A SURVEY ON ADVANCEMENT OF FAULT LOCALIZATION TECHNIQUES IN COMPUTER NETWORKS

Indumathy Murugesan
PG scholar, M.tech(ECE), LBS,College of Engineering Kasaragod
indumathy.km@gmail.com

Abstract

The rapid development and advancement in communication technologies leads to increase communication networks both regarding size and complexity. This constant increase in complexity of communication networks leads to serious challenges for network management operating systems. However, in communication networks, link failures are unavoidable but the detection, identification, and recovery of failures in complex networks in a timely manner is crucial for the reliable operation of the networks. However, fault localization, is a major aspect in network fault management, it is a process of deducing the exact source and location of a failure in a communication link from a set of previous observed failure indications. The research activity is focusing highly to localize the faults as soon as possible due to advent of modern communication systems having complex networks which have high possibilities of fault occurrences. However, due to evolving complexity in communication systems, the requirements on fault identification and localization techniques undergo major changes as well. It should be mentioned that despite this research developments effort, fault localization in complex communication systems is still a major research problem. This paper presents an overview of proposed solutions of the adopted techniques for the past years as well as challenges in localizing fault of complex communication systems, and their advantages, and shortcomings.

I.Introduction

Fault diagnosis and localization are the major aspects of network fault management. As faults are not avoidable in communication systems, quick detection and isolation of faulty network is essential for communication robustness, reliability, and accessibility of a system. In complex communication networks, automating fault management is crucial. Event, is an exceptional condition occurring during the operation of hardware or software in a managed network which is a central concept in fault diagnosis. Faults (unusual condition in a network link) comprise a class of network events that affect other events, but they are not caused by other events.

Faults are classified mainly based on their time duration as: (1) permanent, (2) intermittent, and (3) transient. Permanent fault remains in a network until a repair action is taken. Intermittent faults occur in a random or periodic basis causing service degradation for certain period. However, frequent occurrence of intermittent faults highly degrade service performance. These faults cause a temporary and minor degradation of service and those faults can be automatically repaired by error recovery procedures [1].

Errors are defined as a difference between a computed or measured value to a true or theoretically correct value or condition [1]. Error is the result of a fault. Faults may or may not cause errors. Errors may cause deviation of a service from the specified service, which is visible to the outside world. The term failure refers to this

type of error. Errors need not be corrected directly, and in many cases, they are not externally visible. However, an error may cause a malfunctioning of dependent network devices or software. Thus, they may propagate within the network causing failures of faultless hardware or software [1]. Symptoms are indication of failures [2]. They are indicated by alarms notifications of a potential failure [2]. These notifications are originated by management protocol messages from management agents (e.g., SNMP trap [3] and CMIP EVENT-REPORT [4]) also from management systems monitoring the network status e.g., using ping command [5], and also from system log-files or character streams sent by external equipment [6]. Some faults can be observed directly. On the other hand, there are also many types of faults which are unobservable due to (1) their intrinsically unobservable nature, (2) local corrective mechanisms of management systems that destroy evidence of fault occurrence, or (3) inefficiency of management functionality to provide indications for fault existence. There are some faults which are partially-observable by the management system which indicates fault occurrence, but those indications are not sufficient to localize the fault. Since most of the faults in the network are not directly observable, the management system has to clearly verify the information provided by the received alarms. The reported alarms carry information which may include : the object identity which generated the alarm, failure type, timestamp, alarm identifier, failure severity, a description of the failure, etc. [7,6]. In a communication network, many numbers of alarms that can be created by a single fault which will be delivered to the network management center. The cause of multiple alarms may be a due to (1) repeated fault occurrence, (2) multiple interruptions in the service provided by a faulty component, (3)generating multiple alarms by a device, (4) many devices simultaneously detection and issuing a notification about the same network fault, and (5) error propagating to other network devices which cause them to fail which in turn generate additional alarms [7].

Fault diagnosis process mainly involves three steps:

- Fault detection [4]- process of identifying the occurrence of fault by capturing indications of network disorder from alarms.
- Fault localization [4,5,10] – locating exact fault locations from the information provided by a set of observed fault indications.
- Testing [5,10]- Determining the actual fault location from a number of possible predictions.

This survey focuses on the fault localization which is a process of deducing the exact source of the failure from the set of observed failure indications. The most popular fault localization technique is alarm correlation which is a process of grouping alarms related by having the same cause of failures. Fault localization is subjected to complications resulting from complexity, unreliability and non-determinism of communication systems

II .Fault localization based on Alarm correlation systems

In [11], a method and a tool is presented for the discovery of repeated patterns of alarms databases; these patterns, episode rules, which can be used in real-time alarm correlation systems. The episode rules provide statistical information about repeated phenomena in the alarm stream, by which the correlation systems construction becomes easier with those tools. A research system called TASA employs this methodology, which is used by several telecommunication operators

Large amounts of alarms are produced by the network elements when faults occur in a network. Fully employing this valuable data in network management is difficult, however, due to the high volume, and the fragmented nature of the information. In alarm correlation, a management center automatically analyzes the stream of alarms, notifications and clear messages it receives from a telecommunication network. Alarm correlation is typically based on looking at the active alarms at a time interval and incorporating them as a group. This interpretation can result in filtering of redundant alarms, identification of faults,

and in suggestions for corrective actions. The motive of alarm correlation systems is processing the large alarm data set into a smaller and useful set of reports to ease the work of network managers. The diversity of complex network elements, and the pattern of alarm occurrence variation pose serious problems for network management experts building a correlation model.

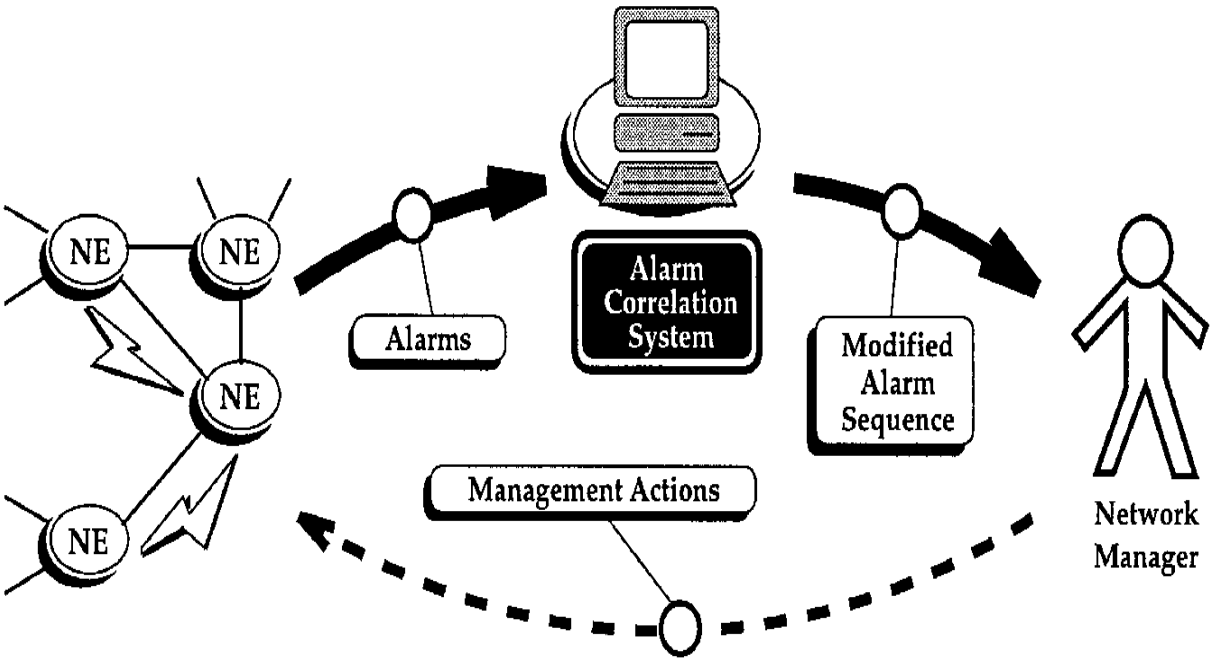

Fig. 2.1. The flow of alarms from a telecommunication network in an alarm correlation system.

In this paper, methods for semi-automatic discovery of patterns is presented in alarm databases; these methods help in the construction of alarm correlation systems. A novel algorithm is used to discover recurrent patterns in large alarm databases. Then iterative information retrieval method is applied to give flexible views to the discovered patterns. The method for generating alarm correlation systems contains the following three steps:

1. Semi-automatic off-linediscovery of alarm patterns.
2. Construction or modification of an alarm correlation system. The discovered patterns are used only to aid the experts in recalling and formulating correlation patterns.
3. The correlation system in real-time alarm management.

The ideas expressed in the article [11] ,have been implemented in a system called TASA, for Telecommunication Alarm Sequence Analyzer. The TASA system has been developed in co-operation with the four telecommunication companies.

III. Various Fault localization techniques

In [12], fault localization challenges in complex communication systems and overview of solutions proposed in the past years, and also their advantages and shortcomings are discussed. Fault diagnosis is the major aspect of network fault management systems. Automating fault diagnosis in large and complex communication networks, is critical.

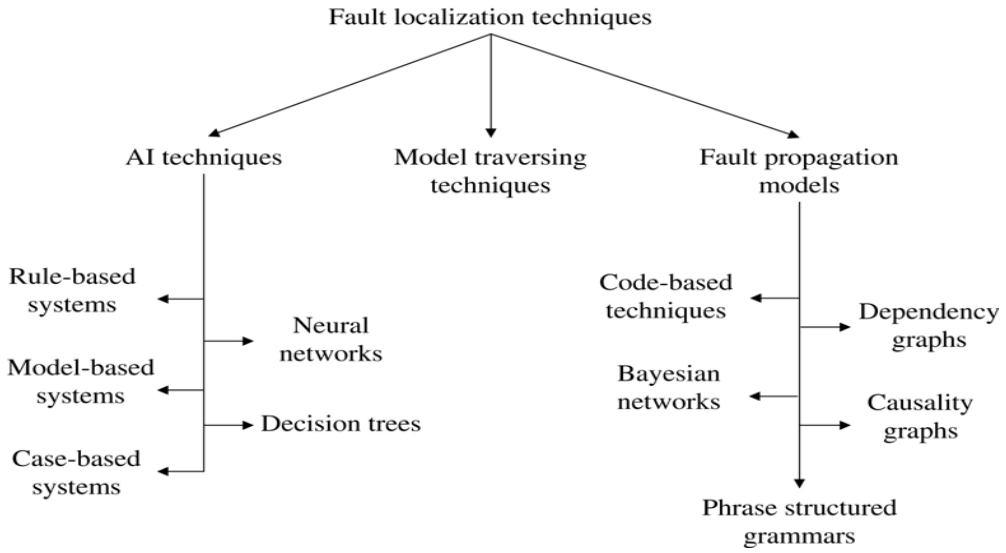

Fig. 2.2. Classification of fault localization techniques.

Expert systems try to imitates knowledge of a human expert when solving problems in a particular domain.

Rule-based systems- Rely solely on surface knowledge, do not require prior understanding of the system architectural and operational principles.

Disadvantage - Rule-based systems include inability to learn from experience, inability to deal with priorly unknown problems, and difficulty in updating the system knowledge.

In model-based expert systems, conditions associated with the rules usually include predicates referring to the system model. The existence of a relationship among system components is tested by these predicates.

Case-based systems are a special class of expert systems that base their decisions on experience, past situations and previously used solutions. Neural networks, which are systems composed of interconnected nodes called neurons, try to mimic operation of a human brain. The main disadvantage in case based systems is that they require long training periods

Decision trees - Assign time or other values to possible outcomes, so that decisions are automated.

Model traversing techniques - use formal representation of a communication system with clearly marked relationships among network entities. By determining these relationships between the network entity that reported an alarm and fault, the fault identification process determines which alarms are correlated and locate faulty network elements.

Graph-theoretic techniques rely on a graphical model of the system, called a fault propagation model. Graph-theoretic techniques requires a priori information of relationship between a failure condition or alarm in one component to failure conditions or alarms in other components.

The most challenging issues concern multi-layer fault localization, distributed diagnosis, temporal correlation, fault localization in mobile ad hoc networks, and root cause analysis in a service-oriented environment.

IV.Fault localization based on probabilistic inference

In [13],a novel network fault localization algorithm is proposed based on active network measurements, probabilistic inference and change detection. The algorithm is computationally efficient for networks with thousands of nodes and requires few configuration parameters. The algorithm is based on active network measurements, probabilistic inference and change detection. Simulation results shows that solution provides fast and accurate localization of performance degradations on tree topologies. One important benefit of our filter-based estimation is the inherent resiliency against noise in the sampling (i.e. measurements and measurement infrastructure) as well as in the measured system (i.e. the network). In other words the filter does not rely on each measurement sample being perfectly accurate.

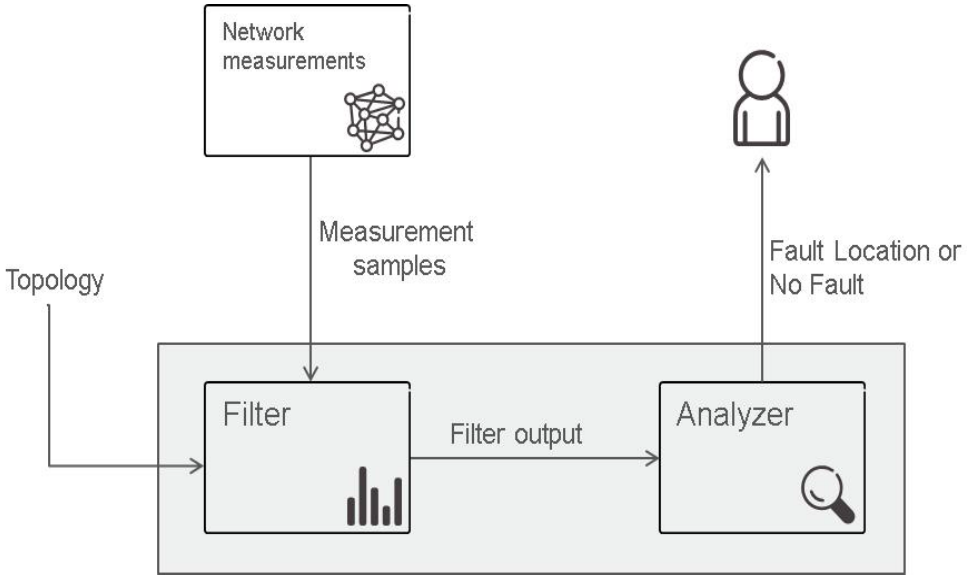

Fig 4.1: Overview of the network performance degradation localization solution.

An additional feature of filters is that sample data is aggregated in the filter outcome over time. The filter itself becomes a storage container for aggregated values of samples collected from the network. This reduces the need for storing previous samples for later processing. Reduced storage decreases the complexity of the implementation. The filter construction described above is robust in the sense that particle weights are updated according to the measurement values that may contain errors, and that the particle corresponding to the problematic edge will eventually have the highest weight. a change detection technique is introduced in order to remove the need to configure the threshold for alarm generation while maintaining the capability to perform online calculations on measurement results as they arrive. Tuning the memory properties of the filter becomes more important as the network size increases. Tree topologies are particular cases of interest in this respect. As the edges connecting the leaves are traversed seldom, the increase factor needs to balance the decreases performed by the filter until the next time the degraded edge is traversed.

TABLE 4.1-Filter and analyzer parameters for different tree sizes

Tree Size	h	T	δ	λ	γ
13	3	4	0.975	5	0.75
40	3	3	0.975	15	0.75
121	3	3	0.975	25	0.75
364	3	2	0.974	40	0.75
1093	3	2	0.995	80	0.75

As shown in Table 4.1, an increase in the tree size determines an increased outspreading effect on the filter probability mass and hence also has a negative influence on the degradation localization time. One way to remedy this is to increase selected parameter values with increasing network size

The paper [13] examines a novel algorithm for determining the location of performance degradations in packet networks. The algorithm is based on discrete state-space particle filters and change detection statistics, it has 3-10 times faster time to localization in many cases compared to our previous method and removes the need to configure alarm

thresholds. The algorithm was evaluated in a simulator where properties such as degradation localization time and false positives were studied in-depth. The outcome of the evaluation showed that the algorithm is effective in automatically identifying the location of a performance degradation. The efficiency is dependent on the exact position of the degradation in a tree topology, the furthest away from the root, the more time it would take to detect a problem.

V. Fault localization using combination of Bayesian Networks and Case-Based Reasoning

In [14], a new hybrid mechanism is proposed as a combination of Bayesian Networks and Case-Based Reasoning to overcome certain limits in fault diagnosis techniques and reduce human intervention in this process. This mechanism identifies the root cause of failure with a finer precision and high reliability with reduced computation time even in the condition of network dynamicity.

The functional model specifies that the following functions, are incorporated by a network management system: Fault, Configuration, Accounting, Performance and Security (FCAPS).

This method presents a new hybrid approach combining Case-Based Reasoning (CBR) and Bayesian Networks (BN). Bayesian Networks are currently the most powerful and popular diagnosis method. However, the complexity of inference in Bayesian Networks increases exponentially with the number of nodes. Hence, this technique is not suitable for large scale systems including a large number of components such as current and future networks with hundreds or thousands of elements. To overcome this limitation, a combined case-based and Bayesian reasoning approach is proposed to improve the BN inference, while keeping the advantages of BN technique. The resulting solution improves the degree of automation of the diagnosis process and requires less intervention of human expertise.Whatever the size of the original network, case-based and Bayesian reasoning approach can precisely identify the root cause and with greater accuracy than the BN technique.

TABLE 5.1- Test of Accuracy

Number of node in BN	**BN approach**	**CBR-BN approach**
10 nodes	2 to 3	1
20 nodes	3 to 4	1
30 nodes	3 to 4	1
40 nodes	3 to 4	1
60 nodes	3 to 4	1
80 nodes	3 to 4	1
100 nodes	4 to 5	1
200 nodes	4 to 6	1
500 nodes	6 to 8	1

The observation of the results highlights that the BN technique is less accurate and the accuracy varies with the size of the network. Table 5.1, shows the results obtained for a network size ranging from 10 to 500 nodes.

An extensive evaluation was conducted in simulation and showed the benefits of the approach in comparison to the pure Bayesian Network approach according to three main metrics, namely: accuracy, reliability and speed. The solution is simple, flexible and scalable. It outperforms the traditional Bayesian Network method in all criteria bringing an increased speed with gains up to two orders of magnitude, combined advantageously with a higher accuracy and reliability. The reduction of the complexity

enabled by the technique is also promising and will be the subject of future investigations in order to formally prove the level of complexity reduction attainable.

VI. Fault detection and diagnosis (FDD) on solar-powered Wireless Mesh Networks (WMNs)

In [15], automated fault detection and diagnosis (FDD) on solar-powered Wireless Mesh Networks (WMNs) is proposed. We have used the Knowledge Discovery in Databases (KDD) methodology and a pre-defined dictionary of failures based on our previous experience with the deployment of WMNs.

Thereafter, the problem was solved as a pattern classification problem. Several classification algorithms were evaluated, such as Naive Bayes, Support Vector Machine (SVM), Decision Table, k-Nearest Neighbors (k-NN) and C4.5. The SVM presented the best results, having 90.59% training accuracy and over 85% accuracy in validation tests.

To produce a history of labeled faults, a set of real-problem emulations were performed in the network. Based on a labelled history database, the supervised learning approach was used as the machine learning technique. Several classification algorithms were considered and tested, namely: Naive Bayes, Support Vector Machine (SVM), Decision Table, k-Nearest Neighbors (k-NN) and C4.5. Another database, containing only naturally occurred faults' data, not emulated ones, was used for results validation.This method goals are: (1) propose the KDD methodology and the supervised learning approach to solve the fault detection and diagnosis problem in WMNs; (2) describe each solution step, the difficulties faced during the development of the proposed solution and how they were overcome; (3) provide an autonomous FDD module to be part of the WMN management integrated platform.

The REMOTE project deployed a communication infrastructure based on WMN. While the ultimate goal is to deploy our solution at the production network of the REMOTE project, in the development phase, prototypes were evaluated in a WMN testbed located on one university campus at UFF. Both the production network and the testbed are infrastructure WMNs and have similar characteristics as energy constraints, the use of a solar power system and multiple radios with the same technologies. Therefore, the methodology and the scenarios used in the development phase have immediate applicability for the production network.

Each mesh router is composed of three modules:

Communication module: consists of a router with two wireless interfaces, a client access interface consisting of an IEEE 802.11g radio, and an interface for communication between nodes (backbone), consisting of an IEEE 802.11a radio. The backbone radio is connected through an RF splitter to two directional antennas pointed towards specific nodes. The network protocol used is the Optimized Link State Routing (OLSR), a link state based protocol designed for ad hoc networks. In the REMOTE's network an OLSR variation is used, the OLSR-ML. This variation uses as cost function the Minimum Loss (ML) metric,which results in routes with minimum error probability in end-to-end communication.

Power module: is formed by a solar power system that comprises a 40 W solar panel, a charge controller and a bank of three 12 V/7Ah lead-acid sealed batteries connected parallel, resulting in a voltage of 12 V and total rated capacity of 21 Ah.

Sensing module: used for site supervision, contains two LM35 temperature sensors, one LDR 5mm light sensor, voltage and current sensors for the solar panel, batteries and primary load (the communication module). It allows monitoring the following physical data of the mesh router: Solar Panel Voltage, Solar Panel Current, Battery Voltage, Communication's Module Voltage, Communication's Module Current, External (ambiance) Temperature, Internal (sealed box) Temperature, Incident Light Intensity, Bytes in/out for each Network Interface, Available Flash Memory, Available RAM memory, CPU Load Average and Link Quality. Instantaneous samples of these data are collected and stored by Mesh Admin every ten minutes.

With the databases formed, a number of well known classification algorithms for the problem were compared, namely Naïve Bayes, Decision Table, k-NN, SVM and C4.5. The result of this evaluation showed that the C4.5 and the SVM algorithms had the best overall prediction performances, with accuracy over 85%. This accuracy level indicates that an

autonomous solution is, indeed, feasible. Their results were brought to a validation test. In this test, the C4.5 presented overfitting characteristics, with poor results when new data was used. While the SVM has shown a good overall performance. An already expected weak point, the Battery Failure detection was identified. This problem was solved using a multi-classification solution - the two classes with higher likelihood of success are presented to the user. With this adjustment, the classifier presented the correct diagnosis (between the two indicated) in all cases and the work was considered satisfactory.

VII. Challenges in fault localization

In [16], fault localization challenges in complex communication systems was discussed and presented an overview of recent techniques. The more recent fault localization research is described in five categories: active monitoring techniques, techniques for overlay and virtual networks, decentralized probabilistic management techniques, temporal correlation techniques, and learning techniques.

ACTIVE MONITORING TECHNIQUES: A probing station is a node in the network that transmits one or more packets called probes for the purpose of monitoring the state of the network. Examples of probes may be ping or traceroute; probes may also be more complex and may be handled by any protocol layer. The use of probes to determine the network behavior or measure the quality of network performance is called probing. Active monitoring techniques use probing for a variety of network management applications. The use of probes helps the NMS to respond more quickly and accurately to the large number of network events, as opposed to the traditional passive event correlation approach. The probes are typically transmitted to obtain end-to-end statistics such as latency, loss, and throughput. These statistics are then used to infer the health of network components. Network parameters and conditions can also be inferred from probe results. Active monitoring techniques have the potential to provide effective solutions for network monitoring applications due to their fundamental end-to-end nature and flexibility in responding to events. However, drawbacks of active monitoring techniques are the invasive character of probes and potentially large overhead. All the necessary tasks required to diagnose a network are addressed in the architecture and are described below.

Probing Station Selection: The task of selecting locations in a network where probing stations should be placed.A minimum requirement of placement is the ability to probe the entire network from the selected probing stations.

Probe Selection: The task of selecting the optimal set of probes after the probing stations have been selected.

This process is divided into two sub-tasks:

Fault Detection: The process of selecting the probes only to detect presence of failures in a network. These probes are few in number and they might not be able to exactly localize faults.

Fault Localization: when a failure is detected, additional probes provide maximum information about the suspected fault area of the network. The probing results are analyzed to localize the exact cause of failure.

Topology Discovery: Exact network topology is required to select probing stations and probes. The network topology can be learned through commands such as ping and traceroute or by using any network discovery agents.

VIII. Traffic engineering (TE)-based machine learning

In [17], a traffic engineering (TE)-based machine learning approach is proposed to detect and localize link failures. Without any topology information and active packets injection to localize a failed link, this machine learning model learn the network traffic behaviour from propagation delay, number of flows and average packet loss at every node in the network both in normal working and failure scenarios. The learning model is trained with machine learning algorithms such as naive Bayes, logistic regression, support vector machine, multi-layer perceptron, decision tree and random forest. The proposed approach is implemented and extensive experiments were carried out using the Mininet platform. The simulation results shows that the machine learning approach localizes link failures with at least 90% accuracy using random forest algorithm while requiring less time-to-localization of a link failure compared to other existing works. Failures are detected if the observed behaviors fail to conform to the predicted ones. Differing from all the above

techniques, the machine learning approach enables a fast fault localization without requiring knowledge about network topology and the previously occurring failures. The TE technique can achieve high accuracy and can adaptively adjusting the learning (fitting) model with new traffic observations, which can be caused by the network dynamics or errors during the data sampling process.

The TE approach has two practical implementations. The first implementation is one in which the end-to-end traffic measurements such as delay and packet loss are monitored by the central server periodically. Frequent the traffic measurement, faster the response if a link failure occurs. The second implementation is the use of an event-driven approach which trigger link fault localization.

When a node experience abnormal behaviours in network traffic, traffic measurements along with a request is sent to the central server for failure localization. Here the machine learning model is trained with the end-to-end traffic observations as the features of the input data at the central server.

For high accuracy of the machine learning algorithms, suitable features of network traffic measurements are required for localizing link failures in the network. At every node in the network, Number of flows that destine to other nodes, Average end-to-end delay and Average packet loss are measured as features. These features are fed to machine learning algorithms as a vector A,all the three traffic measurements are extracted for each aggregate flow.

The learning model, is trained with different machine learning techniques such as naive Bayes, logistic regression, support vector machine, multi-layer perceptron, decision tree and random forest which allows to compare the efficiency of different techniques.

Despite all the methods cited above, obtaining 100% accurate dependency information in an automatic fashion is still an open research problem. The complexity in obtaining dependency information is identifying the fact related to that is a problem that has to be solved separately for every system, layer, or type of device using most of the mentioned techniques.

IX. Conclusions

Fault localization, is the major field of concern in fault management, which exactly identifies the source and node involved in the failure from a set of observed failure indications. Accurate localization of failure is necessary in modern communication systems for fast and reliable recovery. Fault localization is subject to complications resulting from complexity, unreliability, and non-determinism of communication systems. A comprehensive survey of fault localization techniques in communication systems is presented in this paper which are derived from different areas of computer science, including artificial intelligence, graph theory, neural networks, information theory, and automata theory, and include model-based reasoning tools, model traversing techniques, case-based reasoning tools, graph-theoretic approach. The most challenging issues concern multi-layer fault localization, distributed diagnosis, temporal correlation, fault localization in mobile ad hoc networks, and root cause analysis in a service-oriented environment.

REFERENCES

1. Z. Wang, Model of network faults, in: B. Meandzija, J. Westcott (Eds.), Integrated Network Management I, North-Holland, Amsterdam, 1989, pp. 345–352 [68].
2. G. Jakobson, M.D. Weissman, Alarm correlation, IEEE Network 7 (6) (1993) 52–59.
3. J.D. Case, K. McCloghrie, M.T. Rose, S. Waldbusser, Protocol Operations for Version 2 of the Simple
Network Management Protocol (SNMPv2), IETF Network Working Group, 1996, RFC 1905.
4. ISO, Information Processing Systems—OSI, ISO Standard 9596-1: Common Management Information Protocol, Part 1: Specification.
5. W.R. Stevens, TCP/IP Illustrated, vol. I., first ed., Addison Wesley, Reading, MA, 1995.
6. P.H. Schow, The alarm information base: A repository for enterprise management, in: Proc. Second IEEE Internat. Workshop on Systems Management, Los Alamitos, CA, 1996, pp. 142–147.
7. K. Houck, S. Calo, A. Finkel, Towards a practical alarm correlation system, in: A.S. Sethi, F. Faure-Vincent, Y. Raynaud (Eds.),

Integrated Network Management IV, Chapman and Hall, London, 1995, pp. 226–237 [86].
8. A.T. Bouloutas, S. Calo, A. Finkel, Alarmcorrelation and fault identification in communication networks, IEEE Transactions on Communications 42 (2–4) (1994) 523–533.
9. A.T. Bouloutas, S.B. Calo, A. Finkel, I. Katzela, Distributed fault identification in telecommunication networks, Journal of Network and Systems Management 3 (3) (1995).
10. I. Katzela, Fault diagnosis in telecommunications networks, Ph.D. Thesis, School of Arts and Sciences,Columbia University, New York, 1996.
11. M. Klemettinen et al., “Rule Discovery in Telecommunication Alarm Data,” J. Netw. and Syst. Manag., vol. 7, no. 4, Dec. 1999.
12. M. Steinder and A. S. Sethi, “A survey of fault localization techniques in computer networks,” Sci. Comput. Program., vol. 53, no. 2, Nov. 2004.
13. A. Johnsson, C. Meirosu, and C. Flinta, “Online Network PerformanceDegradation Localization using Probabilistic Inference and Change Detection,” in IEEE NOMS 2014, Krakow, Poland, May 2014.
14. L. Bennacer et al., “Optimization of Fault Diagnosis based on the Combination of Bayesian Networks and Case-Based Reasoning,” in IEEE NOMS 2012, Maui, USA, Apr. 2012, pp. 619–622.
15. V. C. Ferreira et al., “Fault Detection and Diagnosis for Solar-powered Wireless Mesh Networks using Machine Learning,” in IFIP/IEEE IM 2017, Lisbon, Portugal, May 2017, pp. 456–462.
16. A. G. Prieto et al., “Toward Decentralized Probabilistic Management,” IEEE Commun. Mag., vol. 49, no. 7, pp. 80–86, Jul. 2011.
17. S. M. Srinivasan, T. Truong-Huu, and M. Gurusamy, “TE-Based Machine Learning Techniques for Link Fault Localization in Complex Networks,” in IEEE FiCloud 2018, Barcelona, Spain, Aug. 2018.