 000 000 000	128 933 470	12,89	62 513 138	6,25
1 (3,33)	1 000 000 000	128 953 660	12,90	70 049 618	7,00
1 (3,00)	1 000 000 000	128 974 280	12,90	79 280 891	7,93

Tabla A.5: Resultados del estudio de desempeño por Montecarlo de SBMD (Solución en Base a un retardo igual a la Máxima Distancia).

Razón	Experimentos	Participaciones		Refinamientos	
rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]
1	1 000 000 000	264 831 906	26,48	264 831 906	26,48

Tabla A.6: Resultados del estudio de desempeño por Montecarlo de SBIRcDREyE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento y uso de Entropía), Métrica Area Promedio Refinada.

Razón	Experimentos	Participaciones		Area
rpub/rpriv	Cantidad	Cantidad	[%]	Promedio
1.909091	3 000 000 000	3 000 000 000	100,00	1.00
1.818182	3 000 000 000	3 000 000 000	100,00	1.00
1.727273	3 000 000 000	3 000 000 000	100,00	1.00
1.636364	3 000 000 000	2 999 974 599	100,00	0.997868
1.545455	3 000 000 000	2 996 004 376	99,86	0.949750
1.454545	3 000 000 000	2 967 264 116	98,91	0.904111
1.363636	3 000 000 000	2 831 109 072	94,37	0.857661
1.272727	3 000 000 000	2 421 643 437	80,72	0.796653
1.181818	3 000 000 000	1 832 915 327	61,10	0.730142
1.090909	3 000 000 000	1 248 930 784	41,63	0.688213

Tabla A.7: Resultados del estudio de desempeño por Montecarlo de SBIRcDRE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento), Métrica Area Promedio Refinada.

Razón	Experimentos	Participaciones		Area
rpub/rpriv	Cantidad	Cantidad	[%]	Promedio
1.909091	4 000 000 000	3 906 921 665	97,66	0.987538
1.818182	4 000 000 000	3 811 473 100	95,27	0.965593
1.727273	4 000 000 000	3 651 787 361	91,28	0.938371
1.636364	4 000 000 000	3 425 568 813	85,62	0.908328
1.545455	4 000 000 000	3 147 320 332	78,68	0.877233
1.454545	4 000 000 000	2 822 101 943	70,55	0.845776
1.363636	4 000 000 000	2 463 053 858	61,58	0.814840
1.272727	4 000 000 000	2 085 432 861	52,14	0.784815
1.181818	4 000 000 000	1 697 537 532	42,45	0.755074
1.090909	4 000 000 000	1 314 374 836	32,87	0.723589

Tabla A.8: Resultados del estudio de desempeño por Montecarlo de SBIR (Solución en Base a un Intervalo de Retardos posible), Métrica Area Promedio Refinada.

Razón rpub/rpriv	Experimentos Cantidad (Lambda)	Participaciones Cantidad	[%]	Area Promedio
1 (6,00)	1 000 000 000	128 949 470	12,89	0.783410
1 (5,66)	1 000 000 000	128 968 100	12,90	0.787591
1 (5,33)	1 000 000 000	128 962 940	12,90	0.791703
1 (5,00)	1 000 000 000	128 963 140	12,90	0.795865
1 (4,66)	1 000 000 000	128 969 790	12,90	0.800173
1 (4,33)	1 000 000 000	128 936 380	12,89	0.804492
1 (4,00)	1 000 000 000	128 920 690	12,89	0.808830
1 (3,66)	1 000 000 000	128 933 470	12,89	0.813200
1 (3,33)	1 000 000 000	128 953 660	12,90	0.817473
1 (3,00)	1 000 000 000	128 974 280	12,90	0.821740

Tabla A.9: Resultados del estudio de desempeño por Montecarlo de SBMD (Solución en Base a un retardo igual a la Máxima Distancia), Métrica Area Promedio Refinada.

Razón rpub/rpriv	Experimentos Cantidad	Participaciones Cantidad	[%]	Area Promedio
1	1 000 000 000	262 631 906	26,26	0.533057

Apéndice B

Tablas de Resultados de Estudio de Casos Particulares

A continuación se presentan las Tablas de Resultados del estudio de casos particulares, en base al método de Montecarlo, del desempeño de las soluciones propuestas. Estas representan el estudio sobre el protocolo propuesto en el caso de usuario a prueba P estático y usuario verificador V estático.

Las Tablas B.1 a B.8 presentan el estudio de desempaño general de las soluciones propuestas.

Tabla B.1: Resultados del estudio de desempeño con variación del factor de tolerancia de SBIRcDREyE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento y uso de Entropía).

Factor de	Razón	Experimentos	Participaciones		Refinamientos		Area Promedio
Tolerancia	rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]	Refinada
0.25	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
0.25	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
0.25	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
0.25	1.636364	10 000 000	10 000 000	100.00	0	0.00	1.00
0.25	1.545455	10 000 000	10 000 000	100.00	6 639	0.07	0.954314
0.25	1.454545	10 000 000	10 000 000	100.00	159 848	1,.60	0.905329
0.25	1.363636	10 000 000	10 000 000	100.00	695 519	6.95	0.852976
0.25	1.272727	10 000 000	10 000 000	100.00	2 047 977	20.48	0.772209
0.25	1.181818	10 000 000	9720316	97.20	3 668 005	36.68	0.700324
0.25	1.090909	10 000 000	6626497	66.26	3 876 003	38.76	0.700739
0.5	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
0.5	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
0.5	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
0.5	1.636364	10 000 000	10 000 000	100.00	0	0.00	1.00
0.5	1.545455	10 000 000	10 000 000	100.00	14 220	0.14	0.951884
0.5	1.454545	10 000 000	10 000 000	100.00	128 853	1.29	0.912417
0.5	1.363636	10 000 000	9 902 409	99.02	790 971	7.91	0.843967
0.5	1.272727	10 000 000	9 235 021	92.35	1 663 004	16.63	0.803267
0.5	1.181818	10 000 000	9 720 316	63.72	1 931 024	19.31	0.787855
0.5	1.090909	10 000 000	6 626 497	31.30	1 630 020	16.30	0.804220
0.75	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
0.75	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
0.75	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
0.75	1.636364	10 000 000	10 000 000	100.00	0	0.00	1.00
0.75	1.545455	10 000 000	10 000 000	100.00	12205	0.12	0.946094
0.75	1.454545	10 000 000	9 877 586	98.77	137 075	1.37	0.908676
0.75	1.363636	10 000 000	9 422 623	94.22	537 348	5.37	0.875988
0.75	1.272727	10 000 000	6 165 688	61.65	696 070	6.96	0.876133
0.75	1.181818	10 000 000	3 209 193	32.09	586 605	5.86	0.889033
0.75	1.090909	10 000 000	1 080 564	10.80	381 210	3.81	0.901514

Tabla B.2: Resultados del estudio de desempeño con variación del factor de tolerancia de SBIRcDRE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento).

Factor de	Razón	Experimentos	Participaciones		Refinamientos		Area Promedio
Tolerancia	rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]	Refinada
0.25	1.909091	10 000 000	10 000 000	100.00	323 839	3.24	0.987698
0.25	1.818182	10 000 000	10 000 000	100.00	896 160	8.96	0.965607
0.25	1.727273	10 000 000	10 000 000	100.00	1 617 439	16.17	0.937189
0.25	1.636364	10 000 000	10 000 000	100.00	2 430 227	24.30	0.904140
0.25	1.545455	10 000 000	10 000 000	100.00	3 352 549	33.52	0.867499
0.25	1.454545	10 000 000	10 000 000	100.00	4 342 767	43.42	0.827757
0.25	1.363636	10 000 000	10 000 000	100.00	5 408 648	54.08	0.785908
0.25	1.272727	10 000 000	9 314 188	93.14	6 061 308	60.61	0.754482
0.25	1.181818	10 000 000	7 066 937	70.67	5 467 803	54.67	0.754518
0.25	1.090909	10 000 000	5 138 613	51.38	4 661 406	46.61	0.745205
0.5	1.909091	10 000 000	10 000 000	100.00	322 403	3.22	0.987782
0.5	1.818182	10 000 000	10 000 000	100.00	889 208	8.89	0.965530
0.5	1.727273	10 000 000	10 000 000	100.00	1 622 838	16.23	0.937066
0.5	1.636364	10 000 000	10 000 000	100.00	2 450 621	24.51	0.904146
0.5	1.545455	10 000 000	10 000 000	100.00	3 358 306	33.58	0.867282
0.5	1.454545	10 000 000	8 790 560	87.90	3 674 576	36.74	0.847281
0.5	1.363636	10 000 000	6 607 707	66.07	3 304 504	33.04	0.846922
0.5	1.272727	10 000 000	4 752 902	47.53	2 917 949	29.18	0.846439
0.5	1.181818	10 000 000	3 231 355	32.31	2 420 051	24.20	0.840991
0.5	1.090909	10 000 000	2 013 219	20.13	1 762 608	17.62	0.827691
0.75	1.909091	10 000 000	10 000 000	100.00	321 053	3.21	0.987743
0.75	1.818182	10 000 000	10 000 000	100.00	892 807	8.93	0.965525
0.75	1.727273	10 000 000	10 000 000	100.00	1 620 171	16.20	0.937077
0.75	1.636364	10 000 000	8 279 942	82.80	1 717 716	17.18	0.928314
0.75	1.545455	10 000 000	6 180 370	61.80	1 562 080	15.62	0.928134
0.75	1.454545	10 000 000	4 390 126	43.90	1 372 132	13.72	0.927932
0.75	1.363636	10 000 000	2 930 081	29.30	1 174 441	11.74	0.927475
0.75	1.272727	10 000 000	1 785 802	17.86	924 781	9.25	0.924642
0.75	1.181818	10 000 000	976 071	9.76	625 070	6.25	0.921739
0.75	1.090909	10 000 000	468 450	4.68	375 136	3.75	0.918569

Tabla B.3: Resultados del estudio de desempeño con variación del factor de tolerancia de SBIR (Solución en Base a un Intervalo de Retardos posible).

Factor de Tolerancia	Razón rpub/rpriv (Lambda)	Experimentos Cantidad	Participaciones Cantidad	[%]	Refinamientos Cantidad	[%]	Area Promedio Refinada
0.25	1 (6,00)	10 000 000	1 629 870	16.29	426 656	4.26	0.857724
0.25	1 (5,66)	10 000 000	1 634 240	16.34	458 293	4.58	0.850834
0.25	1 (5,33)	10 000 000	1 633 700	16.33	488 832	4.88	0.843105
0.25	1 (5,00)	10 000 000	1 631 840	16.31	524 540	5.24	0.836086
0.25	1 (4,66)	10 000 000	1 635 290	16.35	581 593	5.81	0.833382
0.25	1 (4,33)	10 000 000	1 626 630	16.26	642 675	6.42	0.830644
0.25	1 (4,00)	10 000 000	1 632 180	16.32	712 115	7.12	0.825677
0.25	1 (3,66)	10 000 000	1 625 390	16.25	788 436	7.88	0.821003
0.25	1 (3,33)	10 000 000	1 628 730	16.28	891 999	8.91	0.817645
0.25	1 (3,00)	10 000 000	1 640 180	16.40	1 004 038	10.04	0.810699
0.5	1 (6,00)	10 000 000	0	0.0	0	0.0	0.0
0.5	1 (5,66)	10 000 000	0	0.0	0	0.0	0.0
0.5	1 (5,33)	10 000 000	0	0.0	0	0.0	0.0
0.5	1 (5,00)	10 000 000	0	0.0	0	0.0	0.0
0.5	1 (4,66)	10 000 000	0	0.0	0	0.0	0.0
0.5	1 (4,33)	10 000 000	0	0.0	0	0.0	0.0
0.5	1 (4,00)	10 000 000	0	0.0	0	0.0	0.0
0.5	1 (3,66)	10 000 000	0	0.0	0	0.0	0.0
0.5	1 (3,33)	10 000 000	0	0.0	0	0.0	0.0
0.5	1 (3,00)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (6,00)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (5,66)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (5,33)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (5,00)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (4,66)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (4,33)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (4,00)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (3,66)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (3,33)	10 000 000	0	0.0	0	0.0	0.0
0.75	1 (3,00)	10 000 000	0	0.0	0	0.0	0.0

Tabla B.4: Resultados del estudio de desempeño con variación del factor de tolerancia de SBMD (Solución en Base a un retardo igual a la Máxima Distancia).

Factor de Tolerancia	Razón rpub/rpriv	Experimentos Cantidad	Participaciones Cantidad	[%]	Refinamientos Cantidad	[%]	Area Promedio Refinada
0.25	1	1 000 000	493 157	49.31	493 157	49.31	0.549255
0.5	1	1 000 000	249 957	24.99	249 957	24.99	0.557491
0.75	1	1 000 000	0	0.0	0	0.0	0.0

Tabla B.5: Resultados del estudio de desempeño con variación de la distancia entre V y P de SBIRcDREyE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento y uso de Entropía).

Distancia	Razón	Experimentos	Participaciones		Refinamientos		Area Promedio
entre V y P	rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]	Refinada
0.5 r_{pub}	1.909091	10 000 000	10 00 0000	100.00	0	0.0	1.00
0.5 r_{pub}	1.818182	10 000 000	10 000 000	100.00	0	0.0	1.00
0.5 r_{pub}	1.727273	10 000 000	10 000 000	100.00	0	0.0	1.00
0.5 r_{pub}	1.636364	10 000 000	10 000 000	100.00	0	0.0	1.00
0.5 r_{pub}	1.545455	10 000 000	9 988 800	99.88	0	0.0	1.00
0.5 r_{pub}	1.454545	10 000 000	9 842 070	98.42	2 482	0.02	0.966180
0.5 r_{pub}	1.363636	10 000 000	9 376 263	93.76	104 229	1.04	0.913340
0.5 r_{pub}	1.272727	10 000 000	8 060 308	80.60	574 232	5.74	0.847643
0.5 r_{pub}	1.181818	10 000 000	6 124 498	61.24	1 245 625	12.45	0.760252
0.5 r_{pub}	1.090909	10 000 000	4 172 476	41.72	1 599 663	15.99	0.680280
r_{pub}	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
r_{pub}	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
r_{pub}	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
r_{pub}	1.636364	10 000 000	9 999 668	99.99	0	0.00	1.00
r_{pub}	1.545455	10 000 000	9 995 126	99.95	0	0.00	0.993675
r_{pub}	1.454545	10 000 000	9 864 829	98.64	77	0.40	0.938145
r_{pub}	1.363636	10 000 000	9 397 731	93.97	40 730	3.42	0.881252
r_{pub}	1.272727	10 000 000	8 072 931	80.72	1 086 931	10.86	0.824874
r_{pub}	1.181818	10 000 000	6 083 356	60.83	1 787 955	17.87	0.751297
r_{pub}	1.090909	10 000 000	4 157 714	41.57	2 237 433	22.37	0.698924
2 r_{pub}	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
2 r_{pub}	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
2 r_{pub}	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
2 r_{pub}	1.636364	10 000 000	9 999 893	99.99	0	0.00	1.00
2 r_{pub}	1.545455	10 000 000	9 981 972	99.81	5 116	0.05	0.964569
2 r_{pub}	1.454545	10 000 000	9 902 504	99.02	85 857	0.85	0.917221
2 r_{pub}	1.363636	10 000 000	9 447 135	94.47	505 303	5.05	0.867922
2 r_{pub}	1.272727	10 000 000	8 088 944	80.88	1 318 775	13.18	0.808903
2 r_{pub}	1.181818	10 000 000	6 163 545	61.63	2 029 643	20.29	0.738812
2 r_{pub}	1.090909	10 000 000	4 124 438	41.24	2 423 219	24.23	0.688761
3 r_{pub}	1.909091	10 000 000	10 000 000	100.00	0	0.00	1.00
3 r_{pub}	1.818182	10 000 000	10 000 000	100.00	0	0.00	1.00
3 r_{pub}	1.727273	10 000 000	10 000 000	100.00	0	0.00	1.00
3 r_{pub}	1.636364	10 000 000	10 000 000	100.00	0	0.00	1.00
3 r_{pub}	1.545455	10 000 000	9 984 455	99.84	10 791	0.10	0.954038
3 r_{pub}	1.454545	10 000 000	9 878 952	98.78	128 220	1.28	0.908643
3 r_{pub}	1.363636	10 000 000	9 328 763	93.28	599 357	5.99	0.856337
3 r_{pub}	1.272727	10 000 000	7 932 587	79.32	1 428 476	14.28	0.793921
3 r_{pub}	1.181818	10 000 000	6 205 871	62.05	2 071 275	20.71	0.734761
3 r_{pub}	1.090909	10 000 000	4 156 474	41.56	2 440 264	24.40	0.688414

Tabla B.6: Resultados del estudio de desempeño con variación de la distancia entre V y P de SBIRcDRE (Solución en Base a un Intervalo de Retardos posibles con Dos Regiones de Encubrimiento).

Distancia	Razón	Experimentos	Participaciones		Refinamientos		Area Promedio
entre V y P	rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]	Refinada
0.5 r_{pub}	1.909091	10 000 000	9 766 372	97.66	252 407	2.52	0.992873
0.5 r_{pub}	1.818182	10 000 000	9 524 864	95.24	583 930	5.83	0.979937
0.5 r_{pub}	1.727273	10 000 000	9 133 157	91.33	1 240 627	12.40	0.962734
0.5 r_{pub}	1.636364	10 000 000	8 562 177	85.62	1 701 832	17.01	0.944507
0.5 r_{pub}	1.545455	10 000 000	7 869 927	78.69	2 268 010	22.68	0.919383
0.5 r_{pub}	1.454545	10 000 000	7 052 467	70.52	2 601 056	26.01	0.889309
0.5 r_{pub}	1.363636	10 000 000	6 158 113	61.58	2 751 047	27.51	0.854266
0.5 r_{pub}	1.272727	10 000 000	5 215 807	52.15	2 734 505	27.34	0.815397
0.5 r_{pub}	1.181818	10 000 000	4 248 025	42.48	2 640 334	26.40	0.777039
0.5 r_{pub}	1.090909	10 000 000	3 293 442	32.93	2 375 832	23.75	0.741403
r_{pub}	1.909091	10 000 000	9 765 509	97.65	344 882	3.44	0.990420
r_{pub}	1.818182	10 000 000	9 527 514	95.27	944 438	9.44	0.973212
r_{pub}	1.727273	10 000 000	9 126 994	91.26	1 613 282	16.13	0.951005
r_{pub}	1.636364	10 000 000	8 565 564	85.65	2 239 121	22.39	0.924566
r_{pub}	1.545455	10 000 000	7 867 754	78.67	2 816 867	28.16	0.897775
r_{pub}	1.454545	10 000 000	7 054 819	70.54	3 232 500	32.32	0.864577
r_{pub}	1.363636	10 000 000	6 162 169	61.62	3 527 553	35.27	0.836134
r_{pub}	1.272727	10 000 000	5 218 696	52.18	3 620 816	36.20	0.805200
r_{pub}	1.181818	10 000 000	4 243 485	42.43	3 478 305	34.78	0.773327
r_{pub}	1.090909	10 000 000	3 288 756	32.88	3 077 565	30.77	0.741939
2 r_{pub}	1.909091	10 000 000	9 767 543	97.67	316 902	3.16	0.988285
2 r_{pub}	1.818182	10 000 000	9 528 249	95.28	860 507	8.60	0.967076
2 r_{pub}	1.727273	10 000 000	9 128 350	91.28	1 468 996	14.68	0.940668
2 r_{pub}	1.636364	10 000 000	8 563 576	85.63	2 072 499	20.72	0.911140
2 r_{pub}	1.545455	10 000 000	7 870 500	78.70	2 601 327	26.01	0.879706
2 r_{pub}	1.454545	10 000 000	7 050 905	70.50	3 014 869	30.14	0.846345
2 r_{pub}	1.363636	10 000 000	6 160 145	61.60	3 304 765	33.04	0.814058
2 r_{pub}	1.272727	10 000 000	5 215 996	52.15	3 431 001	34.31	0.782406
2 r_{pub}	1.181818	10 000 000	4 248 498	42.48	3 349 349	33.49	0.752795
2 r_{pub}	1.090909	10 000 000	3 296 303	32.96	3 032 467	30.32	0.721873
3 r_{pub}	1.909091	10 000 000	9 768 088	97.68	306 265	3.06	0.987631
3 r_{pub}	1.818182	10 000 000	9 527 611	95.27	835 480	8.35	0.965473
3 r_{pub}	1.727273	10 000 000	9 130 061	91.30	1 424 425	14.24	0.937920
3 r_{pub}	1.636364	10 000 000	8 561 229	85.61	2 008 815	20.08	0.907119
3 r_{pub}	1.545455	10 000 000	7 863 629	78.63	2 525 971	25.25	0.874353
3 r_{pub}	1.454545	10 000 000	7 055 345	70.55	2 944 689	29.44	0.841033
3 r_{pub}	1.363636	10 000 000	6 151 918	61.51	3 233 283	32.33	0.808284
3 r_{pub}	1.272727	10 000 000	5 215 654	52.15	3 372 554	33.72	0.777257
3 r_{pub}	1.181818	10 000 000	4 244 339	42.44	3 304 854	33.04	0.747090
3 r_{pub}	1.090909	10 000 000	3 291 477	32.91	3 010 556	30.10	0.717137

Tabla B.7: Resultados del estudio de desempeño con variación de la distancia entre V y P de SBIR (Solución en Base a un Intervalo de Retardos posible).

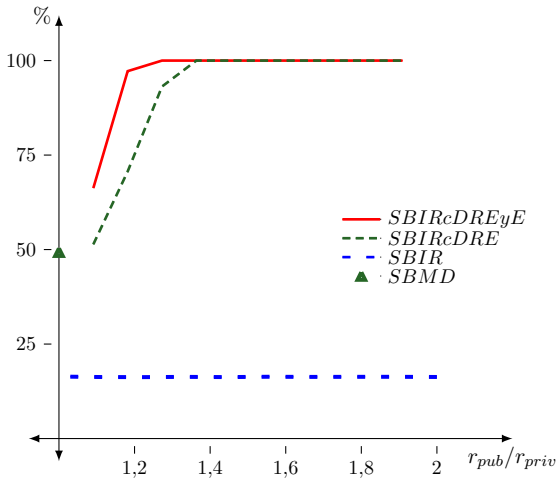
Distancia entre V y P	Razón rpub/rpriv (Lambda)	Experimentos Cantidad	Participaciones Cantidad	[%]	Refinamientos Cantidad	[%]	Area Promedio Refinada
0.5 r_{pub}	1 (6,00)	10 000 000	1 289 690	12.89	226 132	2.26	0.824900
0.5 r_{pub}	1 (5,66)	10 000 000	1 290 380	12.90	270 339	2.47	0.824900
0.5 r_{pub}	1 (5,33)	10 000 000	1 293 220	12.93	270 339	2.70	0.819181
0.5 r_{pub}	1 (5,00)	10 000 000	1 288 940	12.88	296 176	2.96	0.813283
0.5 r_{pub}	1 (4,66)	10 000 000	1 287 960	12.87	326 803	3.26	0.807739
0.5 r_{pub}	1 (4,33)	10 000 000	1 293 810	12.93	363 677	3.63	0.802409
0.5 r_{pub}	1 (4,00)	10 000 000	1 290 960	12.90	402 824	4.01	0.796780
0.5 r_{pub}	1 (3,66)	10 000 000	1 291 090	12.91	451 743	4.51	0.791608
0.5 r_{pub}	1 (3,33)	10 000 000	1 284 150	12.84	507 481	5.07	0.786635
0.5 r_{pub}	1 (3,00)	10 000 000	1 289 250	12.89	580 011	5.80	0.781389
r_{pub}	1 (6,00)	10 000 000	1 289 470	12.89	343 088	3.43	0.836123
r_{pub}	1 (5,66)	10 000 000	1 284 200	12.84	370 008	3.70	0.831433
r_{pub}	1 (5,33)	10 000 000	1 291 290	12.91	403 587	4.03	0.827308
r_{pub}	1 (5,00)	10 000 000	1 282 970	12.83	436 163	4.36	0.822547
r_{pub}	1 (4,66)	10 000 000	1 288 830	12.89	478 649	4.78	0.818255
r_{pub}	1 (4,33)	10 000 000	1 290 420	12.90	526 002	5.26	0.813734
r_{pub}	1 (4,00)	10 000 000	1 295 050	12.95	582 811	5.82	0.809644
r_{pub}	1 (3,66)	10 000 000	1 290 810	12.91	645 405	6.45	0.805106
r_{pub}	1 (3,33)	10 000 000	1 291 610	12.92	723 221	7.23	0.800730
r_{pub}	1 (3,00)	10 000 000	1 289 080	12.89	816 376	8.16	0.796977
2 r_{pub}	1 (6,00)	10 000 000	1 290 450	12.90	343 491	3.43	0.823341
2 r_{pub}	1 (5,66)	10 000 000	1 290 970	12.91	371 672	3.71	0.818935
2 r_{pub}	1 (5,33)	10 000 000	1 289 750	12.90	403 133	4.03	0.814936
2 r_{pub}	1 (5,00)	10 000 000	1 284 400	12.84	436 984	4.36	0.810445
2 r_{pub}	1 (4,66)	10 000 000	1 286 810	12.87	477 919	4.78	0.805773
2 r_{pub}	1 (4,33)	10 000 000	1 291 190	12.91	526 396	5.26	0.801980
2 r_{pub}	1 (4,00)	10 000 000	1 291 910	12.92	581 344	5.81	0.797942
2 r_{pub}	1 (3,66)	10 000 000	1 285 590	12.85	642 795	6.42	0.793831
2 r_{pub}	1 (3,33)	10 000 000	1 289 430	12.89	722 193	7.22	0.789692
2 r_{pub}	1 (3,00)	10 000 000	1 286 480	12.86	814 635	8.14	0.785637
3 r_{pub}	1 (6,00)	10 000 000	1 290 890	12.91	343 416	3.43	0.821417
3 r_{pub}	1 (5,66)	10 000 000	1 292 930	12.93	372 436	3.72	0.817003
3 r_{pub}	1 (5,33)	10 000 000	1 288 010	12.88	402 567	4.02	0.812699
3 r_{pub}	1 (5,00)	10 000 000	1 292 620	12.93	439 502	4.39	0.808614
3 r_{pub}	1 (4,66)	10 000 000	1 287 740	12.88	478 468	4.78	0.804239
3 r_{pub}	1 (4,33)	10 000 000	1 288 410	12.88	525 070	5.25	0.799924
3 r_{pub}	1 (4,00)	10 000 000	1 289 770	12.90	580 036	5.80	0.795761
3 r_{pub}	1 (3,66)	10 000 000	1 292 330	12.92	646 165	6.46	0.792058
3 r_{pub}	1 (3,33)	10 000 000	1 289 020	12.89	722 030	7.22	0.787746
3 r_{pub}	1 (3,00)	10 000 000	1 290 240	12.90	817 073	8.17	0.783663

Tabla B.8: Resultados del estudio de desempeño con variación de la distancia entre V y P de SBMD (Solución en Base a un retardo igual a la Máxima Distancia).

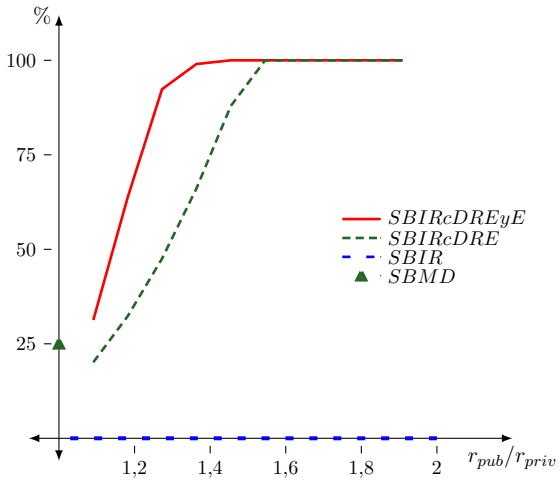
Distancia	Razón	Experimentos	Participaciones		Refinamientos		Area Promedio
entre V y P	rpub/rpriv	Cantidad	Cantidad	[%]	Cantidad	[%]	Refinada
0.5 r_{pub}	1	1 000 000	264553	26.45	264553	26.45	0.593902
r_{pub}	1	1 000 000	264599	26.46	264599	26.46	0.531077
2 r_{pub}	1	1 000 000	265448	26.54	265448	26.54	0.522449
3 r_{pub}	1	1 000 000	265144	26.51	265144	26.51	0.523349

Apéndice C

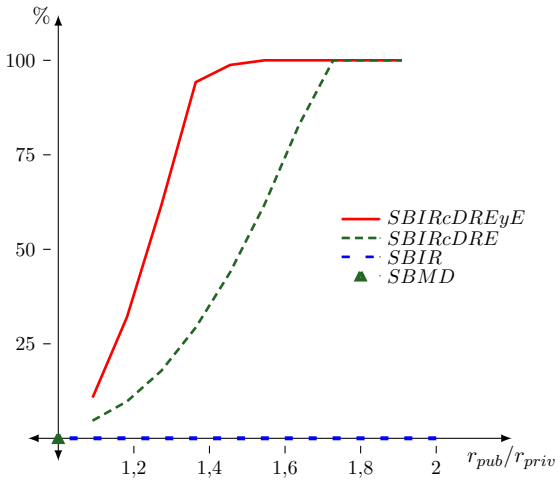
Graficos del Estudio Particular de las Soluciones



(a) Factor de Tolerancia $\tau = 25\,\%$

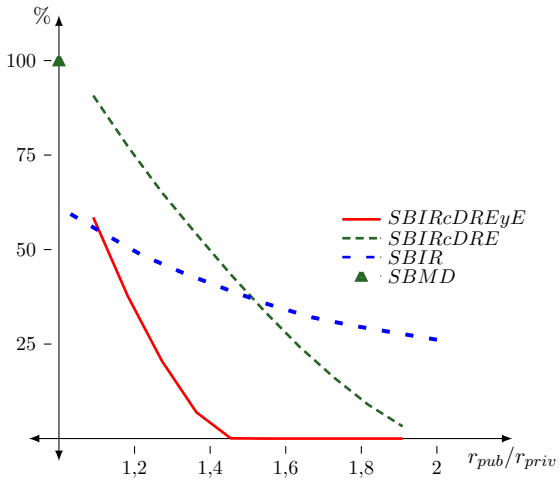


(b) Factor de Tolerancia $\tau = 50\,\%$

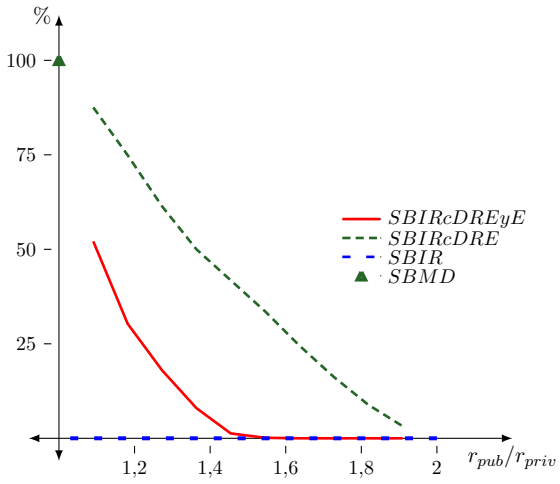


(c) Factor de Tolerancia $\tau = 75\,\%$

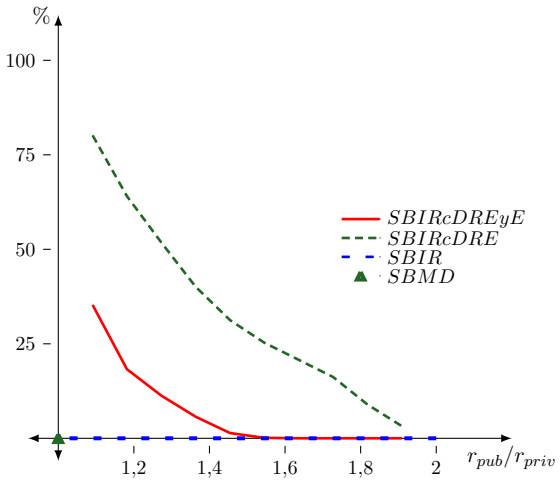
Figura C.1: Estudio particular del Factor de Tolerancia ($\tau = 25\,\%,\ 50\,\%,\ 75\,\%$), Participaciones.



(a) Factor de Tolerancia $\tau = 25\,\%$

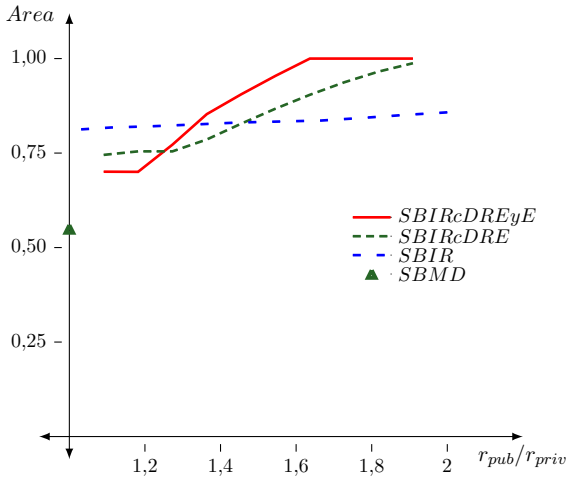


(b) Factor de Tolerancia $\tau = 50\,\%$

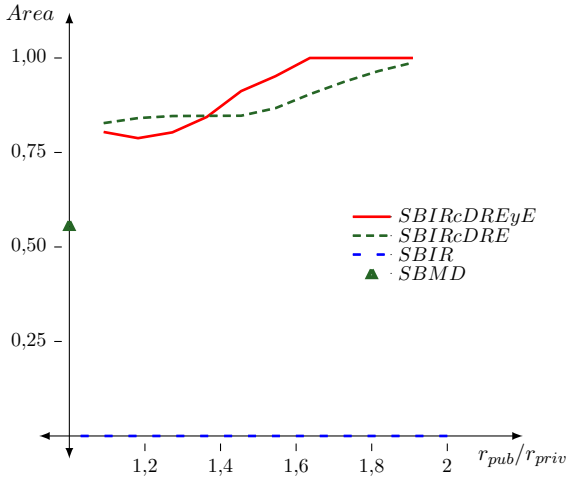


(c) Factor de Tolerancia $\tau = 75\,\%$

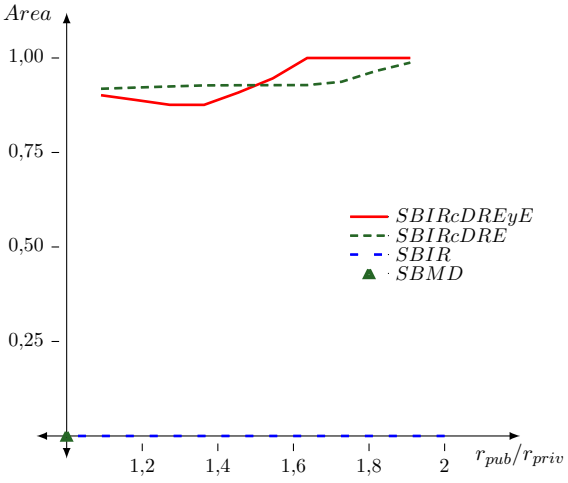
Figura C.2: Estudio particular del Factor de Tolerancia ($\tau = 25\,\%, 50\,\%, 75\,\%$), Número de refinamientos sobre el número de participaciones en el protocolo DBPALP.



(a) Factor de Tolerancia $\tau = 25\,\%$

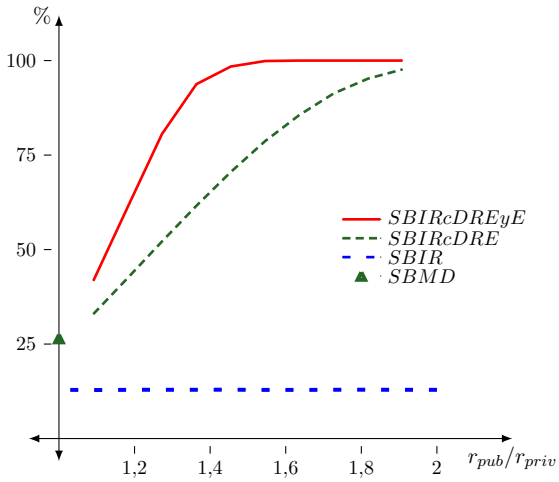


(b) Factor de Tolerancia $\tau = 50\,\%$

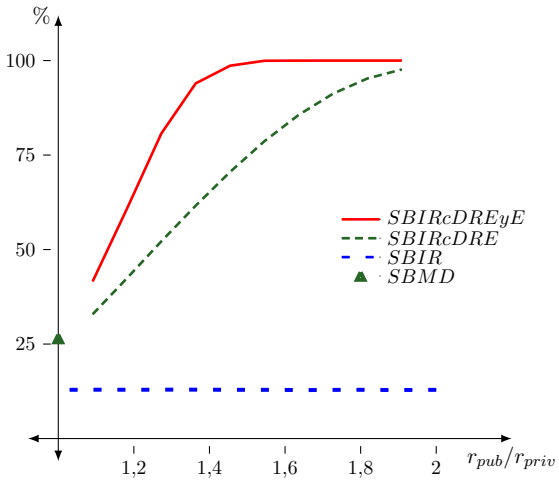


(c) Factor de Tolerancia $\tau = 75\,\%$

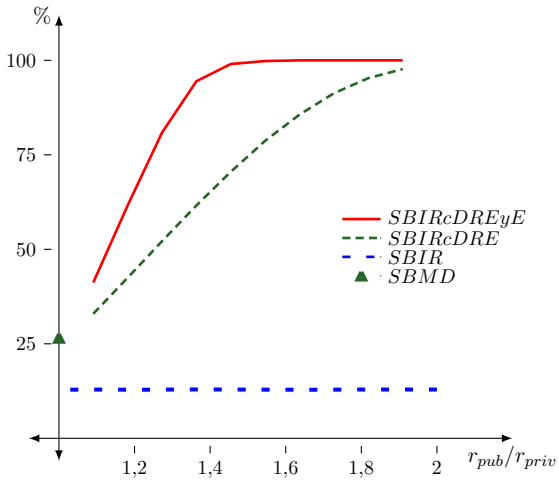
Figura C.3: Estudio particular del Factor de Tolerancia ($\tau = 25\,\%$, $50\,\%$, $75\,\%$), Area promedio refinada sobre el número de participaciones en el protocolo DBPALP.



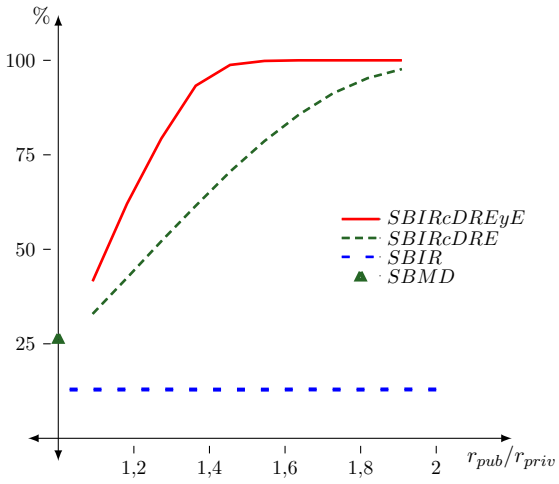
(a) Distancia entre V y $O_{pub} = 0.5r_{pub}$



(b) Distancia entre V y $O_{pub} = r_{pub}$

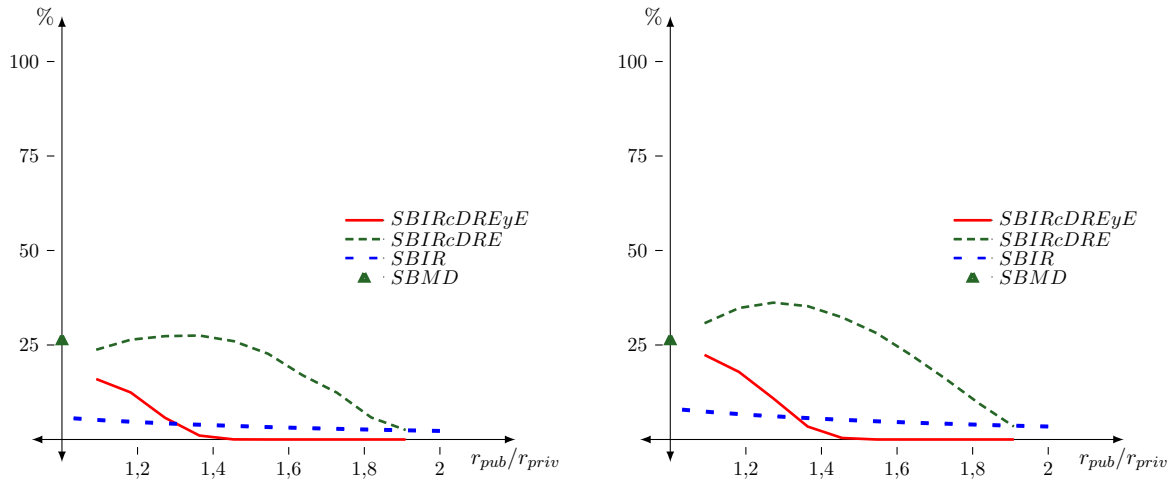


(c) Distancia entre V y $O_{pub} = 2r_{pub}$



(d) Distancia entre V y $O_{pub} = 3r_{pub}$

Figura C.4: Estudio particular de la Distancia entre V y O_{pub} (Distancia = $0.5r_{pub}$, r_{pub}, $2r_{pub}$, $3r_{pub}$), Participaciones.



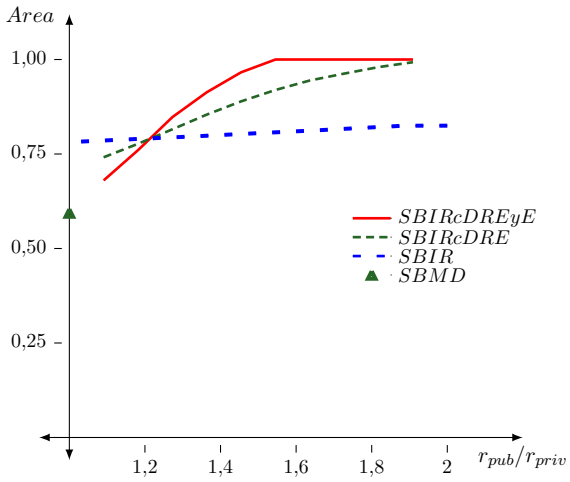
(a) Distancia entre V y $O_{pub} = 0.5r_{pub}$

(b) Distancia entre V y $O_{pub} = r_{pub}$

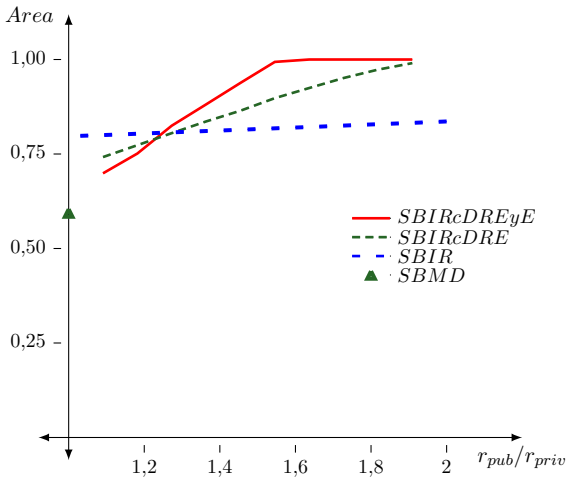
(c) Distancia entre V y $O_{pub} = 2r_{pub}$

(d) Distancia entre V y $O_{pub} = 3r_{pub}$

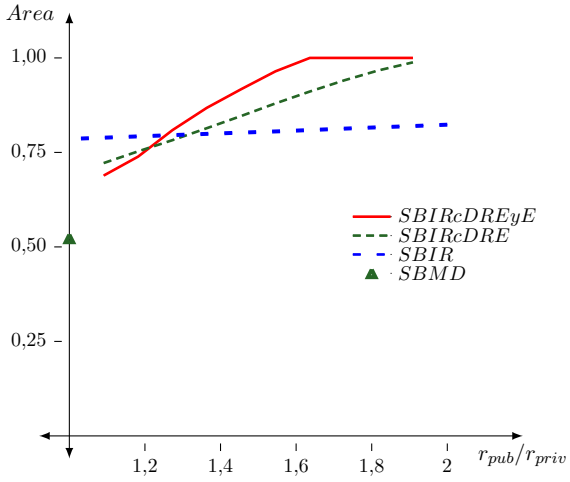
Figura C.5: Estudio particular de la Distancia entre V y O_{pub} (Distancia $= 0.5r_{pub}$, r_{pub}, $2r_{pub}$, $3r_{pub}$), Número de refinamientos sobre el número de participaciones en el protocolo DBPALP.



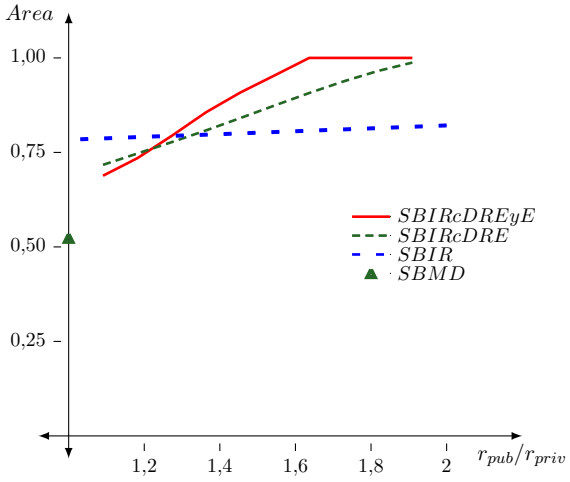
(a) Distancia entre V y $O_{pub} = 0.5r_{pub}$



(b) Distancia entre V y $O_{pub} = r_{pub}$



(c) Distancia entre V y $O_{pub} = 2r_{pub}$



(d) Distancia entre V y $O_{pub} = 3r_{pub}$

Figura C.6: Estudio particular de la Distancia entre V y O_{pub} (Distancia $= 0.5r_{pub}$, r_{pub}, $2r_{pub}$, $3r_{pub}$), Area promedio refinada sobre el número de participaciones en el protocolo DBPALP.