Operational Fault Detection in Cellular Wireless Base-Stations

Sudarshan Rao, *Member, IEEE*

***Abstract*— The goal of this work is to improve availability of operational base-stations in a wireless mobile network through non-intrusive fault detection methods. Since revenue is generated only when actual customer calls are processed, we develop a scheme to minimize revenue loss by monitoring real-time mobile user call processing activity. The mobile user call load profile experienced by a base-station displays a highly non-stationary temporal behavior with time-of-day, day-of-the-week and time-of-year variations. In addition, the geographic location also impacts the traffic profile, making each base-station have its own unique traffic patterns. A hierarchical base-station fault monitoring and detection scheme has been implemented in an IS-95 CDMA Cellular network that can detect faults at – base station level, sector level, carrier level, and channel level. A statistical hypothesis test framework, based on a combination of parametric, semi-parametric and non-parametric test statistics are defined for determining faults. The fault or alarm thresholds are determined by learning expected deviations during a training phase. Additionally, fault thresholds have to adapt to spatial and temporal mobile traffic patterns that slowly changes with seasonal traffic drifts over time and increasing penetration of mobile user density. Feedback mechanisms are provided for threshold adaptation and self-management, which includes automatic recovery actions and software reconfiguration. We call this method, Operational Fault Detection (OFD). We describe the operation of a few select features from a large family of OFD features in Base Stations; summarize the algorithms, their performance and comment on future work.**

***Index Terms*— Statistical fault detection, cellular, wireless, base-stations, static and adaptive thresholds, training, learning.**

I. Introduction

This paper describes practical applications of a statistical framework to detect faults in distributed cellular wireless base-stations which have been widely deployed in the field. As reliance on wireless cellular networks become increasingly prevalent as the primary form of communications, the reliability and availability expected of the wireless services increases. Fault detection is necessary for a Service Provider to know that an installed wireless system is capable of providing the service planned for the End User. Modern wireless systems, although designed, manufactured and installed to the highest standards, can from time to time fail to provide the expected capabilities. The Service Provider needs fault detection capability to detect the fault as soon as possible in order to restore the system to full capability with a minimum loss of revenue. The system may reduce the outage time for many faults by the use of automatic recovery, which restores the system without technician intervention. Whether recovery is done automatically by the system or manually by the technician, however, fault detection capability is needed to initiate the process to correct the fault. Otherwise the fault condition continues unnoticed. Radio-Frequency (RF) fault detection capability focuses on the RF aspects of fault detection as contrasted with the switching aspects of fault detection, which applies more directly to the Mobile Switching Center (MSC).

Another aspect of the maintenance strategy is that mobile customers sometimes play a role. If faults are not detected by the system, customers may eventually report them. If the customers report faults, then the customers perceive that the system has poor quality for a limited time. If mobile customers do not report the faults, the service providers continue to lose revenue and the mobile customers also perceive continuing poor quality. An objective is to have the system report faults before mobile customers do.

Availability and reliability are important measures of a functional cellular network, from a service providers view point. If a network is unavailable for service or provides degraded service, revenue is lost. High availability requires very short downtimes. Downtimes may be due to pre-planned maintenance activities or caused by faults. In either case, end user mobile customer perception is one of service unavailability. The primary goal of fault management is the restoration of services in the presence of faults [1]. Reliability is measured by the mean-time-to-failure (MTTF), while fault management is characterized by mean-time-to-repair or restore (MTTR) services.

Building highly reliable systems with redundancies are expensive and leads to high capital expenditures (CAPEX) by service providers. At the same time, keeping network availability high is crucial from a customer satisfaction perspective. Keeping the operational expenses (OPEX) low will require high reliability systems and/or early and robust fault management systems to keep unavailability extremely low. The overall cost to the service provider includes both CAPEX and OPEX. For more information about availability calculations and the impact of traffic models on availability the reader is referred to [2]. With increasing competition, high availability at affordable cost has become a very important market driver. The pressure to keep capital expense (CAPEX) low while keeping reliability and availability high only increases with time.

In the wireless industry, the complexity of the network is higher than its wire-line counter part. Cellular mobile communications systems are complex interconnections of hardware and software that are prone to unforeseen faults and errors. Mobile users with their handsets communicate with a base-

Manuscript received February 1, 2005; revised February 2, 2006.

S. Rao is with the Radio Access Network Systems Engineering and Architecture Dept., Lucent Technologies Inc., Whippany, New Jersey, USA (e-mail: sarao@lucent.com).

station via radio-frequency (RF) links. Causes of faults could be hardware failures, software errors and bugs, environmental causes such as storms, tornadoes, hurricanes etc causing external base-station equipment such as antennae, cabling and other RF hardware being affected. Increasingly, the major contributor of faults in these complex systems are software faults, unlike in the past when hardware faults dominated.

The number for base-stations are growing rapidly, with every service provider adding additional coverage areas to stay competetive. Based on approximate estimates from the major and smaller service providers in North America (US and Canada), there are over over 80,000 currently deployed, and are distributed geographically over a very wide area of the continent. Due to the nature of the wireless links and the harsh outdoor environment in which the base-stations are deployed, the fault scenarios are numerous and will require complex and sophisticated fault detection, isolation and recovery schemes. The "universe" of all possible faults may not be known. It would be far too costly to induce all possible faults to simply collect the data. A reliable system must be able to detect problems it has never before observed. The Service Provider needs to detect faults in the RF portion of a wireless system in order both to provide the level service to End Users that the system is capable of and also to generate the revenue planned.

Fault management in base-stations is achieved via numerous methods: Board Level Self Tests, Software Error Handlers, Heart-beat mechanisms, Hardware alarms, Functional tests etc. These do not provide a hundred percent fault coverage. Besides, these mechanisms catch known fault scenarios. In addition, network operators may invest in special purpose hardware, which include technology specific signal sources and detectors, to test the functionality of the base-stations periodically or on-demand. These special purpose hardware are, generally, very expensive to install into each base-station and may have to be changed or updated as the air-interface technology changes. In addition, many of these solutions are intrusive in nature, requiring service interruption during testing.

There are trade-offs between OPEX reduction and CAPEX reduction. In an attempt to reduce both costs, we have developed a family of non-intrusive and inexpensive software based fault surveillance mechanism, referred to as operational Fault detection (OFD).

Operational Fault Detection is a new approach to RF fault detection for wireless systems and consists of a number of independent tests. The goal of OFD is to reduce unplanned downtimes caused by faults through non-intrusive fault detection methods. OFD includes a family of statistical algorithms, which is a combination of parametric, semi-parametric and non-parametric statistical models.

OFD is an extension of, and alternative to, the traditional engineering approach of fault detection. In the traditional engineering approach faults are detected by hardware or software features specifically designed for the purpose. A high temperature alarm using a temperature sensor is one example. A software routine that repeatedly executes so that its result can be compared with the known result is another example; if the result of the routine differs from the known result, a fault is indicated. The traditional engineering approach identifies deviations in the system functions from the design. OFD identifies deviations in the system operation from that expected. An example of an OFD approach to fault detection in an early type of telephone switching offices is the technician noticing that the noise had stopped. Crossbar switches generate noise when the contacts open and close, and the technician can tell that the telephone office stopped functioning when the noise stopped. It is certainly possible, but highly unlikely, that suddenly no telephone user chose to make a call; the only reasonable possibility if the noise stops suddenly is that there is a fault. There has, however, been no detection of the fault made by an engineering type test.

The emphasis, and the main contributions, of this paper is on practical application of statistical fault detection techniques in CDMA base-stations. CDMA in this paper includes cellular (IS-95), PCS (ANSI J-STD-008) and 3G (IS-2000 1X)[3] [4]. The methods described are applicable to other technologies as well, with suitable modifications. Applications of statistical methods to UMTS [5], using an approach based on statistical bounds on extreme deviations from the average behavior, is described in [6]. This paper, in contrast, exploits known parametric distributions where available, and on extreme value analysis where the underlying distributions are not known.

In this paper, Section II presents a brief description of a wide-area cellular network. Section III reviews fault management steps, the key challenges to managing cellular networks, a hierarchical fault monitoring scheme and statistical Fault Detection framework for different levels of base-station hierarchy, and also provides context to our work as well as related work. Section IV provides a description of carrier and channel level fault detection, the lowest level in the logical base-station hierarchy. Section V describes sector fault detection, the next higher level in the hierarchy, which is an aggregation of all the RF carriers and channles contained within that sector. The highest level is the detection of an outage of the entire base-station is described in section VI. Section VII provides a summary with a discussion of the strengths and shortcomings of methods reported in this paper, work on other OFD features and future work to improve upon existing implementations.

II. Cellular Network System Model

This section provides a brief description, of a generic macro-cellular base-stations most commonly deployed in the second and third generation voice and data networks. Fig. 1 shows a set of geographically distributed radio towers providing RF coverage for cellular services. The base-stations communicate with a base Station Controller (BSC). A collection of BSC's in turn communicate with an Mobile Switching Center (MSC). The MSC, and sometime a BSC, is connected to other network elements providing specialized services and interconnections, such as security, authentication, billing, location management, voice, video, data, e-mail, internet access etc. Macro-cells refers to base-stations which have wide-coverage areas, typically in the range of a few kilometers, as opposed to micro-cells which may provide only a very small foot print of a several hundred feet. Mobile terminals communicate with the base-stations via wireless RF links. A base-station in turn is organized in a hierarchical manner. Each base-station may contain multiple sectors. The number can range from one to

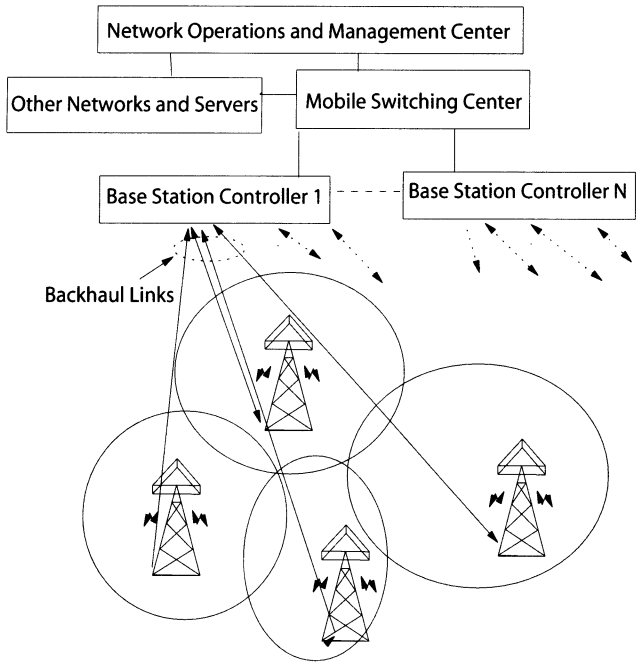

Fig. 1. A typical cellular network architecture.

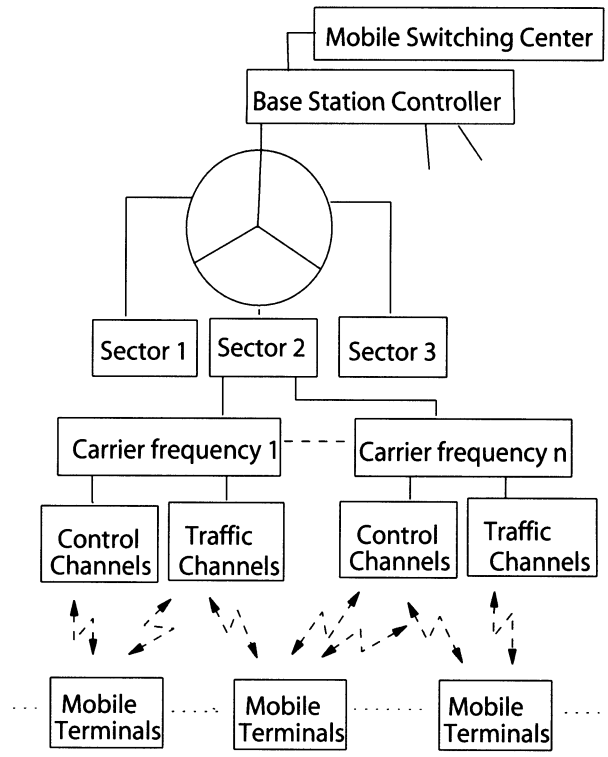

Fig. 2. Logical cellular network hierarchy.

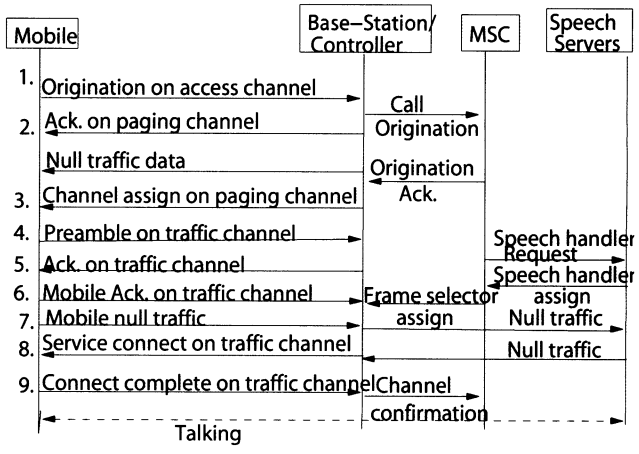

Fig. 3. A simplified call set-up scenario.

many (up to six). However, the most prevalent macro-cells deployed contain three sectors. Directional antennas allow each sector to provides RF coverage to well defined areas. Each base-station coverage area or each sector coverage area may be configured to handle to expected traffic. Specifics of RF capacity and coverage design and optimization can be found in [7].

Fig. 2 shows a base-station organized logically in a hierarchical structure. Each base-station may be divided into multiple sectors. Each sector in turn may contain multiple CDMA RF carriers or frequencies allocated to carry mobile user communications. Depending on the mobile user density in a particular area being served by a sector, the number of carrier may be more or less. Each CDMA carrier is, in turn, composed of control channels and traffic channels. Control channels provide signaling information to mobile terminals for setting up voice or data calls, maintaining calls as they move from the coverage area of one base-station to another and terminating calls. Traffic channels are allocated to for carrying actual mobile user communication, either voice, or data. Depending on the service requested, more than one traffic channel may be allotted.

A very simplified call set-up process of a typical IS-95 based CDMA is shown as a sequence of steps in Fig. 3. The first step is for a mobile to listen to broadcast system parameters and tune in. The mobile terminal sends a service request on the system access channel. The base-station checks if resources are available and responds with traffic channel resource information on the paging channel to the mobile terminal. The mobile then tunes to specified traffic channel and beings communication.

In the call set-up steps discussed above, the availability of the control channels and traffic channels are crucial. The absence or degradation of any one of the channels, due to a fault, will result in service degradation (soft faults) or, in some cases, a hard fault indicative of complete loss of communication. As discussed previously, the cause of faults could be due to hardware malfunction or software faults.

The key parameters that OFD monitors are the call processing activity, which generates revenue for service providers, on each of the control and traffic channels to determine the health of the base-station. The precise description and measures of health and faults will be developed in the subsequent sections. The next section describes the steps taken in fault management, with an emphasis on fault detection.

III. Fault Management Steps

Fault Management, one of the management functional areas (MFAs) of the Telecommunications Management Network (TMN) Recommendations [8], minimizes the adverse effect of faults.

The TMN Recommendations are published by the International Telecommunications Union – Telecommunications Standardization Sector (ITU-T). The other TMN functions are: Security Management, Performance Management, Accounting Management, and Configuration Management.

Fault Management is also known the maintenance part of Operations, Administration and Maintenance (OA&M) [1]. The key elements in fault management are: fault prevention, fault detection, fault localization and isolation, fault repair and restoration. The focus of this paper is, primarily, in the detection step.

The primary adverse effect of a fault in a base-station is to decrease its capacity to support traffic. Effective Fault Management will reduce this adverse effect and therefore maximize the revenue generated. Detecting faults quickly, restoring service on an interim basis by software recovery, and completely repairing the fault as soon as possible reduces the adverse effect of faults in base-stations.

Invasive tests reduce capacity, so that non-invasive test are preferred over invasive tests. Several aspects of Fault Management contribute to the cost to restore a fault, which are explored next.

A. Fault Detection

While every effort is made to prevent faults by designing robust networks and through maintenance, it cannot be avoided totally. Fault detection is, therefore, a crucial step in the fault management process. In the context of this paper, faults are defined as any hardware or software failures that would stop or significantly degrade call processing service on a single carrier or sector or the entire base-station.

The types of failures in a base-station or myriad. Hardware breakdowns such as transmit amplifiers, receive amplifiers, radio failures; software bugs and failures causing abnormal system behavior; overload conditions; environmental effects such as rainfall, tornadoes, storms, winds, snow and icing which may lead to antenna failures, corrosion in cabling, Power outage, large external RF signal jamming etc. Depending on the type of failure, the corresponding effect or fault may be contained to within a carrier, or may propagate to the entire sector outage and in some rare cases the entire base-station may be down. For example, if in a CDMA base-station there is only one carrier and the radio that supports a pilot channel of a sector fails, the entire sector becomes inoperable. Other sectors of the base-station, however, are not affected by the fault and the fault might not be noticed for some time.

There are both hard, or complete, faults and soft, or intermittent faults or degradations to be detected. Hard faults are easier to detect than soft faults and therefore usually detected first. It is more important to detect hard faults because hard faults cause more loss of revenue. Soft faults are important to detect also because they also lower quality and cause loss of revenue. If not detected soft faults are continuing costs.

The algorithms described in this paper declare faults based on observing events related to various mobile call load activity. The primary events monitored for the algorithms discussed in this section are mobile access channel activity, paging channel activity and traffic channel activity at various levels of hierarchy and aggregation.

1) Statistical Framework: OFD includes a family of statistical algorithms, which are a combination of parametric, semi-parametric and non-parametric statistical models. Only a few select set of implemented OFD algorithms, are described in the current paper.

The presence or absence of a fault, given the set of observations is posed as a statistical hypothesis test.

Null hypothesis, H_0 : No Fault
Alternative hypothesis, H_1 : Fault

The results could be:

The null hypothesis is not true, and an extremely unlikely event (Fault) occurred, or the null hypothesis is true (No Fault).

Two types of errors may happen in fault reporting:

- Declaring a Fault when there is no Fault, usually called "False Positives" or "False Alarms" or Type I Error.
- Not Declaring a Fault when there is a Fault, also known as "Missed Faults" or "False Negatives" or Type II error.

Each error type incurs costs to the network administrator, and is described below:

Costs associated with Type I Errors: An appreciable false alarm will result in unacceptable costs to the Service Provider. Technicians may have to travel large distances to get to the affected base-stations with spare parts. These costs are technician time, replacement parts and the loss of revenue when a cell or parts of a cell are taken out of service for testing and diagnosis during "unnecessary" repair. A perceived high false alarm rate will likely cause the Service Provider to delay responding to an alarm due to loss of confidence in the fault reports. Extremely low false alarm rates are desirable.

Costs associated Type II Errors: It is also desirable to rapidly detect a high proportion of faults. Otherwise mobile customers will detect faults before the system does, leading to customer dissatisfaction. A consequence of this type of error is a reduction in quality as perceived by mobile customer and loss of revenue due to missed faults.

These errors in fault detection usually arise from improper threshold settings. Thresholds for detecting faults will be initially set through analysis of the commonality of traffic on the sectors and statistical analysis. Statistical analysis will be a guide to construct the algorithm to balance the possibility of false positives (declaring a fault when there is no fault) against the sensitivity of the test (not declaring a fault when there is a fault). Since false positives are a particular concern because of the high cost of attempting to repair a fault that does not exist, an objective for false positives will be a very low rate.

If we want to minimize both the false alarm rate and the time to detect faults, then the complexity of algorithms increases. Most of the resources in a base-station are reserved for revenue generating call processing with monitoring and maintenance functions being provided lower priority. It is, therefore, extremely important that we have light weight algorithms requiring very low memory costs, message communication costs and computational complexity for fault detectors, since these are performed locally at each base-station.

The application of different statistical fault detection methods in wired networks and services have been presented in

many studies. [9] describes algorithms and implementation for transaction oriented services on AT&T network. IP router fault detection, and experimental results based on application of a statistical GLR test on piece-wise stationary AR(1) models to selected SNMP MIB variables in an IP networks is described in [10] [?].These algorithms are tailored to short time scale dynamics (on the order of 15 seconds to less than a few minutes) of IP networks. The data for performance analysis was obtained from production networks. However the complexity of automating such schemes to run in real time on all IP routers, without human intervention is not clear. The models and implementations are not directly applicable to wireless network due to, either, their computational complexity or memory needs. Neural network based fault detection is described in [12] and belief networks as a basis for fault localization in [13].

[14] proposes modeling the periodic mobile user traffic behavior by a truncated trigonometric series, based on training data. Any deviation from the expected model is considered a fault. Algorithm performance analysis (false alarm rate, time to detect), implementation complexity, memory requirements, model and threshold adaptation to changing traffic patterns are real concerns not fully addressed in the paper. An implementation based on multiple-agents trouble-shooting method is described in [15].

Our work has been implemented and deployed in over 50,000 macro-cellular base-stations world-wide. Key initial lessons learnt were the need to have minimal technician intervention in setting up the fault detection feature with appropriate thresholds and maintaining it. As a result, the entire process of threshold selection and adaptation has been automated. Additional OFD features applied to UMTS are described in [6]. The key differences between the models and algorithms in [6] and this paper are as follows: Sub-hourly "expected load profiles" are learnt and estimated from data and is used as a basel-line to detect significant deviations to signal a fault conditon; an explicit correlation base-line estimation between nearest neighbor cells are estimated and used to signal faults, should the traffic load drops significantly below that predicted by the correlation metric. These two additional OFD methods in [6] add a little more complexity to the fault detection algorithms than those described in this paper, in an attempt to reduce the time-to-detect faults.

B. Restoration of Service

The more rapid and reliable Restoration of Service is, the less loss of revenue a fault will cause. Automatic Software Reconfiguration may be attempted as the first step in the Restoration of Service. When OFD detects a fault, the system has the capability to reconfigure the control channels to different hardware elements on the sector to attempt to restore service on the sector. Repeated reconfigurations indicates a wider malfunction. Automatic Software Reconfiguration saves considerable revenue for the Service Provider in the case of many faults by restoring partial or complete service before a technician can get to a base-station with a fault.

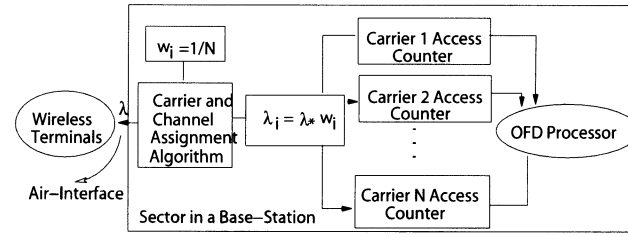

Fig. 4. Carrier assignment and fault monitoring model.

C. Preventative Maintenance

The first three fault management steps are all that has to be done to completely remove the adverse effect of faults if the steps are performed perfectly; Preventative Maintenance facilitates performing Fault Detection via routine maintenance activities, performed daily during off-peak hours. Sometimes, service providers also schedule yearly visits for routine inspection, equipment re-calibration and upgrades.

It is not possible to detect all faults, however desirable that might be. This point may be appreciated by the fact that errors remain in systems that have been in the field for months and even years.

The next section describes a parametric model to detect carrier and channel faults, the lowest level in the logical base-station hierarchy.

IV. Carrier Level Faults

The call processing steps to setup a call and transfer user data was described in section II. Typically, a base-station can contain tens to hundreds of wireless terminals, each of which is either powered-on or powered-off. When a wireless terminal powers on and desires to either register with the wireless telecommunications system or to place a call, the terminal transmits a message to the base-station serving the wireless terminal. The system recognizes the call request and then assigns traffic resources to the mobiles. The resources include a carrier assignment, radio transceivers etc. In this section, we will use the access channel fault detection on each carrier, as a running example, for expository purpose. A similar methodology applies to traffic channel activity as well.

Let us assume there are N access channels, one per carrier, is configured in a sector. Mobile accesses arrive randomly and are received at a given one of the N access channels, as shown in Fig. 4. Typically, the assignment of the mobiles to access channels is performed by a hashing algorithm based on the unique mobile terminal identity number.

If the hardware and radio supporting the access channel message processing is functioning correctly, the system will respond and initiate the process of registration and call set-up. A counter associated with each access channel is incremented each time a successful registration or call set-up request is decoded. In contrast, if the radio is not functioning, the process of registration and call set-up will not commence. When no response is received by the terminal requesting service, it will continue to retry on the same access channel, based on the system hashing algorithm. Since the offered traffic intensity of mobile terminals requesting service or registering

is time-varying and random, the base-station cannot clearly distinguish the lack of activity on a radio between a faulty radio or a functioning radio that received no service requests on the access channel at all.

Notations:

N = number of access channels.

i = index to the access channel under consideration.

n_i^O = Observed number of arrivals measured on the i th access channel.

$\vec{n}^O = [n_i^O, n_2^O, ..., n_N^O]$, vector of observed number of arrivals on the carriers 1 to N.

$n_{lo} = min\{n_i^O; i = 1, 2 \ldots N\}$. Channel with lowest observed number.

$S = \sum_{i=1}^{N} n_i^O$ =Sum of all the counters.

λ = Total arrival rate to the sector.

λ_i = Arrival rate per carrier i. $= w_i\lambda$,where $\sum_i w_i = 1$.

α = fault confidence level, or probability of false alarm

$p_i^E = w_i$= expected distribution on each channel.

$\sum_i p_i^E = 1$.

$n_i^E(\Delta t)$ =Expected number of arrivals in a time duration Δt

$= p_i^E \lambda . \Delta t$

TS = Test-Statistic

χ_α^2 = Chi-Square Distribution within the desired level of confidence α.

We will assume that the weights are estimated or known *a-priori,* by design or based on historic consumer activity data measurementa and analysis. A more general case of learning and estimating these weights using Bayesian methods is not covered in this paper due to space constraints.

A. Uniform Loading Case

Generally, the channel assignment algorithm is designed to distribute the load uniformly across the available access channels. The adjustments for deliberate non-uniform assignment case will be discussed later. The following assumptions are made: based on the hashing algorithm on access channels, the long term expected probability of arrival on any access channel is $p_i^E = 1/N \ \ \forall \ i$ and, the probability of more than one simultaneous access channel failure is unlikely. In case of simultaneous failures of all radios within a sector, higher level fault detectors will catch the resultant fault, as described in the next section under sector faults.

The following computations can be done periodically to determine two values: (1) the sum, S, and (2) the lowest count, n_{lo} . The expected number of arrivals recorded on each channel, n_i^E, should be approximately (S/N). If a particular channel deviates significantly from this value, it could be because of a fault. The channel with the lowest count is suspected to be faulty. However, before declaring a fault, certain conditions must be met, based on the statistical hypothesis test, as described below.

The fault detector then calculates the test statistic (TS), a measure of discrepancy,

$$TS = \frac{((S/N) - n_{lo})^2}{(S/N)} \tag{1}$$

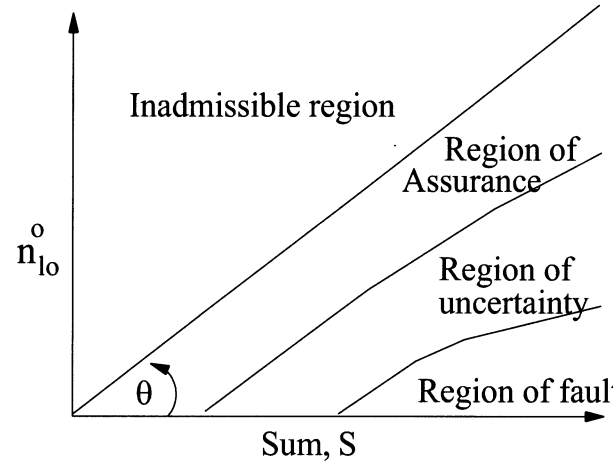

Fig. 5. Fault detection regions.

The statistic TS is χ^2distributed[16].

Functionally, the fault detector poses the null hypothesis, H_0, that the channel associated with n_{lo} is functioning properly. Then, the empirical data is used to show that the null hypothesis is incorrect (i.e., the channel is suffering a fault), with certainty α, when the value

$$TS > \chi_\alpha^2 \tag{2}$$

where χ_α^2 is the upper α point of the Chi-Square Distribution, wherein the degrees of freedom equal $N - 1$. For a given α and N, χ_α^2 can be determined from the Chi-Square formula. χ_α^2 can be determined using either published Chi-Square Distribution tables or from the Chi-Square formula:

$$F(\chi^2) = \int_0^{\chi^2} \frac{1}{2^{\frac{n}{2}}\Gamma(\frac{n}{2})} x^{\frac{n-2}{2}} e^{\frac{-x}{2}} dx \tag{3}$$

Example: Consider the following example with $N = 4, n1 = 24, n2 = 16, n3 = 27$ and $n4 = 19$. The sum $S = 86$, $n_{lo} = n_2$=16(access channel 2) and TS, computed from Eq. 1 and Eq. 3 is equal to 1.407. If we require 95% certainty in declaring access channel 2 as faulty, then from Chi-Square distribution we find for α=0.95 and $(N - 1$=3) degrees of freedom, χ_α^2 =7.81. Since $TS < \chi_\alpha^2$, we cannot declare a fault.

A graph plotting n_{lo}*vs.* S, for a given value of N and α is depicted in Fig. 5. The graph is partitioned into four non-intersecting regions: (1) the region of Inadmissibility, (2) the region of Assurance (no-fault), (3) the region of Uncertainty, and (4) the Region of Certainty (fault).

The Region of Inadmissibility is that region above line *L1*, which intersects the axis at the angle $\theta = \tan^{-1}(1/N)$. No data from a test cycle can be in the Region of Inadmissibility because it is impossible for n_{lo} to exceed (S/N).

The Region of Uncertainty and the Region of Certainty are separated by curve *L2*, which is computed from Eqs. 1 and 2. Solving for n_{lo} and recognizing that n_{lo} is bounded below by 0, we have the following equation for $L2$.

$$L2 = Max\left[0, (S/N) - \sqrt{(S/N)\chi_\alpha^2}\right] \tag{4}$$

where χ^2_α is, as from above, determined for a given N and α. The curve *L2* intersects the X-axis at $N\chi^2_\alpha$, which is the minimum sum, S, at which a hard fault can be detected with certainty α. When we need to have the capability of recognizing soft faults, more data must be collected until that $S > N\chi^2_\alpha$.

When the results of S and n_{lo}, from a given test cycle falls in the Region of Certainty, OFD can reasonably deem, with certainty α, that the channel of interest is malfunctioning.

When a plot of S and n_{lo} fall in the Region of Certainty and $n_{lo} = 0$, then a hard fault is detected. In contrast, when a plot of S and n_{lo} fall in the Region of Certainty and n_{lo}>0, then a soft fault is detected.

When a plot of S and n_{lo} for a given test falls in the Region of Uncertainty, no statement about the existence of a fault or full functionality of the associated channel can be made with certainty α.

The Region of Assurance and the Region of Uncertainty are demarcated by curve *L3*, which is described by the foll0wing curve:

$$L3 = Max\left[0, (S/N) - \sqrt{\chi^2_{\alpha/n}(S/N)}\right] \quad (5)$$

where $\chi^2_{\alpha/n}$ is determined for a given N and a value of $\frac{\alpha}{n}$, where n is chosen appropriately. A value of $n = 2$ can be used as a heuristic. The reasoning behind this is that if the activity is "close to and within reasonable bounds" of expected, then there is likely no fault.

When a fault is certain with the channel with n_{lo}, the radio hardware associated with the channel is taken out of service, and is repaired, if possible. Then new test cycle is started. When the data fail to indicate a malfunctioning channel, the fault detector must determine whether the test cycle is complete or not. To determine if the test is complete, the fault detector considers two factors. First, if S is greater than a restart threshold (RT), then the test cycle is complete. Clearly, the restart threshold should be greater than $S > N\chi^2_\alpha$.The actual choice of restart threshold is implementation dependant and is based on the degree of expediency with which it is desired to recognize a faulty server.

Second, if a plot of S and n_{lo} in the graph of Fig. 5 falls in the Region of Assurance, then the test cycle is considered complete. Alternatively, if the plot of S and n_{lo} fall in the Region of Uncertainty, and n_{lo} is less than the restart threshold, then the test is not considered complete and more data needs to be accumulated.

Since this is a parametric statistical test with known expected distribution, we do not require data for learning or inferring the expected distribution. The assumption of equal loading across access channels and carriers may be relaxed, by adopting methods similar to those described in [6]. By intentionally biasing the load on each carrier or channel by a known pre-determined factor, similar method as above holds with a straightforward manner since expected distribution is known a-priori.

B. Time To Detect Faults

It is relatively easy to determine the time taken to detect hard faults, implying that the faulty channel has n_{lo}=0. If we assume the average arrival rate in the sector is l, the number of channels is N, and , the time-to-detect is given by the following:

$$t_D = \frac{N\chi^2_\alpha}{\lambda} \quad (6)$$

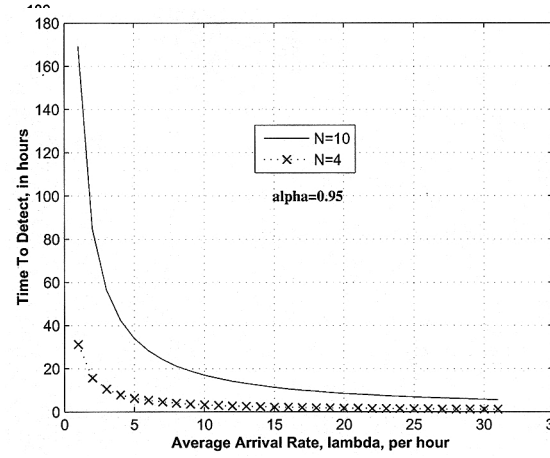

Fig. 6. Detection time as a function of arrival rate (λ).

Fig. 6 shows a plot of time to detect hard faults for two different values of N. As the arrival rate increases, the fault detection time decreases. With increasing N, the time to detect faults increases, for a given value of λ. For soft faults, where n_{lo}>0, the time to detect increases, for a given degree of fault confidence.

C. Non-Uniform Loading Case

There are times when carriers within a sector may be deliberately skewed. This happens when technology evolution leads to addition of deployment of newer services and hardware assets, while at the same time keeping the older generation of hardware active. A classic example is when 1G mobiles gave way to 2G mobiles, and now 2G mobiles are giving way to 3G mobiles etc. Backward compatibility is a requirement mandated by FCC, which requires service providers to support older technologies for a certain duration until all the customers switch-over to the newer technology. Sometimes, with a single air-interface technology, mobiles and base-stations may deploy more efficient speech compression techniques or data services. Many of the continuing improvements will require upgrades to base-station and network assets. A deliberate partitioning or unequal loading may result due to may reasons: due to architectural constraints, the need for testing out the newer services without affecting existing services until a level of maturity is achieved, providing different classes of services by physically partitioning the carriers used by different mobile classes etc.

By intentionally biasing the load on each carrier or channel i by a known pre-determined factor, $w_i \neq w_j$, similar method as above holds with a straightforward manner since expected distribution is known *a-priori*.

The observed distribution of accesses across the N channels can be described by the multinomial distribution, shown in (7)

[?].

$$P(\vec{n}^O) = \frac{S!}{n_1!n_2!...n_N!}\prod_{i=1}^{N}[p_i]^{n_i} \quad (7)$$

To determine the distance between the observed distribution and the expected distribution, we compute the test-statisitc (TS), as we did in the earlier sections. The test-statistic (TS) is Chi-sqare distributed [?].

$$TS = \frac{\sum_{1}^{N}\left(n_i^O - n_i^E\right)^2}{n_i^E} \sim \chi^2 \quad (8)$$

The multinomial hypothesis test is posed as follows:

$$\text{No-Fault}: H_0 : p_i^O = p_i^E, \forall i = 1,..N \quad (9)$$

$$\text{Fault}: H_1 : p_i^O \neq p_i^E, \forall i = 1,..N \quad (10)$$

The empirical data is used to show that the null hypothesis is incorrect (i.e., the channel is suffering a fault), with certainty α, when the value

$$TS > \chi_\alpha^2 \quad (11)$$

Example: Let $N = 3$, $p_1 = 0.5, p_2 = 0.25, p_3 = 0.25, \alpha = 0.05$. Let the counters be sampled every 15 minutes. The observed vector is as follows: $\vec{n}^O = [35, 20, 31]$. Therefore S=86. $\vec{n}^E = [43, 21.5, 21.5].\gamma^2 = 5.7907$. We can compute $\chi_\alpha^2 = 5.99$. We do not reject the null hypothesis at the 5% significance level.

The next section deals with cases when failures in a sector may affect all channels in a sector. Under these circumstances, channel or carrier fault detection will not work since we are comparing activity of one channel with other channels. If all channels have no activity, channel faults will never be detected as the fault detection time goes to infinity. Sector outages are discussed next.

V. Sector Fault

The number of sectors within a base-station may vary, depending on the particular geographic area it is deployed in and traffic densities and expected load a base-station has to serve. Since the majority of the base-stations currently deployed have three sectors, we will focus on this particular example. The framework and methodology applies to base-stations with more than two sectors.

At any given time, there are several factors that contribute to total call activity within a sector in a base-station. These factors can be can classified broadly as follows: call originations within a sector, hand-off between sectors within a base-station, and hand-offs from neighboring base-stations to the sector under consideration as depicted in Fig. 7.

Generally speaking, there is some degree of traffic load correlation between sectors within a macro-cellular base-station. However, since the sectors are facing different geographic regions, each sector may experience different instantaneous traffic loads at different times of the day. Therefore, the degree of correlation could be time-varying. In base-station deployed in very high traffic area, like inside the airports, malls, train-stations or dense down-town market areas, all three sectors may experience approximately uniform loading. For base stations deployed on highways, the sectors facing the highways may have a different traffic loading profile than a sector facing away from the highway, for instance. This may result in some sectors having very large traffic loads at certain times of the day while its neighboring sector may have very little load.

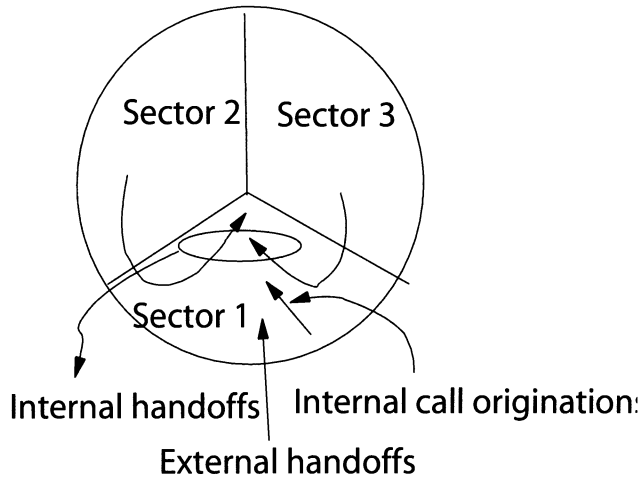

Fig. 7. Sector fault monitoring model.

The expected load distribution in each sector is not known a-priori and, and since each individual sector loading is time-varying function, we cannot extend the simple parametric model described for detecting carrier faults. OFD identifies faults in a sector on a base-station that has no call activity when there are many calls on the other sectors at the same time. The other sectors provide an estimate of the traffic in the area and in this way improve the effectiveness of the test. A combination of learning from empirical data and statistical correlations are used.

When significant deviations from expected activity are observed, a fault is declared. Internal thresholds are set within the algorithm based on empirical training data gathered during normal operating conditions. However, as mentioned before, mobile traffic patterns change with time-of-day, day-of-week and time-of year. One of the key challenges is to make the thresholds adapt to changes in mobile user traffic patterns, while keeping the memory needs and computational requirements very low.

We adopt a semi-parametric model, which takes advantage of the knowledge that there is some minimal degree of correlation between sector activity.

Notation:

M: Number of sectors within the base-station under test.

i : sector under test

p_i = probability of arrival in sector i.

$p_{(M-1)}$ = total probability of arrival in $(M-1)$ sectors neighboring i within the same base-station.

γ : average load imbalance factor between i and neighboring sectors within the same base-station.

γ =1, implies a uniform traffic distribution in all sectors with no traffic imbalance at all, implying $p_i = 1/M$ and $p_{(M-1)} = (M-1)/M$.

Also, $p_i + p_{(M-1)} = 1$

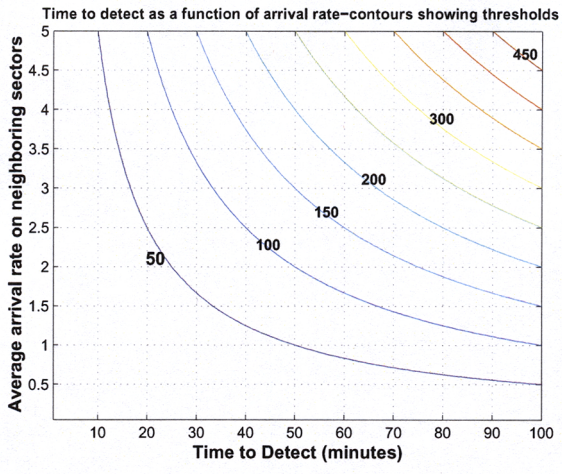

Fig. 8. Detection time-arrival rate-fault threshold relationship.

In general,

$$\gamma = [p_{M-1}/(M-1)]/p_i \tag{12}$$

$\lambda_i^o(t)$: arrival rate of calls being originated within the sector i under test

$\lambda_i^{ho\_internal}(t)$: the arrival rate of hand-offs from adjacent sectors within the same base-station

$\lambda_i^{ho\_external}(t)$:arrival rate of hand-offs from adjacent base-stations.

$\lambda_i^{total}(t)$: total arrival rate within sector i
$=\lambda_i^o(t) + \lambda_i^{ho\_internal}(t) + \lambda_i^{ho\_external}(t)$.

$\lambda_{M-1}^{total}(t)$: total arrival rate in sectors neighboring i in the same base-station.

Now, the value of γ is time varying, due to the time-varying traffic statistics in each sector and can range from $0 < \gamma(t) < \infty$. Since a Fault condition is determined by comparing the activity of each sector with its immediate neighbors, one simple mechanism is to first estimate, or learn, the worst case, or maximum expected value of $\gamma(t) = \gamma_{\max}$. Once this value is known, the following hypotheis test is posed:

$$\text{(No Fault)}: H_0 : p_i \geq p_{M-1}/(M-1)\gamma_{\max} \tag{13a}$$

$$\text{(Fault)}: H_1 : p_i < p_{M-1}/(M-1)\gamma_{\max} \tag{13b}$$

A simple hard fault detection algorithm is to count the total number of arrivals, S, in the neighboring sectors within a base-station when the test sector has no arrivals, i.e. $n_{lo} = 0$. Assuming the number of sectors is M, the probability of false alarm is less than α, and the worst case anticipated imbalance is $\gamma_{\max}$, the equivalent fault threshold number can be computed from the following equation:

$$S^*(\gamma) = \min\left\{S : \binom{S}{n_{lo}} p_i^{n_{lo}}(1-p_i)^{S-n_{lo}} \leq \alpha\right\} \tag{14}$$

If the observed call load traffic $S > S^*(\gamma)$, then a fault likely exists. Empirical data is used to test the hypothesis, much like the carrier fault analysis of the previous section.

Fig. 8 shows the relationship between arrival rates, fault detection time and fault thresholds. For a fixed fault threshold, as the arrival rate increases, the detection decreases. As the fault threshold is increased, it takes longer to detect faults for the same arrival rate.

One option for network operators is, based on their intimate local network and traffic distribution knowledge, to estimate an initial fault threshold selection that may be applicable to majority of the base-stations.

Example: If it is assumed that the worst case expected imbalance is $10:1$ (i.e.$\gamma_{\max}$=10), for $M = 3$ and $\alpha = 10^{-5}$ then $S^*(\gamma) \approx 300$.

The above threshold may be applicable to the majority of the base-stations. However, a certain percentage of base-stations especially in places like rural areas, sectors facing a stadium with occasional and sporadic activity or base-stations with isotropic loading etc., will require fine-tuning the thresholds correctly. If the imbalance factor is lower than predicted, the time to detect is larger, thereby losing valuable revenue. But the probability of false alarm is much lower. If the actual imbalance is higher than predicted by engineering intuition, the time-to-alarm is quicker, but the probability of false alarm may be larger. The latter case is to be avoided as discussed previously. There is, therefore, a need to match the threshold to each sector appropriately. This is discussed next.

A. Empirical Imbalance Estimation

Since the traffic patterns change with time-of-day and day of week, as well as a much slower time-of-year seasonal changes, there is a need to learn and estimate, from empirical data, the worst case expected imbalance factor for each sector in the network, to guide us in threshold setting. Based on traffic engineering studies and engineering trade-offs, a two to three week initial base-line training data collection, learning and estimation is recommended. This time window allows sufficient time for observing the worst case imbalances to be expected during normal operation. The longer the training window, the better the base-line estimation will be. Once the worst case values are obtained, the actual fault threshold value should be set with some safety margin above the worst case observed. A more formal statistical method based on extreme value theory will be reported in a separate paper due to space constraints in this paper.

Asuming a training or learning window of 2-3 weeks for estimating γ, we can approximate it to

$$\gamma = (\lambda_{M-1}^{total}(t).\Delta t)/(M-1)(\lambda_i^{total}(t).\Delta t) \tag{15}$$

where Δt is the on the order of largest inter-arrival times of the test sector i. Essentially what is being monitored and recorded are the extreme imbalance values, which is the ratio of neighboring sector loads to test-sector load. These are time-varying quantities, so only a few of the largest, or extreme, values are recorded in a buffer. These extreme value statistics are then used, with some extra margin, to set appropriate thresholds for fault declaration. Threshold setting based on extreme value theory has been developed and will not be reported here due to space constraints and will be the subject of a future paper. Heuristically, a factor of 1.5 to 2 of the maximum value of γ may be used for conservative threshold setting. A more formal analysis of extreme value theory (EVT)

based threshold analysis is used for fine-tuning the alarm thresholds. This EVT method is not reported here due to space constraints.

B. Automating Threshold Adaptations

The main advantage of the above method of sector fault detection is its low complexity. However, there is a need for initial data collection and learning period to set-up correct thresholds. OFD has the report capability to give the Service Provider information about whether the thresholds should be adjusted. The thresholds might need adjustment because of changes in traffic patterns.

Learning allows the system to adapt to slow variations in traffic dynamics over time. The algorithm records empirically obtained expectations of the normal operating behavior is the network. A number of engineering tradeoffs arise based on choices of how long the system is trained for and how often the training data is updated. While the recommended initial data collection and learning period was about 2-3 weeks accounts for daily and weekly variations, the longer term seasonal variations are not accounted for. Consider the example of a beach resort. It is very likely to encounter high seasonal traffic which tapers off during off-seasons. Similarly, winter ski resorts will only see high activity during winter and little during non-winter months. The initial thresholds depend on the time of initialization and prevailing seasonal traffic. There is a need for automatically proactively adjusting the thresholds on a routine basis. The consequences of not doing so can be categorized as follows:

- If traffic imbalance, $\gamma_{\max}$, increases from the initial baseline, the time-to-detect decreases and Probability of false alarm decreases.
- If traffic imbalance, $\gamma_{\max}$,decreases from the initial baseline, then the probability of false alarm increases.

An open loop routine adjustment process has been implemented which is constantly learning in the background and updating thresholds every few weeks. This update period is adjustable.

VI. Base-Station Outage Detection

The previous sections discussed fault detection in a carrier within a sector and a sector within a base-station. Both were accomplished by comparing activity across correlated carriers and sectors. However, if all carriers and sectors have no activity, the entire base-station will be silent. OFD will also identify when no calls or accesses have been received on all the sectors of the base-station for an extended time, which indicates that the entire base-station is inoperable. The lack of calls on the entire base-station, while possible, is highly unlikely during busy hours. In non-busy and mid-night hours in remote areas, it is likely that there may be extended times, of several hours, when no calls are placed at all. A silent base-station could be a results of a fault or no offered traffic.

It is possible to adopt methods of the previous section on sector fault detection and use correlation of traffic between adjacent and neighboring base-stations. This would require exchanging loading information and communicating across nodes requiring co-ordination and synchronization of data [6].

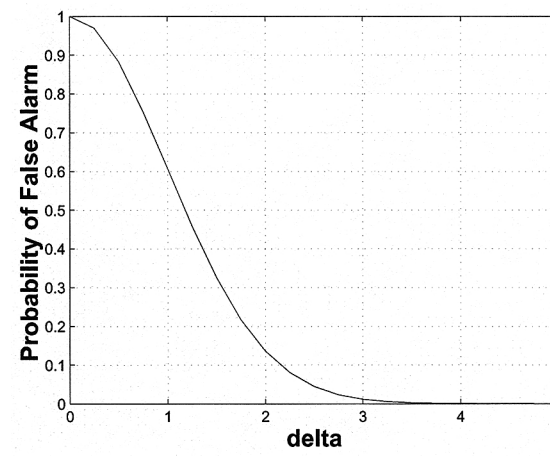

Fig. 9. Probability of false alarm as a function of threshold multiplier, δ.

A simpler method is discussed next, although the time-to-detect fault may be longer.

The key question is, how long should a base-station be silent before we deem it to be due to a fault and not due to absence of real traffic? An easy and simple way is to empirically record the largest silence time, T_S, observed during the initial training time and use it as a guide to set thresholds. The silence time will be dominated by non-busy hour or night-time low activity. The threshold selection criteria would be, as before, to provide a reasonable safety multiplication margin, δ>1, over and above the largest T_S , such that the fault threshold time $T_S^* \geq \delta T_s$. A formal statistical method, one based on exterme value theory that fits the tail distributions, has been developed to set more appropriate thresholds and selection of δ. Due to space constraints, it will be reported in a future paper.

The value of δ depends on the confidence level required before sending an alarm. To bound the probability of false alarm as a function of δ and T_S, we use a modified version of Chernoff bound[17], as shown in Eqn. 17.

$$P_{false-alarm} = P(T_{obs} \geq T_S^*) \leq \alpha \tag{16}$$

$$P\left([T_{obs} - T_S \geq \delta T_S]\right) \leq \mathrm{e}^{-\left(\frac{T_S.\delta^2}{2}\right)} \tag{17}$$

The probability of fault as a function of the multiplier, δ, is shown in Fig. 9. As the safety margin δ increases, the probability of false alarm decreases. The time-to-detect a fault, equal to threshold T_S^*, however increases. One implementation option adopted is to partition the day into busy hour and non-busy hour and use different time thresholds for each of these partitions. The obvious question is why not partition the day into smaller and smaller time epochs to improve fault detection time? This will require increased data collection, storage and processing. For a modified version of silent base-station detection, based on sub-hourly profiles is described in [6].

The impact of seasonal changes in the distribution of T_S is similar to that discussed in the previous sector fault detection section on imbalance factor estimation.

As mentioned before, an actual site visit is expensive and every effort is expended to remove any doubts about the nature of the alarm before actually emabrking on a cell site visit. Generally, technicians try to validate the alarms and cross-check with other base-station performance monitoring functions. These cross-checks may be in the form of using other functional tests with specialized hardware or software, if present or to use performance and call records originating from the base-station and check the trends etc.

VII. Summary and Discussions

We have provided a framework of statistical fault detection and described three simple schemes implemented and deployed in real cellular networks. The emphasis was on very low complexity algorithms. These algorithms provide a last line of defense, when all other existing alarm mechanisms and fault detection methods fail. While the advantages of the algorithms described are its simplicity, the time-to-detect faults may be large, for certain application. Minimizing both false alarm probability and time-to-detect metrics will necessarily require more data collection and hence complexity. The other shortcoming, based on initial field deployment feedback, was the need for automated threshold adjustment. We have since implemented constant learning, adapting and periodic threshold adjustment mechanism. The disadvantages of statistical learning based algorithms are the need for initial training and learning of the base-line activity model, as well as periodic relearning to to adapt to seasonal variations in teletraffic and mobility patterns. There is a tradeoff between the duration of learning and false alarm probability. Thelonger the training or learning period, the lower the probability of false alarms. However, the downside of longer learning is that fault detection is delayed. Therefore, mechanisms to optimize the fault detector performance by judicious choice of learning duration and and false alarm probability is required, either via engineering judgement or explicitly within the algorithm itself.

This framework to detecting faults have been extended to other technologies, services and network elemments such as: UMTS Base-Stations, 1x-EVDO base-stations, Pust-To-Talk/Speak service outage detection, RF capacity degradation detection, Receive path fault detection etc. Non-parametric soft fault detection requires correlation with multiple sources of information, while providing faster response and are more robust, leads to higher communication, memory and algorithmic complexity, as described in [6]. Other extensions to Radio Network Controller and Base-Station Controller and alarm threshold analysis based on extreme value analysis will be reported in future publications.

Acknowledgments

The author would like to thank Dr. T. Wing for his inspiration to pursue this topic. The quality of this paper has improved due to comments from my esteemed colleagues : Dr. F-C Cheng, Dr. M Thomas, Dr. A Gandhi, and Dr. R Sinha. In addition, sincere thanks to anonymous reviewers for their many comments and suggestions for improvements.

References

[1] S. Aidrous and T. Plevyak, eds., *Telecommunications Network Management into the 21st Century: Techniques, Standards, Technologies and Applications*. IEEE Press, 1994.

[2] D. S. Jackson and F. F. Kunzinger, "Calculation of system availability using traffic statistics," *Bell Labs Tech. J.*, vol. 7, no. 3, pp. 139–150, 2003.

[3] ANSI J-STD-008, "Personal station-base station compatibility requirements for 1.8 to 2.0 GHz code division multiple access (CDMA) personal communications systems," Aug. 1995.

[4] TIA/EIA Standards, "Mobile station-base station compatibility standard for dual-mode wideband spread spectrum cellular system," Mar. 1995.

[5] 3GPP TS 23.101, "General UMTS architecture, 1999.

[6] B. Cheung, G. Kumar, and S. Rao, "Statistical algorithms in fault detection and prediction: towards a healthier network," *Bell Labs Tech. J.*, vol. 9, no. 4, pp. 171–186, 2005.

[7] S. C. Yang, *CDMA RF System Engineering*. Artech House Publishers, 1998.

[8] ITU-T Recommendation M.3400, "TMN management functions," 1992.

[9] L. L. Ho, C. J. Macey, and R. G. Hiller, "Real-time performance monitoring and anomaly detection in the internet: an adaptive, object-driven, mix-and-match approach," *Bell Labs Tech. J.*, vol. 4, no. 4, pp. 23–40, Oct.-Dec. 1999.

[10] C. Hood and C. Ji, "Proactive network-fault detection," *IEEE Trans. Reliability*, vol. 46, no. 3, pp. 333–341, Sept. 1997.

[11] M. Thottan and C. Ji, "Proactive anomaly detection using distributed intelligent agents," *IEEE Network*, special issue on network management, vol. 12, no. 5, pp. 21–27, Sept.-Oct. 1998.

[12] R. Sreedhar, B. Fernandez, and G. Y. Masada, "A neural network based adaptive fault detection scheme," in *Proc. American Control Conference 1995*, vol. 5, pp. 3259–3263.

[13] M. Steinder and A. S. Sethi, "Probabilistic fault localization in communcation systems using belief networks," *IEEE/ACM Trans. Networking*, vol. 12, no. 5, pp. 809–821, Oct. 2004.

[14] K. D. Tuchs, M. Cech, and K. Jobmann, "Automatic detection of abnormal deviations from network performance data values," in *Proc. Network Operations and Management Symposium 2002 (NOMS)*, pp. 959–961.

[15] M. Guiagoussou and S. Soulhi, "Implementation of a diagnostic and troubleshooting multi-agent system for cellular networks," *Int. J. Network Management*, vol. 9, pp. 221–237, 1999.

[16] J. E. Freund and R. E. Walpole, *Mathematical Statistics*. Prentice Hall, Inc, 1987.

[17] M. T. Goodrich and R. Tamassia, *Algorithm Design: Foundations, Analysis and Internet Examples*. Wiley, 2002.

Sudarshan A. Rao is a Member of Technical Staff in Base-Station Systems Engineering and Architecture Department, Lucent Technologies, Whippany, NJ. He has been involved in performance and fault management of Base-Station products since 1998. His research interests include automated learning and control algorithms for efficient network operations management, radio resource management, and mobility management.