



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Estudio de Vulnerabilidades en Redes Tácticas LINK.

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Julio César Martín Martín.

DIRECTOR: José María Núñez Ortuño.

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo

MARTIN
MARTIN
JULIO CESAR |
29437292Y

Firmado digitalmente por MARTIN
MARTIN JULIO CESAR |29437292Y
Nombre de reconocimiento (DN): c=ES,
o=MINISTERIO DE DEFENSA,
ou=PERSONAS, ou=CERTIFICADO
ELECTRONICO DE EMPLEADO PUBLICO,
serialNumber=IDCES-29437292Y,
sn=MARTIN MARTIN |2943 7292Y,
givenName=JULIO CESAR, cn=MARTIN
MARTIN JULIO CESAR |29437292Y
Motivo: Soy el autor de este documento
Fecha: 2025.01.29 01:43:21 +01'00'



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Estudio de Vulnerabilidades en Redes Tácticas LINK.

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

UniversidadeVigo

RESUMEN

El Trabajo de Fin de Máster analiza las vulnerabilidades en redes tácticas **Link**, sistemas críticos en operaciones militares modernas para el intercambio seguro y en tiempo real de información entre unidades militares. Estos enlaces, como **Link 11**, **Link 16** y **Link 22**, son vitales para coordinar actividades en el campo de batalla, mejorar la conciencia situacional y facilitar decisiones estratégicas rápidas.

El documento destaca los desafíos de seguridad enfrentados por estos sistemas debido a amenazas cibernéticas y electrónicas sofisticadas, como interceptación, interferencias (*jamming*), suplantación de señales (*spoofing*) y ataques de denegación de servicio (*DoS*). Además, aborda problemas como la dependencia de infraestructuras antiguas, limitaciones en el ancho de banda y complejidades en la configuración.

El trabajo también explora medidas de mitigación, como cifrado avanzado, autenticación robusta, protección contra interferencias y tecnologías de detección de intrusiones. Se evalúan las características y mejoras técnicas de cada enlace, desde la simplicidad de Link 11 hasta la capacidad antijamming y la interoperabilidad avanzada de Link 16 y Link 22.

En un entorno militar donde la ciberseguridad es crucial, se subraya la importancia de una estrategia integral que combine actualización tecnológica, capacitación en seguridad y cooperación internacional. El estudio concluye que la modernización y protección de estos sistemas son esenciales para garantizar la eficacia operativa, la seguridad nacional y la resiliencia frente a ataques futuros.

PALABRAS CLAVE

TDL, Operaciones, Vulnerabilidad, Mitigación, Cifra.

AGRADECIMIENTOS

A mis Padres, por su apoyo incondicional durante todos mis años de formación. Nunca dejaron de creer.
A mi mujer y mis hijos, por su apoyo y comprensión durante la realización de este Máster. Muchas horas invertidas que trataré de devolverles.

Entre todos han hecho posible que yo me encuentre hoy aquí.

A mi tutor de este TFM, José María, por sus recomendaciones y su guía, una luz en las tinieblas de este oscuro mundo de los TDL.

Tabla de contenido

1	Introducción.....	5
1.1	Contexto General.	5
1.2	Justificación.	8
1.3	Objetivos del Trabajo.....	9
2	Marco Teórico.	11
2.1	Enlace de datos tácticos Link 11.....	11
2.2	Enlace de Datos Tácticos Link 11B.....	14
2.3	Enlace de Datos Tácticos Link 16.....	16
2.4	Enlace de datos tácticos Link 22.....	24
2.5	Comparativa entre Link 11B, Link 16 y Link 22.....	28
2.6	Protocolo JREAP.	30
2.7	Estándar de intercambio de mensajes VMF.....	33
2.8	Importancia operacional de los TDL.	36
2.9	Principios de seguridad en los TDL.....	37
3	Vulnerabilidades en los Enlaces de Datos Tácticos.	41
3.1	Vulnerabilidades identificadas en Link 11.....	41
3.2	Vulnerabilidades identificadas en Link 16.....	43
3.3	Vulnerabilidades identificadas en Link 22.....	45
3.4	Vulnerabilidad por Sincronismo en TDL.....	47
4	Análisis de Casos de Estudio de vulnerabilidades.	51
4.1	Interferencia y Spoofing de TDL en un Ejercicio Multinacional OTAN.	51
4.2	Ataques de Denegación de Servicio (DoS) sobre TDL en un Escenario de Entrenamiento.	53
4.3	Vulnerabilidades explotadas en sistemas TDL obsoletos.	55
5	Estrategias de Mitigación y Mejora de la Seguridad en TDL.	57
5.1	Cifrado Avanzado en TDL.....	57
5.2	Autenticación Robusta en TDL.....	64
5.3	Consideraciones sobre tecnologías de cifrado y autenticación en TDL Modernos.	69
5.4	Monitorización y Detección de Intrusiones en TDL.....	69
5.5	Actualización y Parcheo Regular de los Sistemas en TDL.....	72
5.6	Protección Antijamming.	76
5.7	Capacitación y Concienciación en Seguridad.....	80
6	Discusión y Análisis.....	83
6.1	Análisis Comparativo de los Métodos de Mitigación.....	83

6.2 Limitaciones de las Soluciones Actuales.....	84
6.3 Futuro de la Seguridad en los TDL.....	87
7 Conclusiones.	89
7.1 Resumen de Hallazgos Principales.	89
7.2 Implicaciones de los Resultados.	91
7.3 Recomendaciones Finales.	92
8 Referencias.	93

INDICE DE FIGURAS.

Figura 1-1. Empleo de enlaces de datos tácticos en una operación aliada [1].	5
Figura 1-2. Visor Operacional Común (COP) sobre un GIS.	7
Figura 2-1. Arquitectura de Link 11 con PU1 haciendo de NCS.	11
Figura 2-2. Pila de protocolos en Link 11.	12
Figura 2-3. Comunicación terrestre alámbrica punto a punto con Link 11B.	15
Figura 2-4. Concepto de Net (subred) en Link 16. [2]	17
Figura 2-5. Terminales MIDS LVT y FDL. [2]	21
Figura 2-6. Empleo de Link 22 en un despliegue táctico. [1]	24
Figura 2-7. Link 22 puede gestiona mensajes de la serie F y de la serie J, nativos de Link 16. [1]	26
Figura 2-8. Link 22 puede utilizar UHF para LOS y HF para BLOS. [1]	27
Figura 2-9. Despliegue de una Super Network en Link 22.	28
Figura 2-10. Empleo de JREAP-A junto a otros TDL en Ejercicio Aliado (US, FRA & SP).	30
Figura 2-11. Despliegue táctico con interoperabilidad entre JREAP y Link 16.	32
Figura 2-12. Terminal táctico que permite enviar/recibir mensajes VMF. [3]	33
Figura 4-1. Interferencia y Spoofing en TDL en un ejercicio multinacional OTAN. [2]	51
Figura 4-2. Ataque DOS simulado en un ejercicio de entrenamiento.	53
Figura 4-3. Despliegue naval empleando TDL obsoletos.	55
Figura 5-1. Equema de cifrado simétrico [2].	58
Figura 5-2. Equema de cifrado asimétrico.	58
Figura 5-3. Esquema de cifrado híbrido.	59
Figura 5-4. Esquema de cifrado en HSM.	60
Figura 5-5. Esquema de cifrador de flujo.	61
Figura 5-6. Esquema de cifrado homomórfico.	61
Figura 5-7. Esquema de PKI.	62
Figura 5-8. Esquema del Handshake en el protocolo TLS 1.3.	65
Figura 5-9. Esquema de autenticación basada en tokens.	66
Figura 5-10. Esquema de autenticación basada datos biométricos.	66
Figura 5-11. Esquema de protocolo Zero-Knowledge Proofs.	67
Figura 5-12. Esquema de despliegue de 2 IPS (Principal + Alternativo) en una TDL.	71

INDICE DE TABLAS.

Tabla 2-1. Generalidades entre Link 11B, Link 16 y Link 22.	28
Tabla 2-2. Capacidades técnicas entre Link 11B, Link 16 y Link 22.	29
Tabla 2-3. Ventajas/Desventajas entre Link 11B, Link 16 y Link 22.	29
Tabla 2-4. Aplicaciones tácticas de Link 11B, Link 16 y Link 22.	29
Tabla 5-1. Evaluación de los métodos de cifrado.	63
Tabla 5-2. Comparativa de métodos de cifrado entre Link 11, Link 16 y Link 22.	64
Tabla 5-3. Comparativa de métodos de autenticación de Link 11, Link 16 y Link 22.	68
Tabla 5-4. Comparativa de actualizaciones y parcheo entre Link 11, Link 16 y Link 22.	74
Tabla 5-5. Comparativa de actualizaciones entre Link 11, Link 16 y Link 22.	76
Tabla 5-6. Comparativa anti-jamming completa entre Link 11, Link 16 y Link 22.	78
Tabla 5-7. Comparativa anti-jamming resumida entre Link 11, Link 16 y Link 22.	80
Tabla 6-1. Comparativa de métodos de mitigación sobre TDL.	83

1 INTRODUCCIÓN.

1.1 CONTEXTO GENERAL.

Los **Enlaces de Datos Tácticos (TDL¹)** son sistemas de comunicación esenciales que permiten la transferencia segura y en tiempo real de información entre unidades militares como aviones, buques, vehículos terrestres y centros de mando. Estas redes permiten compartir datos críticos, como la posición de tropas y vehículos, la identificación de amenazas y la situación operativa, aspectos clave para tomar decisiones rápidas y coordinadas en situaciones de combate. Este concepto queda perfectamente reflejado en la figura 1-1, empleando para ello el TDL Link 22.

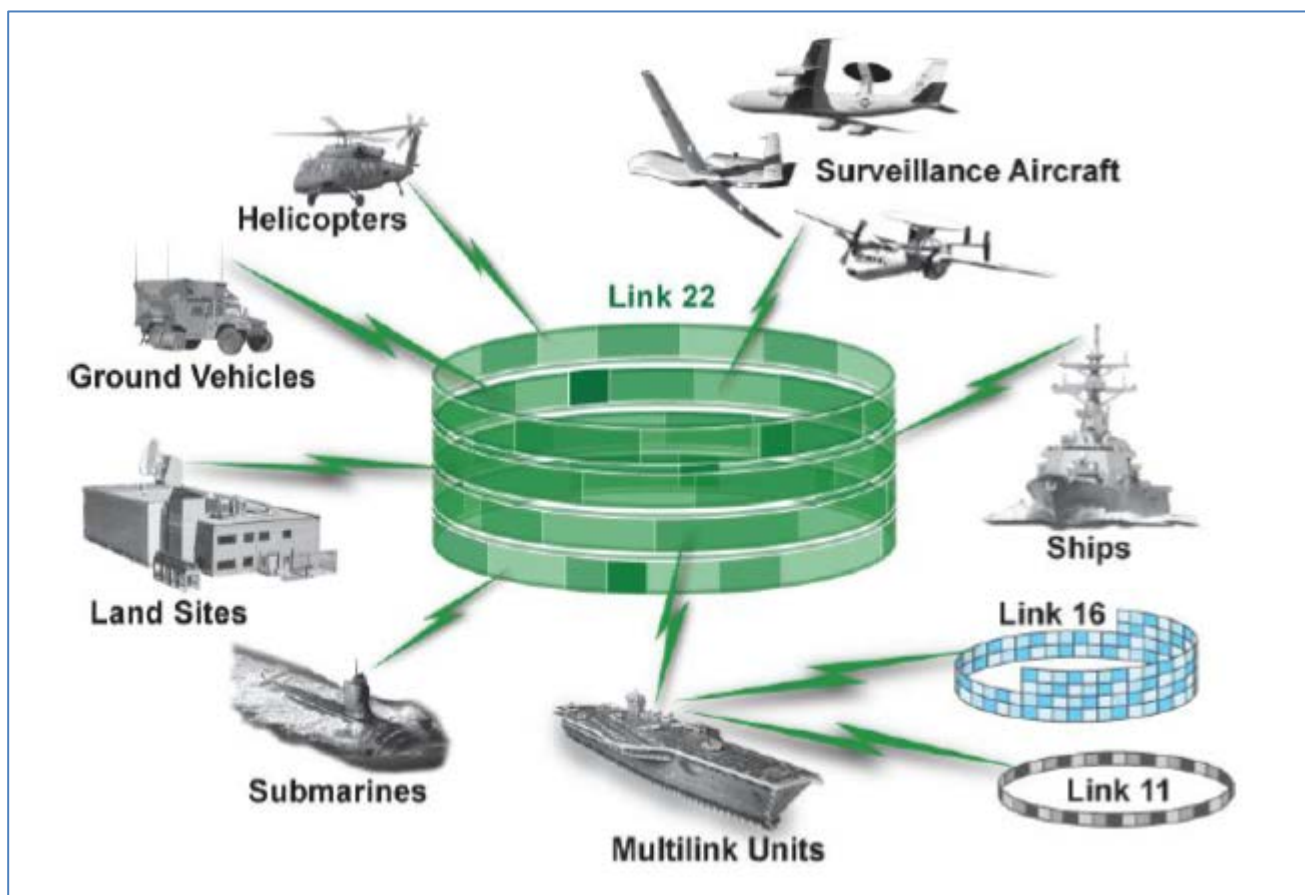


Figura 1-1. Empleo de enlaces de datos tácticos en una operación aliada [1].

En el contexto de las operaciones militares modernas, los TDL se han vuelto fundamentales para optimizar la coordinación y la respuesta táctica, proporcionando a los comandantes una visión completa y actualizada del entorno de batalla. Ejemplos de sistemas TDL ampliamente utilizados son **Link 16** y **Link 22**, ambos desarrollados con protocolos de seguridad diseñados para proteger la integridad y confidencialidad de la información.

Sin embargo, debido a la naturaleza de los conflictos actuales, donde las amenazas cibernéticas y electrónicas son cada vez más sofisticadas, los TDL enfrentan un conjunto significativo de **vulnerabilidades**. Las operaciones modernas dependen de sistemas interconectados y frecuencias de radio que, aunque protegidos, siguen expuestos a ataques de adversarios que intentan interceptar, manipular o bloquear estas comunicaciones. Las vulnerabilidades en los TDL incluyen:

¹ Tactical Data Links.

- **Intercepción de Datos:** Los adversarios pueden interceptar las transmisiones y acceder a información crítica si el cifrado es insuficiente o si existen brechas de seguridad en el protocolo.
- **Spoofing²:** La manipulación de datos para introducir información falsa puede confundir a las fuerzas y hacer que tomen decisiones equivocadas.
- **Interferencia Electrónica (Jamming³):** Al interferir las señales de los TDL, los atacantes pueden bloquear la comunicación entre las unidades, lo que dificulta las operaciones coordinadas.
- **Ataques de Denegación de Servicio (DoS⁴):** Estos ataques pueden saturar el sistema con datos, causando interrupciones y reduciendo la disponibilidad del enlace.

El incremento en la dependencia de los TDL también está acompañado de desafíos de **ciberseguridad**, ya que estos sistemas deben protegerse continuamente de ataques que evolucionan con rapidez. Además, los adversarios no solo intentan explotar vulnerabilidades tecnológicas, sino que también emplean estrategias para explotar **errores humanos y fallos organizacionales**, lo que subraya la necesidad de un enfoque integral de seguridad que considere tanto el aspecto técnico como el humano.

Para reducir estos riesgos, las fuerzas armadas y los desarrolladores de sistemas de defensa están invirtiendo en **tecnologías de cifrado, autenticación avanzada, detección de intrusiones y capacitación en ciberseguridad**. Sin embargo, la complejidad y los altos costes asociados a la modernización de los TDL siguen siendo barreras significativas, especialmente en tiempos de restricciones presupuestarias.

En resumen, los TDL son herramientas vitales para la comunicación táctica en el campo de batalla, pero están expuestos a un conjunto de vulnerabilidades que pueden ser explotadas con facilidad si no se aplican medidas de seguridad robustas. La comprensión y mitigación de estas vulnerabilidades son esenciales para preservar la seguridad y efectividad de las operaciones militares.

IMPORTANCIA DE LOS TDL EN OPERACIONES MILITARES MODERNAS.

Los **Enlaces de Datos Tácticos (TDL)** desempeñan un papel crucial en las **operaciones militares modernas**, donde la capacidad de respuesta rápida y la coordinación precisa son vitales para el éxito en combate. Los TDL permiten que diversas unidades militares, como aviones, buques, vehículos terrestres y centros de mando, se conecten en una red común para compartir información en tiempo real. Esta comunicación directa y continua facilita la interoperabilidad entre fuerzas nacionales y aliadas, proporcionando una ventaja táctica crucial en situaciones de conflicto.

² El **spoofing** es un tipo de robo de identidad que ocurre en los medios digitales y electrónicos. A través de esta práctica ilegal, las personas extraen información sensible de sus víctimas, la cual aprovechan para cometer actos delictivos.

³ El jamming o interferencia electrónica intencionada es la transmisión de señales de radiocomunicación de forma deliberada para perturbar la transmisión de otra señal de radio.

⁴ Denial of Service (DoS): Un ataque de denegación de servicio, tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática.



Figura 1-2. Visor Operacional Común (COP) sobre un GIS.

Los TDL permiten la integración de múltiples plataformas de combate en un **visor operacional común (COP⁵)**. En la figura 1-2 se muestra un COP desplegado sobre un GIS⁶. Gracias a esta conectividad, los comandantes pueden recibir y enviar información clave sobre el campo de batalla, como la ubicación de fuerzas propias y enemigas, identificaciones de amenaza, estado en el que se encuentran los diferentes recursos y objetivos prioritarios, en segundos. Esta capacidad de comunicación en tiempo real permite la creación de un "mapa común" de la situación operativa, lo que resulta esencial para **mejorar la toma de decisiones**, anticiparse a amenazas, y coordinar movimientos tácticos.

La comunicación en tiempo real a través de los TDL permite:

1. **Mejorar la toma de decisiones:** Los datos precisos y actualizados en tiempo real permiten que los comandantes en todos los niveles de la operación puedan realizar decisiones informadas y rápidas, esencial en contextos de combate donde cada segundo, cuenta.
2. **Incremento de la seguridad nacional:** Los TDL facilitan la protección de los territorios nacionales al permitir una respuesta militar más rápida y coordinada a amenazas externas. La integración de fuerzas aliadas y la capacidad de compartir inteligencia a través de enlaces seguros es esencial para la defensa colaborativa y para la prevención de ataques.
3. **Maximización de la eficiencia y efectividad en combate:** Los TDL permiten optimizar los recursos militares, evitando acciones duplicadas y minimizando riesgos para las tropas. Al tener un panorama completo y compartido, los comandantes pueden posicionar las unidades en el momento y lugar correctos, eliminando tiempos muertos y errores derivados de la falta de información o de la información desactualizada.
4. **Reducción de la confusión y la niebla de guerra:** Con un flujo continuo de información entre diferentes plataformas y unidades, los TDL ayudan a reducir la incertidumbre que caracteriza las situaciones de combate, mejorando la comprensión de las intenciones y movimientos del enemigo y facilitando una rápida adaptación del combate.

⁵ COP: Common Operational Picture.

⁶ GIS: Geographical Information System.

5. **Adaptación ante amenazas emergentes:** Al integrar datos de inteligencia de múltiples fuentes en tiempo real, los TDL proporcionan una mayor agilidad para enfrentar amenazas emergentes, ajustando posiciones y adaptando el plan de acción conforme a cambios en el campo de batalla.

IMPACTO EN LA SEGURIDAD NACIONAL.

Los TDL no solo optimizan las operaciones militares en combate, sino que son una **herramienta estratégica** en la defensa de la seguridad nacional. En un contexto donde las amenazas cibernéticas, los conflictos híbridos y los desafíos transnacionales están en aumento, contar con redes de comunicación seguras y en tiempo real permite a las fuerzas armadas mantenerse en constante vigilancia y responder eficazmente a crisis inesperadas. Además, los TDL facilitan la colaboración internacional al permitir una interoperabilidad segura con aliados, lo que fortalece la defensa común y la disuasión ante amenazas hostiles.

Se puede concluir que los Enlaces de Datos Tácticos representan el **nervio central de la comunicación militar moderna**, al habilitar la coordinación táctica, la protección nacional y la superioridad en combate. La efectividad de los TDL en el campo de batalla depende de su capacidad para transmitir información crítica de manera rápida y segura, y su implementación es fundamental para cualquier nación que busque mantener la soberanía y la seguridad de sus fuerzas. Sin los TDL, el riesgo de acciones desacopladas, la descoordinación y la vulnerabilidad frente a ataques aumentaría significativamente, comprometiendo así la efectividad operativa y, en última instancia, la seguridad nacional.

1.2 JUSTIFICACIÓN.

En el contexto de las operaciones militares modernas, los **Enlaces de Datos Tácticos (TDL)** han emergido como componentes críticos para el éxito de las misiones, permitiendo la transmisión de información en tiempo real y una coordinación eficaz entre distintas unidades. Sin embargo, esta interconectividad y dependencia de redes seguras también incrementan la **superficie de ataque**, exponiendo los TDL a un amplio espectro de amenazas cibernéticas y electrónicas. En los últimos años, los **ciberataques** a infraestructuras militares han aumentado en frecuencia y sofisticación, y los sistemas de comunicación tácticos no son la excepción.

Estudiar las vulnerabilidades en los TDL es una prioridad por las siguientes razones:

1. **Evolución de las amenazas cibernéticas:** Las capacidades de los adversarios en el ámbito cibernético crecen constantemente, con herramientas avanzadas para interceptar, manipular o bloquear las comunicaciones. Ataques como el jamming (interferencia), spoofing (suplantación de señales) o incluso ataques de denegación de servicio (DoS) se están utilizando en conflictos globales para degradar la efectividad de las fuerzas armadas. Comprender estas vulnerabilidades en profundidad es crucial para desarrollar defensas efectivas que mantengan la integridad de las comunicaciones tácticas.
2. **Protección de la Seguridad Nacional:** Dado que los TDL son esenciales para la defensa y la soberanía, cualquier vulnerabilidad explotada podría comprometer misiones, exponer información crítica e, incluso, llevar a la pérdida de vidas. Un ataque exitoso contra los TDL podría desarticular las capacidades de respuesta de las fuerzas militares y permitir que el adversario obtenga ventaja estratégica. Por tanto, el estudio de estas vulnerabilidades no solo protege las operaciones militares, sino que es una inversión en la seguridad nacional y la disuasión ante posibles amenazas externas.
3. **Interoperabilidad y colaboración con aliados:** Las fuerzas armadas de diferentes naciones dependen de la interoperabilidad de los TDL para coordinar operaciones conjuntas. Sin embargo, una vulnerabilidad en un sistema TDL de una nación puede comprometer la seguridad de toda la

alianza. La revisión constante de las vulnerabilidades en los TDL es fundamental para asegurar la integridad de la colaboración internacional y el éxito en misiones conjuntas.

4. **Adaptación y modernización tecnológica:** Los TDL fueron diseñados en una época en la que las amenazas cibernéticas no tenían el alcance actual. Aunque se han actualizado con el tiempo, los cambios en el entorno cibernético y la evolución de las tácticas de guerra requieren un enfoque de ciberseguridad adaptable y continuo. Un estudio exhaustivo de las vulnerabilidades en los TDL facilita el desarrollo de estrategias de modernización para proteger estos sistemas críticos en el contexto actual y preparar la infraestructura para las amenazas del futuro.
5. **Optimización de la inversión en defensa:** La investigación en vulnerabilidades permite priorizar inversiones en aquellas áreas que realmente incrementen la seguridad y la resiliencia de los TDL, asegurando que el gasto en defensa sea eficiente y dirigido hacia la protección de los sistemas más críticos.

En conclusión, el estudio de las vulnerabilidades en los TDL no solo responde a las crecientes amenazas cibernéticas que enfrentan las infraestructuras militares, sino que también es fundamental para la defensa de la seguridad nacional, la eficiencia operativa, y el mantenimiento de la superioridad táctica en el campo de batalla. Identificar y mitigar estas vulnerabilidades es una responsabilidad estratégica para las fuerzas armadas, que deben estar preparadas para operar con eficacia en un entorno donde la guerra cibernética y la tecnología avanzan a un ritmo sin precedentes.

1.3 OBJETIVOS DEL TRABAJO.

OBJETIVOS GENERALES.

- Analizar **las vulnerabilidades existentes en los enlaces de datos tácticos** empleados en sistemas de comunicaciones militares y de defensa.
- **Identificar riesgos y amenazas potenciales** que puedan comprometer la seguridad, integridad y disponibilidad de la información transmitida a través de estos enlaces.

OBJETIVOS ESPECÍFICOS.

- **Describir el funcionamiento técnico de los enlaces de datos tácticos**, sus protocolos y estándares (ej., Link 16, Link 22, etc.).
- **Evaluar las principales vulnerabilidades técnicas** en los enlaces de datos tácticos, como interceptación, interferencias, ciberataques y fallos de autenticación.
- **Investigar casos reales o simulados de incidentes de seguridad** en los enlaces de datos tácticos, para entender los métodos de ataque y sus consecuencias.
- **Proponer medidas de mitigación** para minimizar las vulnerabilidades identificadas, incluyendo herramientas de encriptación, autenticación robusta y tecnologías anti-jamming.
- **Analizar la evolución futura de las amenazas** a estos enlaces y explorar tecnologías emergentes que puedan fortalecer su seguridad.
- **Evaluar la importancia de la cooperación internacional** en la estandarización y mejora de las comunicaciones tácticas seguras.

2 MARCO TEÓRICO.

2.1 ENLACE DE DATOS TÁCTICOS LINK 11.

Link 11, también conocido como **TADIL-A (Tactical Digital Information Link - A)**, es un enlace de datos tácticos desarrollado para la transmisión de información táctica en tiempo real entre unidades militares. Este sistema se utilizaba principalmente en operaciones conjuntas navales, aéreas y terrestres para coordinar datos críticos como posiciones de unidades, rastreo de objetivos y planificación de misiones. Aunque limitado en comparación con estándares modernos, su simplicidad y alcance en HF/UHF lo hacen útil para operaciones específicas en entornos menos dinámicos o como respaldo en sistemas de comunicación actuales.

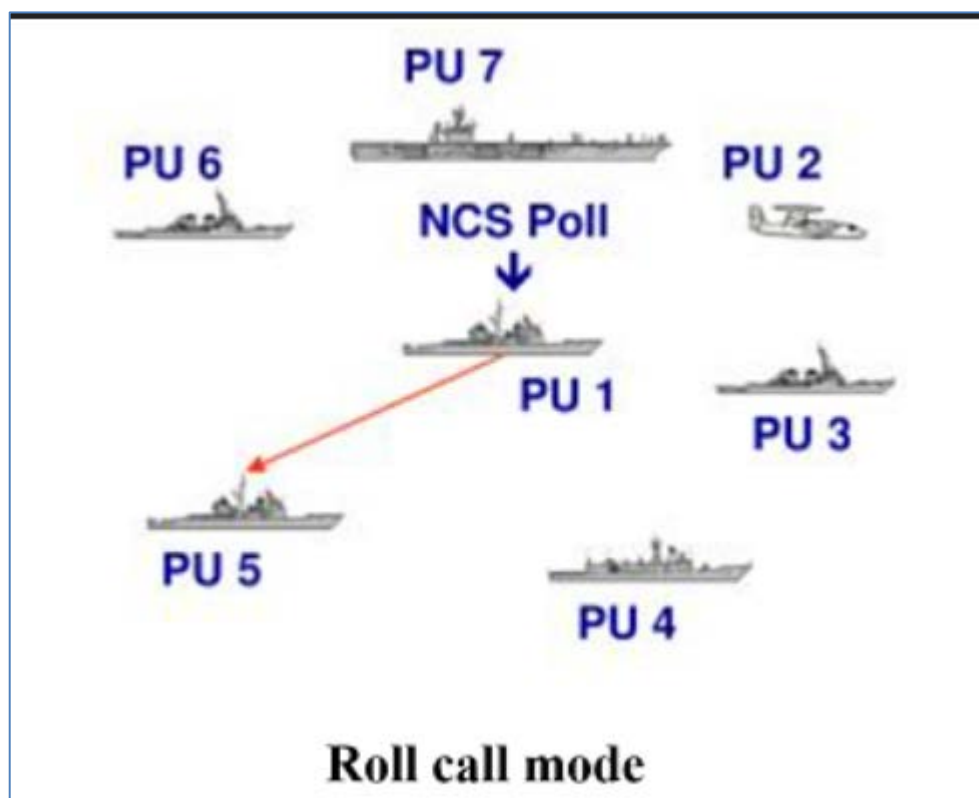


Figura 2-1. Arquitectura de Link 11 con PU1 haciendo de NCS.

CARACTERÍSTICAS PRINCIPALES.

1. Tipo de Red:

- o El Link 11 opera como una **red semidúplex** basada en el modelo **net control station (NCS)**, donde un nodo actúa como controlador central de la red mientras los demás transmiten bajo su coordinación. En la figura 2-1, mas arriba, puede verse un despliegue naval donde la unidad participante nº 1 (PU 1) ejerce la función de NCS para el resto de unidades.

2. Protocolos y Estándares:

- o Emplea el protocolo **DTS (Data Terminal Set)** para transmitir y recibir datos.
- o Utiliza el formato de mensajes estándar de la OTAN **STANAG 5511**, permitiendo la interoperabilidad entre aliados.

3. Frecuencias de Operación:

- o Opera en bandas **HF (Alta Frecuencia)** y **UHF (Ultra Alta Frecuencia)**, lo que le permite alcanzar rangos de comunicación tanto cortos como largos:
 - HF: Usada para largas distancias.
 - UHF: Usada para comunicaciones de línea de vista (LOS⁷).
- 4. **Velocidad de Transmisión:**
 - o Ofrece velocidades relativamente bajas de datos (entre **600 y 2400 bits por segundo**), lo suficiente para transmitir información táctica básica, pero limitada en comparación con sistemas más modernos como el Link 16.
- 5. **Codificación y Seguridad:**
 - o Incorpora técnicas de **encriptación y autenticación** para proteger la confidencialidad e integridad de la información transmitida.

APLICACIONES OPERATIVAS.

1. **Interoperabilidad Multiplataforma:**
 - o Diseñado para conectar **buques, aeronaves, submarinos y unidades terrestres** en una red táctica común.
 - o Proporciona una base para compartir datos de radar, inteligencia electrónica y otras fuentes en operaciones conjuntas.
2. **Control y Rastreo Táctico:**
 - o Permite el intercambio de datos sobre posiciones de objetivos (amigos y enemigos) y estados operativos en tiempo real.
3. **Escenarios de Operación:**
 - o Es utilizado en misiones navales para coordinar flotas y aeronaves.
 - o También es valioso en operaciones de defensa aérea y vigilancia.

La pila de protocolos de **Link-11** (véase más abajo la figura 2-2) está diseñada para habilitar la comunicación táctica entre plataformas militares mediante un sistema estandarizado de intercambio de datos. Este sistema opera principalmente en el dominio naval, aunque también se utiliza en aplicaciones aéreas y terrestres. A continuación, se describe la pila de protocolos Link-11, desde las capas físicas hasta las aplicaciones.

PILA DE PROTOCOLOS EN LINK 11.

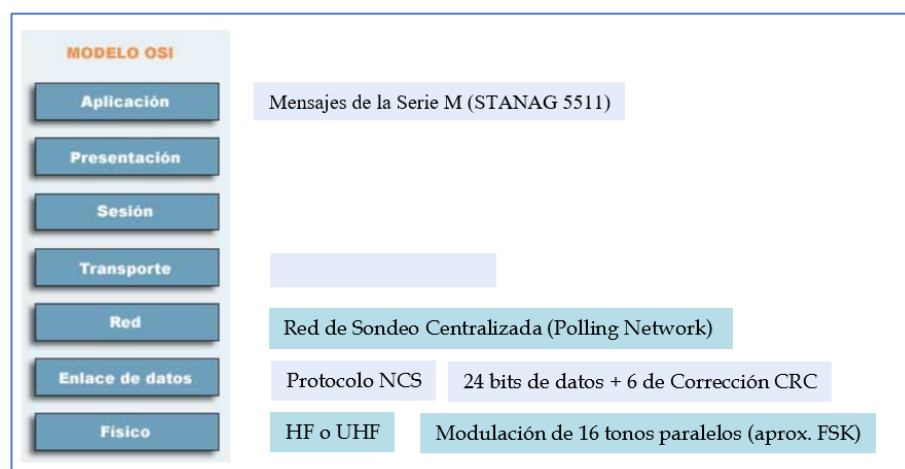


Figura 2-2. Pila de protocolos en Link 11.

⁷ LOS: Line Of Sight.

CAPA DE ENLACE DE DATOS.

La capa de enlace de datos en Link-11 gestiona el formato de los mensajes y las operaciones para garantizar una transmisión confiable.

- **Protocolo de enlace:**
 - o Utiliza el **Protocolo de Control de Acceso de Red (Net Control Station, NCS)**.
 - o Funciona en un esquema de **Polling** centralizado:
 - Una estación controladora de red (NCS) interroga secuencialmente a cada nodo en la red para enviar o recibir datos.
 - Este esquema minimiza las colisiones, pero introduce latencia.
- **Formato de los mensajes:**
 - o Utiliza **palabras de 30 bits**, compuestas por:
 - 24 bits de datos.
 - 6 bits de corrección de errores para proporcionar protección frente a errores de transmisión.
- **Corrección de errores:**
 - o Implementa detección de errores mediante códigos de verificación de redundancia cíclica (CRC) y corrección básica de errores.

CAPA DE RED.

La capa de red en Link-11 define cómo se estructura y gestiona la red táctica.

- **Topología:**
 - o La red opera como una **red de sondeo centralizada** (Polling Network), con la estación NCS como el nodo central que controla el acceso al medio.
 - o Todos los nodos responden a las consultas del NCS en un orden predeterminado.
- **Direcciones:**
 - o Cada nodo tiene una **identificación única** asignada para participar en la red.
- **Gestión de la red:**
 - o Las tareas del NCS incluyen:
 - Coordinar las comunicaciones.
 - Detectar nodos inactivos o no disponibles.
 - Redistribuir los tiempos de sondeo según sea necesario.

CAPA DE TRANSPORTE.

En Link 11, la capa de transporte asegura la entrega confiable de los mensajes a través de mecanismos de retransmisión.

- **Retransmisión de datos:**
 - o Si un nodo no responde durante su turno en el esquema de sondeo, el NCS puede retransmitir la solicitud o pasar al siguiente nodo.
- **Optimización del uso del canal:**
 - o La capa de transporte puede ajustar el ciclo de sondeo para evitar retrasos innecesarios o mejorar la eficiencia en condiciones de alta carga.

CAPA DE APLICACIÓN.

La capa de aplicación gestiona el contenido específico de los datos intercambiados en la red Link 11.

- **Mensajes tácticos:**
 - o Los mensajes están estandarizados según la **OTAN STANAG 5511** y la especificación **TADIL-A**.
 - o Los tipos de mensajes incluyen:
 - **Rastreo de objetivos** (posiciones de aeronaves, barcos, submarinos, etc.).
 - **Datos de control de armas** (designación de objetivos).
 - **Actualizaciones de estado** (condiciones operativas y ambientales).
- **Formato de mensajes:**
 - o Los datos tácticos se empaquetan en un formato estructurado conocido como **Serie de Mensajes M** (M-Series Messages), utilizado ampliamente en los enlaces de datos tácticos.

VENTAJAS Y LIMITACIONES DE LINK 11.

VENTAJAS.

- **Interoperabilidad:**
 - o Permite que plataformas militares de diferentes países compartan datos tácticos de manera estandarizada.
- **Resiliencia en HF:**
 - o Su capacidad de operar en HF permite comunicaciones más allá de la línea de vista (BLOS⁸).
- **Protección básica contra errores:**
 - o El esquema de corrección de errores proporciona una tolerancia limitada a las condiciones adversas del canal.

LIMITACIONES.

- **Velocidad de datos limitada:**
 - o No es adecuado para la transmisión de grandes volúmenes de datos, como imágenes o video.
- **Latencia alta:**
 - o El esquema de sondeo centralizado introduce retrasos en la transmisión.
- **Obsolescencia tecnológica:**
 - o Aunque sigue en uso, Link 11 está siendo reemplazado por **Link 16** y **Link 22**, que ofrecen mayor capacidad y seguridad.

2.2 ENLACE DE DATOS TÁCTICOS LINK 11B.

El **Link 11B** es un estándar de comunicación militar que pertenece a la familia de los enlaces de datos tácticos. Es utilizado para la transmisión de información táctica entre unidades terrestres o estacionarias dentro de una red de defensa. Este sistema de enlace opera de manera similar al **Link 11**, pero está diseñado específicamente para proporcionar comunicaciones **terrestres punto a punto** (véase, más abajo, la figura 2-3) en lugar de comunicaciones aéreas o marítimas.

⁸ BLOS: Beyond Line Of Sight.

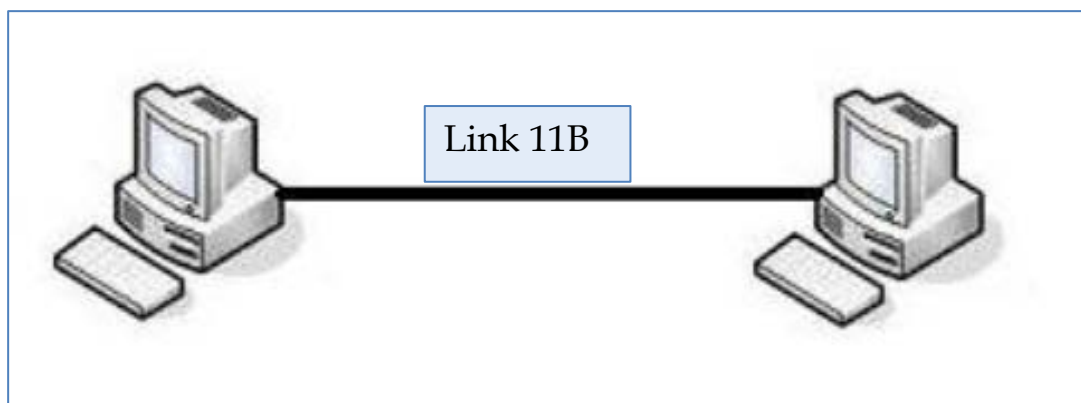


Figura 2-3. Comunicación terrestre alámbrica punto a punto con Link 11B.

CARACTERÍSTICAS PRINCIPALES.

1. **Tipo de Red:**
 - o Es un enlace de datos **sincrónico y punto a punto**, lo que significa que las unidades están directamente conectadas en pares para la transferencia de datos.
 - o A diferencia del Link 11, que puede usar ondas de radio HF/UHF, el Link 11B utiliza principalmente **medios cableados** (como líneas terrestres) o enlaces seguros.
2. **Protocolos de Comunicación:**
 - o Emplea un protocolo conocido como **TDMA (Time Division Multiple Access)**, que asegura que las comunicaciones se realicen en intervalos de tiempo específicos asignados a cada nodo.
3. **Tipo de Información Transmitida:**
 - o Datos tácticos y operativos, como posiciones de unidades amigas y enemigas, asignaciones de objetivos, estados de sistemas de armas, e información de mando y control.
 - o Es compatible con la representación de datos en el **Formato de Mensajes Estándar (Standard Tactical Data Exchange Format, STANAG 5511)**.
4. **Codificación y Seguridad:**
 - o Utiliza mecanismos de **encriptación y autenticación** para garantizar la seguridad y confidencialidad de los datos transmitidos. Esto es crucial en operaciones militares para evitar la interceptación o manipulación por parte de adversarios.
5. **Velocidad y Capacidad:**
 - o Ofrece una velocidad de transmisión moderada comparada con los estándares modernos, pero suficiente para las necesidades tácticas en operaciones terrestres estacionarias.

APLICACIONES OPERATIVAS.

1. **Interoperabilidad:**
 - o Permite la interoperabilidad entre diversas plataformas terrestres en operaciones conjuntas, especialmente en unidades de defensa aérea y sistemas de vigilancia.
2. **Conexión con Otros Enlaces Tácticos:**
 - o Funciona en conjunto con el Link 11 (para unidades aéreas y marítimas) y el Link 16 (más avanzado), brindando una red de comunicación robusta.
3. **Entornos de Operación:**
 - o Está diseñado para operar en **entornos terrestres protegidos** o áreas con infraestructura fija, como bases militares o centros de mando.

LIMITACIONES.

1. **Alcance y Movilidad:**

- o Debido a su naturaleza punto a punto y al uso de medios terrestres, tiene un alcance limitado comparado con enlaces más avanzados como el Link 16.

2. **Dependencia de Infraestructura:**

- o Requiere líneas físicas o enlaces específicos, lo que limita su uso en escenarios de alta movilidad o en operaciones expedicionarias.

3. **Obsolescencia Relativa:**

- o Aunque sigue siendo útil en ciertos escenarios, el Link 11B está siendo progresivamente reemplazado por tecnologías más modernas, como el **Link 16** y otros enlaces digitales.

2.3 ENLACE DE DATOS TÁCTICOS LINK 16 [2].

INTRODUCCIÓN.

El Link 16 es un sistema de enlace de datos tácticos completamente integrado en las operaciones de los Servicios Conjuntos, las fuerzas de la Organización del Tratado del Atlántico Norte (OTAN) y otros aliados. Para la Armada de los Estados Unidos, el Link 16 comenzó a operar en febrero de 1994 con la instalación de terminales JTIDS Clase II.

El propósito general del Link 16 es el mismo que el de los sistemas Link 4A, Link 11 y Link 11B: el intercambio de datos tácticos en tiempo real entre unidades militares. Aunque el Link 16 comparte este objetivo con sus predecesores, también incluye elementos de intercambio de datos que ellos no tienen, además de proporcionar mejoras significativas como:

- Operación sin nodos centrales.
- Resistencia a interferencias (antijamming).
- Flexibilidad en las comunicaciones.
- Seguridad separada para la transmisión y los datos.
- Mayor número de participantes.
- Incremento en la capacidad y velocidad de datos.
- Funciones de navegación relativas.
- Localización e identificación precisa de participantes.
- Capacidad de voz segura y digitalizada.

ARQUITECTURA.

El Link 16 utiliza el principio de **Acceso Múltiple por División de Tiempo (TDMA)**, por sus siglas en inglés), una función automática del terminal Link 16. La arquitectura TDMA utiliza un sistema de intercalado temporal para proporcionar múltiples redes de comunicación aparentemente simultáneas. Todas las Unidades JTIDS⁹ (JUs) tienen preasignados intervalos de tiempo específicos tanto para transmitir como para recibir datos de otras unidades.

- Cada intervalo de tiempo tiene una duración de **1/128 de segundo**, es decir, **7.8125 milisegundos (ms)**.
- Hay disponibles **51 frecuencias** para las transmisiones JTIDS.

⁹ JTIDS: Joint Tactical Information Distribution System. Es un sistema de radio en red de acceso múltiple por división de tiempo distribuido (DTDMA) de banda L utilizado por el Departamento de Defensa de los Estados Unidos y sus aliados para respaldar las necesidades de comunicaciones de datos, principalmente en la comunidad de defensa aérea y de misiles. Produce una señal de espectro ensanchado utilizando la modulación por desplazamiento de frecuencia (FSK) y la modulación por desplazamiento de fase (PSK) para distribuir la potencia radiada en un espectro más amplio (gama de frecuencias) que las transmisiones de radio normales. Esto reduce la susceptibilidad al ruido, las interferencias y las intercepciones.

- La frecuencia no permanece constante durante un intervalo de tiempo; en su lugar, cambia rápidamente (cada 13 microsegundos) siguiendo un patrón pseudorandom preestablecido, técnica conocida como **salto de frecuencia**.

Esto marca una mejora significativa respecto al Link 11, que opera en una sola frecuencia fija.

REDES Y SUBREDES (NETS).

Una **red Link 16** es un conjunto de participantes sincronizados que comparten un entendimiento común de los límites de los intervalos de tiempo. La colección completa de intervalos de tiempo utilizados por todos los participantes puede considerarse una red.

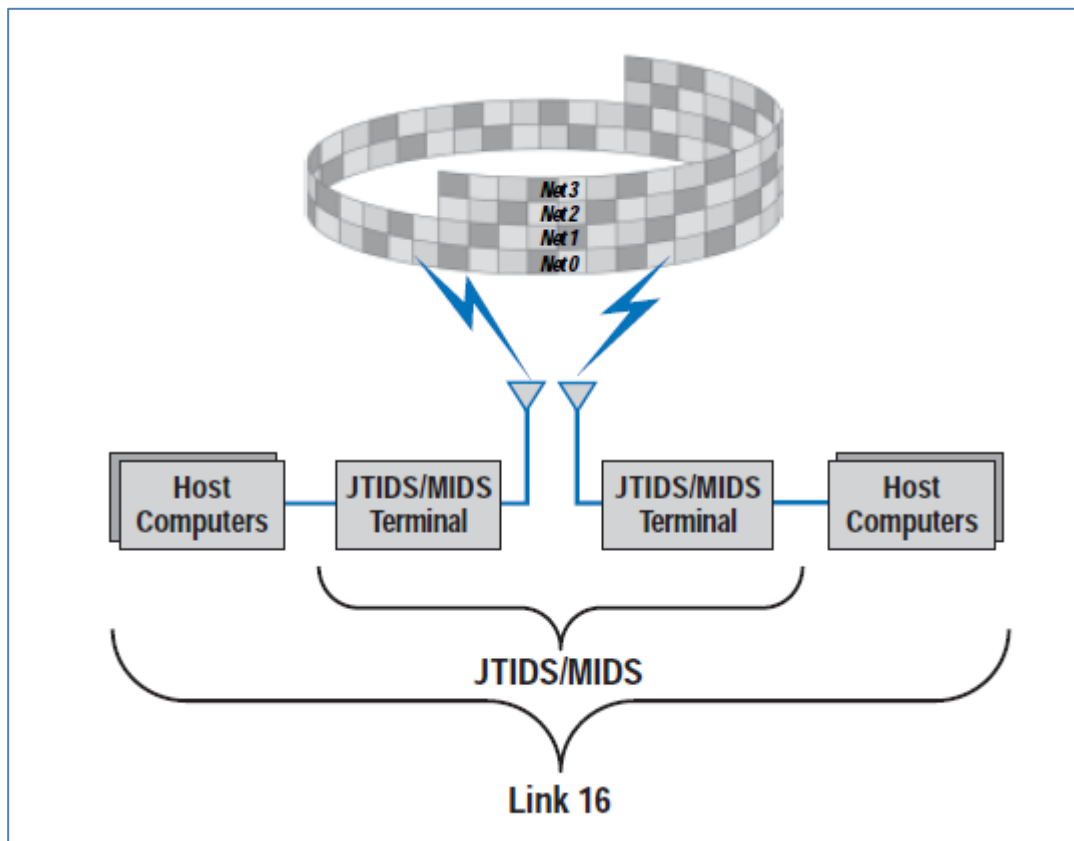


Figura 2-4. Concepto de Net (subred) en Link 16. [2]

Por otro lado, una **subred (net)** es un subconjunto de intervalos de tiempo dentro de una red Link 16, así como de los participantes que comparten esos intervalos de tiempo (véase, más arriba, la figura 2-4). Las subredes del Link 16 se diferencian por sus patrones de salto de frecuencia.

Características de las subredes:

- Una red Link 16 puede consistir en una o más subredes.
- Existen **128 números posibles de subredes**, numeradas del 0 al 126, siendo la subred 127 reservada para uso especial (designada como "Sin Declaración").
- Por lo general, en la ejecución de una red, solo se utilizan de **tres a seis subredes** al mismo tiempo.

INTERCAMBIO DE DATOS.

El Link 16 transmite mensajes que pueden estar compuestos por 3, 6 o 12 palabras de datos en un intervalo de tiempo de **7.8125 ms**, dependiendo de la estructura de empaquetado utilizada:

- **Estructura Estándar:** 3 palabras (210 bits).
- **Empaquetado-2:** 6 palabras (420 bits).
- **Empaquetado-4:** 12 palabras (840 bits).

Cada palabra de datos del Link 16 contiene **70 bits**, análoga a un marco del Link 11. Los mensajes pueden ser de tres tipos:

1. **Formato fijo:** Utilizados para los mensajes de la serie J, con detección y corrección de errores (EDAC).
2. **Texto libre:** Empleados para voz o mensajes sin codificación estructurada.
3. **Formato variable:** Permiten longitud flexible para mensajes específicos.

Los mensajes J-series, codificados con EDAC, permiten tasas efectivas de transmisión de datos tácticos de:

- **26,880 bps** (3 palabras por intervalo).
- **53,760 bps** (6 palabras por intervalo).
- **107,520 bps** (12 palabras por intervalo).

Esto representa una mejora significativa respecto al Link 11, permitiendo reportar **2 a 3 veces más elementos tácticos** en el mismo período de tiempo.

CARACTERÍSTICAS DE LA ARQUITECTURA DEL LINK 16.

El Link 16 introduce varias características clave que mejoran significativamente las comunicaciones tácticas:

1. **Operación sin Nodos:**
 - o A diferencia del Link 11, que requiere una Estación de Control de Red (NCS) para mantener la comunicación, el Link 16 no depende de un nodo central.
 - o Los intervalos de tiempo son preasignados a cada participante, lo que permite que la red funcione independientemente de la participación de cualquier unidad específica.
 - o Los elementos más cercanos a un nodo en el Link 16 son:
 - **Referencia de Tiempo de Red (NTR):** Necesaria para sincronizar y establecer la red.
 - **Unidades de Relé:** Para extender la cobertura más allá de la línea de visión (LOS).
2. **Seguridad:**
 - o Tanto el mensaje como la transmisión están encriptados:
 - **MSEC:** Encriptación de los datos del mensaje.
 - **TSEC:** Encriptación de la forma de onda JTIDS, incluyendo patrones de salto de frecuencia y ruido pseudoaleatorio.
3. **Grupos de Participación en la Red (NPGs):**
 - o Los intervalos de tiempo de una subred pueden asignarse a uno o más **Grupos de Participación de la Red (NPG)**, que se definen por su función y los tipos de mensajes que transmiten. Ejemplos de NPGs:
 - NPG 7: Vigilancia.
 - NPG 9: Control Aéreo.

- NPG 19: Comunicaciones entre Combatientes.

4. **Capacidad Multirred (Multinetting):**

- o El Link 16 puede soportar hasta **127 redes simultáneas**, permitiendo realizar múltiples funciones (por ejemplo, control aéreo y comunicaciones entre combatientes) al mismo tiempo en diferentes subredes.
- o El uso de multiredes se facilita mediante la separación de datos en patrones de salto de frecuencia únicos, determinados por el número de subred y la variable criptográfica TSEC.

CAPACIDADES MEJORADAS O NUEVAS.

- **Direcciones:**

Cada participante, conocido como Unidad JTIDS (JU, por sus siglas en inglés), recibe una dirección única.

- o En el Link 16, las direcciones son números octales de cinco dígitos (00001 – 77777).
- o Esto representa una mejora significativa respecto a las direcciones de tres dígitos del Link 11/11B, que permitían hasta 177 participantes.
- o Las direcciones dentro del rango 00001 – 00177 son equivalentes a las del Link 11/11B, lo que permite interoperabilidad.

- **Números de Seguimiento (Track Numbers, TN):**

- o Los TN en el Link 16 tienen cinco caracteres alfanuméricos (00001 – 77777 o 0A000 – ZZ777), permitiendo hasta **524,284** números de seguimiento únicos.
- o En comparación, el Link 11/11B solo admite TN de cuatro dígitos (0001 – 7777), con un límite de **4,092** números.
- o Este incremento permite asignar bloques permanentes de números de seguimiento a unidades individuales, garantizando una mayor capacidad operativa.

- **Calidad de Seguimiento (Track Quality, TQ):**

- o El Link 16 utiliza un campo TQ de cuatro bits, con valores que varían de 0 a 15, donde el valor más alto indica una precisión de posición mejor a 15,24 metros.
- o Por contraste, el Link 11/11B emplea un campo TQ de tres bits, con un valor máximo de 7 y una precisión mucho menor (posiblemente mayor a 5556 metros).

- **Identificación de Seguimiento:**

- o Las capacidades de identificación en el Link 16 se han ampliado considerablemente, permitiendo clasificar pistas según:
 - Tipo de plataforma.
 - Actividad.
 - Tipo específico.
 - Nacionalidad.
- o También introduce nuevas categorías de identificación, como **Neutral** y **Sospechoso** (en lugar de "Desconocido, Presunto Enemigo").

INFORMACIÓN DE ESTADO DE UNIDADES AMIGAS.

El Link 16 permite un informe mucho más detallado del estado de las unidades amigas, que incluye:

- Estado de los equipos.
- Inventario exacto de armamento, incluyendo tipos de misiles terrestres específicos.
- Canales de radar y misiles activos.
- Cantidad de combustible disponible para transferencias.
- Capacidad de las armas (como cañones).

- Tiempos estimados de llegada y salida (ETA¹⁰ y ETD¹¹) a estaciones asignadas.

GRANULARIDAD INCREMENTADA.

La granularidad, o precisión en el reporte de datos, ha mejorado en el Link 16, especialmente en:

- **Posición de pistas:** Incremento de precisión en coordenadas.
- **Velocidades aéreas:** Se pueden reportar datos más detallados.
- **Altitudes:** Se registra con mayor exactitud.
- **Líneas y Áreas:**
 - o Las líneas pueden ser multisegmentadas.
 - o Las áreas no tienen restricciones de forma (círculos, elipses, rectángulos, etc.).

POSICIONAMIENTO GEODÉSICO.

El Link 16 emplea un sistema de coordenadas tridimensional basado en **latitud, longitud y altitud**, permitiendo reportar posiciones en cualquier parte del mundo.

- Esto representa una mejora respecto al sistema bidimensional cartesiano del Link 11/11B, que limita el reporte de posiciones a un rango cercano a la unidad reportante.
- El Link 16 utiliza el sistema de referencia **WGS-84 (World Geodetic Survey 1984)**.

NAVEGACIÓN RELATIVA.

El Link 16 permite que las unidades determinen su ubicación relativa entre sí mediante la función de **Navegación Relativa Automática (RELNAV)**.

- RELNAV mide el tiempo de llegada (TOA) de mensajes Precise Participant Location and Identification (PPLI) enviados por otras JUs.
- Estas mediciones permiten que los terminales de la red se mantengan sincronizados y actualicen continuamente su posición geodésica.

CAPACIDADES DE GUERRA ELECTRÓNICA (EW).

El Link 16 ofrece capacidades significativamente superiores en guerra electrónica, incluyendo:

- Intercambio de datos paramétricos EW.
- Mayor control y órdenes relacionadas con EW.
- Capacidad para transmitir información de productos EW en el Grupo de Participación en la Red (NPG) de Vigilancia.

PISTAS Y PUNTOS TERRESTRES.

El Link 16 agrega una categoría especial para pistas y puntos terrestres:

- **Puntos terrestres:** Describen objetos físicos, como edificios.
- **Puntos de referencia:** Usados para constructos teóricos, como estaciones o waypoints.

¹⁰ ETA: Estimated Time of Arrival.

¹¹ ETD: Estimated Time of Departure.

- **Pistas terrestres:** Representan objetos móviles, como tanques.

MENSAJES DE LA SERIE J.

Los **mensajes de la serie J** son el núcleo del sistema Link 16. Estos mensajes están optimizados para transmitir datos tácticos en tiempo real con alta precisión y seguridad. Cada mensaje de la serie J está compuesto por uno o más bloques de datos (70 bits por bloque), organizados en un intervalo de tiempo.

Características clave de los mensajes J-series:

1. **Codificación Reed-Solomon (EDAC):** Asegura la integridad de los datos mediante detección y corrección de errores.
2. **Compatibilidad Multiplataforma:** Los mensajes J-series son comprensibles entre múltiples terminales JTIDS/MIDS (véase, más abajo, la figura 2-5), garantizando interoperabilidad.
3. **Tipos de Información Transmitida:**
 - o Ubicación precisa de unidades amigas y enemigas.
 - o Estado de armas y sistemas.
 - o Datos de vigilancia y control aéreo.
 - o Órdenes operativas.

Cada mensaje tiene un identificador único que define su función específica dentro de la red táctica.



Figura 2-5. Terminales MIDS LVT¹² y FDL¹³. [2]

GRUPOS DE PARTICIPACIÓN (NPGS).

¹² LVT: Low Volume Terminal.

¹³ FDT: Fighter Data Link.

La estructura lógica de la red JTIDS permite asignar capacidad de red a "circuitos virtuales" dedicados a funciones específicas. Estos circuitos, conocidos como Grupos de Participación en la Red (NPG, por sus siglas en inglés), se asignan a los participantes según las necesidades de su misión.

Ejemplos de funciones soportadas por los NPGs:

- Vigilancia
- Ordenación de objetivos entre cazas
- Control aéreo
- Comunicación de guerra electrónica (EW)
- Gestión de misión y control de armas
- Comunicaciones de voz seguras

Existen hasta 512 NPGs posibles, de los cuales 30 están asignados a funciones específicas. Las transmisiones en cada NPG consisten en mensajes que soportan su función particular. Por ejemplo, las plataformas de mando y control (C2) operan en todos los NPGs aplicables. El diseño de la red también incluye "mensajes de entrada inicial" y sincronización de ida y vuelta (RTT¹⁴).

ASIGNACIÓN DE RANURAS DE TIEMPO.

La capacidad de red de Link 16 se asigna primero a los NPGs y luego a las unidades JTIDS (JUs) participantes. Las ranuras de tiempo asignadas a cada JU¹⁵ dependen de varios parámetros, como:

- Criptovariables MSEC y TSEC
- Modos de acceso a las ranuras
- Configuración de transmisión, recepción o retransmisión.

El mensaje **OPTASK LINK** comunica esta información a los participantes, especificando también los números de red y los roles de red asignados. Un nuevo concepto llamado **Reasignación Dinámica de Ranuras de Tiempo (TSR)** permite redistribuir dinámicamente la capacidad de las ranuras según las necesidades de los usuarios.

ROLES EN LA RED.

Los roles asignados a una JU en la red determinan sus funciones, como sincronización, navegación y retransmisión de datos. Los principales roles incluyen:

- Referencia de Tiempo de Red (NTR¹⁶)
- Referencia de Posición
- Unidad de Entrada Inicial (IEJU)
- Controlador de Navegación
- Usuario Primario y Secundario
- Unidad Retransmisora (FJU)

El rol de NTR es crítico para establecer el tiempo del sistema y sincronizar la red. Durante las operaciones, los roles pueden transferirse entre unidades para asegurar la continuidad de la red.

¹⁴ RTT: Round Trip Time.

¹⁵ JU: JTIDS Unit.

¹⁶ NTR: Network Time Reference.

ENTRADA A LA RED.

El protocolo de entrada a la red Link 16 se gestiona mediante mensajes J0.0 transmitidos por el NTR. La sincronización puede ser activa (transmitiendo RTTs) o pasiva (escuchando mensajes PPLI¹⁷ en modo silencio). La sincronización activa permite a las terminales ajustarse al tiempo del sistema en segundos, mientras que la pasiva utiliza la llegada de mensajes PPLI para calcular el tiempo.

LOCALIZACIÓN PRECISA DE PARTICIPANTES E IDENTIFICACIÓN.

Las terminales JTIDS utilizan navegación relativa (RELNAV) para determinar su posición y transmitirla periódicamente mediante mensajes PPLI. Estos mensajes incluyen:

- Coordenadas geodéticas (latitud, longitud, altitud).
- Curso y velocidad actuales.
- Información de identificación y estado.

NAVEGACIÓN RELATIVA DE TERMINALES.

La función RELNAV permite a las terminales calcular su posición propia con precisión, utilizando el tiempo de llegada (TOA) de los mensajes recibidos. Esto mejora la sincronización y la precisión en operaciones nocturnas o con mal tiempo.

RECEPCIÓN/CONFORMIDAD.

Los participantes deben cumplir con los parámetros de la red definidos, como el rol asignado, las ranuras de tiempo y las criptovariables. La conformidad asegura el correcto funcionamiento de la red.

RELÉS.

Los relés son componentes críticos para extender el alcance de la red Link 16. Las unidades JTIDS/MIDS configuradas como relés retransmiten datos entre terminales fuera de la línea de visión (LOS).

SEGURIDAD EN LAS COMUNICACIONES.

La seguridad en Link 16 se garantiza mediante criptografía robusta y claves TSEC/MSEC, protegiendo los datos transmitidos contra interceptaciones y accesos no autorizados.

- **Cifrado de mensajes (MSEC):** Protege el contenido de los datos transmitidos.
- **Cifrado de transmisión (TSEC):** Protege la forma de onda utilizada para transmitir los datos.

Estas medidas aseguran que las comunicaciones sean resistentes a la interferencia y al acceso no autorizado.

MULTINETTING.

¹⁷ PPLI: Precise Participant Location and Identification.

El multinetting permite que una terminal JTIDS/MIDS opere simultáneamente en múltiples redes. Cada red utiliza diferentes patrones de salto de frecuencia y criptovariables, lo que permite la separación de datos y la flexibilidad operativa.

TÉCNICAS DE EXTENSIÓN DE RANGO.

Para garantizar la conectividad en áreas extensas, se utilizan diversas técnicas de extensión de rango, como:

- Uso de relés para conectar terminales más allá de la LOS.
- Redes apiladas para maximizar la cobertura y minimizar la interferencia.

2.4 ENLACE DE DATOS TÁCTICOS LINK 22 [1].

INTRODUCCIÓN.

Link 22 es un sistema de radio seguro desarrollado por la OTAN para proporcionar comunicaciones más allá de la línea de visión (BLOS) sin necesidad de usar satélites. Este sistema conecta sistemas tácticos de datos terrestres, aéreos, marítimos y submarinos, permitiendo el intercambio de datos tácticos entre las unidades militares de las naciones participantes (véase, más abajo, la figura 2-6). Link 22 se empleará en tiempos de paz, crisis y guerra, apoyando las misiones operativas de la OTAN y de sus aliados.

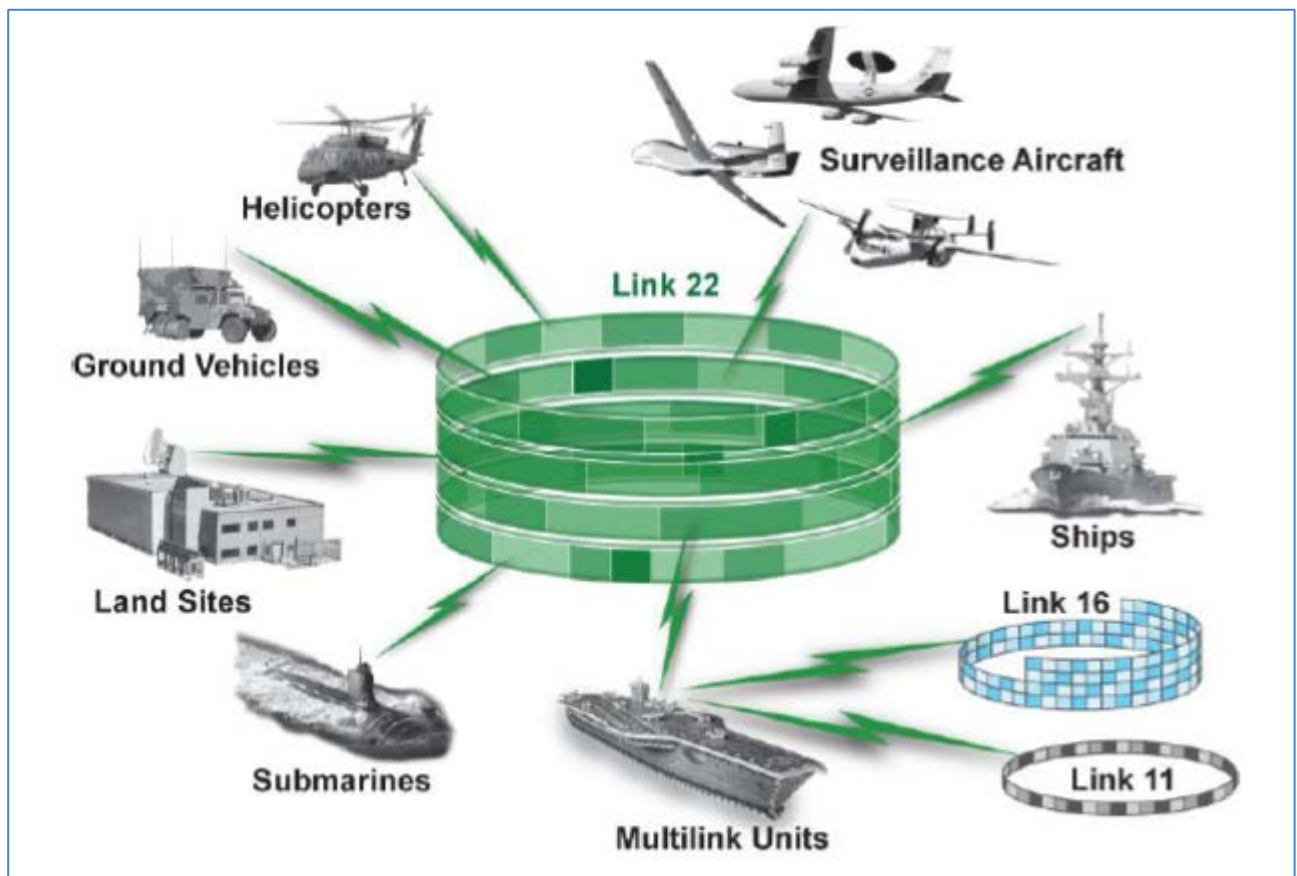


Figura 2-6. Empleo de Link 22 en un despliegue táctico. [1]

El Programa Link 22 fue inicialmente llevado a cabo de forma colaborativa por siete naciones bajo el marco de un Memorando de Entendimiento (MOU, por sus siglas en inglés). Las naciones originales

fueron Canadá, Francia, Alemania, Italia, los Países Bajos, el Reino Unido y los Estados Unidos, siendo estos últimos el país anfitrión. Posteriormente, España reemplazó a los Países Bajos como miembro del programa NILE.

Link 22 fue diseñado para:

- Reemplazar y superar las deficiencias conocidas de Link 11.
- Complementar e interoperar con facilidad con Link 16.
- Facilitar una gestión más automatizada y sencilla que la ofrecida por Link 11 y Link 16.

El programa recibió el nombre de "NATO Improved Link Eleven" (NILE, por sus siglas en inglés), y el enlace táctico de datos creado en el marco de este sistema fue oficialmente designado como Link 22.

SEGURIDAD EN LAS COMUNICACIONES.

Link 22 incorpora un sistema robusto de seguridad en las comunicaciones (COMSEC, por sus siglas en inglés), gracias a un dispositivo integrado de cifrado y descifrado en su sistema. Este componente criptográfico, denominado **Link Level COMSEC (LLC)**, es capaz de:

- Detectar intentos de interferencia o sabotaje en la red.
- Proporcionar un cifrado programable que cumple con la hoja de ruta de modernización criptográfica de la Agencia de Seguridad Nacional de los Estados Unidos (NSA).

Adicionalmente, Link 22 permite aumentar la seguridad de las transmisiones mediante el uso opcional de radios con salto de frecuencia.

MENSAJES TÁCTICOS.

Los datos tácticos en Link 22 se transmiten utilizando mensajes de formato fijo, pertenecientes a la familia **J-Series**, lo que asegura una estandarización con Link 16. Entre las características de estos mensajes se incluyen:

- **Compatibilidad:** Muchos mensajes tácticos de Link 16 pueden transmitirse directamente dentro de Link 22 sin modificaciones.
- **Eficiencia:** Los mensajes específicos de Link 22 están diseñados para ser más compactos y eficientes en el uso del ancho de banda.
- **Optimización:** La priorización y selección de mensajes para transmisión se realiza basándose en los requisitos de calidad de servicio (QoS) y las condiciones operativas.

Link 22 ofrece una gestión avanzada de comunicaciones, reduciendo la necesidad de intervención manual y mejorando la eficiencia en escenarios complejos.

CARACTERÍSTICAS.

Las principales características de Link 22 son:

1. Arquitectura del Sistema:

- o Link 22 utiliza un diseño de comunicación en capas para crear una arquitectura de sistema abierta, con interfaces bien definidas entre los subcomponentes.
- o Esto facilita la extensión del sistema y permite contribuciones de múltiples proveedores.

- o Componentes principales del sistema:
 - **Controlador de Red del Sistema (SNC):** Coordina las funciones de la red.
 - **Cifrado a Nivel de Enlace (LLC):** Asegura la confidencialidad y la integridad de los datos transmitidos.
 - **Controladores de Procesamiento de Señales (SPCs):** Gestionan las señales enviadas y recibidas.
 - **Radios:** Permiten la comunicación mediante frecuencias HF y UHF.
- 2. **Comunicación Segura:**
 - o La seguridad de las comunicaciones se garantiza a través del LLC, que cifra y descifra los datos utilizando claves criptográficas semanales.
 - o Es compatible con radios de salto de frecuencia, mejorando la seguridad de las transmisiones.
 - o Los mensajes tácticos se tratan como "paquetes sellados", lo que permite un nivel adicional de cifrado en los datos tácticos.
- 3. **Transmisión de Mensajes Tácticos:**
 - o Los mensajes tácticos en Link 22 utilizan el formato fijo de la familia J-Series, como en Link 16.
 - o Existen dos tipos de mensajes F-Series (véase, más abajo, la figura 2-7):
 - **Mensajes únicos F-Series:** Diseñados específicamente para Link 22, son versiones más compactas y eficientes de los mensajes de Link 16.
 - **Mensajes FJ:** Encapsulan los mensajes J-Series de Link 16, permitiendo transmitirlos sin modificación.

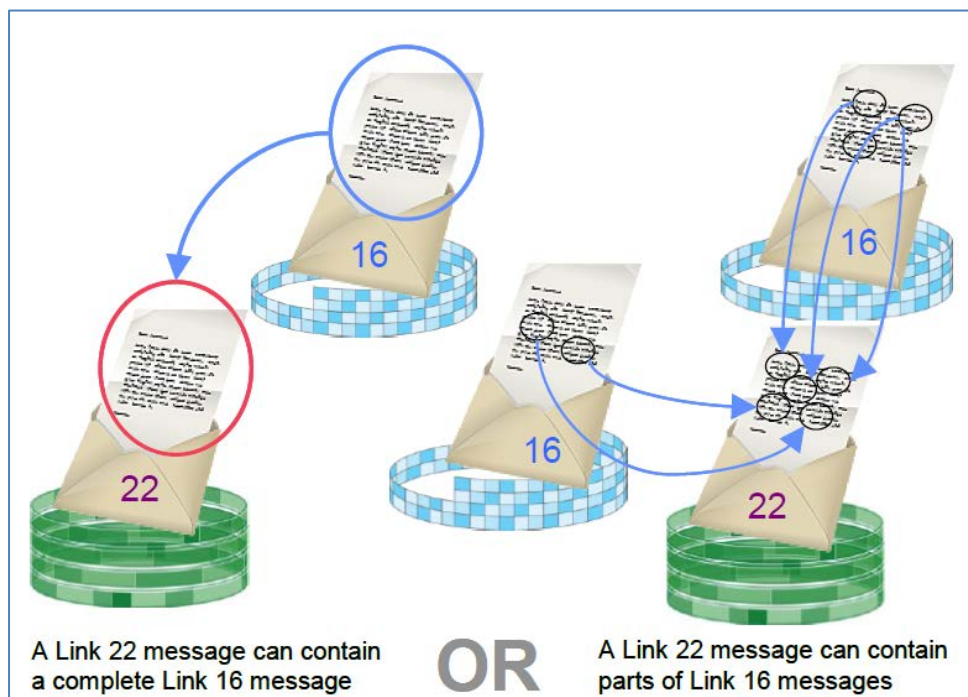


Figura 2-7. Link 22 puede gestionar mensajes de la serie F y de la serie J, nativos de Link 16. [1]

- 4. **Calidad de Servicio (QoS):** Link 22 ofrece múltiples características de calidad de servicio, como:
 - o **Prioridad:** Cuatro niveles (1-4), donde el 1 es el más alto.
 - o **Fiabilidad:** Cuatro niveles para garantizar la recepción, desde estándar hasta protocolos de entrega garantizada con retransmisión.

- o **Caducidad:** Define el tiempo máximo durante el cual los datos siguen siendo relevantes para su transmisión.
 - o **Dirección:** Soporte para diversos modos de direccionamiento (totalcast, neighborcast, punto a punto, entre otros).
5. **Parámetros Fundamentales:**
- o Todos los nodos de la red Link 22 deben compartir un conjunto común de parámetros fundamentales para garantizar la coherencia en la operación.
 - o Estos parámetros se distribuyen a través de mensajes **OPTASK Link** y se cargan durante la inicialización del sistema.
6. **Medios:**
- o Link 22 es compatible con comunicaciones en las bandas de frecuencia HF (2-30 MHz) y UHF (225-400 MHz). Se describen ambas comunicaciones en UHF y en HF, más abajo en la figura 2-8.

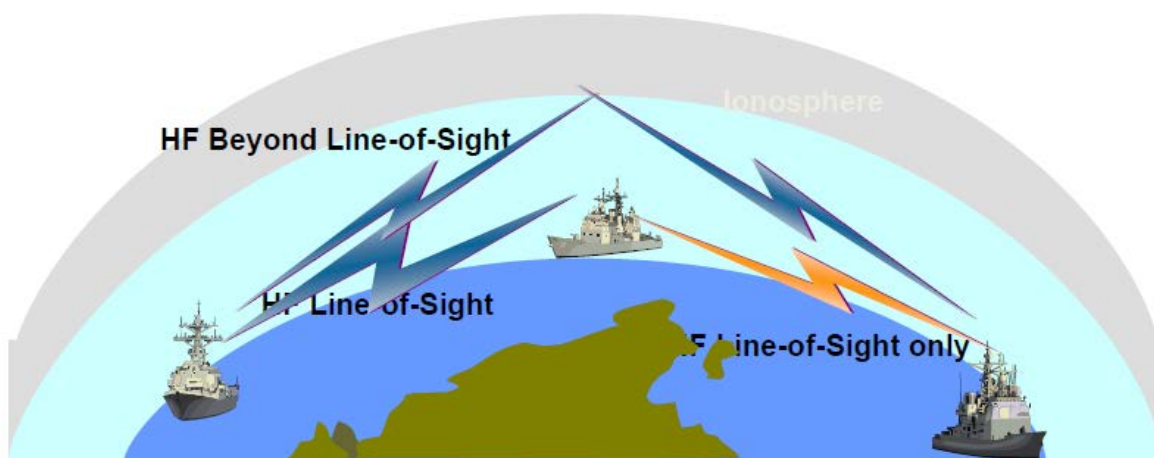


Figura 2-8. Link 22 puede utilizar UHF para LOS y HF para BLOS. [1]

- o Admite tanto frecuencias fijas como radios con salto de frecuencia.
 - o Los medios definidos actualmente incluyen:
 - HF con frecuencia fija.
 - UHF con frecuencia fija.
 - HF con salto de frecuencia.
 - UHF con salto de frecuencia.
7. **Estructura del Ciclo de Red:**
- o La transmisión en Link 22 se organiza mediante el protocolo TDMA (Acceso Múltiple por División de Tiempo).
 - o Cada unidad transmite únicamente en los intervalos de tiempo asignados, lo que asegura un uso eficiente del ancho de banda y evita colisiones.
8. **Gestión de Redes:**
- o Las funciones de gestión de redes están altamente automatizadas, minimizando la necesidad de intervención manual.
 - o Roles de gestión:
 - **Unidad de Gestión de la Super Red (SNMU):** Coordina toda la Super Red (véase, más abajo, la figura 2-9).
 - **Unidades de Gestión de Red (NMU):** Gestionan redes individuales dentro de la Super Red.
 - o Las unidades de respaldo se asignan automáticamente para garantizar la continuidad en caso de fallos.

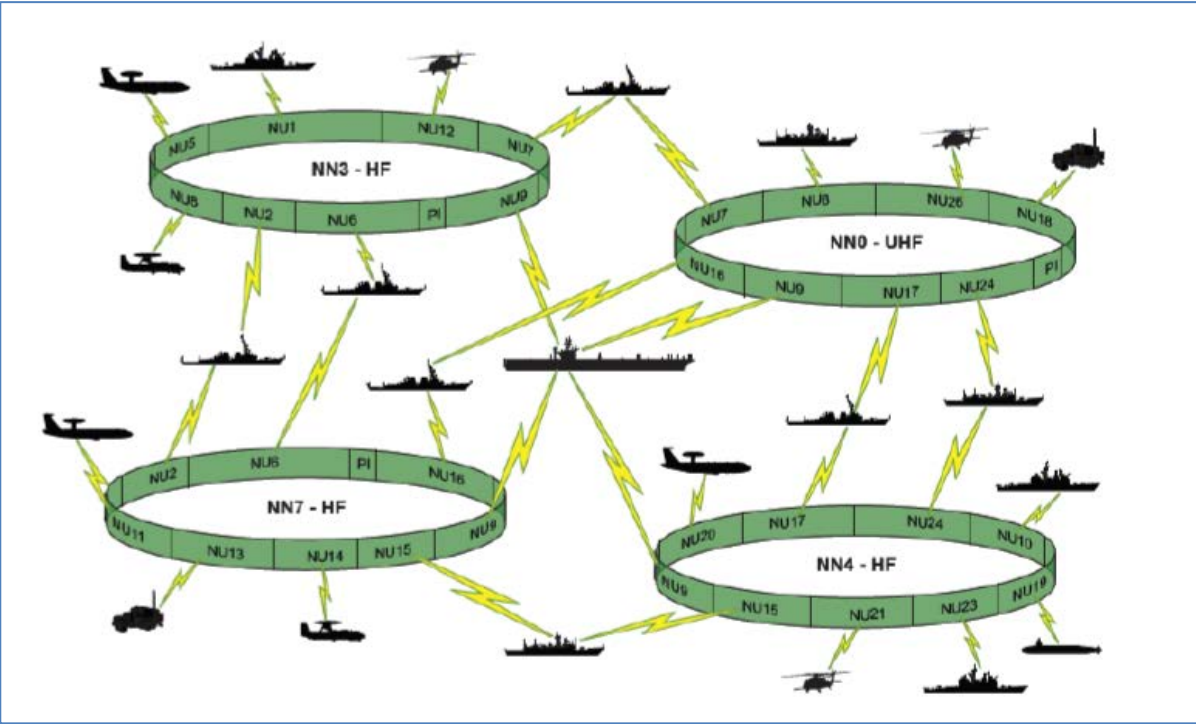


Figura 2-9. Despliegue de una Super Network en Link 22.

9. **Capacidades de Resiliencia:**
- o Los protocolos distribuidos aseguran que no haya un único punto de fallo en el sistema.
 - o En caso de interrupciones, Link 22 ajusta automáticamente los mensajes y las rutas para mantener la conectividad.
10. **Gestión de Congestión:**
- o Link 22 monitorea y ajusta automáticamente la carga de la red para evitar la congestión.
 - o Puede reasignar la capacidad de transmisión o reconfigurar la red en tiempo real.

2.5 COMPARATIVA ENTRE LINK 11B, LINK 16 Y LINK 22 [2] [1].

Los **sistemas de enlace de datos tácticos (Tactical Data Links, TDL)** como Link 11B, Link 16 y Link 22 son fundamentales en la interoperabilidad de las fuerzas armadas modernas, especialmente para operaciones conjuntas y multinacionales. A continuación, se presenta una comparación detallada:

GENERALIDADES.

La tabla 2-1, más abajo, describe de forma genérica las diferencias entre Link 11B, Link 16 y Link 22.

Característica	Link 11B	Link 16	Link 22
Uso principal	Comunicaciones terrestres y navales.	Redes aéreas, terrestres y navales.	Reemplazo/modernización del Link 11B y Link 16.
Introducción	Años 60.	Años 80.	Años 2010.
Estandarización	MIL-STD-6011	MIL-STD-6016	STANAG 5522.

Tabla 2-1. Generalidades entre Link 11B, Link 16 y Link 22.

CAPACIDADES TÉCNICAS.

La tabla 2-2, más abajo, describe las diferencias, en capacidades técnicas, entre Link 11B, Link 16 y Link 22.

Característica	Link 11B	Link 16	Link 22
Tecnología básica	HF/UHF, no seguro.	TDMA (Time Division Multiple Access), anti-jamming.	TDMA avanzado con criptografía mejorada.
Velocidad de datos	Baja (1,8 Kbps).	Media (31,6 Kbps - 1 Mbps).	Alta (hasta 1 Mbps o más).
Seguridad	Criptografía básica.	Criptografía robusta y antiinterferencias.	Criptografía avanzada y mayor robustez.
Topología de red	Maestro-esclavo.	Punto a multipunto, malla distribuida.	Punto a multipunto distribuido.
Espectro	HF/UHF.	UHF (960-1215 MHz).	HF/UHF (mejor aprovechamiento espectral).
Capacidad de interoperabilidad	Limitada.	Alta (NATO y aliados).	Muy alta, diseñada para compatibilidad con TDL modernos.

Tabla 2-2. Capacidades técnicas entre Link 11B, Link 16 y Link 22.

VENTAJAS Y DESVENTAJAS.

La tabla 2-3, más abajo, describe las ventajas/desventajas de Link 11B, Link 16 y Link 22.

Aspecto	Link 11B	Link 16	Link 22
Ventajas	Requiere poca infraestructura.	Muy robusto y confiable.	Sustituye Link 11 y complementa Link 16.
	Funciona en HF (alcance mayor).	Antiinterferencias y cifrado.	Seguridad y flexibilidad mejoradas.
Desventajas	Obsoleto, velocidad baja.	Altamente dependiente de UHF.	Requiere implementación moderna.
	Vulnerable a interferencias.	Costoso y complejidad técnica.	Coste inicial elevado.

Tabla 2-3. Ventajas/Desventajas entre Link 11B, Link 16 y Link 22.

APLICACIONES TÁCTICAS.

La tabla 2-4, más abajo, describe las diferencias de empleo táctico entre Link 11B, Link 16 y Link 22.

Contexto	Link 11B	Link 16	Link 22
Misiones terrestres	Comunicaciones básicas.	Coordinación con fuerzas aéreas.	Integración con sistemas terrestres avanzados.
Operaciones navales	Conexión entre barcos.	Defensa aérea y marítima.	Redes navales modernas (nodos distribuidos).
Fuerzas aéreas	Limitado.	Principal enlace táctico.	Complemento para aviación y operaciones modernas.

Tabla 2-4. Aplicaciones tácticas de Link 11B, Link 16 y Link 22.

FUTURO Y RELEVANCIA.

- **Link 11B:** En desuso progresivo por sus limitaciones tecnológicas. Mantiene relevancia residual en plataformas más antiguas o en escenarios con menos requisitos técnicos.
- **Link 16:** Sigue siendo un estándar robusto y ampliamente utilizado, pero con desafíos en ciberseguridad y saturación espectral.
- **Link 22:** Se perfila como el enlace del futuro por su capacidad de interoperabilidad, seguridad y flexibilidad, diseñado para integrar y reemplazar progresivamente a los sistemas más antiguos.

CONCLUSIÓN.

- **Link 11B** es el más antiguo y limitado, adecuado solo para sistemas con necesidades básicas.
- **Link 16** es la columna vertebral de los sistemas TDL actuales, aunque con restricciones para futuras necesidades de interoperabilidad y escalabilidad.
- **Link 22** representa la evolución hacia una red más flexible, segura y capaz, pero su implementación completa aún está en desarrollo y expansión.

2.6 PROTOCOLO JREAP.

INTRODUCCIÓN.

El **Joint Range Extension Application Protocol (JREAP)** es un protocolo diseñado para extender el alcance de los **enlaces de datos tácticos (TDL)** tradicionales como Link 16 y Link 22. Permite la transmisión de mensajes tácticos a través de redes no convencionales, como satélites y redes IP, lo que amplía significativamente su alcance más allá de la línea de vista (**BLOS**). En la figura 2-10, mas abajo, se muestra un despliegue de unidades OTAN de distintos países donde el JREAP interopera con otros TDL como Link 22 y Link 16.

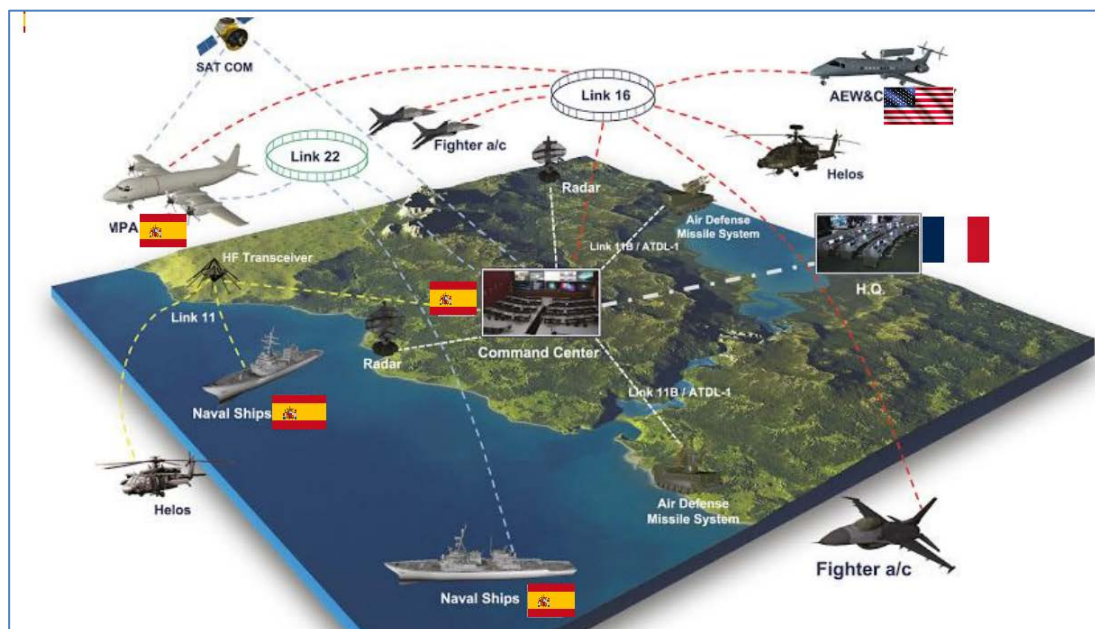


Figura 2-10. Empleo de JREAP-A junto a otros TDL en Ejercicio Aliado (US, FRA & SP).

JREAP es un protocolo diseñado para permitir, una vez encapsulado el mensaje, la transmisión de mensajes de TDL como **Link 22**, **Link 16**, **Link 11**, a través de medios no tradicionales como:

- **Satélites (SATCOM).**
- **Redes IP** (incluyendo redes terrestres y Wi-Fi militar).

- **Enlaces de microondas o fibra óptica** Esto asegura que los datos puedan ser compartidos entre nodos que no tienen línea de vista directa.

JREAP admite múltiples nodos en una red táctica, facilitando operaciones conjuntas entre diferentes fuerzas armadas y plataformas. Se utiliza activamente en ejercicios militares conjuntos de la OTAN y en operaciones de coalición, demostrando su capacidad para interoperar con múltiples plataformas y tecnologías. JREAP permite a las fuerzas armadas escalar redes tácticas desde pequeños equipos operativos hasta operaciones de teatro completo.

Variantes del protocolo:

- **JREAP-A (Asynchronous):** Usado para comunicaciones a través de satélites (SATCOM) con protocolos asincrónicos.
- **JREAP-B (Synchronous):** Usado en enlaces punto a punto a través de conexiones en serie.
- **JREAP-C (Connectionless):** Usado sobre redes basadas en IP, muy útil en entornos con infraestructura de red moderna.

JREAP-A aprovecha satélites de comunicaciones modernas con capacidades de alta velocidad y baja latencia, como los sistemas de satélites de órbita baja (LEO) y media (MEO).

JREAP-C se está integrando cada vez más con redes basadas en IP, utilizando protocolos avanzados como **IPv6**, lo que mejora la capacidad de direccionamiento y la seguridad.

Nuevas implementaciones de JREAP están integradas con sistemas de gestión de batalla (BMS), que automatizan el intercambio de datos y la fusión de información. La eficiencia del ancho de banda se ha mejorado mediante la optimización de las tramas de datos.

Ciberseguridad mejorada: Se han adoptado tecnologías de cifrado robustas (RSA) para proteger los mensajes encapsulados frente a ciberamenazas.

Interoperabilidad con sistemas emergentes:

- Los sistemas de Mando y Control que utilizan inteligencia artificial para la toma de decisiones están comenzando a integrarse con redes que operan bajo JREAP.
- Compatible con terminales de radio definidas por software (SDR), como los sistemas desarrollados bajo el programa **ESSOR**.

JREAP EN UN DESPLIEGUE TÁCTICO.

En un despliegue táctico, es común que unidades (aéreas, terrestres o navales) se encuentren fuera del alcance directo del radio o las antenas Link 16 tradicionales. JREAP utiliza SATCOM o redes IP para extender el alcance y mantener la conectividad en estas situaciones.

JREAP facilita la comunicación entre fuerzas multinacionales o conjuntas que utilizan diferentes medios o plataformas. Además, es compatible con diferentes tipos de mensajes tácticos, asegurando que las unidades puedan compartir datos críticos, como posición de blancos o información del campo de batalla.

Escenarios comunes de uso:

- **Control Aéreo Táctico:** Conectar controladores avanzados en tierra con aeronaves que operan fuera del rango del radio.
- **Defensa Aérea:** Permitir que los sistemas de defensa antiaérea compartan datos de radar con unidades distantes o fuera del área.

- **Operaciones de comando y control:** Extender la red de comunicaciones del centro de operaciones hacia unidades remotas o avanzadas.

EJEMPLO PRÁCTICO.

En un despliegue táctico de una fuerza multinacional:

- Aeronaves: varios cazas de ataque y un avión AWACS¹⁸ (Mando + Control y Alerta Temprana) que transmite datos de objetivos detectados mediante Link 16 al Centro de Mando, en tierra y en una Zona de Operaciones (ZO) situada en África Central.
- Esos datos son enviados desde el Centro de Mando al JFACC¹⁹ situado en una base lejana en Europa utilizando JREAP-A sobre una red SATCOM.
- Desde el JFACC se coordinan acciones con los otros Mandos Componentes del nivel operacional (Terrestre y Marítimo). Estas acciones son comunicadas desde el JFACC, empleando JREAP-A via SATCOM hasta el Centro de Mando en la Zona de Operaciones.
- Desde el Centro de Mando se transmiten órdenes a los cazas de ataque sobre los objetivos designados.

El despliegue está esquematizado en la figura 2-11, más abajo.

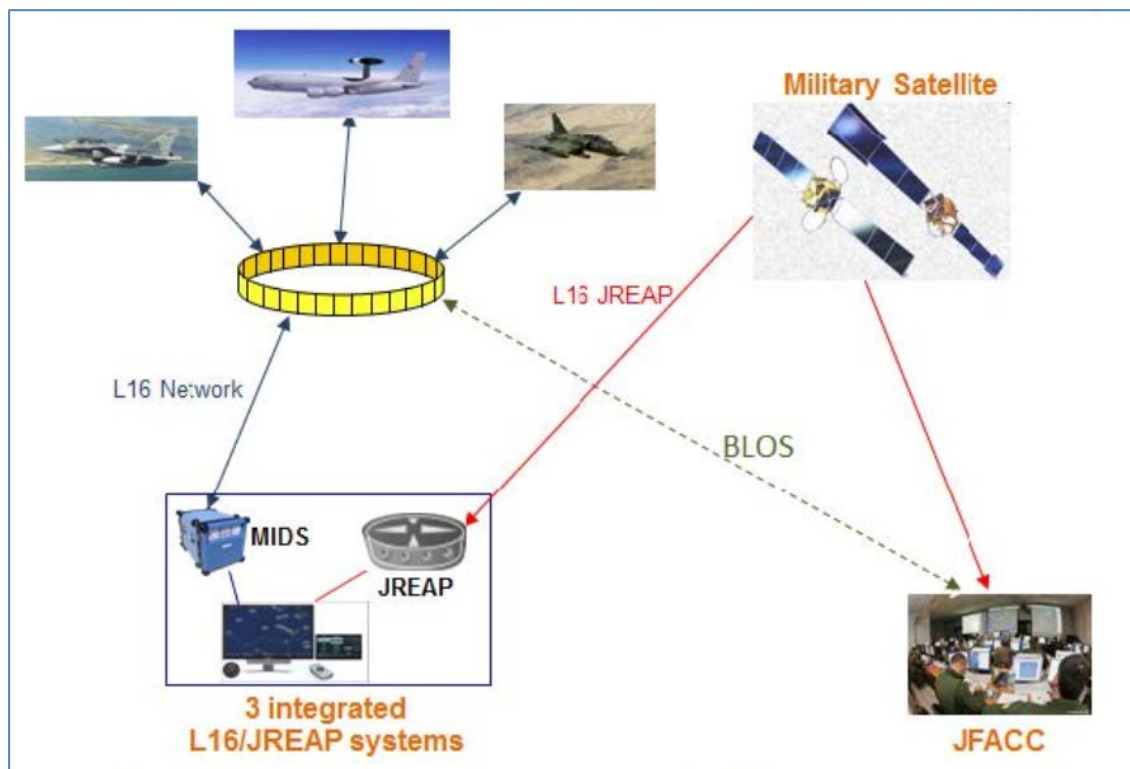


Figura 2-11. Despliegue táctico con interoperabilidad entre JREAP y Link 16.

Este esquema asegura que todas las unidades, independientemente de su ubicación física, tengan acceso a información táctica en tiempo casi real.

¹⁸ AWACS: Airborne Warning And Control System.

¹⁹ JFACC: Joint Force Air Component Command.

2.7 ESTÁNDAR DE INTERCAMBIO DE MENSAJES VMF.

El **Variable Message Format (VMF)** es un estándar de intercambio de mensajes tácticos ampliamente utilizado por las fuerzas armadas para transmitir información crítica en operaciones conjuntas, especialmente en entornos con limitaciones de ancho de banda. VMF ha evolucionado para satisfacer las necesidades de interoperabilidad, eficiencia y adaptabilidad en un panorama militar cada vez más complejo.

En la figura 2-12, de más abajo, se muestra un terminal VMF de la empresa Tecnobit que permite que un JTAC²⁰ o coordinador terrestre de operaciones conjuntas se comuniquen con el piloto del caza para que este último realice un apoyo DACAS²¹ a tropas terrestres (apoyo aéreo cercano mediante TIC) o un JFO²² u observador de fuegos en operaciones conjuntas pueda evaluar el estado de destrucción del objetivo atacado por un caza con el que mantiene comunicación mediante VMF.



Figura 2-12. Terminal táctico que permite enviar/recibir mensajes VMF. [3]

CARACTERÍSTICAS CLAVE DEL VMF.

- **Formato de mensaje basado en estándares militares:**
 - o VMF se basa en un diseño estructurado para garantizar que los mensajes sean compactos, eficientes y consistentes.
 - o Utiliza un enfoque de formato binario, lo que reduce el tamaño del mensaje y permite su transmisión en redes de baja capacidad.
- **Eficiencia en el uso del ancho de banda:**
 - o Diseñado para operar en redes con ancho de banda limitado, como radios tácticas en entornos terrestres o áreas remotas.
 - o Adecuado para redes de comunicación UHF, VHF y HF.
- **Interoperabilidad:**

²⁰ JTAC: Joint Terminal Air Controller.

²¹ DACAS: Digitally Aided Close Air Support.

²² JFO: Joint Fire Observer,

- o Compatible con múltiples plataformas (aéreas, terrestres y marítimas) y sistemas de mando y control (C2).
- o Soporte para integrarse con otros estándares de enlace de datos tácticos como Link 16 y Link 22 a través de gateways.
- **Flexibilidad operacional:**
 - o Amplia gama de mensajes predefinidos diseñados para misiones específicas (artillería, logística, inteligencia, reconocimiento, etc.).
 - o Permite la personalización y definición de nuevos mensajes para adaptarse a necesidades cambiantes.

ESTADO DEL ARTE.

- **Integración con Radios Definidas por Software (SDR):**
 - o VMF se implementa cada vez más en terminales basados en SDR, como los sistemas desarrollados en el programa ESSOR.
 - o Los radios SDR permiten que VMF coexista con otras formas de onda tácticas, ofreciendo mayor flexibilidad en misiones conjuntas.
- **Automatización y fusión de datos:**
 - o Las redes basadas en VMF están siendo integradas con sistemas avanzados de gestión de batalla (BMS), lo que permite:
 1. **Automatización:** Reducción de errores humanos en la generación y envío de mensajes.
 2. **Fusión de datos:** Creación de un "visor campo de batalla común" (COP, Common Operational Picture) en tiempo real.
 - o Ejemplo: Sistemas de gestión avanzada como **FBCB2 (Force XXI Battle Command Brigade and Below)**.
- **Interoperabilidad multinacional:**
 - o VMF ha demostrado ser una solución viable para operaciones conjuntas, ya que puede integrarse con estándares de enlace de datos tácticos utilizados por fuerzas aliadas.
 - o Se utiliza en ejercicios multinacionales y operaciones OTAN para coordinar plataformas aéreas y terrestres.
- **Migración a redes IP:**
 - o Aunque VMF tradicionalmente opera en radios tácticas, su integración con redes basadas en IP ha permitido:
 1. **Transmisión en redes LAN/WAN.**
 2. Uso en operaciones Beyond Line of Sight (BLOS) a través de satélites y JREAP-C.
 3. Mayor alcance en entornos distribuidos.
- **Seguridad mejorada:**
 - o Las implementaciones modernas de VMF incluyen capacidades avanzadas de cifrado y autenticación para proteger los datos en entornos de guerra electrónica y ciberamenazas.
 - o Uso de algoritmos de cifrado como **AES-256** en redes tácticas.

AVANCES RECIENTES.

- **Evolución hacia redes centradas en la información (NCW²³):**
 - o VMF se integra con conceptos de **Network-Centric Warfare**, permitiendo una mayor colaboración y sincronización en tiempo real entre las fuerzas desplegadas.

²³ NCW: Network-Centric Warfare.

- o Soporte para actualizaciones en tiempo real del COP mediante datos obtenidos de sensores distribuidos.
- **Conexión con plataformas no tripuladas:**
 - o Uso de VMF para la comunicación entre sistemas de mando y plataformas no tripuladas como drones (UAV) y robots terrestres.
 - o Ejemplo: Uso en operaciones de reconocimiento para compartir datos en tiempo real.
- **Optimización de mensajes:**
 - o Reducción adicional del tamaño de los mensajes para operar en entornos con interferencias y congestión espectral.
 - o Mejoras en el tiempo de respuesta para aplicaciones críticas, como el apoyo aéreo cercano (CAS).
- **Integración con tecnologías emergentes:**
 - o Soporte para inteligencia artificial (IA) y aprendizaje automático para:
 1. Analizar patrones en los datos transmitidos por VMF.
 2. Optimizar el flujo de mensajes en redes saturadas.

LIMITACIONES ACTUALES.

- **Capacidad limitada de datos:**
 - o Aunque eficiente, el diseño compacto de VMF limita la cantidad de datos que se pueden transmitir en un solo mensaje.
 - o No está optimizado para grandes volúmenes de datos o multimedia.
- **Complejidad de integración:**
 - o Requiere gateways para interoperar con otros estándares como Link 16 o Link 22, lo que puede añadir latencia y costos.
- **Adaptación a redes modernas:**
 - o Aunque se han hecho avances hacia redes IP, VMF no está diseñado originalmente para aprovechar al máximo las redes de alta velocidad.

PERSPECTIVAS FUTURAS.

- **Modernización de estándares:**
 - o Actualizaciones del protocolo para admitir mayores capacidades de datos y flexibilidad.
 - o Mejoras en la interoperabilidad con tecnologías emergentes como el 5G militar.
- **Despliegue en plataformas espaciales:**
 - o Uso de VMF para comunicaciones tácticas con satélites tácticos y plataformas en órbita baja (LEO).
- **Integración total con IA:**
 - o Uso de inteligencia artificial para analizar mensajes VMF y priorizar información crítica en tiempo real.
- **Capacidades de red híbrida:**
 - o Uso combinado con otros estándares de comunicación para crear redes tácticas resilientes y adaptativas en operaciones conjuntas.

IMPACTO ESTRATÉGICO.

- **Eficiencia operativa:** VMF sigue siendo un componente crítico para operaciones conjuntas debido a su eficiencia en redes tácticas limitadas.
- **Interoperabilidad global:** Su capacidad para integrarse con otros estándares lo hace indispensable en ejercicios y operaciones multinacionales.

- **Flexibilidad futura:** Las adaptaciones continuas aseguran que VMF siga siendo relevante en un entorno militar en constante evolución.

2.8 IMPORTANCIA OPERACIONAL DE LOS TDL.

La **importancia operacional de los TDL** radica en su capacidad para mejorar la coordinación, la conciencia situacional y la efectividad en operaciones militares. A continuación, se detalla su relevancia desde una perspectiva operacional:

INTEROPERABILIDAD ENTRE PLATAFORMAS.

- Los TDL permiten la conexión y el intercambio de información en tiempo real entre diferentes sistemas y plataformas militares, como aviones, barcos, vehículos terrestres, centros de mando y satélites.
- Garantizan la interoperabilidad entre las fuerzas armadas de diferentes países, facilitando operaciones conjuntas y multinacionales.

CONCIENCIA SITUACIONAL MEJORADA.

- Proveen un Visor Operacional Común (COP) que consolida información de múltiples fuentes para los comandantes y operadores.
- Facilitan la toma de decisiones basadas en datos precisos y actualizados sobre posiciones enemigas, propias y de aliados.

VELOCIDAD EN LA TOMA DE DECISIONES.

- La transmisión instantánea de datos permite actuar rápidamente en entornos dinámicos, crucial en escenarios donde el tiempo es un factor crítico.
- Reduce los riesgos de errores de comunicación y agiliza las órdenes entre diferentes niveles de mando.

SEGURIDAD Y CONFIABILIDAD.

- Los TDL utilizan métodos de encriptación avanzados para garantizar que la información transmitida sea segura y no pueda ser interceptada o alterada por adversarios.
- Proveen redundancia en las comunicaciones, reduciendo la vulnerabilidad ante interrupciones.

APOYO EN OPERACIONES COMPLEJAS.

- Los TDL son fundamentales en misiones coordinadas como ataques aéreos, defensa antimisiles, vigilancia marítima y rescates.
- Permiten el seguimiento de objetivos en movimiento y la asignación eficiente de recursos.

FLEXIBILIDAD EN EL DESPLIEGUE.

- Los sistemas de TDL, como Link 11, Link 16 o Link 22, pueden adaptarse a diversas plataformas y entornos operativos, ya sea en tierra, mar o aire.
- Se integran fácilmente con sistemas de mando y control (C2) y otros sensores avanzados.

REDUCCIÓN DE LA CONFUSIÓN EN COMBATE.

- Minimiza el riesgo de fuego amigo al compartir identificaciones precisas de las fuerzas propias y aliadas.
- Mejora la sincronización de movimientos y evita duplicación de esfuerzos o conflictos en las operaciones.

En resumen, los TDL son esenciales para modernizar las capacidades operacionales, aumentar la eficiencia táctica y estratégica, y fortalecer la superioridad operativa en entornos militares. Su implementación efectiva asegura que las fuerzas armadas puedan responder de manera coordinada, precisa y segura a los desafíos del campo de batalla moderno.

2.9 PRINCIPIOS DE SEGURIDAD EN LOS TDL.

Los **principios de seguridad de la información en los TDL** son fundamentales para garantizar la protección, confiabilidad y efectividad de las comunicaciones críticas en entornos militares.

CONFIDENCIALIDAD.

- **Definición:** Garantizar que los datos transmitidos a través de los TDL sean accesibles únicamente por entidades autorizadas.
- **Aplicación:**
 - o Encriptación avanzada en las comunicaciones, como el uso de cifrados como AES y algoritmos específicos para entornos militares.
 - o Segmentación de la información según niveles de clasificación para evitar que usuarios no autorizados accedan a datos sensibles.
 - o Autenticación estricta entre nodos de TDL.

INTEGRIDAD.

- **Definición:** Proteger la información transmitida en los TDL contra alteraciones, ya sea por errores accidentales o acciones maliciosas.
- **Aplicación:**
 - o Uso de códigos de detección de errores como CRC (Cyclic Redundancy Check) o algoritmos de *hashing* para validar los datos transmitidos.
 - o Verificación constante del origen y la consistencia de los mensajes.
 - o Sistemas de alarmas para detectar cualquier modificación o intrusión no autorizada.

DISPONIBILIDAD.

- **Definición:** Asegurar que los TDL estén operativos y accesibles en todo momento para las entidades autorizadas.
- **Aplicación:**
 - o Implementación de redundancia en las infraestructuras de TDL para evitar interrupciones.
 - o Uso de mecanismos anti-jamming para contrarrestar interferencias electrónicas.
 - o Monitoreo continuo para identificar y mitigar amenazas de denegación de servicio (DoS).

AUTENTICIDAD.

- **Definición:** Verificar que las entidades que participan en los TDL son legítimas y que los datos provienen de fuentes confiables.
- **Aplicación:**
 - o Uso de claves criptográficas y certificados digitales para autenticar a los participantes.

- o Protocolo de intercambio seguro de claves (por ejemplo, a través de sistemas como COMSEC y TRANSEC).
- o Verificación mutua entre plataformas antes de iniciar el intercambio de datos.

NO REPUDIO.

- **Definición:** Garantizar que los emisores y receptores no puedan negar haber enviado o recibido mensajes a través de los TDL.
- **Aplicación:**
 - o Registro detallado de las transmisiones de datos en sistemas de auditoría.
 - o Implementación de firmas digitales que respalden la autenticidad y trazabilidad de los mensajes.
 - o Sistemas de almacenamiento seguro para conservar el historial de comunicaciones.

MINIMIZACIÓN DE PRIVILEGIOS.

- **Definición:** Restringir el acceso y las capacidades de cada nodo a lo estrictamente necesario para cumplir con sus funciones.
- **Aplicación:**
 - o Aplicación del principio de “necesidad de saber” (*need-to-know*).
 - o Configuración de roles y permisos específicos para cada plataforma conectada al TDL.
 - o Control de acceso dinámico según el contexto operacional.

TRAZABILIDAD.

- **Definición:** Registrar todas las actividades en los TDL para identificar y analizar posibles incidentes de seguridad.
- **Aplicación:**
 - o Uso de sistemas de registro de actividad en tiempo real (*logging*).
 - o Auditorías periódicas de las comunicaciones.
 - o Generación de reportes automáticos para el análisis forense de ciberataques o anomalías.

RESILIENCIA.

- **Definición:** Asegurar que los TDL puedan continuar operando incluso en caso de ataques o fallos técnicos.
- **Aplicación:**
 - o Diseño de arquitecturas tolerantes a fallos para los enlaces de datos tácticos.
 - o Simulaciones y ejercicios para preparar las plataformas ante ciberataques.
 - o Implementación de sistemas de respaldo y recuperación rápida ante interrupciones.

SEGURIDAD POR DISEÑO.

- **Definición:** Incorporar medidas de seguridad desde la concepción y diseño de los TDL.
- **Aplicación:**
 - o Asegurar que las especificaciones de sistemas como Link 11, Link 16, y Link 22 incluyan robustas capas de seguridad desde su diseño.
 - o Pruebas de penetración y análisis de vulnerabilidades antes de su despliegue operacional.
 - o Inclusión de actualizaciones regulares de seguridad durante el ciclo de vida del sistema.

PROTECCIÓN CONTRA INTERFERENCIAS (TRANSEC).

- **Definición:** Asegurar que las señales de los TDL sean resistentes a la detección, interceptación o interferencia deliberada.
- **Aplicación:**
 - o Uso de salto en frecuencias (*frequency hopping*) en los enlaces de datos tácticos.
 - o Implementación de técnicas de disimulación de señales y transmisión aleatoria.
 - o Protección contra amenazas de guerra electrónica (EW).

En resumen, la implementación rigurosa de estos principios asegura que los TDL sean confiables, seguros y capaces de operar eficazmente incluso en entornos hostiles. La combinación de tecnologías avanzadas, protocolos bien diseñados y entrenamiento especializado es clave para mantener la supremacía táctica en el campo de batalla moderno.

3 VULNERABILIDADES EN LOS ENLACES DE DATOS TÁCTICOS.

Los **Tactical Data Links (TDL)**, aunque diseñados para operar de forma segura en entornos hostiles, no están exentos de vulnerabilidades que pueden ser explotadas por actores malintencionados o debido a fallos técnicos. Las vulnerabilidades en los TDL pueden clasificarse en varios tipos, según la naturaleza del problema y el impacto potencial.

3.1 VULNERABILIDADES IDENTIFICADAS EN LINK 11.

FALTA DE CIFRADO EFICIENTE.

- **Descripción:** Link 11 no fue diseñado con sistemas de cifrado avanzados, lo que significa que las transmisiones son susceptibles a ser interceptadas y descifradas por actores malintencionados.
- **Impacto:** Las comunicaciones críticas pueden ser fácilmente comprometidas, permitiendo el espionaje o la alteración de datos tácticos.

VULNERABILIDAD A INTERFERENCIAS (JAMMING).

- **Descripción:** Utiliza modulación analógica (AM/SSB) en frecuencias HF y UHF, lo que lo hace extremadamente vulnerable a interferencias deliberadas o accidentales.
- **Impacto:** Los atacantes pueden bloquear o degradar significativamente las comunicaciones mediante técnicas de jamming, interrumpiendo la coordinación táctica.

FALTA DE AUTENTICACIÓN.

- **Descripción:** Link 11 carece de mecanismos robustos para autenticar a los participantes en la red.
- **Impacto:** Esto permite ataques de "spoofing", donde un atacante puede hacerse pasar por un nodo legítimo, introduciendo información falsa o causando confusión operativa.

SUSCEPTIBILIDAD A LA CAPTURA DE DATOS (SNIFFING).

- **Descripción:** Las señales de Link 11 pueden ser capturadas fácilmente por equipos de escucha debido a su diseño de transmisión no seguro.
- **Impacto:** Los adversarios pueden recopilar información táctica sin ser detectados, comprometiendo las operaciones.

FALTA DE RESISTENCIA A ATAQUES MODERNOS.

- **Descripción:** Diseñado en una era previa a las amenazas cibernéticas avanzadas, Link 11 no tiene contramedidas contra ataques modernos, como inyección de código malicioso o técnicas de explotación basadas en software.
- **Impacto:** La red es vulnerable a ataques que pueden comprometer sistemas conectados o interrumpir operaciones críticas.

BAJA ROBUSTEZ ANTE FALLOS ELECTROMAGNÉTICOS.

- **Descripción:** Su tecnología no fue diseñada para operar eficazmente en entornos con alta interferencia electromagnética (EMI), como los generados por explosiones nucleares o sistemas de guerra electrónica avanzada.
- **Impacto:** Puede fallar en condiciones de combate donde la interferencia EMI es común.

DEPENDENCIA DE SINCRONIZACIÓN PRECISA.

- **Descripción:** Link 11 requiere sincronización precisa entre nodos para su operación, pero no incorpora mecanismos avanzados de corrección de sincronización.
- **Impacto:** La desincronización entre nodos puede causar pérdida de datos o interrupciones en la comunicación.

INTEROPERABILIDAD LIMITADA.

- **Descripción:** Su diseño inicial carece de soporte para estándares modernos y la interoperabilidad multinacional.
- **Impacto:** Las operaciones conjuntas con fuerzas aliadas pueden enfrentar problemas significativos, exponiendo vulnerabilidades durante las misiones multinacionales.

DEPENDENCIA DE INFRAESTRUCTURA FÍSICA ANTIGUA.

- **Descripción:** Muchos sistemas Link 11 todavía dependen de equipos físicos anticuados, que son más susceptibles a fallos y ataques físicos.
- **Impacto:** La manipulación o daño de estos sistemas puede interrumpir las operaciones.

FALTA DE MECANISMOS DE MONITOREO Y RESPUESTA.

- **Descripción:** Link 11 carece de capacidades para monitorear activamente la red en busca de intrusiones o responder a ataques en tiempo real.
- **Impacto:** Los ataques pueden pasar desapercibidos, permitiendo a los atacantes mantener el acceso no autorizado durante períodos prolongados.

MITIGACIONES POTENCIALES ANTE DICHAS VULNERABILIDADES EN LINK 11.

Aunque Link 11 tiene importantes limitaciones, algunas medidas pueden mitigar parcialmente estas vulnerabilidades:

- Implementar cifrado externo utilizando dispositivos modernos para proteger las transmisiones.
- Usar sistemas de autenticación adicionales para verificar la identidad de los nodos.
- Implementar medidas de detección y respuesta en tiempo real para identificar intentos de interferencia o intrusión.
- Modernizar equipos físicos y transceptores para mejorar la resistencia a interferencias y EMI.

CONCLUSIÓN.

Link 11, debido a su diseño obsoleto, presenta numerosas vulnerabilidades que lo hacen inadecuado para los entornos de amenazas modernos. La falta de seguridad inherente, junto con su vulnerabilidad a jamming, spoofing y sniffing, compromete seriamente su utilidad en operaciones contemporáneas.

Migrar a sistemas más modernos como **Link 16** o **Link 22** es esencial para garantizar comunicaciones tácticas seguras y resilientes.

3.2 VULNERABILIDADES IDENTIFICADAS EN LINK 16.

DEPENDENCIA DEL SALTO DE FRECUENCIA DE ESPECTRO ENSANCHADO (FHSS).

- **Descripción:** Link 16 utiliza salto de frecuencia (Frequency Hopping Spread Spectrum, FHSS) para protegerse contra el jamming. Sin embargo, adversarios sofisticados con capacidades avanzadas de guerra electrónica pueden intentar identificar y rastrear los patrones de salto.
- **Impacto:** Si el patrón de salto es comprometido, un atacante podría interferir en las frecuencias utilizadas, reduciendo la efectividad de las comunicaciones.

NECESIDAD DE SINCRONIZACIÓN TEMPORAL PRECISA.

- **Descripción:** Link 16 requiere una sincronización precisa basada en un sistema de tiempo común (como GPS) para funcionar correctamente.
- **Impacto:**
 - o Los ataques que interfieran con las señales de GPS (spoofing o jamming) pueden desincronizar la red, causando fallos en las comunicaciones.
 - o En caso de pérdida de sincronización, los nodos pueden quedar aislados del sistema.

VULNERABILIDAD A INTERFERENCIAS ELECTROMAGNÉTICAS (EMI) AVANZADAS.

- **Descripción:** Aunque resistente a muchas formas de interferencia, Link 16 puede ser afectado por emisiones electromagnéticas extremadamente poderosas, como las generadas por explosiones nucleares o sistemas de guerra electrónica de próxima generación.
- **Impacto:** La degradación del espectro electromagnético puede interrumpir la comunicación en áreas críticas.

COMPLEJIDAD EN LA CONFIGURACIÓN Y OPERACIÓN.

- **Descripción:** La red Link 16 requiere configuraciones complejas, como la asignación de tiempos, frecuencias y claves criptográficas. Errores humanos en la configuración pueden introducir vulnerabilidades.
- **Impacto:** Configuraciones incorrectas pueden resultar en fallos de comunicación o en accesos no autorizados si las claves criptográficas no son adecuadamente protegidas.

LIMITACIONES EN EL ANCHO DE BANDA.

- **Descripción:** Aunque avanzado para su época, el ancho de banda de Link 16 es limitado, lo que puede afectar su capacidad para manejar grandes volúmenes de datos en escenarios modernos.
- **Impacto:** En redes congestionadas, un atacante podría explotar esta limitación enviando tráfico malicioso o introduciendo ruido para degradar la calidad del servicio.

VULNERABILIDAD A COMPROMISOS CRIPTOGRÁFICOS.

- **Descripción:** La seguridad de Link 16 depende de sus algoritmos de cifrado y claves criptográficas. Aunque actualmente se considera seguro, los avances en computación cuántica podrían comprometer estas medidas.
- **Impacto:** Un atacante con recursos suficientes podría descifrar las comunicaciones si las claves criptográficas son comprometidas o si no se implementan algoritmos resistentes al quantum.

FALTA DE PROTECCIÓN CONTRA ATAQUES INTERNOS.

- **Descripción:** Link 16 no tiene mecanismos inherentes para detectar o mitigar ataques provenientes de nodos internos comprometidos.
- **Impacto:** Si un nodo legítimo es capturado o comprometido, un atacante puede enviar datos falsos o recolectar información crítica sin ser detectado.

RANGO OPERATIVO LIMITADO.

- **Descripción:** Link 16 opera en frecuencias UHF/L-Band, lo que limita su rango efectivo a unas 300 millas náuticas aproximadamente.
- **Impacto:** En escenarios de combate donde se requiera comunicación a largas distancias, puede ser vulnerable si los nodos no están dentro del rango adecuado.

INTEROPERABILIDAD Y COMPATIBILIDAD.

- **Descripción:** Aunque diseñado para interoperar entre fuerzas aliadas de la OTAN, la interoperabilidad entre versiones más antiguas y modernas de Link 16 puede ser problemática.
- **Impacto:** Los sistemas antiguos pueden carecer de las actualizaciones necesarias, lo que los hace más vulnerables a ataques que aprovechen fallos o configuraciones no estándar.

ATAQUES BASADOS EN SEÑALES FALSAS.

- **Descripción:** Un atacante podría intentar generar señales falsas que imiten las características de Link 16 para confundir o engañar a los sistemas receptores (spoofing).
- **Impacto:** Esto podría resultar en la recepción de datos erróneos o la pérdida de confianza en las comunicaciones tácticas.

MITIGACIONES POTENCIALES A LAS VULNERABILIDADES EN LINK 16.

Aunque Link 16 tiene vulnerabilidades, muchas pueden ser mitigadas con medidas adecuadas:

1. **Actualización Criptográfica:** Implementar algoritmos de cifrado post-cuánticos para proteger las comunicaciones contra futuras amenazas.
2. **Fortalecimiento de Sincronización:** Integrar fuentes de sincronización redundantes para minimizar la dependencia del GPS.
3. **Entrenamiento y Procedimientos:** Mejorar las prácticas de configuración y manejo de claves criptográficas para reducir errores humanos.
4. **Monitoreo Activo:** Implementar sistemas de detección de intrusiones y monitoreo de red en tiempo real para identificar comportamientos anómalos.
5. **Modernización de Equipos:** Actualizar nodos más antiguos para garantizar la compatibilidad con los estándares más recientes y la resistencia frente a ataques.

CONCLUSIÓN.

Aunque **Link 16** es significativamente más robusto que su predecesor **Link 11**, presenta vulnerabilidades que lo hacen susceptible a amenazas avanzadas, como ataques de guerra electrónica, interrupciones de sincronización y compromisos criptográficos. Para garantizar su efectividad, es fundamental mantener actualizaciones regulares, implementar medidas de ciberseguridad modernas y capacitar al personal para mitigar posibles fallos en la configuración y operación del sistema.

3.3 VULNERABILIDADES IDENTIFICADAS EN LINK 22.

Link 22, también conocido como **NILE (NATO Improved Link Eleven)**, es un estándar de enlace de datos táctico diseñado para mejorar la interoperabilidad y la comunicación segura entre las fuerzas de la OTAN. Aunque ofrece importantes ventajas sobre los estándares previos, como Link 11 y Link 16, también enfrenta riesgos y vulnerabilidades. A continuación, se presentan las principales vulnerabilidades identificadas en Link 22:

VULNERABILIDADES DE SEGURIDAD.

INTERCEPCIÓN DE DATOS (EAVESDROPPING).

- **Descripción:** Los adversarios pueden interceptar las transmisiones si el cifrado es insuficiente o las claves no están bien gestionadas.
- **Mitigación:**
 - o Implementar algoritmos de cifrado modernos y robustos (como AES-256).
 - o Utilizar protocolos de encriptación certificados y actualizados.
 - o Establecer una política de rotación frecuente de claves de cifrado.

SUPLANTACIÓN DE IDENTIDAD (SPOOFING).

- **Descripción:** Un atacante podría hacerse pasar por un nodo legítimo y enviar información falsa a la red.
- **Mitigación:**
 - o Implementar mecanismos de autenticación fuerte, como certificados digitales.
 - o Utilizar tokens de sesión únicos y marcas temporales para validar mensajes.

MANIPULACIÓN DE DATOS (DATA TAMPERING).

- **Descripción:** Alteración de mensajes en tránsito para desinformar o comprometer operaciones.
- **Mitigación:**
 - o Utilizar códigos de autenticación de mensajes (MACs) para verificar la integridad.
 - o Implementar firmas digitales para garantizar la autenticidad de los mensajes.

ATAQUES DE DENEGACIÓN DE SERVICIO (DOS).

- **Descripción:** Saturación de la red con tráfico malicioso, lo que degrada o interrumpe la comunicación.
- **Mitigación:**
 - o Configurar límites de tráfico y capacidades de filtrado.
 - o Implementar sistemas de detección y prevención de intrusiones (IDS/IPS).
 - o Diseñar redundancias en la arquitectura de la red.

ATAQUES DE REPETICIÓN (REPLAY ATTACKS).

- **Descripción:** Reutilización de mensajes interceptados previamente para confundir o comprometer operaciones.
- **Mitigación:**
 - o Incluir marcas temporales y números de secuencia en los mensajes.
 - o Validar la unicidad de los mensajes recibidos en tiempo real.

VULNERABILIDADES DE DISPONIBILIDAD.

INTERFERENCIAS ELECTROMAGNÉTICAS (EMI).

- **Descripción:** Bloqueo o degradación de las comunicaciones mediante guerra electrónica.
- **Mitigación:**
 - o Usar frecuencias de comunicación dinámicas y técnicas de salto de frecuencia.
 - o Implementar antenas de alta ganancia con capacidades antiinterferencia.

DEPENDENCIA DE PUNTOS ÚNICOS DE FALLO.

- **Descripción:** Un nodo crítico caído puede afectar toda la red.
- **Mitigación:**
 - o Diseñar una arquitectura distribuida y redundante.
 - o Asegurar que todos los nodos puedan reconfigurarse automáticamente para mantener la conectividad.

LATENCIA Y CONGESTIÓN DE LA RED.

- **Descripción:** Retrasos en la transmisión de mensajes críticos por congestión o limitaciones técnicas.
- **Mitigación:**
 - o Optimizar la priorización del tráfico basado en la criticidad de los mensajes.
 - o Implementar herramientas de monitoreo para identificar y resolver cuellos de botella.

VULNERABILIDADES DE CONFIGURACIÓN.

GESTIÓN DEFICIENTE DE CLAVES DE CIFRADO.

- **Descripción:** Uso de claves predeterminadas o mala rotación de las mismas puede comprometer la seguridad.
- **Mitigación:**
 - o Adoptar sistemas automatizados de gestión de claves.
 - o Realizar auditorías regulares para validar la seguridad de las claves.

CONFIGURACIÓN INCORRECTA DE LA RED.

- **Descripción:** Errores humanos o configuraciones inconsistentes pueden generar vulnerabilidades.
- **Mitigación:**
 - o Establecer políticas claras de configuración y estándares.
 - o Utilizar herramientas de validación automatizada para verificar configuraciones.

USO DE SOFTWARE DESACTUALIZADO.

- **Descripción:** Las versiones antiguas pueden contener vulnerabilidades conocidas.
- **Mitigación:**
 - o Realizar actualizaciones regulares del software.
 - o Monitorear continuamente las alertas de seguridad relacionadas con Link 22.

VULNERABILIDADES ORGANIZATIVAS.**CAPACITACIÓN INSUFICIENTE DEL PERSONAL.**

- **Descripción:** Errores humanos debido a falta de conocimiento pueden introducir riesgos.
- **Mitigación:**
 - o Proveer capacitación periódica y simulaciones realistas para operadores.
 - o Crear manuales operativos claros y accesibles.

FALTA DE COORDINACIÓN MULTINACIONAL.

- **Descripción:** Implementaciones divergentes del estándar pueden causar incompatibilidades.
- **Mitigación:**
 - o Adoptar estándares estrictos de interoperabilidad en todos los países miembros.
 - o Realizar pruebas multinacionales regulares para verificar la compatibilidad.

RESUMEN DE MITIGACIONES CLAVE.

- **Ciberseguridad:** Cifrado fuerte, autenticación robusta y herramientas de detección de intrusos.
- **Redundancia:** Diseño de redes tolerantes a fallos y con capacidad de reconfiguración automática.
- **Automatización:** Uso de herramientas para gestionar claves, validar configuraciones y monitorear la red.
- **Capacitación y Procedimientos:** Asegurar que el personal esté bien entrenado y disponga de recursos adecuados.
- **Actualizaciones:** Mantener software y hardware actualizados para cerrar brechas conocidas.

3.4 VULNERABILIDAD POR SINCRONISMO EN TDL.

El sincronismo es un aspecto fundamental para el correcto funcionamiento de los **Tactical Data Links**, como Link 11B, Link 16, Link 22 y otros sistemas de enlace táctico. Una vulnerabilidad por sincronismo ocurre cuando los nodos de la red no logran mantener una sincronización temporal precisa, lo que afecta la comunicación, la transmisión de datos y la coordinación operativa.

DESCRIPCIÓN DE LA VULNERABILIDAD.

1. **Dependencia del Tiempo en los TDL:**
 - o Los TDLs operan en base a **tiempos altamente precisos** para coordinar las transmisiones entre nodos.
 - o La falta de sincronismo genera:
 - Mensajes fuera de secuencia.
 - Colisiones de datos.
 - Retransmisiones innecesarias.
2. **Causas Comunes de Pérdida de Sincronismo:**

- o **Interferencias Electromagnéticas (EMI):**
 - Actores maliciosos pueden emplear **jamming** para desestabilizar las señales de sincronización.
 - o **Ataques de Spoofing:**
 - Envío de señales falsas que desincronizan los nodos de la red.
 - o **Fallo en el GPS o Fuentes de Tiempo:**
 - Los TDLs suelen depender de sistemas GPS para sincronización, y su pérdida puede causar desincronización.
 - o **Deriva de Reloj (Clock Drift):**
 - Diferencias en la velocidad de los relojes internos entre nodos a lo largo del tiempo.
3. **Impacto Operacional:**
- o **Pérdida de Datos Críticos:**
 - Los mensajes fuera de sincronismo pueden ser descartados por los nodos receptores.
 - o **Descoordinación Táctica:**
 - Las fuerzas operativas pueden actuar basándose en datos incompletos o incorrectos.
 - o **Degradación de la Red:**
 - La desincronización provoca colisiones y retransmisiones, reduciendo la eficiencia del enlace.

IMPLICACIONES TÉCNICAS.

- **Colisiones de Transmisión:**
 - o Cuando varios nodos intentan transmitir al mismo tiempo debido a la falta de coordinación.
- **Desincronización de Mensajes:**
 - o Los datos llegan en un orden incorrecto, lo que afecta la coherencia táctica.
- **Fallos en el Modo de Enlace:**
 - o En TDL como Link 16 o Link 22, el uso de tiempos compartidos (Time Division Multiple Access, TDMA) depende de sincronización precisa. Sin ella, el esquema TDMA colapsa.

ESTRATEGIAS DE MITIGACIÓN.

FUENTES DE TIEMPO REDUNDANTES.

- Utilizar múltiples fuentes de sincronización:
 - o **Relojes Atómicos:** Ofrecen alta precisión como respaldo en caso de pérdida del GPS.
 - o **Redes de Tiempo Distribuido:** Permiten mantener la sincronización incluso si un nodo pierde acceso a la fuente primaria.

ROBUSTEZ CONTRA INTERFERENCIAS.

- Implementar **técnicas de salto de frecuencia (Frequency Hopping)** para evitar interferencias en frecuencias fijas.
- Usar algoritmos de **filtrado de señales** para identificar y rechazar señales de spoofing.

MECANISMOS DE RECUPERACIÓN AUTOMÁTICA.

- Diseñar sistemas de autoajuste que:

- o Detecten automáticamente la desincronización.
- o Recalibren los nodos para volver a alinearse con el tiempo de referencia.

SUPERVISIÓN CONTINUA.

- Implementar herramientas de monitoreo en tiempo real para detectar desviaciones en el sincronismo.
- Configurar alarmas para advertir al personal de problemas de sincronización.

DISEÑO RESILIENTE.

- Configurar nodos clave con capacidad de operar de manera autónoma en caso de desincronización temporal.
- Crear arquitecturas de red distribuidas que no dependan exclusivamente de un solo nodo o fuente de tiempo.

ENTRENAMIENTO DEL PERSONAL.

- Capacitar al personal técnico y operativo para:
 - o Identificar señales de pérdida de sincronismo.
 - o Responder rápidamente ante anomalías temporales en la red.

EJEMPLO PRÁCTICO DE ATAQUE Y MITIGACIÓN.

- **Ataque:** Un adversario utiliza jamming para interrumpir las señales GPS utilizadas para la sincronización.
- **Impacto:** La red pierde su referencia temporal, y los mensajes críticos no se entregan correctamente.
- **Mitigación:**
 - o Se activan relojes atómicos locales como respaldo.
 - o La red implementa salto de frecuencia para evitar el canal interferido.
 - o Un sistema de monitoreo detecta el ataque y alerta a las unidades operativas.

La **vulnerabilidad por sincronismo** en los TDL es crítica debido a su impacto directo en las operaciones tácticas. Mediante la adopción de fuentes redundantes, sistemas de monitoreo, protección contra interferencias y capacitación, se puede mitigar significativamente este riesgo.

4 ANÁLISIS DE CASOS DE ESTUDIO DE VULNERABILIDADES.

4.1 INTERFERENCIA Y SPOOFING DE TDL EN UN EJERCICIO MULTINACIONAL OTAN.

En este caso, analizaremos cómo la interferencia y el *spoofing* (suplantación) en los **TDL** pueden afectar la seguridad y efectividad de las operaciones militares durante un ejercicio conjunto. Este ejemplo servirá para comprender las vulnerabilidades asociadas a los TDL y las contramedidas aplicables.

El escenario propuesto (véase la figura 4-1, más abajo) es un ejercicio multinacional de la OTAN y presenta las siguientes características:

- Un ejercicio militar multinacional simula un escenario de combate terrestre, naval y aéreo con varios países aliados.
- Las plataformas participantes son aviones de combate, buques de guerra, unidades de infantería acorazadas, sistemas de defensa antiaérea y centros de mando y control (C2), todos interconectados a través de **Link 22**, **Link 16**, **Link 11** y **JREAP**.

El **objetivo** del ejercicio es mejorar la coordinación entre fuerzas aliadas y probar la interoperabilidad de los sistemas de comunicación.

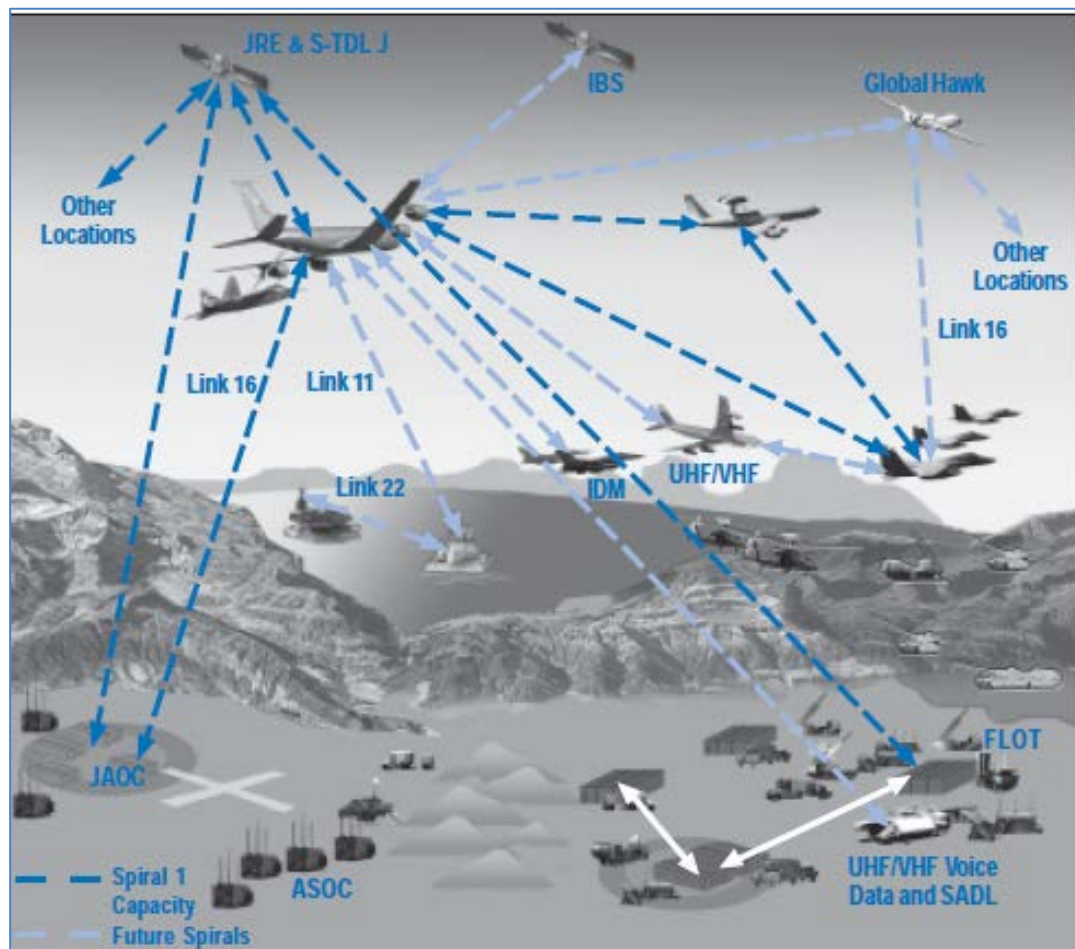


Figura 4-1. Interferencia y Spoofing en TDL en un ejercicio multinacional OTAN. [2]

Secuencia de eventos que ocurrirán:

- **Interferencia Electrónica (Jamming):** Un actor malintencionado, simulando ser parte de las fuerzas enemigas, utiliza un sistema de guerra electrónica para lanzar un ataque de interferencia (*jamming*) contra las frecuencias utilizadas por Link 16. El resultado es previsible:
 - Las comunicaciones entre los buques y los aviones aliados se ven degradadas.
 - El flujo de datos tácticos, como ubicaciones de objetivos y alertas de amenazas, se ralentiza o se interrumpe por completo.
 - Las unidades afectadas tienen que recurrir a canales de comunicación alternativos, lo que introduce demoras y aumenta el riesgo de errores.
- **Spoofing (Suplantación):** El atacante también emplea técnicas de *spoofing* para inyectar mensajes falsos en la red Link 16, haciéndose pasar por nodos legítimos. Hechos registrados de Spoofing:
 - Se envían coordenadas falsas de un supuesto objetivo enemigo, desviando los recursos aliados hacia un área vacía.
 - Un buque de guerra recibe órdenes falsas de reposicionamiento, creando una brecha en la formación táctica.
 - Los sistemas de defensa aérea reciben identificaciones falsas de aeronaves aliadas, clasificándolas como amenazas (*misidentification*), lo que podría llevar a un posible fuego amigo.

Desde el Centro de Mando y Control se ordenan **medidas de mitigación** para contrarrestar dichos ataques:

- **Contra la interferencia (Jamming):**
 - o Utilizar salto de frecuencias en espectro ensanchado tanto en Link 22 como en Link 16 para dificultar la localización y el bloqueo de la señal.
 - o Implementar transmisores de mayor potencia para superar interferencias.
 - o Emplear técnicas de análisis de espectro para detectar y contrarrestar ataques de interferencia.
- **Contra el Spoofing:**
 - o Usar autenticación criptográfica robusta para validar la identidad de los nodos participantes:
 - En Link 16, la autenticación robusta entre nodos se realiza mediante claves cifradas con KG-40/40A, compartidas y distribuidas periódicamente mediante procedimiento semi-automático.
 - En Link 22, la autenticación robusta entre nodos se realiza mediante Infraestructura de clave pública (PKI) con autenticación mutua.
 - Link 11 no dispone de autenticación robusta pues sus claves son compartidas mediante distribución manual. Se obligará a cambiar las claves de autenticación cada semana para intentar evitar el Spoofing.
 - o Implementar algoritmos de detección de anomalías en **dos IPS** (Intrusion Prevention System) de marca “Palo Alto Networks Threat Prevention” que colocaremos en los gateways y diversos nodos centrales para que identifiquen patrones de comunicación no esperados. Se activan ambos IPS (en configuración Activo-Reserva) para identificar patrones de tráfico anómalos en tiempo real.
- **Resiliencia y Continuidad Operativa:**
 - o Diseñar planes de contingencia para cambiar rápidamente a sistemas de respaldo.
 - o Usar redundancia en las redes de comunicación, como sistemas de enlace satelital o comunicación por fibra óptica.

- o Entrenar a los operadores en el manejo de fallos de los TDL y en el uso de métodos de comunicación alternativos.
- **Auditorías y Pruebas:**
 - o Realizar simulaciones periódicas de ataques para identificar vulnerabilidades en los sistemas de TDL.
 - o Actualizar constantemente el software y las claves criptográficas de los sistemas.

4.2 ATAQUES DE DENEGACIÓN DE SERVICIO (DOS) SOBRE TDL EN UN ESCENARIO DE ENTRENAMIENTO.

El escenario de entrenamiento propuesto tiene los siguientes requisitos:

- Las fuerzas armadas de un país realizan un entrenamiento conjunto de operaciones aéreas y terrestres.
- El ejercicio incluye la coordinación entre aviones de combate, vehículos terrestres y un centro de mando y control (C2), todos conectados a través de **Link 16**.
- El objetivo del ejercicio es evaluar la capacidad de respuesta y la interoperabilidad de las unidades bajo condiciones de combate simulado.
- Se simulará un ataque de Denegación de Servicio (DOS).

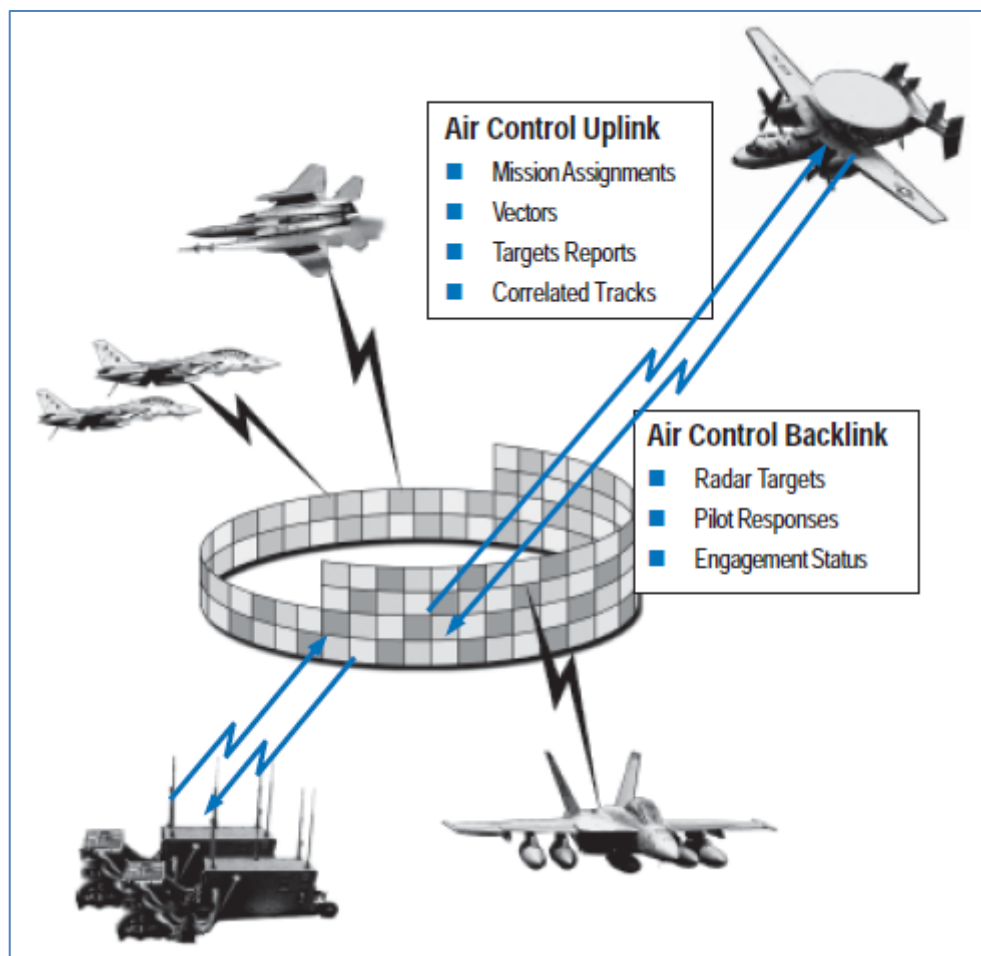


Figura 4-2. Ataque DOS simulado en un ejercicio de entrenamiento.

Descripción del Ataque: Un adversario simulado utiliza un sistema de guerra electrónica avanzado para llevar a cabo un ataque DoS. Este ataque sobrecarga la red Link 16 mediante:

- **Generación de tráfico malicioso:** El atacante introduce un gran volumen de señales falsas en las frecuencias del TDL.
- **Jamming selectivo:** Se concentra en saturar los canales de comunicación más críticos.

El **Impacto Inicial registrado** es el siguiente:

- Las unidades conectadas experimentan una **degradación en la velocidad y calidad de la comunicación**.
- Los mensajes clave, como alertas de amenazas, asignación de objetivos y actualizaciones de posición, no se transmiten correctamente.
- El tiempo de respuesta de las unidades se ve comprometido debido a la falta de información en tiempo real.

Desde el Centro de Mando y Control se ordenan **medidas de mitigación** para contrarrestar dichos ataques:

- **Prevención y Resiliencia:**
 - o Se ajusta el **Salto en frecuencia (Frequency Hopping)**: Se ajusta la configuración de Link 16 para emplear patrones de salto de frecuencia más rápidos y menos predecibles.
 - o **Potencia de Transmisión Ajustable**: Se incrementa la potencia de los transmisores para superar las señales de interferencia.
 - o Se adquieren **dos** IPS (Intrusion Prevention System) de marca “Palo Alto Networks Threat Prevention” que colocaremos en dos nodos centrales de la red Link 16. Se activan ambos IPS (en configuración Activo-Reserva) para identificar patrones de tráfico anómalos en tiempo real.
- 2. **Mitigación Durante el Ataque:**
 - o **Reconfiguración Dinámica**: Los nodos del TDL Link 16 cambian automáticamente a canales menos saturados.
 - o **Redirección de la Información**: El tráfico crítico se prioriza y se enruta a través de sistemas de comunicación redundantes (satélites y enlaces directos).
- 3. **Acciones Posteriores:**
 - o **Análisis Forense**: Se recopilan datos sobre el ataque, como la intensidad y las técnicas empleadas, para mejorar las defensas.
 - o **Actualización de Protocolos**: Se realizan ajustes en las configuraciones de seguridad del TDL para mitigar futuras vulnerabilidades.
 - o **Entrenamiento Complementario**: Se incluye una capacitación adicional para que las unidades puedan manejar fallos en las comunicaciones de forma más efectiva.

Lecciones aprendidas tras el simulacro:

- o La dependencia excesiva de un solo sistema de comunicaciones puede ser un riesgo crítico.
- o Las simulaciones deben incluir ataques DoS como parte del entrenamiento para mejorar la preparación de las fuerzas.

Los ataques de denegación de servicio representan una amenaza seria para los TDL, especialmente en escenarios de entrenamiento donde se evalúan capacidades críticas. La implementación de medidas preventivas, una rápida respuesta ante ataques y una estrategia de resiliencia a largo plazo son esenciales para garantizar que las fuerzas armadas puedan operar eficazmente incluso bajo condiciones adversas.

4.3 VULNERABILIDADES EXPLOTADAS EN SISTEMAS TDL OBSOLETOS.

Este caso analiza cómo las vulnerabilidades inherentes a sistemas de **TDL** obsoletos pueden ser explotadas en un contexto militar, comprometiendo la seguridad, la interoperabilidad y la efectividad operativa. El objetivo es resaltar las implicaciones de mantener sistemas desactualizados y las posibles soluciones.

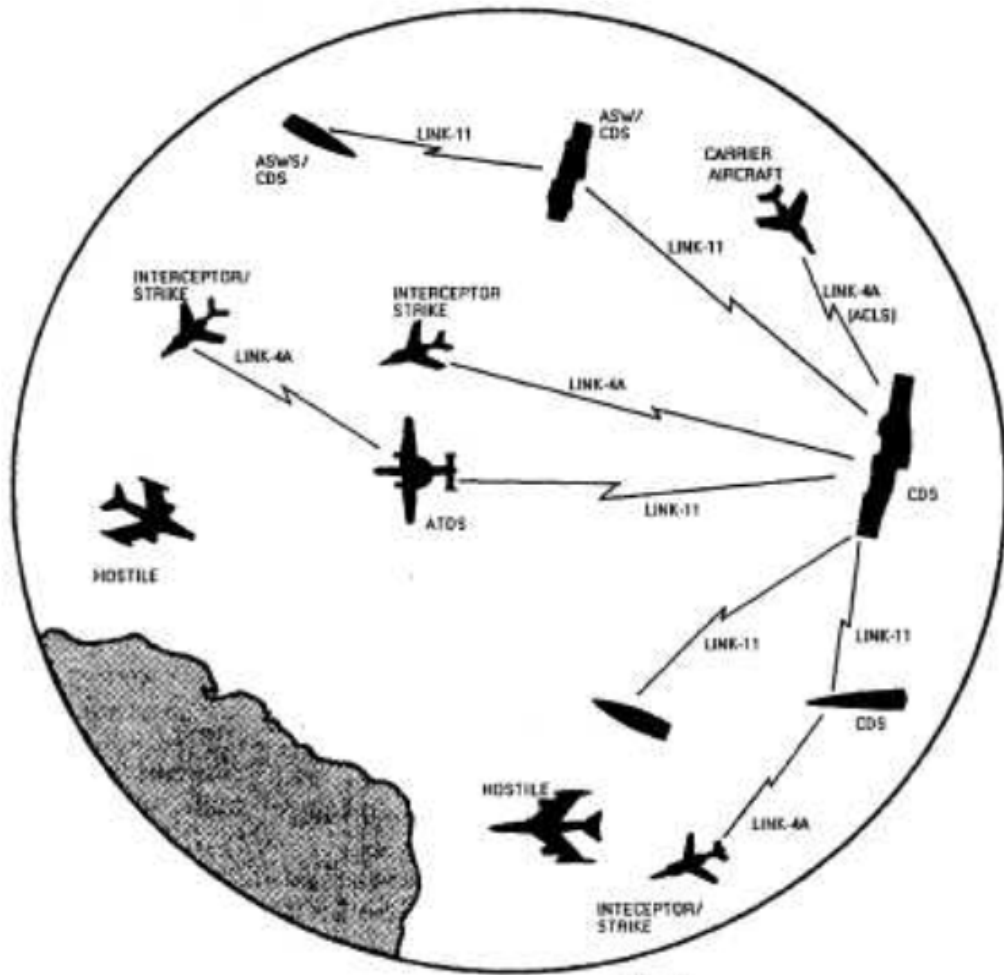


Figura 4-3. Despliegue naval empleando TDL obsoletos.

El **escenario** es una operación de vigilancia y patrulla con los siguientes requisitos:

- Un grupo naval de un país determinado utiliza **Link 11** y **Link 4A**, TDL obsoletos, para coordinar las operaciones de vigilancia y patrullaje en una zona marítima estratégica.
- El sistema conecta buques de guerra, aviones de patrullaje marítimo (MPA) y un centro de mando y control (C2) situado en un portaaviones, permitiendo el intercambio de datos tácticos sobre amenazas potenciales.

Se han registrado ciertas **acciones por parte del enemigo**:

- **Intercepción de Comunicaciones:** Un adversario utiliza equipo de inteligencia de señales (SIGINT) para interceptar transmisiones de Link 11, que carece de un cifrado robusto y utiliza técnicas de modulación más fáciles de descifrar. Como consecuencia:
 - El atacante obtiene información crítica, como posiciones de buques, trayectorias de vuelo y patrones de patrulla de los MPA.

- Se revela el alcance y la ubicación de los activos desplegados en la operación.
- **Inyección de Datos Falsos:** El adversario, tras analizar los datos interceptados, utiliza técnicas de **spoofing** para introducir información falsa en la red. Se registran determinadas acciones de Spoofing:
 - o Se envían ubicaciones ficticias de submarinos enemigos, desviando a los buques aliados y creando confusión táctica.
 - o Los aviones de patrulla reciben alertas falsas que los llevan a áreas sin actividad hostil.
- **Ataques de Denegación de Servicio (DoS):** Aprovechando las limitaciones técnicas de Link 4A y Link 11, el adversario lanza un ataque de saturación contra las frecuencias utilizadas. Como consecuencia se registran los siguientes efectos:
 - o La red experimenta interrupciones severas, dejando a las unidades sin capacidad para coordinarse efectivamente.
 - o Los operadores se ven obligados a usar sistemas de respaldo menos seguros, como radios de alta frecuencia (HF).

Desde el Centro de Mando y Control se ordenan **medidas de mitigación** para contrarrestar dichos ataques:

- **Modernización de los Sistemas TDL:** Se inicia un proceso de transición de Link 4A y Link 11 a **Link 16** o **Link 22**, que ofrecerán:
 - Cifrado robusto con estándares actuales.
 - Mecanismo TRANSEC de salto de frecuencias (*frequency hopping*) para resistir ataques de interferencia.
 - Mejores capacidades de autenticación de nodos.
- Se adquieren **dos IPS** (Intrusion Prevention System) de marca “Palo Alto Networks Threat Prevention” que colocaremos en dos nodos centrales de la red desplegada. Se activaran ambos IPS (en configuración Activo-Reserva) para identificar patrones de tráfico anómalos en tiempo real.
- **Fortalecimiento de las Prácticas Operativas:**
 - o Actualización de protocolos de operación para priorizar la seguridad de la información.
 - o Entrenamiento de los operadores en el manejo de situaciones de ciberseguridad, como ataques de interceptación o inyección de datos.
- **Simulaciones y Pruebas:**
 - o Realización de ejercicios regulares que incluyan escenarios de ciberataques en TDL obsoletos.
 - o Evaluación constante de las capacidades de los sistemas de comunicación para detectar vulnerabilidades emergentes.

Lecciones aprendidas identificadas tras el ataque:

- **Riesgos de Usar Tecnología Obsoleta:** Los sistemas desactualizados no pueden hacer frente a las amenazas modernas, exponiendo las operaciones a riesgos significativos.
- **Importancia de la Modernización:** La inversión en tecnologías avanzadas como Link 16 y Link 22 es esencial para mantener la superioridad operativa y la seguridad.
- **Preparación Ante Ciberataques:** Las fuerzas armadas deben integrar la ciberseguridad como una prioridad en todas las etapas de planificación y ejecución operativa.

Este caso de uso demuestra cómo las vulnerabilidades en sistemas TDL obsoletos pueden ser explotadas para comprometer operaciones militares. Modernizar las tecnologías, implementar contramedidas y entrenar a los operadores en ciberseguridad son pasos críticos para garantizar la seguridad, la interoperabilidad y la eficacia táctica en entornos militares complejos.

5 ESTRATEGIAS DE MITIGACIÓN Y MEJORA DE LA SEGURIDAD EN TDL.

5.1 CIFRADO AVANZADO EN TDL.

Los **Tactical Data Links (TDL)** son sistemas críticos en operaciones militares, ya que facilitan la comunicación y el intercambio de datos tácticos en tiempo real entre plataformas terrestres, aéreas, navales y centros de mando. Sin embargo, su importancia los convierte en objetivos clave para adversarios que buscan comprometer su confidencialidad, integridad y disponibilidad.

Para contrarrestar estas amenazas, se requiere la implementación de **cifrado avanzado** y mecanismos de **autenticación robustos** como pilares de la seguridad de los TDL.

CIFRADO AVANZADO.

El cifrado avanzado en **Tactical Data Link (TDL)** es un pilar crítico para garantizar la **confidencialidad, integridad y autenticación** en las comunicaciones tácticas. Dada la naturaleza sensible de los datos intercambiados, como información de vigilancia, control de fuego y coordinación táctica, el cifrado avanzado protege contra interceptaciones, manipulaciones y accesos no autorizados. Este análisis aborda los principios, métodos y desafíos del cifrado avanzado en TDL.

El cifrado avanzado en TDL emplea algoritmos criptográficos para transformar los datos en un formato ilegible para agentes no autorizados. Esto garantiza que solo las entidades legítimas con las claves apropiadas puedan descifrar y usar la información transmitida.

FUNDAMENTOS DEL CIFRADO AVANZADO.

Objetivos Principales.

1. **Confidencialidad:** Proteger los datos contra la interceptación.
2. **Integridad:** Garantizar que los datos no sean alterados durante la transmisión.
3. **Autenticación:** Confirmar la identidad de los emisores y receptores.

Componentes del Cifrado.

- **Algoritmo de cifrado:** Define cómo se transforman los datos (AES, RSA).
- **Claves criptográficas:** Elementos secretos que controlan el proceso de cifrado y descifrado.
- **Gestión de claves:** Incluye la distribución, almacenamiento y renovación de claves.

MÉTODOS DE CIFRADO EN TDL.

Cifrado Simétrico.

- **Descripción:** Ambas partes usan la misma clave para cifrar y descifrar datos. Se describe someramente el cifrado simétrico en la figura 5-1, más abajo.

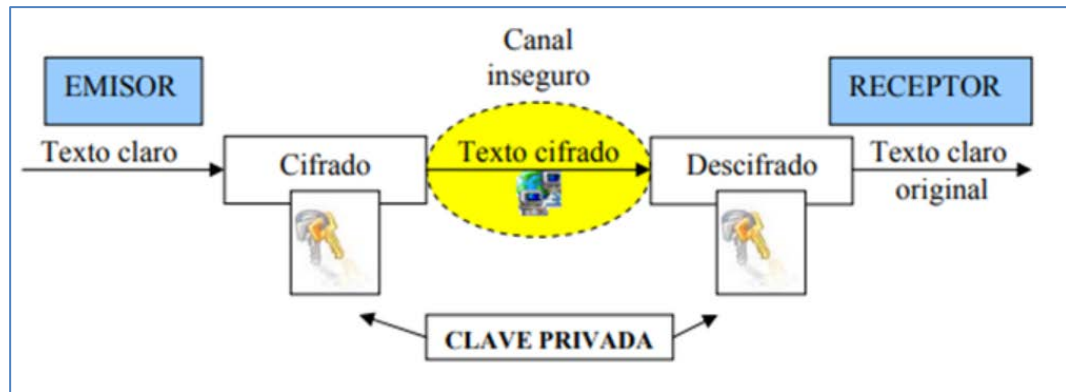


Figura 5-1. Equema de cifrado simétrico [2].

- **Ejemplo: Advanced Encryption Standard (AES)**
 - **Características:**
 - o Longitudes de clave: 128, 192 o 256 bits.
 - o Resistencia a ataques de fuerza bruta.
 - **Ventajas:**
 - o Velocidad y eficiencia computacional.
 - o Amplio soporte en hardware.
 - **Desventajas:**
 - o Requiere una gestión segura de claves para evitar compromisos.

Cifrado Asimétrico.

- **Descripción:** Usa un par de claves: una pública (cifrado) y una privada (descifrado). Se describe dicho proceso en la figura 5-2, más abajo.

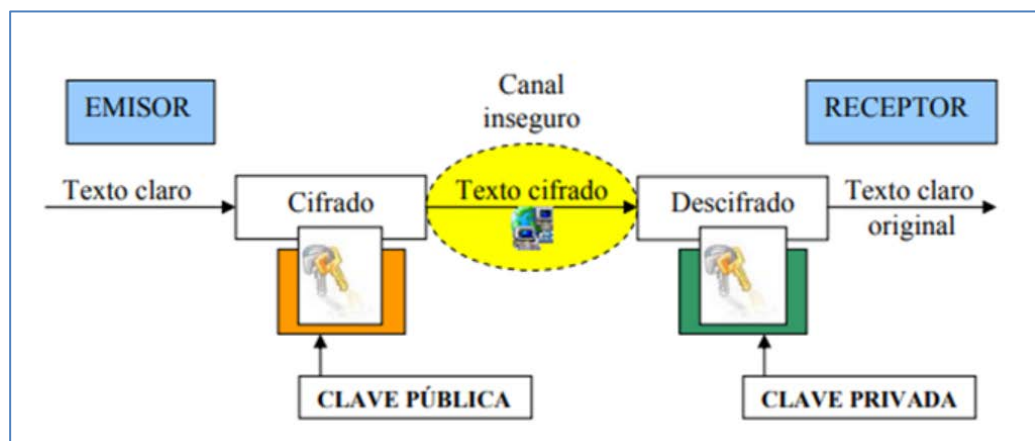


Figura 5-2. Equema de cifrado asimétrico.

- **Ejemplo: RSA (Rivest-Shamir-Adleman).**
 - **Características:**
 - o Basado en la dificultad de factorizar números grandes.
 - o Longitudes de clave típicas: 2048 a 4096 bits.
 - **Ventajas:**
 - o No requiere el intercambio directo de claves privadas.
 - **Desventajas:**
 - o Más lento que el cifrado simétrico.

- o Consume más recursos.

Cifrado Híbrido.

- **Descripción:** Combina cifrado simétrico y asimétrico para aprovechar las fortalezas de ambos. Se describe dicha tecnología de cifrado, más abajo, en la figura 5-3.

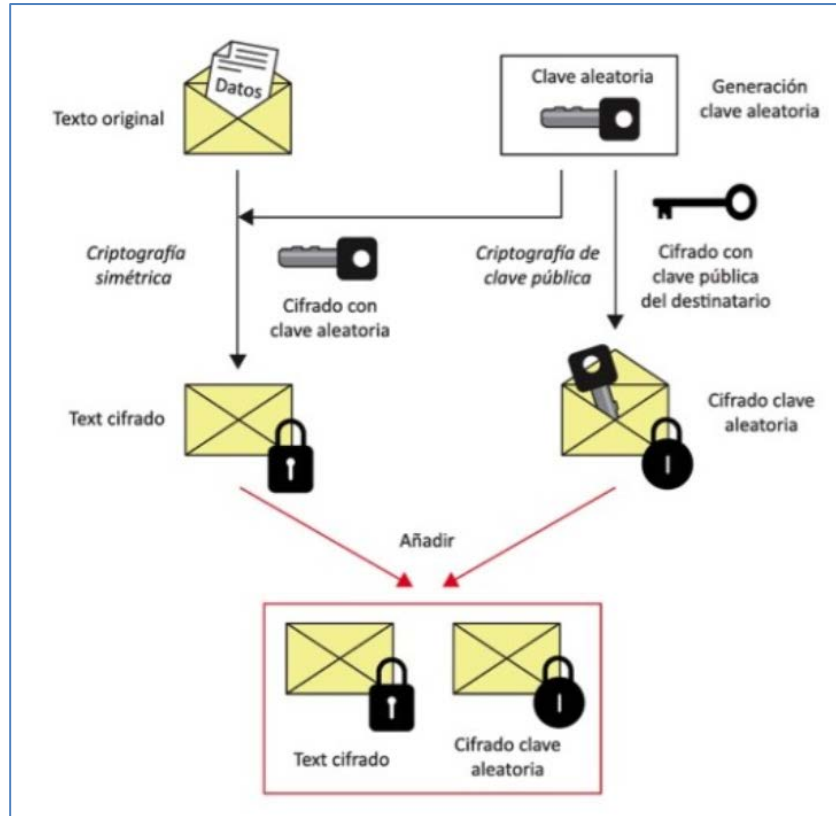


Figura 5-3. Esquema de cifrado híbrido.

- **Ejemplo: Intercambio de claves mediante RSA y cifrado de datos con AES.**
 - **Proceso:**
 1. RSA cifra la clave simétrica (AES).
 2. La clave cifrada se transmite al receptor.
 3. Los datos se cifran con AES.
 - **Ventajas:**
 - o Alta seguridad combinada con eficiencia.
 - o Ideal para entornos dinámicos como TDL.

TÉCNICAS AVANZADAS DE CIFRADO EN TDL.

CIFRADO BASADO EN HARDWARE.

- **Descripción:** Uso de módulos de hardware seguros (HSM²⁴) para realizar operaciones criptográficas. Estos dispositivos de hardware especializados se utilizan para gestionar, proteger y realizar operaciones criptográficas de alto rendimiento. Están diseñados para proporcionar un

²⁴ HSM: Hardware Security Module.

entorno seguro que evita accesos no autorizados y asegura la integridad de los datos críticos. El proceso de cifrado usando módulo hardware HSM está descrito, más abajo, en la figura 5-4.

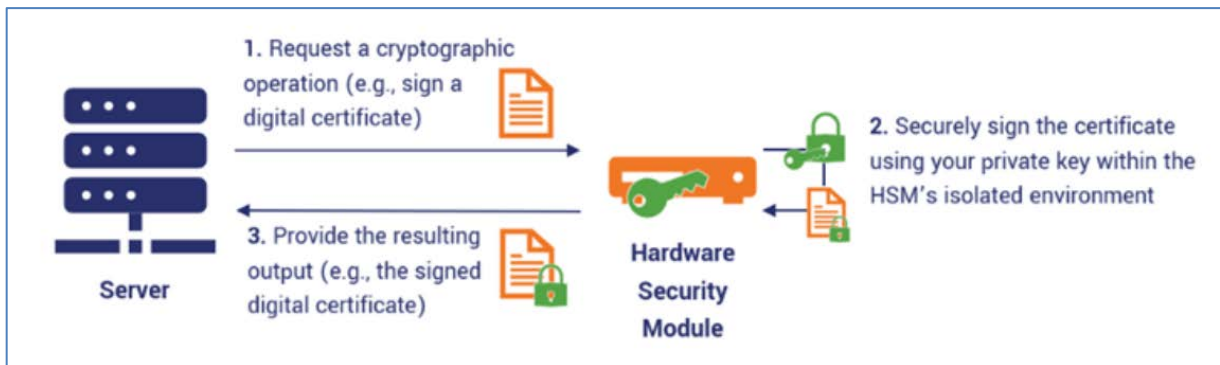


Figura 5-4. Esquema de cifrado en HSM.

- **Ventajas:**
 - o Mayor velocidad que el cifrado basado en software.
 - o Protección física contra manipulaciones.
- **Aplicaciones:** Encriptadores de red integrados en plataformas militares.

CIFRADO POST-CUÁNTICO.

- **Descripción:** La criptografía post-cuántica (también conocida como criptografía a prueba de cuántica, segura para la cuántica o resistente a la cuántica) se refiere a los algoritmos criptográficos (a menudo algoritmos de clave pública) que se espera que sean seguros contra un asalto criptoanalítico por parte de un ordenador cuántico.
- **Ejemplo:** Algoritmos como CRYSTALS-Kyber y CRYSTALS-Dilithium.
- **Ventajas:**
 - o Proporciona resistencia a amenazas futuras.
- **Desafíos:**
 - o Implementación temprana en sistemas TDL existentes.

CIFRADO DE FLUJO.

- **Descripción:** Un cifrado de flujo trabaja generando una cadena de bits pseudo-aleatorios que después combina con el contenido que va a cifrar mediante la operación XOR, también conocida como suma módulo 2. Para descifrar un texto cifrado, el algoritmo genera los mismos bits pseudo-aleatorios y los vuelve a combinar, dejando así solamente el texto claro. A esta cadena de bits pseudo-aleatoria se le conoce como el *keystream* o *cadena de bits de clave*. Dicho proceso se describe gráficamente en la figura 5-5, más abajo.



Figura 5-5. Esquema de cifrador de flujo.

- **Ventajas:**
 - o Alta velocidad en transmisiones continuas.
 - o Baja latencia.
- **Ejemplo:** Algoritmos basados en RC4 o ChaCha20 (aunque RC4 es obsoleto por vulnerabilidades).

CIFRADO HOMOMÓRFICO.

- **Descripción:** Permite realizar operaciones sobre datos cifrados sin necesidad de descifrarlos. El cifrado homomórfico es un método de cifrado que permite realizar cálculos en datos cifrados sin descifrarlos primero con una clave secreta. Los resultados de los cálculos también permanecen cifrados y solo pueden ser descifrados por el propietario de la clave privada (responsable). El proceso queda gráficamente descrito en la figura 5-6, más abajo.

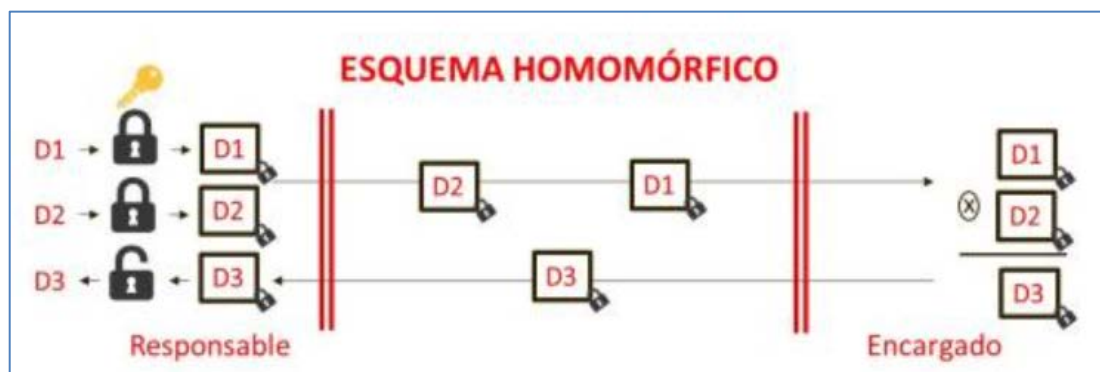


Figura 5-6. Esquema de cifrado homomórfico.

- **Ventajas:**
 - o Seguridad durante el procesamiento.
- **Aplicaciones:** Procesamiento en nodos intermedios de TDL.

GESTIÓN DE CLAVES CRIPTOGRÁFICAS.

INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI).

- **Descripción:** Sistema jerárquico para generar, almacenar y revocar certificados digitales. Un usuario de PKI puede consultar, en todo momento, un certificado de otro usuario de PKI y la

lista de certificados revocados (CRL²⁵). El proceso queda gráficamente descrito, más abajo, en la figura 5-7.

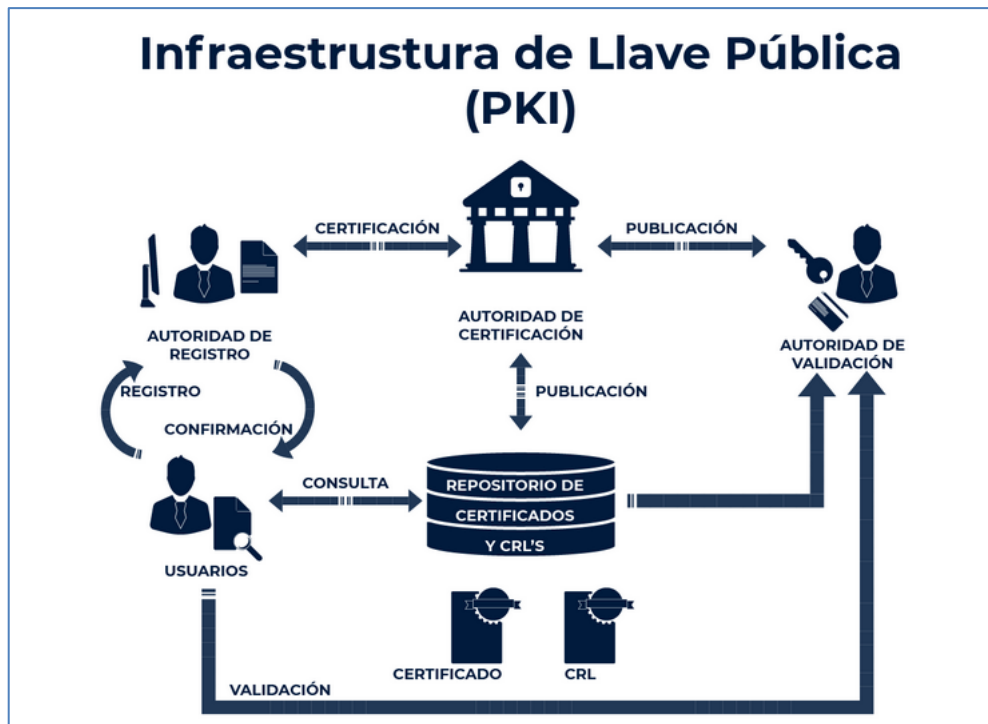


Figura 5-7. Esquema de PKI.

- **Ventajas:**
 - o Facilita la autenticación de entidades.
 - o Escalable para grandes redes.
- **Limitaciones:**
 - o Complejidad en la implementación y mantenimiento.

DISTRIBUCIÓN DE CLAVES EN TIEMPO REAL.

- **Método:** Uso de protocolos como Diffie-Hellman para el intercambio seguro de claves.
- **Desafíos:**
 - o Resistencia a ataques de intermediarios.
 - o Latencia adicional en redes TDL.

EVALUACIÓN DE LOS MÉTODOS DE CIFRADO.

La tabla 5-1, más abajo, evalúa los diferentes métodos de cifrado.

²⁵ CRL: Certificate Revocation List.

Método	Ventajas	Desventajas	Casos de Uso
AES	Rápido, eficiente, y altamente seguro	Requiere gestión segura de claves	Cifrado de datos en tiempo real
RSA	Resistente al intercambio inseguro	Lento y consume recursos	Intercambio de claves
Cifrado híbrido	Combina seguridad y eficiencia	Más complejo de implementar	Redes de alta seguridad
Post-cuántico	Resistente a computación cuántica	En etapa experimental	Preparación para amenazas futuras
Cifrado homomórfico	Seguridad en procesamiento	Lento y con alto costo computacional	Operaciones avanzadas en nodos TDL

Tabla 5-1. Evaluación de los métodos de cifrado.

DESAFÍOS DEL CIFRADO AVANZADO EN TDL.

1. **Latencia:** Los algoritmos avanzados pueden introducir retrasos en la transmisión de datos críticos.
2. **Interoperabilidad:** La integración de nuevos estándares de cifrado con sistemas heredados es compleja.
3. **Ciberseguridad avanzada:** Aparición de amenazas como computación cuántica y ataques dirigidos a la gestión de claves.
4. **Restricciones de hardware:** La necesidad de hardware especializado puede limitar la implementación en sistemas más antiguos.

COMPARATIVA DE MÉTODOS DE CIFRADO ENTRE LINK 11, LINK 16 Y LINK 22.

La tabla 5-2, más abajo, compara los diferentes métodos de cifrado de Link 11, Link 16 y Link 22.

Aspecto	Link 11	Link 16	Link 22
Época de Introducción	Década de 1950	Década de 1970	Década de 2000
Contexto de Desarrollo	Comunicaciones iniciales con protección limitada.	Red táctica avanzada diseñada para aliados de OTAN.	Enlace de datos moderno enfocado en interoperabilidad y alta seguridad.
Método de Cifrado Principal	Cifrado de flujo simple, basado en algoritmos simétricos.	Algoritmos simétricos avanzados como el cifrado KG-40/40A.	Algoritmos modernos, incluyendo AES (Advanced Encryption Standard).
Longitud de Clave	< 64 bits	128 bits (variable según la implementación).	128-256 bits, adaptable según políticas.
Nivel de Seguridad	Bajo. Vulnerable a ataques actuales.	Moderado. Resistente para su época pero insuficiente frente a ataques cuánticos.	Alto. Preparado para amenazas modernas y adaptable a cifrado post-cuántico.
Gestión de Claves	Manual, estática.	Distribución periódica mediante JRE.	Gestión automatizada, con rotación dinámica.
Resistencia a Interceptación	Limitada. Susceptible a criptoanálisis.	Buena, pero expuesta a ataques de larga duración.	Excelente, con alta resistencia incluso en escenarios prolongados.
Preparación Cuántica	No	No	Sí, con diseño modular para cifrado post-cuántico.

Tabla 5-2. Comparativa de métodos de cifrado entre Link 11, Link 16 y Link 22.

CONCLUSIÓN.

El cifrado avanzado es fundamental para la seguridad en Tactical Data Link. Métodos como AES, RSA y enfoques híbridos ofrecen una combinación de robustez y eficiencia, mientras que tecnologías emergentes como el cifrado post-cuántico y homomórfico apuntan al futuro de la seguridad en TDL. La elección del enfoque adecuado debe considerar el equilibrio entre seguridad, rendimiento y la capacidad de integración con sistemas existentes.

Para maximizar la eficacia, es crucial implementar un sistema de gestión de claves robusto y mantener una actualización constante frente a las amenazas emergentes.

5.2 AUTENTICACIÓN ROBUSTA EN TDL.

La **autenticación robusta** en **Tactical Data Links (TDL)** es un componente crítico para garantizar la seguridad y la confiabilidad de las comunicaciones tácticas. Su implementación protege contra accesos no autorizados, evita ataques de suplantación y asegura que los nodos participantes en la red sean legítimos y confiables. Este análisis aborda los principios, métodos y desafíos asociados con la autenticación robusta en TDL.

La autenticación robusta tiene como objetivo verificar la identidad de los nodos y usuarios en la red TDL antes de que se permita el intercambio de datos. Esto es crucial en entornos donde la pérdida de control de la red podría comprometer la misión, poner vidas en peligro o revelar información clasificada.

Las amenazas debidas a una deficiente autenticación en los TDL pueden provocar:

- **Ataques de suplantación de identidad (spoofing):** Donde un actor malicioso se hace pasar por un nodo legítimo.

- **Ataques de intermediarios (Man-in-the-Middle):** Interceptación de datos y manipulación durante el proceso de autenticación.
- **Repetición (Replay Attacks):** Uso de credenciales legítimas capturadas previamente.
- **Ataques de denegación de servicio (DoS):** Sobrecarga de solicitudes falsas para saturar los mecanismos de autenticación.

MÉTODOS DE AUTENTICACIÓN EN TDL.

AUTENTICACIÓN BASADA EN CLAVE COMPARTIDA.

Los nodos comparten una clave secreta previamente distribuida y esta clave se utiliza para generar valores hash o cifras que validan la identidad.

Las ventajas son la simplicidad, la rapidez y eficiencia en términos de ancho de banda.

Las desventajas son la vulnerabilidad a compromisos de la clave compartida y la difícil escalabilidad en redes grandes.

AUTENTICACIÓN BASADA EN INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI).

Cada nodo tiene un par de claves: una pública y otra privada. Los certificados digitales, emitidos por una Autoridad Certificadora (CA), verifican la autenticidad de las claves públicas.

Las ventajas son la alta seguridad que atesoran y el hecho de no requerir compartir claves privadas.

Las desventajas son la complejidad en la implementación y gestión de certificados y la latencia adicional debido a las verificaciones.

AUTENTICACIÓN MUTUA CON PROTOCOLOS DE SEGURIDAD.

Describiré como ejemplo de protocolo de seguridad el protocolo TLS (Transport Layer Security) adaptado a TDL. Sus características más destacadas son:

- Proporciona autenticación mutua mediante certificados.
- Establece un canal cifrado para evitar interceptaciones. En la figura 5-8, en el lateral derecho, se describe el proceso de saludo inicial (handshake) del protocolo TLS 1.3.

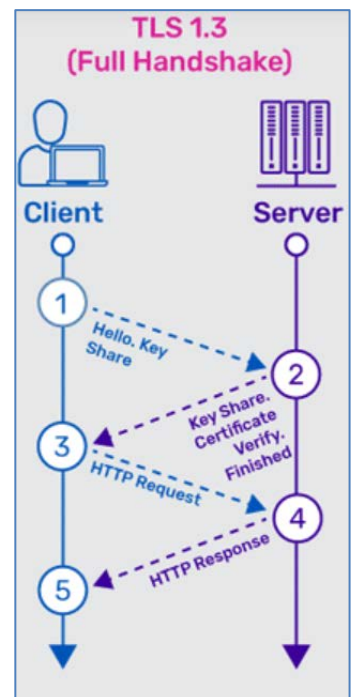
Figura 5-8. Esquema del Handshake en el protocolo TLS 1.3.

Las ventajas que ofrece son la prevención de ataques de intermediarios y la autenticación bidireccional.

Las desventajas que presenta son un mayor consumo de recursos y la necesidad de hardware especializado.

AUTENTICACIÓN BASADA EN TOKENS.

Cada nodo recibe un token único generado por un servidor de autenticación. Los tokens tienen una validez limitada y deben renovarse periódicamente. Dicho proceso queda gráficamente descrito, más abajo, en la figura 5-9.



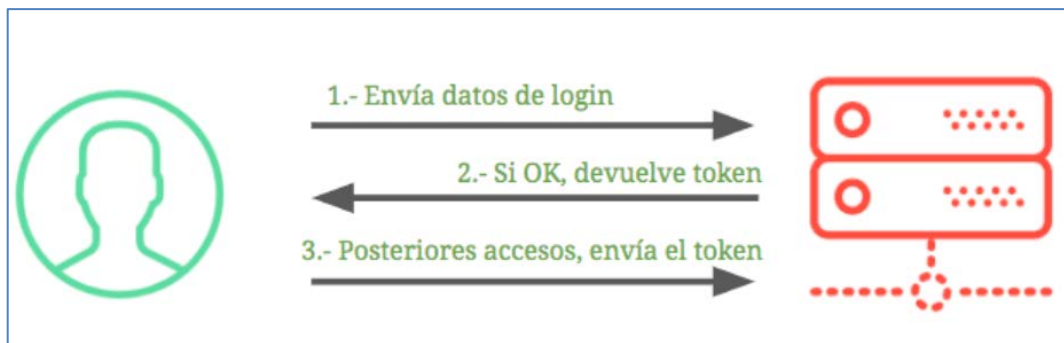


Figura 5-9. Esquema de autenticación basada en tokens.

Las ventajas que ofrece son la reducción del riesgo de uso indebido y el empleo de tokens temporales que minimizan el impacto de compromisos.

Las desventajas que presenta son que requiere una sincronización constante y tiene una dependencia de un servidor central.

MÉTODOS BASADOS EN BIOMETRÍA.

Son métodos que utilizan características biométricas como voz o huellas dactilares para autenticar usuarios. En la figura 5-10, más abajo, se muestran diferentes fuentes de datos biométricos a tener en cuenta para el ser humano.



Figura 5-10. Esquema de autenticación basada datos biométricos.

Las ventajas que ofrece son que son difíciles de falsificar y son útiles para autenticación en dispositivos móviles.

Las desventajas que presenta son la dificultad de implementación en entornos dinámicos como nodos aéreos y los problemas de privacidad que generan al guardar los datos biométricos.

AUTENTICACIÓN DE TERCERA GENERACIÓN: MÉTODOS CRIPTOGRÁFICOS AVANZADOS.

Protocolos Basados en Zero-Knowledge Proofs (ZKP):

Verifican la identidad sin revelar información sensible. Las pruebas de conocimiento cero (ZKP) nos permiten validar la verdad de algo sin revelar cómo conoces esa verdad (Prover) o compartir el contenido de esta verdad con el verificador (Verifier). Este principio se basa en un algoritmo que toma

algunos datos como entrada y devuelve 'verdadero' o 'falso'. El proceso se muestra en la figura 5-11, más abajo.

Ejemplo: Protocolos Schnorr.

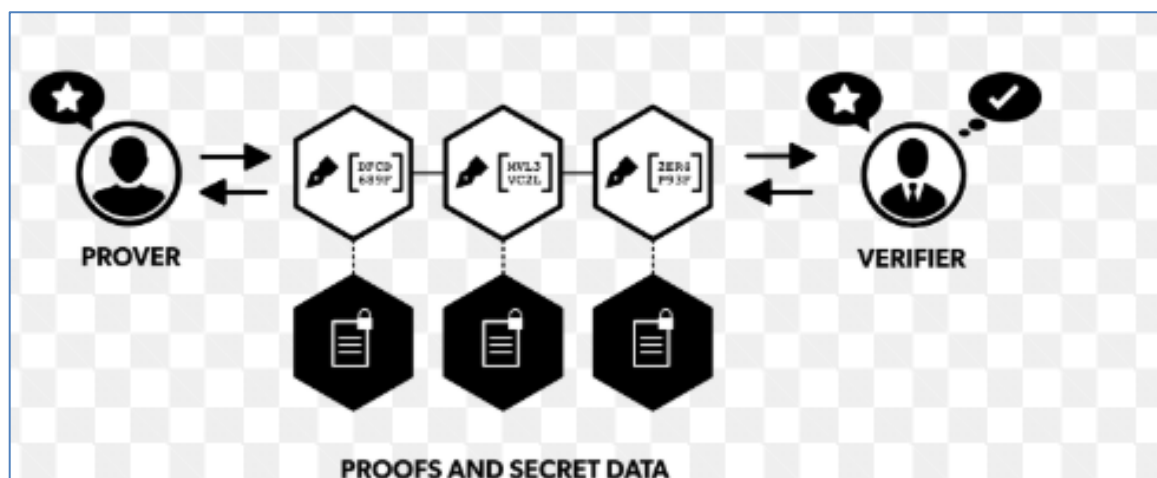


Figura 5-11. Esquema de protocolo Zero-Knowledge Proofs.

Autenticación Post-Cuántica:

Resistente a ataques de computación cuántica. La intención es desplegar algoritmos poscuánticos (PQC²⁶) antes de que exista un ordenador cuántico a gran escala capaz de romper los algoritmos de clave pública de uso generalizado en la actualidad. La hipótesis de trabajo es que mientras las personas adquieren confianza en los algoritmos PQC y sus implementaciones, los protocolos de seguridad utilizarán una mezcla de algoritmos tradicionales y PQC.

Ejemplo: Firmas digitales basadas en Lattice (Dilithium).

DESAFÍOS EN LA IMPLEMENTACIÓN DE AUTENTICACIÓN ROBUSTAS.

La autenticación robusta de los nodos en TDL presenta una serie de desafíos:

- **Limitaciones de Ancho de Banda:** Métodos avanzados, como PKI y ZKP, consumen más ancho de banda, lo que puede ser problemático en redes TDL de baja capacidad.
- **Latencia:** Los procesos de autenticación, especialmente los criptográficos, pueden introducir retrasos inaceptables en aplicaciones tácticas.
- **Interoperabilidad:** Los TDL, como Link 16 y Link 22, a menudo operan en entornos multinacionales con estándares heterogéneos.
- **Gestión de Claves y Certificados:** La rotación y distribución de claves/certificados es compleja, especialmente en escenarios tácticos dinámicos.

²⁶ PQC: Post Quantum Cryptography.

ESTRATEGIAS PARA FORTALECER LA AUTENTICACIÓN EN TDL.

Las estrategias para fortalecer la autenticación en TDL son las siguientes:

- **Uso de Sistemas Híbridos:** Combinar métodos tradicionales (de clave compartida) con tecnologías modernas (PKI o ZKP).
- **Implementación Modular:** Diseñar sistemas que permitan incorporar nuevas tecnologías de autenticación sin cambiar toda la infraestructura.
- **Evaluación y Simulación:** Probar nuevos métodos de autenticación en simulaciones operativas antes de su implementación en campo.

COMPARATIVA DE MÉTODOS DE AUTENTICACIÓN.

La tabla 5-3, más abajo, compara los métodos de autenticación utilizados por Link 11, Link 16 y Link 22.

Aspecto	Link 11	Link 16	Link 22
Época de Introducción	Década de 1950	Década de 1970	Década de 2000
Contexto de Desarrollo	Primera generación de enlaces digitales, con capacidades limitadas.	Red digital táctica avanzada para operaciones aliadas de OTAN.	Red diseñada para interoperabilidad y seguridad avanzada.
Método de Autenticación Principal	Basado en claves compartidas (simple).	Claves criptográficas distribuidas y sincronizadas periódicamente.	PKI (Infraestructura de Clave Pública) y autenticación mutua.
Nivel de Seguridad	Bajo. Protección básica para evitar accesos no autorizados.	Medio. Mejor resistencia contra suplantación y ataques básicos.	Alto. Resistencia frente a ataques avanzados y amenazas modernas.
Distribución de Claves	Manual, con alta dependencia de medios físicos.	Claves distribuidas a través de un sistema centralizado (JRE).	Automatizada y compatible con sistemas de gestión criptográfica moderna.
Frecuencia de Cambio de Claves	Estática, rara vez actualizada.	Actualización periódica basada en sincronización de nodos.	Dinámica, con rotación automatizada según políticas configuradas.
Interoperabilidad	Limitada, diseñado para fuerzas locales o regionales.	Ampliamente interoperable dentro de OTAN y aliados.	Global, con estándares compatibles en contextos multinacionales.
Resistencia a Amenazas Modernas	Vulnerable a ataques avanzados, como interceptación y análisis de claves.	Moderada, pero vulnerable a ataques computacionales avanzados (pre-cuánticos).	Alta, incluyendo protección frente a amenazas cuánticas.
Flexibilidad para Actualizaciones	Baja, limitado por su diseño antiguo.	Moderada, admite ciertos avances criptográficos.	Alta, con diseño modular para integrar nuevos métodos.

Tabla 5-3. Comparativa de métodos de autenticación de Link 11, Link 16 y Link 22.

CONCLUSIÓN.

Como **conclusión** se puede afirmar que la autenticación robusta en TDL es fundamental para proteger las comunicaciones tácticas frente a una variedad de amenazas. Métodos modernos como PKI, ZKP y autenticación post-cuántica ofrecen un nivel superior de seguridad, aunque enfrentan desafíos técnicos y operativos. Un enfoque híbrido y modular, combinado con pruebas rigurosas y una planificación estratégica, puede garantizar una transición segura hacia sistemas de autenticación más avanzados y resilientes.

5.3 CONSIDERACIONES SOBRE TECNOLOGÍAS DE CIFRADO Y ATENTICACIÓN EN TDL MODERNOS.

Tras pasar de forma rápida por el estado del arte de los TDL Link 11, Link 11B, Link 16 y Link 22, conviene destacar ciertas consideraciones a tener en cuenta:

- **Link 16 y Link 22:** Ambos TDL utilizan técnicas avanzadas de cifrado y autenticación. Link 22 incluye mejoras en la resistencia a ataques y en interoperabilidad.
- El documento **MIL-STD-188-220** es un protocolo estándar que define requisitos de seguridad para redes tácticas militares.
 - o Las **Redes Definidas por Software (SDN)** facilitan la implementación de algoritmos de cifrado y autenticación, actualizables.

Existen ciertos **desafíos en la implementación** de tecnologías de cifrado y autenticación en TDL:

- **Capacidad de Procesamiento:** Los nodos con recursos limitados, como drones o vehículos autónomos, pueden tener dificultades para manejar algoritmos avanzados.
- **Gestión de Claves:** La distribución y el almacenamiento seguro de claves criptográficas en entornos dinámicos son tareas complejas.
- **Compatibilidad con Sistemas Legados:** Los sistemas antiguos deben actualizarse o integrarse cuidadosamente con tecnologías modernas para mantener la seguridad y la funcionalidad.

Se dictan ciertas **recomendaciones** para implementar Cifrado y Autenticación en TDL:

- **Adoptar Estándares Modernos:** Migrar a sistemas como Link 16 y Link 22 con capacidades de cifrado avanzado.
- **Entrenamiento Regular:** Capacitar a los operadores en el manejo de sistemas seguros y en la detección de ataques.
- **Monitoreo Continuo:** Implementar sistemas de detección/prevención de intrusiones (IDS/IPS) para identificar intentos de acceso no autorizado en tiempo real.
- **Pruebas de Seguridad:** Realizar auditorías y simulaciones regulares para evaluar y mejorar las defensas de los TDL.

5.4 MONITORIZACIÓN Y DETECCIÓN DE INTRUSIONES EN TDL.

La **Monitorización y Detección/Prevención de Intrusiones (IDS/IPS)** en redes de **Tactical Data Links**, como Link 22, Link 16, Link 11, o sistemas similares, es un aspecto crítico para garantizar la seguridad y confiabilidad de la comunicación militar. Estas redes permiten la transmisión de información táctica entre plataformas, lo que las convierte en objetivos atractivos para ciberataques o interferencias.

Un **Sistema de Prevención de Intrusiones (IPS)** en el contexto de Link 11B, Link 16 o Link 22 es una herramienta de seguridad que no solo detecta actividades maliciosas en la red, sino que también responde automáticamente para neutralizar amenazas en tiempo real. El IPS es una evolución de los Sistemas de Detección de Intrusiones (IDS), diseñado específicamente para redes críticas, como los enlaces de datos tácticos utilizados en entornos militares.

Los modelos de IPS recomendados para Link 22, Link 16, Link 11 serían, dependiendo del presupuesto económicos (de menos a más):

Soluciones de IPS comerciales adaptadas:

- Palo Alto Networks Threat Prevention
 - Ofrece análisis avanzado basado en inteligencia artificial.
 - Detecta y bloquea amenazas conocidas y de día cero.
 - Compatible con redes cifradas y entornos de baja latencia.
- Cisco Firepower Next-Generation IPS
 - Integración profunda con redes IP tácticas.
 - Soporte para monitoreo distribuido en redes complejas.
 - Capacidad de análisis basado en comportamiento y firmas.
- Fortinet FortiGate IPS
 - Ofrece seguridad multinivel y gestión centralizada.
 - Escalable para redes dispersas y entornos militares.
 - Cifrado seguro y análisis de tráfico en tiempo real.
- Snort (Código abierto)
 - Altamente personalizable para entornos militares.
 - Bajo costo, ideal para despliegues flexibles.
 - Amplia base de datos de firmas y soporte para desarrollos específicos.

Sistemas IPS diseñados para uso militar (mayor coste económico, mayor eficiencia y resiliencia):

- Raytheon Cyber Solutions
 - Diseñado específicamente para operaciones de defensa.
 - Cumple con los estándares de interoperabilidad militar.
 - Altamente robusto frente a amenazas cibernéticas avanzadas.
- General Dynamics TACLANE
 - Integración directa con redes tácticas.
 - Compatible con cifrado militar y transmisión segura de datos.

CARACTERÍSTICAS PRINCIPALES DE UN IPS DISEÑADO PARA USO MILITAR.

Las características exigibles a un IPS diseñado para uso militar y que deberemos considerar a la hora de su adquisición, son:

1. Detección y Prevención Activa:

- Analiza el tráfico en tiempo real para identificar patrones maliciosos, como intentos de spoofing, ataques de jamming o inyecciones de mensajes falsos.
- Responde automáticamente mediante bloqueo de tráfico sospechoso, aislamiento de nodos o reconfiguración de la red.

2. Compatibilidad con Esquemas de Encriptación:

- Integración con los protocolos de cifrado de Link 22 para inspeccionar mensajes sin comprometer la seguridad.

- o Verifica la autenticidad y la integridad de los mensajes cifrados.
- 3. **Supervisión de Anomalías:**
 - o Usa inteligencia artificial y aprendizaje automático para identificar comportamientos fuera de lo normal en el tráfico de red.
 - o Detecta intentos de infiltración o manipulación, incluso si no coinciden con patrones conocidos.
- 4. **Defensa Contra Amenazas Específicas:**
 - o Ataques de Denegación de Servicio (DoS): Monitorea y limita el tráfico excesivo que podría saturar la red.
 - o Spoofing: Valida la identidad de los nodos emisores utilizando mecanismos de autenticación robustos.
 - o Interceptación: Implementa técnicas de detección de sniffing y monitorea intentos de escucha pasiva.

EJEMPLO PRÁCTICO.

Escenario: Un atacante intenta enviar mensajes falsos utilizando un nodo no autorizado para confundir a las fuerzas desplegadas en la operación. En la figura 5-12, más abajo, se describe un escenario de TDL con dos IPS, uno principal y uno alternativo.

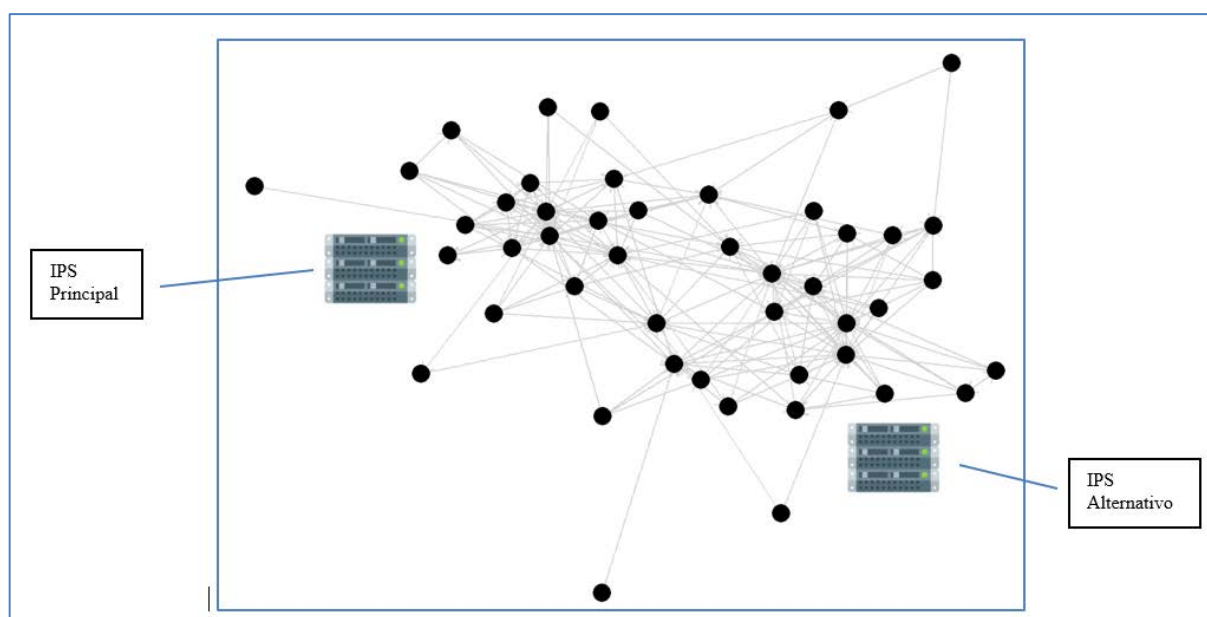


Figura 5-12. Esquema de despliegue de 2 IPS (Principal + Alternativo) en una TDL.

Acción a tomar: Se adquirirán **dos IPS** (Intrusion Prevention System) de marca “Palo Alto Networks Threat Prevention” que colocaremos en dos nodos centrales de la red desplegada. Se activarán ambos IPS (en configuración Activo-Reserva) para identificar patrones de tráfico anómalos en tiempo real.

La respuesta del IPS:

- Identifica que el mensaje proviene de un nodo no autenticado.
- Bloquea automáticamente el tráfico de ese nodo y envía una alerta al equipo de seguridad.
- Reconfigura las rutas de datos para minimizar el impacto del intento de intrusión.

El empleo de IPS presenta ciertos **desafíos y consideraciones** a tener en cuenta:

- **Sobrecarga del Sistema:** El análisis en tiempo real puede generar una carga significativa en redes de baja capacidad. Solución: Optimizar el IPS para priorizar amenazas críticas y reducir falsos positivos.
- **Interoperabilidad:** Asegurar que el IPS sea compatible con configuraciones multinacionales, especialmente en operaciones conjuntas de la OTAN.
- **Capacitación del Personal:** Formación especializada para interpretar alertas y configurar políticas adecuadas.

La implementación de un IPS en **Link 22** proporciona una capa esencial de defensa frente a amenazas modernas, asegurando la seguridad de las comunicaciones tácticas y la resiliencia operativa en entornos críticos.

5.5 ACTUALIZACIÓN Y PARCHEO REGULAR DE LOS SISTEMAS EN TDL.

La **actualización y parcheo regular de los sistemas en Tactical Data Links (TDLs)** es una práctica esencial para mantener la seguridad, disponibilidad y rendimiento de estas redes críticas en entornos operativos. Dado el contexto militar y de defensa en el que operan los TDL, cualquier vulnerabilidad puede ser explotada con graves consecuencias tácticas y estratégicas.

IMPORTANCIA DE LAS ACTUALIZACIONES Y PARCHEOS.

1. **Corrección de Vulnerabilidades:**
 - o Los desarrolladores de sistemas TDL lanzan parches para cerrar brechas de seguridad identificadas.
 - o Esto protege contra exploits conocidos que podrían comprometer la integridad o confidencialidad de los datos.
2. **Compatibilidad y Rendimiento:**
 - o Las actualizaciones pueden incluir mejoras en la interoperabilidad entre diferentes plataformas.
 - o Optimización del uso del ancho de banda y mejora en el procesamiento de datos.
3. **Adaptación a Amenazas Emergentes:**
 - o Las amenazas evolucionan rápidamente, y los sistemas TDL deben mantenerse a la par para enfrentar ataques sofisticados, como **interferencias electrónicas** o **ciberataques dirigidos**.
4. **Cumplimiento Normativo:**
 - o En entornos militares, es obligatorio adherirse a estándares actualizados de seguridad como STANAG 5516 (para Link 16).

DESAFÍOS EN EL PARCHEO DE TDL.

1. **Entornos Operativos Críticos:**
 - o Los sistemas TDL operan frecuentemente en tiempo real en escenarios tácticos. Las interrupciones para aplicar parches deben minimizarse.
2. **Complejidad Técnica:**
 - o La arquitectura de TDL incluye nodos distribuidos, equipos especializados y protocolos únicos que complican el proceso de actualización.
3. **Dependencia de Certificaciones:**
 - o Los parches deben ser rigurosamente probados y certificados antes de su implementación en sistemas críticos.
4. **Aislamiento de Red:**

- o Muchos sistemas TDL funcionan en entornos cerrados o con conectividad limitada, lo que dificulta la distribución de actualizaciones.

ESTRATEGIA DE ACTUALIZACIÓN Y PARCHEO.

- 1. Evaluación y Priorización:**
 - o Clasificar las vulnerabilidades según su impacto y probabilidad de explotación.
 - o Priorización de parches críticos relacionados con vulnerabilidades de día cero o exploits activos.
- 2. Pruebas en Entornos Simulados:**
 - o Antes de implementar un parche, probarlo en un entorno que simule el sistema TDL real para garantizar compatibilidad y estabilidad.
- 3. Parcheo Programado:**
 - o Establecer ventanas de mantenimiento para aplicar actualizaciones sin interrumpir operaciones críticas.
- 4. Mecanismos de Respaldo:**
 - o Asegurar que existan copias de seguridad completas antes de la implementación del parche.
 - o Planes de contingencia para revertir cambios en caso de fallos.
- 5. Automatización:**
 - o Uso de herramientas que permitan programar y monitorear actualizaciones en múltiples nodos de forma remota.

BUENAS PRÁCTICAS PARA EL PARCHEO REGULAR.

- 1. Ciclo de Vida del Software:**
 - o Implementar una estrategia de gestión del ciclo de vida que contemple actualizaciones regulares.
- 2. Entrenamiento y Capacitación:**
 - o Capacitar a los operadores para reconocer la importancia de las actualizaciones y ejecutar los procesos según protocolos establecidos.
- 3. Colaboración con Proveedores:**
 - o Trabajar estrechamente con los fabricantes para garantizar el acceso a parches certificados y recibir alertas tempranas sobre vulnerabilidades.
- 4. Monitoreo Continuo:**
 - o Implementar herramientas de monitoreo que permitan identificar vulnerabilidades antes de que sean explotadas.

COMPARATIVA DE ACTUALIZACIONES Y PARCHEO.

La tabla 4-2, más abajo, compara los métodos de actualización y parcheo empleados en Link 11, Link 16 y Link 22.

Aspecto	Link 11	Link 16	Link 22
Época de Introducción	Década de 1950	Década de 1970	Década de 2000
Capacidad de Actualización Inicial	Limitada. Diseñado como un sistema estático.	Moderada. Capacidad para incorporar mejoras puntuales.	Alta. Diseñado para actualizaciones modulares y continuas.
Método de Implementación	Manual. Requiere reemplazo de hardware en muchos casos.	Combinación de software y hardware.	Basado principalmente en software, con menor dependencia de hardware.
Frecuencia de Parcheo	Muy baja. Parches raramente aplicados.	Moderada. Ciclos de parcheo periódicos, pero no automatizados.	Alta. Compatible con actualizaciones regulares y automatizadas.
Manejo de Vulnerabilidades	Reactivo. Difícil de abordar vulnerabilidades emergentes.	Moderadamente reactivo. Vulnerabilidades tratadas con retraso.	Proactivo. Mecanismos de detección temprana y respuesta ágil.
Interoperabilidad en Actualizaciones	Baja. Actualizaciones específicas para cada sistema.	Moderada. Sincronización necesaria entre nodos aliados.	Alta. Estandarización multinacional con compatibilidad plena.
Coste de Implementación de Parches	Alto, debido al enfoque manual y dependiente de hardware.	Medio, con necesidad de intervención técnica.	Bajo, gracias a la automatización y soporte remoto.
Preparación para el Futuro	Inexistente. Obsoleto frente a nuevas amenazas.	Limitada. Requiere reemplazos significativos para grandes mejoras.	Alta. Diseñado para integrar avances tecnológicos.

Tabla 5-4. Comparativa de actualizaciones y parcheo entre Link 11, Link 16 y Link 22.

ACTUALIZACIONES Y PARCHEO EN LINK 11.

Características Clave.

- **Enfoque:** Diseño original estático, sin considerar la necesidad de actualizaciones frecuentes.
- **Método de Parcheo:** Requiere intervenciones manuales y, en muchos casos, reemplazo físico de componentes.
- **Frecuencia:** Muy baja. Las actualizaciones eran excepcionales, realizadas solo en casos críticos.
- **Manejo de Vulnerabilidades:**
 - o Reactivo y poco efectivo para abordar nuevas amenazas.
 - o Dificultades para mitigar vulnerabilidades críticas debido a la obsolescencia del diseño.

Ventajas:

- Simplicidad en su tiempo de implementación inicial.

Desventajas:

- Incapacidad para adaptarse a las amenazas modernas.
- Alto coste y esfuerzo para implementar cambios.

ACTUALIZACIONES Y PARCHEO EN LINK 16.

Características Clave.

- **Enfoque:** Introducción de capacidades de actualización mediante hardware y software.
- **Método de Parcheo:** Requiere sincronización manual o semiautomatizada entre nodos.
- **Frecuencia:** Moderada. Las actualizaciones se aplican periódicamente pero no en tiempo real.
- **Manejo de Vulnerabilidades:**
 - o Mayor capacidad para abordar amenazas emergentes, aunque con limitaciones en velocidad de respuesta.
 - o Dependencia de sistemas externos (e.g., JRE) para aplicar parches de manera coordinada.

Ventajas:

- Mejor capacidad de actualización en comparación con Link 11.
- Interoperabilidad mejorada dentro de OTAN y aliados.

Desventajas:

- Proceso de actualización relativamente lento.
- Necesidad de soporte técnico especializado para implementar parches.

ACTUALIZACIONES Y PARCHEO EN LINK 22.

Características Clave.

- **Enfoque:** Diseñado para actualizaciones regulares y modulares, con enfoque en software.
- **Método de Parcheo:** Automatizado, con capacidad de despliegue remoto y sincronización en tiempo real.
- **Frecuencia:** Alta. Compatible con ciclos de parcheo regulares y respuestas rápidas a nuevas amenazas.
- **Manejo de Vulnerabilidades:**
 - o Proactivo, con sistemas avanzados de detección y mitigación.
 - o Diseño modular que facilita la integración de nuevas tecnologías (cifrado post-cuántico, por ejemplo).

Ventajas:

- Proceso eficiente y económico de actualizaciones.
- Respuesta ágil a vulnerabilidades y amenazas emergentes.
- Alta interoperabilidad en escenarios multinacionales.

Desventajas:

- Complejidad inicial en la configuración y despliegue.
- Dependencia de infraestructura moderna para actualizaciones remotas.

COMPARACIÓN RESUMIDA: EVOLUCIÓN DE LAS ACTUALIZACIONES.

La tabla 5-5, más abajo, compara la capacidad de actualización de Link 11, Link 16 y Link 22.

Aspecto Evolutivo	Link 11	Link 16	Link 22
Capacidad Inicial	Limitada.	Moderada.	Alta.
Automatización	No.	Parcial.	Sí, completa.
Frecuencia de Parches	Muy baja.	Moderada.	Alta y continua.
Interoperabilidad OTAN	Baja.	Moderada.	Óptima.
Preparación para Futuro	Inexistente.	Limitada.	Completa.

Tabla 5-5. Comparativa de actualizaciones entre Link 11, Link 16 y Link 22.

CONCLUSIÓN.

La capacidad de actualización y parcheo ha mejorado drásticamente a lo largo del tiempo. **Link 11**, diseñado en una era con menores riesgos cibernéticos, carece de flexibilidad para adaptarse a amenazas modernas. **Link 16** representa un avance significativo, pero aún depende de procesos manuales y semiautomatizados. Por otro lado, **Link 22** incorpora mecanismos automatizados y modulares que permiten responder rápidamente a vulnerabilidades y adoptar nuevas tecnologías, posicionándolo como la opción más segura y eficiente para las comunicaciones tácticas modernas.

La transición hacia **Link 22** y la mejora continua de **Link 16** son esenciales para mantener la seguridad y la interoperabilidad en un entorno de amenazas tecnológicas en constante evolución.

5.6 PROTECCIÓN ANTIJAMMING.

La **protección antijamming** en **Tactical Data Links** es una medida crítica para garantizar la integridad, disponibilidad y resiliencia de las comunicaciones en entornos militares. Los ataques de interferencia (jamming) buscan degradar o bloquear las señales de comunicación mediante la emisión de ruido o señales maliciosas en las frecuencias utilizadas por los TDL. Dado que los TDL como Link 22, Link 16, Link 11 o JREAP son esenciales para el intercambio de datos tácticos, su protección es una prioridad estratégica.

Los **desafíos** del Jamming en TDL a tener en cuenta son los siguientes:

- **Tipos de Interferencias:**
 - o **Interferencia Barrido (Sweeping):** Señal de barrido continuo que afecta un rango amplio de frecuencias.
 - o **Interferencia Puntual (Spot Jamming):** Ataque dirigido a una frecuencia específica.
 - o **Interferencia de Seguimiento (Follower Jamming):** Cambia dinámicamente para interferir con las frecuencias activas.
 - o **Pulse Jamming:** Ataques intermitentes diseñados para evitar detección inmediata.
- **Entornos Adversos:**
 - o Operación en áreas de combate con alta densidad de dispositivos de guerra electrónica.
 - o Uso de tecnologías avanzadas de jamming por parte de adversarios.

- **Naturaleza de los TDL:**
 - La sincronización precisa y la dependencia de la integridad de los datos hacen que los TDL sean vulnerables a perturbaciones en la señal.

Las **estrategias** de protección antijamming que deben ser consideradas son:

- **Espectro Ensanchado:** Utilizar técnicas como **Frequency Hopping Spread Spectrum (FHSS)**, donde las señales cambian rápidamente entre múltiples frecuencias.
 - Ejemplo: Link 16 emplea FHSS con hasta 51.2 kbps, haciendo difícil que un atacante bloquee toda la banda simultáneamente.
- **Potencia de Señal Adaptativa:** Ajustar dinámicamente la potencia de transmisión para contrarrestar interferencias y reducir la posibilidad de detección.
- **Codificación y Modulación Robustas:** Implementar esquemas de modulación resistentes a interferencias, como **M-Code** o técnicas de corrección de errores como **Reed-Solomon**.
- **Detección y Evitación:** Sistemas que monitorean el espectro y reubican automáticamente las señales a frecuencias menos saturadas o afectadas.
- **Uso de Ondas Directivas:** Tecnologías como **antenas direccionales** o **arrays de fase** para concentrar las señales en la dirección del receptor y minimizar la exposición al ruido externo.
- **Integración con Guerra Electrónica:** Vincular los sistemas TDL con plataformas de guerra electrónica (EW) para detectar, localizar y neutralizar fuentes de jamming.

Las **tecnologías** a tener en consideración para la protección antijamming son:

- **Frequency Hopping Spread Spectrum (FHSS):** Cambios rápidos y pseudoaleatorios de frecuencia basados en claves criptográficas.
 - Ejemplo: La estructura de Link 16 cambia frecuencias hasta 77,000 veces por segundo.
- **Direct Sequence Spread Spectrum (DSSS):** Distribuye la señal en una banda más ancha, lo que reduce su densidad de potencia y dificulta el bloqueo.
- **Criptografía TRANSEC:** Transmisión segura con claves criptográficas que protegen tanto la sincronización como el patrón de frecuencia.
- **Beamforming:** Antenas avanzadas que ajustan dinámicamente la dirección de la señal para evitar interferencias.
- **Software Defined Radios (SDRs):** Equipos flexibles que pueden adaptarse a diferentes estrategias de mitigación en tiempo real.
- **Cámaras de Vigilancia del Espectro:** Herramientas como **RTSA (Real-Time Spectrum Analysis)** para supervisar el entorno electromagnético y anticipar intentos de interferencia.

COMPARATIVA DE PROTECCIÓN ANTI-JAMMING.

La tabla 5-6, más abajo, compara las diferentes capacidades de protección anti-jamming de Link 11, Link 16 y Link 22.

Aspecto	Link 11	Link 16	Link 22
Época de Introducción	Década de 1950	Década de 1970	Década de 2000
Tecnología de Transmisión	Radiofrecuencia analógica con modulación AM/SSB ²⁷ .	Salto de Frecuencia en Espectro Ensanchado (Frequency Hopping Spread Spectrum).	Salto de Frecuencia con protocolos avanzados.
Método Anti-Jamming Principal	Modulación básica con limitada resistencia.	Salto de frecuencia (FHSS) y encriptación.	FHSS mejorado y técnicas de dispersión espectral.
Capacidad de Resistencia	Baja. Vulnerable a interferencias deliberadas.	Alta. Excelente resistencia frente a jamming activo.	Muy alta. Mejora significativa sobre Link 16.
Interoperabilidad OTAN	Limitada.	Alta. Compatible con aliados OTAN.	Óptima. Estándar para interoperabilidad multinacional.
Preparación para Nuevas Amenazas	Nula.	Limitada. Necesita actualizaciones.	Alta. Preparado para entornos modernos y futuros.
Frecuencia Operativa	HF/UHF.	UHF/L-Band.	HF/UHF/L-Band ²⁸ .

Tabla 5.6. Comparativa anti-jamming completa entre Link 11, Link 16 y Link 22.

PROTECCIÓN ANTI-JAMMING EN LINK 11.

CARACTERÍSTICAS CLAVE.

- **Método Principal:** Modulación analógica en frecuencias HF y UHF.
- **Capacidad de Resistencia:**
 - o Muy limitada. La señal es fácilmente identificable y bloqueable con interferencias deliberadas.
 - o Vulnerable al ruido electromagnético y ataques básicos de jamming.
- **Limitaciones:**
 - o Diseñado en una era con amenazas electrónicas mínimas.
 - o Sin técnicas avanzadas de dispersión o salto de frecuencia.
- **Ventajas:**
 - o Simplicidad de implementación.
 - o Adecuado para su contexto histórico.
- **Desventajas:**
 - o Totalmente obsoleto frente a amenazas modernas.

²⁷ Modulación AM/SSB: Modulación de banda lateral única o SSB (Single Side Band) es una evolución de la AM.

²⁸ Banda L: La Banda L es un rango de radiofrecuencia de las microondas IEEE que usa las frecuencias de 1 a 2 GHz.

- o Muy vulnerable a cualquier interferencia.

PROTECCIÓN ANTI-JAMMING EN LINK 16.

CARACTERÍSTICAS CLAVE.

- **Método Principal:** Salto de Frecuencia de Espectro Ensanchado (FHSS) con intervalos cortos de tiempo.
- **Capacidad de Resistencia:**
 - o Alta. El salto rápido de frecuencia hace que sea difícil para los adversarios bloquear toda la señal.
 - o Uso de técnicas de encriptación para evitar la identificación de patrones.
- **Limitaciones:**
 - o Aunque robusto, puede ser vulnerable a interferencias electrónicas avanzadas si el enemigo posee tecnología altamente sofisticada.
 - o Operaciones pueden verse afectadas por congestión del espectro.
- **Ventajas:**
 - o Excelente resistencia frente a jamming activo.
 - o Interoperabilidad amplia dentro de OTAN.
- **Desventajas:**
 - o Requiere sincronización precisa entre nodos.
 - o Necesidad de modernización para enfrentar amenazas emergentes.

PROTECCIÓN ANTI-JAMMING EN LINK 22.

CARACTERÍSTICAS CLAVE.

- **Método Principal:** FHSS mejorado con técnicas avanzadas de dispersión espectral.
- **Capacidad de Resistencia:**
 - o Muy alta. Incorpora mejoras sobre las técnicas de Link 16, incluyendo algoritmos más eficientes para gestionar el espectro.
 - o Preparado para operar en entornos electromagnéticos altamente contestados.
- **Limitaciones:**
 - o Mayor complejidad técnica en comparación con Link 16.
 - o Requiere infraestructuras modernas para un rendimiento óptimo.
- **Ventajas:**
 - o Máxima resistencia a interferencias deliberadas.
 - o Modularidad para integrar nuevas técnicas anti-jamming.
- **Desventajas:**
 - o Implementación más compleja y costosa.
 - o Mayor consumo de recursos en sistemas más antiguos.

COMPARACIÓN RESUMIDA: EVOLUCIÓN ANTI-JAMMING.

La tabla 5-7, más abajo, compara la capacidad de evolución en medidas anti-jamming de Link 11, Link 16 y Link 22.

Aspecto Evolutivo	Link 11	Link 16	Link 22
Nivel de Protección	Muy baja.	Alta.	Muy alta.
Automatización	No.	Parcial.	Sí, avanzada.
Adaptabilidad Cuántica	No.	Limitada.	Preparada.

Tabla 5-7. Comparativa anti-jamming resumida entre Link 11, Link 16 y Link 22.

En la evolución de la protección anti-jamming en los sistemas TDL destaca la transición desde la vulnerabilidad de **Link 11** hasta la sofisticación de **Link 22**. **Link 16** representa un hito importante con su introducción de técnicas FHSS, mientras que **Link 22** eleva la resistencia a un nivel superior mediante mejoras en la gestión del espectro y modularidad. **JREAP** y **VMF**, aunque flexibles, dependen en gran medida del medio físico y la infraestructura, lo que limita su efectividad en entornos hostiles.

Para operaciones en entornos altamente contestados, **Link 22** es la opción más robusta, seguido de **Link 16** con actualizaciones adecuadas. **JREAP** y **VMF** pueden ser útiles en contextos específicos, pero requieren soporte adicional para resistir interferencias deliberadas.

5.7 CAPACITACIÓN Y CONCIENCIACIÓN EN SEGURIDAD.

La **capacitación y concienciación en seguridad en Tactical Data Link** es esencial para garantizar la protección de datos sensibles, la interoperabilidad de sistemas y la seguridad operativa en entornos de comunicaciones críticas. Los Tactical Data Links son sistemas clave en operaciones militares y de defensa, por lo que mantener la seguridad y la eficiencia en su uso, es fundamental.

OBJETIVO DE LA CAPACITACIÓN EN SEGURIDAD PARA TDL.

Asegurar que el personal involucrado en la operación, mantenimiento y supervisión de los sistemas de TDL tenga los conocimientos y habilidades necesarios para proteger la integridad, confidencialidad y disponibilidad de la información transmitida a través de estos enlaces.

COMPONENTES CLAVE DE LA CAPACITACIÓN Y CONCIENCIACIÓN EN SEGURIDAD EN TDL.

FUNDAMENTOS DEL TDL Y SEGURIDAD DE LA INFORMACIÓN.

- **Introducción a TDL:**
 - o Conceptos básicos: qué son los Tactical Data Links y su importancia en el intercambio de datos en tiempo real.
 - o Protocolos comunes: Link 11, Link 16, Link 22, JREAP, entre otros.
- **Principios de seguridad de la información:**
 - o Confidencialidad, integridad y disponibilidad de los datos.
 - o Identificación de amenazas específicas a los sistemas de enlace de datos.

GESTIÓN DE ACCESOS Y AUTENTICACIÓN.

- **Roles y privilegios:**
 - o Definición de roles claros para operadores, supervisores y administradores.

- o Asignación de privilegios mínimos necesarios para cada función.
- **Autenticación y cifrado:**
 - o Uso de certificados digitales y claves de autenticación.
 - o Implementación de sistemas de cifrado robustos para proteger las transmisiones.

PROTECCIÓN CONTRA AMENAZAS CIBERNÉTICAS.

- **Identificación de amenazas:**
 - o Reconocimiento de intentos de interceptación, suplantación o denegación de servicio.
 - o Riesgos asociados al spoofing y al jamming en redes TDL.
- **Mitigación de vulnerabilidades:**
 - o Actualización regular de software y firmware en sistemas de enlace.
 - o Implementación de firewalls y sistemas de detección de intrusiones (IDS).

NORMAS Y PROTOCOLOS DE SEGURIDAD.

- **Cumplimiento normativo:**
 - o Familiarización con estándares internacionales como STANAG (NATO Standardization Agreements) y normas nacionales.
- **Políticas de seguridad organizacional:**
 - o Directrices específicas de la organización para el uso de TDL.

PROCEDIMIENTOS DE RESPUESTA A INCIDENTES.

- **Gestión de incidentes de seguridad:**
 - o Protocolos para identificar, reportar y responder a eventos de seguridad en tiempo real.
 - o Plan de recuperación ante ataques o fallos en los enlaces de datos.
- **Simulacros de seguridad:**
 - o Ejercicios regulares para evaluar la preparación del equipo ante posibles incidentes.

CONCIENCIACIÓN DEL PERSONAL.

- **Impacto de los errores humanos:**
 - o Reconocer cómo los errores en la operación pueden comprometer la seguridad de los TDL.
 - o Desarrollo de una mentalidad de seguridad y atención al detalle.
- **Capacitación continua:**
 - o Programas regulares de formación para actualizar conocimientos frente a nuevas amenazas y tecnologías.

HERRAMIENTAS Y TÉCNICAS DE MONITOREO.

- **Supervisión activa:**
 - o Uso de sistemas de monitoreo para analizar tráfico y detectar anomalías en tiempo real.
- **Auditorías de seguridad:**
 - o Evaluaciones periódicas de los sistemas para identificar y corregir vulnerabilidades.

FOMENTO DE UNA CULTURA DE SEGURIDAD.

- **Integración de la seguridad en operaciones diarias:**
 - o Establecer prácticas estándar para garantizar la seguridad en todas las interacciones con los TDL.
- **Comunicación efectiva:**
 - o Promover la cooperación y el intercambio de información entre equipos operativos y de ciberseguridad.

La implementación de un programa sólido de capacitación y concienciación en seguridad asegura la confiabilidad y efectividad de los Tactical Data Links en misiones críticas.

6 DISCUSIÓN Y ANÁLISIS.

6.1 ANÁLISIS COMPARATIVO DE LOS MÉTODOS DE MITIGACIÓN.

La tabla 6-1, más abajo, compara el costo de empleo de los diferentes métodos de mitigación.

Método	Eficacia	Ventajas	Limitaciones	Costo
Implantación de Relojes atómicos	Alta frente a los ataques de degradación de GPS.	Resiliencia en sincronismo.	Infraestructura adicional.	Moderado a alto
Cifrado de Comunicaciones	Alta	Confidencialidad e integridad de datos.	Latencia y necesidad de actualización.	Moderado a alto
Salto en frecuencias	Alta frente a jamming	Resiliencia ante interferencias.	Requiere sincronización precisa.	Moderado
Autenticación de Nodos	Alta frente a spoofing	Confianza en los emisores.	Infraestructura adicional.	Moderado
RBAC ²⁹	Moderada	Protección por roles.	No aborda jamming o interceptación.	Bajo
IDS	Alta	Detección proactiva de amenazas.	Dependencia de monitoreo continuo.	Moderado
Actualización de Sistemas	Alta	Solución integral y moderna.	Costo elevado y tiempo de implementación.	Alto

Tabla 6-1. Comparativa de métodos de mitigación sobre TDL.

Tras el análisis de los distintos métodos de mitigación de las vulnerabilidades detectadas en TDL se puede **concluir** que es necesaria una combinación de métodos, ya que ninguna solución individual aborda todos los riesgos. En general, la solución de mitigación deberá contener:

- **Implantación de relojes atómicos** para aumentar la resiliencia del TDL ante un más que probable ataque de degradación de GPS
- **Cifrado y Salto en Frecuencia:** son las herramientas más efectivas para proteger la confidencialidad y la disponibilidad de los datos.
- **Autenticación de Nodos e IPS:** son esenciales para detectar y prevenir ataques de spoofing y otras intrusiones.
- **Actualización de Hardware y Software:** es ideal para organizaciones que buscan una solución a largo plazo, aunque puede ser costosa.
- **RBAC** es un método complementario que mejora la seguridad operacional al limitar el acceso a funciones específicas.

La elección de los métodos dependerá del presupuesto, la infraestructura existente y los requisitos operativos. Una solución híbrida que combine estas estrategias suele ser la más efectiva para proteger la red TDL.

²⁹ RBAC: Role Based Access Control. Control de Acceso basado en roles.

6.2 LIMITACIONES DE LAS SOLUCIONES ACTUALES.

LIMITACIONES DE LA SOLUCIÓN LINK 16.

Link 16 es un estándar ampliamente utilizado en las redes tácticas de comunicación de las fuerzas armadas, diseñado para proporcionar intercambio seguro y en tiempo real de datos entre plataformas terrestres, aéreas y marítimas.

A pesar de sus capacidades avanzadas, Link 16 presenta ciertas limitaciones que pueden impactar su desempeño y aplicabilidad en ciertos entornos operativos:

- **Ancho de Banda Limitado:** Link 16 opera dentro de un espectro de frecuencia limitado y está diseñado principalmente para transmitir datos críticos y mensajes tácticos.
- **Impacto:**
 - o Restricción en la cantidad y el tamaño de los datos que se pueden transmitir simultáneamente.
 - o En escenarios con múltiples usuarios activos, puede generarse congestión en la red.
- **Mitigación:** Priorización de datos críticos y uso de sistemas complementarios para transmisión de grandes volúmenes de datos.
- **Alta Emisión Electromagnética:** Las transmisiones de Link 16 generan una firma electromagnética significativa, lo que puede delatar la ubicación de los nodos.
 - **Impacto:** Mayor vulnerabilidad a la detección y localización por parte de adversarios equipados con tecnología avanzada de guerra electrónica.
 - **Mitigación:** Uso de modos de transmisión con menor potencia y técnicas de salto de frecuencia para minimizar el riesgo de detección.
- **Vulnerabilidad a Interferencias (Jamming):** Aunque incorpora técnicas de salto de frecuencia, los adversarios sofisticados pueden emplear contramedidas de guerra electrónica para interferir en las comunicaciones.
 - **Impacto:** Pérdida temporal de conectividad en entornos altamente disputados.
 - **Mitigación:** Uso de sistemas complementarios con mayor resistencia al jamming o integración con redes redundantes.
- **Capacidad de Red Limitada:** Link 16 tiene un límite en la cantidad de usuarios que pueden estar activos en la red simultáneamente, debido a las restricciones del protocolo TDMA (Time Division Multiple Access).
 - **Impacto:** En operaciones conjuntas con muchos participantes, puede resultar insuficiente para coordinar eficazmente todas las plataformas.
 - **Mitigación:** Segmentación de la red y asignación de ranuras TDMA en función de las prioridades operativas.
- **Latencia en Escenarios Complejos:** En escenarios con una alta densidad de nodos y mensajes, el protocolo TDMA puede introducir latencia en la transmisión de datos.
 - **Impacto:** Puede afectar la sincronización de las operaciones, especialmente en entornos de combate rápido.

- **Mitigación:** Configuración óptima del plan de red y asignación eficiente de tiempos de transmisión.
- **Dependencia de Línea de Vista:** Link 16 opera principalmente en el rango de frecuencias UHF, lo que limita la propagación de señales a líneas de vista directa.
 - **Impacto:** Las comunicaciones pueden verse interrumpidas en terrenos montañosos, áreas urbanas o en condiciones adversas.
 - **Mitigación:** Uso de nodos de retransmisión o integración con redes satelitales.
- **Complejidad de Configuración y Mantenimiento:** La configuración de una red Link 16 requiere experiencia técnica avanzada y planificación detallada para asegurar la interoperabilidad y funcionalidad.
 - **Impacto:** Riesgo de errores en la configuración inicial que pueden afectar el desempeño de la red.
 - **Mitigación:** Capacitación continua y simulaciones previas para probar configuraciones.
- **Costes de Implementación y Operación:** Los equipos Link 16, incluidos terminales y sistemas de soporte, tienen un costo elevado, lo que puede limitar su adopción en fuerzas armadas con presupuestos restringidos.
 - **Impacto:**
 - o Puede no ser una solución viable para todas las plataformas o países.
 - **Mitigación:**
 - o Colaboración internacional para compartir costes y aprovechar economías de escala.
- **Riesgo de Interoperabilidad Limitada:** Aunque diseñado para interoperar entre diferentes ramas y naciones, los problemas de interoperabilidad pueden surgir debido a configuraciones específicas, versiones de software o estándares locales.
 - **Impacto:**
 - o Dificultad para coordinar operaciones conjuntas.
 - **Mitigación:**
 - o Adopción de estándares comunes y pruebas regulares de interoperabilidad.
- **Riesgo de Obsolescencia Tecnológica:** Link 16 fue desarrollado en la década de 1970 y, aunque se han realizado actualizaciones, algunos de sus aspectos fundamentales pueden quedar obsoletos frente a tecnologías más modernas.
 - **Impacto:** Podría no cumplir con los requisitos de las operaciones futuras sin actualizaciones significativas.
 - **Mitigación:** Inversiones continuas en investigación y desarrollo para mantener la relevancia del sistema.

Conclusión: Link 16 es una solución robusta para las comunicaciones tácticas, pero sus limitaciones deben tenerse en cuenta al planificar operaciones. Para superar estos desafíos, es esencial adoptar estrategias de mitigación como el uso de sistemas complementarios, capacitación continua y actualizaciones tecnológicas regulares. Una planificación adecuada garantizará que Link 16 siga siendo una herramienta efectiva en el entorno operativo moderno.

LIMITACIONES DE LA SOLUCIÓN LINK 22.

Link 22 es una mejora sobre su predecesor, Link 11, diseñada para proporcionar comunicaciones tácticas más seguras, resilientes y eficientes entre las fuerzas armadas. Sin embargo, como cualquier sistema, tiene limitaciones inherentes que pueden afectar su desempeño, implementación y adaptabilidad en ciertos escenarios. A continuación, se detallan las principales limitaciones:

1. Complejidad de Implementación. La configuración inicial de Link 22 requiere una planificación exhaustiva, recursos especializados y capacitación del personal.

- **Impacto:**
 - o Alta curva de aprendizaje para operadores y administradores.
 - o Dificultad para integrar Link 22 en sistemas de comando y control existentes, especialmente en plataformas más antiguas.
- **Mitigación:** Implementación escalonada y simulaciones previas para entrenar al personal.

2. Dependencia de Infraestructura y Hardware. Requiere hardware y software específicos que deben ser interoperables entre todas las plataformas participantes.

- **Impacto:**
 - o La interoperabilidad puede verse afectada si los nodos utilizan hardware obsoleto o no compatible.
 - o Las actualizaciones de hardware pueden ser costosas y lentas.
- **Mitigación:** Estandarización de equipos y planificación presupuestaria para actualizaciones regulares.

3. Vulnerabilidades a Interferencia y Jamming. Aunque Link 22 mejora la resistencia frente a interferencias en comparación con Link 11, no es completamente inmune a ataques de jamming sofisticados.

- **Impacto:** Puede haber pérdida temporal de conectividad en entornos hostiles con adversarios avanzados.
- **Mitigación:** Uso de técnicas como el salto de frecuencia (FHSS) y antenas direccionables.

4. Requisitos de Ancho de Banda. Link 22 requiere un mayor ancho de banda para transmitir datos en comparación con sistemas más antiguos.

- **Impacto:** En entornos con restricciones de espectro o congestión, el desempeño puede degradarse significativamente.
- **Mitigación:** Priorización de tráfico y compresión de datos cuando sea posible.

5. Riesgo de Obsolescencia. Aunque Link 22 es una tecnología avanzada, está diseñada sobre estándares actuales que podrían quedar obsoletos frente a avances futuros en tecnología y ciberseguridad.

- **Impacto:** Exposición a ataques más sofisticados (zero-day) si no se actualiza continuamente.
- **Mitigación:** Adopción de un programa de mantenimiento proactivo y alineación con estándares emergentes.

6. Costes de Implementación y Mantenimiento. Los costes asociados a la implementación y mantenimiento de Link 22 pueden ser elevados, especialmente para fuerzas armadas de menor capacidad presupuestaria.

- **Impacto:** Limitaciones en su adopción por parte de países o unidades con recursos limitados.
- **Mitigación:** Colaboración multinacional para compartir costes y recursos de desarrollo.

7. Resiliencia a Ciberataques. Aunque incluye medidas avanzadas de seguridad, no es invulnerable a ciberataques sofisticados, como suplantación de nodos o explotación de vulnerabilidades de software.

- **Impacto:** Posibles fugas de información crítica o alteraciones en la operatividad.
- **Mitigación:**
 - o Monitoreo continuo de la red (IDS/IPS).
 - o Autenticación robusta y segmentación de la red.

8. Latencia en Comunicaciones de Largo Alcance. Aunque optimizado para comunicaciones rápidas, pueden surgir problemas de latencia en escenarios de despliegue global con enlaces satelitales.

- **Impacto:** Afecta la sincronización de las operaciones en tiempo real.
- **Mitigación:** Integración de técnicas de preprocesamiento de datos para reducir la carga.

Conclusión: Las limitaciones de Link 22 pueden mitigarse con una combinación de planificación adecuada, inversión en infraestructura y adopción de tecnologías complementarias. Sin embargo, es fundamental que las fuerzas armadas consideren estas limitaciones en su estrategia operativa para maximizar la efectividad y la resiliencia del sistema. Una vigilancia continua de las necesidades y amenazas emergentes es crucial para mantener la relevancia de Link 22 en el futuro.

6.3 FUTURO DE LA SEGURIDAD EN LOS TDL.

Los Tactical Data Links, fundamentalmente Link 16 y Link 22, son sistemas esenciales para garantizar la interoperabilidad y el intercambio de información en tiempo real entre fuerzas armadas en diversos dominios: terrestre, marítimo, aéreo y espacial. Sin embargo, a medida que las amenazas evolucionan, también lo deben hacer las medidas de seguridad. El futuro de la seguridad en los TDL se centra en la implementación de tecnologías avanzadas, enfoques proactivos y la adaptación a escenarios operativos cada vez más complejos.

Las **tendencias futuras** en seguridad para los TDL son:

- 1. Implementación de Cifrado Cuántico:** El cifrado cuántico utiliza principios de la mecánica cuántica para crear claves inquebrantables, protegiendo la información frente a los ataques de computadoras cuánticas. **Impacto Futuro:** Asegura comunicaciones ultra-seguras contra adversarios con capacidades tecnológicas avanzadas y reduce el riesgo de interceptación y decodificación de mensajes. **Desafíos:** Implementación costosa y necesidad de infraestructura compatible.
- 2. Inteligencia Artificial (IA) para la Detección de Amenazas:** Los sistemas de IA y aprendizaje automático pueden analizar patrones de tráfico en los TDL para identificar y responder a actividades sospechosas en tiempo real. **Impacto Futuro:** Mitigación proactiva de amenazas como jamming, spoofing y ciberataques y mejora en la capacidad de respuesta frente a ataques emergentes. **Desafíos:** Dependencia de grandes volúmenes de datos para entrenar modelos y evitar falsos positivos.
- 3. Redes Definidas por Software (SDN):** Las SDN permiten una gestión más flexible y dinámica de las redes TDL, adaptando rutas y configuraciones en función de las amenazas detectadas. **Impacto Futuro:** Mayor resiliencia frente a ataques de denegación de servicio (DoS) y capacidad de segmentar la red para contener brechas de seguridad. **Desafíos:** Vulnerabilidades en los controladores centrales y la necesidad de altos niveles de redundancia.

4. **Autenticación Basada en Biometría y Multifactor:** Uso de autenticación biométrica (huellas dactilares, reconocimiento facial) y multifactor para asegurar el acceso a los nodos de los TDL. **Impacto Futuro:** Reducción de riesgos de acceso no autorizado y mejora de la trazabilidad de los usuarios en la red. **Desafíos:** Posibles problemas de privacidad y costes asociados a la implementación.
5. **Integración con Blockchain:** El blockchain puede asegurar la integridad y autenticidad de los datos transmitidos en los TDL mediante un registro descentralizado e inmutable. **Impacto Futuro:** Garantiza que los datos no sean manipulados durante su transmisión y mejora la confianza en la procedencia de la información. **Desafíos:** Latencia en la transmisión y escalabilidad en redes de gran tamaño.
6. **Redes Autónomas y Auto-Reparables:** Sistemas que detectan fallos o ataques y reconfiguran automáticamente las comunicaciones para evitar interrupciones. **Impacto Futuro:** Resiliencia frente a interferencias y ataques cibernéticos y mayor disponibilidad operativa incluso en entornos altamente disputados. **Desafíos:** Complejidad en el desarrollo y validación de algoritmos autónomos.
7. **Comunicación Basada en Espectro Dinámico:** Uso de tecnologías de espectro cognitivo que permiten a los TDL identificar y operar en frecuencias menos congestionadas o interferidas. **Impacto Futuro:** Reducción del impacto de los ataques de jamming y mayor flexibilidad operativa en entornos saturados. **Desafíos:** Requiere hardware avanzado y coordinación en tiempo real entre los nodos.
8. **Seguridad Zero Trust:** Modelo de seguridad que asume que ningún usuario o dispositivo es confiable por defecto, implementando verificaciones constantes. **Impacto Futuro:** Protección contra amenazas internas y accesos no autorizados y mejora en la segmentación y monitoreo de la red. **Desafíos:** Requiere cambios significativos en la arquitectura de los TDL existentes.

Los **Desafíos Claves** en el Futuro son:

- **Amenazas Cuánticas:** Las computadoras cuánticas tienen el potencial de romper los sistemas de cifrado actuales. Se requerirá un cambio hacia criptografía post-cuántica para contrarrestar este riesgo.
- **Escalabilidad:** A medida que los TDL se amplían para incluir más nodos, sensores y dispositivos IoT, garantizar la seguridad sin sacrificar el rendimiento será un desafío.
- **Interoperabilidad Multinacional:** Las operaciones conjuntas entre diferentes fuerzas armadas exigen estándares comunes de seguridad, pero las discrepancias en tecnologías y presupuestos dificultan la implementación uniforme.
- **Costes y Presupuestos:** La implementación de tecnologías avanzadas como IA, blockchain y redes cuánticas puede ser prohibitiva para algunas naciones.
- **Adversarios Sofisticados:** Los estados adversarios y actores no estatales están adoptando tecnologías avanzadas, aumentando la sofisticación de los ataques.

El futuro de la seguridad en los Tactical Data Links estará definido por la adopción de tecnologías avanzadas, la cooperación internacional y la evolución hacia sistemas más resilientes y autónomos. La clave será mantener un enfoque proactivo, con inversiones constantes en investigación y desarrollo para anticipar y contrarrestar amenazas emergentes. Un enfoque integral que combine tecnología, capacitación y colaboración asegurará que los TDL sigan siendo una herramienta crucial en las operaciones militares del siglo XXI.

7 CONCLUSIONES.

7.1 RESUMEN DE HALLAZGOS PRINCIPALES.

Los Tactical Data Links son sistemas esenciales para las operaciones militares modernas, pero también son objetivos críticos para los adversarios debido a su papel en la coordinación y el intercambio de información táctica. Estas redes enfrentan diversas vulnerabilidades que, si no se abordan, pueden comprometer seriamente la eficacia operativa. A continuación, se describen las vulnerabilidades clave, sus efectos potenciales y las estrategias más efectivas para mitigarlas.

VULNERABILIDADES CLAVE.

1. PÉRDIDA DE SINCRONISMO.

La sincronización en los TDL implica mantener un marco temporal común entre todos los nodos de la red para garantizar que las transmisiones de datos se produzcan en los intervalos de tiempo asignados.

- **Efectos:**
 - o **Colisiones de Datos:** Los nodos pueden transmitir en el mismo intervalo de tiempo, causando pérdida de mensajes.
 - o **Pérdida de Mensajes Críticos:** Los datos enviados fuera de las ranuras asignadas pueden ser ignorados por otros nodos.
 - o **Interrupción de la Red:** La pérdida de sincronización en un nodo puede propagarse a otros, afectando la operación general de la red.
 - o **Reducción de la Eficiencia:** Aumento en la latencia y la disminución de la tasa efectiva de transmisión de datos.
 - o **Impacto en la Toma de Decisiones:** Datos tácticos desactualizados o ausentes pueden llevar a errores operativos.
- **Estrategias de Mitigación:**
 - o **Fuentes de Sincronización Redundantes:** Integrar fuentes secundarias de sincronización, como relojes atómicos internos o referencias terrestres.
 - **Beneficios:** Reduce la dependencia exclusiva del GPS y minimiza los riesgos de desincronización.
 - o **Técnicas de Resiliencia al Jamming:** Implementar algoritmos de salto de frecuencia (FHSS) y espectro ensanchado para resistir interferencias.
 - **Beneficios:** Asegura la estabilidad de las señales de sincronización en entornos disputados.
 - o **Algoritmos de Sincronización Distribuida:** Permitir que los nodos en la red compartan información de tiempo entre sí para corregir desajustes.
 - **Beneficios:** Crea un sistema de sincronización más robusto que no depende de un único nodo o fuente.
 - o **Monitoreo en Tiempo Real:** Usar sistemas avanzados para detectar y corregir desviaciones de sincronización de manera proactiva.
 - **Beneficios:** Permite identificar problemas antes de que afecten el rendimiento de la red.
 - o **Actualizaciones de Hardware y Software:** Mantener los relojes internos y los sistemas de sincronización al día con las últimas tecnologías.
 - **Beneficios:** Mejora la precisión y confiabilidad del sistema.

- o **Uso de Inteligencia Artificial y Aprendizaje Automático:** Emplear IA para predecir y corregir posibles fallos de sincronización en base a patrones de comportamiento de la red.
 - **Beneficios:** Aumenta la capacidad de respuesta ante cambios dinámicos en la red.
- o **Capacitación Operativa:** Entrenar a los operadores en la identificación de señales de desincronización y la aplicación de procedimientos correctivos.
 - **Beneficios:** Mejora la capacidad de respuesta humana en situaciones críticas.

INTERFERENCIA Y JAMMING.

Los TDL operan en espectros de frecuencia que pueden ser saturados o bloqueados por señales maliciosas diseñadas para interrumpir las comunicaciones.

- **Efectos:**
 - o Pérdida de conectividad entre nodos.
 - o Retrasos en la transmisión de datos críticos, lo que afecta la toma de decisiones.
- **Estrategias de Mitigación:**
 - o Uso de salto de frecuencia (FHSS) para cambiar dinámicamente las mismas.
 - o Incremento en la potencia de transmisión o uso de antenas direccionales.
 - o Implementación de sistemas de espectro cognitivo para evitar frecuencias interferidas.

SPOOFING.

Un adversario suplanta nodos legítimos en la red para transmitir información falsa o confundir a los operadores.

- **Efectos:**
 - o Decisiones operativas erróneas basadas en datos falsificados.
 - o Pérdida de confianza en la integridad de la red.
- **Estrategias de Mitigación:**
 - o Implementación de autenticación robusta, como certificados digitales y claves dinámicas.
 - o Uso de técnicas de detección de anomalías mediante inteligencia artificial.
 - o Encriptación fuerte en el intercambio de mensajes.

ATAQUES DE DENEGACIÓN DE SERVICIO (DOS).

Los adversarios inundan la red con tráfico falso para saturar los recursos y evitar el intercambio de datos legítimos.

- **Efectos:**
 - o Red congestionada, lo que afecta la coordinación táctica.
 - o Inhabilitación temporal de nodos clave en la red.
- **Estrategias de Mitigación:**
 - o Segmentación de la red para contener el impacto de un ataque.
 - o Filtrado avanzado de paquetes para bloquear tráfico no autorizado.
 - o Implementación de medidas de redundancia en los nodos.

VULNERABILIDADES DE CIBERSEGURIDAD.

Brechas en el software o hardware que permiten accesos no autorizados, malware o robo de información crítica.

- **Efectos:**
 - o Fugas de información confidencial.
 - o Control por parte del adversario de sistemas críticos.
- **Estrategias de Mitigación:**
 - o Aplicación de actualizaciones y parches regulares en el software de los TDL.
 - o Monitoreo constante de la red mediante sistemas de detección y prevención de intrusiones (IDS/IPS).
 - o Uso de arquitecturas de seguridad "Zero Trust".

DEPENDENCIA DE LÍNEAS DE VISTA.

Los TDL como Link 16 operan principalmente bajo la limitación de comunicación directa en línea de vista, lo que los hace vulnerables en terrenos irregulares o entornos urbanos.

- **Efectos:**
 - o Pérdida de comunicación en áreas con obstrucciones físicas.
 - o Limitación en el alcance operativo de la red.
- **Estrategias de Mitigación:**
 - o Uso de plataformas de retransmisión como UAVs o satélites.
 - o Integración con redes híbridas que utilicen enlaces satelitales y terrestres.

LATENCIA EN ESCENARIOS COMPLEJOS.

La alta densidad de nodos y tráfico en la red puede introducir demoras en la transmisión de datos.

- **Efectos:**
 - o Información desactualizada que afecta la sincronización de operaciones.
- **Estrategias de Mitigación:**
 - o Optimización del protocolo TDMA para asignar ranuras basadas en prioridades.
 - o Priorización de mensajes críticos sobre datos secundarios.

FALLOS POR INTEROPERABILIDAD.

Diferencias en configuraciones o versiones de software pueden dificultar la interoperabilidad entre fuerzas conjuntas.

- **Efectos:**
 - o Inhabilidad de coordinar operaciones multinacionales o interramas.
- **Estrategias de Mitigación:**
 - o Adopción de estándares comunes y pruebas regulares de interoperabilidad.
 - o Uso de gateways para traducir formatos y protocolos entre diferentes sistemas.

7.2 IMPLICACIONES DE LOS RESULTADOS.

EFFECTOS COMBINADOS DE LAS VULNERABILIDADES.

1. **Degradación Operacional:** La incapacidad de transmitir información crítica afecta la capacidad de coordinar operaciones tácticas, comprometiendo la efectividad de la misión.
2. **Exposición a Riesgos Estratégicos:** La pérdida de datos sensibles o la interferencia en las comunicaciones puede dar a los adversarios una ventaja táctica o estratégica.
3. **Pérdida de Confianza:** Las vulnerabilidades no mitigadas pueden reducir la confianza de los usuarios en el sistema, limitando su adopción en escenarios críticos.

ESTRATEGIAS GENERALES DE MITIGACIÓN.

1. Diseño Resiliente.

- Incorporar redundancia y sistemas autónomos para asegurar la continuidad operativa ante ataques o fallos.
- Uso de arquitecturas de red flexibles como Redes Definidas por Software (SDN).

2. Cifrado Avanzado.

- Implementar algoritmos de criptografía post-cuántica para proteger datos frente a futuros avances en tecnología cuántica.

3. Capacitación y Simulaciones.

- Entrenar al personal en la identificación y manejo de ciberamenazas específicas de los TDL.
- Realizar simulaciones regulares para evaluar la capacidad de respuesta ante ataques.

4. Monitoreo y Actualización Continua.

- Integrar sistemas de monitoreo en tiempo real para identificar anomalías en la red.
- Mantener un programa activo de actualización de hardware y software.

5. Cooperación Multinacional.

- Establecer foros y acuerdos para compartir conocimientos y estándares de seguridad entre aliados.

7.3 RECOMENDACIONES FINALES.

Los Tactical Data Links son una herramienta crucial en las operaciones militares modernas, pero enfrentan amenazas sofisticadas que evolucionan constantemente. La clave para garantizar su seguridad reside en adoptar tecnologías avanzadas, mantener una vigilancia proactiva y promover la interoperabilidad global. Una estrategia integral que combine medidas técnicas, operativas y de capacitación garantizará la resiliencia de los TDL frente a las amenazas presentes y futuras.

8 REFERENCIAS.

- [1] N. Grumman, Link 22 Guidebook, Naval Information Warfare Systems Command, 2022, p. 784.
- [2] N. Grumman, Understanding Link 16., San Diego, California, USA, 2004, p. 320.
- [3] T. d. G. OESIA, «Grupo OESIA.COM,» Tecnobit del Grupo OESIA, [En línea]. Available: https://grupooesia.com/wp-content/uploads/VLAD_comunicaciones_tacticas_tecnobit_eng.pdf. [Último acceso: 22 enero 2025].
- [4] INCIBE, «Instituto Nacional de Ciberseguridad,» 21 enero 2025. [En línea]. Available: <https://www.incibe.es/>.
- [5] «European Defence Cooperation: PESCO Projects,» 2023. [En línea]. Available: <https://pesco.europa.eu>. [Último acceso: 11 enero 2025].
- [6] E. Consortium, «ESSOR Consortium. (2022). ESSOR HDR Base Waveform Technical Specifications.,» 2022. [En línea]. Available: <https://www.occar.int/>. [Último acceso: 11 enero 2025].
- [7] T. Group, «Thales Group. Thales and ESSOR: Advancing Secure Communications.,» 2023. [En línea]. Available: <https://www.thalesgroup.com>. [Último acceso: 11 01 2025].
- [8] L3Harris, «l3harris.com,» 11 01 2025. [En línea]. Available: <https://www.l3harris.com/all-capabilities/mids-lvt-terminals>.
- [9] Leonardo, «Leonardo. (2023). Leonardo's Role in the ESSOR Project.,» 2023. [En línea]. Available: <https://www.leonardocompany.com>. [Último acceso: 11 enero 2025].
- [10] OCCAR, «ESSOR SDR,» 11 01 2025. [En línea]. Available: <https://www.occar.int/our-work/programmes/essor-european-secure-software-defined-radio>.
- [11] N. G. M. Systems., «Todos los capítulos,» de *Understanding Link 16.* , septiembre de 2004, p. 754.