VOL. 10, NO. 5, MARCH 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

ENHANCED HYBRID FRAMEWORK OF RELIABILITY ANALYSIS FOR SAFETY CRITICAL NETWORK INFRASTRUCTURE

Chandana Priyanka G. H.[1], Aarthi R. S.[1], Chakaravarthi S.[1], Selvamani K.[2] and Kannan A.[3]
[1]Department of Computer Science and Engineering, Saveetha University, Chennai, India
[2]Department of Computer Science and Engineering, Anna University, Chennai, India
[3]Department of Information Science and Technology, Anna University, Chennai, India

ABSTRACT

This work proposes enhanced hybrid frame work for reliability analysis for Safety Critical Network Infrastructure. The proposed frame work enables design and development of web service for the safety critical systems to identify the component failures in the network infrastructure. The enhanced hybrid frame work of reliability analysis for multilayer in Safety Critical Network Infrastructure results in accuracy of identifying the failure of the component, failure modes of the component that makes the system more reliable and reduces the error rate in the network infrastructure. The Safety Critical Network Infrastructure requires a monitoring mechanism that can be used for public sector enables to detect failures as early as possible in the layers of the network. In order to work as a service provider for the critical components to the user a web service was designed and these failure results are used as database for efficient utilization of the data.

Keywords: SCNI, RBD, reliability analysis, CWAN, Web services.

1. INTRODUCTION

The phenomenal growth of the internet and mobile communication is playing an important role in the fields of air traffic control systems, telephone switching, real time military systems, medicine, remote monitoring and disaster management. Due to the extraordinary growth of the information-oriented society, today's world has become more dependent on information sharing through interconnected networks and find wider applications in space exploration, meteorological department, nuclear power station, educational institutions and business process management. In line with these developments, the size and complexity of computing systems have grown manifold from single processor based systems to multiple processor based one. Developments in communication bandwidth and processing capacity has further enabled the development of distributed and cloud computing. Today's computing environment is heavily dependent on networks for load balancing (web servers), resource sharing (storage arrays), data redundancy (database replication), security (cryptography), high capacity and availability (distributed and cloud computing). The tasks carried out by these systems vary from small scale programs to very large scale resource sharing networks that cater to the needs of local and global demands. Since all such systems remain interconnected, a heavy dependability on computer network necessitates fail-proof systems to ensure connectivity, availability, maintenance of bandwidth and performance. Each and every component of the network should comply with certain standards to ensure that these systems shall perform to the expected level at all the times and still remain fault tolerant.

2. PREVIOUS WORK

Several reliability models were developed to predict the component failure. A reliability prediction model predicts the rate at which a given component is expected to fail. These predictions help in the (1) selection of a suitable component for the desired purpose, (2) assess the stress level that each component can withstand, (3) development of possible alternative designs that are most suitable for the given purpose. The most critical problems concerning network reliability, modeling and analysis are summarized by Jereb (1999) as following and described briefly in the following paragraphs:

1. Connectivity measures.
2. Maxflow (capacity) measures.
3. Multicommodity flow measures.
4. Performability measures.

2.1(a) Connectivity measures

In 1970s and early 1980s, reliability was considered as the connectivity of the graph representing the network. In this case, a subset of graph nodes, called *K*, is defined. The most general measure of reliability is the *K*-terminal probabilistic connectivity, which is the probability that certain connections exist in the graph among the nodes in *K* (Hwang *et al*., 1981; Locks, 1985). However, connectivity is not able to properly reflect the degradation of the performance of the network. This is mainly due to the fact that a software or hardware malfunction may degrade the performance of the network while still remaining connected. During disconnection, the network shall remain dead and there shall be no way to measure the performance issue such as effective bandwidth and delay arising from rerouting.

2.1(b) Maxflow (capacity) measures

Later on, as the demand for communication bandwidth has grown the need to communicate given information within a short-time gained momentum. Under such a situation Lee (1980) defined network reliability as the probability of successfully transmitting the required amount of information from the source to the destination. Here performance indices were utilized by keeping the

maximum capacity of the network as the normalization factor (Hwang *et al*., 1981; Locks, 1985; Rai and Soh, 1991).

2.1(c) Multicommodity flow measures

The main difference between maxflow and multicommodity flow measures is that in the later, the reliability is measured by performance indices to the former but with the realized simultaneous transmission capacity among its endpoints as the normalization factor. This approach enabled inclusion of considerations on the impact of actual routing schemes compared to the maxflow measure approach. Detailed discussions are available in Barezzani *et al*. (1992) where usual definition of availability of a network component is extended to network availability.

2.1(d) Performability measures

Earlier definitions of reliability were mainly focused on the quality of the network components and the service provided. Depending on the topology and various components of the network, the reliability was affected. However, another point that should be given due consideration is that the demand for network services is not constant – and this variable demand may degrade the performance of the network. For example, in a heavily crowded network, the traffic routing can significantly influence the performance of the network. Thus, performability of a network is given importance in the study of reliability of network by Sanso *et al*. (1991).

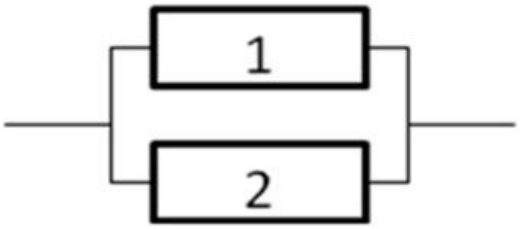
2.2. Reliability assessment

Over a period of time several techniques were developed for the assessment of reliability. The most widely used techniques in computing systems are reliability block diagrams, network diagrams, fault tree analysis, failure mode effect analysis, Monte Carlo simulation, and Markov model (MinXie *et al*., 2004). In a networked environment, knowledge of the reliability of all components is utilized for making prediction of the reliability of the entire network.

2.2.1. Reliability block diagram

A reliability block diagram is one of the conventional and most widely utilized tool for system reliability analysis (Bastani *et al*., 1992; MinXie *et al*., 2004). A major advantage of using the reliability block diagram approach is the ease of reliability expression and evaluation. A reliability block diagram shows the system reliability structure. It is made up of individual blocks and each block corresponds to a system module or function. Those blocks are connected with each other through certain basic relationships such as, series and parallels. The series relationship between two blocks is depicted by Figure-1a and parallels by Figure-1 b.

(a) Series blocks



(b) Parallel blocks

Figure-1. (a)(b) Relationship between two blocks - continued.

Suppose that the reliability of a block for module i is known or estimated, and it is denoted by R_i. Assuming that the blocks are independent from a reliability point of view, the reliability of a system with two serially connected blocks is

$$R_S = R_1 \cdot R_2$$

And that of a system with two parallel blocks is

$$R_p = 1 - \prod_{i=1}^{2} (1 - R_i)$$

2.2.2. Network diagram

Network diagrams are commonly used in representing communication networks consisting of individual links. The computation of network reliability is the primary application of network diagrams purpose of a network is to execute programs by connecting different sites that contain processing elements and resources.

3. RESEARCH METHOD

Combining powerful computation facilities (Safety Critical Systems) with high-speed digital communications (Network infrastructure) can lead to systems that are thousands of times more complex than would normally be considered in a hardware system, such as the electronic funds transfer system within the financial network or the supervisory and control mechanisms within the electric power grid. Such systems are referred to as Critical Infrastructure (CI).

3.1. Safety critical network infrastructure

A Safety Critical Network Infrastructure (SCNI) in Figure-2 is considered as a layered hierarchal network structure that provides high performance and only some layers are susceptible for congestion. It also provides an efficient management strategy to organize the network and provides several troubleshooting options. In addition to this, it also provides a policy frame work that specifies the filter rules to manage the network, and scalability options by dividing the network into several key functional units.

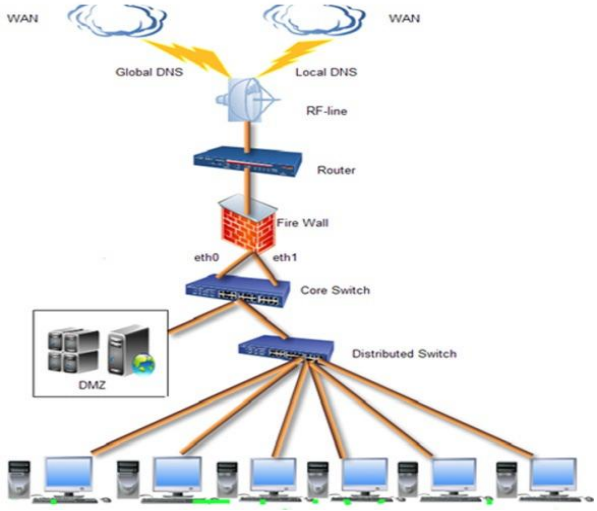


Figure-2. Safety critical network infrastructure.

3.1.1. Parts count analysis

From the below Tables 1 (a), (b), (c) list the major components and their quantity level are identified from the report. In the router, the hardware components of the network infrastructure components are redundantly present. So the frequency of failures is minimal. In case of router component the bus error crash leads to network failure. In other components of the network there is deviation from the normal mode of operation without total failure. Its results are equally harmful that effects on the system operation.

Table-1(a). Major components in core layer.

	Internal component name	Quantity level
Major components of core layer	RF Line	1
	Local DNS	1
	Global DNS	1

Table-1(b). Major components in access layer.

	Internal component name	Quantity level
Major components of access layer	Distribution switches	1
	Hubs	1
		1

Table-1(c). Major components in distribution layer.

	Internal component name	Quantity level
Major components of distribution	Router	1
Layer	Firewall	1
	Switches	3

3.1.2. Failure mode effect analysis

The factors that are considered for this approach are (1) fault identification, (2) potential effects of fault, (3) estimated or projected compensation, (4) identify, implement and document the recommended actions. The analysis process in the FMEA approach has the following columns the Risk Priority Numbers (RPN) methodology for analyzing the risks associated with potential problems identified during the FMEA (R and D staffs, 2001). The RPN is the critical indicator for determining proper corrective action on the failure modes.

Table-2.FMEA - DNS hardware components.

Hardware networking device	Hardware networking element problems	Hardware networking component failure mode	O	D	S	RPN	Effects of networking elements	
							Critical	Non critical
DNS failure	DNS failure	Trouble in resolving the names of other computers	**3**	**2**	**10**	**60**	DNS Failure	-
	Memory allocation failed	No free space to allocate the query	**4**	**5**	**1**	**20**	-	Performance Degradation
	Isolation of network segment	Power failure , network cable problem	**2**	**2**	**2**	**8**	-	Gradual Failure of The component
	Configuration problem	Network segment use the same DNS server	**3**	**3**	**3**	**27**	-	Operating at Reduced performance
	Generic routine problem	Configured DNS server was unreachable	**5**	**3**	**2**	**30**	-	Operating at Reduced performance

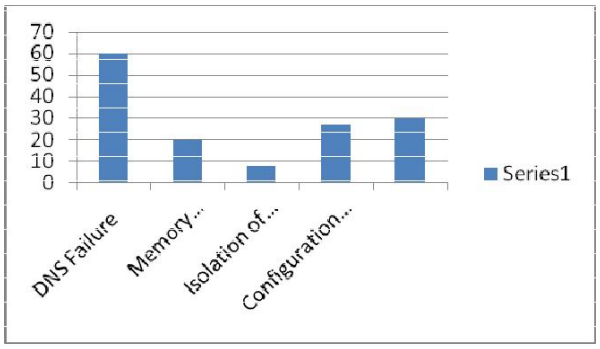


Figure-3. DNS hardware problems Vs RPN.

From Table-2 it is inferred that DNS failure happens when there is trouble in resolving the names of other computers. The other networking problems are memory allocation failure, isolation of network segment, configuration problem, and generic routine problem. The failure modes for DNS elements are no free space in allocating the requested query; network cable problem due to power fluctuation, network segment uses the same DNS server, configuration problem if the server status is not in reach. In Figure-3, the graphical representation illustrates that DNS failure where the chance of network down is higher. In case of genetic routine problems the criticality is moderate. The memory allocation failure and isolation of network segment, the state of criticality is at negligible level.

4. CONCLUSIONS

Effective communication across various services is essential as accessibility is an important consideration. The information about the failure probabilities from the SCNI model are to be properly utilized by the public sector. Creation of the web service for CWAN satisfies the above factor. The theory behind service oriented architecture are publish, find, bind are implemented using the web service for CWAN. The monitoring service is a web service which calls upon the services of core layer, distribution layer and access layer of their service methods. Using these three services the fault identification and correction mechanism of the three layers can be invoked remotely. The interoperability feature is performed by the web service for CWAN by separating the mechanism of access from the implementation. The client can access any one of the service (Core service, Distributed service, Access service) in CWAN by accessing only its service but the client is hidden from how the implementation process for the development of the web service.

REFERENCES

Barezzani. M, Pupolin. P, Zorzi. M, A New Definition of Transmission Network Availability with Applications, European Trans. On Telecommunications, Vol.3, No.4, July/August 1992, pp. 349-357.

Buttyan. L, Application Of Wireless Sensor Networks In Critical Infrastructure Protection: Challenges And Design Options, IEEE Wireless Communications, 2010.

Hyper Text Transfer Protocol Activity at Wide Web Consortium. http://www.w3.org/Protocols/Activity.html

Jereb. L, Network Reliability: Models, Measures, and analysis, 6th IFIP ATM'98, U.K, 1998, pp. T02/1-10.

John C.Knight, "Safety Critical Systems: Challenges and directions", ICSE proceeding of the 24th International Conference on Software Engineering, 2002.

Lee. S, Reliability Evaluation of flow network, IEEE trans. Reliability, vol. R-31, 1980, pp. 24-26.

Min Xie, Yuan-Shun Dai and Kim-Leng Poh. Computing System Reliability: Models and Analysis. Kluwer Academic/ Prenum Publishers, 2004.

Papadopoulos Y, Parker D, Grante C, " Automating the Failure Mode and Effect analysis of safety critical systems", High Assurance systems Engineering, 2004.

R and D staffs, "Examining Risk Priority Numbers in FMEA", Reliability EDGE, Volume 4, Issue 1, 2001.

Sanso.B, Soumis.F, Gendreau.M, On the Evaluation of Telecommunications Network Reliability Using Routing Models, IEEE Trans. On Communications, Vol. COM -39, 1991, pp. 1494-1501.

W3C, Web Services Architecture Working Group - Web Services Architecture, http: //www. w3. org/TR/2 004/NOTE-ws-arch-20040211/

Workshop on object-Oriented Web Services OOPSLA Tampa, Florida, USA.

Xie, M., Software Reliability Modelling, World Scientific Publishing Co., Singapore, 1991

Zio.E, "Reliability Engineering: Old problems and new challenges", Reliability Engineering and System Safety, vol. 94, pp. 125-141, 2009.