Universidad Central “Marta Abreu” de Las Villas
Facultad de Ingeniería Eléctrica
Dpto. Telecomunicaciones y Electrónica

UNIMINUTO
Corporación Universitaria
Minuto de Dios

Seguridad en Redes Inalámbricas

Dr. Vitalio Alfonso Reguera
Profesor Titular, Facultad de Ingeniería Eléctrica
Departamento de Telecomunicaciones y Electrónica
UCLV, vitalio@uclv.edu.cu

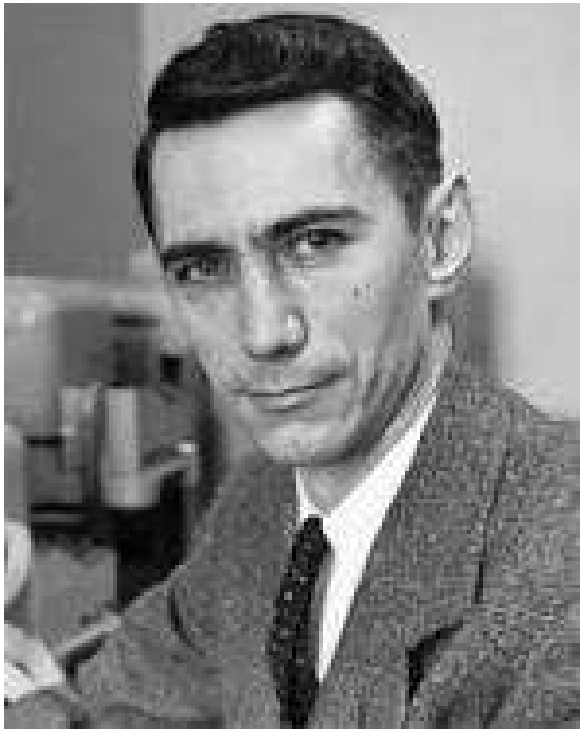
Colombia, 2016

¿Que tan seguras son las comunicaciones?

…se asume que el enemigo tiene cualquier equipo necesario para interceptar y registrar la señal transmitida…

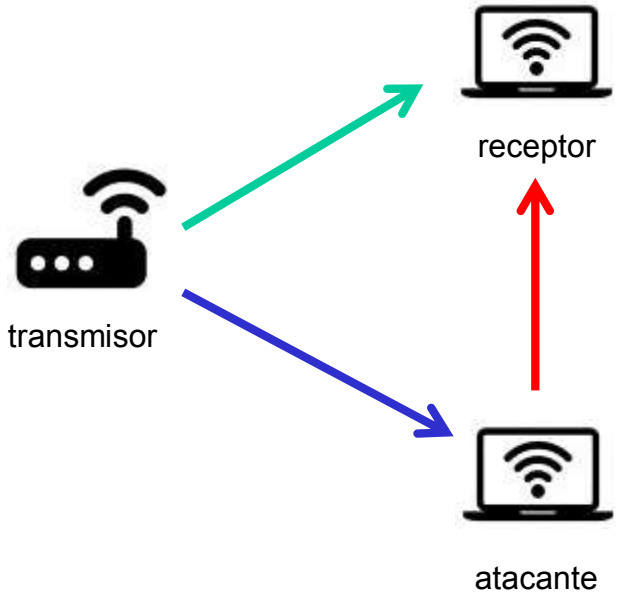
C. E. Shannon

Communication Theory of Secrecy Systems
Bell system technical journal 28.4 (1949)



Seguridad en Redes Inalámbricas

La naturaleza abierta del canal de comunicaciones inalámbrico, donde las señales se difunden y se superponen, facilita los ataques de interceptación (escucha) y la interferencia intencionada (jamming)



Mecanismos de Seguridad en Redes Inalámbricas

Sistemas Criptográficos

- Trabajan en las capas altas de la pila de protocolos
- Asumen bajo poder computacional del atacante

Técnicas de espectro extendido (FH, CDMA)

- Trabajan en la capa física
- Asumen conocimiento limitado por parte del atacante

Seguridad basada en la teoría de la información

- Trabaja en la capa física
- No pone limites a la capacidad computacional o cognitiva del atacante.

La combinación de todos los mecanismos: enfoque multidimensional.

Sistemas Criptográficos

Se basan en el concepto de la **seguridad computacional**, el cual aún no se ha logrado demostrar matemáticamente. La complejidad de estos sistemas dificulta su uso e implementación en **redes ad-hoc**. Por un lado los sistemas de **criptografía simétrica**, presentan el problema del intercambio de clave, mientras el uso de la criptografía de **clave pública** normalmente requiere de infraestructura y demanda un alto costo computacional.

Ver: https://en.wikipedia.org/wiki/RSA_Factoring_Challenge#The_mathematics
https://en.wikipedia.org/wiki/Shor%27s_algorithm

Seguridad Wi-Fi

Wired Equivalent Privacy (WEP)

- Estándar de seguridad de 802.11, 1997
- Se basa en el uso del algoritmo RC4 para generar cadenas de claves que son combinadas (XOR) con el mensaje.
- En agosto de 2001se pública un criptoanálisis que expone las vulnerabilidades de WEP y logra recuperar la clave RC4.
- Hoy existen varias herramientas en Internet que permiten subvertir la seguridad WEP en pocos minutos (aircrack-ng).

Wi-Fi Protected Access (WPA)

- Resuelve los problemas de seguridad de WEP
- Emplea TKIP (Temporal Key Integrity Protocol)
- Su versión más reciente WPA2 (IEEE 802.11i, 2004) utiliza AES

Medidas de seguridad para proteger una red Wi-Fi

Medidas simples pero que aportan poca seguridad.

- Ocultar el SSID
- Filtro de direcciones MAC
- Direccionamiento IP estático

Medidas recomendadas de seguridad

- Habilitar y usar WAP, preferentemente WAP2
- Emplear los mecanismos de autenticación de IEEE 802.1X (EAP)

Medidas de seguridad adicionales

- Blindaje de RF
- Reforzar la seguridad empleando VPNs (Ej. PPTP, IPSec)

NITS, SP 800-153, Guidelines for Securing Wireless Local Area Networks(WLANs) (February 2012), http://dx.doi.org/10.6028/NIST.SP.800-153

Seguridad de las Redes Móviles

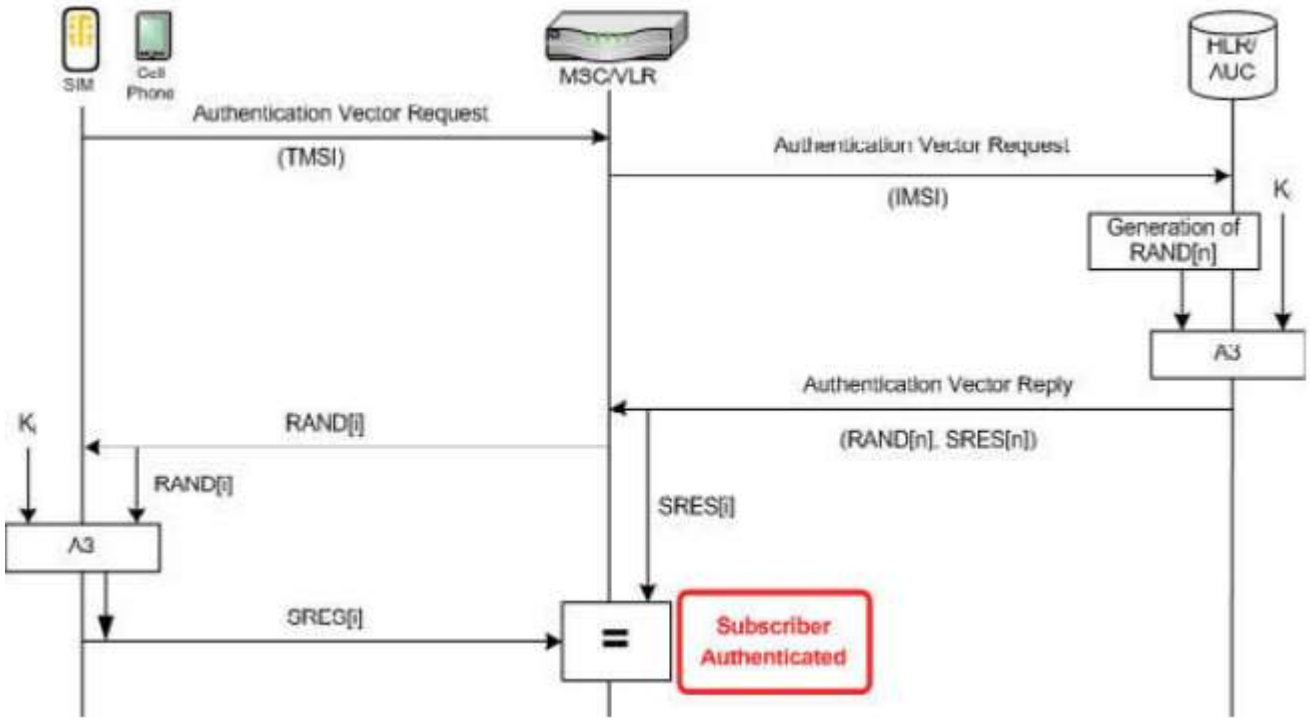
La mayor parte de la seguridad en redes GSM está centrada en la BSS y se limita al control de acceso y la encriptación del enlace de radio.

Subscriber Identity Module

- IMSI (International Mobile Subscriber Identity)
- Ki (GSM AKA Secret Key)
- LAI (Location Area Identity)
- PIN (Personal Identity Number)
- Address book + Services and Applications

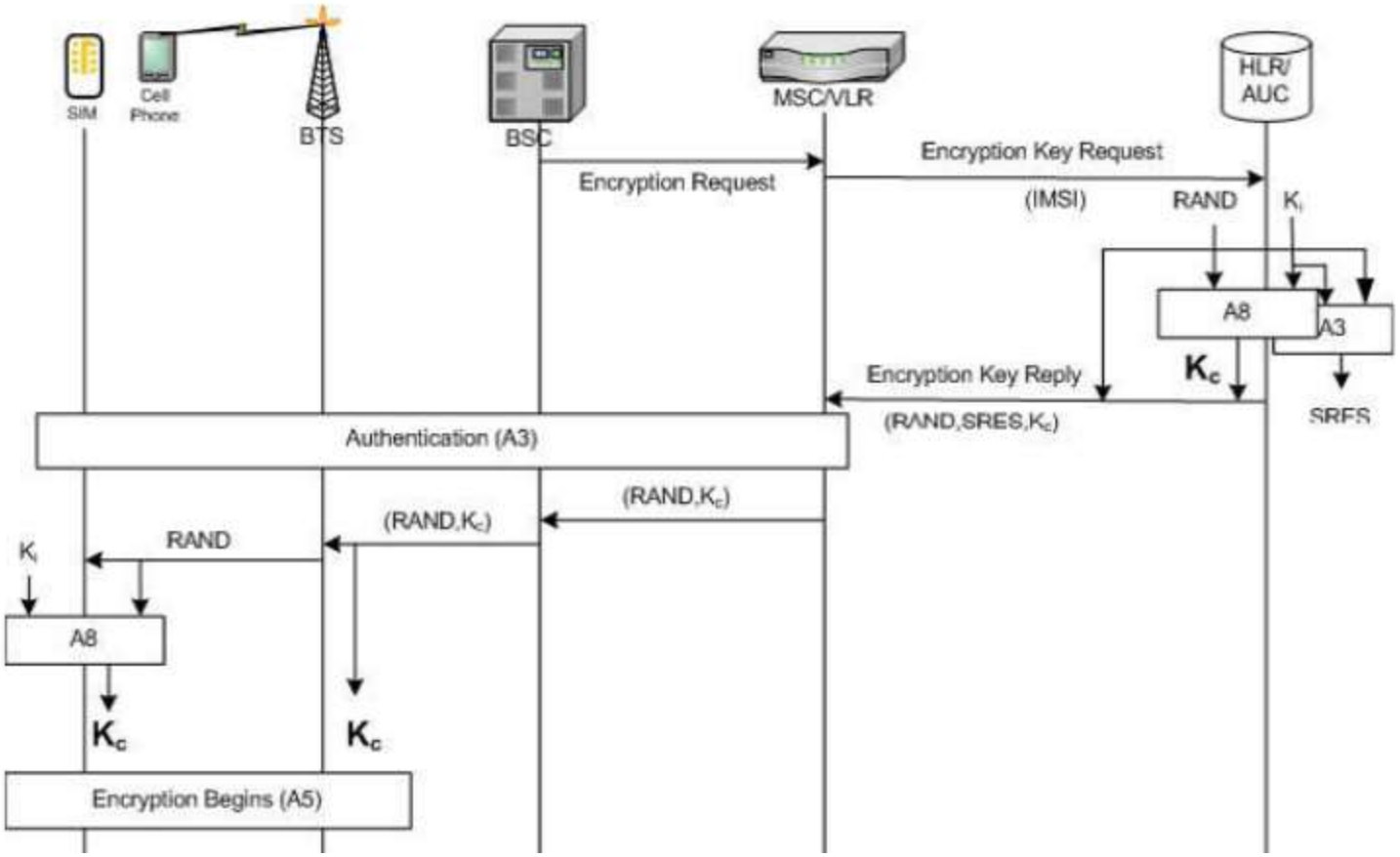
Seguridad de las Redes Móviles

Autenticación GSM. GSM AKA (Authentication and Key Agreement)



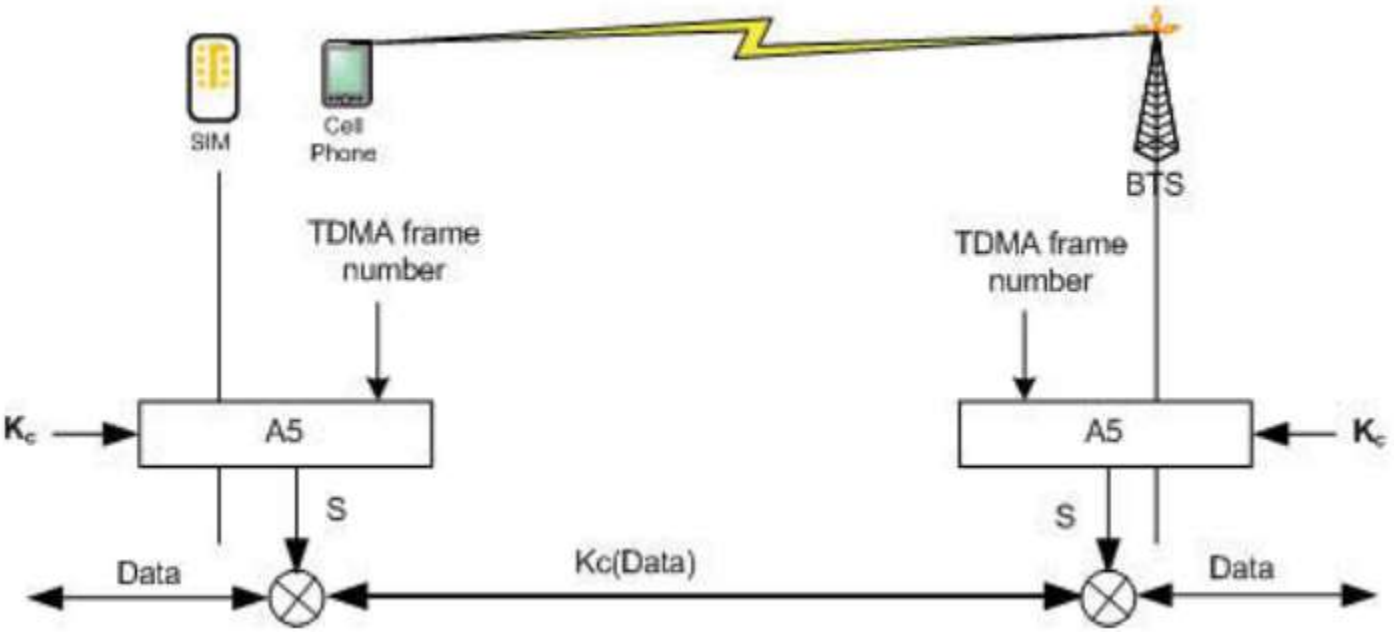
Seguridad de las Redes Móviles

Generación de la clave de encriptación en GSM



Seguridad de las Redes Móviles

Encriptación GSM



Problemas de seguridad en GSM

Como estrategia de seguridad adicional las redes móviles han empleado tradicionalmente el principio de "**security through obscurity**". Los algoritmo de encriptación (AX) nunca han sido oficialmente publicados. Muchos de estos algoritmos han sido estudiados mediante ingeniería inversa y sometidos a criptoanálisis, dejando al descubierto algunas fallas.

M. Briceno, I. Goldberg, D. Wagner, "Internet Security, Applications, Authentication and Cryptography (ISAAC)", http://www.issac.cs.berkley.edu/issac/gsm-faq.html.

A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of A5/1 on a PC", Lecture Notes in Computer Science, vol. 1978, pp. 1-18, 2001.

¿Cómo protegerse de la interferencia intencionada?

La interferencias intencionada (**jamming**) es una transmisión que deliberadamente bloquea o interfiere una comunicación inalámbrica.

Las técnicas de **espectro expandido** son un mecanismo eficaz para **combatir las interferencias intencionadas**. Además las técnicas de espectro expandido incrementan la **resistencia a la interferencia natural** y **previenen** la **detección no autorizada** de la señal de radio.

Técnicas de espectro expandido

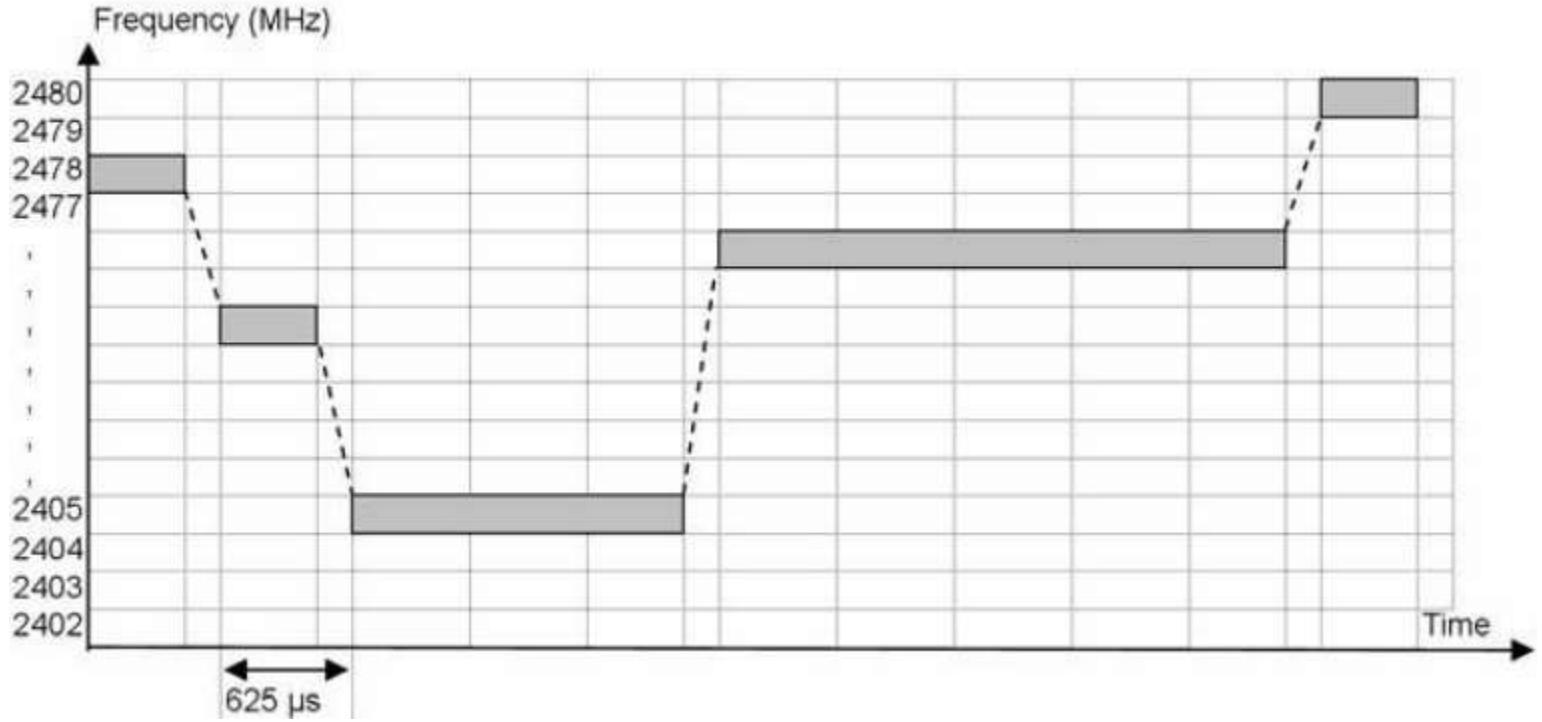
Las técnicas espectro expandido expanden la señal en el dominio de la frecuencia, resultando en una ancho de banda de transmisión mucho mayor que el mínimo necesario para transmitir la información. Entre las técnicas de espectro expandido más empleadas se encuentran las técnicas de salto de frecuencia (**Frequency Hopping, FH**) y de secuencia directa (**Direct Sequence, DS**).

Salto de Frecuencia (FH)

El espectro expandido por salto de frecuencia consiste en una **conmutación rápida de la portadora** en una amplia gama de bandas de frecuencia, usando una **secuencia pseudoaleatoria** conocida por el transmisor y el receptor

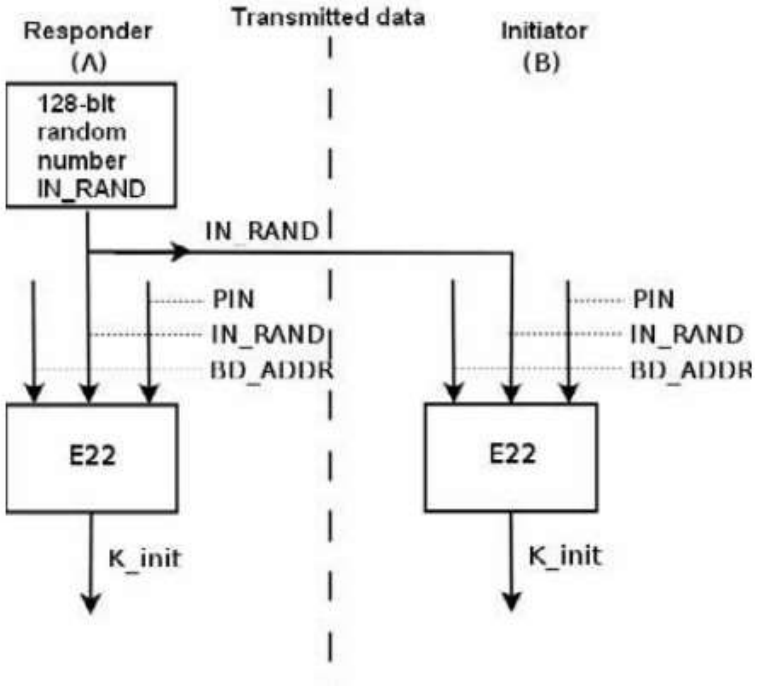
Protección de Bluetooth contra interferencias

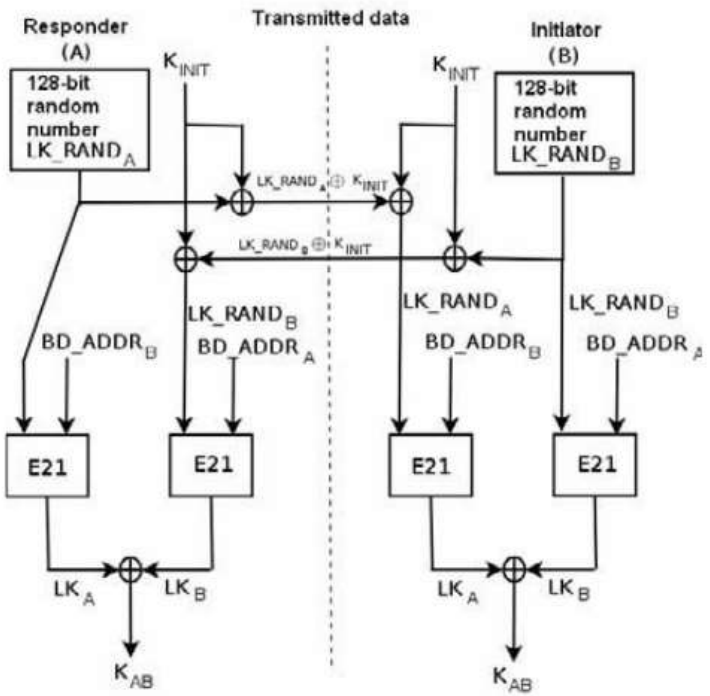
Bluetooth implementa un mecanismo de salto de frecuencia **adaptativo** (AFH) utilizando 79 canales físicos de 1 MHz en la banda ISM (Industrial, Scientific and Medical)



Encriptación de data en Bluetooth

Existen tres modos de seguridad en Bluetooth: no seguro, seguridad a nivel de servicio y seguridad a nivel de enlace.





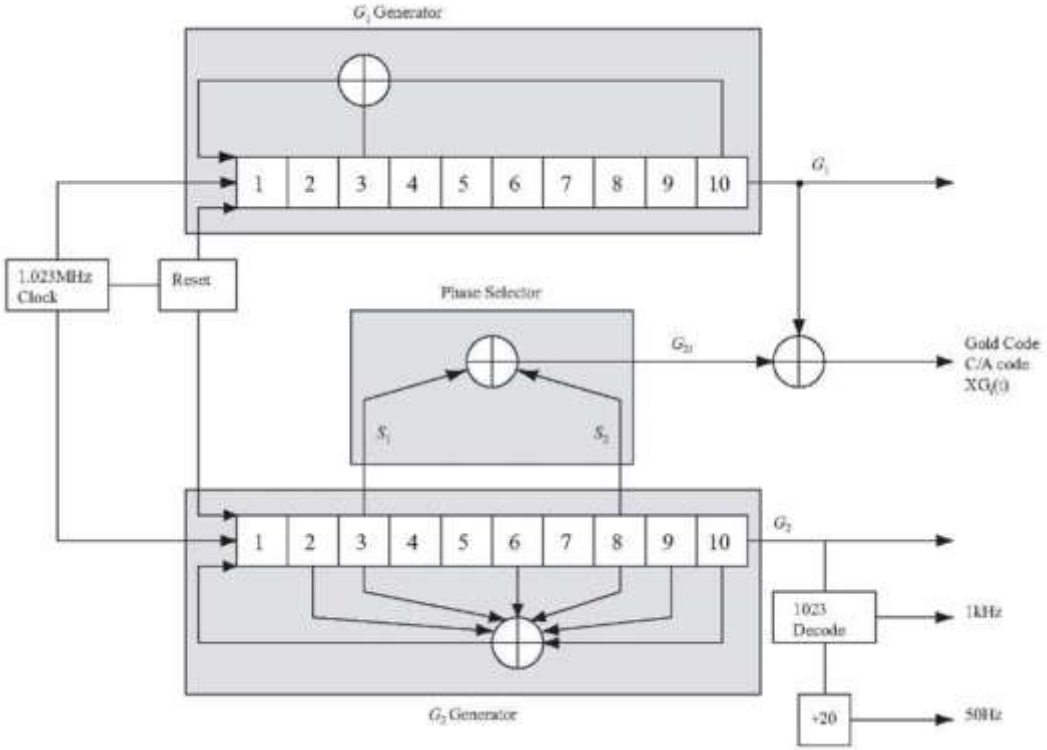
NIST SP 800-121 Revision 1, Guide to Bluetooth Security. http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf

Secuencia Directa (DS)

En la técnica de espectro expandido de secuencia directa la señal a transmitir se usa para modular una secuencia pseudoaleatoria de pulsos (**código PN**) de corta duración (mayor ancho de banda). Este código debe ser conocido por le receptor para recuperar la señal transmitida. Esta técnica es la base de los sistemas **CDMA**

Sistema de Posicionamiento Global

GPS emplea la técnica de espectro expandido de secuencia directa para la transmisión. Cada satélite (32) utiliza un código PN diferente para la transmisión.

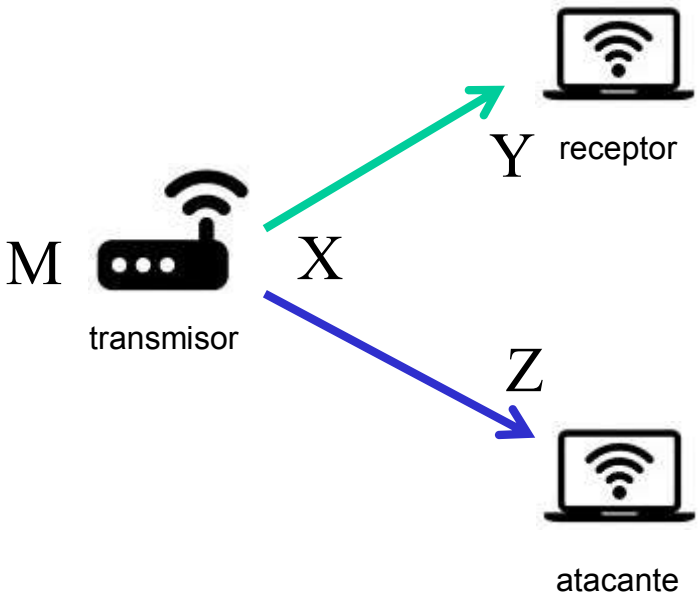


Seguridad de la capa física

La principio fundamental relacionado con la seguridad de la física (**PLS, Physical Layer Security**)es emplear la **aleatoriedad del ruido y del canal** de comunicaciones para limitar la cantidad de información que puede ser extraída por un receptor no autorizado. Este acercamiento a la seguridad se basa en la **teoría de la información** y cuenta con una solida **fundamentación matemática.**

PLS sin claves

Se basa en la asunción de que el canal entre el transmisor y la escucha no autorizada es una versión probabilísticamente degradada del canal principal



$$R\text{-}Re = I(\mathrm{M};\mathrm{Z}) \sim 0$$

Wyner, Aaron D. "The wire-tap channel." The bell system technical journal 54.8 (1975): 1355-1387.

Generación de claves en la capa física

En canales con mucho desvanecimiento el canal es caracterizado por los extremos de la comunicación, esto es pares de usuarios diferentes observan diferente información del estado del canal (**CSI, Channel State Information**). Esta información puede ser usada por los usuarios legítimos para acordar una clave basado en el principio de **secreto perfecto**.

Maurer, Ueli M. "Secret key agreement by public discussion from common information." IEEE Transactions on Information Theory 39.3 (1993): 733-742.

Limitaciones de la seguridad de la capa física

- Se basa en asumir que la naturaleza del ruido y del canal de comunicaciones exhibe un comportamiento significativamente diferente entre los usuarios legítimos y el atacante.
- Hasta el presente existen muchos estudios teóricos y pocas implementaciones prácticas

Internet de la Cosas (IoT)

- La interconexión de dispositivos físicos, vehículos, edificaciones y otros elementos representa un reto desde el punto de la seguridad.
- Las Redes de Sensores Inalámbricos (**WSN**) es una de las tecnologías dominantes dentro de la IoT.
- Las características de los nodos en WSN (**limitado poder de computo y suministro de energía**) representan un desafío para implementar mecanismo de seguridad confiables.
- Numerosos son los incidentes reportando fallas de dispositivos con algún tipo de acceso inalámbrico.
- Las cosas se complican: **La Internet de Todo (IoE)**

Posibles trabajos futuros

- Diseño de esquemas de seguridad que tengan en cuenta las peculiaridades de cada tecnología (Ej. WSN, IoE).

- Mejora, adaptación a escenarios reales, implementación y verificación de los estudios teóricos relacionados con la seguridad de la capa física.

- Diseños cross-layer con un enfoque multidimensional que integren de los diferentes mecanismo de seguridad para aumentar sus prestaciones.

Universidad Central “Marta Abreu” de Las Villas
Facultad de Ingeniería Eléctrica
Dpto. Telecomunicaciones y Electrónica

UNIMINUTO
Corporación Universitaria
Minuto de Dios

¡Gracias!

Dr. Vitalio Alfonso Reguera
Profesor Titular, Facultad de Ingeniería Eléctrica
Departamento de Telecomunicaciones y Electrónica
UCLV, vitalio@uclv.edu.cu

Colombia, 2016