Vol.2013-MBL-67 No.3
Vol.2013-CDS-8 No.3
2013/9/12

On-site Configuration of Wireless Multihop Access Networks
無線マルチホップアクセスネットワークのオンサイトの構成

Quang Tran Minh[(1)(2)], Kien Nguyen[(1)], Shigeki Yamada[(1)]
{quangtran, kienng, shigeki}@nii.ac.jp

Disasters may destroy everything including communications infrastructures isolating people in the disaster-stricken areas. Recovery of these infrastructures is often prolonged which is not suitable for disastrous fast-responses. This work proposes practical deployments of on-site configured access networks for disaster recovery. Although infrastructures are definitely damaged right after the occurrence of disasters, battery-based mobile devices (smart phones, laptops, tablet PCs) still work for some extended times. These mobile devices automatically change their roles working in both common station mode and access point mode to establish multihop access networks. These networks are extended until still alive Internet gateways (IGWs) are reached providing Internet access to the victims. The proposed scheme requires no further equipments except commodity mobile devices which are ubiquitously available.

地震や津波などの災害はすべてを破壊し、通信も途絶して人々を孤立させてしまいます。このため、情報通信ネットワークは災害からすぐに復旧して再構築されるようにすることが重要です。この研究では、被災地で人手を要せずに、すぐに構築できる災害復旧用アクセスネットワーク技術を提案しています。具体的には、情報通信ネットワークの一部が破壊されても、被災地にあるモバイル端末（スマートフォン、ラップトップ PC、タブレット端末等）を、生き残っているネットワークの端までマルチホップで接続することによって、被災地の人々が被災直後からインターネットを自由に使えるようにすることを目指しています。

1. Introduction

Natural disasters such as earthquake, hurricane, flood, cyclone, fire, volcano eruption turmoil human activity, disconnect communication services. Failure in communications and information exchange causes further heart-breaking crisis to human being [1]. Recent tragic disasters, such as the Great East-Japan Earthquake (Mar, 2011) [2], show limitations of current communication technologies. Disasters destroyed hundreds of wireless base stations (BSs), disconnected thousands of kilometers of cables, flooded millions of buildings and offices, isolated people in the afflicted areas. Recovery of these infrastructures, however, is often complicated and prolonged due to extensive damage and lack of experiences about the situations. Therefore, **strategic approaches whereby resilient wireless access networks are quickly established using on-site users' devices** are very important for **crisis mitigation and disaster recovery**.

The first 72-hour after an emergency is the "golden time" [3] since chance of saving lives significantly degrades after this period. As a result, communication networks should be recovered as soon as possible, providing connection means for safety information exchanging. Unfortunately, as reported by NTT East, it needed around 2 months for recovering their common services which had been destroyed by the Mar. 2011 Tohoku earthquake [2]. Obviously, paying long time for recovery communication infrastructures is impractical for first disaster responses. Instead, key-points on communication infrastructures should be recovered first, while on-site configured wireless access networks are established on-demand to provide short-term Internet connection to the victims.

This paper proposes a novel approach to resilient access networks for disaster recovery. "Resilience" can be interpreted as the ability of providing and maintaining an acceptable level of services in the face of various faults [4], [5]. More concretely, the requirements for a resilient access network as well as the resilience metric will be thoroughly discussed. According to those criteria, a novel concept namely the wireless multihop virtualization is proposed. Based on this concept, an effective on-site configured wireless multihop access network approach is devised. As a result, users/victims in the disaster areas can connect to the Internet through the proposed access networks transparently (without any difficulty) as if they are connected to the common access points (APs) in conventional wifi networks.

The rest of the paper is organized as follows: After reviewing current technologies for disaster recovery access networks in Section II, essential requirements for resilient disaster recovery access networks are clarified in Section III. The proposed wireless multihop access network will be described in Section IV. Section V analyzes the feasibility and the scalability of the proposed approach through experimental evaluations. Section VI concludes the paper followed by future work directions.

2. Related Work

Mobile carriers (e.g. KDDI, NTT,…) are pursuing to construct more robust technologies such as 3G, WiMAX, LTE [6], [7], or even satellite [8]. These technologies are powerful in terms of coverage, performance and serving capacity. However, these technologies are vulnerable to disasters due to their complicated power supply and antenna systems. It takes long time and a lot of

†1 National Institute of Informatics, Tokyo, Japan
†2 Hochiminh City University of Technology, Vietnam

money to recover such systems if they are damaged or malfunctioned by disasters.

Wireless access networks including mobile ad-hoc network (MANET) [9], wireless mesh network (WMN) [10], disruption/delay tolerant network – DTN [11], [12] are theoretically suitable for severe disrupted environments such as in large-scale disasters. However, these technologies have not yet been commercialized nor actively supported by mobile carriers. One of the reasons is that access networks may not be good business models. Therefore, realizing access networks retains many research challenges.

The conventional MANET exposes its disadvantages in performance (e.g. through put, packet loss, delay,…) in large-scale multi-hop communications [13]. It is reported that conventional MANET properly works only under a modest number of hops, namely smaller than 5. When the number of hops becomes larger, network performance significantly declines revealing infeasibility in real-world applications. In addition, network auto-configuration software (NAS) including routing protocols such as AODV [14], OLRS [15], etc., must be installed in each mobile node (MN) in advance to setup the MANETs. In some cases, multiple network interface cards (NICs) are required for setting up multihop communications. These requirements could not be satisfied in the actual disaster recovery situations.

Wireless mesh network (WMN) is a special type of wireless ad-hoc network designed for large-scale outdoor communications which is suitable for disaster recovery [10]. It requires, however, mesh routers (MRs) to be deployed in advance at optimal fixed locations. This requirement cannot be satisfied in real disaster recovery since nobody knows where and when a disaster may occur. Meanwhile, it is impossible to install WMNs at every location. Several researches have proposed practical approaches by which WMNs can be setup quickly and on-demand when they are needed. However, in some cases people cannot reach the necessary locations in disaster areas.

A series of studies from Niigata University proposed the so-called SkyMesh [16] which is a WMN on the sky for disaster recovery. In this work, MRs are attached on commercial balloons. The merit of the SkyMesh is that since the WMN is deployed on the sky, line-of-sight (LOS) between MRs can be easily achieved and transmission range is extended. It showed that the communication range between balloons is as large as 500m [16]. However, the SkyMesh is also stuck in the inherent issues rooted from the MWN technology: (a) the network must be established in advance at places where constructors can reach; (b) special devices like MRs and supplement equipments such as balloons in SkyMesh, etc., are required; and (c) it requires lots of manpower for real deployments. These requirements are unlikely to be satisfied in the actual disaster recovery.

Another drawback revealed from MANET and WMN is that both of them require the availability of end-to-end (E2E) communication paths at any time. If a node moves out the transmission range of its counterpart, data will be dropped. Delay/disruption tolerance network (DTN) [11], [12] does not require E2E paths by providing in-network storage mechanisms. As a result, communications can tolerate with longer disconnections. Theoretically, DTN is more robust and flexibly adaptable to severe disrupted environments such as natural disasters. Unfortunately, DTN has not matured enough to be applied in real-world applications.

Our work is completely different compared to the aforementioned technologies. In the proposed approach, multihop access networks can be established on-demand using on-site commodity mobile devices (without any special equipment).

3. Resilience Requirement

Obviously, people cannot wait for the backbone networks to be recovered, which may take several weeks, to conduct disaster responses/recoveries. Therefore, wireless access network is useful for short term fixing of Internet disconnection. To that end, wireless access networks must be easily setup using on-site commodity mobile devices (laptops, tablet PCs, smart phones,...). More concretely, ordinary users/victims in the disaster areas can transparently connect to the Internet, through the proposed networks, as easy as they are connecting to the conventional APs. This section clarifies requirements as well as evaluation metrics for a resilient wireless access network.

3.1 Requirements

The US Department of Homeland Security's SAFECOM [17] program has issued a Statement of Requirements (SoR) for public safety wireless communication as follows:

- Integration services including voice and data communications
- Use of commercial off-the-shelf devices/equipments
- Support for mobility
- Security (privacy and access control)
- Immediate on-scene access
- Real-time information sharing
- Scalability

TABLE I. REQUIREMENTS FOR RESILIENT DRANS

Requirement	Description
(R1) Connectivity	Victims in the disaster-stricken area can connect to the Internet
(R2) On-site establishment	The network is setup on-site using commodity mobile devices
(R3) Easy to configure	No difficulty for ordinary users to setup the network
(R4) Scalability	The network should be able to scale well to cover a large area
(R5) No specific hardware	Only commodity mobile devices are needed
(R6) Software downloadable	The network configuration software (NAS) can be download on-demand

In this work, this SoR has been clarified considering fundamental feasibilities of the desired networks for disaster recovery. Essential requirements for resilient disaster recovery

access networks (DRANs) are summarized in Table I and described as follows:

Among the requirements presented in Table I, *connectivity* is the most important one. Obviously, right after a disaster occurs users need to connect to the Internet for updating evacuation instructions as well as sharing their safety status to their families. Common web-based applications such as web-mail, common websites, etc., must be available for the users. Metrics for evaluating the connectivity resilience of a disaster recovery access network will be presented in the next sub-section. Other requirements such as (R2) on-site configuration, (R3) easy to be configured, (R4) scalability, (R5) no requirement for special/additional hardware, and (R6) software downloadable are the fundamental considerations for the proposed approach.

3.2 Resilience metric

As mentioned before, *connectivity* is the most important factor that represents the resilience of a disaster recovery network. The connectivity can be represented by *availability* and *reliability*. Availability is the *readiness* of the system when it is required. Reliability is the ability of the system to *remain operable* for a specific period of time. Obviously, these concepts are so general thus they need to be evaluated by a quantified metric.

The basic measures of the system dependability (i.e. availability and reliability) are the *mean time to failure* (MTTF) and the *mean time to repair* (MTTR) [4]. The MTTF is the expected value of the *failure density function* while the MTTR is the expected values of the r*epair density function*. In order to define the MTTF, we need to define the *"failure"* which may be varied from different types of applications. As mentioned before, the victims in a disaster need to access a web-site for checking evacuation information or sending an email. Therefore, failures in http connections are taken into consideration. More concretely, the http-based failure can be defined as follows

$$Failure = 1\_if\_\begin{bmatrix} network\_complete\_disconnection \\ RT > http\_timeout \end{bmatrix} \quad (1)$$

Users cannot get the website's content if the network is completely disconnected or the webpage response time, denoted as RT in equation (1), is larger than the http default timeout which is set to 120s in this work. The MTTR is the average time needed to repair such a disconnection.

The availability, denoted as *A*, scan be quantified in equation (2)

$$A = \frac{MTTF}{MTTF + MTTR} \quad (2)$$

The reliability, denoted as *R(t)*, is the probability that a system works without fail in a specific period of time *t*. *R(t)* is defined in equation (3)

$$R(t) = \Pr(work\_properly\_in[0,t]) = 1 - Q(t) \quad (3)$$

In this equation, *Q(t)* is the failure *cumulative distribution function* (CDF) during a time period *t*. The value of *t* can be defined as a period of time that is necessary to complete a task in disaster situations. For example, less than 5 minutes is the time required for sending a short email notifying about the safety status.

At this stage, the requirements and quantified criteria for a resilient disaster recovery access network (DRAN) have been clarified. The next section describes the proposed approach to on-site auto-configuration of DRANs using only commodity mobile devices.

4. Proposed Approach

4.1 Wireless multihop virtualization

In order to realize multihop communication, conventional access networks like MANET require complicated routing protocols such as AODV [14], OLSR [15] to be installed in each mobile device in advance. This requirement is impractical in actual disaster recovery. In order to overcome this difficulty, we proposed the concept of **multihop virtualization** whereby multihop is considered as a chain of single hops. Concretely, if single-hop connections can be chained, multihop communication is established. In this approach, any intermediate node must work in both modes, namely the common station (STA) mode to connect to the actual access point (AP) and the access point mode to provide connection means to the nearby nodes. Accordingly, after connecting to the network, a node transforms itself into a virtual access point (VAP) providing connection means to the nearby nodes.

Obviously, since a node works in both modes concurrently, multiple network interface cards (NICs) are needed. However, this requirement could not be satisfied by commodity mobile devices. In this work, this issue is resolved by utilizing the wireless virtualization (WV) [18] mechanism. The WV abstracts a single NIC into two virtual NICs: one works as a common STA, and the other serves as a VAP. Consequently, instead of installing additional hardware (i.e. physical NIC) into a MN, the issue can be solved by a software solution. The network auto-configuration software (NAS) at each MN will conduct following tasks:

- Transforms a single physical NIC into two virtual NICs, namely NIC_0 and NIC_1

- Changes the MAC addresses of the two abstracted NICs to assure that their MAC addresses are not conflict

- Associates and connects to the nearby AP using NIC_0

- Transforms the MN into a VAP using NIC_1. Network address translation (NAT) functionality and the dynamic host configuration protocol (DHCP) server will be installed in the VAP

An emerging issue is that how to install the NAS in each MN when the network has not been established. It could not assume that the NAS is installed in each MN in advance as

assumed in the conventional MANET. This difficulty will be addressed in the next sub-section.

4.2 Network configuration

In order to overcome the aforementioned issue, the proposed network is initiated by the nodes which are close to a still alive Internet gateway (IGW) as shown in Fig. 1. Node 1 initiates the network configuration by simply associating to the IGW. The IGW assigns IP address to node 1 enabling it to access to the Internet. Once node 1 connects to the Internet (via the IGW) and open the Internet browser (e.g. IE, Firefox, Chrome,...), a special function installed on the IGW directs the connection to a special website. The user will be asked to click on a particular button which fires a trigger forcing the node to download the NAS from the Internet. When the NAS is completely downloaded and installed in the node, the node can access to any website as usual.

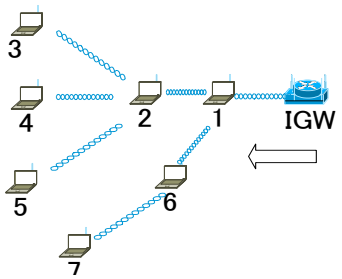

Figure 1. Multihop wireless access network based on the multihop virtualization concept

The previously installed NAS transforms node 1 into a VAP which serves as a virtual IGW providing Internet connection means to the nearby nodes (e.g. nodes 2 and 6). This procedure is iterated when a node joins the network. Consequently, the network is incrementally extended as a tree-based network by contributions of users at disaster areas.

5. Evaluation

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

5.1 Evaluation environment

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

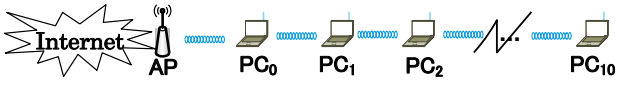

Figure 2. A tandem network with 11 PCs

Several scenarios of the proposed wireless multihup access network were established using 11 laptop PCs. Two representative network topologies have been created: (a) a tandem network, and (b) a tree-based network as shown in Fig. 2 and Fig. 3, respectively. The distance between any pair of nodes in these two representative networks is 50m.

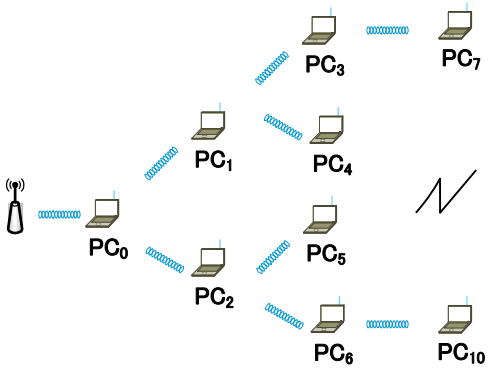

Figure 3. A tree-based access network with 11 PCs

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 wireless NIC at each mobile node is abstracted into 2 virtual NICs which are assigned appropriate IP addresses, default IGWs, etc. Table II shows an example observed from the tandem network (Fig. 2). As a result, each node can smoothly access to the Internet.

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

Node	STA IP Address *(for vwlan0)*	VAP IP Address *(for vwlan1)*
PC0	136.187.82.88	192.168.50.1 (default IGW for PC1)
PC1	192.168.50.50	192.168.124.1 (default IGW for PC2)
PC2	192.168.124.50	192.168.97.1
PC3	192.168.97.50	192.168.133.1
PC4	192.168.133.50	192.168.59.1
...		

Table III shows the services that we have checked at each node. As shown, both the networks work well with text-based webpage surfing and voice communication services. When the number of hops is large, such as 8 hops or larger in the tandem network, delay occurs revealing some jolts for video streams and video chat using Skype. However, the delay is acceptable, especially in the case of disaster recovery.

For further evaluating of the network performance, round trip time (RTT) latency and jitter in multihop communications were recorded. As shown in Fig. 4, 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.

TABLE III. EVALUATED APPLICATIONS AT DIFFERENT CONDITIONS (NETWORK TOPOLOGIES AND NUMBER OF HOPS)

Application	Capacity	
	Tree-based network	Tandem network
Text-based website	Smoothly	Smoothly
Online video (Youtube)	Smoothly	Smoothly until PC7. From PC8, acceptable delay occurs
Voice IP service and video communications (Skype)	Smoothly	Smoothly with voice communication. From PC8, video communications reveals some jolts

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 5 shows that the jitter increases when the number of hops increases. However, this increment is still acceptable. Moreover, as presented in Table III, as long as the number of hops is around 7 to 8 hops, user can experience smooth VoIP calls using Skype. This result reveals the feasibility of VoIP services in multihop communications deployed in our proposed approach.

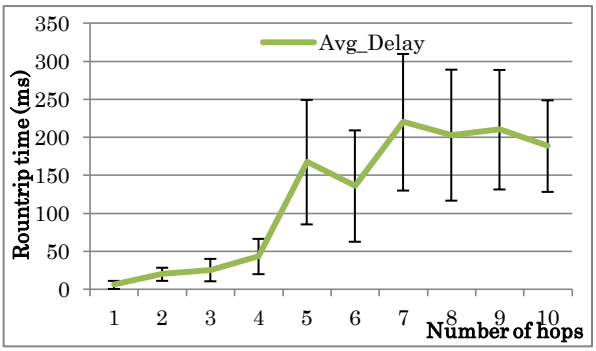

Figure 4. Round trip time latency in multihop communications

As a brief conclusion, the experiments, supported by tables II, III, and Figures 4, 5, confirm the feasibility as well as the effectiveness of the proposed approach. All requirements presented in section III have been satisfied. Concretely, connectivity (R1), on-site configuration (R2), easily to configure (R3), scalability (R4 - large number of hops, different topologies such as tree-based and tandem networks), no additional NIC (R5) and the ability of software auto-download (R6) have been satisfied by the proposed approach.

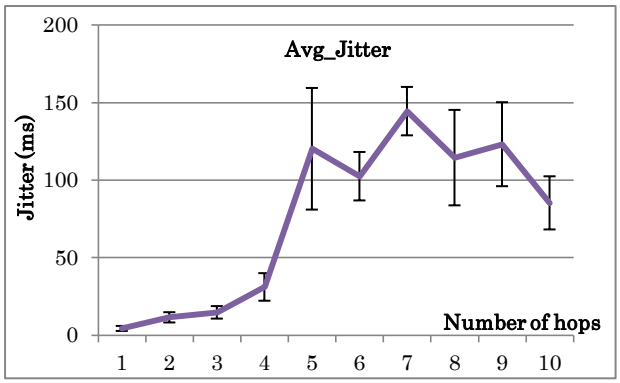

Figure 5. Jitter in the proposed multihop access network

6. Concluding Remarks

In this research a new concept, namely *multihop virtualization* has been proposed. Based on this concept, tree-based wireless access networks can be established on-site using commodity mobile devices. The network is completely transparent to users meaning that the ordinary users can easily connect to the Internet through the proposed network as if they are connected to the conventional access points.

The real field experiments show the feasibility as well as the scalability of the proposed approach. Both the tandem network and the tree-based network have been successfully created with a large number of users (nodes) and a large number of hops.

However, the tree-based nature of the network also reveals essential weakness. For example, the network is sensitive with failures at root nodes. If a root node dies, all the nodes in its sub-tree could not connect to the Internet. We are planning to investigate mechanism to improve the robustness of the network. One of the solutions is that if any up-link node dies, the child nodes try to bypass the failed node or find out alternative path to the destination (i.e. to the IGW). Another solution is to utilize the availability of multiple IGWs. That means multiple tree-based networks can be created. As a result, a particular node can connect to the Internet via several paths.

In addition to improving the robustness of the proposed approach, more real-field experiments are needed to confirm the feasibility, the effectiveness as well as the scalability of the proposed scheme.

Acknowledgments: *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).*

Reference

1) D. Endo, k. Sugita, *"A study on Design of Disaster Information - A proposal of Coordinate System for Supply and Demand on Disaster Recovery,"* P2P, Parallel, Grid, Cloud and Internet Computing, pp.303-306, Barcelona, Spain, Oct. 2011.

2) Tohoku Earthquake and Tsunami (Mar. 2011) *"http://en.wikipedia.org/wiki/2011_T%C5%8Dhoku_earthquake_and_tsunami,"* Apr. 2013.

3) Y. N. Lien, T. C. Tsai, H. C. Jang, *"A MANET Based Emergency Communication and Information System for Catastrophic Natural Disaster,"* The 2nd International Workshop on Specialized Ad Hoc Networks and Systems, pp.412-417, Quebec, Canada, Jun. 2009.

4) 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.

5) T.M. Quang, K. Nguyen, S. Yamada, *"Virtualized Multihop Access Networks for Disaster Recovery,"* The 5th International Workshop on Hot Topics in Mesh Networking (IEEE HOTMESH 2013) in conjunction with IEEE WoWMoM 2013, 4-7 June 2013, Madrid, Spain (flash disk edition).

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, *"Proposal of Never Die Network with the Combination of Cognitive Wireless Network and Satellite System,"* The 13th International Conference on Network-Based Information Systems (NBiS2010), pp. 365-370, Gifu, Japan, Sep. 2010.

9) Y. Shibata, H. Yuze, T. Hoshikawa, K. Takahata, N. Sawano *"Large Scale Distributed Disaster Information System based on MANET and Overlay Network,"* The 27th International Conference on Distributed Computing Systems Workshop, Toronto, Canada, Jun. 2007 (CD edition).

10) M. Portmann, and A. A. Pirzada, *"Wireless Mesh Networks for Public Safety and Crisis Management Applications,"* IEEE Internet Computing, Vol 12. No.1, pp.18-25, 2008.

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

13) N. C. Ping, L. C. Soung, *"Throughput Analysis of IEEE 802.11 Multi-hop Ad hoc Network,"* IEEE/ACM Transactions on Networking, Vol. 15, No. 2, pp.309-322, Apr. 2007.

14) E. C. Perkins, B. M. E. Royer, *"Ad-hoc on-demand distance vector routing,"* Mobile Computing Systems and Applications, pp.90-100, New Orleans, USA., Feb. 1999.

15) R. Stephane, B. Farid, L. Damien, S. Laurent, *"Overview and optimization of flooding techniques in OLSR," WoWMoM'11*, pp.1-7, Lucca Italy, Jun. 2011.

16) H. Suzuki, Y. Kaneko, K. Mase, S. Yamazaki, H. Makino, *"An Ad Hoc Network in the Sky, SKYMESH, for Large-scale Disaster Recovery,"* the 64th Vehicular Technology Conference, pp.1-5, Quebec, Canada, Sep. 2006.

17) SAFECOM Program, *"Public Safety Statement of Requirements for Communications & Interoperability,"* US Dept. of Homeland Security;http://www.safecomprogram.gov/library/lists/library/DispForm.aspx?ID=302, Accessed Apr. 2013.

18) 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.