

Capítulo 2: Descripción de la “Guerra Electrónica”

La “Guerra Electrónica” de las comunicaciones o *EW* por sus siglas en inglés “*Electronic Warfare*” es el nombre que se le da a todas aquellas acciones que tienen por objetivo bloquear, interceptar o negar la comunicación de un punto transmisor a otro receptor [5, 6, 7]. Esta llamada “guerra” tiene tres elementos principales [5,6]:

- ✓ El ataque electrónico (*EA, Electronic Attack*)
- ✓ El apoyo electrónico (*ES, Electronic Support*)
- ✓ La protección electrónica (*EP, Electronic Protect*)

2.1 Ataque electrónico

El AE (ataque electrónico) se puede realizar por medio de tres tipos de acciones o técnicas [5, 6, 8]:

- 1) *Jamming*
- 2) Engaño
- 3) Radiación directa de energía

2.1.1 Técnica de *jamming*

El término *jamming* no posee una traducción acertada que englobe todo el concepto. En su más puro significado, *jamming* se define como aquella actividad que afecta la línea de tiempo en alguna comunicación [6, 8]. Es decir, logra que la información no llegue al receptor en el momento que debía de hacerlo. Al afectar esto, se afecta también la relevancia de la información. Esto se debe a que la información solamente es útil en determinado instante. No es útil si se recibe antes o después del tiempo establecido.

2.1.2 Técnica de engaño

La técnica de engaño tiene como objetivo formar una nueva ruta de comunicación [6]. Es así que en lugar de que la información llegue al receptor deseado, ésta sufre un cambio de ruta y es recibida por otro sistema receptor. De igual forma, el engaño puede consistir en la sustitución del sistema transmisor. En este caso el receptor original está recibiendo una

señal que proviene de un segundo sistema transmisor. Cuando el receptor está ocupado no puede recibir la señal emitida por el transmisor original.

2.1.3 Técnica de radiación directa de energía

La radiación directa de energía es la manera más fácil de atacar a un sistema de comunicación. Sin embargo, es la más fácil de detectar y poder evitar. Consiste en enviar una determinada señal con determinada potencia para dañar o destruir completamente la comunicación entre transmisor y receptor. La potencia emitida debe ser mayor a la que emplea el transmisor del sistema que está sobre ataque [8].

Un dispositivo capaz de emplear cualquiera de las tres técnicas o una combinación de ellas para interferir, dañar o destruir la transmisión de información dentro de un sistema electrónico de comunicaciones es llamado *jammer* [8].

2.2 Apoyo electrónico

El apoyo electrónico funciona como auxiliar del AE. Su función es la medición de parámetros de interés en el sistema de comunicación [6]. Una de las razones principales de hacer esto radica en que si no hay señal que interferir no tiene caso gastar la potencia del *jammer* implementado. Sin embargo, dependiendo de la aplicación será el tipo de *jammer* que se emplee. Es así que se puede mantener en operación un *jammer* por tiempo indefinido o se puede encender siempre y cuando se detecte una comunicación. Todo esto se verá más adelante cuando se analicen los distintos tipos de *jammers* que existen. Entre los parámetros que se encarga de medir el apoyo electrónico se encuentran [6, 8]:

➤ ***SNR (Signal-to-Noise Ratio)***

Determina la calidad con la que llega la señal al receptor después de recorrer la ruta del sistema de comunicación e ir contaminándose por ruido.

➤ ***JSR (Jam-to-Signal Ratio)***

Determina si la potencia con que transmite el *jammer* es mayor o menor que aquella que emplea el transmisor original del sistema [6].

➤ ***PSR (Packet Send Ratio)***

Relaciona los paquetes que fueron enviados correctamente por una ruta de tráfico con los paquetes que trataron de ser enviados fuera de la capa *MAC* [8].

➤ ***PDR (Packet Delivery Ratio)***

Compara los paquetes que llegaron al receptor con los que fueron enviados [8].

➤ ***BER (Bit Error Rate)***

Indica la fracción de bits que contiene o pudiera contener errores. Es decir, es la probabilidad de que un bit sea incorrecto. El *BER* se puede escribir también como P_e [6].

➤ ***SER (Symbol Error Rate)***

Es la probabilidad de que un símbolo sea incorrecto y se llega a escribir como P_s [6].

➤ ***SIR (Signal-to-Interference Ratio)***

Relaciona la potencia de la señal deseada con la potencia de la suma de las señales no deseadas [5, 7].

2.3 Protección electrónica

La PE (protección electrónica) consiste en el uso de estrategias para evitar los dos primeros elementos de la llamada “Guerra Electrónica”, es decir, el ataque y el apoyo [6]. La codificación y la modulación entran dentro de este elemento. Con la unión de modulación y codificación nacieron las comunicaciones *AJ* por sus siglas en inglés, *antijam*. Este tipo de comunicaciones tienen como objetivo evitar que un sistema externo pueda dañar, bloquear o interceptar la comunicación de otro sistema.

2.3.1 Tipos de señales *AJ* (*antijam*)

A pesar de existir varios tipos de señales *AJ*; no es parte de este trabajo mencionar todas. Es por eso que se discutirán las dos principales. Las dos tipos de señales *AJ* a tratar tienen que ver con la telefonía móvil. El primero consiste en la secuencia directa de amplio espectro o *DSSS (Direct Sequence Spread Spectrum)* [6]. Este tipo de señal es empleado en el estándar de segunda generación de telefonía móvil IS-95A conocida común y erróneamente como *CDMA*. Se debe recordar que *CDMA (Code Division Multiple Access)*

es una técnica de acceso múltiple y no un estándar. De igual forma, se emplea en el estándar de 2.5G IS-95B y en el de 3G *Cdma2000*.

El segundo tipo de señal *AJ* es el salto de frecuencia o *FHSS* (*Frequency Hopping Spread Spectrum*) [6]. El estándar de segunda generación de telefonía móvil *GSM* emplea esta técnica para lograr la diversidad de frecuencia.

Para que una señal pueda ser considerada como *AJ* es necesario que el sistema que la transmita sea un sistema *LPD* (*Low Probability of Detection*) y/o *LPI* (*Low Probability of Intercept*) [5, 6].

En un sistema *LPD* el objetivo es lograr que la señal permanezca tan oculta como sea posible. *DSSS* es un ejemplo de sistema *LPD* [5, 6]. En *DSSS* esto se logra al distribuir la señal por todo el espectro disponible, lo que hace que la potencia sea muy baja y parezca ruido. Es así que se vuelve complicado detectar si la señal es de información, o es simplemente ruido.

En un sistema *LPI* (*Low Probability of Intercept*) puede ser que se haya detectado la señal, pero mientras no se intercepte la información, ésta estará protegida [5, 6]. Un ejemplo de estos sistemas es *FHSS*. En *FHSS* la protección se logra cambiando de frecuencia constantemente. Contrario a *DSSS*, donde el ancho de banda requerido es grande, en los sistemas que emplean *FH* la señal ocupa generalmente un ancho de banda angosto que depende del propio sistema, de la aplicación y de la técnica de modulación.

Existen dos tipos de salto de frecuencia. *FFH* (*Fast Frequency Hopping*) y *SFH* (*Slow Frequency Hopping*). La diferencia radica en el número de bits de datos que “saltan”. Cuando el salto es rápido, *FFH*, existen muchos cambios de frecuencia pero se encuentran involucrados pocos bits de datos. En cambio, en *SFH* es mayor la cantidad de datos pero los cambios de frecuencia no son tan numerosos [6, 14].