Doctoral Dissertation (Shinshu University)

Disaster Ready Networks: With a Novel Management and Monitoring Approach

March 2016

Bishnu Prasad Gautam

ACKNOWLEDGEMENTS

It is the fact that the Ph.D. research project and the dissertation writing assignment would not be possible without the support of number of people. Therefore I am grateful to all my well-wishers, students, colleagues and supervisor for their support in number of ways and I would like to show my gratitude to the following people in particular.

First of all, I would like to express my heart-felt gratitude to Prof. Wasaki Katsumi. He provided me the opportunity to be a Ph.D. student of Interdisciplinary Graduate School of Science and Technology of Shinshu University in his lab, which was one of the best career choice that I ever have made. During the entire period of research as a Ph.D. student, I got a numerous encouragements, continuous guidance and constructive feedback from him and it was very fortunate to be his student since my master degree at Shinshu University. Without his support it would not have been possible for me to balance the Ph.D. research while at the same time working as a full time faculty member at Wakkanai Hokusei Gakuen University. I must say here that he is an excellent supervisor and a great mentor who continuously provided me the opportunity to build professional network, considerable amount of mentoring support and the encouragement to translate my ideas into the research hypotheses. Furthermore, I have a great respect, and the liberty that he provided to me to choose a research topic that I am passionate about and the valuable inputs during my tenure as a Ph.D. student. Without his continuous support, this research would not have been successful.

Beside this, I would also like to mention here that I came up with wonderful group of students each of them deserves my special gratitude: Dambar Raj Paudel, Shree Krishna Shrestha, Suresh Shrestha, Narayan Sharma, Dambar Pun and Amit Batajoo. I would especially like to thank some of the collaborator who also deserve my gratitude: Rajendra Paudel, Jhalak Paudel, Ramji Gautam, Rajendra Gautam, Prof. Sato Kazuhiko, and Asso.Prof. Kitani Tomoya. They provided support in numerous ways and I learned a lot from the site survey of Himalaya in Nepal and Soya regions of Hokkaido, Japan. This research was the inspiration of those visits for which I got a support from my collaborators. Working with local government and the public of Kaski, Nepal and Wakkanai, was a great experience that brought together the knowledge of forestry, electronics,

smart community and computer science. I also would like to thank my colleagues Bharat Pokhrel, Top Raj Gurung and Om Gnawali who continuously encouraged me to enroll in Ph.D. and help me in different ways.

In the end, I would also like to thank all of my current and past students, colleagues and staff of both Wakkanai Hokusei Gakuen University and Shinshu University for their continuous support and also to my valuable entire family members, without the support of them this research project would not have been possible

ABSTRACT

Network has become a critical infrastructure on which our society depends for their critical and non-critical activities. To provide network services continuously and consistently, proper management and monitoring of network is essential and the system must be operated in a stable manner at all the times. There are numerous research projects designed in this area have been continuously carried out. Despite the fact of research on the quality control, quality of service (QoS) and traffic monitoring of TCP/IP network have been carried out largely from the past, research without limiting to management and monitoring of network infrastructure but covering comprehensive study in the areas of service quality, operational management and monitoring of the services including automation of these services even in the extreme weather condition and disasters are rare.

In particular, there are limited studies that examined the characteristics and to analyze the similarities between wireless network under extreme climatic conditions and the network during disaster in which only a few nodes are able to continue the services. Though, network administrator and help of maintenance personnel are greatly required in network maintenance, many places lack these kinds of human resources leading to improper management of networks and inadequate monitoring. Thus there is a need for a research project that address on how to manage a network, especially at the times of disaster, with techniques that are mostly automated and do not require a lot of human resources. In this dissertation, I examined the characteristics of the unstable network and discussed the management and monitoring techniques that should be applied to increase stability of the networks that can also tolerate the disasters. Specifically, an investigation followed by survey and evaluation were performed for the following 3 problems which are related to unstable networks.

1. Lack of realistic models for wireless networks in challenging environments. Our proposal of the network model on the basis of fieldwork can enhance network stability.

2. There is little automation of networking monitoring services, especially involving physical spaces and assets. I propose a novel network monitoring and management devices to automate the monitoring and management process.

3. Scenarios such as disaster relief require a reliable and highly available and stable computational resources. We conduct development of interoperable and deployable services in fog computing infrastructure.

In order to address the first challenge, an experimental survey of Wi-Fi network was conducted in Wakkanai, Hokkaido Japan and Himalayan Region of Nepal. On the basis of this experiment, we proposed L1, L2 and L3 redundancy for stable link. Consequently, in order to manage and monitor the unstable network, it is clear that new automated monitoring and management approaches are required.

To address the second challenge, I propose to automate the network monitoring and management process by developing a mobile networking device, a novel concept and approach, which we called Tensai Gothalo in this dissertation. Specifically, while L2 network connection is unstable and disconnected, mobile robotic networking device (Tensai Gothalo) can detect the situation and proceed to the area where it troubleshoots basic networking problems to quickly repair and provide continuous networking services. In this way, monitoring and management of network can be automated and thus can improve the quality of communication infrastructure. This device can move to a predefined path and it has the capacity to monitor device, service and application. Furthermore, it can also be deployed in place of L3 router thereby co-operating with L2 switches.

To solve third challenge, I propose to develop a portable HA (Highly Available) cluster and developed a model of operational services developed within this infrastructure. We tested and evaluated these services in order to formulate a guidelines so that any organization can have such kind of portable infrastructure which can be rapidly deployed in disaster relief programs. In order to make this infrastructure portable and deployable with minimum downtime, I have recommended to utilize portable IoT devices. In this dissertation, this infrastructure is named as a fog infrastructure. To achieve the final goal of this research project, we have tested the applicability of

these tools in order to ensure business continuity of local government, organizations and educational institutions that could be certified as disaster ready networks by employing the approach discussed in this dissertation.

This page is intentionally kept blank

TABLE OF CONTENTS

List of Tables

List of Figures

List of Acronyms

Term	Initial components of the term
AJAX	Asynchronous JavaScript and XML
CWN	Community Wireless Network
DRN	Disaster Ready Network
DRR	Disaster Risk Reduction
DTN	Disaster Tolerant Networks
FTP	File Transfer Protocol
HA	High Availability
HFN	Hastily Formed Network
HTML	Hyper Text Markup Language
IETF	Internet Engineering Task Force
IoD	Inform on Demand
IR	Infrared
JSON	JavaScript Object Notation
L1	Layer 1
L2	Layer 2
L3	Layer 3
L4	Layer 4
L5	Layer 5
MRTG	Multi Router Traffic Grapher
NTOP	Network Probe
PHP	HyperText PreProcessor
PI	Priority Index
RIP	Routing Information Protocol

RT	Response Time
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol /Internet Protocol
TG	Tensai Gothalo
VRRP	Virtual Router Redundancy Protocol
WLAN	Wireless Local Area Network

Glossary

Term	Description goes here
Jyaguchi	Jyaguchi is a platform at which java based application can be built and exported to the client over a network. This very means of exporting java application over a network is supported by the underlying middleware technologies such as RMI and Jini
Tensai Gothalo	Tensai Gothalo, a network monitoring robotic vehicle developed during this research. Tensai Gothalo uses Wi-Fi modules to communicate with its slave node and also uses IR sensor modules that detects the path agent called the passage and assists an autonomous robotic vehicle called the Master Tensai Gothalo in capturing the powered off server
Zigbee	ZigBee is a wireless protocol based on IEEE 802.15.4- specification for the communication of Internet of things networks.
Wi-Fi	Wireless Fidelity
Campus-SIA	Student information management system developed during the study of Ph.D research and implemented at Wakkanai Hokusei Gakuen Unviersity

Chapter 1. Introduction

This chapter highlights the key issue of unstable networks of extreme climatic areas and during disaster situation thereby providing a technique such that these networks can be made disaster ready networks. To properly describe this work, this chapter presents a brief definition of unstable networks, the problem formulation and then highlights the methodological procedure for the research. The main contributions are then presented along with a structure of the dissertation chapters.

1.1. Research Overview

The history of computer networks roughly begins from around 1960 with the advent of ARPA project followed by ARPANET which becomes a large complex networks consisting of millions of nodes which we call the Internet today. Internet was created through a series of technological progress, inventions and innovations in fields ranging from electronics, computing and communications to social networks and business. This achievement have contributions from a significant portions of researchers, academicians, engineers and business sectors.

Network has become an inevitable social infrastructure for our society in the absence of which, it is almost impossible to continue our daily activities. This research project has been developed to understand the characteristics of unstable networks, finding out similarities of unstable networks and the networks failure during disaster. This research project aimed to develop a new model of network monitoring and management system by which one can achieve a better management system of their networks. However, there are numerous issues which need to be properly analyzed. One should ask what the differences between normal and unstable networks are. It is important to spot the instability of any networks? How can we manage such unstable network? How can we prepare the networks to safeguard from the potential disasters? How can we continue network services even after the disasters? Answers to such types of questions are vital in order to

properly manage and monitor the networks not only in the area of unstable networks, but also for entire networks which are disaster prone.

In order to provide network services consistently at all the times, a proper management and monitoring scheme needs to be deployed in any organization. The research regarding to quality control and traffic monitoring has been the subject of active research over the last two decades. However, a comprehensive study covering entire layer of TCP/IP especially focusing in the areas of service quality, operational management and monitoring of the services including automation of those services even in the extreme weather condition and disasters are overdue.

In spite of consistent progress in underlying technology of computer networks, one of the biggest problems with network management and monitoring is that they do not meet the requirement of monitoring and management during disaster and in the regions where climatic condition are extreme. We identified the need for such a comprehensive study which allows us to analyze the characteristics of such networks and recommend computer networking communities about how to design and maintain a network that is disaster ready. To address this broader issue, this project has been divided into three major project sub-components:

- Firstly, we conducted a comprehensive survey and analysis selecting proper regional areas of Hokkaido, Japan and Himalayan region of Nepal. We conducted few surveys in both areas, analyzed the issues and proposed a model network. We designed the network and did a simulation study and also subsequently tested the network physically. Our study suggest that a disaster ready network can be designed by providing appropriate redundancy in each layer of TCP/IP. From this study it has been clear that a proper monitoring scheme is required.

- Secondly, we developed a network monitoring and management device with movable feature. A device having multiple capabilities such as monitoring, and management, and it can perform basic networking services is a novel networking device developed in the field of computer networks. We designed, developed and tested the feature of this device in the lab. By adding further functions into this device, it can be deployed in the practical field. Regions where the computer networks are unstable due to

climatic condition and where the technical human resources is insufficient can benefit largely from our innovative device. We believe that this work bring new inspiration in the field of disaster management and monitoring of networks.

- Thirdly, we developed a portable HA (Highly Available) cluster that can be deployed for disaster relief program and can provide basic networking services. During a disaster relief program, it has often been suggested that communication infrastructures are highly prone to damage and consistent networking services are impossible to provide. Also, building up an infrastructure in a short time is very challenging tasks. To address this situation, a highly portable and reliable data center is vital. Our study suggest that managing such type of portable device would benefit any organization, companies or academic institutions to tackle with the situation after disaster. In this study, we developed highly effective and portable cluster on which we developed different kinds of networking services, categorized them and evaluated their feasibility to deploy during post disaster relief program.

1.2. What is an Unstable Network?

Stability and quality in networks and communication technology has become dominant issue over the last many years. For example, network stability, reliability, fault tolerant and delay tolerant have become buzzwords for many different networking technologies including cluster computing, cloud computing, fog computing and many disciplines of computer and communications technology. These terms are more or less related to provide reliable yet stable services to the users. Stable services are possible to deliver only in stable and reliable networks. Nonetheless, we found relatively little impact in the current literature about how and why the network services are difficult to deliver in unstable networks? And what kind of services can be provided in unstable networks? It is the fact that in current literature, we find remarkable mention of fault tolerant[1]–[6], delay tolerant networks[7]–[14], redundant networks[15]–[19], cognitive networks [20]–[25] community wireless networks [26]–[31]and many others related[32]–[39] computer technologies. Despite the interest of research in the above mentioned field, there is little

agreement among researchers as to what should exactly be defined as standard definition. Thus, we understand that these terms certainly have no common agreed definition in the literature of computer technology however this dissertation apply the reasonable justification while using these terms in the networks. This dissertation defines a self-consistent terminology for unstable networks and the concept of monitoring and management of such networks is based on an observation of existing definitions within the literature and my own insight with respect to network-based services, tools and application.

The concept of unstable network has been emerged in this research project since I was involved in the research of wireless networks in Himalayan region of Nepal [40]. The research conducted in the Himalayan region and the Soya region [41], [42] have few climatic similarities. Networks of both sites were greatly influenced by extreme weather and thus these networks were not stable. We termed these kinds of networks as unstable networks[43]. Though there are various research going on as mentioned in the literature, there are very few or negligible footsteps of research regarding unstable networks nor any movable and portable monitoring scheme has been implemented. From our practical survey and field experiences, we recognized that networks are unstable due to number of reasons. Some of the significant causes that attributed to unstable networks are power outage, signal loss, extreme weathers, disaster effect etc. Shiratori et al [44], [45] have significant contribution in how to build a never die networks that could survive in disastrous situation.

This research aims to manage and monitor such kind of unstable networks in order to qualify these networks with more reliable services. Essentially, the idea is to provide stable network services by using redundant link so that the subscribers of the networks can utilize networks without worrying about the network outage. In other words, these networks aimed to be fault tolerance network. Providing fault tolerance capacity into the networks certainly enable the reliability or stability. The approach taken by us in order to provide stability includes redundancy, pre-disaster measure and robust monitoring system. In this way, the quality of network services can be uplifted. This level of service assurance requires the redundancy in different layers of TCP/IP networks and also the robust system to monitor and manage the network.

1.3. Problem Formulation and Research Assignment

We witnessed that for more than 50 years of history, computer systems have evolved in a twisting way of centralized system to distributed system. Computer history experience its journey from being huge centralized processing power to distributed to again moving into more federated and collaborated cloud computing systems. Between these developments, the progress in network bandwidth has tremendous achievement. Nonetheless, this story does not apply to whole regions of world. There are still a place where networks are not reliable and millions of users are still deprived of stable network services.

For example, during our early research in Himalayan regions, we found extremely challenging issue that the networks of these areas are unstable and unreliable. Due to the power outage and without proper early scheduling, these networks are often interrupted in a frequent manner. In order to overcome this issue, we have come up with number of technique and considerations that could address this problem. Some of those issues which necessitate a thoughtful considerations are provided below:

Issue 1: Networks in geographically challenged areas are vulnerable to disaster, very unreliable and unstable

Issue 2: How can we sort out management and monitoring challenges of these area's networks?

Issue 3: How can we manage the network where network administrator are not available? (Network automation)

Issue 4: How to qualify unstable networks to disaster ready networks?

Issue 5: What sort of services can be deployed in these kinds of networks?

Issue 6: How can we continue the services in case the disaster happens and how can we continue the service as pre-disaster?

Similarly, I was involved in number of research[40], [46] which were geographically related to Soya region of Hokkaido, Japan. At the time of this research, the field of unstable networks and disaster readiness in terms of network management and monitoring was still less explored. We know that research papers describing the redundant networks and the practical

experiences are published in number of occasions and can be found profoundly in the literature. However, the research regarding unstable networks, its monitoring scheme and the services that can be hosted in such networks are less reported. To simplify the problem formulation, we categorized the above issues into three major research sub components which are listed below:

Research Assignment 1: Conduct a survey of unstable networks, analyze the characteristics of unstable networks and propose the network model that address instability.

Research Assignment 2: Propose a automation framework for network monitoring and management process

Research Assignment 3: Develop a deployable fog infrastructure as a model service infrastructure of DRN (Disaster Ready Networks)

1.4. Research Objective

The current state of the art in monitoring and management of networks relies solely on underlying protocols and commands (e.g SNMP, ping, traceroute etc) which can sense whether the packet are reachable or not. Monitoring tools such as MRTG, Nagios and NTOP also utilize underlying protocols to monitor the networks. The nodes send sensory information relying upon the underlying protocols and these nodes have no capacity to move and monitor surrounding situation such as power outage and other factors that can be the cause of network disruption. After getting the information about reachability, sensory nodes of monitoring device generates the report about service disruption. In contrast, our work introduces a novel approach of monitoring and management in which we propose to deploy a node that can not only sense about service disruption but also can supplement the network by being an agent of outage node and continue the network services. Furthermore, it provides power supply in case the nodes are out-functioned or mal-functioned due to power outage. The problem of power outage are not significant in developed countries, however, this is being one of the crucial problem in Himalayan regions of Nepal and many other regions around the world. Furthermore, this situation also looks similar when natural disaster hampers the energy infrastructure co-related with communication infrastructure.

Specially, this work propose to utilize movable network device that can continuously monitor and manage some basic network troubles. This capacity enables computer networks to be more disaster ready in number of ways. For example, network administrator can be benefited with time so that he can prepare to enhance the network that can tolerate natural disaster.

More importantly, In order to address the issues mentioned in section 1.3, we propose a novel model of networks called Disaster Ready Networks (DRN) which utilizes the redundancy in each layer of TCP/IP. We did a survey in order to test the coverage of redundant link thereby providing a stable network that can sustain a disaster. We consider redundancy as an inevitable approach to provide stable services because failures are still common problems in current data centers [47]–[53]. For example, there are sufficient report of failures which are related to server, link, switch, hub and various device failures due to hardware, software, power outage and weather related problems. The probability of failures increases as the size of networks increases. Therefore, fault tolerance in DRN requires redundancy not only in physical connectivity but in entire layer of TCP/IP and robust mechanisms to monitor and manage this networks.

Furthermore, a detail study of redundancy was conducted. This survey task was also modeled by using simulation tool and a number of experiments were conducted. This dissertation proposes a model of disaster ready networks that can suit the geographical regions where extreme climatic condition often hamper the networks, services and application. Furthermore, it proposes a workable solution that can monitor and manage those kinds of networks without requiring much human interferences. The proposed mechanism can offer a working solution that can well monitor the network and can perform some basic network trouble shootings tasks by using lab grown device which we call Tensai Gothalo. The proposed mechanism and the device employs a number of technologies which are not limited to TCP/IP but also to the broad area of robotics, electronics, computer science thereby leveraging a multidisciplinary working platform.

To summarize, the purpose of this research work is to investigate the possible framework of management and monitoring applications of hardware and software systems. We know that there are a number of approach available to manage and monitor the networks. However, it is the fact that management and monitoring of unstable networks and disaster ready networks lacks the

ideal solution for structuring management applications. In this dissertation, we develop, test and evaluate the merits and limitations of newly developed management and monitoring framework through following an unbiased approach, that aims at to monitor, manage and provide emergency detour network where mobility in terms of physical movement can really benefit to build more flexible, scalable and robust management hardware systems. Furthermore, we developed a series of model services that can be offered in those kinds of networks and investigates how this monitoring framework can be applied in such kinds of networks.

1.5. Methodological Background and Approach

The major contribution of this dissertation includes a significant portion of network monitoring, management and the applications that can be employed in unstable networks. Similarly a compelling focus lies on the very specific consideration of redundancy in different layers of TCP/IP networks, monitoring of such networks and the services that can be built upon these networks. There are numbers of problems that can be arisen while monitoring and managing such networks. Nonetheless, there are no specific or standard method that can recommend the best possible architecture which can survive in extreme weather. Due to the fact that network monitoring and management technology is not a new facet, a numbers of approaches and the issues have been proposed. However, most of the approaches are proposed which are feasible to apply only in a stable networks. In other words, previous concepts are not appropriate to apply in the regions where the underlying condition of the networks is not suitable.

This dissertation proposed an architecture of managing an unstable Network by using lab grown IoT devices which continuously monitors the health of networks and try to provide network services in a very minimal downtime. The proposed architecture utilizes the different kinds of network devices including the lab-grown Tensai-Gothalo which is capable of providing different kinds of services such as monitoring, management, routing or switching. Furthermore, it proposes an architecture of micro-data center that can be launched in unstable networks and the platform at which different kinds of services can be built upon, published and finally be utilized by the end users.

A series of case studies that can contribute to this research project have been conducted in real field in order to measure the instability of the network. On the basis of real world experience, an architecture of stable networks has been proposed that can properly be monitored and managed. Similarly, experiments have been conducted in different layers of TCP/IP by using simulators followed by with real hardware. In order to maximize the quality of networks, a special emphasis has been given for redundancy. As a practical scenario, we surveyed the potential of establishing redundant Wi-Fi networks in schools in the Soya region of Hokkaido to proactively create a bypass communication network that can be used if a natural disaster occurs. During emergency situations such as earthquakes, tsunamis, and floods, a traditional disaster response may not be able to provide adequate communication services to emergency-management teams. To explore the potential of establishing an emergency survival communication network in Wakkanai, Hokkaido, we conducted a medium-scale trace-driven study of redundant networks to determine how to decrease disaster risk. We set up wireless nodes at four network locations of different sizes, including an access link between the Wakkanai city office and Wakkanai Hokusei Gakuen University networks. Furthermore, we model the optimal redundant topology and discuss the simulation result. By proactively establishing a redundant wireless network as a detour emergency route using our approach, an organization can rapidly reduce disaster risk.

During the course of this dissertation, the above mentioned issues were analyzed to produce a workable concept that provides a solution for the problems mentioned above. Furthermore, a number of survey, and the number of prototype system (Jyaguchi Fog) including hardware devices (Tensai Gothalo) were developed and implemented in the lab. The principal conclusion and contributions of this dissertation can be seen as a network design model that is based on redundant architecture which is monitored by using movable network devices having high-performance results for trouble detection while still managing the networks that can sustain unstable weather. Furthermore, a set of services having proper categorization semantics which can be deployed in these kinds of networks are also elaborated.

This research conducted a theoretical and practical study of the literature in order to provide a framework for a disaster ready network. This work includes entire process of constructing a network with redundant link, monitoring of the network by developing an innovative device called

Tensai Gothalo, developing different types of services that can be hosted in these networks and develop a portable data center that can be deployed in case the disaster occurs. During the research periods a numbers of surveys were carried out not only in Soya region but also in Himalayan region of Nepal. Then a sample network in both areas were constructed and investigated. Hence, this study uses both theoretical and practical approach to come to the conclusion.

Finally, in order to meet the objective of this research, firstly a literature review was conducted to analyze theoretical concepts related to unstable networks and disaster readiness and to identify key issues of such networks. Furthermore, we designed our research methodology in more systematic timeframe and a number of sub-projects were implemented. The detail methods and approach taken is described below.

1.5.1. Research Approach

In order to accomplish our objective mentioned in section 1.4, we divided the projects into multiple sub-projects. Firstly, we started to survey a networks which are not stable. For example, we did detail survey of community wireless networks of Himalaya[40], [46] and the network of Soya areas of Hokkaido[41]. Fortunately, author has a good advantages of being from Nepal and has long working experience in Soya regions, conducting surveys in these areas has less administrative hurdles. After surveying and analyzing the local issues, we proposed a more reliable networks with redundant links and other recommended measures that should be applied in these networks. On the basis of our survey and the issues identified from unstable networks, we proposed a more robust network supplemented with redundant links. The proposed networks was again tested in Wakkanai city followed by number of simulation.

Secondly, we would like to automate the monitoring and management issues. In order to accomplish this objective, we proposed to design a movable network device by which a network can properly monitored and also managed while there is a lack of network administrator. Similarly, this device would provide network services in the case the primary network goes offline.

Thirdly, we propose to model the services computing infrastructure that can be hosted in such networks. We called this infrastructure as fog computing infrastructure.

As mentioned above, we took more practical approach rather than solely relying upon theoretical approach of study. Our approach of study utilize empirical data and experience that can be gained from the real field. There are several reasons why this research is performed with such approach. The strong focus on the objective of computer networks management in extreme climatic regions is highly important to us because, our study can benefit practical problems that has been faced by the society of such regions. As being a researcher in the field of computer science and engineering, this study brings newer possibility to face with post disaster management of networks. The results of our research project, also reflect and express the networking societies with more practical and reliable output. Our output are not provided in abstract forms rather they are provided with working model and devices. We believe that our study offers substantial possibilities to enhance the quality of computer networks that can sustain not only the extreme climatic condition but can also be used for post disaster relief program.

1.5.2. Prototype Development

In order to accomplish our objective, we implemented number of porotype related to this dissertation. First of all, we designed a redundant network that can represent unstable networks. We analyzed this network and found out the vulnerabilities of such networks. Afterwards, we modify this network so as to make disaster ready networks. A number of surveys was carried out in Soya region and Himalayan region. On the basis of these surveys a detail simulation study was carried out.

Secondly, we designed and developed a monitoring device which we call Tensai Gothalo [54] that can monitor such networks and also be able to trouble shoot fundamental network problems. We further developed an enhanced version of this device by using IR sensor and obstacle avoidance sensors so that the device can proceed to the targeted areas to trouble shoot the networks. Furthermore, we developed few services and categorized those services into three sub-categories: mega services, macro services and mini services. These services are considered to be hosted in unstable networks. Experimentation has been done to monitor and manage these services by creating HA cluster. In this way, we have conducted our research.

Thirdly, we developed a HA (High Availability) cluster by using IoT devices. Our purpose of developing this HA cluster is to provide a movable and portable data center that can provide network services during disaster. We called this cluster as fog infrastructure.

Finally, we developed number of services and categorized these services as mini, macro and mega service.

1.5.3. Experiment and Evaluation

Experiment was carried out for each sub-projects. As all sub-projects are equally important to deepen our understanding and to address our research issues, we conducted experiment for each sub-projects. Some experiments are directly related to our system developed in the lab whereas some are related to the research field and some are related only with simulation. The detail of each experiment are explained in corresponding chapters. On the basis of those experiment and evaluation, appropriate conclusion has been made.

1.6. Summary of Major Contribution

The major goal of this dissertation is to justify that traditional ways of disaster preparation is not sufficient, and that new approaches that can better enhance the tolerance capacity of entire networks is required. This dissertation introduces one such approach called *A Novel Management and Monitoring Approach*, and presents techniques for designing and constructing redundancy in each layer of TCP/IP networks along with monitoring and management device that ultimately contribute to pro-disaster readiness in computer networks. By applying this novel approach, local government, organization or the communities can have better solution for the disaster management and relief program. This research fills a gap in the current literature by experimentally surveying, simulating, developing and examining the role of monitoring and management system which is portable and deployable.

This works are disseminated through in various forms such as in the forms of articles in journal, conference proceedings or in technical reports of the academic society with which the

author is affiliated. Though I have not included all the published papers, the major contributions and the relation of those articles with this dissertation is highlighted and some of the references from those papers which are not elaborated in this dissertation are included.

The most notable article was published in the IEEJ Transactions on Electrical and Electronic Engineering. This article presented the model of redundancy in each layer of TCP/IP networks and the survey conducted by the authors in relatively severe climatic regions of Hokkaido, Japan. A model presented in this article can be a good example for the network communities who can take references of this work while deploying the networks in extreme weather or in disastrous regions. The elaborated version of this article will be presented in Chapter 3 of this dissertation. The second major publication appeared as a journal article in International Journal of Future Computer and Communication. This article discusses the development of robotic vehicle that can monitor and manage the unstable network presented in previous article. The core concept of network monitoring and management has been discussed all over the dissertation however the detail concept with PHY layer is extended in Chapter 4 of this dissertation. The paper regarding this chapter was submitted for publication to Elsvier Journal of Applied Research and Technology in October 2015. However, no decision for the publication has been available till the completion of this dissertation.

The content of Chapter 5, 6 and 7 were well presented among the research community and published in the SIG technical reports of IPSJ-ITS society of Japan.

Other publications are not directly used in this dissertation however if any parts are included in this dissertation are genuinely referenced.

1.7. Structure of Thesis

The rest of the dissertation is organized as described below: Chapter 2 presents the detail literature review along with important definitions of the core concept of this dissertation. In the further course of the chapter, the summary of core concept of the dissertation is described in order to visualize the flow of the dissertation.

Chapter 3 focuses the survey of unstable networks conducted in Wakkanai city. In this chapter, we have highlighted the shortcomings of networks in Soya region of Hokkaido. We have also given how such kind of networks can be upgraded by providing multiple links and redundant resources. This chapter creates the foundational theory why redundancy is required in order to resolve unstable networks and qualify them to be Disaster Ready Networks (DRN)

On the basis of Chapter 3, we understand the importance of monitoring and management of unstable networks in order to qualify such networks to disaster readiness. Therefore, we introduce the concept of deploying monitoring networking devices in Chapter 4. It shows how to accurately proceed to the trouble server by using IR sensor. Specifically, it describes the design and implementation of the IR sensor based obstacle avoidance and movable networking device, which implements our own IoD (Inform on Die) protocol steps. Specifically, it introduces a PHY layer of monitoring device which we named Tensai Gothalo (TG). In this chapter we have given substantial space to describe how IR sensor can be utilized for sensing the path and obstacle avoidance. This chapter actually try to discuss how can we manage and monitor DRN and why such kind of innovative monitoring device is required. Our discuss lead into the requirement of services that can be deployed in DRN. Thus, Chapter 5 mainly discusses the introduced prototype implementation of HA cluster which can be deployed during disaster. The objective of Chapter 5 is to provide a cost effective HA cluster that should be available for every organization. In the case of disaster prone areas, a portable HA cluster is recommended. Chapter 5 highlights the design and development strategies of such HA cluster. We believe that for any disaster ready networks, such kind of portable cluster would play a significant role.

Chapter 6 further positioned this work by giving further experimental infrastructure of fog services. This work indicates why DRN networks requires portable fog infrastructure which can be carried out by TG and deals with some of the necessary premises to understand how the introduced concepts are important for DRN networks and DRN datacenters. The example of services presented here have low granularities.

Chapter 7 presents an example of mega service that can be hosted in DRN datacenter. The intent of providing this chapter is that we should be able to deliver the different types of services

including mega services in DRN datacenter. Once, we are able to host from mini, macro to mega services, we will be able to fully utilize such networks and monitoring of these services by using TG could show complete framework of developing, monitoring and management of DRN networks and DRN datacenters.

Finally, we have presented a conclusion, future directions and closing remarks in the last chapter, i.e chapter 8.

Chapter 2. Background and Literature Review

In this chapter, we present the definition of Disaster Ready Networks (DRN) and related works. We first describe about DRN networks and then present current research works. Based on our DRN definitions, we try to present the overview of implementation details of our research work. We proceed with our discussion of related work from four major aspects: (1) Enhancement of Unstable Networks, (2) Automation of Monitoring and Management Process of Unstable Network, (3) Fog infrastructure (4) Deployable services in fog infrastructure and their classification. We also describe how to implement cloud services in such fog infrastructure. What is the basis of classification of the services so that end-users can utilize the services during disaster? Finally, we describe a mega service or application that can be deployed as a local service rather than hosting in the cloud.

2.1. DRN (Disaster Ready Networks) and Motivation of the Study?

2.1.1. Trend of Natural Disaster

In section 1.2, we understood that there are still significant portions of networks which are not stable. Furthermore, if a disaster happens these networks may face multiple failures in the

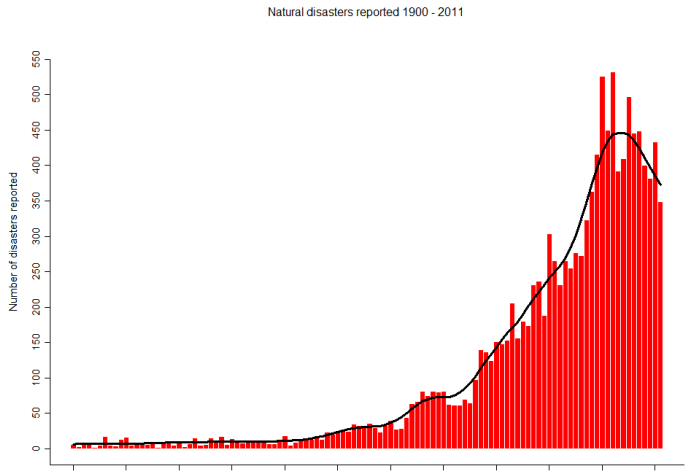


Figure 2-1: Trend of Natural Disaster

physical infrastructure disconnecting and degrading services provided in these networks. Considering that disaster recovery may take days or even weeks, networks can become vulnerable to post-disaster also and sequential correlated failures may require for a relatively long recovery period[55]. Some disasters have damaged remarkable portions of networks. Figure 2-1 (data source: http://www.emdat.be/natural-disasters-trends) shows that the number of natural disasters occurred since 1900 to 2011 is increasing. Similarly, in 2008 Shichuan earthquake which damaged 30,000 kilometers of fiber optic cables and 4,000 telecommunication offices [56]; Figure 2-2 (data source: http://www.emdat.be/natural-disasters-trends)shows increasing trend of person killed during natural disaster.

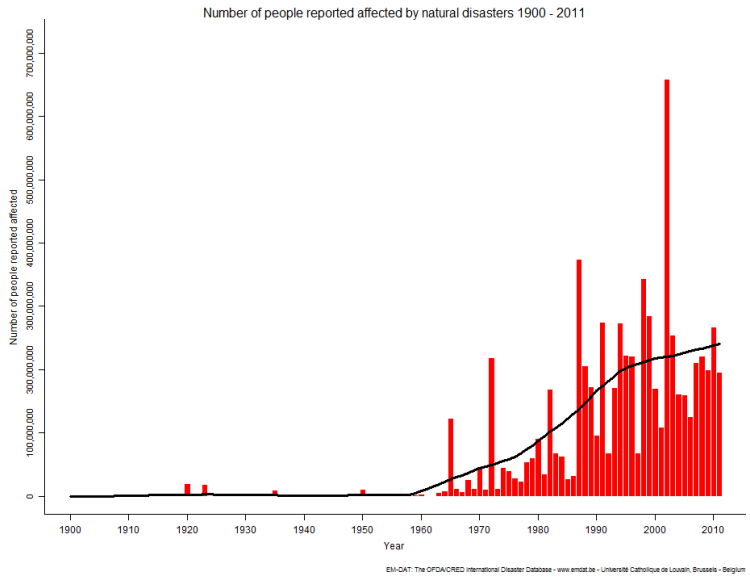


Figure 2-2: Number of people afffected by natural disaster

On 11th March 2011, an earthquake registering 9.0 MW occurred in the Pacific Ocean with an epicenter 130km east of Sendai City in northern Japan. Due to this earthquake approximately 1.2 million fixed telephone lines and 15,000 mobile base stations were unusable and 80% of these breakdowns in both cases were caused by widespread and prolonged power outages[57].

More recently (on 25th April, 2015), there was an earthquake in Nepal which killed more than 9,000 people and damaged a great deal of infrastructure in the country. While the loss of

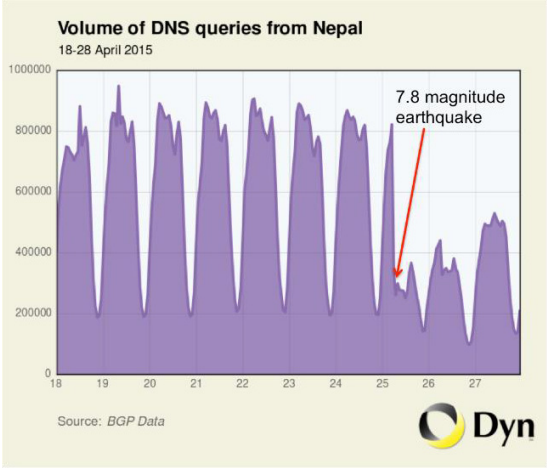


Figure 2-3: Instabilities of Network

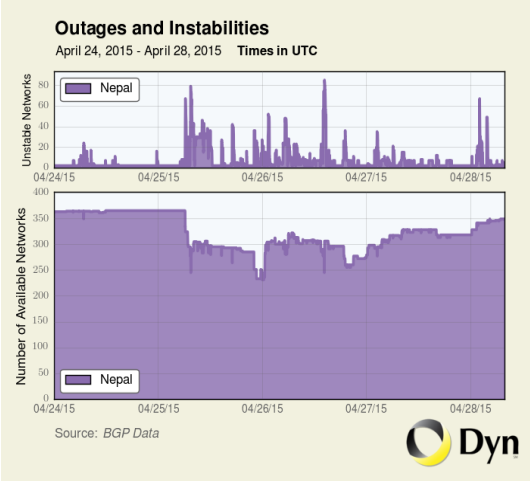


Figure 2-4: DNS Queries

Internet connectivity is insignificant in comparison to the loss of life, the connectivity among domestic networks and international was unstable. Figure 2-3 and Figure 2-4 (data source: http://research.dyn.com/2015/04/earthquake-rocks-internet-in-nepal/) shows the situation of network performance during that time.

2.1.2. Understating Disaster Readiness and Significance of Research

To minimize impact of natural disaster, communication infrastructure is very important and it should be recover without taking much time in order to enable smooth relief operation. However, if the network infrastructure has a great damage, the underlying economic loss due to this damage would be remarkable. Thus a network needs to be disaster ready. Disaster Ready Networks are such kinds of network which can deliver service even after the disaster without getting much damage to its infrastructure physically and virtually.

We noted that the very nature of networks at disastrous situation is resembled with the nature of unstable networks at Himalayan regions of Nepal and Soya regions of Hokkaido, Japan. We observed that these two areas have various similarities in terms of computer networks and its management. The networks of both of the regions are unstable. However, there is no comprehensive

study regarding how unstable networks in these regions can be enhanced to be more robust and disaster ready networks. What is the proper way to monitor these networks? Despite this question, it is very difficult for network communities to predict and specify where and when network service disruptions will take place. Furthermore, we also could not inform the users about how long the disruption will take place. Therefore a very comprehensive study of network monitoring and management is essential before natural disasters occur. Accordingly we also need to understand how networks respond after a natural disaster. Thus, understanding the degree of readiness before natural disasters is an important problem to study.

We define disaster ready networks as those kind of networks which have high degree of readiness and can respond well even after the natural disaster. Degree of readiness can be increased by applying various techniques of redundancy, monitoring and management. In this study we apply all of these techniques and also developed a device that can monitor and manage such networks.

2.2. Related Work

DRN includes broad areas of research while this work does a first of its kind in depth research with a novel solution approach. In this dissertation, we include only those areas of research that is related to enhancement of unstable networks along with the field of network monitoring and management that can shed light into this field and that can directly inspire this research. Related work, such as deploying services in cloud or fog computing infrastructure is also included as work related to this area is still lacking in the literature. Our work also considers service infrastructure built upon IoT devices because our experience suggests that in order to manage unstable networks well, we need to upgrade and qualify unstable networks to be disaster ready networks. Service infrastructure built upon IoT devices are portable and relatively cost effective. Other areas for unstable and disaster ready networks include management and monitoring techniques, tools and environments for management design, architecture refinement from specification to implementation, and case studies of deployed network management tools, devices and scheme. As this dissertation work is a combination of a number of projects, related work is mentioned in the corresponding chapters.

Due to the broad nature of this research, we begin with a wide foundation examining surveyed data that motivates this research. Then we proceed with examining the phenomena and technologies that can be implemented in the project thereby focusing on how our proposed solutions can address these problems and can contribute with additional results. The next section presents a discussion of how to model and describe the key technologies and also introduces terms related to our issues. In each chapter, we introduce related references work from other researchers in this emerging area of research. In each sub-section, we briefly review work related to unstable networks, fault tolerance, monitoring automation and other related works

2.2.1. Enhancement of Unstable Networks

First of all, we need to identify unstable networks after surveying and analyzing the characteristics of networks. Survey should include the records of network trouble, its occurrence and other related factors which are causing network to be unstable. Once we identify such networks, we need to design how these networks can be enhanced to be more stable and reliable such that even in disastrous situations, these networks will be able to continue their services. In order to analyze the properties of unstable networks, we propose to choose two sites. One is networks in Soya regions of Hokkaido, Japan [58] and the other is Himalayan region of Nepal[40].

Our research suggests the following design principle or guideline:

- Do an assessment of disaster prone or unstable networks
- Find out vulnerabilities of those networks
- Design redundancy for each layer as much as possible. Nonetheless, consideration of cost and other factors are also important
- Consider redundancy at each layer. For example L1, L2, L3, L4 and L5

We have observed that there are various studies and project plans from different sectors in response to the disaster relief and recovery plan around the world. Most of these projects are not running as collaborative projects among different sectors. There is little research that co-relate not only with the entire layers of TCP/IP but also relates above application layer which we believe that

co-relation with public, government and other stake-holders is also required. We noticed that there is sufficient research conducted to achieve fault tolerant of the networks[2], [3], [5], [6], [59]–[61]. However, these work have less description about disaster readiness than we are focusing on. Nonetheless, we found few which can be taken into consideration [14], [11], [13], [14]. The other related research are found in [55], [63]–[69] have some content relevant to this research. Among these, only few have proposed research about disaster tolerant networks [65] which can be insightful for us. Most of these research is focused on post-disaster measures. In contrast to these research, we focus more in disaster preparedness and thus our measure is pre-disaster by putting enough consideration in each layer of TCP/IP. Nonetheless, we do also sufficiently recognize the importance of pro-disaster measure once the disaster happens. Our research does not ignore this fact and thus includes post-disaster measure thereby providing portable HA-cluster in order to resume the interrupted network services.

2.2.2. Automation of Monitoring and Management Process of Unstable Network

Monitoring and management is required in order to increase availability, reliability and performance of the network. There are various tools available in order to check network availability and performance. Network administrators often use ping, traceroute and many other tools in order to check the availability of the network. Similarly, other tools often utilized to monitor and manage the network are Nagios, MRTG, NTOP, tcpdump, wireshark and many others. Some tools are commercial whereas some are open source. The generic framework of network monitoring starts from availability checking of network nodes, then if the node has a problem the monitoring tools or programs generate a message indicating the problem in that particular nodes and notify the network administrator. Network administrators get the notification and tries to solve the problem.

The aim of monitoring and management tools is to support network administrators in order to identify the problem as early as possible. Earlier detection of the problem leads to minimize the potential damage of the business. Therefore, an efficient and automatic network monitoring is always required for large organizations like universities, government offices, banking sectors, private companies and other business institutions where manual monitoring of network is always

difficult[70]–[72]. All the tools and research work aimed to improve the quality of networks also target improving the working conditions of network administrators. As we know, Network monitoring and diagnosis tools or programs are used by many organizations for daily network management operations. However, we have found very rare results from the monitoring and management operations conducted at unstable networks. Trouble detected by monitoring tools is useful while there are network administrators. However, there are still regions where sufficient network administrators are not available. In such cases, a movable network managing device would be necessary. The end objective of such a device is to automate entire network monitoring and management process. However, achieving complete automation is a hard dream. In this research, we design a monitoring device that monitors the networks and also aims to trouble-shoot basic networking problems. As of today, much of the literature defines the ideal network monitoring and management device should be able to do the followings:

- It should be able to monitor the network continuously with minimal human interference.
- It should be able to generate reporting message to network administrator without taking much time.
- It should be able to locate the point and time of trouble.

We agree with these properties, however, we found some additional properties that are lacking here; if the monitoring and management device is deployed to manage unstable networks. This dissertation claims to design a movable device that can monitor and manage networks while the primary network goes offline. Disaster readiness is not possible to achieve without providing such kind of functionality. In this way, automation of monitoring and management is vital for DRN networks.

2.2.3. Portable HA cluster and Fog Infrastructure

Organization can lose critical data and application if they do not have sufficient preparation for disaster management. In order to protect their critical data and application from the disaster, many organizations take a backup of their data. We found few examples and tools that maintain a

backup of their data and applications. However these examples tackle only a few pieces of the problem and rely on others to do the rest. They have not tackled the issue as proposed in our work.

In our work, we design and implement a portable HA cluster on which the critical data and the application can be deployed and backed up. This cluster is made up IoT devices. Our technique of keeping clusters as portable as possible enhance the disaster relief procedure and makes more effective.

As described in the literature of many other researchers in the database replication, we build working models of the system and implemented a prototype. Our work emphasizes incorporating these models in making them portable. Most other work, however; focuses only on replication but excludes making them portable as ours.

2.2.4. Service Dimension in Fog Services

Demarcation of services between cloud and end user plane is becoming challenging issue in the field of cloud computing. One of the major proposal of storing data in the cloud is to keep business data as a backup so that organizations will not lose their mission critical data if disasters happen. However, this feature of cloud is pointing towards another level of problem which is the problem of data residency and data legality. For example, cloud data centers can cross the country or continent so that there would be a great difference between the rule, policy and the laws between the consumer society and providers' society. Furthermore, the issue of potential access to data by foreign governments is part of a wider issue, which is that the use of services based in other countries may result in customers being affected by laws of those countries. In order to solve these kinds of issue, a new kind of computing architecture is necessary. The above mentioned data theft issue can only be minimized by keeping the data inside your premise. And this can be offered by utilizing fog computing infrastructure. We propose a method to categorize and classify the services so that end-users can choose between cloud and fog infrastructure while protecting their data. The classification of services depends upon the dimension of the service. We have classified these dimension into three major group:

- Mega Service
- Macro Service
- Mini Service

There is sufficient research in cloud based system. Google, IBM and Amazon are the technological frontiers. However, there is very little effort done to categorize the services as we proposed.

Chapter 3. Survey and Simulation of Network Topology

Deployment of Wi-Fi Network as an Emergency Survival Communication Network in Wakkanai, Hokkaido

---

This chapter presents the design of redundant networks and the detail consideration that should be given for the improvement of unstable networks. It presents simulation result and the scenario of actual survey conducted in Wakkanai city of Japan which is based upon our approach and model that forms the basis for the requirement of monitoring device and HA cluster included in this dissertation

3.1. Introduction

Networks must be safeguarded against disasters. From the network-management viewpoint, safeguards should be considered during the network design phase. In this study, we surveyed the potential of establishing redundant Wi-Fi networks in schools in the Soya region of Hokkaido to proactively create a bypass communication network that can be used if a natural disaster occurs. During emergency situations such as earthquakes, tsunamis, and floods, a traditional disaster response may not be able to provide adequate communication services to emergency-management teams. To explore the potential of establishing an emergency survival communication network in Wakkanai, Hokkaido, we conducted a medium-scale trace-driven study of redundant networks to determine how to decrease disaster risk. We set up wireless nodes at four network locations of different sizes, including an access link between the Wakkanai city office and Wakkanai Hokusei Gakuen University networks. Furthermore, we model the optimal redundant topology and discuss the simulation result. By proactively establishing a redundant wireless network as a detour emergency route using our approach, an organization can rapidly reduce disaster risk.

Disaster risk reduction (DRR) is a strategic approach to reducing the risk of hazards and panic in a society during disasters, both natural and man-made. DRR aims to identify, assess, and

reduce the risks of disaster, as well as reduce socioeconomic vulnerabilities to disaster. DRR should not be performed in isolation. Rather, it should be an integral part of a disaster response, such that government, private–public organizations, and other stakeholders can coordinate their response. DRR is a much broader and deeper approach than conventional risk management.

Research suggests that natural disasters have recently assailed Japan with greater frequency and intensity than in the past. Such natural disasters include not only earthquakes but also floods and storms[73]. These disasters have harmed the national economy and the lives of people living in affected communities, and have drawn the attention of the Japanese government, of humanitarian relief organizations, and of researchers all over the world. The disasters highlight the need to improve humanitarian relief operation and management [74]. Specifically, after the nuclear disaster at the Fukushima Daiichi Nuclear Power Station, the Japanese government expressed concern regarding energy issues affecting a broad segment of the public. The government also responded quickly by accelerating its demand-side management and energy-efficiency project timeline from 2020 to 2015.

The use of information and communication technology is also being explored as a way to make the energy supply more sustainable and networks more stable. Recent research on networks has emphasized the importance of network stability for business activities in organizations such as schools and universities. Note also that over time, changes can affect both the vulnerability of a computer network and the causes, nature, and intensity of the hazards that the network faces.

Redundant Wi-Fi networks are a good option if a disaster occurs in a geographic location such as Wakkanai. For example, in an emergency situation, the community expects a rapid response from the rescue-management team. To ensure a rapid response, emergency communication systems cannot take hours to deploy. Rapid and easy deployment of the communication system is critical during a disaster. Our study investigates the establishment of backup links to provide a network that can be reestablished more rapidly and easily during disasters as an emergency detour route.

3.2. Methodological Background

Researchers often use modeling and simulation techniques to verify their research data. However, modeling a proactive DRR approach using emergency network routes presents a number of difficult methodological problems. The social and political parameters required for DRR simulation are difficult to simulate, the simulation process is difficult to represent and trace, there is no standard simulation model, and current literature about DRR for computer networks does not include a sufficiently iterative process for formulating the problem. Therefore, simulation alone is unlikely to comply with strategic scientific guidelines or yield sufficiently rigorous results.

Because simulation data would be unreliable, we conducted an experiment in the field to test our strategy directly on real networks as a part of a trace-driven approach. We first conducted a preliminary survey of the site. We then tested the links between nodes and identified vulnerable sites. From the results of the test, we proposed redundant networks that would maintain the survivability of the network during natural disasters. On the basis of our proposed design, we performed a simulation experiment and created redundant topology. We then began the survey after performing 1) vulnerability and survivability analysis and 2) risk-reduction analysis.

The two types of analysis allowed us to assess overall risk for different networks by identifying the points that are most likely to fail in a natural disaster, and which of those points of failure will most affect network assets and the survival of communication systems.

3.3. Experimental Strategy and Discussion

A network is said to be stable and reliable if it satisfies communication demands not only in normal situations but also in the majority of natural disasters. However, the importance of a redundant network that uses alternative media for a stable network has largely been ignored in schools and on campuses. At our research site, the network is generally maintained over a single infrastructure, such as a fiber-optic or wired network. This paper systematically reviews the potential of establishing a redundant network between Wakkanai Hokusei Gakuen University and schools in the Soya region. The principal benefits of redundant networks, as identified in the

networking literature, include risk management, alternate routes, and the ability to back up a network to provide a backhaul network allowing access to an external network. In our work, there are two interesting challenges and solutions we came up with to make the design and implementation of backup links in our networks:

1. We explored a technique to determine line-of-sight orientation of WiFi antenna without using any modern equipment. We used a simple mirror on one end of the link and visual orientation based on the reflection from that mirror on the other end of the link to align the two antenna at the two ends. Note that such low-tech techniques can be applied in emerging and rural parts of the world.

2. We wanted to deploy WiFi antenna in general area of the school and campus but wanted to make that process of determining the locations for deployment efficient. Our goal is to make sure the network survives even when there is a disaster. Fortunately, the government has already surveyed the cities and villages for areas that are safe, or created these areas as shelter for the population. These areas are called lifeline spots in Japan. Our deployment specifically leverages this database of lifeline spots for deployment planning and we believe we are the first group to plan a network that will survive emergencies by using this database from the government. We showed this is feasible and others in network design community may be inspired by our work to look for similar scenarios in their communities.

3. By using the technique of above, we believe that a redundant network can be established using Wi-Fi at relatively low cost in Soya areas which can also be used as an emergency detour route during a disaster

3.4. Motivation

3.4.1. Issues and Objectives

Disasters, by their very nature, destroy existing network infrastructure. Disasters can also lead to data overloading and saturation, which also destroy networks. The use of mobile ad hoc

networks and the distribution of antennas in disaster areas can often encounter these problems. Although networks can be reestablished in disaster areas, doing so may not be feasible in large-scale emergencies. Some authors[75]even suggest the use of a wireless opportunistic network based on mobile devices carried by emergency personnel to forward the data created and collected in disaster areas to coordination points[75]–[77]. These approaches are all post-disaster measures.

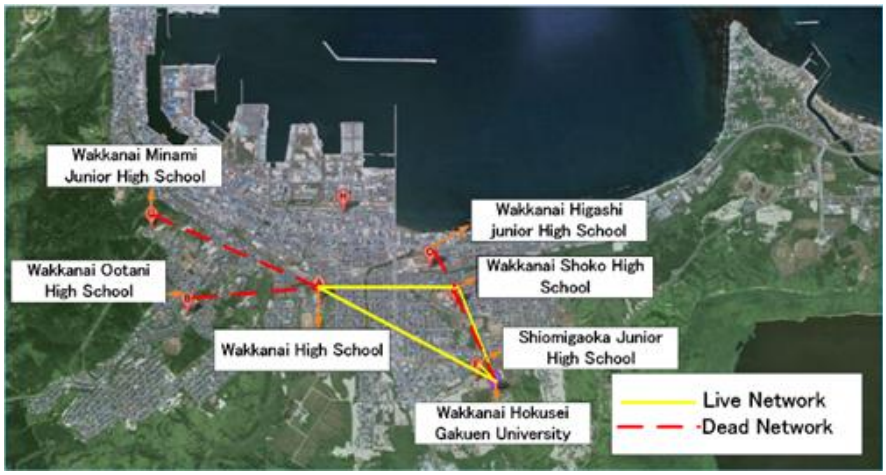


Figure 3-1：Geographical Locations of School in Wakkanai

In contrast, our approach is a pre-disaster measure that provides more robust management by establishing redundant physical links using Wi-Fi technology. There are a number of network trouble-shooting tools and methods, but they require further research. Better communication infrastructure design can make infrastructure more reliable, reduce the time and money required to manage the infrastructure, and improve the strategy for managing the infrastructure. The objective of this research is to identify the need for communication at the distribution-network level, the substation level, the distributed-source level, and the end-user level, and to suggest steps to improve communication at these levels. However, we mostly work at the network level to measure the reliability and sustainability of network solutions. Figure 3-1 shows the geographical location of schools in the Soya region. Most school networks are connected by single links, making them vulnerable at these single points of failure.

In a disaster, the needs of local residents exceed the response capabilities of the community and community organizations. Risks to be considered include those from natural hazards, neighbors,

building environments, and political and social unrest, and risks connected with information technology and data security [74], [75].

The Fukushima nuclear disaster graphically illustrates the difficulty of protecting a network during a disaster. There may be no alternative way to re-establish a network after it goes down in a disaster. One potential solution is to establish a hastily formed network (HFN). An HFN is a portable IP (Internet Protocol) based network that is deployed in the immediate aftermath of a disaster, when normal communications infrastructure has been degraded or destroyed [40], [46], [78]–[80]. However, significant human resources are required to deploy an HFN, and these can be difficult to find during disasters.

3.4.2. Importance of Redundancy

Generally, redundancy implies the existence of a backup system that allows service to continue after the main system fails. Redundancy can be provided for systems such as networks, hardware systems, power systems, and locations. In this paper, we describe network redundancy, particularly network-path redundancy, and its importance. Not only campus networks, but any network that requires high availability and survivability or needs to perform important operations can benefit from network-path redundancy. Network-path redundancy can provide alternative paths for networks with outdated switches and cables. If a switch or cable breaks, or if an outdated network device is no longer able to provide services, a redundant system ensures continuity and avoids disruption of critical communication and data flow. The Soya regional network that links Wakkanai Hokusei Gakuen University with city high schools, secondary schools, and primary schools in the Soya region is completely connected with fiber optics. However, the constituent networks have single points of failure if they are cut off from the wireless networks provided by

Wakkanai Hokusei Gakuen University. In our research, we found that most of these schools have no redundant network path.

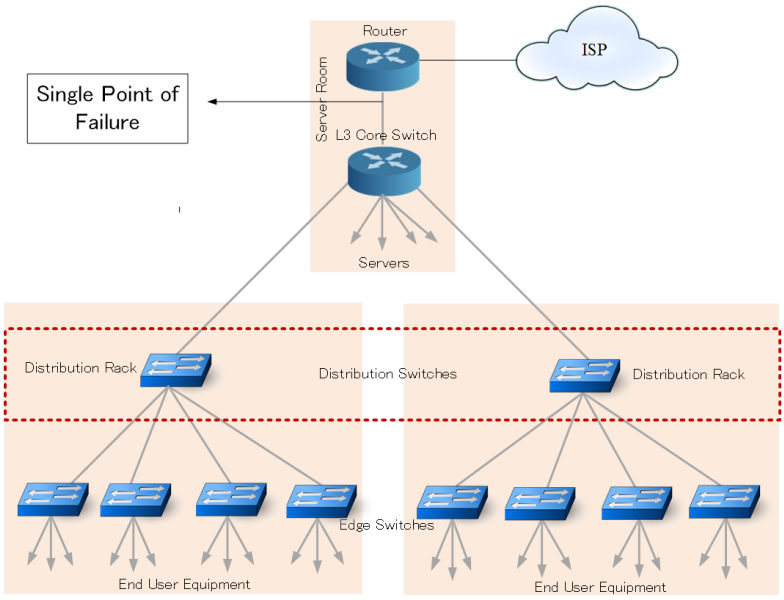


Figure 3-2：General network topology at schools in the Soya region

Unless these schools implement redundant network topologies, they will be unable to provide stable services to the end users. We note that Wi-Fi and redundant technologies are already abundantly used in the world. However, we strive to explore these existing technologies by applying our newer methodology stated in section 1.2 above in order to exploit their advantage in areas where their usage are not well explored. In this regard, our research explores setting up emergency survival communication network in places where the weather conditions are extreme, and places which are prone to tsunamis and earthquakes. Wakkanai, Hokkaido is an example of such a place. Wakkanai is a city where the year round temperature goes very low and snow falls for more than 4 months in a year, and where there is a constant threat of strong wind and natural disasters such as earthquakes and tsunamis. There is very little existing research about Wi-Fi and redundant technologies in such areas. Thus, our research will have a large impact on Wakkanai city.

3.4.3. Problem Analysis of Existing Networks

To build a network that can provide stable services during disasters, one must include redundant links in the design methodology. Figures 3-1 and 3-7 demonstrate that very few schools have redundant links to Wakkanai Hokusei Gakuen University. The common weakness of regional schools in the Soya region is that their networks have been built without consideration of the importance of redundancy. Site priorities and the location of key services contribute to fault-tolerant design, in which resilience is built into the network infrastructure and services and resources spread over a wide geographical area[77].

The common weakness of these regional school networks is that none of the schools have analyzed the risk posed by single points of failure. Figure 3-2 shows the most common network topology at the schools. The weaknesses of the topology are as follows.

The topology does not have a proper network-management system—there is no proper tool for configuration management, performance management, security management, and traffic management. The topology lacks a backup communication system that can be used during a disaster. The topology lacks a data and network recovery strategy. Furthermore, from a fault-tolerance point of view, the present configuration of the school networks has a number of weaknesses. Ideally, there should be no single point of failure; however, the common topology has two single points of failure. One core switch connects all sub-core switches. If the core switch fails, most of the school network will fail with it.

The topology has only one outgoing route to the Internet service provider. If this connection fails, the school network will lose Internet services.

3.5. Related Works

The field of wireless networks has been the subject of extensive research [74],[40], [46], [78]–[80]. However, little of that research directly analyzes how Wi-Fi networks can be used as redundant networks during disasters—most of the research discusses the general-purpose use of

Wi-Fi networks. For example, Kanayama and Takizawa first investigated the use of Wi-Fi in Wakkanai city in 1998[81], and they continue to conduct Wi-Fi research in the Wakkanai area [82]–[84]. Their research concerned the construction and improvement of communication networks, but did not address the design of redundant networks to reduce network problems during disasters. We can find no other reliable documentation or practical research describing the implementation of redundant networks in the Soya region. Nonetheless, the studies of Kanayama and Takizawa provide substantial lessons for our future research.

Research has also been done on the use of wireless networks in disaster situations[85]–[88]. Some researches[89], [90] on energy efficient routing in ad-hoc disaster recovery networks have also been proposed. However, most of the studies do not concern the use of Wi-Fi networks as redundant networks for DRR. In contrast, our work clearly shows the potential of using a Wi-Fi network as an alternative route for a network in a disaster situation. The research is of value not only to academic institutions but also to local governments.

This study also contributes reliable guideline materials for the future development of networks in these settings. The physical network topology suggested by this study uses Wi-Fi to provide a high level of reliability and survivability. The study shows how schools in Wakkanai can deploy Wi-Fi to optimize network design and thus provide reliability and survivability without the need for a further survey.

3.6. Proactive DRR Measures That Enhance Network Survivability

DRR measures are proactive disaster mitigation measures taken to eliminate or reduce the impact of hazards before a disaster occurs. Generally, DRR activities should incorporate assessment of the evolving risk environment. Some typical examples of DRR measures include hazard mapping, the enforcement of building and other civil engineering codes, and flood, tsunami, and earthquake mapping. While these DRR activities can reduce the harm that disasters do to societies, this paper focuses more specifically on reduction measures that can be applied to computer networks. We describe these measures in the following sections.

3.6.1. Proposed Community Disaster-ready Network

The primary objective of this research is to provide concrete guidelines for designing networks that can best survive natural disasters. Furthermore, we want to minimize the effects of

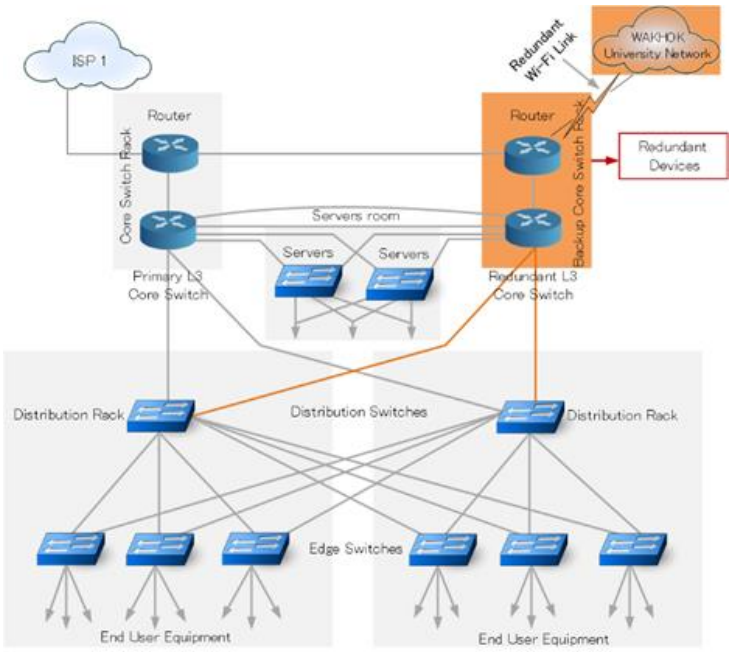


Figure 3-3：Proposed Redundant Network Topology

natural hazards on networks and thus minimize the social and economic disruption caused by these hazards. We want to use effective network design to help control hazards, thereby preventing them from developing into disasters.

During a disaster, regional government generally uses voice radio systems and other broadcasting systems for disaster response. However, disasters can damage wired networks, either destroying them or rendering them unable to maintain the bandwidth and data management required for regional communication. In such situations, backup wireless networks can provide a better alternative.

3.6.2. Redundant Topology

Redundant connections provide a quick-response backup system, which is available for use during unplanned outages and ensures continuity of operation. Power outages in Wakkanai can occur not only during natural disasters, but also in winter, which might result in significant loss in the economy of this region. As history has shown, Wakkanai experiences numerous unpredictable outages during winter. Therefore, investment in network redundancy is a good strategy. Figure 3-3 shows our proposed topology, which uses Wi-Fi links to provide network redundancy. The problem that we want to address through this topology and redundant architecture is to strengthen the robustness of the network during disaster in Wakkanai. Wakkanai city government has already identified the lifeline spots in Wakkanai which are capable of tolerating potential earthquakes or tsunamis. More specifically, these lifeline spots are the local schools and local university buildings where local citizens can take shelter during disasters. We assume that Wi-Fi access points deployed in these lifeline spots are capable of retaining its quality of providing wireless networks during disasters. Therefore, our proposed geographical topology as shown in Figure 3-1 has covered the link between these schools, and the architecture we propose is based on redundancy in each layer. The link coverage between the schools was surveyed during our research. Figure 3-3 demonstrates the redundant design in the core, distribution and access layers. The components involved in these layers are routers and L3 and L2 switches. The proposed network uses both L2 and L3 redundancy, because hardware failures can occur not only in L3 but can also occur in L2. Similarly, redundancy in links between L2 and L3 switches and border routers are also increased. The redundancy has been increased with a factor of two in each layer. This will lead to a cost increment during deployment, however by keeping the topology design simpler and highly scalable as shown in Figure 3-3, it can greatly reduce the cost in the long run. In our design, we have limited our redundancy up to two. Increasing redundancy to more than two nodes or links may lead to decrease in serviceability, manageability and determinism. A network design as shown in Figure 3-3, in which the L2/L3 boundary is in the distribution layer is the recommended best practice that is scalable, and manageable. We recommend a hierarchical model to allow for a scalable network and meet evolving future needs of the schools and organizations. Our approach keeps the topology modular which makes the network easy to scale, understand, and troubleshoot by promoting

deterministic traffic patterns. In the long run, such modular and manageable topology reduces the maintenance cost too

3.6.3. Consideration of Data Recovery

Disaster recovery is the process of restoring data and communication links or business processes. Recovery from an emergency situation is always a complex task, particularly in mass-casualty disasters[73]–[75]. In these scenarios, a quick and coordinated response is not possible without establishing a redundant network that can be used in such a situation. The recovery process must improve the efficiency of rescue teams and save as many lives as possible. For a network, the data recovery process includes the restoring of routers, switches, and other devices that make up the network. After a network has recovered, work—either local or remote—can be done to restore data-oriented servers.

Among the activities in a disaster recovery framework, off-site data protection is the process of copying critical data to a physically remote site where storage resources are available. Today, the most widely used solutions for backing up data rely on a combination of two technologies: RAID[74] and Fiber Channel[75]. Off-site data protection should be organized such that, if a site crashes, the required number of server machines is restarted at another network site to maintain and reactivate the offered services. Indeed, in order to quickly reactivate services and avoid excessive slowdown of running services, the number of server machines that must be restarted at remote sites should be reduced. Generally, servers are deployed so that if a power outage occurs the backup power system provides power instantly, obviating the need for a restart. However, in some cases these backup power systems cannot maintain power for more than an hour. During our survey, we found that such servers are restarted during a power outage, and the restart usually results in file-system problems and data loss.

3.6.4. Use of Redundancy Protocols

The use of redundancy protocols to provide a redundant route is crucial when a master router loses its connection to the outside world. To provide a stable connection to the local area

network without affecting the services in the network, it is recommended to use redundancy protocols in a router. A redundant router works as a backup router, and must be deployed such that it can receive packets sent by the master router. The network must also be configured so that the interface of the master router is monitored, and when it loses its connection with the outside world the backup router takes over and restores connectivity.

In some cases, two or more routers can be set up to act as the gateway, and a dynamic routing protocol such as routing information protocol (RIP) or open shortest path first (OSPF) is used by hosts to determine the gateway router to use as the next hop in a path to a specific IP destination. However, dynamic routing should not be applied in every situation. When static routing is used, the hosts on the local area network are unable to communicate with hosts in the outside world if the statically configured router fails. Virtual router redundancy protocol (VRRP) can be used to address this problem by being located at the top of physical routers to act as the master router. VRRP can provide a stable network, because the physical router can be well monitored, and if any interface is down, VRRP can monitor both of the operational status of interface or of the port.

3.6.5. Network-path Redundancy through Alternative Media such as Wi-Fi

Many networks used wired connection for backup link. In our case, there is danger of earthquake and tsunami, so the wired backup link may have the same vulnerability as the primary link. On the other hand, wireless backup link will have different property and vulnerability, thus provide a better chance of survival during earthquake or tsunamis. Even among wireless, there are many options. Wi-Fi is one of the most popular wireless communication standards used today. It uses a wireless transmission medium (electromagnetic waves) to transmit information such as text, audio, and video content. The Wi-Fi Alliance defines Wi-Fi as all “wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers’ (IEEE) 802.11 standards,” since most modern WLANs are based on these standards. Wi-Fi can be used for an alternative, redundant network path. Network-path redundancy entails the use of a backup path to provide stable network services when a network loses its route to the outside world. Besides Wi-Fi, these days, there are a few other link technologies such as Zigbee, 3G, 4G and many others. 3G

and 4G are licensed spectrum and the cost per gigabyte is directly transferred to the end-users. Zigbee only works at short distances and offers low data rates. Comparing Wi-Fi with 3G and 4G, we found that Wi-Fi is less expensive and economically feasible for the regions. Furthermore, Wi-Fi can be set up easily and can allow different entities of public buildings to turn their existing Wi-Fi network infrastructure into more integral part of fog computing, sensor networks and IoT solution which are important communication infrastructure for a smart community. Due to these reasons, we have chosen Wi-Fi for our work as we can scale out the existing networks of Wakkanai without replacing its existing infrastructure in a relatively low cost.

Wireless devices are good candidates for redundant network paths. A completely redundant system requires redundant switches, redundant communication ports, and redundant device pairs. Complete redundancy can make a network extremely reliable and stable, minimizing data loss and hastening recovery time.

3.6.6. Redundant Power Supply

Although power outages are inconvenient and expensive—especially in modern society—extensive electrical outages continue to occur in developed cities, including those in the Soya region. Power outages are disastrous and difficult to mitigate without expensive backup power systems[40], [80]. Our experience of network administration at Wakkanai Hokusei Gakuen University suggests that we should use redundant power supplies for routers, switches, and servers.

Without redundant power supplies, providing a stable network is impossible, even with redundant network topology. Furthermore, sudden fluctuations in voltage during unpredictable power outages hamper the operation of hardware devices. A redundant power supply is also a requirement of a fault-tolerant power system. When a network designer considers power availability, the designer should ensure that even if one parallel supply fails, the system continues to provide full power to its power bus[78]–[80].

Each power-supply source must include a circuit that automatically disconnects the redundant power-supply module if it malfunctions. Automatic disconnection functionality is

usually provided using isolation (ORing) diodes or metal–oxide–semiconductor field-effect transistors (MOSFETs) placed in series with the output of each parallel supply [80]. If a power-supply module short circuits or shuts down for any reason, the MOSFET switch must be turned off to prevent a high-impedance state. In addition to having this automatic output "disconnect" feature, each supply module must include a signal and visual indicator that can alert a user or external monitoring system that a specific redundant power supply has failed, so that it can be replaced or repaired [40], [80].

3.6.7. Adding Redundant Nodes

One fundamental problem of network design is the design of a network with an independent node. This problem arises in designing communication networks that have single-node failures. A network must meet certain link and node connectivity requirements to demonstrate that it can survive failures. We recommend increasing the number of redundant nodes to guarantee that there are at least two nodes that are connected to the outside world. Note that the number of redundant nodes should be increased not for the purpose of increasing link capacity but to improve survivability.

3.7. Simulation Scenarios and Results

3.7.1. Simulation Scenarios

The main focus of this practically oriented research was to obtain results from the field directly rather than relying solely on simulation results. Nevertheless, we conducted a set of experiments using the Cisco Packet Tracer simulation tool and Riverbed modeler academic addition with different parameters to test the availability of a network when introducing a redundant path.

To analyze various scenarios, we designed networks of varying size having different numbers of nodes and different traffic rates for each set of nodes in both simulators. In this paper, we present and analyze the relevant results obtained from our simulation with the optimized number of nodes. Specifically, we focus on redundancy test, packet loss and PDV. These data are crucial in recommending the construction of a redundant network in the urban area of Wakkanai to be used in a disaster. The topology of the simulated network represents our recommended redundant topology design. We assume that we require at least three layers, namely core, distribution, and access layers. Each layer maintains a redundant link and redundant node. The simulation scenario is shown in Figure 3-4. Each layer is surrounded by rectangular dotted lines with different colors. Our simulation uses the topology design recommended in section 4 therefore this simulation design includes core, distribution and access layers. The core layer has four routers which are connected with a full meshed design however we do not recommend full meshed redundancy because it reduces manageability. Therefore two interfaces in the core layer and in the distribution layer are

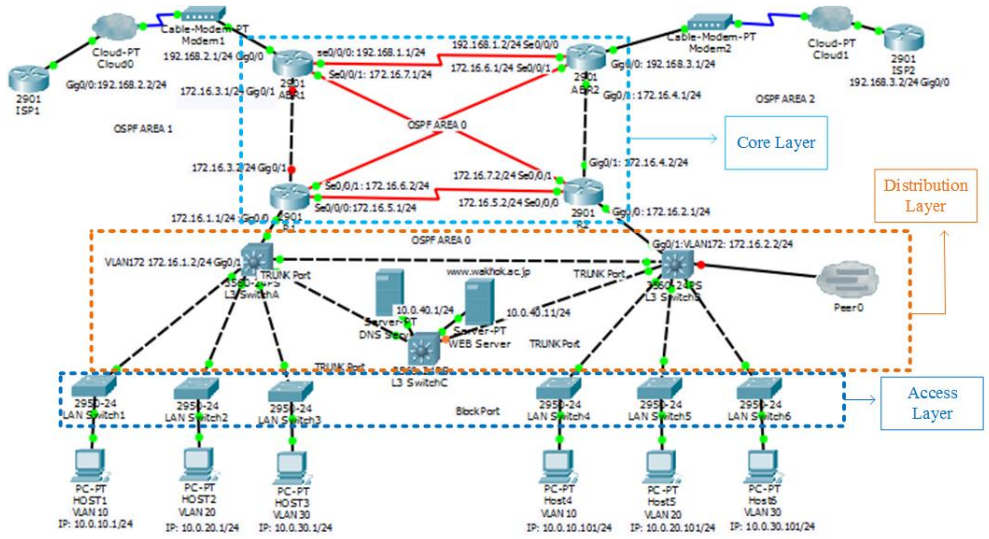


Figure 3-4：Simulated Scenario of Redundant Topology

deactivated intentionally to keep them more manageable. The small red disks in the links indicate those links are deactivated. The simulator we use is a Cisco packet tracer which has a similar kind of functionality as real devices such as the L2, L3 switches and routers. In our simulator, we configured all devices, created VLAN in the distribution layer and configured OSPF in the core

```
PC>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.0.10.254
  2    0 ms      0 ms      0 ms      172.16.1.1
  3    0 ms      0 ms      0 ms      172.16.3.1
  4    2 ms      2 ms      1 ms      192.168.2.2

Trace complete.
```

```
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=3ms TTL=252
Reply from 192.168.2.2: bytes=32 time=10ms TTL=252
Reply from 192.168.2.2: bytes=32 time=3ms TTL=252
Reply from 192.168.2.2: bytes=32 time=3ms TTL=252

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 10ms, Average = 4ms
```

Figure 3-5: Connection test in simulation scenario

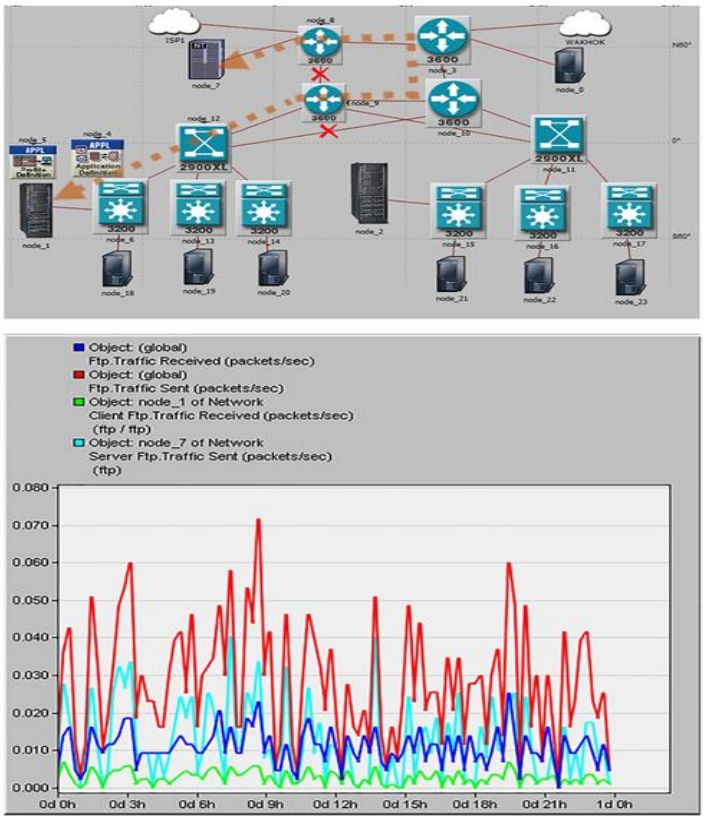


Figure 3-6: Simulation Scenario and the Test of Traffic Flow

layer routers. In our first simulation, we simultaneously deactivated redundant links and started sending ICMP packets by using ping tools and also started tracing the path. In this simulation, we use three L3 switches in the distribution layer and six L2 switches in the access layer. The results of this simulation is shown in Figure 3-5.

3.7.2. Redundant Link Test and Traffic Description

The second simulation approach tested on Riverbed Modeler is based on injecting real FTP traffic into existing network and observing the resulting delay, jitter, and packet loss. We follow this approach in order to test the robustness of our topology supported with redundant links. We redesigned the simulation as shown in Figure 3-6 and conduct simulation with different design scenarios. This simulation represents the topology that we recommended in section 3.6.1. In this simulation also, we use the hierarchical topology. Our approach is to keep the modular design to make the network easy to scale, understand, and troubleshoot by promoting deterministic traffic patterns. We found that jitter may happen while the packets take different route for ingress and egress.

As shown in Figure 3-6, traffic was generated between node 1 and node 7 by uploading a 50KB file. Links of 100 Mbit/s for access layer and 1000 Mbit/s for distribution and core layer were employed. The red crossed lines indicate the link failure scenarios. We transmitted packets from a FTP server executed in node 7 and a FTP client at node 1. The direction and path is indicated by a dotted directed arrow. Traffic demand flow was done between these 2 nodes and the simulation was rendered. FTP traffic flow between these two nodes are plotted in the graph. The graph shows that traffic sent and received has high differences. This can happen due to asymmetric nature of traffic flow in this topology. Asymmetric traffic may result in packet drops if the ingress took longer time. This was an interesting result as this happened while there were multiple activated link. In some occasion, packets transmitted from a source reached their destination with different delays. In fact, TCP delay has been noted during this simulation.

The issue of jitter may arise for a greater number of hosts. However, after deactivating the redundant links a number of times and continuing the simulation, we got average ftp traffic flow which indicates no difference between ingress and egress. This is also plotted in the graph in Figure 3-6. Our observations demonstrate that a combination of wired and wireless redundant networks can increase network availability.

3.7.3. Redundant Node Test and Traffic Scenario

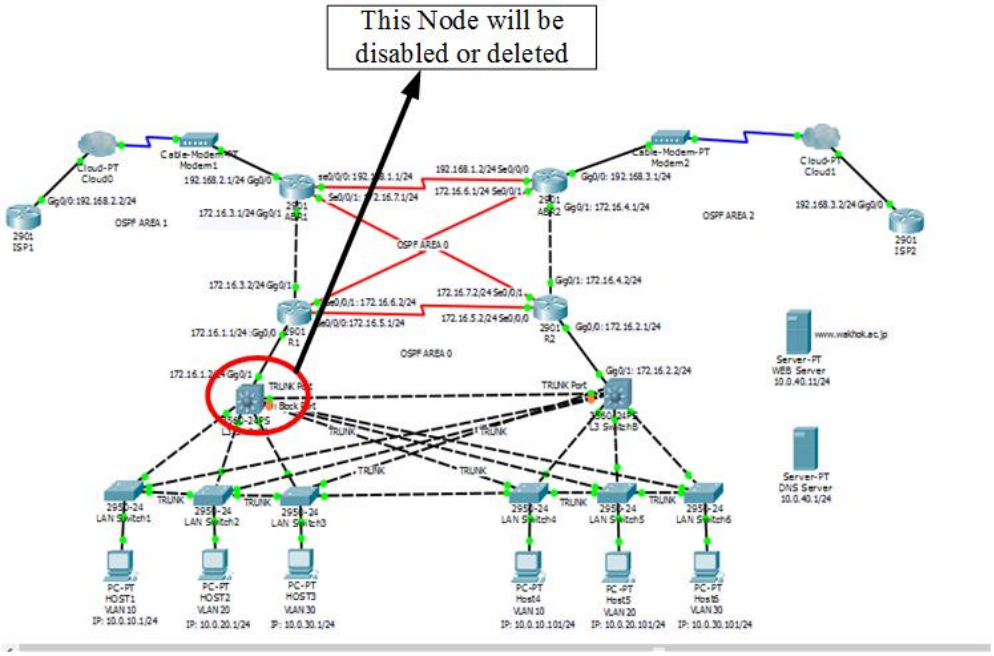


Figure 3-7: Redundant Node Test with Relatively Balanced Tree

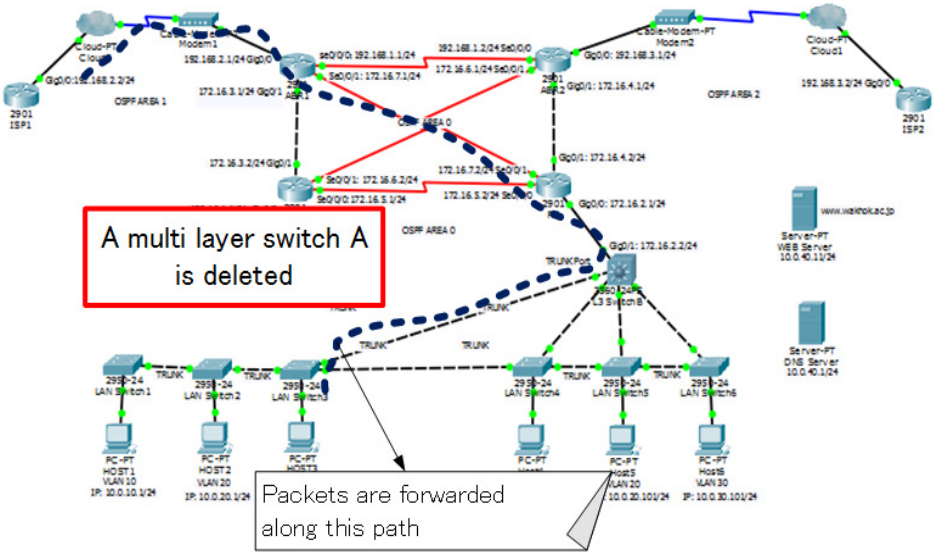


Figure 3-8: Redundant Node Test with Unbalanced Tree

Next, we experimented the elimination of node from the topology and observe how this can affect the entire network. Node elimination was conducted in order to assure and observe that the topology has no other single point of failure. Despite the multi-path redundancy in each layer, a single link failure can temporarily cause the loss of all packets destined to a particular set of end hosts. For instance, in [91] has mentioned that a link failure at the top level of a 3-level, 64-port fat tree can disconnect as many as 1,024, or 1.5%, of the topology's hosts. This can drastically affect storage applications that replicate (or distribute) data across the cluster; there is a significant

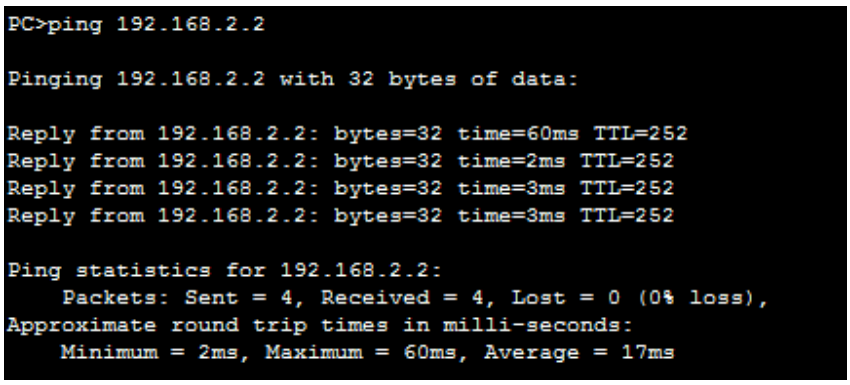


Figure 3-9: Connection Test

probability that the failure of an individual node can affect the backup storage of the data center[91]. In order to perform this experiment, we first increase the double attached node (DAN). Please note that our link topology has been changed from Figure 3-4 to Figure 3-7. After increasing the attached node with multiple links, node deletion was conducted on distribution layer. Please see Figure 3-7 and Figure 3-8 in which we have deleted the left node of the distribution layer resulting very unbalanced tree as shown in Figure 3-8. We tested the connection from the node having IP of 10.0.30.1 to node having IP of 192.168.2.2 and found that it has not lost the connection. The ping result is shown in Figure 3-9. Experimental results as shown in Figure 3-9 confirmed that an improvement of the topology is acquired by providing redundancy in distribution layer too. By increasing the redundancy as far as possible in each layers, we increase the survivability and availability of the networks. The obvious trade-off is that by increasing the acceptable redundancy we increase the availability of the communications. However, the trade-off between budget and the redundancy need to be investigated.

Table 3-1: Experiment Scenario

Experiment	Layer 2	Layer 3
Link Deletion	● 6 links were deleted ● Applied Protocol PVST and RSTP	OSPF
Node Deletion	Generic + Multilayer Switch Nodes	Router Nodes

Table 3-1 shows the scenario of experiment in which we conducted two types of test. The first test was conducted to disconnect links at a different level. For instance, we disconnected the link at layer two and also at layer three. We noted that redundant links increase the capacity of fault tolerance at different level. In layer two, while we disconnect the redundant link, a secondary link took part for communication to resume another subset of switches at those levels.

Similarly, we deleted a node (Switch A) as shown in Figure 3-8 in order to test node failure scenario at distributed layer. Deleting of switch A results in failure of entire links attached with this switch and thus the topology as shown in Figure 3-8 is produced. When the packets reaches switch 3, it realizes that the intended link between switch 3 and switch A is unavailable and instead uses its second connection to switch B. Then, it simply forwards packets destined for 192.168.2.2 as shown in Figure 3-9. In this experiment, we deleted switches and their descendants' links were also removed from the topology, ultimately resulting in a decrease in the number of links and the switch supported by the topology. This experiment suggested that a fault tolerant capacity can be increased in the topology by increasing multiple links and nodes as shown in our topology.

3.8. Case Study of Wakkanai

Considering the importance of an alternate path, we investigated the use of a Wi-Fi

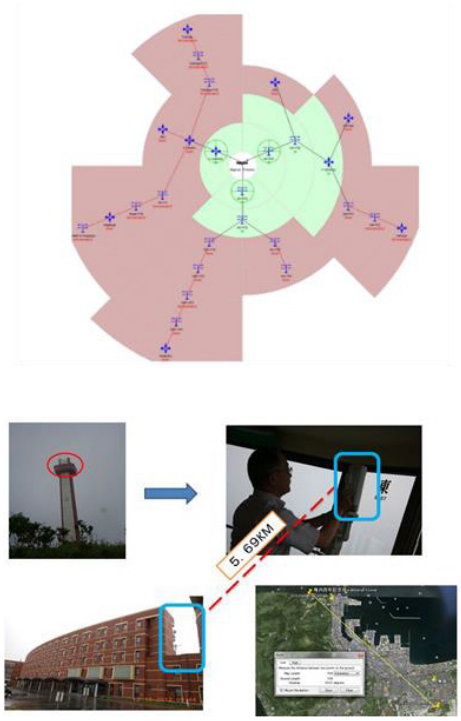


Figure 3-10: Link Coverage Survey for Different Points

Figure 3-11: Wi-Fi experiment near Wakkanai Memorial Tower

backhaul router. Figure 3-11 shows photographs of our equipment and experimental setup. We first surveyed the existing networks and network coverage. Figure 3-10 show that there were only a few active links between Wakkanai Hokusei Gakuen University and the regional school networks. The green areas depict active network coverage and the red areas depict dead networks. We found that

more than 50% of the network was inactive. The reason seems to be that the wireless receivers in those networks were not in working condition or were simply unavailable.

3.8.1. Scenario of the Field Experiment

To re-identify the access points and network coverage, we conducted a new survey. We tested connections using the traditional method of locating the two ends, and used a mirror at both ends and reflected sunlight to identify the direction of the point-to-point connections required for the two ends. The red rounded object in Figure 3-11 is the mirror that we used to reflect sunlight and notify our counterparts of our relative positions. We then mounted a wireless device parallel to the direction of the mirror reflection. We also agreed on where to place radio receivers and transmitters. A person with a receiver then rotated and moved the wireless device to receive the signal from the transmitter. After a few attempts, we were able to receive the signal from the wireless access point at the university. This scenario is shown in Figure 3-10. After receiving the signal, we were able to establish a connection between the university and the Wakkanai Memorial Tower. If the transmitter device was located anywhere other than near the Wakkanai Memorial Tower, receiving devices had great difficulty receiving the signal. Our experiment suggests that a transmitter device located at the Wakkanai Memorial Tower can cover almost 80% of Wakkanai with a Wi-Fi signal.

3.8.2. Discussion

We found that almost every school in the Soya region has a single point of failure in its network. This situation is common in schools in Japan. Only two schools have two links- one provided by Wakkanai Hokusei Gakuen University and the other provided by an Internet service provider. The remaining networks have only a single connection. A network with a single link has a single point of failure, and will fail if that link breaks. Bad weather causes frequent link failures on networks in Wakkanai, and multi-hop wireless networks with redundant nodes are thus an important alternative. Redundant nodes are often introduced in mesh networks, where they can maintain network availability and survivability.Redundant nodes do not increase network bandwidth, but rather increase network reliability by providing failover links when a link on the

shortest path fails. This paper includes a basic topology that can be used to identify the optimal topology of redundant nodes for a given school network. To help network designers choose the optimal topology, we provide a method by which they can calculate the additional network reliability that will result from adding a redundant node to a given topology.

3.9. Future Work and Conclusions

In this research, we observed that most schools in the Soya region are connected to the outside world by a single physical link. Only two schools are connected with two links—one to the university and one to an outside Internet service provider. Although most of the links are connected with fiber optics and stable Internet services are provided, these networks are vulnerable to network outages during natural disasters. Our future work will include the actual installation of redundant links. However, the implementation of redundant links will require funding support from either local government or the Ministry of Education, Culture, Sports, Science and Technology of Japan.

We believe that disaster-response and disaster-ready networks are crucial for preventing unexpected damage to communities. Disaster-response networks are typically connected to sensor networks that can detect disastrous events before they impact communities by warning communities to seek shelter and to take other appropriate measures[75]. However, network failures can severely hamper the ability of sensor networks to gather useful information in a timely manner. For example, networks aimed at monitoring fast-moving destructive physical phenomena, such as earthquakes and floods, must be designed to be disaster ready. During disasters, large-scale geographically correlated failures often occur. In addition, individuals use the network to contact each other and to request help, which leads to serious network congestion, possibly even tying up channels completely and exacerbating failures. This paper provides guidance for designing a topology with redundancy in the Soya region. Although designed for the Soya region, the topology can be used for designing redundant networks in any locations. We found that most Soya schools can use a Wi-Fi backhaul link from Wakkanai Hokusei Gakuen University. This Wi-Fi backhaul link can be used as an emergency survival communication network when the main wired networks of the schools are disrupted by a natural disaster. In addition to helping a network meet hierarchical

network design guidelines, redundancy also allows a network to be highly available and reliable, even during disasters. By “reliable,” we mean that even if a network failure occurs, a network has connectivity through failover links. Thus, our focus is on the availability and reliability of network services when a disaster occurs, considering several measures of risk and operating on the assumption that link failures are independent. We allocated the highest priority to issues that render networks vulnerable to sudden outages not only during natural disasters but also during winter. We examined the redundant link in different scenarios using Packet Tracer and Opnet simulation tools. We also surveyed the potential links in Wakkanai that cover disaster-ready areas in order to visualize disaster scenarios for university computer networks and disaster areas such as Fukushima, and thus describe how a disaster may occur and how it can negatively affect organizational computer networks. There are many potential techniques, troubleshooting tools, and practices—having a wide range of costs and levels of complexity—that can be used to safeguard networks. We have presented considerations to take into account when constructing a stable network. Furthermore, with regard to disaster preparedness in the Soya region, we recommend providing disaster education and disaster mitigation plans for school networks to school teachers. Education and planning should enhance teacher readiness to act during natural disasters in a way that supports the proposed emergency operation plan. Because natural disasters such as earthquakes can occur without warning, a proper network-management plan for natural disasters is essential.

Chapter 4. Development of Monitoring Device

Enhanced Tensai Gothalo: Development of Movable Navigating Router Device with Precise Path Tracing and Network Monitoring Capabilities

---

This Chapter describes how a network can be monitored and managed by using a movable and portable device. In this chapter, I particularly focus on the development process of monitoring device which was developed during entire research project. It also demonstrates the utility of IR sensor that has been used to detect the path. Some experiment results are provided in order to evaluate the performance of the device.

4.1. Introduction

Tensai Gothalo [54] is a movable router that can participate in a network as a router device. This device is equipped with a movable unit that is equipped with DC motors. A path tracing movable router is a basic routing and monitoring device that can be used in the disaster prone areas to construct emergency networks[42]. In disaster prone areas, the networks of Tensai Gothalo can be deployed as an emergency networks. To begin, we designed a black-topped path that can vary from as simple as a black line on the floor to as complex as embedded lines or magnetic lines. To detect or trace the path, different navigation schemes or vision schemes can be employed. These navigation schemes may vary from as simple and cheap as IR sensor circuits to as complex and expensive as vision circuits[92]. Though the decision of what type of path-tracing schemes is to be employed depends on various factors such as the requirements of users, cost, and locality, we employed IR sensor circuits to detect the path, as this can be developed with a low budget. Applying simple and cheap technology is of good advantage in areas where rails or conveyor belts are not possible to deploy. A simple black path can be traced by using simple IR sensors. A more precise path-tracing circuit is embedded in a device that can perform with less error to prevent the device from moving off of the track.

4.1.1. Requirement and Challenge

Enhanced Tensai Gothalo is a mobile navigating router that has the ability to move from one location to another along a specific path. Traditional router devices are not movable, as they are designed with a fixed device and routing features are provided without assuming movement capabilities. Current computer networks can be constructed without the inclusion of movable routing features in the router. The question is then in what situation a movable router is necessary.

The motivation of this research is to develop a computer network device that has movement capability that enables it to explore a path and proceed to a targeted area without human interference. Traditionally, prior to the development of the movable router, mobility was provided through the process of handover from one specific device to another. Mobile phones successfully achieve mobility by deploying relay devices in various locations. The mobility occurs as the users walk from one destination to another while carrying the mobile device. These devices can transmit voices, text and other information to nearby routing points or relays that transfer the signals from the source to the destination. These relay devices are fixed but provide mobility in communication. Nonetheless, a problem may arise in that when the fixed devices experience technical problems, the areas covered by those devices will be deprived of communication. To restart the communication, one needs to replace those troubled devices. In our scenarios, we provided route points with both routing capability and also movement capability. This capability enables the router device to dynamically replace the service that has been halted due to the troubled router and continue its service delivery without requiring human interference. In our future work, we will replace the path and equip the device with pathless functionalities that can reach a target by considering the surrounding situation. In this paper, we propose the design process of such a device.

Our challenge in developing such a device is that it is difficult to develop a device that can sense the network trouble, proceed to the troubled area, analyse the nature of the problem, and troubleshoot. It requires the combination of a number of technologies, including hardware, software, and protocols. It is quite challenging to arrange the low-level hardware technology by developing mechanical modules, implementing an electronic circuit, developing a control program and integrating everything into a high-level application that can monitor the entire network.

In summary, the implementation of TG to monitor and manage networks demands a good electronic circuit implementer, a low-level programming skill having knowledge of hardware programming, and high-level programming including a complete knowledge of TCP/IP and other related technologies

4.1.2. Organization of the Sections

The rest of this paper is structured as follows. Section 4.2 briefly summarizes the conceptual framework of network monitoring. Section 4.3 explores the detailed architecture and working principal of TG along with the fundamentals of the inform-on-die (IoD) algorithm. Section 4.4 investigates the state-of-the-art path navigation scheme applied in this project. Section 4.5 provides the detailed description and architecture of the control circuit and power supply module. Section 4.6 describes the experimental results with different case studies. Finally, Section 4.7 presents the conclusions and provides insights for future research.

4.2. The Conceptual Framework of Network Monitoring

As suggests Figure 4-1, our concept of network monitoring is to automate the monitoring system and reduce the time of human intervention. Let suppose that M1 is the master TG and there are two other slave TG: S1 and S2. The working principal of TG based monitoring and automation is that M1 continuously monitors the networks and when there is a trouble, it detects it automatically and then instruct the nearby slave TG to trouble shoot the problem. In this way, monitoring and restoration of network is conducted. We assume that in future networks, monitoring and management will entirely be automated. The primary objective of this research project is to present a working model or solution for a movable router that can autonomously track the path and detect the troubled server. To supplement its movability capacity, we employ a robotic vehicle that has a routing capacity while working as a network monitoring node. When there is a power outage in the server, the master node of Tensai Gothalo [54] will first receive the signal of the network outage from the sensor that we embedded in the monitoring nodes, and then it will instruct slave node to respond accordingly. We have experimented to switch on the server once it is accidently powered off. We assume that when the services are shut down, this status will be checked by the master, which will instruct the slave to re-start the services. In this way, the network will be monitored and managed automatically. We propose to deploy this model to monitor and manage the unstable networks the authors have previously investigated[40], [41].

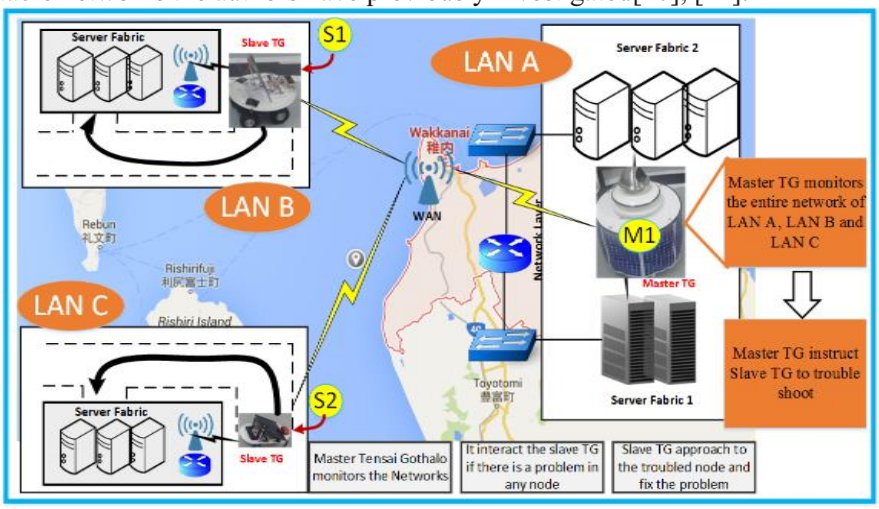


Figure 4-1: Conceptual Framework of Network Monitoring

Figure 4-2 shows the working principle of the TG router that can work on autosensing and manual modes. Autosensing mode is built upon IR sensors that can proceed on the predefined path, while in manual mode, the TG proceeds as per the instruction of the operator. The mode of TG can be automated as per the surrounding situation. When it finds the predefined path, it can automatically sense it and proceed as per the track. Similarly, when it does not find the track, a manual mode will be activated, and the operator can handle TG as per his wish. Our concept of a movable router is that this device would be used when disaster occurs or when emergency survival communication is required during rescue operations. In such a situation, this device should be able to provide services of routing or switching while the primary routers, servers or switches are broken. In such a situation, we assume that a black-topped path constructed near the server would be helpful. However, in certain situations, these paths are not available or would be unfeasible to construct. In this type of scenario, a manually driven device is required so that an administrator can guide the device to the needed area. To meet these particular requirements, our design indicates the working principle as shown in Figure 4-2.

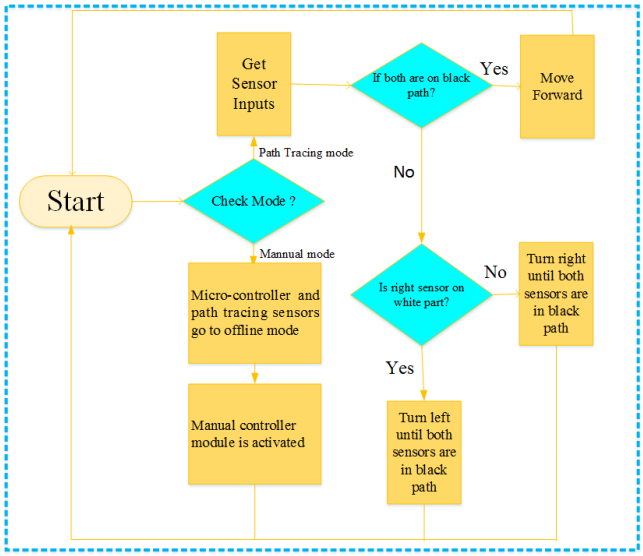


Figure 4-2 : Manual and Path Sensing Modes and its Working Principal of Tensai Gothalo

4.3. Architecture and Working Principal of Slave TG

Figure 4-3 shows the block diagram of the Tensai Gothalo. In this system, we have proposed to use a solar panel as a power source. This will provide power to the battery through a charge controller circuit.

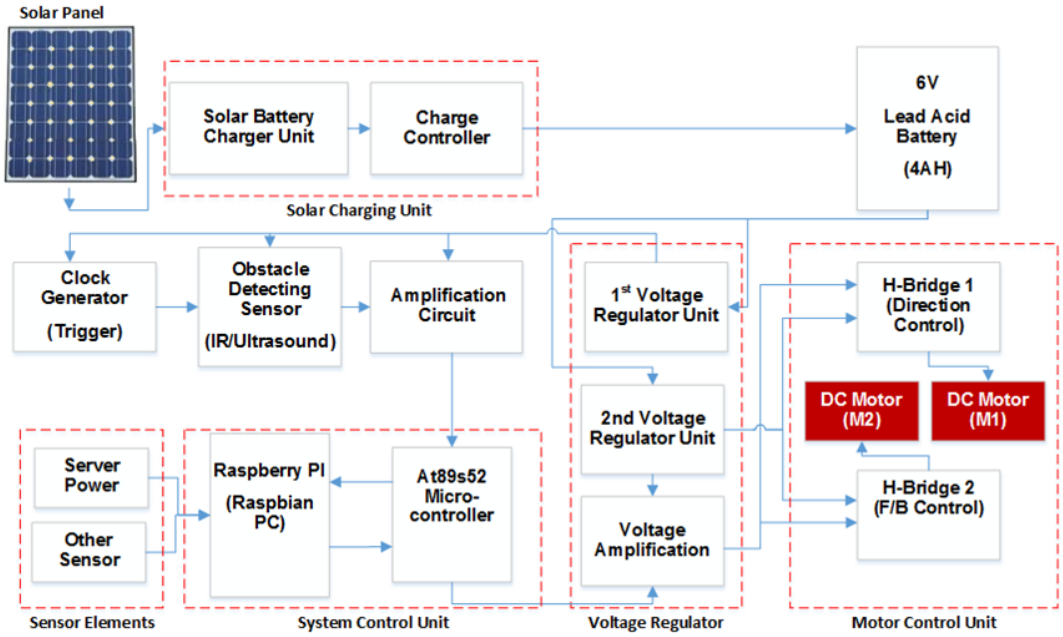


Figure 4-3 : Entire Architecture of Slave TG

The output of the battery is regulated by a voltage regulator, and a microcontroller manages the movement and direction of the motors, which is further amplified and controlled again by an H-bridge circuit. Finally, the wheels of TG are directed on the basis of information from the H-bridge to the DC motors attached in TG. The details of the modules are described in sections 4, 5 and 6.

4.3.1. Inform on Die Protocol Steps

In this section, we explain the working procedure of our solar powered robotic vehicle Tensai Gothalo (TG), which functions on the basis of IoD protocol steps. We have divided the

working principle into three different categories. IoD will be applied for all these three categories. As shown in the Figure 4-4 annotation A, just as soon the server face some problems, the sensor module attached to it notifies the master Tensai Gothalo. When the problem is just a simple power cut off, the sensor will detect the status and immediately notify the master TG. If the problems are different, such as from the services, then the monitoring server on the master TG will detect the issue. Our focus in this paper is to elaborate on the power failure issue. As soon as it detects the problem of power failure, the sensor attached to it will immediately inform the master TG using IR transmitting signal. As shown in Figure. 4-4 annotation B, when the master TG receives a signal regarding the trouble at server, it immediately responds to that signal, giving very first priority to it and instantly taking action to resolve the problem. Furthermore, sequences of programs will be executed to solve the problems. First, programs detect the status of the sensor with respect to the trouble, and it then immediately informs Master TG, which provides instruction to the slave TG to immediately solve that problem.

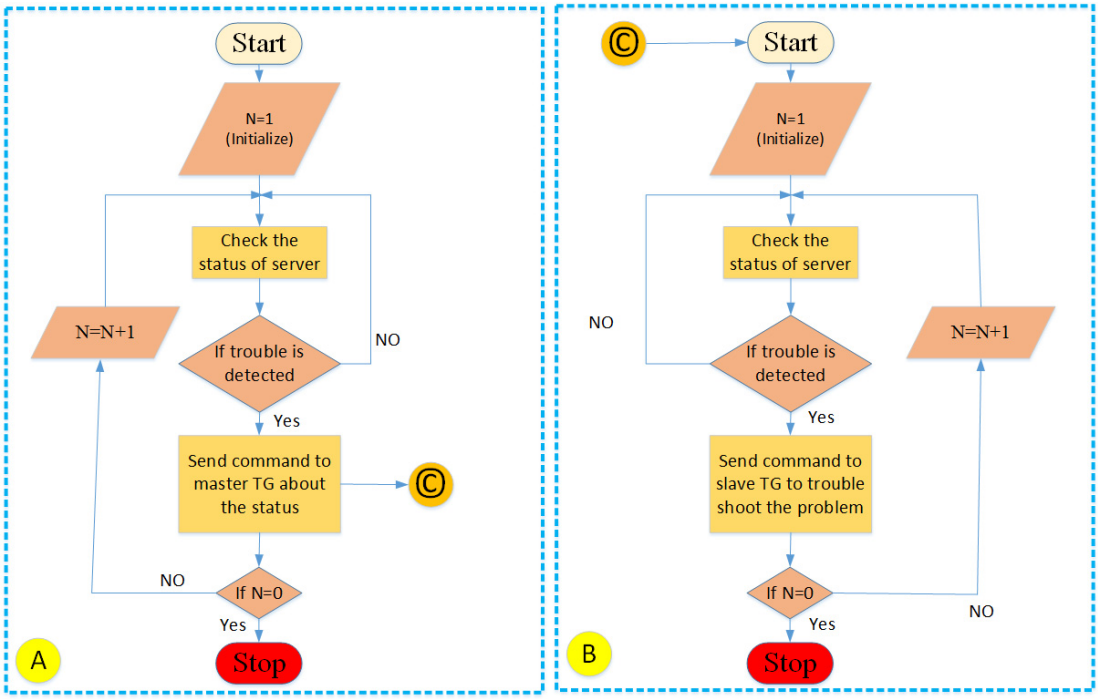


Figure 4-4 : (a) Sensor response at server pc (b) Master Tensai Gothalo

Table 4-1 shows the proposed algorithm that should be applied at the server that will be monitored by TG:

Table 4-1: Proposed Inform on Die Protocol at Server Fabric

Inform on Die Protocol Steps at Server Fabric (PHY 1)	
Step 1:	Detect Trouble at Server Fabric
Step 2:	WHILE(TRUE)
Step 2-1:	IF (Troubles are Detected)
	Send Command to Master TG
	END IF
	END WHILE

1) 4.3.1.1 Proposed Inform on Die Protocol at Server Fabric

Table 4-1 shows the stepwise description of IoD protocol that should be applied while the monitoring event is executed. The different steps of the scenario will be described below for easy understanding.

Step 1: In this step, all the sensors are in alert state so that it can receive a message from the server if anything goes wrong.

Step 2: In this step, the status of the sensor is checked. If the sensors are activated, indicating that a problem is found in the server, the next stage will be activated.

Step 2-1: In this step, the command for slave TG will be executed. The loop will be ended.

Table 4-2: Proposed Inform on Die Protocol at Master TG

Inform on Die Protocol Steps at Master TG (PHY 1)	
Step 1:	Wait for Signal from Server Fabric
Step 2:	WHILE(TRUE)
Step 2-1:	IF (Troubles are Detected)
	Send Command to Slave TG
	END IF

2) 4.3.1.2 Proposed Inform on Die Protocol at Master TG

Similarly, the following steps should be applied while monitoring is performed by the master TG. The steps are summarized in Table 4-2, and the details are described below.

Step 1: In this step, all the sensors are in alert state so that it can receive a message from the server if anything goes wrong.

Step 2: In this step, the status of the sensor is checked. If the sensors are activated, indicating that a problem was found in the server, the next stage will be activated.

Step 2-1: In this step, the command for slave TG will be executed. The loop will be ended

Table 4-3: Proposed Inform on Die Protocol at Slave TG

Inform on Die Protocol Steps at Slave TG (PHY 1)	
Step 1:	Receive signal from Master TG
Step 2:	WHILE(TRUE)
Step 2-1:	IF (Troubles are Detected)
	● Proceed to the path as per the sensor inputs
	● Trouble shoot the server
	END IF
	END WHILE

3) 4.3.1.3 Proposed Inform on Die Protocol at Slave TG

Table 4-3 shows the summarized version of the IoD protocol that should be applied while awaiting commands from the master TG.

Step 1: In this step, the receiver of the slave TG is always in alert position to receive a signal from the master TG about trouble in the networks.

Step 2: In this step, if the trouble information is received, TG will proceed as per the sensor inputs.

Step 2-1: In this step, the command to troubleshoot the server will be executed. Once the trouble is resolved, it will return to its original position and wait for the next command.

4.3.2. Operation of Slave

The Slave TG plays a significant role in managing the networks. Once it receives a signal from the master TG, it proceeds to the troubled server and starts working. The flow diagram is given below. As shown in Figure 4-5, the program embedded in the slave TG will be executed, and the value of N is initialized. For the slave to function, N is initialized to 1 at the first loop. Because the slave TG is always in the standby position for troubleshooting, the value of N will not be zero, except when the slave TG is interrupted by external factors such as the administrator. Accordingly, if the battery backup of TG goes below the threshold, the operation of the slave TG will be halted.

Under any other condition, it will always be in working condition, and the value of N will be incremented for each iteration.

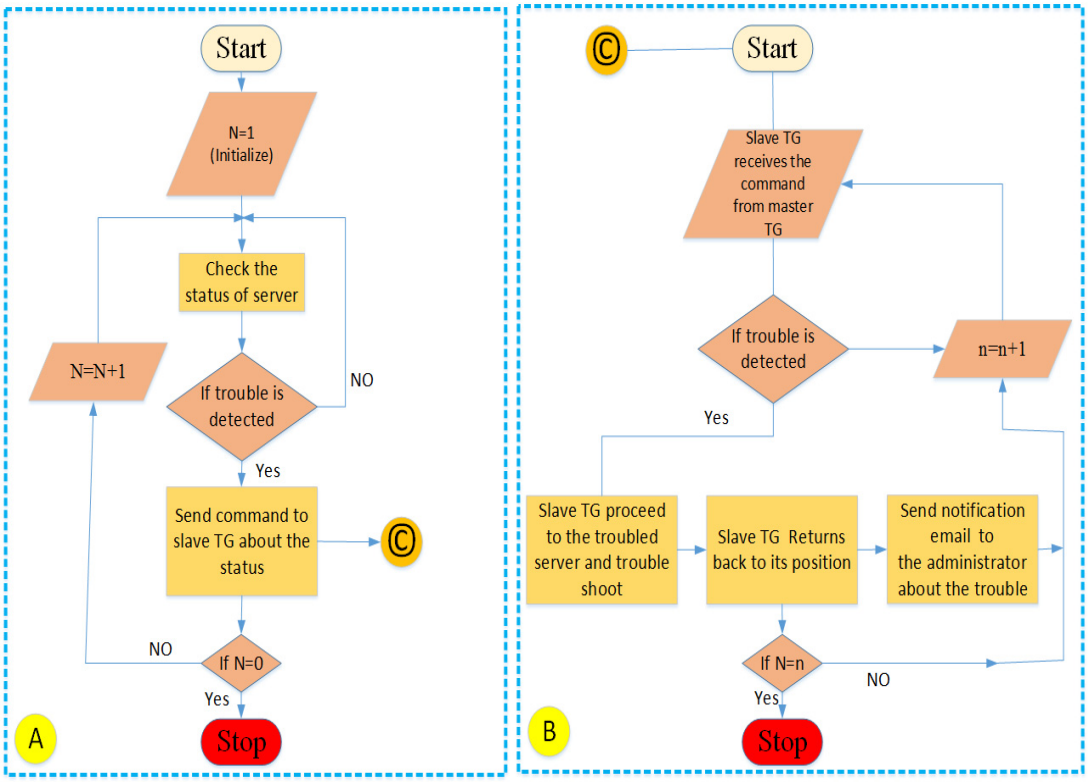


Figure 4-5 : Work flow of Master-Slave TG

4.4. Path Navigation and Movable Routing Feature in TG

Tensai Gothalo uses the black-topped track to navigate to the targeted server. Currently, the path is designed as a predetermined oval shaped path that is placed near the server so that the IR sensors can sense the signal from each other.

The slave of Tensai Gothalo starts moving from the start point and stops after finding the targeted server, for which it sends the IR signal to start or stop the server and services. Figure 4-7 shows the navigating track for the experimental environment of Tensai Gothalo in the lab. There are currently two objects, the master Tensai Gothalo and the slave Tensai Gothalo. The slave always remains on the track and awaits the signal from the master.

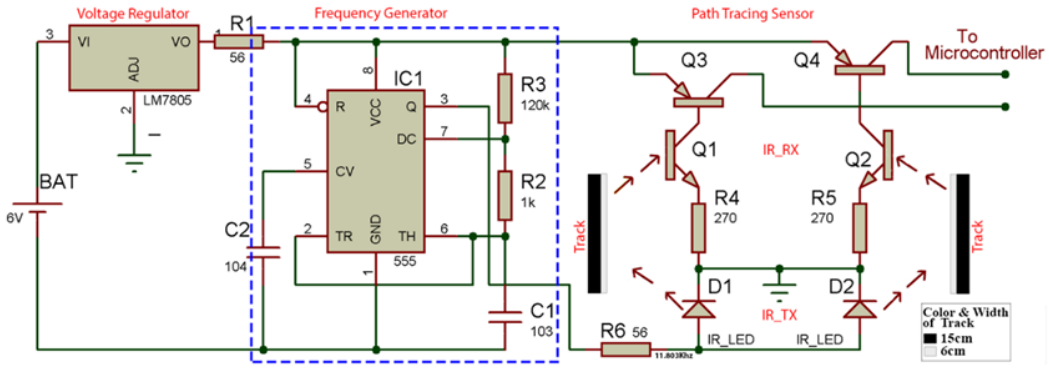


Figure 4-6 : Enhanced Path Tracing Scenario

4.4.1. Enhanced Path Tracing Sensor and Working Principle

We generate an approximately 12 KHz frequency, determined by R3, R2 and C1, as shown in Figure 4-6. We tested an IR emission providing a DC voltage with no frequency in a previous version of TG [54]. However, this could not achieve the desired result, as the vehicle had difficulties in following the track. This occurred because the IR transmitter signal fades out quickly, and the receiver could not fetch the appropriate signal to drive the vehicle along the path. We needed to fix this situation. Therefore, we used a 555 timer to sustain the fading time such that the IR receiver can receive the appropriate signal and the vehicle can go along the path without error.

We built a circuit with the main components of a 555 timer and IR TX-RX pairs, R3= 120k, R2= 1K and C1=0.001 uf. We used three different frequencies, 1 kHz, 1.2 kHz, and 11.803 kHz.

Among these, we achieved the desired result from the 11.083 kHz frequency, the calculation of which is shown in Table IV below.

Table 4-4: Frequency Calculation

F	= 1.44/ (R3+2R2)*C1
	=1.44/ (120+2)*0.001
	=11.803 KHz
T_H	=0.693*(R3+R2)*C1
	= 0.693*(120+1)*0.001
	= 0.0838 Milliseconds
T_L	=0.693*R2*C1
	=0.000693 Milliseconds

Where,F=Frequency, T_H =high voltage interval, T_L = low voltage interval. In our circuit we use T_H for tracing the path of vehicle

Where T_H transmitted through IR Transmitter Diode D1 and D2 is received by IR Receiver Transistor Q1 and Q2.

4.4.2. Movable Routing Feature in TG

The routing capacity has been provided by integrating Raspbian with TG. In using Raspbian, we have identified several significant advantages that we found compelling in this research. For example, we can utilize a monitoring protocol more easily in this set up because we can deploy SNMP (Simple Network Monitoring Protocol) or a monitoring tool such as Nagios without much trouble. Similarly, we have more resources to embed the programming in Raspbian than in a micro-controller. Furthermore, we can implement a routing protocol in this device to utilize it as a router. In this way, we can separate the very low-level programing and high-level programming between Raspbian and the micro-controller. The other major objective of providing routing capacity in this monitoring slave TG is that it can provide the networking service while the principal network is offline. The detailed procedure of the routing feature being activated is shown in Table 4-5.

.

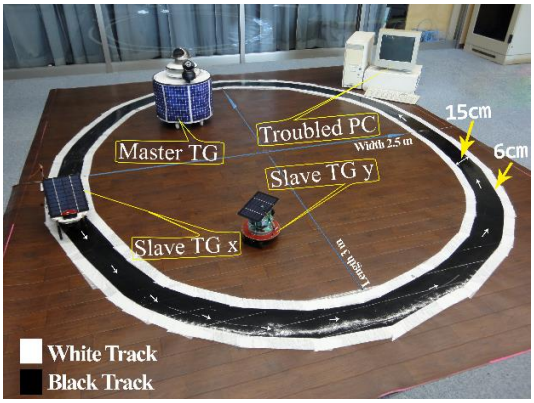


Figure 4-7: Navigating Path of Tensai Gothalo in Lab

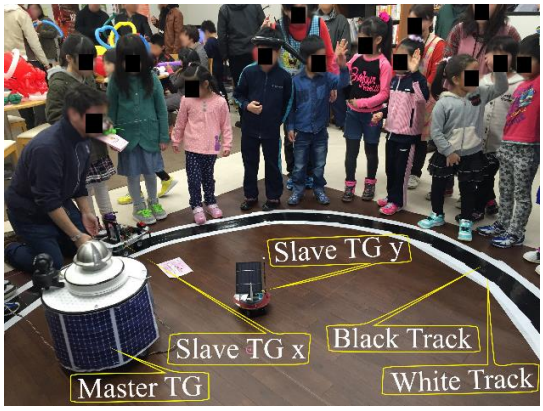


Figure 4-8: Demonstration in Wakkanai

Table 4-5: Activation Timing of Routing Feature

	Steps:	Function of Master TG	Function of Slave TG	Remarks
1:	Step	Detect trouble in the node	Wait signal from master TG	Stand by position
2:	Step	Instruct slave TG about trouble if detected	Proceed to the trouble server if instruction is received from master TG	Auto movement of TG from one place to another
3:	Step	Instrcut another slave TG to start routing functions	Routing functionalities are activated	Routing feature is activated for emergency propose

The Routing feature can be employed in a number of ways in our TG. For example, a static routing can be performed for point to point routing. When we need communication between the slave nodes, we can apply point to point communication. However, in this particular research, we are just interested in providing an emergency network when the principal network goes offline, and thus we can provide TG, being a Wi-Fi router, as a hotspot. In such a situation, the slave TG can act as a Wi-Fi hot spot node as per the steps shown in Table V. Similarly, if multiple network paths are available, we can utilize TG, where a dynamic routing (i.e., RIP or OSPF) can also be implemented. In such a case, it is recommended to deploy a software router (e.g., Quagga) in TG

once Raspbian is installed, and thus the routing feature can be included in TG. This feature is very important to provide an emergency survival communication network[40], [41] as the authors have been researching for the last few years. In this way, the movable routing feature has been achieved in TG. Coming sections elaborate on the details of the movable features and its architecture.

4.5. Implementation and Circuit Architecture

4.5.1. Overview

The path-tracing router has a very simple and modular circuit architecture so that we can

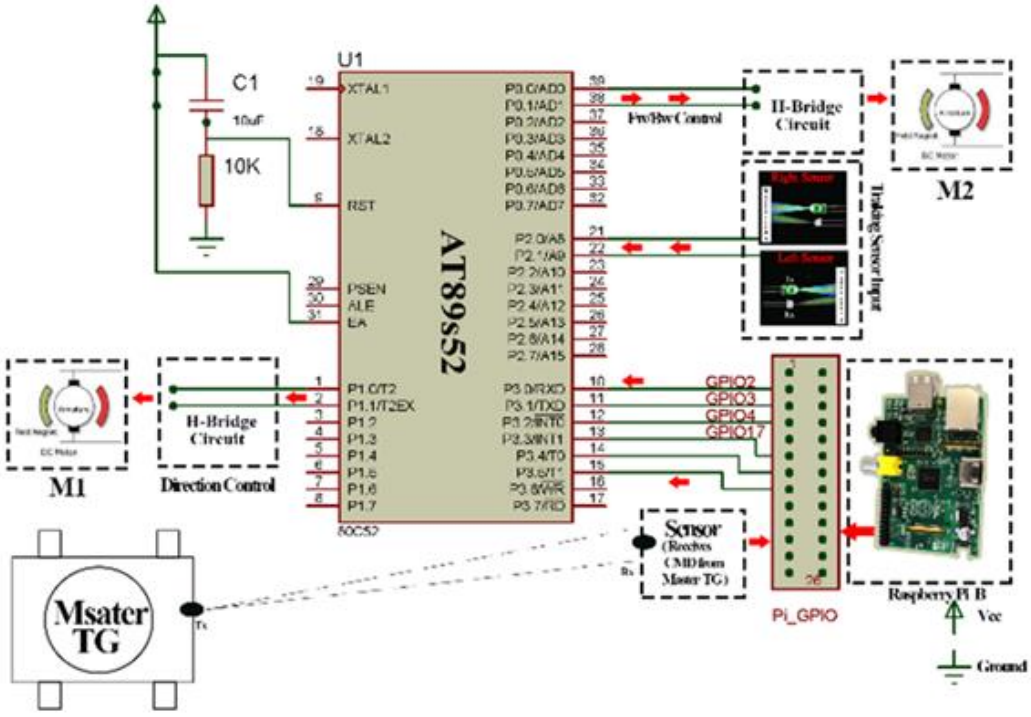


Figure 4-9 : Complete Controlling Circuit Architecture of Tensai Gothalo

add features in the future. It consists of a two-sensor unit that can be constructed using either IR sensor. The actuator unit is simply a DC motor. Moreover, microcontroller is used as a controlling unit that will take the input from the sensor, match the exact action that needed to be performed and then send the output to the actuator. Figure 4-9 shows the alignment between sensor, actuator

and controlling unit and the one of the complete prototype of slave Tensai Gothalo is shown in Figure 4-10 with annotations. We developed a few number of TG and the functionalities of these TG were tested and demonstrated (please see Figure 4-8) in few occasions in the public.

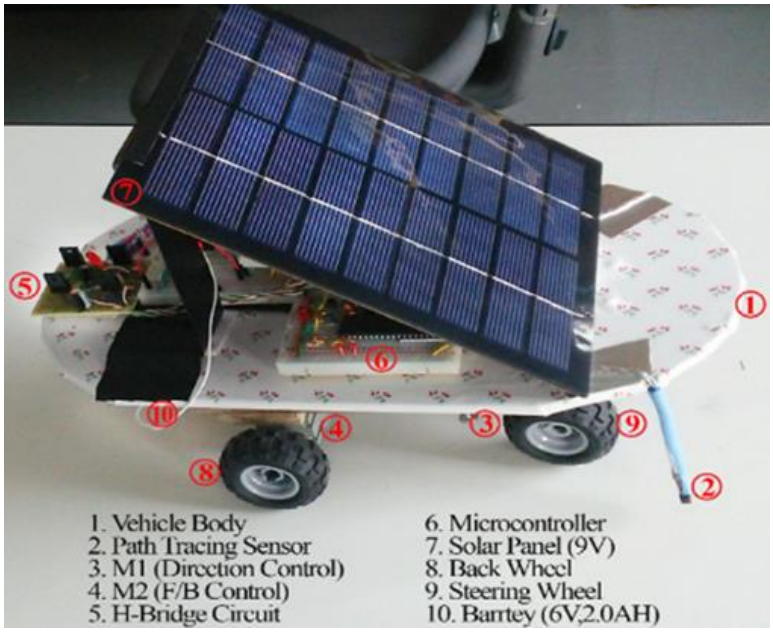


Figure 4-10：Prototype of Slave TG for Network Monitoring

4.5.2. Working Principle of IR Sensors

Tensai Gothalo has multiple sensors. Currently, we are using IR sensors to navigate the path and manage the server. Improvement has been achieved by re-arranging the positions of the IR sensors. Moreover, the quality and the shape of the path were modified slightly so that Tensai Gothalo does not lose the track. Experimental results show that our sensors were able to drive the vehicle more than 97% accurately on the track.

4.5.2.1 IR Sensors in the Track

Currently, the path is designed with black colour in the middle sandwiched by white taped material on both sides. We have placed two side by side sensors that provide the waves to the surfaces. The black surface absorbs the IR waves, whereas the white surface reflects them. This

sensor consists of an IR transmitter and receiver. The output of the IR receiver will be fed to the control unit, and thus the device will be controlled as per the signal from the sensor.

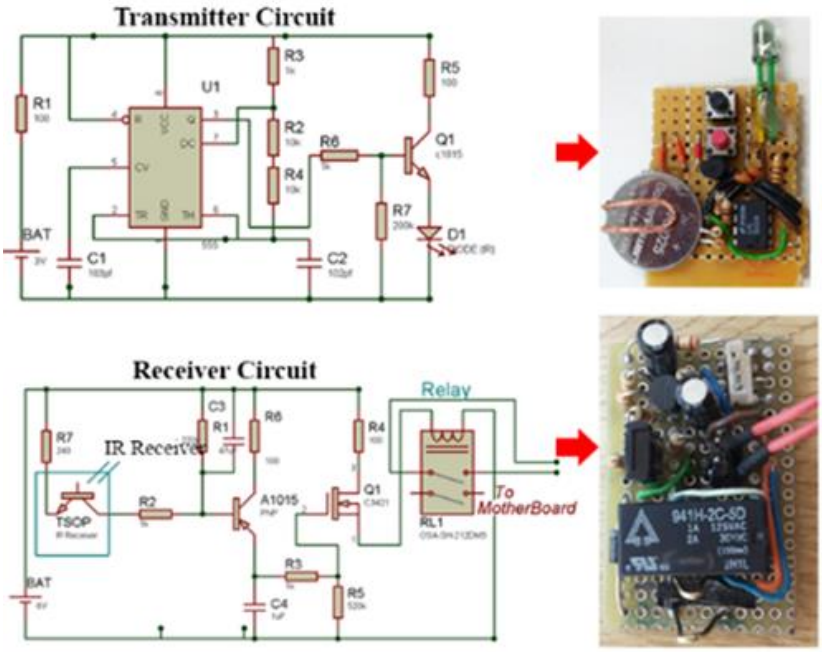


Figure 4-11 : IR Transmitter, IR Receiver and Lab Made Chip Set

4.5.2.2 IR sensors in the Server Node

To monitor the server nodes in the network, we have plugged the IR sensors into the server also. Our IR transmitter in the server PC transmits the IR signal to the robotic vehicle (receiver section), informing it that power has gone off and the server is off. As soon as microcontroller gets the information about the server off through Raspberry Pi, it immediately takes response and sends a command to the motor driver circuit, and the vehicle moves to the room and waits for the power to come. If there is already power in the room before the vehicle arrives, it immediately sends a command to switch the server and return back to its original location

Both the IR transmitter and the receiver module were built in our lab. The completed circuit and the chipset are shown in Figure 4-11. The receiver module is attached to the server, and the transmitter module is attached to the slave TG. This transmitter and receiver pair works instantaneously to troubleshoot server power problems. The IR sensor attached to the front of the

direction control wheel of the slave Tensai Gothalo is responsible for path detection. The IR sensor and encoded program will control the direction and will be able to drag the vehicle to the target. Figure 4-9 shows the overall control architecture.

4.5.3. Design for Power Supply

The source of the power supply in the enhanced Tensai Gothalo is provided through solar power. We are using a sealed lead-acid rechargeable battery for this purpose. The power consumption of Tensai Gothalo is further distributed into two units, one for driving the motor and H-Bridge unit and the other in the monitoring unit. The monitoring unit consumes comparatively less energy than that of the previous unit. This solar-based battery charging circuit uses a 4 watt, 9 V, 440 mA solar panel and a variable voltage regulator IC LM 350. As shown in Figure 4-12, the charging current passes through D1 (SCHOTTKY BARRIER RECTIFIER) to the voltage regulator IC LM 350. By adjusting its adjust pin, the output voltage and current can be regulated. RV1 (Variable Resistance) is placed between the adjust pin and ground to provide a regulated output voltage to the battery. Here, diode D3 prevents discharge (drainage) of the current from the battery during the night and during those times when there is no output from the solar panel. Transistor Q1 and Zener diode D2 act as a cut-off switch when the battery is full. Initially, transistor Q1 is off, and the battery gets the charging current. However, as soon the terminal voltage of the battery rises above 6.8 volts, the Zener diode (D2) starts conducting and provides the base current to Q1. As a result, Q1 starts conducting, and then it turns on the grounding. Hence, there is no output from LM350, and the battery is prevented from overcharging. The overall operation is controlled by the following equation.

$$Vout = 1.25V (1+R2/R1) +Iadj (R2)$$

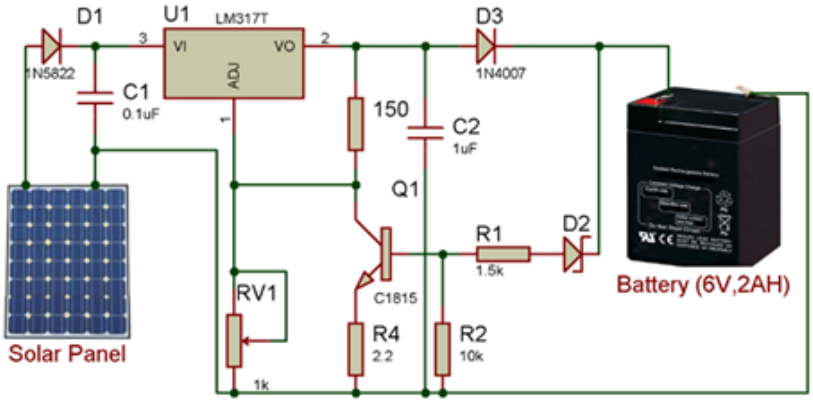


Figure 4-12: Solar Charging system used in TG

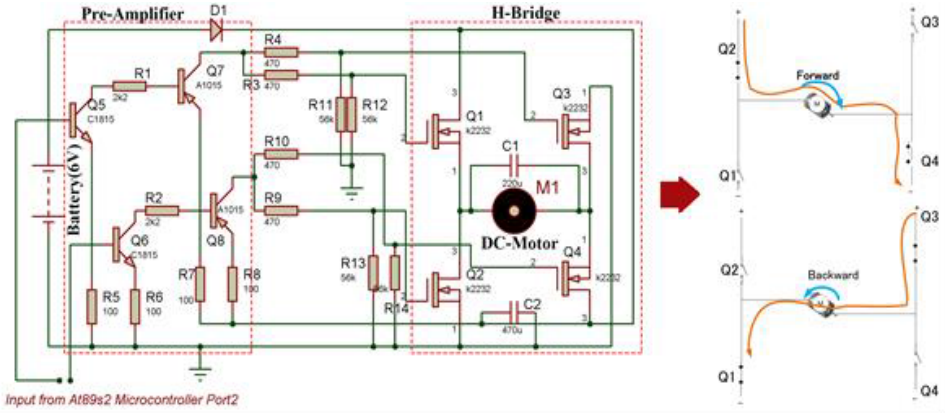


Figure 4-13: H-Bridge Circuit for Direction Control

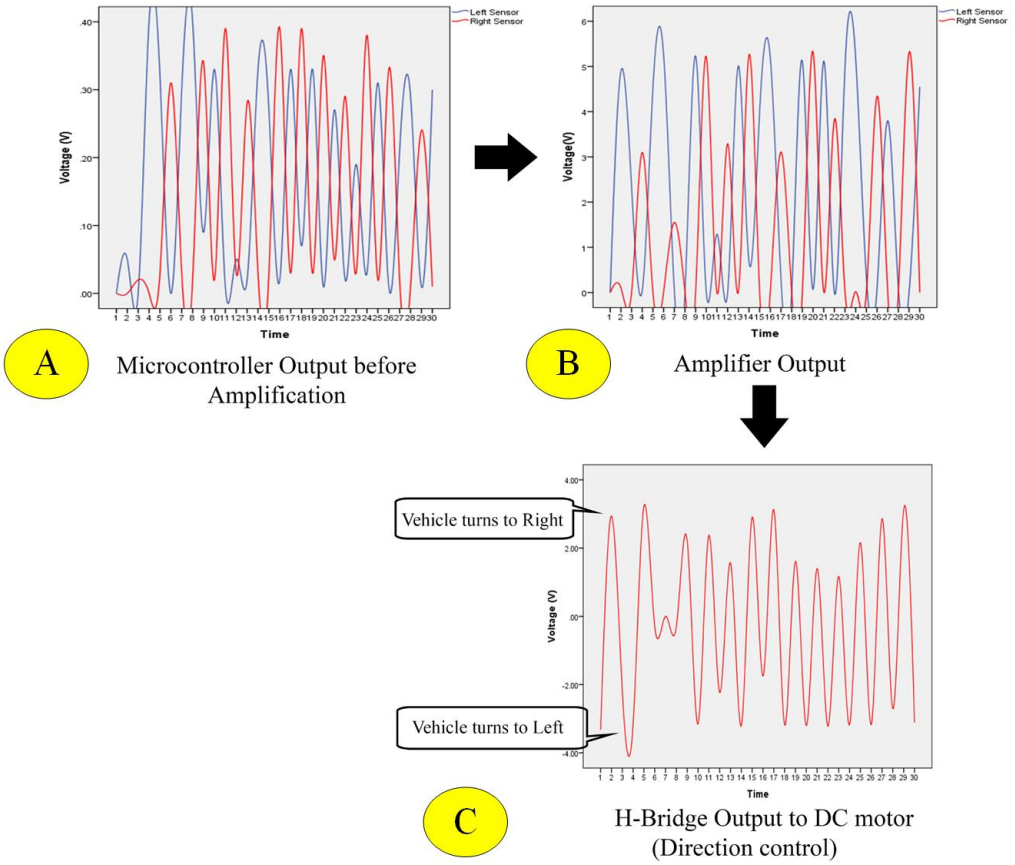


Figure 4-14: H-Bridge Circuit output in Graph

4.5.4. H-Bridge and Motor Control

The ground mobility feature of the Tensai Gothalo is dependent upon the movable unit, which is supported by an automated direction control and movement circuit. Particularly, the direction and movement of this module is controlled through an H-Bridge circuit designed in our lab, refer to Figure 4-13. There are various schemes by which a voltage flow can be controlled through the H-Bridge [54], [93], [94].

When the path tracing IR sensor detects the information of the path from the track, it immediately gives a response to the microcontroller. While the microcontroller receives the

information from the sensor unit, it processes this information, and according to the track information received from the sensor, it produces and relays an output to the transistor connected to its output port. This is controlled by the program that we burnt into the microcontroller AT89252. In the above H-Bridge circuit diagram Figure 4-13, Mosfets Q1, Q2, Q3, and Q4 are responsible for driving the motor M1 (direction control). Transistors Q5, Q6, Q7, and Q8 are used to preamplify the low-level signal that is received from the microcontroller. Because the output from the microcontroller is not sufficient to directly drive the Mosfets and hence the motor, we need to pre-amplify the signal before applying it to the Mosfet. Here, the microcontroller is programmed in such a way that Mosfets Q2 and Q4 are OFF when Mosfets Q1 and Q3 are ON, and vice versa.

The output of the direction control via the H-bridge is plotted in the graph shown in Figure 4-14. We observed experimentally that the initial high-speed output voltage levels when the vehicle is in motion from the microcontroller vary between 0 and 0.4 V. As this voltage level is insufficient to control the H–Bridge directly we amplify it to a certain level so that the MOSFET can be activated. We observed the voltage fluctuations between 0 to 6 V after amplification. This voltage is sufficient to control the H-Bridge, which is plotted in the third portion of Figure 4-14 graph. The variable voltage range during the bi-directional output from the H-Bridge is in the range of -4.2 to 3.8 volts. This range of voltage level is sufficient to drive our vehicle on the proper track.

Table 4-6 shows an H-bridge regulator and the conditions required for the DC to drive the TG into the exact direction and path. It consists of four switches, Q1, Q2, Q3, and Q4, implemented with MOSFETs. However, these MOSFETSs are unable to function with the weak signal received directly through the microcontroller. To make those MOSFETs work properly, we need to pre amplify these weak signal levels. These inputs are amplified through an amplifier circuit placed just before the MOSFET H-bridge circuit. The H-bridge is able to handle the DC motor bi-directionally, depending on the settings of the switches. It uses two voltage logic levels, one the HIGH level of “1” that is required to drive the DC motor and the other the LOW logic level of “0” that is used for stopping the motor.

Table 4-6: Voltage Amplification and Direction Control of DC motor

Voltage Amplification	Closed Switch	Motor Status
Q6, Q8	Q2, Q4	Clockwise Direction
Q5, Q7	Q1, Q3	Anticlockwise Direction

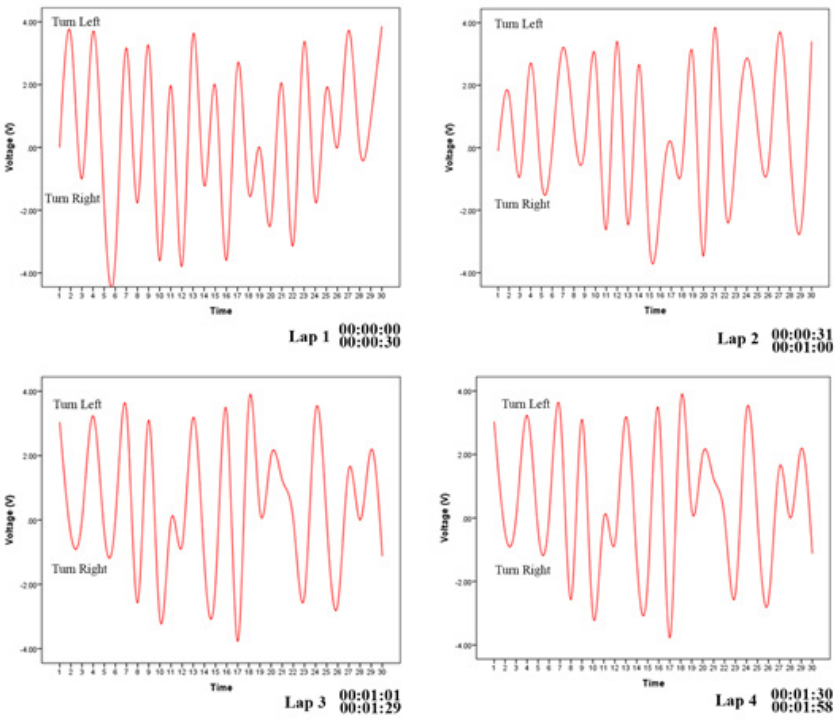


Figure 4-15 : Voltage swing during track navigation

Table 4-7: Vehicle Experimenty Scenario

Measurement	Number of Rises	Direction Changed by Vehicle on Track	Number of Falls	Direction Changed by Vehicle on Track	Lap Completion Time (Sec.)
1	11	Right	11	Left	30
2	13	Right	12	Left	31
3	12	Right	12	Left	31
4	11	Right	11	Left	31

Experimentation of vehicle to test the voltage swing during its movement has been tested along the path and the readings of voltage was carried out for four times of loops. Total time taken for entire four loop is 1 m and 58 seconds. In order to interpret the voltage swing more properly, the result of voltage swings and their interpretation is presented in Table VII. According to the study of the nature of the voltage swing of the H-Bridge circuit, we can further prevent the vehicle from being out of the track. If the rise of the voltage spike in Figure 4-15 goes above a certain predefined level (4 V in our experiment), the vehicle tends to be out of track. However, this condition can be controlled by providing –ve (negative) feedback to the gate of the Mosfet used (i.e., K2232) during such conditions. Hence, a more accurate path tracing feature can be implemented.

4.6. Lab Experiment and System Evaluation of Obstacle Avoidance Module

In addition to its path-sensing capabilities, the slave TG is equipped with an obstacle avoidance unit. Although sufficient literature is available on obstacle avoidance using an IR sensor, sonar system, vision scheme and many other methods, the practical aspects of utilizing an IR sensor in specific circuit configurations at different frequency levels and at different power levels require that circuitry design and implementation engineers pay attention to a number of aspects. There are

numerous studies that have contributed significantly in the field of obstacle avoidance [43], [95]–[97] . However, we realize that a cost-effective obstacle avoidance scheme based on an IR sensor can be built up. To demonstrate a workable solution, we have developed a lab grown obstacle avoidance unit. In this section, we would like to describe the stepwise method of this unit with the output of experiments. The following lab experiments and case studies were conducted to increase the precision of the circuit.

Case 1: Usage of 555 Timer

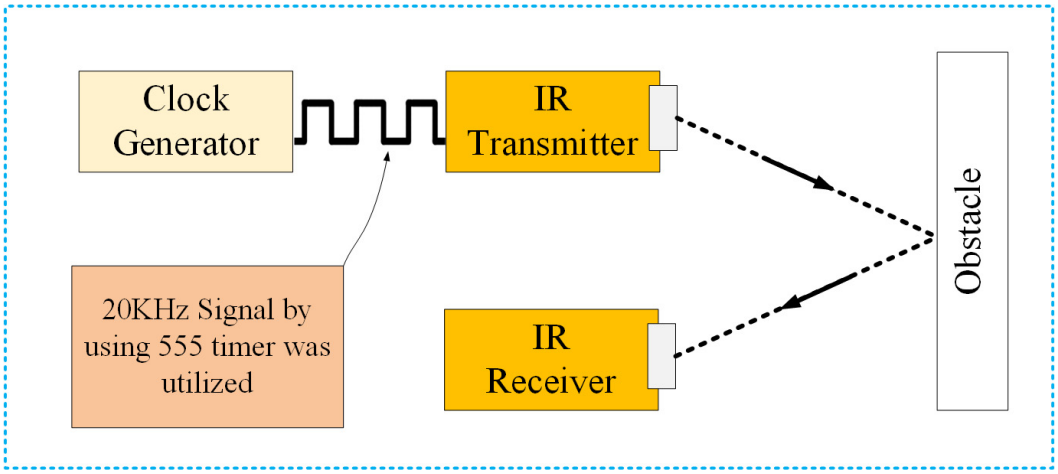


Figure 4-16 : Principal of TX-RX System in TG the Case 1

In this case study we use simple IR transmitter and receiver diode pair and implement it on our robotic vehicle. First we generate a 20 kHz signal using 555 timer and then pass this signal to the IR transmitter diode and receive using normal IR detecting diode. Figure 4-16 shows the basic concept of this case study.

However, we found the following limitations to this implementation:

- White non-metallic objects were detected from maximum distance of 11 cm.
- Whereas metallic objects were detected from 11 to 15 cm only at maximum.
- Nonetheless, black colored objects were detected only from 3 cm.
- IR receiver is not able to filter sun light and other IR generating sources such as electric lamps, heater and other IR signal generating sources so this system consists of several errors.
- Sensor show errors and obstacle is not avoided when the
- robotic vehicle is taken to outdoor environment i.e. exposed
- The obstacle detection time range of vehicle is quite short. This could not captured well in order to give proper control

Case 2: Usage of TSOP1738

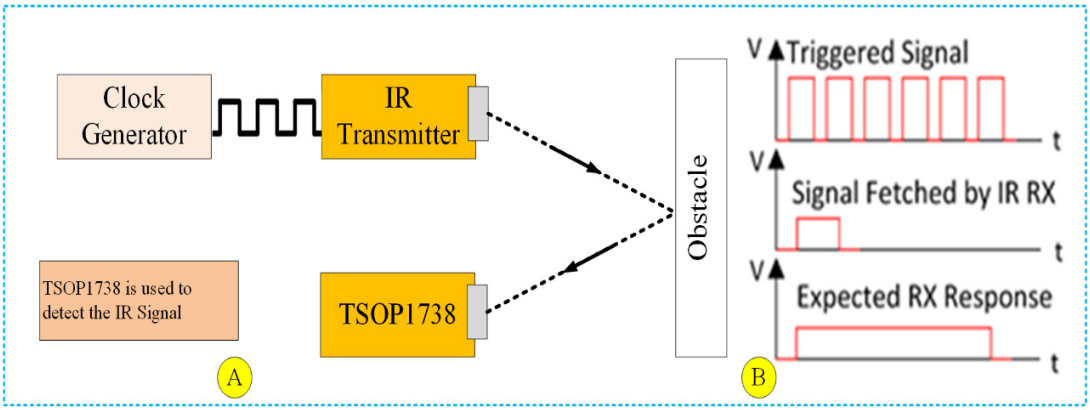


Figure 4-17 : Improvement Scenario of Signal Receiving by Using TSOP1738

In this case we made a slight change in the circuit of Figure 4-16 and use TSOP1738 (as shown in Figure 4-17 left portion) instead as an IR signal receiver. Primarily a clock signal is generated and passed to an IR led and then we receive the reflected IR signal using TSOP1738. The improvement has been described below:

- IR diode continuously transmit the signal with 38 kHz using 555 timer IC.
- When an obstacle is detected IR sensor at first receives the signal and the signal is continuously transmitted till some period of time for instance 1.5 second or for 2 second. And suddenly that signal fades out i.e. converts zero and hence signal is very hard to captured by IR receiver even if there is obstacle in front of the robotic vehicle.
- In order to address this signal fading problem (received from TSOP1738) we are required to changes further in our architecture otherwise it's still quite hard for vehicle to immediately change the path. If decision is not taken reciprocal to the signal vehicle has greater chance of collision with the obstacle then obstacle avoidance and reaching the targeted server is reasonably difficult.

Case 3: Usage of Vcc Generator

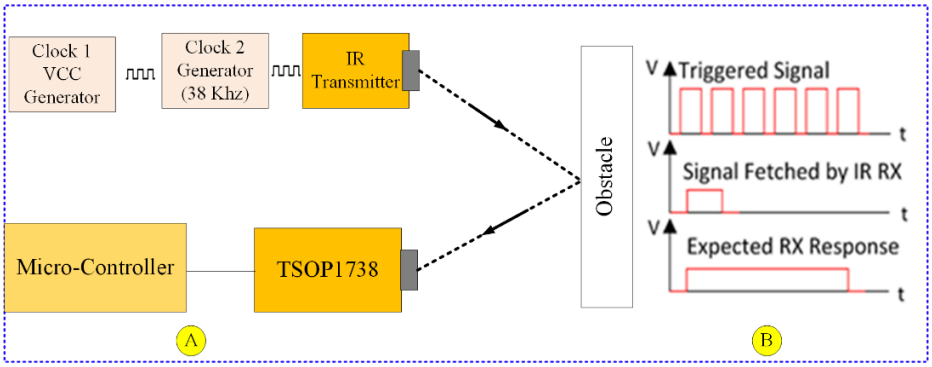


Figure 4-18 : IR TX-RX System in TG Study III

In this case, we study Tsop1738 as an IR signal receiver with some modification, as shown in Figure 4-18. Here, we generate a clock signal of discontinuous voltage (Vcc) and give this voltage to the next clock. In this case, when an obstacle is detected, the signal is reflected back. The received reflected IR signal is detected using the TSOP1738 IR receiver. For the enhanced solution of the troubles arising in the network, we require a faster and more precise response from the sensor, and hence the detection of the perfect path is possible. For the instantaneous obstacle detection, we use this modification in the circuit. Hence, after certain modifications in the programming, the obstacle detection becomes easier than in our earlier case studies.

Mathematical Calculation for clock 1 and its output is shown below.

Calculation for NE555 timer

F_{out} (Clock1) =1.4/ (R1+2R2)*C1 ……..1

= 1.4/ (1+2*20)*47

= 0.7265 Hz

This frequency is used to supply the Vcc to the clock generator (38 KHz).

The above solution gives us the perfect solution for the TG vehicle to detect the obstacle and reach the target. The output waveform is shown below. The logic behind the longer time

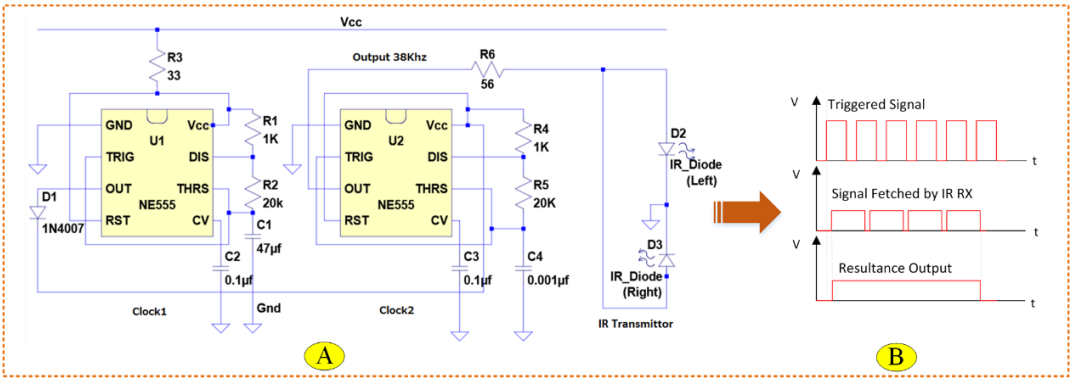


Figure 4-19 : Final Circuit and Resultant Wave Form

duration is that we have been successful in dividing the frequency so that the response from the IR sensor is timed with a lower frequency at which the DC motor can continuously receive the voltage.. In fact, the voltage of motor is interrupted however, this interruption has no significant impact to the motor. We wanted this effect to our motor so that it can continue its operation. This kind of tricky scenario was necessary in order to implement workable module in the field. On the basis of this output, we were successful to get the expected output from the TG. Figure 4-19 shows the wave form on the basis of this logic.

After analysing our case studies and obtaining proper results, we implemented our control circuit and designed the vehicle as shown in Figure 4-10. Similarly, we set up a random scenario of obstacles, as shown in Figure 4-20. These obstacles have different shapes and sizes. We performed several experiments to test whether the TG can avoid the obstacle or not. In our testing, it has successfully avoided the obstacles.

We have conducted different types of experiments to test the performance and accuracy of the sensor in the Electronics and Networking lab of Wakkanai Hokusei Gakuen University

The test Condition and results are:

1. During all the tests, the speed, i.e., forward movement of the vehicle, is fixed and constant.

2. All the readings are taken using a normal digital multimeter.

3. Up and down voltage curves on the graph above are the turns that are taken by the TG during the moves.

4. Test is made on elliptical path, where the width of the black portion is 12 cm and the total length of the test path is 2.5 meters.

5. As the output response, during the turns, the voltage level varies between +ve voltage to –ve voltage, and vice versa. The curves at the upper and lower peaks denote the changes in direction when the vehicle follows the elliptical path, while the duration between the two curves joined by a line is the movement along the straight path.

6. The wider the black track, the less the error is in the path tracing, and a proper white surface reflects sufficient infrared emitted from the path tracing sensor such that microcontroller can make an instant decision of the path. A less white and dirt-covered surface is a source of error.

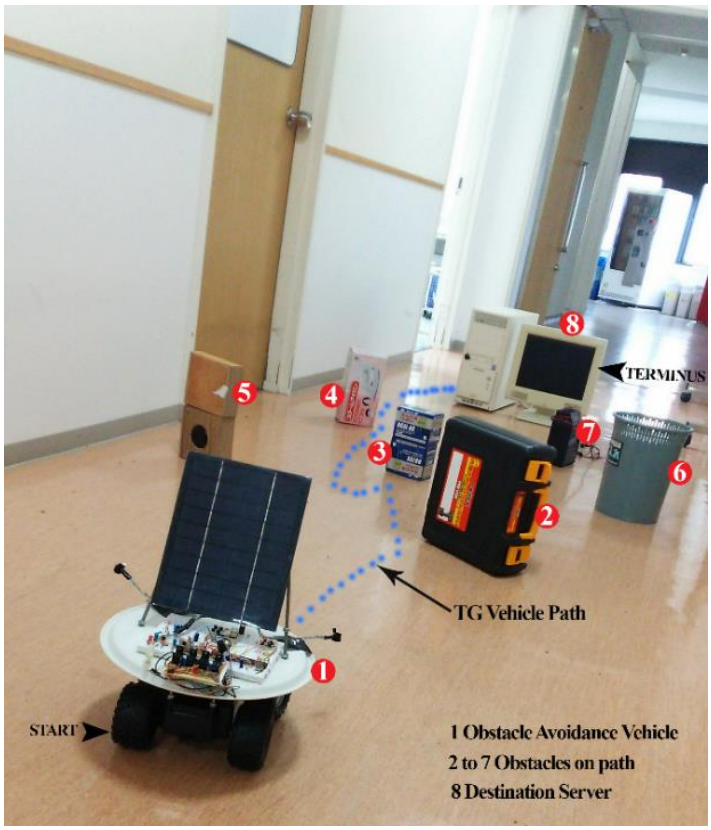


Figure 4-20：Experiment scenario of obstacle avoidance

4.7. Conclusion

In this paper, an innovation in a movable router was discussed and tested. This movable router is designed using a robotic vehicle with the integration of a microcontroller and Raspberry Pi. This movable capability can be applied in numerous occasions and scenarios to monitor and manage the networks. The IR sensors, both in the track and the servers, have been tested. From our lab experiment, the IR sensor based obstacle avoidance presented in this paper has the following characteristics:

- The path-tracing movable router has the ability to detect a black-topped path and to smoothly follow the path. It also can work in manual mode if the vehicle goes off the track or needs precise control by the operator.

- It has the ability to proceed to the troubled server and perform the necessary troubleshooting actions. This innovation has many advantages and can be used in disastrous areas or to monitor unstable networks.
- It has an ability to conduct work on a master-slave basis.

In addition to these capacities, we need to work on some aspects necessary for improvement:

- It is better to utilize a camera-based vision scheme and feed into the system to plan the path. In that way, the vehicle would understand the surrounding situation. Other multiple modes will be employed to ensure that it can still function even if some of the modes fail to work.
- We also recommend sonar-based sensors for better results.

Chapter 5. Development of Monitoring Infrastructure

Portable Tensai Gothalo: Leveraging Network Availability, Survivability, and Manageability through Movable Redundant Device

---

This chapter introduces a novel approach of managing disaster survival networks through the deployment of Tensai Gothalo, a master-slave architecture for network monitoring, management and automation. Tensai Gothalo is a mechanism that enhances the automation, monitoring and management processes of a network without compromising on the existing architecture that executes the prescribed devices and functions. This ensures scalability of the network to meet changing demands. It also investigates fault nodes in the network and initiates the recovery process of fault nodes on the basis of a master-slave monitoring architecture, thereby providing survivability, high availability and manageability. Further, we have expanded on our previous architecture by adding HA clusters so that Tensai Gothalo can act as a proxy server when necessary.

5.1. Introduction

Tensai Gothalo[54] is a network device that can participate in a network as a movable router device. This device is equipped with a movable unit supported by DC motors along with a controlling circuit attached to the device. A path tracing module has been implemented in order to lead the device to the location of a troubled node in a network. Upon finding this node, it will attempt to troubleshoot it and recover the failed network. However, while it cannot recover a trouble node, it will act as a proxy node and deliver network services during the troubleshooting period, thereby preventing the interruption of internet services for users. We designed a path and tested the movability on which Tensai Gothalo operates and traces over it in order to identify the troubled

node. Initially, our research began by simply designing a black-topped path that can be detected by IR sensors; this path can be something as simple as a black line on the floor, or something as complex as embedded lines, magnetic lines, etc. In order to detect or trace the path, different kinds of navigation schemes or vision schemes can be employed. These navigation schemes may vary from simple and cheap IR sensor circuits to complex and expensive vision circuits [95]. Although the decision of which kind of path tracing scheme should to be employed depends on various factors, such as the requirements of users, costs, localities, we have employed IR sensor circuits to detect the path as this can be developed on a low budget. Simple and inexpensive technology offer good advantages in areas where rails or conveyor belts cannot be created. A simple black path can be traced by using simple IR sensors; however, if the device accidently leaves the path, it is difficult to get it back on track.

In our previous studies, we have already completed the development of a movable module. We further enhance Tensai Gothalo by extending its architecture with a highly available cluster (HA cluster) that is supported with a portability feature. In this chapter, we will focus on the design and development of the HA cluster, highlighting its portability feature.

5.2. Problem Identification

Often, large enterprises require a highly available, survivable and secure network infrastructure in order to support their day-to-day business. In order to meet their business demands, it is necessary to design and implement a highly available network. Most of the time, this requirement is fulfilled by providing hierarchical approach leveraging and a high-speed routed core network layer, which often come attached with multiple independent distribution blocks. However, this architecture may not work due to a lack of consideration of the portability of their design and implementation; problems may arise when the network has to physically migrate from one place to another. Similarly, a network may not be re-usable if it has been damaged by natural disaster.

While it is agreed that network availability, survivability and manageability can be achieved by applying a traditional approach, the lack of portability of a system demands a new architectural approach, one that is implemented using a comprehensive strategy. Previous studies

and implementation have paid little attention to the portability of artifacts other than the main hardware or software module. For example, there are no generally accepted portability metrics to measure the entire system, i.e., both the hardware and the software. In this study, we apply a portability measure that can enhance the QoS of the entire system.

5.3. Design Requirement of Portable Tensai Gothalo

One of our major design goals for Tensai Gothalo is to develop a movable and portable network device that can deliver routing services. Besides providing a routing service, our aim is to equip with the capability to deliver other services, such as monitoring and managing the network along with cluster nodes that it can carry over when necessary. Further, it should provide network services during disaster situations, including to remote areas where network administrators are not available. We witnessed that, during disasters, network devices are susceptible to damage, making it necessary to have backup portable devices that operate in a dynamic way. Thus, Tensai Gothalo has multiple objectives.

Portability, in terms of routing, refers to a network's capability of movement from one place to another. However, portability should also include features that enable the device to be by carried by both humans and machines. This factor is very important as people cannot carry heavy equipment effectively the disastrous environments.

In the past, there was perhaps no requirement for such kinds of routers or network devices, since there was never a requirement for systems to operate dynamically. However, there now exists a requirement to provide network services during disasters when the main route of the network stops working. In certain cases, such as in tunnel construction, some scenarios necessitate a specific communication range, which can vary as the length of the tunnel can change during construction.

The other design requirement is to provide a highly available network. In our previous research, we were able to develop portable devices, but availability was not properly considered. Problems may arise if the service of Tensai Gothalo is interrupted or if the device stops working.

In order to address this kind of situation, a redundant node should be considered. We assume that by adding redundant node, we could increase both availability and survivability of network.

5.4. Portability in Tensai Gothalo

This research proposes a novel architecture that incorporates portability considerations into the hardware implementation process. Maximizing portability, nonetheless, is a demanding process that requires phase-wise evaluation of each cycle of hardware implementation. Further, our architecture also demands the enhancement of portability into the software implementation lifecycle. In this particular study, we identify certain issues and propose development guidelines in order to increase portability.

Tensai Gothalo is equipped with a moving module to increase its portability; portability can be enhanced by providing movable and flying capacities in the device. We have paid sufficient attention to increase the portability of Tensai Gothalo as compared to our previous versions.

In order to properly evaluate the device's portability, we need to apply a certain kind of metric. We applied a standard method studied by [98] in our design implementation. We utilized a hardware unit to indicate the hardware module that was incorporated into our entire system. Thus, we define a network system implementation process as a combined implementation process of hardware and software units. In this paper, we use the term Tensai Gothalo to refer to both of these units.

5.4.1. How to Achieve Portability

If a system achieves mobility, modularity/replaceability, compatibility, cost-effectiveness, extensibility and adaptability, we consider the system to be portable. The narrow concept of portability in hardware may refer to the feature of handiness and compactness. Generally, we determine that a device is portable when it is transportable without much difficulty. However, this line of thought does not include broad meaning. As per our design principle, we employed the

concept of the degree of portability measure by applying the following portability metrics introduced by [98] with further clarification.

DoPM=1-(cost to port/cost to redevelop)

A system is portable if the value of the above equation is more than 0. First, let us clarify the meaning of the term “cost”. Cost means the total value of portability parameters. Portability parameters include mobility, modularity, compatibility, extensibility and adaptability. If all of these parameters are addressed, we assign 0 and only count the cost to port. If any of these parameters are not addressed properly, that means there is some cost of port that will be divided by the cost of redevelopment and the output is calculated for the value of degree of portability metrics (DoPM). Theoretically, the value of portability will be 1 when there is perfect portability; however, such a situation can hardly be achieved..

5.5. Redundancy and HA Cluster

5.5.1. Overview of HA Cluster

As per our portability principle, we need to develop the hardware module on a modular basis. Considering modularity and portability, we have developed an HA cluster module. Figure 5-1 shows the general conceptual architecture of the HA cluster that to be implemented in Tensai Gothalo. In this architecture, we have set up six nodes. Each node consists of Raspberry Pi with Debian Wheezy. A summarized specification is provided in Table 5-1. Among the six nodes, two are proxy servers that balance the load between the servers. Figure 5-2 shows the logical topology of the same, in which all traffic requested from a client will be balanced by a load balancer and proxied through HAProxy. Therefore, when designing a load balance solution, it is crucial to realize that all network traffic flows through it. Our design principle indicates that in order to increase portability, we have to include physical mobility in the device also. This feature has been accomplished in our previous studies [42], [43], [54], where we have implemented a movability feature in our device. In order to test this feature, we performed a number of demonstrations, which can be seen in Figure 5-3 annotation 1. In this research, we further extended our functionality and

thus added the feature of availability of servers. In order to achieve this quality of high availability, we decoupled the architecture and the HA cluster.

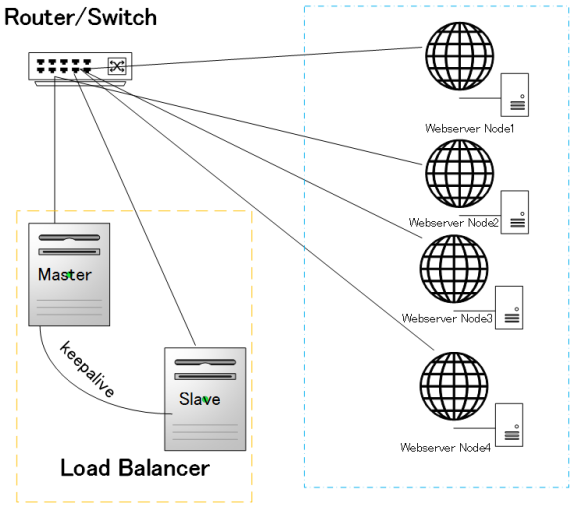


Figure 5-1 : Physical Topology of HA Cluster

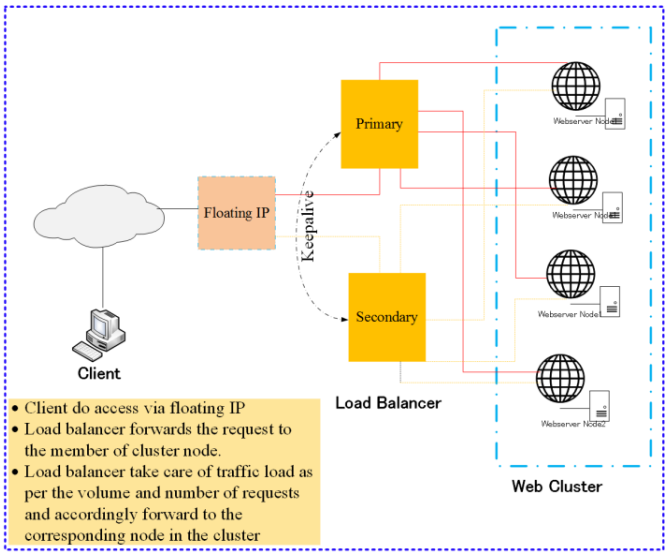


Figure 5-2: Logical Topology of HA Cluster

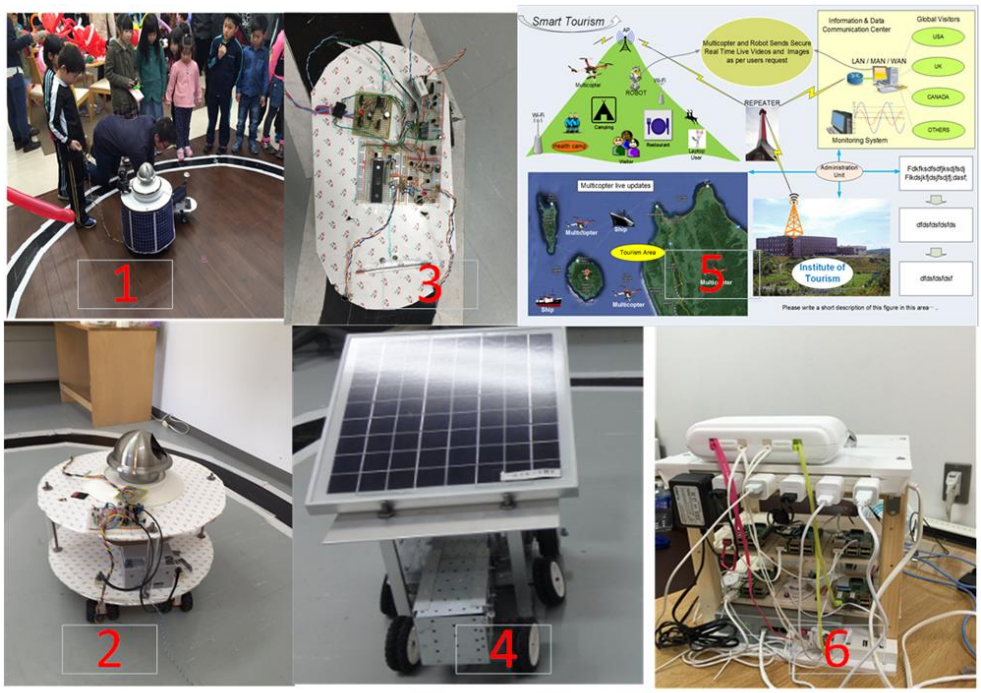


Figure 5-3：Concept and Demonstration Scenario of Tensai Gothalo

separately. Our description about hardware architecture will focus only on this pluggable portion. Further, let us describe the annotation in Figure 5-3 in more detail. Annotation 1 indicates the demonstration of a movable Tensai Gothalo, in which the testing of movability was done during a special event held in Wakkanai city. Annotations 2, 4 are the nodes of the master Tensai Gothalo. These master nodes necessitate higher computing capacity so that it can observe the entire network. While a network faces a problem (for example, the network in annotation 5), it will inform the slave Tensai Gothalo, which will then proceed to the troubled node and try to solve the problem. Annotation 3 indicates the slave Tensai Gothalo, which can proceed along the path. Further,

annotation 5 shows the potential network environment in which Tensai Gothalo can operate in future.

5.5.2. Monitoring Topology and Process

The primary objective of developing an HA cluster is not only to provide a computing resource during a disaster, but also to provide a stable monitoring framework before substantial

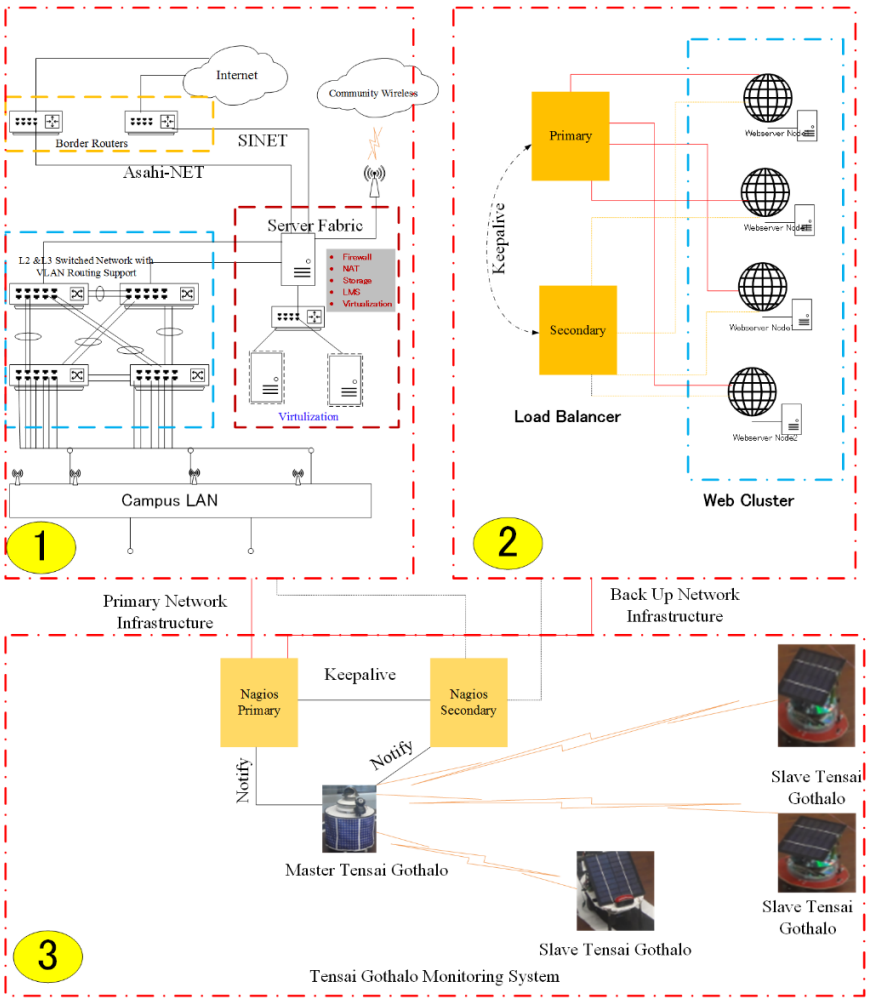
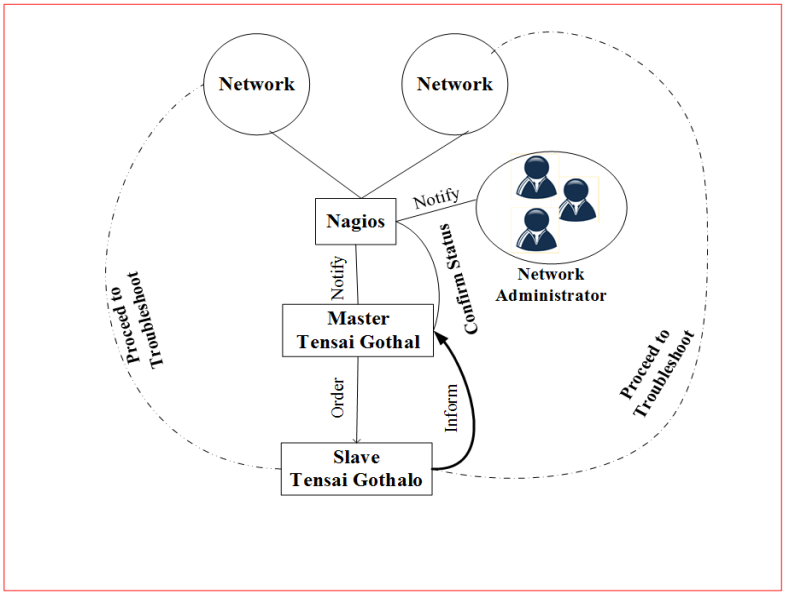


Figure 5-4: Monitoring Framework

damage occurs in a network and business. Figure 5-4 shows our entire monitoring framework. Let us suppose that an organization has a network, as depicted in annotation 1, which was designed on the basis of our simulation scenario (see Chapter 3). In order to provide a disaster-ready network,

a backup of this network infrastructure is necessary. Annotation 2 indicates the skeleton of this network, which we call an HA cluster, developed in a relatively low cost. Accordingly, annotation 3 indicates our monitoring scenario of these computing resources. This monitoring framework is designed with the integration between Nagios and Tensai Gothalo monitoring and management devices. The integration of such devices is required because Nagios does not have the capacity to troubleshoot the network on its own; it just monitors the availability of the resources. However, monitoring of availability alone is not sufficient to guarantee network availability during a disaster.



Monitoring and Trouble Shooting Process

- Nagios detects the trouble in a network
- It notifies to the Master and Administrator about the problem
- Master TG instructs slave TG to trouble shoot the corresponding trouble node in the network.
- Slave TG proceed to the trouble node and fix the problem.
- It informs Master TG about the status.
- Nagios detects the update of status and accordingly notifies to the admnistrator.

Figure 5-5: Monitoring and Troubel Shooting Process

It also requires a troubleshooting mechanism on the fly. To address this issue, this framework integrates Tensai Gothalo into the system. The working principle of monitoring and management of this framework is indicated in Figure 5-5. As shown in Figure 5-5, the Nagios process monitors availability of network services; if it finds any trouble in the network, it notifies the problem to the network administrator and the master Tensai Gothalo. The master Tensai Gothalo will then instruct

the slave Tensai Gothalo to proceed to troubleshooting. Upon troubleshooting the problem, it will update the master Tensai Gothalo with the status. As the Nagios process continuously updates the status of the network, the network administrator can monitor the entire scenario of the network. In the case of extreme situations, such as an unexpected shutdown of the entire network, a backup network is required. Tensai Gothalo, then, provides its own networking services, providing wireless LAN and also deploying the HA cluster for emergency networks. In the following section, we describe the operation and performance of this HA cluster.

5.6. System Development Process and Evaluation

On the basis of our design principle, we needed to implement an HA cluster. As shown in Figure 5-1, this cluster has seven nodes. There is a root node to which the other six nodes are connected. The root node resides inside the cluster, delivering connectivity to all the other nodes. Among these, two of the nodes are ported with a master-slave architecture. Master and slave nodes are necessary to acknowledge each other by sending a keep-alive message. In a real-life scenario, the master Tensai Gothalo will carry the master node , while the slave Tensai Gothalo will carry the slave node. Although only a single node of a load balancer can handle the entire traffic, we need to consider the redundancy of this load balancer. Balancing traffic flow among cluster nodes can be carried out by a single load balancer. Nonetheless, this sort of solution is not sufficient when a robust HA cluster is required for critical services. Therefore, our design combines the load balancer and failover capability with a redundancy solution, allowing users to access various servers; this is a relatively effective and reliable solution.

Our aim of designing HA cluster in this research is to increase availability of network and other services even in the disaster situation. Various researches[41], [42], [99] show that network connections, disruptions and base station blackouts occur during natural disastrous. The authors well witnessed the “great east Japan earthquake” on March11, 2011, in which

Table 5-1: Experimental Setup

Particulars	Details/Quantity	Remarks
Virtual Interface		10.X.X.251
Operating System	Raspbian	Model B+
Master Load Balancer	1	Eth0: 10.X.X.250
Slave Load Balancer	1	Eth0: 10.X.X.249
Server Nodes	4	10.X.X.248 10.X.X.247 10.X.X.246 10.X.X.245
CPU Model	Hardware: BCM2708	ARMv6-compatible processor rev 7 (v6l)

Table 5-2: Load Testing and Benchmarking

Number of Users	Transactions	Availability	Elapsed time	Data Transferred	Response Time	Transaction Rate	Throughput	Concurrency	Failure Transaction
10	8806	100%	59.71s	1.23MB	0.05s	147.48t/s	0.02MB/s	6.95	0
20	8331	100%	59.26s	1.16MB	0.08s	140.58t/s	0.02MB/s	11.25	0
30	9316	100%	59.29s	1.30MB	0.19s	157.13t/s	0.02MB/s	29.73	0
40	9452	100%	59.90s	1.32MB	0.25s	157.8t/s	0.02MB/s	39.55	0
50	9222	100%	59.21s	1.28MB	0.32s	155.75t/s	0.02MB/s	49.28	0
60	9253	100%	59.65s	1.29MB	0.38s	155.12t/s	0.02MB/s	58.93	0
90	9200	100%	60.08s	1.28MB	0.57s	153.13t/s	0.02MB/s	87.28	0
120	9118	100%	60.01s	1.27MB	0.75s	151.94t/s	0.02MB/s	114.31	0
150	9028	100%	60.36s	1.26MB	0.93s	149.57t/s	0.02MB/s	139.00	0
180	8399	99.98%	60.02s	1.17MB	1.13s	139.94t/s	0.02MB/s	158.32	6
210	8824	99.95%	60.34s	1.23MB	1.17s	146.24t/s	0.02MB/s	171.21	4
240	8510	99.93%	59.96s	1.18MB	1.32s	141.93t/s	0.02MB/s	186.96	6

270	8252	99.77%	59.90s	1.15MB	1.39s	137.76t/s	0.02MB/s	192.17	19
300	8239	90.90%	60.33s	1.15MB	1.39s	136.57t/s	0.02MB	189.62	8

a lot of information and communications technology (ICT) were disrupted. Suggino [100] presented the summary of the damages of the great east Japan earthquake and tsunami in March 2011. The damages to the telecommunication network, in terms of service disruption, network traffic congestion, and base station blackouts, were discussed in the paper [100].

Further elaboration can be found in the paper[99]. This report revealed that 1.9 million fixed telephone lines and 29,000 cellular base stations were damaged during this natural disaster. High availability in the past has been addressed just by providing only a redundant node (either in active/passive or active/active mode) without considering portability in the architecture [99].

This research proposes that in order to build a high availability infrastructure, we can employ a better approach to support and promote greater system adaptability and flexibility. The reason why network infrastructure in the past has been so inflexible is largely due to limitations of physical portability. We generated varieties of packets, and sent these packets at different times to different locations. In our architecture, we built upon the entire system in a modular design basis. Our movable parts were already implemented during our previous researches [43], [54], [95]. Therefore, we will not go into the details of our movable portion. Rather, we describe here our system of the HA cluster.

Table 5-1 shows the IP planning of this cluster. There are two nodes, which are built using a master-slave architecture. The master node will be carried out by our master Tensai Gothalo, while the slave node will be carried out by our slave Tensai Gothalo. These two nodes are configured with an HA (High Available) proxy. The objective of designing an HA cluster in this research is to test whether Tensai Gothalo can provide services when the primary data center cannot. In such cases, Tensai Gothalo has a couple of options. It can either troubleshoot the server and recover the service in a short downtime period, or deliver services on its own, thereby providing service availability. Priority is given to whether the HA cluster will fulfill the service demands, considering the outage of service in the primary data center. The performance of the cluster has

been tested by measuring different types of parameters, as shown in the Table 5-2. The next section will include the corresponding discussion.

5.6.1. Load Testing and Benchmarking

Load testing was carried out in order to measure the performance of the HA cluster at any load level by simply increasing the number of requests until the desired load is achieved. We set up a simple web page with an index file, and decided to test if the cluster can handle multiple requests at the same time. Sending large numbers of requests to the servers requires a proper methodology. Therefore, we used 10 concurrent users and increased 10 users per test incrementally. As the data shows in Table 5-2, we gained 100% availability for up to 150 users. However, as we increased the number with an additional 30 users, availability decreased to 99.98%. We continued to increase portability and high availability by sensing network problems in the infrastructure, thereby providing a redundant node dynamically.

5.7. Results and Discussion

5.7.1. Load Balancing

One of our major objectives in the development of HA clusters is to provide continuous availability of services by eliminating any potential single points of failure. We were able to achieve such results by applying our design, as described in Chapter 3. However, a problem occurred when

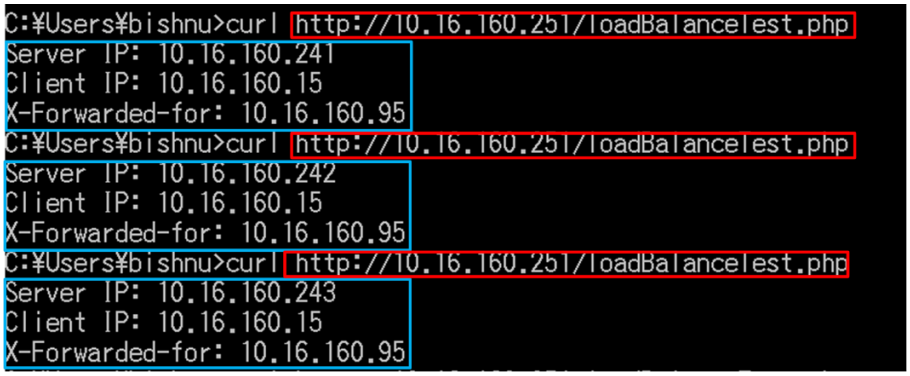


Figure 5-6: Load Balance Testing by CURL Tool

there was a problem in the load balancer. As per our design consideration, it is important to note that the load balancer also needs to be supported with a backup node. Thus, we also considered the redundancy of the load balancer. As shown in Figure 5-2, failover is accomplished by providing a secondary node for the load balancer. Node failures in HA clusters and also in the load balancer are not visible to clients outside the cluster.

5.7.2. Availability Analysis

Table 5-2 shows the results of the load testing and benchmarking of our HA cluster. We aimed to increase availability, serviceability and manageability by using a redundant device: the Tensai Gothalo. Many previous researches have emphasized the importance of redundancy and most of the practices have been involved with layer-based redundancy. However, these studies lack a focus on mobility and portability.

Our prototyped HA cluster has produced high availability for up to 150 concurrent users. We have not observed any failure in transaction at this level of concurrent users. Services were not been interrupted until the number of concurrent users was increased to 300; then, the level of availability sharply decreased to 80%. We believe that availability can be increased even more by increasing the number of nodes in the cluster. It was also observed that when the response time crossed the 1-second mark with 180 concurrent users, the availability percentage decreased.

5.7.3. Survivability Analysis

The term “network survivability” has been in existence for a long time. It has been studied and defined as “the capability of a system to fulfill its mission in a timely manner, in the presence of attacks, failures, or accidents” [101]. It also refers to the capability of a system to offer services during nodes failure. With regard to our studies, this poses the question: If one of our redundant nodes is offline, will another node continue to provide the service? Upon testing this feature, we observed that there was continuous connectivity during the entire experiment. This confirms that if any master or slave node of this cluster is offline, the other redundant node will continue to offer the service.

However, we agree that survivability may suffer while installing the current prototype in harsh geographical regions. In order to increase survivability, we need to secure the device by attaching a secure covering box to the cluster in order to protect it from the harsh environment.

5.8. Future Work

We have begun considering portability features not only in the realm of software implementation, but also in hardware implementation. However, the complete implementation for hardware has not yet been achieved. Nonetheless, the concept of portability has been considered, and a much-expanded, design-based work has begun; for this, an HA cluster has been integrated in the lab. A prototype has been designed and experiments have been conducted to test the robustness of the implementations. Research into the capabilities of embedded systems and how they can be leveraged for hardware architecture has also been accomplished. Since portability is a concept that needs careful and phase-wise implementation, it requires standardarized methodology and documentation in order to overcome potential problems during future implementations.

Our future works will also emphasize employing and documenting more concrete steps so that the more abstract portions of the design remain detailed and well-tested. For example, the complex design and integration between the microcontroller and other OSs should be formalized, detailed and tested. Furthermore, we would like to enhance the survivability of networks during disasters by providing alternative energy or power backup systems. Survivability suffers critically in terms of power backup during disastrous situations. Similarly, manageability of the network will increase by integrating the management operation by Tensai Gothalo and other software tools. An intensive study will also be conducted to improve the manageability of networks.

5.9. Conclusion

In this research, we designed the prototype and touched upon the relatively broad concepts of portability, high availability, survivability and manageability, focusing mostly on hardware architecture, which will guide further specifications and implementations for a relatively low cost.

However, this is not the complete scenario of the discussion. We have initiated enough discussion into these areas in terms of portability, so that future research will bring deeper and standardized concepts into this area of computing. While most researchers are not currently focusing on deploying movable modules for network infrastructures, we have shed sufficient light upon this architecture. As per our architecture, we believe that physical mobility is not a difficult part of the implementation process; in fact, it should be considered deliberately.

Further, our study provides crucial academic value. For example, due to the high costs of network infrastructure, most of academic institutions are reluctant to allow their students to work with hardware in the lab. This trend poses a challenge to researchers, who have to adjust their curriculum to meet the new challenges posed by the field of computer science. Further, instructors in the colleges or universities need to abandon lower-layer content from their curricula in order to make the content digestible to the students. This trend will definitely lead to a great loss in terms of hardware knowledge in the field of computer science. As academicians and researchers, we must combat such situations by introducing relatively low-cost infrastructure, which has been made possible with the use of Raspberry Pi as our core computing resource.

To conclude, this paper incorporates the issues of portability that should be considered as one of the principal activities of the system implementation process in Tesnsai Gothalo. This study shows the guideline of portability implementation in Tensai Gothalo; however, this guideline can be applied to any other system implementation. The key point is to incorporate portability in both hardware and software in order to maximize effectiveness. While portability has been the subject of software development processes, it has thus far been considered mostly in terms of handiness or compactness in the hardware sector. This paper has considered portability issues and shed light on the concept of portability that includes, crucially, the mobility of a system and portability metrics. These concepts will collectively enhance the manageability, survivability and availability of networks.

Chapter 6. Deployable Service infrastructure in DRN

Fogging Jyaguchi Services in Tensai Gothalo

This chapter describes an efficient method of fogging in Tensai Gothalo. Tensai Gothalo is a novel dynamic router device developed in the Gautam-Asami Laboratory of Wakkanai Hokusei Gakuen University, which has sensing, actuating, monitoring and movable capabilities. Similarly, fogging is a new concept of cloud computing in which the data plane is defined as a user device. In this paper, we would like to present a stepwise explanation of how to fog in Tensai Gothalo. Further, we will elaborate upon a technique to decentralize data with improvements in QoS and reductions in latency, without affecting the legacy services of clouds that can still work together when needed.

6.1. Introduction

Fog computing is a new paradigm that enhances the cloud computing paradigm from a data center plane to the clusters of the end-user-devices plane, which we have termed as “fog” in this paper. Cloud computing has shifted computing resources more or less from the user plane to the data center plane, thereby centralizing the computing infrastructure into huge data centers. In contrast, fog computing decentralized the resources from cloud centers to the end-users or to the edge of the network, thus enabling a new breed of applications and services with new potentials. More specifically, fog computing is a computing paradigm that brings data processing, service utilization, networking, storage and analytics closer to the devices and applications that are closer to users. In this paper, we argue that fog computing is a new paradigm of computing that uses the

platform of the Internet of Things (IoT), Smart Grid, Smart Communities, or newly developed computing devices.

6.2. Significance of Fog Infrastructure

Due to the intense growth of the Internet over the past few years, computing resources are now more ubiquitously available. This growth has brought about significant achievement; for example, it has enabled the realization of a new computing concept called “cloud computing”. Cloud computing infrastructure is categorized into three main categories: SaaS, IaaS, PasS. Though these seem to be demarcated into three separate categories, all three are utilized together to build the application. The big giants of cloud computing are Google, Microsoft, and Amazon.

The main goal of cloud computing is to leverage the Internet to consume software or other IT services on demand. Cloud users can share processing power, storage space, bandwidth, memory, and software. In response to their usage, cloud providers charge users according to their consumption. This sort of business concept has been derived from the concept of utility business; thus, cloud computing sometimes refers to utility computing, too. In this way, users are not required to set up or to buy hardware on their own. This has brought about a huge paradigm shift in the market. However, it has not addressed all the issues raised in the user front.

Regardless of its supremacy in terms of providing resources to the end users, this technology has number of issues:

- Cloud computing has given rise to new data security challenges. Existing data protection mechanisms, such as encryption, have failed in preventing data theft attacks, especially those perpetrated by an insider at the cloud providing service.

- A notable research to address this issue, which involves applying disinformation attack methods that return large amounts of decoy information to the attacker, has been introduced. However, once the data are transferred from the local LAN to the Internet, there always remains the vulnerability of data theft.

- The more notable issue could be data residency. Cloud data centers can span the country or continent, so there could be great differences in the rules, policies and the laws between the consumer's society and the provider's society. Further, the issue of potential access to data by foreign governments is part of a wider issue, which is that the use of services based in other countries may result in customers being affected by the laws of those countries.

In order to solve these kinds of issues, a new kind of computing architecture is necessary. The abovementioned data theft issue can only be minimized by keeping the data inside one's premises. This can be offered by utilizing fog computing infrastructure.

6.3. Related Research

Research related to fog computing has emerged since this term was coined by Prof. Salvatore J. Stolfo. However, on the industrial research front, Cisco System Inc [102] seems to be the frontrunner in adapting this technology. Being a relatively new term, there are very few studies that make a significant contribution to the literature. However, there are some studies in academic areas, for example, [103] uses fog computing infrastructure for healthcare systems. Similarly, [104] focuses on mobile users, whereas [105] highlights security issues in fog computing.

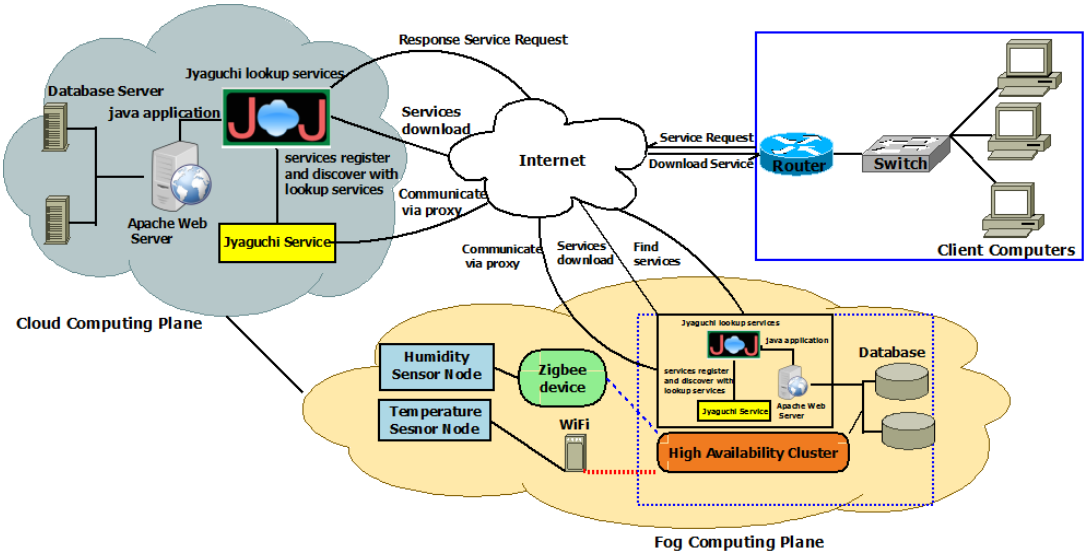


Figure 6-1 : Jyaguchi Fog Architecture

Our research not only explores the existing methods and challenges faced by the cloud, but it also conducts practical research and explores new methods that can enhance fog computing research. Further, we have integrated fog infrastructure with newly developed devices, such as Tensai Gothalo, which the authors have previously developed.

6.4. Domain of Jyaguchi Fog

We have identified the following areas where Jyaguchi fog can contribute its features. Here, we highlight the major characteristics that Jyaguchi fog should maintain, such as it:

- Should manage wide-spread geographical distribution, such as for sensor nodes;
- Should have support to mobility access;
- Should have diversity of devices, nodes or users;
- Should maintain essential access to varieties of link connections, such as wired and wireless;
- Should have strong presence of streaming and real-time applications;
- Should have heterogeneity of devices and data sources;
- Should support big data analysis;

- Should have low latency for quality of service and location awareness.

6.5. Tensai Gothalo as an infrastructure node of fog

Tensai Gothalo[102], [103],[104] is a robotic vehicle that has routing and monitoring capabilities. This device can be used either as a router device or as an end-user device, the cluster of which can also create fog infrastructure. In a current paradigm of Internet of Everything (IoE), we can consider Tensai Gothalo to be a thing. A thing in IoE is any natural or man-made object that can be assigned an IP address and participate in the communication. Jyaguchi fog can transmit data over a Tensai Gothalo network that resides relatively close to the end-users. Transmitting data through the Internet to a data center might consume great deal of bandwidth. However, data transferred by Jyaguchi fog can be controlled, whether it is used to cross routers or to put into the fog devices of Tensai Gothalo. Data residing in fog devices do not always cross the access router, and thus reduce the suffering of latency.

6.6. Architecture and Resource Allocation Decision Process in Jyaguchi Fog

Figure 6-1 shows the overall architecture of the Jyaguchi fog infrastructure. Jyaguchi has adopted the new phenomena of controlling the residency of services. Its types of services are often categorized in terms of granularity. It has the following categories:

- Mini Services: Services have very minimal granularity
- Macro Services: Services relatively have larger granularity than mini services
- Mega Services: Services with larger granularity than macro services and which are preferred to reside within end-user premises or relatively closer to end-users.

The details about granularity are described in [106] in detail. Among these services, we found out that few services are necessary to handle properly. For example, services which need higher security and the services which have higher granularities. Services that needs higher securities are vulnerable while they are exposed in the public cloud. Therefore, these sorts of

services may require to be kept inside the premises with higher security. The other types of services, such as mega services, which require higher bandwidth, are recommended to be kept inside the premises. Further, in the case of mega services outside the end-users premises, it is recommended that it be kept as near as to the user's network as possible. In such cases, multiple fog environments can be created, thereby proving a cluster of Jyaguchi fog. A topology-based redirection can be applied in order to redirect the traffic to the nearest user networks.

6.7. Service Allocation Decision Process

Resource sharing or allocation process is a process that tries to reduce the mean response time in order to access the resource in a network. A very simple line of thought to decide where to access depends upon the response time. The greater the time it requires to response, the lower the performance it offers. There needs a service allocation decision process that must account for the fact such that when designing an algorithm for resource sharing in the Jyaguchi fog, a quantifying method should be applied in order to measure the performance and the efficiency. First, let us describe our consideration about quantitative evaluation approach for the decision process. In this evaluation process, we highly advocated the evaluation criteria by measuring the response time (RT) of the resource. RT would be core metrics to account its performance.

The RT value could be the response time of the entire cluster or a particular service. The equation for this is given as below:

Total Response Time = $\sum_{i=1}^{n}(RT(each\ host(i))$ ----------1

Equation 1 indicates the method of calculating total response time of the infrastructure. The higher the response time, the lower is performance. Response time can have influences of CPU, memory and the network bandwidth. The cumulative effect will be reflected to the value of response time.

Jyaguchi service provider can select the better RT value in which it can register its service. Whereas Jyaguchi client can access to the resource where the RT value is low. Considering this value, resource allocation policy can be defined.

The same formula will be enhanced in order to recommend the metric for which the client and service provider can take the reference. This reference values can be taken automatically through program or by manual.

$$\text{Priority Index (PI)} = \frac{Total\ RT}{\text{Total Number of Measurement}}$$

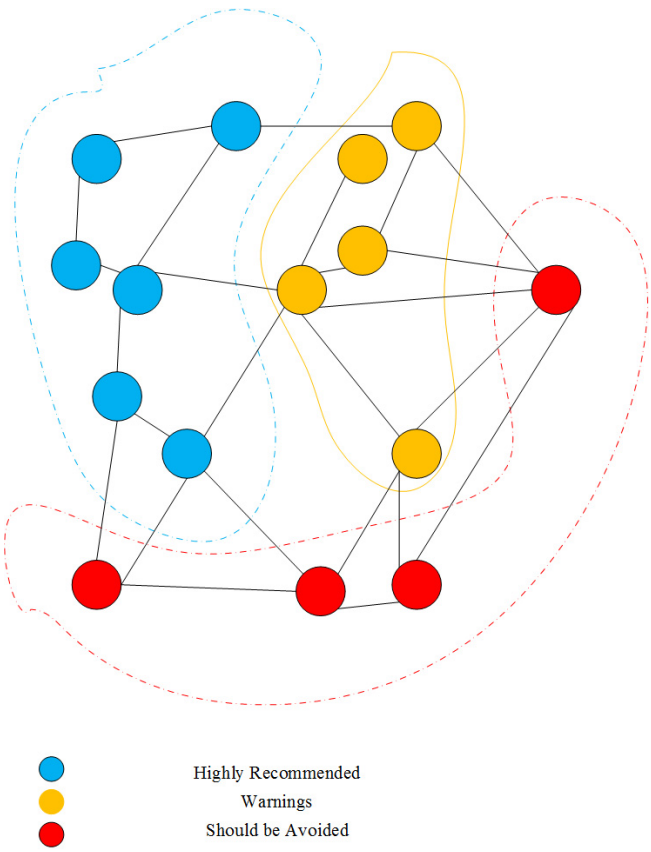


Figure 6-2 : Visualization Map of Priority Indicator

Where the value of PI is obtained by dividing the total response time by the total number of measurement. This is the mean value of the response time which will be taken into consideration while allocating the resource. Jyaguchi service provider or user can state this PI metric with the representation as shown in Figure 6-2.

Figure 6-2, shows an example of the visualization of the map representing the priority indicator. The blue nodes indicate the best recommended candidate that both the service provider and the client can utilize to either access the resource or to publish the resource. Similarly, the yellow nodes need to be used with a higher level of caution, whereas the red ones are not recommended at all.

6.8. Implementation of Fog Services

Conventionally, the Jyaguchi platform has been used to develop cloud computing services. Further, the platform of Jyaguchi has also been utilized in hybrid computing infrastructure network integrated with smart devices and Micro Engineering Tools [106] in the cloud. Micro engineering tools are the highly dynamic and interactive services developed in the Jyaguchi Cloud platform at which Java based application can be built and exported to the client over a network [106]. The implementation process is quite similar with previously implemented process. Thus, there is no overhead in learning to adapt the new computing infrastructure. We have already discussed the significance of fog computing infrastructure in Section 2. In this section we discuss the implementation process of fog services. For our description, we consider only few services which utilizes our premises in order to collect the real time data. For example, we have built upon weather report services by using our own hardware units. These units are equipped with sensor nodes which collect the data from the surrounding environments. For our experimental setup, we utilized temperature and humidity sensors. The figures of these sensors, circuit and the communication with Raspberry pi is also given in the Figure 6-4. The basic reason of the development of Fog Services in Tensai Gothalo [54], [95] is to improve efficiency of data to be transported in fog network for data processing, analysis and storage. As previous studies contributed to the emergence of Tensai

Gothalo as one of the most reliable and robust network devices, we selected fogging infrastructure to build upon the services integrated with this device.

Next, let us discuss the process of fogging Jyaguchi in Tensai Gothalo in a stepwise manner:

- Phase 1: First, we need to set up a fog infrastructure. This infrastructure needs different components. The details of our experimental setup developed in our lab is provided in Table 6-2. Also see the Figure 6-5 and Figure 6-6 for our environmental setup and the connections between different architecting nodes.
- Phase 2: Next, we need to install the Jyaguchi infrastructure in TG. However, TG must be equipped with sufficient computing resources. This has been achieved by integrating Raspberry Pi in TG. The details of the Jyaguchi Infrastructure are as follows:

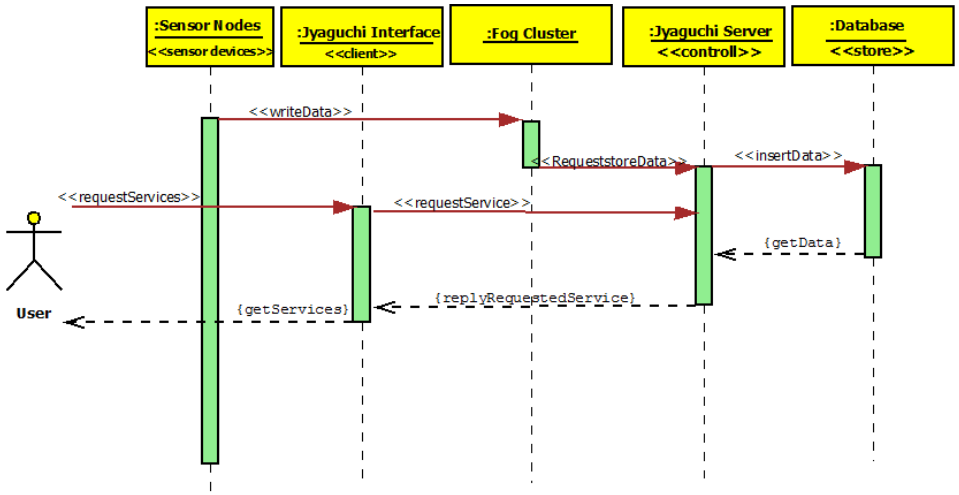


Figure 6-3 : Standard Sequence Diagram of Fog Service

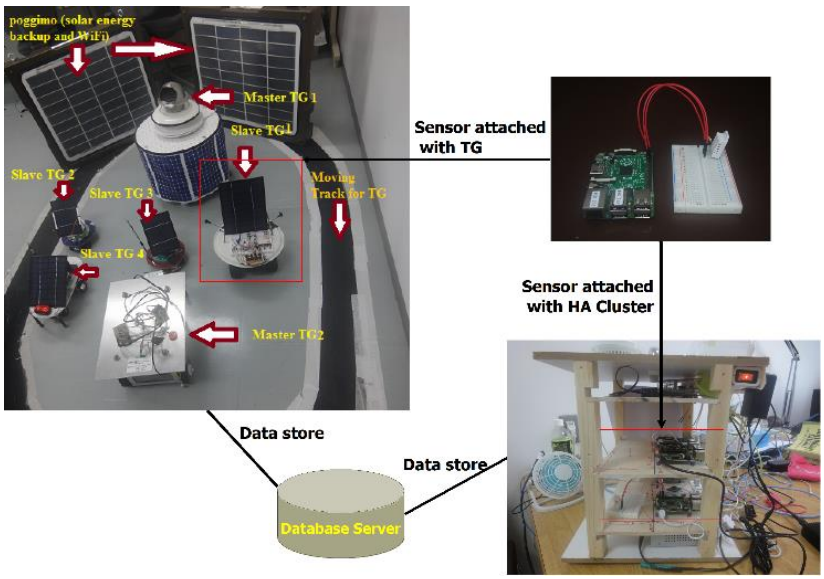


Figure 6-4：Experimental Setup of Hardware

Table 6-1: Specification of Fog Computing Experimental Setup

Name Of Device	DETAILS	QUANITY
Tensai gothalo	Master	2
Tensai gothalo	Slave	4
Cluster	Ha proxy	1
Sensors	Humidity/temperature and other sensors (e.g dht22/dh11)	As per requirement
Power backup system	● Poggimo device ● Solar panel and battery	2
Other network devices	Router/switch	As per requirement

Table 6-2: Details of Jyaguchi Computing Resources

Resources	Details	Remarks
Lookup service	Apache River 2.2.2	For unicast and Multicast lookup service
Service Provider	Jyaguchi Platform	Micro, Macro and Mega Services
Database server	MySQL Database server	Version no: 5.5.43
Web server	Apache	Version No:2.2.22
Language	Java	
Client Interface	Jyaguchi Universal Browser	

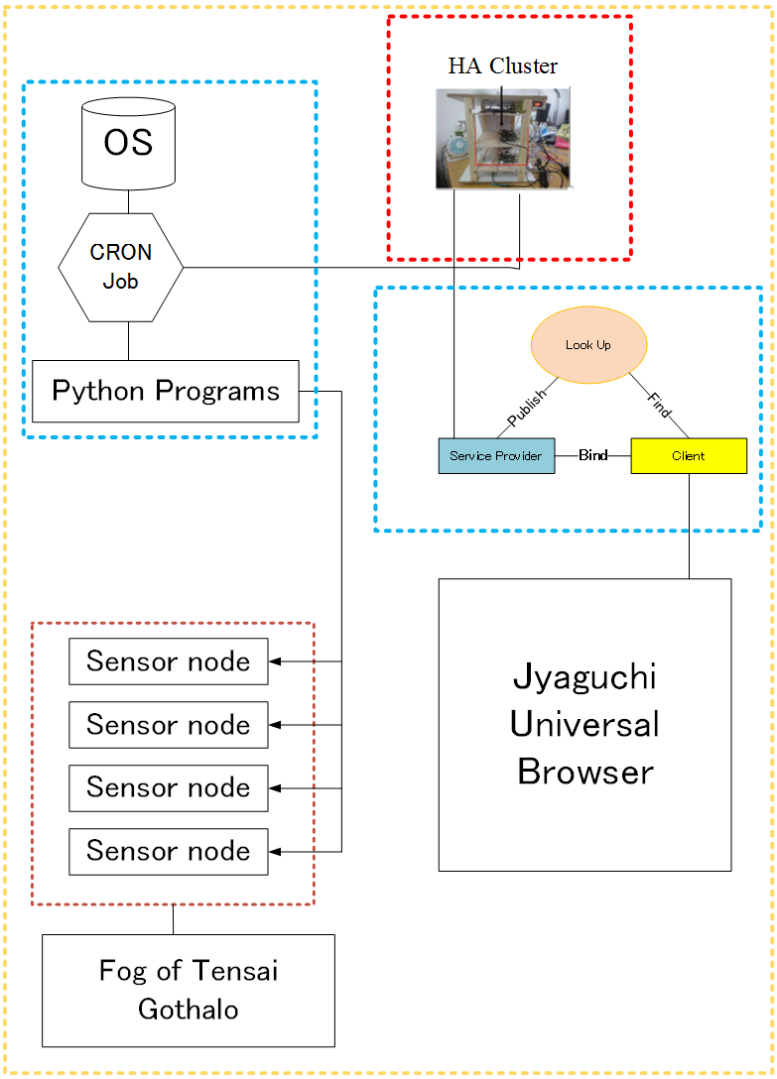


Figure 6-5：Sensor Nodes and Jyaguchi System

Phase 3: In this pahse, the real development of the services is done. Here, we follow the same strategies as in the development of fog services in the Jyaguchi platform:

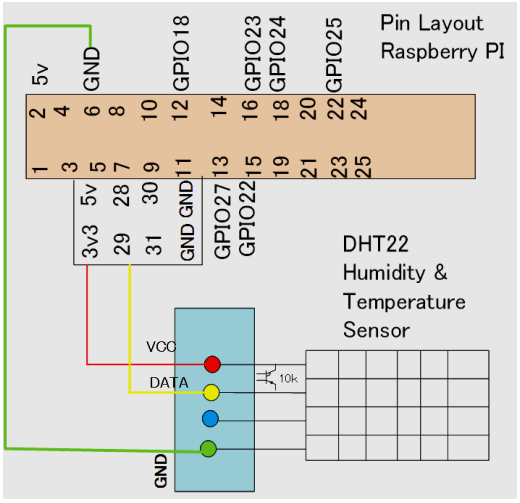


Figure 6-6：Temperature Sensor with Raspberry PI

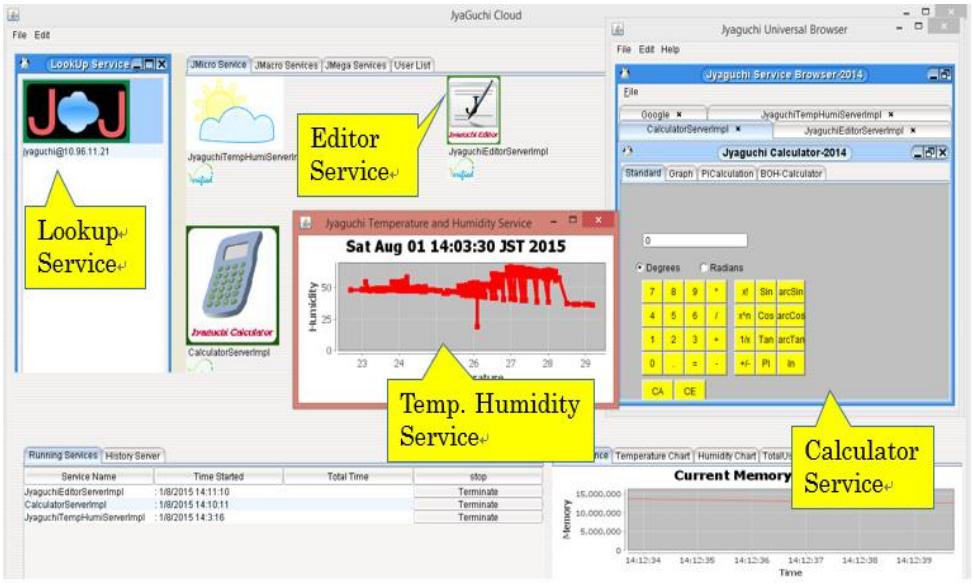


Figure 6-7：Jyaguchi Universal Browser Displaying Services

6.8.1. Temperature Service

This service is implemented in order to measure the temperature of the surrounding environment. We used AYWS DHT22/DH11 sensor, which can be bought at a relatively low cost as compared to other sensors, and can be activated by using 3–5V in order to build this service. While it is easy to install, careful handling is necessary if the surrounding environment is full of chemical vapor as it can hampered the sensor and its calibration to produce accurate data. This sensor is connected with Raspberry PI. Sensor produces digital data which are pruned with python script and the intended data of temperature has been passed to the database server. This data is retrieved and the data is plotted by temperature service. Data are represented by using our temperature service, as shown in Figure 6-7. This service can be downloaded by users.

6.8.2. Humidity Service

Similarly, the data of humidity in the air has been sensed by this sensor and this data is also plotted by Jyaguchi service, as shown in Figure 6-7. As Jyaguchi services are built upon SOA-based architecture, as in [107], [108] users within the fog or cloud can utilize it as and when required.

6.8.3. Migration of Legacy Services

Most of the time, it becomes challenging task to cut over legacy services to targeted services that can adapt new environment. A through study is required to complete migration task. We need to consider the capacity of CPU, memory power, software platform and other dependencies. This task includes varieties of techniques such as reverse engineering, business logic reengineering, schema mapping and translation, data transformation, application maintenance, human computer-interaction and testing. There are few techniques introduced in the literature [109], [110],[111]. However, the convenient method of migration is to wrap the legacy services with new interface that can operate as a proxy module which can fit new environment. Also following the step wise converting approach from legacy to new service is recommended. The limited computing resources as experimented in our test case, may generate certain problems while migrating the legacy services. We have successfully migrated our legacy services, such as calculating service,

editor services and few other services which were previously developed for the cloud computing environment.

6.9. Evaluation and Results

We have developed micro services which were entirely depended upon low level hardware. We also needed to activate sensor and interpreted its sensing data which requires low level language. In order to communicate with the device output, we utilized python script the result of which was inserted in database. These data are re-queried by Jyaguchi services and displayed accordingly. Data are polled in every minute basis as every second will generate un-necessary load for the device. The precisions of humidity and temperature entirely depend upon the quality of sensor hardware.

Our results (see Figure 6-7 for legacy Jyaguchi services) show that the cutover of legacy systems and the development of new services in Tensai Gothalo is possible however certain QoS may suffer if the computing capacity of Tensai Gothalo is not expanded for example by clustering the hardware resources or by using virtualization technology. The research of which is need to be explored further.

6.10. Future Works

We have already built the Jyaguchi fog infrastructure, which can communicate with our sensor nodes some which are carried by our Tensai Gothalo. Future works will emphasize to build upon service dispatcher that can publish the service as per the security requirements of the services. We would also like to implement following services in the future:

- Other geographical environmental data such as barometric pressure, wind speed, rain fall, sun light exposure, GPS value and many others which are important for particular geographical areas.
- A meaningful data analysis services so that each sensor data can be utilized by the users with meaningful interpretations.
- A service dispatcher that can dynamically allocate the service either in the fog or in the cloud

without requiring the interruptions of the service provider.

6.11. Concluding Remarks

We have pointed out some challenges of cloud computing sector which can be addressed by fog computing infrastructure. There are millions of users who are worried about data theft that can be happened in cloud infrastructure. However, in fog computing infrastructure, once the computing premises is domiciled in the end user plane, it is relatively safer. Furthermore, the problem of insider data theft attacks which can be happened more in case of cloud can be lowered in fog computing infrastructure by dynamically generated decoy files. The reason for worry in the field of cloud computing is that the threat of malicious attacks are happening due to a lack of transparency among cloud providers. We have successfully demonstrated the experimental setup of fog computing infrastructure supported by Tensai Gothalo, in which fog services can be built upon. One of the biggest challenges of adopting fog computing infrastructure is that while you cut over legacy system into a new system a targeted new system must be able to retain the functionality and the quality, and the important data of the original legacy system, which were successfully obtained while fogging Jyaguchi in Tensai Gothalo.

Chapter 7. Mega Services in DRN Networks

SOA-based Campus Administration Management System using Multi-layered Architecture: Campus-SIA

In this chapter, we would like to demonstrate a sample of mega service which has been deployed in the office network of Wakkanai Hokusei Gakuen University. We called this service as mega service: Campus-SIA. Our motivation behind implementing this service is that we would like to test whether this sort of mega service can be deployed in HA cluster or not. We would also like to test the performance of this mega service and would present the relevant results.

7.1. Introduction

Administration management in academic front has been realized one of the challenging issues as service provided in the administration has crucial role for the development of student and organization itself. Further, data obtained in the administration requires proper saving and management system which is difficult with traditional monolithic tools. However, we witnessed that saving, managing, reporting and manipulating of data in campus administration are still practiced with monolithic tools due to lack of proper collaborative tools. In this paper, we are highlighting the shortcomings of monolithic tools and proposing the new tool of web based Campus-SIA that we implemented during our research. Furthermore, we purpose the concept of social administrative software that is introduced in Campus-SIA in order to maximize the collaborative management. To support efficient handling of multiple management tasks, we further recommend the concept of social software and the service oriented architecture in order to extend our major business components into a multi-user setting. By architecting the entire system into multi-layered architecture, extensive security and high performance results are achieved and are considered highly efficient and provably secure.

Administration management requires the effective usage of ICT technology not only in business and industrial societies but also in academic front. Several trends in software technologies

are opening up for effective data management and administration management that uses either monolithic desktop based tools or web based system. There is also a trend of using “software as a service” (SaaS) a newly adopted computing architecture, transforming data centers into pools of computing service on a huge scale. This trend of using SaaS in order for data management is still rising in positive scale.

However, in academic front, there are still pools of institutions, colleges and Universities that utilize the traditional desktop based tools and web based tools to capture, analyze and to format the reports required for management and auditing purpose. Storing and managing growing amounts of student data requires administrators to apply intelligent data management tool that helps reduce management costs and to achieve enhanced efficiency and fulfill the effective service for students.

In this paper we will highlight the effective administration management through Campus-SIA (Campus Student Information Application) that we built in this research. Campus-SIA is a web enabled software application that utilized service oriented architecture which leverages the management of student data thereby enabling the administration to enter the academic and financial data related to the student through web browser that ultimately enhances the overall productivity of the administration[112].

The objective of the paper is to describe the effective administration management that can be achieved through the deployment of Campus-SIA in campus administration. We achieve effective management by introducing Campus-SIA in the administration of Wakkanai Hokusei Gakuen University. We describe our practical approach of administration management on the basis of our experience gained through the deployment of Campus-SIA. Further, we will highlight the modules and the architecture adopted during the implementation of Campus-SIA. The major data modules are personal information management, student financial management, student career management and dynamic reporting components as major modules by which campus administration can extract maximum utility in order to enhance the productivity.

Before going into detail of this work, we summarize the major contribution of the work:

1 We presented a component oriented architecture that can be applied for the development

of any campus administration and management system.

2 We demonstrate how to assign roles and responsibilities to academic staff to manage academic and financial data enabling them to be more accountable.

3 We highlight the role of social administration software [112], [113],[114] and its importance to retain the collective knowledge of campus administration for future business process.

4 We successfully tested that mega service as such (Campus-SIA) is possible to deploy in the HA-cluster which we built as a backup data center. Our objective of this test is to present the first large-scale analysis of deploying mega service in a redundant portable data center. Through our analysis, we seek to answer several fundamental questions: what scale of services are possible to deploy? What causes the failures of services in such cluster? What sorts of methods would be effective to provide load balance in the cluster.

7.1.1. Data Management in Campus-SIA

Campus-SIA provides users to enter student specific data with file upload functionality containing image data. The currently supported formats include CSV (Comma Separated Values), different spreadsheet formats (Excel and pdf). To achieve ease Columns of use, the number of steps a user needs to go through before the data is in the systems is reduced remarkably by enabling the system through tab based data entry form. Rather than having the user go entry from form one to next the implemented system provides the tab based entry form automatically and it provides verification of each data entered through the tab based from.

In addition, even though data insertion into the database is done in the background, we try to maintain a responsive import process also. This importing of data is done by the system automatically. Further, the system does not ask the user to specify data types for the entry field provided. Instead, as we describe shortly, it attempts to provide the required data type by pre-defined data set.

7.1.2. Problem Scenario at Campus Administration

Campus administration task should be associated with security aware, responsiveness and well managed task in order to maximize quality of service and the performance of administration that can pave the way for the academic success of each student and also the management of the University. However, these very determining features of effective management are often ignored by administration staff knowingly or unknowingly due to the lack of proper management tools and expertise.

There are numbers of student management system developed and used in software industries which vary in size, scope and capability, from packages that are implemented in relatively small campuses to cover student records alone, to enterprise-wide solutions that aim to cover most aspects of running large multi-campus organizations with significant local responsibility [112]. Many systems can be scaled to different levels of functionality by purchasing add-on modules and can typically be configured by their home institutions to meet their local needs. However, most of the times, the industry standard tools can't meet the specific requirement of the university due to their inflexibility while configuring the system.

We have developed and demonstrated Campus-SIA system, which is dynamic and can be easily customized, based on the size and need of the organization (e.g. departments or divisions or the entire university).

7.2. Motivation and Related Works

We believe that academic success of a student is also associated with the quality of service that the campus administration provides. The purpose of this paper is to provide a prototype for supporting the establishment of effective management-focused campus community so that campus may achieve adequate yearly progress, ensuring that all students achieve adequate services in a timely manner [112].

Campus SIA is a distributed system developed with object oriented development approach. The web enabled system comprised of a centralized database that allows users to handle all daily operations of campus administration includes entering new enrollments, tracking student personal information, tracking and monitoring fee payment, processing student's status (e.g. enter, drop, expelled and other). It allows campus staff to update, share, and use student information among academic staff in a secured manner.

7.2.1. Requirements of Social Administrative Software

We have focused on the introduction of social administrative software concept [112], [114], [115] in order to foster the tacit knowledge that is gained in the administration. From our long past experiences in corporate and academic institutions we can conclude that the accessibility in technology and personal behavior of the staff are the principal characteristics of a public administration that can impact to the nature of society and organization, whereas the tacit knowledge[116] determines the actions and service quality of organization. The knowledge gained during management cycle has a greater role to create explicit knowledge artifacts to be accessible to others in the organization growing process.

Knowledge management cycle determines the quality of service in public administration. In order to socialize these services in terms of knowledge sharing among the staff in the organization, we have decided to incorporate the social characteristics into the software system and try to define this concept. We agree that it is difficult to incorporate all kind of features of social characteristics into the software however we must agree to the point that tacit knowledge of the organization can be lost due to the lack of proper preservation tools.

Thinking insufficiency of this feature, we realize to incorporate the social features in Campus-SIA. Nonetheless, we do not incorporate all of the features of social software rather introduce new features that were lacked in prevailing social software which could depict the concept of optimization of internal administrative processes of campus through a simple, effective and efficient web enabled application at which all staff can work together in collaborative manner[117]. We have seen very positive effect in terms of knowledge sharing and the

administrative businesses process is possible to operate within a friendly environment. This sort of working environment was lacking in previous infrastructure however we regained it by introducing Campus-SIA it and due to of which the staffs are constantly on the move and closely working together.

7.2.2. Desktop Oriented Monolithic Management Tools

As discussed in previous sections, knowledge preservation could not take positive effect in the absence of proper tools. Though, for the past decades or so, ICT technology has revolutionized the way we expect the services in the organization. We cannot ignore the fact that the tools that are being utilized to manage the data in Universities or other organizations are desktop oriented monolithic tools. In academic front, we are working with new generations of students who use more ICT tools and services and who has greater expectations of service quality. For example, this generations use emails, blog, wiki, message board, twitter etc. for communications at which message can be sent to recipients instantaneously. In this way, this layer of users is much more connected and in result we are facing new challenges also. The new challenges in the area of services and communication sectors arisen due to new tools cannot be addressed with traditional monolithic tools. The problem of monolithic tools such as Excels and other desktop oriented tools[114] used in the administration has limitations for effective data management such as organizing, sorting, deleting, and version control. In terms of data management, there are lots of campus staffs who still use Microsoft access; however, these tools have lots of difficulties and the campus staffs were compelled to encounter these difficulties as follows:

1) The prevailing monolithic tools are only accessible to limited number of campus staff and could not update the data at the same time

2) It requires numbers of redundant tasks as per the change of each academic year.

3) These tools are entirely static and are very inflexible due to monolithic design and require IT expertise to upgrade and change with business requirements.

4) It involves large paper work to support key business activity such as enrollment, course adjustments, handling records of finance, student information and other reports.

5) The system does not have relations with other software applications used by the university such as financial management, human resource management and schedule systems.

7.2.3. Related Works

Much research has identified component architecture as a key resource for Student Management System. Campus-SIA complements this work by introducing the configuration and customizable technique which is more users friendly and can be handled with relatively less effort. Campus-SIA is scalable due to its dynamic feature in its architecture. One can add, delete or update number of campuses with this system without modifying the application as it has been architected with easily customizable components. In academic front, we have observed number of campus management system and we found very similar kind of research done at Fiji National University[118].

The management system developed in their research is called FNU-CIS6) which has similar functionalities in terms of security, performance, and accessibility. In commercial front, we have done a case study of Campus-SQUARE12), A2zcampus13) implemented by NS-Solutions and CYBROSYS technologies respectively; however, we found that their research and solutions also did not indicate about the dynamic configuration of the modules such as fee structures and reporting architecture required for documentation in the campus administration. For example, the fee structure of the campus may change in the future academic years; however, due to their static nature of tuition fee structure; those systems are not adaptable for changing structure of the tuition fee.

In contrast, Campus-SIA implemented in our research can support the changing structure of tuition fees and other financial modules as per the configuration thereby provide easily customizable tools for each successive year in order to automate and minimize the administrative tasks.

7.3. SOA-based Management System (Campus-SIA)

In the case of monolithic oriented management system, we highlighted the shortcomings and the lack of co-operative management process characterized by collective management strategy. Collective management process could not be well practiced with monolithic management tools due to its inflexibility and less adaptive feature. Business process of any organization characterized by less adaptive strategy with changing environments has direct or indirect role of monolithic tools. In order to succeed enterprises including academic institutions, the essence of flexible business processes can be taken as key success factor. Flexible business process cannot take substantial pace in the business cycle without flexible business strategy and which is only possible with the applications and the architecture applied in the business process that supports such feature. Often, these business processes are directly coupled with the business strategy adopted in the organization and these processes can smoothly executed if the architecture of applications are built with the concept of service oriented architecture (SoA)[112], [119], [120]. Rainer discusses that SoA based management concept is very well suited to support flexible business processes and application systems because capabilities (in form of services) can be composed in the most efficient way to achieve a high level of agility[121]. However, the management of SoA-founded application systems is often neglected in academic intuitions too.

Thus, we present an SOA based approach that enhances the underlying traditional business process and concept with additional management functionality, e.g. role based management and dynamic reporting system. Campus-SIA supports and execute most parts of a university administrative business processes and the modules mentioned above are architected with SoA concept. Business process flexibility strongly depends on the flexibility of the underlying applications and IT architecture

7.3.1. Overview of Campus Administration Management

Campus-SIA (Campus Student Information Application) is a web enabled software application for the management of student data. It enables the administration to enter the academic and financial data related to the student through web enabled browser that ultimately enhances the

overall productivity of the administration. Productivity has been enhanced due to its feature of collaborative management at which all campus staff can work together which has created better chance to address the given task in the administration efficiently[122].

7.3.2. Role-based User Management

Resources are generally allocated through some application, which enforces access control restrictions by allowing only authorized access[123], [124]. Allocating resources in case of Campus-SIA1) is carried through by settings some real rules[125] or applying the concept of role on the basis of administration policy in the administration. For example, each staff member having certain responsibility in administration can be assigned one or more roles as per the policy of administration. A role determines the nature of tasks the staff can perform in the system and what information he or she can view.

This architecture covers certain tasks and access capabilities associated with the Campus Administrator and Super administration roles. The role assigned to each user is shown in Table 7-1. These roles can be assigned to each user during user creation as per the policy of the administration.

7.3.3. Dynamic Reporting System

Reporting is an important part of document management which determines the overall performance scenario of the institutions. Report documents are necessary not only at the time of creation but also for the future purpose that's why it is equally important to archive well and should be availed.

Table 7-1: User Role

Name of Role	Particulars
Financial Administrator	• View Report • Component Configuration (Financial Section) • Student Account Management
Career Administrator	• Student Career Management • View Report
General Registered User (Manager)	• View Report Only

However, we often see situation in the institution that the generating process of which is not given sufficient attention. In order to increase the end output of the institution it is also important to improve reporting process. We have achieved good reporting output by improving reporting process by introducing the reporting architecture and by making the reporting process more dynamic.

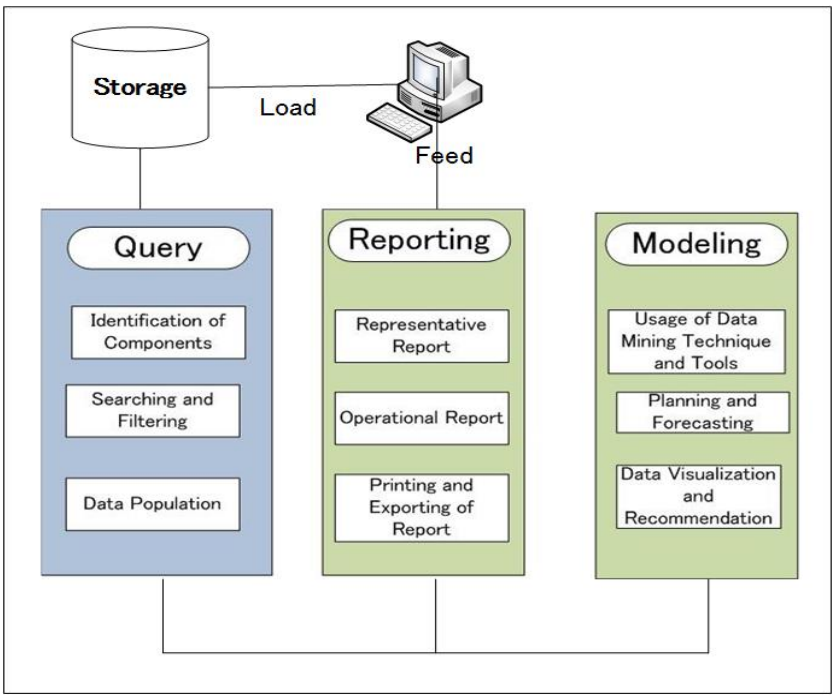


Figure 7-1: Reporting Architecture of Campus-SIA

The Dynamic Reporting system implemented in Campus-SIA allows data to retain in the database through web enabled entry form provided in the interface. The data entered by the administrative staff can be changed as per the requirement and accordingly the reports are generated automatically.

Figure 7-1 shows that layering architecture of Campus-SIA enables you to group the reporting system into two different categories. We have defined these categories as operational group and representative group. Operational groups of reports are the reports at which administrative staffs can work and manipulate their data as daily work. Whereas, representative

reports are the report which has specific format that meets the format of administration. These reports are submitted to the city educational council and the ministry of education, science and technology.

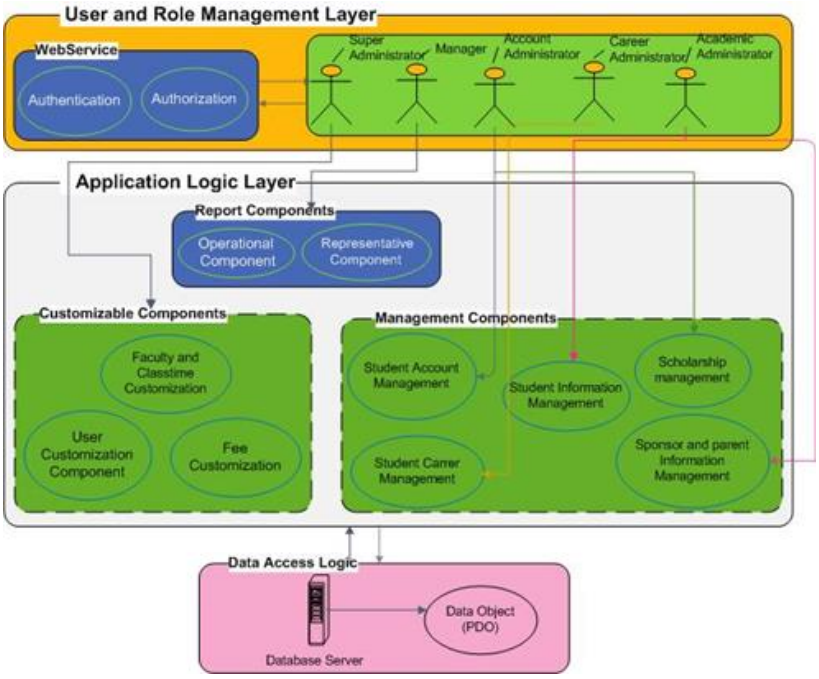


Figure 7-2 : Architecture of Campus-SIA

As shown in Figure 7-2, we have modeled our reporting architecture into 3 different layers such that our reporting process starts from capturing data via query process. We have designed reporting process that starts from query modules followed by reporting modules and finally end up with modeling modules. However in the current architecture we are not able to fully implement modeling part of the architecture

7.3.4. Customization Capability

During the architectural design phase, we have structured Campus-SIA such that it could be reconfigured easily and enhance its capacity to meet the changing structure of organization. As per the needs of the University, Campus-SIA can be customized and configured. All of its components are capable of resizing and reconfiguring in order to re-structure, which gives any

institutions flexibility to make changes and add options to meet their specific needs. For example, university may increase or decrease its campus, faculty or department; in such case the administrator of this system can easily customize the system to Campus-SIA thereby providing a highly customizable and flexible platform, where one can tailor everything from data entry screens to reports generation.

7.4. Multi-layered Architecture Design

This paper proposes a multi-layered architecture with three fundamental layers. We have categorized those fundamental layers as user interface layer, business logic layer and data base layer.

The first layer can propagate user interface with multiple sets of data entry form followed by configurations thereby providing data entry functionalities that is posted to database layer. Accordingly, this layer is enhanced with the functionalities by which user can view different kinds of reports. This layer is implemented using HTML and PHP. The dynamicity on usability of the user interface is added using JQuery and AJAX Technology. The user interface is totally managed from the user role management which means the interface will be changed dynamically according to the role of the logged in user. For example, the user management interface is only displayed for the super administrator, student account management and scholarship management interface will only be displayed for Account Administrator and so on.

The other layer is consists of database servers. The major work of this layer is to store the data captured at user interface layer and also stores the data manipulated by application logic. We have designed the database so as to keep data neutral and independent from application servers or business logic. Providing data base layer as separate entity also improves scalability and performance.

The key layer of Campus-SIA is application logic layer which implements the main business logic of the entire system. This layer takes input from user interface layer and stores information in the database layer according to applied business logic. The input data are logically

separated according to the business logic which has divided whole Application Logic Layers into 3 major components. Various components are used to customize the business logic itself. The faculty and class time customization, user customization and fee customization is used to configure the parameter of business logic. Each management components are dedicated to their respective tasks and responsibility. Report Components are the output for the User Interface layer generating the report by joining the datasets from different table to make data analysis task more easy and effective.

7.4.1. System Architecture and Use Case

In order to develop the system properly, we must agree with the requirement document. We had done number of discussion to analyze requirement document with the administration. Accordingly, we discussed about the access policy as one of the motivation of our research was to implement access control policies which can adapt rapidly in order to follow organizational needs. Such requirements demand skilled policy administrators, who are able to change policies to support ad-hoc collaborations, while ensuring that the policies full fill their fundamental purpose, for example they can control authorized and unauthorized access.

After analyzing access policy that meet the requirement, we architected the system and the part of it that reflects role based resource allocation is depicted in the use case diagram in Figure 7-3.

7.4.2. The Fully Web Enabled Model

In the case of campus administration of Wakkanai Hokusei Gakuen University, there are still numbers of offices at which, the job of an administrator is seen as monolithic: to perform a collection of tasks that are, with few exceptions, carried out alone. And the status of tasks are obscured from their colleagues. In most colleges and universities, this kind of repetitive and monolithic approach can be labor-intensive and cost ineffective, thus needs to be transferred with web enabled application that is more transparent [112]. Individual administrative member can work with this web enabled Campus-SIA and deliver multiple works, each of which can be assisted and

monitored by other colleagues. This type of web-based applications can be used largely as supplemental resources for administrative efficiency and productivity.

7.4.3. Transparency of Workflow

Campus-SIA provides accountability at all levels thus data entered in the system will be

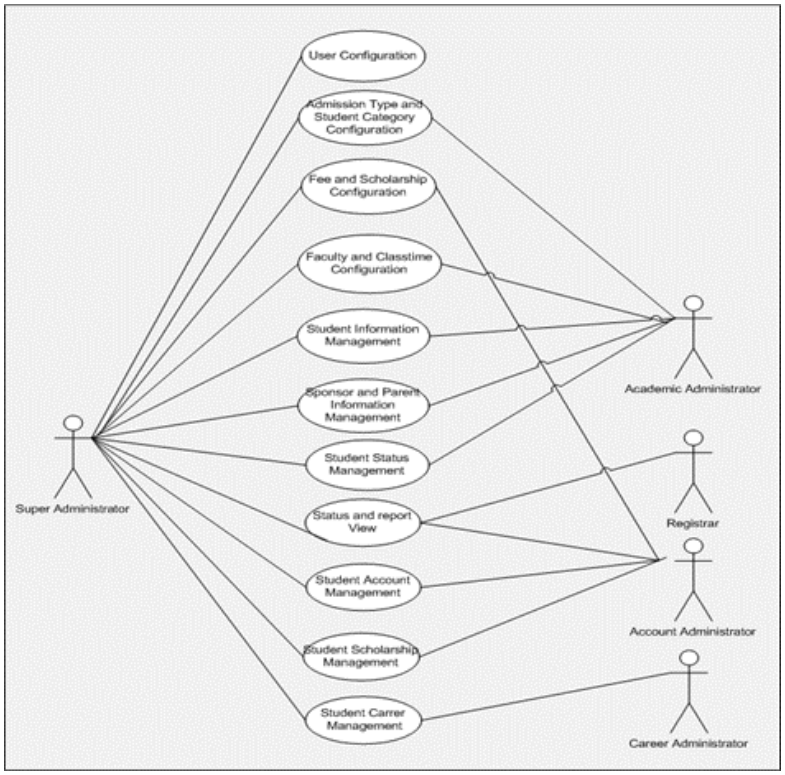


Figure 7-3 : Use Case

opened by the top level management. It makes all staff accountable towards the data and thus, the management can have a closer look on the activities of the campus.

Campus-SIA has been built in such a way that it can automate redundant tasks and ensures that uncompleted tasks are followed up and their status are updated to all staff that have privileges to monitor, modify or update the tasks. The system reflects the steps required for the completion of each task and produces report of corresponding task that has been completed. We emphasizes in creation of report for each business process as it is one of the troublesome for campus staff who

need to produce the report in timely manner and requires much effort. Unless documentation and report creation is performed properly, both systems and administrative processes will become a black box somewhere in the workflow. Campus-SIA is capable of generating reports automatically, which enables the transparency – a vital feature for an efficient workflow

7.5. Implementation and Practical Usage

In this section we briefly introduce about our experience of deployment and practical usage of Campus-SIA in the administration of University. Nowadays, not only the business of enterprises and industries but also the business process of Universities relies on networked computer systems to support distributed applications. To plan for the required level of management, two basic areas must be considered to address the data management of University. One of which is the security and the other is number of potential users and scalability. Accordingly, we need to plan the hardware specification and network topology. The servers that we need to plan in the case of Campus-SIA are data base server, web server, and authentication servers. In our case, we separated our servers from our main data center and design a small network nearby the administration. The picture of datacenter is provided at the Figure 7-4 which is separated from the LAN at which Campus-SIA resides.

Figure 7-4: Data Center of Wakanai Hokusei Gakuen University

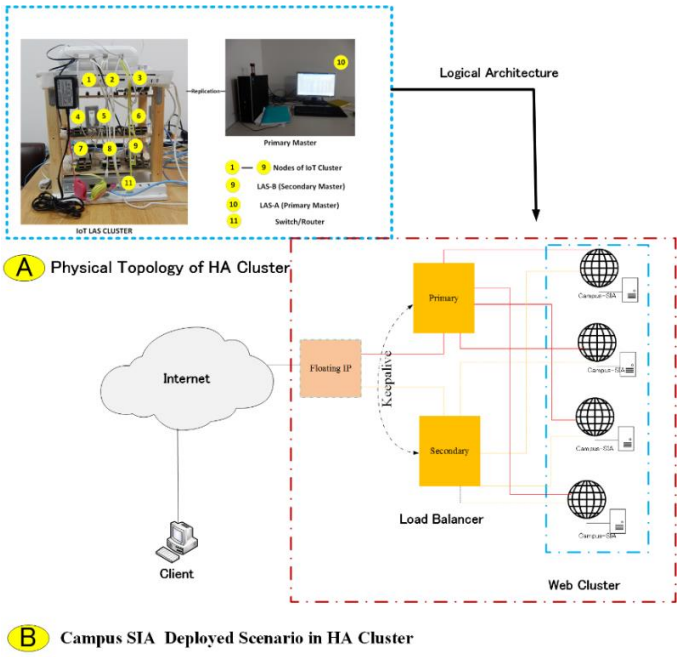


Figure 7-5: Campus-SIA in HA-Cluster

This separation of network from our datacenter adds up extra security layer as our firewall and natbox resides in the main data center and the campus-SIA in separate LAN. In this practical scenario we have virtually and physically separated campus-SIA and make it more securely located inside the administration. We have tested Campus-SIA in 2 ways. At first, we have separated data base server, authentication server and apache web servers. We can replicate each server to increase the availability. However, allocating different servers as shown in Figure 7-8 for different purposes depend on the numbers of users and the scale of administration.

Considering the fact of WAKHOK administration, we centralized each server and design the simple network as shown in Figure 7-6.

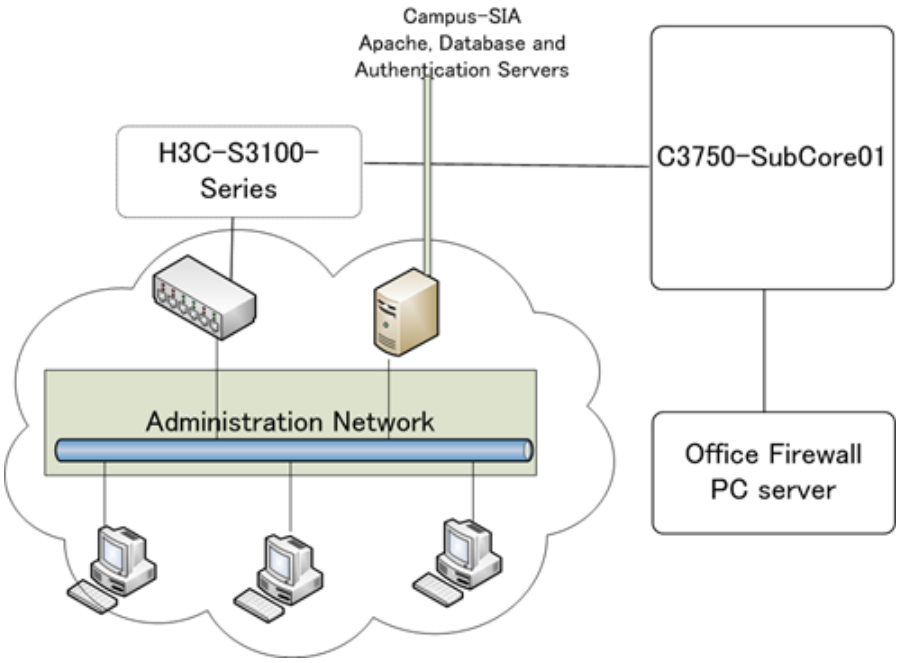


Figure 7-6: Network Scenario

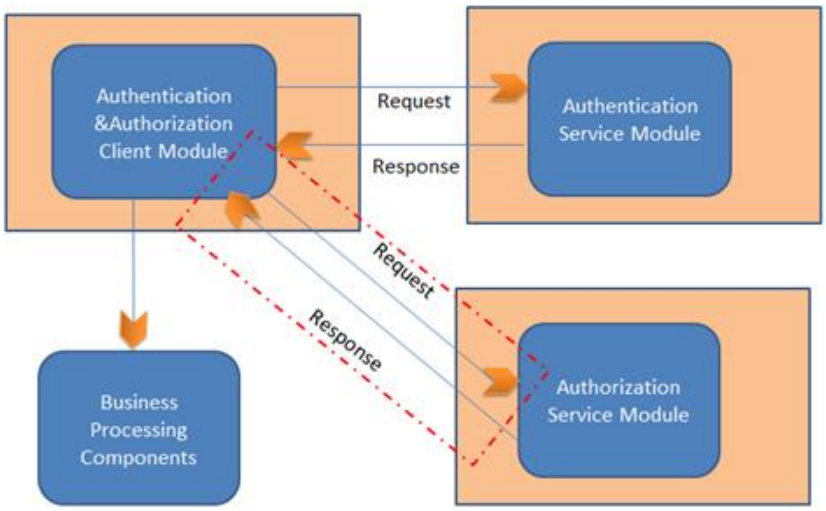


Figure 7-7 : Authentication Scenario

Campus-SIA is architected with SOA based concept. Though we tried to implement all components to be supported with Service Oriented Architecture, we were unable to support all the components with service oriented feature. However, we completely implemented our user authentication and authorization module in SOA based concept as shown in the Figure 7-7.

As shown in Figure 7-7, in order to authenticate, the client program sends the request to the server program having authentication parameters. In the case of authentication service, we pass the object of Authentication class as parameter to the JSONRPC Server. This server checks the status of user whether it is created in the database server of Campus-SIA or not. Once, it finds its existence, the server return the id of that user thereby providing login functionality. The snapshot of code is given below:

```
$auth = new Authentication();

jsonRPCServer::handle($auth)
    or print 'no request';
```

In the very similar way, we can use the service of authorization too. The snapshot is given below:

```
$auth = new Users();

jsonRPCServer::handle($auth)
    or print 'no request';
```

At this time, we have created the object of Users class and which is set as parameters in the jsonRPCServer thereby requesting the authorization to the sent users. In this way, we can objectify most of the components into server modules and reduce the client side codes which are inevitable in service oriented architecture. Further, the architecture of Campus-SIA is featured by the modular type of software architecture along with separating presentation logic, web logic, business logic and data logic as desired by the users.

7.5.1. Case Study of Wakkanai Hokusei Gakuen University

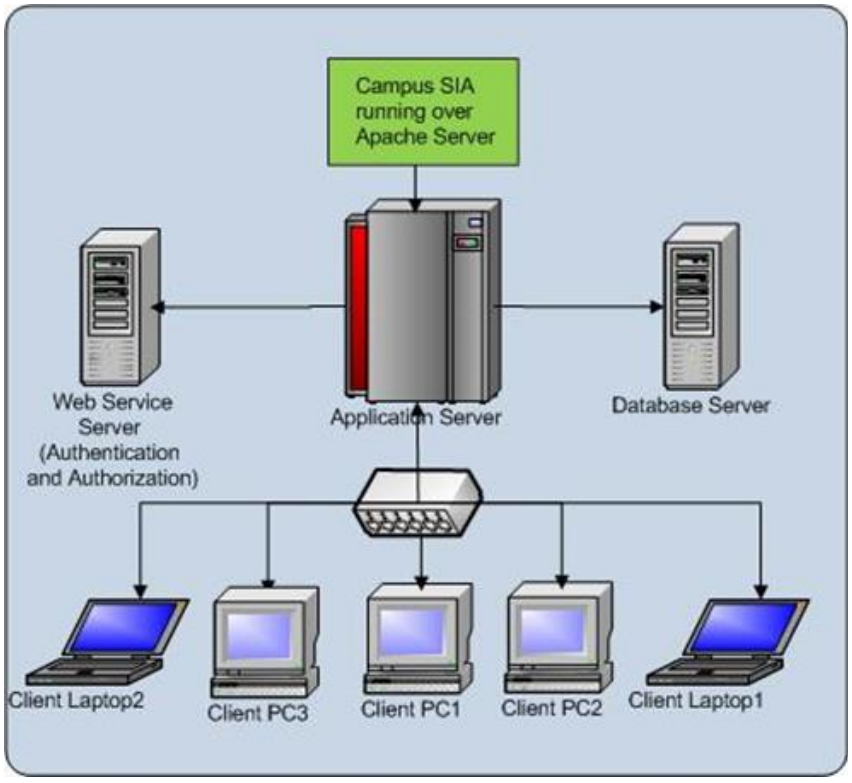


Figure 7-8：Distribution of Servers

Wakkanai Hokusei Gakuen University was established in 1987 and having only one post-secondary institution in Wakkanai city. It is a semi-public institution, and has a great contribution to promote research and academic excellence for the welfare and needs of the communities in Soya area of Hokkaido as well as communities in the region and abroad. In order to promote its ICT infrastructure the administration has decided to re-evaluate its administration management system and this research is believed to improve its overall performance after successful implementation.

From the academic year of 2012 we have introduced Campus-SIA in the administration of Wakkanai Hokusei Gakuen University. Traditionally, the administration of Wakkanai Hokusei Gakuen University used to save information data in monolithic desktop based system which has lots of limitations and lack the functionalities of co-operative management. Further, the

administration has faced number of bottlenecks regarding data management among the departments and sections of the University.

They have 4 sections which has direct relation with services and management of student: student support section, student career support section, maintenance section and financial section. Before introduction of Campus-SIA, these sections were working independently and numbers of redundant tasks were carried out due to lack of proper tools and software. For example, whenever there is any change in personal data of the student, each section used to enter the same data into their monolithic tool. This sort of working style due to the lack of integrated tool, obviously hamper the entire performance and business flow. These tools have also no relation with the other tools introduced in the administration.

7.5.2. Performance Enhancement of the Administration

The traditional administrative tools utilized in the administration for managing student records, including student financial records and other information system, has become bottle neck for the total performance of any college or university. We have witnessed such changes in campus working culture, especially due to the wide usage of Internet; have raised student expectations for the services provided by technology. However, there are still few colleges and universities who still utilize those traditional tools characterized by monolithic approach which cannot meet desired quality of services as expected by the students.

As a result, those colleges and universities are vulnerable and may lose trust from their own students. This will obviously affect future student enrollment.. Information management system such as Campus-SIA can become an important management tool that builds trust among students through delivering services effectively and efficiently on a timely manner. One of the goals of development of Campus-SIA was to maximize overall performance of campus administration.

Before deciding the development of Campus-SIA, we benchmarked the current performance of the administration on the basis of the tools and the system they currently used. Our preliminary assessment suggested that the existing system was inadequate and inefficient to provide

necessary outputs and there is a need to develop a flexible, efficient and robust system to enhance productivity of administrative staffs. The key decision factor of this case study was to understand performance management from perspectives of different parameters and develop a framework that meets all the objectives of performance enhancement. In order to meet this goal, we developed Campus-SIA so as to enable the administration to understand all steps required in performance enhancement and examine shortcomings on each stage. The facility of providing common interface to each individual at which all members of the administration can work in the application simultaneously maximizes their performance and productivity.

7.5.3. Lesson Learned

On the basis of our experience of development and launching of Campus-SIA at WAKHOK University in responding to the effective campus management that have been achieved over times, there are several lessons learned that can be shared with other academic institutions and organizations in their planning, deployment and response to similar situations. We have identified these lessons and practices which span several domains: administration, infrastructure, development, and architecture. We do not want to ignore the consideration of infrastructure, development and architecture, however, among of these, we would like to focus our most considerable lessons which are more of administration or management oriented. The reason of choosing this consideration is that the management of the University will measure the success or failure of project or practical research as per adherence of the project to its end-to-end project timelines as well as by the stability and performance of the application rather than by the elegance of the internal composite and attractive UML design of the system. In order to complete the research within given time frame, we have realized to give sufficient priority under this category and which are highlighted as below:

- First, requirement analysis should be done with all concerned staffs who are potential users of the system. These staffs might have good knowledge of the process execution in the campus administration. This knowledge should be reflected during requirement analysis so as to protect the system having broken features from the initial phase.
- Second, institutions and organizations seeking to change management system by consolidating with similar management tool need to factor in the time and effort of the office staff who will

be involved to test, review, advice, and revise the business process. This preliminary testing process will examine whether the executed process reveal expected business flow or not. Accordingly, it will affect entire development decision.

- Third, development team needs to investigate and evaluate the available tools such as programming language, database system and development framework. We agree that we should have utilized distributed database in order to increase the system availability from the beginning though the current system can be extended with NoSQL database in the future.
- Fourth, adequate considerations should be given to the new, emerging open source management tools and products in order to reduce the development time and other associated costs. We have developed each module from the scratch.

7.6. System Evaluation and Service Deployment Test in HA Cluster

In this section, we present the system evaluation of this mega service hosting in different kind of environment. First of all, we would present the performance metrics in normal computing resources of Wakkanai Hokusei Gakuen University and then we would also conduct a system evaluation on the basis of HA cluster. We assume that performance would be one of the major decision factor for the adoption of HA cluster during disaster. To gain insight into the performance provided by HA cluster that we developed, a proper measurements of system performance and metrics are needed. Though, we could find various benchmarks and metrics that focus on cloud environments, such benchmarks are usually focused on only to the specific aspects of cloud services and thus not feasible to test the system performance of Campus-SIA. Thus, our focus of system evaluation is bounded to compare the performance between actual running environment and in the HA cluster that we proposed in this dissertation.

7.6.1. Basic Idea and Experimental Setup

Our idea of performance evaluation is based upon benchmarking technique. It has been often criticized about benchmarking that it should be used as a tool for gauge and not a precise tool. Therefore, we need to understand what we are going to measure first. In our measurement, we

would like to measure transaction rate in terms of time and would like to figure out actual performance. In order to keep our method free from biased benchmarking, we separate the behaviours of application from underlying platform. First of all, we would test the behaviours in two different computing environments, then we will measure the performance based on the HA cluster that we built. The resulting metrics reflects the expected behavior of the application on provided platform.

Table 7-2: Specification of Experimented Machines

Specification	Tester machine	Target Machine
OS	Windows 8.1	Windows 7
RAM	4.0 GB	4.00GB
CPU	i5-:4200U	Pentium-Dual-Core 2.5Ghz×2

7.6.2. Performance and Capacity Testing

We suggest that one must take into account of whole system such as CPU, memory, storage, operating system and many others as per the tool applied for benchmarking. Therefore, we have provided specification of tested target machine and the tester machine in Table 7-2. In order to project the metrics gained through benchmarking method is a fair reflection of the system, one need

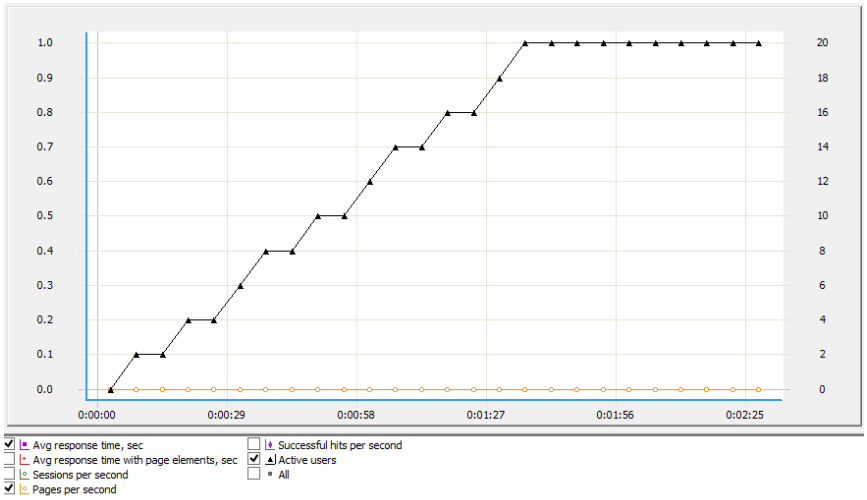


Figure 7-9: Performance Testing of Campus-SIA

to provide the detail experimented result. For this case, we tested various simulation scenario and the average output is indicated in Figure 7-9.

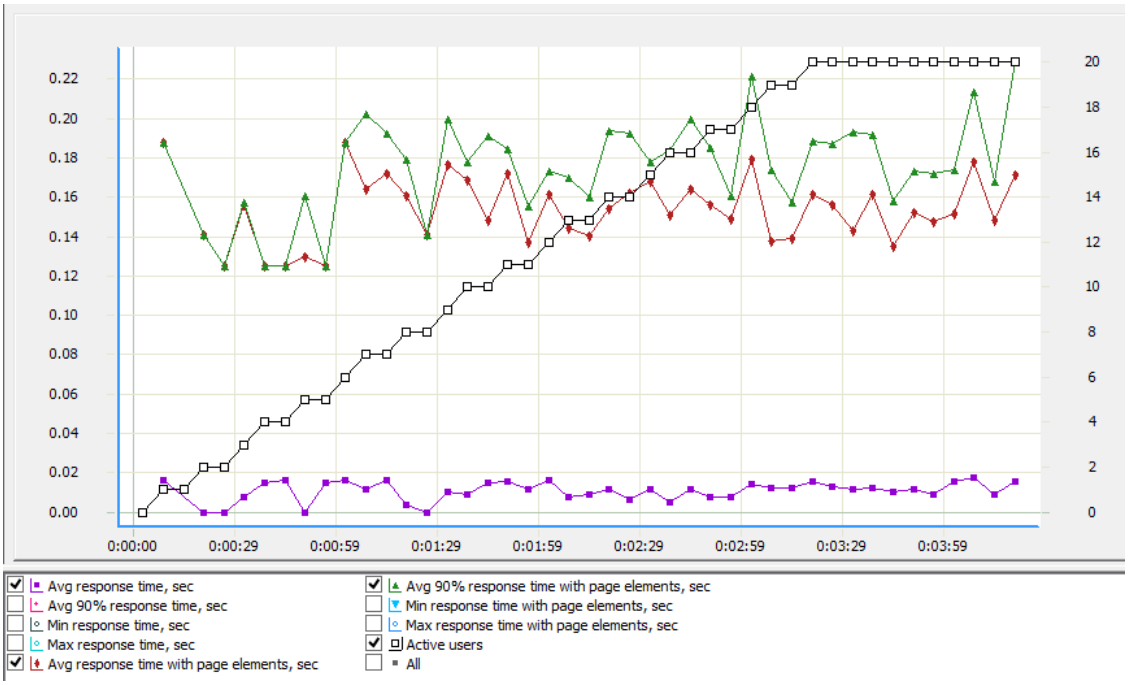


Figure 7-10: Timing Graph with Average Response Time having page element

From this test, we conclude that Campus-SIA can provide quality of service with a limited load. We assume that the load at deployed environment does not exceed 20 users concurrently. Therefore we set the testing profile accordingly. As shown in the Figure 7-10, when the number of users simultaneously working with the site goes beyond 8, average response time starts to grow proportionally. However, it never cross 0.02 seconds until the con-current users are 20.

Furthermore, load testing was conducted by using different scenario by using Neoload as shown in Table 7-3. We did not find any substantial differences between our experimented results and thus we concluded that while there are concurrent users until 20, it will response without having much difficulties.

Table 7-3:Comparision of Testing Scenario

Particulars	Scenario 1	Scenario 2	Comparison value
Average pages/s	0.7	0.7	+0%
Average requests/s	1.2	1.2	+0%
Total pages	89	89	+0%
Total requests	145	145	+0%
Average Request response time	0.09 s	0.092 s	+2.2%
Total request errors	28	28	+0%
Error rate	19.3	19.3	+0%
Average Page response time	0.147 s	0.15 s	+2%
Total throughput	1.01 MB	1.0 MB	-1%
Average throughput	0.07 Mb/s	0.07 Mb/s	+0%
Total users launched	5	5	+0%
Total iterations completed	33	33	+0%
Total action errors	0	0	+0%
Alerts total duration	0 %	0 %	+0%

7.6.3. Service Deployment in HA cluster

One of the major feature of DRN network is to provide a service even in a disastrous situation without compromising the quality of service. To retain this kind of high level feature is a challenging task. In order to sustain this level of quality, we experimented whether some critical services of any organization with large scale can be deployed in our portable HA cluster or not.

Figure 7-5 shows both of the physical and logical scenario of our HA cluster. We have implemented the design presented in this paper, by using HA proxy for load balance. A key feature of this implementation is that it has considered never die feature, in the sense that it has multiple nodes of Campus-SIA which are load balanced through HA proxy. These multiple nodes can provide the services regardless of any node failures inside the cluster. We deployed Campus-SIA, a mega service already in operation at Wakkanai Hokusei Gakuen University, in our HA cluster and tested the load balance scenario. Figure 7-11 and Figure 7-12 shows the screenshots taken during the experiment. As shown in the figure, both pages were accessed via floating IP assigned to our load balancer. In fact, as HTTP is a stateless protocol, each request of the page are regarded as separate transaction. This feature has no problem with the sites where login sessions are not used, however, this has troubled us because our load balancer forwarded each request to different servers. Forwarding the request to different servers without keeping its state will result in losing the login information and thus we were unable to achieve the expected result. To solve this issue, we tweak the settings of load balancer so that it can send the traffic to the same server while there is login session. Finally, this has been achieved. Our major concern of this experiment was to test whether the Mega services (for instance, Campus-SIA and Moodle) can be resumed after the disaster from our HA cluster or not. We observed that our HA cluster can successfully host Campus-SIA.

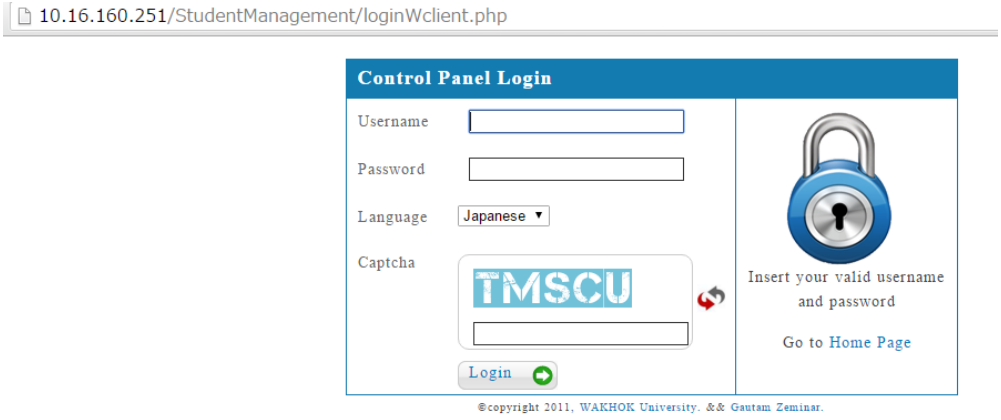


Figure 7-11: Login Panel of Campus-SIA

Figure 7-12: Front End of Campus-SIA Deployed in HA-Cluster

7.7. Conclusion

We conclude that desktop based monolithic tools are lacking the social relation building and knowledge exchange within organizational communities. Further these tools are lacking dynamic features. Even simple changes of business processes demand a tremendous customizing effort and thus hinder the entire performance of the academic institutions. Furthermore, our experience shows that Campus-SIA can be deployed in our portable HA-cluster. This experiment also suggest that it is possible to set up DRN services for any kind of organization if such organization carefully allocate the budget for their infrastructure.

The feature of knowledge sharing through socially aware tools has more capacity to adapt with changing environments and changing business strategies. This feature of adaptation is enhanced with SoA based architecture that we implemented in Campus-SIA. However, we faced with the condition at which some of its components are not capable of supporting SoA and these modules have broken features of SoA.

In the future, we will try to fix the broken architectures of Campus-SIA and make it fully SoA enabled. In order to internationalized University or campuses, administration and academic staffs must be ready to face with the challenging and changing environment. A crucial competitive factor to adapt with such changing environment is the ability to react quickly, flexibly, and efficiently by adapting the management strategy and business that meets new conditions and new expectations. These management strategies should be reflected in the tools and which are more achievable with flexible architectures as adopted in Campus-SIA which has supporting features to adapt with changing business process. The design we have presented in this paper can be extended in several ways, for example, it can be deployed in limited resources as shown in our HA-cluster. Though we implemented each node without using any replication methods, in our future work, we would plan to engineer a system that combines the important features from both designs including replication of each node in the cluster.

Chapter 8. Conclusion and Future Directions

Natural disaster occurred in the course of history and normally left us with a number of challenges and difficulties. From those incidences, we learned that there is an urgent need to develop novel monitoring and management framework system that considers a DRN networks for the large organization, universities, schools or government agencies. For example, we experienced the Great East Japan Earthquake in 2011, which caused many casualties and recovery process of communication networks took substantial amount of time. Disaster rescue process cannot be quicker without having proper communication networks. These networks can be made disaster ready with number of efforts. In this dissertation, we presented a guideline and few recommendations on the basis of which we can build up disaster ready networks. Furthermore, we have also presented a prototype device that can monitor basic network troubles and also can trouble shoot basic networking troubles. We know that during disaster, network disconnection greatly delayed the rescue work, and thus the purpose of this research project is to provide a complete and practical framework while designing a Disaster Ready Networks such that any organization can sustain the disaster that can be happened in future. To accomplish this objective, a detailed literature review with needful survey, simulation, design and implementation of the prototypes were carried out.

We concluded that there are various regions around the world where the networks are not stable. Specifically, the networks of Himalayan regions and Soya regions of Hokkaido are two significant areas where our study was held. These networks are qualified as unstable networks. In order to make those networks more stable, our approach of DRN could increase disaster preparedness of the local government. This dissertation demonstrated on how to design complete disaster ready networks, and how to provide systematic support to manage and monitor such networks. Specifically, we developed a novel network monitoring and management device called Tensai Gothal. We also surveyed and studied the general properties of unstable networks and its bottleneck. Insight into unstable networks and bottleneck properties helped us solve the problem of disaster preparedness for the regions of Himalaya and Soya regions. We also proposed a monitoring and diagnostic platform that supports all the monitoring and management operations.

In this chapter, we summarize our contribution of this dissertation, and then discussed future work that can build on the results of this dissertation.

8.1. Summary of Contribution

The main contributions of this work lies in three aspects. The first is an identifying the properties of unstable networks of Himalayan regions and Soya regions. The second is introducing monitoring and management framework as a novel network monitoring approach, i.e., monitoring and management of network by using Tensai Gothalo. The third is an analysis and proper classification of network-services that can be deployed in portable HA cluster. These are further listed as below:

8.1.1. Survey and Analysis of Unstable Networks

We conducted field survey and analyzed unstable networks. There were many similarities between the networks of Himalayan region and Soya regions. Though geographically in different locations, the characteristic of networks are similar in these two locations due to their extreme climatic conditions. We proposed and simulated a redundant network considering redundancy in each layer of TCP/IP.

8.1.2. Development of a Novel Monitoring and Management Device

A novel monitoring and management device was developed and tested its functionality to trouble shoot basic networking troubles without requiring human interference. This would increase self-healing capacity of network where the network administrators are lacking. Furthermore it increase the fault tolerance after the disaster.

8.1.3. Simulation of Services in Portable HA cluster

We modeled a portable HA cluster and deployed the services in order to analyze which kinds of services are possible to deploy during disastrous situations. We demonstrate a model of

HA cluster which should be arranged on each organizations for emergency propose. This kind of backup arrangement will definitely increase the disaster readiness of the organization.

8.1.4. Multi-master replication for Disaster Readiness

We proposed a replication model that incorporate multi-master replication such that sincere database can be located in different geographic locations yet to have persistent and consistent database. Our method of hybridizing replicating algorithm with Galera cluster increased survivability, reliability and fault tolerance of the application.

8.1.5. Mega Service (Campus-SIA) in Operation

The other notable contribution is Campus SIA. It is one of the system (Campus-SIA described in Chapter 7) presented in this dissertation which has been delivered to Wakkanai Hokusei Gakuen University, Faculty of Integrated Media and has begun operation since 2014. We observed its performance, evaluated the system and recommended the improvement of the system by incorporating the result to the entire monitoring and management framework for the rest of the communities in the future.

8.2. Future Directions

There are few additional things that can leverage on the results of this dissertation which are discussed below:

8.2.1. Improving the current systems

In a current system, monitoring device can act after getting sensing information from master node. These monitoring of physical properties (such as power outage etc) are conducted by the usage of sensors that means it does not need to rely upon any calculated information. This feature has some advantages because it does not require computing resources. However, this becomes dis-advantage too. For example, while the node require integration between sensing

information and the information of other monitoring tools such as Nagios, MRTG etc, a powerful computing resource is necessary. In such a case, we need to supply application that can integrate sensing information and third parties monitoring tools. We recommend that a monitoring application should further be enhanced so that these information can be helpful to the administrator. For example, when a trouble occurs in the node being monitored, the trouble shoot node (Slave node) is notified via the monitoring node (Master node) of the fault information. Slave node can proceed to the location of fault node however if a variety of information can be displayed while a network administrator click the message including display of the location of fault occurrence would further sooth the trouble shooting process. The other benefits for visualization is that from receiving fault location as displayed in the screen, administrator also can locate the place of device, name of the device and name of the services, then he/she can immediately proceed and investigate for further trouble shoot in case the movable trouble shoot could not be solved properly.

8.2.2. Improving Obstacle Avoidance Unit

In a current obstacle avoidance functionalities, we emphasized to use IR sensor due to cost effectiveness. However, entirely relying upon IR sensor may need to compromise the quality and performance of the monitoring device. Thus, we recommend to apply integrated sensor between IR, ultra-sonic sensor and vision sensors. Though, position of node is not important for Tensai Gothalo, it might be useful for administrator, therefore, a GPS to track the position of monitoring node and trouble node should be implemented.

8.3. Closing Remarks

Management and monitoring framework with innovative network monitoring device has been demonstrated in this dissertation as a novel solvable approach in the field of disaster management of networks. Path tracking and obstacle avoidance with IR sensor mechanism has also been discussed. Furthermore, various techniques for example providing a backup link at physical layer and network layer, database replication in application layer have been implemented and described. Similarly, it also described the methodology by which a portable HA cluster on which

extremely important data and application can be deployed. These techniques are crucial to enhance the unstable nature of computer networks thereby making them disaster ready. However, these kinds of precautions and arrangement are not widely used or integrated yet in a co-related method. One reason is that most of the previous works are centered with post disaster measures. Providing a disaster recovery schemes seems to be already a good measure to work with disaster management. The second reason is that, as our survey shows, most of the organizations, including companies, schools or universities are still dominated with broad band links of fiber optics except in Himalaya regions. Their assumption is that secondary and redundant links is not required as fiber optics is one of the robust networking infrastructure. These assumptions prevail to the impression that further enhancement of network infrastructure is not important. However, this line of thought will have big shift in the near future due to re-occurrence of large scale of natural disaster as happened in Japan and Nepal. We will see more and more organizations will prepare to integrate our techniques to obtain disaster readiness of their underlying network infrastructure and to improve their adaptability to challenging situations. For the same reason, I believe that the techniques presented in this dissertation to monitor and manage the networks have foreseen a bright future. And at last, without making our communication disaster ready, human civilization will not be able to protect our intellectual property. I believe that this dissertation have made substantial contribution to shed light in this discipline

REFERENCES

[1] C. Guo, H. Wu, K. Tan, L. Shi, Y. Zhang, and S. Lu, "DCell: A Scalable and Fault-Tolerant Network Structure for Data Centers," *Proc. ACM SIGCOMM 2008 Conf. Data Commun. - SIGCOMM '08*, pp. 75–86, 2008.

[2] V. Liu, D. Halperin, A. Krishnamurthy, and T. Anderson, "F10: A fault-tolerant engineered network," *NSDI'13 Proc. 10th USENIX Conf. Networked Syst. Des. Implement.*, pp. 399–412, 2013.

[3] H. Miyajima, "Fault tolerant server," *US Pat. App. 14/204,567*, pp. 1–15, 2014.

[4] W. Szpankowski, D. Marinsecu, and V. J. Rego, "Stability Problems in Local Area Networks : A Qualitative Approach," 1985.

[5] X. Li, P. Wan, Y. Wang, and C. Yi, "Fault Tolerant Deployment and Topology Control in Wireless Ad Hoc Networks," pp. 1–24, 2003.

[6] P. LeMahieu, V. Bohossian, and J. Bruck, "Fault-tolerant switched local area networks," *Proc. First Merged Int. Parallel Process. Symp. Symp. Parallel Distrib. Process.*, no. iii, pp. 747–751, 1998.

[7] E. Jones and P. Ward, "Routing strategies for delay-tolerant networks," *ACM Comput. Commun. Rev.*, 2006.

[8] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H. Weiss, "Delay-tolerant networking: an approach to interplanetary internet," *Commun. Mag. IEEE*, vol. 41, no. 6, pp. 128–136, 2003.

[9] K. Fall, "A delay-tolerant network architecture for challenged internets," *Proc. 2003 Conf. Appl. Technol. Archit. Protoc. Comput. Commun. - SIGCOMM '03*, p. 27, 2003.

[10] H. Ntareme and M. Zennaro, “Delay Tolerant Network on smartphones : Applications for communication challenged areas,” *Proc. 3rd Extrem. Conf. Commun. Amaz. Exped.*, pp. 14:1–14:6, 2011.

[11] S. Jain, K. Fall, and R. Patra, “Routing in a delay tolerant network,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 4, p. 145, 2004.

[12] F. Warthman, “Networks (DTNs),” *Delay-and Disruption-Tolerant Netw.*, vol. 2.0, 2012.

[13] V. Mahendran, S. K. Anirudh, and C. S. R. Murthy, “A realistic framework for delay-tolerant network routing in open terrains with continuous churn,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6522 LNCS, pp. 407–417, 2011.

[14] M. Demmer, “A Delay Tolerant Networking and System Architecture for Developing Regions,” University of California, Berkeley, 2008.

[15] A. P. Guimaraes, H. M. N. Oliveira, R. Barros, and P. R. M. Maciel, “Availability analysis of redundant computer networks: A strategy based on reliability importance,” *Commun. Softw. Networks (ICCSN), 2011 IEEE 3rd Int. Conf.*, pp. 328–332, 2011.

[16] A. T. Document, “Arista Universal Cloud Network,” no. June, pp. 1–51, 2015.

[17] S. A. Rafiullah Khan, “Conceptual Framework of Redundant Link Aggregation,” *Comput. Sci. Eng. An\rInternational J.*, vol. 3, no. 2, pp. 1–9, 2013.

[18] X. Zhang, C. Jing, F. Tang, S. Fowler, H. Cui, and X. Dong, “Joint redundant and random network coding for robust video transmission over lossy networks,” *Mob. Inf. Syst.*, vol. 8, no. 8, pp. 213–230, 2012.

[19] G. Boe and V. Faltinsen, “Recommendations for a redundant campus network Best Practice Document,” no. December, 2011.

[20] A. Abdelaal and H. H. Ali, “Community wireless networks: Emerging wireless commons for digital inclusion,” *2009 IEEE Int. Symp. Technol. Soc.*, no. May, pp. 1–9, 2009.

[21] M. Petrova, “Cognitive wireless networks: your network just became a teenager,” *25th IEEE Int.*, 2006.

[22] D. H. Friend, “Cognitive Networks: Foundations to Applications,” *PhD Thesis*, p. 158, 2009.

[23] A. Baronchelli, R. Ferrer-i-Cancho, R. Pastor-Satorras, N. Chater, and M. H. Christiansen, “Networks in Cognitive Science,” *Trends Cogn. Sci.*, pp. 1–13, 2013.

[24] A. Rabbachin, T. Q. S. Quek, H. Shin, and M. Z. Win, “Cognitive network interference,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 480–493, 2011.

[25] A. Wyglinski, “Cognitive radio communications and networks,” *IEEE Commun. Mag.*, 2008.

[26] C. Szabó, K. Farkas, and Z. Horváth, “Motivations, design and business models of wireless community networks,” *Mob. Networks Appl.*, vol. 13, no. 1–2, pp. 147–159, 2008.

[27] A. Neumann, E. Lopez, and L. Navarro, “An evaluation of BMX6 for community wireless networks,” *2012 IEEE 8th Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, pp. 651–658, 2012.

[28] S. Kalyanaraman and M. Klein, “A Geography-Aware Scalable Community Wireless Network Test Bed,” *First Int. Conf. Testbeds Res. Infrastructures Dev. NeTworks COMmunities*, pp. 82–91.

[29] P. A, Frangoudis, and G. C. Polyzos, “Wireless Community Networks: An Alternative Approach for Nomadic Broadband Network Access,” 2011.

[30] R. Flickenger, *Building Wireless Community Community Networks*, no. January. 2003.

[31] P. a. Frangoudis, G. C. Polyzos, and V. P. Kemerlis, “Wireless community networks: An alternative approach for nomadic broadband network access,” *IEEE Commun. Mag.*, vol. 49, no. 5, pp. 206–213, 2011.

[32] W. Robert, “Next Generation Networks architecture by ITU-T,” no. January, 2009.

[33] J. Kleinberg, “Complex networks and decentralized search algorithms,” *Proc. oh Int. Congr. Math.*, vol. 3, pp. 1019–1044, 2006.

[34] O. Bonaventure, “Computer Networking : Principles, Protocols and Practice,” *Practice*, 2010.

[35] M. E. J. Newman, “The structure and function of complex networks,” *Cond-Mat/0303516*, vol. 45, no. 2, pp. 167–256, 2003.

[36] T. Networks, “Central Office and Local Loop,” pp. 1–16, 1999.

[37] “Advanced Network Technology June 1993,” no. June, 1993.

[38] European Parliament, “Next Generation Networks,” no. July, 2009.

[39] K. Knightson, “N Ext -G Eneration N Etworks : P Art 1,” *Data Commun. Manag.*, pp. 1–15, 2003.

[40] D. R. Paudel, K. Sato, B. P. Gautam, and D. Shrestha, “Design and implementation of partial mesh community wireless network in Himalayan region,” *2012 Third Asian Himalayas Int. Conf. Internet*, pp. 1–6, 2012.

[41] B. P. Gautam, K. Wasaki, and P. Dambar, “Experimentation of Emergency Detour Route to Enhance Unstable Networks in Wakkanai , Hokkaido,” pp. 279–286, 2014.

[42] B. P. Gautam and K. Wasaki, “Using a redundant Wi-Fi network as an emergency detour route to proactively reduce disaster risk in Wakkanai, Hokkaido,” *2014 Int. Conf. Inf. Sci. Electron. Electr. Eng.*, vol. 3, no. April, pp. 1830–1837, 2014.

[43] B. P. Gautam, N. Sharma, S. Shrestha, and R. Gautam, “Monitoring and Management of Unstable Network through Solar Powered Robotic Vehicle,” *Wakhok Bull.*, vol. 14, pp. 19–30, 2014.

[44] N. Shiratori, N. Uchida, Y. Shibata, and S. Izumi, “DISASTER-RESISTANT INFORMATION,” pp. 6–22.

[45] N. Uchida and K. Takahata, “Never Die Network Based on Cognitive Wireless Network and Satellite System for Large Scale Disaster,” ... *Wirel. Mob. Networks, ...*, pp. 74–93, 2012.

[46] B. P. Gautam, D. R. Paudel, and S. S. Krishna, “A study and site survey in Himalayan region for proper utilization of wireless community networks : an assessment of community wireless implementation in heterogeneous topography,” vol. 11, pp. 23–36, 2011.

[47] A. Shieh, S. Kandula, A. Greenberg, C. Kim, and B. Saha, “Sharing the data center network,” pp. 23–23, 2011.

[48] C. From, “a Ccepted From O Pen C All W Ireless D Ata C Enter N Etworking,” no. September, pp. 46–53, 2011.

[49] W. Tschudi, T. Xu, and D. Sartor, “RoadMap for Public Interest Research for High Peformance Data Centers,” California, 2002.

[50] M. Altman, L. Andreev, M. Diggory, G. King, D. L. Kiskis, E. Kolster, M. Krot, and S. Verba, “An Overview of the Virtual Data Center Project and Software,” *JCDL {\textquoteright}01 First Jt. Conf. Digit. Libr.*, pp. 203–204, 2001.

[51] A. Greenberg, J. Hamilton, D. a Maltz, and P. Patel, “The Cost of a Cloud : Research Problems in Data Center Networks,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, pp. 68–73, 2009.

[52] Symantec, “State of the Data Center Regional Data - Global (Second Annual Report 2008),” vol. 2, p. 13, 2008.

[53] E. Network, “Data Center 2025 : Exploring the Possibilities,” 2014.

[54] B. P. Gautam, N. Sharma, and K. Wasaki, “Tensai Gothalo: A Solar Powered Robotic Vehicle for Real Time Network Monitoring and Management Using Raspberry Pi,” *ScieXplore Int. J. Res. Sci.*, vol. 1, no. 1, pp. 42–50, 2014.

[55] C. C. Meixner, F. Dikbiyik, M. Tornatore, C. Chuah, and B. Mukherjee, “Disaster-Resilient Virtual-Network Mapping and Adaptation in Optical Networks,” *17th Int. Conf. Opt. Netw. Des. Model.*, pp. 107–112, 2013.

[56] Y. Ran, “Considerations and suggestions on improvement of communication network disaster countermeasures after the wenchuan earthquake,” *Commun. Mag. IEEE*, vol. 49, no. 1, pp. 44–47, 2011.

[57] ITU-T Focus Group on Disaster Relief Systems Network Resilience and Recovery, “Technical report on Telecommunications and Disaster Mitigation,” 2013.

[58] B. P. Gautam and K. Wasaki, “Deployment of Wi-Fi network as an emergency survival communication network in Wakkanai, Hokkaido,” *IEEJ Trans. Electr. Electron. Eng.*, vol. 10, no. i, pp. S60–S68, 2015.

[59] G. Cao, “Designing Efficient Fault-Tolerant Systems on Wireless Networks 2 Fault-Tolerant Channel Allocation 3 Coordinated Checkpointing for Mobile Systems,” *Work*, no. June, pp. 1–4, 1999.

[60] R. Zhang-Shen and N. McKeown, “Designing a fault-tolerant network using valiant load-balancing,” *Proc. - IEEE INFOCOM*, pp. 301–305, 2008.

[61] B. Müller, T. Führer, and F. Hartwich, “Fault tolerant TTCAN networks,” *CAN Newsletter, CiA*, p. 18, 2002.

[62] C. Connecticut, “Delay Tolerant Networks : Challenges and Applications.”

[63] Y. Lien, H. Jang, and T. Tsai, “P2Pnet : A MANET Based Emergency Communication System for Catastrophic Natural Disasters,” *Communications*, pp. 1–23, 2010.

[64] J. Cucurull, S. Nadjm-tehrani, and M. Asplund, “Anomaly detection and mitigation for disaster area networks,” *Recent Adv. Intrusion Detect.*, pp. 339–359, 2010.

[65] N. Imaizumi, K. Utsu, H. Sano, and H. Ishii, “Effective Flooding over Disaster Tolerant Ad Hoc Network based on exchange of Neighbor Information,” *Proc. 2013 Int’l Conf. Parallel Distrib. Process. Tech. Appl.*, pp. 1–5, 2013.

[66] R. Jain, “Wireless Networks for Disaster Relief,” pp. 1–10, 2014.

[67] A. Meissner, T. Luckenbach, and T. Risse, “Design Challenges for an Integrated Disaster Management Communication and Information System,” *First IEEE Work. ...*, no. Diren, 2002.

[68] S. C. Liew and K. W. Lu, “A framework for caracterizing disaster-based network survivability.pdf,” *IEEE J. Sel. Areas Commun.*, vol. 12, no. 1, 1994.

[69] K. T. Norrison and A. & T, “Rapidly Recovering from the Catestrophic Loss of a Major Telecommunications Office,” *IEEE Commun. Mag.*, vol. 49, no. 1, pp. 28–35, 2011.

[70] N. Hu, “Network Monitoring and Diagnosis Based on Available Bandwidth Measurement,” 2006.

[71] D. W. H. Ten, S. Manickam, S. Ramadass, and H. A. Al Bazar, “Study on Advanced Visualization Tools In Network Monitoring Platform,” *2009 Third UKSim Eur. Symp. Comput. Model. Simul.*, pp. 445–449, 2009.

[72] J. Tanaka, “Network Monitoring and Data Center Operation Self-Introduction Basic Knowledge of Network Monitoring,” *Network*, pp. 1–37.

[73] Y. Shibata, N. Uchida, and N. Shiratori, “Analysis of and proposal for a disaster information network from experience of the Great East Japan Earthquake,” *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 44–50, 2014.

[74] K. F. Doerner, W. J. Gutjahr, and L. Van Wassenhove, “Special issue on optimization in disaster relief,” *OR Spectr.*, vol. 33, no. 3, pp. 445–449, 2011.

[75] A. Martín-Campillo, J. Crowcroft, E. Yoneki, and R. Martí, “Evaluating opportunistic networks in disaster scenarios,” *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 870–880, Mar. 2013.

[76] a. R. AlBattat and a. P. Mat Som, “Emergency Preparedness for Disasters and Crises in the Hotel Industry,” *SAGE Open*, vol. 3, no. 3, pp. 59–76, 2013.

[77] C. B. Nelson, B. D. Steckler, and J. a. Stamberger, “The evolution of hastily formed networks for disaster response: Technologies, case studies, and future trends,” *Proc. - 2011 IEEE Glob. Humanit. Technol. Conf. GHTC 2011*, no. Dmi, pp. 467–475, 2011.

[78] J. Baker, C. Bond, J. C. Corbett, J. Furman, A. Khorlin, J. Larson, J.-M. Leon, Y. Li, A. Lloyd, and V. Yushprakh, “Megastore: Providing Scalable, Highly Available Storage for Interactive Services,” *Proc. Conf. Innov. Data Syst. Res.*, pp. 223–234, 2011.

[79] E. Jenelius, “Redundancy importance: Links as rerouting alternatives during road network disruptions,” *Procedia Eng.*, vol. 3, pp. 129–137, 2010.

[80] I. Stojmenovic and X. Lin, “Power-aware localized routing in wireless networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 12, no. 11, pp. 1122–1133, 2001.

[81] A. Osamu and K. Norio, “Progress of Wakkanai Experimental Community Project,” *J. Natl. Inst. Inf. Commun. Technol.*, vol. 51, pp. 193–216, 2004.

[82] T. Yanagida, Y. Sato, and K. Norio, “Multicast Broadcasting Over wireless community networks,” in *The fourth workshop on Internet Technology*, 2001, pp. 133–139.

[83] K. Norio, “Long Range wireless network in geographically disadvantageos regions,” in *Proceedings of North Internet Symposium*, 2007, pp. 74–77.

[84] K. Norio, “A decade of Wakkanai Community Networks and Internet Technology,” 2006, pp. 171–174.

[85] C. Mutch, “The role of schools in disaster preparedness, response and recovery: what can we learn from the literature?,” *Pastor. Care Educ.*, vol. 32, no. 1, pp. 5–22, 2014.

[86] P. M. Anderson, G. M. Chintaluri, S. M. Magbuhat, and R. F. Ghajar, “An improved reliability model for redundant protective systems-Markov models,” *IEEE Trans. Power Syst.*, vol. 12, no. 2, pp. 573–578, 1997.

[87] C. Chiasserini and R. R. Rao, “Improving energy saving in wireless systems by using dynamic power management,” *IEEE Trans. Wirel. Commun.*, vol. 2, no. 5, pp. 1090–1100, 2003.

[88] F. Legendre, T. Hossmann, F. Sutton, and B. Plattner, “30 Years of Ad Hoc Networking Research: What About Humanitarian and Disaster Relief Solutions? What Are We Still Missing?,” *Proc. Int. Conf. Wirel. Technol. Humanit. Reli.*, pp. 217–217, 2011.

[89] G. Zussman and A. Segall, “Energy efficient routing in ad hoc disaster recovery networks,” *Ad Hoc Networks*, vol. 1, no. 4, pp. 405–421, 2003.

[90] A. Chamam and S. Pierre, “On the Planning of Wireless Sensor Networks: Energy-Efficient Clustering under the Joint Routing and Coverage Constraint,” *IEEE Trans. Mob. Comput.*, vol. 8, no. 8, pp. 1077–1086, 2009.

[91] M. Walraed-Sullivan, A. Vahdat, and K. Marzullo, “Aspen Trees: Balancing Data Center Fault Tolerance, Scalability and Cost,” *Proc. Conex.*, pp. 85–96, 2013.

[92] L. Gautam, R. K. Verma, and C. Sharma, “Developing Manual Control for a Line Follower Robot,” vol. 3, no. 3, pp. 305–310, 2013.

[93] Y. Han, L. Xu, G. Yao, L. Zhou, and C. Chen, “Operation Principles and Control Strategies of Cascaded H-bridge Multilevel Active Power Filter,” *Electr. Eng.*, vol. 91, no. 3, pp. 71–76, 2009.

[94] H. Tsuchiya, Y. Michitaka, N. Shinkawa, H. Akaba, and A. Yasuda, “A Novel Boost Class-D Amplifier Using an H-bridge Circuit,” *IEEJ Trans. Electr. Electron. Eng.*, vol. 5, no. 6, pp. 660–663, 2010.

[95] B. P. Gautam, K. Wasaki, and N. Sharma, “Using a Solar Powered Robotic Vehicle to Monitor and Manage Unstable Networks,” *Int. J. Futur. Comput. Commun.*, vol. 3, no. 6, pp. 415–420, 2014.

[96] W. H. Huang, B. R. Fajen, J. R. Fink, and W. H. Warren, “Visual navigation and obstacle avoidance using a steering potential function,” *Rob. Auton. Syst.*, vol. 54, no. 4, pp. 288–299, Apr. 2006.

[97] Y. Aloimonos, “Is visual reconstruction necessary? obstacle avoidance without passive ranging,” *J. Robot. Syst.*, vol. 9, no. 6, pp. 843–858, 1992.

[98] J. D. Mooney, “Bringing Portability to the Software Process,” *Dept. Stat. Comp. Sci., West Virginia Univ., Morgant. WV*, 1997.

[99] T. Sakano, Z. Fadlullah, T. Ngo, H. Nishiyama, M. Nakazawa, F. Adachi, N. Kato, A. Takahara, T. Kumagai, H. Kasahara, and S. Kurihara, “Disaster Resilient Networking - A New Vision based on Movable and Deployable Resource Units,” vol. 27, no. 4, pp. 40–46, 2013.

[100] I. Sugino, “Disaster Recovery and the R&D policy in Japan’s telecommunication networks,” 2012.

[101] Y. Adachi and H. Obata, “Disaster prevention measures of NTT for telecommunications network systems,” *IEEE Commun. Mag.*, vol. 28, no. 6, pp. 18–24, 1990.

[102] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog Computing and Its Role in the Internet of Things,” *Proc. first Ed. MCC Work. Mob. cloud Comput.*, pp. 13–16, 2012.

[103] S. Ghulam, J. Schubert, G. Tamm, and V. Stantchev, “Integrating Smart Items and Cloud Computing in Healthcare Scenarios,” no. c, pp. 75–81, 2014.

[104] T. H. Luan, L. Gao, Z. Li, Y. Xiang, and L. Sun, “Fog Computing: Focusing on Mobile Users at the Edge,” *eprint arXiv:1502.01815*, 2015.

[105] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, “An overview of Fog computing and its security issues,” *Concurr. Comput. Pract. Exp.*, p. n/a–n/a, 2015.

[106] B. P. Gautam, K. Wasaki, and A. Batajoo, “Encapsulation of Micro Engineering Tools in a Co- Operative Jyaguchi Computing Infrastructure,” *ScieXplore Int. J. Res. Sci.*, vol. 1, no. 1, pp. 34–41, 2014.

[107] B. P. Gautam, “An Architectural Model for Legacy Resource Management in a Jini Based Service Cloud Over Secured Environment,” *SIG Tech. Reports*, vol. 53, no. EIP-43, pp. 55–62, 2009.

[108] B. P. Gautam and D. Shrestha, “A Model for the Development of Universal Browser for Proper Utilization of Computer Resources Available in Service Cloud over Secured Environment,” *Lect. Notes Eng. Comput. Sci.*, vol. 2180, pp. 638–643, 2010.

[109] S. Tilley, *Perspectives on Legacy System Reengineering*. Carnegie Mellon University, 1995.

[110] Bing Wu, D. Lawless, J. Bisbal, J. Grimson, V. Wade, D. O’Sullivan, and R. Richardson, “Legacy systems migration-a method and its tool-kit framework,” *Proc. Jt. 4th Int. Comput. Sci. Conf. 4th Asia Pacific Softw. Eng. Conf.*, pp. 312–320, 1997.

[111] H. S. Kim and J. M. Bieman, “Migrating legacy software systems to CORBA based distributed environments through an automatic wrapper generation technique,” *Proc. Jt. Meet. 4th World Multiconference Syst. Cybern. Informatics 6th Int. Conf. Inf. Syst. Anal. Synth.*, 2000.

[112] B. P. Gautam and S. K. Shrestha, “Effective Campus Management through Web Enabled Campus-SIA (Student Information Application),” *Proc. Int. Multiconference Eng. Comput. Sci.*, vol. I, pp. 608–613, 2012.

[113] Z. Zhang, Y. Sun, and Y. Lu, *Interactive and Collaborative E-Learning Platform with Integrated Social Software and Learning Management System*, vol. 212. 2013.

[114] R. Parikh, “Social Software,” *New York*, pp. 1–22.

[115] J. van Eijck and R. Verbrugge, “Discourses on Social Software,” vol. 5, p. 248, 2010.

[116] P. A. Busch, “Knowledge Management Implications of Articulable Tacit Knowledge : Case Studies on its Diffusion,” 2004.

[117] V. Henrich, E. Hinrichs, M. Hinrichs, and T. Zastrow, “SERVICE-ORIENTED ARCHITECTURES : FROM DESKTOP TOOLS TO WEB SERVICES AND WEB APPLICATIONS.”

[118] B. A. Kumar, “Thin Client Web -Based Campus I nformation,” *Int. J. Softw. Eng. Appl.*, vol. 2, no. 1, pp. 13–26, 2011.

[119] K. Sahin, “Service oriented architecture (SOA) based web services for geographic information systems,” *XXIst ISPRS Congr. Beijing*, pp. 625–630, 2008.

[120] B. P. Gautam, “An architectural model for time based resource allocation and optimized resource allocation in a Jini based service cloud,” Shinshu University, 2009.

[121] R. Berbner, T. Grollius, and N. Repp, “An approach for the Management of Service-oriented Architecture (SoA) based Application Systems.,” *Enterp. Model. Inf. Syst. Archit.*, pp. 208–221, 2005.

[122] M. a Jabr and H. K. Al-omari, “e-Learning Management System Using Service Oriented Architecture,” *Comput. Sci.*, vol. 6, no. 3, pp. 285–295, 2010.

[123] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Role-Based Access Control Models,” *IEEE Comput.*, vol. 29, no. 2, pp. 38–47, 1995.

[124] D. F. Ferraiolo and D. R. Kuhn, “Role-Base Access Controls,” *ACM Trans. Inf. Syst. Secur.*, vol. 2, no. 1, pp. 34–64, 1992.

[125] L. Zhao, “A Role-based Access Control Security Model for Workflow Management System in an E-healthcare Enterprise,” *Administrator*, 2008.

Appendix I: Hardware Cost Details of Tensai Gothalo

Table 8-1: Total Cost Details

Details	Cost	Remarks
Master TG	71500	Table 8-2
Slave TG (Path Tracing)	72570	Table 8-3
Slave TG (Secondary Node)	49010	Table 8-4
Slave TG (Obstacle Avoidance)	53280	Table 8-5
Total Cost	**246360**	

Table 8-2: Tentative Cost of Master Tensai Gothalo

Item. No	Device Name	Quantity	Amount (in JPY)	Remarks
1	Nch power MOSFET 2SK2232 (60V25A)	8	800	
2	5.1V5W Zener diode 1N5338BRLG	4	100	
3	Electrolytic capacitor 100μF35V85 ℃	4	80	
4	ceramic capacitor 0.1μF50V	10	100	
5	Three-terminal regulator 5V1.5A L7805CV	2	60	
6	Breadboard EIC-801	2	540	
7	Breadboard jumper wire 15cm	1	350	
8	Transistor 2SA1015Y 50V150mA	3	30	
9	RF receiver module	1	2200	Third Party
10	Tact switch (black)	4	40	
11	BG4L-BS 12V 3Ah/10HR	1	20,000	
12	wheels	4	12000	Third Party (Lego)
13	Dc motor	2	10000	Third Party (Lego)
14	7 Ohm 3watt speaker	1	200	
15	Raspberry Pi with SSD card	1	10000	
16	Solar Panel with Battery	1	15000	
	Total		**71500**	

Table 8-3: Tentative Cost of Slave Gothalo1 (For Path Tracing)

Item. No	Device Name	Quantity	Amount (in JPY)	Remarks
1	Nch power MOSFET 2SK2232 (60V25A)	9	900	
2	General purpose rectifier diode 1000V1A 1N4007-B	2	20	
3	Electrolytic capacitor 100μF35V85 ℃	8	160	
4	ceramic capacitor 0.1μF50V	10	100	
5	Three-terminal regulator 5V1.5A L7805CV	2	60	
6	Breadboard EIC-801	5	1350	
7	Breadboard jumper wire 15cm	1	350	
8	Transistor 2SA1015Y 50V150mA	4	40	
9	Transistor 2SC1815GR 60V150mA	4	40	
10	IR sensor TX-RX pair	2	200	
10	Timer IC NE555P	1	30	
11	Solar panel OPL90A44101 4w, 9.0v, 440mA	1	1950	
12	Hall effect sensor	1	20	
13	At89s52 microcontroller	1	250	
14	941H-2C-5D relay	1	100	
15	wheels	4	12000	
16	Dc motor	2	10000	
17	Raspberry Pi with SSD card	1	10000	
18	Solar Panel with Battery	1	15000	
19	BG4L-BS 12V 3Ah/10HR	1	20,000	
	Total		**72570**	

Table 8-4: Cost of Slave Tensai Gothalo Secondary Node

Item. No	Device Name	Quantity	Amount (in JPY)	Remarks
1	Nch power MOSFET 2SK2232 (60V25A)	4	400	
2	General purpose rectifier diode 1000V1A 1N4007-B	2	20	
3	Electrolytic capacitor 100μF35V85 ℃	3	60	
4	ceramic capacitor 0.1μF50V	4	40	
6	Breadboard EIC-801	1	270	
7	Breadboard jumper wire 15cm	1	350	
9	Transistor 2SC1815GR 60V150mA	2	20	
11	Solar panel OPL60A33101 2w, 6.0v, 333mA	1	950	
15	6v 2.0 AH sealed lead-acid Battery	1	400	
15	Toy car wheels and motor	4+2	1500	
16	Raspberry Pi with SSD card	1	10000	
17	Solar Panel with Battery	1	15000	
18	BG4L-BS 12V 3Ah/10HR	1	20,000	
19	**Total**		**49010**	

Table 8-5: Cost of Slave Tensai Gothalo
(With Obstacle Avoidance Funtionality)

Item. No	Device Name	Quantity	Amount (in JPY)	Remarks
1	Nch power MOSFET 2SK2232 (60V25A)	8	800	
2	General purpose rectifier diode 1000V1A 1N4007-B	2	20	
3	Electrolytic capacitor 100μF35V85 ℃	6	160	
4	ceramic capacitor 0.1μF50V	6	60	
5	Three-terminal regulator 5V1.5A L7805CV	1	30	
6	Breadboard EIC-801	4	1080	
7	Breadboard jumper wire 15cm	1	350	
8	Transistor 2SA1015Y 50V150mA	6	60	
9	Transistor 2SC1815GR 60V150mA	6	60	
10	IR Led	3	30	
10	Timer IC NE555P	1	30	
	Infrared remote control receiver module PL-IRM1261-C438	3	300	
11	Solar panel OPL90A44101 4w, 9.0v, 440mA	1	1950	
13	At89s52 microcontroller	1	250	
14	6V4Ah WP4-6 sealed lead-acid Battery	1	700	
15	Toy car wheel and Dc motor	4+2	2400	
16	Raspberry Pi with SSD card	1	10000	
17	Solar Panel with Battery	1	15000	
18	BG4L-BS 12V 3Ah/10HR	1	20,000	
19	**Total**		**53280**	

Appendix II: Hardware Cost Details of HA Cluster

Table 8-6: Total Cost of HA Cluster

Item No	Device Name	Quantity	Amount (JPY)	Remarks
1	Raspberry Pi (Model B+)	10	70,000	
2	Power Cable	10	4,000	
3	Layer 2 Switch	1	100,000	
4	DHT-22 Sensor	2	7,000	
5	**Total**		**181,000**	