Performance Metrics for Disaster Monitoring Systems

Tuncay Bayrak
Western New England College
tbayrak@wnec.edu

ABSTRACT

Understanding the performance of disaster monitoring systems is a key to understanding their success, therefore; various qualitative and quantitative measures and metrics can be applied in the characterization and analysis of such systems. Through evaluation studies, problems that impede a disaster monitoring system performance can be identified. The results can be used for system control, design, and capacity planning. Previous studies address technical performance analysis metrics for analyzing monitoring systems leaving out human and organizational dimensions of such systems. Thus, the primary objective of this study is to identify and describe a set of disaster monitoring systems performance analysis metrics that may be employed to evaluate such systems. This study may be valuable to researchers and practitioners involved in disaster and emergency response studies in planning the transportation of vital first-aid supplies and emergency personnel to disaster-affected areas, and in improving chances of survival after a natural disaster.

Keywords

Disaster monitoring systems, natural disasters, computer networks

INTRODUCTION

Having been ravaged by the 2005 tsunami that devastated several communities, a number of countries in various regions are now developing and setting up real-time disaster monitoring systems that would help plan for and respond to natural disasters. Hence, it is essential that such systems be designed and built using a robust, reliable, and survivable infrastructure. As well, their performance must be measured using various metrics to verify whether they perform to their specifications.

The World Health Organization (WHO) defines a disaster as any occurrence that causes damage, destruction, ecological disruption, loss of human life, human suffering, deterioration of health and health services on a scale sufficient to warrant an extraordinary response from outside the affected community or area (WHO, 1999). Thus, a disaster monitoring system may be a combination of information and communication technologies used to monitor such occurrences and hazards that negatively affect society or environment.

In order to eliminate or at least to minimize the problems associated with disaster monitoring system management, a range of network performance measurement metrics may be utilized. As monitoring systems become more and more complex and integrated, measurement becomes especially important as a slight deviation in their performance may produce serious damage, injury and threat to human life or the environment. Consequently, disaster monitoring systems should constantly be measured to make sure they execute as required.

Measurement metrics are needed to compare two different entities, events, technologies, devices and so on. In this context, metrics act like a universal language among scientists. However, a key issue in any disaster monitoring system evaluation study is the question of metrics. Further, as new monitoring networking technologies emerge and replace existing ones, the issues of metrics and measurements need to be redefined in order to guarantee interoperability. Therefore, the enforcement of metrics and measures is a key to interoperability of monitoring networks in various settings. Thus, the primary objective of this study is to identify and describe a set of metrics that may be employed to evaluate disaster monitoring networks/systems.

BACKGROUND

Performance is usually defined as the accomplishment of a task or an activity expressed in some terms (Savolainen, 1999), and, as argued by Lirow (1997), the performance of a computer system is best characterized and measured in terms of the business functions performed by the system. In general, the purpose of the performance evaluation is to assess the accomplishment of the subject matter in terms of qualitative and quantitative criteria (Savolainen, 1999). The dominant measures of computer systems originated in the perception that these measures represented systems characteristics (Giladi and Ahituv, 1995). Performance criteria for computer systems were first incorporated in the American National Standards Institute (ANSI) (Lindberg, 1995).

Once performance objectives have been stated, it is important to measure the system routinely in order to verify the objectives that the system is meeting, identify objectives that are not being met, and identify objectives that are marginally being met and might therefore be in jeopardy in the future (Lirow, 1997). The performance of a system is often measured to make sure it can provide the responsiveness that all the users require (Blommers, 1996). Similarly, reasons for measuring a network's performance include the fact that a monitored and benchmarked network can keep user response times low, increase user productivity, provide for future growth, ensure successful deployment of new applications, and provide troubleshooting information about bottlenecks (Blommers, 1996). Thus, performance evaluation can help identify and isolate problems in order to enhance performance.

As suggested by Krishna (1996), a good system performance measure should have characteristics such as the measure will be relevant in the context of the application, and the measure will allow an unambiguous comparison to be made between machines.

Haring and Kostis (1994) point out that measures can be either task-oriented or system-oriented. Task-oriented measures typically say something about the end-to-end performance as perceived by the system users. Examples are the end-to-end throughput or expected performance level over some time interval of system usage. System-oriented measures say something about how the system performs its tasks. Examples are the average queue length, the number of operational components of some time, or utilization of a server. Stuck and Arthurs (1985) discuss two types of measures: those oriented toward customers or end users of the system, and those oriented toward the system as a whole. In general, Sahinoglu and Tekinay (1999) suggest, users are most interested in metrics that provide an indication of the likelihood that their information will get to the destination in a timely manner. From the point of view of a user of a system, one might be interested in the delay for each job from arrival to the initial wait for service, through service, and the final clean up for prior to completion. On the other hand, from the point of view of the system as a whole, one might wish to record over a given time interval, the fraction of time each resource is busy doing work, and the mean throughput rate of executing jobs (Arthurs, 1985).

If a computer system is shared by many users, two types of performance metrics need to be considered: individual and global. Individual metrics reflect the utility of each user, while global metrics reflect the system-wide utility. Resource utilization, reliability, and availability are global metrics, while response time and throughput may be measured for each individual as well as globally for the system (Jain, 1991). Other techniques can be used to evaluate the performance of distributed communication networks as well. In distributed environments, the failure of one or more system components causes the degradation of its effectiveness to complete a given task as opposed to complete network breakdown. Here two static measures can be employed, namely, Distributed Program Performance Index (DPPI) and Distributed System Performance Index (DSPI). These metrics can be used to determine if the network with high reliability and low capacity, or low reliability and high capacity, is better for a given program execution (Kumar and Agrawal, 1996). Moreover, in distributed network systems, performance may be measured in terms of jobs per second, response time, or transaction per second (El-Rewini and Lewis, 1998). In order to achieve high end-to-end performance in widely distributed applications, a great deal of analysis and tuning is needed (Tierney et al., 1996). Finally, Kirner (1997) focuses on reliability, security, safety, maintainability, and usability as essential requirements for real-time safety-critical systems such as disaster monitoring systems.

Previous studies have often focused on hardware and software leaving out any representation of the humans using disaster monitoring systems, and the organizations hosting them. Few studies have linked computer system performance and organizational performance, or organizational performance and user performance with a computer system. Thus, in this study we argue that disaster monitoring system should be evaluated using three sets of performance measures; technical performance measures pertaining to the computer infrastructure used to gather environmental data, user performance measures pertaining to the human operators using the disaster monitoring networks, and organizational performance measures pertaining to the organizations hosting them.

PERFORMANCE ANALYSIS METRICS FOR DISASTER MONITORING SYSTEMS

Disaster monitoring systems are often distributed, heterogeneous, integrated, and complex systems, which may depend on hardware, software, and human operators, and, as argued by Smith et al., (1996), the increasing level of complexity in such reliable and safety-critical systems significantly complicates the determination of metrics. Similarly, Tierney et al., (1996) content that it is often difficult to track down system performance problems because of complex interactions between the many distributed system components.

Because humans and technology cooperatively perform tasks in network-centered large-scale disaster monitoring systems, the measures discussed in this research for evaluation of disaster monitoring systems involve multiple disciplines and considerations. This multidisciplinary approach enables us to look at networked organizations and human operators, and to evaluate network performance, human performance with the network, and the network's impact on organizational performance.

Thus, it could be argued that such systems should be evaluated using both quantitative and qualitative performance criteria, metrics and measures. For example, such systems use data communication systems and networks to gather environmental data from various remote stations. Hence, using such quantitative metrics as response time, throughput, and reliability might allow to evaluate their technical performance. Similarly, human operators monitoring and maintaining such systems might be evaluated using qualitative performance measures such as workload and vigilance level. Finally, organizations using these systems to make critical decisions should be evaluated to improve their effectiveness, efficiency and overall system performance. In the following sections we explore three sets of metrics which may be used to evaluate such systems.

Technical Performance Analysis Metrics

A variety of performance criteria, metrics and measures have been proposed to measure performance of different communication networks. Lavenberg (1983) suggests many performance models can be quantitatively analyzed to obtain such performance measures as utilization, throughput, and average response times. Similarly, traditional well-defined metrics such as delay, packet loss, flow capacity, and availability are fundamental to measurement and comparison of network performance (Sahinoglu and Tekinay, 1999). Nevertheless, the following metrics include the most widely used criteria in network performance evaluation: Availability, Reliability, Accuracy, Robustness, Response time, Throughput, Workload, and Traffic control (Ghetie, 1997).

Availability represents the ability of the network to work almost continuously within assigned performance value. A value of 99.8% is typical. Availability is particularly a key metric for servers in safety-critical applications such as disaster monitoring systems (Hennessy, 1999). Accuracy may be defined as the probability of detecting errors (Ghetie, 1997). The reliability of a system is usually measured by the probability of errors or by the mean time between errors (Jain, 1991). Response time is the time taken to obtain response, after making a request (El-Rewini and Lewis, 1998). Throughput is defined as the transaction response time or number of transactions per second (Wu, 1999). Traffic control is especially an important issue for efficient utilization of network resources in wide and local area networks. Traffic control schemes can be classified into two categories, reactive congestion control and preventive congestion control. Reactive congestion control is the way to resolve network congestion after its occurrence. Preventive congestion control, on the contrary, is intended to prevent a network from its falling into congestion (Fdida and Onvural, 1995) and important measures for congestion control in a node are the average waiting time, the mean response time, and the average queue length (Puigyaner et al., 1998).

Despite the fact that each network may be subject to evaluation from wide range of perspectives, metrics in Table 1 find applications in many network evaluation studies. For instance, reliability must be carefully thought about for maintenance scheduling.

Performance Measures		
Measure	**Units**	**Potential Use**
Throughput	Processes/unit time	Productivity evaluation
Capacity	Processes/unit time	Planning
Response Time	Units of time	Usability evaluation
Utilization	Percent of time	Configuration
Reliability	Mean time to fail	Maintenance scheduling
Availability	Percent of time	Usability evaluation
Backlog	Number of processes	Usability evaluation

Table 1. Performance Measures (Molloy, 1989)

By using the information obtained from network performance evaluation, a network engineer can ensure and make plans to figure out that adequate capacity is available to support demonstrated demand and to allow growth requirements to be anticipated and supplied before bottlenecks occur (Tittel, 1996).

The performance of the network can be evaluated via measurements if a particular network system is built and running. For example, traditionally, three types of measurements, defined in (Wood, 1993), have been used in evaluating the performance of networks:

- Empirical measurements, which utilize real data,
- Simulation measurements, which construct a computer model of the program and then monitor the model's performance with simulated data, and
- Analytical measurements, which utilize an abstract model of a data structure to provide an evaluation in terms of abstract time or space.

Criteria	Analytical Modeling	Simulation	Measurement
Stage	Any	Any	Post-prototype
Time required	Small	Medium	Varies
Tools	Analysts	Computer Languages	Instrumentation
Accuracy	Low	Moderate	Varies
Trade-off evaluation	Easy	Moderate	Difficult
Cost	Small	Medium	High

Table 2. Criteria for Selecting Network Evaluation Technique (Jain, 1991)

Table 2 depicts traditional network evaluation measurements. Each of these techniques has its own unique advantages and disadvantages. Depending on point of view, any of these measurements can be utilized. For instance, a cost-conscious network administrator may be inclined to utilize analytical modeling with which small cost is associated. On the other hand, those who are concerned with accuracy may employ simulation, which usually presents higher accuracy than that of analytical modeling.These studies suggest that various metrics may be used to evaluate the computer network infrastructure of disaster monitoring systems.

Operator Performance Analysis Metrics

Human operators are a significant part of disaster monitoring systems. It could be argued that disaster monitoring systems will be as effective as human operators who are monitoring them and making real-time decisions using data gathered by such systems. In this study, we argue that human operator performance should also be evaluated as many errors in complex systems may be attributed to human operators. Although, in terms of evaluating operator performance, a variety of methods are used including real-time monitoring on the job, specially designed simulation exercises, checklists, and annual written performance appraisals (NRC, 1997), in this study, we focus on two most essential tools, that is, vigilance and workload, for measuring human performance with a disaster monitoring systems.

Operators' vigilance levels in safety-critical environments where constant vigilance is expected of an operator are critical element of system performance. In disaster monitoring system networks, operators monitor the network, provide maintenance and 24x7 operational support, which may lead to problems in sustaining operator vigilance. Vigilance is defined as a state of readiness to detect and respond to certain small changes occurring at random time intervals in the environment (Mackworth, 1957). Parasuraman (1987) indicates that when vigilance failures in complex monitoring occur, they may result either from a vigilance decrement or from a low overall vigilance level. System performance can be enhanced in a joint human-computer monitoring systems if computer monitors can compensate for lowered human performance. Teichner, (1974) suggests that human performance with a network, particularly in a monitoring task, is impacted by the tendency for vigilance to degrade within 30 minutes of task inception, which is the well-known vigilance decrement. A network operator needs to maintain his/her vigilance continuously in order to take control and corrective actions when and if the network fails.

Operator vigilance level may be measured using the Stanford Sleepiness Scale (SSS) developed by a group of scientists at Stanford University for assessing the vigilance of the human operator during a monitoring task (Stanford, 2006).

The Stanford Sleepiness Scale is a subjective fatigue and vigilance levels assessment instrument used to perform subjective vigilance assessment on human operators working with human-machine systems (Table 3). It is a multi-scale rating procedure, which assesses overall vigilance levels based on seven scale ratings: 1: Feeling active, vital, alert, or wide awake, 2: Functioning at high levels, but not at peak; able to concentrate, 3: Awake, but relaxed; responsive but not fully alert, 4: Somewhat foggy, let down, 5: Foggy; losing interest in remaining awake; slowed down, 6: Sleepy, woozy, fighting sleep; prefer to lie down, and 7: No longer fighting sleep, sleep onset soon; having dream-like thoughts. Thus, low score on the SSC indicate high vigilance levels, while high scores indicate low vigilance levels.

Degree of Sleepiness	**Scale Rating**
Feeling active, vital, alert, or wide awake	1
Functioning at high levels, but not at peak; able to concentrate	2
Awake, but relaxed; responsive but not fully alert	3
Somewhat foggy, let down	4
Foggy; losing interest in remaining awake; slowed down	5
Sleepy, woozy, fighting sleep; prefer to lie down	6
No longer fighting sleep, sleep onset soon; having dream-like thoughts	7
Asleep	X

Table 3. The Stanford Sleepiness Scale (SSS)

Another important factor that human operators should be aware of when monitoring a disaster monitoring systems is workload, which, generally referred to as mental workload, is the load associated with the mental process of the human operator, rather than (or in addition to) the operator's physical workload (Moray, 1979). One might suggest that operators may be more prone to making mistakes as they experience increased level of workload. Hence, in order to minimize the number order mistakes made by the operators, their workload must be constantly assessed.

Operator workload associated with the monitoring task may be measured using the NASA Task Load Index (TLX) developed by the human performance group at NASA Ames Research Center for assessing the subjective workload imposed by a given task (NASA, 2002). The NASA TLX is a subjective workload assessment tool, used to perform subjective workload assessments on operator(s) working with various human-machine systems (Figure 1). It is a multi-dimensional rating procedure that derives an overall workload score based on a weighted average of ratings on six subscales: Mental Demands, Physical Demands, Temporal Demands, Own Performance, Effort, and Frustration. Description of each subscale is seen in Figure 1. Each scale in the NASA TLX is presented as a line divided into 20 equal intervals anchored by bipolar descriptor (i.e., high/low). The 21 vertical tick marks on each scale divide the scale from 0 to 100 increments of 5. (http://iac.dtic.mil/hsiac/products/tlx/tlx.html, 01/2002). Thus, high scores on mental, physical, temporal demand, effort, and frustration on the NASA TLX indicate more workload, while low scores indicate less workload. On the other hand, high scores on performance indicate high operator confidence he/she has when performing a task.

Rating Scale Definitions

Title	**Endpoints**	**Definitions**
MENTAL DEMAND	Low/High	How much mental and perceptual activity was required (e.g., thinking, deciding, calculating, remembering, searching, etc.)? Was the task easy or demanding, simple or complex, exacting or forgiving?
PHYSICAL DEMAND	Low/High	How much physical activity was required (e.g., pushing, pulling, turning, controlling, activating, etc.)? Was the task easy or demanding, slow or brisk, slack or strenuous, restful or laborious?
TEMPORAL DEMAND	Low/High	How much time pressure did you feel due to the rate or pace at which tasks or task elements occurred? Was the pace slow and leisurely or rapid and frantic?
EFFORT	Low/High	How hard did you have to work (mentally and physically) to accomplish your level of performance?
PERFORMANCE	Low/High	How successful do you think you were in accomplishing the goals of the task set by the experimenter (or yourself)? How satisfied were you with your performance in accomplishing these goals?
FRUSTRATION	Low/High	How insecure, discouraged, irritated, stressed and annoyed versus secure, gratified, content, relaxed, and complacent did you feel during the task?

Figure 1. NASA TLX Rating Scale Definitions

Organizational Performance Analysis Metrics

Organizations hosting a disaster monitoring system usually operate in dynamic environments. In order for such organizations to survive in ever-changing environments, a number of organizational features have been suggested. For example, such essential organizational features as connectivity and communality (Monge et al., 1998), adaptability (Jarvenpaa, 1994), and interoperability (Park and Ram, 2004) have been discussed in the literature. Since, when hosting a disaster monitoring system, such organizations will be using a communication network to gather data from remote stations, one might argue that the relationship between the communication network and the organization should be studied.

The operational performance, efficiency and effectiveness of an organization have been linked with network performance in several studies. So and Durfee (1996) discuss how organization design can predict performance for a distributed data gathering task, and they classify the various factors that affect the performance of the organization into two broad classes: task-environmental factors and organizational factors. In their model, organizational performance is jointly determined by the features of the organization and the features of the task environment. Their model consists of three components: the organizational model, the task environmental model, and the performance model. The organizational model is tightly related to the task environmental model, which includes the tasks and environmental characteristics that affect the performance of the organization. In their study, task type, size, rate of change, and structure are important characteristics affecting the performance of organizations. In addition, response time, throughput, system utilization, communication cost, reliability, availability, and solution quality were also found to be important organization and network performance measures.

Orlikowski et al., (1995) examined communication networks that help organizational members work flexibly, collaborate effectively, and span organizational boundaries. They suggest that since communication networks are expected to increase efficiency by improving communication among organizational members, sharing information, and making decisions in a broad range of settings, organizational performance measures should address communication and decision making issues. Bakos (1991) evaluated interorganizational communication links from an economic point of view and suggested that organizations consider such measures as the efficiency of gathering and communicating information across participating organizational members, as well as cost reductions as measures of organizational impact. Similarly, Yang et al., (2001) suggest that an enterprise's network performance can impact its operational performance. With a high-performance enterprise network, they suggest, an enterprise can operate more efficiently and improve its competitive capability. These findings suggest that a variety of measures have been used for assessing the contribution of a network to organizational success. It could be argued that there exists a direct relationship between a disaster monitoring system performance and technical performance, human operator performance, and organizational performance.

CONCLUSIONS

Understanding the performance of disaster monitoring systems is a key to understanding their success. Various qualitative and quantitative measures and metrics can be applied in the characterization and analysis of such systems. Through evaluation studies, problems that impede a disaster monitoring system performance can be identified. The results can be used for disaster monitoring system performance optimization, system control, design, and capacity planning Complex interactions among disaster monitoring networks, human operators monitoring them, and organizations hosting them mandate that such systems' performance be evaluated from a number of perspectives using various measures. As failure of one component of disaster monitoring systems may have an adverse impact on the entire system, such systems should be evaluated using a holistic approach, a concept we advocate in this study. A combination of quantitative assessments of disaster monitoring networks and qualitative measurements of human operators' performance with disaster monitoring networks is important for understanding relationships between human operators and networks and the impact of both on organizational performance; such an approach is presented by this research. This study implies that disaster monitoring network performance, human performance with such networks, and organizational performance should not be looked at in isolation, but rather considered as interdependent and integral parts of each other. Technical metrics such as reliability, accuracy, and response time, certainly impact disaster monitoring system performance, as do users' performance with such systems. In turn, disaster monitoring system performance influences human performance, as well as the performance of the system that the disaster monitoring system serves. This study may be valuable to researchers and practitioners involved in disaster and emergency response studies, trainers in disaster managements, state and federal agencies, public sector managers, and administrators in planning the transportation of vital first-aid supplies and emergency personnel to disaster-affected areas, and in improving chances of survival after a natural disaster.

REFERENCES

1. Bakos, J. Y. (1991) Information Links and Electronic Marketplaces: The Role of Interorganizational Information Systems in Vertical Markets, *Journal of Management Information Systems*, 8, 2, 31-52.
2. Blommers, J. (1996) Practical Planning for Network Growth, Prentice Hall.
3. El-Rewini, H., and Lewis G.T. (1998) Distributed and Parallel Computing, Manning Publishing.
4. Fdida, S., and Onvural, O. R. (1995) Data Communications and Their Performance, Chapman & Hall.
5. Ghetie, G.L. (1997) Networks and Systems Management, Platform Analysis and Evaluation, Kluwer Academic Publishers.
6. Giladi, R. and Ahituv, N. (1995) SPEC as a Performance Evaluation Measure, *Computer*, 28, 8, 33-42.
7. Jain, R. (1991) The Art of Computer Systems Performance Analysis, John Wiley & Sons.
8. Jarvenpaa, S., Ives, B. (1994) The Global Network Organization Of The Future: Information Management Opportunities And Challenges, *Journal of Management Information Systems,* 10, 4, 25-33.
9. Jurison, J. (1996) The Temporal Nature of IS Benefits: A Longitudinal Study, *Information & Management,* 75-79.
10. Kumar, A., and Agrawal, P.D. (1996) Parameters for System Effectiveness Evaluation of Distributed Systems, *IEEE Transactions on Computers*, 746-752.

11. Kirner, G, T.(1997) Quality Requirements for Real-Time Safety Critical Systems, *Control Engineering Practices*, 5, 7, 965-973.
12. Lavenberg, S. S. (1983) Computer Performance Modeling Handbook, Academic Press.
13. Haring, G., and Kotsis, G. (1994) *Proceedings of the 7th International Conference of Computer Performance Evaluation, Modeling Techniques and Tools,* Vienna*,* Austria, Springer-Verlag.
14. Hennessy, J. (1999) The Future of Systems Research, *Computer*, 27-33.
15. Lindberg, C.B. (1995) Digital Broadband Network and Services, McGraw Hill.
16. Lirow, Y. (1997) Mission-Critical Systems Management, Prentice Hall.
17. Mackworth, N.H. (1957) Some Factors Affecting Vigilance*, Advancements in Science,* 53, 389-393.
18. Molloy, M. K. (1989) Fundamentals of Performance Modeling, MacMillan, New York, NY.
19. Monge, P. R., Fulk, J., Kalman, M. E., and Flanagin, A. J. (1998) Production Of Collective Action In Alliance-Based Interorganizational Communication And Information Systems, *Organization Science,* 9, 3, 411-433.
20. Moray, N. Models and Measures of Mental Workload, in N. Moray (ed.). (1979) Mental Workload: Its Theory and Measurement, Plenum Press, New York, 13-21.
21. NASA, National Aeronautics and Space Administration. NASA Task Load Index (TLX). Retrieved February 1, 2002, from http://iac.dtic.mil/hsiac/products/tlx/tlx.html.
22. Orlikowski, W. J., Yates, J., Okamura, K., and Fujimoto, M. (1995) Shaping Electronic Communication: The Metastructuring of Technology in the Context of Use, *Organization Science,* 6, 4, 423-444.
23. Parasuraman, R. (1987) Human Computer Monitoring, *Human Factors*, 29, 6, 695-706.
24. Park, J., Ram, S. (2004) Information Systems Interoperability: What Lies Beneath? *ACM Transactions on Information Systems* (TOIS), 22, 4, 595-632.
25. Puigyaner, R., Savino, N. N., and Serra, B. (1998) *Proceedings of the 10th International Conference of Computer Performance Evaluation, Modeling Techniques and Tools,* Spain, Springer.
26. Sahinoglu, Z., and Tekinay, S. (1999) On Multimedia Networks: Self-Similar Traffic and Network performance, *IEEE Communication Magazine*, 48-42.
27. Savolainen, V. (1999) Perspectives of Information Systems, Springer.
28. Smith, T.D., Johnson, W.B., and Profeta.A.J. (1996) System Dependability Evaluation via a Fault List Generation Algorithm, *IEEE Transaction on Computers*, 974-979.
29. So, Young-Pa and Durfee, H. E. (1996) Designing Tree-Structured Organizations for Computational Agents, *Computational and Mathematical Organization Theory*, 219-245.
30. Stanford, (Stanford Sleepiness Scale (SSS), Retrieved on 11/01/2006, from http://www.stanford.edu/~dement /sss.html
31. Stuck, W.B., and Arthurs, E. (1985) A Computer and Communications Network Performance Analysis Primer, Prentice-Hall.
32. Teichner, W. H. The Detection of a Simple Visual Signal as a Function of Time on Watch, *Human Factors*, 16, 339-353.
33. Tierney, L. B., Johnston, E.W., Lee, R. J. and Hoo, G. (1996) Performance Analysis in High Speed Wide Area IP over ATM Networks: Top-to-Bottom End-to-End Monitoring, *IEEE Network,* 26-39.
34. Tittel, E. (1993) PC Networking Handbook, AP Professional.
35. Wood, D. (1993) Data Structures, Algorithms, and Performance, Addison-Wesley.
36. WHO, (World Health Organization), (1999). Community Emergency Preparedness: A Manual for Managers and Policy-makers, Received March 28, 2005, from http://whqlibdoc.who.int/publications/9241545194.pdf
37. Wu, J. (1999) Distributed System Design, CRC Press.
38. Yang, C., Chen-Hua, F., and Yueh-Heng, T (2001). Enterprise Traffic with a Differentiated Service Mechanism, *International Journal of Network Management*, 11, 2, 113-28.