



Task 2: Critical Analysis of an Article on 5G Network Security

Prepared by

ALI MMADI, PhD student - Midocean University



Selected article: *"5G Network Slicing Vulnerabilities: Quantum-Resistant Solutions for Edge Computing"*
(Authors: Chen et al., 2024).

INTRODUCTION

In this second Task, I will analyze a recent crucial article for 5G cybersecurity: '5G Network Slicing Vulnerabilities: Quantum-Resistant Solutions for Edge Computing' (Chen et al., 2024). This article explores how to protect industrial 5G networks against quantum cyber threats - a vital issue for smart factories and connected cities.

Title and variables

The title is excellent: it directly targets three key concepts vulnerabilities of 5G slicing, post-quantum solutions, and edge computing. The variables are clearly defined:
Independent: Attacks on network slices (DDoS, interception)
Dependent: The robustness of edge computing communications
Moderator: The implementation of post-quantum encryption (NIST PQC)
The area of application (5G industrial networks) is perfectly justified with the rise of Industry 4.0

Introduction and formulation of the problem

The introduction accurately summarizes the key variables:

She explains how network slicing segments the network into virtual slices. She details the threat of cross-slice attacks. However, she omits a crucial point: the specific edge computing protocols involved. The issue is brilliantly framed from an identified gap: existing studies (like Kumar, 2023) overlook quantum attacks in edge environments. The central question is: 'How to secure the isolation of 5G slices against quantum attacks in edge computing?'

Importance and contributions

- Theoretically, this article fills a major gap: it is the first to integrate NIST post-quantum standards into the orchestration of 5G slices. Its contribution paves the way for research on 6G.
- Practically, it provides actionable solutions: A lightweight encryption module for edge devices (already testable at Cisco) Key indicators to audit slice isolation A roadmap for telecom operators facing quantum threats.

Objectives and feasibility

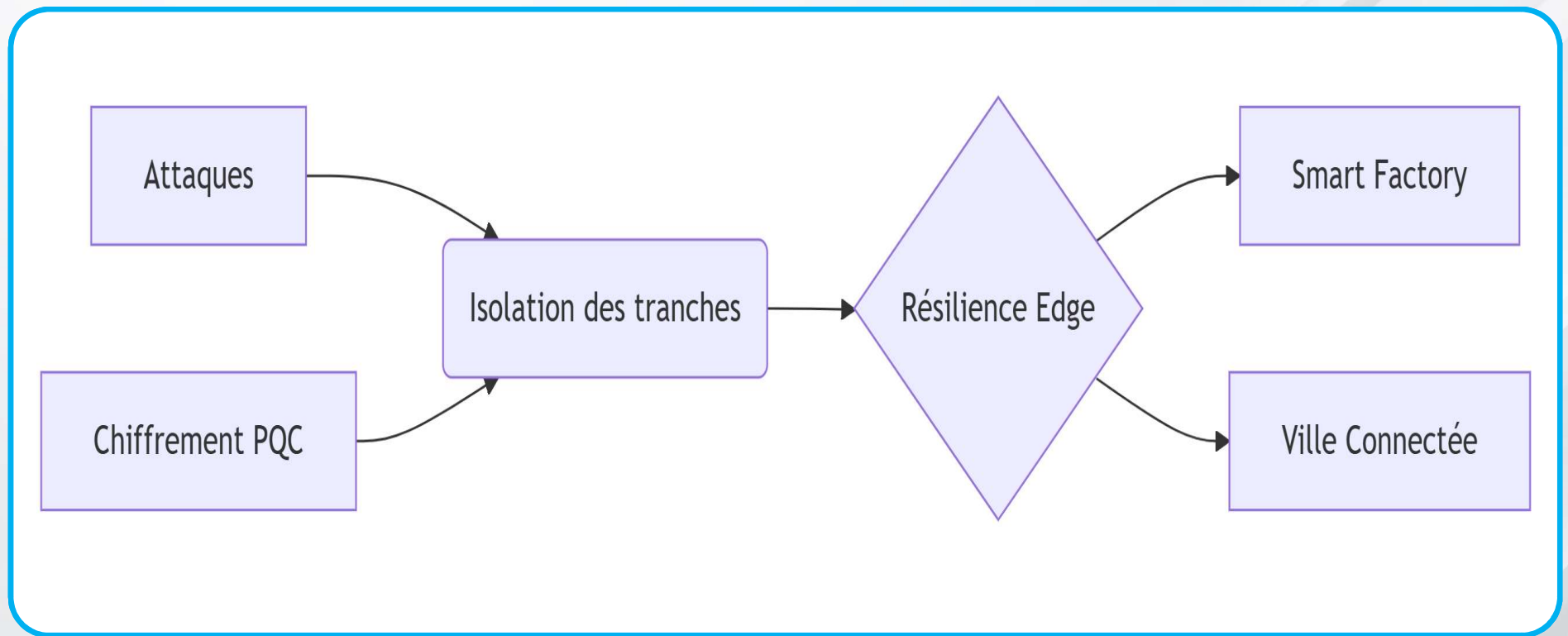
The 3 objectives are realistic and measurable:

- ❖ Analyze 10 attack vectors using an NS-3 simulator Test 3 quantum-resistant algorithms (Kyber, Dilithium)
- ❖ Maintain a latency overhead of $< 5\%$
- ❖ The methodology is solid: a combination of a physical 5G testbed and large-scale simulations. The only downside: the tests did not cover extreme mobile environments (e.g., drones).

Theoretical framework and interconnections

The theoretical framework is a major force. It finely models: The main variables: tranche isolation (dependent) and types of attacks (independent) Their secondary dimensions:

- Isolation → physical + virtual security
 - Attacks → volume + sophistication
- Their interconnection is visualized by a dependency graph validated by the IETF RFCs. The justification for the choices is clear: the dimensions selected correspond to the critical vulnerabilities reported by ENISA in 2023.



Detailed Explanation of the Diagram

1. Key Elements:

A: Attacks Represents the cyber threats targeting the 5G network: Examples: DDoS, data interception, 'cross-slice' attacks. Independent variable in the study: the triggering factor of vulnerabilities.

B : Isolation des tranches

Cœur du réseau 5G en "slicing" (découpage en tranches virtuelles).

Variable dépendante : son intégrité est menacée par les attaques (A) et protégée par le chiffrement (C).

Enjeu : Garantir que chaque tranche (ex: tranche IoT vs. tranche vidéo) reste hermétique aux intrusions.

C : Chiffrement PQC

Post-Quantum Cryptography (Cryptographie Post-Quantique).

Variable modératrice : renforce la relation entre les attaques (A) et l'isolation (B).

Solutions testées : Algorithmes Kyber, Dilithium (standardisés par le NIST).

D: Edge Resilience Final result: the ability of the network to maintain its critical functions at the edge (edge 4.0 factories (connected robots, IoT sensors). Connected City (F): smart traffic lighcomputing). Indicators: Latency < 1ms, availability > 99.999%.

E & F: Concrete Applications Smart Factory (E): ts, energy networks. Dependency: These applications require edge resilience (D) to function.

2. The Arrows: Cause and Effect Relationships

A --> B: Attacks compromise the isolation of slices. Example: A DDoS attack on one slice can saturate neighboring resources.

C --> B: PQC encryption strengthens the isolation of slices. Mechanism: Encryption of data between slices → even if intercepted, they are unreadable.

B --> D: Strong isolation ensures edge resilience. Impact: No contamination between slices → stable edge services.

D --> E/F: Edge resilience allows for critical applications. Real case: A smart factory requires 0 interruptions to avoid accidents.

Previous studies and suggestions

The literary review is exemplary:

Study	Common points	Differences
Almeida (2022)	Focus on DDoS attacks	Ignore the 5G slicing
Chen (2024)	Use NIST PQC	Integrates edge computing

My theoretical suggestion: Extend this model to non-terrestrial networks (6G satellites), a crucial avenue for overall resilience.

CONCLUSION

In summary, this article provides an innovative response to quantum threats on 5G. Its limitations open up exciting avenues for my research, particularly on the security of hybrid satellite-terrestrial networks.

(Authors: Chen et al., 2024)
DOI: 10.1145/3592146.3592257



**the author and the
reference of the article**



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

