Journal of Mobile Multimedia, Vol. 10, No. 1&2 (2014) 030-042
© Rinton Press

MDRAN: MULTIHOP DISASTER RECOVERY ACCESS NETWORK

Quang TRAN-MINH(1) (2), Kien NGUYEN(1), Eiji KAMIOKA(3), Shigeki YAMADA(1)

(1)*National Institute of Informatics, Tokyo, Japan*

(2)*Hochiminh City University of Technology, Hochiminh, Vietnam*

(3)*Shibaura Institute of Technology, Tokyo, Japan*

{quangtran, kienng, shigeki}@nii.ac.jp, kamioka@shibaura-it.ac.jp

This paper proposed a novel approach to resilient wireless multihop disaster recovery access networks (MDRAN). Both virtual access point (VAP) and wireless virtualization (WV) techniques have been combined in an appropriate way thereby the networks can be automatically setup on-demand using on-site commodity mobile devices (laptops, tablet PCs, smart phones). In the proposed approach, difficulties remained from conventional access network technologies such as the requirements of installing special hardware (e.g. multiple network interface cards - NICs, particular mesh routers, etc.,) and software (e.g. network auto-configuration software including routing protocols) on each mobile node (MN) in advance have been resolved. As a result, users can connect to the proposed MDRAN as easily as connecting to conventional APs. After connecting to the proposed network, users naturally and unconsciously contribute to the network extension. This feature improves the self-supporting capability at the disaster's local communities. Experimental evaluations reveal the feasibility, effectiveness as well as the scalability of the proposed approach. As a result, the proposed scheme is ready to be realized in the actual disaster recovery applications.

Key words: Resilience, Wireless virtualization, Multihop communications, Access network, Virtual access point.

1 Introduction

Recent tragic disasters, such as "The Great East-Japan Earthquake" in March 2011 [1], "The Earthquake off Sumatra Islands" in 2009, "The Iwate-Miyagi Nairiku Earthquake" in June 2008, etc., show limitations of the current communication technologies. Disasters may destroy everything including communication infrastructures isolating people. Obviously, **Internet connection** is one of the most important channels for sharing disaster related information such as the victims' vital states, where they are, number of casualties, the way to reach evacuation locations, and so on. However, recovery of large-scale damaged communication infrastructures is prolonged which is inappropriate for first disaster responses.

Multihop wireless access network (MWAN) established using on-site devices without any requirement from communication infrastructure is suitable approach to disaster recovery. Existing MWAN technologies such as wireless mesh backhaul network (WMN) [3], mobile ad-hoc network (MANET) [4], and disruption/delay tolerance network (DTN) [5] are potential technologies for disaster recovery. Nevertheless, these technologies still disclose several limitations hindering the realization of real disaster recovery networks. For example, WMN must be deployed in advance at particular locations using special hardware (e.g. mesh routers). Similarly, MANET requires special network auto-configuration software (NAS) to be installed and well configured in each MN beforehand. These tasks are overcomplicated to ordinary users (e.g. elderly and non-technical people) at disaster areas. Meanwhile, DTN is not mature enough for real-world applications.

In order to overcome these technological gaps, this work proposes a novel solution for quickly setting up on-site **multihop disaster recovery access networks** (MDRAN). The proposed MDRAN can be established using only commodity mobile devices (laptops, tablets, smart phones, etc.,) without any requirement from communication infrastructure or additional hardware. In MDRAN, nearby devices connect with each other naturally, creating a **multihop communication network** to reach the still alive Internet gateways (IGWs) for **Internet connectivity**. As a result, every victim in the disaster-stricken areas, even those who are far apart from the IGW, is bridged to the outside world. The main contributions of this paper are summarized as follows:

(a) A novel on-site MDRAN creation scheme, including overall architecture and network management protocol, is proposed

(b) Internet connectivity related issues such as IP allocation and management in the proposed scheme are thoroughly discussed

(c) A multihop communications model using commodity mobile devices equipped with a single built-in WiFi interface (WIF) is proposed

The rest of the paper is organized as follows: Section II reviews current technologies for disaster recovery access networks, while essential criteria for on-site configured MDRAN are clarified in Section III. Section IV describes the proposed approach in details. Section V evaluates the proposed approach, while section VI concludes this work and draws out future work directions.

2 Related Work

The current cellular network technologies like 3G, WiMAX, LTE [6], [7] systems offer services in relatively large coverage areas. These systems are based on fixed base stations (BSs) hence they are vulnerable to disasters. Satellite systems have been proposed to be applied in disaster recovery [8] since they are robust in terms of coverage and tolerance to ground damages. However, this technology requires specific transceiver devices using very small aperture terminals (VSATs) which are unlikely to be always on-site available.

Consequently, WMN becomes one of the key solutions for emergency relief applications [3], [9] since it can be established without any requirement for communication infrastructure. In general, WMN is an access network combining of wireless networking technologies, ad-hoc multihop routing protocols, and the capability of self-configuration. However, WMN is facing on several inherent issues: (a) the WMN is a type of infrastructure network which must be established in advance at places where constructors can reach; (b) to setup the network, special devices such as mesh routers (MRs) are required; and (c) it requires lots of skillful manpower to deploy the network. These requirements are unlikely to be satisfied in the actual disasters. Therefore, it is necessary to have a smarter solution where the network can be established on-demand.

MANET [4] has been proposed to resolve the WMN issues mentioned above, based on its capability of mobility, self-configuring, self-healing. However, many issues related to real deployments of disaster recovery MANETs still remain. For instance, similar to WMN, special NAS including complicated multihop routing protocols [10] must be installed in each MN beforehand. It would be difficult for ordinary and non-technical users to appropriately install and configure such complicated routing protocols for Internet connectivity. In addition, the MANET throughput significantly degrades under multihop communications and it requires a concrete end-to-end (E2E) path to set a communication medium.

Disruption/delay tolerant network (DTN) is an advanced version of MANET where more flexible mobility and long disruption/delay are considered [11], [12], [13]. It does not assume any explicit E2E path for routing protocols. Therefore, DTN routing becomes more challenging compared to that in other wireless technologies such as WMN, MANET, etc. As a result, DTN routing has almost become an independent research area [14]. Several studies have been dedicated to DTN routing protocols like Epidemic [15] protocol, probabilistic routing protocol using history of encounters and transitivity (PROPHET) [16], or social network inspired routing protocols [17], [18]. A useful survey on this field can be found in Zhang's paper [19]. Theoretically, DTN is suitable to be applied in severe disrupted environments such as disasters since it tolerates well with long communication delays by providing "in-network" storage capability. However, most of researches in this field mainly focus on routing protocols and rely on simulations to confirm the effectiveness of their proposed solutions [20], [21]. It is difficult to find reliable real-world deployments of DTN for disaster recovery. Consequently, even DTN is a potential technology it is not mature enough to be applied in real disaster recovery.

Our work is completely different to aforementioned technologies. This paper proposes a novel scheme for practically establishment of on-site configured multihop disaster recovery access networks. Here, a virtualization approach in which both the software access point (Soft-AP) and wireless virtualization (WV) techniques [22] are utilized and well combined. The WV abstracts the single built-in WIF in a commodity MN into different logical WIFs which can be used simultaneously. Soft-AP transforms a MN into a virtual access point (VAP) which functions as an actual AP, providing Internet access means to the nearby nodes. In addition, the feasibility as well as the effectiveness of the proposed approach are not merely proved based on simulations but based on real-field experiments. The experimental results reveal the readiness of this technology to be realized in real-world applications for actual emergency relief.

3. Essential Requirements and Problem Definition

3.1. MDRAN Essential Requirements

J. P. G Sterbenz et al. have defined *resilience as the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation* [2]. As disasters are a unique category of external challenges to communication networks, they cause correlated failures over large areas. Disasters extremely destroy communication infrastructures while simultaneously prevent operators from normal maintaining and restrict information access by decision-makers (e.g. government, emergency operation center, etc.,) resulting in serious crisis. Recovery of large-scale damaged backbone networks is prolonged taking several weeks which is not suitable for disaster responses.

Wireless multihop disaster recovery access network (MDRAN) is an appropriate approach for short term fixing of Internet disconnection. To that end, concrete criteria for a resilient MDRAN must be clarified in the context of large-scale disasters. Unfortunately, none of the existing work mentioned in Section II has thoroughly discussed on those matters. This section proposes a practical approach to clarifying essential criteria for the proposed MDRAN. Based on those criteria, requirements and corresponding issues which must be resolved are clarified.

The SAFECOM program, the US Department of Homeland Security, has issued a Statement of Requirements (SoR) for public safety wireless communication [22] as: (a) the network must provide integrated services including voice and data communications, (b) it can be setup using commercial off-the-shelf devices, (c) it supports for mobility, and (d) it must be on-scene access. For the requirement (a), it would be nice if the newly established network (the alternative one) can provide high-resource-consumed services like video, multimedia streaming. However, as shown in N. Uchida et al. study [8] after a disaster occurs lasting to two days, people needs the information about shelter, safety status, and disaster areas. This information is mostly text data which can be exchanged in low performance networks. Therefore, rather than network performance (throughput, latency, etc.,) the **Internet connectivity** is the must. It is also required that the proposed MDRAN scales well to cover a **large disaster area** via **multihop communications**. It must be ensured that every victim who may be very far from the still alive IGWs, can access to the Internet for sharing their safety status. In order to have an on-fly access network that satisfies those requirements, concrete technical issues must be thoroughly resolved as described below.

3.2. Problem Definition

We assume that there are some still alive IGWs around the disaster areas. Our work is mainly finding the way to make multihop communication networks bridging any isolated MN to the IGWs. To that end, essential issues which must be resolved can be summarized as follows:

(i) How to establish multihop communication networks using single built-in WiFi (IEEE 802.11) interface (WIF) commodity mobile devices? In multihop communications, each intermediate MN concurrently connects to different networks. For example, on one hand the MN, as a common station (STA), connects to an upstream node for Internet access. On the other hand, the MN also provides the Internet connection means to the nearby (downstream) MNs. This fact requires multiple network interface cards (NIC) to be equipped in each MN. In this work, we utilize WIF as a wireless communication means since it is widely used in every commodity mobile devices. However, it is unrealistic to require multiple WIFs to be installed in each MN just for the disaster recovery purpose. This issue must be thoroughly resolved in this work.

(ii) When nodes connect with each other creating a multihop network, each node must be well identified. IP address allocation and IP duplication avoidance mechanisms must be well discussed.

(iii) Last but not least, a simple and effective network management protocol to manage the network topology is needed.

Solutions for the aforementioned issues are thoroughly proposed in the following sections.

4. On-site Configured MDRAN

4.1. Overall Architecture

The overall architecture of a resilient MDRAN is shown in Fig.1. When the conventional communication infrastructures such as cellular BSs, backbone routers, etc., have been damaged (Fig. 1a), MNs should dynamically change their communication modes to connect to the nearby nodes creating a multihop wireless access network which extends to reach a still alive IGW (a MR, a BS, or an AP) located somewhere inside/outside the disaster area. Through multihopping, all MNs in the established MDRAN can access to the Internet as shown in Fig. 1b. It should be noted that because of the limitation on WiFi transmission range, there may be a gap between any pair of nodes. This fact is common in disaster situations and can be overcome by having volunteer users move into the site and cover the gaps as shown in Fig. 1b.

In Fig. 1b, each intermediate MN (e.g. PC1) connects to different networks simultaneously requiring multiple WIFs. In addition, to make a multihop E2E communication, e.g. from M1 to AP (as the IGW for Internet connectivity), an appropriate routing protocol is needed. This research proposes a novel solution to clear the requirements for additional hardware (additional physical WIFs) and to simplify the routing mechanism for multihop communications in MDRAN. Under this approach, wireless multihop access networks can be established on-demand using on-site commodity devices without any interference from and completely be transparent to users. As a result, the proposed MDRAN is definitely suitable and resilient to disaster recovery. Details of the proposed approach are described in the following sub-sections.

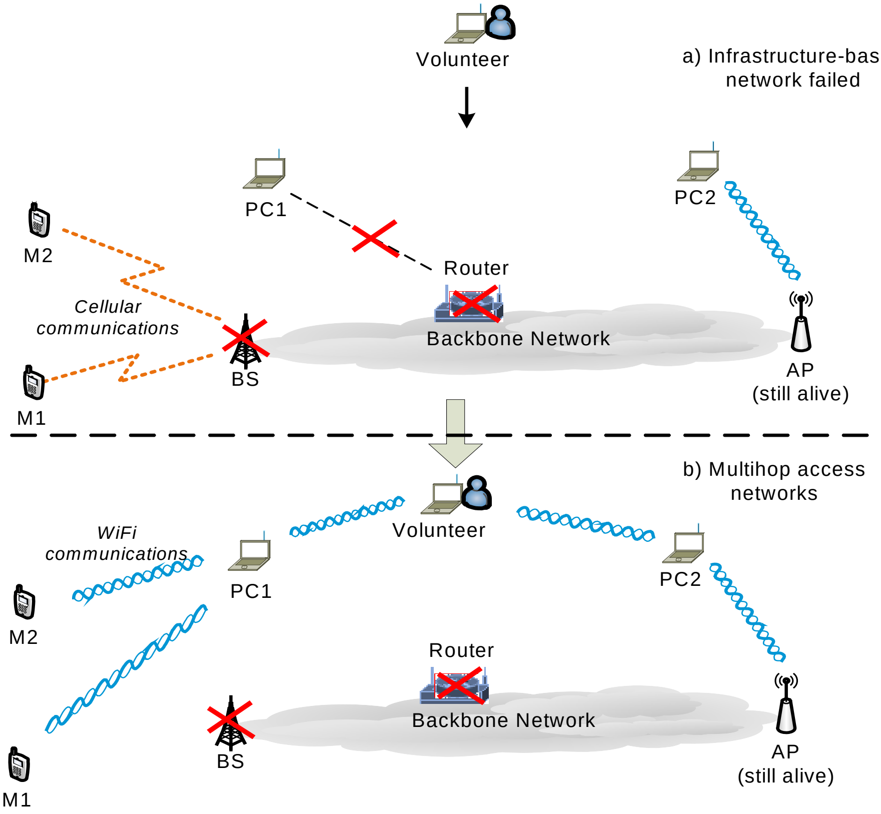

Fig. 1. Internet access through wireless multihop communications network

4.2. Network Design

In order to keep the resilience of the proposed MDRAN, specific assumptions should be avoided. Here, the network can be established and properly work with a single assumption as "**there is at least a still alive IGW around the disaster area**."

In order to avoid using additional hardware (physical WIFs), a software based approach is utilized. In this work, we proposed special network auto-configuration software, namely the DrNet (Disaster recovery Network) for network establishment. DrNet's main components are shown in Fig. 2 and can be described as follows.

- The **Wireless Virtualization** (WV) component abstracts the single built-in physical WIF into two logical interfaces, namely WIF1 and WIF2. This task assures that any node is viable for concurrently connecting to different networks using its different logical WIFs

- The **Virtual AP Establishment** component deals with virtual AP (VAP) creation and management. It makes the MN connect to an upstream AP (or VAP) for Internet connectivity using the node's WIF1. The second WIF (WIF2) is used for the VAP. The basic functionalities of the VAP as an actual AP such as *AP advertisement, accepting association requests from STAs*, etc., are provided by this component

- The **Network Management** component keeps in charge managing new nodes that join the network, assigning IP addresses to new joining nodes, managing the network topology information that the considering node can be aware of

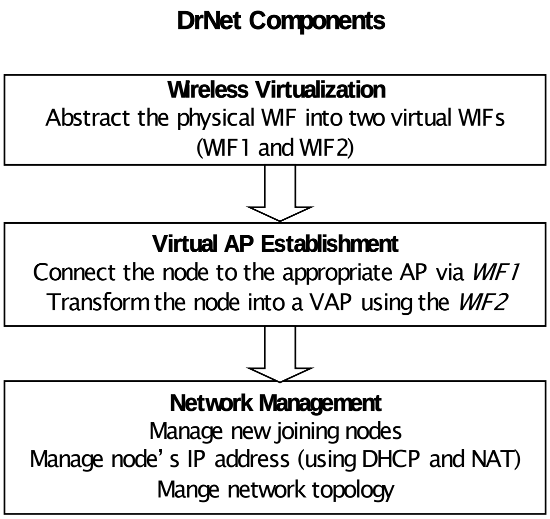
DrNet Components
Wireless Virtualization
Abstract the physical WIF into two virtual WIFs
(WIF1 and WIF2)
Virtual AP Establishment
Connect the node to the appropriate AP via WIF1
Transform the node into a VAP using the WIF2
Network Management
Manage new joining nodes
Manage node’s IP address (using DHCP and NAT)
Mange network topology

Fig. 2. Components in Disaster recovery Network auto configuration system (DrNet)

An emerging issue is that the DrNet is also required to be installed in each MN in advance. However, this issue can be solved by having the DrNet installed in the devices of volunteering users as shown in Fig. 3. These volunteering devices serve as VAPs for victims' devices (commodity devices). The commodity device can connect to the volunteering VAP using its common STA (served by the physical WIF). After connecting to the volunteering device, the DrNet is downloaded to the victim's device to transform this MN into a MDRAN node with the VAP functionality serving connection means to nearby nodes. This procedure is illustrated in Fig. 3. As shown, after connecting to the VAP at the volunteering MN (step 3), the DrNet is uploaded from the volunteering PC to the victim's device. This software transforms the victim node into a VAP at step 5, and from then (step 6) this node can be seen as a VAP from nearby nodes (not appear in the figure).

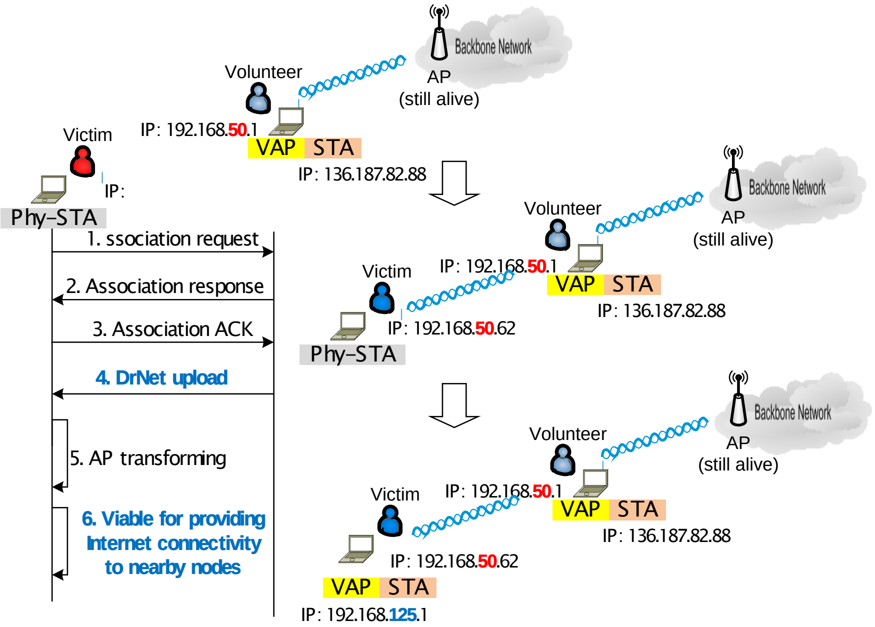

Fig. 3. Sequence diagram for transforming a commidity node into a MDRAN node

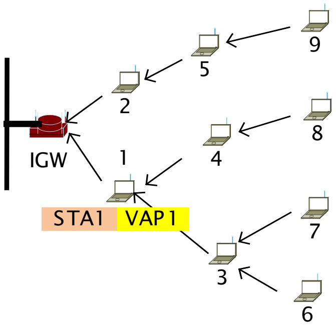

Fig. 4. A tree-based MDRAN extends the network coverage

As each MDRAN node working in both modes, namely STA and VAP modes, concurrently, every node can connect to the upstream infrastructure network (provided by the upstream VAP) for Internet access (using its STA mode) and provide the Internet connectivity to the downstream nodes (using its VAP mode) at the same time. This feature helps to extend the network as a tree-based topology to cover a large area as shown in Fig. 4. As a result, victims who are far apart from the still alive IGW can have a chance to access to the Internet via the proposed MDRAN. The network management protocol for this network topology is presented in the next section.

4.3. Network Management Protocol

The network management protocol of the proposed MDRAN requires each node to manage two tables as follows. The **information** table stores information about the network topology a particular node can be aware of. The **neighborhood** table manages information about the neighbors of a node. The structure of these two tables is presented in Tables I, and II, respectively. The last column in each table shows an example for the node 1 in Fig. 4. It should be noted that even though nodes 3, 4 are in the transmission range of node 1, they are not in the node 1's *neighborhood* table since they are already included in the node 1's *information* table. The status of a node can be *"connected"* or *"disconnected"* representing whether the node is a member of the network or not, respectively.

Each node detects the availability of its children, parents and neighbors to update the two aforementioned tables. A node detects the availability of its children by waiting children's packets (either data or *Hello* packets). A node unicasts a *Hello* packet to its parent-node in every *Hello_interval*, if no data has been sent, to notify about its availability. A child-node confirms the availability of its parent node by checking ACK. The *Hello* packet consists of *(nodeID, parentId, IGW, hop_count)* which is also included in the header of each data packet. A node also extracts this information when it overhears messages from its neighbor nodes. Using this information, a node can update its **information** and **neighborhood** tables.

TABLE I. INFORMATION TABLE

Field name	Description	Example
Parent	Id of the parent node	IGW
IGW	The actual IGW that provides the Internet connection to this node (the network can be extended with several IGWs)	IGW
hop_count	Number of hop from the node to the IGW	1
childrenList{}	List of the node's children	{3, 4}
Status	*"Connected"* or *"disconnected"*	*Connected*

TABLE II. NEIGHBORHOOD TABLE

Field name	Description	Example
nodeId	Id of the neighbor node	{2}
hop_count	Number of hop from the nodeId to the IGW	{1}
sameIGW	(Y/N), saying that whether this node shares the same IGW with the considered node or not	Y
Status	*"Connected"* or *"disconnected"*	*Connected*

The procedures for automatically setting up the network are presented in Fig. 5. The procedure for a client (a MN with the STA mode) to associate with a VAP (or AP) is presented in Fig. 5a. A node frequently scans for the available VAPs (the line with the * mark). It tries to associate and connect to the appropriate VAP in the available list of serving VAPs. For simplicity, the strength signal of VAPs (RSSI - radio signal strength indicator) is used for selecting the appropriate VAP (the line with the ** mark). If the association is successful, the node updates its *information* table by calling the *update()* function which is presented in the lower part of the Fig. 5a. Figure 5b shows the procedure to accept a client association request at the VAP side. If the VAP gets an association request from a MN, it assigns an IP address, the default IGW, and the DNS server name to the associating node, providing Internet connection means to such a node. It also updates its *childrenList* and fires the *DrNet_trigger* forcing the client (the associating node) to download the DrNet which is necessary to transform the node into a VAP providing Internet connection means to further nearby nodes.

```
// (a) At a client node
Procedure joinNetwork(){
   Boolean f = False;
   Scan for available VAP; // *
   While (VAPList ≠ ∅) && !f{
        VAP$_i$ = (SELECT VAP from VAPList
            WHERE VAP$_i$.RSSI =
Max(RSSI)//**
                 And   VAP$_i$ not In
lastTry_VAP{});
        Associate to VAP$_i$;
        If success{
        update(this, VAP$_i$)
       };// end if
        f=true;}

Procedure update(node i,  node VAP$_i$){
        Infortable t = i. informtable;
        t.status = "connected";
        t.parent = VAP$_i$;
        t.IGW = VAP$_i$.IGW;
        t.hopcount = VAP$_i$.hopcount + 1;
}// end update
```

```
// (b) At a serving (VAP) node
Procedure acceptNodeJoin(node j){
   assign IP_address to j;
   add assined IP_address to NAT
table;
   assigns default IGW and DNS
server to j;
   this.childrenList.add(j);
   fire the DrNet_trigger asking
node j to download and install
the DrNet;
   } // end acceptNodeJoin
```

Fig. 5. Network configuration procedures: The left is for the client MN and the right is for a VAP node

5. Evaluation

This section evaluates the feasibility as well as the effectiveness of the proposed approach. Firstly, the **Internet connectivity** is verified. After that, details about network performance will be analyzed.

5.1 Evaluation Environment

The proposed MDRANs are established using ASUS U24A-PX3210 laptop PCs with 4GB memory, corei5 2.5Ghz CPU, and Windows 7 OS.

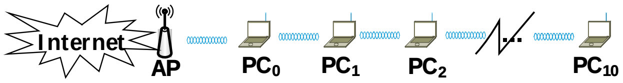

Fig. 6. A multihop tandem network

Several scenarios of the proposed MDRANs were established using 11 laptop PCs. Two representative network topologies have been created: (a) a multihop tandem network, and (b) a tree-based network as shown in Fig. 6 and Fig. 7, respectively. The distance between any pair of nodes in these two representative networks is 50m.

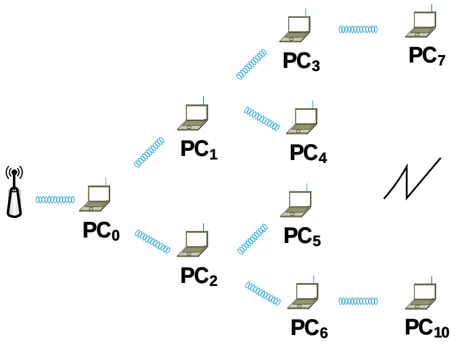

Fig. 7. A tree-based multihop access network

5.2 Feasibility and Effectiveness

In the experiments we recorded that it took just only **several seconds** at each node to join the network and to transform itself into a VAP. This time is short enough in terms of establishing an alternative network in disaster recovery.

As expected, the network configuration procedure works correctly at each node. A single physical built-in WIF at each MN is abstracted into 2 logical WIFs which are assigned appropriate IP addresses, default IGWs, etc. Table III shows an example observed from the tandem network (Fig. 6). As a result, each node can smoothly access to the Internet.

TABLE III. IP ADDRESS IS AUTOMATICALLY ASSIGNED TO EACH NODE IN THE TANDEM NETWORK

Node	STA IP Address *(for WIF1)*	VAP IP Address *(for WIF2)*
PC0	136.187.82.88	192.168.50.1 (default IGW for PC1)
PC1	192.168.50.62	192.168.125.1 (default IGW for PC2)
PC2	192.168.125.57	192.168.67.1
PC3	192.168.97.35	192.168.137.1
PC4	192.168.137.9	192.168.91.1
...		

For further evaluating of the network performance, round trip time (RTT) latency and jitter in multihop communications were recorded. As shown in Fig. 8, even the RTT increases when the number of hops increases, the average RTT still keeps in a low enough value. For example, the average RTT is around 200ms even at 10 hops. This RTT is qualified even for VoIP services and obviously it is quite good for http applications.

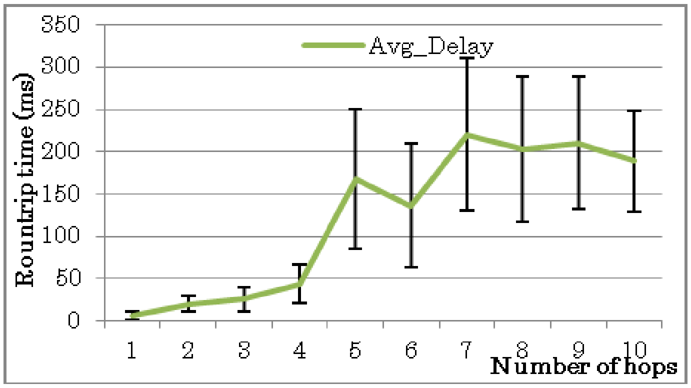

Fig. 8. Round trip time latency in multihop communications

We also target on providing smooth VoIP services in multihop communications since in disaster users tend to call to their families for sharing their safety information. Besides RTT, jitter is an important factor that influences the quality of VoIP services. Figure 9 shows that the jitter increases when the number of hops increases. However, this jitter increment is still acceptable for smooth VoIP services. This result reveals the feasibility of VoIP services in the proposed MDRAN.

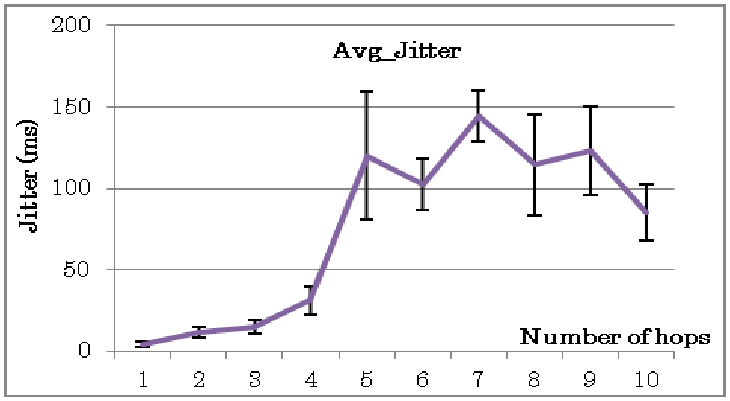

Fig. 9. Jitter in the proposed multihop access network

6. Concluding Remarks

This paper proposed a novel approach to on-site configuration of wireless multihop disaster access networks (MDRAN). The MDRAN includes a notable network design and a practical network establishment scheme where each node can work in both the STA and the VAP modes concurrently. As a result, every commodity mobile devices can provide Internet connection means to the nearby nodes. This feature significantly supports the network scalability. The feasibility as well as the effectiveness of the proposed MDRAN are proved by real-field experiments. The experimental results also show that the network configuration is transparent to users. Ordinary users can easily connect to the Internet through the proposed MDRAN as if they are connected to the conventional APs.

The tree-based topology is the nature of the proposed MDRAN scheme. However, this topology naturally reveals inherent issues which need to be thoroughly resolved. For example, the performance bottlenecks at nodes which are close to the root degrade the robustness of the whole network. High workload at "root" nodes due to forwarding packets to the destination (IGW) on behalf of its descendants may cause malfunctions at root nodes. Consequently, if any root node dies, all of its descendants (in its sub-tree) cannot connect to the Internet. Therefore, appropriate load balancing mechanisms utilizing mutiple IGWs (for multiple trees) are interesting directions for the future work.

Acknowledgements

This research was supported in part by the JSPS (Japan Society for Promotion of Science) Grant-in-Aid for Young Scientist (B), No. 25730067 (FY. 2013 - 2014).

References

1. Tohoku Earthquake and Tsunami (Jan. 2014),

   "http://en.wikipedia.org/wiki/2011_T%C5%8Dhoku_earthquake_and_tsunami".

2. J. P. G. Sterbenz, D. Hutchison, E. K. Cetinkaya, A. Jabbar, J. P. Rohrer, M. Scholler, and P. Smith, *"Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines,"* Computer Networks, Vol. 5, pp.1245-1265, 2010.

3. J. Ishmael, S. Bury, D. Pezaros, N. Race, *"Deploying Rural Community Wireless Mesh Networks,"* IEEE Internet Computing, Vol. 12, No. 4, pp.22-29, 2008.

4. L. Pelusi, A. Passarella, M. Conti,*"Opportunistic networking: data forwarding in disconnected mobile ad hoc networks,"* IEEE Communications Magazine, pp. 134-141, vol. 44, Issue 11, 2006.

5. Mc. Alex, F. Stephen, *"Delay- and Disruption-Tolerant Networking,"* IEEE Internet Computing, Vol. 13, No. 6, pp.82-87, 2009.

6. A. Yarali, S. Rahman, M. Bwanga, *"WiMAX: The Innovative Wireless Access Technology,"* Journal of Communication (JCM), Academy Publisher, pp. 53-63, Vol. 3, No. 2, 2008.

7. T. Doumi, M. F. Dolan, S. Tatesh., A. Casati, G. Tsirtsis, K. Anchan, D. Flore, *"LTE for Public Safety Networks,"* IEEE Communications Magazine, pp. 106-112, Vol. 51, No. 2, 2013.

8. N. Uchida, K. Takahata, Y. Shibata, N. Shiratori, *"Never Die Network Extended with Cognitive Wireless Network for Disaster Information System,"* The 5th International Conference on Complex, Intelligent and Software Intensive Systems, pp. 24-31, Seoul, Korea, Jun. 2011.

9. A. Yarali, A. Babak, R. Saifur *"Wireless Mesh Networking: A key Solution for Emeegency & Rural Applications,"* The 2nd International Conference on Advances in Mesh Networks, pp. 143-149, Athens/Glyfada, Greece, Jun. 2009.

10. J. Luo, D. Ye, L. Xue, M. Fan, *"A survey of multicast routing protocols for mobile Ad-Hoc networks,"* IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, pp.78-91, 2009.

11. K. Fall, *“A Delay-Tolerant Network Architecture for Challenged Internets,”* in Proc. ACM SIGCOMM ’03, pp.27–34, New York, NY, USA: ACM Press, 2003.

12. DTN history *"http://en.wikipedia.org/wiki/Delay-tolerant_networking,"* Access Jan. 2014.

13. S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf., B. Durst, K. Scott, H. Weiss, *"Delay-tolerant networking: an approach to interplanetary Internet,"* IEEE Communications Magazine, Vol. 41, No.6, pp.128-136, 2003.

14. K. Fall, S. Farrell, *“DTN: An Architecture retrospective,”* IEEE Journal on Selected Areas in Communications, Vol. 26, No. 5, pp.828-836, Jun. 2008.

15. V. Amin, B. David, *“Epidemic routing for partially con-nected ad hoc networks,”* Technical Report CS-200006, Duke University, Apr. 2000.

16. A. Lindgren, A. Doria, O. Schelen, *“Probabilistic Routing in Intermittently Connected Networks,”* In Proceedings of the The First International Workshop on Service Assurance with Partial and Intermittent Resources (SAPIR 2004), Fortaleza, Brazil, Aug. 2004.

17. A. Elwhishi, P. H. Ho, K, Naik, B. Shihada, *"A Novel Message Scheduling Framework for Delay Tolerant Networks Routing,"* IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No.5, pp.871-880, 2013

18. G. Wei, C. Guohong, T. L. Porta, H. Jiawei, *"On Exploiting Transient Social Contact Patterns for Data Forwarding in Delay-Tolerant Networks,"* IEEE Transactions on Mobile Computing, Vol. 12, No. 1, pp.151-165, 2013.

19. Z. Zhang, *“Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges,”* IEEE Communications Surveys and Tutorials, vol. 8, No. 1, pp.24–37, 2006.

20. Mc. A. Florence, N. Sathya, G. X. Geoffrey, *"Performance Analysis of Message Prioritization in Delay Tolerant Networks,"* Military Communication Conference (MILCOM2012), pp.1-6, 2012.

21. Md. N. Huda, F. Yasmeen, S. Yamada, and N. Sonehara, *“An Approach for Short Message Resilience in Disaster-Stricken Areas,”* Proc. of International Conference on Information Networking (ICOIN2012), pp.120-125, Bali, Indonesia, Feb. 2012.

22. R. Chandra, P. Bahl, *“MultiNet: Connecting to Multiple IEEE 802.11 Network Using a Single Wireless Card,”* IEEE INFOCOM, pp. 882-893, Hong Kong, Mar. 2004.

23. SAFECOM Program, *“Public Safety Statement of Requirements for Communications & Interoperability,”* the US Dept. of Homeland Security; http://www.safecomprogram.gov/library/lists/library/DispForm.aspx?ID=302, Jan. 2014.