Machine Learning Techniques for Self-Managing Networks

Bechir Boujelbene, Johannes Späth*, Max Helm*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: bechir.boujelbene@tum.de, spaethj@net.in.tum.de,helm@net.in.tum.de

***Abstract*—As modern network systems become increasingly complex and dynamic, traditional approaches to Root Cause Analysis (RCA) encounter inherent limitations when confronted with the needs of real-time analysis, scalability and the processing of vast volumes of generated input data. RCA refers to the process of identifying the root causes of observed failures within a network system. In this regard, Machine Learning (ML) approaches have emerged as a compelling alternative, capitalizing on their ability to process large-scale data and uncover complex patterns and distributions. This paper presents popular ML techniques and discusses their applicability to derive models for RCA in network fault management, highlighting their strengths, scalability and limitations.**

***Index Terms*—network failure diagnosis, root cause analysis models, telemetric data, machine learning**

1. Introduction

With the growing complexity and expansion of modern network topologies and the rising amount of generated traffic and connected devices [1], efficient network management has become more needed than ever. Network management encompasses all applied processes and tools designed to ensure the reliability, efficient performance and security of the network infrastructure [2]. In particular, root cause analysis (RCA) is considered to be a central aspect of network management. RCA models are designed to backtrack and identify the set of potential root causes that are responsible for a network failure [3].

Traditionally, constructing such models relies on the domain expertise of human operators, with the eventual aim of deriving a knowledge base of rules to diagnose network failures [4]. These rules depend on telemetric data measurements collected from various network devices and monitoring tools. The relevant input data for RCA models may include interface statistics or system logs from routers, or performance metrics such as CPU and memory usage from servers and endpoints [5].

However, as modern network traffic becomes more complex, vast amounts of data are being generated, which makes it impossible for humans to entirely process it. This results in traditional models failing to exploit all of the collected data and ignoring certain features that could potentially decrease the diagnostic output accuracy. Moreover, the process of constructing these rules is time consuming, unsuitable for environments where real-time reaction is essential, and not scalable to larger networks [4].

In this context, and in light of the recent success of machine learning (ML) applications in many areas of technology and science [6], ML techniques have emerged as a promising alternative to traditional RCA models. ML models feed off large volumes of input data [7], which is increasingly available on modern networks. In this paper, we present and discuss popular ML approaches that can be applied for deriving RCA models in networks based on input telemetric data.

The remainder of this paper is structured as follows: Section 2 presents key concepts of RCA in the context of network management. Section 3 highlights briefly previous related works. Section 4 introduces various suitable approaches for deriving RCA models and discusses their strengths and limitations.

2. RCA in Network Management

This section presents the fundamental concepts and terminology related to the field of network management and RCA, which are essential to understand the subsequent discussions of the approaches used to derive RCA models.

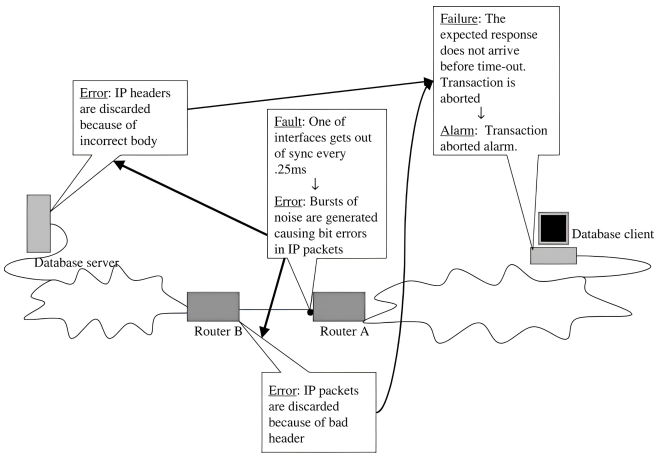

Figure 1: Illustration of different terminologies in RCA process (Figure from [8])

2.1. Terminology

We introduce the following terminologies, based on the previous works [9] [4]:
Network Error: is defined as the discrepancy between a condition of the network system and its theoretically

 doi: 10.2313/NET-2025-05-1_11

correct condition and is caused by one or many faults.
Network Faults: are also called root causes. These are network errors that can cause other errors but are not themselves caused by other errors. In other words, a network fault is the root cause of some error.
Network Failure: is an error that is observable from outside the system through external indicators called symptoms such as alarms raised upon anomaly detection. Upon detecting the failure, the telemetric data and statistics generated by network devices are then collected and used as input for the RCA model for diagnosis and producing the most likely root causes as outputs.
Root cause analysis: RCA is the process of determining the set of faults or root causes that generated originally the network failure observed by the given set of symptoms and associated with the generated telemetric data. Figure 1 illustrates these concepts using a network scenario where a failure occurs when a client attempts to access a database server. The failure is detected through a raised alarm, triggered by the absence of a response from the server. The fault originates from a hardware issue in the interface of a router along the path between the client and the server, causing bit errors in packets sent by the client, which are subsequently discarded by the server. This scenario also demonstrates how faults can originate at locations far from where their failure manifestations are observed.

2.2. RCA Workflow

The complete RCA process, starting from the model construction to the inference of probable root causes for a network failure, adheres to the workflow depicted in Figure 2. The first step would be to collect labeled telemetric data, which are historically observed data instances in network devices upon detecting symptoms of a network failure. Each instance is annotated with the corresponding fault or set of faults as labels. Combined with domain and system knowledge, an appropriate RCA model is constructed. These additional knowledge sources, however, are not always necessarily used, particularly when large datasets are available and the RCA models rely entirely on ML approaches with complex architectures. These models act from the outside as black boxes, extracting patterns from large datasets without requiring domain or system knowledge. Once training is complete and the RCA model is constructed, it can be used for inference. Telemetric data generated in response to new network failures is fed into the model to produce as an output the expected root causes. Furthermore, if a change in the network system occurs upon for example removing or adding new devices, the RCA model is updated.

3. Related Work

The preceding survey [3] highlighted the existing RCA models in various IT systems disciplines and not specifically in the context of network management. The survey emphasized the generation and inference algorithms of the models, with particular attention paid to performance aspects. In addition, previous papers [10] [8] discussed the challenges of fault localization in complex modern network systems and presented an overview of recent techniques and models as proposed solutions.

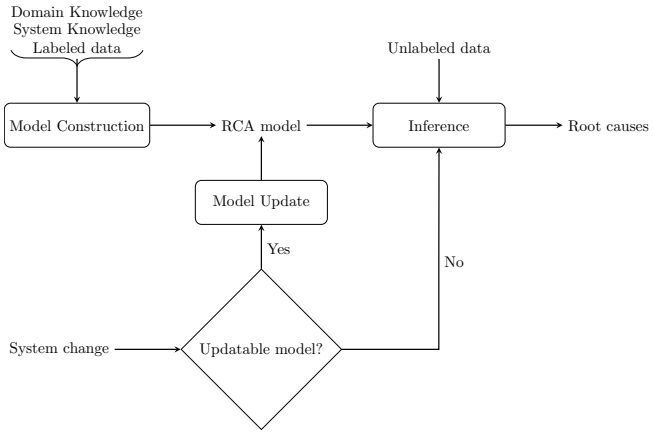

Figure 2: RCA workflow (Diagram was adapted from [3])

4. Approaches for RCA Models Derivation

This section provides an overview of various suitable approaches and techniques for deriving RCA models. In particular, we start by briefly introducing non-ML models and then proceed to delve in depth into ML models, highlighting their advantages, disadvantages, and scalability as summarized in Table 1.

4.1. Non ML Models

Non-ML models for RCA are based on deterministic approaches that do not involve any training algorithms or optimization techniques on the input telemetric data given the corresponding labels. While they are often easier to interpret and understand, their effectiveness is limited in modern, dynamic networks where it becomes quite challenging for such models to describe the complex distribution of the correlation between symptom data and faults. A review of the literature reveals numerous examples of such models that were used as the primary solution for RCA and localizing the root causes of network failures. In the following we list two widely applied approaches.

Rule-based Models: These models rely on predefined logical rules that are derived from human expertise in domain and system knowledge [11]. The rules are often expressed as if-then statements and the models rely on forward-chaining inference to produce potential faults as an output by executing the rules that were triggered, i.e., those whose conditions matched the input data [8]. One common method for representing the rules is through the use of codebooks, which map each network fault to a set of symptom data that should be observed in the faulty component itself and any affected components resulting from the original fault. The underlying root causes are then diagnosed by identifying the closest match to the observed input data. Reali et al. [12] employed this technique within a real Next Generation Network (NGN) that deployed wireline Voice over Internet Protocol (VoIP).

Pattern Mining-based Models: Pattern mining is a central task in the subfield of data mining that aims to analyze data in order to extract recurring patterns and strong

 doi: 10.2313/NET-2025-05-1_11

TABLE 1: Summary of Advantages and Disadvantages of ML Approaches for RCA

ML Approach	Advantages	Disadvantages
Decision Trees	Human-interpretable models; logical rules are easy to extract and align with domain knowledge; efficient inference execution.	Susceptible to overfitting and noisy network data; require ensemble methods for better generalization; limited in scalability.
Artificial Neural Networks	Capable of handling large-scale network data and capturing complex distributions; perform well in presence of noisy telemetric data.	Acts as a black box; lacks interpretability; training process can be expensive especially for complex architectures.
Support Vector Machines	Effective for high-dimensional telemetric data in network's RCA; can deal with non linear complex distributions.	Training is computationally expensive for large scale datasets; can underperform when trained to predict a large number of root causes.
Clustering	Useful when no historical labeled telemetric data is available.	Requires pre-selection of the number of clusters; unable to identify specific root causes but can only group based on similar observations.
Bayesian Networks	Human-interpretable models; readable dependencies; can combine domain knowledge with data-driven inference.	Model construction is expensive for large-scale networks; requires expert knowledge to define graph structure.

correlations [13]. This helps to facilitate decision-making for many tasks such as classification and prediction. In the context of network management, pattern mining techniques have been applied to analyze telemetric network data, enabling the discovery of meaningful patterns that assist in fault localization and RCA. For instance, Lozonavu et al. [14] applied sequential pattern mining [15] to discover correlations between network alarm instances. This approach constructs a directed weighted graph, where the nodes and directed edges represent the relations between different alarms and the associated weights illustrate the strength or also called the confidence of these relations. By deploying these dependencies, the model starts its inference with a network entity that reported an alarm. It then determines which other alarms are correlated, enabling the system to pinpoint the faulty network elements more precisely.

4.2. ML Models

ML is a scientific discipline concerned with the design of models capable to learn patterns and distributions of input data. The latter is typically partitioned into three complementary subsets: training, validation and testing sets [16]. The training set is used to train the model by optimizing its parameters to minimize a loss function between true outputs and predicted outputs by the model. The validation set fine-tunes hyperparameters and prevents overfitting, while the testing set assesses accuracy and generalization on unseen data [16]. This subsection reviews popular ML techniques that can be applied for RCA in network systems and summarizes the advantages, disadvantages and scalability of these approaches, as illustrated in Table 1.

Decision Trees: Decision Trees have been widely applied to fault localization and RCA in network systems. In particular, it is a supervised learning technique that requires labeled telemetric data annotated with the corresponding network faults [17]. Each distinct network fault or set of faults is represented by a class and the collected metrics such as interface statistics, bandwidth and memory usage are referred to as attributes.

A decision tree is a tree-like model that classifies data instances into classes represented by leaf nodes based on their attribute values. Internal nodes represent a test of an attribute and each outgoing branch from an internal node represents a possible range of values of this attribute. Learning a decision tree involves deciding which attribute and its associated test should be selected at each internal node to optimally split the data into branches. In general, optimal splits are picked by maximizing the "Gain" in information. The gain can be computed using various criteria, such as Entropy or Gini Index but the choice itself should not affect the ultimate model performance [18]. The inference algorithm for new instances is then applied by traversing the learned tree from the root node and following the branches based on the attribute values until a leaf node is reached which acts as the predicted root cause(s) of the model.

Chen et al. [17] deployed a decision tree based model combined with post processing performed on paths of the tree in order to identify causes of failures in large internet systems. In the field of RCA in network management, decision trees can be preferred as they have the advantage of yielding human interpretable results, which makes it easier to follow and understand the decisions made along the output path [10]. Furthermore, the model exhibits efficient runtime performance for the inference algorithm, rendering it well-suited for systems where time sensitivity and real-time analysis are crucial factors [3]. However, the scalability of these techniques can be limited to using only specific attributes of the input data, and the accuracy of the model can be severely degraded in the presence of noisy input data, a problem that is exacerbated in large-scale networks [17].

In fact, to address the last limitation and to improve generalization on unseen data, Random Forest (RF) techniques can be employed. RF is an ensemble learning method and its core concept lies in constructing multiple decision trees during the training process, rather than deriving only one. The inference outputs of the trees are then combined typically through majority voting, to make more robust and accurate predictions. For instance, Sauvanaud et al. [19] implemented an RF algorithm to localize root causes in Virtual Network Functions (VNFs).

Artificial Neural Networks (ANNs): ANNs are computational models inspired by the structure and learning mechanisms of biological neural networks (NNs) in the human brain. An ANN consists of multiple layers of interconnected neurons. Each neuron receives multiple inputs

 doi: 10.2313/NET-2025-05-1_11

from the previous layer, processes them, and generates a single output that is fed to each neuron in the next layer. This processing involves a weighted sum of the inputs, an addition of a bias, and the application of an activation function. The weights and biases represent the learned parameters of the model [20].

In the context of RCA in networks, the neurons of the input layer represent the telemetric data during network failures and the output neurons correspond to the root causes. The root cause associated with the output neuron exhibiting the highest value represents the predicted fault of the model. Wietgrefe et al. [21] developed a system called Cascade Correlation Alarm Correlator (CCAC) based on an ANN to predict the root causes of alarms in cellular phone networks. Each input neuron represents an alarm type and takes a binary value (active or inactive), while each output layer neuron corresponds to a failure's cause. The findings of [21] indicate that CCAC yields high prediction accuracy even in the presence of noise in the training data such as missing or irrelevant alarms. Furthermore, in a comparative study conducted by Wietgrefe et al. [22], it was demonstrated that CCAC is more accurate at predicting alarm causes than traditional approaches such as rule-based reasoning models. In general, ANN approaches have the ability to process the large-scale telemetric data produced by modern networks and can produce accurate predictions even with the presence of noisy data.

The above advantages may justify the fact that ANNs have been the subject of extensive research and are widely employed in numerous domains and fields [20]. However, it seems that ANNs have not achieved the same dominance in the area of RCA in network systems, unlike other disciplines. The primary reason behind this is that these models, especially those possessing complex architectures like deep ANNs, act from outside like black boxes and return predicted root cause(s) as an output, but it is almost impossible for human operators to backtrack and provide a logical explanation for it [3]. Moreover, such approaches use exclusively the labeled input dataset to construct the RCA models and are difficult to combine with available domain knowledge to derive meaningful and interpretable rules [3].

Support Vectoring Machines: Support Vector Machine (SVM) is another popular ML technique that can be applied to RCA and fault management in networks. SVM is essentially a linear supervised classifier that is based on the margin maximization principle [23]. To deal with non linear problems, which is the case in network's RCA, the input data can be preprocessed and mapped to higher dimensions using kernel methods. This process is called non-linear SVM [4].

Based on the training labeled telemetric data, an SVM is learned to find optimal separating hyper planes with each plane representing a network failure root cause(s). In the literature, we can find the application of SVM methods to a variety of network management tasks. For instance, the study conducted by Zidi et al. [24] applied an SVM-based model to detect failures in Wireless Sensor Networks (WSNs). WSNs consist of autonomous devices collaborating together through a wireless channel. The training dataset included both normal data measurements as well as measurements associated with different types of faults. Once the SVM model is trained, the inference algorithm predicts if new observations belong to a normal or a faulty case. The experimental results conducted by Zidi et al. [24] show that their SVM method achieves high accuracy rates.

In general, SVMs have the advantage of performing well in scenarios with high-dimensional input data [3], making them suitable for analyzing complex telemetric datasets in network management. However, SVMs seem to underperform when trained to predict a relatively large number of output classes, a common scenario when representing the diverse root causes of network failures [25]. As a result, their applicability can be limited to specific network failure scenarios.

Clustering: Clustering methods are unsupervised learning techniques that group data instances into clusters based on similar features or patterns, without the need for labeled data [9]. This is useful in network's RCA when the training telemetric data is not accompanied by the corresponding root causes. Such scenarios may arise due to a lack of historical labeled data or the presence of excessively noisy data, making supervised learning impractical.

Sozuer et al. [26] applied clustering techniques to identify correlated alarms belonging to the same cluster during network failure. This helps pinpoint the faulty network elements more precisely and localize the root causes. However, clustering models require predefining the number of clusters, and without expertise knowledge of the underlying network system, an incorrect choice can result in meaninglessly grouping telemetric measurements that do not originate from the same root cause(s) [9].

Bayesian Networks: A Bayesian Network (BN) is a probabilistic graphical model that represents variables and their conditional dependencies through a directed acyclic graph (DAG) [25]. The conditional probabilities are learned using techniques like Maximum Likelihood Estimation (MLE) or Bayesian Estimation [3]. In the context of RCA in networks, Bayesian Networks can model the causal relationships between the telemetric data, symptoms, and faults that act as variables of the model. For example, if an interface fault in a router causes increased latency and packet drops, a BN can capture these dependencies and help infer the root cause when these symptoms are observed.

Ruiz et al. [27] developed a BN model to identify the root causes of network failures at the optical layer. Khanafer et al. [28] proposed a failure diagnosis model using BN approach for Universal Mobile Telecommunications System (UMTS) networks. The dependencies between the variables in BN models are intuitively easy for human operators to understand. Moreover, the explicit representation of causes and effects enhances readability, making it easier to derive meaningful rules and integrate them with domain and system knowledge. However, constructing BNs can be computationally expensive, particularly for large-scale networks, and requires significant expertise to define the graph structure and which variables are included. Additionally, their scalability may be limited when dealing with high-dimensional datasets [25].

5. Conclusion

In this paper, we examined various approaches that can be applied to derive RCA models in network systems. Initially, we showed that traditional non-ML models, while easier to read and interpret, face major limitations when employed in dynamic and large-scale networks. We then proceeded to explore in depth ML models. Our review demonstrated that these techniques are able to handle large amounts of input telemetric data and identify the root causes of network failures more accurately and adaptively. Nevertheless, challenges such as explainability, computational cost, and exclusive reliance on input data still remain. A possible future work could aim to address these limitations by exploring hybrid models that combine the strengths of ML techniques with domain knowledge from traditional approaches, leading potentially to more robust RCA solutions.

References

[1] A. M. Odlyzko, "Internet traffic growth: Sources and implications," in *Optical transmission systems and equipment for WDM networking II*, vol. 5247. SPIE, 2003, pp. 1–15.

[2] L. Tawalbeh, *Network Management*, 04 2020, pp. 99–115.

[3] M. Solé, V. Muntés-Mulero, A. I. Rana, and G. Estrada, "Survey on models and techniques for root-cause analysis," *arXiv preprint arXiv:1701.08546*, 2017.

[4] M. Nouioua, P. Fournier-Viger, G. He, F. Nouioua, and Z. Min, "A survey of machine learning for network fault management," *Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics: Theories and Applications*, pp. 1–27, 2021.

[5] T. Wang and G. Qi, "A comprehensive survey on root cause analysis in (micro) services: Methodologies, challenges, and trends," *arXiv preprint arXiv:2408.00803*, 2024.

[6] R. Pugliese, S. Regondi, and R. Marini, "Machine learning-based approach: global trends, research directions, and regulatory standpoints," *Data Science and Management*, vol. 4, pp. 19–29, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666764921000485

[7] "Training Data Quality: Why It Matters in Machine Learning — v7labs.com," https://www.v7labs.com/blog/quality-training-data-for-machine-learning-guide, [Accessed 03-12-2024].

[8] M. łgorzata Steinder and A. S. Sethi, "A survey of fault localization techniques in computer networks," *Science of Computer Programming*, vol. 53, no. 2, pp. 165–194, 2004, topics in System Administration. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167642304000772

[9] S. P. Kavulya, K. Joshi, F. D. Giandomenico, and P. Narasimhan, "Failure diagnosis of complex systems," *Resilience assessment and evaluation of computing systems*, pp. 239–261, 2012.

[10] A. Dusia and A. S. Sethi, "Recent advances in fault localization in computer networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 3030–3051, 2016.

[11] T. Marques, "A symptom-driven expert system for isolating and correcting network faults," *IEEE Communications Magazine*, vol. 26, no. 3, pp. 6–13, 1988.

[12] G. Reali and L. Monacelli, "Definition and performance evaluation of a fault localization technique for an ngn ims network," *IEEE Transactions on Network and Service Management*, vol. 6, no. 2, pp. 122–136, 2009.

[13] P. Fournier-Viger, W. Gan, Y. Wu, M. Nouioua, W. Song, T. Truong, and H. Duong, "Pattern mining: Current challenges and opportunities," in *International Conference on Database Systems for Advanced Applications*. Springer, 2022, pp. 34–49.

[14] M. Lozonavu, M. Vlachou-Konchylaki, and V. Huang, "Relation discovery of mobile network alarms with sequential pattern mining," in *2017 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2017, pp. 363–367.

[15] J. Pei, "Mining sequential patterns efficiently by prefix-projected pattern growth," in *Proc. of 17th International Conference on Data Engineering (ICDE 2001)*, 2001, pp. 215–224.

[16] O. Hazzan and K. Mike, *Core Concepts of Machine Learning*. Cham: Springer International Publishing, 2023, pp. 209–224.

[17] M. Chen, A. Zheng, J. Lloyd, M. Jordan, and E. Brewer, "Failure diagnosis using decision trees," in *International Conference on Autonomic Computing, 2004. Proceedings.*, 2004, pp. 36–43.

[18] L. Breiman, *Classification and regression trees*. Routledge, 2017.

[19] C. Sauvanaud, K. Lazri, M. Kaâniche, and K. Kanoun, "Anomaly detection and root cause localization in virtual network functions," in *2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE)*, 2016, pp. 196–206.

[20] S. Agatonovic-Kustrin and R. Beresford, "Basic concepts of artificial neural network (ann) modeling and its application in pharmaceutical research," *Journal of Pharmaceutical and Biomedical Analysis*, vol. 22, no. 5, pp. 717–727, 2000. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0731708599002721

[21] H. Wietgrefe, K.-D. Tuchs, K. Jobmann, G. Carls, P. Fröhlich, W. Nejdl, and S. Steinfeld, "Using neural networks for alarm correlation in cellular phone networks," in *International Workshop on Applications of Neural Networks to Telecommunications (IWANNT)*. Citeseer Stockholm, Sweeden, 1997, pp. 248–255.

[22] H. Wietgrefe, "Investigation and practical assessment of alarm correlation methods for the use in gsm access networks," in *NOMS 2002. IEEE/IFIP Network Operations and Management Symposium.'Management Solutions for the New Communications World'(Cat. No. 02CH37327)*. IEEE, 2002, pp. 391–403.

[23] M. M. Adankon and M. Cheriet, "Support vector machine," *Encyclopedia of biometrics*, pp. 1303–1308, 2009.

[24] S. Zidi, T. Moulahi, and B. Alaya, "Fault detection in wireless sensor networks through svm classifier," *IEEE Sensors Journal*, vol. 18, no. 1, pp. 340–347, 2018.

[25] N. G. Lo, J.-M. Flaus, and O. Adrot, "Review of machine learning approaches in fault diagnosis applied to iot systems," in *2019 International Conference on Control, Automation and Diagnosis (ICCAD)*, 2019, pp. 1–6.

[26] S. Sozuer, C. Etemoglu, and E. Zeydan, "A new approach for clustering alarm sequences in mobile operators," in *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2016, pp. 1055–1060.

[27] M. Ruiz, F. Fresi, A. P. Vela, G. Meloni, N. Sambo, F. Cugini, L. Poti, L. Velasco, and P. Castoldi, "Service-triggered failure identification/localization through monitoring of multiple parameters," in *ECOC 2016; 42nd European Conference on Optical Communication*. VDE, 2016, pp. 1–3.

[28] R. M. Khanafer, B. Solana, J. Triola, R. Barco, L. Moltsen, Z. Altman, and P. Lazaro, "Automated diagnosis for umts networks using bayesian network approach," *IEEE Transactions on vehicular technology*, vol. 57, no. 4, pp. 2451–2461, 2008.