

Capítulo 3: Descripción de *Jamming*

3.1 Estrategias de *jamming*

Existen distintas estrategias que puede emplear un *jammer* para atacar a las diversas aplicaciones. Cada una de estas estrategias tiene sus ventajas y sus desventajas, es por eso que se debe de estudiar el “blanco” para elegir la mejor opción.

Cuando se trata de atacar sistemas que empleen señales *AJ*, el *jammer* debe de emitir una señal portadora en banda base que puede ser modulada por uno o más impulsos o bien por una señal de ruido [5, 6].

3.1.1 *Jamming* por ruido

La portadora emitida por el *jammer* es modulada por una señal aleatoria de ruido [3]. El ruido que se introduce puede ocupar ya sea todo el ancho de banda empleado por la señal *AJ*, o simplemente una parte de él. Los efectos serán distintos pero se debe de considerar que no siempre se necesita atacar todo el ancho de banda para interrumpir de manera eficiente la comunicación. Se divide en *jamming* por ruido de banda-ancha, *jamming* por ruido de banda-parcial y *jamming* por ruido de banda-angosta [5, 6].

3.1.1.1 *Jamming* por ruido de banda-ancha

El ruido de banda ancha o *BBN* (*Broadband noise*) introduce energía a través de todo el ancho del espectro de frecuencias en el que opere la aplicación blanco. A este tipo de *jamming* se le conoce también como *jamming* de banda completa. Este tipo de *jamming* es aplicable a cualquier tipo de señal *AJ* [6].

El nivel de potencia de *jamming* se denomina J_0 , y está medido en Watts/Hertz. La principal limitante de este tipo de *jamming* es que tiene un bajo J_0 , ya que la potencia es esparcida en una parte amplia del espectro.

El *BBN jamming* funciona elevando el nivel de ruido en el receptor lo que ocasiona un decremento en la relación señal-a-ruido [5, 6, 7]. La eficiencia de este tipo de *jamming* depende del nivel de potencia y por tanto de la distancia entre el *jammer* y el receptor.

3.1.1.2 *Jamming* por ruido de banda-parcial

Se conoce también como *PBN (Partial-band noise)*. En este caso se introduce energía a través de una parte específica del espectro, cubriendo solamente algunos canales. Estos canales pueden ser o no continuos. Este tipo de *jamming* es mejor que el anterior debido a que no desperdicia tanta potencia. En muchos casos no es necesario introducir ruido en todo el espectro, sino simplemente en los lugares donde importa. Por ejemplo, si se conoce la parte del espectro en donde se encuentran los canales de sincronización será mejor introducir ruido en esta parte que en todo el ancho del espectro. Al no haber sincronización la comunicación no llega a ser exitosa [5, 6].

3.1.1.3 *Jamming* por ruido de banda-angosta

Conocido como *NBN (Narrowband noise)*, esta manera de generar *jamming* introduce energía en solamente un canal. El ancho de banda de esta energía podría abarcar todo el canal o simplemente una parte de él. Una vez más la diferencia radica en la potencia empleada y el espectro cubierto. La eficiencia de esta forma de *jamming* dependerá en parte del conocimiento de la aplicación blanco, esto es porque se debe de atacar el lugar exacto en el espectro en donde se encuentren los canales de interés. La potencia se puede canalizar toda a una pequeña parte del espectro, lo que representa una ventaja [5, 6].

3.1.2 *Jamming* por tonos

Esta estrategia consiste en colocar uno, *single-tone (ST)*, o varios, *multiple-tone (MT)*, tonos a lo largo del ancho de banda donde se encuentra la señal *AJ* [6]. La eficiencia de esta técnica depende completamente del lugar en el espectro donde se coloquen los pulsos. Es por eso que se requiere estudiar la señal objetivo de manera cuidadosa. En un sistema *DSSS* es posible emplear *single-tone jamming* para modificar el *offset* en los receptores y ocasionar que se sobrepase el nivel máximo de la señal, lo que produce que no se pueda recibir la información. La relación entre la fase del tono emitido por el *jammer* y la fase de

la señal es un parámetro importante. Si se manda un solo tono, éste estará presente ya sea en la frecuencia del cero o del uno. Si se encuentra en la frecuencia del uno entonces la fase representa un problema, ya que si el tono no se encuentra en fase no se podrá bloquear o interferir la transmisión del símbolo. En cambio si el tono se encuentra en la frecuencia del cero, entonces podrá bloquear la transmisión al símbolo siempre y cuando la potencia sea adecuada sin depender de la fase [5, 7].

En un caso de *MT* si los tonos se colocan en canales continuos, el desempeño del *jammer* será teóricamente igual al desempeño de *jamming* por ruido de banda-parcial. Debido a que los tonos se colocan en canales continuos se conoce a este particular caso de *MT* como *comb jamming* [6].

El que se produzca una correcta interferencia dependerá en primer lugar de que el tono se coloque en una parte del espectro en donde exista un tono que represente un símbolo, en ese caso el *JSR* debe ser lo suficientemente alto; en segundo lugar dependerá de que una vez que el tono del *jammer* esté en la frecuencia del tono del símbolo, la fase entre ellos sea igual.

Este tipo de *jamming* es muy poco eficiente contra sistemas *FH* debido a que depende de que la señal salte a la frecuencia en la cual se ha colocado el tono emitido por el *jammer*. Es por eso que si se utilizan tonos estos deben estar barriendo una parte del espectro y no estar en una frecuencia específica. Este es el caso de una estrategia de *jamming* posterior.

3.1.3 *Jamming* por pulsos

Esta estrategia es similar en resultados al *jamming* por ruido de banda-parcial. En este caso el factor a tomar en cuenta no es el ancho del espectro cubierto, sino el tiempo que es *jammer* está encendido. A pesar de que una de las estrategias se enfoca a frecuencia y la otra a tiempo, la eficiencia es prácticamente la misma. Sin embargo, cuando se analiza el funcionamiento se encuentran similitudes con el *jamming* por ruido de banda-ancha. Esto se debe a que el tiempo que está encendido, el *jammer* que trabaja por pulsos abarca una

parte amplia del espectro. Esta estrategia ahorra de manera considerable la potencia, lo que la hace eficiente si se diseña correctamente el ciclo de trabajo [5, 7].

3.1.4 *Jamming* por barrido

Es un concepto similar al de ruido por banda-ancha o por banda-parcial [6, 8]. De hecho se puede considerar como una estrategia complementaria. Consiste en introducir ruido en una pequeña parte del espectro; y una vez colocada está señal, se realiza un barrido por todo el ancho de banda que ocupe la señal *AJ*. Esta estrategia se puede emplear en un sistema *FHSS* [5]. Sin embargo, se tiene que considerar que el barrido debe de ser tan rápido como para identificar la frecuencia en la que se encuentre la señal pero sin llegar a una velocidad tal, que cuando se sitúe sobre el salto se tenga efecto solamente sobre una parte de él. Supongamos que para lograr interferir un sistema de comunicación se debe tener un *BER* de 10^{-1} . Un *BER* de 10^{-1} significa que es necesario bloquear la transmisión de un bit de diez, o para un sistema *AJ* que está mandando datos a una velocidad de 20kbps, la transmisión de 2000 bits debe ser bloqueada para alcanzar este *BER*. Si este sistema es de tipo *SHF* y maneja 100 saltos por segundo, cada salto contendrá 200 bits (sin considerar el tiempo entre saltos). De ahí que se necesite aplicar de manera exitosa *jamming* sobre 10 saltos por segundo. Ya que estos saltos pueden estar en todo el espectro asignado, al menos 10 barridos por segundo son necesarios para que el *jammer* sea eficiente.

A pesar de que el concepto es parecido al de *jamming* por ruido de banda-ancha, en este caso se optimiza el uso de la potencia. Esto se debe a que no se debe esparcir la potencia por todo el ancho del espectro, sino que se utiliza la máxima potencia en determinado lugar y en determinado momento.

3.1.5 *Jamming* por seguimiento

Esta estrategia se aplica generalmente a sistemas *FHSS*. Consiste en localizar la frecuencia a la cual “saltó” la señal, identificar la señal como el blanco y emplear *jamming* por ruido, tonos o pulsos. Se conoce también como *jamming* de respuesta y *jamming* de repetición [5].

Sus principales limitantes al usarlo contra sistemas *FH* fueron determinadas por Torieri. Estas limitantes están relacionadas con el tiempo de procesado del *jammer*. Esto se debe a que el proceso de *jamming* en este caso comienza por conocer la frecuencia a la que ha saltado la señal. Esto se hace midiendo la energía del espectro para saber si ha habido ganancias o pérdidas. Si se detecta mayor energía en un punto se podría concluir que esa es la nueva frecuencia, aunque esto no es siempre cierto. Debido a la velocidad del salto de frecuencias es difícil averiguar el nuevo blanco.

Además de esto existen otros problemas. Si se aplica *jamming* al mismo tiempo en más de un canal, la potencia estará distribuida entre estos y probablemente no será suficiente para reducir la relación señal-a-ruido a un nivel donde no puede existir comunicación. Incluso las distintas modulaciones son un escudo ante esta estrategia. Por ejemplo, si se emplea *BFSK* como técnica de modulación el *jammer* no sabe cuál es el canal complementario. En este caso la probabilidad de que el *jammer* sea eficiente se reduce a la mitad. Es por estas razones que a pesar de ser un estrategia eficiente cuando se diseña correctamente, es muy compleja y no representa una opción de sencilla implementación [5, 6].

3.1.6 *Jamming* inteligente

Es común que cuando se aplica alguna estrategia de *jamming* sobre una señal *AJ*, se desperdician recursos y no siempre se elige la opción más adecuada. Cuando se conoce como funciona el sistema que se desea atacar, se pueden optimizar los recursos. Realmente el *jamming* inteligente no es una estrategia como las anteriores, sino que se refiere al estudio del blanco para lograr mejores resultados. Por ejemplo, se puede atacar la señalización en sistemas de telefonía móvil para evitar el uso de móviles [5, 7].

Por ejemplo, en los sistemas de telefonía móvil es común encontrar canales de sincronización. En el caso de IS-95 se usa un canal codificado por código Walsh que se encarga de la sincronización. Si se identifica a este canal y se aplica alguna estrategia de *jamming* sobre él, será posible interrumpir de manera eficiente toda la comunicación.

Dentro de este tipo de *jamming* se encuentra el *jamming* de engaño. En esta estrategia se envía un mensaje falso para mantener a una de las partes del sistema de comunicación en estado de recepción. De esta manera, se logra que nunca haya confirmación de que se recibió el mensaje y se genera una interrupción en la comunicación. Otra manera de engañar al sistema sobre el cual se aplica *jamming*, es interceptar la señal del transmisor y con ello establecer una ruta de comunicación incorrecta [5, 7].

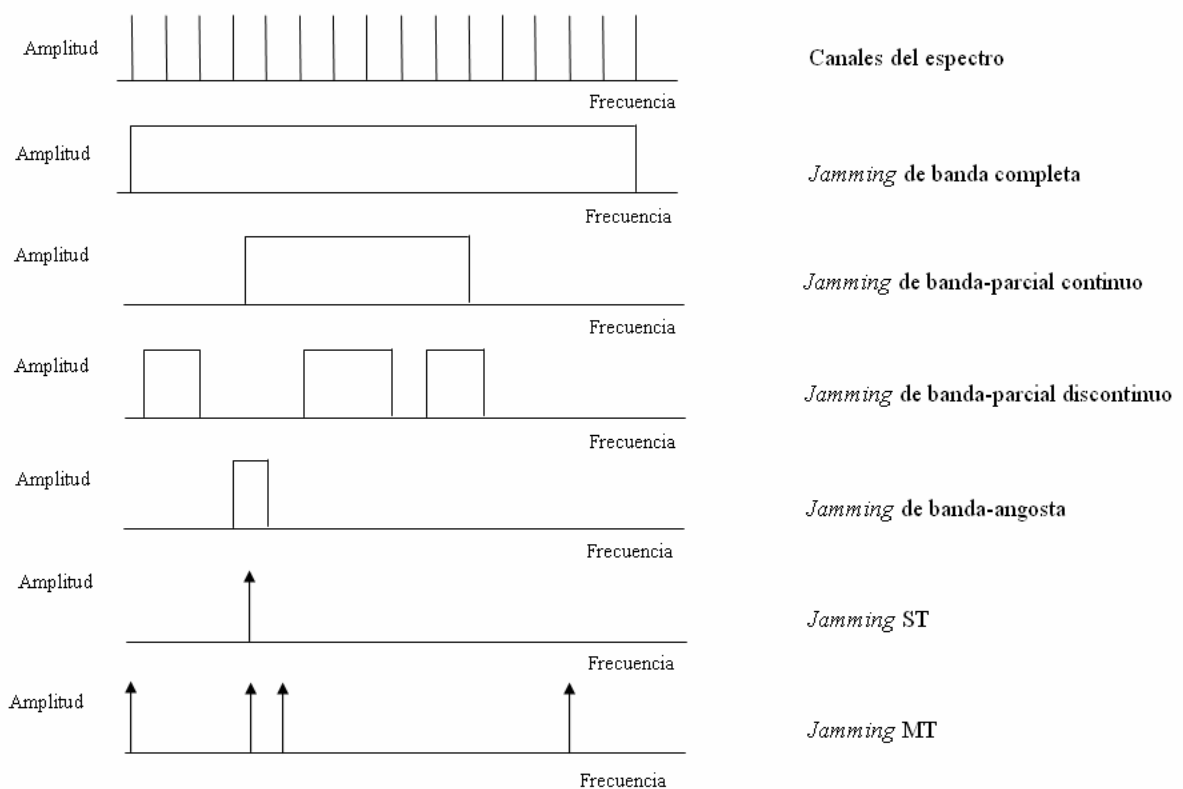


Figura 3.1 Estrategias de *jamming*

3.1.7 Técnicas para incrementar la eficiencia del *jammer*

Una manera de incrementar la eficiencia de un *jammer* es incrementar el número de señales que puede bloquear o interferir simultáneamente. Esto es posible mediante algunas

técnicas que involucran el compartir la potencia entre los distintos blancos y el poder encender y apagar el *jammer* por determinado tiempo para dedicarlo a uno o a otro blanco.

3.1.7.1 Look-Through

Cuando las señales no son de espectro extendido, esta técnica es empleada para determinar si el blanco ha cambiado de frecuencia o simplemente ha dejado de operar. Esto se hace para no malgastar la potencia y de esta manera emplearla en más de un objetivo o simplemente ahorrarla. Al momento de apagar el *jammer* se mide la actividad en el espectro y se determina si el blanco está en funcionamiento o no. Podría pensarse como solución para sistemas *FH* y como una forma de *jamming* por seguimiento. Sin embargo, debido a la velocidad de salto no se emplea esta técnica para tal propósito. Esta técnica se puede aplicar a sistemas *DSSS* siempre y cuando se pueda detectar su actividad [5, 7].

3.1.7.2 Potencia compartida

Una manera de compartir la potencia entre dos o más blancos está representada por la estrategia de múltiples tonos. En esta estrategia de *jamming* los tonos se pueden colocar en diferentes partes del espectro sin necesidad de que los canales sean continuos para lograr atacar varios blancos [5].

3.1.7.3 Tiempo compartido

Otra técnica para cubrir más de un blanco es orientar la máxima potencia del *jammer* hacia cada blanco pero en momentos distintos. Cuando se aplica *jamming* a una señal digital no se tiene que estar todo el tiempo introduciendo ruido. Basta con incrementar el *BER* hasta cierto nivel. En el caso de las comunicaciones de voz el nivel necesario para cortar la transmisión es más alto que en el caso de datos. En el caso de las comunicaciones de voz analógicas es necesario bloquear o interferir solamente un 30% de la transmisión para que no entienda el mensaje. De ahí que el *jammer* pueda estar orientado a distintos blancos en diferentes momentos [5].

3.2 Clasificación general de *jammers*

De las distintas estrategias de *jamming* se derivan cuatro tipos principales de *jammers*. La elección del tipo de *jammer* dependerá de la aplicación específica.

3.2.1 *Jammer* constante

Este tipo de *jammer* emplea la estrategia de ruido y la de barrido. Su principal ventaja es la relativa facilidad de implementarse. Sin embargo, en aplicaciones donde se desea que el *jamming* pase desapercibido no es recomendable emplear un *jammer* constante [8]. Esto se debe a que al momento de analizar la transmisión de la información se detectará ruido que excede los niveles comunes. Una vez detectado el ruido es posible encontrar la fuente que lo genera. Además de esta desventaja, es necesario considerar que la potencia requerida es grande.

3.2.2 *Jammer* de engaño

Emplea la técnica de engaño que pertenece al *jamming* inteligente. En este caso se envían señales que parecen ser legítimas, pero no se incluye una separación entre ellas. Esto ocasiona que se mantenga el estado de recepción y no haya confirmación de haber recibido información alguna [8]. Este tipo de *jammer* logra mayor invisibilidad que el constante. Sin embargo, aún es posible detectarse. La potencia requerida también es grande.

3.2.3 *Jammer* aleatorio

Este tipo de *jammer* funciona por determinado tiempo y deja de hacerlo por otro [8]. Los tiempos son programados y se debe hacer conocer la aplicación para obtener resultados positivos. Se puede utilizar *jamming* por ruido, por pulsos, por tonos e incluso por barrido [6]. La potencia es menor debido a que no se encuentra en operación todo el tiempo. La detección es posible al realizar un análisis de la actividad de la red.

3.2.4 *Jammer* reactivo

Este tipo es el más complejo pero es el que ofrece una menor posibilidad de ser detectado. Consiste en sensar la actividad de la red para saber en que momento debe de actuar el *jammer* [8]. Podría pensarse que el consumo de potencia es mínimo. Sin embargo,

a pesar de no ser excesivo si se requiere determinada potencia para estar monitoreando la actividad de la red. Una vez que se detecta el envío de la señal, se realiza un *jamming* por ruido, por tonos o por pulsos.