A Study on the Allocation of Network Resources Using Misson-Critical Networking

Aniket Uttamrao Vikhe[1], Dr. Amit Jain[2]

[1]Research Scholar, OPJS University, Churu, Rajasthan
[2]Assistant Professor, OPJS University, Churu, Rajasthan

Abstract

The deployment of mission-critical web-based services necessitates careful consideration of scalability, dependability, and performance in order to ensure that these services are always available. Furthermore, as the use of communications solutions grows, network operators must guarantee that their networks are capable of promptly and cost-effectively offering high-quality, innovative convergent services. A framework for delivering mission-critical network services on a continuous basis is presented. The risk is evaluated in a binary manner, i.e., there is no risk until the network system maintains the services for the whole period of the operation; otherwise, the mission fails, resulting in failure effect. To allocate network resources, the suggested framework is employed.

Keywords: *Continuity; Network; Reliability; Mission-Critical.*

I. INTRODUCTION

MCN (Mission-Critical Networking) is networking for application areas in which life or livelihood is at danger. Critical infrastructure protection and operation, emergency and crisis response, healthcare services, and military operations are all common application fields for MCN. In our complex environment, characterized by unpredictability, heterogeneity, emerging behaviors, and the requirement for dependable and rapid reaction, such networking is critical for safety, security, and economic viability. MCN should include networking technologies, infrastructures, and services that may reduce risk and improve connection for mission-critical information exchange among heterogeneous, widely dispersed, mobile users.

The deployment and dynamic configuration and evolution of communication networks that are trustworthy, robust, autonomic, secure, adaptable, and fast deployable to serve important missions and priorities is a major problem for MCN. The deployed networks must be able to offer safe and effective services including location determination of both authorized and unauthorized entities, Quality-of-Service (QoS) aware audio and video communication, emergency calling and alerting, and in-situ and distant sensing and control. Furthermore, cross-layer optimization, cognition, resource engineering, on-demand federation, and service-oriented design may benefit the efficient functioning of such networks, which often involve numerous and diverse resource-constrained components. Integration of MCN with the Internet is also critical in order to minimise deployment and maintenance costs while also improving reachability and ubiquity.

II. CONFIGURATION AND DATA COLLECTION ISSUES IN MCN

Quality-of-Service Issues

T.H. Szymanski and D. Gilbert tackle the fascinating and difficult subject of delivering mission-critical tele robotic control services across Internet backbone networks. These services must meet three important requirements:

i. essentially 100% restoration capability;

ii. small and bounded end-to-end queuing delays; and

iii. very low-jitter communications.

The authors offer methods for providing mission-critical services over the Internet with near-perfect QoS and near-perfect restoration capabilities. Background traffic is routed using various edge-disjoint pathways, whereas mission-critical traffic is routed using the principle of shared backup protection paths, or p-cycles. The idea of recursive stochastic matrix decomposition is used to plan mission-critical traffic in order to meet two constraints: (i) near-zero end-to-end queuing latency and jitter; and (ii) essentially-perfect QoS. Extensive simulations of a saturated Internet backbone network supporting tele robotic services as well as competitive background traffic are given to illustrate the usefulness of the suggested algorithms.

Security Issues

Unoma N. Okorafor and Deepa Kundur discuss security in directional wireless optical sensor networks routing and localization. These networks have the ability to deliver gigabit per second speeds while consuming relatively little power, allowing for burst traffic and a longer network lifetime. For mission-critical circumstances where high-speed connection assurances in hostile environments are required, untethered sensor nodes communicate directionally through free space optical communications. The research presents a low-weight, security-aware integrated routing and localization strategy that takes advantage of the benefits of wireless optical sensor networks' intrinsic connection directionality. The SIRLoS method, which uses the base station's resources and a hierarchical network structure to find topological information and detect security violations in neighborhood discovery and routing processes, is a circuit-based approach.

Configuration and Data Collection Issues

For MCN, I. Kulkarni and D. Pompili investigate the work allocation problem for autonomous underwater vehicles. Gliders and propeller-driven vehicles are the two forms of autonomous underwater vehicles (AUVs) in their model (PDV). Gliders spend less energy than PDVs, although PDVs may go quicker. There is a trade-off between speed and energy in this situation. The research proposes a paradigm for establishing an optimum vehicle crew based on job assignment. The framework generates an optimization problem that aims to: (i) maximize the team of AUVs' available energy after the mission, (ii) minimize the energy required by the team of AUVs to complete the mission, and (iii) maximize the minimum available energy of AUVs in the mission, all while keeping the total mission time under control.

III. SYSTEM MODEL

The following three service performance measures are used to describe service requirements: (a) Capacity: a metric measuring a system's capacity to transmit data. The terms bandwidth and throughput are interchangeable. The theoretically possible capacity is referred to as bandwidth. The system's or its components' realisable capacity is referred to as throughput. (b) Delay: the time it takes for one unit of data to travel from the source to the destination node. (c) Reliability: the ability to convey a service correctly at the specified time.

There are two aspects to the resource allocation for delivering end-to-end connection for RTMC services: Part 1 (Resource Allocation for Service Accessibility): the stream of traffic flow should be supplied by a succession of nodes connected by communicative links to maintain smooth service continuity between source and destination nodes. Part 2 (Resource Allocation for Failure Recovery): If a node sequence fails, the defective node sequence should be changed to keep the node sequence between two specified nodes intact. As a result, a failure recovery mechanism is required to restore the flow within the time constraints. There are two techniques to failure recovery: (a) creating a completely new sequence while sacrificing existing nodes, or (b) using part of the existing nodes for service accessibility.

To make the process of resource allocation suitable for the RTMC services the following additional steps have to be taken:

- Resource allocation process should be able to handle the largeness of link constraints and network topology connectivity
- This needs a fast path computation algorithm to support traffic flows within permissible delay boundaries.

- A proposal of self-healing method of failure handling in the autonomic computing environment is necessary to enable recovery from faults within the current service state

- Resource allocation has to be realized by developing the decision-making capability in the network.

The two types of TMC service needs are (a) temporal and (b) geographical. The former is concerned with transmission time limits, whereas the latter is concerned with the connection and reliability of service delivery infrastructure. The following is a method for assigning network resources to ensure the availability of end-to-end connectivity that meets temporal and geographical constraints. We suggest a two-step solution to the resource allocation problem. The following are the fundamental assumptions that underpin our model:

1. Network graph is directed and has no parallel/duplicate links.

2. Each node is perfectly reliable.

3. The capacity of a link is a non-negative integer value.

4. Data is transmitted in the network on the basis of the store-and-forward processing and the first-in-first-out queuing.

5. The two types of failures, i.e., breakdown and performance failures, are considered.

6. Whole traffic is transported over a single path only, and splitting of the transmitted data is not permitted due to time-sensitivity.

7. Software for computing the resource allocation is failure-free.

8. Mission-critical services are allotted over the network with the highest priority.

9. During fault-recovery cycle, no repairs/additional resources other than those already available on the network are considered.

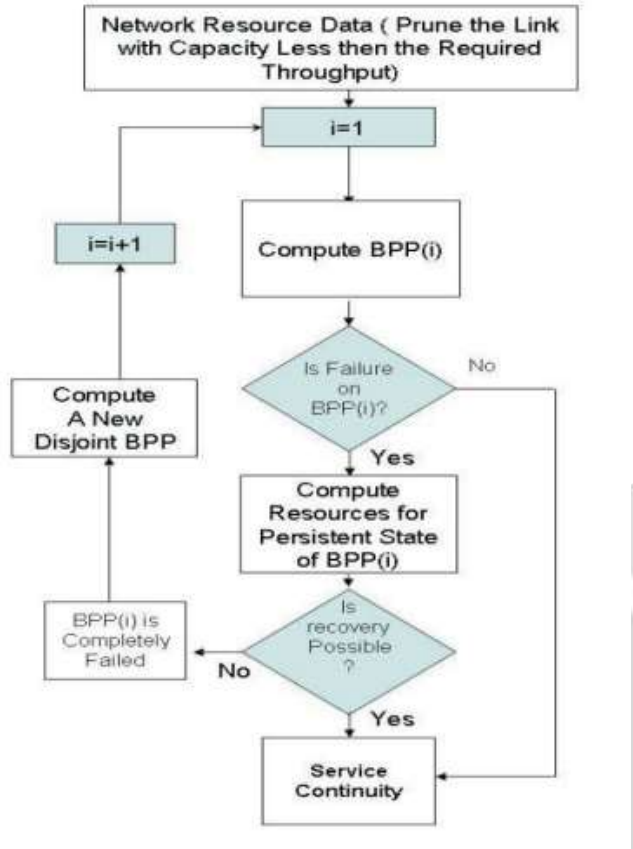

Figure 1: Flow-chart of the proposed fault-recovery scheme known as the 'self-node traction'.

IV. METHODOLOGY

The initial phase in our process is to determine the best-performing path, followed by resource allocation for failure recovery. The 'best-performing route algorithm' has been presented, which considers the triple (p, c, d) — reliability p, capacity c, and latency d — as the description of service performance and the associated risk indicators. The values are determined by the service provider's path selection criterion for assigning resources via various protocols for end-to-end connection between the source and destination terminals. The first step is to develop a path selection criterion that improves both reliability and performance. To put it another way, a chosen channel should meet the latency and bandwidth requirements with a high operational probability (low risk), i.e., the path should have a high uptime. For determining the shortest distance way, the minimal latency path, the maximum bandwidth path, and the maximum reliability path, a variety of path selection techniques are utilised. However, there are only a few methods that include reliability limitations with other path selection criteria. In the path selection process, the method integrates dependability, capacity, and latency, however it is only applicable for equal values of the component reliabilities. The technique suggested below, on the other hand, is applicable to networks with links with varying levels of dependability, capacity, and latency. The quantity of data to be conveyed influences the computation of the best-performing route. The shortest path algorithm is used in the BPP (Best-Performing Path) algorithm below. The suggested approach may be used on a data network with known triples (p, c, and d) for each edge. The weight of edge (u, v), represented as w (u, v), is equal to ln p and is determined by the weight function w: E [0, 1]. (u, v). As a result, the non-negative cost of transferring data from vertex u to vertex v is w (u, v) = ln p (u, v). A weighted directed graph G (V, E) and a source vertex s G are used as inputs to the method. The algorithm is identical to the shortest-path algorithm, except that the weights employed are connected to the above-mentioned w rather than the connection lengths.

Although the 'best-performing route' method can deliver the highest performance while maintaining the appropriate dependability, it may not be resilient to faults and hence does not safeguard connections from failure risks. Path

variety has long been recognised as a key aspect in network resiliency. Diversity can take several forms, including node, link, span, and segment. With the use of disjointing methods, the trait of route variety may be used to preserve mission-critical connections.

The suggested resource allocation technique is depicted in Fig. 1 as a flowchart. The related idea of a persistent state is established as the foundation for the network-based delivery of RTMC services. The fault-recovery technique in the flowchart in Fig. 1 is based on the concept of'self-node traction.' The goal of this fault recovery strategy is to offer backup capacity by allocating network resources from backup resources to provide backup capacity. The following are the four essential processes in this fault-recovery scheme: • Compute all discontinuous best-performing pathways, as BPP-1, BPP-2, and up to BPP-k.

- Assign permanent states to each of the pathways that are disjoint.
- Begin traffic routing along BPP-1 and use its persistent state to redirect traffic.
- Route traffic along the next discontinuous BPP and reroute traffic using its persistent state. Only when no path with assumed c and d levels is available between the source and destination terminals will the service be halted.

The purpose of self-node traction is to find the best node sequence for maintaining end-to-end connection without losing the service's present state.

V. CONCLUSION

The deployment of mission-critical web-based services necessitates careful consideration of scalability, dependability, and performance in order to ensure that these services are always available. Furthermore, as the use of communications solutions grows, network operators must guarantee that their networks are capable of promptly and cost-effectively offering high-quality, innovative convergent services. Vendors of hardware and software confront a variety of obstacles, including greater complexity, tight deadlines, diminishing budgets, and shifting standards.

VI. REFERENCES

1. K. Houliotis, P. Oikonomidis, P.Charchalakis, E. Stipidis, “An Efficient Approach to Designing Mission-Critical Systems, Case Study: Defensive Aid Suite (DAS) Systems”, 2017 International Conference on Military Technologies (ICMT), Brno, Czech Republic May 31 – June 2, pp 402-409, 2017
2. F. Ciccozzi, I. Crnkovic, D. Di Ruscio, I. Malavolta, P. Pelliccione, R. Spalazzese, “Model-Driven Engineering for Mission-Critical IoT Systems.” in IEEE Software, vol. 34, no. 1, pp, 46-53, Jan.-Feb.2017
3. J. P. Lobo, P. Charchalakis, and E. Stipidis, “Safety and security aware framework for the development of feedback control systems,” 10th IET System Safety and Cyber-Security Conference 2015, 2015
4. J. Chamber, Beyond the hype: Internet of Things shows up strong at Mobile World Congress, PC World, 2014.
5. O. Obi, a Deshpande, E. Stipidis, and P. Charchalakis, “Intrusion Tolerant System for Integrated Vetronics Survivability Strategy,” 8th IET International Safety Conference incorporating the Cyber Security Conference, Cardiff, 2013
6. P. Chołda et al., “Towards Risk-aware Communications Networking,” Reliab. Eng. Syst. Saf., Jan. 2013.
7. D. Miorandi, et al., Internet of things: Vision, applications and research challenges, Journal Ad Hoc Networks, vol. 10, no. 7, 2012, pp. 1497-1516.
8. L. Atzori, et al., The Internet of Things: A survey, Computer Networks, vol. 54, no. 15, 2010, pp. 2787-2805.
9. Daniel Câmara, Christan Bonnet and Navid Nikaein, Wireless Public Safety Networks Techniques and Challenges, Tutorial, IEEE LATINCOM 2010, Bogotá D.C., Colombia, September 14-17, 2010