

Dyaptive SYSTEMS

DMTS-8000 Assisted TroubleShooting for CDMA2000 Networks



April 13, 2005

1	CDMA2000 Fault Diagnosis and Troubleshooting using DMTS-8000	1
2	Testing for Protocol Errors (Software Faults) in Closed Loop Power Control:	4
3	Testing for Protocol Errors (Software Faults) in Soft Handoff Decision Algorithm:	4
4	Testing for Duplicate or Correlated Code assignments and invalid Pilot PN Offsets:	4
5	Testing for the Integrity of System Messages	4
6	Testing Authentication Center	5
7	Testing of Network Support for Mobiles with Different Capabilities	5



1 CDMA2000 Fault Diagnosis and Troubleshooting using DMTS-8000

CDMA2000 is a complex system composed of numerous protocols and components. In addition to IS-2000 specific RF components, IS2001 specific terrestrial and IS-41 specific signaling components also constitute parts of a CDMA2000 cellular system. Several vendors contribute their equipment and software to put together a CDMA2000 deployment. In addition, being an integral part of the global communications network, CDMA2000 networks are also required to smoothly interoperate with the Internet, PSTN (Public Switched Telephone Network) and other cellular networks. All the leading network equipment vendors and firmware developers follow strict guidelines for testing, verification and quality control before shipping out their products for deployment. However, it will be overly optimistic to assume that these products are tested for interoperability under a wide range of traffic, user mobility and channel conditions. In such a complex system that handles thousands of calls per hour, detecting an anomalous call and subsequently localizing and identifying the root cause of the anomaly is like locating a needle in a large pile of hay.

In telecommunications networks, fault diagnosis and troubleshooting is managed by (third party) fault management systems. Network components, in general, generate alarms as external manifestations of internal disorders or faults. Fault management systems collect these alarms to determine and subsequently repair an abnormal condition of any part of the network. Such OSs (Operations System) fulfill following key functions:

- Fault Detection
 - Using mostly alarms
- Fault Diagnosis and Trouble Shooting, which involves
 - Fault Localization i.e. identifying the device or protocol at fault
 - Fault Identification i.e. identifying the nature of the fault
- Facilitating Repair and Service Restoration
- Fault Prediction

There are several limitations to fault diagnosis and troubleshooting. These include:

- lack of alarms
 - dependent on component self-diagnosis
- lack of enough information in the alarms
 - alarms usually do not contain where and why
- discrepancy between number of symptoms and their causes
- complexity of telecommunication networks
 - thousands of components involved
 - each component can fail in various ways (multi-state machines)
 - multiple faults can occur at the same location and at the same time masking each other
- cascading



- a primary fault causes a number of secondary faults and consequently numerous secondary alarms, further obstructing correct and timely problem resolution
- low observability
 - some network components are difficult to monitor and their state must be deduced by observing other components
 - self diagnosis
- synergistic alarm interpretation
 - alarms must be interpreted collectively, using chronological, causal, structural and textual information simultaneously
- noise
 - alarms may get lost
 - the temporal information may be inconsistent due to lack of clock synchronizations

Fault management systems therefore perform alarm correlation to simplify their task. Alarm correlation is the process of preprocessing the alarms with the purpose of reducing the number of alarms or messages presented to the fault diagnosis system or network operator. An effective alarm correlation increases the semantic information associated with the alarms; isolates primary alarms from the secondary and thus less relevant alarms; and, perhaps, helps predict future alarms and subsequent faults.

Methodologies for fault diagnosis & trouble-shooting can be generally classified into rule-based or model-based. Either case necessitates thorough testing of an integrated CDMA2000 system, at least in a lab setup, under a wide range of traffic, mobility, channel and other user/environment conditions to produce a comprehensive rule base or devise an accurate model for fault diagnosis and trouble shooting.

In wireless networks, with unpredictable RF channels, the fault diagnosis and troubleshooting problems are further compounded due to false alarms and missed alarms. As an example, in a CDMA2000 system a relatively longer duration of higher than normal FER (Frame Error rate) will result in a loss of fundamental, supplemental and/or control channel. Now, this may have been caused by timing & synchronization errors, software fault in the power control procedures, or other degradations in the base station's or mobile's RF equipment. Yet another possibility is that it may have occurred naturally due to a particular terrain obstructing the line-of-sight between the mobile equipment and the base station.

Upon receiving a customer complaint, or having observed service underperformance through network monitoring, a network operator has to quickly troubleshoot and diagnose the problem, and restore the service to its normal mode of operation. The network operator needs to find out if the deterioration is natural or due to network fault. In case it is due to network fault, then is the fault in the user equipment or in the network equipment? Finally, if the fault is in the network, where is the fault and what is the fault? Any delay will have direct impact on customer satisfaction and revenue. Wrong diagnosis will further add to the cost overruns. In conventional frequency reuse based cellular networks, a faulty RF equipment at the base station or in the user device, or errors in some control procedures may impact only one call or limited number of calls. In CDMA systems, such as CDMA2000, where numerous calls frequency- and time-share a single



carrier, such faults and errors not just impact one call but all the calls in the sector or cell, causing outages.

The DMTS-8000 from Dyaptive Systems is well positioned to play a central role in the testing, fault diagnosis and troubleshooting of a CDMA2000 system. The DMTS-8000 loads up a CDMA2000 system with thousands of calls of various service types, and emulates specified subscriber mobility, channel conditions and other environmental conditions. With thousands of calls in progress in a CDMA test-bed, DMTS-8000 allows network engineer to zoom-in on any (emulated) mobile, its particular registration or call attempt, and expose the finest possible details and slightest visible anomaly that occurred during its life span. The DMTS-8000 not only provides a comprehensive testing environment for all layers of the CDMA2000 protocol stack, from physical to application, but by loading the integrated CDMA2000 test-bed with traffic in a controlled manner, it also facilitates testing of the IS-2001 as well as IS-41 specific network components. DMTS-8000 also helps test and verify various third party network monitoring probes and fault management system used by the network operator for various OA&M (Operations Administration & Management) tasks. Using DMTS-8000 the network operator can, to a large extent, replicate in the lab setup, network and environment conditions leading up to the observed or reported degradation in the live network and determine the cause of the degradation.

The DMTS-8000 is complimentary to other fault diagnosis and alarm correlation systems deployed in the network. As mentioned earlier, these systems require either a rule base or a model to effectively troubleshoot and diagnose a network. For relative new systems, such as CDMA2000, due to lack of historical data, a comprehensive set of rules or an accurate model for trouble shooting and fault diagnosis do not yet exist. The DMTS-8000 alleviates this problem by stimulating the CDMA2000 test-bed with a wide variety of traffic, mobility and channel conditions; stress tests various components, protocols and interoperability; and, leveraging other network monitoring probes and systems deployed in the network, helps produce rules and models needed for accurate fault localization and identification. Consider for example a situation where the base station is behind a building. As soon as the mobile moves from behind the building to the front, a strong Pilot from that base station is suddenly detected. The mobile would ask for soft handoff but the interference may have already started causing drops in the Handoff Direction Messages. In normal situations, the pilot strength increases gradually and the handoff is initiated long before the pilot strength becomes too strong. In urban areas, however, this could be a common cause of handoff request failures. Now, if the handoff procedures are methodically tested by emulating such scenarios using DMTS-8000 before their actual deployment, the network operator will have acquired enough knowledge and intuition to quickly decide with confidence whether a reported degradation that was preceded by handoff failures is caused by such line-of-sight issues, congestion in the signaling channels causing delay in the Handoff Direction Message arrival or Fault in the handoff procedures. In the first case it will be only a few mobiles in a particular location in the sector exhibiting such problems, in the second case the problem must have been reported by mobiles distributed uniformly in the sector and under heavy signaling traffic, whereas in the third case the mobiles must have reported such degradations in other sectors (containing friendly terrains) as well.

Mobile emulations that intentionally disobey or misinterpret network directives or, in one sense or another, violate the protocols are introduced using DMTS to discover the network's response to such misbehaving mobile terminals and test the stability of various



CDMA protocols such as open loop or closed loop power control, soft handoffs and call processing procedures etc.

Described below are few examples of DMTS-8000's applicability to troubleshooting and fault diagnosis of CDMA2000 protocols and network components.

2 Testing for Protocol Errors (Software Faults) in Closed Loop Power Control:

The network engineer configures DMTS-8000 for generating BHCA to a cluster of CDMA2000 cells. Various combinations of channel models, subscriber distributions and subscriber mobility models are selected. Mobile speed is varied. The Reverse SINR, Forward SINR, Power Control Bits in R-FCH, F-FCH and R-PICH, Loss of Channel Declarations statistics are monitored. Power control directives from Base Station to Mobile are compared with values computed theoretically for a given particular location, distance from the base station and the inter- and intra-cell interference. Any significant discrepancies are reported as anomalies.

3 Testing for Protocol Errors (Software Faults) in Soft Handoff Decision Algorithm:

The network engineer configures DMTS to emulate a single mobile. The Pilot Signal Strength of neighboring base stations is varied (this is achieved by suitably fading the Pilot Strength Signal reaching the emulated mobiles). The mobile shall receive appropriate Handoff Directive Messages within the timeout if the Pilot Signal Strength from the base stations crosses certain threshold, otherwise an anomaly is reported. The tests are repeated using different mobility models and mobile speeds. The reason of handoff failures or handoff call block could simply be the wrong choice of (T_ADD, T_DROP) pair and T_TDROP timer (also SOFT_SLOPE, ADD_INTERCEPT, and DROP_INTERCEPT if available). The values are adjusted using the test-bed until the handoff efficacy is restored.

4 Testing for Duplicate or Correlated Code assignments and invalid Pilot PN Offsets:

The network engineer configures DMTS to continuously increase the network load to a cell cluster sharing the same carrier. The code assignments from the base station are tested for duplicate or correlated codes. If one or more instances of duplicate or correlated codes is discovered then error in code generation procedure is reported and impact on the forward/reverse SINR measured.

5 Testing for the Integrity of System Messages

The network engineer configures DMTS with services that require use of supplemental channels (e.g. Service Option 33). The load on a cell cluster is continuously increased. Upon receiving the Supplemental Channel Assignment Messages, the SCCL (Supplemental Channel Code List) in the message is compared with the list in the mobile's database and with other mobiles' databases for an integrity check. Any discrepancies that are found are reported.

Similarly the integrity of the contents of various other system messages is tested and verified. Some examples are as follows:



- During the call setup the mobile negotiates the service option. DMTS tests and verifies that the service option response from the BTS is consistent with the capabilities of the mobile terminal, and the call processing procedure never enters an undetermined state if certain mobile terminal capabilities expected by the network are missing.
- If the QPCH is enabled, DMTS can check if there is any discrepancy between the paging indicators and the actual FPCH or FCCCH slots carrying the information for the specific mobile.
- DMTS-8000 can monitor FPCHs or FCCCHs of several sectors at the same time and verify the integrity of overhead messages such as access parameters message, system parameters message, CDMA Channel List message, extended System Parameters message and extended neighbor list message by comparing them to the mobile database, messages received by other mobiles and network databases.

6 Testing Authentication Center

The network engineer tests the Session Key generation algorithm and authentication process by configuring some Mobiles in DMTS with invalid IMSI, ESN (Electronic Serial Number), MIN (Mobile Identification Number) and A-Key, whereas the rest of the mobiles are correctly configured. Any instance of an unauthorized mobile getting authenticated and correctly encrypt and decrypt data is reported.

7 Testing of Network Support for Mobiles with Different Capabilities

The network engineer tests the network against different mobile configurations that are presently in use in the network or that are likely to be in use in the reasonable future. Examples of such devices include 2G and 3G, common channel support only, low data rate only, etc.

