Title

Self-Reconstruction of Wireless Mesh Networks in Disaster Situation

Supervisor
Professor Kazuhiko Kinoshita

Author
Erdenetuya Dorj

March 2020

Department of Information Science and Intelligent Systems,
Graduate School of Advanced Technology and Science,
Tokushima University

Self-Reconstruction of Wireless Mesh Networks in Disaster Situation

Erdenetuya Dorj

Abstract

In recent years, the world endured natural disasters in common, taking out hundreds of physical network devices, disconnected numerous vital communication and electricity cables. In order to cope effectively with post-disaster emergency situations, verify the safety of people, facilitate information sharing in the vicinity, and provide communication services, network recovery mechanisms must be improved. Therefore, the vital features of computer networks available for disaster situation is reliable, fault tolerance and self-configurable. As a basis of such a system, wireless mesh networks (WMNs), which aim at becoming a key practical communication solution to provide higher reliable network infrastructure for numerous emergent applications, have attracted much attention. Moreover, by adopting the capabilities of ad-hoc, such as dynamic self-forming, and self-healing, WMNs can accomplish flexible network architecture, easy deployment and configuration, fault tolerance, mesh connectivity, and network resilience.

However, most of the existing works are based on IEEE 802.11 ad-hoc mode and considered as unpractical, so that developers give much attention to the widely-used IEEE 802.11 infrastructure mode because of easy practical usage and cost reduction. In WMNs based on infrastructure-mode, the mesh routers are divided into an access point (AP) that can typically connect to many stations (STAs) and a STA that can connect to only one AP. All mesh routers are likely to transmit an information data to a wired backbone network zone via their serving gateways (GWs). Different from the ad-hoc mode, in the infrastructure mode, each interface must decide its working mode; AP or STA. An interface in AP mode can connect to any number of interfaces in STA mode. To the contrary, an interface in STA mode can connect to only one interface in AP mode. This causes another challenge in WMNs.

In this thesis, we propose an effective method to reconstruct a WMN based on the IEEE 802.11 infrastructure mode in disaster situation, comprising of one or more GW routers and mesh routers. Some mesh routers go down due to a disaster occurrence. As a result, some other routers can be isolated from the wired network. The proposed method makes an association isolated routers with the wired network using spare APs and all mesh routers including spare AP must be converged in the standard IEEE 802.11 infrastructure mode.

To achieve our goal, we first develop a spare AP placement method that mainly focuses on discovering an adequate location for a spare AP and making all the isolated routers reachable to the wired network. It has the following two phases; connectivity restoration phase and rerouting phase. In the connectivity restoration phase, we formulate received signal strength indication (RSSI) based localization algorithm to find the optimal point for placing the spare AP. In the rerouting phase, each isolated router can assign an appropriate infrastructure mode such as AP and STA to its interfaces in order to establish neighbor association so that it can be converged as having a potential route to the wired network. Furthermore, we consider that only public workers without any experience with wireless communication technologies must decide upon the adequate locations for spare APs and install them.

For the spare AP placement method, we still need to make a potential route of an isolated router practical. Furthermore, it leads us to elaborate an interface mode assignment method that decides which mode is suitable for an interface of an isolated router to establish an association with its neighbor router in order to enable all the isolated routers reachable to the wired network via a GW router. This method is invoked after a spare AP has been installed. It consists two phases including tentative routing and interface mode selection. In the tentative routing phase, each isolated router can discover a route to a GW in a distributed manner. In the interface mode selection phase, each isolated router can automatically form its neighbor connection in an infrastructure mode along its route to the GW. Consequently, all the isolated router should be reachable to the wired network working in the infrastructure mode.

We show the results of performance evaluations to prove the effectiveness of both methods. In addition, the results of field trials express the feasibility of the spare AP placement method.

Keywords

wireless mesh network, infrastructure mode, disaster, reconstruction

List of Figures

List of Tables

Contents

1 Introduction

In the last decades, numerous of man-made and natural disasters occurred, causing physical damage, electricity outage, and traffic congestion. If the disaster-affected area had been accurately defined and information sharing in the vicinity was possible, recovery/response would likely have been much improved.

Therefore, researchers have been studying the deployment of robust network infrastructure for disaster information systems for more than a century, which has the goal being to transmit information at all stages of an emergency, including disaster mitigation and citizen preparation. In addition, from the practical aspects of the network infrastructures of the disaster system, we should assume the core capabilities such as wireless connectivity in wide range, ease of use, low cost, and so on. It is also essential to restore the network infrastructure swiftly. Mobile base stations, local switches and transmission medium may undergo major damage in disasters. In order to respond effectively to post-disaster emergency situations, verify the safety of individuals, facilitate information-gathering, and provide means of communication, infrastructures should be recovered by employing every possible means. From the viewpoint of network resilience and recovery (NRR), the above two issues are considered fundamental and crucial. Preventing, mitigating, or circumventing congestion in an emergency situation and minimizing disruption to communications in the event of infrastructure damage are two major objectives of NRR. [1, 2, 4–6].

For these reasons, wireless mesh networks (WMNs), which aim at becoming a key practical communication solution to provide a higher reliable network infrastructure for numerous emergent applications, have also attracted much attention of many researchers. Moreover, by adopting the capabilities of ad-hoc, such as dynamic self-forming, and self-healing, WMNs can accomplish flexible network architecture, easy deployment and configuration, fault tolerance, mesh connectivity, and the NRR.

However, these kinds of ad-hoc mesh networks are considered to be unpractical infrastructure since the ad-hoc mode suffers from the following three issues: (1) smartphones do not support ad-hoc mode; (2) supporting the ad-hoc mode is inefficient since every device needs additional MANET (Mobile Ad-hoc NETwork) protocols for routing and address resolution; (3) mobile device vendors and operating system developers give much attention to the widely-used IEEE

802.11 infrastructure mode due to ease of practical use and cost reduction.

In this kind of infrastructure-mode based WMNs, the mesh routers are divided into an access point (AP) that can typically connect to many stations (STAs) and a STA that can connect to only one AP. All mesh routers are likely to transmit an information data to a wired backbone network zone via their serving gateways (GWs) [1, 2, 4–6]. Different from the ad-hoc mode, in the infrastructure mode, each interface must decide its working mode; AP or STA. An interface in AP mode can connect to any number of interfaces in STA mode. To the contrary, an interface in STA mode can connect to only one interface in AP mode. This causes another challenge in WMNs [3].

Since a disaster strikes, some mesh routers go down so that some other routers can be isolated from the wired network. It is significant that the WMN should be recovered and reachable after the disaster as soon as possible. Suppose that local recovery cannot be performed to provide communication for the isolated routers to reach the wired network so that the isolated routers should be reachable to the wired network autonomously. Therefore, the main goal of our study aims to deploy an effective method to provide self-reconstruction of the standard IEEE 802.11 infrastructure mode based mesh network in a disaster situation. Specially, an isolated router are range out of a connected router so that it needs a spare AP to make an association with a serving GW.

At first, by interviewing public workers, we noticed the following requirements/constraints with regard to mesh network recovery. (1) The number of available spare APs and portable batteries are limited. (2) Firefighters and/or members of the self-defense forces can survey disaster-affected areas to identify locations for spare AP placements while their original activity. (3) Public workers, who may not be well-versed with wireless communication technologies, can nonetheless install the spare AP(s).

Considering these requirements/constraints, we propose a self-reconstruction method of WMN based on the IEEE 802.11 infrastructure mode in disaster situation using as minimum as spare APs. More specifically, we aim to highlight practical aspects of the study. Hence, we need to address the following two key issues; (i) how to accurately discover adequate location of spare APs, (ii) how to tackle which infrastructure mode is suitable for each interface of isolated mesh router to achieve a full converged and recovered network.

To achieve our goal by dealing with the above two issues, we first elaborate a spare AP placement method that has two phases: connectivity restoration phase and rerouting phase. In the connectivity restoration, this phase determines an adequate point for the installment of a spare AP using a Received Signal Strength Indicator (RSSI) based ranging and positioning algorithm for making an isolated router associate with a reachable/connected router to a GW.

In a whole process of the method, at first, public workers, typically firefighters, trace RSSI values from the isolated routers using their smartphones while going through disaster area for investigation and/or rescue. The collected data enables to estimate transmission range of the isolated routers and find overlapping transmission ranges between isolated and reachable routers in order to determine the adequate location for spare APs. Then, a spare AP is installed at an adequate point that can be the central point of an overlapping transmission range. Therefore, we should formulate a RSSI-based ranging and localization algorithm for our method. The algorithm, consequently, should accomplish a fully reconstructed mesh network, where all the isolated routers have connected to the connected region via as much as minimum spare APs. In the rerouting phase, each isolated router should select which infrastructure mode is suitable for its interface in order to establish neighbor association with a connected router. Furthermore, we consider that only public workers without any experience with wireless communication technologies must decide upon the adequate locations for spare APs and install them.

Second, we present an interface mode assignment method that decides which mode is suitable for an interface of an isolated router to establish an association with its neighbor router in order to enable all the isolated routers reachable to the wired network via a GW router. This method is invoked after a spare AP has been installed. It consists two phases including a tentative routing and an interface mode selection. In the tentative routing phase, each isolated router needs to discover a next hop router reachable to the wired network in a distributed manner. In the interface mode selection phase, each isolated router can automatically form its neighbor connection in an infrastructure mode along its route to the GW. Consequently, the mesh network is fully reconstructed when the interface mode selection phase is complete.

The performance of the spare AP placement method was evaluated in two assumed network topologies such as a partial mesh and full mesh to show the effect. Moreover, the performance of the interface mode assignment method was evaluated in an assumed WMN with or without spare AP. In addition, fundamental and disaster field experiments are executed to confirm the feasibility of the spare AP placement method.

In chapter 2, we introduce some past literature works. In chapter 3, we discuss proposed methods; (1) Spare AP placement method and (2) Interface mode assignment method. In addition, we present performance evaluation results for each proposed method separately. Chapter 4 shows the feasibility of the spare AP method via field trial. Finally, chapter 5 states discussion, conclusion and future work.

2 Related Work

Many past related works have made large contributions to the development of WMNs for use in the unlicensed spectrum at low cost by considering multiple characteristics such as self-forming, self-configuring, and self-healing. Hence, these features make the use of WMNs advantageous in terms of low upfront cost, easy network maintenance, robustness, and reliable service coverage, in particular for public safety and emergent applications. In the following sections, each related work is introduced.

2.1 Outline of WMNs

In this section, we describe main features of WMNs including network design, characteristics, and applications at first. Next, routing algorithms in WMNs are introduced. Especially, some distributed routing algorithms are explained briefly.

[1] assumes that WMNs are defined as a key technology among wireless networks. In WMN, nodes are mesh routers and clients in Fig. 2.1. Self-organizing, self-configuring, and self-healing abilities allow each node to establish mesh connectivity. WMN has a great opportunity of working with other networks such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, and sensor networks. Moreover, mesh GW and bridging technologies play a key role of their integration. Therefore, an integrated WMN is utilized for the applications of a variety of networks such as broadband home networking, enterprise networking, metropolitan area networks, and wide area networks.

[2] also explains the main infrastructure of WMNs and highlights on the importance of the efficiency of WMNs design including fixed and unfixed topologies. For the fixed topologies based approaches, the performance of a multi-channel and multi-hop WMNs can be improved by solving the issues in terms of routing metric, channel assignment, and interference. In the unfixed topologies approaches, there are two classifications such as fixed-gateways and unfixed gateways. To improve the optimization of such topologies based approaches, links capacity and optimal placement of APs for a required area are considered. In addition, although there are many challenges and opportunities, layered protocols and cross-layer design are applied to a variety of applications.

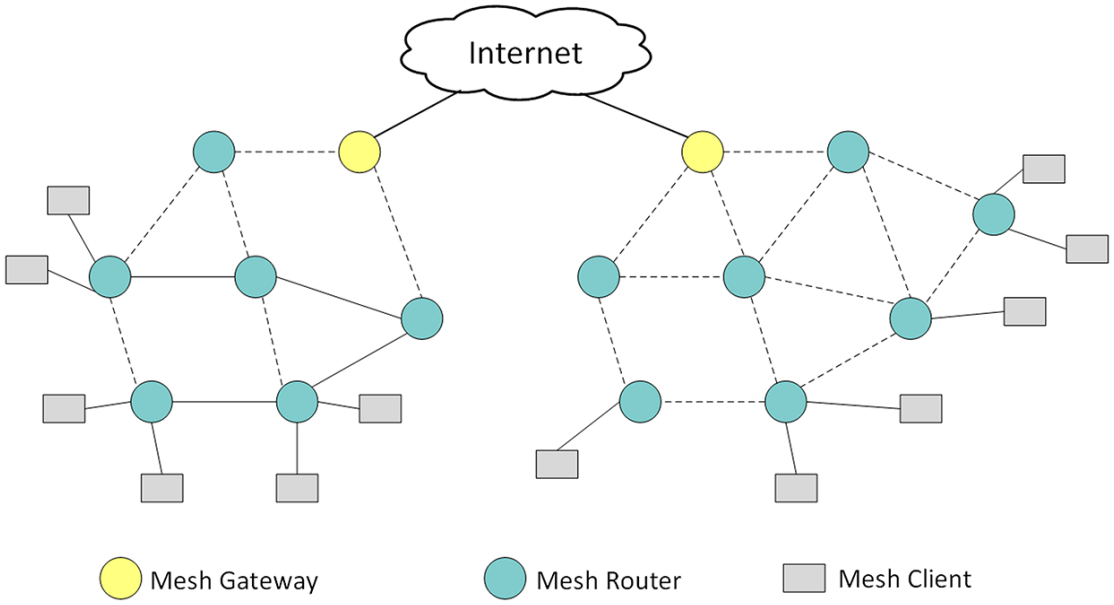


Figure. 2.1: General Architecture of WMN

[4] and [5] show improvements in the performance of WMNs using directional antennas. To reduce transmission delay of multi-radio multi-channel (MR-MC) WMNs, they consider optimal antenna beam selection and scheduling algorithms for creating a broadcast routing tree from a root to other nodes [6]. [7] indicates that using directional antenna in MR-MC WMNs allows to construct a robust topology rather than using omnidirectional antenna.

[8] shows the comparison results of the common routing algorithms such as AODV, zone routing protocol (ZRP), and DSR in ad-hoc based WMNs under disaster situation. AODV protocol shows good implementation result compared to others in all four cases. In [9], routing protocols play an important role to increase WMNs efficiency and reliable. They consider distributed routing protocols have many advantages than centralized routing protocols.

2.2 WMNs based on ad-hoc mode with disaster consideration

In last decades, the world has faced natural disasters such as hurricanes, earthquakes, floods, and tsunamis, causing numerous casualties, damage to properties, and destruction of millions of homes and businesses. Therefore, WMNs are actively studied as disaster-resilient networks and have become a key practical communication solution to provide higher resilient network infrastructure for use in the unlicensed spectrum and at low cost based on the IEEE 802.11 ad-hoc mode by considering multiple characteristics such as network design, scalability, quality of

service, and fault tolerance in the last decades.

For this purpose, [10] highlights the WMN in ad-hoc form with self-organizing, self-forming, and self-healing characteristics. In addition, they aim at deploying four types of communication infrastructures including personal area networks (PANs), an incident area network (IAN), a jurisdiction area network (JAN), and extend area networks (EANs) in a major crisis situation as well as note their two kinds of requirements for functional and performance. As a result, the current WMNs are not good enough to provide the requirements of public safety and crisis management communication in terms of scalability and quality of service (QoS). In a case that these limitations get overcome, WMN technology can be a major network infrastructure for emergent situations. With the capabilities of ad hoc networking, WMNs can accomplish a main network architecture for public safety and crisis management communications.

[11] presents the results of a real mesh test bed deployed on a campus to improve ad-hoc WMN survivability in a disaster scenario. [12] shows that a multi-channel and multi-radio ad-hoc WMN can achieve high capacity compared to dual-radio and single-radio WMNs. In particular, these features make the use of WMNs advantageous in terms of low upfront cost, easy network maintenance, robustness, and reliable service coverage [13]. Wireless virtualization mechanisms, namely wireless multi-hop access network virtualization are applied to a tree-based mobile ad hoc network (MANET) architecture for disaster recovery. At first, a node connects to an internet gateway as a common STA. After that, it transforms into virtual AP working as a bridge between isolated nodes and the internet gateway [14, 15].

[16] considers a reliable routing technique for disaster recovery. Using reliable routing technique has been given the simulation results of high performance and guaranteed reliable packet delivery at a destination device using network simulator version 2. [17] designs and implements an experimental test-bed of WMN with a highly de-centralized architecture and small unmanned aerial systems. They offered disaster tolerant WMNs with three features according to the level of disaster affected areas:

- To maintain communication services using survived nodes and links under partial damage in the network.
- To maintain local communication services under the loss of links to the Internet or core networks and the damage of servers in the Internet.
- To recover a part of communication links rapidly to the isolated areas where road and network infrastructure are totally damaged.

[18] shows the comparison results of the common routing algorithms such as AODV, ZRP, and DSR in ad-hoc based WMNs under disaster situation. AODV protocol shows good implementa-

tion result compared to others in all four cases. In the experiment of [19], at first, they introduce a kind of mesh network called "NerveNet" and show how it was used for disaster recovery after the Kumamoto earthquakes. An SDN-based resilient architecture against disaster failures has been designed in which an algorithm proposes for geographic-based backup topologies generation and splicing considering the load distriburtion between nodes [20].

Although the above research works are essential, there are still some limitations of the use of WMNs with the IEEE 802.11 infrastructure mode.

2.3 Reconstruction Approaches for WMNs

In this section, according to the assumption of fault tolerant approaches for recovering WMNs in a failure situation, the investigations and implementation were conducted. Specifically, link failure approaches have been considered.

[22] shows the fault tolerant base station planning algorithm in WMNs and places base stations on adequate locations based on radio coverage information. The algorithm allows to handle link failures among different base stations and clients. [23] assumes reconfiguration approach named autonomous reconfiguration system improving the performance of WMNs using necessary changes in channel assignment to avoid a link failure. [24] studies numerous reconfiguration techniques of two main approaches such as neighbor discovery mechanism and cross-layer approach. Greedy channel assignment method among their techniques successfully handled link failures by monitoring link quality, whereas another [25] reviews fault tolerance issues, such as link failures in different types of WMNs. Additionally, in [25], a fault tolerant system has major three steps including fault detection, diagnosis and recovery in case of link and node failure.

[26] presents an enhanced reconfiguration system to recover WMNs from link failure. In a whole process of the system, the quality of links of each node is accurately monitored in a distributed manner and quality of service (QoS) satisfiable reconfiguration is performed. [27] implements ARS in a Linux operating system for reconfiguration of WMNs and evaluated it in a testbed. In [24], they survey an issue related to the estimation of reliable data transmission in WNMs. The mechanism they propose includes multi-path routing and random network coding techniques in order to improve the conventional method of coding nodes selection. However, the biggest challenge pertaining to WMN infrastructure is resolving impracticalities such as the lack of IEEE 802.11 control frames and connectivity availability to unlicensed mobile devices (e.g., smartphones, laptops, and so on).

2.4 Wireless Node Localization Techniques

Wireless node localization techniques are often used for Wireless Sensor Networks (WSNs). All algorithms of localization techniques are totally classified in two groups of "range-free" (algorithms not based on distance measurement)) and "range-based" (algorithms based on distance measurement) localization. The range-based techniques are usually applied for localization because the accuracy is better than range-free method. However, range-free method has an advantage such as cost-effective, especially for large-scale networks [30].

Therefore, we study more about the range-based techniques. In the range-based algorithms, there are four classification based on measurements to calculate the distance or angle between sensors (point-to-point measurement) and usually need extra hardware for localization and provide information on a specific signal: (1) Time of Arrival (TOA); (2) Angle of Arrival (AOA); (3) Time Difference of Arrival (TDOA); (4) RSSI; Although each method has its advantages and disadvantages, the RSSI-based localization techniques do not require additional hardware that other techniques. Usually a device's location is usually estimated by monitoring a distance dependent parameter such as wireless signal strength from a base station whose location is known. In practical deployments, signal strength varies with time and its relationship to distance is not well defined so that accuracy is not enough for the RSSI-based technique. However, it is often used for localization in a variety of wireless technologies. A localization process is done by two steps: ranging and position computation. In ranging step the distance between two nodes (unknown position node and known position node) is computed by some method such as TOA, TDOA, RSSI, or AOA. In the positioning step the location of unknown node calculated by some methods such as Trilateration or Triangulation (based on geometric principle in triangles by using distance or angle information) [31].

Also, the range-based algorithms can be executed in two manners including centralized and distributed. Generally, centralized algorithms can be used when we need more accuracy while distributed algorithms have better scalability. In the centralized approach, we have a powerful central-base server node that the other sensor nodes communicate with and the central server node does the computation and sends localization information to the other sensor nodes. In this method, after sending data (measurements) from the sensor nodes to the server (it needs a database for saving received signals and computational data), they must receive acknowledge. This method reduces the problem of computation in sensor nodes and gives possibility to execute more complicated algorithms. However, the communication cost and scalability are some limitations and possibility of sensor node or central node failure are two issues. In some applications such as monitoring patients, controlling home, monitoring humidity and temperature in precise agriculture with central architecture, it is easy to use centralized localization. There are three common

algorithms in centralized localization.

- MDS-MAP: First, the shortest path distance between a pair of nodes is computed to construct a distance matrix for MDS and then, by applying classical MDS to the distance matrix, a 2D or 3D relative map is created. Second, given anchor nodes transform the relative map to an absolute map.

- Localization node based on simulated annealing: This algorithm is used to gather an estimate of location of the localizable sensor node based on other information of the neighbor nodes in the system. Any errors caused by flip ambiguity is omitted.

- A RSSI-based centralized localization: this algorithm is based on signal attenuation to define distance. It is practical and self-organized program but uses more power to send much information to the central server. First, RF (Radio Frequency) mapping of the network is built by storing RSSI value of transmitted packets between the two anchors. Second, all the recorded RSSI values are used for creation of the ranging model. Finally, an optimization problem is solved and provides the position of the nodes for centralized localization model [29].

In the distributed localization approach, computation for positioning does not rely on one single node. Each sensor node has small memory and small processing time (limited processing potential). It means that the algorithm must be simpler than centralized approach and sensors communicate with each other to find their location in the network. There are six common algorithms in distributed localization.

- Beacon-based distributed algorithms: In the algorithms, a group of nodes with unknown positions finds their locations by using measured distance to the other nodes using beacon messages. There are two kinds of algorithms such as Diffusion, Bounding Box and Gradient in common [29].

- Relaxation-based distributed algorithms: In the algorithms, a coarse algorithm is used to reach an optimal solution, working in some refinement stages. Spring model and Cooperative Ranging Approach belong to such kind of category [29].

- Coordinate system stitching based distributed algorithms: In the algorithms, an area of sensors is firstly divided into small overlapping optimal local maps and then the local maps merge into a single map using cluster based approach [29].

- Hybrid localization algorithms: Such kinds of algorithms use two different localization techniques such as MDS (multidimensional scaling) and APS (ad-hoc positioning system) to decrease communication and computation cost [29].

- Interferometric ranging based localization: the main idea of this algorithm is to use two transmitters to create interference signals and then measure the composite signal frequency. Although the measurement of the algorithm is very accurate, it may limit localization to the small networks since Interferometric ranging needs a large set of measurements [29].

- Error propagation aware localization: this algorithm is based on integration of path loss and distance measurement error model. When a sensor node (with unknown position) finds its position with WLS (weighted least square), the algorithm becomes an anchor node (with known position) and broadcasts its information. This process continues until all sensors become anchors [29].

Above all, the RSSI-based ranging and positioning techniques in WMNs, considering RSSI characteristics, algorithms, and challenges.

The RSSI-based techniques estimate the distance between a sensor node and receiver with an antenna which can accurately measure the signal strength. It is based on a propagation signal model. After defining the transmitted signal power, antenna gained power and effects of different source of propagation error make possibility for localization. The relation between signal strength and distance is $(Signalstrength \propto 1/d^2)$. RSSI: is a measurement to show the condition of received signal strength in the anchor nodes and it is used in most of the wireless communication standard [30]. Theoretically, RSSI is a function of distance, affected by environment. In the RSSI techniques, the unknown sensor node broadcast frames to the other sensors in the communication area and then the distance is calculated based on received RSSI values. The relationship between the distance and the value of RSSI is regressive so that more the distance between unknown node and anchor increases indicates less the value of the RSSI will decrease in Eq. (2.1).

$$P_r(d) = P_t + G_t + G_r + 20\log_{10}(\frac{\lambda}{4\pi D}) \tag{2.1}$$

In Eq. 2.1, P_t and G_t denote transmission power of antenna and antenna gain of transmitting signal, respectively in dBm or dB. P_r and G_r denote reception power of antenna and antenna gain of receiving signal, respectively in dBm or dB. d is the distance between transmitting and receiving antennas and λ is signal wavelength. In real environment, the RSSI-based localization techniques do not indicate very accurate result when using the antenna gains so that a path loss model is considered in Eq. (2.2), where $P_L(d)$ indicates the path loss of the receiving signal when the measuring distance is d [m]. δ is the random shadowing effect in dB, which may have a different value at each anchor point. β is the path loss exponent and its value is various in different environment in Table. 2.1 [31, 32].

$$P_L(d) = P_L(d_0) + 10\beta\log(\frac{d}{d_0}) + \delta \tag{2.2}$$

Table. 2.1: Path Loss Exponent

Environment	Path Loss Exponent
Free Space	2
Urban area cellular radio	2.7-3.5
In-building LOS	1.6-1.8
Obstructed in-building	4-6
Shadowed urban area	3-5

[40] presents the free space propagation model where the line of sight path is assumed without any obstacle, as shown in Eq. (2.3).

$$\frac{P_r}{P_t} = [\frac{\sqrt{G_t * G_r \lambda}}{4\pi d}]^2 \rightarrow P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2} \tag{2.3}$$

2.5 WMNs based on infrastructure mode

The WMNs based on the standard IEEE 802.11 infrastructure mode is a vital consideration of studies. Therefore, in this section, we focus on some related works that cover the standard IEEE 802.11 infrastructure mode assignment approaches. The approaches can be categorized into centralized and distributed.

We focus on [42–46], which presented experimental results on WMNs with IEEE 802.11 infrastructure mode. A prototype of meshcluster network architecture is implemented using multiple radios such as 802.11 and 802.16 communications and highlighted routing/monitoring of it [42]. [43] addresses client-side transparency characteristics in an mesh networking architecture named iMesh, in which APs not only build multi-hop interconnections between each other with wireless distribution system (WDS) links, but also provide seamless network connection to clients. [44] shows that the transmission range of single AP can be improved using a WDS technology. [45] dedicates a mobile ad-hoc Wi-Fi (MA-Fi) architecture comprising a two-tier hierarchy of router nodes (RONs) and STAs. RONs are responsible for assigning the AP mode and the STA mode to two virtual interfaces on the single physical radio interface. In the performance evaluation, MA-Fi outperforms ad-hoc mode communication and offers throughput comparable to Wi-Fi even over multiple hops. Nodesjoints [46] is formulated for tree-based MANET in IEEE 802.11 infrastructure mode. In [47], a station can connect to a software-based AP via Wi-Fi direct.

[48] considers communications in both infrastructure mode and ad-hoc mode. [50] assumes both Wi-Fi ad-hoc and Wi-Fi-Opp in static and mobile forms and compared their simulation

results. [49] aims to increase transmission speed for sharing information between nodes in an opportunistic infrastructure-based Wi-Fi networks. They showed the advantages of the proposed approach as comparing the Wi-Fi-Opp method. However, [48–50] are not available with disaster recovery system.

Previous studies not only discuss but also recommend various ways to build a robust city-wide WMN infrastructure by studying a broad range of WMN characteristics such as coverage, connectivity, planning, multipath effect, and interference. However, the biggest challenge pertaining to the Wi-Fi mesh network based on the IEEE 802.11 infrastructure mode is resolving impracticalities such as the lack of 802.11 control frames and connectivity availability to unlicensed mobile devices (e.g., smartphones, laptops, and so on).

For these reasons, we focus on the studies by [43] and [45], which present experimental results on IEEE 802.11 infrastructure mode-based WMNs.

In [51], a drone-based WMN has been designed and implemented to provide high speed Wi-Fi. The drone in AP mode can transmit video data with the rate of 80 Mbps at distance of 60 m.

[52] also designs 802.11 infrastructure based network architecture and combines a WDS to provide a connection between APs for peer-to-peer metropolitan medical response system (MMRS). It deploys and access mesh network where several APs make association each other using WDS and connect to their clients in STA mode using the standard 802.11b infrastructure mode. In performance evaluation, TCP data and UDP data are transmitted successfully between the clients placing at the distance of 1000 feet.

In [53], therefore, Tree-based disaster recovery access network is designed and implemented for reconfiguring disconnected links, where nodes have been equipped a virtual interface in AP mode based on the software-based access node (SAN). Windows-based laptops are used for the nodes. Experiment evaluation is performed three nodes $MN1$, $MN2$, and $MN3$ connected in a row and $MN1$ is used for a GW node to a real AP in a backbone network. Suppose that the link $MN1$-$MN2$ is failed, $MN2$ can make a new association with the real AP as updating its connectivity status table where its neighbor information is in. Round trip time and packet loss have been estimated.

In addition, in [54], MANET routers are designed and implemented for an emergency fire response system working in a disaster system. In the disaster system, a radio system provides connectivity between base stations (BSs). Each BS has two wireless interfaces, placed on a fire engine. One interface works in AP mode and another works in STA mode. To evaluate the system performance, nine fire engines equipped with the BS transmitted TCP data each other and to two WINDS satellite stations successfully.

[58] proposes a route reconstruction method with spare APs. It is based on a reasonable idea

according to interviews with firefighters and civil servants.

Although past research revealed the many advantages of the WMN network infrastructure with regard to the capabilities of the 802.11 infrastructure-mode, some vital capabilities of ad hoc mesh networking, such as dynamical self-forming and self-configuration, have not been implemented. Therefore, we propose practical implementation for self-reconstructing WMNs based on infrastructure mode using spare APs.

As we introduced above, some works construct WMNs with IEEE 802.11 infrastructure mode. However, they assign interface mode statistically. We try to assign interface mode dynamically in distributed manner after disaster to a physical interface of a mesh router.

3 Proposed Methods

3.1 Spare AP Placement Method

3.1.1 Overview

As we mentioned before, fault-tolerant communication infrastructures are essential in a disaster situation. But, the mesh network infrastructure can be destroyed, even if it has disaster resilient characteristics. Therefore, some mesh routers are going down and some routers may become isolated from the wired network even if they are active. To implement self-reconstruction capability of the mesh network has a high priority to facilitate effective and immediate disaster response, wherein additional equipments can be deployed for communication restoration. However, disaster communication systems, which aim at making self-restoration easy, pleasant, and efficient by solving the problems of the lack of their utilization in peacetime and the difficulty for a non-expert to manage them, have gain much attention of the world. Therefore, we have given a vital emphasis on the development of self-restoring and self-organizing WMN infrastructure that is able to work in both normal and disaster conditions, using the standard 802.11 infrastructure mode. Our goal is to identify a way to reconstruct the mesh network by adding the minimum number of spare APs to provide reachability of all the isolated routers to the wired network via a GW. Furthermore, we assume that only non-experienced public workers and firefighters should mainly work with wireless communication technologies.

Our proposed spare AP placement method is to determine one or more required spare AP locations to get reachable the isolated routers as possible as to the wired network. We also the following requirements/constraints with regard to mesh network recovery. (1) Spare APs and portable batteries are limited. (2) Firefighters and/or members of the self-defense forces surveying disaster-affected areas can identify locations for spare AP placements. (3) Public workers, who may not be well-versed with wireless communication technologies, can nonetheless install the spare AP(s). Considering these requirements/constraints, we propose a practical method to reconstruct the network infrastructure using spare APs, allowing the unreachable routers to restore their connections to the wired network easily. The main goal of the method is to collect radio wave signals from the mesh routers using smartphone application. Then, we estimate the

adequate locations of the spare APs and install them. Finally, the reconstruction is completed as all the isolated routers have become reachability to the wired network via the GW.

3.1.2 Assumed Network Model

In this section, we present the network model devised for this study. It consists of mesh routers equipped with two radio interfaces, which can connect to adjacent mesh routers using directional antenna with a beamwidth of 60°. Note that we assume the use of a kind of patch antenna due to cost constraints. Each interface supports the IEEE 802.11 infrastructure mode, and thus, it works in either the AP or the STA mode. While most mesh routers can be installed on traffic and street lights, a few of them can be installed in public facilities such as government offices, police stations, and hospitals, which are considered as gateways (GWs) for providing connectivity to the management server (MS) in the backbone network via wired connections, as shown in Figure 3.1.

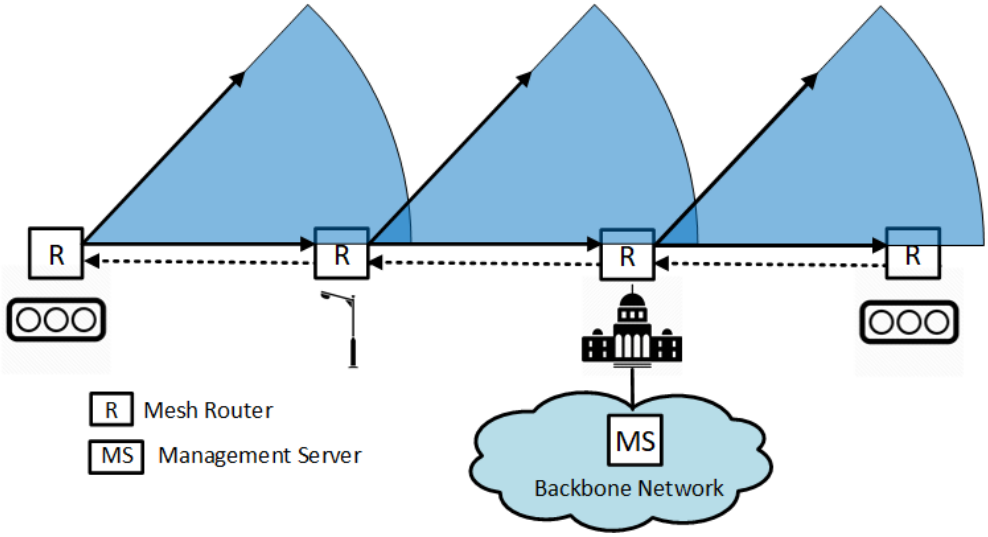


Figure. 3.1: System Architecture

More specifically, we show an assumed network model in Figure 3.2. Simply put, it is a standard IEEE 802.11 infrastructure mode based multi-hop wireless mesh network architecture consisting of a multi-channel WMN core. It is connected to a wired backbone network through a GW equipped with either wireless or wired network interface controllers [1, 11–13]. The mesh routers maintain themselves autonomously and provide an IEEE 802.11 infrastructure mode supported service for user terminals without any special configuration and softwares. The GW can transmit data packets between sets of mesh routers and the backbone network via wired network. All the mesh routers are placed along the road at a variety of distances from each other. Each of them has two radio interfaces equipped one or two directional antennas. The black dashed

arrows indicate the orientations of directional antennas at radio interfaces 1 and 2, respectively. In addition, the number of channels each router uses simultaneously is equal to the number of equipped radio interfaces. Consequently, the network, as a whole, uses three different channels configured in constant conditions. In normal situations, all the mesh routers are reachable to the backbone network via the GW.

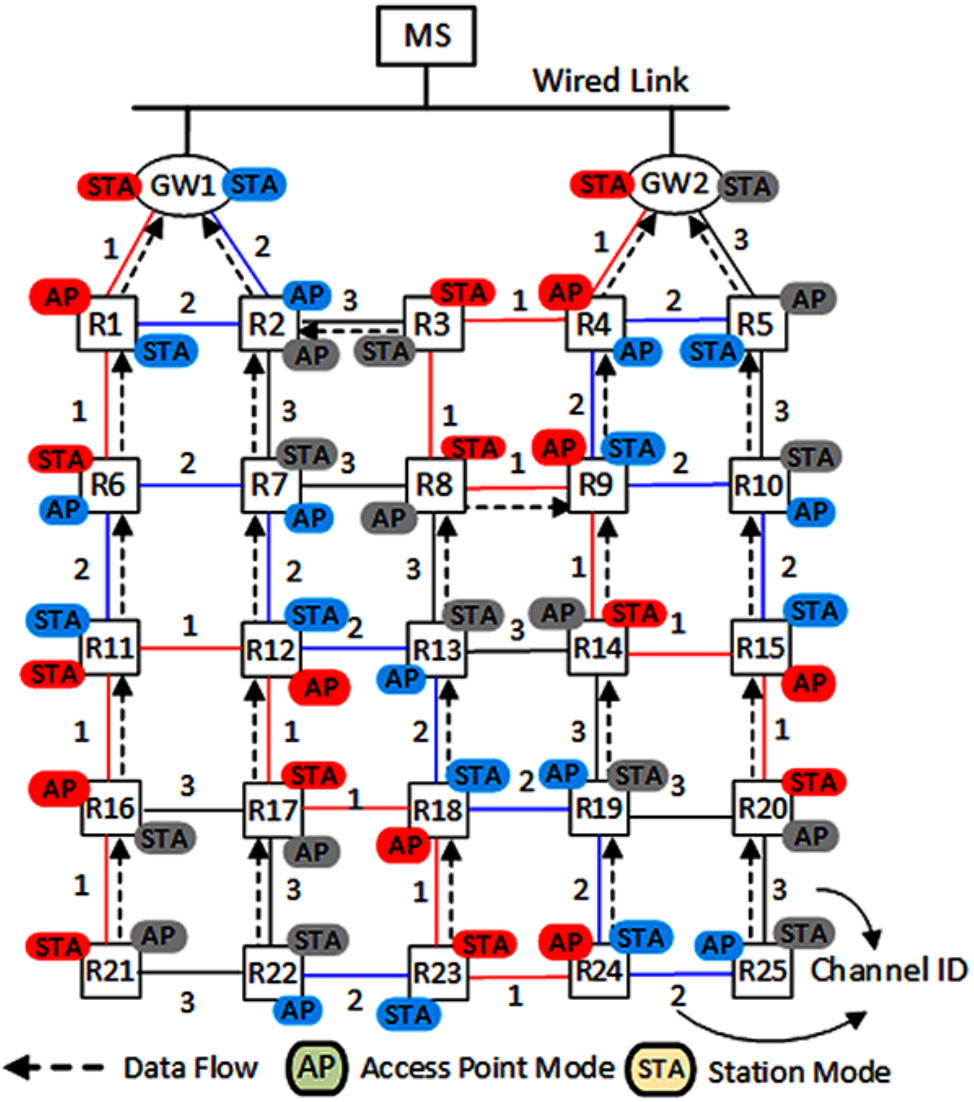


Figure. 3.2: Assumed Network Model

One or more feasible paths must be suggested for each mesh router to reach the GW. Weighted cumulative expected transmission time (WCETT) is proposed as a link metric for WMNs, which can be changed depending on the bandwidth, error rate, and channel diversity in a path [58]. Each mesh router selects a primary path with the lowest sum of the WCETT as its best route in its routing table, and others as feasible paths in the topology table. Thereafter, an interface

mode selection method should be performed automatically in order to assign either the AP or the STA mode on their interfaces and then feasible interfaces. Consequently, each neighbor table is updated with the selected mode information and the convergence process is completed.

3.1.3 Problem Definition

Now, we have an IEEE 802.11 infrastructure mode based mesh network modeled as a connected graph $G(V, E)$ comprising a set of wireless routers $V = \{v_0, v_1, ..., v_N\}$, and $E = \{e_{ij}\}$ is a set of links. An edge $e_{ij} \in E$ between nodes $v_i, v_j \in V$ exists if and only if they are in their transmission area each other. Serving GW can provide primary routes for a set of routers to reach the backbone network. Each node has r radio interfaces equipped with z directional antennas, which are used for establishing point-to-point communication with their neighbor nodes. The green and blue small circles indicate radio interface 1 and 2 respectively, whereas the black line between neighbor routers denotes orientated directional antennas at their radio interfaces. Moreover, for the assumed network infrastructure, each directional antenna has a fixed beamwidth θ. Then, a beam can be uniquely described by two parameters: its transmitting node and its orientation [45].

In the case of a disaster event, a large number of mesh routers stop functioning and/or some directional antennas lose their original angle. Thus, we consider restoring a 802.11 infrastructure mode based network where one or more mesh routers have lost their connectivity to the backbone network by using GWs. According to Figure 3.3, V is divided into three sets: C, U, and F. Routers in C can communicate with the backbone network. U consists of a set of unreachable mesh routers that have lost their primary routes to their serving GW. F is a set of failed nodes. U can be divided into some isolated parts (U_i).

We assume that local recovery cannot be performed to provide communication for an unreachable router to reach a connected area. In other words, one or more unreachable routers cannot be connected to a router in a connected area. Therefore, we aim to restore the 802.11 infrastructure mode based mesh network by establishing network connectivity from isolated mesh routers to their serving GW using the minimum number of spare APs. Consequently, our core problem lies in making all the nodes in the set of $V \setminus F \cup U \cup B$ ($= C \cup U \cup B$) reachable, where B denotes the set of spare APs.

To achieve this goal, we need to overcome the following two main challenges. One is to determine optimal locations where spare APs can be installed. The other is to reconstruct a fully converged 802.11 infrastructure mode based mesh network in which each mesh router has at least one primary route to a serving GW with the mode selection algorithm.

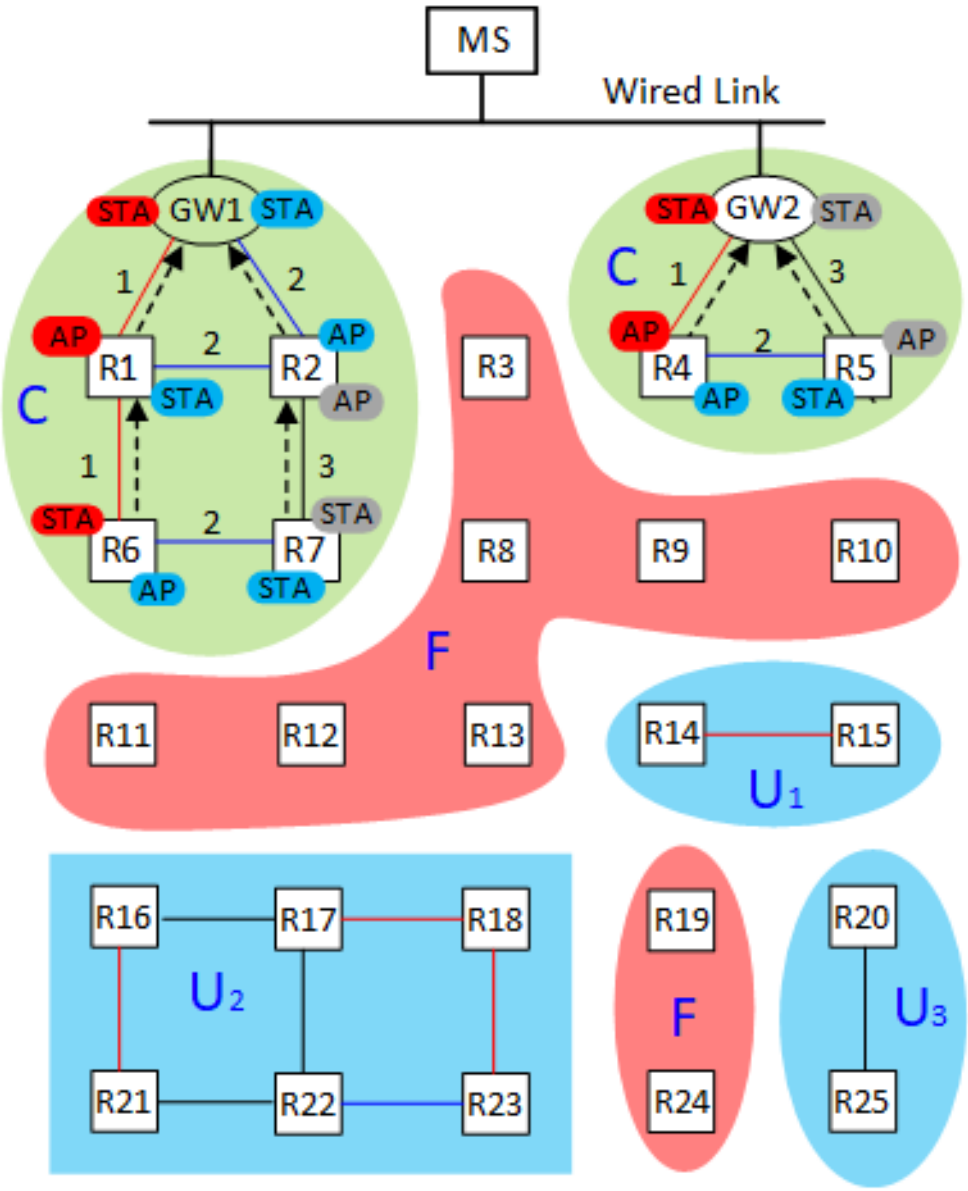


Figure. 3.3: Failure Situation

We also assume that the public workers are not experienced in wireless communication technology. Thus, they can only place a spare AP at the recommended location. This is a reasonable assumption as per the interviews conducted with public officers. Therefore, we do not use directional antennas with spare APs. In other words, a spare AP is not able to make neighboring with any other spare APs, since their interfaces should work in the AP mode.

Formally, each spare AP must connect to at least one router in C and at least one router in U. We aim to not only determine the adjacent nodes and their routing paths to the wired network, but also to assign either the AP mode or the STA mode, as far as possible, at their primary links. On the other hand, we do not focus on channel assignment. Thus, all interfaces are supposed to

use the same channel hereafter.

3.1.4 Existing Methods

First, we introduce the following parameters for implementing a localization system [38].

1. The objects in the localization system can be relative to each other or absolute to a reference point and coordinate system, respectively.
2. The localization can be processes periodically or specifically.
3. The initiator of the process can be target node or the anchor nodes.
4. The localization approach can be active (the surrounding objects determine the location of target node), passive (target node determines its location) or interactive (combination of the mentioned approaches).
5. The implementation algorithm can be two dimensional or more.
6. The localization system can be fast to track moving object just position static objects.
7. The anchors in the system can be tightly coupled (wired to the central unit) or loosely coupled (with wireless communication).
8. The system can be centralized (with a central unit for measurement and positioning) or decentralized (with considering the network traffic management).

In the RSSI-based localization, distance measurement is a crucial and first phase. As we mentioned before, path loss shadowing model is used as the mathematical algorithm for measuring distance. First, the path loss shadowing model is calculated using path loss exponent and reference loss (measured in 1 meter reference distance) are calculated, as shown in Eq. (3.1.1) and Eq. (3.1.2). After that the distance is calculated in Eq. (3.1.3) [39].

Path loss shadowing mode:

$$P_L(d) = P_L(d_0) + 10\beta \log(\frac{d}{d_0}) + X_\delta \tag{3.1.1}$$

Path loss exponent parameter when d_0 is 1m:

$$\beta = \frac{P_L(d) - P_L(d_0) - X_\delta}{10 \log(d)} \tag{3.1.2}$$

Distance:

$$d = 10^{\frac{P_L(d) - P_L(d_0) - X_\delta}{10\beta}} \tag{3.1.3}$$

In the second phase, the positioning algorithm is used to calculate the coordinates of the target node. For two dimensions localization the number of anchor nodes should be at least three anchors. In this method, the coordinates of the anchors (reference nodes) are denoted by $(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$ and then their distances from the target node $d_1, d_2, \cdots, d_3$ are calculated using Eq. (3.1). [41].

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = {d_1}^2 \\ (x - x_2)^2 + (y - y_2)^2 = {d_2}^2 \\ \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ (x - x_n)^2 + (y - y_n)^2 = {d_n}^2 \end{cases} \tag{3.1}$$

Then, Eq. (3.2) is subtracted from the Eq. (3.1).

$$\begin{cases} {x_1}^2 - {x_n}^2 - 2(x_1 - x_n)x + {y_1}^2 - {y_n}^2 - 2(y_1 - y_n)y = {d_1}^2 - {d_n}^2 \\ {x_1}^2 - {x_n}^2 - 2(x_1 - x_n)x + {y_1}^2 - {y_n}^2 - 2(y_1 - y_n)y = {d_1}^2 - {d_n}^2 \end{cases} \tag{3.2}$$

The above Eq. (3.2) can be demonstrated as $AX = b$ where A, b, and X are defined by the following Eq. (3.3), Eq. (3.4), and Eq. (3.5) respectively.

$$A = \begin{bmatrix} 2(x_1 - x_n) & 2(y_1 - y_n) \\ & \vdots \\ 2(x_{n-1} - x_n) & 2(y_{n-1} - y_n) \end{bmatrix} \tag{3.3}$$

$$b = \begin{bmatrix} {x_1}^2 - {x_n}^2 + {y_1}^2 - {y_n}^2 - {d_1}^2 + {d_n}^2 \\ \\ {x_{n-1}}^2 - {x_n}^2 + {y_{n-1}}^2 - {y_n}^2 - {d_{n-1}}^2 + {d_n}^2 \end{bmatrix} \vdots \tag{3.4}$$

$$X = \begin{bmatrix} x \\ y \end{bmatrix} \tag{3.5}$$

The coordinate of the target node is estimated for standard minimum mean square using Eq. (3.6).

$$\widehat{X} = (A^T A)^{-1} A^T b \tag{3.6}$$

3.1.5 Phases of Spare AP Placement Method

In this section, we propose a route reconstruction method for restoring Wi-Fi mesh networks. It has two phases; the connectivity restoration phase and the rerouting phase. Fault management approaches for WMNs are deployed in order to recover link or node failures [23–25]. Thus, we assume three major steps of the fault management approach such as fault detection, diagnosis and recovery in the proposed method. Connectivity restoration phase is responsible for fault detection and diagnosis. A spare AP is installed at an adequate point in the connectivity restoration phase. Finally, in the rerouting phase, one or more routes are reconstructed from isolated routers to the MS.

A. Connectivity Restoration Phase

In this subsection, we propose how to run RSSI-based ranging and localization algorithm. In the algorithm we propose, the place where RSSI information is collected is defined as an *a*nchor point. For node $v_i \in (C \cup U)$, several anchor points $a_{ix}(x = 1, 2, ...)$ are assumed to be obtained.

Based on the collected data, the MS executes an RSSI-based ranging and localization algorithm. Consequently, we estimate the transmission range of the routers in the first step and find overlapping transmission ranges between unreachable and reachable routers in order to determine adequate locations for spare APs in the second step.

Based on the collected data, we aim to estimate the transmission range of the isolated routers and to find overlapping transmission ranges between isolated and connected routers in order to determine adequate locations for spare APs. To achieve these objectives, we need to study wireless node positioning techniques based on RSSI information. In order to deal with the issues on discovering the location points to install spare APs, we should formulate a RSSI ranging and localization algorithm.

The RSSI ranging and localization algorithm uses a database which mainly contains RSSI values of the unreachable routers and their known location information. Eq. (1) shows a path loss model. In this equation, $P_L(d)$ indicates the path loss of the receiving signal when the measuring distance is d [m]. It indicates the absolute power in dBm. d_0 [m] is the reference distance at which the reference loss is calculated. β is the path loss exponent. In a free space environment, β is set at 2 [31–33, 40]. δ is the random shadowing effect in dB, which may have a different value at each anchor point.

$$P_L(d) = P_L(d_0) + 10\beta \log(\frac{d}{d_0}) + \delta \tag{1}$$

Eq.(2) shows the manner of calculation for the path loss for anchor point x.

$$P_L(d_x) = P_L(d_0) + 10\beta \log(\frac{d_x}{d_0}) + \delta_x \tag{2}$$

In Eq.(3), P_x and P_t refer to the signal strength at anchor point x and the signal transmission power, respectively.

$$P_t - P_L(d_x) = P_x \tag{3}$$

Using the measured RSSI values of each anchor point and P_t (which is assumed to be given), $P_L(d_x)$ can be calculated. As a result, δ_x can be estimated using Eq. (4).

$$P_L(d_x) - P_L(d_0) - 10\beta \log(\frac{d_x}{d_0}) = \delta_x \tag{4}$$

Eq. (5) shows the path loss at the maximum transmission range, denoted as $P_L(d_{max})$ in case P_{min} denotes the minimum signal strength for reliable packet delivery, which can be considered to be constant.

$$P_t - P_L(d_{max}) = P_{min} \tag{5}$$

Consequently, we can also calculate d_{max_x}, as follows.

$$d_{max_x} = \frac{10^{(\frac{P_L(dmax) - P_L(d_0) - \delta_x}{10\beta})}}{d_0} \tag{6}$$

Figure 3.4 demonstrates the manner of estimation of the sector area of a radio interface r of a router v_i using the collected RSSI values, denoted as $\omega_x^{i_r}$ and measured at anchor point x. Since the coordinates of locations (X_i, Y_i) and (X_x, Y_x) of router v_i and anchor point x are given, the distance between them is defined as Eq.(7), denoted by d_{ix}.

$$d_{ix} = \sqrt{(X_i - X_x)^2 + (Y_i - Y_x)^2} \tag{7}$$

Consequently, we compute the coordinates of locations (X_M, Y_M) of a point denoted by $M_x^{i_r}$ at $d_{max_{ix}}$ using Eq.(8).

$$X_M, Y_M = \begin{cases} {d^2}_{max_{ix}} = (X_M - X_i)^2 + (Y_M - Y_i)^2 \\ (d_{max_{ix}} - d_{ix})^2 = (X_M - X_x)^2 + (Y_M - Y_x)^2 \end{cases} \tag{8}$$

Then, we create a sector area with double θ degree, containing two endpoints $R_x^{i_r}$ and $Q_x^{i_r}$ as well as the interior point $M_x^{i_r}$. Furthermore, the coordinates of locations (X_R, Y_R) of

the endpoint $R_x^{i_r}$ and the coordinates of locations (X_Q, Y_Q) of another endpoint $Q_x^{i_r}$ are calculated using Eq. (9).

$$\begin{cases} X_R = \cos(\theta) * d_{max_{ix}} + X_i; \\ Y_R = \sin(\theta) * d_{max_{ix}} + Y_i; \\ X_Q = \cos(-\theta) * d_{max_{ix}} + X_i; \\ Y_Q = \sin(-\theta) * d_{max_{ix}} + Y_i; \end{cases} \tag{9}$$

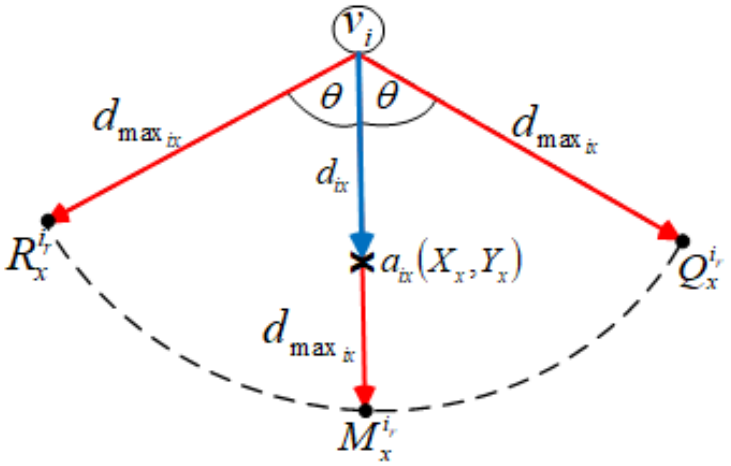


Figure. 3.4: Transmission Range Estimation procedure

However, the transmission range is likely to be smaller due to some obstacles. Therefore, we propose estimating the real transmission range using several anchor points as follows. Figure 3.5 shows four anchor points for router v_1.

For each anchor point, σ_x can be obtained using Eq. (4). As a result, the interior point $M_x^{1_0}$ as well as the endpoints in terms of $R_x^{1_0}$ and $Q_x^{1_0}$ for each anchor point x of the router v_1 are also computed as shown in Figure 3.4. By connecting all the interior points and two endpoints, the transmission range, denoted as T^{1_0} separated by blue solid lines for the radio interface 0 of router v_1, can be obtained.

As a result of the ranging step, the transmission ranges, denoted by T^{0_0} and T^{2_0}, are also obtained in the same manner for the radio interface 0 of both routers v_0 and v_2. In the positioning step, the area, denoted by S, which is covered by the transmission ranges of the maximum number of routers is selected as the adequate location for setting a spare AP. Note that at least one of the routers must be in C.

Algorithm 1 is the pseudo code of the RSSI ranging and localization algorithm. Let U and C denote the set of isolated routers that are already in the operation and the set of remaining

routers, respectively. Initially, U contains an isolated router v_i discovered at the first xth anchor point a_{ix}. We consider some constant parameters such as P_t signal transmission power , P_{min} minimum signal strength for reliable packet delivery , δ_x random shadowing effect, z directional antennas, and θ beamwidth. In the ranging step, to estimate transmission range of a router with an anchor point , firstly, we compute sector areas using its RSSI values measured at each anchor point and then define the intersection of its all the sector areas (lines 2-11). In the positioning step, we define all possible isolated and connected routers in neighbor relation and their overlapping transmission ranges are considered as adequate points for spare APs (line 12-22).

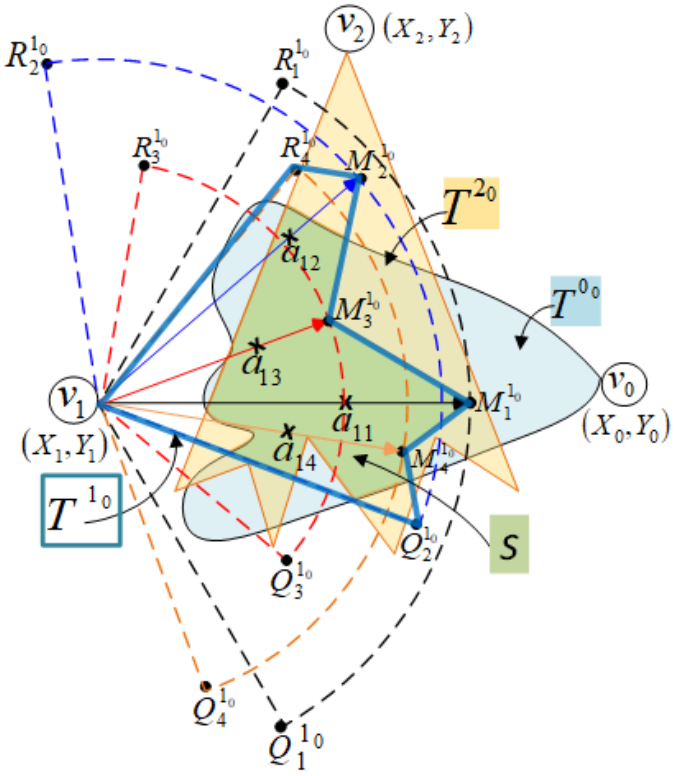


Figure. 3.5: Discovering Spare AP location Procedure in Disaster Situation

B. Rerouting Phase

We first discuss rerouting procedure. Note that before rerouting, first of all, while public workers working in the disaster area are going along tracking routes, an application software on their smartphones automatically measure RSSI levels of all the unreachable routers at anchor points [35]. For example, as shown in Figure 3.6(a), receiving all the information from the public workers, MS can estimate the communication range of each router. since some routers are supposed to get down and $R13$ has been changed its antenna orientation, overlapping communication ranges of the unreachable routers and the closest routers is de-

Algorithm 1: RSSI-based ranging and localization algorithm

Result: Define adequate locations for spare APs

Input : The set of routers *C*, *F*, and *U*

$V = \{v_0, v_1, ...v_N\}$ *i=[0;N]* $//the\ set\ of\ all\ the\ routers$

$a_{ix}(x = 1, 2, ...)$ $//the\ set\ of\ AnchorPoints$

$P_t, P_{min}, \delta_x, \theta, z$ $//constant\ parameters$

Output: S $//Adequate\ areas\ of\ spare\ APs$

$U \leftarrow V$ - C - F $//All\ isolated\ routers\ including\ down\ routers$

`/* Step1.Ranging */`

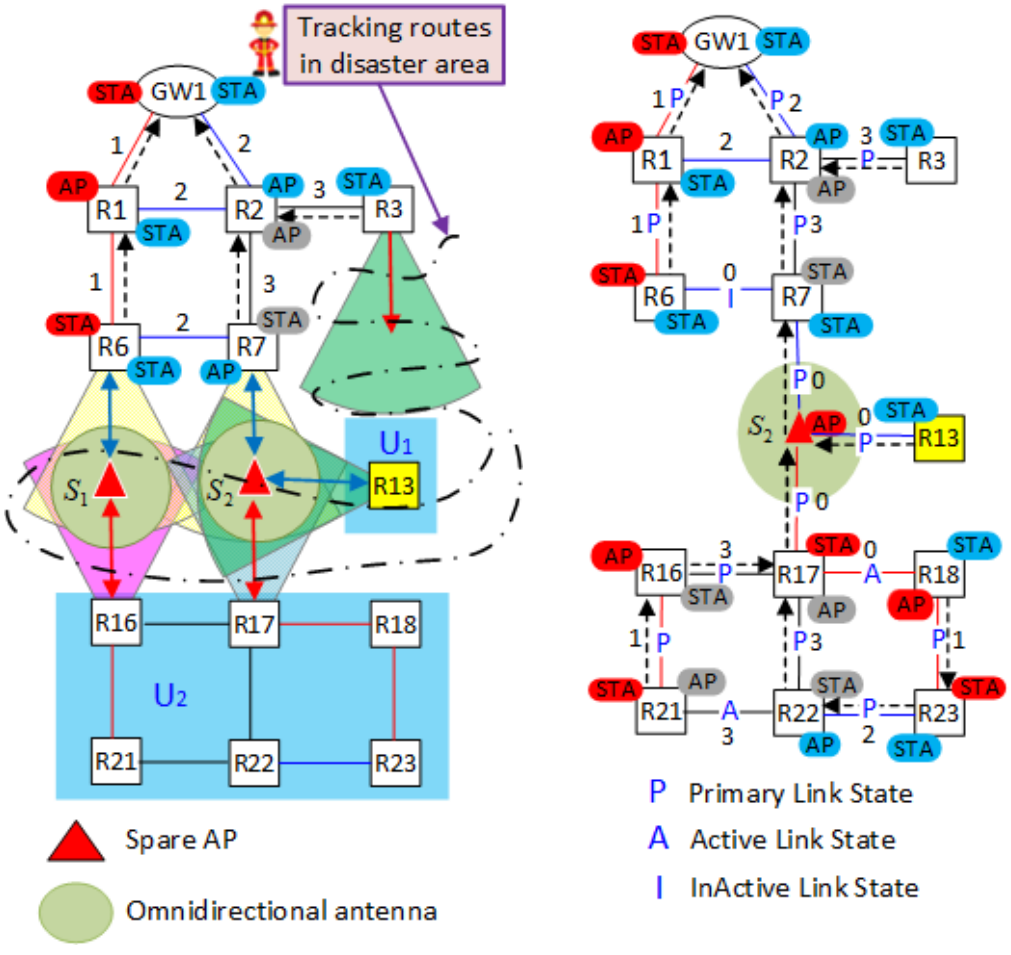
while $a_{ix} \neq \emptyset$ **do**
  for *each* a_{ix} **do**
    if $v_i \notin C$ $//the\ isolated\ routers$
    then
      $d_{ix} \leftarrow AnchorDistance(a_x(X_x, Y_x), v_i(X_i, Y_i))$ $//Eq.\ 7$
      $d_{max_{ix}} \leftarrow MaximumDistance(P_t, P_{min}, \delta_x)$ $//Eq.\ 4, 5, 6$
      $T^{i^z} \leftarrow TransmissionRange(d_{max_{ix}}, \theta)$ $//Eq.\ 9$
    end
  end
end

`/* Step2.Positioning */`

for $v_i \in U$ **do**
  for $v_{i-i} \in U$ **do**
    for $v_j \in C$ **do**
      for $v_{j-1} \in C$ **do**
        if $d_{iji-1j-1} < 2 * d_{max}$ **then**
          $S \leftarrow OverlappingTransmissionRange(T^{i^z} \cap T^{i-1^z} \cap T^{j^z} \cap T^{j-1^z})$;
        end
      end
    end
  end
end

rived as candidate locations for spare APs. Before installing spare APs, rerouting technique should be simulated for each candidate location area S_1 and S_2 on MS, respectively. In this demonstration, spare APs at S_1 location only provide route for the unreachable routers in the area U and spare AP at S_2 location can provide routes for all the unreachable routers in both U_1 and U_2.

In Figure 3.6(b), when the installed spare AP is turned on, it must first discover a route to a proper GW. For this purpose, it performs active scanning on all channels to maintain a neighbor and routing table. In this case, the spare AP is considered as a root, since it has a single radio interface with an omnidirectional antenna (denoted as the green circle). In addition, it must work in the AP mode. After the scanning process, if the spare AP first discovers its parent node (such as R7) as its neighbor, as shown in Figure 3.6(b), the link between them is considered as a primary link.



(a) Initial Routing (b) Rerouting

Figure. 3.6: Route Reconstruction procedure in Disaster situation

The best route is a chain of the primary links for each router. In addition, if there is no

neighboring connection with any node, an router takes STA mode and Active state by default. Simply, we consider a link cost as a same static value of WCETT. Each mesh router selects a primary path with the lowest WCETT as its best route in its routing table and others as feasible paths in the topology table. Note that each link must have one of the following statuses: Primary, Active, or Inactive. Both the Primary and Active statuses indicate that this link is available. The Primary and Active links are used for the main and backup routes, respectively. Inactive indicates that this link is not available since the connected interfaces works in the same mode [58].

The main constraint is that the router R7 cannot allow its parent route or feasible route to be used for connection with the spare AP via its interface. R7, R13, and R17 must set the STA mode at their interfaces to connect to the spare AP, and then, their channels must be assigned. After R17 becomes reachable, it is able to receive primary route requests from other unreachable routers (such as R16, R18, and R22) in a neighbor relationship. The main constraint is that a router must first create a neighboring connection with its parent node, and then, with its child nodes. We consider nodeID for each node. Thus, a router with the lowest node ID takes AP mode at its radio interface. Since R17 provides a primary route for two neighbors (R16 and R22) connected via the same interface, both of R16 and R22, will take the STA mode. Thus, both will become reachable nodes. R21 can be recommended a primary route with the same WCETT by either R16 or R22 and will choose R16 with the lower nodeID as its parent node. R16 and R21 have no child node at the interface, and thus, the parent node R16 can take the AP mode. However, the link between R21 and R22 is not used as the best route for both, and thus, the status is Active. Thereafter, since R17 has already used the interface connected to R18 for its own primary route to the spare AP, R18 will connect to the backbone network through R23. Finally, the rerouting process is complete when all the unreachable routers have their own primary route to the MS.

Here, we demonstrate how the proposed method works with partial mesh network topology in Fig. 3.7.

There are multiple GWs denoted by GW1 and GW2, which can transmit data packets between set of routers and MS. Each router has two interfaces and each interface has one or two directional antennas. Red and blue solid arrows indicate orientations of directional antennas at radio interface 1 and 2, respectively. Dashed lines denote data flows from router to GW so that we can see that the network topology has been converged.

Suppose that $R2$, $R6$, and $R8$ have failed by a big earthquake so that $R7$, $R11$, $R12$, and $R13$ have lost their connection to their serving GW, as shown in Fig. 3.8.

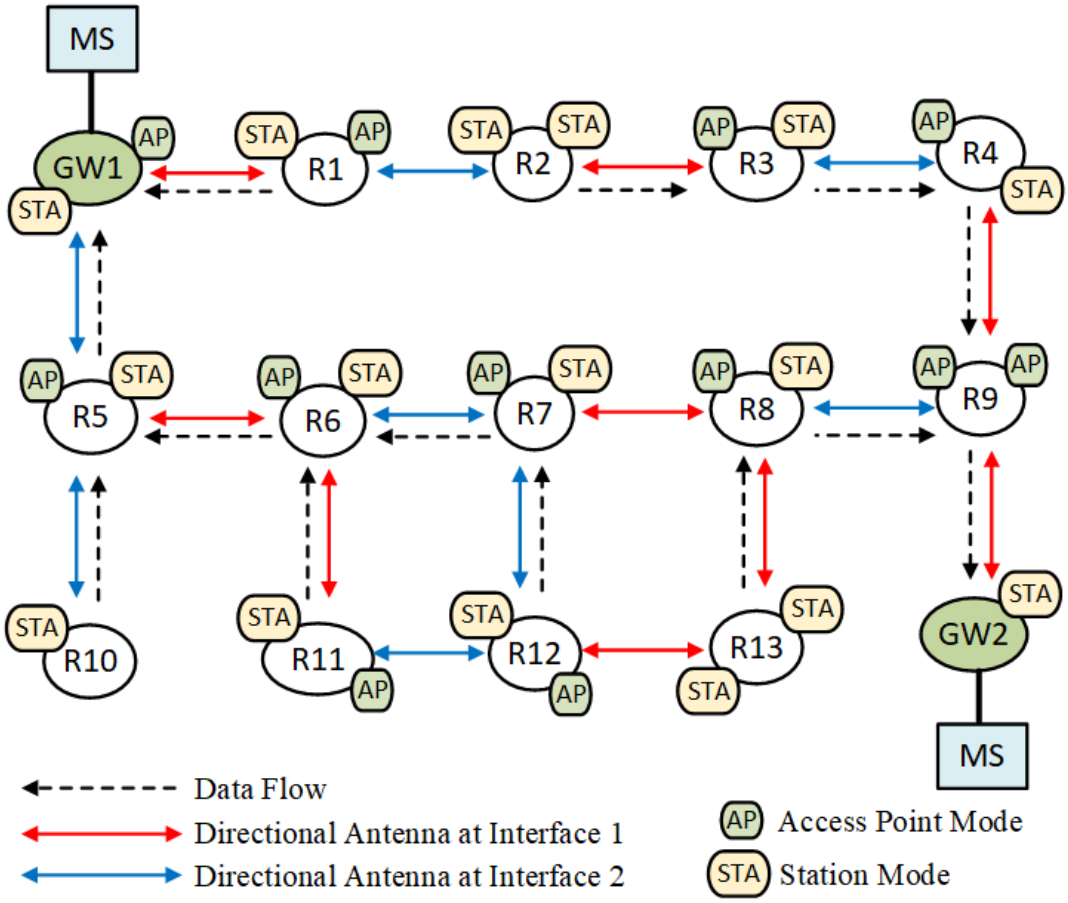


Figure. 3.7: Example of Partial Mesh Network

In this case, first of all, while public workers working in the disaster area are going along tracking routes, an application software on their smartphones automatically measure RSSI levels of all the isolated routers at anchor points [33]. Receiving all the information from the public workers, MS can estimate the communication range of each router. Next, overlapping communication ranges of the isolated routers and the closest routers is derived as candidate locations for spare APs. Before installing spare APs, rerouting technique should be simulated for each candidate location A, B, and C on MS, respectively. In this demonstration, spare APs at B and C locations only provide route for $R7$ and $R13$ respectively and spare AP at A location can provide routes for all the isolated routers.

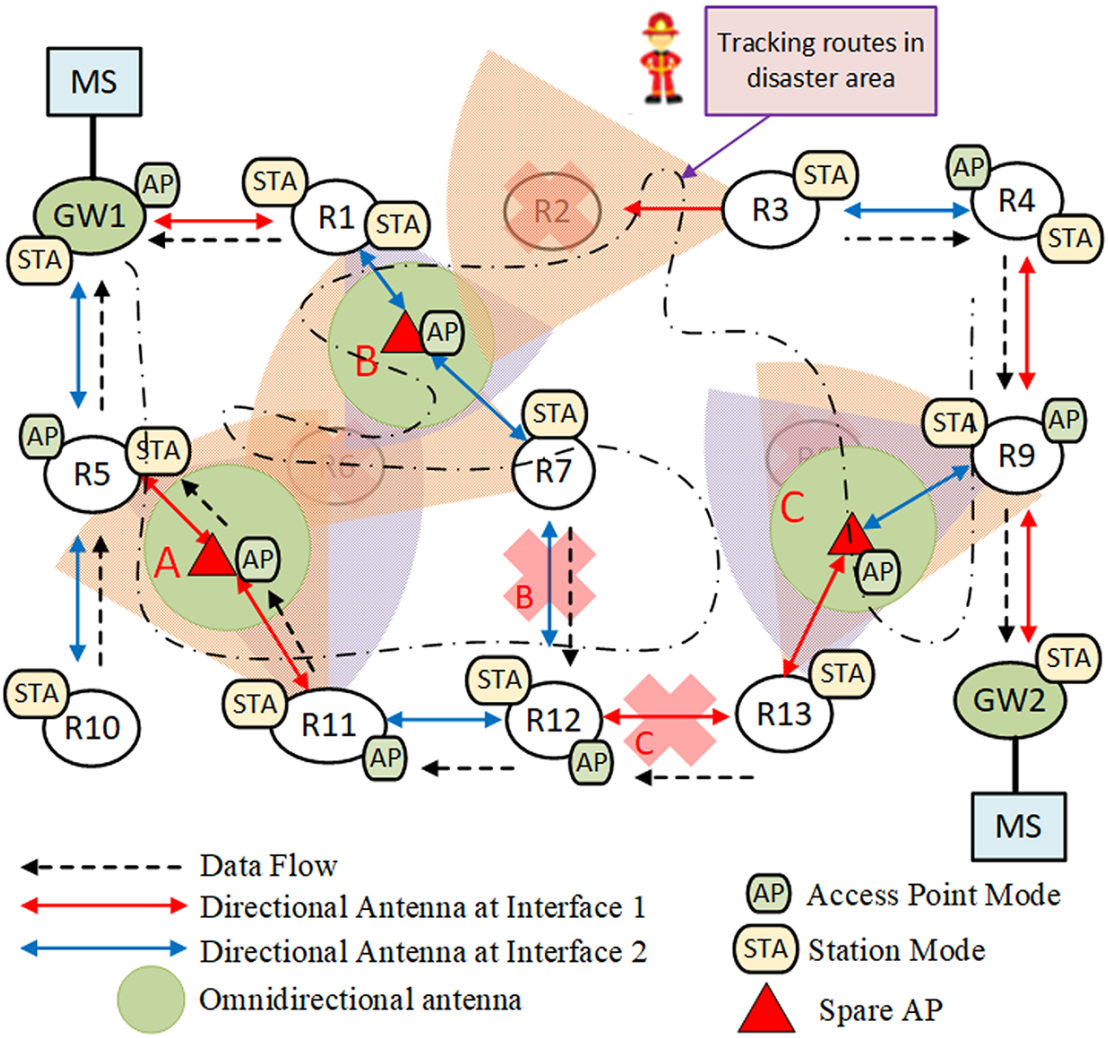


Figure. 3.8: Execution Example of Route Reconstruction Procedure

3.1.6 Performance Evaluation

In this section, we evaluate the performance of the proposed methods via simulation experiments using ns-3.26 [61].

A. Full Mesh Network

The WMN topology in Figure 3.2 was built as a simulation model. All the nodes had directional antennas oriented to their neighbor nodes. In normal situations, all the routers are reachable to the backbone network via the their serving gateway GW. The evaluation parameters in the simulation environment is shown in Table. 3.1.

Table. 3.1: Evaluation Parameter

Parameter	**Value**
Signal transmission power	16 dBm
Total number of routers	25
Propagation model	Log Distance Propagation Loss Model
MAC interface	802.11g
Wi-Fi type	Infrastructure mode
Gain of directional antenna	9 dBi
Gain of omni-directional antenna	2 dBi
Transport Layer Protocol	TCP
Application Protocol	FTP

To create a disaster situation, n random routers were assumed to be down. Also, another n routers' antenna orientations changed randomly. Their interface numbers were selected randomly. We changed n from 2 to 5, and tested 100 different failure cases for each n.

Figure 3.9 shows successful recovery probability using the proposed route reconstruction method. "Recover" means that all the active routers became reachable to the MS after the reconstruction process. Given that at most four routers remained in the failed state, the proposed method could recover routers with a high enough probability. Even if five routers went down and the antenna orientations of another five routers changed, in about 78% of the cases, one or two spare APs could restore the whole reachability. Consequently, the proposed method is practical.

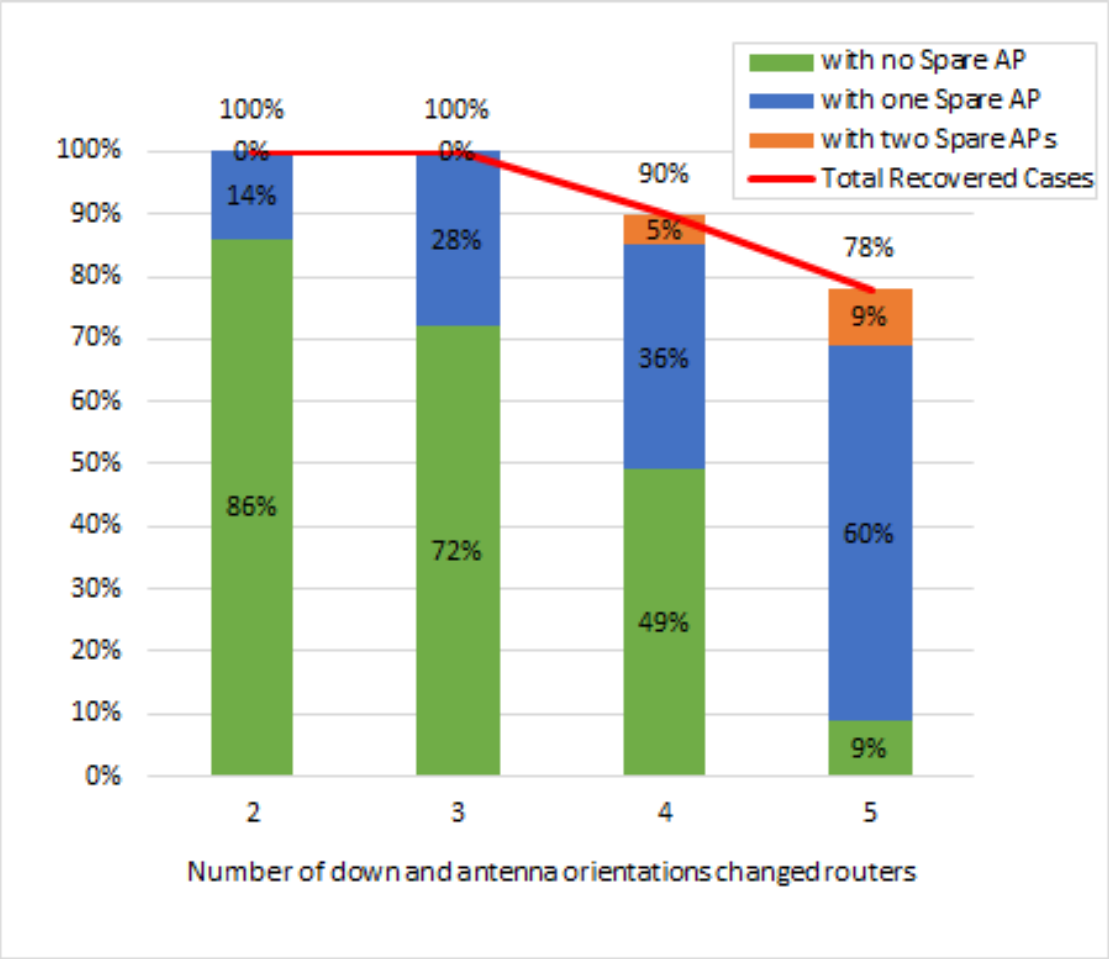


Figure. 3.9: Successful Recovery Probability

B. Partial Mesh Network

The WMN topology in Figure 3.7 was built as a simulation model. The evaluation parameters in the simulation environment is shown in Table. 3.2.

Table. 3.2: Evaluation Parameter

Parameter	**Value**
Signal transmission power	16 dBm
Total number of routers	13
Propagation model	Log Distance Propagation Loss Model
MAC interface	802.11g
Wi-Fi type	Infrastructure mode
Gain of directional antenna	9 dBi
Gain of omni-directional antenna	2 dBi
Transport Layer Protocol	UDP
Application Protocol	OnOffApp

All the routers were placed at the same distance (220m) from each other and had oriented directional antennas to their neighbor nodes. In normal situation, all the routers were reachable to the MS. To create disaster situation, n routers were randomly down. We changed n from 2 to 5 and made 100 different failure cases for each n. To recover any failure situations, only one spare AP was used.

In Fig. 3.10, successful recover probability of the partial mesh network by the proposed route reconstruction method compared with that of the full mesh network recovered by only one spare AP. Note that one condition such as n down routers was used for the partial mesh network. With 4 or less failed routers, the proposed method achieves to recover with enough high probability. Even if 5 routers went down, in about 68% cases, just one spare AP restores the whole reachability. Consequently, the proposed method is practical. Although the full mesh network considered two conditions such as n down routers and another n antenna orientations changed router to create disaster situation for case, its successful recover probability was higher than the partial mesh network's. Therefore, full mesh network is more suitable in disaster situation.

Fig. 3.11 shows the summary why the reachability has not been recovered for total scenarios in the partial mesh topology. In most cases, the reason is the lack of spare AP. Other few cases are related to the mode selection mechanism. For example, when $R5$ and $R8$ are down, $R6$, $R7$, $R10$, $R11$, $R12$ nodes are considered unreachable. Suppose that spare

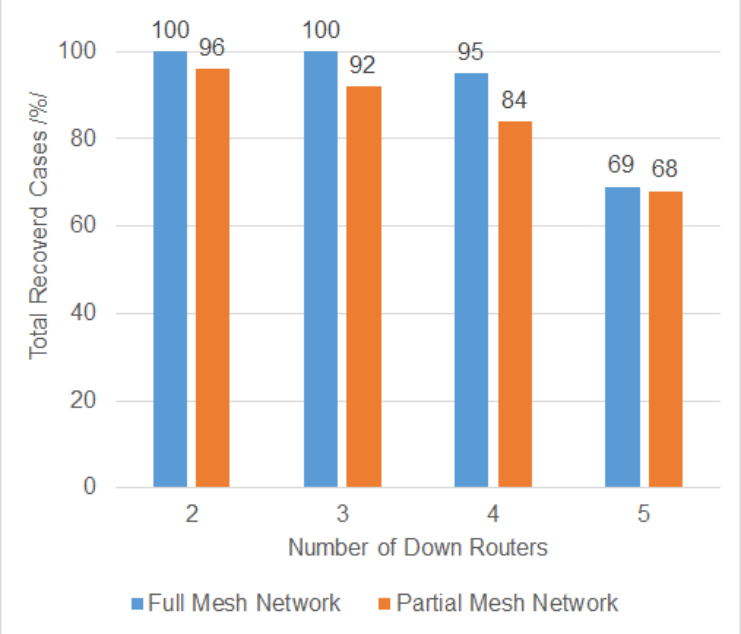


Figure. 3.10: Comparison of Recover Probability

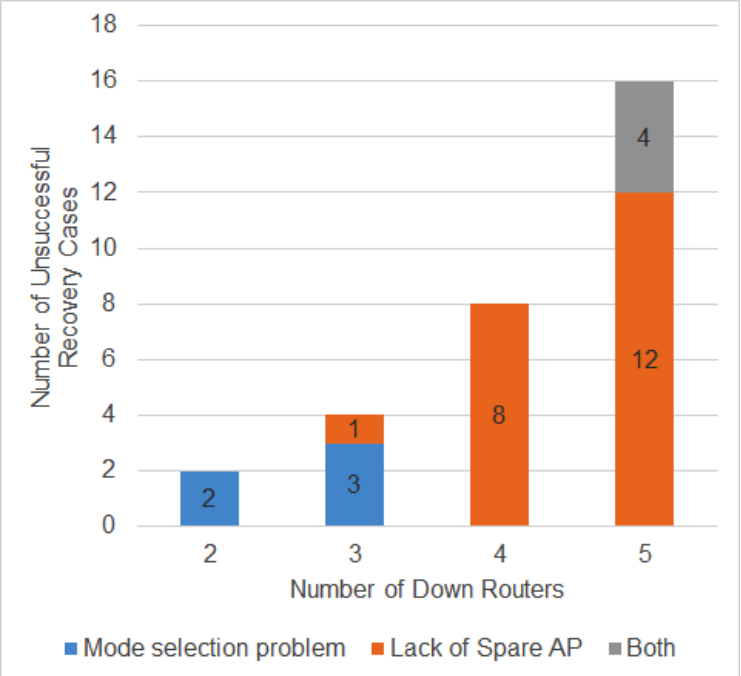


Figure. 3.11: Unsuccessful Recovery Cases for Each Scenario in Partial Mesh Network

AP can be installed overlapping range of GW1, $R6$ and $R10$, $R6$ must change mode to AP on its interface 1 so that $R11$ does not have its primary route. Even $R12$ is not able to change the STA mode on its interface 2, because it is used for its primary route. To avoid the mode selection problem, any router has to use different interface to communicate with

its different neighbors.

3.2 Interface Mode Assignment Method

3.2.1 Overview

Next, we elaborate the interface mode assignment method to deal with another issue that which infrastructure mode is suitable for each interface of isolated mesh router to achieve a full converged and recovered network. This method should be executed for each isolated router in decentralized manner after a spare AP has been installed. The isolated router can either assign an AP mode or a STA mode to its interface. Moreover, the proposed method can give each isolated router the opportunity to decide which mode in distributed manner. It comprises of two phases; (1) Tentative routing phase, (2) Interface mode selection phase. In the tentative routing phase, each isolated router needs to discover a next hop router reachable to the wired network in a distributed manner. In the interface mode selection phase, each isolated router can automatically form its neighbor connection in an infrastructure mode along its route to the GW. Consequently, the mesh network is fully reconstructed when the interface mode selection phase is complete.

3.2.2 Assumed Network Model

This section presents an assumed network model. It is a multi-hop wireless mesh network architecture based on IEEE 802.11 infrastructure-mode. It is connected to a wired backbone network through a GW which has been equipped with both of wireless and wired network interface controllers.

This network is expressed by an undirected graph $G(V, E)$. V is a set of routers including GW. A router v_i has one or more interface cards $c_{i,a}$. E is a set of links. Note here that, in this thesis, a link $e(c_{i,a}, c_{j,b})$ shows a possible association. In other words, it means that interfaces $c_{i,a}$ and $c_{j,b}$ are in a radio communication area, but it does not necessarily mean an association is established between them. We define three types of links; Primary, Feasible, and Unavailable. A *primary* link is actively used for communications. A *feasible* link is between an interface working as AP mode and the other interface in STA mode, but an association is not established between them. It is not currently but possibly used for communications. In a typical case, the interface in STA mode has an association with another interface. An *unavailable* link is between the interfaces in the same mode.

As shown in Fig. 3.12, mesh routers are placed along a road. In a normal situation, all the mesh routers are reachable to the wired network via the GW. Each mesh router v_i has two interfaces and

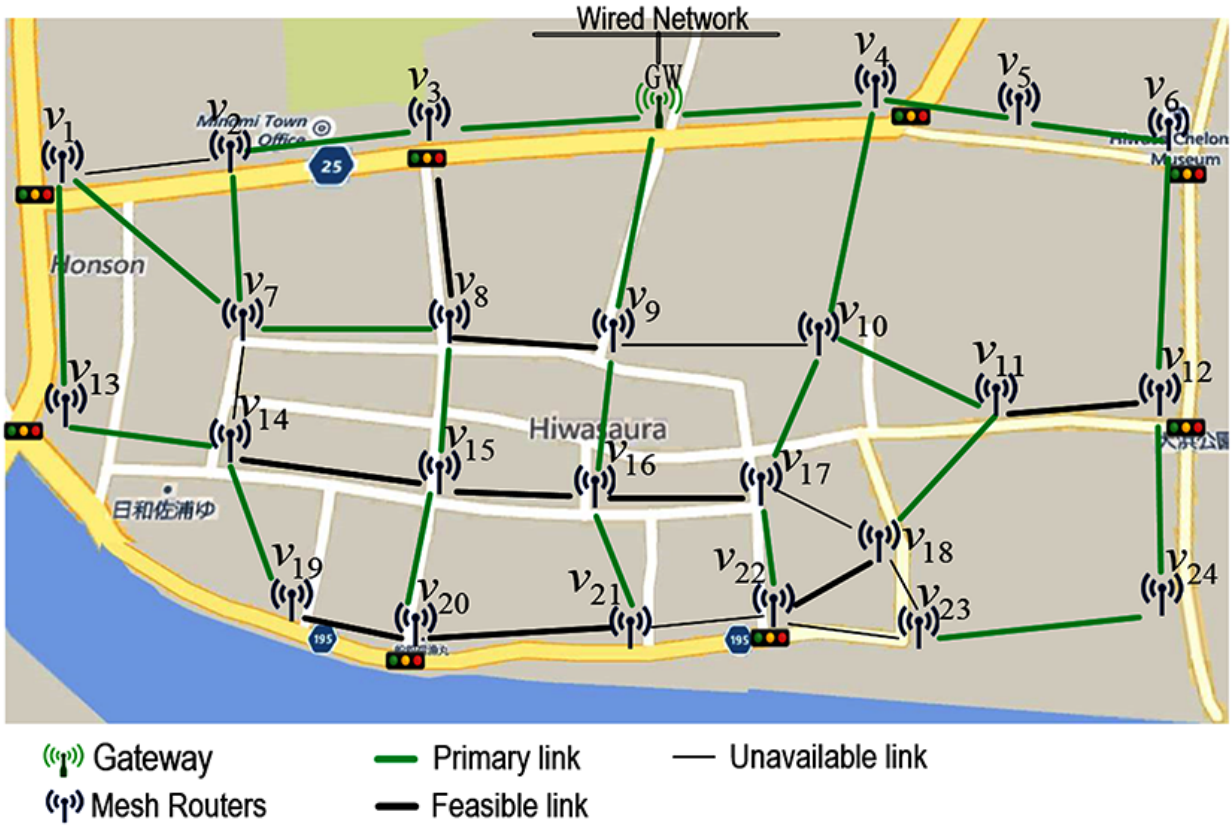


Figure. 3.12: Assumed Network Model

each interface equips two directional antennas. In Fig. 3.13, blue or red dough-nut shape indicates each interface and the direction of its directional antennas [58]. Each interface is equipped with one or two directional antennas with a fixed beamwidth θ.

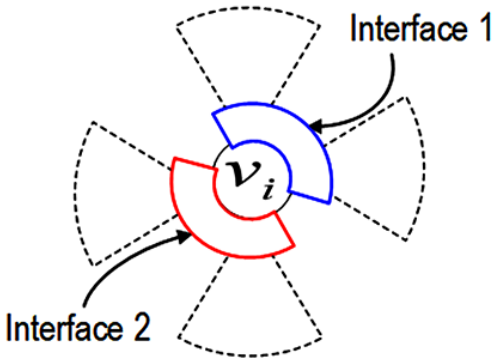


Figure. 3.13: Interface Structure of Mesh Router

Fig. 3.14 illustrates a failure situation where some routers are supposed to be failed and the

mesh network is isolated, when a large-scale disaster occurs.

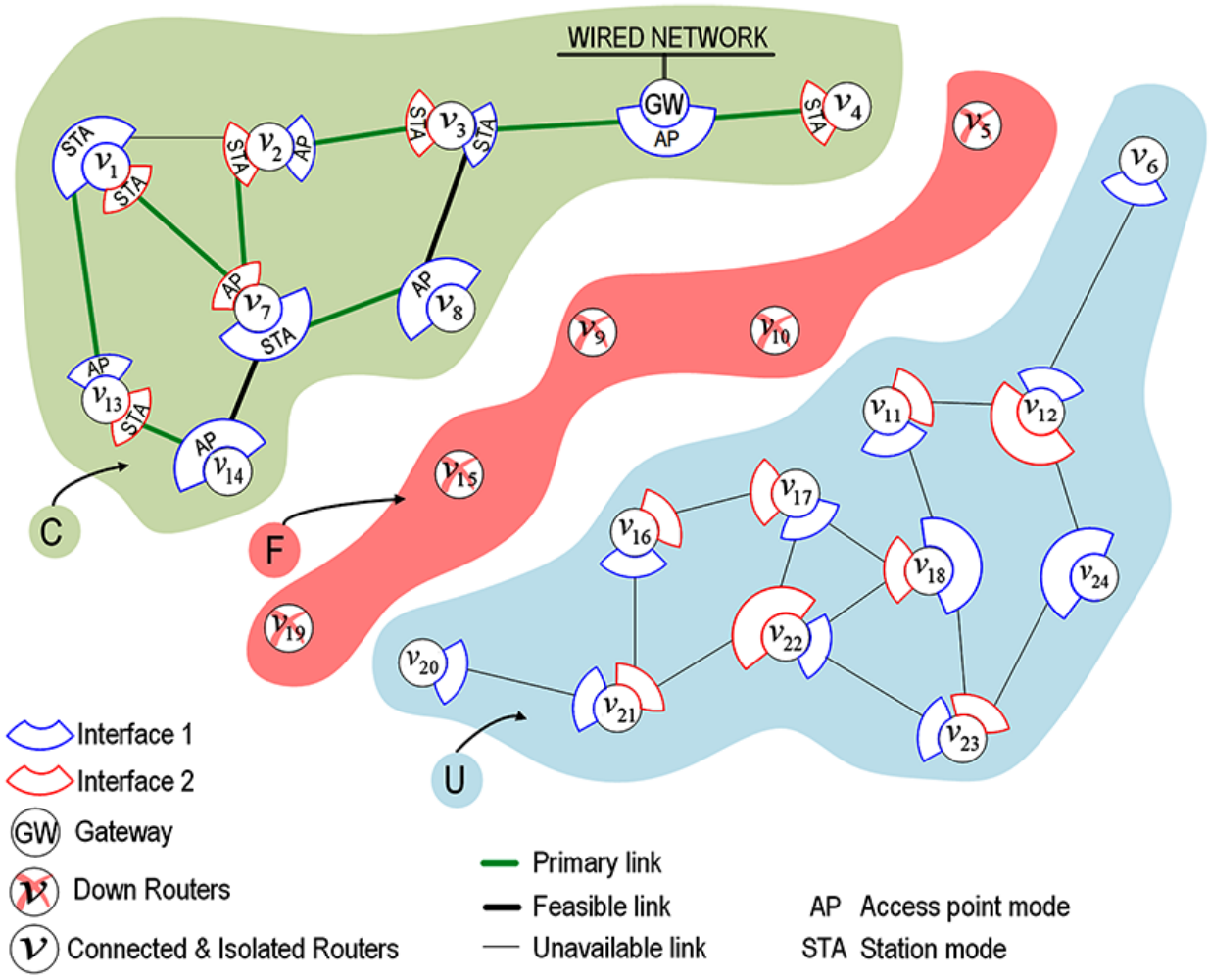


Figure. 3.14: Failure Situation

We suppose that v_5, v_9, v_{10}, v_{15}, and v_{19} have failed by a disaster thereby v_6, v_{11}, v_{12}, v_{16}, v_{17}, v_{18}, and v_{20} to v_{24} have lost their connection to their serving GW. Consequently, V is divided into three different sets such as connected routers C, isolated routers U, and failed routers F.

To overcome this situation, we proposed an algorithm to find the adequate location of spare AP equipped with an omnidirectional antenna. In Fig. 3.15, we assume that a spare AP denoted by v_s has been installed. The spare AP v_s lies in the transmission ranges of either the connected or the isolated routers and it must connect to at least one router in C and at least one router in U in order to play a role of bridge. All the routers in the set of $V \setminus F \cup U \cup B$ $(= C \cup U \cup B)$ can be potentially reachable to the backbone network where v_s denotes the set of spare APs. For instance, in Fig. 3.15, all isolated routers can potentially be reachable to the GW via v_s establishing associations with router v_{14} in C and router v_{20} in U [58].

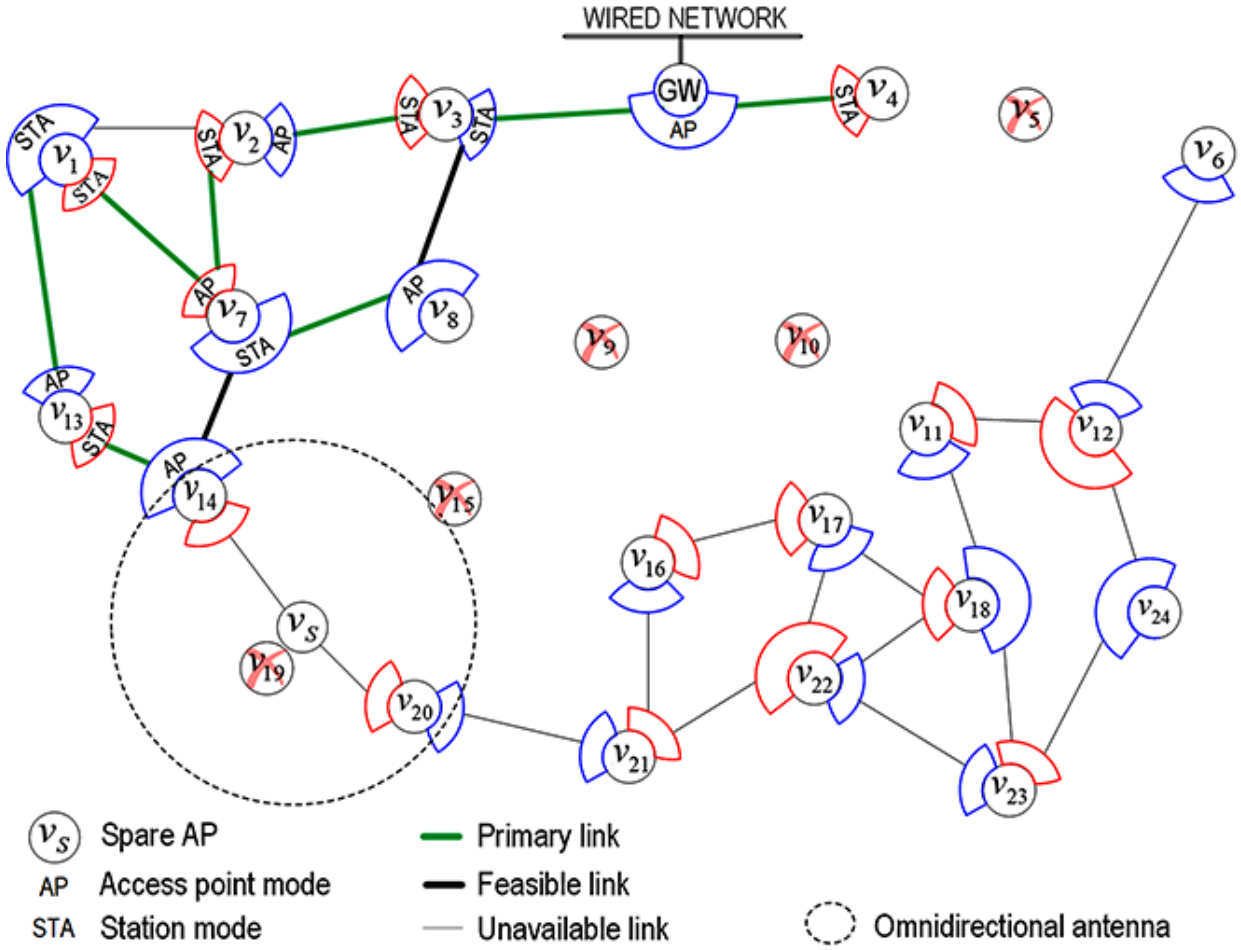


Figure. 3.15: Installation of Spare AP

Note here that, however, before making a path through the installed spare AP, adequate interface mode has to be assigned to establish an association with neighbor routers. It must be done in a distributed manner.

3.2.3 Problem Definition

In this section, we consider the following requirements/constraints for the interface mode assignment to reconstruct the mesh network.

(1) Each router constantly exchanges keep-alive messages with its neighbor routers and the GW. When it misses the messages in a predefined interval, it decides that the reachability of the network has been lost and invokes the proposed reconstruction method. At the same time, all interface change their channel to the predefined common one.

(2) A Wi-Fi router constantly sends beacon messages [56]. We suppose that it can put some

information on the message to advertise their own existence and also discover the existence of one-hop neighboring routers within the transmission range.

(3) Routes for reconstruction make a tree topology rooted by the GW.

(4) An interface must work either in AP or STA mode. An interface in AP mode can connect to any number of interfaces in STA mode. To the contrary, an interface in STA mode can connect to only one interface in AP mode.

(5) A spare AP must take AP mode because it has only one interface.

3.2.4 Phases of Interface Mode Assignment Method

Fig. 3.16 shows the flowchart of the proposed method. In a whole reconstruction process, each isolated router including spare AP should discover a tentative route to the GW in a distributed manner. Note that a tentative route is a chain of *unavailable* links.

After an isolated router has found at least one route to the GW, it starts the interface mode selection phase assigning a suitable mode to each interface. Once a tentative route for an isolated router is decided, it never changes until interface mode selection phase completes.

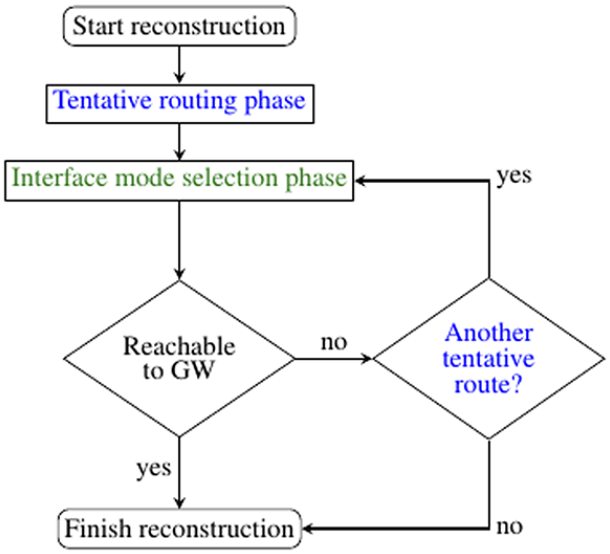


Figure. 3.16: Flowchart of Recontruction

If the isolated router v_i has not become reachable to the GW, it starts the interface mode selection phase again for its next possible tentative route. If the interface mode selection phase has completed successfully, the reconstruction process finishes for v_i.

In an infrastructure network, an AP sends out beacon frames to advertise its existence and capabilities to STAs in its infrastructure basic service set (IBSS). Beacons are sent periodically

in beacon interval time. Fig. 3.17 shows the format of the standard 802.11 beacon frame. In the frame body, there are mandatory and common optional fields, as shown in Table. 3.3.

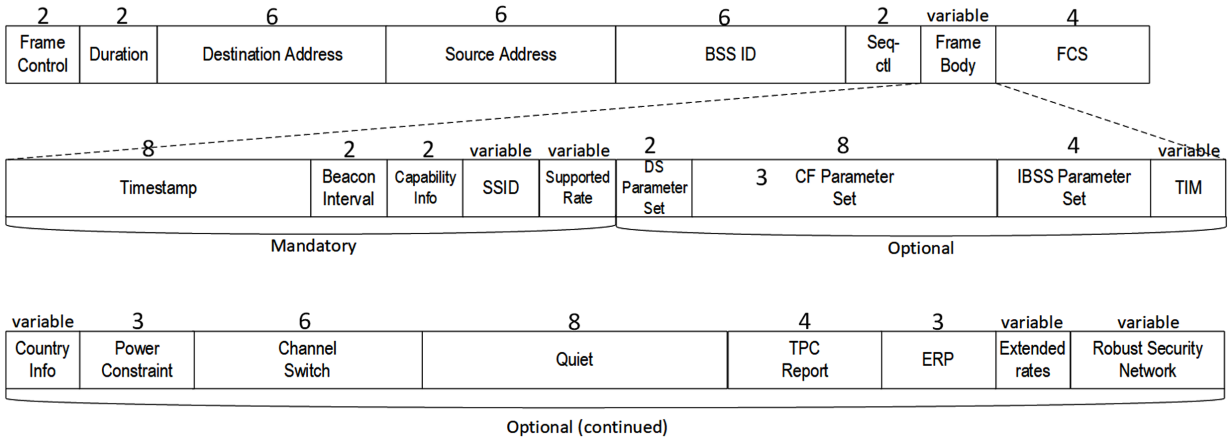


Figure. 3.17: Format of Beacon Message

Table. 3.3: Fields of Beacon Message

Field Name	**Size in Byte**	**Description**
Timestamp	8	The time is measured in microseconds, in which AP has been active.
Beacon Interval	2	The number of time units (TU) Default value is 100TU (102.4 milliseconds)
Capability info	2	Consists of subfields such as radio measurement, QoS information, and so on.
SSID	variable	Service set identifier 16 or 32 characters
Supported Rates	variable	Standard IEEE 802.11g supports rates up to 54 Mbps
IBSS parameter	4	Present only within beacon frames generated by stations in IBSS
Power Constraint	3	Value of max power
Extended Supported Rates	variable	Supported rates not carried in the Supported Rates Element
Robust Secure Network	variable	Indicate Authentication Cipher, Encryption Cipher & other RSN capability of stations

At the physical layer of the standard IEEE 802.11 frames, sending and receiving messages is all about the frequency band, modulation, signal-to-noise ratio (SNR) with which the signal is received. To look at the Data Rate value and the SNR, we can observe signal strength indicator (SSI) signal value (combined with the SSI Noise value). The SSI signal value is more commonly known as the RSSI (Received Signal Strength Indication). These fields will vary with different frames.

A. Tentative Routing Phase

In the tentative routing phase, an isolated router tries to discover a next hop router in the connected area using beacon messages. At first, an isolated router finds one or more tentative routes to the GW. In the proposed method, Routing Information Protocol version 2 (RIPv2) can be applied for this route construction. RIPv2 is a distance vector routing protocol where the number of hops is used as its metric [55].

Fig. 3.18(a) shows that an isolated router v_i has found a router v_j connected to the GW based on exchanging their beacon messages. Therefore, v_i and v_j identify their common link $e(c_{i,a}, c_{j,b})$ as an *unavailable* link. In the same manner, v_i also has *unavailable* links to v_k and v_l.

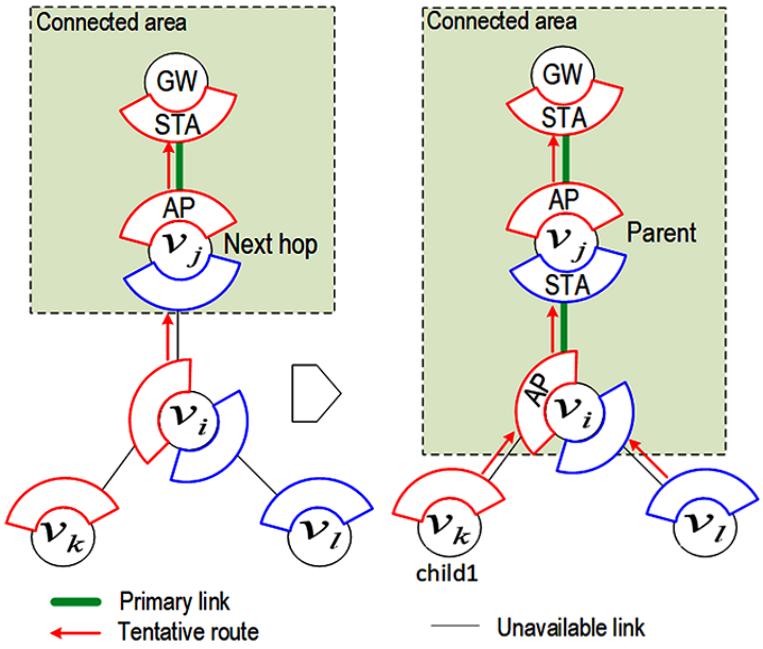


Figure. 3.18: Parent and Child of Mesh Router

Along the *unavailable* link, v_j can recommend a tentative route to the GW for v_i. Thus, v_i adds v_j as its next hop and it starts its interface mode selection phase. Note that the mode

of their interfaces is STA as default. But the link is still unavailable until the interface mode selection phase is successfully completes. Fig. 3.18(b) shows that v_i send *Join* message to negotiate its mode with v_j, and v_j replies *Accept* message and becomes a parent of v_i. By this procedure, link $e(c_{i,a}, c_{j,b})$ becomes a *primary* link and v_i belongs to the connected area. After that, v_i sends out the routing message to its neighbors v_k and v_l and adds them as its childs. On receiving the message, v_k and v_l start their interface mode selection phase, since v_i is currently a connected router. Reconstruction of a route of an isolated router to the GW represents that the proposed method has been completed successfully.

B. Interface Mode Selection Phase

When an isolated router discovers its next hop router in the connected area, it starts the interface mode selection phase. At first, the isolated router sends $Join$ message to its next hop. If the next hop router replies $Accept$ message, the isolated router becomes a connected router and adds its next hop as its parent in its routing table. Fig. 3.19 shows the flowchart of the interface mode selection.

With the following parameters such as $Mode$, N, and $Status$ for link $e(c_{i,a}, c_{j,b})$.

- $Mode$: A variable to indicate the working mode, where $Mode(c_{i,a})$ means the mode of interface a of router v_i.
- N: The degree of an interface of a router, where $N(c_{j,b})$ means the total number of *primary* links and *unavailable* links used for its childs.
- $Status$: The link status. where $Status(e(c_{j,b}, c_{i,a}))$ is unavailable as a default.

The steps of the phase in Fig. 3.19 contain the conditions of which modes at the link of $e(c_{i,a}, c_{j,b})$ get selected. Here, there are two routers; isolated node v_i that has found its own tentative route and its next hop router v_j. Step1 checks whether v_i is a spare AP or not. If *yes*, $Mode(c_{j,b})$ must be STA to make an association since a spare AP has only one interface and its mode must be AP. Before the assignment, if $Mode(c_{j,b})$ is AP in Step2, Step3 checks the degree of the interface $N(c_{j,b})$ equals 1 or not. If *yes*, STA mode is assigned to $c_{j,b}$ since this link is available for the association. Otherwise, $Status(e(c_{j,b}, c_{i,a}))$ becomes *infinity* so that it is unable to make an association between v_i and v_j. Step4 checks whether $Status(e(c_{j,b}, c_{i,a}))$ is *infinity* or not. If *yes*, Step5 checks the degree of the interface $N(c_{j,b})$ equals 1 or not. If *yes*, $Mode(c_{j,b})$ becomes STA since this link is available for the association. Otherwise, this link is unavailable for a new connection. In the same manner, Step6 considers the case that v_j is a spare AP. If *yes*, $Mode(c_{i,a})$ becomes STA. Otherwise, Step7 checks $Mode(c_{i,a})$ is AP or not. Before the assignment, Step8 checks whether the degree of the interface $N(c_{j,b})$ equals 1 or not in the same

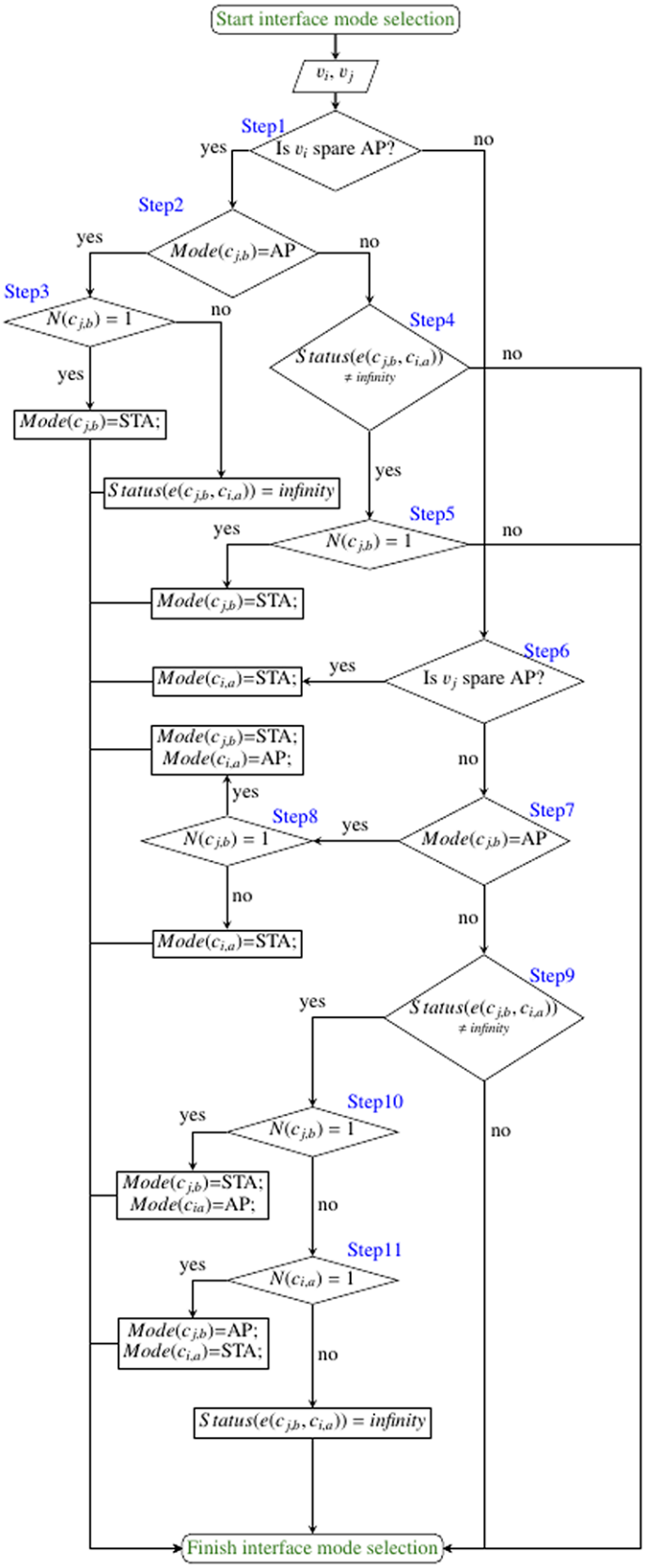


Figure. 3.19: Flowchart of Interface Mode Selection Phase

manner of Step3. If *yes*, AP mode is assigned to $c(i,a)$ since the mode of $c(j,b)$ is changed AP to STA. Otherwise, STA mode is assigned to $c(i,a)$ since this link is available for the association. Step9 checks whether $Status(e(c_{j,b}, c_{i,a}))$ is *infinity* or not. If *yes*, it means that a mode has not selected yet. Therefore, $Mode(c_{j,b})$ and $Mode(c_{i,a})$ become STA and AP, respectively, when Step10 is *yes*, in which it is checked whether the degree of the interface $N(c_{j,b})$ equals 1 or not. Before next assignment, Step11 checks whether the degree of the interface $N(c_{i,a})$ equals 1 or not. If *yes*, AP and STA are assigned to $c_{j,b}$ and $c_{i,a}$, since v_i has no child. Otherwise, the link status $Status(e(c_{j,b}, c_{i,a}))$ becomes *infinity*.

If there is no condition to meet in the above steps, it is considered as impossible to assign modes to the link so that v_i has to find another tentative route.

We assume the following 11 different cases and their result to emphasize how the interface mode selection method works. Each case has been considered in different conditions.

1. Reconstruct isolated routers via one spare AP through a connected router with its interface in STA mode

   In this case, we highlights the reconstruction of a spare AP through a connected router which is already selected as the next hop of another connected router via its same interface in STA mode. Fig. 3.20(a) demonstrates how the mode selection phase works under the assumption that routers v_1 to v_4 are connected routers having routes to the GW whereas v_s and v_5 to v_7 are isolated routers.

   Before the mode selection phase started, v_s found out its neighbor router v_3 using beacon message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_3 adds v_s to its neighbor table. Routers v_5 and v_6 are added to v_s's neighbor table as its childs. Since v_s has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_3 with the start of its mode selection phase. Note that an interface of router v_3 having a link to the interface of v_s should be in STA mode to make an association.

   Although v_3 is selected the next hop router of v_s, it is the next hop router of v_4 via its interface in AP mode. Therefore, the condition of Step3 in Fig. 3.19 is satisfied in its mode selection phase of the link $e(c_{s,1}, c_{3,1})$. In this case, as shown in Fig. 3.20(b), v_3 should execute *leaving* process to dissolve with v_4 in order to make itself the next hop router of v_s. In the leaving process, v_3 sends *Leave* message to v_4 to dissolve the association. Suppose that v_4 has another route to the GW, it replies *Accept* message. As a result, v_3 could successfully handle the leaving process to dissolve with v_4 in Fig. 3.20(b). After that, the degree of interface $N(c_{3,1})$ becomes 1 and then v_3 can send *Accept* message to v_s to make a new association. $Status(e(c_{3,1}, c_{4,2}))$ is configured as *infinity* and v_3 declares it

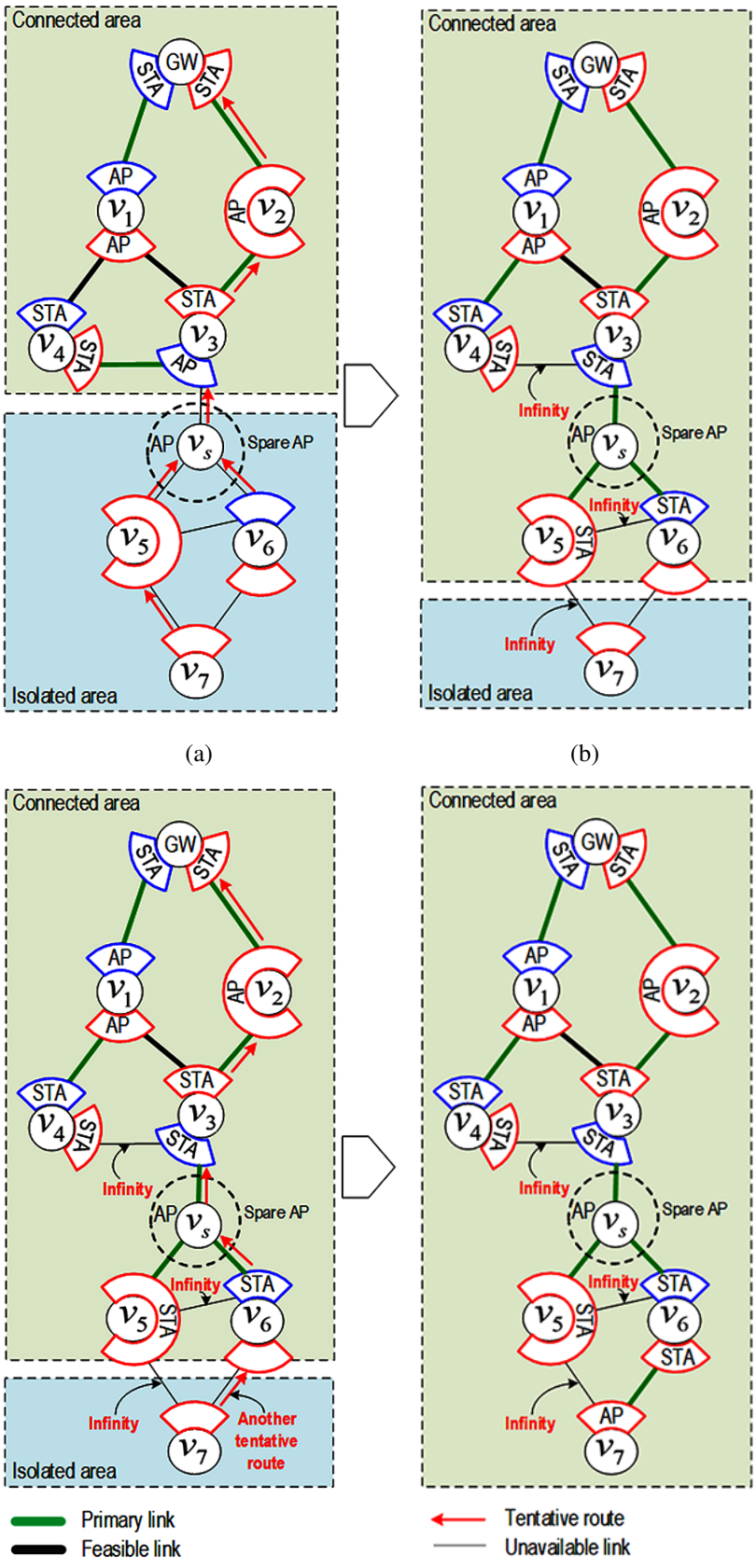


Figure. 3.20: Reconstruction Process of Case 1

to its neighbor routers via its interface, as shown in Fig. 3.20(b). It means other links beside of $e(c_{3,1}, c_{4,2})$ are not possible to use for any tentative routes. If v_3 receives *Reject* message from v_4, it is impossible to to get selected as the next hop of v_s. In this case, v_3 sends back *Reject* message to v_s. As a result, v_s should discover another router to the GW.

After v_s becomes a connected router, as shown in Fig. 3.20(b), routers v_5 and v_6 can take STA mode at their interface connected with v_s according to Step6 in the Fig. 3.19. As a result, routers v_5 and v_6 become connected routers. After that, v_7 is available to start its mode selection phase since v_5 is selected as the next hop router of v_7. But, the link statuses $Status(e(c_{3,1}, c_{4,2}))$, $Status(e(c_{5,2}, c_{6,1}))$, and $Status(e(c_{5,2}, c_{7,2}))$ are configured as *infinity* so that router v_7 has to find another tentative route in Fig. 3.20(c). If it has no tentative route of v_7, it keeps itself as an isolated router and declares. Finally, router v_7 has a new tentative route via router v_6 in Fig. 3.20(c) and its mode selection phase is satisfied with the condition in Step10, as shown in Fig. 3.20(d).

2. Reconstruct isolated routers through a connected router with its interface in STA mode

   In this case, we assume how four isolated routers become reachable to the GW through a connected router with its interface in STA mode. Fig. 3.21(a) assumes that routers v_1 to v_4 are connected routers having routes to the GW whereas v_5 to v_8 are isolated routers.

   Before the mode selection phase started, v_5 found out its neighbor router v_3 using beacon message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_3 adds v_5 to its neighbor table. Routers v_6 and v_7 are added to v_5's neighbor table as its childs. Since v_5 has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_3 with the start of its mode selection phase. Note that an interface of router v_5 having a link to the interface of v_3 should be in AP mode to make an association.

   Although v_3 is selected the next hop router of v_5, it is the next hop router of v_4 via its interface in STA mode. Therefore, the condition of Step10 in Fig. 3.19 is satisfied in its mode selection phase of the link $e(c_{5,2}, c_{3,1})$. In this case, as shown in Fig. 3.21(b), v_3 should execute *leaving* process to dissolve with v_4 in order to make itself the next hop router of v_5. In the leaving process, v_3 sends *Leave* message to v_4 to dissolve the association. Suppose that v_4 has another route to the GW, it replies *Accept* message. As a result, v_3 could successfully handle the leaving process to dissolve with v_4 in Fig. 3.21(b). After that, v_3 can send *Accept* message to v_5 to make a new association and then the degree of interface $N(c_{3,1})$ becomes 1. $Status(e(c_{3,1}, c_{4,2}))$ is configured as *infinity* and v_3 declares it to its neighbor routers via its interface. It means other links beside of $e(c_{3,1}, c_{4,2})$ are not possible to use for any tentative routes. If v_3 receives *Reject* message from v_4, it is impossible to to get selected as the next hop of v_5. In this case, v_3 sends back *Reject* message to v_5. As a result, v_5 should discover another router to the GW.

   After v_5 becomes a connected router, as shown in Fig. 3.21(b), routers v_6 and v_7 can take STA mode at their interface connected with v_5 according to Step7 and Step8 in the Fig. 3.19. As a result, routers v_6 and v_7 become connected routers. After that, v_8 is available to start its mode selection phase since v_6 is selected as the next hop router of v_8. But, the link statuses $Status(e(c_{3,1}, c_{4,2}))$ and $Status(e(c_{6,2}, c_{8,2}))$ are configured as *infinity* so that router v_8 has to find another tentative route in Fig. 3.21(c). If it has no tentative route of v_8, it keeps itself as an isolated router and declares. Finally, router v_8 has a new tentative route via router v_7 in Fig. 3.21(c) and its mode selection phase is satisfied with the condition in Step10, as shown in Fig. 3.21(d).

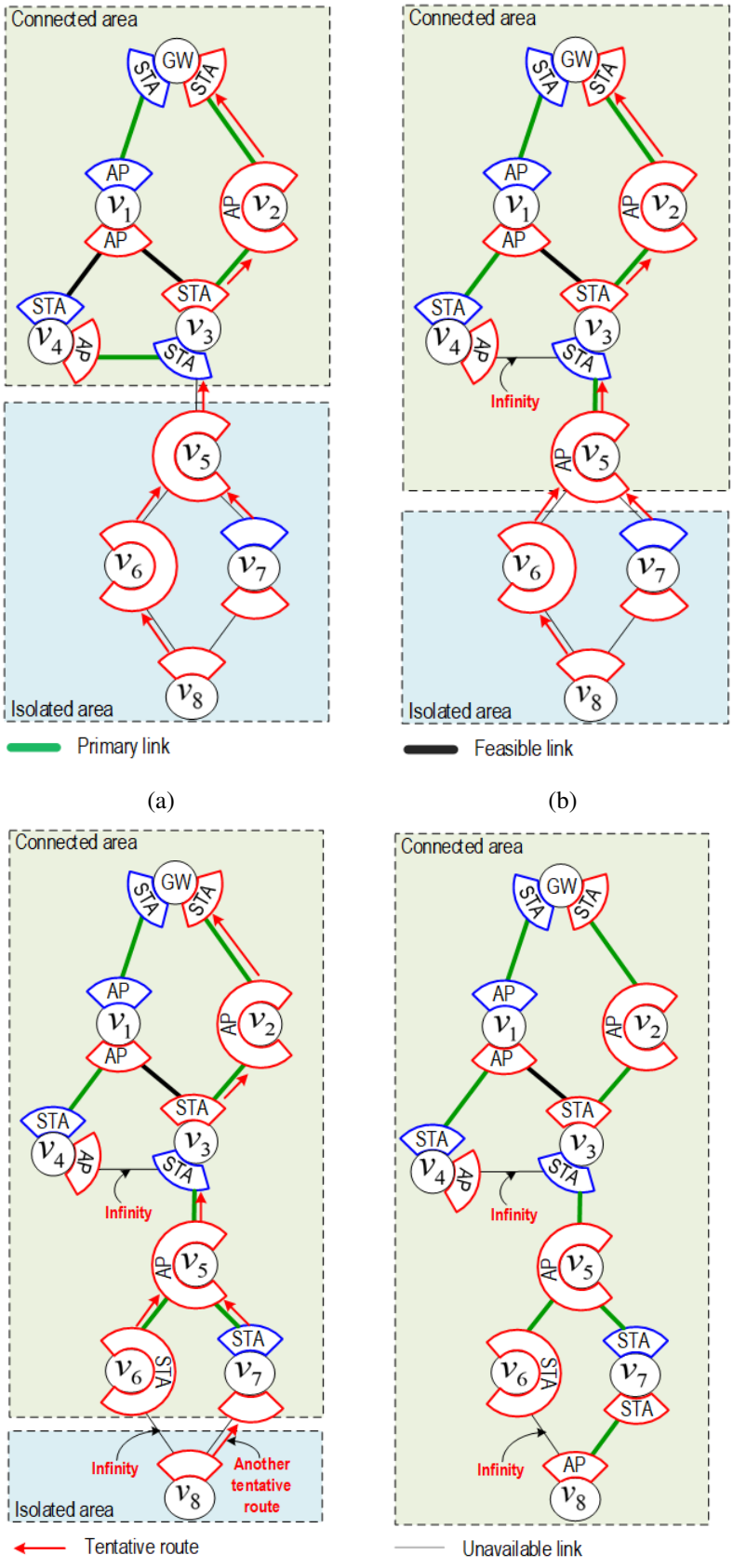
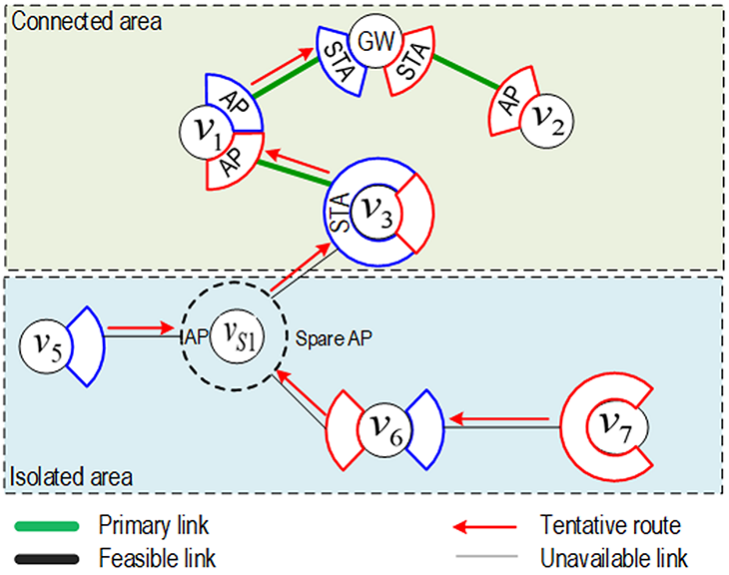


Figure. 3.21: Reconstruction Process of Case 2

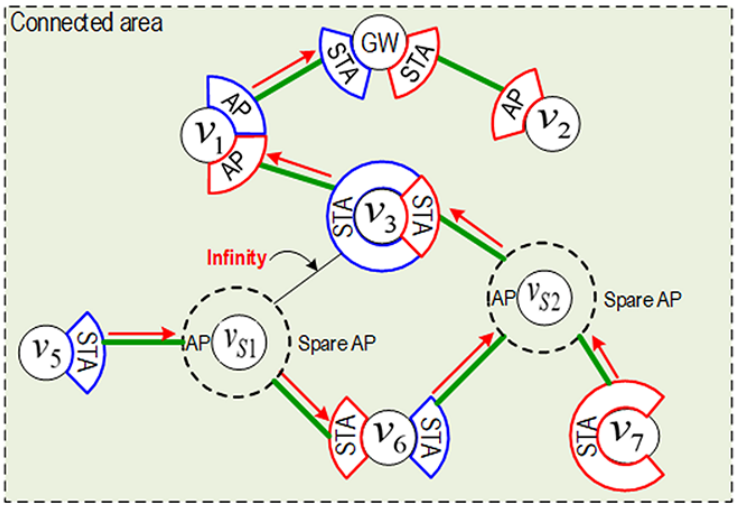
3. Reconstruct isolated routers via two spare APs

   In this case, we highlight why one spare AP is unable to make isolated routers reachable to GW. Fig. 3.22(a) assumes a case with two spare APs, in which routers v_1 to v_3 are connected routers having routes to the GW whereas v_{S1} and v_5 to v_7 are isolated routers.

   Before the mode selection phase started, v_{S1} found out its neighbor router v_3 using beacon message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_3 adds v_{S1} to its neighbor table. Routers v_5 and v_6 are added to v_{S1}'s neighbor table as its childs. v_7 selects v_6 as its next hop.



(a)



(b)

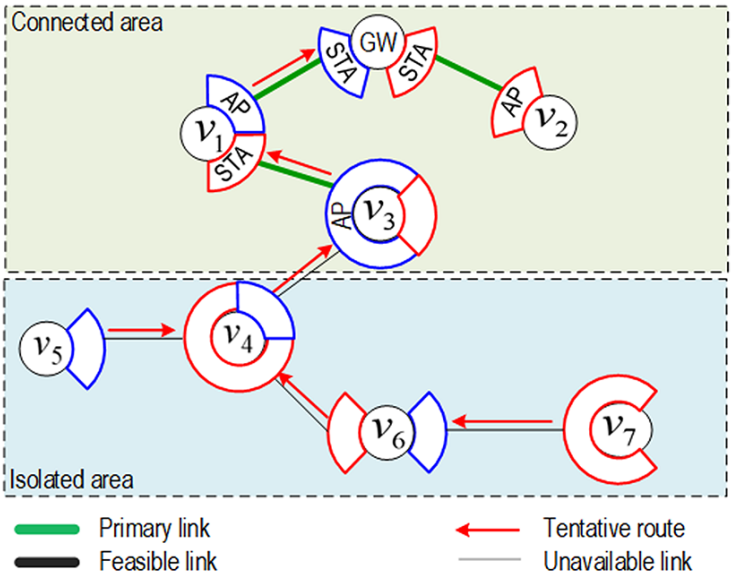
Figure. 3.22: Reconstruction Process of Case 3

Since v_{S1} has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_3 with the start of its mode selection phase. Note that an interface of router v_3 having a link to the interface of v_{S1} should be in STA mode to make an association. Although v_3 is selected the next hop router of v_{S1}, it has only one route to GW via its next hop router of v_1 using its interface in STA mode. Therefore, the condition of Step5 in Fig. 3.19 is *no* so that the link $e(c_{S1,1}, c_{3,1})$ is unavailable for the association. v_3 sends *Reject* message to v_{S1}. After that v_{S2} has constructed a tentative route to the GW via v_3 and other routers discover their new tentative routes to the GW in the same manner. v_{S2} sends $Join$ message to v_3 with the start of its mode selection phase. Since Step5 in Fig. 3.19 is $\hat{\text{y}}$es, v_3 can send *Accept* message to v_{S2} to make a new association and then v_{S2} becomes a connected router, as shown in Fig. 3.22(b).

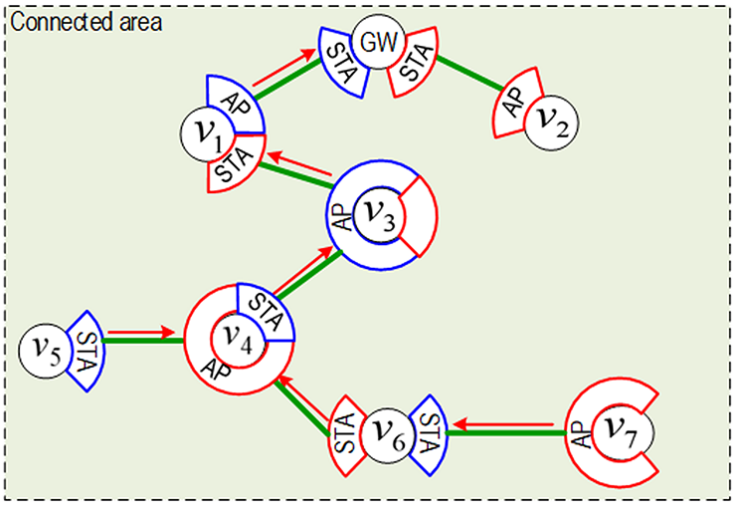
After that, routers v_6 and v_7 can take STA mode at their interface connected with v_{S2} according to Step6 in the Fig. 3.19. As a result, routers v_5 and v_6 become connected routers. After that, v_{S1} is available to start its mode selection phase since v_6 is selected as the next hop router of v_{S1} because the link status $Status(e(c_{S1,1}, c_{3,1}))$ is configured as *infinity*. Note that v_5 is range out of v_6 so that it needs v_{S1} to find another tentative route to the GW. Finally, router v_5 has a new tentative route via router v_{S1} and its mode selection phase is satisfied with the condition in Step6, as shown in Fig. 3.22(b).

4. Reconstruct isolated routers through a connected router with its interface in AP mode

   In this case, we assume the opportunity how a connected router provide a route to isolated router via its interface connected to its next hop router. Fig. 3.23(a) assumes that routers v_1 to v_3 are connected routers having routes to the GW whereas v_4 to v_7 are isolated routers. Before the mode selection phase started, v_4 found out its neighbor router v_3 using beacon



(a)



(b)

Figure. 3.23: Reconstruction Process of Case 4

message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_3 adds v_4 to its neighbor table. Routers v_5 and v_6 are added to v_4's neighbor table as its childs.

Since v_4 has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_3 with the start of its mode selection phase. Therefore, the condition of Step8 in Fig. 3.19 is satisfied in its mode selection phase of the link $e(c_{4,1}, c_{3,1})$. In this case, as shown in Fig. 3.23(b), v_3 can send *Accept* message to v_4 to make a new association and then $Mode(c_{4,1})$ becomes STA.

After v_4 becomes a connected router, as shown in Fig. 3.23(b), routers v_5 and v_6 can take STA mode at their interface connected with v_4 according to Step11 in the Fig. 3.19. As a result, routers v_5 and v_6 become connected routers. After that, v_7 is available to start its mode selection phase according to Step10 in the Fig. 3.19.

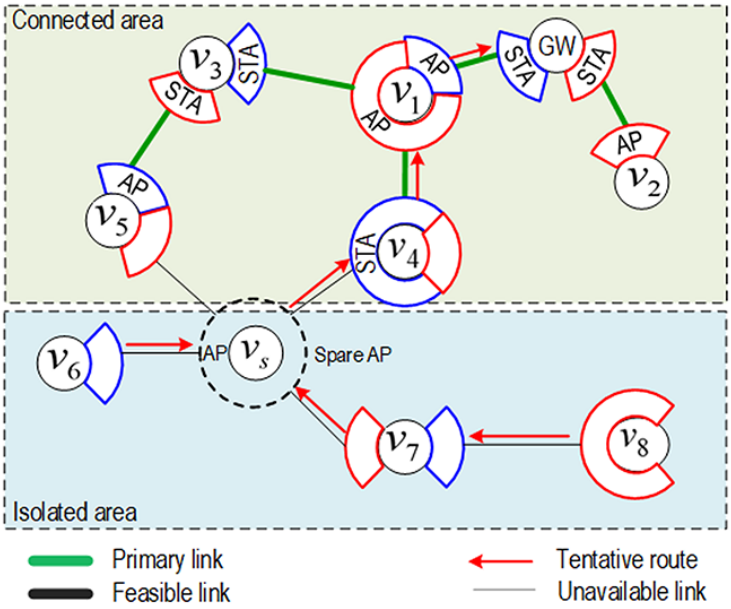
5. Reconstruct isolated routers via a spare AP with two routes to a GW

   In this case, we emphasize how the method works for a spare AP having two routes to its serving GW. Fig. 3.24(a) assumes that routers v_1 to v_5 are connected routers having routes to the GW whereas v_s and v_6 to v_8 are isolated routers.

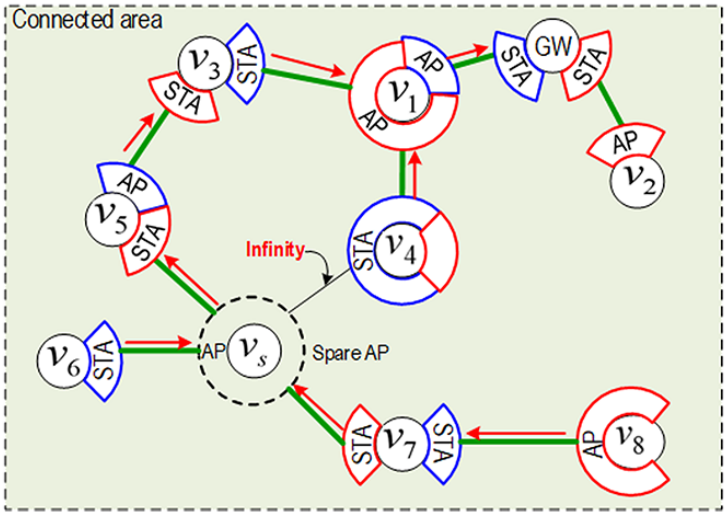
   Before the mode selection phase started, v_s found out its neighbor router v_4 using beacon message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_4 adds v_s to its neighbor table. Routers v_6 and v_7 are added to v_s's neighbor table as its childs. Since v_s has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_4 with the start of its mode selection phase. Note that an interface of router v_4 having a link to the interface of v_s should be in STA mode to make an association.

   Although v_4 has its route to the GW via its next hop router of v_1 in its interface mode $Mode(c_{4,1})$ is in STA mode. Also $v4$ has no backup route. Therefore, the condition of Step3 in Fig. 3.19 is unsatisfied, v_4 replies *Reject* message, as shown in Fig. 3.24(a). $Status(e(c_{4,1}, c_{s,1}))$ is configured as *infinity* and v_4 declares it to its neighbor routers via its interface. It means other links beside of $e(c_{4,1}, c_{s,1})$ are not possible to use for any tentative routes. In this case, as shown in Fig. 3.24(b), v_s should find another next hop router to reach to the GW.

   As a result, v_s found out its neighbor router v_5 using beacon message and added a tentative route to the GW to its routing table. After that, v_5 can send *Accept* message to v_s to make a new association because Step4 in the Fig. 3.19 is satisfied. After v_s becomes a connected router, as shown in Fig. 3.24(b), routers v_6 and v_7 can take STA mode at their interface connected with v_s according to Step6 in the Fig. 3.19. As a result, routers v_6 and v_7 become connected routers. Finally, router v_8 has its tentative route via router v_7 and its mode selection phase is satisfied with the condition in Step10, as shown in Fig. 3.24(b).



(a)

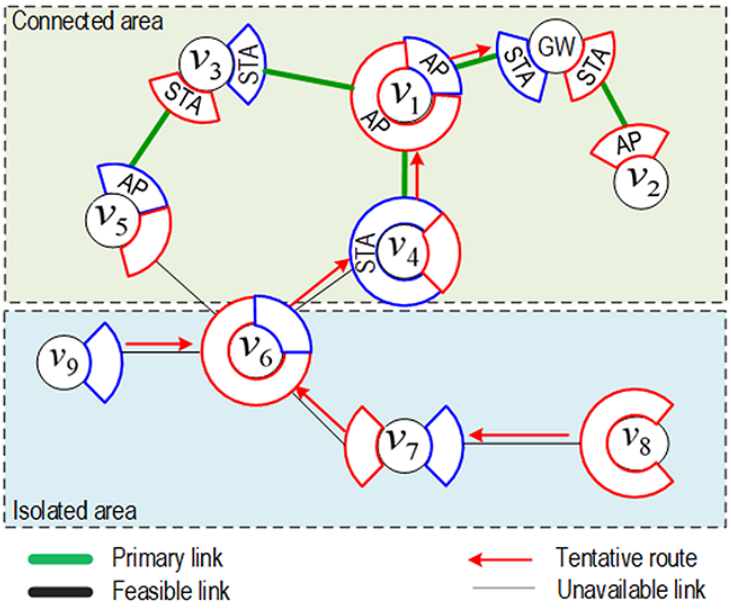


(b)

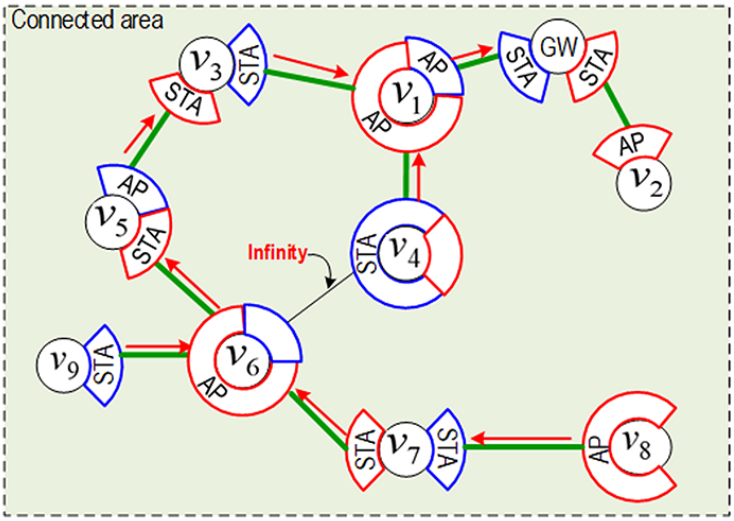
Figure. 3.24: Reconstruction Process of Case 5

6. Reconstruct isolated router with two routes to a GW

In this case, we emphasize how the method works for an isolated router having two routes to its serving GW. Fig. 3.25(a) assumes that routers v_1 to v_5 are connected routers having routes to the GW whereas v_6 to v_9 are isolated routers.



(a)



(b)

Figure. 3.25: Reconstruction Process of Case 6

Before the mode selection phase started, v_6 found out its neighbor router v_4 using beacon message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_4 adds v_6 to its neighbor table. Routers v_7 and v_9 are added to v_6's

neighbor table as its childs. Since v_6 has constructed a tentative route to the GW via v_4, it sends $Join$ message to v_4 with the start of its mode selection phase.

Therefore, the condition of Step11 in Fig. 3.19 is satisfied, v_4 should take AP mode. But, an interface of router v_4 has only one route to the GW so that $Status(e(c_{4,1}, c_{6,1}))$ is configured as *infinity* and v_4 declares it to its neighbor routers via its interface. It means other links beside of $e(c_{4,1}, c_{s,1})$ are not possible to use for any tentative routes. v_4 replies *Reject* message, as shown in Fig. 3.25(b). In this case, as shown in Fig. 3.25(b), v_6 should find another next hop router to reach to the GW.

As a result, v_6 found out its neighbor router v_5 using beacon message and added a tentative route to the GW to its routing table. After that, v_5 can send *Accept* message to v_s to make a new association because Step4 in the Fig. 3.19 is satisfied. After v_6 becomes a connected router, as shown in Fig. 3.25(b), routers v_7 and v_9 can take STA mode at their interface connected with v_6 because Step8 in the Fig. 3.19 is unsatisfied. As a result, routers v_7 and v_9 become connected routers. Finally, router v_8 has its tentative route via router v_7 and its mode selection phase is satisfied with the condition in Step10, as shown in Fig. 3.25(b).

7. Reconstruct isolated router having one interface via spare AP

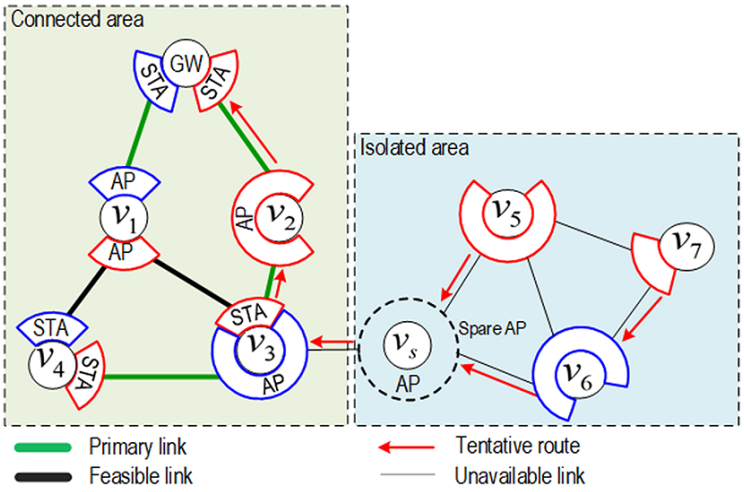
   In this case, we assume each isolated router has one interface. Three isolated router need to become reachable via a spare AP. Fig. 3.26(a) assumes that routers v_1 to v_4 are connected routers having routes to the GW whereas v_s and v_5 to v_7 are isolated routers.

   Before the mode selection phase started, v_s found out its neighbor router v_3 using beacon message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_3 adds v_s to its neighbor table. Routers v_5 and v_6 are added to v_s's neighbor table as its childs. Since v_s has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_3 with the start of its mode selection phase. Note that an interface of router v_3 having a link to the interface of v_s should be in STA mode to make an association.

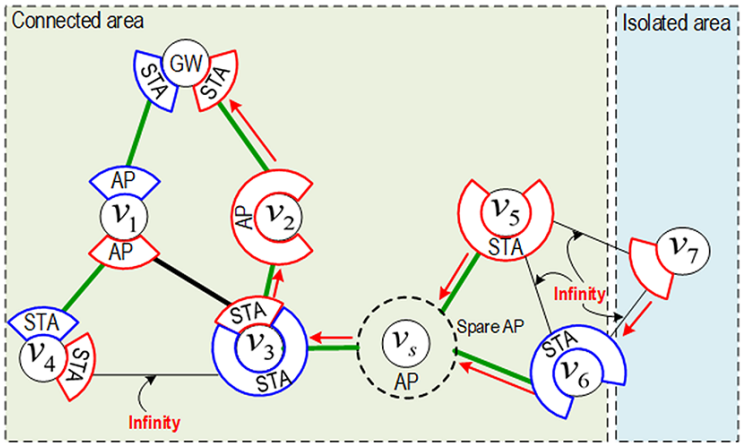
   Although v_3 is selected the next hop router of v_s, it is the next hop router of v_4 via its interface in AP mode. Therefore, the condition of Step3 in Fig. 3.19 is satisfied in its mode selection phase of the link $e(c_{s,1}, c_{3,1})$. In this case, as shown in Fig. 3.26(b), v_3 should execute *leaving* process to dissolve with v_4 in order to make itself the next hop router of v_s. In the leaving process, v_3 sends *Leave* message to v_4 to dissolve the association. Suppose that v_4 has another route to the GW, it replies *Accept* message. As a result, v_3 could successfully handle the leaving process to dissolve with v_4 in Fig. 3.26(b). After that, v_3 can send *Accept* message to v_s to make a new association and then the degree of interface $N(c_{3,1})$ becomes 1. $Status(e(c_{3,1}, c_{4,2}))$ is configured as *infinity* and v_3 declares it to its neighbor routers via its interface. It means other links beside of $e(c_{3,1}, c_{4,2})$ are not possible to use for any tentative routes.

   After v_s becomes a connected router, as shown in Fig. 3.26(b), routers v_5 and v_6 can take STA mode at their interface connected with v_s according to Step6 in the Fig. 3.19. As a result, routers v_5 and v_6 become connected routers. After that, v_7 is available to start its mode selection phase since v_5 is selected as the next hop router of v_7.

   But, the link statuses $Status(e(c_{5,2}, c_{6,1}))$, $Status(e(c_{5,2}, c_{7,2}))$, and $Status(e(c_{6,1}, c_{7,2}))$ are configured as *infinity* so that router v_7 has no tentative route and then it keeps itself as an isolated router and declares. v_7 is still unreachable to the GW so that the network has not been reconstructed yet. Another spare AP may be required in this case.



(a)

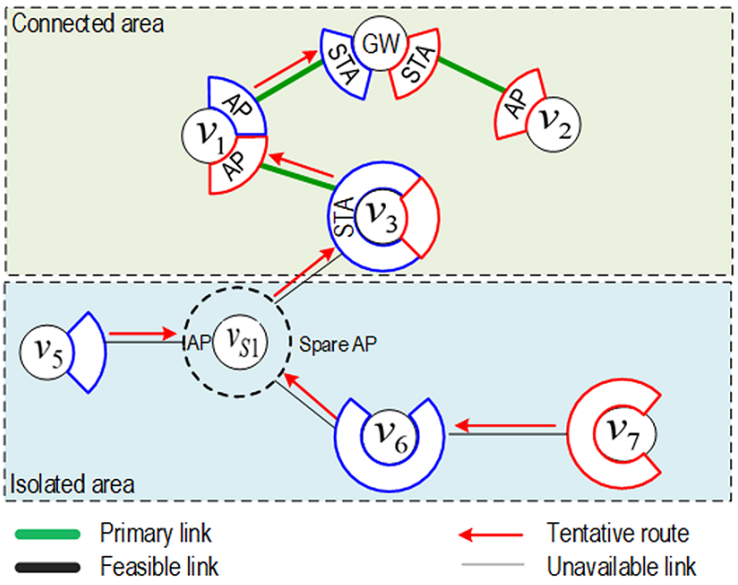


(b)

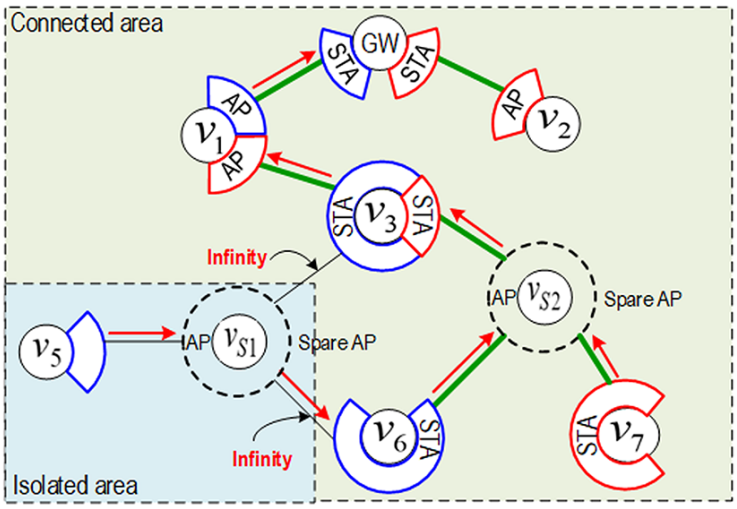
Figure. 3.26: Reconstruction Process of Case 7

8. Reconstruct isolated router having one interface via two spare APs

In this case, we assume each isolated router has one interface. Three isolated router need to become reachable via two spare APs. Fig. 3.27(a) assumes that routers v_1 to v_3 are connected routers having routes to the GW whereas v_{S1} and v_5 to v_7 are isolated routers. Before the mode selection phase started, v_{S1} found out its neighbor router v_3 using beacon



(a)



(b)

Figure. 3.27: Reconstruction Process of Case 8

message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_3 adds v_{S1} to its neighbor table. Routers v_5 and v_6 are added to v_{S1}'s neighbor table as its childs. v_7 selects v_6 as its next hop.

Since v_{S1} has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_3 with the start of its mode selection phase. Note that an interface of router v_3 having a link to the interface of v_{S1} should be in STA mode to make an association. Although v_3 is selected the next hop router of v_{S1}, it has only one route to GW via its next hop router of v_1 via its interface in STA mode. Therefore, the condition of Step5 in Fig. 3.19 is *no* so that the link $e(c_{S1,1}, c_{3,1})$ is unavailable for the association. v_3 sends *Reject* message to v_{S1}. After that v_{S2} has constructed a tentative route to the GW via v_3 and other routers discover their new tentative routes to the GW in the same manner. v_{S2} sends sends $Join$ message to v_3 with the start of its mode selection phase. Since Step5 in Fig. 3.19 is ŷes, v_3 can send *Accept* message to v_{S2} to make a new association and then v_{S2} becomes a connected router, as shown in Fig. 3.27(b).

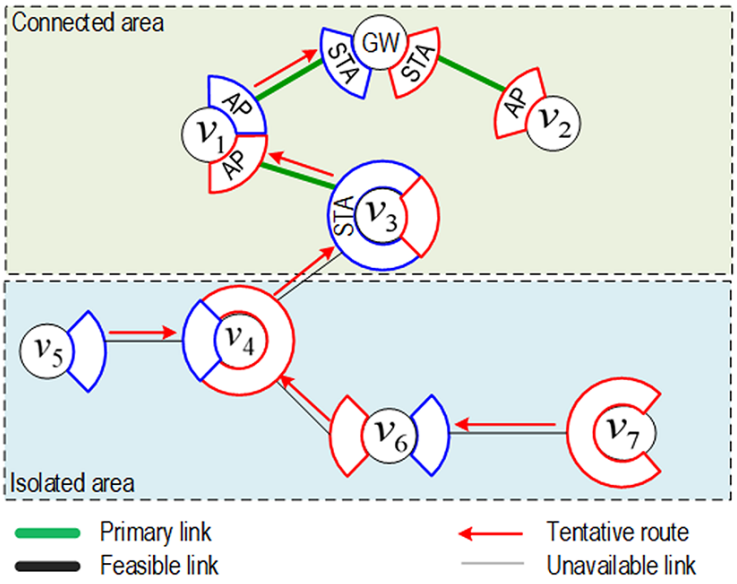
After that, routers v_6 and v_7 can take STA mode at their interface connected with v_{S2} according to Step6 in the Fig. 3.19. As a result, routers v_5 and v_6 become connected routers. After that, v_{S1} is available to start its mode selection phase since v_6 is selected as the next hop router of v_{S1} because the link status $Status(e(c_{S1,1}, c_{3,1}))$ is configured as *infinity*. But, both v_{S1} and v_5 keep themselves as isolated routers and declare, since the link status $Status(e(c_{S1,1}, c_{6,1}))$ is also configured as *infinity*.

9. Reconstruct isolated router in mode selection problem using a spare AP

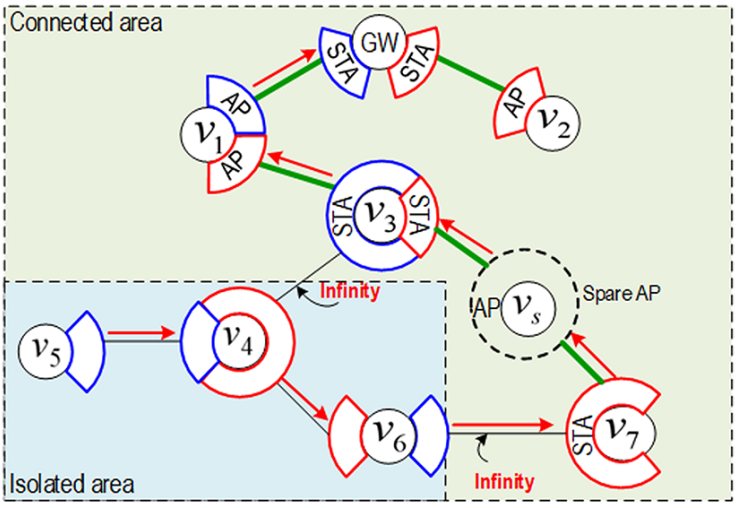
   In this case, an isolated router are unreachable to a GW because of its mode selection problem. We show how a spare AP helps it to become reachable to the GW. Fig. 3.28(a) assumes that routers v_1 to v_3 are connected routers having routes to the GW whereas v_4 to v_7 are isolated routers.

   Before the mode selection phase started, v_4 found out its neighbor router v_3 using beacon message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_3 adds v_4 to its neighbor table. Routers v_5 and v_6 are added to v_4's neighbor table as its childs. v_7 selects v_6 as its next hop.

   Since v_4 has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_3 with the start of its mode selection phase. Although v_3 is selected the next hop router of v_4, it has only one route to GW via its next hop router of v_1 via its interface in STA mode. Therefore, the condition of Step11 in Fig. 3.19 is *no* so that the link $e(c_{3,1}, c_{4,2})$ is unavailable for the association. v_3 sends *Reject* message to v_4. After that v_s has constructed a tentative route to the GW via v_3 and other routers discover their new tentative routes to the GW in the same manner. v_s sends sends $Join$ message to v_3 with the start of its mode selection phase. Since Step5 in Fig. 3.19 is ŷes, v_3 can send *Accept* message to v_4 to make a new association and



(a)



(b)

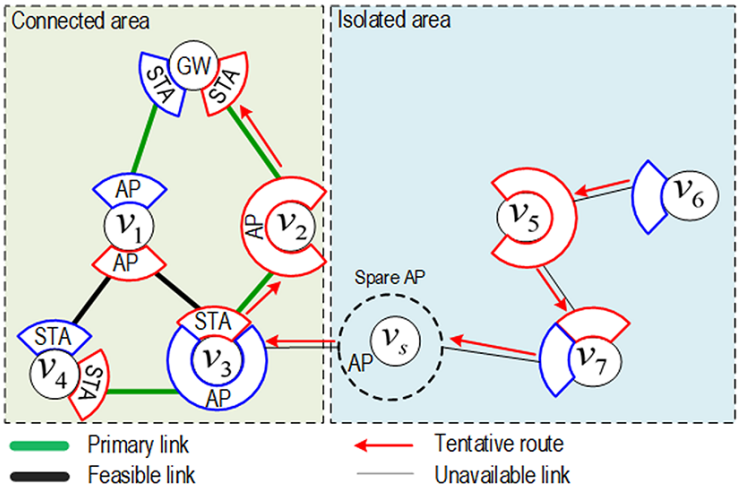
Figure. 3.28: Reconstruction Process of Case 9

then v_4 becomes a connected router, as shown in Fig. 3.28(b).

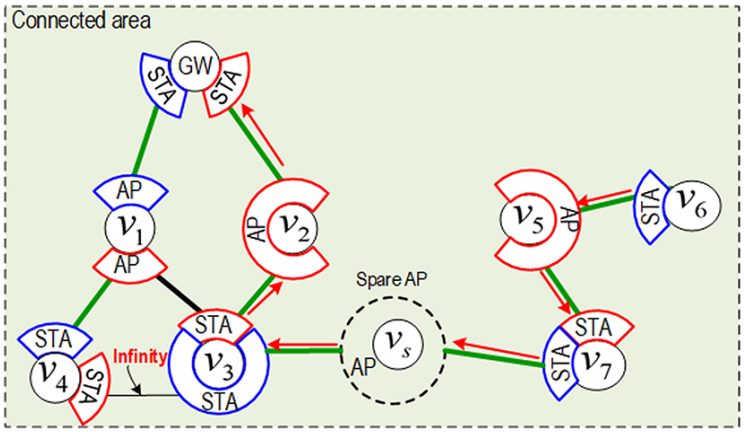
After that, routers v_7 can take STA mode at their interface connected with v_4 according to Step6 in the Fig. 3.19. As a result, routers v_7 becomes a connected router. But the link status $Status(e(c_{7,2}, c_{6,1}))$ is configured as *infinity* so that routers v_6, v_4, and v_5 keep themselves as isolated routers and declares.

10. Reconstruct isolated routers via one spare AP through a connected router with its interface in AP mode

    In this case, we highlight the reconstruction of a spare AP through a connected router which is already selected as the next hop of another connected router via its same interface in AP mode. Fig. 3.29(a) assumes that routers v_1 to v_4 are connected routers having routes to the GW whereas v_s and v_5 to v_7 are isolated routers.



(a)



(b)

Figure. 3.29: Reconstruction Process of Case 10

Before the mode selection phase started, v_s found out its neighbor router v_3 using beacon message and added a tentative route to the GW to its routing table. In terms of the tentative routing tree, router v_3 adds v_s to its neighbor table. Routers v_7 is added to v_s's neighbor table as its childs. v_5 selects v_7 as its next hop and it is selected as the next hop router of v_6.

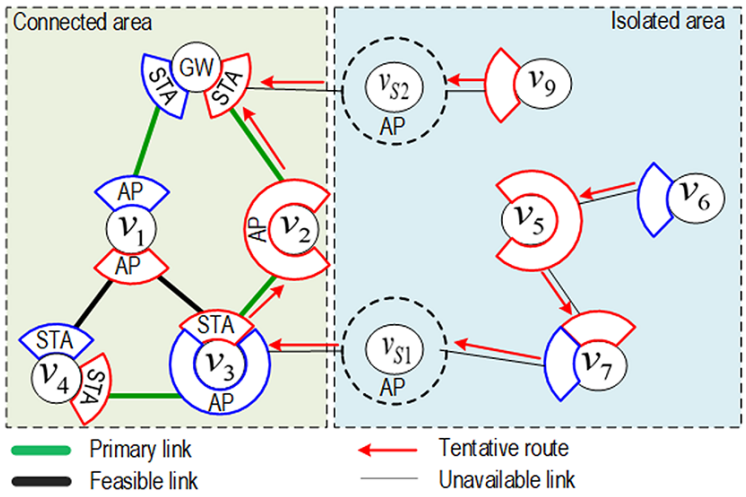
Since v_s has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_3 with the start of its mode selection phase. Note that an interface of router v_3 having a link to the interface of v_{S1} should be in STA mode to make an association.

Although v_3 is selected the next hop router of v_s, it is the next hop router of v_4 via its interface in AP mode. Therefore, the condition of Step3 in Fig. 3.19 is satisfied in its mode selection phase of the link $e(c_{s,1}, c_{3,1})$. In this case, as shown in Fig. 3.29(b), v_3 should execute *leaving* process to dissolve with v_4 in order to make itself the next hop router of v_s. In the leaving process, v_3 sends *Leave* message to v_4 to dissolve the association.suppose that v_4 has another route to the GW, it replies *Accept* message. As a result, v_3 could successfully handle the leaving process to dissolve with v_4 in Fig. 3.29(b). After that, v_3 can send *Accept* message to v_s to make a new association and then the degree of interface $N(c_{3,1})$ becomes 1. $Status(e(c_{3,1}, c_{4,2}))$ is configured as *infinity* and v_3 declares it to its neighbor routers via its interface. It means other links beside of $e(c_{3,1}, c_{4,2})$ are not possible to use for any tentative routes. If v_3 receives *Reject* message from v_4, it is impossible to to get selected as the next hop of v_s. In this case, v_3 sends back *Reject* message to v_s. As a result, v_s should discover another router to the GW.

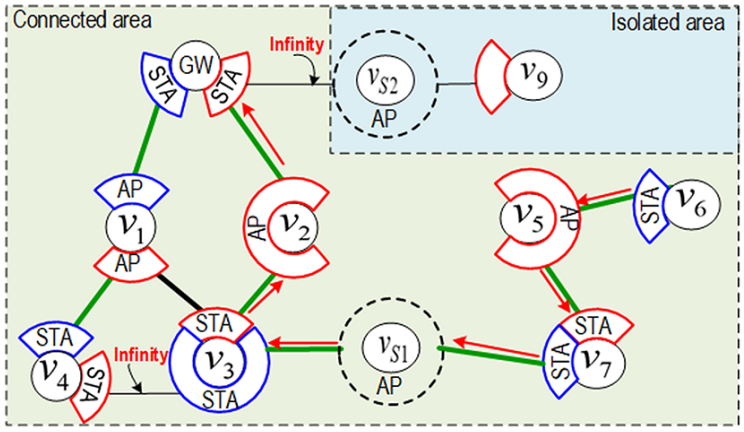
After v_s becomes a connected router, as shown in Fig. 3.29(b), router v_7 can take STA mode at their interface connected with v_s according to Step6 in the Fig. 3.19. As a result, router v_7 becomes a connected router. After that, v_5 is available to start its mode selection phase since v_7 is selected as the next hop router of v_5. After that, router v_5's mode selection phase is satisfied with the condition in Step10, as shown in Fig. 3.29(b) and interfaces $c_{7,2}$ and $c_{5,2}$ take STA mode and AP mode, respectively. Finally, v_6 starts its mode selection phase since v_5 became a connected router. Since Step8 in Fig. 3.19 is no, the mode of interface $Mode(c_{6,1})$ becomes STA.

11. Reconstruct two isolated areas

In this case, we highlight the reconstruction of two isolated areas using two spare APs. Fig. 3.30(a) assumes that routers v_1 to v_4 are connected routers having routes to the GW whereas spare APs v_{S1} and v_{S2} provide isolated routers v_5 to v_7 and v_9, respectively.



(a)



(b)

Figure. 3.30: Reconstruction Process of Case 11

Before the mode selection phase started, v_{S1} found out its neighbor router v_3 using beacon message and added a tentative route to the GW to its routing table. v_{S2} found out its neighbor GW router using beacon message In terms of the tentative routing tree, router v_3 adds v_{S1} to its neighbor table. Routers v_7 is added to v_{S1}'s neigbor table as its childs. v_5 selects v_7 as its next hop and it is selected as the next hop router of v_6.

Since v_{S1} has constructed a tentative route to the GW via v_3, it sends $Join$ message to v_3 with the start of its mode selection phase. Note that an interface of router v_3 having a link

to the interface of v_{S1} should be in STA mode to make an association.

Although v_3 is selected the next hop router of v_{S1}, it is the next hop router of v_4 via its interface in AP mode. Therefore, the condition of Step3 in Fig. 3.19 is satisfied in its mode selection phase of the link $e(c_{S1,1}, c_{3,1})$. In this case, as shown in Fig. 3.30(b), v_3 should execute *leaving* process to dissolve with v_4 in order to make itself the next hop router of v_{S1}. In the leaving process, v_3 sends *Leave* message to v_4 to dissolve the association.suppose that v_4 has another route to the GW, it replies *Accept* message. As a result, v_3 could successfully handle the leaving process to dissolve with v_4 in Fig. 3.30(b). After that, v_3 can send *Accept* message to v_{S1} to make a new association and then the degree of interface $N(c_{3,1})$ becomes 1. $Status(e(c_{3,1}, c_{4,2}))$ is configured as *infinity* and v_3 declares it to its neighbor routers via its interface. It means other links beside of $e(c_{3,1}, c_{4,2})$ are not possible to use for any tentative routes. If v_3 receives *Reject* message from v_4, it is impossible to to get selected as the next hop of v_{S1}. In this case, v_3 sends back *Reject* message to v_s. As a result, v_{S1} should discover another router to the GW.

After v_{S1} becomes a connected router, as shown in Fig. 3.30(b), router v_7 can take STA mode at their interface connected with v_{S1} according to Step6 in the Fig. 3.19. As a result, router v_7 becomes a connected router. After that, v_5 is available to start its mode selection phase since v_7 is selected as the next hop router of v_5. After that, router v_5's mode selection phase is satisfied with the condition in Step10, as shown in Fig. 3.30(b) and interfaces $c_{7,2}$ and $c_{5,2}$ take STA mode and AP mode, respectively. Finally, v_6 starts its mode selection phase since v_5 became a connected router. Since Step8 in Fig. 3.19 is no, the mode of interface $Mode(c_{6,1})$ becomes STA. Step11 in the Fig. 3.19 is unsatified so that the link status $Status(e(c_{GW,2}, c_{S2,1}))$ is configured as *infinity*. As a result, there is unable to make association between GW and v_{S2} and then v_9 keeps itself as an isolated router.

3.2.5 Performance Evaluation

In this section, we evaluate the performance of the proposed method via simulation experiments with two scenarios. The assumed network in Fig. 3.12 was built as a simulation model. In the both scenarios, we assumed that one router was configured as a GW whereas others were isolated routers. All the routers were placed at the coordinate list in Table. 3.4 and had directional antennas oriented to their neighbor nodes. In normal situations, all the routers are reachable to the backbone network via the their serving gateway GW.

A. Reconstruction of WMN without Spare AP

In the first scenario, we consider that routers v_1 to v_{24} are considered as isolated routers. In addition, there is no change of the interfaces and locations of both of the GW and the routers. In other words, this scenario supposes no physical damages on APs and software settings are reset. It aims to evaluate the fundamental performance of the proposed method. We allow to configure not only router GW bust also routers v_1 to v_{24} providing the function

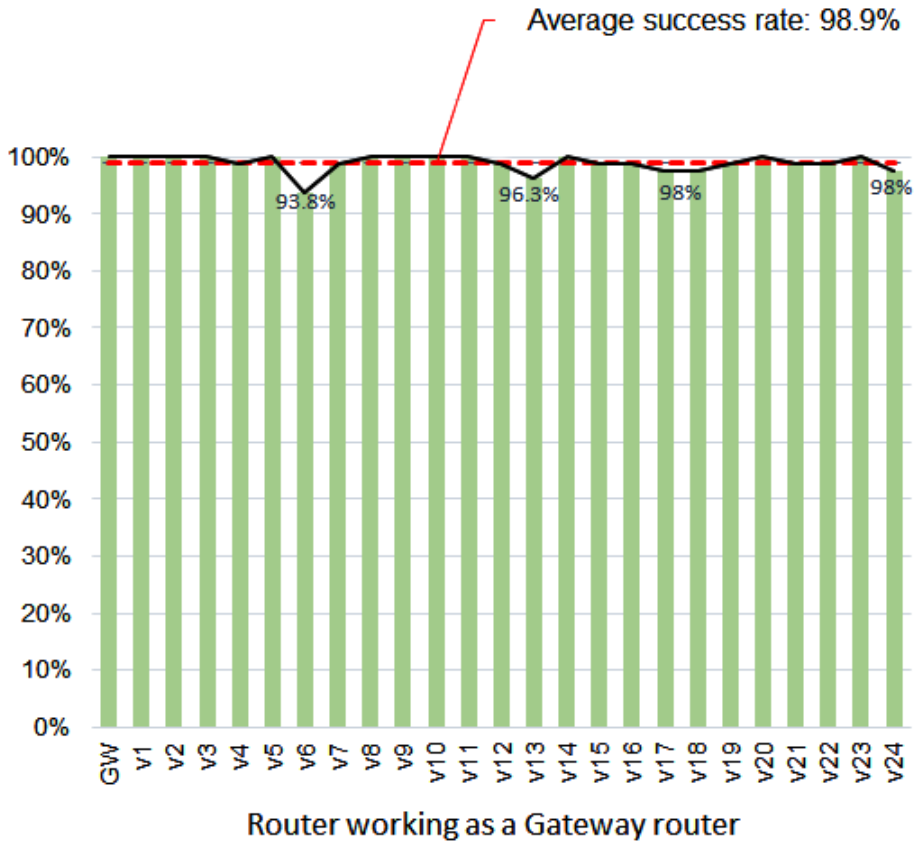


Figure. 3.31: Successful Recovery Probability without Spare APs

Table. 3.4: The Coordinate list of routers' position

Router Name	**X[m]**	**Y[m]**
GW	1375	25
R1	0	150
R2	400	100
R3	850	50
R4	1825	0
R5	2150	50
R6	2500	100
R7	375	500
R8	850	500
R9	1200	550
R10	1650	550
R11	2025	700
R12	2425	700
R13	0	725
R14	350	800
R15	875	900
R16	1225	925
R17	1575	925
R18	1925	1025
R19	525	1150
R20	825	1225
R21	1300	1200
R22	1600	1150
R23	1925	1200
R24	2475	1150

of a GW. The proposed method was executed 100 different cases for each GW router. To build the different cases, each router was equipped with one or two interfaces randomly.

Fig. 3.31 shows that 98.9% of 2500 cases in total are recovered successfully. When router v_6 or v_{13} was selected as a GW router, the lowest success rate of 93.8% or 96.3% was observed, respectively. The reason why is that both of routers v_6 and v_13 have not only two active interfaces but also use the same interfaces for their neighbor connections. Therefore,

it causes the lack of tentative route because usually the link statuses are configured as *infinity*. Other routers are equipped with three or more interfaces.

B. Reconstruction of WMN with Spare AP

In the second scenario, n random routers were assumed to get down. Also, another n routers' antenna orientations changed randomly. We changed n from 2 to 6, and tested 300 different failure cases for each n. Therefore, when some isolated routers are range out, one or more spare APs should be used to provide a route to the GW for them. This scenario assumes that a significant disaster has occurred.

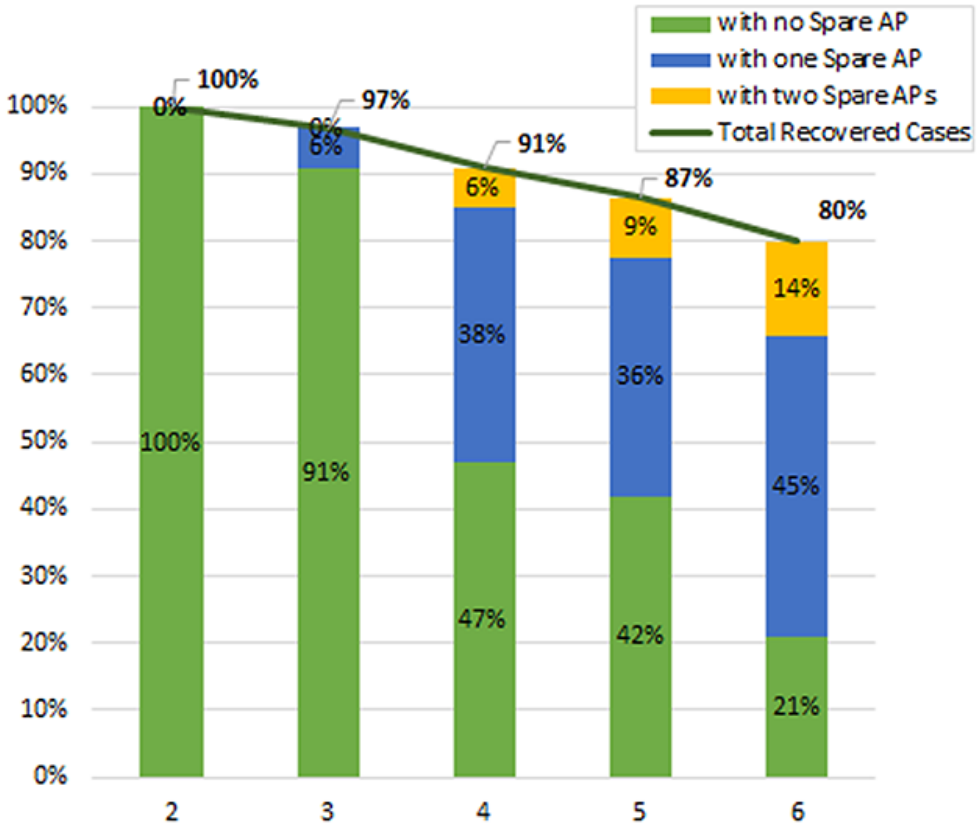


Figure. 3.32: Successful Recovery Probability with Spare APs

Fig. 3.32 shows the successful recovery probability as a function of n. Even if six routers which is one-fourth of total routers went down changed, in about 80% of the cases, the proposed method is practical.

Fig. 3.33 shows the routing (next hop router and the number of hops to the GW) and location informations of each mesh router.

ID	Name	Type	Parent	Hop	X	Y
1	1	Gateway	0	0	1375	25
2	2	Router	8	4	0	150
3	3	Router	8	4	400	100
4	4	Router	1	1	850	50
5	5	Router	1	1	1825	0
6	6	Router	5	2	2150	50
7	7	Router	6	3	2600	100
8	8	Router	9	3	375	500
9	9	Router	10	2	850	500
10	10	Router	1	1	1200	550
11	11	Router	10	2	1650	550
12	12	Router	19	5	2025	700
13	13	Router	7	4	2425	700
14	14	Router	2	5	0	725
15	15	Router	8	4	300	900
16	16	Router	21	5	875	900
17	17	Router	10	2	1350	1025
18	18	Router	17	3	1775	925
19	19	Router	18	4	2125	1125
20	20	Router	21	5	450	1250
21	21	Router	22	4	825	1325
22	22	Router	17	3	1300	1500
23	23	Router	18	4	1750	1300
24	24	Router	23	5	2225	1575

Figure. 3.33: Route and location of Mesh Router

Fig. 3.34 shows the neighbor information of mesh routers.

All Edges

Add Edges

ID	Edge Status	Link1			Link2		
		Node	Int	Mode	Node	Int	Mode
1	No status	2	1	ST	3	2	No
2	Primary	2	1	ST	8	1	AP
3	Primary	2	2	ST	14	2	AP
4	No status	3	1	ST	4	1	ST
5	Primary	3	1	ST	8	2	AP
6	Primary	1	1	AP	4	1	ST
7	No status	4	2	No	9	2	ST
8	Primary	1	1	AP	5	1	ST
9	Primary	1	2	ST	10	1	AP
10	Primary	5	2	ST	6	1	AP
11	No status	5	1	ST	11	1	No
12	Primary	6	2	ST	7	1	AP
13	Primary	7	1	AP	13	2	ST
14	Primary	8	1	AP	9	2	ST
15	Primary	8	2	AP	15	2	ST

Figure. 3.34: Neighbor Information of Mesh Router

Fig. 3.35 shows an example of reconstructed mesh network without any spare AP by the proposed method.

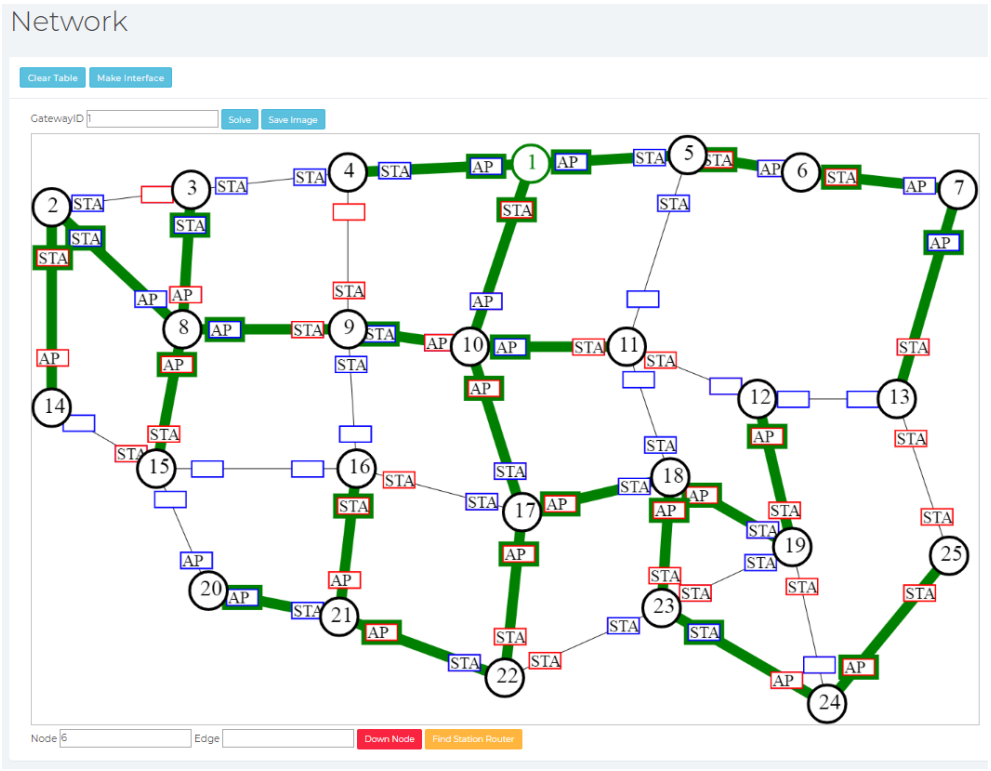
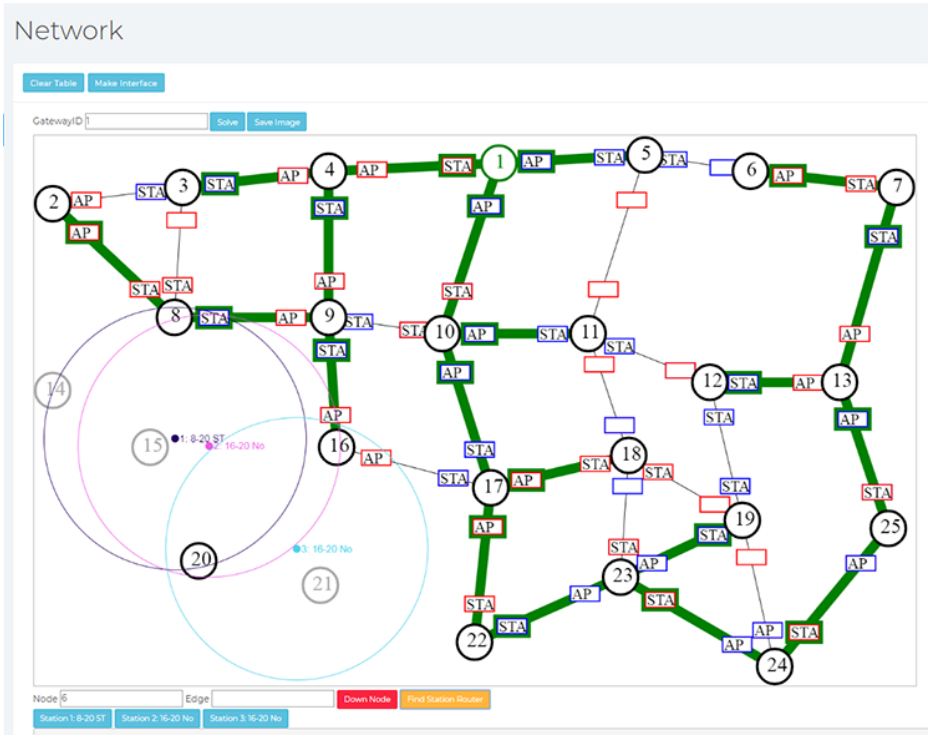
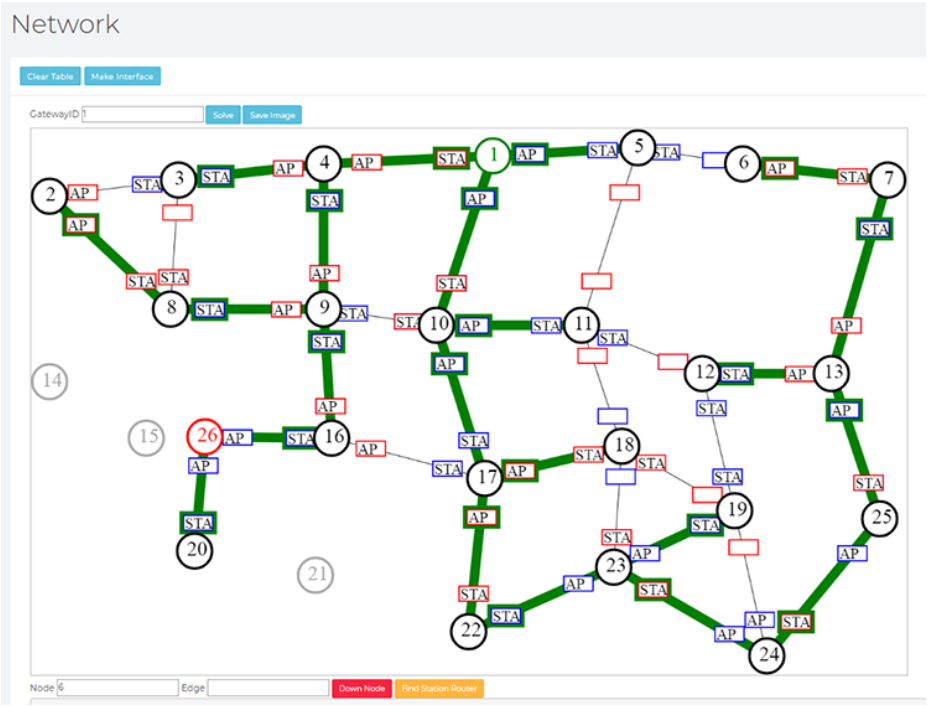


Figure. 3.35: Reconstructed Mesh Network without Spare AP

Fig. 3.36(a) shows an example of discovered spare APs whereas Fig. 3.36(b) shows an example of reconstructed mesh network with the spare AP by the proposed method.



(a)



(b)

Figure. 3.36: Reconstructed Mesh Network with Spare AP

4 Field Trial

4.1 Fundamental Experiment

In order to evaluate the basic characteristics of mesh networks in environments which is free of radio interference and obstacles, we deployed the test network topologies along Yoshino River in Tokushima city in March 13 to 15, 2018, as shown in Fig. 4.1. In this experiment we used three edge servers working in the standard IEEE 802.11g, as shown in Fig. 4.2. We demonstrated three different experiment works in single-hop and multi-hop communications with common or individual channel.

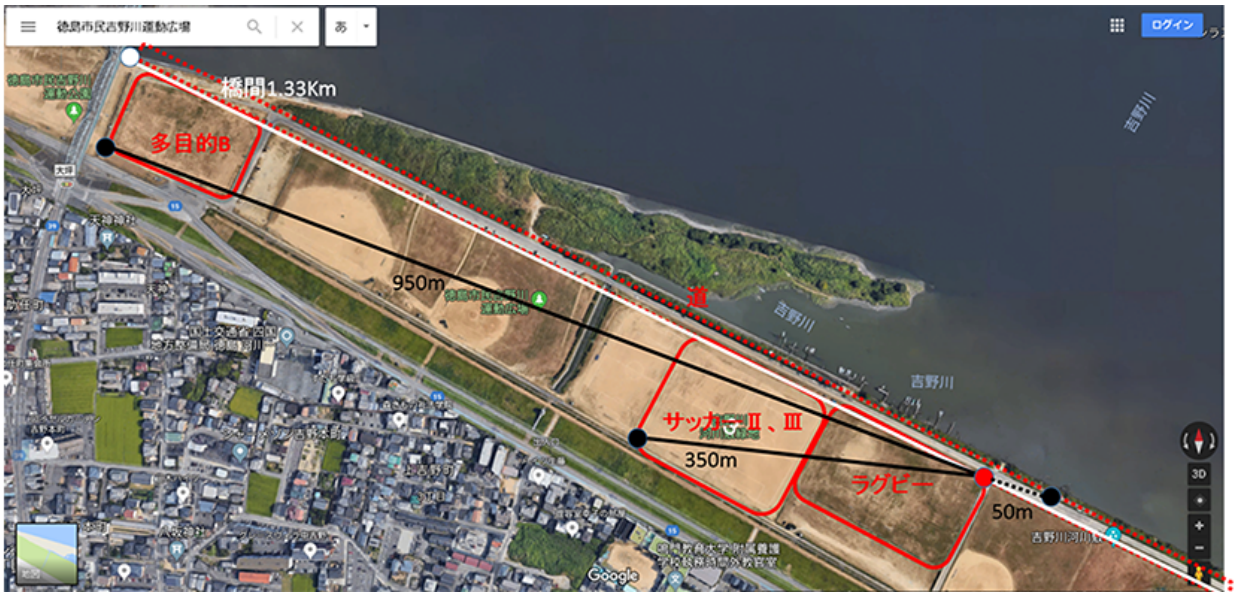


Figure. 4.1: Fundamental Experiment Place

We assumed the following requirements of the edge servers.

1. Ability to compute local information in real time
2. Ability to storage that can hold Local Dynamic Map (LDM) information efficiently
3. Wi-Fi interface configuration that builds a stable WMN and enables service provision to vehicles

4. Power supply configuration that can operate independently even in the event of a disaster

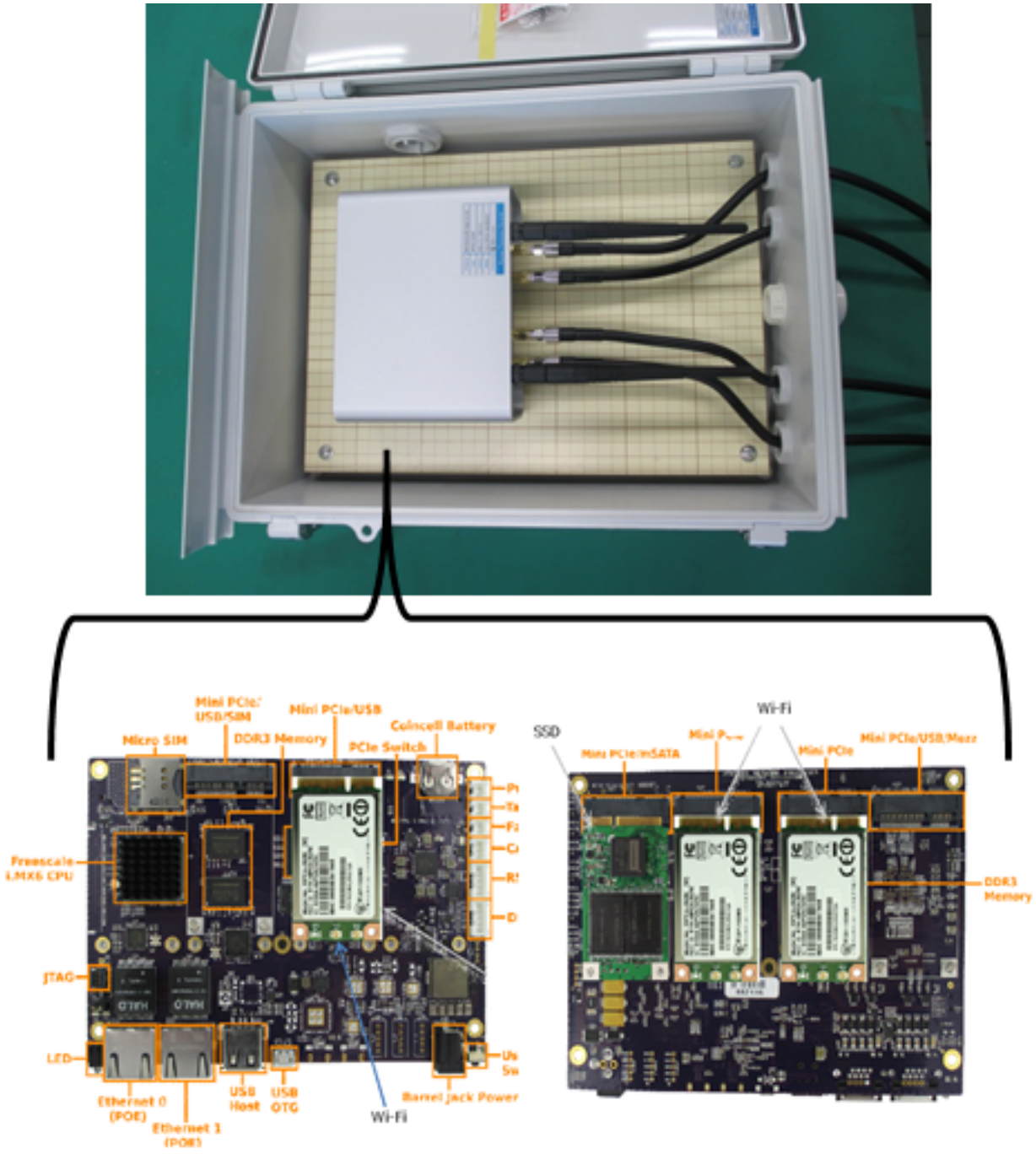


Figure. 4.2: Prototype Edge Server

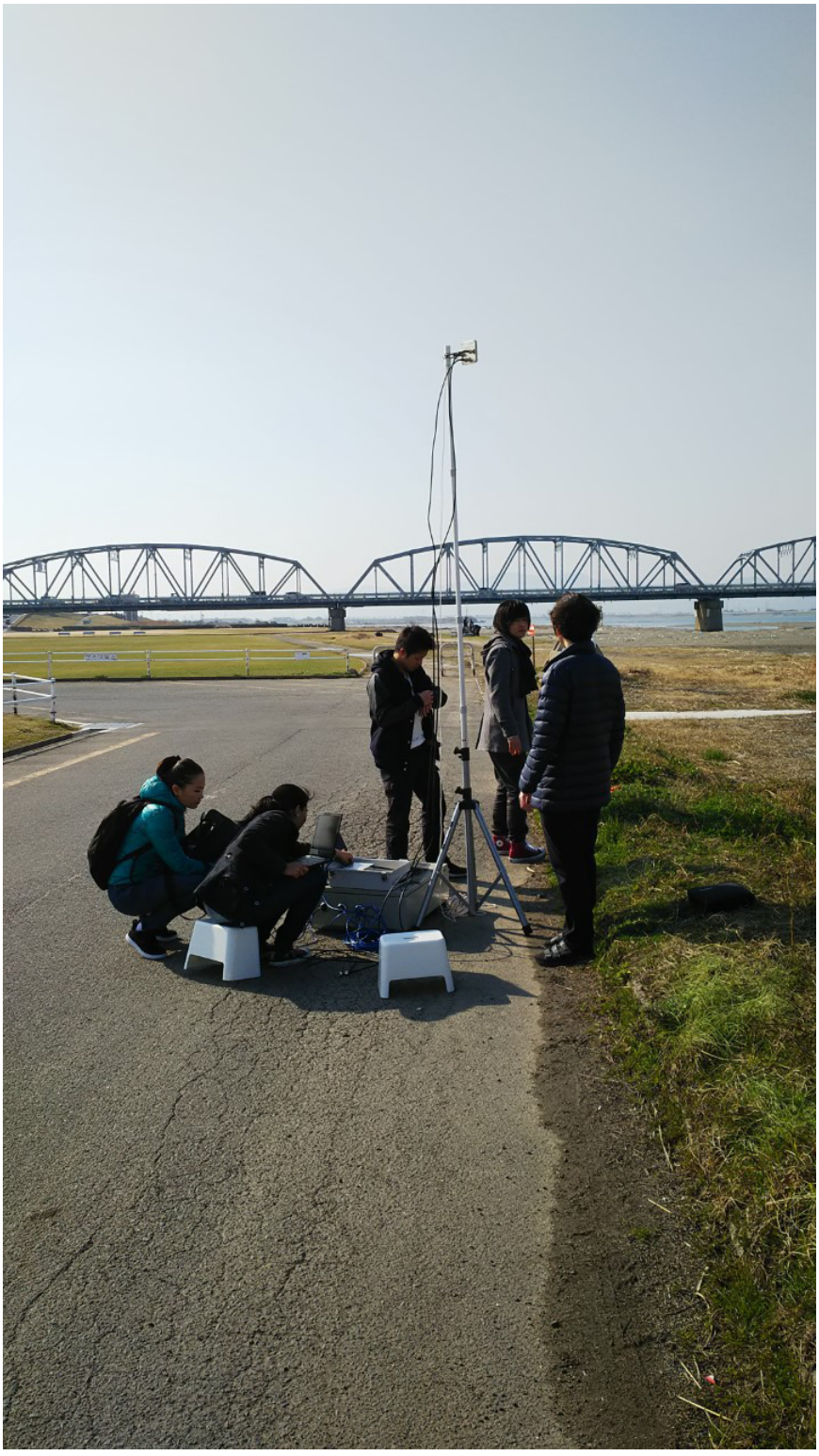


Figure. 4.3: Demonstration of Fundamental Experiment

The specification of the prototype edge server is shown in Table. 4.1.

Table. 4.1: Prototype Edge Server Specification

Specification	**Value**
CPU	Quad Core 1 GHz
Memory	2 GByte
Storage	256 GByte SSD
Wi-Fi interface	3 (IEEE802.11a / g / n)
Battery capacity	288Wh
Wi-Fi type	Infrastructure mode
Patch antenna	Gain (9 dBi), Beamwidth 60° (for mesh)
Dipole antenna	Omnidirectional, Gain (2 dBi) (for service)

A. Single-hop Communications

Two edge servers equipped with oriented directional antennas with their gain of 9 dB and height of 3 m were installed at the distance of 100m to 1200m in point-to-point network shape, as shown in Fig. 4.3.

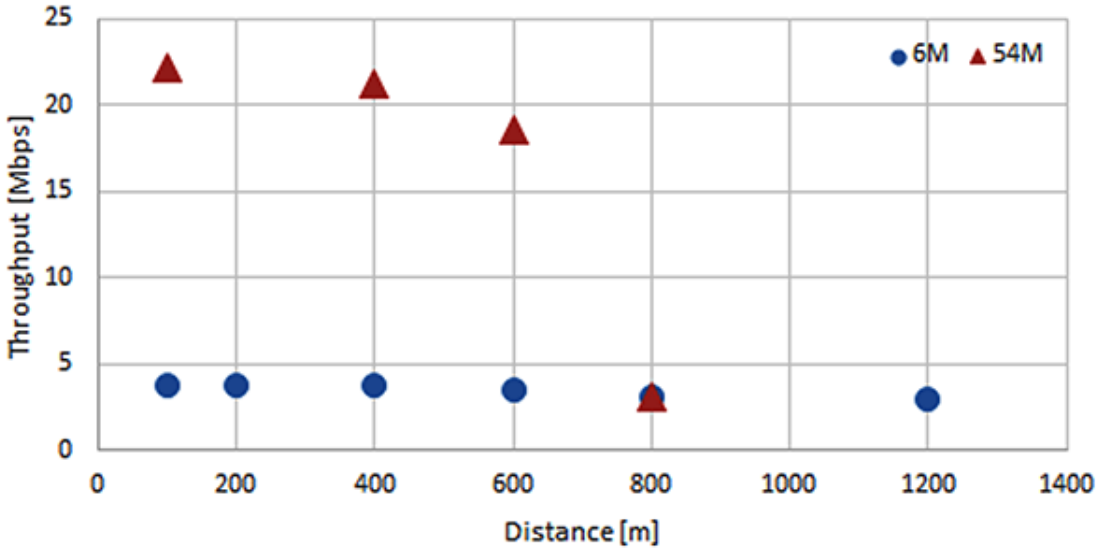


Figure. 4.4: Distance vs Throughput

One server transmitted TCP traffic another in the speed of 6 Mbps or 54 Mbps. We used the iperf software. The observed TCP throughput was illustrated in Fig. 4.4. From the experimental results, throughput of rate 54 Mbps was lower than that of rate 6 Mbps when the distance was up to more than 800 m.

B. Multi-hop Directional Communications

Three edge servers numbered 1, 2, and 3 were installed in a row at the same distance of 400 m, as shown in Fig. 4.5. Each roadside server has also radio interfaces equipped with directional antenna. 1 transmitted TCP traffic to 3 via 2. We configured channel 1 at the link between edge servers 1 and 2 whereas changed channel 1 to 7 at the link between edge servers 2 and 3 during transmission. The measured throughput was shown in Fig. 4.6.

Figure. 4.5: Topology of Multi-hop Directional Communications

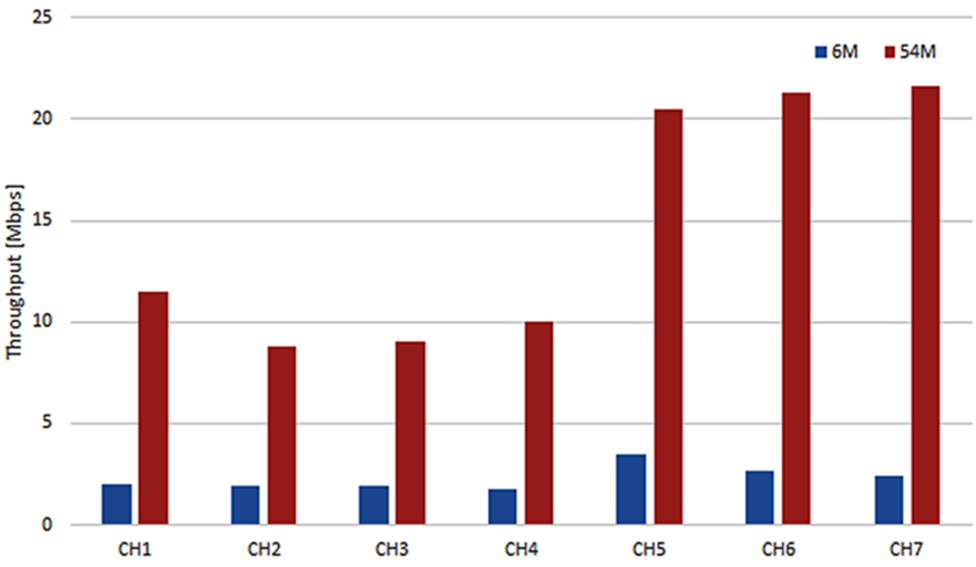


Figure. 4.6: Throughput per channel

From the experiment result, we can see that 19% to 75% of the rate of 6 Mbps and 78% to 87% of the rate 54 Mbps were used for the transmission.

C. Multi-hop Omnidirectional Communications

Four APs 1, 2, 3, and 4 were installed at the same distance of 70 m from each other, as shown in Fig. 4.7. The specification of the AP is shown in Table. 4.2. Each AP has two radio interfaces

equipped with omnidirectional antenna, as shown in Fig. 4.8. We configured source AP 1 and destination AP 4, respectively. TCP traffic were transmitted from AP 1 to AP 4 throughout APs 3 and 4 using the rate of 6 Mbps.

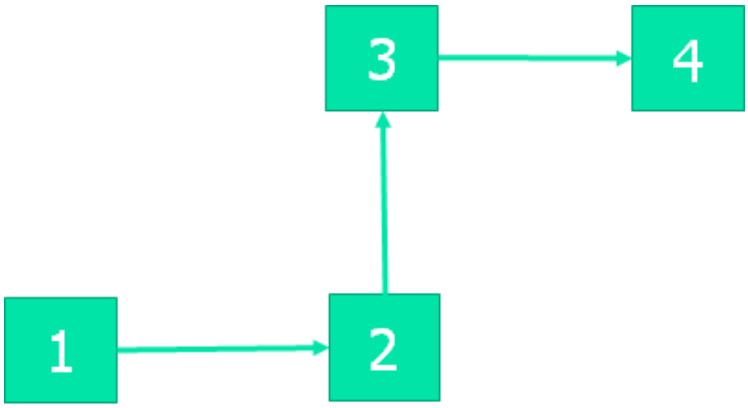


Figure. 4.7: Topology of Multi-hop Omnidirectional Communications

First, we configured the same channel 1 for each link and estimated end-to-end throughput at 4. It showed throughput of 1.11 Mbps. Second, three different channels 1, 6, and 11 were configured at links 1-2, 2-3, and 3-4, respectively. Its end-to-end throughput was 1.32 Mbps that showed the improvement of 18% compared to the case of that the same channel was set for all the links.

Table. 4.2: AP Specification

Specification	**Value**
CPU	Dual Core 1.46GHz
Memory	2 GByte
Storage	256 GByte SSD
Wi-Fi interface	2 (IEEE802.11a / g / n)
Battery capacity	42Wh
Dipole antenna	Omnidirectional, Gain (2 dBi)

(a)

(b)

Figure. 4.8: Prototype of AP

4.2 Disaster Field Experiment

We used the value of parameters confirmed by the results of the fundamental field experiment to conduct a disaster field experiment. In this experiment, we used a mobile application for firefighters or other first responders to collect radio wave conditions within the disaster area proposed in [59]. A web application has been also developed to visualize and analyze the collected RSSI information using our mobile application.

A network recovery system is composed of three main parts: (1) mobile application, (2) Web application, and (3) data manager (Scenargie®Scene Manager). The mobile application is mainly used for data acquisition. In [33, 34], the radio wave collection system has been applied for the system.

Figure. 4.9: Mobile application

The Web application is used for data visualization and analysis of the aggregated data. The data manager is used for aggregation and synchronization of the measured and calculated data from both the mobile and Web applications. The mobile application was run on Android, wherein it measures the Wi-Fi radio waves at frequencies of 2.4 GHz and 5 GHz. The user's activity (such as rescuing) is not inhibited since the application requires no special operations. Figure 4.9 shows a snapshot of the developed mobile application developed in [13].

Based on the collected data, a Wi-Fi radio map is then constructed. The collected Wi-Fi beacon data consist of the RSSI, service set identifier, channel frequency, and channel bandwidth at a certain location and time. These values are then uploaded to the data manager, and using the acquired RSSI value and position information, the radio wave status is displayed as a heat map chart on the mobile device in [59].

In order to demonstrate the effectivity of the system for disaster mesh network recovery, the system was deployed in-field in a small area near Hiwasa Station in Tokushima Prefecture, Japan, shown in Fig 4.10. As mentioned before, we were able to determine the suitable targets for equipment deployment with the aggregated information and the RSSI ranging and localization algorithm described above. Three routers equipped with directional antennas with their gain 9dB were installed at locations shown in Fig. 4.11. The routers are depicted in Fig. 4.2. They were not be able to communicate each other before installing a spare AP.

Figure. 4.10: Disaster Field Experiment Place

Figure. 4.11: Routers and Spare AP Locations

First, we collected the RSSI information using the mobile application in Fig. 4.9. Then, the RSSI ranging and localization algorithm was executed based on the collected database. Table. 4.4 shows the calculated maximum distance for each anchor point measured using the spare AP placement method with parameters in Table 4.3.

Table. 4.3: Parameters for Spare AP location Procedure

Parameters	**Value**
Minimum signal strength (P_{min})	-80dBm
Path loss exponent ($beta$)	2
Reference distance (d_0)	1m
Reference path loss ($P_L(d_0)$)	40dBm
Signal transmission power (P_t)	18dB
θ	30°

Consequently, the dashed circle in Fig. 4.11 shows the adequate area for a spare AP, which was obtained by the proposed methods with 19 anchor points in Table. 4.4. Moreover, the green, red, and yellow points are depicted as the measured anchor points R_1, R_2, and R_3, respectively. A triangle means a point where we installed a spare AP actually. When we put the spare AP at a point indicated by blue triangle, all routers had been reachable each other. On the other hand, however, when we set the spare AP at a point indicated by red triangle, one of 3 routers had been still isolated. In other words, the obtained area includes a few meters of estimation error.

Consequently, however, even if there are some obstacles such as houses, cars, and trees, the proposed method works well and successfully recovers a connection between at least two routers. It is sufficiently practical.

Table. 4.4: Measured Anchor Points for Each Router

Router	**Latitude and Longitude of Anchor points**	**Measured RSSI level [dBm]**	**The maximum distance [m]**
R1	14976129.53, 3992580.745	-76	324.447
	14976130.93, 3992552.974	-74	395.426
	14976151.16, 3992528.87	-73	480.466
	14976108.32, 3992580.196	-73	411.773
	14976169.69, 3992539.888	-77	331.406
	14976111.27, 3992586.474	-79	212.153
	14976169.75, 3992541.126	-76	372.081
	14976118.75, 3992524.394	-69	647.163
	14976027.96, 3992520.433	-68	363.675
R2	14976274.86, 3992318.037	-65	365.489
	14976136.37, 3992559.73	-89	120.531
	14976015.41, 3992256.352	-87	119.718
	14976151.16, 3992528.87	-82	242.48
	14976129.53, 3992580.745	-78	454.787
	14976264.19, 3992320.674	-70	220.988
R3	14976174.81, 3992499.515	-84	156.321
	14976170.73, 3992536.529	-83	149.242
	14976167.16, 3992733.671	-46	813.175
	14976118.28, 3992544.232	-79	236.884

Figure. 4.12: Router Implementation of Disaster Field Experiment

Figure. 4.13: Spare AP Implementation of Disaster Field Experiment

5 Discussion and Conclusion

To summarize our study, chapter 2 introduced the fundamentals of WMNs, range-based localization algorithms in WMNs, and application of infrastructure mode in WMNs. In our findings, RSSI-based localization algorithm was suitable for defining optimal locations of spare APs. Also, according to the past literature works, no existing works are able to assign suitable infrastructure mode to each interface of mesh router in distributed manner.

Chapter 3 described both methods. First, we described our formulated RSSI-based ranging and localization algorithm of the spare AP placement method. The algorithm was executed 500 different cases of a full mesh network and another 500 different cases of partial mesh network, respectively. Even if 5 routers went down, successful recover probabilities of the partial and full mesh networks, recovered by only one spare AP were 68% and 69%, respectively. Therefore, the method is practical. Second, we presented the whole process of the interface mode assignment method and confirmed its effectiveness as executing over than 11 execution cases. The practicability of the method has been proved the performance evaluation to reconstruct 2500 different cases of an assumed WMN without any spare AP and 1500 different cases of the assumed WMN with one or two spare APs. Since the successful recover probabilities of both scenarios were 80% and more, this method is also practical.

Chapter 4 conducted fundamental and disaster field experiments of the spare AP placement method. In the fundamental field experiment, single-hop and multi-hop communications of WMNs were performed and then suitable relation of RSSI levels and distances was determined. After that, we conducted the disaster field experiment to discover the adequate location of a spare AP to communicate three routers.

Self-configuration and self-organization play a crucial role in maintaining WMNs. With the capabilities, WMNs can accomplish flexible network architecture, easy deployment and configuration, fault tolerance, and mesh connectivity. However, these kinds of the ad-hoc mesh networks are considered to be unpractical infrastructure so that developers have gained much attention to the widely-used the standard IEEE 802.11 infrastructure mode as considering ease of practical use and cost reduction. Since an enormous disaster strikes, some mesh routers go down so that others can be isolated from the backbone network. In this thesis, we presented an effective approach to implement self-reconstruction the IEEE 802.11 infrastructure mode based mesh network, more

specially for providing a connection to the isolated routers with spare APs.

To achieve the goal of our proposed method, we developed two methods such as a spare AP placement and an interface mode assignment. In the spare AP placement method, we elaborate two phases; connectivity restoration phase and rerouting phase. In the connectivity restoration phase, we determined adequate points for installing spare APs that provide one or more connections between all the isolated nodes to one or more connected nodes. In the rerouting phase, we reconstructed fully a routing tree from each isolated router to its serving gateway based on the candidate topology by one or more spare APs. As a result, each isolated router will have its own primary route consisting of primary links along the path from the isolated node to the gateway. In order to obtain adequate locations for spare APs, we formulated an RSSI-based ranging and location as well as a mode selection algorithm in order to build a converged network. Simulation results showed that the proposed method achieved the satisfaction degree of successful recovery for each failure scenarios using the minimum number of spare APs. In addition, as a result of the field trial, the location points of the adequate area for installing spare AP were successfully defined. We consider that only public workers without any experience with wireless communication technologies must decide upon the adequate locations for spare APs and install them.

Next, routes are reconstructed from isolated routers to the wired network in the recovered topology using interface mode selection algorithm, which can provide automatically an appropriate infrastructure mode such as AP and STA to radio interfaces in order to establish neighbor relationship between an isolated router and its parent node, providing the best route to it. As a result, all the isolated routers can be reachability to the wired network. The process of the method must be executed in a distributed manner. We elaborated two phase of the method such as a tentative routing and an interface mode selection. The tentative routing phase allowed an isolated router to find a route to a GW and then the mode selection phase was executed for the isolated router. As all the isolated router became reachable to the GW, the mesh network has been fully reconstructed.

As a future work, I will evaluate the performance of the interface mode assignment method in an extended network topology.

Acknowledgement

First of all, I would like to give my sincere thanks to my honorific supervisor Professor Kazuhiko Kinoshita of the Department of Information Science and Intelligent Systems in Graduate School of Advanced technology and Science, Tokushima University, who accepted me as his Ph.D student without any hesitation when I introduced him my research proposal. Thereafter, he always offered me his great supervision, continuing encouragement, valuable discussions, academic advises, and various supports throughout my studies and the preparation of this manuscript. I would like to express my feeling that I have learned a lot from him. Also, I could not have finished my research work and dissertation successfully without his help.

Special thanks are also given to Associate Professor Kenji Ikeda of the Department of Information Science and Intelligent Systems in Graduate School of Advanced technology and Science, Tokushima University, who supported me to become a PhD student. I must also acknowledge the kind assistance, comments and various assists of him.

I would like to give a special thanks of gratitude to Professor Khishigjargal Gonchigsumlaa of School of Information and Communication Technology, Mongolian University of Science and Technology. She helped me to find a supervisor when I expressed my desire to pursue my PhD research further. She also gave me the golden opportunity to participate an international joint project, which helped me a lot of experience in doing a research work and I came to know about so many new things.

I would like to express my sincere appreciation to the Higher Engineering Education Development Project that JICA has been implementing since 2014, named Mongolia Japan Engineering Education Development (MJEED). I have been participating in joint research funded by MJEED since 2016 under Professor Kishigjargal Gonchigsumlaa. In 2017, I received a great opportunity to study doctoral program in Japan and full financial support from MJEED.

I also appreciate Professor Otgonbayar Bataa of School of Information and Communication Technology, Mongolian University of Science and Technology. Her encouragement and help made me feel confident to fulfill my desire and to overcome every difficulty I encountered.

I would like to express my eternal appreciation towards my husband Munkhbayar Khurelbaatar and my son and parents who have always been there for me no matter where I am, for all unconditional support and patience. Thank you for being ever so understanding and supportive.

Besides, I would like to thank Ms. Jovilyn Fajardo and Mr. Taka Maeno of Space-Time engineering, Japan. They helped me do field trials and finish my first journal paper.

Finally, I am particularly grateful to the fellow student at laboratory, who have willingly helped me out with their abilities.

Bibliography

[1] I. F. Akyildiz, X. Wang, and W. Wang (2005) “Wireless mesh networks: a survey,” Computer Network ISDN Systems, Vol. 47, No. 4, pp. 445–87.

[2] D. Benyamina, A. Hafid, and M. Gendreau, “Wireless Mesh Networks Desgin - A Survey,” IEEE Communications Survey & Tutorials, Vol. 14, No.2, Second Quarter, 2012.

[3] K. Sohraby, D. Minoli, and T.Znati (2007) “Wireless Sensor Networks: Technology, Protocols, and Applications,” John Wiley & Sons, Inc., Hoboken, New Jersey.

[4] K. Umesh, G. Himanshu, and R.D. Samir (2006) “A Topology Control Approach to Using Directional Antennas in Wireless Mesh Network,” IEEE International Conference on Communications.

[5] A. Capone, I. Filippini, and F. Martignon (2008) “Joint Routing and Scheduling Optimization in Wireless Mesh Networks with Directional Antennas,” IEEE International Conference on Communications.

[6] M. Rajesh and J. M. Gnanasekar (2015) “Routing and Broadcast Development for Minimizing Transmission Interruption in Multirate Wireless Mesh Networks using Directional Antennas,” Innovative Systems Design and Engineering, Vol. 6, No. 7, pp. 30–42.

[7] X. Bao, L. Han, C. Deng, H. Zhang, and W. Tan (2016) “Robust Topology Construction Method with Radio Interface Constraint for Multi-rado Multi-channel Wireless Mesh Network using Directional Antennas,” International Journal of Distributed Sensor Networks, Vol. 16(9), pp. 1–14.

[8] A. Alotaibi and B. Mukherjee (2012) “A Survey on Routing Algorithm for Wireless Ad-Hoc and Mesh Networks,” Computer Networks, Vol. 56, Iss. 2, pp. 940-965.

[9] W. Ahmad and M. K. Aslam (2009) “An Investigation of Routing Protocols in Wireless Mesh Networks under certain Parameters,” Master Thesis, Blekinge Institute of Technology, Karlskrona Campus, Sweden.

[10] M. Portmann and A. A. Pirzada (2008) “Wireless Mesh Networks for Public Safety and Crisis Management Applications,” IEEE Internet Computing, Vol. 12, Iss. 1, pp. 18–25.

[11] R. B. Dilmaghani and R. R. Rao (2008) “Hybrid Wireless Mesh Network with Application to Emergency Scenario,” Journal of Software, Vol. 3, No. 2, pp. 52–60.

[12] A. Yarali, B. Ahsant, and S. Rahman (2009) “Wireless Mesh Networking: Key Solution for Emergency & Rural Applications,” Second International Conference on Advances in Mesh networks.

[13] S. Vural, D. Wei, and K. Moessner (2013) “Survey of Experimental Evaluation Studies for Wireless Mesh Network Deployments in Urban Areas towards Ubiquitous Internet,” IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, pp. 223–239.

[14] M. Q. Quang, K. Nguyen, E. Kamioka, and S. Yamada (2013) “Tree-based disaster recovery multihop access network,” 19th Asia-Pacific Conference on Communications (APCC13), pp. 415–420.

[15] M. Q. Tran, K. Nguyen, and S. Yamada (2013) “DRANs: resilient disaster recovery access networks,” First IEEE International Workshop on Future Internet Technologies (IWFIT), in Conjunction with IEEE COMPSAC, pp. 754–759.

[16] V. G. Menon, J. P. Pathrose, and J. Priya (2016) “Ensuring Reliable Communication in Disaster Recovery Operations with Reliable Routing Technique,” Mobile Information Systems, Vol. 2016, Article ID. 9141329, pp. 1–10.

[17] R. Miura, M. Inoue, Y. Owada, K. Takizawa, F. Ono, M. Suzuki, H. Tsuji, and K. Hamaguchi (2013) “Disaster-Resilient Wireless Mesh Network - Experimental Test-bed and Demonstration,” 16th International Symposium on Wireless Personal Multimedia Communications.

[18] Chaitany, K. Gupta, and C. Chakraborty (2017) “Efficient Routing Algorithm for Disaster Recovery over Wireless Mesh Networks Based Communication System,” IEEE 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).

[19] Y. Owada, J. Byonpyo, H. Kumagai, Y. Takahashi, M. Inoue, G. Sato, K. Temma, and T. Kuri (2018) “Resilient Mesh Network System Utilized in Areas Affected by the Kumamoto Earthquakes,” 5th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM).

[20] A. Xie, X. Wang, G. Maier and S. Lu (2014) “Designing a Disaster-resilient Network with Software Defined Networking,” IEEE 22nd International Symposium of Quality of Service (IWQoS).

[21] K. Nguyen, T.M. Quang, and S. Yamada (2013) "A software-defined networking approach for disaster-resilient WANs," IEEE 22nd International Conference on Computer Communications and Networks (ICCCN), pp. 1–5

[22] J. Gupta, P. K. Bedi, and N. Gupta (2011) " Fault Tolerant Wireless Mesh Network: An Approach, " International Journal of Computer Applications, Vol. 23, No. 3, pp. 43–46.

[23] P. Sharnya and J. S. Raj (2013) " Self Organizing Wireless Mesh Network, " International Journal of Innovation and Applied Studies, ISSN 2028-9324, Vol. 3, No 2, pp. 486–492.

[24] K. Pendke and S. U. Nimbhorkar (2013) " Reconfiguring Wireless Mesh Network Using Link Recovery Technique, " IRACST - International Journal of Computer Networks and Wireless Communications, ISSN:2250-3501, Vol. 3, No.3, pp. 257–260.

[25] S. K. Singh and P. K. Manjhi (2016) " Fault Tolerance Issue in Wireless Mesh Network, " Imperial Journal of Interdisciplinary Research (IJIR), Vol. 2, Iss. 5, pp. 874–885.

[26] G. Murugaboopathi, P. Sharmila, P. A. Partibhan and R. Sivakumar (2013) " Feasibility based Reconfiguration Approach for Recovery in Wireless Mesh Networks, " International Journal of Recent Scientific Research, Vol. 4, Iss. 5, pp. 592–596.

[27] K. H. Kim and K. G. Shin (2011) " Self-Reconfigurable Wireless Mesh Networks, " IEEE/ACM Transactions on Networking," Vol. 19, Iss. 2, pp. 393–404.

[28] Y. Peng, Q. Song, Y. Yu, and F. Wang (2013) " Fault-Tolerant Routing Mechanism based on Network Coding in Wireless Mesh Networks, " Journal of Network and Computer Applications, Vol. 37, pp. 259–272.

[29] A. Pal (2010) " Localization algorithms in Wireless Sensor Networks: Current Approaches and Future Challenges, " Network Protocols and Algorithms, Vol.2, No. 1, pp. 45–74.

[30] T. He, C. Huang, B. M. Blum, J.A. Stankovic, and T. Abdelzaher (2003) "Range-free Localization Schemes for Large Scale Sensor Networks, " 9th Annual International Conference on Mobile Computing and Networking.

[31] H. Wang, Z. Gao, and Y. Huang (2012) " A Survey of Range-based Localizatio Algorithms for Cognitive Radio Networks," Second International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 844–847.

[32] A. Shojaifar (2015) "Evaluation and Improvement of the RSSI-based Location Algorithm," Doctoral Thesis, Faculty of Computing Institute, Blekinge Institute of Technology, Karlskrona, Sweden.

[33] M. Yassin and E. Rachid (2015) “ A Survey of Positioning Techniques and Location based Services in Wireless Network, ” IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES).

[34] Z. Zhang. G. Wan, M. Jiang, and G. Yang (2011) “Research of an adjacent correction positioning algorithm based on RSSI-distance measurement,” 8th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 2319—2323.

[35] J. Fajardo, T. Maeno, and K. Kinoshita (2018) “A Radio Wave Condition Collection System for Mesh Network Recovery During Disasters,” IPSJ Multimedia, Distributed, Cooperative, and Mobile Symposium (DOCOMO 2018), pp. 1752–1755.

[36] J. Fajardo and K. Kinoshita (2018) “Implementation of a Radio Wave Condition Collection System for Disaster Mesh Network Recovery, ” IEICE General Conference, B15-15.

[37] J. Fajardo, T. Maeno, and K. Kinoshita (2019) “ Application of the Radio Wave Condition Collection System for Determining the Spare AP Location, ” IEICE General Conference, B15-25.

[38] M. Baunach, R. Kolla, and C. Muhlberger (2007) ”Beyond Theory: Development of a Real World Localization Application as Low Power WSN,” 32nd IEEE Conference on Local Computer Networks, pp. 872–884.

[39] W. Chongburee, V. Vikiniyadhanee, and P. Chittisathainporn (2009) ”Formula and Performance Simulation of a Signal Strength Based Position Estimation in Lognormal Channels,” 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, pp. 924– 927.

[40] M. Tsai (2011) ”Path-loss and Shadowing (Large-scale Fading),” https://www.csie.ntu.edu.tw/.

[41] Z. Deng, W. Ren and L. Xu (2008) ”Localization algorithm based on difference estimation for wireless sensor networks in Pervasive Computing Environment,” International Conference of Pervasive Computing and Applications.

[42] K. N. Ramachandran, M. M. Buddhikot, G. Chandranmenon, S. Miller, E. M. Belding-Royer, and K. C. Almeroth (2005) “On the Design an Implementation of Infrastructure Mesh Networks,” IEEE Wireless Communication.

[43] V. Navda, A. Kashyap, and S. R. Das (2005) “ Design and Evaluation of iMesh: An Infrastructure-mode Wireless Mesh Network, ” 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks.

[44] S.C. Yang, M.K. Yoon, D.H. Kim, and J.D. Kim (2010) "Implementation of a multi-radio, multi-hop wireless mesh network using dynamic WDS based link layer routing," 7th International Conference on Information Technology, pp. 908–913.

[45] H. Wirtz, T. Heer, T. Backhaus, and K. Wehrle (2011) " Establishing Mobile Ad-Hoc Networks in 802.11 Infrastructure Mode, " 6th ACM workshop on Challenged networks, pp. 49–52.

[46] M.H. Sarshar, P.K. Hoong, and I.A. Abdurrazaq (2013) "Nodesjoints: a framework for tree-based MANET in IEEE 802.11 infrastructure mode" 2013 IEEE Symposium on Computers & Informatics (ISCI), pp. 190–195.

[47] D. Camps Mur, A. Garcia, and P. Serrano (2013) "Device to device communications with wi-fi direct: overview and experimentation," IEEE Wireless Communication. Mag., 20 (3), pp. 96–104.

[48] J. Chen, S. H. Gary Chan, J. He and S. Liew (2003) " Mixed-Mode WLAN: The Integration of Ad Hoc Mode with Wireless LAN Infrastructure, " IEEE GLOBECOM, pp. 231—235.

[49] D. J. Dubois, Y. Bando, K. Watanabe and H. Holtzman (2013) "Lightwieght Self-organizing Reconfiguration of Opportunistic Infrastructure-mode WiFi Networks, " IEEE 7th International Conference on Self-Adaptive and Self-Organizing Systems, pp. 247–256.

[50] S. Trifunovic, B. Distl, D. Schatzmann and F. Legendre (2011) " WiFi-Opp: Ad-Hoc-less Opportunistic Networking, " 6th ACM workshop on Challenged networks, pp. 37–42.

[51] G. S. L. K. Chand, M. Lee, and S. Y. Shin (2018) "Drone Based Wireless Mesh Network for Disaster/Military Environment," Journal of Computer and Communications, Vol. 6, pp. 44–52.

[52] M. Arisoylu, R. Mishra, R. Rao, and L. A. Lenert (2005) "802.11 Wireless Infrastructure To Enhance Medical Response to Disasters," AMIA Annual Symposium Proceedings Archieve.

[53] Q. T. Minh, Y. Shibata, C. Borcea, and S. Yamada (2016) "On-site Configuration of Disaster Recovery Access Networks Made Easy, " Ad Hoc Networks, Vol. 40, pp. 46–60.

[54] Y. Owada, B. Jeong, N. Katayama, K. Hattori, K. Hamaguchi, M. Inoue, K. Takanashi, M. Hosokawa, and A. Jamalipour (2016) " An Implementation of Multichannel Multi-Interface MANET for Fire Engines and Experiments with WINDS Satellite Mobile Earth Station, " IEEE Wireless Communications and Networking Conference.

[55] J. Kurose and K. W. Ross (2017) “Computer Networking: A Top-Down Approach,” 7th Edition.

[56] M. S. Gast (2005) “802.11 Wireless Networks: The Definitive Guide,” 2nd Edition.

[57] E.Dorj and K.Kinoshita (2018) “A Routing Method for Wireless Mesh Networks based on IEEE 802.11 Infrastructure Mode in Disaster Situation,” IEICE General Conference, BS2-7.

[58] E.Dorj and K.Kinoshita (2018) “A Route Reconstruction Method with Spare AP for Wireless Mesh Networks in Disaster Situation,” International Symposium on Computers and Communications (ISoCC2018).

[59] E.Dorj and K.Kinoshita (2019) “Automatic Mode Selection Method for Disaster Recovery in Wi-Fi Mesh Networks,” IEICE Society Conference, BS2-7.

[60] “Scenargie,” http://www.spacetime-eng.com/.

[61] “ns-3 Tutorial Release ns-3.26,” https://www.nsnam.org/.