Taller de Tercer Corte

Comunicaciones Industriales con IA y Computación Cuántica

David Stiven Quinchanegua Cely
Luis Felipe Garzón Camacho

Presentado al Profesor: Diego Alejandro Barragán Vargas
Universidad Santo Tomás – Facultad de Ingeniería Electrónica
Octubre 2025

1. Algoritmos de IA para Redes Industriales

1.1. Detección de Errores con Machine Learning

Algoritmos principales:

- **Support Vector Machines (SVM):** Clasificación binaria normal/falla. Precisión: 96.1 % [1]
- **Isolation Forest:** Detección de anomalías sin supervisión. Tiempo: $<$ 50ms [2]
- **Autoencoders (DNN):** Aprenden patrones normales, detectan desviaciones [3]
- **LSTM Networks:** Predicción de fallas en series temporales [4]

Arquitectura implementada:

Sensores IoT (PLCs, SCADA, Temperatura)
↓
Preprocesamiento (Normalización, Filtrado)
↓
Módulo IA (SVM + Isolation Forest + LSTM)
↓
Sistema de Alertas (Dashboard, Notificaciones)

Métricas de desempeño: Precisión 95-98 %, latencia $<$ 100ms, falsos positivos $<$ 2 % [2,3].

1.2. IA en Firewalls y Routers

Algoritmos heurísticos aplicados:

- **QAOA (Quantum Approximate Optimization):** Optimización de reglas de firewall, reducción de redundancias
- **Genetic Algorithms (GA):** Enrutamiento dinámico, balanceo de carga adaptativo
- **Particle Swarm Optimization (PSO):** Asignación óptima de recursos de red [5]

Implementación práctica: Check Point ThreatCloud AI logra 99.9 % de bloqueo de amenazas con ML integrado [6]. Cisco DNA Center utiliza ML para predicción proactiva de problemas de red, reduciendo tiempo de resolución en 70 % [7].

1.3. IoT Industrial y Ethernet

Protocolos industriales: EtherNet/IP, Modbus/TCP, PROFINET, OPC UA, MQTT.

Simbiosis IoT-Ethernet-IA:

La convergencia de IoT industrial con Ethernet permite comunicación determinística de bajo retardo (< 1ms) esencial para control en tiempo real. La IA se integra en tres capas:

1. **Edge AI:** TinyML en dispositivos IoT para decisiones locales instantáneas
2. **Fog Computing:** Procesamiento intermedio con latencia < 10ms
3. **Cloud AI:** Análisis avanzado, entrenamiento de modelos, gemelos digitales

Beneficios medidos: Reducción de ancho de banda 60 % (compresión IA), detección de anomalías comportamentales con 97.5 % precisión [8].

2. Computación Cuántica en Comunicaciones

2.1. Estado Actual y Aplicaciones

¿Se visualiza en comunicaciones industriales? SÍ, con horizonte de adopción 5-10 años [9].

Aplicaciones potenciales:

- **QKD (Quantum Key Distribution):** Distribución de claves criptográficas cuánticamente seguras. Distancia actual: 400 km en fibra. Empresas: ID Quantique, Toshiba [10]
- **Optimización cuántica:** Algoritmos QAOA para enrutamiento NP-hard, scheduling de red, asignación de recursos. Ventaja: reducción de latencia 30 % vs. clásico [11]
- **Quantum Sensing:** Sincronización ultra-precisa (< 1 picosegundo), medición de latencia 100x-1000x más precisa [12]

2.2. Integración con 6G

Las tecnologías cuánticas se integrarán en redes 6G (2030+) proporcionando:

- Latencia < 0.1ms (10x mejor que 5G)
- Velocidad hasta 1 Tbps
- Seguridad post-cuántica nativa (QKD + PQC)
- Densidad: 10^7 dispositivos/km^2 [13]

Timeline de adopción:

Período	Tecnología	TRL
2025-2027	QKD Comercial	7-8
2028-2030	Quantum Repeaters	4-5
2030-2035	Quantum Internet	3-4
2035-2040	6G Cuántico	2-3

Inversión global 2023: \$6.7B. Proyección 2040: \$173B. EU invierte \$1.1B, China \$11B, US \$5.1M en infraestructura cuántica [14].

3. Propuesta MinCiencias: SAQCIS

3.1. Información General

Título: Sistema Inteligente de Monitoreo y Seguridad para Redes Industriales IoT con IA y Criptografía Post-Cuántica (SAQCIS)

Duración: 24 meses **Presupuesto:** $450,000,000 COP

3.2. Problema

Las redes industriales colombianas enfrentan: (1) 78 % sufrieron ciberataques en 2024, (2) detección tardía de fallas (4-6 horas promedio), (3) protocolos sin cifrado nativo, (4) amenazas cuánticas futuras comprometiendo RSA/AES.

3.3. Solución Propuesta

Sistema híbrido con 4 módulos integrados:

Módulo 1 - IA Detección: Isolation Forest + Autoencoder + One-Class SVM. Meta: precisión $>$ 95 %, latencia $<$ 100ms.

Módulo 2 - Predicción ML: LSTM + Random Forest para predicción de fallas. Output: probabilidad de falla, tiempo hasta falla (RUL), recomendaciones.

Módulo 3 - Seguridad Post-Cuántica: Implementación de CRYSTALS-Kyber (KEM) y CRYSTALS-Dilithium (firma digital), aprobados por NIST [15]. Preparación para integrar QKD futuro.

Módulo 4 - Optimización Heurística: Genetic Algorithm + PSO + Simulated Annealing para enrutamiento óptimo, balanceo de carga, configuración de firewalls.

3.4. Objetivos

General: Desarrollar sistema inteligente que mejore disponibilidad, seguridad y eficiencia de plantas industriales colombianas mediante IA y criptografía post-cuántica.

Específicos:

1. Implementar algoritmos IA para detección de anomalías en protocolos industriales con precisión $>$ 95 %
2. Desarrollar módulo de seguridad PQC reduciendo vulnerabilidades 80 %
3. Crear algoritmos de optimización reduciendo latencia 30 % y mejorando throughput 25 %
4. Validar prototipo en planta piloto colombiana durante 6 meses
5. Capacitar 50 profesionales y publicar 3 artículos indexados

3.5. Metodología

Fase 1 (M1-6): Investigación, diseño de arquitectura, selección de algoritmos.

Fase 2 (M7-14): Desarrollo de módulos, integración con protocolos, pruebas.

Fase 3 (M15-20): Validación en planta piloto, monitoreo 6 meses, ajustes.

Fase 4 (M21-24): Transferencia, capacitaciones, publicaciones, escalamiento.

3.6. Resultados Esperados

Métrica	Actual	Meta	Impacto
Detección fallas	4-6h	$<$ 10min	-95 %
Falsos positivos	15-20 %	$<$ 2 %	-90 %
Disponibilidad	95 %	$>$ 99.5 %	+4.5 %
Vulnerabilidades	25-30	$<$ 5	-83 %
Latencia	50ms	35ms	-30 %

Productos: 3 artículos Q1/Q2, 2 patentes, prototipo TRL 7, 2 tesis maestría.

4. Cuadrante Mágico de Gartner

4.1. Estructura del Magic Quadrant

El Magic Quadrant de Gartner posiciona proveedores tecnológicos en dos ejes: **Capacidad de Ejecución** (horizontal) y **Completitud de Visión** (vertical), generando 4 cuadrantes [16,17,18].

4.2. Los Cuatro Cuadrantes

1. LEADERS (Líderes):

Características: Alta ejecución + visión completa. Productos maduros, gran base de clientes, innovación continua, soporte global.

Impacto: Opción más segura para implementaciones críticas. Definen estándares. Mayor costo pero menor riesgo.

Ejemplos 2025:

- **Fortinet** (Hybrid Mesh Firewall): ASICs personalizados, FortiOS único, líder en 12 Magic Quadrants [16]
- **Check Point**: ThreatCloud AI, 99.9 % block rate, plataforma abierta [16]
- **Palo Alto Networks**: Único líder simultáneo en SSE, SASE y SD-WAN [17,18]

2. CHALLENGERS (Retadores):

Características: Alta ejecución + visión limitada. Productos sólidos, gran base de clientes, pero menos innovadores.

Impacto: Excelente para necesidades actuales. Pueden dominar nichos regionales/verticales. Riesgo medio-bajo.

Perfil típico: Empresas establecidas que perfeccionan lo existente. Fuertes en un segmento (ej: on-premise) pero débiles en otros (cloud).

3. VISIONARIES (Visionarios):

Características: Ejecución media + visión innovadora. Tecnologías disruptivas, alta innovación, menor escala.

Impacto: Ideal para ventaja competitiva temprana. Alto riesgo/alto retorno. Futuros líderes potenciales.

Ejemplo: Cloudflare (SSE 2025): Edge-native global, innovación rápida (cientos de features anuales), aún escalando [17].

4. NICHE PLAYERS (Jugadores de Nicho):

Características: Ejecución y visión limitadas. Especialización profunda en segmentos específicos.

Impacto: Mejor para necesidades muy específicas. Excelente costo-beneficio en su nicho. No para estrategias enterprise amplias.

4.3. Análisis por Categoría

Hybrid Mesh Firewall 2025 [16]:

Evalúa protección de redes híbridas (on-prem + cloud + edge), gestión unificada, performance. Tendencias: convergencia networking-security, IA para threat prevention, Zero Trust, preparación post-cuántica.

Impacto industrial: Comunicaciones OT/IT seguras, protección PLCs/SCADA, segmentación inteligente.

Security Service Edge (SSE) 2025 [17]:

Evalúa Secure Web Gateway, CASB, ZTNA, DLP. Palo Alto Networks lidera 3 años consecutivos. Tendencias: SASE, work-from-anywhere, cloud-native, AI-driven detection.

Impacto industrial: Acceso remoto seguro a sistemas industriales, protección aplicaciones cloud, control granular.

SD-WAN 2024 [18]:

Evalúa gestión inteligente WAN, optimización tráfico, integración security. Líderes: Palo Alto (Prisma), Fortinet, Cisco. Tendencias: AI-driven path selection, integración 5G, edge computing, SASE convergence.

Impacto industrial: Conectividad optimizada entre plantas, priorización tráfico crítico (SCADA), reducción costos WAN.

4.4. Guía de Uso

Para toma de decisiones:

1. Identificar necesidades y criticidad
2. Seleccionar cuadrante: Leaders (crítico), Visionaries (innovación), Niche (específico)
3. Evaluar vendors: leer informe completo, revisar limitaciones
4. Hacer POC con top 2-3, validar en ambiente real

4.5. Tendencias Futuras

2025-2027: AI-Native Security, Zero Trust masivo, SASE consolidation, PQC readiness.

2027-2030: Quantum-Safe Networks, Autonomous Security, 6G integration, Digital Twin Security.

2030+: Quantum Internet comercial, AGI-Powered NOC, comunicaciones holográficas.

5. Conclusiones

Este taller investigativo demuestra que la convergencia de IA, computación cuántica y comunicaciones industriales está transformando el sector:

1. IA es realidad actual: Algoritmos como Isolation Forest, SVM y LSTM logran 95-98 % precisión en detección de anomalías con latencias < 100ms, listos para implementación industrial.

2. Computación cuántica es futuro cercano: QKD está en TRL 7-8 (2025-2027), mientras que quantum internet llegará 2030-2035. La industria debe prepararse con criptografía post-cuántica *ahora*.

3. SAQCIS es factible: La propuesta integra tecnologías maduras (IA) con preparación futura (PQC), abordando necesidades reales del sector colombiano con impactos medibles (-95 % tiempo detección, +4.5 % disponibilidad).

4. Gartner orienta selección: El Magic Quadrant permite decisiones informadas: Leaders (Fortinet, Check Point, Palo Alto) para proyectos críticos, Visionaries para innovación controlada.

5. Integración es clave: El éxito requiere simbiosis IoT-Ethernet-IA en arquitecturas multi-capa (edge-fog-cloud) con protocolos industriales estándar (Modbus/TCP, PROFINET, OPC UA).

Referencias (Selección)

1. Chang, C-W. et al. (2021). "Machine Learning Based Network Status Detection". *ResearchGate*. DOI: 10.13140/RG.2.2.35302.95129
2. Nile Secure (2024). .Anomaly Detection Using AI & ML". nilesecure.com
3. Scientific Reports (2025). "Deep learning for industrial machinery health". *Nature*. DOI: 10.1038/s41598-024-79151-2
4. PMC (2022). Ïndustrial network behavioral anomaly detection". PMC8935250
5. Ericsson (2019). .Automated fault management with ML". ericsson.com/blog
6. Check Point (2025). Ïnfinity ThreatCloud AI". checkpoint.com
7. Cisco (2024). "DNA Center ML Insights". cisco.com
8. PMC (2021). Ïntelligent Network Monitoring". PMC8348484
9. McKinsey (2021). "Quantum communication market". mckinsey.com
10. EPJ Quantum Tech (2021). "Quantum in telecom". DOI: 10.1140/epjqt/s40507-021-00108-9
11. arXiv:2406.02240v1 (2024). "Quantum Computing in Wireless"
12. arXiv:2504.17133v1 (2025). "Quantum for 6G Networks"
13. IEEE ComSoc YP (2025). "Quantum reducing latency". yp.comsoc.org
14. GAO (2022). "Quantum Status & Prospects". GAO-22-104422
15. NIST (2024). "Post-Quantum Cryptography Standards". nist.gov/pqc
16. Gartner (2025). "MQ Hybrid Mesh Firewall". Kaur, R., Hils, A. et al.
17. Gartner (2025). "MQ Security Service Edge". Winckless, C. et al.
18. Gartner (2024). "MQ SD-WAN". Forest, J., Brown, K. et al.