

Prediction of Faults in Cellular Networks Using Bayesian Network Model

Okuthe P. Kogeda and Johnson I. Agbinya++

Department of Computer Science (Center of Excellence for IP and Internet Computing)
University of the Western Cape, Private Bag X17, Bellville 7535, Republic of South Africa.

Email: pkogeda@uwc.ac.za

++Faculty of Engineering (Information & Communication Technology Group),
University of Technology, Sydney, NSW 2007, Australia; agbinya@eng.uts.edu.au

Abstract –Cellular network service providers compete with each other for the vast and dynamic market that is characterized by the ever-changing services on offer and technology. These services require very reliable networks that can meet the customer service level of agreement (SLA). We are motivated by this to model the cellular network service faults and this paper reports on results of faults prediction modelling. Cellular networks are uncertain in their behaviours and therefore we use a Bayesian network to model them. We derive probabilistic models of the cellular network system in which the independence of relations between the variables of interest are represented explicitly. We use a directed graph in which two nodes are connected by an edge if one is a direct cause of the other. We present the simulation results of the study.

Index Terms: Fault Prediction, Bayesian network, Cellular networks, simulation, fault management and services.

I. INTRODUCTION

Network faults can be classified into two groups as malfunctions and outages [1],[2]. Malfunction is said to occur when the active network elements (NE) may be working with some errors in some sense but not well, while outages occur when the active network elements are completely knocked out and do not work at all. Malfunctions are normally characterized by performance degradation in various performance parameters, for example, unclear reception, increase in noise level, increase in delay, etc.

An outage may be clear such that even network users may notice when it has occurred. Its impact on the services being offered can be quantified in monetary terms [1]. In our previous work we related faults to services [1], [2], outlining the vulnerable services to certain faults. This makes the cellular service providers to put in place proactive fault detection [6], [7] mechanisms to avoid these effects.

In this paper, we propose a probabilistic fault prediction modelling that can be used by cellular network service providers that could lead to prevention of the faults before they actually occur. This will lead to reduction in revenue leakage as a result of faults [1]. Cellular service providers may also enhance their chances of maintaining their customers as a result of high quality of service provision. In the long run the cellular service provider improves its revenue earnings and customer base.

This paper is organized as follows. In section II, we give a brief overview of faults prediction in cellular networks. We present faults prediction model in cellular network service providers in section III and faults prediction using Bayesian Network in section IV. We simulate the cellular network

service faults and provide the simulation results in section V and draw conclusions in the subsequent section.

II. OVERVIEW OF FAULTS PREDICTION

The rigorous process of determining what will happen under specific conditions can be referred to as prediction. A telecommunications fault is an abnormal operation that significantly degrades performance of an active entity in the network or disrupts the flow of communication. All errors are not faults as protocols can mostly handle them. Generally faults may be indicated by an abnormally high error rate [1], [2]. Therefore fault prediction is the process of determining which telecommunication fault will occur under certain specific conditions.

In the past few years, some amount of research progress has been made in this area. This includes a classifier training method for anomaly fault detection in [10], use of reinforcement learning for proactive network management in [9] and fault management in communication networks in [11]. While a dynamic Bayesian belief network for intelligent fault management systems in [3] explored ways of applying the Bayesian Belief Network in fault prediction, the paper falls short of explaining how services over the network are likely to be affected with the faults. An intelligent monitoring system using adaptive statistical techniques in [6] can detect faults before they actually occur but do not relate these faults to services. While they apply Bayesian reasoning techniques to perform fault localization in complex communication systems using dynamic, ambiguous, uncertain, or incorrect information about the system structure and state [5], it fails to give a predictive formula. In this paper we present this predictive formula for performing the preventative maintenance of the network.

In our previous publication [4], we proposed probabilistic fault prediction in cellular networks. With the data from a certain communications network service provider, we present more detailed fault prediction models in relation to services in this paper.

Faults prediction brings several advantages to cellular service providers. These include: help in supporting project planning and steering; helps network managers in re-routing of network traffic in case of foreseen problems in a route; network managers can take corrective action before the faults occur, thereby ensuring services reliability and availability over the network; decision making; increases the effectiveness of quality assurance; system quality increases as more faults are found and operations cost will be minimized as faults are found earlier when they are cheaper to repair [6-8 and 12].

The purpose of faults prediction is to enable timely and successful high-level service failures-compromises or proac-

tive failure correction, thereby increasing the chances for proactive error correction before failures set in. This leads to preventative maintenance, which consists of deciding whether or not to maintain a system according to its states, can decrease the cost of maintenance by avoiding overstocking of spare parts and over repairing.

We have used Bayesian network (also called *belief networks*) model to evaluate the probabilities associated with the occurrence of one or more faults, based on the information received from the system under diagnosis. This information is constituted by the alarms generated during the operation of the managed NE, or obtained as a result of previous correlation processes.

III. FAULTS PREDICTION MODEL

A Bayesian network is a directed acyclic graph in which each node represents a random variable (may be *discrete* or *continuous*) to which conditional probabilities are associated, given all the possible combinations of values of the variables represented by the directly preceding nodes. An edge in this graph indicates the existence of a direct causal influence between the variables corresponding to the interconnected nodes. This type of network depends on probability and causal factors, known as *causal Markov condition* [20]. Bayesian networks are also called *causal networks*. Figure 1 shows a Bayesian network for telecommunication network diagnosis.

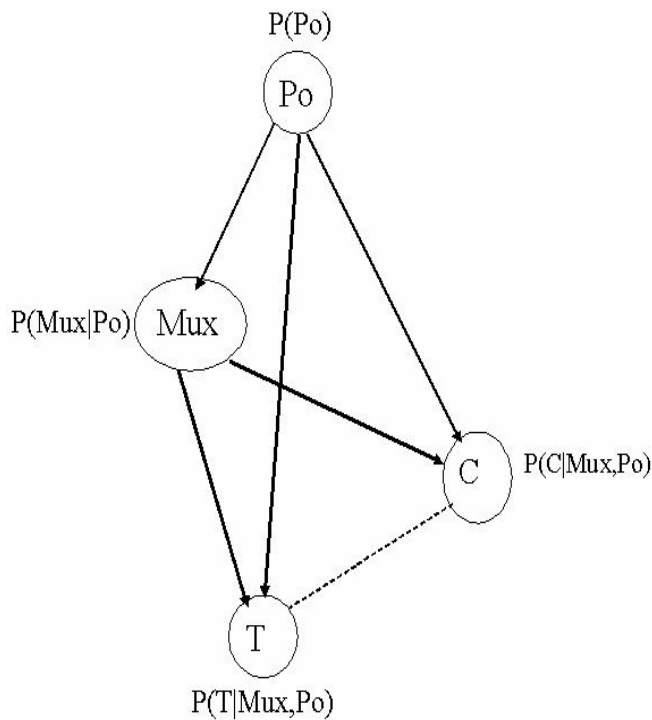


Figure 1: A Bayesian network for cellular network faults diagnosis

A subjective probability expresses the degree of belief of an expert related to the occurrence of a given event, based on the information this person has available up to the moment. We evaluate the conditional probabilities from empirical data obtained from a certain cellular network service provider. The data is about the study of the behaviour shown in the past by the system being studied.

Given a Bayesian network and a set of evidences up to the moment it is possible to evaluate the network, that is, to

calculate the conditional probability associated with each node. Generally speaking, this is a NP-hard problem [13-15] but with the use of appropriate heuristics and depending on the problem dealt with networks containing thousands of nodes may be evaluated in an acceptable time.

The Bayesian Network provides the advantages of [6-8]: mathematical support; robustness; facility for construction; capacity to identify, in polynomial time, all the conditional independence relationships, from the information propagated by the Bayesian network structure; capacity for non-monotonic reasoning, through which previously obtained conclusions may be withdrawn as a result of new information.

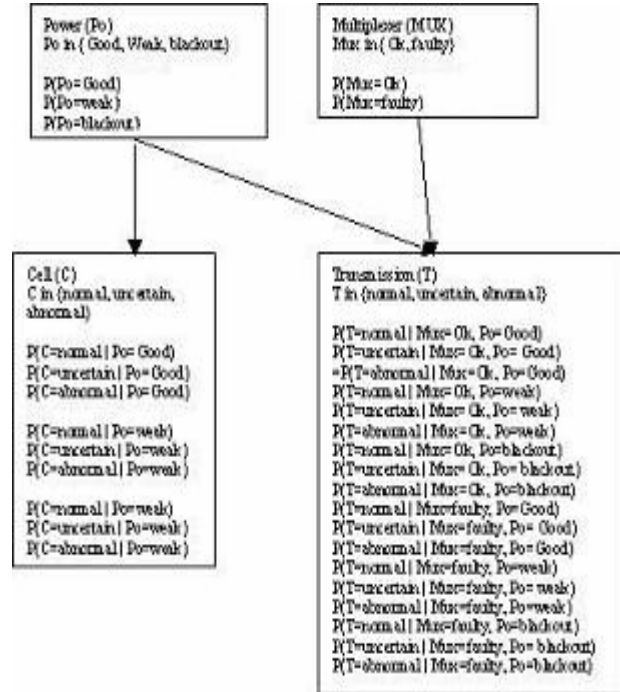


Figure 2: Example of a Bayesian network [4]

Figure 2 shows a Bayesian network of four nodes corresponding to discrete variables of two or three states each. The variables are Power (Po), Multiplexer (Mux), Cell (C) and Transmission (T) with *Good, weak and blackout; Ok and faulty; normal, uncertain and abnormal; normal, uncertain and abnormal* states respectively. However, power can be considered as continuous variable as shown in **Table 1**. Let the probability (P) of event X occurring be denoted by $P(X)$.

Therefore we compute $P(Po)$, $P(C)$, $P(T)$ and $P(Mux)$ equals to 0.36%, 0.42%, 76.57% and 22.63% respectively [1], [2]. We derive *local a posteriori probabilities* [19], for each one of them is conditioned to the occurrence of a certain pattern of values of the direct predecessors of the node. For instance, assuming that multiplexer is ok and power is normal.

The reasons why a cell may not discharge some of its functionalities may include: broken cables and other network elements, natural disaster and planned maintenance [figures 1 and 2]. Nevertheless, the probability that a cell will be in normal state given multiplexer is ok and with the background knowledge that power is in normal state is calculated using;

$$P(C | Mux, Po) = \frac{P(C | Po) * P(Mux | C, Po)}{P(Mux | Po)} \quad (1)$$

Where:

$$P(Mux | Po) = \int P(Mux | C, Po) * P(C | Po) dC \quad (2)$$

$P(Mux|Po)$ is the likelihood function.

The joint probability distribution $P(x_1, x_2, \dots, x_n)$ for a Bayesian network may be obtained through the product of the *local probability distributions* [16] for each random variable. For example, the Bayesian network of figure 2 in which the joint distribution $P(Po, Mux, C, T)$ may be calculated as;

$$P(Po, Mux, C, T) = P(Po) * P(Mux) * P(C | Po, Mux) * P(T | Mux) \quad (3)$$

Therefore if one knows a set of evidences

$e = \{X_m = x_m, \dots, X_p = x_p\}$, constituted by all the known values of the random variables of a Bayesian network, where $\{X_m, \dots, X_p\} \subset X = \{X_1, X_2, \dots, X_n\}$, the calculation of the probability (or ‘belief’) that a variable $X_k \notin \{X_m, \dots, X_p\}$ assumes the value x_k is given by

$$P(X_k = x_k | e) = \frac{P(X_k = x_k) * P(e | X_k = x_k)}{P(e)} \quad (4)$$

Let us take a Bayesian network for a set of variables $X = \{X_1, \dots, X_n\}$, which consists of a network structure S that encodes a set of conditional independence assertions about variables in X , and a set P of *local probability distributions* [16] associated with each variable. Together, these components define the joint probability distribution for X . The network structure S is a directed acyclic graph. The nodes in S are in one-to-one correspondence with the variables X . We use X_i to denote both the variable and its corresponding node, and Pt_i to denote the parents of node X_i in S as well as the variables corresponding to those parents. The lack of possible arcs in S encodes conditional independencies. In particular, given structure S , the joint probability distribution for X may also be given by the equation below:

$$P(X) = \prod_{i=1}^n P(x_i | pt_i) \quad (5)$$

The distributions corresponding to the terms in the product of Equation 5 are local probability distributions P . The pair (S, P) encodes the joint distribution $P(x)$. We learn the networks from data and therefore the probabilities will be physical and their values may be uncertain [19].

To illustrate the above derivations, we use the Bayesian network of figure 2. Supposing that $e = \{T = abnormal\}$ is the set of all the known evidences, the belief that the power is good is given by:

$$P(Po = Good | T = abnormal) = \frac{P(Po = Good, T = abnormal)}{P(T = abnormal)}$$

$$P(Po = Good | T = abnormal) = \frac{0.3815}{0.3828} = 0.9966 \approx 99.66\%$$

This example demonstrates the capacity for non-monotonic reasoning of the Bayesian networks [8], [12] and [17], while the only known evidence was that the transmission was abnormal, the belief that the power was good was 99.66%. As it is known that the multiplexer was faulty, we recalculated the belief with a higher value of 99.68% being gotten. This belief grew with the new revelation that the Cell was found to be in normal state was made available. Our calculation brought a higher value of 99.71%.

IV. FAULT PREDICTION USING BAYESIAN NETWORK

For each variable of a Bayesian network some states corresponding to faults may be defined, whose probability will be evaluated during a diagnosis session. This would be the case, for example, of the states $Po = blackout$, $Mux = Ok$, $T = Normal$ and $C = Uncertain$ in the network of Figure 2.

Any variable of a Bayesian network may also be defined as an observation node, if its state is possible to be observed during a diagnosis session. These variables would be capable of providing information on when a fault may occur according to the probability observed. It must be pointed out that a node may be an observation one at the same time as the corresponding variable may contain fault states.

Fault prediction in a Bayesian network consists of the evaluation of the probabilities associated with the occurrence of one or more faults, based on the information received from the system under diagnosis. This information is basically constituted by the alarms generated during the operation of the managed network elements, or obtained as a result of previous correlation processes.

A. Uncertainty causing factors

Strictly speaking, for any type of fault prediction that is considered, the set of alarms data to be considered will always be subject to errors and omissions. Such errors and omissions may be generated both in the network element responsible for the original fault as in elements situated in other points of the managed network, they may also be caused by communication failures or by the network management system itself. Besides that, the simultaneous occurrence of two or more faults may generate an alarm pattern that is characteristic of a fault that has not occurred, thus inducing the alarm correlation system to error. We may conclude, therefore, that uncertainty is inherent to any alarm correlation process where we got our data.

The main uncertainty-causing factor as it is inherent to the correlation process is due to error possibilities, which has four main sources. These include:

1. The influence of factors not captured by the managed system model.
2. The imprecision in the attribution of values for the probabilities distributions
3. The imprecision in the capture and transference of the alarms. This may be illustrated even in simple systems such as the one of Figure 2, where errors may occur both in the observation of the power voltage, due to the difference in the reading of the power voltage, due to errors in the voltmeter operation or to a defect of the network element itself.
4. Imprecision in the information obtained as the result of other correlation processes.

B. Markov chain method

This method was named after Andrei Markov and is a discrete-time stochastic process with the Markov property. In such a process, the past is irrelevant for predicting the future given knowledge of the present. A Markov chain is a sequence X_1, X_2, X_3, \dots of random variables. The range of these variables, i.e., the set of their possible values, is called the *state space*, the value of X_n being the state of the process at time n . If the conditional probability distribution of X_{n+1} on past states is a function of X_n alone, then:

$$P(X_{n+1} = x | X_0, X_1, X_2, \dots, X_n) = P(X_{n+1} = x | X_n) \quad (6)$$

Where x is some state of the process. The identity above identifies the Markov property.

Table 1: An imagined Database for the Cellular faults

CASE	Power	Multiplexer	Cell	Transmission
1	240 – 3000	Ok	N	N
2	190 – 240 & >3000	faulty	U	N
3	<190	Ok	A	A
4	<190	faulty	N	U
5	240 – 3000	faulty	A	N
6	<190	Ok	U	U
7	190 – 240 & >3000	Ok	U	A
8	190 – 240 & >3000	faulty	A	N
9	240 – 3000	Ok	N	A
10	240 – 3000	faulty	N	U

V. FAULTS SIMULATION

In order to investigate the performance of the models we have developed so far, we carried out extensive simulation experiments under various conceivable cellular network environments. Some of these include: different power supply behaviour, typical background traffic, and anomaly transmission characteristics.

In this section we give an overview of fault simulation. Categories of simulation techniques are explored in the following section. We give preliminary simulation results and lastly analysis of the results.

A. Overview of fault simulation

Simulation is the representation or imitation of a process or system by another device. In a test environment, a simulator can be used in place of a network element or a part of the network to produce desired conditions. For instance, when testing a Radio Network Controller (RNC), the test equipment can simulate the Core Network (CN) behaviour, keeping the RNC independent of the network. Simulators are used to do the following:

- To get information about the dependability of a network element (NE); normal and abnormal situations are specified and simulated, and the NE's ability to cope

with the simulated environment allows the operator to predict how well the NE will perform in the field; simulations are also used for conformance testing where standardized conditions are applied to the NE.

- To substitute missing network elements or parts of a network during the development process; simulation creates a realistic operating environment for the item under development.
- To save development and installation costs; the strong and weak points of an item can be discovered in the development process, before introducing it to an operating network.

B. Categories of Fault Simulation

Fault models are categorized as logical and delay. Logical fault models can be structural or functional, permanent or intermittent, single or multiple. Delay fault models can be transport or inertial. Transport delay fault model can be further divided into unity delay, transition-independent delay, ambiguous delay fault model or nominal delay fault model.

Our main focus in this work is stuck-at structural faults. Saboteurs or mutants perform fault injection methods [21]. A saboteur is a model of a component instantiated in the original circuit that is added to a circuit to cause a fault. Saboteurs can be simple serial, complex serial or parallel. Mutant of a model is a faultable model resulted from a transformation of the original model. A mutant is made by adding saboteurs to descriptions, replacing subcomponents, generating wrong operators or manually modifying the original model. The mutant method is generally more abstract than the saboteur.

Fault Simulation techniques are categorized as: serial, parallel, deductive and differential fault simulations. The use of a particular technique depends on task and type of the devices to be simulated. For instance, fault simulation for combinational circuits may be done by the above techniques or parallel-pattern single-fault propagation or critical path tracing technique.

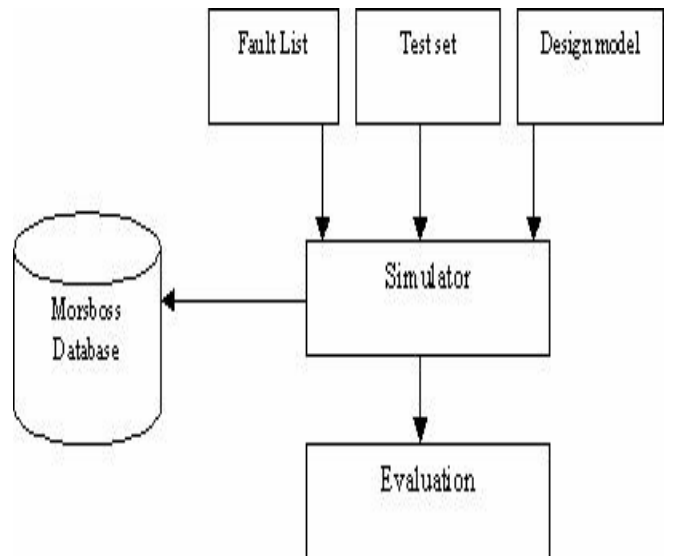


Figure 3: Fault simulation flow diagram

A fault simulator needs in addition to the circuit model, stimuli and expected responses (that are needed for true-value simulation as shown in Figure 3), fault model and fault list. The proposed fault simulation flow [figure 3] con-

sists of design model, test set and fault list all being input to simulator. The simulation process takes place inside the simulator with evaluation of results and data being stored in Morsboss database. The fault simulator must classify the given target faults as *detected* or *undetected* by the given stimuli.

Let detected faults be D , detectable faults be D_f and faults coverage be F_c . We compute the fault coverage using:

$$F_c = \frac{D}{D_f} \quad (7)$$

One of the great strengths of simulation modeling is the ability to model and analyze the dynamical behavior of a system. This makes simulation an ideal tool for analyzing the telecommunication faults, which exhibit very complex dynamical behavior.

C. Preliminary simulation results

We used Bayesian network and statistical analysis models, which bases its calculations on probability density function (PDF) algebra. The use of PDFs is more informative and allows for flexibility than using isolated values or perhaps their averages [10]. We sampled four variables (faults) in our simulation experiment. Power as one of the faults in the cellular network under study is a continuous variable. Figure 4 shows the PDFs of power as a network fault, which represents the distribution of voltage of power observed during a time window. The uniform percentile partitioned into 42 Bins is shown in Figure 5.

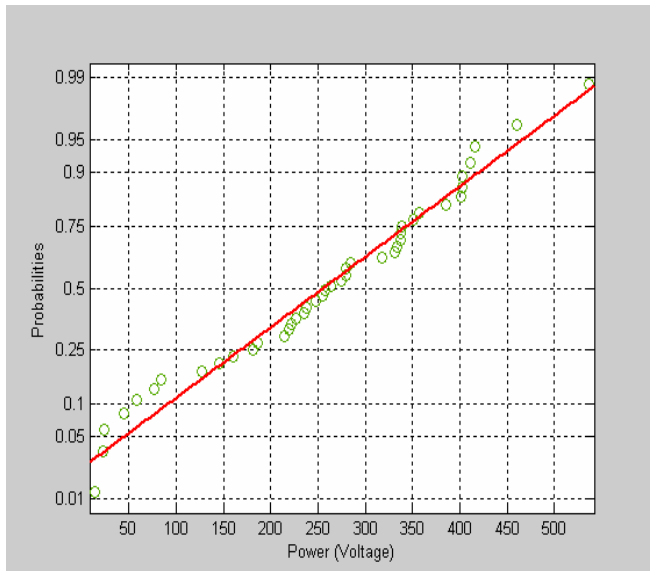


Figure 4: PDF of Power as Network fault

We simulated a cellular network service provider fault conditions by injecting various volumes (i.e., voltage incase of power) or conditions of each of the four variables into the simulation testbed. Specifically, in the test network, a network element (NE) is assumed to be faulty, either when there is excessive power supply leading to its damage (though most NEs have power stabilizers) or when power supply is less than required voltage (assumed in this study to be 240Volts). We assume [as in Figure 1] that power is the parent node of all the variables. Therefore, incase of power

failure the other NEs are bound to malfunction or fail as well.

As mentioned above, we carried out extensive simulation experiments. The purpose of the experiment is to ascertain and give some predictive expression of faults as they occur in a cellular network service provider. The combination of different variables for these simulation experiments is given in Table 1. The data sets collected are used to estimate fault models and to simulate fault data for various scenarios of a cellular network service provider.

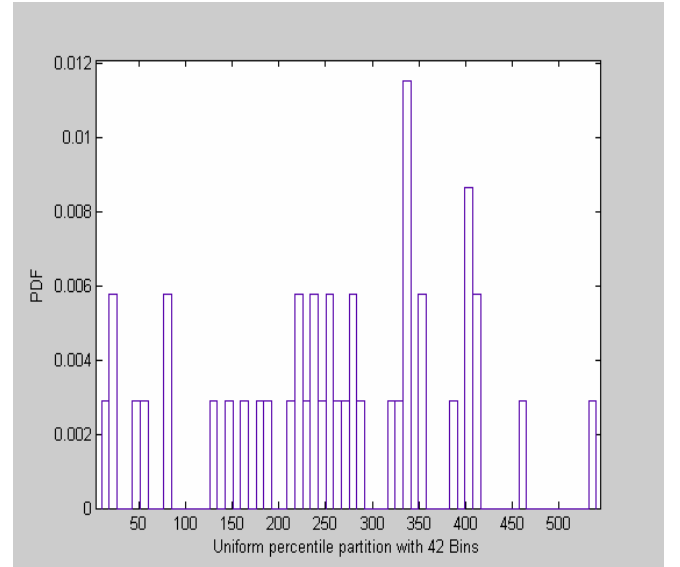


Figure 5: PDF of power

D. Analysis of results

The actual data from a certain cellular network service provider are used for training datasets. The results are used as the base because they are the best that can be achieved for the actual cellular service provider network. The generated PDF data are used for training purposes, while the actual data are used for testing.

The results of the experiments are shown in Figure 6, where the x-axis is the false alarm rate and the y-axis is the detection rate. In our experiments the false alarm rate is the rate of the typical variable being classified as faults or anomalies, while the detection rate, is calculated as the ratio between the number of correctly detected faults or anomalies to their total number (refer equation 7).

From the simulation experiments, we observe that there is little difference in actual data and simulated environments results. This gives us confidence that this model can work under real environments and it can be used to predict network faults with the confidence level of 99.8%.

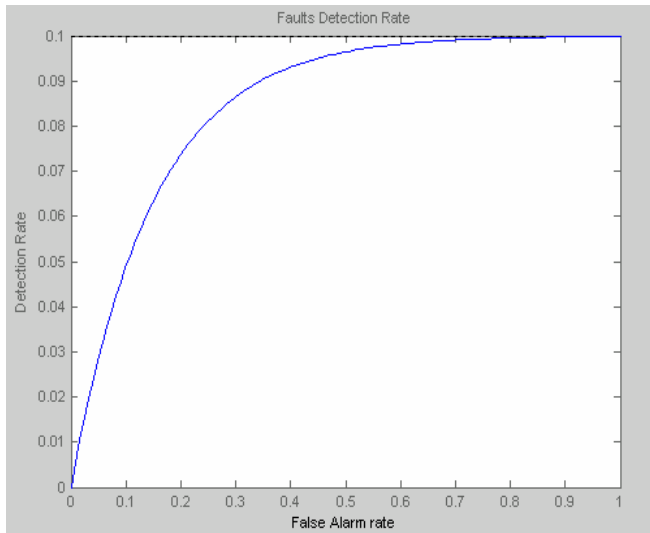


Figure 6: False Detection Rate

VI. CONCLUSION

Probabilistic fault prediction models were presented. The simulation results were presented with further research to be conducted on the accuracy of the models presented. Different environments will be studied with services being affected as well being simulated.

VII. ACKNOWLEDGEMENT

Okuthe P. Kogeda would like to thank the National Research Foundation, South Africa for the financial support that has made this work possible.

VIII. REFERENCES

- [1] Okuthe P. Kogeda, Johnson I Agbinya and Christian W. Omlin, "Impacts and Cost of faults on Services in Cellular Networks", Proc. IEEE International conference on Mobile Business, Sydney, Australia, 11 - 13 July 2005, pp. 551 - 555.
- [2] Okuthe P. Ogeda, Johnson Agbinya and Christian Omlin, "Faults and Service Modeling for Cellular Networks", SATNAC 6th -8th September 2004, page 369-370, Cape Town, South Africa.
- [3] Sterritt, R; Marshall, A H; Shapcott, C M; McClean, S I; *Exploring dynamic Bayesian Belief Networks for intelligent fault management systems*; PROC IEEE INT CONF SYST MAN CYBERN. Vol. 5, pp. 3646-3652. 2000
- [4] Okuthe P. Kogeda, Johnson I. Agbinya and Christian W. Omlin, "Probabilistic Faults Prediction in Cellular Networks", Proc. SATNAC 11th - 14th September 2005, Drakensberg, South Africa.
- [5] Malgorzata Steinder, Adarshpal S. Sethi, "Probabilistic Fault Localization in Communication Systems Using Belief Network", IEEE/ACM Transactions on Networking, vol. 12, no. 5, October 2004.
- [6] Cynthia S. Hood and Chuanyi Ji; *Proactive Network Fault Detection*; In Proceedings of the IEEE INFOCOM, Kobe, Japan, April 1997.
- [7] Cynthia S. Hood, Chuanyi Ji, "Automated proactive anomaly detection" Proceedings of the fifth IFIP/IEEE international symposium on Integrated network management V: integrated management in a virtual world: integrated management in a virtual world, San Diego, California, United States, pp. 688-699, 1997.
- [8] Cynthia S. Hood, Chuanyi Ji. "Intelligent Agents for Proactive Fault Detection," *IEEE Internet Computing*, vol. 02, no. 2, pp. 65-72, March/April 1998.
- [9] Q. He and M.A. Shayman, "Using Reinforcement Learning for Proactive Network Fault Management," *Proceedings of the International Conference on Communication Technologies*, Beijing, PR China, August 2000.
- [10] Jun Li, Manikopoulos C.; "Network fault detection: classifier training method for anomaly fault detection in a production network using test network information"; *Local Computer Networks*, 2002. Proceedings. LCN 2002. 27th Annual IEEE Conference on 6-8 Nov. 2002 Page(s): 473 - 482.
- [11] Mark A. Shayman and Emmanuel Fernandez-Gaucherand, "Fault Management in Communication Networks: Test Scheduling with a Risk-Sensitive Criterion and Precedence Constraints", IEEE Conference in Decision and Control, Sydney, Australia, December 2000.
- [12] Danyluk, A. and F. Provost, "Telecommunications Network Diagnosis", In W. Kloesgen and J. Zytow (eds.), *Handbook of Knowledge Discovery and Data Mining*, 2002
- [13] Irina Rish, Mark Brodie, Natalia Odintsova, Sheng Ma, Genady Grabarnik, "Problem Diagnosis in Distributed Systems using Active Probing", UAI-2003 workshop on Bayesian Modeling Applications, August 2003, Acapulco, Mexico.
- [14] G. F. Cooper, "The computational complexity of probabilistic inference using Bayesian belief networks", *Artificial Intelligence*, 42:393-405, 1990.
- [15] Eugene Charniak, "Bayesian networks without tears", *AI Magazine*, (Winter 1991): 50 - 63, 1991.
- [16] D. Heckerman, "A tutorial on learning Bayesian networks", technical report MSR-TR-95-06. Technical report, Microsoft Research, 1995.
- [17] C. S. Chao, D. L. Yang, and A. C. Liu, "An automated fault diagnosis system using hierarchical reasoning and alarm correlation," *J. Network System Manage.*, vol. 9, no. 2, pp. 183-202, 2001.
- [18] R. Dechter, "Bucket elimination: A unifying framework for probabilistic reasoning", In M. I Jordan (Ed.), *Learning in Graphical Models*, Kluwer Academic Press, 1998.
- [19] David Ackerman, "A Tutorial on Learning With Bayesian Networks", Technical Report MSR-TR-95-06, March 1995.
- [20] Spirtes, P., Glymour, C., and Scheines, R., "Causation, Prediction, and Search", Springer-Verlag, New York 1993.
- [21] S.A. Aftabjahani, Z. Navabi. "Functional Fault Simulation of VHDL Gate Level Models," *viuf*, p. 18, 1997 VHDL International User's Forum (VIUF '97), 1997.