Reliable Multihop Wireless Network Based on Neighbor Node Behavior

Daiki NOBAYASHI

Preface

With the spread of the Internet, many researchers have focused on various methods of network construction that offer improved communication performance. A wireless local area network (LAN) adhering to the IEEE 802.11 standard can connect terminals to the Internet using wireless communication. Wireless LANs are widely used in universities, businesses, and homes among other places. It is easy to construct a wireless LAN, since terminals join the LAN by connecting to an access point (AP) that connected to an existing network. However, two or more APs are necessary for the construction of a wireless LAN with a large range, because the effective range of wireless communications is at most 50 m. When two or more APs are configured in an existing wireless LAN, an administrator must connect each AP to an existing network with a cable. This increases the cost and effort required for installation and management of the network. A multihop wireless network (MWN), in which APs connect to each other using radio communication, is thus the focus of many researchers.

In an MWN, little effort is required to expand the area covered by wireless access because each new AP requires only wireless communication with another AP. A cable is not necessary because the APs wirelessly communicate with each other. Thus, an MWN offers low-operating cost and high availability. However, the ease with which an MWN can be expanded significantly influences the network's availability. An environment in which an individual AP cannot transmit packets, for example, because of damage (electrical outage or failure), a selfish or malicious AP, or radio waves in the area, negatively affects the entire network. To maintain network availability, the APs that constitute an MWN must be highly

reliable. Therefore, a mechanism is required by which each AP autonomously evaluates the reliability of the network and deals appropriately with misbehaving APs.

Chapter 2 describes the basic wireless LAN technology and the MWN. We also describe threats to which MWNs are vulnerable, for example, behavior of an unexpected, selfish, and malicious node.

In Chapter 3, we propose a scheme by which APs in an MWN can evaluate neighboring APs by using the packet transfer rate. Existing schemes for detecting misbehavior in a mobile ad hoc network assume an environment with a single interface/radio. Thus, each node on these schemes can overhear the behavior of neighboring nodes. However, an MWN, such as a wireless mesh network, can use a node with multiple interfaces/radios to enhance communication performance. In this case, it is difficult to use existing schemes of misbehavior detection because nodes cannot overhear the behavior of neighboring nodes. Thus, we propose an evaluation scheme in which a target AP is monitored by peripheral APs. Each AP shares its monitoring results with the other peripheral APs and evaluates the behavior of the target AP. In this context, we verify this scheme using a network simulation, and demonstrate that it can correctly detect misbehaving APs in an MWN.

In Chapter 4, we describe the design and implementation of the scheme proposed in Chapter 3, to verify that it can be used in an actual MWN. APs with multiple interfaces/radios are created using a small personal computer. Because the APs implement the proposed scheme, we demonstrate that each AP correctly evaluates the misbehavior of other APs by monitoring packet transfer. Furthermore, each AP can autonomously reconstruct a network that eliminates the problematic AP after detecting misbehavior. As a result, we show that our proposed scheme yields a reliable multihop wireless network.

In Chapter 5, we proposed a novel network reconfiguration scheme to maintain the network performance of MWNs. In this scheme, each node reconstructs the network autonomously using the interfaces of neighboring nodes linked to a misbehaving node. The proposed scheme reconfigures a topology with an emphasis on interface reuse, the number

of links required to build the network, transmission rates, performance anomaly, and network connectivity. We evaluate the effectiveness of the proposed schemes by a simulation. We show that the simulation results indicate that the proposed scheme can prevent degradation of the communication performance of the entire MWN.

Finally, we hope that this dissertation will be helpful for achieving reliable multihop wireless networks.

Mar. 2011

Daiki NOBAYASHI

Acknowledgements

I would like to acknowledge the support and encouragement received from a number of people for several years.

First of all, I wish to express my sincere appreciation to Associate Professor Takeshi Ikenaga of Kyushu Institute of Technology. His constant encouragement, guidance through this research, invaluable discussions and advice have greatly helped in accomplishing the research. I also thank him for his careful reading of all papers on the research.

I wish to thank Professor Seiichi Serikawa, Professor Nobuo Kuwabara, and Professor Yoshihiko Tagawa of Kyushu Institute of Technology for their invaluable discussions and comments.

I also would like to express my gratitude to Associate Professor Yoshiaki Hori of Kyushu University and Associate Professor Yutaka Nakamura of Kyushu Institute of Technology for their valuable comments, time and help in completing the research. Their steady support has greatly helped my study.

I wish to thank Professor Yuji Oie and Masato Tsuru, Associate Professor Kenji Kawahara, Assistant Professor Yutaka Fukuda, Hitomi Tamura and Kazuya Tsukamoto, and Dr. Masayoshi Shimamura of Kyushu Institute of Technology for their invaluable discussions and comments.

I would like to express my gratitude to Mr. Takashi Sera now in SEIKO EPSON Corporation concerning the work in Chapter 5 for his precise works and comments.

I am very grateful to Associate Professor Katsuyoshi Iida of Tokyo Institute of Technol-

ogy and Hiroyuki Koga of University of Kitakyushu for their kind instructions and invaluable discussions.

I extend thanks to Mr. Koji Tsubouchi, Mr. Kei Higashijima, Ms. Fumie Miki, Mr. Yuki Nakata, and all other members of the Network Engineering Research Group at Kyushu Institute of Technology for their kindly supports and valuable discussions.

Finally, my greatest appreciation goes to my parents, Shirou and Yukiko Nobayashi, and my sister and her husband, Maiko and Youichirou Okita, for their understandings and supports for me. And, I extend thanks to Mr. Takuya Aoki, Mr. Kazuya and Mrs. Izumi Norimura, Mr. Koji Kuramoto, and all other friends for their constant supports.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The Internet is a worldwide network that links billions of computers in homes, universities, businesses, and government among others. The Internet was originally developed for military applications, and later spread to universities and research laboratories. In the 1990s, Internet use became wide spread among ordinary users with the development of TCP/IP and the decreasing cost of computers. The number of Internet users is estimated to have reached approximately two billion as of 2010 [WOR].

With the growth of the Internet, various online services were deployed. For example, services using the Internet provide not only World Wide Web (WWW), e-mail, and e-commerce but also streaming, document creation, spread-sheet, creation and maintenance, and management of individually owned information. To use these services, users connect to the Internet via a terminal. Thus, in the Internet society of the future, the construction of access networks on which users can access the Internet anytime and anywhere is an important issue.

Many researchers have been focusing on multihop wireless networks (MWNs) as they are highly flexible and extensible access networks. In an MWN, access points (APs) using a wireless local area network (LAN) jointly constructs an access network. Because all the APs do not need to be connected to cable infrastructure, a network with a low up-front cost can be easily constructed. However, this flexibility makes the APs in such a network considerably vulnerable to malicious users. In this dissertation, we focus on the construction of reliable, autonomous multihop wireless network.

This chapter is organized as follows. In section 1.1, we introduce the types of services

that use the Internet and describe the requirements of a novel access network. In particular, we give an overview of wireless LANs as a conventional access network. In section 1.2, we introduce MWNs and describe how they are typically used. Finally, we demonstrate the challenges of MWNs and outline this dissertation in section 1.3.

1.1 Services Using Internet and Requirements for Internet Access Network

The Internet has grown explosively owing to the increasing diversification of network media and the devices that deliver it. At the dawn of the Internet age, communication was achieved using coaxial cables. Communication over optical fiber and various wireless modes has recently become possible, and the available communication bandwidth has also become very large. Furthermore, the Internet is accessed through not only computers but also mobile terminals such as cellular phones and various types of sensors. As a result, many people can use the Internet, and the number of users increases every year.

The increase in users provides a great opportunity for many enterprises that do business on the Internet to obtain profit. These enterprises provide services of various types. When Internet usage began to spread, it was used for information-gathering using WWW and individual communication using e-mail. Many Internet services have emerged more recently, for example, video conferencing, sharing photos and movies, document creation, and creating and maintaining spread-sheets. Furthermore, in conventional usage, various operations are performed on a user's terminal, and data are shared over Internet. In contrast, the use of services, such as grid computing, which effectively uses computational resources existing in a network or on the Internet, has recently begun to spread. The Internet has achieved wide general usage as a result of breakthroughs in technology, and today many users depend on the Internet for a variety of services.

To use these services, a user should be able always be able to connect to a network that

provides these services, or to the Internet. User can easily access the Internet by using the cellular phone network. Because the communication range of one base station is vast, users can communicate in many locations. However, to expand the area covered by the network, a carrier must set up many expensive base stations. Furthermore, network management is considerably difficult and the operation cost increases because the number of users is very large.

On the other hand, wireless LANs that operate in accordance with the IEEE 802.11 standard also offer Internet access. The peak communication rate of a wireless LAN can reach many hundreds of Mb/s. To wirelessly access the Internet, users need only connect to an AP with an Internet connection, which serves as a base station for a wireless LAN. APs are currently very inexpensive, so a user can easily buy and use one. Users anywhere in a wireless communication area provided by an AP can access the Internet. As a result, wireless LANs that meet the IEEE 802.11 specification are common in offices, homes as the access technology connecting users' terminals to the Internet. However, two or more APs are needed to construct a wireless LAN with a large range because the effective range of wireless communications is at most 50 m. With this method of expanding a wireless LAN, the cost and effort required for installation and management increase because each AP must be connected to the Internet by a cable. An alternative, the MWN, in which APs connect to each other using radio communication, is thus the focus of many researchers.

1.2 Multihop wireless networks

MWNs are expected to be developed as a newer architecture for network access infrastructure. In an MWN, the APs connect with each other using wireless communication, and forward data packets to each other. Because a cable infrastructure using need not be built to each AP, a network with a low up-front cost can easily be constructed. Furthermore, an MWN is self-organizing and self-configuring, since each AP in the network configures and maintains itself autonomously. A user can access the MWN using any terminal with a wire-

less network interface card. Thus, the user can always access the Internet at any location. Below we describe some feature of an MWN and examples of MWN operation.

First, small and medium-sized MWNs are very easy to build. When another AP is within wireless communications range of an AP that is part of an MWN, those APs form a network by constructing a mutual connection. An administrator sets up APs depending not on where cable can be laid, but rather on the range at which APs can be communicate with each other. The administrator can construct an efficient network by appropriately setting up APs.

For example, Fig. 1.1 shows an MWN in a shopping area. When a service provider wants to present digital signage, the provider constructs a low-cost wide-area network by using an MWN. As a result, each shop updates its advertisements through the network, and users check for the latest information from each shop by accessing the MWN with a portable terminal, such as a cellular phone or PDA. Furthermore, Fig. 1.2 shows an example of an MWN in a company's offices. Whether an administrator wants to construct a network within one of the company's buildings or among different buildings, an MWN can easily provide the needed network. Because the administrator can construct a network simply by installing an AP on each floor or office, a sketch of the building and a complex design proposal for cable construction are unnecessary. Thus, an MWN can provide a small or medium-sized network with low cost and easy maintenance.

Second, an MWN can easily expand the area connected to a backbone network. To enhance the area covered by an existing Internet connection, an Internet service provider (ISP) must increase the base and introduce expensive routers and switches. Management and operation are very costly because the ISP must supply a phone line or an optical fiber to each home. Thus, an MWN offers an attractive alternative for constructing the backbone network. Fig. 1.3 shows an example of an MWN used to expand the backbone network provided by an ISP. An AP connected to the Internet becomes a gateway, and each AP forms an MWN centering on the gateway AP. Furthermore, because an AP on the roof of each home connects with the APs on neighboring houses, the ISP need not lay cable to each home. As

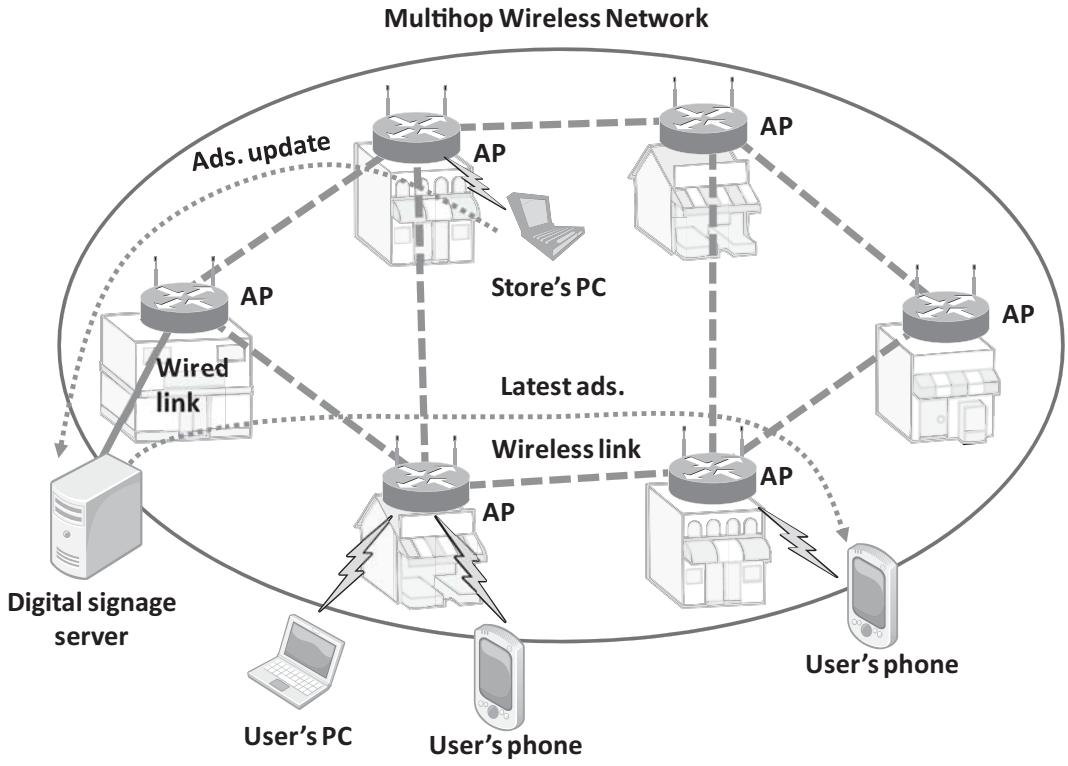


Figure 1.1: Example of MWN in commercial setting

another example, a carrier that provides cellular phone service must typically install much expensive base station to expand its coverage area. In contrast, Fig. 1.4 shows how a carrier can expand the communication area without setting up base stations by connecting a base station with the edge of an MWN.

A hybrid MWN that combines two types of MWN described above has been recently examined.

1.3 Outline of this dissertation

As described above, MWNs offer low cost and flexibility. However, the ease with which an MWN can be expanded significantly affects the network's availability. An environment in which an AP cannot transmit packet, for example, because of damage (electrical outage

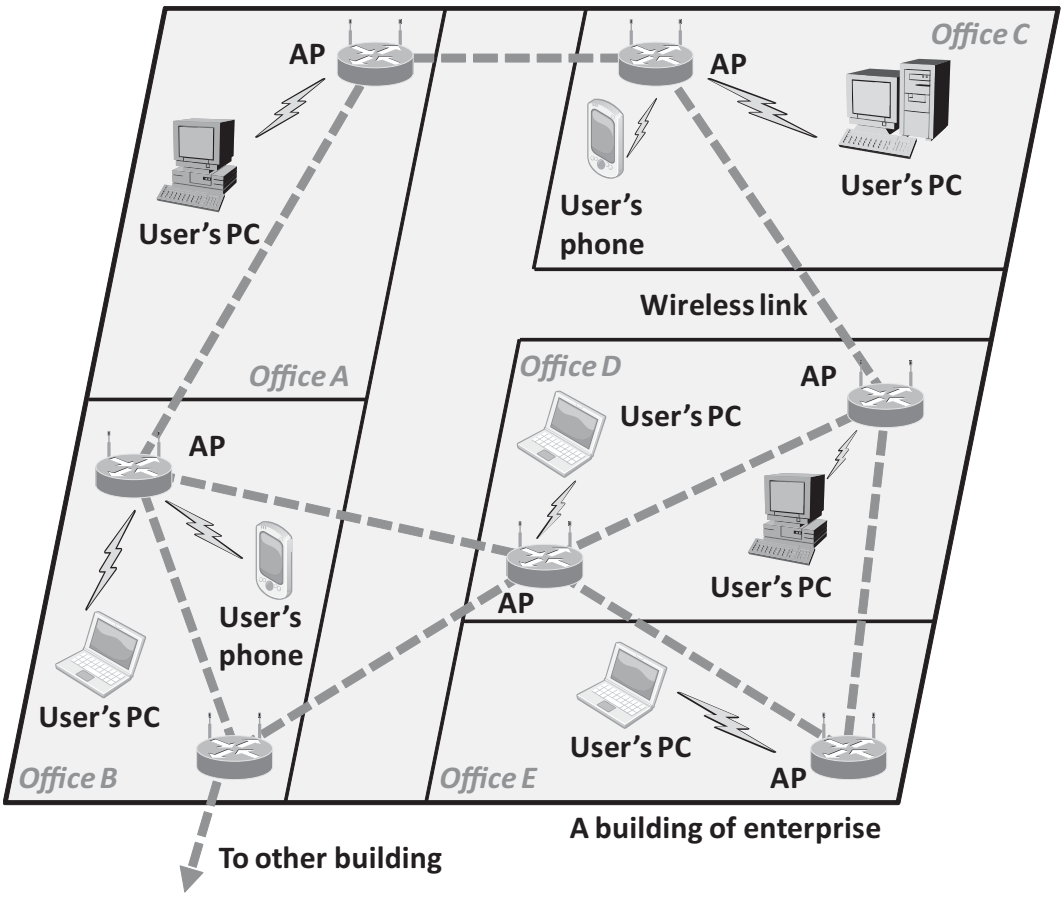


Figure 1.2: Example of MWN in office building

or failure), the behavior of selfish or malicious APs, radio waves in the area, negatively affects the entire network. To maintain network availability, an AP in an MWN must provide reliable operation. Therefore, a mechanism by which each AP autonomously evaluates the reliability of the network and deals appropriately with misbehaving APs is needed. In this dissertation, we focus on achieving a reliable multihop wireless network.

In Chapter 3, we propose a scheme by which APs in an MWN can evaluate neighboring APs by using the packet transfer rate. Existing schemes for detecting misbehavior in a mobile ad hoc network assume an environment with a single interfaces/radio. Thus, each node on these schemes can overhear the behavior of neighboring nodes. However, an MWN,

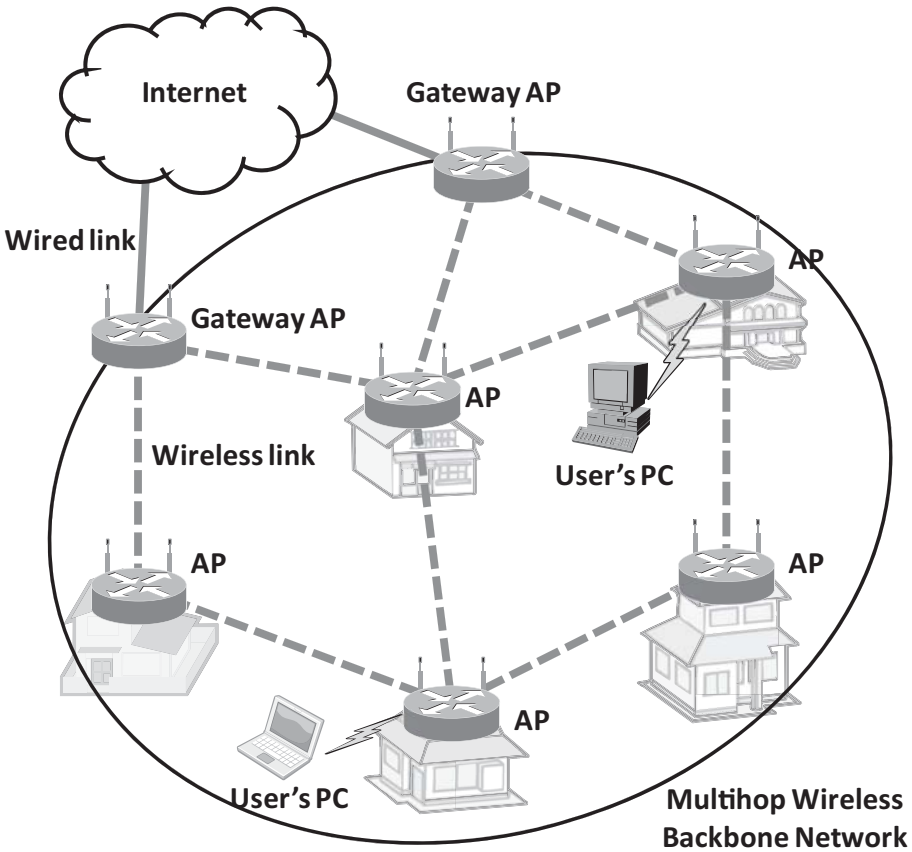


Figure 1.3: Example of MWN used by ISP to expand ts backbone network

such as a wireless mesh network, can use a node with multiple interfaces/radios to enhance communication performance. In this case, it is difficult to use existing schemes of misbehavior detection because nodes cannot overhear the behavior of neighboring nodes. Thus, we propose an evaluation scheme in which a target AP is monitored by peripheral APs. Each AP shares its monitoring results with the other peripheral APs and evaluates the behavior of the target AP. In this context, we verify this scheme using a network simulation, and demonstrate that it can correctly detect misbehaving APs in an MWN.

In Chapter 4, we describe the design and implementation of the scheme proposed in Chapter 3, to verify that it can be used in an actual MWN. APs with multiple interfaces/radios are created using a small personal computer. Because the APs are implemented the proposed

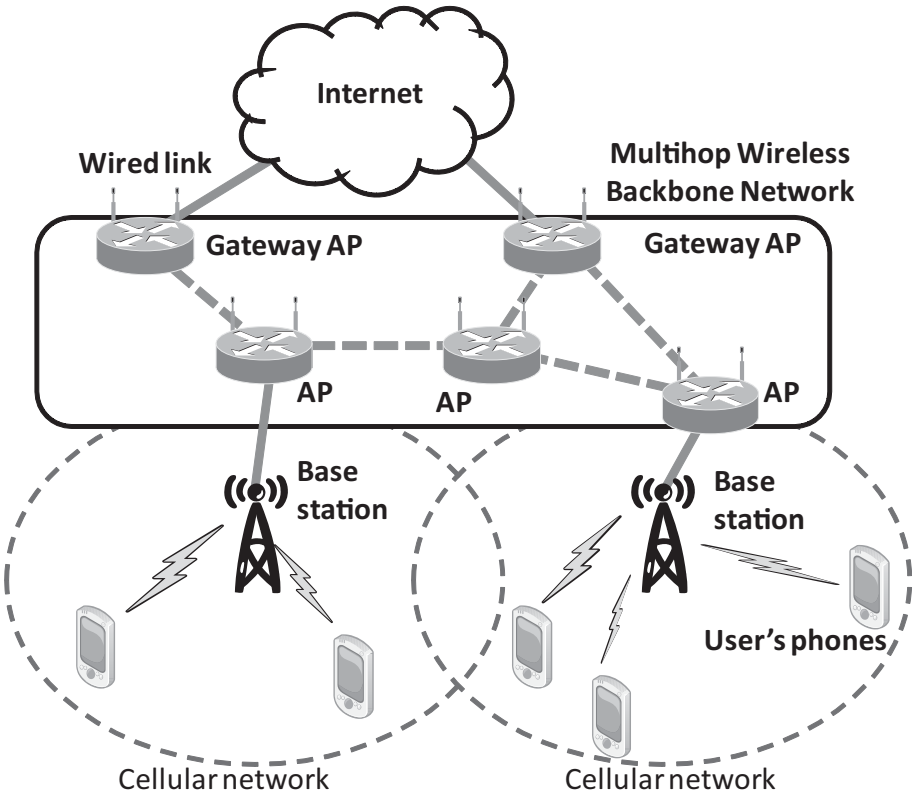


Figure 1.4: Example of MWN used by carrier to expand its network

scheme, we demonstrate that each AP correctly evaluates the misbehavior of other APs by monitoring packet transfer. Furthermore, each AP can autonomously reconstruct a network that eliminates the problematic AP after detecting misbehavior. As a result, we show that our proposed scheme yields a reliable multihop wireless network.

In Chapter 5, we proposed a novel network reconfiguration scheme to maintain the network performance of MWNs. In this scheme, each node reconstructs the network autonomously using the interfaces of neighboring nodes linked to a misbehaving node. The proposed scheme reconfigures a topology with an emphasis on interface reuse, the number of links required to build the network, transmission rates, performance anomaly, and network connectivity. We evaluate the effectiveness of the proposed schemes by a simulation. We show that the simulation results indicate that the proposed scheme can prevent degrada-

tion of the communication performance of the entire MWN.

The result discussed in Chapter 3 are mainly taken from [NNI+09a], Chapter 4 from [NNI+08][NNI+09b], and Chapter 5 from [NSN+10].

Chapter 2

Wireless LAN Technologies and Multihop Wireless Network

In this chapter, we describe a wireless LAN and the applied technology.

A local area network (LAN) is a computer network used on a scale of one organization. Recently, the LAN is used widely at an ordinary home, office of enterprise, laboratory, and factory. Though many methods of LAN exist, intranet that chiefly combines IEEE 802.3 as the Ethernet [IEEb] with TCP/IP that is Internet protocol is general now. These wired LAN appeared in the latter half the 1970's. The LAN has spread rapidly with an office automation (OA) and a factory automation (FA) by high performance and reducing the price of the computer. Moreover, the transmission rate rose to 10 Gb/s by development and the miniaturization of a computer though the rate of LAN was approximately several Mb/s at first. When the terminal is connected with a network, constructing LAN cable in each terminal is necessary. For example, it is necessary to construct LAN cable newly to change the position of the terminal and to introduce the terminal newly. To solve this problem, the wireless LAN that used wireless communication is appeared, and this wireless LAN is very expected as a new communication method.

Characters of the wireless LAN is as follows.

1. The construction of LAN to the existing building is enhanced easily and very freely, because the cable is not constructed.

2. The movement of the terminal can be easy and users access to the network from all

places

2.1 IEEE 802.11 Standard

To increase demand of wireless LAN, the standardization of wireless LAN was rapidly needed. Standardization concerning wireless LAN started formally since 1990 in 802.11 working group (WG) of the IEEE 802 committee that was the standardization of United States LAN organization [IEEa]. This 802.11 WG completed the standard with the transmission rate of the 1 Mb/s and 2 Mb/s in 1997. This original standard uses the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) based on the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) that is distributed control method used by the Ethernet for a technology of the MAC layer. Moreover, we can select a polling method as an option. In polling method, each terminal needs a right to transmit packets from a point coordinator. Three methods of the spread spectrum method by frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) using 2.4 GHz bandwidths and the infrared data communication method were defined in a physical layer. Then, the IEEE 802.11b standard and the IEEE 802.11a standard were settled on in 1999. The IEEE 802.11b standard achieves 11 Mb/s by introducing Complementary Code Keying (CCK), and the IEEE 802.11a standard achieves 54 Mb/s by introducing Orthogonal Frequency Division Multiplexing (OFDM) using 5 GHz bandwidths.

2.2 Network Construction with Wireless LAN

We describe a network construction with wireless LAN in accordance with IEEE 802.11 standard. A network construction with wireless LAN has two types. One is an infrastructure mode; the other is an ad hoc mode.

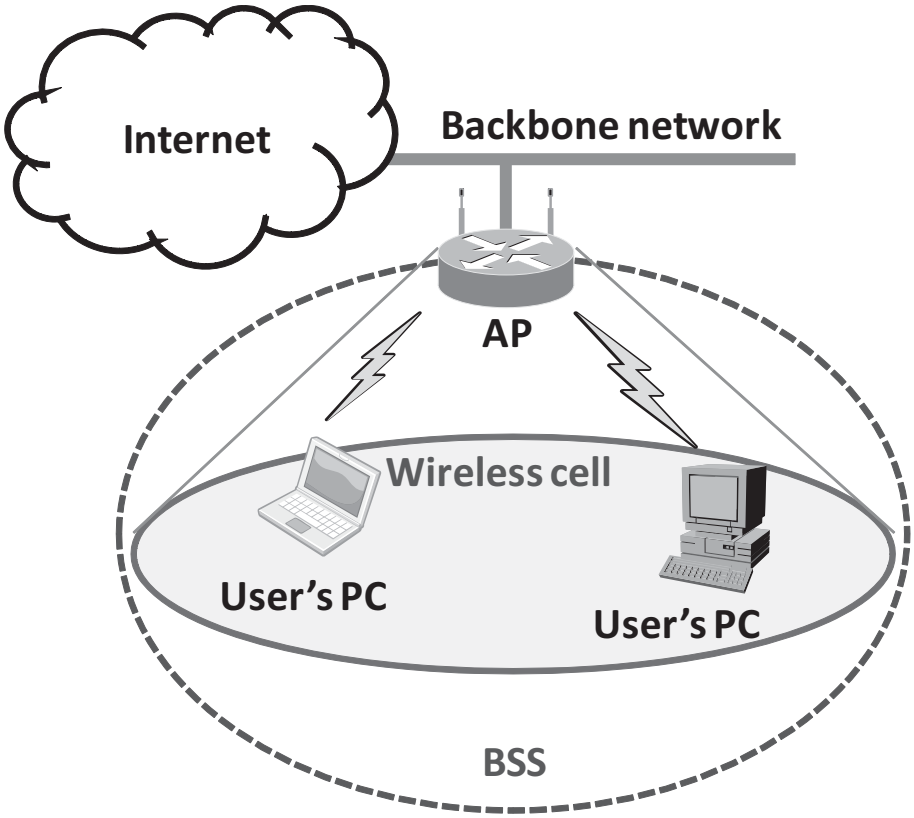


Figure 2.1: Infrastructure mode

2.2.1 Infrastructure Mode

Fig. 2.1 shows an overview of an infrastructure mode. In this mode, a network is composed of a base station called an access point (AP) and station (STA) communicated with the AP. One network composed of an AP and STAs connected with it is called Basic Service Set (BSS). A STA establishes a logical connection (Association) to AP. An AP connects to a backbone network with Ethernet, and AP forwards packets between STAs and a backbone network. Thus, STAs near AP's wireless can always communicate with a backbone network. The general network with wireless LAN such as public hot spot is constructed by an infrastructure mode.

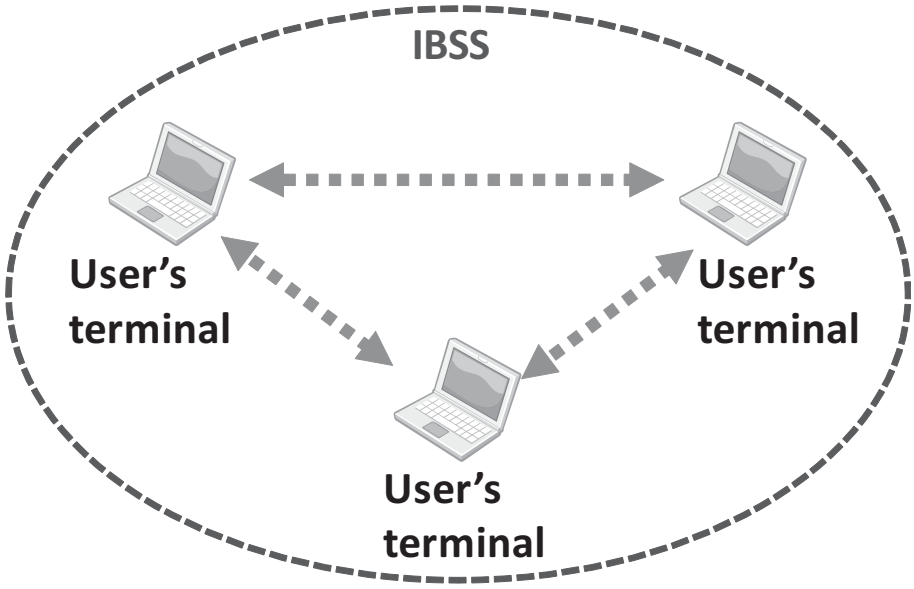


Figure 2.2: Ad hoc Mode

2.2.2 Ad-hoc Mode

Fig. 2.2 shows an overview of ad hoc mode. The ad hoc mode constructs a network using terminals without a AP. The network composed of terminals is called IBSS in order to distinguish the BSS of infrastructure mode. Terminals don't have a function that forwards data packets generally, and each terminal communicates directly to transmit packets. Thus, an ad hoc mode is used to construct a network with terminals that can be composed there mutually. A network using an ad hoc mode is described specifically in section 2.4.1.

2.3 Multihop Wireless Network

We described a wireless network with single hop that STA communicates directly with AP. In this section, we describe a multihop wireless network (MWN) to which each AP communicate mutually by wireless LAN and each AP relays the communication. A multihop wireless network is expected from the lowering the cost of the network construction and the

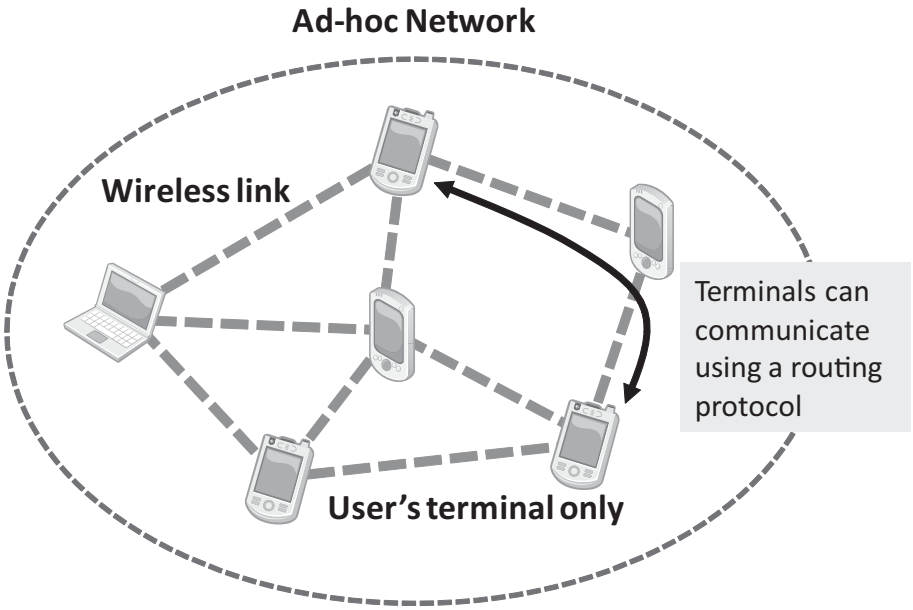


Figure 2.3: Ad hoc Network

easiness of enhancing [OTMI06][AWW05][AW05][SAM06].

We describe two types of multihop wireless networks, such as an ad hoc network and a wireless mesh network.

2.3.1 Ad-hoc Network

An ad hoc network is constructed with two or more terminals that have the ability on wireless communications and the network. The ad hoc network is constructed of the terminal of an ad hoc mode that has the packet forwarding ability. When communicating with other terminals outside the wireless communications range, the packets are forwarded to a destination terminal by forwarding them of each terminal. Fig. 2.3 shows an overview of an ad hoc network.

An ad hoc network has self-organized mechanism and a high adaptive capacity. A shape of the network topology is not constant due to administrator does not exist in the network. Each terminal has mobility, shares information and uses services to detect, and communicate

other terminals.

A terminal that has wireless interfaces exists various types in ad hoc network; for example, a personal digital assistant (PDA), a laptop PC, and cell-phone that can use IP communication, and so on. The specification of these terminals, such as computing power, capacity of storage, and performance of communication is different according to the terminal. Thus, each terminal should not only find the terminal that can be connected but also understands their devise type and attribute. Furthermore, each terminal should always update the route information due to the terminals have mobility. The dissipation power of terminals in an ad hoc network is an important problem because each terminal works by using the battery.

In general, the ad hoc network including the terminal with mobility is called a mobile ad hoc network (MANET).

2.3.2 Wireless Mesh Network

The range of an effective communication of wireless LAN is approximately 50 m, and the range is very small compared with cell-phones and PHSs. Thus, when a service area of wireless LAN is enhanced, it is necessary to set up two or more AP. Because an AP connects to the backbone network with a cable, an administrator should construct the cable to each AP. Because the constructing cable to cost highly to work and resource, this influences flexibility and extendibility to the AP addition and the layout change. These problems can be solved by using wireless communication between each AP. In general, this network is called a wireless mesh network (WMN) from the connection of AP such the reticulation [AWW05][SAM06]. Fig. 2.4 shows an overview of the wireless mesh network. Because the construction of the network with multi hop connection was researched as the ad hoc network than before, this WMN contains a lot of concepts of the ad hoc network. Furthermore, in IEEE 802.11s TG, the standardization of WMN have been advancing as of 2010 [dot].

In the MWN, each AP detects the neighboring node and constructs a network autonomous. Therefore, the range of the wireless to provide service can be enhanced only in the place

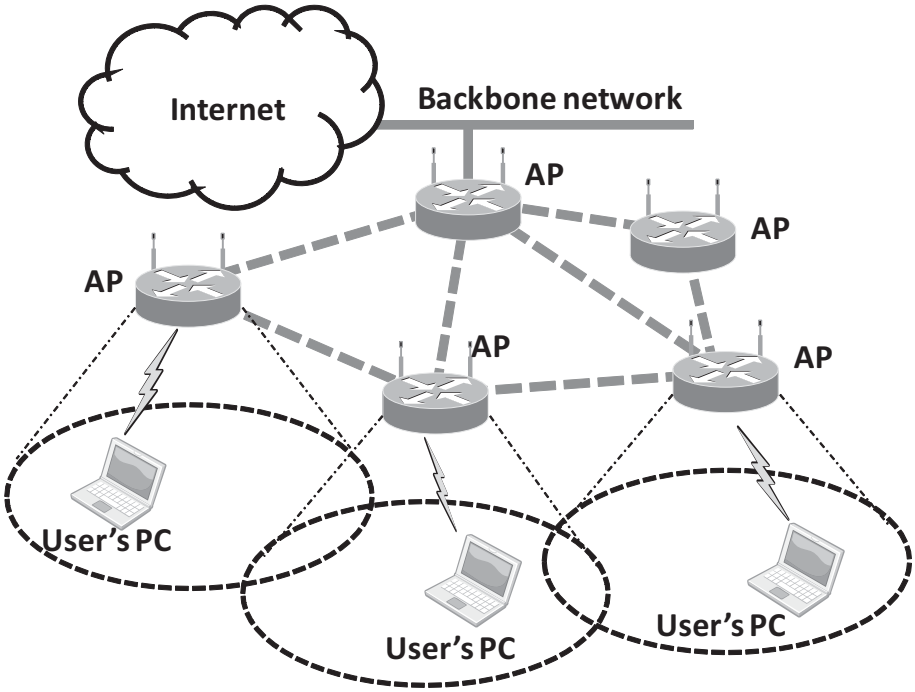


Figure 2.4: Wireless Mesh Network

where AP is set up within the range of the WMN.

2.4 Reliability of Access Point on Multi-hop Wireless Network

A multihop wireless network is expected as a network architecture that supports the social infrastructure in the future. To construct the communication infrastructure that the user can use anytime and anywhere, the construction of the access network that uses wireless communication is indispensable. The access network that has a cheap, flexible topology can be constructed by using multihop wireless network. Furthermore, in the multihop wireless network, many researchers have been advancing the examination of a function such as a composition of a network autonomously and a routing protocol when the state of network

is unstable. However, to construct the multihop wireless network that will becomes a social infrastructure, the technology of ad hoc networks and wireless mesh networks is insufficient, and reliability and availability are required.

Reliability and availability in a multihop wireless network improve because each AP that composes the network forwards packets correctly. Availability in the packet forwarding network shows that the data can be transmitted from a source node to a destination node by the quality more than constancy. Current Internet architectures have an assumption that each entity composing a network operate ideally without troubles and failures. Thus, this network has extremely vulnerability compared with attacks not anticipated and troubles outside assumption.

MWN that composes the whole network of wireless communication can provide a wide service area because many AP construct the network. Thus, each AP should operate normally partially of the network so as not to decrease the availability of the network. Many factors to decrease reliability in a multihop wireless network exist.

The first factor is unexpected accidents of a power outage and a failure of instrument. In case of the state that AP cannot be used due to a power outage and a failure, STA associated the AP cannot transmit data.

Second, a selfish behavior decreases the reliability of AP. To occupy my bandwidth, selfish AP does not forward the traffic from other AP. This selfish AP is not discovered by routing protocols, such as Dynamic Source Routing (DSR) [JHM07], Ad hoc On-Demand Distance Vector Routing (AODV) [PBRD03], Optimized Link State Routing (OLSR) [CJ03], in order to forward the packet necessary for participation on the network. Thus, users cannot receive satisfactory service.

Finally, a malicious node that aims to create network confusion by attacking other nodes affects reliability of the network.. Furthermore, the malicious node has aimed at sniffing/tampering of packet that flows on the network. For example, the denial of service (DoS) attack that the node attacks other nodes using flooding or transmits excess packets for a

Table 2.1: Summery of Misbehaving in Multihop Wireless Network

1. Unexpected nodes
– a power outage
– a failure of instrument
– a degradation of wireless environment
2. Selfish nodes
– a nonparticipation of current route
– not forwarding packet from other nodes
3. Malicious nodes
– a sniffing packets
– a tampering a routing packet
– a DoS attack
– a blackhole attack

specific node, the blackhole attack that the node advertises fiddled routing information to peripheral nodes and suck packets and tampers/drops those packets, and so on [KNKJ07].

Table 2.1 shows the summary of misbehaving in multihop wireless network [KKSW04]. In this study, we mainly focus to the attack “the data packet is not relayed”, including unexpected nodes, selfish nodes, and malicious nodes, through many misbehaving in a wireless network.

From the above-mentioned problems, the construction of MWN with self-organizing, self-reconfiguring, and self-healing functions [NNS+07].

Chapter 3

Access Point Evaluation with Packet Transfer Ratio in Multi-hop Wireless Network

3.1 Introduction

Wireless LAN with IEEE 802.11 standard that is a method to connect user terminals with the Internet access has been widely used in business offices, universities and homes, and so on. In these the wireless LAN, access points (APs) connect an existing backbone network called the “Infrastructure”. Since stations (STAs) can access the Internet to connect to APs using wireless communication, a network with wireless LAN is constructed easily. However, the limit within the effective range of wireless is around 50 meters. Hence, when LAN over the wide range is constructed, many APs to cover the area is necessary. Since the conventional method that uses two or more APs should construct the cable from the infrastructure for all AP, this method increases the cost for the network construction. Moreover, in order to have to construct the cable for new AP, a high construction cost is generated for the network expansion. From such a backbone, a multihop wireless network (MWN) to which each AP communicates mutually by wireless LAN and each AP relay the communication is focused and expected by many researchers as newer backbone network.

Multihop wireless networks (MWNs) are expected to be developed as a newer architec-

ture of infrastructure network access. To improve network availability on MWNs, the network administrator should eliminate each malfunctioning access point (AP) from the MWN. To reduce the total operational cost of an MWN, we have to develop a new AP management scheme that monitors all APs and uses appropriate controls to reconfigure the network topology automatically. To check whether each AP is available, all APs should be monitored. The Simple Network Management Protocol (SNMP) has typically been used for such management. A SNMP agent runs on each AP and sends information about its current status, e.g., the state of each network interface, including packet and byte counters. However, this scheme requires a central management server that collects information from SNMP agents, and if SNMP packets cannot be delivered to the central server or a SNMP agent is unavailable, the network administrator cannot collect enough information. Thus, we want to build an autonomous and distributed management scheme to manage many APs in a MWN.

In this paper, we propose a new mechanism in which each AP evaluates one or more neighboring APs cooperatively in a MWN. Using the proposed scheme, each AP's behavior can be evaluated by neighboring APs; whether the AP behaves can normally be judged based upon the monitoring results. Moreover, we carry out simulations to verify the effectiveness of our proposed scheme for AP anomaly detection in MWNs.

This chapter is organized as follows. Section 3.2 describes the evaluated method of neighboring AP in a mobile ad-hoc network (MANET). Section 3.3 describes our proposed evaluated method of neighboring AP that cooperates 2 hop neighbor APs. Section 3.4 provides simulation models and its results. Finally, we summarize this study in Section 3.5.

3.2 Neighboring Node Monitoring and Evaluation for Wireless Nodes

Nodes that have a negative effect on an MWN are classified as malicious or selfish [SXA08]. These nodes have different characteristics that affect the performance of a network. Mali-

cious nodes attack intentionally to degrade network availability, whereas selfish nodes act greedily to get a communication bandwidth for themselves without cooperating with neighboring nodes. In this study, we focus on selfish nodes.

3.2.1 Collaborative schemes

Selfish nodes discard packets forwarded from external APs and forward only packets that they themselves originate. In mobile ad hoc networks (MANETs), various collaborative schemes for detecting anomalous nodes are proposed. Collaborative schemes can be classified as credit-based, reputation-based, game-theory-based, and so on [SXA08]. Credit-based schemes adapt a currency model to packets, and involve trusting nodes that paid more prices. However, a credit-based scheme has difficulty detecting attacks that send many packets. Game-theory-based schemes can detect selfish nodes based on complex network analysis. However, deploying to an actual network is difficult, since this scheme is unrealistic. In this paper, we focus on reputation-based collaborative schemes.

3.2.2 Reputation-based schemes

In reputation-based schemes, each node monitors a neighboring node and generates the reputation score of the neighboring node based on the monitoring results. Various reputation-based schemes, e.g., CORE [MM02], CONFIDANT [SB02], MobIDS [KKSW04], and others [LDM06], are proposed. The following overview of reputation-based schemes assumes an MWN consisting of nodes that have a single interface and a single radio. We assume that the source node transmits data packets to a neighboring node. The node that receives the packets relays them to the next neighboring node based on a routing table. Fig. 3.1 illustrates the overhearing of neighboring nodes in MANETs. The source node can overhear the data that its neighbor transmits to the next neighboring node, since the source node uses the same wireless channel as the neighbor. Hence, the source node monitors the behavior of its neighbor. Next, the source node generates a reputation score based on the monitoring results.

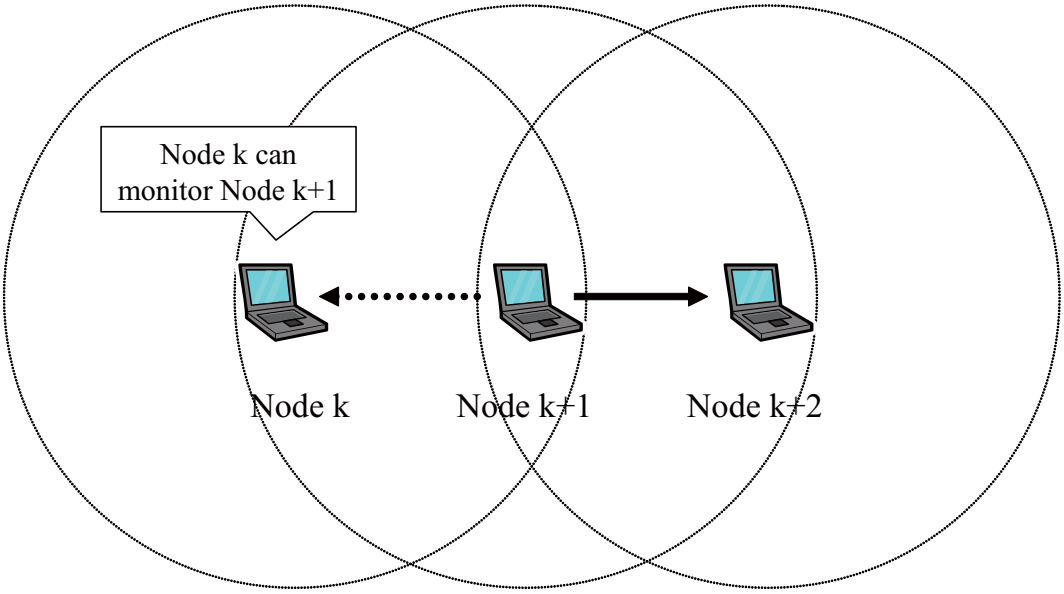


Figure 3.1: Overhearing of Neighboring Nodes in MANETs

To run the reputation-based mechanism on each node, all nodes should be able to monitor neighboring nodes and estimate their reputations autonomously.

In the following subsection, we provide two typicall reputation-based scheme in a MANET.

3.2.3 CORE

Petro Michiardi, et al. proposed “CORE” [MM02] which is a solution based on evaluating the behavior of neighbor nodes. In the CORE, each node creates other nodes’ score by reputation mechanism. This reputation score is created for network functions of the node’s behavior such as data packet transfer, sending routing information and so on. The following reputation scores are generated.

- Subjective Reputation
- Indirect Reputation

Subjective Reputation is generated directly based on the result of overhearing what a neighbor node transmits. The node preserves the overhearing result obtained when a neigh-

bor node is in a correct state as an expected value, and compares an actual overhearing result with the expected value. If the actual value equals the expected value, an evaluated value is positive. On the other hand, if the actual value is lower than the expected value, the function deduces that the node is not performed correctly and the reputation score is negative. A subjective reputation score is computed directly by using of monitoring results and past reputation scores.

A subjective reputation score which each node computed is advertised to all of the nodes in a network. To prevent transmitting negative evaluation results intentionally by selfish nodes, each node advertises only evaluation value is positive. A node uses the reputation notified from other nodes as an indirect reputation.

The reputation for every function is calculated using the subjective reputation and the indirect reputation. And final reputation is calculated to weight for every function. The node that reputation score is negative is excepted from a network. In the CORE, examples using functions to calculate a reputation, such as state of packet transmission, and behavior of DSR, are shown.

3.2.4 CONFIDANT

The CONFIDANT [SB02] is proposed as the method of evaluating neighbor nodes from the monitoring result of neighbor nodes. At monitoring method of CONFIDANT, a transmission of the data packet in neighbor nodes and a behavior of routing protocol is monitored, and a direct reputation is created. When a node detects that the neighbor node carried out malicious behavior, the node has a function which transmits an alarm to nodes other than the anomaly node. It is the major difference between CORE and CONFIDANT to notify a minus estimating to circumscription. Each node calculates a final reputation from a direct reputation and the reputation notified from the neighborhood node. In CONFIDANT, the path containing the node judged not to be normal by the final reputation is excepted.

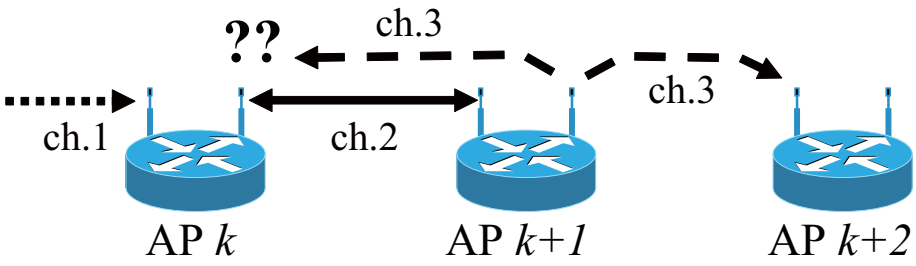


Figure 3.2: Difficulties with node monitoring in a multi-interface MWN

3.2.5 Problems with monitoring of neighboring APs

Nodes in a MANET using the neighboring nodes monitoring method must be able to overhear the behavior of a neighboring node. In an MWN, in order to prevent deterioration of communication quality by interference on the same radio channel, research has progressed to allow each node to have two or more interfaces. When an AP has two or more wireless interfaces, it is difficult to monitor the behavior of all neighboring APs.

The difficulties of AP monitoring in a MWN are shown in Fig. 3.2. The case where AP_k transmits data to AP_{k+2} via AP_{k+1} is discussed. Each AP holds two interfaces, and it is assumed that the AP uses different channels for receiving and transmitting. As shown in Fig. 3.2, the receiving interfaces of AP_k, AP_{k+1}, and AP_{k+2} are set to channels 1, 2, and 3, respectively. AP_k transmits data to AP_{k+1} via channel 2, and AP_{k+1} transmits data to AP_{k+2} via channel 3. Since the receiving interface of AP_k is set to the channel 1, AP_k cannot overhear the information that AP_{k+1} transmits via channel 3. Although AP_{k+1} reports to AP_k that it has transmitted the packet to AP_{k+2}, information in the report is not reliable because it may have been prone. Thus, when each AP has two or more interfaces and uses two or more radio channels, it is difficult for an AP to monitor the data transfer of a neighbor.

3.3 Proposed Mechanism

In this paper, we propose a cooperative mechanism for monitoring and evaluating neighboring APs in MWNs in which each AP has multiple interfaces. In this proposal, we select the

packet transfer rate from various metrics for evaluating the behavior of a neighboring AP, because the packet transfer rate is the simplest metric that reflects network availability.

3.3.1 Method of monitoring neighboring AP behavior

Each AP (AP_s) evaluates its neighbor in cooperation with another AP (2HN-AP, 2 Hop Neighboring AP) that also neighbors the target AP (AP_t). This solves the multi-interface and multi-channel monitoring problems. Furthermore, since each AP uses information not from the directly neighboring AP but from two or more 2HN-APs, this technique can prevent an attack such as a false report, solving a problem in existing schemes.

In our proposal, the evaluation value of each AP is calculated from the transfer rate for packets that traveled from AP_s to each 2HN-AP through AP_t, which is the target for evaluation. The packet transfer rate is calculated using the following two kinds of packets:

- Data packets that flow into a route (packets for routing protocols are also included),
- Probe packets, which are transmitted in order to measure the transmission rate.

AP_s measures the number of packets transmitted to each 2HN-AP via AP_t. Next, each 2HN-AP measures the number of packets transmitted from AP_s. If timely data is not flowing between 2HN-AP and AP_s, AP_s will generate a probe packet and transmit to the 2HN-AP. Each 2HN-AP periodically sends AP_s a report packet containing the number of received packets, which is the measurement result. AP_s calculates a packet transfer rate based on the number of received packets reported from each 2HN-AP and the number of packets that it transmitted itself.

3.3.2 Calculating the evaluated value

AP_s calculates the evaluation value (global value, GV) of a neighboring AP from the following two values.

- Direct Value (DV): The evaluation value of AP_t that AP_s calculates from a packet transfer rate.
- Indirect Value (IV): The evaluation value of AP_t that AP_s receives from each 2HN-AP.

Direct Value

AP_s creates a DV based on the direct ratio (DR) that calculated from the number of packet transmissions of AP_t collected from each 2HN-AP. AP_s calculates a packet transfer rate per 2HN-AP using the number of packet transmissions of AP_t reported by each 2HN-AP, and the number of packet transmissions it performed itself. DR is calculated from the packet transfer rate calculated for each 2HN-AP by the weighted moving average using the packet transfer rate for the most recent transmission [equation (3.1)]. Hereafter, 2HN-APs for AP_t of AP_s are denoted by APc, APd, ..., APn.

$$DRa_{b-c}(t) = \frac{1}{\alpha} DRa_{b-c}(t-1) + (1 - \frac{1}{\alpha}) R(t) \tag{3.1}$$

$DRa_{b-c}(t)$ is the DR that APa calculated from APc to APb in time t, $R(t)$ is the packet transfer rate in time t, and α is the weight of a weighted average. Finally, after AP_s calculates the DR for each 2HN-AP, AP_s sets these minimum values to the DV [equation (3.2)].

$$DVa_b(t) = min(DRa_{b-c}(t), ..., DRa_{b-n}(t)) \tag{3.2}$$

$DVa_b(t)$ is the DV for APb that APa calculated in time t.

IndirectValue

IV represents the evaluation value of AP_t by the neighboring AP rather than the value calculated by APs itself. All the APs create a DV for each neighboring AP. Each AP sends DV of

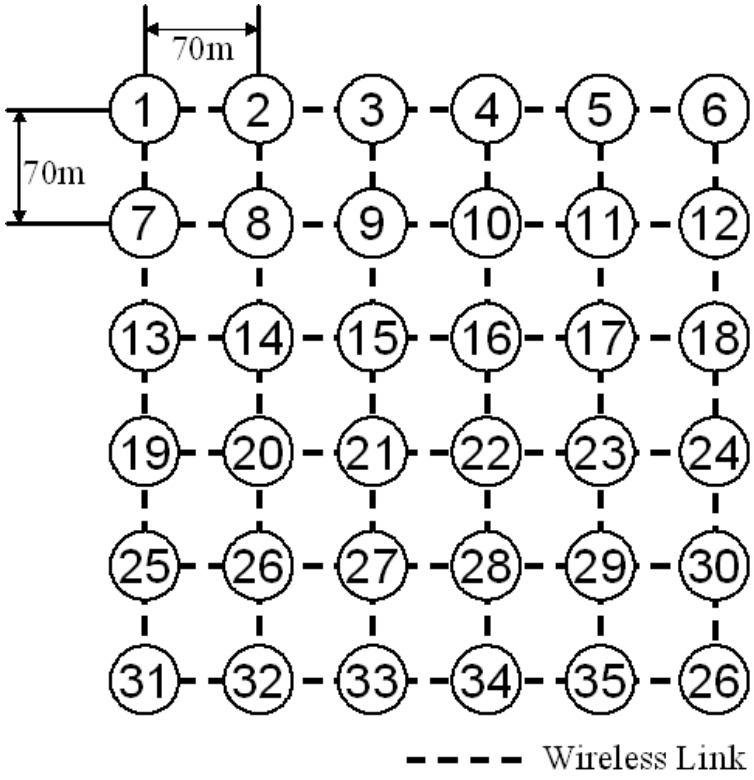


Figure 3.3: Topology for the simulation

its neighbors to the 2HN-APs. The reception side is used for the evaluation of AP_t by setting the IV from the information about AP_t sent from two or more APs.

Global Value

Each AP maintains DVs for every neighboring AP and IVs from 2HN-AP for AP_t. Each AP calculate the GV of the neighboring AP from the minimum of the DVs and IVs [equation (3.3)].

$$GVa_b(t) = min(DVa_b(t), IVa_{b-c}(t), ..., IVa_{b-n}) \tag{3.3}$$

$GVa_b(t)$ is the GV for APb that APa calculates in time t, and $IVa_{b-c}(t)$ is the IV for APb that APa received from APc in time t. Furthermore, each AP uses the GV for AP_t obtained from the packet transfer rate as an indicator of AP_t's reliability. For example, the GV will be used as a metric that removes an AP that does not behave normally from the network in

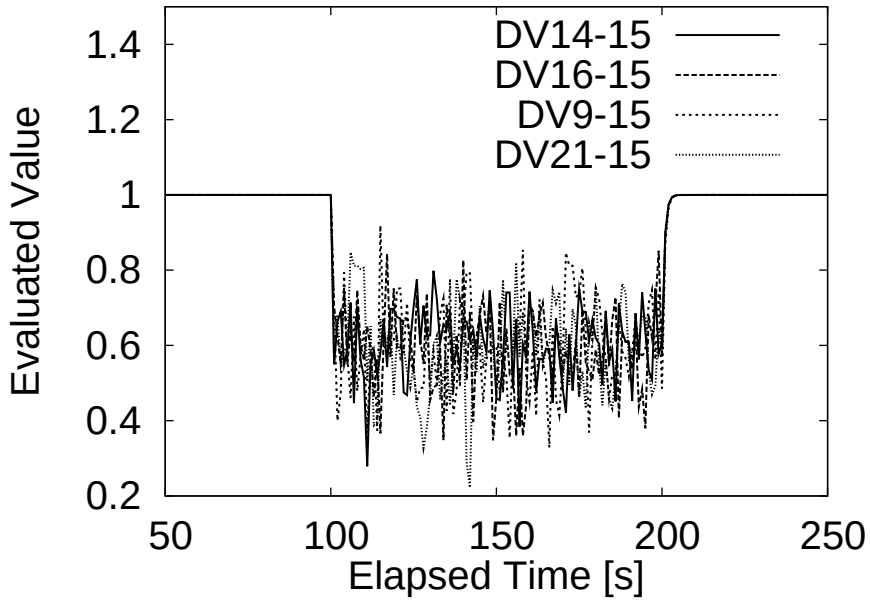


Figure 3.4: DVs of AP15

cooperationg with routing protocols.

3.4 Simulation and Result

In this study, we verify cooperative evaluation of the neighboring APs in a MWN. To show clearly that each AP can detect an anomalous AP autonomously using our proposed method, We use the network simulator Qualnet 4.0.1. For each AP to cooperate with 2HN-APs and calculate a packet transfer rate, APs are in the shape of a 6x6 grid, and the distance between APs is 70 m (Fig. 3.3). In Fig. 3.3, the short dashed line that connects pairs of APs indicates a radio link, each AP has a wireless interface for every neighboring AP, and different channels are set up to avoid radio frequency interference with other APs' interfaces. If an AP does not receive data for 0.1s or more, it transmits a probe packet to 2HN-AP every 0.1 s. When data is flowing, each AP counts the number of data packets for every 2HN-AP. Every 1.0 s, each AP sends a report packet to every 2HN-AP the number of packets transmitted. The values

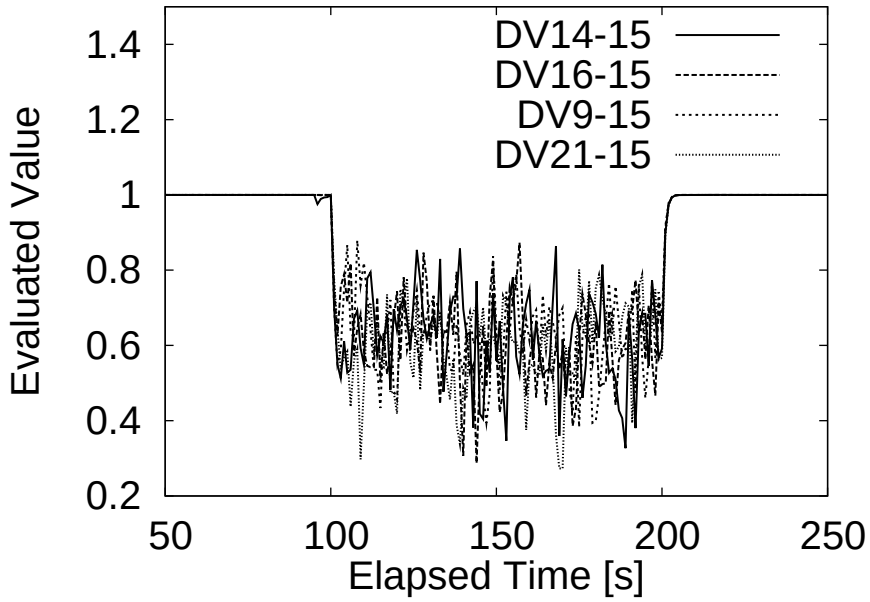


Figure 3.5: DVs (FTP) of AP15

for the transmission intervals of probes and reports are based on the result of earlier research using a simulation. Moreover, the share interval of GV is 1.0 s. The simulation time is 300 s. In this simulation, α of a moving weighted average is 4 to focus on the present state.

3.4.1 DirectValue and GlobalValue

Packet loss occurs on AP15, and there is always has a 30% probability of loss occurring on AP15 from 100 to 200 s AP15's neighbors are 9, 14, 16, and 21. DV*x*-*y* (indicated in the legends of Figs. 3.4-3.6) is the DV of AP*y* that AP*x* has, and GV*x*-*y* is the GV of AP*y* that AP*x* has. Fig. 3.4 shows DVs using only a probe packet to AP15. Figs. 3.5 and 3.6 show DVs and GVs to AP15, respectively. In Figs. 3.5-3.6, instead of the probe packet, FTP is used as real data traffic; it flows beginning at 95 s and ending 205 s from AP14 to AP16. Moreover, a probe packet is used along the path for which FTP is not used. The DVs in Fig. 3.4 are almost the same as those in Fig. 3.5. The result shows that generation of the evaluation value

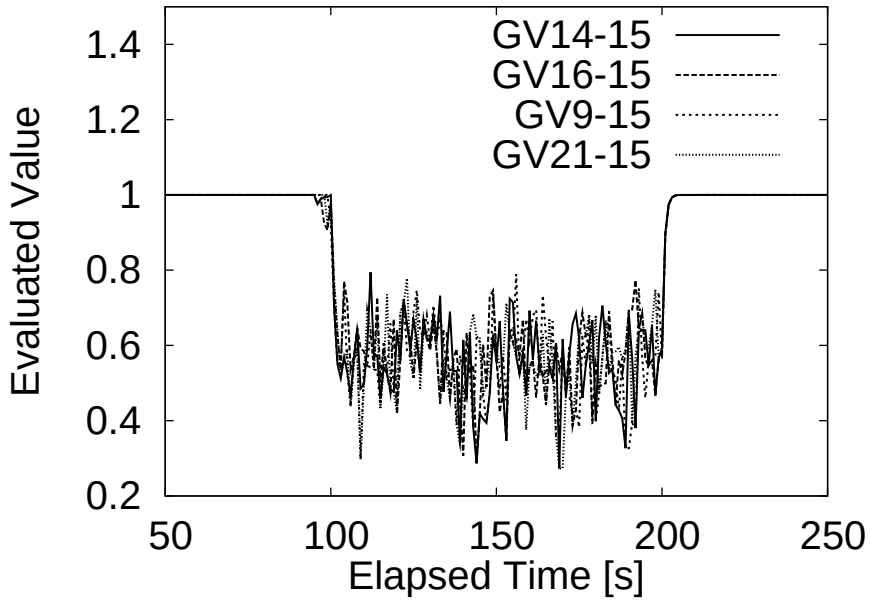


Figure 3.6: GVs (FTP) of AP15

using real traffic, such as FTP, instead of a probe packet is effective. From Fig. 3.5 and 3.6, the fluctuation in GV is smaller than that in DV. Thus, GV can offer a more stable estimation than DV. Furthermore, Figs. 3.4-3.6 show that all the evaluation values of a neighboring AP exhibit the same characteristics.

3.4.2 Compare of anomaly detection

Fig. 3.7 shows a GV held by AP14, when parameter α of EWMA is set $\frac{4}{3}$ and Packet loss occurs on AP15, which is always has a 30% probability of loss occurring on AP15 from 100 to 200 s. FTP traffic is also used for this value generation. From comparing Fig. 3.6 and Fig. 3.7, Fig. 3.7 shows loose variation of GV by emphasizing past state, and variation width of GV is smaller than Fig. 3.6.

Fig. 3.8 and Fig. 3.9 show GV at the time when packet loss to AP15 occurring every 10 s was switched off. GV*x*-*y* (indicated in the legend for the graph) represents the GV of AP*y*

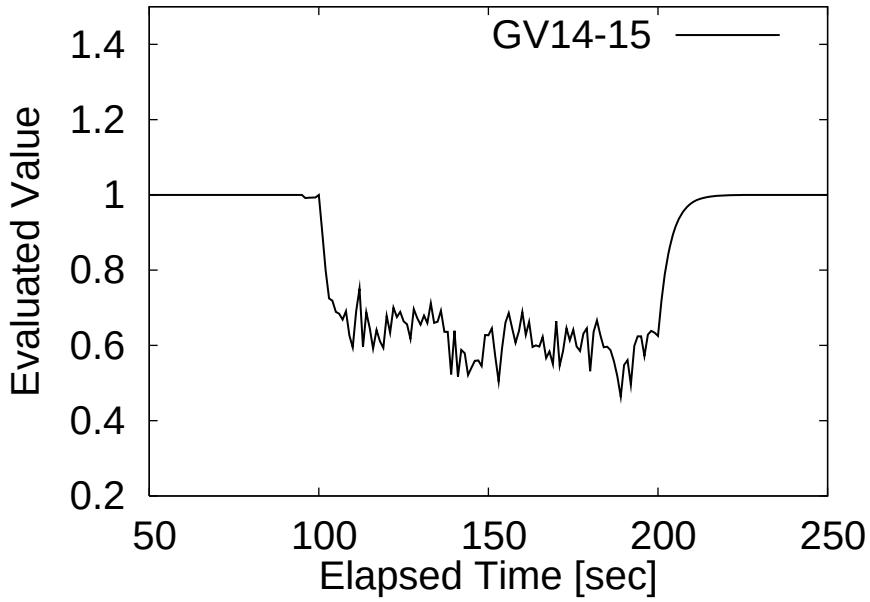


Figure 3.7: $\alpha = \frac{4}{3}$: GVs (FTP) of AP15 held by AP14

that APx has. From comparing Fig. 3.8 and Fig. 3.9, Fig. 3.8 shows that our scheme can react sharply to intermittent packet loss. Since fluctuation of the estimation value of AP becomes large, frequent packet loss makes network activity unstable. Fig 3.9 shows loose variation of GV than Fig 3.8. However, case of emphasizing past state cannot sensitively correspond to anomaly APs.

Therefore, in the future, we need to discuss a calculation method that quickly detects a decline in the evaluation value based on the packet transfer rate and prevents instability. In order to make use of these evaluation value for a network reconstructing of MWN, it is necessary to detect trouble before the data is sent to routing protocols such as OLSR. Cooperation between these routing protocols and our proposed mechanism is also a subject of future works.

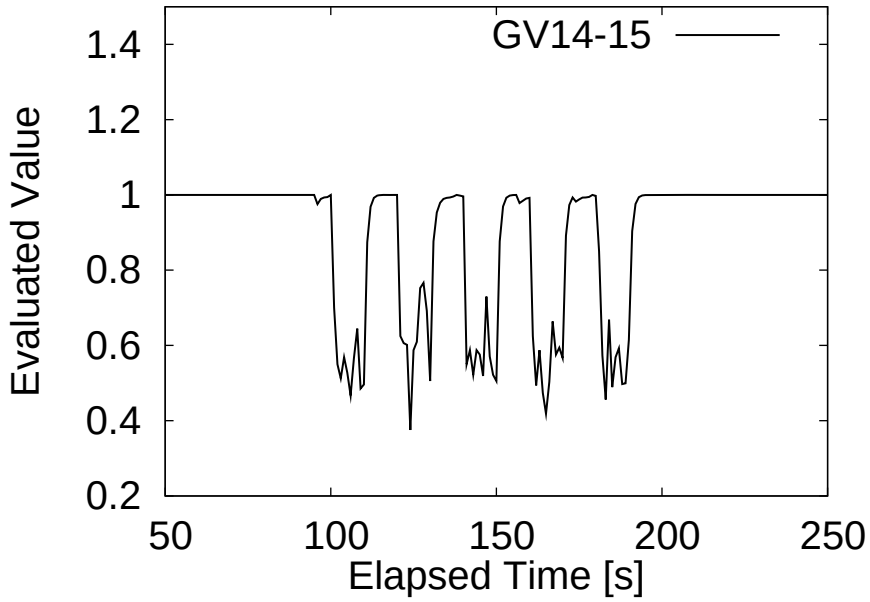


Figure 3.8: α = 4: GVs (FTP) of AP15 held by AP14 (variable packet loss)

3.5 Judgement of Misbehaving APs

We can calculate the evaluation value using a packet transfer rate. Each AP in MWNs must eliminate anomaly APs using this evaluation value. However, a definition of misbehaving APs varies by a network size and policies of a network administrator. If the administrator uses an evaluation value using a packet transfer rate, he or she should consider two situation as follows.

- The administrator cannot accord small packet loss, when a MWN is used for TCP protocol, such as FTP.
- The administrator can accept small packet loss, when a MWN is used for UDP protocol, such as video streaming.

Furthermore, the administrator must consider dealing with instantaneous packet loss of APs. APs loss packets for a quick moment, such as variant of wireless environment, and

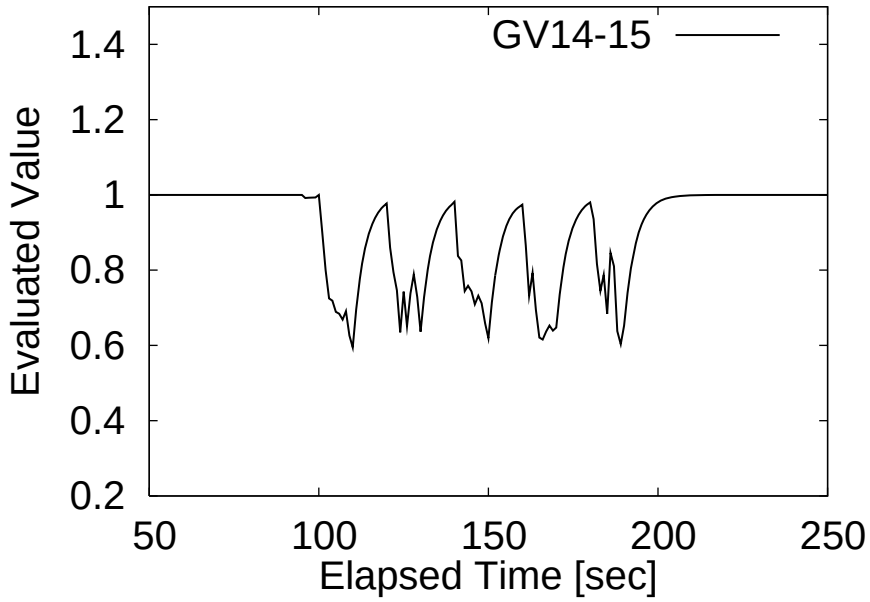


Figure 3.9: $\alpha = \frac{4}{3}$: GVs (FTP) of AP15 held by AP14 (variable packet loss)

temporal decreasing of electric power supply. Those APs has the possibility of returning normally at once. The administrator must not judge those APs as misbehaving APs.

The administrator needs to consider an objective of a MWN, and should design a network policy, In this section, we discuss judgement and dealing with misbehaving APs.

3.5.1 Dealing with Misbehaving APs

If each AP that consists a MWN detects misbehaving APs, they eliminate misbehaving APs from the network or avoid the APs from a route of a network. As a result, the administrator can keep a stability of a whole network. However, each AP cannot stop a monitoring for the misbehaving AP after eliminating or avoiding it from the network. Because each AP should put in the AP that recovers normally. Thus, after detecting of misbehaving AP, each AP has monitored a movement carefully of APs.

An administrator of a MWN should deal with misbehaving APs as follows.

- Decreasing GV from a normal state to an anomaly state: each AP judge the AP decreasing GV as misbehavior, since a misbehaving AP should be detected immediately.
- Increasing GV from an anomaly state to an normal state: each AP judge the recovering AP carefully; however, temporal packet loss must be considered.

3.5.2 Algorithm for Judgement of Misbehaving AP

In this section, we propose an algorithm for judgement of misbehaving APs. This algorithm aims that each node can detect the misbehaving AP correctly and carefully.

First, we define a variant J for judgement of misbehavior. If J is lower than arbitrary threshold th, the AP is judged to be a misbehavior by this algorithm. J changes basically by GV. Thus, when GV is updated, J is updated at same time. To judge the misbehaving AP carefully and correctly, we introduce three phases for monitoring target AP.

- Normal phase
- Alert phase
- Anomaly phase

The normal phase shows that target AP has no anomaly. In this phase, the value of J is equal to GV. If J of target AP is lower than th, an AP changes the target to the alert phase.

When the target AP becomes the alert phase, each AP bewares the AP to judge be anomaly. In this phase, the value of J is also equal to GV. If J of target AP is higher than th, an AP changes the target to the normal phase. While, if J is lower than th γ times in a row, an AP changes the target to the anomaly phase. From this scheme, a misbehaving AP is not occurring by temporal packet loss.

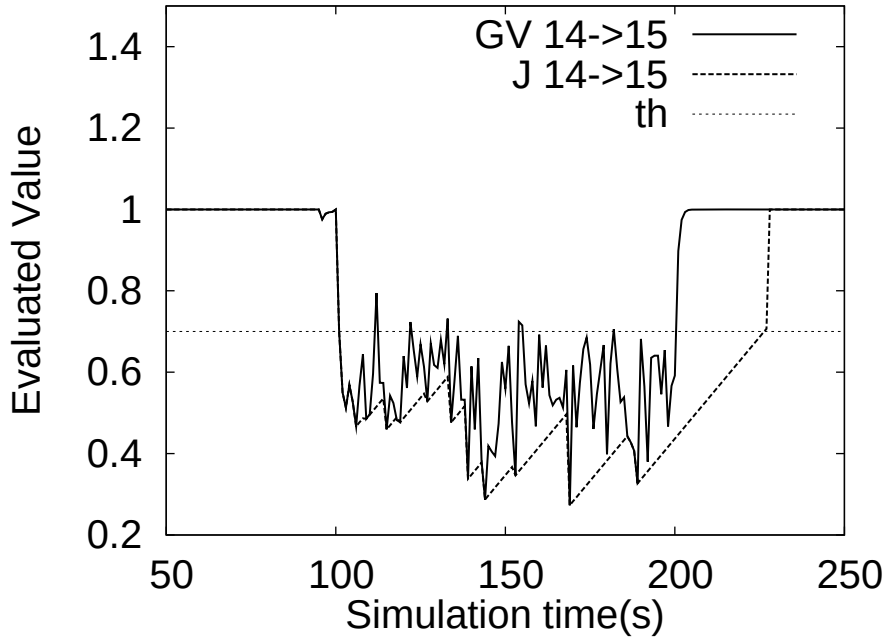


Figure 3.10: Example of the Judgement Algorithm

The anomaly phase shows that target AP has any anomaly. In this phase, J is set from the following formula.

$$\begin{cases} J(t) := GV(t) & (J(t) \geq GV(t)) \\ J(t) := J(t-1) + \beta & (J(t) \leq GV(t)) \end{cases} \tag{3.4}$$

If J is higher than GV, the value of J is equal to GV. This is because of immediately corresponding to the decrease of GV due to the deterioration of a misbehaving AP. While, if J is lower than GV, an arbitrary β is added to J. This is because a misbehaving AP is carefully recovered when the evaluation to the AP rises. Then, if J is higher than th, an AP changes the target to the normal phase.

By this algorithm, each AP can judge a misbehaving AP accurately and carefully.

3.5.3 Example of the Judgement Algorithm

Fig. 3.10 show an example of the judgement Algorithm. We set that th is 0.7 in this example, because packet loss rates is set 0.3 in this simulation. Furthermore, β is set 0.01 and γ is set 5. This graph show a GV of AP15 that AP14 has in Fig. 3.5 and J. First, the J varies according to GV. After J is lower than th, this AP change the anomaly phase via the alert phase. In the anomaly phase, J rises gradually though increases GV. As a result, AP14 can detect the misbehaving AP immediately, and recover carefully.

From this result, each node can appropriately detect a misbehaving AP by using this algorithm according to the policy of the network.

3.6 Conclusion

In this paper, we proposed a neighboring AP evaluation mechanism using the packet transfer rate for detecting APs that do not behave normally. The operation of the proposed mechanism and the evaluation values generated for an AP that cannot transmit packet normally were examined by simulation. As a result, we showed clearly that APs can detect when a neighboring AP is not behaving normally by sharing the evaluation value that each AP calculates using the data packet transfer rate with other neighborhood APs.

Chapter 4

Design and Implementation of Reputation Mechanism for Multihop Wireless Network

4.1 Introduction

A multihop wireless network (MWN) provides a flexible network architecture that supports the addition of one or more access points (APs) to expand the service area. Because an MWN is easy to construct and has low management costs, the use of MWNs is expected to grow in next-generation network systems. In such networks, the reliability of each AP affects the reliability of an MWN backbone, because a backbone network covers a wide area that consists of many APs. For example, when an AP malfunctions because of a power outage or a malicious attack, it cannot forward packets correctly. Therefore, to ensure reliability of MWNs, each AP must detect any malfunctioning or compromised AP in the network and resolve such problems appropriately.

Current research related to mobile ad hoc networks (MANETs) includes cooperative monitoring schemes, such as credit-based, reputation-based, and game-theory-based approaches [SXA08]. In these schemes, each node calculates an evaluation score of a target node (a neighboring node) in a self-organized manner on the basis of direct behavior monitoring or behavior reports sent by the target node; however, in an actual MWN, it is difficult

to monitor all traffic of a neighboring node because the target node may use two or more different channels for achieving a high throughput. Furthermore, although availability of these schemes has been estimated by network simulation, most have not been implemented and evaluated in detail. Therefore, their effectiveness in actual networks has not been verified.

As detailed in Section 3, we proposed a reputation-based evaluation method for neighboring APs in which each AP cooperates with peripheral APs [NNI+09a]. Specifically, each AP monitors a neighboring AP using 2 hop neighbor APs, and shares the monitoring results with them. As a result, the proposed method establishes "reputations" for each neighboring AP and detects malfunctioning or compromised APs using such reputations. We evaluated my proposed method using the QualNet as a network simulator, which showed that each AP correctly detects misbehaving nodes.

In this chapter, we describe the design and implementation of my proposed reputation mechanism. We constructed an MWN by creating APs using a personal computer; we verified that these APs can autonomously detect misbehaving nodes in a wireless environment using 2 hop neighbor APs. Furthermore, this implementation revealed that each AP can autonomously reconstruct the network omitting all misbehaving APs. This implementation provides a highly reliable MWN that will considerably decrease management costs.

In addition to this introductory section, this chapter is organized as follows: Section 4.2 defines misbehaving APs and solutions to such problems; Section 4.3 provides details of design and implementation; Section 4.4 provides results of my proposed solution using actual terminals; and finally, Section 4.5 summarizes this study.

4.2 Influence of a Misbehaving AP in a MWN

In this section, we describe the behavior of APs that cause degradation in communication performance of an MWN. Furthermore, we provide methods for detecting misbehaving APs and how APs cooperate to overcome these potential performance pitfalls.

4.2.1 Misbehaving AP: a malicious and a selfish node

APs that negatively influence MWNs can be classified into two types: malicious APs that attack peripheral APs and selfish APs that are uncooperative members of the network. Malicious APs intentionally disrupt other APs within the network, by attacks such packet sniffing and falsification of packets. For example, denial of service (DoS) attacks occur when an AP attacks other APs by packet flooding or excess packet transmission; similarly, black-hole attacks occur when a AP advertises incorrect routing information to peripheral APs to attract more incoming packets. The AP then tempers with the packets or drops them altogether [KNKJ07]. Current solutions against these types of attacks include preparing blacklists to fight DoS attacks and verifying the legitimacy of routed messages to combat black-hole attacks [KNKJ07].

Selfish APs, the second type of negative influence on MWNs, are greedy APs that are uncooperative members of a network, aiming to maximize their throughput of sent data. For example, selfish APs may transmit packets it creates correctly; however, the AP fails to forward packets from other APs. Furthermore, by exploiting weakness in the MAC layer protocols, the AP may send its own information, although it presents an attitude of participation in the surrounding network [SXA08]. Countermeasures against such selfish APs are studied in the field of mobile ad-hoc networks (MANETs).

Many researchers are studying malicious nodes that occur in MANETs in which mobile nodes dynamically compose a network. APs exist via a network administrator in MWNs. Therefore the probability that malicious or selfish APs exist is low. As a result, researchers have considered such occurrences as accidental or failures in MWNs; however, MWN of the half management which composes user's original wireless backbone at the edge of the managed MWN is reported. Thus, the fore-mentioned malicious and selfish APs cannot be disregarded.

4.2.2 Existing schemes for detecting misbehaving APs

For MANETs, many researchers have proposed methods in which individual nodes autonomously detect misbehaving nodes [SXA08]. Such methods are classified into credit-based schemes, game-theory-based schemes, and reputation-based schemes.

To measure the currency of packets flowing to each node qualitatively, credit-based schemes establish evaluated values for each node by identifying a money supply of each node. A typical credit-based scheme is the Nuglets scheme [BH01]. The characteristics of MANETs are node mobility and uniform flow of data packets to all nodes. Hence, there is little bias regarding the number of packets flowing to a node. Thus, MANETs can use credit-based scheme such as the Nuglets: however, APs used to construct a MWN have no mobility. It is therefore difficult to use a credit-based scheme in an MWN, because the number of data packets flowing to the nodes may not be uniform.

Game-theory-based schemes, such as generous tit-for-tat [PSN+03], detect selfish nodes by analyzing the behavior of each node using game-theory, such as Nash Equilibrium. It is difficult to implement this scheme because assumptions and implementation of a network model for verifying effectiveness are unrealistic, although this scheme can analyze complex behavior of nodes.

In reputation-based schemes, each node monitors neighboring nodes and creates a "reputation" measure of neighboring nodes. Such reputation-based schemes identify a misbehaving node using these reputation measures, and therefore, detect misbehaving nodes without the need for centralized management. Typical reputation-based schemes include Watchdoc [MGLB00], CORE [MM02] and CONFIDANT [SB02]. The proposed evaluating scheme of neighboring nodes in chapter 3 is classified into the reputation-based scheme.

A detail and some problems of the reputation-based scheme were described in Section 3.2. Thus, they are omitted in this chapter, and we describe an outline of a design and an implementation the proposed scheme at the following.

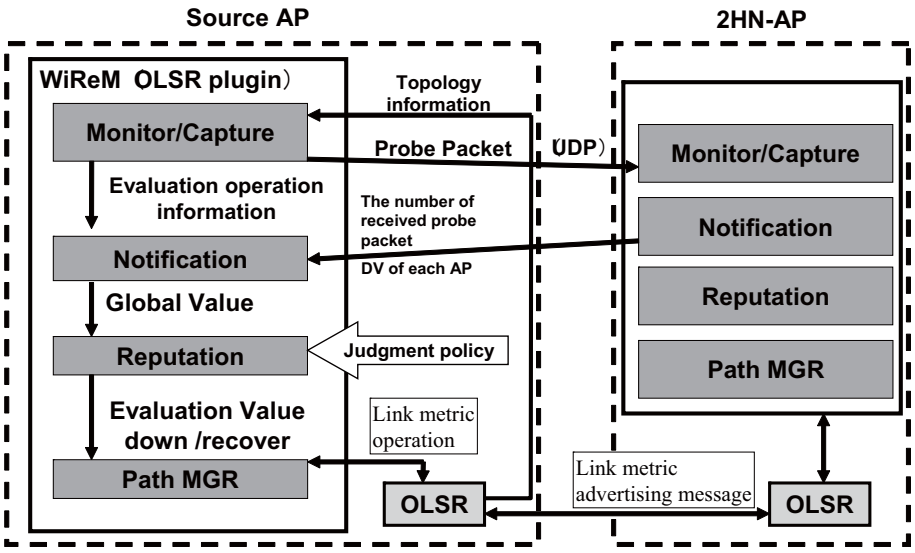


Figure 4.1: Design Overview

4.3 Design and Implementation

The operation of my proposed scheme in chapter 3 verified the effectiveness by a simulation. To verify that the proposed scheme operates effectively in an actual MWN, we designed and implemented the scheme as described in the following subsections.

4.3.1 Design overview

Fig. 4.1 shows an overview of the design. For implementation the proposed scheme is built into an OLSR protocol [CJ03], proactive routing protocol for use in MWNs, because OLSR can easily incorporate each function as a plugin.

The proposed scheme consists of the following four functions.

- Monitor/Capture Function: sends and receives probe packets.
- Notification Function: advertises AP's Direct Values (DVs).
- Reputation Functions: calculates Global Value (GV) from DV and the Indirect Values (IVs), also determines misbehaving nodes based on given

evaluation policies.

- Path Manager (MGR): coordinates link management function of OLSR.

Each of the above functions, as well as a GUI, is detailed in the following subsections.

4.3.2 Monitor/Capture function

The monitor function finds neighboring APs and 2HN-APs to evaluate neighboring AP along with topology information of the OLSR. The monitor function refers to the LSDV of OLSR regularly, and maintains information of a pair of target (neighboring) AP and its corresponding 2HN-AP. Furthermore, this function sends a probe packet to each 2HN-AP based on pair information. This probe packet should pass through the target AP to be evaluated; however, if this function uses the default routing table managed by OLSR, a problem occurs in which a neighboring AP does not forward the probe packet. To solve this problem, this function maintains a separate routing table to transmit the probe packet.

The capture function receives probe packets from 2HN-APs, and maintains a count of the number of received packets, the number of lost packets, and the number of duplicate packets per source AP. Note that duplicate probe packets are generated by damage or loss of the ACK frame in the MAC layer. When such duplicated packets are generated, because the number of probe packets received at a receiving AP grows more than the number of probe packet transmitted at the transmitting AP, the function cannot correctly calculate a forwarding rate without also counting the number of duplicate packets. Thus, by a adding a sequence number to the probe packet, the function can determine whether the same probe packet was received.

4.3.3 Notification function

The notification function advertises information, such as the number of received packets, lost packets, duplicate packets, and DVs per neighboring AP to 2HN-APs. Furthermore, when this function receives information from a notification function of 2HN-AP, it stores such DVs

as IVs. The notification function of each AP calculates the DR of each neighboring AP per 2HN-APs with the information received using equation (3.1) above.

4.3.4 Reputation function

The reputation function calculates DV of a neighboring AP by using DR from equation (3.2). Furthermore, this function calculates the GV of each neighboring node by using this AP's DV and IV received by the notification function and calculated from each 2HN-AP based on equation (3.3).

4.3.5 Path MGR

The path MGR provides a mechanism to eliminate or recover a target (neighboring) AP from a network by using evaluation results of the reputation function. The path MGR consists of a function of link metric manipulation, functions of notification/management, and a function of route calculation to reflect a link metric. Each of these is described below.

A function of link metric manipulation operates a link metric in OLSR. When the GV of a neighboring AP decreases more than a given threshold in each AP, this function increases the link metric of an interface for the neighboring node. OLSR calculates a routing table by using this link metric, and as a result, the target (neighboring) AP is eliminated from a network. When the GV of the neighboring AP recovers, this function decreases the corresponding link metric for the interface, and eventually the target AP can be recovered in the network.

Functions of notification/management send notification messages announcing changes of link metrics to the entire network (i.e., MPR flooding); these function also receive such messages. These functions provide synchronizations of LSDB for all APs. Because version 0.5.5 of the OLSR protocol does not have a mechanism for advertising link metrics, this notification/management functionality is added to 210th MSG types (UDP). The notification for MPR flooding considers the loss by UDP; the function of notification advertises the message for a constant period. When OLSR receives this message and confirms the alteration

to a link metric, OLSR recalculates the routing table. OLSR determines the shortest path by using Dijkstra's algorithm, in which the number of hops is considered as a link metric. Hence, OLSR can calculate the routing table by using link metrics. As a result, when a route having a given AP that decreases GV becomes the shortest path, the OLSR protocol does not select this route as an optimal route.

From the fore-mentioned implementation, each AP can evaluate neighboring APs, and can eliminate misbehaving nodes from the network based on evaluation results.

4.3.6 GUI

To observe the network topology using my proposed scheme, a GUI is used that displays in real time the number of APs that compose the network, details of the topology state, and the GV of each AP. A specific server is unnecessary in this GUI display because each AP can output this GUI.

4.3.7 Implementation specifications

The proposed scheme is implemented on a terminal having operating system FedoraCore 6 [Fed], and olsrd version 0.5.5 [OLS] of olsrd.org as OLSR. The implementation language is C, with version of GNU Compiler Collection [GCC]. JDK 1.5.0 [JDK] and Tomcat 5.5.23 [Tom] are used for a GUI server software, and Adobe Flash [Fla] is used for the GUI client.

4.4 Verification of Performance

To verify the operation of this implementation, we built an MWN by using a terminal and performed experiments. We first verified cooperative evaluation schemes of neighboring AP with 2HN-APs. Second, we verified eliminating and recovering schemes for a misbehaving AP.

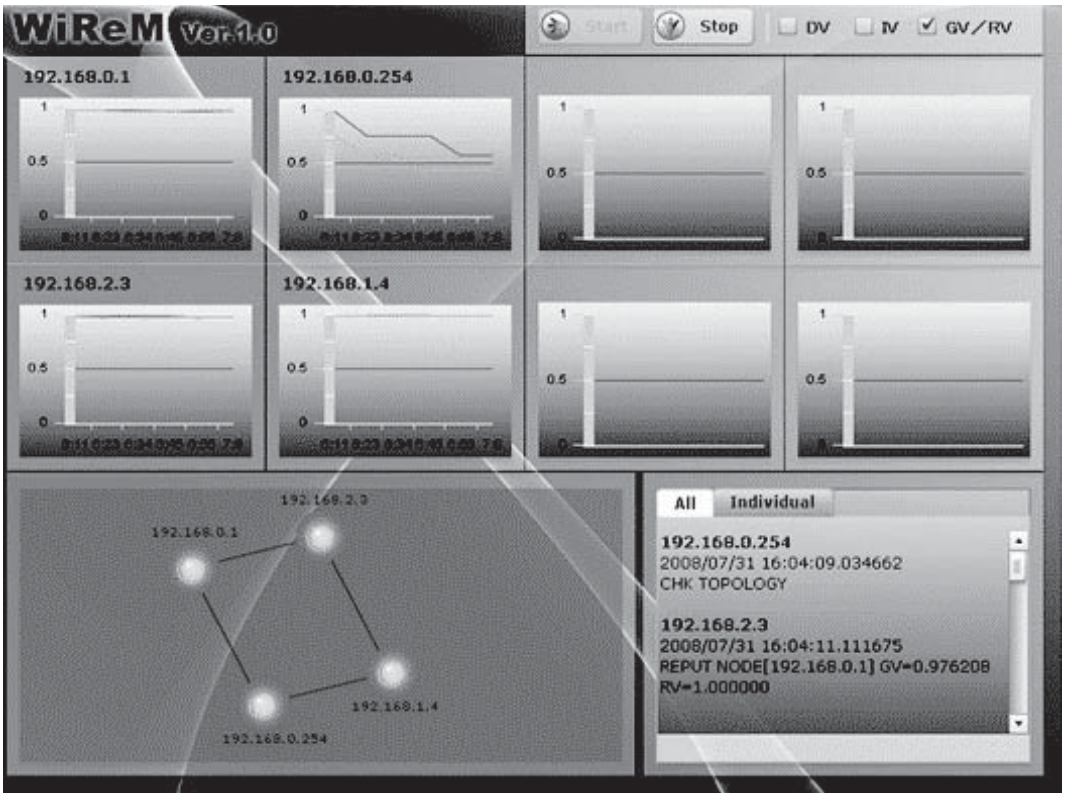


Figure 4.2: GUI Screenshot

4.4.1 Environment

To verify the operation of this implementation using my proposed scheme, we created AP using a PC with two wireless interfaces. The hardware used for AP is MP965-D of AOpen Co., having a Core2Duo 2.2 GHz CPU and 1 GB memory. Each AP has two wireless interfaces having IEEE 802.11 a/b/g of Lenovo Co., and supports the multi-interface/radio environment. Each AP has CentOS 5.1 as an operating system. Each AP is connected in ad hoc mode using IEEE 802.11a; the wireless channel is set to interfere as little as possible. However, because the distance between each wireless card stored in the terminal is approximately 5 cm, interference in the terminal did occur. The purpose of this study is detecting misbehaving APs according to packet loss at the network layer. Thus, communication performance degradation caused by wireless interference at a PHY/MAC layer is acceptable and

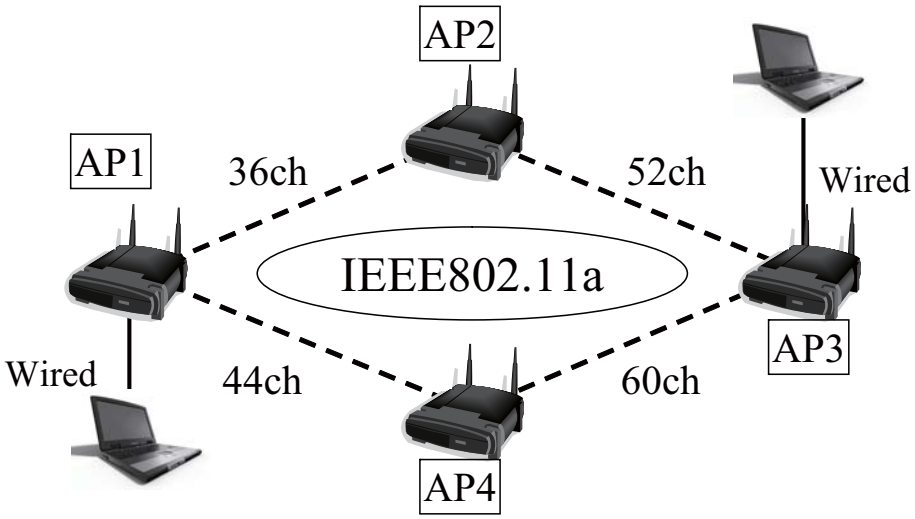


Figure 4.3: Experiment topology: one 2HN-AP

outside the scope of this study.

The sample GUI of Fig. 4.2 shows each AP that comprises this network; the variation of the evaluation value and network topology can be observed in real time. In Fig. 4.2, the upper half of the screenshot shows the state of each evaluation value, and the lower half shows the state of the network topology.

4.4.2 Cooperative evaluating mechanism of neighboring AP with 2HN-APs

In this section, we verify the effectiveness of my proposed cooperative evaluation schemes. To investigate the difference between the number of 2HN-APs and the variation of evaluation values, we verified my proposed scheme in the topology shown in Figs. 4.3, 4.4, and 4.5.

The distance between APs is approximately 50 cm in each topology. To artificially generate a misbehaving AP, AP that intentionally discards probe packets is set up. This misbehaving AP is occurred AP4 in Fig. 4.3, AP5 in Fig. 4.4, and AP5 in Fig. 4.5. After steady state behavior for 60 s, a period of 60 s is set for packet discarding. Figs. 4.6, 4.7, and 4.8

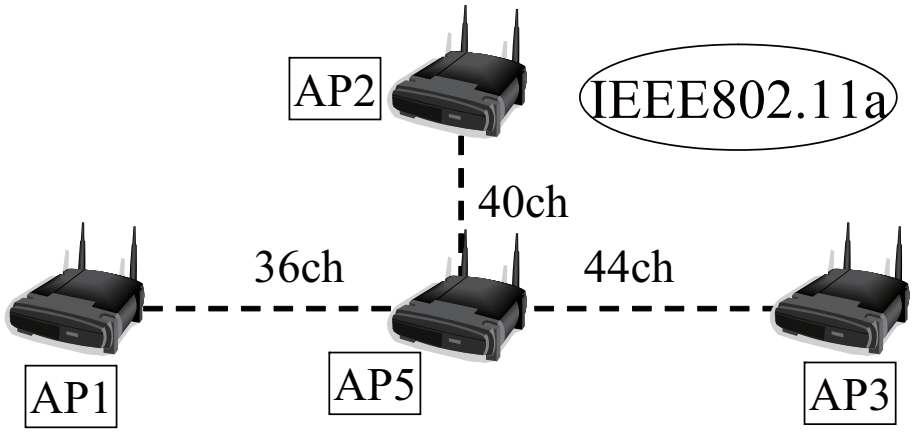


Figure 4.4: Experiment topology: two 2HN-APs

show the GVs of APs that are neighbors of the misbehaving AP. In these figures, the horizontal axis shows the elapsed time and the vertical axis shows the GV. Legends with in the figure noted “APa->APb GV” map the GV of APb that APa maintains.

From the results of Figs. 4.6, 4.7, and 4.8, an AP that is a neighbor of a misbehaving AP decreases the GV of the misbehaving AP after probe packet discards occur. The GV drops to zero approximately 20 s after packet discards start occurring. Furthermore, the GV recovers gradually after packet discarding ends. The GV linearly increases until the threshold at which each AP eliminates a misbehaving node from a network is exceeded; this threshold is set to 0.5 in this experiment. After exceeding the threshold, it reaches the lowest value of DV and IV.

From the results of these experiments, we confirmed that my proposed scheme can detect a misbehaving node even when the number of 2HN-AP is varies. A delay between one and three seconds was observed in the GV calculation for each result. The time difference between each AP is approximately 0.1 s, because each AP uses the network time protocol [Mil92]. We conclude that this delay is caused by the time that elapses from the receipt of IVs from 2HN-APs to the calculation of GV.

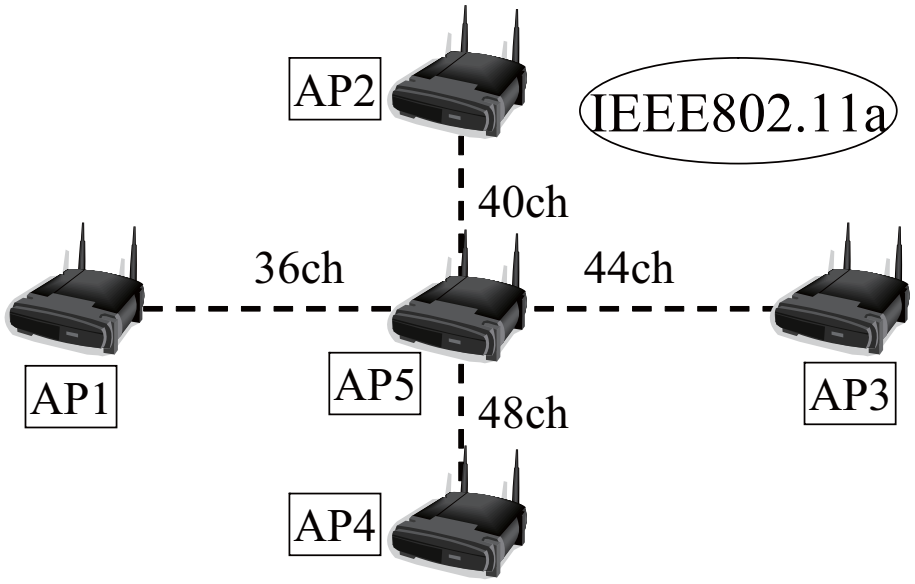


Figure 4.5: Experiment topology: three 2HN-APs

4.4.3 Verification of routing table reconstruction

In this section, we verify the successful operation of the routing table reconstruction mechanism. In this experiment, we use the network topology shown in Fig. 4.3. Each station (terminal) connects to AP1 and AP3 with a wire, and TCP traffic flows between these stations. A route via AP4 is set as the priority in the olsrd. In this state, AP4 is then set to discard probe packets, and each AP evaluates neighboring APs autonomously. Through this experiment, we confirmed that this network switches the route to AP2 instead of AP4.

Five seconds after the simulation begins, iperf simulates the flow of TCP traffic from AP1 to AP3. To confirm that the route switches correctly, traffic via AP2 and AP4 is measured. After 60 s, packet discarding is set to occur in AP4 for 60 s.

Fig. 4.9 shows measurement results of the simulated traffic. In this graph, the horizontal axis shows the elapsed time and the vertical axis shows the amount of traffic. Between 0 and 60 s, traffic flows at approximately 5 Mb/s via AP4; however, GVs for AP4 of AP1 and AP3 decrease as a result of packet discarding of AP4. When the GVs fall below the default

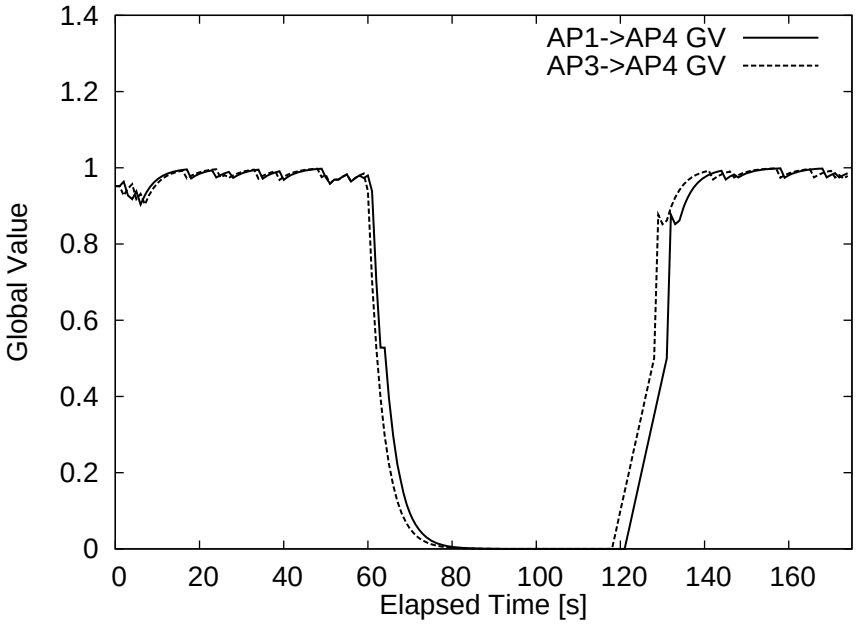


Figure 4.6: Result of GV: one 2HN-AP

threshold of 0.5, AP1 and AP3 both increase a link metric for AP4. AP1 and AP3 create a routing table including a new route via AP2. A delay of approximately four seconds occurs in creating the routing table. It can be observed from Fig. 4.9, that the route that the network uses switches from AP4 to AP2. Furthermore, after packet discarding terminates at 120 s mark, GVs for AP4 in AP1 and AP3 gradually recover. AP1 and AP3 decrease link metrics for AP4 when the GVs exceed the default threshold of 0.5. As a result, AP4 returns to the network. From Fig. 4.9, it can be observed that traffic switches back to the route via AP4 after approximately 12 s.

From these results, we conclude that each AP can reconstruct a routing table autonomously because of a decrease in the GV in one or more neighboring APs. This can be used to incorporate the malfunctioning AP when it recovers.

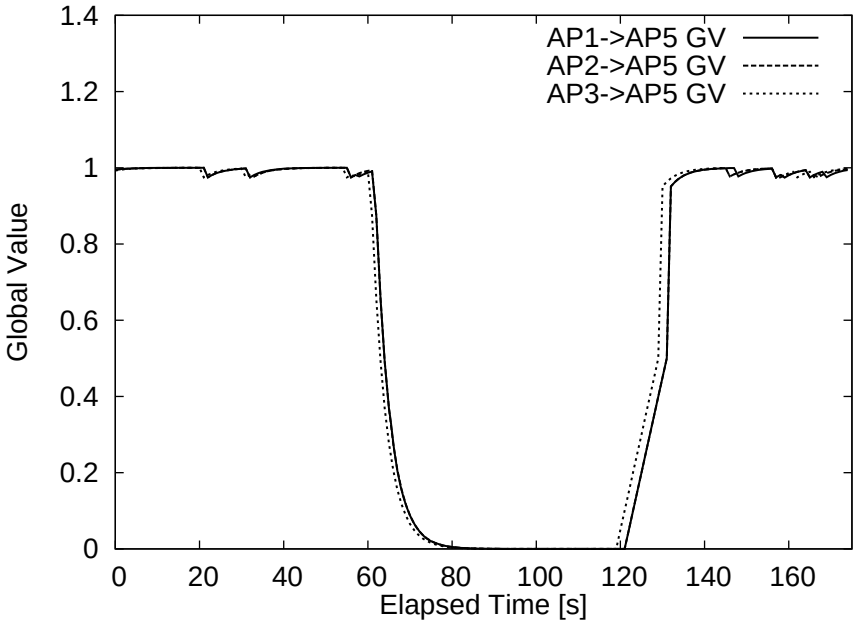


Figure 4.7: Result of GV: two 2HN-APs

4.5 Conclusion

In this chapter, we verified my proposed cooperative evaluation scheme for neighboring AP with 2HN-AP by implementing the proposed scheme on an actual AP. In this implementation, to build the proposed scheme into the OLSR protocol, we examined a mechanism that evaluates each neighboring AP's effectiveness and efficiency. AP that did not forward packets correctly was detected as a result of the verification experiment in which a PC was used to construct APs. Furthermore, we verified the functions of eliminating the misbehaving AP and incorporating this AP once it had recovered. The results verified that my proposed evaluation scheme for neighboring AP operated appropriately in an actual MWN. We showed that this scheme is effective for the improvement of network reliability.

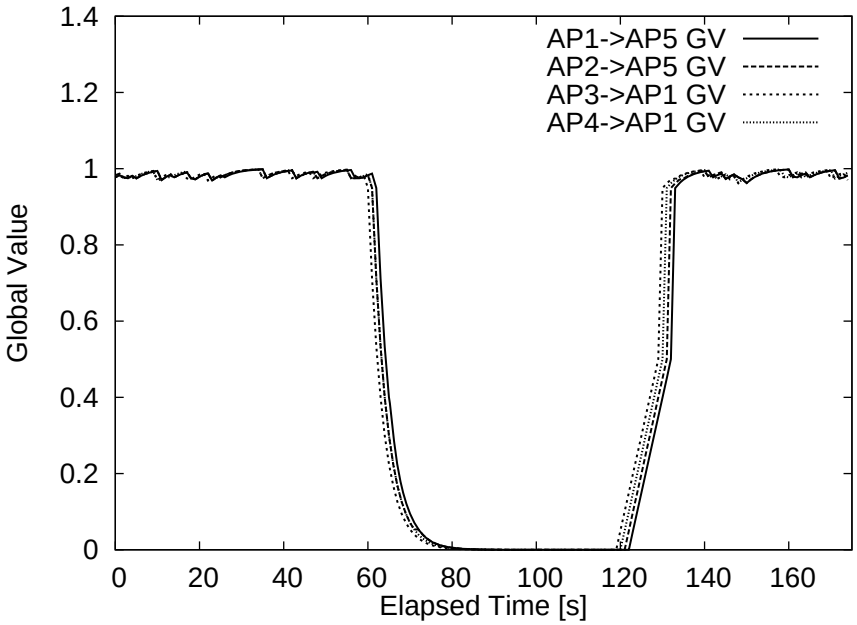


Figure 4.8: Result of GV: three 2HN-APs

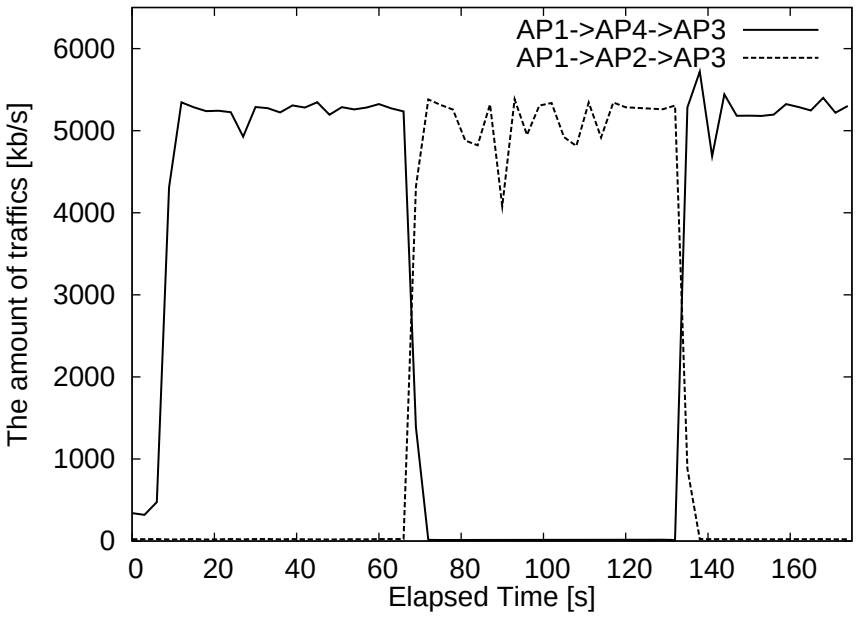


Figure 4.9: The amount of traffics on AP3

Chapter 5

A Network Reconfiguring Scheme against Misbehaving Nodes

5.1 Introduction

A multi-hop wireless network (MWN), where wireless stations (nodes) connect to each other using radio communication, has been investigated by many researchers. Because an interface (I/F) can be used at each link, reducing the cost of a wireless device, the use of MWNs is expand bandwidth and improve communication performance. To maintain high communication performance, higher reliability is required for nodes in the network. However, nodes may not always function well. A node may stop functioning due to a power outage, or can malfunction because of various reasons, including sabotage. Such a misbehaving node must be detected quickly and eliminated, because it can decrease the performance of the entire network.

Many researchers have been studying the detection of a misbehaving node, such as a malicious or selfish node, in mobile ad hoc networks (MANETs) and sensor networks. In CORE and CONFIDANT[MM02][SB02], a node monitors the behavior of neighbor nodes by overhearing the data that they transmit. Each node creates a reputation of its neighbor nodes using the results of this monitoring. Such methods are called a reputation-based scheme. However, in a MWN that consists of nodes with multi-interface and multi-radio characteristics, it is difficult for each node to monitor the behavior of its neighbor nodes [GPM08].

Therefore, a conventional reputation-based scheme cannot be used in such a MWN. We proposed a novel neighbor-node monitoring method in a MWN with multi-interface and multi-radio [NNI+09a] [NNI+08]. In this detection method, each node creates a reputation of its neighbor nodes with cooperating two-hop neighbor nodes, and assesses whether the neighbor nodes are misbehaving. We evaluated the detection method by a simulation and an experiment that used a terminal with the Linux operating system: it was clearly shown that the detection method can detect a misbehaving node correctly [NNI+09a] [NNI+08].

In this paper, we will discuss a network reconfiguring scheme against misbehaving nodes after their detection. As a network reconfiguring against misbehaving nodes, many researchers investigated a routing approach that eliminates the misbehaving node from a communication path by providing information about the node to the routing protocol has been investigated. However, when eliminating a misbehaving node completely from a network, the communication performance of the whole network can degrade, because the link bandwidth that can be used is reduced simultaneously. In this paper, we propose a network reconfiguring scheme in which nodes linked to a misbehaving node cooperate with other nodes, and unused I/Fs can be used efficiently. The aim of this scheme is to suppress the degradation of communication performance.

In our proposed scheme, each node reconstructs a network autonomously using the I/F of the neighbor nodes linked to a misbehaving node. Because this scheme considers connectivity as important, it uses nodes with only a few link numbers with priority, and builds a link with a high transmission rate. The degradation in communication performance is suppressed by obtaining sufficient network capacity and constructing a network using the optimal link. We evaluate the effectiveness of our proposed scheme using simulations. We carry out simulations with thirty topologies created at random and investigate the throughput properties. We examine an advantage of the proposed reconfiguring scheme by comparing with several reconfiguring schemes.

This chapter is organized as follows. In Section 5.2, we discuss the existing studies and

their limitations. In Section 5.3, we demonstrate our proposed network reconfiguring scheme for misbehaving nodes. Section 5.4 describes our simulation environment. We present the simulation result and discussion in Section 5.5. Finally, we summarize our study in Section 5.6.

5.2 Detection schemes and Countermeasures against Misbehaving Nodes

In this section, we describe existing detection schemes for misbehaving nodes, as well as reconfiguring schemes using routing protocols after the detection of misbehaving nodes.

5.2.1 Detection Schemes for Misbehaving Nodes

Various schemes for detecting misbehaving nodes in mobile ad hoc network (MANETs) were proposed. Detection schemes in MANETs, such as CORE and CONFIDANT, are classified as reputation-based schemes [MM02][SB02]. In such schemes, each node can overhear the data that its neighbor node transmits to the next neighbor node, and it generates the reputation score of the neighbor node based on the monitoring result. However, these detection schemes cannot be used effectively on WMNs with multi-interface and multi-radio, because it is difficult for a node to overhear data from a different channel that a neighbor node sends in a multi-interface and multi-radio environment. Therefore, we proposed a novel neighbor-node monitoring scheme for a WMN with multi-interface and multi-radio [NNI+09a] [NNI+08]. In this scheme, for detecting misbehaving nodes, each node creates a reputation of neighbor nodes with cooperating two-hop neighbor nodes. We evaluated the proposed scheme using a simulation and an experiment on a terminal with the Linux operating system: it was clearly shown that this method can detect a misbehaving node correctly.

5.2.2 Reconfiguring Scheme against Misbehaving Nodes

Many researchers have studied the countermeasure of misbehaving nodes in mobile ad hoc and sensor networks. In these countermeasures, the routing protocol receives information regarding misbehaving nodes found by its detecting method [SNYA06][KW03][GA08]. Further, the misbehaving nodes are eliminated from the network, because the routing protocol modifies a link cost around misbehaving nodes.

The AODV-REX is a routing protocol that employs countermeasures against misbehaving nodes [OR08]. This is a modification of AODV, which uses a hop count for routing cost. However, in a MWN that has an I/F for every link, the node that adjoins a misbehaving node cannot use an I/F linked to the misbehaving node when the anomalous node is eliminated from the network. Because the available communication capability in the whole network decreases, the performance of each node may also be degraded.

5.2.3 Challenges for Network reconfiguring

Existing misbehaving node detection methods are discussed by only misbehaving detection. As a countermeasure after detecting the misbehaving nodes, each node eliminates misbehaving nodes from a network by cutting the link connected to the misbehaving nodes. Or each node modifies a link cost around the misbehaving nodes and avoids those nodes, by providing a routing protocol with the information on misbehaving nodes. Hence, a network that misbehaving nodes are eliminated degrades communication performance, because the network cannot use I/Fs and wireless resources efficiently. On challenge for network reconfiguring, it needs efforts that the performance is not degraded. First, each node must avoid that a network is divided, after eliminating the misbehaving nodes. Only by cutting a network simply, a network island is formed and the node that cannot communicate to other nodes may occur. Therefore, each node considers network connectivity completely. Second, nodes that adjoin the misbehaving nodes share various information autonomously, and each node must know utilizable I/Fs. If the nodes cannot share the information, it is difficult to construct a stable

Table 5.1: Transmission rate based on Distance

Transmission rate [Mb/s]	54	48	36	24	18	12	9	6
Distance between nodes [m]	5	7	9	20	25	40	50	60

network, because nodes cannot link each other. Third, each node must consider influences of wireless characteristic, and use wireless resources efficiently. If utilizable I/Fs are connected by a single wireless channel, a communication performance may degrade. Finally, the existing detection and reconfiguring schemes do not consider the environment of MWNs with multi-interface, multi-radio, and multi-rate. In this chapter, the network reconfiguring scheme that considered the above problems must be proposed.

5.3 Proposed Scheme

In this section, we first define a network environment and a misbehaving node in our proposed scheme. Our proposed countermeasure is then described, which reconfigures the network with unused I/Fs after the detected misbehaving nodes are eliminated from the network.

5.3.1 Assumption of Network Entities and Misbehaving Nodes

In this research, each node constructs a backbone network as a mesh network in a variety of MWNs. Hence, the nodes do not have mobility. All nodes have multiple I/Fs. In the case of the initial construction of a MWN, an I/F is used to connect a link, and all links use different channels. Moreover, not all nodes use multiple channels for an I/F. The transmission rate between links is set up according to the distance that a frame error does not cause. As shown in TABLE 5.1, the transmission rate based on the distance between nodes is computed by QualNet 4.5 [Qua], a network simulator. To construct a backbone network without mobility nodes, a proactive-type routing protocol is used, such as Optimized Link State Routing

Table 5.2: Transmission Rate of each candidate link

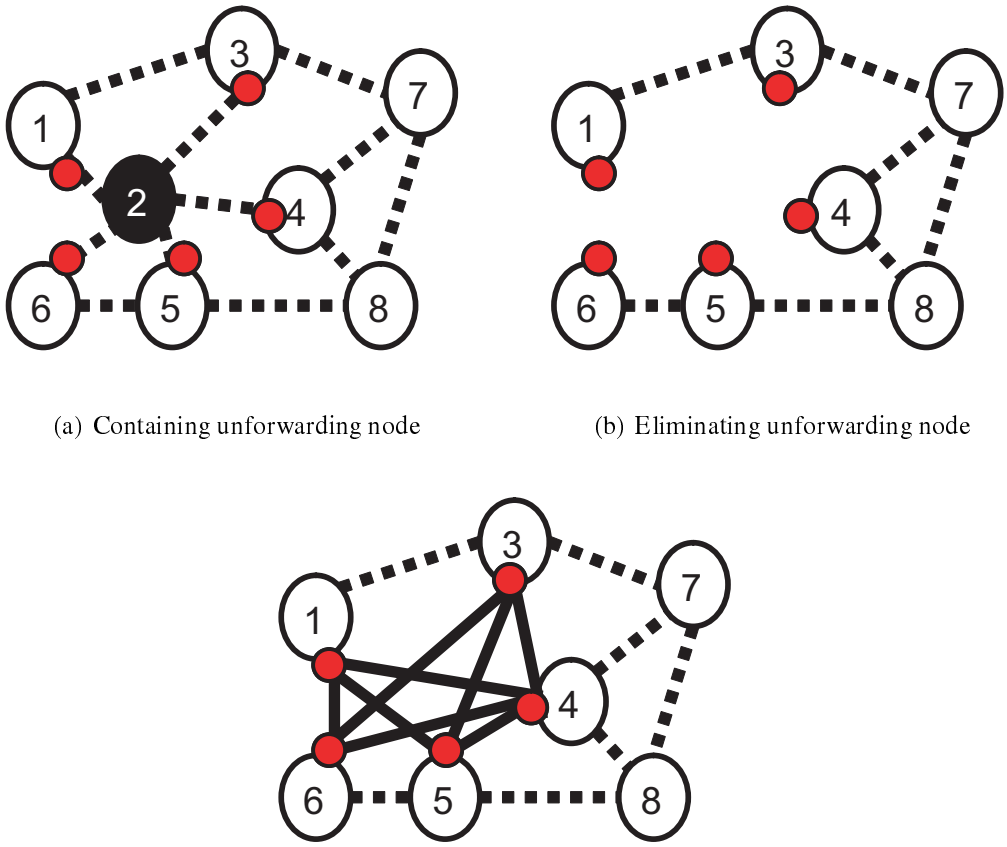
both end nodes of a candidate link	transmission rate [Mb/s]	both end nodes of a candidate link	transmission rate [Mb/s]
1-4	18	3-5	24
1-5	36	3-6	24
1-6	36	4-5	24
3-4	36	4-6	24

(OLSR).

A misbehaving node is generally a node that conducts various attacks, a troublesome node caused by a failure or instantaneous blackout. Misbehaving nodes can be classified into the following three categories. Firstly, a "malicious node" that aims to create network confusion by attacking other nodes: for example, by floating false routing information. Secondly, a "selfish node" that does not transmit packets from other nodes, in order to save power consumption and to retain its available bandwidth [SXA08]. Third, a "failure node" that simply cannot function normally because of physical reason. However, in this paper, a misbehaving node is defined as the node which has a problem in the packet transmission, affecting availability of networks containing a malicious, selfish, and failure nodes. We call such nodes "unforwarding nodes." When two or more unforwarding node occurs, the proposed scheme eliminates them in the sequential order which malfunction caused. For our further discussion, we assume that the unforwarding node has been accurately detected, because the detection method is beyond the scope of this paper.

5.3.2 Eliminating Unforwarding Nodes and Deciding on Candidate Links

In our proposed scheme, the node that adjoins unforwarding nodes disconnects them after unforwarding nodes detection, and eliminates unforwarding nodes from a network. The



(a) Containing unforwarding node

(b) Eliminating unforwarding node

(c) Candidate Links (solid lines)

Figure 5.1: Sample topology of the proposed scheme

network that maintains a high level of communication performance is constructed using the I/Fs optimally linked to the unforwarding nodes. An I/F that is connected to an unforwarding node is called a “neighbor”, and “candidate links” are defined as the links that can connect with the neighbor and other neighbors. Links that are not influenced by an unforwarding node are defined as “actual links”. In the proposed scheme, the merging chosen obtains the best communication performance from candidate links.

Fig. 5.1 shows the flow of candidate-link determination. When node 2 is an unforwarding node, as shown in Fig. 5.1(a): this node is eliminated from the network as shown in

Table 5.3: Transmission Rate of actual links

both end nodes of an actual link	transmission rate [Mb/s]	both end nodes of an actual link	transmission rate [Mb/s]
1-3	36	5-6	54
3-7	36	5-8	24
4-7	48	7-8	48
4-8	54		

Fig. 5.1(b). A network is reconfigured using the neighbor whose I/Fs can be reused for the elimination of an unforwarding node. The solid lines in Fig. 5.1(c) are candidate links that can be newly connected. Moreover, the dotted lines in Fig. 5.1(c) are actual links that are not influenced by an unforwarding node. The transmission rate of each candidate link is decided on the basis of the distance between the neighbors. The transmission rate of the candidate links in Fig. 5.1(c) is shown in Table 5.2.

5.3.3 Topology reconfiguring Scheme

In the proposed countermeasure, a neighbor assigns the priority to connect one-to-one with another neighbor. The neighbor that obtains the preference is called a priority neighbor, and a neighbor connected to the priority neighbor is called a target neighbor. The pairing of the priority neighbor and the target neighbor creates a link. The pair is repeatedly chosen until the neighbor that is not connecting the link is left. In addition, the topology reconfiguring defined by the autonomous behavior of nodes is described.

Determination of a Priority Neighbor

A priority neighbor is determined in order to choose the connecting link for reconfiguring a network from the candidate links. The priority neighbor can select the connecting link from

the candidate links preferentially. This neighbor is chosen from all the neighbors that are still not connected by the link between neighbors, and only one is determined, according to the following rules. First, the node that has the minimum number of the candidate links is found. Considering the connectivity of topology, there is a decrease in the possibility that the connecting link will be isolated from a network by this rule after the network is reconfigured. Second, to use a neighbor connected at a higher transmission rate than other priority neighbors, a neighbor with the maximum sum of the transmission rates on candidate links is searched for. Third, a neighbor with many actual link numbers is chosen to reduce the communication hop count in the network after the network is reconfiguring. Finally, a neighbor with the large sum of the bandwidth of actual links is found because a network obtains more bandwidths.

The order of priority neighbor determination is summarized to the following.

pre) Unconnected to other neighbors.

i) Minimum number of the candidate links.

ii) Maximum sum of the transmission rates on candidate links.

iii) Maximum number of actual links.

iv) Maximum sum of bandwidth of actual links.

Determination of a Target Neighbor

A neighbor that connects with a priority neighbor is defined as a target neighbor. The target neighbor is selected from the nodes that have not connected a link with other neighbors. First, a priority node chooses, as a target node, the neighbor with the least candidate links whom the neighbor will be connected with. This is to avoid isolating this connecting link from the network during the determination of a priority neighbor. Second, when there are two or more candidates for the target node, a priority node chooses a neighbor connectable

at a high transmission rate. Third, a priority neighbor selects the neighbor in which the total transmission rate of the candidates of a target node is minimal. When the candidate of two or more target nodes that were not chosen connects with other priority nodes in this phase: this rule establishes a high transmission rate for both the link of the target node chosen in this phase that of the node that was not chosen. Fourth, a priority neighbor selects the sum of the number of the actual links and the bandwidth at the time of priority-node determination. Finally, a priority neighbor determines a node with largest received signal strength indication (RSSI) as a target node.

The order that a priority neighbor chooses a target neighbor is summarized as the following.

pre) Unconnected to other neighbors.

i) Minimum number of the candidate links.

ii) Maximum transmission rates has.

iii) Minimum total transmission rate has.

iv) Maximum number of actual links.

v) Maximum sum of bandwidth of actual links.

vi) Maximum RSSI.

After determining the pairing of a priority and target nodes, the link is connected using a wireless channel that does not interfere with other links. A channel of a link connected to an unforwarding node is allocated to the link to be reconfigured. The channel is used for small order. The determination of a priority node and a target node is repeated until the number of neighbors that are not connecting the link to all the neighbors is one or less.

Effective Connection of a Surplus Neighbor

If the number of neighbors that are not connecting a link is one, the neighbor cannot build a link using the abovementioned procedure. This surplus neighbor should be used effectively. First, the surplus neighbor searches a connecting rate with both of the end neighbors of all constructing links. Because the performance decreases (by performance anomaly) when the transmission rate between the surplus neighbor and the end neighbor is less than that of the link, the surplus neighbor connect with a link that a transmission rate is higher than itself. A performance anomaly is a problem caused when using the wireless of the same channel of the wireless LAN of IEEE 802.11 standard, and the throughput of nodes at higher rates will be limited to the equivalent throughput level of the lower transmission rate [HRBSD03]. If the surplus neighbor cannot connect with all neighbors, the surplus neighbor doesn't be used. The following processing is conducted when there is a neighbor of the candidate who can connect. Second, when two or more connectable neighbor pairs exist, to construct the network of a low communication hop count, the surplus neighbors choose a pair with the highest total number of actual links that both the end neighbors of the reconfigured link have. Finally, when a connecting link cannot be determined, the surplus neighbor chooses a neighbor pair with the maximum total bandwidth of links.

The procedure of determining the neighbor that a surplus neighbor connects is summarized to the following.

pre) Searching of a connecting rate with both end neighbors

i) Eliminating the neighbors that has transmission rate less than itself.

ii) Maximum number of links.

iii) Maximum total bandwidth of links.

Autonomous Behavior of Nodes

In our proposed scheme, each node is reconfigured to operate autonomously without intensive control. For the node to operate fully autonomously, all nodes must know the shape of the network topology, the number of links of each node, and the channel used. The network topology and link number are obtained from the routing tree provided by the proactive routing protocol. Regarding the channel used, when eliminating unforwarding nodes and reconfiguring the topology, the scheme that does not include the channel of a neighbor is required. This is solved by sharing the information to all the neighbors on the channel, using a beacon, as to which neighbor was determined (such as the smallest channel) after the unforwarding node disconnection.

5.3.4 Example of the Flow of the Proposed Scheme

The example of a topology reconfiguring is shown in Figs. 5.1 and 5.2. Transmission rates of the topology are shown in Tables. 5.2 and 5.3. First, the priority neighbor is decided from all neighbors. From Fig. 5.1(c), because node 4 has four candidate-links and nodes 1, 3, 5, and 6 have three candidate-links, node 4 is passed over candidate of the priority neighbor (requirement III.C.1.i). Additionally, its attention is paid to total transmission rate of candidate-links, node 1 is 90 Mb/s and nodes 3, 5, and 6 is 84 Mb/s from Table 5.2 (requirement III.C.1.ii). Hence, the I/F of node 1 is determined as a priority neighbor. Second, the candidates for the target neighbor for node 1 are nodes 4, 5, and 6. Because node 4 has four candidate-links and nodes 5 and 6 have three candidate-links from the requirement III.C.2.i, node 4 is passed over a candidate of the target neighbor. Because the maximum transmission rate of nodes 5 and 6 are 36 Mb/s, a candidate of target neighbor cannot be determined from requirement III.C.2.ii. Node 1 chooses node 5 as a target neighbor from requirement III.C.2.iii , because node 5 has two actual links and node 6 has one actual link. Next Step, a next priority neighbor is decided from the remaining nodes, nodes 3, 4, and 6. Nodes 3, 4, and 6 have three candidate-links, because they are a triangle topology. Its attention is paid to

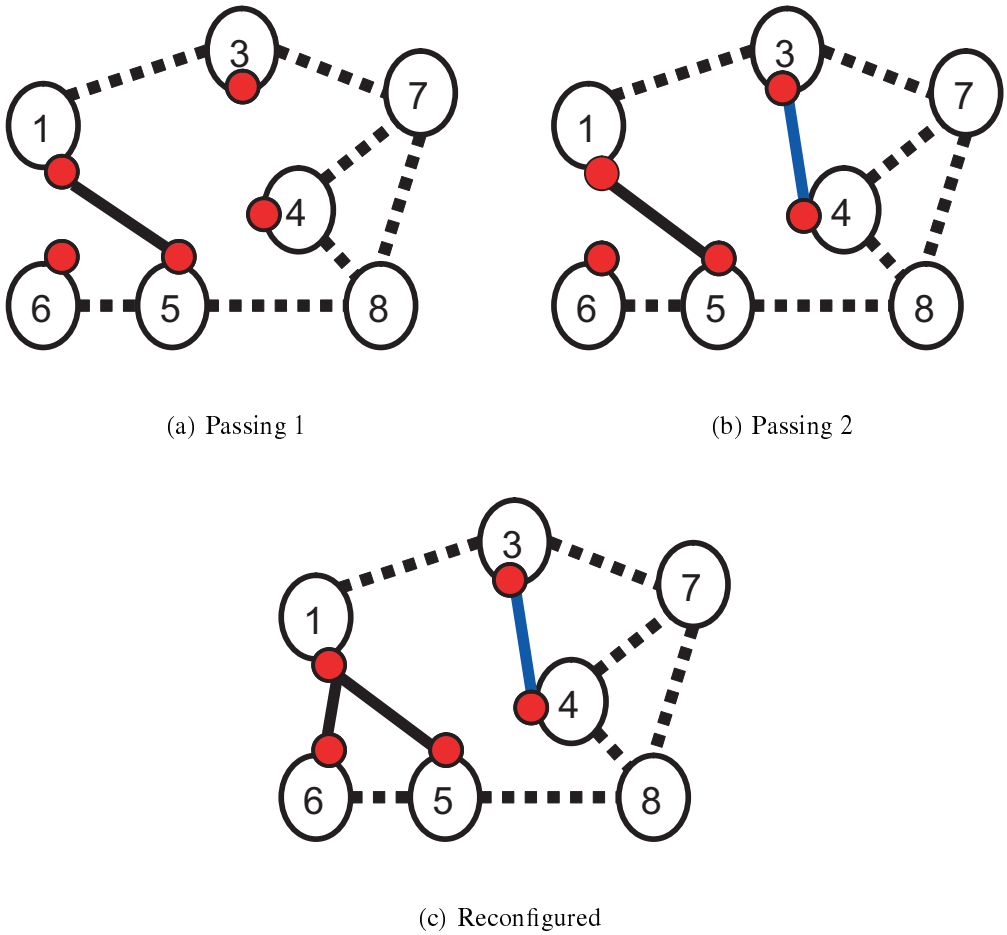
total transmission rate of candidate-links, nodes 3 and 4 is 60 Mb/s and node 6 is 48 Mb/s. Nodes 3 and 4 have two actual links. In total transmission rate of actual links, node 3 has 60 Mb/s and node 4 has 102 Mb/s(Table 5.3). Hence, the I/F of node 4 is determined as a priority neighbor. Next, the candidates for the target neighbor for node 4 are nodes 3 and 6. Nodes 3 and 6 have two candidate-links, and maximum transmission rates of node 3 is 36 Mb/s and node 6 is 24 Mb/s. Therefore, node 4 chooses node 3 as a target neighbor. Node 6, which remains examines a connecting rate with all its neighbors. Node 6 can connect to link 3 and 4 at 24 Mb/s, and can connect to link 1 and 5 at 36 Mb/s. Node 6 is connected to link 1 and 5 as a result of considering performance anomaly. The network reconfigured by our proposed scheme is shown in Fig. 5.2(c).

5.4 Simulation Model

The effectiveness of our proposed method is evaluated by the network simulator QualNet 4.5 [Qua]. When a network is first constituted, all links are assigned a different channel, and it is assumed that the influence of an interference of wireless channels does not occur. The transmission rate, based on Table 5.1, such that a frame error does not occur according to the distance is set for each link. The FTP flows, which set the packet size as 1460 bytes, flows for 30 s among all the wireless I/F without an unforwarding node and neighbors are set as a source and a destination node. An unforwarding node causes a packet loss at probability of 0% to 10%. The total throughput of all flows is used as a performance metric.

5.4.1 Simulation Topology

A random arrangement of seven to ten nodes in the range of 30 ms around is used as a topology. For the simulation, we use a topology containing an unforwarding node comprising three to five sets of links. An example of each topology is shown in Figs. 5.3, 5.4, and 5.5. For a comparative study of the topology for our proposed method, we use the topology con-



(a) Passing 1

(b) Passing 2

(c) Reconfigured

Figure 5.2: An example of reconfiguring of topology

taining an unforwarding node (original), eliminating an unforwarding node (conventional), reconfiguring by our proposed method (proposed), and an one-to-one connection (1:1 connection) by transmission rate or RSSI preference. The connecting rates of candidate links in Figs. 5.3 and 5.4 are Tables 5.4 and 5.5, respectively. Moreover, the connecting rate of candidate links in Fig. 5.5 is indicated in Table 5.2 of Section 3.

Furthermore, thirty topologies created at random are simulated in the same environment as the above, and verified the throughput properties. The throughput performance of each reconfiguring scheme is normalized and compared in this simulation. Thereby, the proposed

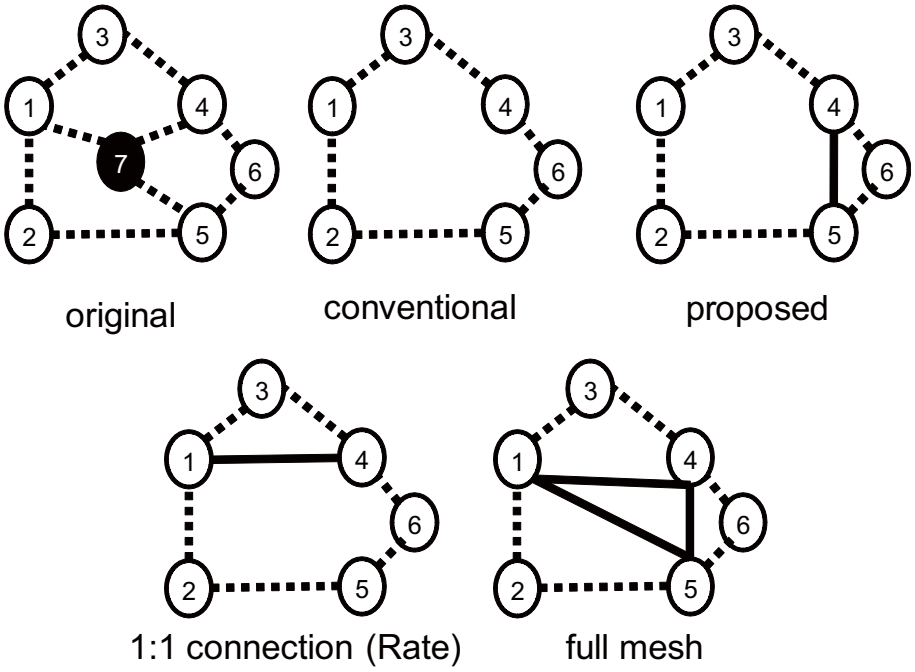


Figure 5.3: Simulation topology 1

scheme will show that it is the highly efficient reconfiguring scheme as compared with others.

5.5 Simulation Result

First, a total throughput of the simulation topology 1 (Fig. 5.3) is shown in Fig. 5.6. The proposed method obtained good throughput compared with other methods in this topology. Hence, the proposed method has little channel conflict, and can maintain a higher transmission rate than other methods can do. Second, a total throughput of the simulation topologies 2 and 3 (Figs. 5.4 and 5.5) is shown in Figs. 5.7 and 5.8. In these topologies, an existing method obtains better result than the proposed method when a packet loss rate is 3% or less. However, in case the packet-loss rate increases, the proposed method obtains a better throughput than other methods. In the simulation topology 3, a proposed method can connect among nodes 1, 5, and 6 at a high transmission rate. Therefore, the proposed method

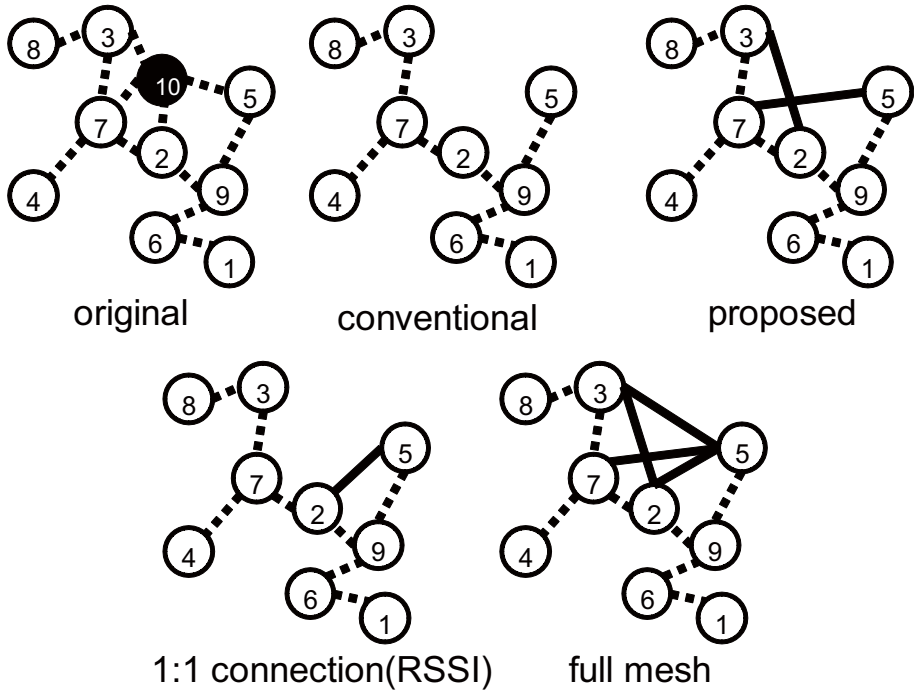


Figure 5.4: Simulation topology 2

can obtain a high throughput compared with 1:1 connections (RSSI and transmission rate), which use two channels equally. Moreover, the network with proposed scheme showed performance better than all the networks which construct of combinations of candidate links in each topology.

Next, a mean hop count for each topology is shown in Table 5.6. A mean hop count has the smallest construction connected with full mesh. Compared with methods of full mesh, the hop count of the proposed methods is large. However, when the proposed methods are compared with other constructing methods, the hop count from other methods decreases, because methods with full mesh are constituted in the scope that performance anomaly does not occur.

Furthermore, we simulated thirty topologies created at random and verified the throughput properties. The throughput and confidence interval of 95% of the reconfiguring of each topology are shown when the total throughput of the topology that eliminated an unforward-

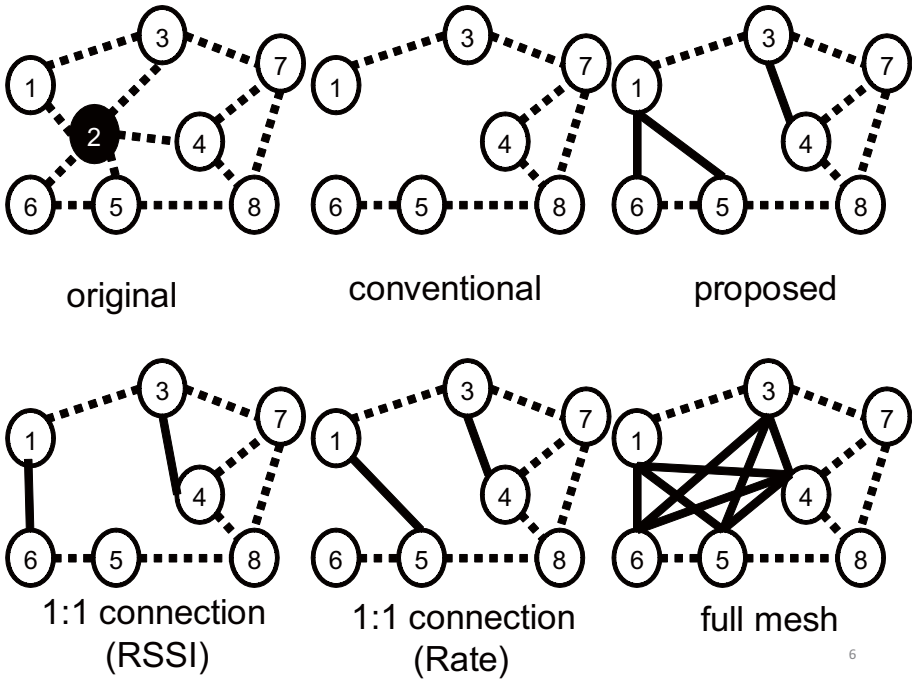


Figure 5.5: Simulation topology 3

ing node is normalized as 1.0. This result indicates that the topology reconfiguring by our proposed method obtained good throughput compared with other reconfiguring methods in which a high packet loss occurred.

The simulation results are summarized as follows. In a topology containing an unforwarding node, the communication performance decreased sharply with the increment in the packet-loss rate of the unforwarding node. Each method of a reconfigured topology can obtain good throughput compared with a topology containing and eliminating an unforwarding node. The proposed method obtained a high throughput compared with other methods. Because the proposed method considers the connectivity of the topology, it can reduce the mean hop count. Furthermore, because a high transmission rate is maintained and it reconfigures the topology using the I/F of all its neighbors, the proposed method can effectively utilize a link bandwidth.

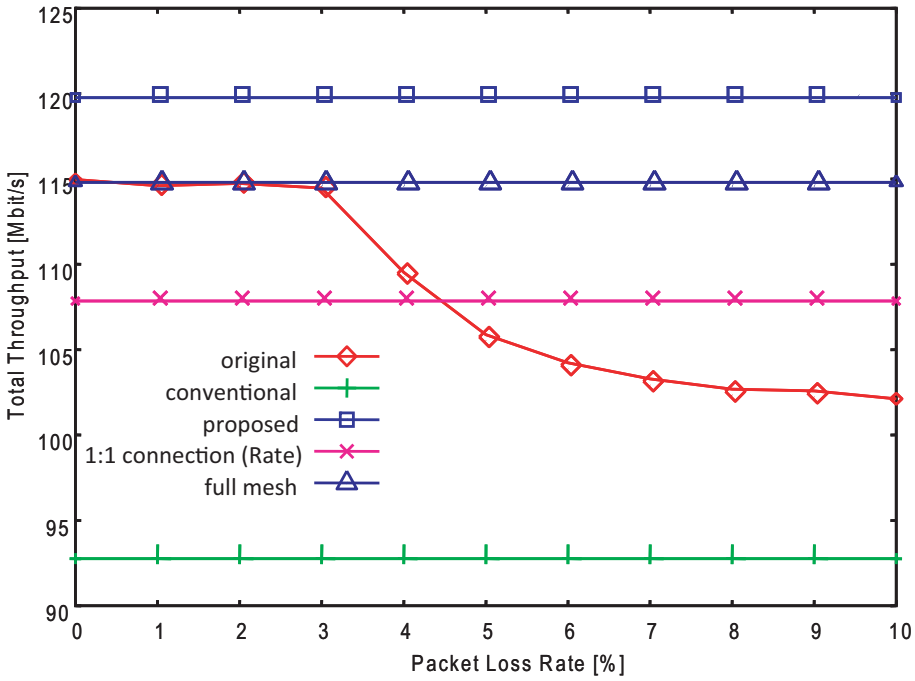


Figure 5.6: Simulation result: unforwarding node with three I/Fs

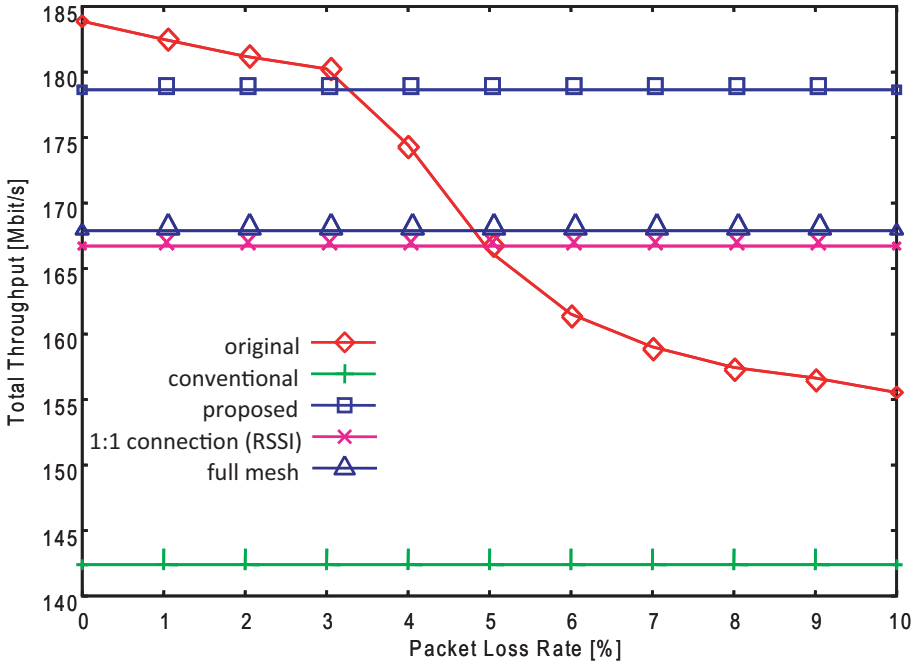


Figure 5.7: Simulation result: unforwarding node with four I/Fs

Table 5.4: Candidate links with three I/Fs (Simulation topology 1)

both end nodes of a candidate link	transmission rate [Mb/s]	both end nodes of a candidate link	transmission rate [Mb/s]
1-4	24	4-5	54
1-5	24	-	-

Table 5.5: Candidate links with four I/Fs (Simulation topology 2)

both end nodes of a candidate link	transmission rate [Mb/s]	both end nodes of a candidate link	transmission rate [Mb/s]
2-3	36	3-5	36
2-5	54	5-7	36

5.6 Conclusion

This paper focused on the communication performance degradation caused by a misbehaving node in MWNs. An unforwarding node, which does not transmit a packet and adversely influences the network availability, was defined. The authors proposed a countermeasure for unforwarding nodes (a topology-reconfiguring method), in which the neighboring node of an unforwarding node cooperated mutually with peripheral nodes and reconfigured a network autonomously. Our proposed method reconfigures topology with an emphasis on the reuse of I/F, the number of the links required to construct, transmission rates, performance anomaly, and a network connectivity. The results of simulation indicate that the proposed method can prevent the communication performance degradation of the entire MWN, and thus the effectiveness of our proposed method is demonstrated.

In future works, it will investigates that the proposed scheme can detect unforwarding node normally, when a MWN becomes larger-scale. Moreover, a verification in various side,

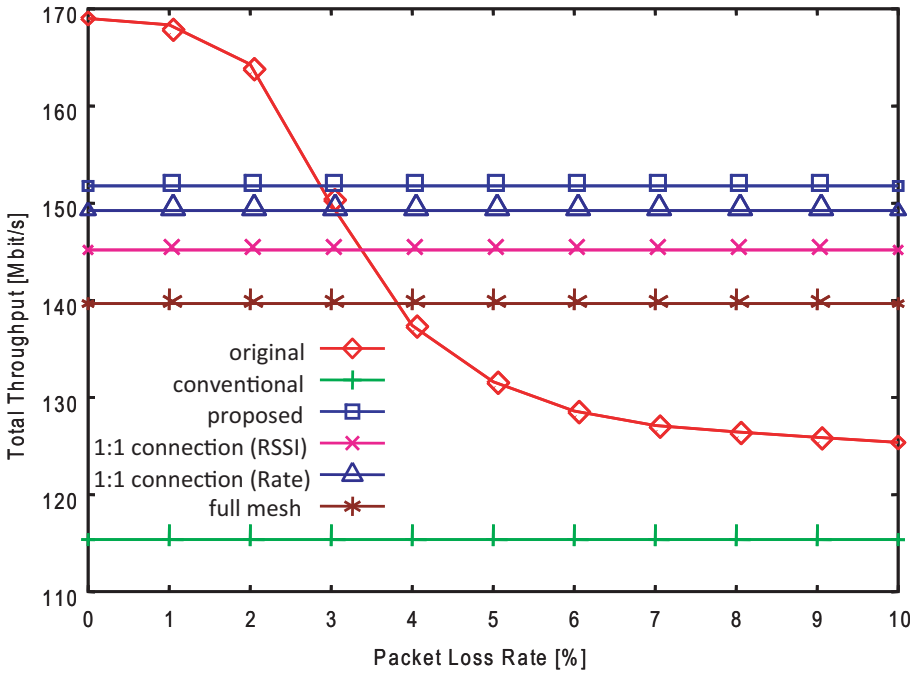


Figure 5.8: Simulation result: unforwarding node with five I/Fs

such as time which a restructuring needs to each node in the proposed scheme, is advanced. Furthermore, the performance in actual MWN is verified by implementing our proposed scheme in Linux terminals.

Table 5.6: Average hop number for each topology

topology	original	conventional	1:1 connection (RSSI)	1:1 connection (Rate)	full mesh	proposed
Fig. 5.3	1.8	1.8	—	1.6	1.35	1.6
Fig. 5.4	2.29	2.53	2.04	—	2.00	2.30
Fig. 5.5	1.62	1.85	1.63	1.56	1.29	1.52

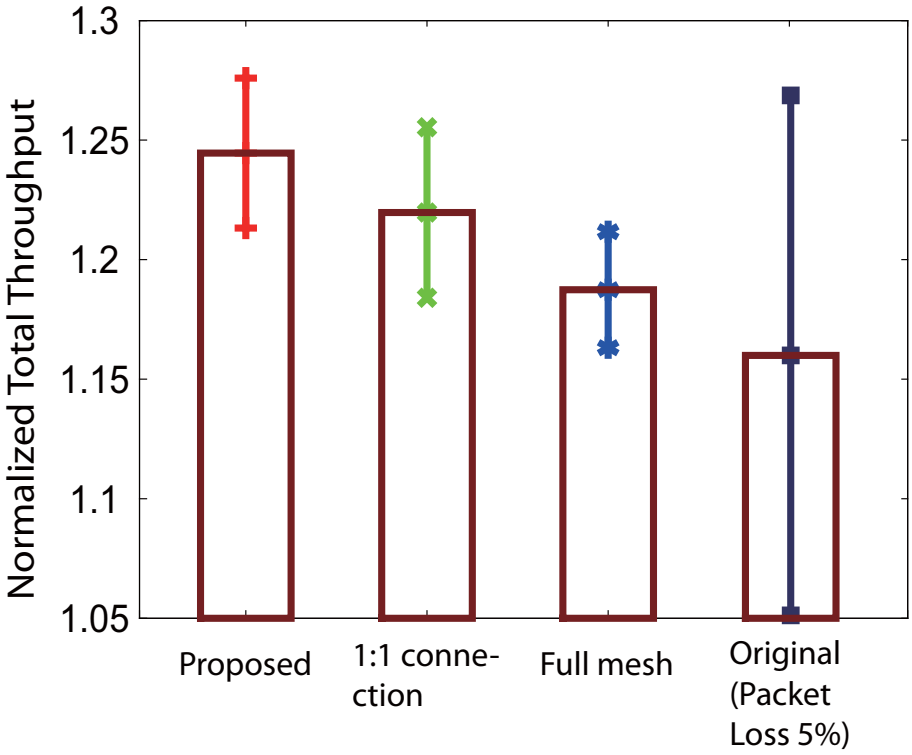


Figure 5.9: Total throughput of each reconfiguring method

Chapter 6

Concluding Remarks

6.1 Summary of this dissertation

In this dissertation, we have focused an actualization of a reliable multihop wireless network. To achieve this network, we have proposed the access point evaluation with packet transfer rate and the reconfiguration scheme.

In Chapter 2, we introduced an IEEE 802.11 wireless LAN technology that is an important entity to achieve a multihop wireless network (MWN). We provided some forms of the access network using wireless LAN. We showed that only a MWN set up the access point (AP) and wireless coverage could be expanded easily. Then, a MWN has some vulnerabilities due to it can construct the network flexibly, and we introduced some threats for a MWN. We explained a requirement of a self-healing scheme that each AP evaluated other AP autonomously and reconstructed the network for an achieving of reliable MWN.

In Chapter 3, we proposed the evaluated scheme of neighboring AP for a MWN with multi-interface/radio. Conventional neighboring node evaluation approaches in MANET evaluated its behavior in order to each AP overhear directly. However, in a MWN with multi-interface/radio, each AP cannot monitor a behavior of neighboring AP immediately to communicate with a different channel. We considered that neighboring AP evaluation can be made by each AP cooperates with peripheral APs. Thus, we proposed the evaluation scheme that each AP monitors a neighboring AP with 2 hop neighbor AP (2HN-AP). This proposed scheme is comprised in reputation-based schemes that each AP calculates evaluated value

of neighboring AP to share information of its behavior with 2HN-AP. Evaluated metric for neighboring AP use a packet transfer rate because it shows directly a network availability. We verified this proposed scheme using simulations, and we showed clearly that APs can detect a neighboring AP that is not behaving normally by sharing the evaluation value with 2HN-APs.

Next, in Chapter 4, we implemented the evaluated scheme proposed in Chapter 3 for verifying its effectiveness in an actual multihop wireless network. We extracted functions for implementing the proposed scheme as follows. First, the monitor function transmits and receives a probe packet, and the capture function that transmit and receive a report packet, Second, the notification function advertises packet transfer rates for a neighboring AP to 2HN-APs, third, the reputation function calculates the reputation for a neighboring AP from packet transfer rates. Fourth, the path manager (MGR) eliminates a misbehaving AP to co-operate routing protocol. To build the MWN, we create an AP that has multi-interface using a small-size PC. Those functions are embedded an OLSR that is typical routing protocol in a MWN. We build actual MWN using these APs that are implemented the proposed method, and we verified an operation of each AP when a misbehaving AP is occurring intentionally. As a result of this experiment, we confirmed that each AP can detect the misbehaving AP and eliminate the AP from a route of the network in an actual multihop wireless network.

In Chapter 5, we consider a network reconfiguring scheme after detection of a misbehaving node. Communication performance of whole network decrease due to a misbehaving node is eliminated from the network, because available links decrease. Thus, we proposed a network reconfiguring scheme that does not decrease communication performance. In this proposed scheme, we defined the “Neighbor”. The Neighbor is the interface that had connected to misbehaving nodes. This proposed scheme appropriately builds a link using Neighbors. If all Neighbors connect mutually as mesh state, communication performance decreases due to occur interference of wireless channels. Furthermore, in multihop wireless network using multi-rate communication, the performance decreases by the performance

anomaly problem. A process of the proposed scheme provided a high connectivity of a network and considered the performance for character of wireless LAN. We verified this proposed reconfiguration scheme using simulations, the results of simulation indicate that the proposed method can prevent communication performance degradation of the entire MWN.

6.2 Future Works

In this dissertation, we proposed some schemes for achieving of a reliable multihop wireless network. For further developing of research, we describe some future works.

First, An evaluation of the proposed schemes is needed on large-scale actual MWN. We verified the effectiveness of our proposed evaluated schemes of neighboring AP using actual APs in Chapter 4. However, in no distant future, a MWN will be used at commercial avenues and businesses. In such case, communication performance of the MWN decreases dramatically, because various wireless communication, such as cellular phone, transceiver, and GPS, and be used widely. Therefore, we will experiment and verify the proposed schemes in a MWN under a very bad wireless environment.

Second, the scheme for evaluating neighboring AP by more detailed granularity is required. This scheme focus a misbehaving AP that affects an availability of MWN, in other words, does not transfer data packets. However, all misbehaving APs do not discard all packets. A selfish AP drops the packet of a specific destination only. In MWN where such a AP exists, there are a possibility that a normal link is not used by the AP evaluation scheme. Detecting a misbehaving AP including such as selfish AP by researches in the future is necessary.

Bibliography

[AW05] Ian F. Akyildiz and Xudong Wang, "A Survey on Wireless Mesh Network", *Communication Magazine*, Vol. 43, pp. 23–30, Sep. 2005.

[AWW05] Ian F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey", *Computer Networks and ISDN Systems*, Vol. 47, No. 4, pp. 445–487, Mar. 2005.

[BH01] L. Buttyan and J.-P. Hubaux, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks", Technical report, Technical Report DSC/2001/001, Swiss Federal Institute of Technology, 2001.

[CJ03] T. Clausen and P. Jacquet, "RFC 3626: Optimized Link State Routing Protocol (OLSR)", Oct. 2003, `http://www.ietf.org/rfc/rfc3626.txt`.

[dot] "IEEE 802.11 TG s", `http://grouper.ieee.org/groups/802/11/Reports/tgs\_update.htm`.

[Fed] "Fedora Project", `http://fedoraproject.org`.

[Fla] "Adobe Flash", `http://www.adobe.com/products/flash/`.

[GA08] I. Gawedzki and K. A. Agha, "How to avoid packet droppers with proactive routing protocols for ad hoc networks", *International Jounal of Network Management*, Vol. 18, No. 2, pp. 195–208, Mar./Apr. 2008.

[GCC] "the GNU Compiler Collection (GCC)", http://gcc.gnu.org.

[GPM08] S. Glass, M. Portmann, and V. Muthukkumarasamy, "Securing Wireless Mesh Network", *IEEE Internet Computing*, Vol. 12, No. 4, pp. 30–36, Jul./Aug. 2008.

[HRBSD03] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, "Performance anomaly of 802.11b", in *Proc. INFOCOM 2003*, Vol. 2, pp. 839–843, March 2003.

[IEEa] "IEEE 802.11 Ethernet Working Group", http://www.ieee802.org/11/.

[IEEb] "IEEE 802.3 Ethernet Working Group", http://www.ieee802.org/3/.

[JDK] "Java Development Kit", http://www.oracle.com/technetwork/java/index.html.

[JHM07] D. Johnson, Y. Hu, and D. Maltz, "RFC 4728: The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", Feb. 2007, http://www.ietf.org/rfc/rfc4728.txt.

[KKSW04] F. Kargl, A. Klenk, S. Schlott, and M. Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks", in *Proc. of 30th Euromicro Conference*, pp. 152–165. Springer, Aug. 2004.

[KNKJ07] B. Kannhavong, H. Nakayama, Y. Nemoto N. Kato, and A. Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks", *Wireless communications*, Vol. 14, No. 5, pp. 85–91, Oct. 2007.

[KW03] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", *Sensor Network Protocols and Applications*, Vol. 1, No. 2-3, pp. 293–315, Sep. 2003.

[LDM06] S. Laniepce, J. Demerjian, and A. Mokhtari, "Cooperation Monitoring Issues in Ad hoc Networks", in *Proc. of the 2nd International Wireless Communications and Mobile Computing Conference (IWCMC)*, Jul. 2006.

[MGLB00] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating router misbehavior in mobile ad-hoc networks", in *Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom)*, Aug. 2000.

[Mil92] David L. Mills, "RFC 1305: Network Time Protocol (Version 3)", Mar. 1992, `http://www.ietf.org/rfc/rfc1305.txt`.

[MM02] P. Michiardi and R. Molva, "CORE: Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad hoc Networks", in *Proc. of the IFIP TC6/TC11 Sixth Joint Working Conference on Communication and Multimedia Security*, Sep. 2002.

[NNI+08] D. Nobayashi, Y. Nakamura, T. Ikenaga, Y. Hori, K. Nakamura, H. Ishinishi, and S. Kaizaki, "Autonomous Reliable Wireless Mesh Network Using a Neighboring Access Point evaluation Mechanism", in *The Third International Workshop on Self-Organizing System (IWSOS 2008)*, Dec. 2008.

[NNI+09a] D. Nobayashi, Y. Nakamura, T. Ikenaga, Y. Hori, K. Nakamura, H. Ishinishi, and S. Kaizaki, "Access Point Evaluation with Packet Transfer Ratio in Multihop Wireless Network", in *Proc. of the International Conference on Information Networking (ICOIN) 2009*, pp. CD–ROM, Jan. 2009.

[NNI+09b] D. Nobayashi, Y. Nakamura, T. Ikenaga, Y. Hori, K. Nakamura, H. Ishinishi, and S. Kaizaki, "Design and Implementation of Reputation Mechanism for Multihop Wireless Network (in Japanese)", *IEICE Transactions on Communications*, Vol. J92-B, No. 7, pp. 1061–1071, Jul. 2009.

[NNS+07] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, and J. Wang, "Wireless Mesh Networks: Current Challenges and Future Directions of Web-in-the-Sky", *IEEE Wireless Communicaitons*, Vol. 14, pp. 79–89, Aug. 2007.

[NSN+10] D. Nobayashi, T. Sera, Y. Nakamura, T. Ikenaga, and Y. Hori, "A Network Reconfiguring Scheme against misbehaving Nodes", in *Proc. of the 35 th IEEE Conference on Local Computer Networks (LCN) 2010*, pp. 432–439, Oct. 2010.

[OLS] "Optimized link state routing protocol (olsr)", `http://www.olsr.org`.

[OR08] F. Oliviero and S. P. Romano, "A Reputation-based Metric for Secure Routning in Wireless Mesh Networks", in *Proc. IEEE GLOBECOM 2008*, pp. 1–5, Nov. 2008.

[OTMI06] Yasunori Owada, Hiroyasu Terui, Kenichi Mase, and Hiroei Imai, "An Proposal of Multihop-Wireless LAN and Its Implementation (in japanese)", *IEICE Transactions on Communications*, Vol. J89-B, No. 11, pp. 2092–2102, Nov. 2006.

[PBRD03] C. Perkins, E. Belding-Royer, and S. Das, "RFC 3561: Ad hoc On-Demand Distance Vector (AODV) Routing", Jul. 2003, `http://www.ietf.org/rfc/rfc3561.txt`.

[PSN+03] V. S. Pavan, V. S., P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in Wireless Ad Hoc Networks", in *In Proceedings of IEEE Infocom*, pp. 808–817, 2003.

[Qua] "Qualnet 4.5", `http://www.scalable-networks.com`.

[SAM06] Shiro Sakata, Hidenori Aoki, and Kenichi Mase, "Mobile Ad Hoc Networks and Wireless LAN Mesh Networks", *IEICE Transactions on Communications*, Vol. J89-B, No. 6, pp. 811–823, Jun. 2006.

[SB02] J-Y. Le Boudec S. Buchegger, "Performance Analysis of the CONFIDANT protocol", in *Proc. of ACM International Symposium on Mobile Ad hoc Networking and Computing*, Jun 2002.

[SNYA06] L. Santhanam, N. Nandiraju, Y. Yoo, and D. P. Agrawal, "Distributed Self-policing Architecture for Fostering Node Cooperation in Wireless Mesh Networks", *Personal Wireless Communications*, pp. 147–158, Sep. 2006.

[SXA08] L. Santhanam, Bin Xie, and D. Agrawal, "Selfishness in Mesh Networks: Wired Multihop MANETs", *IEEE Wireless Communications*, pp. 16–23, Aug. 2008.

[Tom] "Apache Tomcat", `http://tomcat.apache.org/`.

[WOR] "Internet World Stats", `http://www.internetworldstats.com/stats.htm`.