社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

GICS: Group-based Internet Connection Spreading Architecture for Disaster Recovery

Xuan Thien PHAN, Quang TRAN MINH, Kien NGUYEN, Shigeki YAMADA

National Institute of Informatics 2-1-2 Hitostubashi, Chiyoda-ku, Tokyo 101-8430 Japan
E-mail: xuanthiencs@gmail.com, {quangtran, kienng, shigeki}@nii.ac.jp

Abstract Disconnection of Internet access in case of natural disasters may cause serious obstacles for relief works. Immediately providing Internet connection in disaster regions is still a challenge because infrastructure-based networks may have been disabled by the disaster. This paper proposes a Group-based Internet Connection Spreading (GICS) architecture for disaster recovery. This architecture supports groups of unconnected mobile devices to connect to the Internet through still alive infrastructure access points or groups of Internet-connected mobile devices in an effective way. By the support of the Internet-connected Device Discovery mechanism in proposed GICS, mobile devices can discover nearby devices that have already reached the Internet connection. GICS enables mobile devices within groups collaborate together to bring reasonable Internet connection to all group members. Moreover, GICS can flexibly adapt with changes in network condition since GICS groups can necessarily rearrange the roles of group members to maintain the suitable the Internet connection. In addition, the quality of connection between devices in GICS is reliable based on IEEE 802.11 (Wi-Fi) standard.

Keyword Internet connectivity, Mobile communications, Wireless networks, Wi-Fi Direct, Disaster recovery

1. Introduction

In natural disasters (earthquakes, hurricanes, tsunamis,...), computer networks and mobile communication networks are the very important channels that maintain the communication for relief and recovery works. However, these communication networks seem not to be as resilient and survivable as needed for such emergency situations [1]. In disasters, their physical infrastructures such as cable, antenna and power supply systems may be destroyed causing the disability of their services. Quickly providing the Internet access in disaster-effected areas is still a challenge because there is currently no mature technology that supports maintaining the Internet connection in case infrastructure – based networks are disabled.

Spreading the Internet connection from still alive access points (APs) or gateways nearby to mobile devices is almost the only possible solution to provide Internet access in disasters. The problem is that the current methods and proposals are not reliable and efficient enough to be deployed for real life disasters.

Wireless access networks such as wireless mesh network (WMN) [2] and mobile ad hoc network (MANET) [3] are self-configuring and self-healing networks in which mobile devices are wirelessly connected. These networks support multi-hop communications in which two nodes can communicate with each other through intermediate nodes in case they cannot make direct communication with each other. However, these networks are not well supported by currently popular mobile platforms like iOS and Android. The authors in [4] and [5] propose network structures which improve multi-hop mechanism for network scalability. The disadvantage of these structures is that they rely on the tree-based approach, which is difficult to handle mobility and changes in the network condition. In [6, 7], the authors propose a network architecture that allows mobile devices in each cluster to connect to a cellular network through an intermediate mobile device called cluster head. This architecture takes advantage of Wi-Fi Direct (WFD) capabilities [8, 9, 10, 11] to support mobile devices to communicate with each other using 802.11 interfaces. However, this architecture does not support multi-hop mechanism. Therefore, it is not a suitable solution to be applicable in disasters.

In this paper, we propose an architecture (called Group-based Internet Connection Spreading or GICS) that supports groups of mobile devices to get the Internet connection through working infrastructure APs or intermediate groups of devices that have already reached the Internet. By the support of the Internet-connected Device Discovery mechanism proposed in GICS, mobile devices in groups can discover the Internet connection status in nearby devices to help their groups obtain the

Internet connection. By the support of current technologies like Wi-Fi Direct [8,9,10,11], devices in GICS can perform functionality like Software Access Points (Soft APs) to issue Internet access for other devices. In addition, through the proposed Internet connection spreading mechanism, Internet connection can be delivered from still alive infrastructure APs through Internet-connected groups of devices (that play roles as intermediate Soft APs) to further groups of devices in an effective way.

Unlike existing approaches, GICS enables mobile devices to actively search for Internet connection status in its nearby devices. Moreover, within a GICS group, mobile devices can collaborate together to bring the reasonable Internet connection to all group members. In addition, GICS can flexibly adapt with changes in the network condition since each GICS group can determine on which Internet connection is efficient among the possible candidates that the group members can obtain, and necessarily rearrange the roles of group members to maintain the suitable Internet connection.

The main contributions of this paper are as follows: (*i*) we design a novel network architecture that allows Internet-connected groups of mobile devices to share their Internet connection in infrastructure mode based on the support of WFD technology; (*ii*) We provide a minor extension for WFD – supported devices to enable them to discover the Internet connection status of nearby devices while keeping the compatibility with WFD standard; (*iii*) we design a mechanism that efficiently spread the Internet connection to mobile devices through alive infrastructure APs or intermediate groups of Internet-connected mobile devices in case the infrastructure – based networks are disabled.

The rest of the paper is organized as follow. Section 2 gives an overview of WFD technology. Section 3 describes the proposed architecture, the proposed Internet-connected Device Discovery mechanism as well as explains how Internet connection can be spread from still alive infrastructure APs to Internet-unconnected groups of mobile devices. In section 4, we conclude the paper and address the direction for future work.

2. Overview about Wi-Fi Direct Technology

2.1. Architecture

Wi-Fi Direct (WFD) [8, 9, 10, 11] is a technology defined by Wi-Fi Alliance that enables devices to connect with each other easily for file transfer and Internet connectivity at typical Wi-Fi speeds. Different from traditional Wi-Fi that requires the use of a central access point for communication between devices, WFD uses a 'Software Access Point' (Soft AP). A WFD-supported device can play a role of an AP with functions similar to a traditional AP as well as a role of a wireless local area network station (WLAN-STA or STA). These are logical roles that are dynamic and could be executed concurrently by the same device (Concurrent Mode operation [8]).

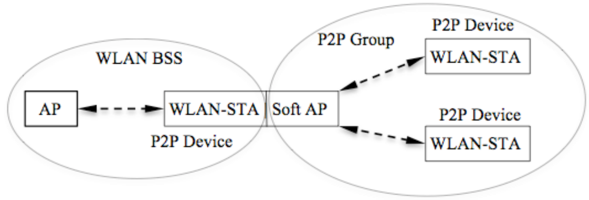

Figure 1. An example of Wi-Fi Direct-supported topology

In order to establish a communication, the devices perform Group Formation procedures to form Peer-to-Peer (P2P) groups, which are functionally equivalent to traditional Wi-Fi infrastructure networks. In these procedures, the devices negotiate with each other for the role that each device will assume. A P2P group includes a device implementing AP-like functionality (called P2P Group Owner or P2P GO) and other devices acting as clients (called P2P Clients). Once the P2P group is established, the other P2P Clients and legacy clients can join the group by connecting to the P2P GO as in a traditional Wi-Fi network. A legacy device is not required to support enhanced functionalities defined in WFD and simply 'see' the P2P GO as a traditional AP.

The P2P GO of a group advertises itself through *beacons* like a traditional AP. These *beacons* as well as all management frames defined in WFD contain additional *P2P Information Elements* (P2P IEs). The device that plays the role as a P2P GO can also support the Dynamic Host Configuration Protocol (DHCP) Server functionality to provide IP addresses to P2P clients.

2.2. Device Discovery

In order to establish a connection, P2P devices have to find each other by performing the Device Discovery procedures. P2P devices use scanning process defined in IEEE Std 802.11-2007 [12] to find other P2P devices or P2P groups and to locate the best potential operating channel to establish P2P groups. By scanning on all supported channels, P2P devices collect information about surrounding P2P devices or Wi-Fi networks. P2P devices send *Probe Request* frames that contain *P2P IEs* to elicit Probe Response frames from legacy networks and the P2P Group Owner. Once a P2P device receives a

Probe Response, it can process Group Formation procedures to establish connection with responding devices. Once associating in a P2P group, only the GO is discoverable by legacy clients because only the GO are allowed to response *Probe Requests*.

The *P2P IE* is defined using the Vendor Specific information element format (as defined in IEEE Std 802.11-2007 [12]). One or more than one *P2P IEs* may be included in a single frame. Each *P2P IE* contains a number of *P2P Attributes* as illustrated in Fig. 2.

P2P IE									
Elem. ID	Length	OUI	OUI Type	Attr. ID	Length	Attr. Body	Attr. ID	Length	Attr. Body
				P2P Attributes					

Figure 2. An example of two P2P attributes carried in a P2P IE

2.3. Group Formation

Once two devices have found each other, they perform Group Formation procedures to form a group. The devices negotiate their roles using a three-way handshake (*GO Negotiation Request/ Response/ Confirmation*), where by the two devices agree on which device will play the role as P2P GO and on the channel where the group will operate. In order to determine the P2P GO, P2P devices include a numerical parameter (*GO Intent value*) in their *GO Negotiation Requests* and *GO Negotiation Responses*. The device declaring the highest intent value will become the P2P GO. Once the GO Negotiation phase has completed, devices can perform Provisioning phase to form a group.

Together with the Device Discovery and Group Formation procedures, WFD also supports Service Discovery, Security and Power Saving procedures. The detail of these procedures can be referenced at [8, 9, 10].

3. Group-based Internet Connection Spreading Architecture

We propose the Group-based Internet Connection Spreading (GICS) architecture for Internet connectivity in disaster regions. GICS delivers Internet connection from working infrastructure APs to groups of mobile devices efficiently. In GICS, an Internet-connected Device Discovery mechanism is additionally proposed based on WFD technology. This mechanism enables devices to discover surrounding devices that have connected to the Internet. These are covered in the following sections.

3.1. GICS System Architecture

We assume that in disasters, each device can connect to its nearby devices to form GICS groups using WFD technology. A GICS group includes a Group Head (GH) and a number of clients connecting to the GH. A GH can play a role as a Soft AP and a role as a client similar to the GO in WFD. As a Soft AP, the GH can perform functionality similar to a traditional AP to issue Internet access for other devices. As a client, the GH can connect to any infrastructure AP or another Soft AP to get Internet connection. Devices that play client role can simply ‘see’ and connect to Soft APs issued by other devices like traditional APs. In a GICS group, the GH also provides a DHCP Server application to assign IP addresses to its clients. With the current paradigm, WFD fulfills these requirements. Therefore, the devices that play GH roles in GICS are required to support the functionalities defined in WFD. The GH is also required to embed Network Address Translation (NAT) application [13] to operate routing functionality in the system.

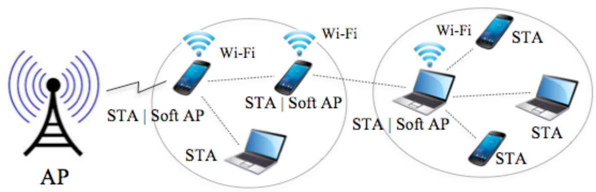

Figure 3. GICS architecture

Before proceeding with next sections, we now introduce the definitions used in the paper:

- **GICS Group**: A group of mobile devices in which one of them plays a role as a Group Head and others play roles as Group Clients in the GICS architecture.
- **GICS Device**: A mobile device that support required functionalities in the GICS architecture.
- **Group Head (GH)**: A group member that performs Soft AP functionality and other procedures similar to the Group Owner in WFD. The GH is required to perform additional NAT functionality [13] to operate routing in the group.
- **Group Client**: A group member that supports the Client role defined in WFD.
- **Legacy Client**: A STA that is not required to support WFD functionality. These devices simply ‘see’ Soft APs like traditional APs.

3.2. Internet-connected Device Discovery

The GICS requires devices to be able to discover nearby Internet-connected devices of other groups. Currently, WFD has no mechanism to support this ability. By current support of WFD, a legacy client cannot discover Internet connection status of surrounding devices except the GO of a group or devices associated with an infrastructure AP. We propose an Internet-connected Device Discovery mechanism that enables devices to advertise their Internet connection status to be discoverable by other devices.

In order to enable GICS devices to advertise about its Internet connection status, we propose a minor extension to Wi-Fi Direct by defining a new additional P2P Attribute named '*Internet Connection Status*'. This new attribute is defined in the reserved fields in P2P Attribute IDs Table defined in WFD specification [8]. Table 1 shows this new attribute (whose attribute ID is 19) together with other WFD – defined attributes (which have attribute IDs from 0 to 18).

Table 1. Extended WFD P2P Attribute ID Definitions Table with the proposed '*Internet Connection Status*' attribute.

Attribute ID	**Notes**
0	Status
…	…
18	Invitation Flags
19	**Internet Connection Status**
20-220	Reserved
221	Vendor specific attribute
222-255	Reserved

The format of the *Internet Connection Status* attribute is showed in Table 2.

Table 2. The *Internet Connection Status* attribute format

Field	**Size (octets)**	**Value**	**Description**
Attribute ID	1	19	Indentifying the type of P2P attribute.
Length	2	1	Length of the following fields in the attribute.
Internet Connection Status Code	1	0-1	A Internet connection status code.
Internet Connection Quality	1	0-10	A Internet connection quality value.
Hop-count	1	0-255	A Hop-count value.

In Table 2, the *Internet Connection Status Code* is 1 if the device has Internet connection and 0 if not. The *Internet Connection Quality* value is a numerical value from 0 to 10 representing the quality of the Internet connection in the device. The *Hop-count* value is a number of Hops (intermediate Soft AP nodes) counting from the infrastructure AP that originally issues the Internet connection to the current device. In GICS, each node is required to store its *Hop-count*. A node that directly connects to an infrastructure AP has *Hop-count* equal to 1. Once a node connecting to the Internet through a Soft AP node, its *Hop-count* is equal to the *Hop-count* of the Soft AP node plus 1.

In GICS, in order to advertise the Internet connection status, Internet-connected devices include an additional *Internet Connection Status* attribute in the P2P IEs of their *Probe Request* frames and *Probe Response* frames before sending them. In this attribute, the *Internet Connection Status Code* is set to 1. The *Internet Connection Quality* is set by a value from 0 to 10 based on the signal strength of the Internet connection. The *Hop-count* is set based on the Hop-count value stored in the device.

Once a device receives a *Probe Request* frame or *Probe Response* frame from a nearby device, it checks if this frame contains an *Internet Connection Status* attribute or not. If the frame contains that attribute with the *Internet Connection Code* equal 1 (together with the information about *Internet Connection Quality* and *Hop-count*), the device can realize that the nearby device is Internet-connected. The exchange of *Probe Requests* and *Probe Responses* between devices is illustrated in Fig. 4.

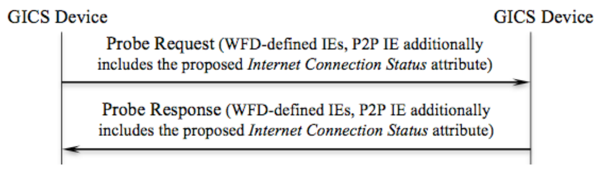

Figure 4. Probe Request/ Response exchange in the Internet-connected Device Discovery mechanism

In GICS, clients in an Internet-connected group are also allowed to response the received *Probe Requests* by sending *Probe Response* frames. These frames include the *Internet Connection Status* attribute in their *P2P IEs* as mentioned above. By this way, group clients can also advertise its Internet connection status instead of just the GO as defined in WFD. Once a device discovers an Internet-connected device, it can get the Internet connection from this device following the *GICS Connection* procedure described in section 3.4.

3.3. Internet Connection Spreading Mechanism

This section explains how Internet connection is spread from infrastructure APs to Internet-unconnected groups in the proposed architecture.

Once a group is formed, it tries to find nearby devices that are already have Internet connection. With the support of the proposed Internet-connected Device

Discovery mechanism, devices can discover if a nearby device is Internet-connected or not. All group members including the GH are responsible for this searching process. Possible cases may occur as follow.

- If the GH (e.g. node GH 1 or GH 2 in Fig. 5) finds an infrastructure AP (or some infrastructure APs) nearby, it connects to the AP (or the most suitable AP based on their signal strengths). Then, the GH switches on its Soft AP functionality to issues Internet access for all group clients (e.g. group 1 or group 2 in Fig. 5).
- If the GH does not find any infrastructure AP but an Internet-connected node (called c-node) nearby:
  - If this c-node is a GH of an Internet-connected group (called c-GH), the GH can join the group as a client and get Internet connection from the c-GH (following the WFD – supported group formation procedures). Then, the GH issues Internet access to group clients by switching on its Soft AP functionality.
  - If the c-node is a client of an Internet-connected group (e.g. node C 2.2 in Fig. 5), the GH (e.g. node GH 4 in Fig. 5) will request the c-node to switch on its Soft AP functionality. Then the GH connects to the c-node to get the Internet connection for its group using the *GICS Connection* procedures (see section 3.4).

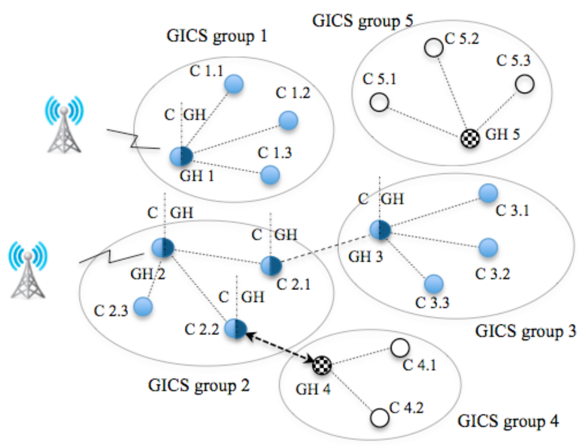

Figure 5. Internet connection spreading mechanism in GICS

In case the GH (e.g. node GH 5 in Fig. 5) of an Internet-unconnected group does not find any infrastructure AP or c-node but one of its group clients (e.g. node C 5.1) finds a nearby c-node (e.g. node C 1.2 in Fig. 5), the client requests the c-node to switch on its Soft AP functionality and gets the Internet connection from the c-node using the *GICS Connection* procedure. Once obtaining the Internet connection, the client requests the current GH of its group to exchange the GH role by the support of the *GH Role Change* procedures (see section 3.5). The client now becomes the new GH of the group, switches on its Soft AP functionality to issue Internet access for all group members.

3.4. GICS Connection Procedures

In the GICS device discovery process, once a device receives a *Probe Response* frame from a nearby device, it checks if this frame contains an *Internet Connection Status* attribute. The existence of an *Internet Connection Status* attribute with *Internet Connection Status Code* equal 1 means that the nearby device is Internet-connected. In this case, the device can connect to this c-device to get the Internet connection. First, device sends a *GICS Internet Connection Request* message to the c-device to suggest the c-device to switch on its Soft AP functionality. The c-device responses this request by sending to the device a *GICS Internet Connection Response* message to confirm that it can issue Internet connection (or notify failures if not). The two devices then perform the *GH Negotiation* procedures to negotiate their roles. These negotiation procedures are similar to the *GO Negotiation* procedures defined by WFD [8, 9, 10, 11] with a minor change in setting the *GO Intent value*. The requesting device set the *GO Intent value* in its *GO Negotiation Requests* to 0, and the c-device set the *GO Intent value* in its *GO Negotiation Responses* to 15. These settings are to make sure that the c-device will be a GH to issue the Internet access to the device which now playing the role as a client.

3.5. Group Head Role Change Procedures

In case a client in a GICS group discovers an Internet-connected device nearby, it can request to become a GH replacing the role of the current GH. In a GICS group, a GH may receive more than one GH role requests from its clients. In this case, the GH can determine the reasonable client that may potentially become the new GH among the candidates. The criteria to choose the reasonable device are the Internet Connection Quality and the Hop-count included in the GH Role requests that the GH received from the clients. The device choosing determination between two devices is depicted in Fig. 6.

Once the GH finds a requesting client whose Internet connection is more reasonable than its Internet connection (based on the similar device choosing determination method as mentioned), it can resign the GH role to the client. In this case, the client sends a *GH Role Change Request* message to the GH. Once the GH receives this request, it responses by sending a *GH Role Change*

Response message to the client. This message contains the updated list of members together with their WFD – defined device information. Second, the GH sends *GH Role Change Notification* messages to all clients in the group to notify about the role change. Once completing these procedures, the clients connect to the new GH to re-form the GICS group.

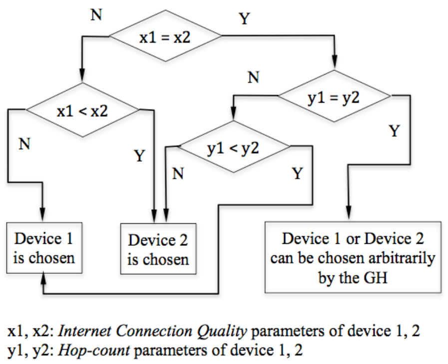

Figure 6. Device choosing determination flowchart

4. Conclusions and Future Work

This paper proposed a Group – based Internet Connection Spreading architecture to quickly provide Internet access for mobile devices in case infrastructure – based networks are disabled. In GICS, Internet-connected groups of devices play roles as software access points to issue Internet access for other groups of devices based on an efficient paradigm. The Internet-connected Device Discovery mechanism in GICS, which is proposed as an extension of Wi-Fi Direct standard, enables devices to discover nearby devices that have already connected to the Internet. By the support of this feature, and through an effective spreading mechanism, the Internet connection is efficiently spread from still alive access points to Internet-unconnected groups of mobile devices.

The devices within a group in GICS can collaborate together to obtain reasonable Internet connection for the group. Therefore, GICS can flexibly adapt with changes of network conditions as well as network topology. The Internet connectivity in GICS is also reliable since the connection between devices is based on Wi-Fi standard.

With the addressed advantages, GICS can be a promised approach for Internet connectivity in disasters. Our future work concentrates on real deployment as well as experimentation to evaluate the feasibility and scalability of the proposed architecture.

References

[1] J. P. G. Sterbenz, D. Hutchison, E. K. Cetinkaya, A. Jabbar, J. P. Rohrer, M. Scholler, P. Smith, "Resilience and survivability in communication networks: strategies, principles, and survey of discriplines", In *Journal of Computer Networks,* Vol. 54, pp. 1245-1265, 2010.

[2] M. Portmann, and A. A. Pirzada, "Wireless Mesh Networks for public safety and crisis management applications," In *IEEE Internet Computing*, Vol. 12, No. 1, pp. 18-25, 2008.

[3] J. C. Kim, D. Y, Kim, S. M. Jung, M. H. Lee, K. S. Kim, C. K. Lee, J. Y. Nah, S. H. Lee, J. H. Kim, W. J. Choi, S. K. Yoo, "Implemetation and performance evaluation of Mobile Ad hoc Network for emergency telemedicine system in disaster areas," In *31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 1663-1666, USA, 2009.

[4] M. H. Sarshar, P.K. Hoong, I. A. Abdurrazaq, "NodesJoints: a framework for tree-based MANET in IEEE 802.11 infrastructure mode", in *IEEE Symposium on Computers & Informatics*, Malaysia, 2013.

[5] Q. T. Minh, K. Nguyen, S. Yamada, "Virtualized multihop access networks for disaster recovery", in *WoWMoM*, Spain, June 2013.

[6] A. Asadi, V. Mancuso, "On the compound impact of opportunistic scheduling and D2D communications in cellular networks", in *MSWiM'13*, Spain, 2013.

[7] A. Asadi, V. Mancuso, "WiFi Direct and LTE D2D in Action", in *Wireless Days*, Spain, 2013.

[8] Wi-Fi Alliance, P2P Technical Group, WiFi Peer-to-Peer (P2P) technical specification v. 1.14, 2010.

[9] WiFi Alliance, "Wi-Fi Certified Wi-Fi Direct", White Paper. Available: http://www.wi-fi.org/knowledge-center/white-papers/wi-fi-certified-wi-fi-direct™-personal-portable-wi-fi®-technology-2010.

[10] Huges Systique, "Wi-Fi Direct", 2013. Available: http://www.hsc.com/Portals/0/Uploads/Articles/WFD_Technology_Whitepaper_v_1.7635035318321315728.pdf

[11] D. Camp-Mur, A. Garcia-Saavedra, P. Serrano, "Device to device communications with WiFi Direct: overview and experimentation", in IEEE Wireless Communications Magazine, p. 96-104, June 2013.

[12] IEEE, IEEE Std 802.11-2007 IEEE standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[13] Wikipedia, "Network Address Translation", 2013. Available: http://en.wikipedia.org/wiki/Network_address_translation.