

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 في الإعلام الآلي 8 ماي 1945 بسيدي بلعباس
École Supérieure en Informatique 8 Mai 1945 Sidi Bel Abbès



THESIS

to obtain the Diploma of Engineering

Field: Computer Science | **Specialty:** Computer Systems Engineering (ISI)

Theme

**Spatio-Temporal Foundation Model for Network
Intrusion Detection Systems (NIDS):
Self-Supervised Zero-Day Detection via Hybrid Masked
Transformers**

Presented by:
CHIALI Akila

Submission Date:
21/06/2026

In front of the jury composed of:

Dr. BENSENANE Hamdane	President
Dr. BENDAOUD Fayssal	Supervisor
Dr. BABA-AHMED Manel	Examiner

Academic Year: 2025-2026

Abstract

Nowadays, the cybersecurity field is facing a significant dilemma caused by the exponential evolution of cyber threat vectors. The emergence of AI-driven intrusion techniques, has rendered traditional detection frameworks increasingly insufficient. Consequently, identifying malicious intent now requires more than simple pattern recognition; it demands a deep understanding of the underlying dynamics of network communication.

This thesis proposes a robust **Network Intrusion Detection System (NIDS)** built upon the complexity of packet flow analogies. By leveraging **Hybrid Masked Spatio-Temporal Transformers**, we redefine network traffic as a spatio-temporal volume. Unlike classical models, our approach utilizes self-supervised learning to capture the joint evolution of internal packet structures (spatial) and flow sequences (temporal).

Through this architecture, the model achieves a profound understanding of both historical attack patterns and "New" unobserved exploits. By mastering the fundamental "Grammar" of the network, the proposed system provides not only a solution to detect known attacks through their signatures but also promises a scalable and adaptive resolution for **Zero-Day detection**.

Keywords: Spatio-Temporal Transformers, Masked Modeling, NIDS , Zero-Day Detection, AI , Self-Supervised Learning..

ملخص

في الوقت الراهن، يواجه مجال الأمن السيبراني معضلة كبيرة ناجمة عن التطور المتسارع لمتجهات التهديدات الإلكترونية. لقد أدى ظهور تقنيات التسلل المعتمدة على الذكاء الاصطناعي إلى جعل أطر الكشف التقليدية غير كافية بشكل متزايد. ونتيجة لذلك، فإن تحديد النوايا الخبيثة يتطلب أكثر من مجرد التعرف على الأنماط البسيطة؛ إذ يستلزم فهماً عميقاً للديناميكيات الكامنة وراء اتصالات الشبكة، متجاوزاً بذلك مجرد الكشف عن التوقيعات الساكنة.

تقترح هذه الأطروحة نظاماً قوياً للكشف عن التسلل في الشبكات (NIDS) مبنياً على تعقيد قياسات تدفق الحزم. ومن خلال الاستفادة من المحولات الهجينة المقنعة للزمكان (Hybrid Masked Spatio-Temporal Transformers)، قننا بإعادة تعريف حركة مرور الشبكة كحجم زمكاني. وخلافاً للنماذج الكلاسيكية، يستخدم نهجنا التعلم الذاتي الإشراف (Self-Supervised Learning) لالتقاط التطور المشترك للهياكل الداخلية للحزم (البعد المكاني) وتسلسلات التدفق (البعد الزمني).

من خلال هذه البنية، يحقق النموذج فهماً عميقاً لأنماط الهجمات التاريخية وكذلك "الثغرات الجديدة" غير المكتشفة. ومن خلال إتقان "القواعد" الأساسية للشبكة، لا يوفر النظام المقترح حلاً للكشف عن الهجمات المعروفة عبر توقعاتها فحسب، بل يعد أيضاً بحل قابل للتوسع والتكيف للكشف عن هجمات اليوم الصفر (Zero-Day Detection)، مما يسد الفجوة بين قدرات الحوسبة العالية والتعقيدات الدقيقة للأمن السيبراني الحديث.

الكلمات المفتاحية: المحولات الزمكانية، الذكاء الاصطناعي، النمذجة المقنعة، نظام الكشف عن التسلل في الشبكات (NIDS)، الكشف عن هجمات اليوم الصفر، التعلم الذاتي الإشراف.