

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي 8 ماي 1945 سيدي بلعباس
École Supérieure en Informatique
8 Mai 1945 Sidi Bel Abbès



THESIS

To obtain the diploma of **Engineer**

Field: **Computer Science**

Specialty: **Computer Systems Engineering (ISI)**

Real-Time AI-Based Detection of PFCP Flooding Attacks in 5G Core Networks

Presented by:

Ait Chabane Merieme

Submission Date: **21/06/2026**

In front of the jury composed of:

Dr. BENDAOUD Fayssal	President
Dr. IRATNI Naima	Examiner
Dr. BABA-AHMED Manel	Supervisor
Mr. Ouamri Amine	Co-Supervisor

Academic Year : 2025-2026

ABSTRACT

The global deployment of fifth-generation (5G) mobile networks introduces a fundamentally expanded attack surface, driven by the adoption of a SBA, NFV, and SDN. A particularly critical vulnerability lies in the PFCP, governing the N4 interface between the SMF and the User Plane Function (UPF). PFCP session establishment flooding attacks can saturate the UPF session table and cause network-wide service degradation, yet remain undetectable by traditional rule-based and signature-based mechanisms.

This thesis presents the design, implementation, and evaluation of a real-time AI-based detection system targeting PFCP flooding attacks in 5G Core Networks. It establishes a technical foundation covering the 5G Core architecture, the PFCP protocol, and attack vectors on the N4 interface, followed by a review of existing 3GPP security mechanisms. The relevant Deep learning architectures are then presented, including LSTM, BiLSTM, Autoencoders, and the Transformer Autoencoder. A critical survey of nine state-of-the-art AI-based approaches, spanning supervised deep learning, unsupervised autoencoders, federated learning, and P4-programmable detection, identifies persistent gaps in deployment readiness, dataset reproducibility, and PFCP-specific coverage.

The proposed system generates a reproducible dataset using Open5GS and UERAN-SIM, covering 60 UEs across five behavioral profiles and six PFCP flooding attack scenarios. A sliding-window pipeline extracts 21 engineered features per window. Three models are benchmarked: a unidirectional LSTM, a BiLSTM, and an unsupervised Transformer Autoencoder trained on normal traffic only, all exported to ONNX and evaluated under CPU-only conditions. The BiLSTM achieves 99.22% accuracy with an FPR of 0.84%, while the Transformer Autoencoder reaches 99.20% accuracy, a recall of 99.80%, an FNR of 0.20%, and the lowest inference latency at 0.335 ms per sample. A real-time pipeline in Rust provides deterministic, GPU-free detection on live N4 interface traffic.

Keywords: 5G Core Network, Intrusion Detection System, PFCP Protocol, Anomaly Detection, Real-Time Detection, Deep Learning, Network Security.

الملخص

يؤدي النشر العالمي لشبكات الهاتف المحمول من الجيل الخامس (5G) إلى توسيع مساحة الهجوم بشكل جذري، مدفوعاً بتبني كل من SBA وNFV وSDN. وتكمن ثغرة أمنية بالغة الخطورة بشكل خاص في بروتوكول PFCEP، الذي يتحكم في واجهة N4 بين SMF ووظيفة المستوى المستخدم (UPF). يمكن لهجمات إغراق إنشاء جلسات PFCEP أن تؤدي إلى تشبع جدول جلسات UPF وتسبب تدهوراً في الخدمة على نطاق الشبكة بأكملها، ومع ذلك تظل غير قابلة للكشف بواسطة الآليات التقليدية القائمة على القواعد والتوقعات.

تقدم هذه الأطروحة تصميم وتنفيذ وتقييم نظام كشف في الوقت الفعلي قائم على الذكاء الاصطناعي يستهدف هجمات الإغراق عبر بروتوكول PFCEP في شبكات 5G الأساسية. وتضع الأطروحة أساساً تقنياً يشمل بنية شبكات 5G الأساسية، وبروتوكول PFCEP، ووسائل الهجوم على واجهة N4، يلي ذلك استعراض لآليات الأمان الحالية التي حددها 3GPP. ثم يتم عرض بني التعلم العميق ذات الصلة، بما في ذلك LSTM وBiLSTM والمشفرات الذاتية (Autoencoders) و (TransformerAutoencoder). ويجري مسح نقدي لتسعة من أحدث النهج القائمة على الذكاء الاصطناعي، والتي تشمل التعلم العميق الخاضع للإشراف، والمشفرات الذاتية غير الخاضعة للإشراف، والتعلم التعاوني، والكشف القابل للبرمجة عبر P4، ويحدد الثغرات المستمرة في جاهزية النشر وقابلية تكرار مجموعات البيانات والتغطية الخاصة ببروتوكول PFCEP.

ينتج النظام المقترح مجموعة بيانات قابلة للتكرار باستخدام Open5GS وUERANSIM، تغطي 60 وحدة مستخدم (UE) عبر خمسة أنماط سلوكية وستة سيناريوهات لهجمات الإغراق عبر PFCEP. وتقوم سلسلة معالجة ذات نافذة منزقة باستخراج 21 سمة مُهندَسة لكل نافذة. تم إجراء اختبار أداء لثلاثة نماذج: LSTM أحادي الاتجاه، وBiLSTM، وAutoencoder Transformer غير الخاضع للإشراف الذي تم تدريبه على حركة المرور العادية فقط، وتم تصديرها جميعاً إلى ONNX وتقييمها في ظل ظروف تعتمد على وحدة المعالجة المركزية (CPU) فقط. يحقق نموذج BiLSTM دقة تبلغ 99.22% مع معدل FPR يبلغ 0.84%، بينما يصل Autoencoder Transformer إلى دقة تبلغ 99.20%، ومعدل استرجاع يبلغ 99.80%، ومعدل FNR يبلغ 0.20%، وأقل زمن استجابة للاستدلال عند 0.335 ملي ثانية لكل عينة. يوفر مسار معالجة في الوقت الفعلي مكتوب بلغة Rust اكتشافاً حتمياً وخالياً من وحدة معالجة الرسومات (GPU) لحركة مرور واجهة N4 الحية.

الكلمات المفتاحية: الشبكة الأساسية للجيل الخامس (5G)، نظام كشف التسلسل، بروتوكول PFCEP، كشف الانحرافات، الكشف في الوقت الفعلي، التعلم العميق، أمن الشبكات.

RÉSUMÉ

Le déploiement mondial des réseaux mobiles de cinquième génération (5G) entraîne une augmentation considérable de la surface d'attaque, due à l'adoption des technologies SBA, NFV et SDN. Une vulnérabilité particulièrement critique réside dans le PFCP, qui gère l'interface N4 entre le SMF et la fonction de plan utilisateur (UPF). Les attaques par inondation lors de l'établissement de sessions PFCP peuvent saturer la table de sessions de l'UPF et entraîner une dégradation des services à l'échelle du réseau, tout en restant indétectables par les mécanismes traditionnels basés sur des règles et des signatures.

Cette thèse présente la conception, la mise en œuvre et l'évaluation d'un système de détection en temps réel basé sur l'IA et ciblant les attaques par inondation PFCP dans les réseaux centraux 5G. Elle établit une base technique couvrant l'architecture du cœur de réseau 5G, le protocole PFCP et les vecteurs d'attaque sur l'interface N4, suivie d'une revue des mécanismes de sécurité 3GPP existants. Les architectures d'apprentissage profond pertinentes sont ensuite présentées, notamment les LSTM, les BiLSTM, les auto-encodeurs et l'auto-encodeur Transformer. Une étude critique de neuf approches de pointe basées sur l'IA, couvrant l'apprentissage profond supervisé, les auto-encodeurs non supervisés, l'apprentissage fédéré et la détection programmable via P4, identifie des lacunes persistantes en matière de préparation au déploiement, de reproductibilité des ensembles de données et de couverture spécifique au PFCP.

Le système proposé génère un ensemble de données reproductible à l'aide d'Open5GS et d'UERAN-SIM, couvrant 60 terminaux (UE) répartis selon cinq profils comportementaux et six scénarios d'attaques par inondation PFCP. Un pipeline à fenêtre glissante extrait 21 caractéristiques artificielles par fenêtre. Trois modèles sont évalués : un LSTM unidirectionnel, un BiLSTM et un auto-encodeur Transformer non supervisé, entraîné uniquement sur du trafic normal ; tous sont exportés au format ONNX et évalués dans des conditions de traitement exclusivement sur CPU. Le BiLSTM atteint une précision de 99,22% avec un FPR de 0,84%, tandis que l'auto-encodeur Transformer atteint une précision de 99,20%, un rappel de 99,80%, un FNR de 0,20% et la latence d'inférence la plus faible, à 0,335 ms par échantillon. Un pipeline en temps réel réalisé en Rust assure une détection déterministe, sans GPU, sur le trafic en direct de l'interface N4.

Mots-clés: Réseau coeur 5G, système de détection d'intrusion, détection d'anomalies, apprentissage automatique, apprentissage profond, PFCP, découpage du réseau, sécurité, LSTM, auto-encodeur, apprentissage fédéré.