On-the-Fly Establishment of Multihop Wireless Access Networks for Disaster Recovery

Quang Tran Minh, Kien Nguyen, Cristian Borcea, and Shigeki Yamada

ABSTRACT

This article proposes a novel approach to on-the-fly establishment of multihop wireless access networks (OEMAN) for disaster response. OEMAN extends Internet connectivity from surviving access points to disaster victims using their own mobile devices. OEMAN is set up on demand using wireless virtualization to create virtual access points on mobile devices. Virtual access points greedily form a tree-based topology, configured automatically for naming and addressing, which is then used to provide multihop wireless Internet access to users. Ordinary users can easily connect to the Internet through OEMAN as if they are connected through conventional access points. After connecting, users naturally contribute to the network extension, realizing the self-supporting capability of a disaster's local communities. The proposed scheme establishes a wireless access network quickly, which is essential in emergency relief situations. Furthermore, OEMAN is transparent to users and cost effective as it does not require additional hardware. Experimental evaluations on top of our preliminary prototype over Windows-based laptops confirm OEMAN's feasibility and its effectiveness for multihop paths of up to seven hops, and standard Internet services such as audio and video streaming.

INTRODUCTION

The world has recently seen catastrophic natural disasters that have caused the loss of hundreds of thousands of lives and destroyed millions of homes. Sadly, failures in communication services lead to heartbreaking human crises. Recent tragic disasters, such as the Great East Japan Earthquake in March 2011 (Tohoku Earthquake) and the Haiyan typhoon in November 2013 in the Philippines show the limitations of current communication technologies.

In disasters, safety information including the number of victims, their location, and their safety status (e.g., injured) is essential for rescue and crisis mitigation. It is necessary for people to access the Internet and share their safety status with rescuers as soon as possible. Our experience from analyzing disaster recovery efforts suggests that the first 24 hours represent the "golden time" for emergency relief. Nevertheless, the recovery of network infrastructure is often complicated and prolonged.

While a large part of a wireless access network is destroyed in disaster regions, there are always a number of still-alive Internet connected access points (APs). Unfortunately, these APs are generally placed around the disaster area, and are not easily accessible to most of the victims. This work aims to quickly extend Internet connectivity from these APs to victims by leveraging their mobile devices to form on-the-fly multihop wireless access networks that effectively help in saving lives and mitigating losses. To achieve this goal, these networks must be established quickly and transparently to users, as victims cannot be expected to perform setup operations or have certain multihop protocols installed on their devices. Practically, two essential challenges must be overcome:

- Setting up multihop access networks that leverage users' mobile devices without requiring any action from the victims
- Configuring addressing, naming, and routing in these networks in a simple and automatic way

This article proposes a novel approach to address the above challenges, on-the-fly establishment of multihop wireless access networks (OEMAN), for quick disaster response. OEMAN has three novel contributions:

- Turn commodity mobile devices into virtual access points (VAPs) using wireless virtualization technology.
- Extend Internet connectivity by greedily building tree-based network topologies of VAPs.
- Automatically configure IP addresses and Domain Name Service (DNS) resolution in the tree-based topology for smooth Internet connectivity.

OEMAN works in an iterative fashion. First, nearby users connect to surviving APs, and their devices are instructed to download the necessary

Quang Tran Minh is with the National Institute of Informatics and Hochiminh City University of Technology.

Kien Nguyen and Shigeki Yamada are with the National Institute of Informatics.

Cristian Borcea is with the New Jersey Institute of Technology.

0163-6804/14/$25.00 © 2014 IEEE

software for network establishment. Then these devices are configured as VAPs and start serving dual purposes: they act as Internet clients for their owners, and as Internet providers to other users who are not covered by the original AP. The access network is extended using the same two steps as more users connect to the network forming a tree-based topology, which is subsequently auto-configured. We built a preliminary OEMAN prototype on Windows-based laptops and tested it in networks with paths of up to seven hops. The experimental results demonstrate that despite the overhead introduced by wireless virtualization, the latency and throughput are good enough to support standard Internet services such as Skype and YouTube video streaming.

Review of Wireless Network Solutions for Disaster Recovery

Research on wireless multihop ad hoc networks such as wireless backhaul mesh networks [1], mobile ad hoc networks (MANETs) [2], and delay/disruption tolerant networks (DTNs) [3] has been an active research field in the last decade. Although these approaches have potential, there are still fundamental barriers that hinder their realization in disaster recovery. The complexity of network configuration such as complicated ID management, dedicated multihop routing protocols, and meticulous mode changing tasks (e.g., from infrastructure mode to ad hoc mode) prevent these technologies from being easily deployable. Our approach provides a solution transparent to users that can quickly be deployed with today's technologies.

Camara *et al.* [4] proposed a virtual access point (VAP) approach implemented on mobile nodes to extend the coverage of real APs. However, this approach is completely different from our work: the VAPs work as store-carry-forward nodes in a DTN to opportunistically improve the delivery rate. Consequently, this work focused on solving issues of caching, rebroadcasting, and switching the mode of a mobile node (i.e., common or VAP mode). In contrast, our focus is on simplifying network configuration, the routing protocol, IP address management, and DNS resolution to quickly bring Internet connectivity to disaster victims. The VAPs in our work serve as real APs providing Internet access in their vicinity.

The emerging IEEE 802.11s standard [5] provides a new framework for multihop mesh networks, reducing the network establishment difficulties. From the network structure point of view, this approach is similar to ours. However, IEEE 802.11s-compliant network interface cards (NICs) are required for the deployment of such infrastructure-based mesh networks, and the number of nodes in an IEEE 802.11s mesh network is limited to 32. In contrast, OEMAN establishes a multihop access network using commodity WiFi-equipped devices that are ubiquitous, and the network can be extended to an arbitrary number of nodes.

WiFi Direct [6] is closely related to our proposal, whereby each node can work in both station (i.e., client) and software-based AP modes. This solution groups nearby nodes together, with one node serving as a group owner to manage the communication within the group. The Internet connection is shared from the owner to the group members. The feasibility of multihop-based Internet connection sharing using WiFi Direct has not been addressed so far, but we are investigating it as an alternative to our current wireless virtualization-based OEMAN.

On-demand deployment of WiFi APs or cellular base stations that connect to the Internet using satellite communication and are potentially carried by emergency vehicles is a common solution in disaster recovery [7, 8]. However, this solution is expensive, and it may take a substantial amount of time before emergency teams reach some disaster areas. Roofnet [9] is a mesh network solution to extend the coverage of wireless community networks by encouraging volunteers to deploy Roofnet nodes. Even though the deployment of Rooftnet nodes is simple given the Roofnet kits (PC, antenna, and necessary devices) with pre-installed Roofnet software, this approach still suffers from difficulties such as requirements of software pre-installation, dedicated hardware, and a complex routing protocol. These issues hinder its realization for quick emergency response. Our work complements these solutions with a free and fast approach to extend Internet connectivity to disconnected victims, leveraging their mobile devices.

To summarize, the solution proposed in this article is different from the aforementioned works as it proposes a novel scheme for on-the-fly establishment of multihop wireless access networks for disaster recovery. OEMAN effectively brings Internet connectivity to disaster victims by using their own devices, which are always available on site.

OEMAN Design

Illustration of the Main Ideas

Figure 1 shows, at a high level, how a network topology is formed to extend Internet connectivity to victims who have been left disconnected. In Fig. 1a, the main components (routers, base stations, etc.) of the infrastructure-based network have been destroyed, disabling Internet access for any user in the disaster-stricken area. At that moment, the devices that are close to the surviving AP, such as MN1, try to associate to this AP (step 1, Fig. 1b). The AP initiates OEMAN by asking MN1 to download the necessary software (step 2), which transforms MN1 into a VAP, thus extending the Internet access to farther nodes (step 3). MN1 works as a common AP for nearby nodes. Consequently, the OEMAN configuration software will be transferred and installed to any node that associates with a VAP. As a result, every intermediate mobile node, when connected, becomes a VAP providing Internet connectivity in its vicinity, as shown in Fig. 1c. As on-site commodity mobile devices are utilized to set up on-demand wireless access networks, OEMAN is not only cost effective, but also fast, and spreads Internet connectivity to

The complexity of network configuration such as complicated ID management, dedicated multihop routing protocols, and meticulous mode changing tasks prevent these technologies from being easily deployable. Our approach provides a solution transparent to users that can quickly be deployed with today's technologies.

large areas, satisfying the critical requirement of quick emergency response.

Design Features

A network controller managed by an emergency operation center initiates the OEMAN establishment process when a disaster occurs by launching a command that puts all the reachable APs into *emergency relief state* (ERS). Any node that connects to an AP in ERS is forced to download the disaster recovery network auto-configuration software (DrNAS) to transform itself into a VAP, as illustrated in step 2 of Fig. 1b. At the same time, ERS is activated at the VAP, forcing the associated nodes to download the DrNAS and transform themselves into VAPs to extend the network; thus, Internet access is extended to farther victims.

DrNAS is the heart of OEMAN and consists of three essential functions:

1. Transform a commodity MN into an OEMAN node that can work in both the STA (e.g., client) and VAP modes concurrently to seamlessly connect different networks supporting multihop Internet communication.
2. Provide a greedy method to create a tree-based topology to simplify the routing in the multihop network.
3. Manage IP address allocation and duplication avoidance, as well as DNS resolution, in an automatic fashion.

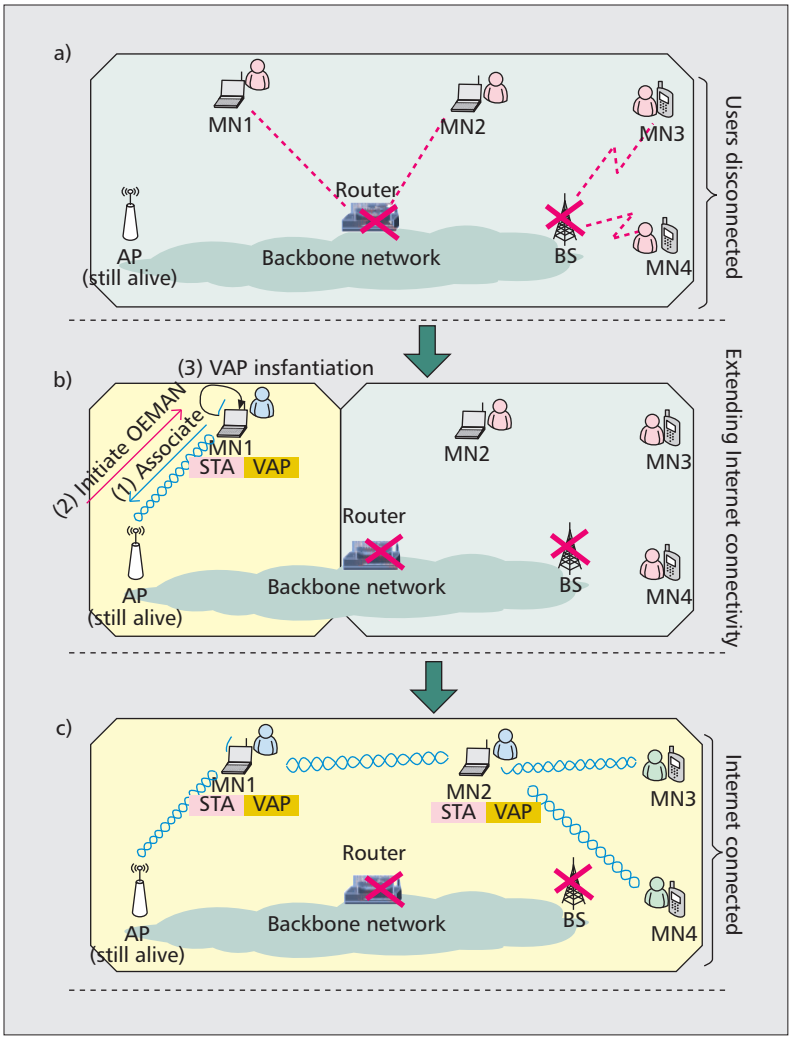

Figure 1. OEMAN establishment: a) Most of the wireless infrastructure has failed or is disconnected from the Internet; b) extending the Internet to victims; c) multihop wireless access network for Internet connectivity.

Wireless virtualization: Each node should maintain two modes, STA and VAP, to connect to two networks concurrently. Accordingly, the STA mode connects the MN to the upstream AP/VAP for Internet access, while the VAP mode shares this Internet connection in the vicinity. To provide this functionality, one solution is to switch between these modes using a single built-in wireless interface. However, the switchover time is long enough to significantly degrade network performance, reducing the network coverage in multihop communication. Another solution is to have multiple wireless interfaces at each node, but this is not a realistic requirement. To solve this issue, OEMAN leverages wireless virtualization [10] to abstract a single physical wireless interface into two logical interfaces: one is used for STA (WIF_STA), and the other for VAP (WIF_VAP). In order to transform a commodity MN into an OEMAN VAP, we use a software-based AP approach [11].

Simple routing in tree-based topology: Routing is one of the challenging issues in multihop communications. For example, proactive routing overhead in MANETs can be very large because each node must be aware of all the other nodes. Meanwhile, the route discovery and maintenance processes have high overhead in the reactive counterparts. Our approach is different as OEMAN greedily builds a tree topology (Fig. 1c), and the routing for Internet communication is done along this tree. Specifically, the routing is simplified to the minimum by utilizing *translated connection* (not routed connection) [12] supported by the network address translator (NAT) at each VAP. The NAT serves as an IP router, translating addresses for packets being forwarded between OEMAN nodes and Internet hosts. As a result, the routing overhead is minimal as nodes are not required to perform route discovery. This solution works because our goal is to offer Internet connectivity through the root (i.e., AP), not node-to-node communication. Hence, each node just needs to know the next connected node in its infrastructure-based network to forward the packets. For example, when MN4 (Fig. 1c) wants to connect to the Internet, it sends its packets to its associated VAP, MN2. In turn, MN2's VAP handles (using the NAT-ing mechanism) the packets to its STA for forwarding to the upstream VAP, MN1. Finally, the packets reach the actual AP where a traditional routing protocol is implemented to route the packets in the Internet. Note that communication is always initiated by mobiles in OEMAN. These mobiles are not directly reachable from the Internet as they use private IP addresses as described next.

Auto configuration: For Internet connectivity, IP address allocation and duplication avoidance as well as DNS resolution are needed. Each MN has two logical wireless interfaces; thus, each must be assigned an individual IP address.

WIF_STA's IP address is assigned by a DHCP server installed at the associated AP/VAP. Since the VAP on WIF_VAP serves as a network gateway for the associated nodes, WIF_VAP 's IP address is in the form of 192.168.*x*.1. Here, *x* is automatically computed from the MAC address of the physical WIF as shown below, thereby it is different from the third octet, *y*, of WIF_STA's IP. This procedure satisfies two essential criteria:

- Easily assigns IP addresses to the local network gateways
- Avoids addressing conflicts that occur when the two interfaces in the same node belong to the same subnet (192.168.*x*.0/24)

```
x = mod(y + Sum(digit in WIF's
MAC),252) + 2
```

Since each VAP implements its own DHCP server for assigning local/private IP addresses to clients in its network, NATs are needed at each VAP to communicate over the Internet. NATs support a simple layer 3 routing mechanism over the OEMAN tree topology by simply forwarding the packets to the next connected node. Concretely, for the upstream flows (from the node to the AP), the VAP of an intermediate node just handles the packets to its STA for forwarding to its associating VAP (on the upstream node). For the downstream flows (from the AP to the individual destination), the NAT at the VAP of a node identifies to which client the data should be forwarded. In addition, since each VAP serves as a default network gateway with DNS proxy service, it supports DNS resolution for the associated nodes. Accordingly, any leaf node just asks for DNS resolution by sending a DNS query to the default gateway, with intermediate nodes forwarding the query to their default gateways until they reach the AP and the query is finally resolved.

To summarize, the procedure that allows a common node to connect to an ERS VAP, get the DrNAS software, and transform itself into an ERS VAP is depicted Fig. 2. After associating (steps 1 and 2) with the surviving AP, MN1 is forced to download DrNAS from the AP (step 3). This software transforms MN1 into a VAP (step 4) using its second logical wireless interface, while the first logical interface works as a common client. MN1's VAP brings Internet connectivity to nearby nodes (step 5), such as MN2 and MN3. The IP addresses of these nodes are assigned by the DHCP server on MN1's VAP.

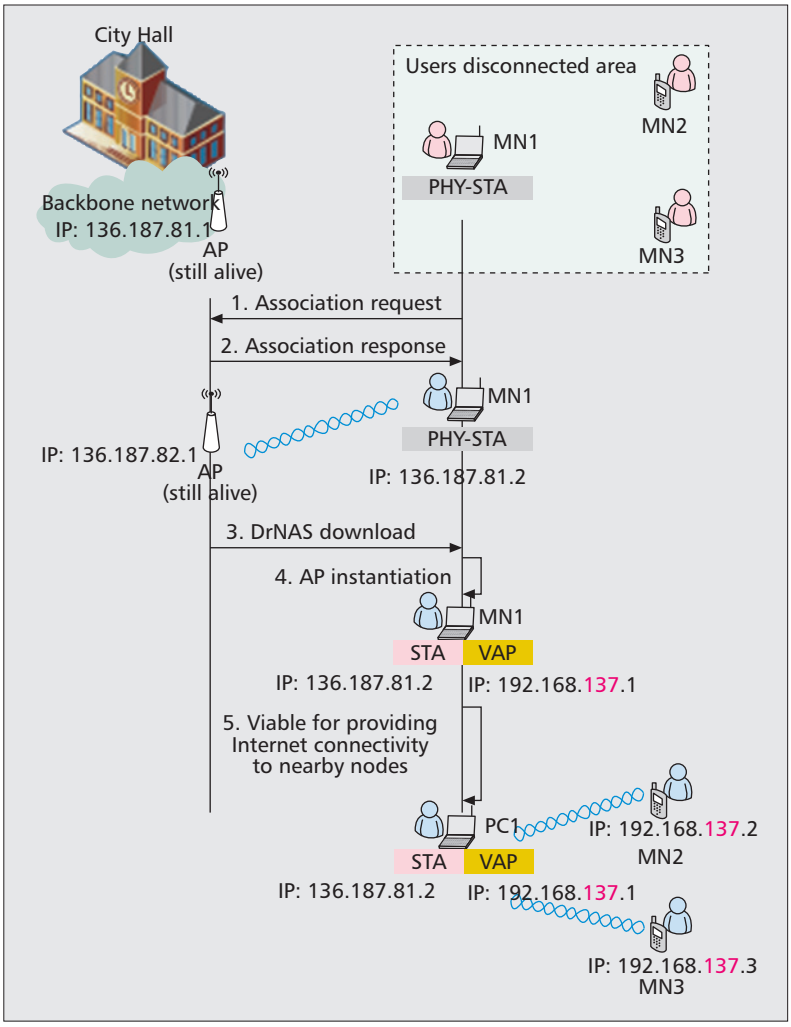

Figure 2. Procedure for DrNAS download and network configuration.

Preliminary Prototype

This section presents the preliminary prototyping of OEMAN using commodity Windows-based laptops. An experimental network topology is illustrated in Fig. 3. This tree-based topology demonstrates the novel features supported by OEMAN:

- Each intermediate node concurrently serves multiple clients.
- Multihop communication is supported (e.g., three hops from MN5 to the actual AP).

In our prototype, intermediate nodes with DrNAS deployment are ASUS U24A-PX3210 laptops with 4 Gbytes memory, corei5 2.5 GHz CPU, Atheros AR9002WB — 1NG WiFi Network Adapter, and Windows 7 OS.

The implementation details of the procedures to create the prototyping network in Fig. 3 are described, step by step, as follows.

1. **Wireless virtualization and VAP transformation:** The command (in administrator mode) that performs these two tasks is shown below. Here, <ssid> is the SSID of the newly set VAP, and <passPhrase> is the password used for associating with this VAP.

```
Netsh Wlan set hostedNetwork Mode=allow
SSID=<ssid>          Key=<passPhrase>
keyUsage=persistent
```

2. **Start the VAP functionality:** This task is achieved by the following command. After this command, the VAP can be seen by nearby nodes for association.

```
Nestsh Wlan start hostedNetwork
```

3 **Deploying the DHCP server and NAT on the established VAP:** Windows provides the Internet Connection Sharing (ICS) utility to share the Internet connection of a particu-

lar node. This utility includes DHCP, NAT, and DNS proxy services utilized for our purpose. ICS is used to share the current wireless connection at the primary logical interface (WIF_STA) with the secondary interface (WIF_VAP) at the newly built VAP. Figure 4 shows a screenshot at MN2 where its primary WIF has connected to the VAP named **disaster1** running at MN1, and ICS is used to share this connection to the secondary WIF for MN2's VAP, **disaster2**.

It should be noted that the IP address of the MN2's STA is assigned by the DHCP on the MN1's VAP. This IP address is in the form of 192.168.*y*.*z*, where *y* is the third octet in the IP address of MN1's VAP (192.168.*y*.1), and *z* is given by the DHCP server. The IP address of the MN2's VAP is automatically generated in the form of 192.168.*x*.1. As mentioned earlier, *x* and *y* must be different. Since Windows uses the default address 192.168.137.1 for the VAP's IP at every node, if a VAP has been created on MN1, MN2 cannot be transformed into a VAP. Consequently, the multihop communication network shown in Fig. 3 cannot be established. To solve this issue, the third octet *x* is computed using the mechanism discussed earlier and is stored in the **ScopeAddress** parameter in Windows' registry. Figure 3 also illustrates the IP address assignment to different interfaces (logical STA, VAP, and physical STA) at devices on the demonstrated network.

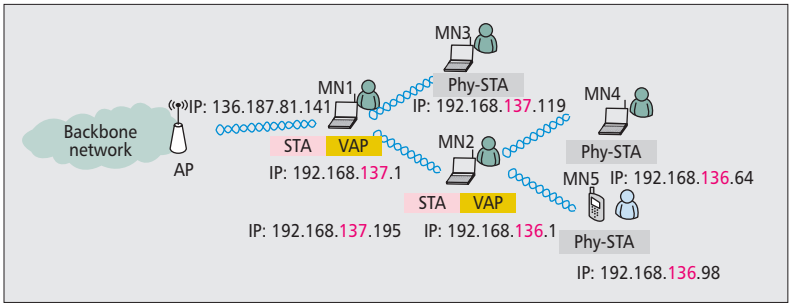

Figure 3. Demonstration of a tree-based multihop OEMAN.

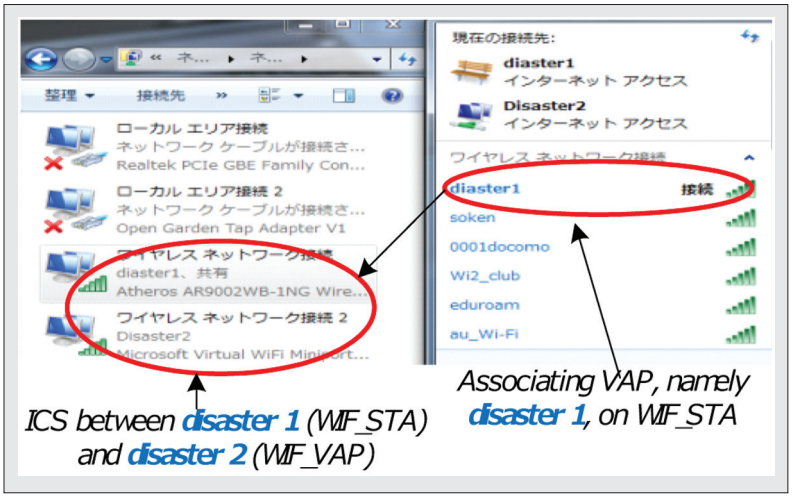

Figure 4. Internet connection sharing between the primary Internet connected WIF (disaster 1) and the secondary WIF (disaster 2).

Real-World Evaluation

The main purpose of this evaluation is to verify whether OEMAN works well to bring Internet connectivity to isolated people. Specifically, we evaluated network performance in terms of delay, jitter, and throughput for a multihop topology. In addition, actual Internet-based services such as voice chat on Skype and video streaming on YouTube have been verified.

Several field experiments have been conducted at Iwate Prefectural University, Japan. Iwate is a prefecture that was significantly affected by the Tohoku Earthquake. The network topology shown in Fig. 5 was created by connecting (one by one) laptops placed along the corridors of the campus buildings. Five nodes (MN0 to MN4) were deployed on the second floor, and three others (MN5 to MN7) were on the fourth floor. The distance between any pair of nodes was 50 m. MN0 was connected to the real AP, while MN*i* ($i = 1 \ldots 7$) was connected to the Internet via the deployed OEMAN. As can be observed in the figure, we created a line topology to experiment with the worst case scenario (i.e., longest multihop path). The WiFi technology used is IEEE 802.11b with transmission rate 11 Mb/s.

Figure 6a shows the average round-trip time (RTT) and the throughput between MNi ($i = 1;\ldots 7$) and MN0. We chose not to measure the performance across the Internet through the AP because our goal was to isolate the performance of the OEMAN network. Although the RTT has higher values when the number of hops increases, the RTT is still low, less than 250 ms even for the longest path. The throughput decreases with the number of hops, but it still reaches an acceptable value, 1.5 Mb/s, in the worst case. Since throughput degradation is slow after the first four hops, and its value is well above the speed of dial-up technology, which is acceptable for common web-based applications such as webmail and surfing, we conclude that OEMAN could achieve broad coverage. The results also lead us to infer that OEMAN's overhead (especially that of wireless virtualization) does not significantly impact the network delay and throughput. Similarly, the jitter increases with the number of hops. However, the worst jitter for the longest path is limited to around 140 ms. These network performance parameters are acceptable for smooth VoIP services and for web browsing.

In order to verify the ease of network configuration and the configuration time, an experiment was conducted using the first version of DrNAS, the multihop access network auto-configuration software (MHANS). MHANS was hosted on a website on the Internet. The first time an OEMAN user accesses to the Internet, she is directed to this website to download MHANS. Three time variables were evaluated and are shown in Fig. 6b: the time needed to establish Internet connectivity ($t1$), that is, from starting to associate with the upward AP/VAP until the user successfully loads the website hosting MHANS; the time to download MHANS ($t2$); and the time to install and initiate MHANS ($t3$). The total time (t) needed for a node to complete joining OEMAN and transforming into

a VAP increases with the number of hops since the download time, *t2*, increases. However, the total time *t* is less than 143 s, even in the worst case, which is quick enough for emergency response.

We also verified several Internet-based services: text-based web surfing, video streaming (YouTube), and text, voice, and video chat using Skype. These services worked smoothly even in the worst case scenario (i.e., video chat from MN7). These results reveal the feasibility as well as the effectiveness of OEMAN.

Discussion

As confirmed in the previous section, OEMAN is feasible and effective for quick disaster response. However, these results only show preliminary achievements. In order to make OEMAN more robust, we plan to address several issues:

1) **Handling mobility and node failure:** After a disaster, users commonly do not move fast and frequently. In this context, the current network establishment mechanism provided by OEMAN still works well. Nevertheless, in situations where nodes move faster or more frequently, or die because of battery shortage, maintenance mechanisms are needed for the tree-based topology. We plan to leverage work on tree maintenance in MANETs to develop such mechanisms [13].

2) **Load balancing:** Our current tree formation solution is greedy, which has the advantage of simplicity and low overhead. However, this solution may lead to imbalanced trees causing performance bottlenecks at nodes that are close to the root. Similarly, specific traffic patterns may lead to the same problem. Therefore, we will examine protocols that quickly detect unbalanced traffic and perform tree reconfiguration with minimal overhead. One solution is to extend the capability of VAP such that it can detect and compute the current traffic load. When a node is overloaded, it performs a handover operation by asking the appropriate clients to connect to alternative VAPs. The clients that have to move are selected based on the amount of data traffic they generate through this VAP. The advantage of this approach is twofold: it quickly reduces the load of heavy traffic nodes and minimizes the overhead of handovers.

3) **Multiple surviving APs:** Currently, OEMAN uses just one surviving AP, but in reality multiple APs could survive. In this case, we will study the trade-offs between dividing the nodes among individual APs (acting as tree roots) and letting the nodes connect to the Internet through multiple APs concurrently. The choice is between separate networks/trees and overlapping networks/trees. The first solution has lower overhead, but it may lack load balanc-

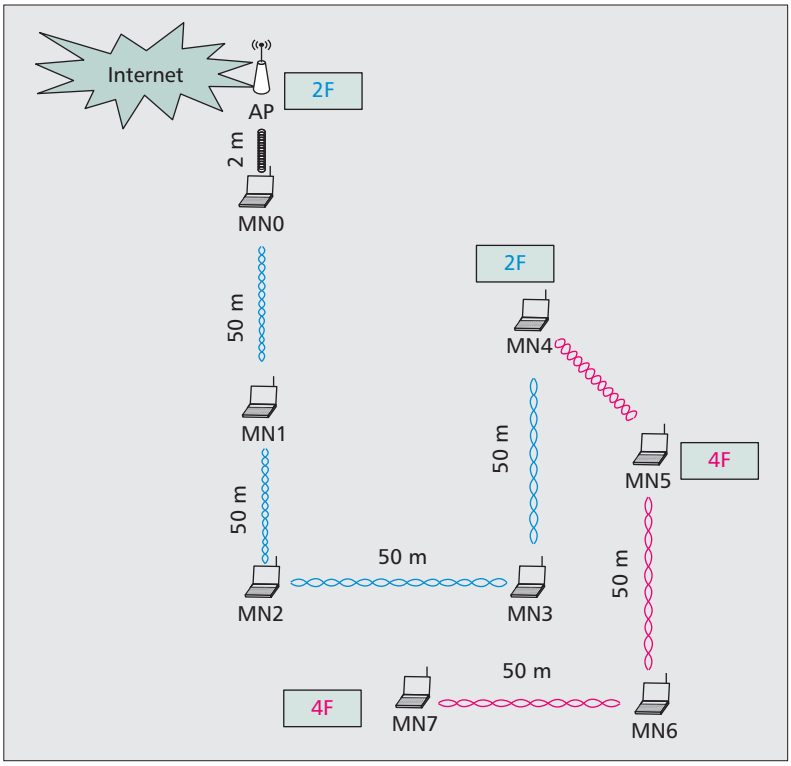

Figure 5. Real deployment of an eight-hop OEMAN network.

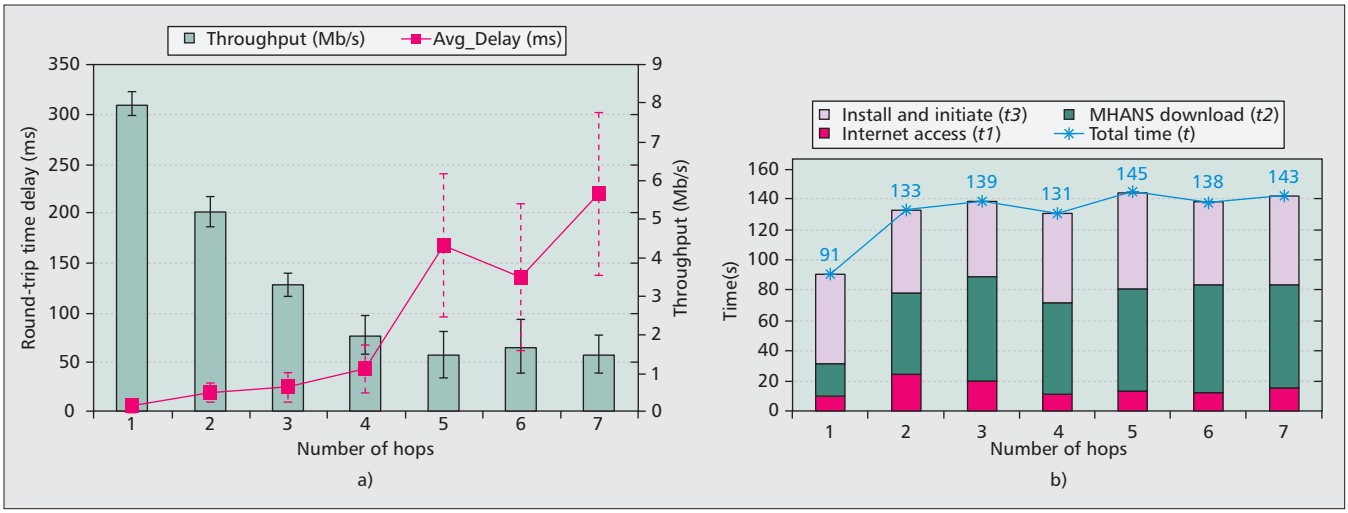

Figure 6. Network performance and the time needed to establish OEMAN: a) network performance: RTT and throughput; b) time needed for network configuration.

The main novelty of OEMAN is that Internet connectivity is moved closer to the victims by using the on-site mobile devices. This feature improves the self-supporting capability of local communities affected by disasters, which is very useful for emergency relief.

ing and higher availability features. The second solution could solve these issues at the expense of extra-overhead. Selecting the most appropriate AP for each node (in both solutions) is also a challenging problem we plan to address.

4) **Power consumption:** OEMAN is suitable for evacuation areas where possibilities to recharge mobile devices exist, such as cars, external batteries, solar panels, and diesel generators. It is expected to work for several days right after a disaster occurs until the network infrastructure is recovered. However, to make the system more resilient, energy saving and harvesting solutions should be considered.

Conclusion

This article proposes a novel approach to on-the-fly establishment of multihop wireless access networks, OEMAN, for disaster recovery. Our approach is not only cost effective, but also fast and transparent to ordinary users. The main novelty of OEMAN is that Internet connectivity is moved closer to the victims by using the on-site mobile devices. This feature improves the self-supporting capability of local communities affected by disasters, which is very useful for emergency relief.

We have built a preliminary prototype and tested it in a network deployed in an area widely affected by the Tohoku Earthquake. Experiments conducted with multihop wireless access networks with paths as long as seven hops have demonstrated the feasibility and effectiveness of OEMAN. The first version of the network configuration software has been developed and used to evaluate the ease of configuration and its latency. Concretely, OEMAN is practical and ready for quick emergency response.

References

[1] M. Portmann and A. A. Pirzada, "Wireless Mesh Networks for Public Safety and Crisis Management Applications," *IEEE Internet Computing*, vol. 12, no. 1, 2008, pp. 18–25.

[2] J. Luo *et al.*, "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks," *IEEE Commun. Surveys & Tutorials*, vol. 11, No. 1, 2009, pp. 78–91.

[3] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," *Proc. ACM SIGCOMM '03*, 2003, pp. 27–34.

[4] D. Camara *et al.*, "Virtual Access Points for Disaster Scenarios," WCNC, Budapest, Hungary, Apr. 2009, pp. 1–6, 5–8.

[5] IEEE Std 802.11s, "Amendment 10: Mesh Networking," Sept. 2011.

[6] D. Camps Mur, A. Garcia, and P. Serrano, "Device to Device Communications with Wi-Fi Direct: Overview and Experimentation," *IEEE Wireless Commun.*, vol. 20, no. 3, June 2013, pp. 96–104.

[7] "Emergency Management Applications for the LAN-Cell 3G/4G Cellular Router"; http://www.proxicast.com/emergency/emergency-dr.htm, accessed June 2014.

[8] D. Abusch-Magder *et al.*, "911-NOW: A Network on Wheels for Emergency Response and Disaster Recovery Operations," *Bell Labs Tech. J.*, vol. 11, no. 4, 2007, pp. 113–33.

[9] J. Bicket *et al.*, "Architecture and Evaluation of an Unplanned 802.11b Mesh Network," *ACM MobiCom '05*, 2005, pp. 31–42.

[10] R. Chandra and P. Bahl, "MultiNet: Connecting to Multiple IEEE 802.11 Network Using a Single Wireless Card," *IEEE INFOCOM*, Hong Kong, Mar. 2004, pp. 882–93.

[11] Wireless Hosted Network, http://msdn.microsoft.com/en-us/library/windows/desktop/dd815243%28v=vs.85%29.aspx, accessed June 2014.

[12] Translated and Routed Connection, http://technet.microsoft.com/en-us/library/cc754703(v=ws.10).aspx, accessed June 2014.

[13] L. Mottola, G. Cugola, and G. P. Picco, "A Self-Repairing Tree Topology Enabling Content-Based Routing in Mobile Ad Hoc Networks," *IEEE Trans. Mobile Computing*, vol. 7, no. 8, Aug. 2008, pp. 946–60.

Biographies

Quang Tran Minh [M] (qu-tran@kddilabs.jp) is a researcher in the Network Design Department at KDDI R&D Laboratories and a visiting researcher at Shibaura Institute of Technology, Japan. He has been a researcher at the National Institute of Informatics, Japan, from 2012 to 2014. His research interests include mobile and ubiquitous computing, big network traffic data analysis, and disaster recovery systems. He received his Ph.D. in functional control systems from Shibaura Institute of Technology. He is a member of IEICE and IPSJ.

Kien Nguyen (kienng@nict.go.jp) is currently a research associate at the Smart Wireless Laboratory, National Institute of Information and Communications Technology (NICT), Japan. From 2012 to 2014, he worked as a project researcher at the National Institute of Informatics, Japan. He received his Ph.D. from the Graduate University for Advanced Studies, Japan, in 2012. His research focuses on software defined networking, disaster-resilient networked systems, and next generation wireless networks.

Cristian Borcea [M] (borcea@njit.edu) is an associate professor in the Department of Computer Science at New Jersey Institute of Technology, Newark. He is also a visiting associate professor at the National Institute of Informatics. His research interests include mobile computing and sensing, ad hoc and vehicular networks, distributed systems, and cloud computing. He received his Ph.D. in computer science from Rutgers University. He is a member of ACM and Usenix.

Shigeki Yamada [SM] (shigeki@nii.ac.jp) is a professor and director in the Principles of Informatics Research Division at the National Institute of Informatics. His research interests include mobile networks, ad hoc networks, SDN-based networks, delay-tolerant networks, and cloud computing. He received his Ph.D. in electronic engineering from Hokkaido University, Japan. He is a member of IEICE and IPSJ.