

الجزائرية الديمقراطية الشعبية الجمهورية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

المدرسة العليا للإعلام الآلي - 08 ماي 1945 – بسيدي بلعباس
Ecole Supérieure en Informatique
Mai 1945- Sidi Bel Abbès 08-



MEMOIRE

En Vue de l'obtention du diplôme de **Master**

Filière : **Informatique**

Spécialité : **Intelligence Artificielle et Sciences des Données (IASD)**

Thème

**Intelligent Alarm Management for Telecom Networks:
Real-Time Correlation, Root Cause Identification, and Cascade
Prediction Using Graph Neural Networks**

Présenté par :

- Mr Yassine Ramla

Soutenu le : **01/10/2026**

Devant le jury composé de :

- | | |
|-----------------------|-----------|
| - Pr. ELOUALI Nadia | Président |
| - Dr. KHALDI Belkacem | Encadreur |
| - Dr. MAHAMMED Nadir | Examineur |

Année Universitaire : 2025 / 2026

Abstract

The fault management of a mobile network produces a large flow of alarms. One fault is often reported by many alarms on several elements, and the engineers of the network operations center must find which alarms belong together and where the fault lies. This work, carried out at Ooredoo Algeria, studies three tasks on one export of the operator’s alarm log: next-alarm prediction, alarm correlation and root-cause identification. The topology of the network links the three tasks.

We first present the background of these tasks: mobile networks and alarms, the data mining methods used for correlation, and the sequence and graph models used for prediction. We then build two network graphs from the alarms themselves, one between managed elements and one between sites. For prediction, we train sequence models of the next alarm code and add graph information to them in three forms: static graph embeddings, dynamic graph features, and attention over the active alarms of neighbouring elements, all under the same leakage controls. Predicting the next element instead was tried and paused after a negative result. For correlation, we mine a catalogue of statistically tested rules between alarm codes at several topological distances and use it in a correlator that groups the alarm stream into incidents. For root cause, we name the root site and the root alarm of each incident.

The export covers about 11 hours: 99% of its alarms fall on one day. On this data, no graph model beat the sequence model by more than the measured noise floor of 0.015 macro F1, and diagnostics trace this negative result to the small number of examples per alarm code, not to the models. The graph is useful instead for grouping and locating alarms. On the test period, the correlator reduces the number of items to handle by a factor of 9.0 and keeps 89.1% of the vendor’s root–child links inside one incident. The root-cause method names the right site in 18 of 19 labelled incidents, against 13 for the site of the earliest alarm. We also design the application that would run these methods in the network operations center.

Keywords: fault management, alarm correlation, root-cause analysis, alarm prediction, graph neural networks, association rules, mobile networks.

ملخص

تُنتج إدارة الأعطال في شبكة الهاتف النقال تدفقاً كبيراً من الإنذارات. وكثيراً ما يُبلغ عن عطل واحد بعدة إنذارات تصدر عن عدة عناصر، فيتعيّن على مهندسي مركز عمليات الشبكة معرفة الإنذارات التي تنتمي إلى المشكلة نفسها وتحديد موضع العطل. يدرس هذا العمل، الذي أنجز لدى أوريدو الجزائر، ثلاث مهام على ملف واحد مُصدّر من سجل إنذارات المتعامل: التنبؤ بالإنذار التالي، وربط الإنذارات، وتحديد السبب الجذري. وتجمع طوبولوجيا الشبكة بين هذه المهام الثلاث.

نعرض أولاً الخلفية النظرية لهذه المهام: الشبكات النقالة والإنذارات، وطرق التنقيب في البيانات المستعملة في الربط، ونماذج المتتاليات والمخططات المستعملة في التنبؤ. ثم نبني من الإنذارات نفسها مخططين للشبكة، أحدهما بين العناصر المُدارة والآخر بين المواقع. في التنبؤ، ندرب نماذج متتاليات تنبأ برمز الإنذار التالي، ونضيف إليها معلومات المخطط بثلاث طرق: تضمينات ثابتة للمخطط، وخصائص ديناميكية للمخطط، وآلية انتباه على الإنذارات النشطة لدى العناصر المجاورة، مع الضوابط نفسها ضد تسرب البيانات. أما التنبؤ بالعنصر التالي فقد جُرب ثم علّق بعد نتيجة سلبية. في الربط، نستخرج فهرساً من القواعد المختبرة إحصائياً بين رموز الإنذارات على عدة مسافات طوبولوجية، ونستعمله في أداة ربط تجمع تدفق الإنذارات في حوادث. وفي تحديد السبب الجذري، نعيّن لكل حادثة الموقع الجذري والإنذار الجذري.

لا يغطي الملف المُصدّر سوى نحو 11 ساعة، إذ يقع 99% من إنذاراته في يوم واحد. وعلى هذه البيانات، لم يتفوق أي نموذج بياني على نموذج المتتاليات بأكثر من حد الضجيج المقاس، وهو 0.015 في مقياس macro F1، وتُرجع التشخيصات هذه النتيجة السلبية إلى قلة الأمثلة لكل رمز إنذار، لا إلى النماذج. في المقابل، يفيد المخطط في تجميع الإنذارات وتحديد موضعها. ففي فترة الاختبار، تقلّص أداة الربط عدد العناصر الواجب معالجتها بمعامل 9.0، وتُبقي 89.1% من روابط المورد بين الإنذار الجذري والإنذار التابع داخل حادثة واحدة. وتعيّن طريقة السبب الجذري الموقع الصحيح في 18 حادثة من أصل 19 حادثة موسومة، مقابل 13 لموقع أقدم إنذار. ونصمّم أخيراً التطبيق الذي يشغل هذه الطرق في مركز عمليات الشبكة.

الكلمات المفتاحية: إدارة الأعطال، ربط الإنذارات، تحليل السبب الجذري، التنبؤ بالإنذارات، الشبكات العصبية البيانية، قواعد الارتباط، الشبكات النقالة.