IEEJ Transactions on xx
Vol.139 No.1 pp.1–9 DOI: 10.1541/ieejxxs.139.1

Paper

Interface Mode Assignment Method for Self-Reconstruction of Wireless Mesh Networks based on IEEE 802.11 Infrastructure-mode

Erdenetuya Dorj* Non-member, Kazuhiko Kinoshita** Non-member

The key features of computer networks available for disaster situation is reliable, fault tolerance and self-configurable. Therefore, using wireless mesh network for disaster prevention and recover system has gain much attention from the research community in last decades. In addition, from the practical aspects of the network infrastructures of the disaster system, we should assume the core capabilities such as wireless connectivity in wide range, ease of use, and low cost so on. In this paper, we propose an interface mode assignment method for reconstructing a route from an isolated router to a gateway (GW) router in a wireless mesh network based on IEEE 802.11 infrastructure mode after a disaster occurrance. The proposed method assigns an adequate mode to each interface in an isolated router to recover the network reachability in distributed manner. Simulation results show the effectiveness of the proposed method via two different scenarios.

Keywords: wireless mesh network, infrastructure mode, reconstruction, disaster

1. Introduction

The world has endured a number of natural disasters over the centuries, causing physical damage, electricity outage, traffic congestion, and telecommunication disruption. In order to cope effectively with post-disaster emergency situations, verify the safety of people, facilitate information sharing in the vicinity, and provide communication services, network recovery mechanisms must be improved. From the aspect of disaster recovery, resilient wireless networks are considered as fundamental and crucial. As a basis of such a system, a wireless mesh network (WMN) has dynamic self-forming, self-healing, and self-organization capabilities. In a WMN, each access point (AP) works as a router to maintain network connectivity autonomously via wireless multi-hop communications without physical cables and the limited number of APs work as a gateway (GW) to the backbone network such as the Internet. Therefore, WMNs can provide a cost-effective way of deploying a network infrastructure with higher reliability in disaster situation [(1)~(5)].

However, most of the existing WMNs are based on IEEE 802.11 ad-hoc mode and considered to be unpractical due to poor security [(6)(7)]. Further, mobile device vendors and operating system developers, especially Wi-Fi alliances, give much attention to the development of IEEE 802.11 infrastructure mode, considering the ease of practical use and cost reduction. Consequently, in this paper we focus on WMNs based on IEEE 802.11 infrastruture mode.

Different from the ad-hoc mode, in the infrastructure mode, each interface must decide its working mode; AP or STA. An interface in AP mode can connect to any number of interfaces in STA mode. To the contrary, an interface in STA mode can connect to only one interface in AP mode. This causes another challenge in WMNs [(8)]. When an enormous disaster strikes, some mesh routers go down so that some other routers can be isolated from the backbone network in the wireless mesh network. It is critical and that the WMN should be recovered after the disaster as soon as possible. We proposed an effective route reconstruction method for Wi-Fi mesh network in disaster situation with spare AP, thereby we figured out the appropriate location points of the candidate spare APs using received signal strength identification (RSSI) information of the wireless mesh routers gathered by smartphones of the firefighters [(9)].

In the IEEE 802.11 infrastructure mode, however, the working mode of each interface must be redetermined after spare AP placement, before rerouting. Therefore, this paper proposes an interface mode assignment method that decides which mode is suitable for an interface of a mesh router to establish an association with its neighbor router in order to enable all the isolated routers reachable to the backbone network via the GW router. The GW router is responsible for connecting the mesh routers to the wired network [(8)].

Moreover, note that this process must be executed in a distributed manner. To the best of our knowledge, no existing works tackle to this problem.

The rest of this paper is organized as follows. In section 2, we introduce some related works. Network model and problem formulation are introduced in section 3. In section 4, we discuss the proposed method. Section 5 shows the feasibility of the proposed method via simulation experiments. Finally, section 6 states conclusions and future works.

2. Related Work

2.1 General WMNs WMNs have become a key practical communication solution to provide higher resilient network infrastructure for use in the unlicensed spectrum and at low cost based on the IEEE 802.11 ad-hoc mode by consid-

* Graduate School of Advanced Technology and Science, Tokushima University, Japan. +81-88-656-7495
** Graduate School of Technology, Industrial and Social Science, Tokushima University, Japan. +81-88-656-7495

ering multiple characteristics such as network design, scalability, quality of service, and fault tolerance. In particular, these features make the use of WMNs advantageous in terms of low upfront cost, easy network maintenance, robustness, and reliable service coverage [10].

[11] shows the comparision results of the common routing algorithms such as AODV, zone routing protocol (ZRP), and DSR in ad-hoc based WMNs under disaster situation. AODV protocol shows good implementation result compared to others in all four cases. In [12], routing protocols play an important role to increase WMNs efficiency and reliable. The authors considered distributed routing protocols have many advantages than centralized routing protocols.

2.2 WMNs based on ad-hoc mode with disaster consideration WMNs are actively studied as disaster-resilient networks [1]~[4] in the last decades. [1][2] highlight the WMN in ad-hoc form with self-organizing, self-forming, and self-healing characteristics. Wireless virtualization mechanisms, namely wireless multihop access network virtualization are applied to a tree-based mobile ad hoc network (MANET) architecture for disaster recovery. At first, a node connects to a internet gateway as a common STA. After that, it transforms into virtual AP working as a bridge between isolated nodes and the internet gateway [3][4].

In [13], the authors aim at software defined network (SDN) based dynamic packet forwarding approach for not only handling routing/packet forwarding rules through some surviving APs but also optimizing load-balancing routing between them. An SDN-based resilient architecture against disaster failures has been designed in which an algorithm proposes for geographic-based backup topologies generation and splicing considering the load distriburtion between nodes [14] .

[5] considers a reliable routing technique for disaster recovery. In [15], the authors design and implemented an experimental test-bed of WMN with a highly de-centralized architecture and small unmanned aerial systems. [6] shows the comparision results of the common routing algorithms such as AODV, zone routing protocol (ZRP), and DSR in ad-hoc based WMNs under disaster situation. AODV protocol shows good implementation result compared to others in all four cases. In the experiment of [7], at first, the authors introduce a kind of mesh network called "NerveNet" and show how it was used for disaster recovery after the Kumamoto earthquakes. Although the above research works are essential, there are still some limitations of the use of WMNs with the IEEE 802.11 infrastructure mode.

2.3 WMNs based on infrastructure mode without disaster consideration Here, we focus on [16]~[22], which presented experimental results on WMNs with IEEE 802.11 infrastructure mode. In [16], a drone-based wireless mesh network has been designed and implemented to provide high speed Wi-Fi. A prototype of meshcluster network architecture is implemented using multiple radios such as 802.11 and 802.16 commuications and highlighted routing/monitoring of it [18]. [19] addresses client-side transparency characteristics in an mesh networking architecture named iMesh, in which APs not only build multi-hop interconnections between each other with wireless distribution system (WDS) links, but also provide seamless network connection to clients. [17] also designs 802.11 infrastructure based network architecture and combines a WDS to provide a connection between APs for peer-to-peer metropolitan medical response system (MMRS). [20] shows that the transmission range of single AP can be improved using a WDS technolgy. [21] dedicates a mobile ad-hoc Wi-Fi (MA-Fi) architecture comprising a two-tier hierarchy of router nodes (RONs) and STAs. RONs are responsible for assigning the AP mode and the STA mode to two virtual interfaces on the single physical radio interface. In the performance evaluation, MA-Fi outperforms ad-hoc mode communication and offers throughput comparable to Wi-Fi even over multiple hops. Nodesjoints [22] is formulated for tree-based MANET in IEEE 802.11 infrastruture mode. In [23], a station can connect to a software-based AP via Wi-Fi direct.

[24] considers communications in both infrastructure mode and ad-hoc mode. [25] assums both Wi-Fi ad-hoc and Wi-Fi-Opp in static and mobile forms and compared their simulation results. [26] aimed to increase transmission speed for sharing information between nodes in an opportunistic infrastructure-based Wi-Fi networks. They showed the advantages of the proposed approach as comparing the Wi-Fi-Opp method. However, [24]~[26] are not available with disaster recovery system.

2.4 WMNs based on infrastructure mode with disaster consideration In [27], therefore, Tree-based disaster recovery access network is designed and implemented, in which nodes have been equipped a virtual interface in AP mode based on the software-based access node (SAN). In addition, in [28], MANET routers are designed and implemented for an emergency fire response system working in a disaster system.

[9] proposes a route reconstruction method with spare APs. It is based on a reasonable assumption according to interviews with firefighters and civil servants.

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

3. Network Model

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

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

between the interfaces in the same mode.

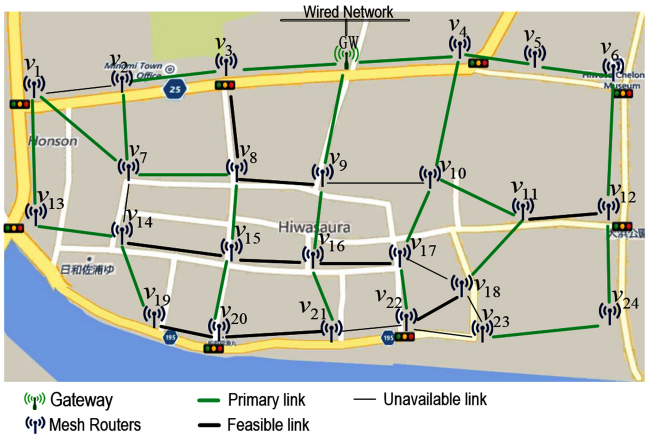


Fig. 1. Assumed Network Model

As shown in Fig. 1, mesh routers are placed along a road. In a normal situation, all the mesh routers are reachable to the wired network via the GW. Each mesh router v_i has two interfaces and each interface equips two directional antennas. In Fig. 2, blue or red dough-nut shape indicates each interface and the direction of its directional antennas [9].

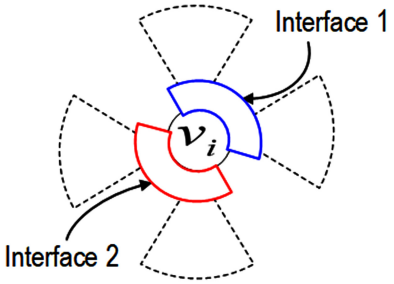


Fig. 2. Interface Structure of Mesh Router

Fig. 3 illustrates a failure situation where some routers are supposed to be failed and the mesh network is isolated, when a large-scale disaster occurs.

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

To overcome this situation, we proposed an algorithm to find the adequate location of spare AP. Note that it is equipped with an omnidirectional antenna for easy installation by non-experts such as firefighters and public workers. In Fig. 4, we assume that a spare AP denoted by v_s has been installed. The spare AP v_s lies in the transmission ranges of either the connected or the isolated routers and it must connect to at least one router in C and at least one router in U in order to play a role of bridge. All the routers in the set of $V \setminus F \cup U \cup B$ $(= C \cup U \cup B)$ can be potentially reachable to the backbone network where B denotes the set of spare APs. For instance, in Fig. 4, all isolated routers can potentially be reachable to the GW via v_s in B establishing associations with

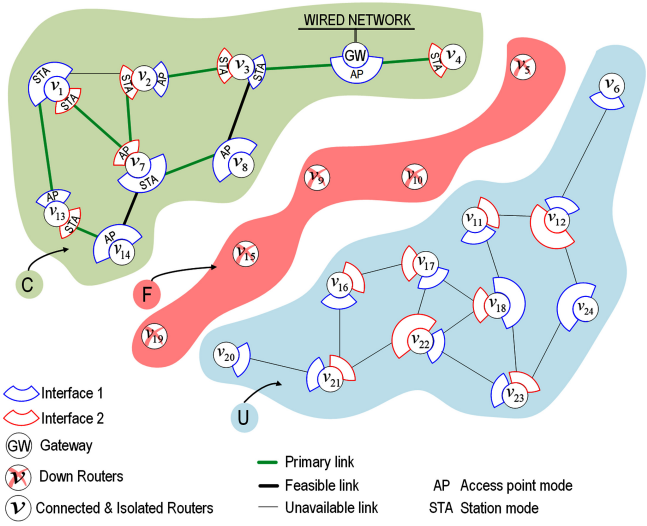


Fig. 3. Failure Situation

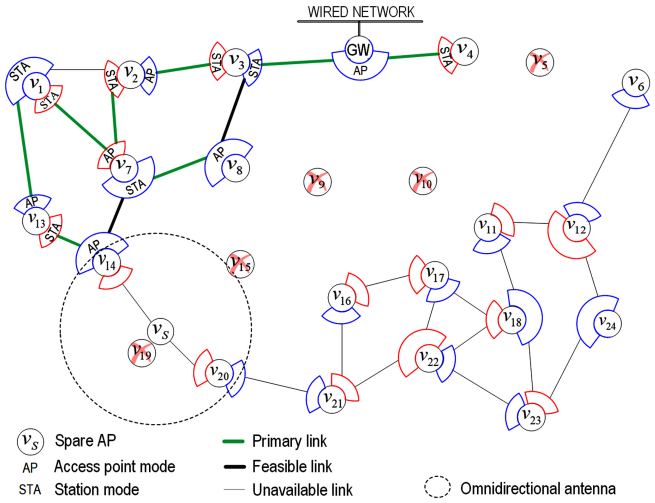


Fig. 4. Installation of Spare AP

router v_{14} in C and router v_{20} in U [9].

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

3.2 Problem Description In this paper, we consider the following requirements/constraints for the interface mode assignment to reconstruct the mesh network.

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

(2) A router constantly sends beacon messages in IEEE 802.11 infrastructure mode based mesh networks [29]. We suppose that it can put some information on the message to advertise their own existence and also discover the existence of one-hop neighboring routers within the transmission range.

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

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

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

4. Proposed Method

4.1 Overview In this section, we propose an interface mode assignment method including two phases: tentative routing phase and interface mode selection phase.

Fig. 5 shows the flowchart of the proposed method. In a whole reconstruction process, each isolated router including spare AP should discover a tentative route to the GW in a distributed manner. Note that a tentative route is a chain of *unavailable* links.

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

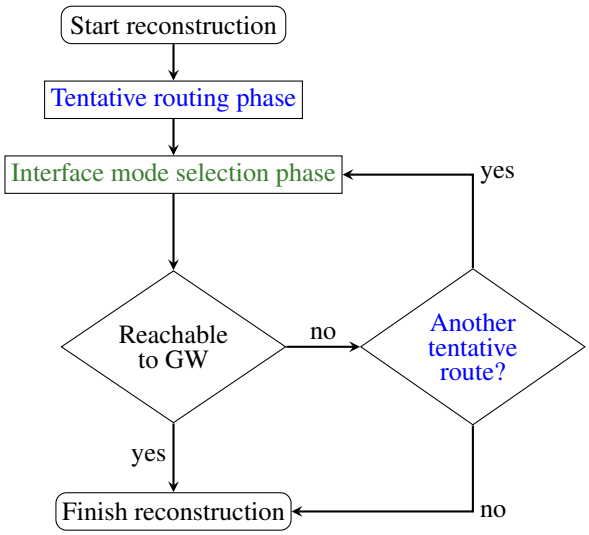


Fig. 5. Flowchart of Recontruction

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

4.2 Tentative Routing Phase In the tentative routing phase, an isolated router tries to discover a next hop router in the connected area using beacon messages. At first, an isolated router finds one or more tentative routes to the GW. In the proposed method, Routing Information Protocol version 2 (RIPv2) can be applied for this route construction. RIPv2 is a distance vector routing protocol where the number of hops is used as its metric [30].

Fig. 6(a) shows that an isolated router v_i has found a router v_j connected to the GW based on exchanging their beacon messages. Therefore, v_i and v_j identify their common link $e(c_{i,a}, c_{j,b})$ as an *unavailable* link. In the same manner, v_i also has *unavailable* links to v_k and v_l.

Along the *unavailable* link, v_j can recommend a tentative route to the GW for v_i. Thus, v_i adds v_j as its next hop and it starts its interface mode selection phase. Note that the mode of their interfaces is STA as default. But the link is still unavailable until the interface mode selection phase is successfully completes. Fig. 6(b) shows that v_i send *Join* message to negotiate its mode with v_j, and v_j replies *Accept* message and becomes a parent of v_i. By this procedure, link $e(c_{i,a}, c_{j,b})$ becomes a *primary* link and v_i belongs to the connected area. After that, v_i sends out the routing message to its neighbors v_k and v_l and adds them as its childs. On receiving the message, v_k and v_l start their interface mode selection phase, since v_i is currently a connected router. Reconstruction of a route of an isolated router to the GW represents that the proposed method has been completed successfully.

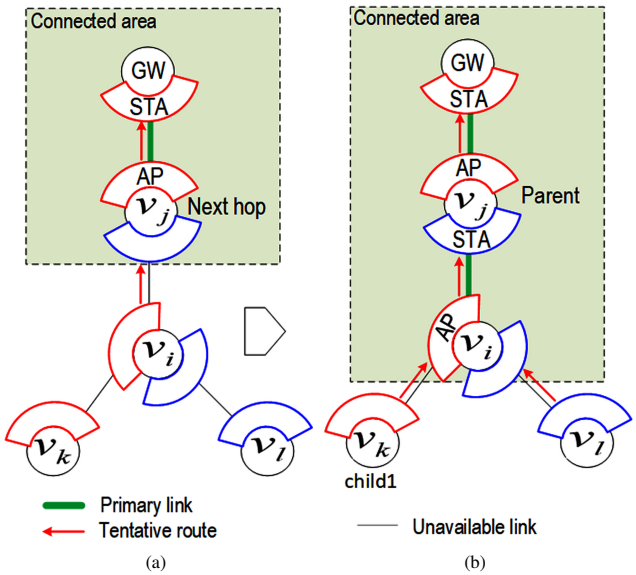


Fig. 6. Parent and Child of Mesh Router

4.3 Interface Mode Selection Phase When an isolated router discovers its next hop router in the connected area, it starts the interface mode selection phase with the following parameters such as *Mode*, N, and *Status* for link $e(c_{i,a}, c_{j,b})$.

- *Mode*: A variable to indicate the working mode, where $Mode(c_{i,a})$ means the mode of interface a of router v_i.
- N: The degree of an interface of a router, where $N(c_{j,b})$ means the total number of *primary* links and *unavailable* links used for its childs.
- *Status*: The link status. $Status(e(c_{j,b}, c_{i,a}))$ is *undecided* as a default. When the interface mode of $c_{i,a}$ and $c_{j,b}$ have been decided, it becomes *decided*. In a case that a connected router has a primary link at its interface in STA mode, the status of other links at the same interface is defined as closed. It means that the link is not available for new association.

At first, the isolated router sends *Join* message to its next hop. If the next hop router replies *Accept* message, the isolated router becomes a connected router and adds its next hop as its parent in its routing table. In a case that a connected router has a primary link at its interface in STA mode, the

status of other links at the same interface is defined as closed. It means that the link is not available for new association. Fig. 7 shows the flowchart of the interface mode selection.

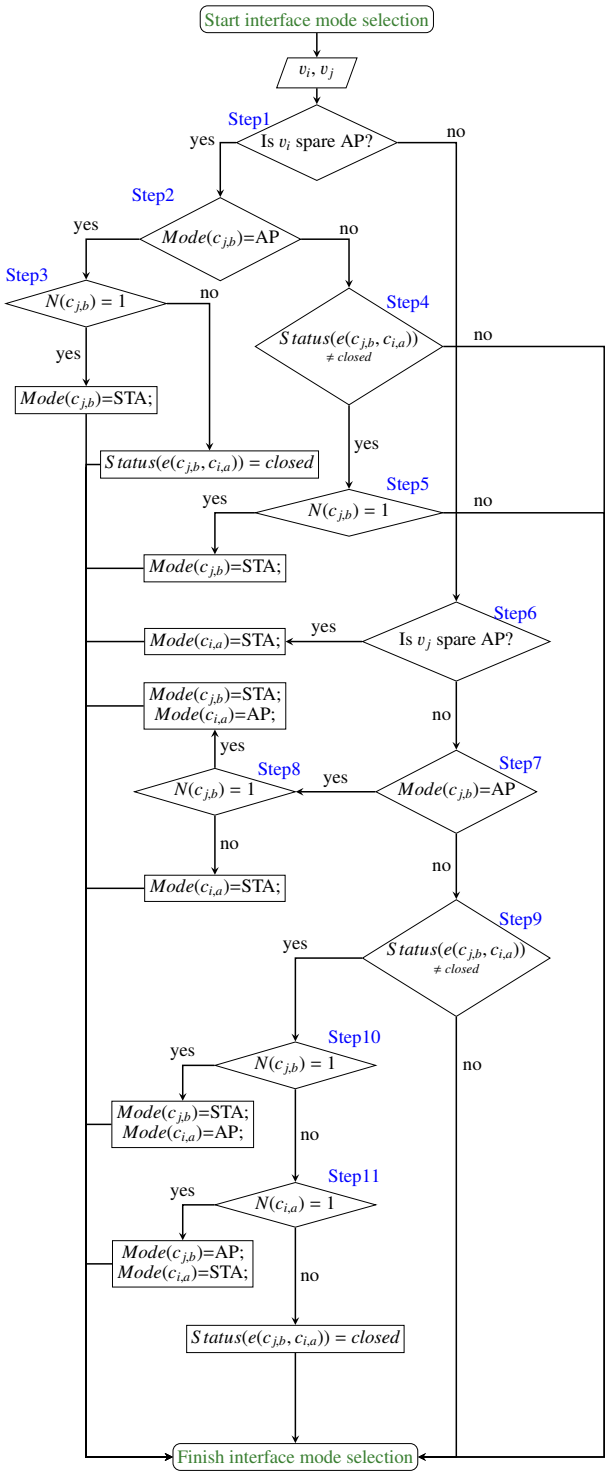


Fig. 7. Flowchart of Interface Mode Selection Phase

The steps of the phase in Fig. 7 contain the conditions of which modes at the link of $e(c_{i,a}, c_{j,b})$ get selected. Here, there are two routers; isolated node v_i that has found its own tentative route and its next hop router v_j. Step1 checks whether v_i is a spare AP or not. If *yes*, $Mode(c_{j,b})$ must be STA to make an association since a spare AP has only one interface and its mode must be AP. Before the assignment, if $Mode(c_{j,b})$ is AP in Step2, Step3 checks the degree of the interface $N(c_{j,b})$ equals 1 or not. If *yes*, STA mode is assigned to $c_{j,b}$ since this link is available for the association. Otherwise, $Status(e(c_{j,b}, c_{i,a}))$ becomes *closed* so that it is unable to make an association between v_i and v_j. Step4 checks whether $Status(e(c_{j,b}, c_{i,a}))$ is *closed* or not. If *yes*, Step5 checks the degree of the interface $N(c_{j,b})$ equals 1 or not. If *yes*, $Mode(c_{j,b})$ becomes STA since this link is available for the association. Otherwise, this link is unavailable for a new connection. In the same manner, Step6 considers the case that v_j is a spare AP. If *yes*, $Mode(c_{i,a})$ becomes STA. Otherwise, Step7 checks $Mode(c_{i,a})$ is AP or not. Before the assignment, Step8 checks whether the degree of the interface $N(c_{j,b})$ equals 1 or not in the same manner of Step3. If *yes*, AP mode is assigned to $c_{i,a}$ and $Mode(c_{j,b})$ is changed from AP to STA. Otherwise, STA mode is assigned to $c_{i,a}$ since this link is available for the association. The reason is as follows. $N(c_{j,b}) = 1$ means that v_j has only one child v_i at its interface $c_{j,b}$. In this case, if STA mode is assigned to interface $c_{i,a}$, v_i cannot be next hop router for any other isolated routers which probably have multiple choices of their tentative routes to GW. Consequently, AP mode should be assigned so that v_i is available to have one or more childs at its interface $c_{i,a}$. Step9 checks whether $Status(e(c_{j,b}, c_{i,a}))$ is *closed* or not. If *yes*, it means that a mode has not selected yet. Therefore, $Mode(c_{j,b})$ and $Mode(c_{i,a})$ become STA and AP, respectively, when Step10 is *yes*, in which it is checked whether the degree of the interface $N(c_{j,b})$ equals 1 or not. Before next assignment, Step11 checks whether the degree of the interface $N(c_{i,a})$ equals 1 or not. If *yes*, AP and STA are assigned to $c_{j,b}$ and $c_{i,a}$, since v_i has no child. Otherwise, the link status $Status(e(c_{j,b}, c_{i,a}))$ becomes *closed*.

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

Fig. 8(a) demonstrates how the mode selection phase works under the assumption that routers v_1 to v_4 are connected routers having routes to the GW whereas v_s and v_5 to v_7 are isolated routers.

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

Although v_3 is selected the next hop router of v_s, it is the next hop router of v_4 via its interface in AP mode. Therefore, the condition of Step3 in Fig. 7 is satisfied in its mode selection phase of the link $e(c_{s,1}, c_{3,1})$. In this case, as shown in Fig. 8(b), v_3 should execute *leaving* process to dissolve with v_4 in order to make itself the next hop router of v_s. In the leaving process, v_3 sends *Leave* message to v_4 to dissolve the association. Suppose that v_4 has another route to the GW, it replies *Accept* message. As a result, v_3 could successfully handle the leaving process to dissolve with v_4 in Fig. 8(b). After that, the degree of interface $N(c_{3,1})$ becomes 1 and then

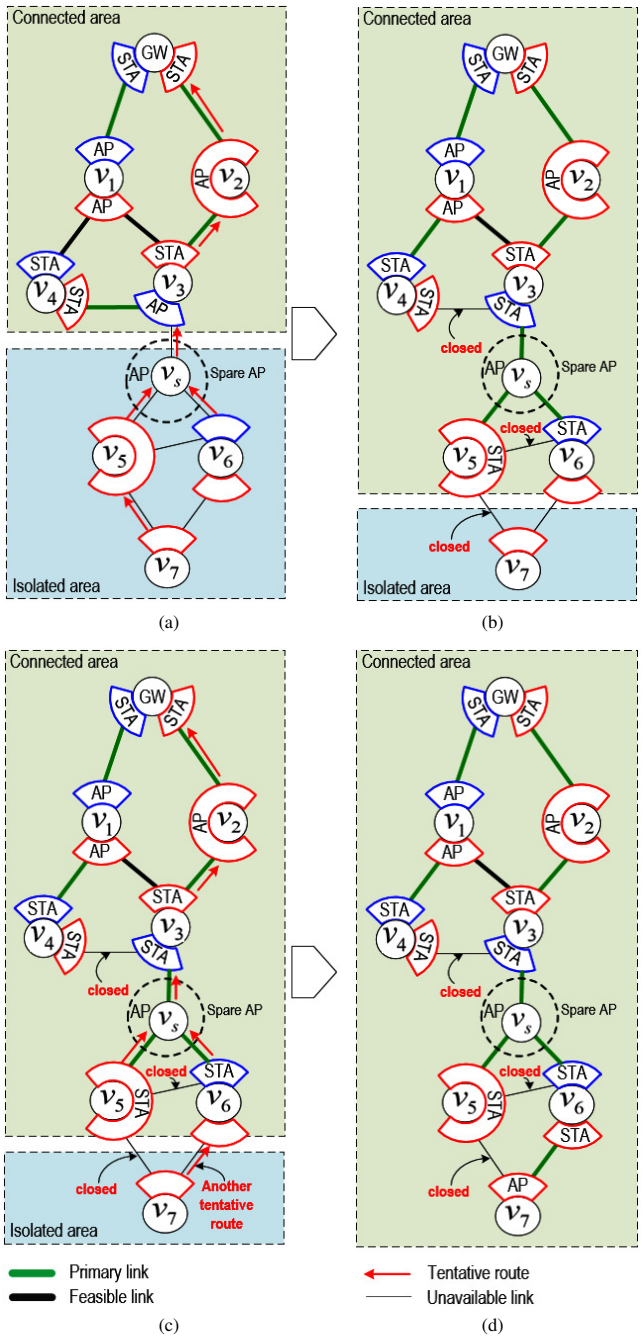


Fig. 8. Reconstruction Process of Case 1

v_3 can send *Accept* message to v_s to make a new association. $Status(e(c_{3,1}, c_{4,2}))$ is configured as *closed* and v_3 declares it to its neighbor routers via its interface, as shown in Fig. 8(b). It means other links beside of $e(c_{3,1}, c_{4,2})$ are not possible to use for any tentative routes. If v_3 receives *Reject* message from v_4, it is impossible to to get selected as the next hop of v_s. In this case, v_3 sends back *Reject* message to v_s. As a result, v_s should discover another router to the GW.

After v_s becomes a connected router, as shown in Fig. 8(b), routers v_5 and v_6 can take STA mode at their interface connected with v_s according to Step6 in the Fig. 7. As a result, routers v_5 and v_6 become connected routers. After that, v_7 is available to start its mode selection phase since v_5 is selected as the next hop router of v_7. But, the link statuses $Status(e(c_{3,1}, c_{4,2}))$, $Status(e(c_{5,2}, c_{6,1}))$, and $Status(e(c_{5,2}, c_{7,2}))$ are configured as *closed* so that router v_7 has to find another tentative route in Fig. 8(c). If it has no tentative route of v_7, it keeps itself as an isolated router and declares. Finally, router v_7 has a new tentative route via router v_6 in Fig. 8(c) and its mode selection phase is satisfied with the condition in Step10, as shown in Fig. 8(d).

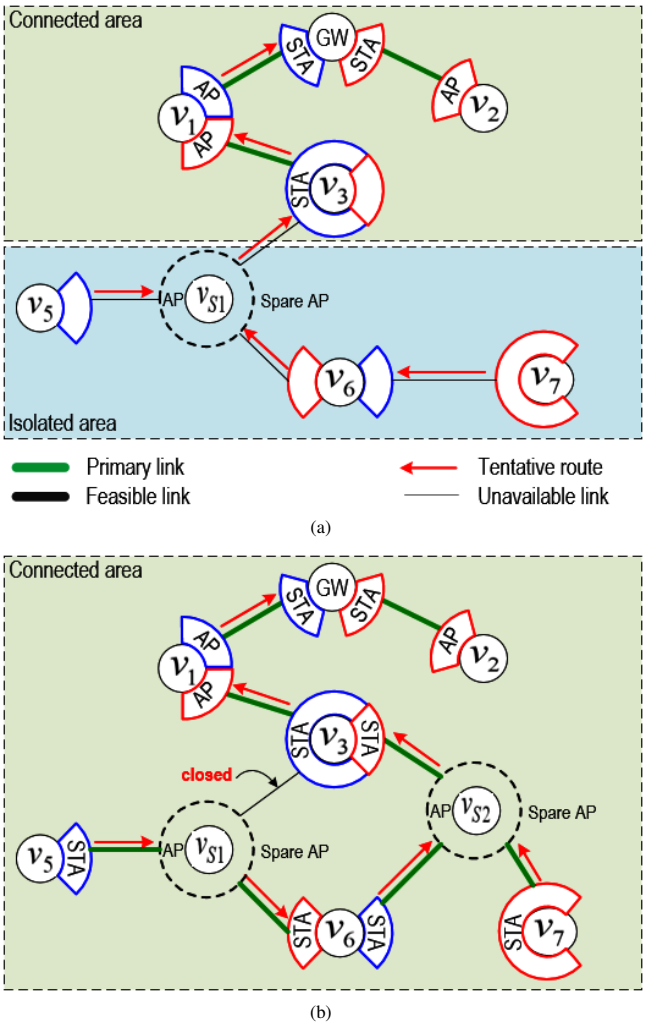


Fig. 9. Reconstruction Process of Case 2

Fig. 9(a) assumes a case with two spare APs, in which routers v_1 to v_3 are connected routers having routes to the GW whereas v_{S1} and v_5 to v_7 are isolated routers.

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

Since v_{S1} has constructed a tentative route to the GW via v_3, it sends *Join* message to v_3 with the start of its mode selection phase. Note that an interface of router v_3 having a link to the interface of v_{S1} should be in STA mode to make an association. Although v_3 is selected the next hop router of v_{S1}, it has only one route to GW via its next hop router of v_1 via its interface in STA mode. Therefore, the condition of Step5

in Fig. 7 is *no* so that the link $e(c_{S1,1}, c_{3,1})$ is unavailable for the association. v_3 sends *Reject* message to v_{S1}. After that v_{S2} has constructed a tentative route to the GW via v_3 and other routers discover their new tentative routes to the GW in the same manner. v_{S2} sends *Join* message to v_3 with the start of its mode selection phase. Since Step5 in Fig. 7 is ŷes, v_3 can send *Accept* message to v_{S2} to make a new association and then v_{S2} becomes a connected router, as shown in Fig. 9(b).

After that, routers v_6 and v_7 can take STA mode at their interface connected with v_{S2} according to Step6 in the Fig. 7. As a result, routers v_5 and v_6 become connected routers. After that, v_{S1} is available to start its mode selection phase since v_6 is selected as the next hop router of v_{S1} because the link status $Status(e(c_{S1,1}, c_{3,1}))$ is configured as *closed*. Note that v_5 is range out of v_6 so that it needs v_{S1} to find another tentative route to the GW. Finally, router v_5 has a new tentative route via router v_{S1} and its mode selection phase is satisfied with the condition in Step6, as shown in Fig. 9(b).

5. Performance Evaluation

In this section, we evaluate the performance of the proposed method via simulation experiments with two scenarios. The assumed network in Fig. 1 was built as a simulation model. In the both scenarios, we assume one router is configured as a GW whereas others are isolated routers. The proposed method was executed total 24 routers beside one GW.

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

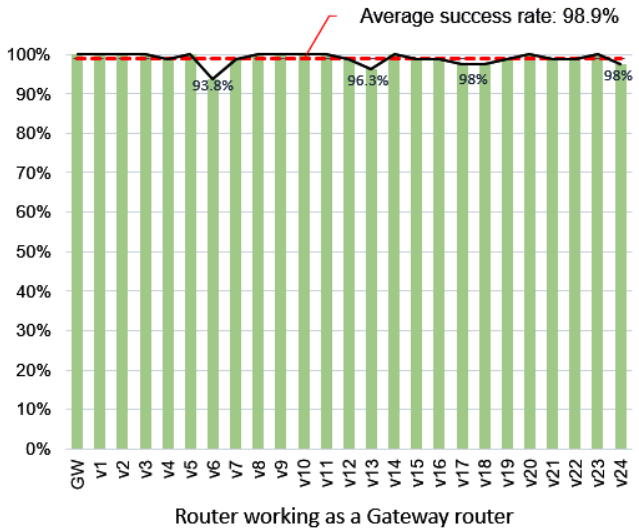


Fig. 10. Successful Recovery Probability without Spare APs

bust also routers v_1 to v_{24} providing the function of a GW. The proposed method was executed 100 different cases for each GW router, where each router was equipped with one or two interfaces randomly. Fig. 10 shows that 98.9% of 2500 cases in total are recovered successfully. "Recover" means that all isolated routers became reachable to the GW after the reconstruction process. When router v_6 or v_{13} was selected as a GW router, the lowest success rate of 93.8% or 96.3% was observed, respectively. The reason why is that both of routers v_6 and v_13 have not only two active interfaces but also use the same interfaces for their neighbor connections. Therefore, it causes the lack of tentative route because usually the link statuses are configured as *closed*. To overcome this situation, GW router should have three or more interfaces.

In the second scenario, n random routers were assumed to get down. Also, another n routers' antenna orientations

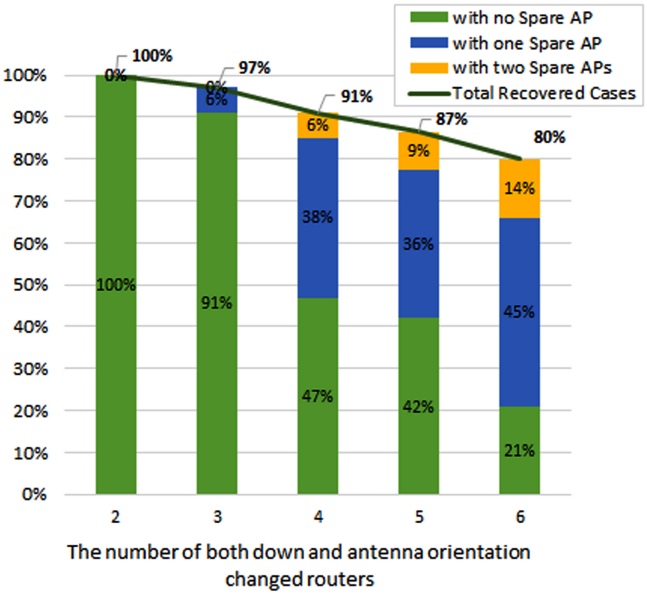


Fig. 11. Successful Recovery Probability with Spare APs

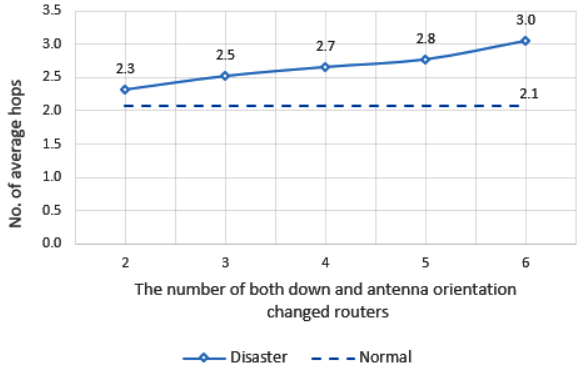


Fig. 12. The number of hops

changed randomly. We changed n from 2 to 6, and tested 300 different failure cases for each n. Therefore, when some isolated routers are range out, one or more spare APs should be used to provide a route to the GW for them. This scenario assumes that a significant disaster has occurred. Fig. 11 shows the successful recovery probability as a function of n. Even if six routers which is one-fourth of total routers went down

changed, in about 80% of the cases, the proposed method is practical. Fig. 12 shows the average number of hops for all 24 routers. The difference between in the normal scenario and in the disaster scenario is less than 1. It means that the proposed method has no significant impact on communication quality.

Finally, we discuss how long it takes to reconstruct the mesh network. Once a spare AP has been set, it takes at most 1 minute to find and negotiate with a neighbor router. The reconstruction process can be completed in less than 1 hour. According to [31], in the 2011 great earthquake in Japan, it took 4 days until 50% of cellular system got recovered. Compared with it, 1 hour is small enough.

6. Conclusion

In this paper, we proposed an interface mode assignment method for the mesh networks. After a disaster has occurred, the proposed method recovers the reachability with two phases such as tentative routing and interface mode selection.

Simulation results showed that the proposed method achieved the satisfaction degree of successful recovery for two different scenarios.

In this paper, we assume that each router has 2 interfaces and each interface has 2 directional antennas. Therefore, as a future work, we will prove the effectiveness of the proposed interface mode assignment for the cases where each router has any number of interfaces and each interface has a any number of antennas. On the other hand, in a larger scale of mesh network, multiple gateways may be used. It is also a future work to enhance the proposed method for such an environment.

References

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

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

(3) T. M. Quang, K. Nguyen, E. Kamioka, and S. Yamada (2013) "Tree-based disaster recovery multihop access network," 19th Asia-Pacific Conference on Communications (APCC13), pp. 415-420.

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

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

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

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

(8) K. Sohraby, D. Minoli, and T.Znati (2007) "Wireless Sensor Networks: Technology, Protocols, and Applications," John Wiley & Sons, Inc., Hoboken, New Jersey.

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

(10) D. Benyamina, A. Hafid, and M. Gendreau, "Wireless Mesh Networks Desgin - A Survey," IEEE Communications Survey & Tutorials, Vol. 14, No.2, Second Quarter, 2012.

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

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

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

(14) A. Xie, X. wang, G. Maier, and S. Lu (2014) "Designing a Disaster-resilient Network with Software Defined Networking," IEEE 22nd International Symposium of Quality of Service (IWQoS).

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

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

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

(18) K. N. Ramachandran, M. M. Buddhikot, G. Chandranmenon, S. Miller, E. M. Belding-Royer, and K. C. Almeroth (2005) "On the Design an Implementation of Infrastructure Mesh Networks," Proceedings of the IEEE Workshop on Wireless Mesh Networks (WiMesh).

(19) V. Navda, A. Kashyap, and S. R. Das (2005) "Design and Evaluation of iMesh: An Infrastructure-mode Wireless Mesh Network," Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks.

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

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

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

(23) D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano (2013) "Device to device communications with wi-fi direct: overview and experimentation," IEEE Wireless Communications, Vol. 20, Iss. 3, pp. 96-104.

(24) J. Chen, S. H. Gary Chan, J. He and S. Liew (2003) "Mixed-Mode WLAN: The Integration of Ad Hoc Mode with Wireless LAN Infrastructure," IEEE GLOBECOM, pp231—235.

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

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

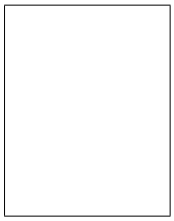
(27) Q. T. Minh, Y. Shibata, C. Borcea, and S. Yamada (2016) "On-site Configuration of Disaster Recovery Access Networks Made Easy," Ad Hoc Networks, Vol. 40, pp. 46–60.

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

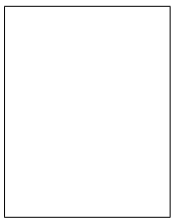
(29) M. S. Gast (2005) "802.11 Wireless Networks: The Definitive Guide," 2th Edition.

(30) J. Kurose and K. W. Ross (2017) "Computer Networking: A Top-Down Approach," 7th Edition.

(31) K. Kinoshita, Y. Ito, H. Kimura and Y. Maeda (2012) "Technologies and Emergency Management for Disaster Recovery - With Focus on the Great East Japan Earthquake," IEICE Transactions on Communications, Vol.95, No.6, pp. 1911–1914.



Erdenetuya Dorj (Non-member) received her B.Sc. and M.Sc. degrees in Information Network from Mongolian University of Science and Technology, Mongolia, in 2007, and 2008, respectively. She is currently pursuing a Ph.D. degree in Information Science and Intelligent Systems at Tokushima University, Japan. Her academic interests include wireless multi-hop mesh network, QoS in Internet of Things.



Kazuhiko Kinoshita (Non-member) received the B. E., M. E. and Ph. D degrees in information systems engineering from Osaka University, Osaka, Japan, in 1996, 1997 and 2003, respectively. From April 1998 to March 2002, he was an Assistant Professor at the Department of Information Systems Engineering, Graduate School of Engineering, Osaka University. From April 2002 to March 2008, he was an Assistant Professor at the Department of Information Networking, Graduate School of Information Science and Technology, Osaka University. From April 2008 to January 2015, he was an Associate Professor at the same University. Since February 2015, he has been a Professor at Tokushima University. His research interests include mobile networks, network management, and agent communications. Dr. Kinoshita is a member of IEEE and a senior member of IEICE.