Ad Hoc Networks 40 (2016) 46–60

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

On-site configuration of disaster recovery access networks made easy

Quang Tran Minh[a,*], Yoshitaka Shibata[b], Cristian Borcea[c], Shigeki Yamada[d]

[a] Ho Chi Minh City University of Technology, Ho Chi Minh, Viet Nam
[b] Iwate Prefectural University, Takizawa, Japan
[c] New Jersey Institute of Technology, Newark, NJ, USA
[d] National Institute of Informatics, Tokyo, Japan

ARTICLE INFO

Article history:
Received 5 December 2014
Revised 4 December 2015
Accepted 25 December 2015
Available online 7 January 2016

Keywords:
Wireless multihop communication abstraction
Access network
Disaster recovery
Tree-based network
On-site configuration

ABSTRACT

Catastrophic disasters can destroy large regions and, in the process, leave many victims isolated from the rest of the world. Recovering the communication infrastructure is typically slow and expensive, which is not suitable for emergency response. Multihop wireless access networks have the potential to quickly provide Internet connectivity to victims, but so far no simple and practical solution has been proposed to help people configure these networks easily. We are pursuing the approach of utilizing wireless virtualization techniques to establish wireless access networks on-the-fly using on-site mobile devices. While our previous work has demonstrated proof-of-concept solutions, it lacked fundamental communication abstractions, a rigorous design, and a thorough analysis on the effectiveness of these solutions. The main new contributions of this article are: (1) the *wireless multihop communication abstraction* (WMCA) as a fundamental communication concept for a practical *tree-based disaster recovery access network* (TDRAN), (2) the complete design and implementation details of TDRAN, and (3) a comprehensive analysis of the effectiveness of the proposed approach based on field experiments, both in indoor and outdoor settings, at different sites in Japan. The results demonstrate the effectiveness of the proposed solution for on-site configuration of wireless access networks, as it can easily extend to 20 hops by 15 m-distance and 16 hops by 30 m-distance networks, which result in 300 m and 480 m (respectively) in radius or about 1 km in diameter. This work also confirms that our approach is ready for realization as a real disaster recovery solution.

1. Introduction

The world has recently seen catastrophic natural disasters which caused loss of hundreds of thousands of lives and destroyed millions of houses as well as the communication infrastructure in the affected regions [1]. Failure in communication and information exchange leads to further heart-breaking crises to human beings [2]. Recent tragic disasters, such as the Great East-Japan Earthquake in March 2011 [3] and the Haiyan typhoon in November 2013 (in The Philippines), show the limitations of current communication technologies in the event of disasters.

Safety information including the number of wounded people, their locations and real-time health status are

* Corresponding author. Tel.: +84 969852729.
E-mail addresses: quangtran@cse.hcmut.edu.vn, goldenqht@gmail.com (Q.T. Minh), shibata@iwate-pu.ac.jp (Y. Shibata), borcea@njit.edu (C. Borcea), shigeki@nii.ac.jp (S. Yamada).

http://dx.doi.org/10.1016/j.adhoc.2015.12.008

essential for rescue and crisis mitigation. It is necessary for people to access the Internet to share their safety status with rescuers as soon as possible. Our experience from analyzing disaster recovery efforts suggests that the first 24-h represent the "golden time" for emergency relief. However, recovery of disaster-damaged communication infrastructure is complicated and prolonged which is not suitable for emergency response. Strategic approaches should be proposed considering the following essential requirements:

(R1) **Quickly re-establish Internet connectivity**: Immediately after a disaster occurs, users need Internet access to data such as information about the disaster, evacuation notifications, their families status, etc., using common Internet-based applications (e.g., email, web browsing, Skype). Quickly providing Internet connectivity is a hard but essential requirement which must be satisfied by the proposed approach.

(R2) **Leverage commodity mobile devices**: Commodity mobile devices (laptops, tablets, smart phones) carried by disaster victims should be leveraged in the process of re-establishing Internet connectivity when part of the network infrastructure is down. This feature becomes very useful, for example, in and around evacuation centers where people gather after a disaster.

(R3) **Configure and extend the network in an easy way**: The network must be configured easily, requiring no technical skills from the disaster victims. Ordinary users should access the Internet as easily as if they are connected to conventional WiFi access points (APs). Furthermore, once joining the network, users should automatically contribute to the extension of the network coverage as per (R2).

In order to satisfy these requirements, a wireless multihop communication approach to reach the still-alive Internet gateways (IGWs) or Internet connected WiFi APs is the best solution. This work aims at **quickly extending Internet connectivity** from surviving IGWs/APs to victims by leveraging their mobile devices to form multihop wireless access networks.

Existing multihop ad hoc network approaches face difficulties in real-world deployment, especially in emergency response situations since they require dedicated hardware (e.g., additional mesh routers or network interface cards—NICs), complicated routing protocols, and IP address allocation and network configuration mechanisms to be installed on each mobile node (MN) in advance. In addition, it is still too complicated for ordinary users to change their devices into ad hoc mode and configure ad hoc networks.

We are pursuing the idea of quickly setting up wireless multihop access networks for disaster recovery utilizing wireless virtualization techniques [4–7]. Concretely, a novel approach to on-the-fly establishment of multihop wireless access networks to extend Internet connectivity from surviving APs to disaster victims using their own mobile devices has been proposed in [6]. The network is set up on-demand using wireless virtualization to create virtual access points (VAPs) on mobile devices which greedily form a tree-based topology to bridge far apart victims with a surviving AP. Ordinary users can easily connect to the Internet through the established network as if they are connected through conventional APs; the users also contribute to increase the network coverage, which is essential in emergency relief situations. A proof-of-concept prototype for this approach has been built and demonstrated in practice. However, this approach still lacks a high-level fundamental communication abstraction that can simplify network establishment and configuration, a more rigorous design, and a thorough analysis of its effectiveness in different real-life settings.

This paper overcomes these drawbacks and presents the following main new contributions:

(i) The **wireless multihop communication abstraction** (WMCA) is devised as a fundamental communication concept for the design of a practical **tree-based disaster recovery access network** (TDRAN). This concept helps to hide the inherent complexity of multihop communication establishment as each node is simply aware of only its associated AP (or VAP) using one of its virtual WiFi interface (WIF), and serves as a VAP using another WIF.

(ii) A full system design and implementation of the TDRAN scheme, which details the new features in this work, as compared to those in [4–6]. We also propose the **software-based WiFi access node** (SAN) concept, which involves the **software-based implementation of network functions** that run on mobile devices without the need for additional hardware. In addition, we propose a mechanism for auto-reconfiguration of link failures to improve the usefulness of the proposed network establishment and configuration approach. This mechanism has been implemented to display the connectivity status table (CST) at each node.

(iii) A thorough feasibility and performance analysis based on medium-scale field experiments, including indoor and outdoor setups. The experiments were conducted at two different locations seriously affected by the Great East-Japan Earthquake, namely Iwate and Miyagi prefectures, Japan. The analysis of the results provides a comprehensive understanding of the effectiveness and feasibility of the proposed approach. These new experimental results reveal that the proposed network is capable of extending to 20 hops by 15 m-distance and 16 hops by 30 m-distance networks, which result in 300 m and 480 m (respectively) in radius or about 1 km in diameter (much larger than that of 7 hops obtained by previous experiments in Iwate prefecture [6]). This coverage is large enough for disaster recovery and evacuation centers.

It is worth noticing that the simple yet practical mechanisms for auto IP addresses configuration and IP address conflict avoidance, as well as routing and DNS resolution in the tree-based networks [5,6] are carefully integrated in the design of TDRAN proposed in this paper.

The rest of the article is organized as follows: Section 2 reviews the related work revealing the necessity of this research. Section 3 presents the problem definition and introduces the WMCA concept.

The details of the TDRAN design and implementation are described in Section 4. The field experiments and result analysis are described in Section 5, and Section 6 concludes this paper.

2. Related work

Wireless multihop ad hoc/access networks dedicated to disaster recovery [1,8–10] have been an active research field in the last decade. In addition, the delay-tolerant characteristics encountered in partitioned mobile networks have been leveraged for disaster recovery networks [11,12]. Although these approaches have potential, there are still fundamental barriers that hinder their deployment in real-world disaster recovery applications. Concretely, the complexity of network configuration such as complex IP assignment and management mechanisms, dedicated multihop routing protocols [19,20], and meticulous working mode changing tasks (e.g., from infrastructure mode to ad hoc mode in WiFi) prevent these technologies from being deployed in practice. Our approach aims at simplifying network establishment for quickly providing **Internet connectivity** to disaster victims.

The emerging IEEE 802.11s standard [21] 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. Nevertheless, IEEE 802.11s-compliant NICs or network interface firmware is required for this infrastructure-based mesh network deployment, and the complexity of path discovery may burden the wireless NICs and thus degrading the performance of the mesh networks [22]. In contrast, the ability of utilizing commodity WiFi-equipped devices which are always available on-site together with the simple tree-based network establishment and management mechanisms provided by our approach can be a practical solution for immediate deployment.

The Wireless Distribution System (WDS) utilizes relay stations to enhance the coverage of a single AP [23]. This approach is useful for extending a stationary WiFi network, but it is limited in terms of multihop network extension for large-scale disaster recovery. The SoftRepeater [24] applies wireless virtualization which was first introduced by Chandra and Bahl [7] to transform a commodity WiFi equipped device into a client repeater. This approach mainly addresses the rate anomaly problem in WiFi networks to improve the whole network performance [24]. However, multihop communication leveraging multiple SoftRepeaters, which would be useful for disaster recovery wireless access networks, has not been discussed.

WiFi Direct [25] is closely related to our work whereby each node can work as both a station (i.e., client) and a software-based AP. This solution groups nearby nodes together, with one node serving as a group owner to manage the communication within the group. Internet connection is shared from the owner to the group members. However, the feasibility of multihop-based Internet connectivity sharing in WiFi Direct has not been addressed.

On-demand deployment of movable WiFi APs (carried by emergency vehicles), cellular base stations (BSs), satellite communication systems, and so forth is a common solution in disaster recovery [26–28]. These solutions are expensive for deployment and could be slow because specific equipment is not always available on-site (e.g., movable and deployable resource units (MDRUs), transceivers using very small aperture terminals (VSATs) for satellite systems). Therefore, it may take a substantial amount of time before emergency rescue/technical teams reach the disaster areas to deploy these equipments/networks. Our approach complements these solutions with a free and fast mechanism to extend the Internet to the disconnected victims by leveraging their mobile devices. For example, as shown in Section 5, it takes less than 154 s on average for common users to setup an access network to connect to the Internet using our solution.

Similar to our project, several works have been dedicated to finding solutions for realizing ad hoc multihop networks using single WiFi equipped mobile devices. Al-Hazmi and De Meer [29] and Wirtz et al. [30] propose a virtualization of IEEE 802.11 NIC for establishing wireless mesh networks. In these works, the physical WIF is virtualized into multiple logical WIFs allowing a node to concurrently connect to different networks. Nevertheless, the main focus of these works is not on Internet connectivity in disaster conditions, thus could not be directly applied to solve our problem. Concretely, the work in [29] utilizes the ability of connection sharing at client nodes to shutdown APs which are serving a small number of clients to save energy. The ability of ad hoc multihop communication establishment, which is the main target in our work, has not been discussed. MA-Fi (Mobile Ad hoc Wi-Fi) [30] and NodesJoints [31] are closer to our work where wireless virtualization is leveraged. However, the multihop network establishment in these approaches is still complicated and cannot be quickly setup by ordinary users for emergency responses.

Different from the aforementioned works, our approach aims at simplifying the establishment of multihop communication by proposing an abstract view of the multihop network as a chain of one-hop WiFi networks, which simplifies the network model and allows for easy reasoning about the network properties and configuration. This concept is realized by carefully integrating existing technologies in a practical implementation. As a result, ordinary users can set up a multihop access network easily right after a disaster occurs using their commodity mobile devices.

Finally, a number of works could be leveraged to optimize our solution. For instance, research has been dedicated to improving the network intelligence, such as biology-based algorithms [13,14]. We can use such algorithms to detect the network topology and automatically adapt it to changes in the environment. Also, work done on multihop routing protocols with smart data collection and compression capabilities [15–18] could be used to address the potential bottleneck issue in our tree-based network.

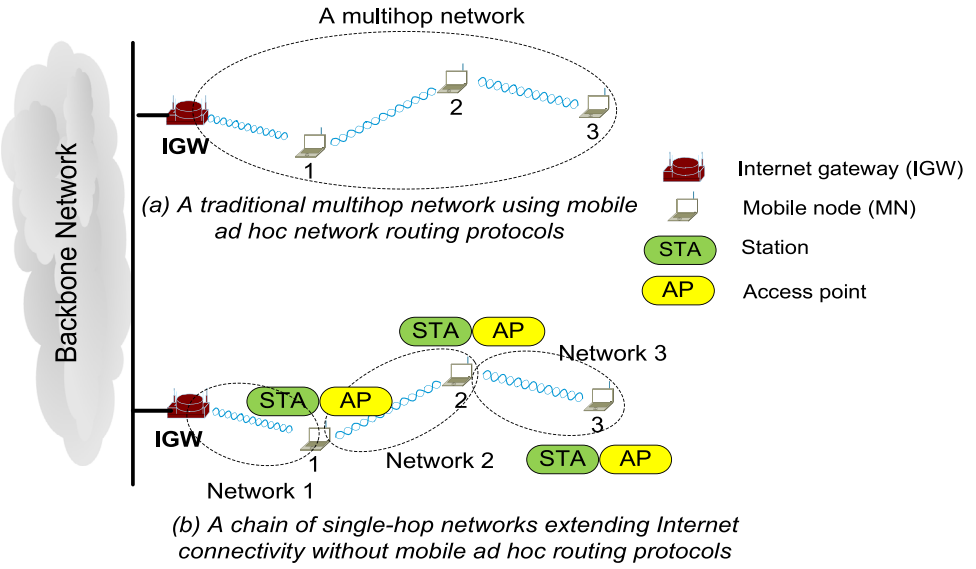

Fig. 1. Wireless multihop communication abstraction—WMCA.

3. Wireless multihop communication abstraction (WMCA)

3.1. Problem definition

While a large part of an access network is destroyed in the disaster region, there could be a number of still-alive APs that can be used to access the Internet. Unfortunately, these APs could not be easily accessible to most of the victims. This work aims at **quickly extending Internet connectivity** from surviving APs to victims by leveraging their mobile devices to form multihop wireless access networks. To achieve this goal, these networks must be established quickly and transparently to users as victims cannot be expected to perform setup operations or to have certain multihop enabled software installed on their devices. Practically, two essential challenges must be overcome:

- How to establish multihop access networks without requiring any action from the victims?
- How to configure addressing, naming, and routing in these networks in a simple and automatic way?

In order to solve these essential difficulties, this article proposes the **wireless multihop communication abstraction** (WMCA) concept and its realization on a **tree-based disaster recovery access network** (TDRAN) scheme. These approaches are summarized as follows.

3.2. Solution overview

WMCA: *The multihop communication is abstracted to be viewed as a chain of single-hop setup operations. Accordingly, a chain of WiFi-based managed networks, each of them working as a regular AP providing WiFi connectivity to mobile devices, is viewed as a whole access network that is quickly established to extend the coverage.*

Fig. 1 illustrates the advantages of the WMCA concept. Fig. 1a shows a conventional view of a multihop access network where each node must implement a traditional mobile ad hoc network routing protocol and maintain the routing information for all the nodes. In contrast, each node in the WMCA approach (Fig. 1b) works as both a station (STA) connecting to the WiFi infrastructure network for its Internet access and a VAP for extending its connectivity. Each VAP is responsible for its own SSID providing an infrastructure-based WiFi network for the nearby nodes. In this way, a tree-based multihop access network is naturally formed. The individual users are not aware of this topology because they have just a localized, 2-hop view of the network: their mobile devices associate as STA with the previous hop and act as a VAPs for other clients (the next downward hop). This approach abstracts the complexity of a multihop network as a chain of conventional infrastructure-based WiFi networks, hence simplifying the network establishment and management. The built-in WIF is utilized to implement the STA and VAP functionality on each individual node. As a single WIF is available on a commodity mobile device, the wireless virtualization [7] technique is employed to improve the performance of switching the WIF between the two modes. Details of this implementation are described in Section 4.

4. Tree-based disaster recovery access network (TDRAN)

As presented in Section 3.2, the WMCA concept allows each individual node to manage a particular network in VAP mode and connect with another network in STA mode. Consequently, a tree-based topology is a natural implementation of this concept. This section describes the details of TDRAN design and implementation.

4.1. Overall architecture

Fig. 2 shows the overall architecture of TDRAN. We assume that a network controller managed by an emergency

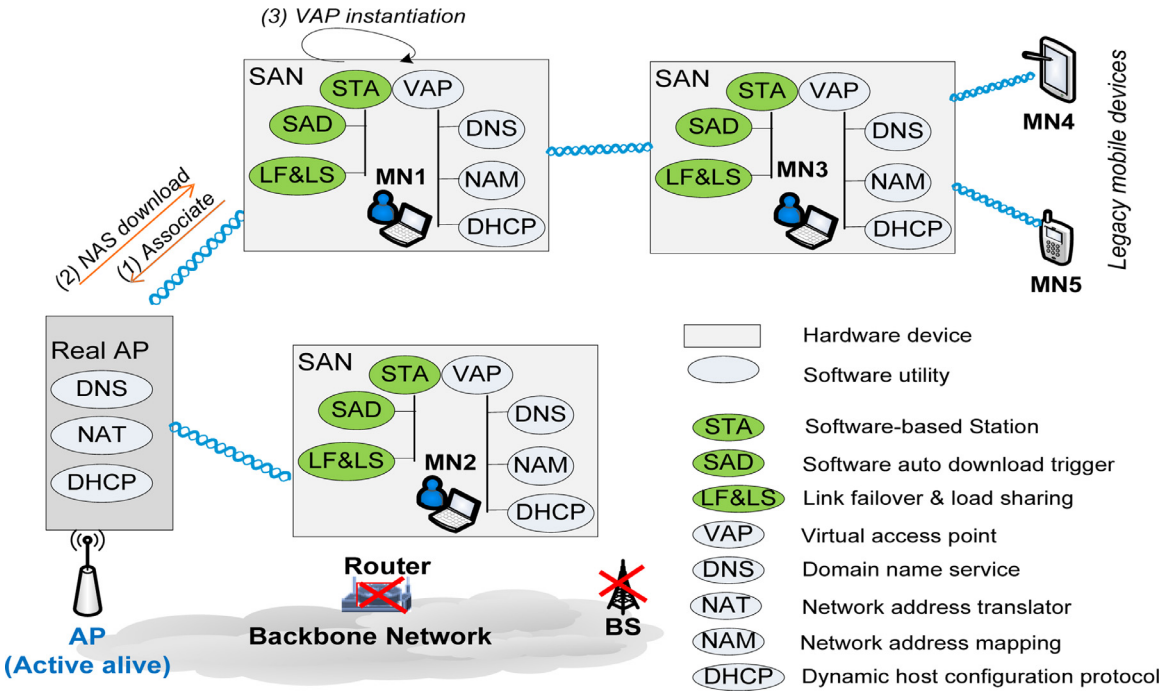

Fig. 2. TDRAN: tree-based disaster recovery access network.

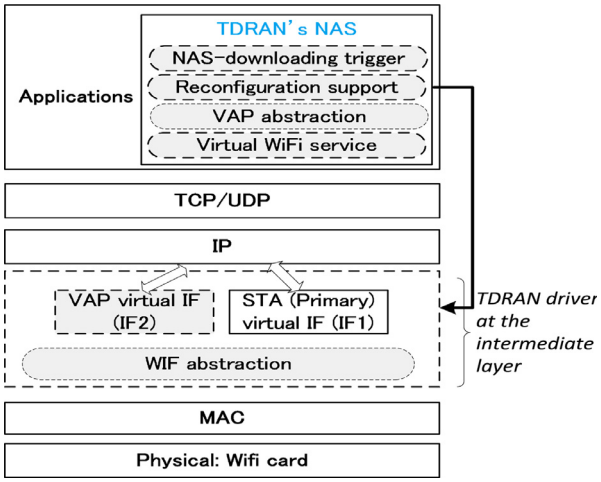

Fig. 3. NAS components running on each SAN.

operation center initiates the network establishment process when a disaster occurs by turning all the reachable (surviving) IGWs/APs into "emergency relief state" (ERS). Devices which are close to the active AP try to associate to this AP in a common way using their available WIFs. Any node that connects to an ERS IGW/AP is instructed to download a special network auto-configuration software (NAS, shown in Fig. 3) to transform itself into a software-based access node (SAN) which can work in both the STA and VAP modes. At the same time, the ERS is activated at the newly created VAP, forcing its associated nodes to download the NAS and transform themselves into SANs to form a tree-based disaster recovery access network.

A SAN is a commodity MN which functions as an AP (we named it virtual access point or VAP) to coordinate its associated nodes. These functions are incorporated in a software system that runs on mobile devices. The details of SAN are described as follows:

(a) A SAN can work in both the STA (e.g., client) and the VAP modes concurrently to seamlessly connect different networks, thus supporting multihop Internet communication.
(b) A SAN abstracts the single available WIF into multiple virtual WIFs; each virtual WIF associates to a particular network realizing the capability in (a).
(c) A SAN manages a network consisting of itself (as VAP) and its associated nodes (connected to VAP as STA). This network connects to the parent node in the tree topology using the STA mode of the SAN.
(d) A SAN allocates IP addresses to its associated nodes using a DHCP server-like function and avoids the address duplication using a network address mapping (NAM) function. This function maps every address of an internal network (the sub-tree downward the TDRAN) to a corresponding address in the external network (upward the TDRAN), thus it allows the associated nodes to communicate with the outside networks and over the Internet. The NAM also supports a simple layer 3 routing mechanism over the network.

The inter-connection of SANs forms a chain of single-hop WiFi networks bringing Internet connectivity from surviving APs to participating nodes

including legacy nodes (i.e., nodes without SAN enabled which connect as leafs in the network tree). Concretely, each SAN manages its own infrastructure-based network with a specific SSID (Service Set Identifier) and a chain of them forms the TDRAN which is automatically extended to a large area with the joining of new MNs. This approach is not only simple and cost effective, but also fast and spreads Internet connectivity to large areas satisfying the critical requirements of quick emergency response.

4.2. TDRAN design features

As discussed, NAS is the essential software which transforms a commodity MN into a SAN. NAS implements a number of essential components as illustrated in Fig. 3: (1) **wireless interface abstraction**; (2) **virtual AP abstraction**; (3) **reconfiguration support**; and (4) **NAS auto downloading trigger**.

1. **WIF abstraction**: Since every intermediate SAN must connect to different networks concurrently using two different modes, namely STA and VAP, multiple WIFs are needed. To cope with the restriction of having only one physical WIF on commodity mobile devices, this component abstracts the single physical WIF into several logical WIFs using wireless virtualization [7]. Wireless virtualization is implemented as a **WIF abstraction** in the intermediate layer driver (just above the MAC layer but below the IP layer) and a **Virtual WiFi service** in the application layer. The WIF abstraction driver deals with switching and buffering packets between logical WIFs, while the control logic is implemented as an application layer utility.
2. **VAP abstraction**: This component transforms a commodity MN into a SAN which is able to work in both the STA and the VAP modes at the primary and the secondary logical WIFs, respectively. DHCP, NAM, and default gateway assignment for DNS resolution functionalities are also included in this component.
3. **Reconfiguration support**: This component deals with network reconfiguration due to link failures. It provides a user-friendly mechanism such that a network administrator or a volunteer user can quickly detect and reconfigure disconnected links in a large tree-based network.
4. **Software auto downloading trigger**: NAS also includes a software auto downloading trigger which forces the associated node to download the NAS software automatically.

It should be noted that the components at the intermediate layer can be easily implemented in open source systems like Linux [32] or Windows by embedding them in the Network Driver Interface Specification (NDIS) layer [7]. The Virtual WiFi service component in the application layer interacts with the WIF abstraction component at the intermediate layer via the I/O Control Codes (ioctls) [33].

4.3. Internet connectivity in TDRAN

This section discusses how TDRAN simplifies routing issues and conducts network auto-configuration to quickly bring Internet connectivity to victims.

Routing simplification: Routing is one of the challenging issues in multihop communication. Proactive routing in MANETs produces a large overhead since every node must maintain the routing information for all the other nodes. Reactive routing, on the other hand, introduces extra latency and overhead due to the dynamic route discovery and maintenance processes. As shown in Fig. 2, our approach is different as TDRAN greedily builds a tree topology, and the routing for Internet communication is done along this tree which simplifies significantly the process.

Our approach utilizes the concept of "translated connection" (not routed connection) [34] supported by the network address translator (NAT) at the IGW and the network address mapping at each VAP. These entities serve as "IP routers", translating addresses for packets being forwarded between the tree-topology nodes and the Internet hosts. Thus, the routing overhead is minimal as nodes are not required to collect topology information and compute routes. This solution works because our goal is to offer Internet connectivity through the root of the tree (i.e., IGW/AP), not node-to-node communication. Consequently, each node just needs to know the next connected nodes (upstream/downstream) in its infrastructure-based network to forward the packets.

For example, when MN4 in Fig. 2 wants to connect to the Internet, it initially sends packets to its associated VAP, namely MN3. In turn, MN3's VAP handles (using the NAT-ing mechanism) the packets to its STA for forwarding to the upstream VAP, namely MN1. The packets finally reach the actual AP where a traditional routing protocol is implemented to route the packets in the Internet. In this approach, communication is always initiated by mobiles in the TDRAN. When the upstream communication is successfully conducted at each involved intermediate node up to the IGW, the NAT-ing mechanism at each node can deal with the downstream packet forwarding (i.e., from the Internet through the IGW) to corresponding TDRAN nodes. Let us note that mobiles in the TDRAN are not directly reachable from the Internet as they use private IP addresses described as follows.

Auto-configuration: Internet connectivity needs IP address allocation and duplication avoidance, as well as DNS resolution. Each MN has two logical WIFs, namely WIF1 and WIF2, and each one should be assigned an individual private IP address. In this approach, the WIF1's IP private address is assigned by a DHCP server installed at the associated AP/VAP. Since the VAP on WIF2 serves as a network gateway for the associated nodes, WIF2's IP private address is in the form of 192.168.*x*.1, where *x* is automatically computed from the MAC address of the physical WIF in such a way that its third octet is different from that of WIF1's IP address. The procedure for WIF2's IP address assignment is illustrated in Algorithm 1. As shown, *x* is in the range of 2–254 (line 2) and is different from the third octet of WIF1's IP (lines 4 and 5). This procedure satisfies two essential criteria: (a) easily assign IP addresses to the

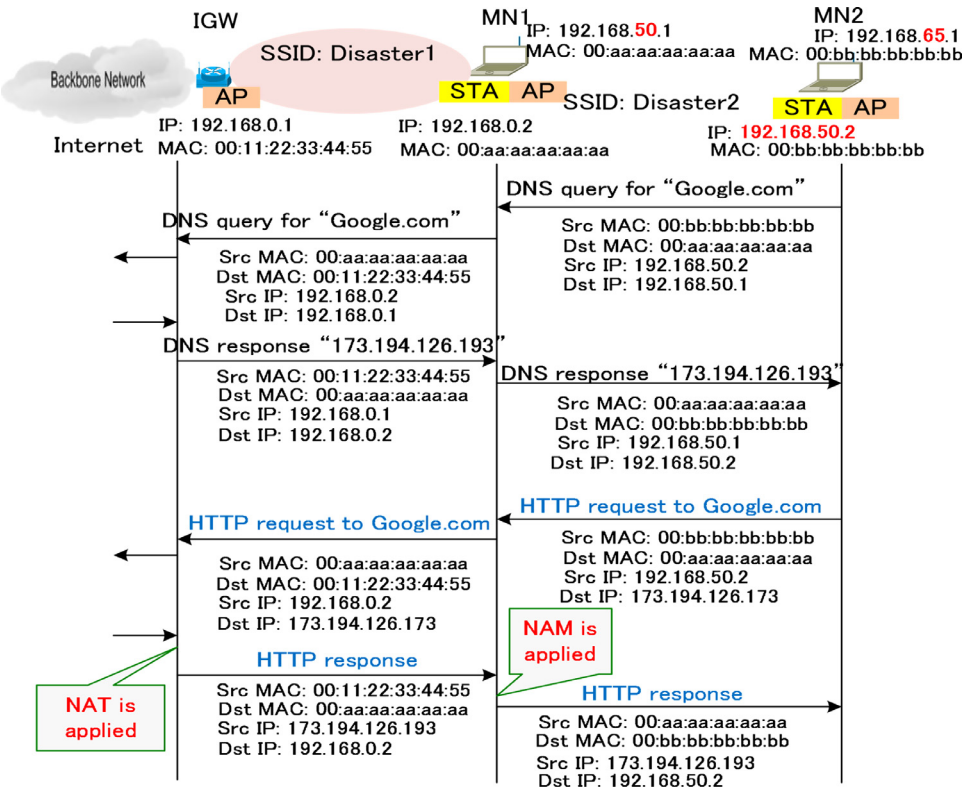

Fig. 4. DNS resolution for an HTTP request.

Algorithm 1 IP address auto configuration.

```
1: procedure WIF2_IP_ALLOCATION()
2:     int x=mod(2*Sum(digit in WIF's MAC), 252)+2;
3:     int y=third octet of WIF1's IP;
4:     if (x == y) then
5:         x++;
6:     end if
7:     Assigns 192.168.x.1 to WIF2's IP;
8: end procedure
```

local network gateways (VAPs), and (b) avoid addressing conflicts that occur when the two interfaces of the same node belong to the same subnet (192.168.*x*.0/24).

The NAM at each VAP resolves the private IP addresses at STAs, thereby they can communicate with outside networks and over the Internet. NAM also supports a simple layer 3 routing mechanism over TDRAN by simply forwarding the packets to the next connected node. Concretely, for the upstream flows (from an MN to the IGW), the VAP of an intermediate node just hands the packets to its STA for forwarding to its upstream node. For the downstream flows (from the IGW to individual destinations), the NAM at the VAP of a node identifies to which client the data should be forwarded. In addition, since each VAP serves as a default gateway, it supports DNS resolution for the associated nodes. Accordingly, any client just asks for DNS resolution by sending a DNS query to its default gateway, with intermediate nodes forwarding the query to their default gateways until it reaches the actual AP and is finally resolved.

Fig. 4 shows an example in which MN2 starts a DNS resolution by issuing an HTTP request. MN2 submits the DNS query (for "Google.com") to its default gateway, namely the VAP on MN1. MN1 delegates this request to its default gateway, which is IGW. With its DNS resolution mechanism, IGW gets the DNS response and propagates it to the original requester (MN2) via MN1. Having the actual (global) IP address of the web server (173.194.126.193), MN2 can issue an HTTP request to that host. Similarly, this request reaches IGW via multihop communication. IGW is in charge of forwarding the request to the correct web server and receives the HTTP response. The NAM at each intermediate node (e.g., MN1) deals with forwarding the response downward. Finally, packets reach MN2, the original requester, correctly.

4.4. Reconfiguration support

Despite its simplicity and ease in configuration, TDRAN faces an inherent issue on detecting and reconfiguring disconnected links. As TDRAN does not rely on any multihop routing protocol, it does not maintain information about the whole network topology. Instead, each node knows only its parent (i.e., upstream VAP) and its children (i.e., downstream STAs), thus originally it cannot detect and recover its Internet connectivity when a far apart link fails. For example, node B in Fig. 5 knows its upward VAP,

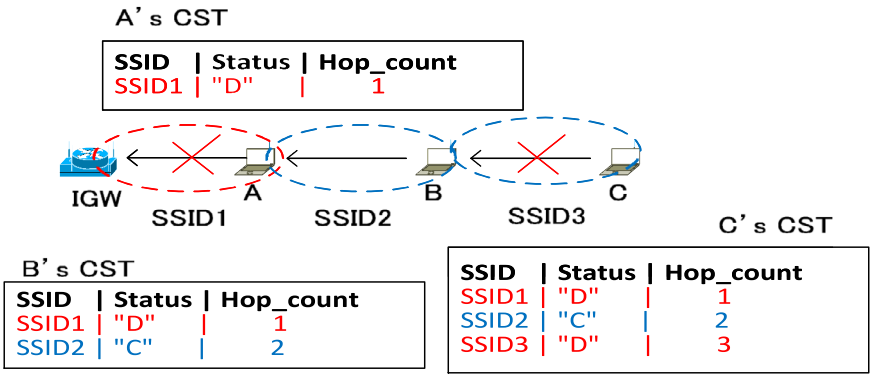

Fig. 5. A chained network with two link failures and the nodes' CSTs.

namely SSID2 on node A, while it is not aware of the disconnection on a further link (A-IGW). This missing information confuses the users who experience Internet inaccessibility while their connection to SSID2 is still in a good condition.

In order to detect any link failure on the path from a particular node to the IGW, each node manages a connectivity status table (CST) containing the status of all the links on such a path. It should be noted that this table does not contain the status of downstream links since a node does not manage nodes that are not included in its network. This table is managed by the "Reconfiguration support" component as illustrated in Fig. 3. An example of CSTs is depicted in Fig. 5.

Here, a **link** describes a connection between a node and an AP/VAP in a network represented by an SSID (e.g., link A–B is represented by SSID2). The state of a link can be *connected* ("C") or *disconnected* ("D"). A link can disconnect because of node mobility, battery shortage, or many other reasons in a severely disrupted environment. A link connects again when the failure is recovered (i.e., the disconnected node (re-)connects to its previous VAP or to a new VAP).

Each CST row represents the state of a particular upstream link with the following format *(SSID, Status, hop_count)*. *Hop_count* is the number of hops from the corresponding SSID to the IGW.

In order to update a CST, the connectivity status is sent from the upstream node (VAP) to downstream nodes (STAs) under the following conditions: (i) when a link connects or disconnects, the corresponding **up/down link notification** is automatically sent (by the immediately connected node) and is propagated (by downstream nodes) to any node in the path until the notification reaches the leaf nodes. This notification is conducted by broadcasting; (ii) the owner of a node can issue a *CST request* manually to update the node's CST. According to the CST request, a *CST response* is delivered. The *CST request* and *CST response* are paired and sent by unicasting. In every notification message, the whole CST of the notifying node is sent to the downstream nodes. Three types of messages, namely *CST request*, *CST response*, and *CST propagation* (this message is also used for automated up/down link notification) are sent on the network to manage and update the CST using UDP. The formats of these messages and their corresponding fields are described in detail as follows and in Table 1.

CST request(SrcIP, DestIP, TransID, Type)

CST response(SrcIP, DestIP, TransID, Type, CST_Content)

CST propagation(SSID, TransID, Type, CST_Content)

The *CST_Content* (last row in Table 1) is the content of the notifying node's CST which is sent to its clients; it is a variable length field with the following format:

CST_Content (SSID, status, hop_count)

Table 1
Field in the connectivity status notification messages.

Field	Size (Bytes)	Description
SrcIP	4	IP address of the requester (child node)
DestIP	4	IP address of the receiver (parent node)
TransID	2	Transaction ID (used to avoid looping)
Type	1	The message type (1 means CST request, 2 CST response, 3 CST propagation)
SSID	20	SSID of the notification broadcasting node
CST Content	Variable	The content of CST. Its length is variable depending on the number of rows in CST

4.5. Multiple surviving APs and load balancing

This work directly aims at providing Internet connectivity to the victims in disaster areas, hence we set the minimal requirements for emergent disaster recovery networks, focusing on simplicity and ease of configuring on-site access networks in severe disasters. Consequently, our current tree formation solution is greedy, which may lead to imbalanced trees resulting in performance bottlenecks at nodes with high workloads (i.e., nodes which are close to the root). Similarly, specific traffic patterns may lead to the same problem. In addition, several APs may still survive, thus providing more chances to provision Internet connectivity. In this situation, the problem is how to divide the nodes among individual APs acting as IGWs while maintaining a good load balance with minimal overhead. This

section presents design guidelines and potential solutions to resolve these problems.

Multiple surviving APs/IGWs would be beneficial to the network because they could improve the network performance by eliminating the tree topology bottleneck and shorting the paths (in terms of hop count) from the victims to the appropriate IGW. However, this would lead to a more complex network topology. In order to apply our solution for a network with multiple IGWs, one needs to choose between maintaining separated networks/trees and maintaining overlapping networks/trees. In the former solution, we create multiple separated networks, each rooted at one surviving IGW. Hence, a node is member of only one network. This solution has lower overhead, but it may lack load balancing and availability features. The latter solution also creates multiple networks, each network being rooted at one surviving IGW, but the nodes could be part of multiple networks at the same time. This solution could resolve the load balancing and availability problems of the first solution at the expense of extra-overhead. Selecting the most appropriate AP for each node (in both solutions) is also a challenging problem. One solution is to leverage work on balancing the lifetime of nodes in wireless sensor network to develop a load balancing mechanism for our networks [35]. In addition, the smart data collection and compression mechanisms proposed in [15–18] could be applied as possible solutions for the potential bottleneck issue in our tree-based network.

Another potential solution that we are pursuing is an SDN-based dynamic packet forwarding [36] approach, whereby the routing/packet forwarding rules could be implemented at one (or some selected) surviving APs to help optimize the load balancing between multiple APs. However, this approach may introduce additional cost and complexity.

We also consider to extend the capability of the CST approach presented in the previous sub-section. Concretely, the CST could detect and compute traffic load at individual nodes. When a node is overloaded, it asks the appropriate associated clients to migrate to alternative VAPs. The client that needs to move is the one that has more data to be served by the considered VAP compared to those of other clients. The advantage of this approach is two-fold: (a) quickly reduces the load of a heavy node, and (b) minimizes the overhead of mitigating load imbalance.

5. Evaluation

The main purpose of the evaluation is to verify whether TDRAN works well to bring Internet connectivity to isolated people. Specifically, we evaluated the effectiveness of the network establishment and its performance in terms of round trip time (RTT), packet loss, and throughput in multihop topologies. In addition, actual Internet-based services such as voice chat over Skype and video streaming on YouTube have been verified.

5.1. Prototyping

A prototype of TDRAN has been developed using commodity Windows-based laptops. We named this software MHANS (MultiHop Access Network Software) and its novel features on establishing TDRAN are demonstrated in Fig. 6 and summarized as follows: (a) each intermediate node concurrently serves multiple clients; (b) multihop communication is supported, e.g., 3 hops from MN3 to the actual AP; (c) the IP addresses of the two virtual WIFs and the SSID name provided by the VAP at each node are appropriately assigned; (d) the CST is dynamically updated according to the change of network topology.

As shown in the lower part of Fig. 6, the CST of MN3 is updated according to the change in network conditions. At the beginning, MN3 is 3 hops apart from the real AP (named “soken”) as shown in the rightmost CST. When the link MN2-MN1 failed, the CST is updated to disaster_403 for this link. Finally, the CST is updated as shown in the leftmost one when MN2 made a new connection to the real AP. It should be noted that the software auto downloading trigger and solutions for load balancing in a multiple surviving APs environments have not been implemented in this version. We defer these implementations to future work for advanced disaster recovery access networks.

5.2. Experimental methodology

In order to evaluate the ease of a user joining TDRAN and transforming his/her MN into a SAN to extend the network, as well as to quantify the network performance when the number of nodes and the number of hops increase, several field experiments have been conducted at the Iwate Prefecture University (IPU) and Ishinomaki Senshu University (ISU), Japan. Iwate and Miyagi (where ISU is located) are prefectures that have been significantly affected by the Great East-Japan Earthquake.

A tandem network (i.e., a node-after-node topology where one node serves at most 1 client) and a tree-based network, as shown in Fig. 7a and b, respectively, have been constructed on-site using our prototype. An MN can associate with any available AP/VAP for Internet connectivity using the built-in WIF. After connecting to a VAP, the web browser (e.g., Internet Explorer) on the user’s device directs the user to the website where MHANS is hosted. The user downloads MHANS and installs it on his mobile device. When the MHANS is installed and initiated, the user’s MN is transformed into a SAN sharing Internet connectivity to its vicinity. In this experiment, it requires users to go to the website to download and install the MHANS. However, this process can be done automatically by the software auto downloading trigger implemented in the NAS, as discussed in Section 4.2.

The total time needed for an MN to join TDRAN and transform itself into a SAN, and the network performance in terms of average RTT, packet loss, and throughput according to network size are thoroughly evaluated. Concretely, the average RTT, packet loss and the throughput between MNi (i=1...n) and MN0 in both topologies were evaluated. We choose not to measure the performance across the Internet through the physical AP because our goal was to isolate the performance of the TDRAN network. FPing [37] was used to evaluate RTT and packet loss, while Iperf [38] was utilized for measuring the

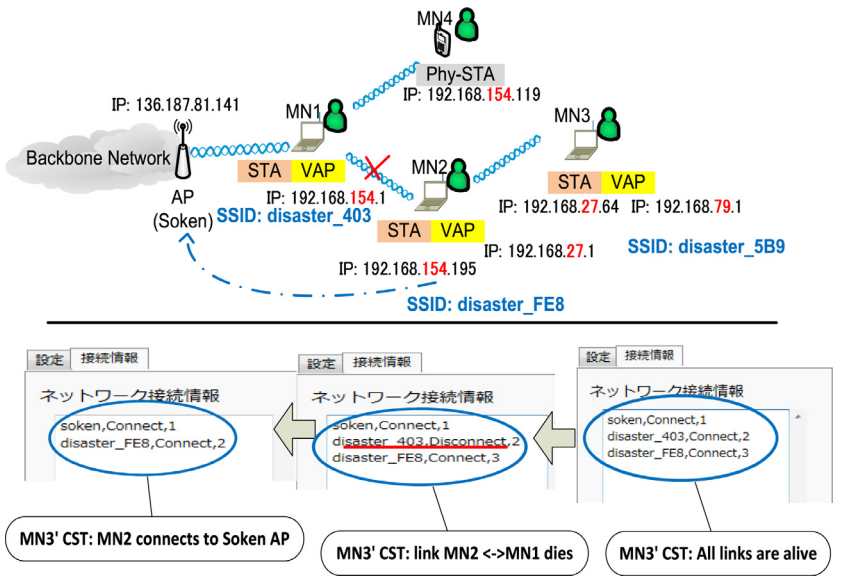

Fig. 6. Demonstration of TDRAN using MHANS.

Table 2
Experimental parameters.

Parameter	Value/description
Topology	Tree-based and tandem networks
Environment	Indoor and outdoor settings
Hop distance	-Tree-based: 30 m between levels -Tandem indoor (at IPU): 50 m -Tandem outdoor (at ISU): 15 m and 30 m
Network size	-Tree-based outdoor: three levels (hops) and 15 nodes -Tandem indoor (at IPU): 14 hops (area: 700 m in radius) -Tandem outdoor (at ISU): 20 hops and 16 hops (area: 300 m and 480 m in radius) for 15 m-distance and 30 m-distance networks, respectively
Mobile node (MN)	ASUS U24A-PX3210 laptop with 4GB memory, Core-i5 2.5 GHz CPU, Atheros AR9002WB-1NG WiFi, and Windows 7 OS
TCP window size	64KB
Buffer length (in Iperf)	8KB: Iperf works by writing an array of 8KB continuously
Maximum Transmission Unit (MTU)	1500 Bytes
Evaluation duration	100 s
Wireless link	IEEE 802.11g
Packet size (FPing)	1470 Bytes

throughput. An FPing utility and an Iperf client were installed on each MNi, while an Iperf server was installed on MN0. It should be noted that the throughput experiments and RTT/packet loss experiments were conducted separately. The evaluation parameters are summarized in Table 2. Every experiment was conducted during 100 s and the average values of five consecutive tests were drawn out with the assumption that the testing condition (affected by the surrounding environment) in each setting (tree-based, indoor tandem, and outdoor tandem networks) does not change significantly during the experiments.

5.3. Ease of network establishment

The ease of network configuration and the configuration time were evaluated by asking users to make a tandem network as the one in Fig. 7a whose hop-distance is 30 m in the open air (outdoor), and try to access the Internet. Three time periods, namely the time needed for making Internet connectivity (t1), i.e., from starting to associate with the upward AP/VAP until the user can successfully load the default website that hosts MHANS; the time to download MHANS (t2); and the time to install and initiate MHANS (t3) were evaluated and shown in Fig. 8.

The time for a node to associate with the nearest AP/VAP and access the Internet (t1), and the time to install and initiate MHANS (t3) are almost constant. The total time (t) needed for a node to completely join TDRAN and transform itself into a SAN increases with the hop_count since it takes longer time to download MHANS (t2). However, this time is less than 154 s (up to 8 hops) which is quick enough for emergency response.

5.4. Network performance evaluation

RTT, packet loss, and throughput as function of the network size/number of hops have been thoroughly evaluated. Experiments have been conducted in two periods: (1) a

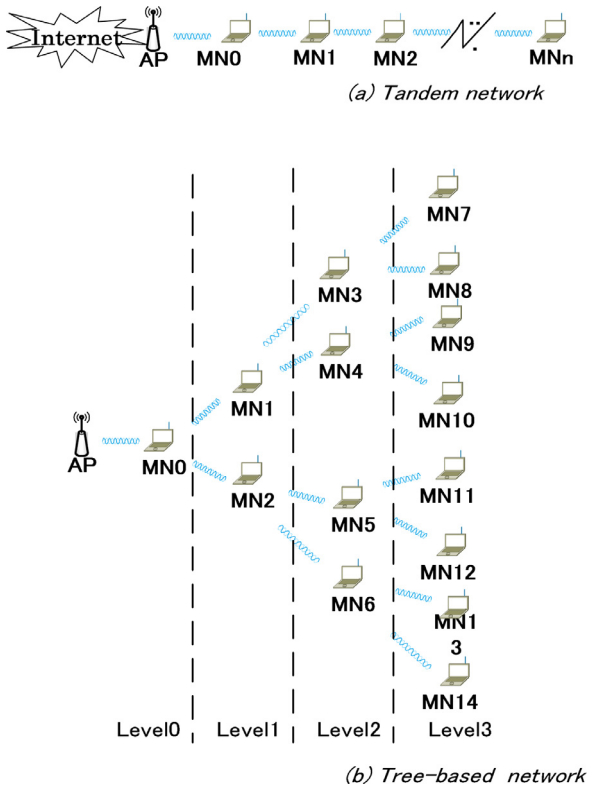

Fig. 7. Tandem and tree-based network deployments for evaluation.

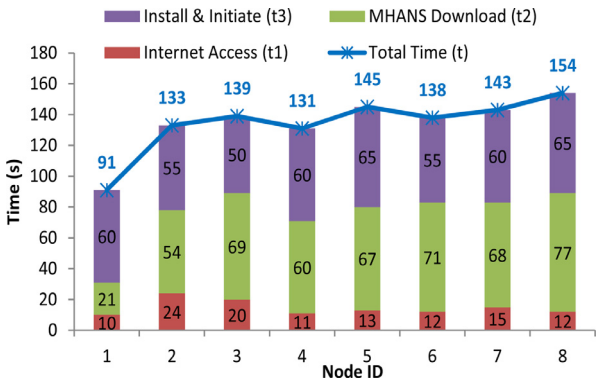

Fig. 8. Time consumed for network establishment.

3-day (indoor) experiment at IPU in July 2013, and (2) another 3-day (outdoor) experiment at ISU in May 2014. In (1), we used Connectify [39] software to deploy our idea of WMCA while the experiment in (2) used our developed software, MHANS.

RTT and packet loss need to be measured in multi-hop networks especially when the number of hops is large. An indoor tandem topology was established with 15 MNs (MN0 to MN14) placed along the corridors of IPU's campus buildings as shown in Fig. 9. Here, MN0 to MN4 were on the second floor, and the other 10 MNs were on the fourth floor. The hop-distance was 50 m. MN0 was connected to

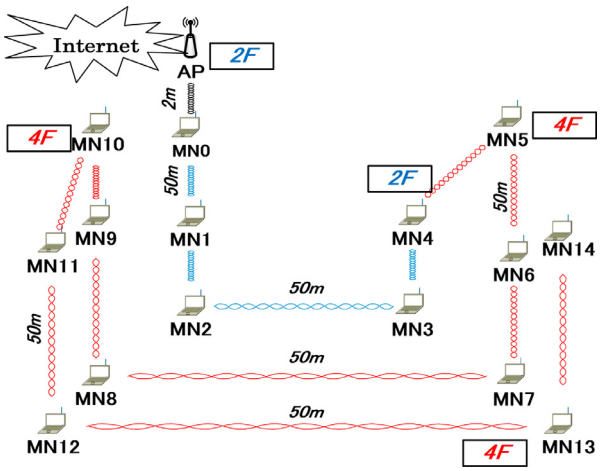

Fig. 9. An indoor tandem topology TDRAN with 50 m hop-distance (Connectify is used to deploy this network).

the real AP, while each MNi (i = 1...14) was connected to the Internet via the deployed TDRAN.

Fig. 10 shows the variation of the average RTT and packet loss with the change in the number of hops in the indoor tandem network shown in Fig. 9. For legibility, the deviation of the packet loss is not displayed; it ranges from 0% to 4.5% when number of hops is less than 11, and from 3% to 7% for larger number of hops. We observe that RTT linearly increases with the number of hops, but its values are still low enough to be practical for many applications and Internet services. For example, the RTT is as small as 200 ms and the packet loss is almost less than 20% when the number of hops is 12. These results are acceptable for common Internet-based applications commonly used in emergency situations such as VoIP services and web browsing.

One of the interesting observations from this experiment is that, at the lunch time, a lot of students moved around, creating serious interference. This interference declined the link quality and caused link failures. We succeed with 13 and 14 hops after the lunch time (2:00 PM) when there were fewer students around. However, the connections at nodes MN13 and MN14 were still intermittent because of high link failure probability. That is why packet loss at those nodes significantly increases. In addition, packet loss at 10 hops is larger than that at 11 and 12 hops. This is because the data at 10 hops was collected at the lunch time while the data at 11 and 12 hops was collected in the afternoon.

Another interesting fact is that it was easy to establish and maintain a network with 12 hops. However, it became more difficult to reach a network with 13 and 14 hops. The main reason is the aggregated availability of the chained network. Concretely, if any link in the chained network fails, then a far-away node (e.g., node 13 or 14) cannot reach the IGW (i.e., the actual AP) for DNS querying. Obviously, when the number of hops increases, the probability of intermediate link failure also increases. In our experiments, the "breaking point of the network" was determined to be 12 hops.

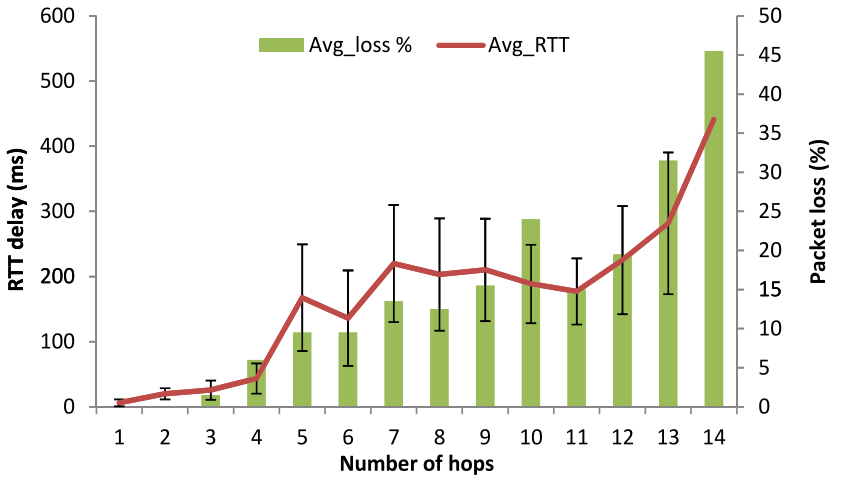

Fig. 10. RTT and packet loss in the indoor tandem topology (hop-distance is 50 m).

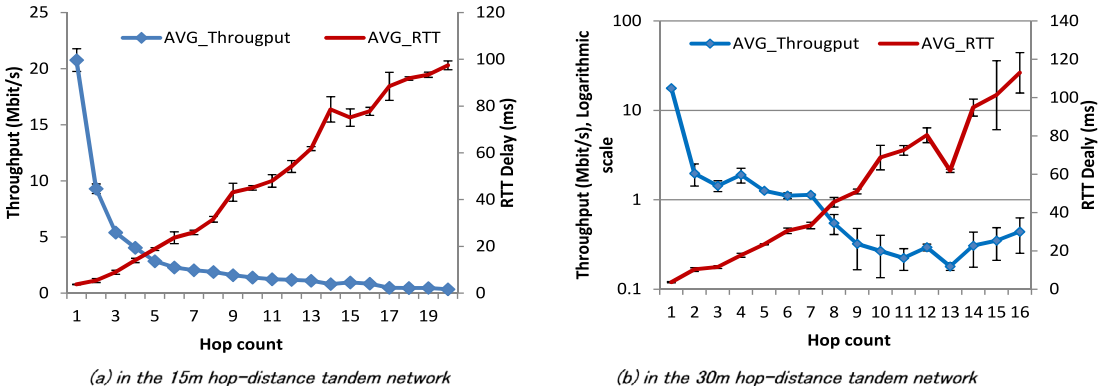

Fig. 11. RTT and throughput in outdoor tandem networks.

In the experiments at ISU, we focused on outdoor network establishment and also measured the throughput in addition to RTT and packet loss. Fig. 11a and b show the RTT and throughput on tandem networks with 15 m and 30 m hop-distance, respectively. Again, RTT linearly increases at a rate of around 5 ms per hop. As a result, RTT is still low, namely less than 120 ms, even for the longest path (i.e., 20 hops and 16 hops in 15 m and 30 m hop-distance networks, respectively). The throughput decreases with the number of hops, but it still reaches an acceptable value, which is around 200Kbps in the worst case. Therefore, we conclude that TDRAN's overhead (especially that of wireless virtualization and packet forwarding) does not significantly impact the network delay and throughput.

Further analysis reveals that the throughput degrades at a rate of 1/2, 1/3, 1/4 for the first three nodes in the 15 m hop-distance network (Fig. 11a). This degrading rate is lower at further nodes since the interference decreases and nodes can concurrently transmit (forward) the data to their next-hop nodes. This feature reveals the stability of TDRAN.

Fig. 12 shows the average packet loss in 15 m hop-distance and 30 m hop-distance tandem networks. The latter introduces larger packet loss since longer hop-distances affect wireless links, degrading the success of packet delivery. Because of this reason, the availability of the 15 m hop-distance network is higher than that of the 30 m hop-distance counterpart. More concretely, the 15 m hop-distance network worked properly almost all the time during the evaluation which lasted for half day, and we

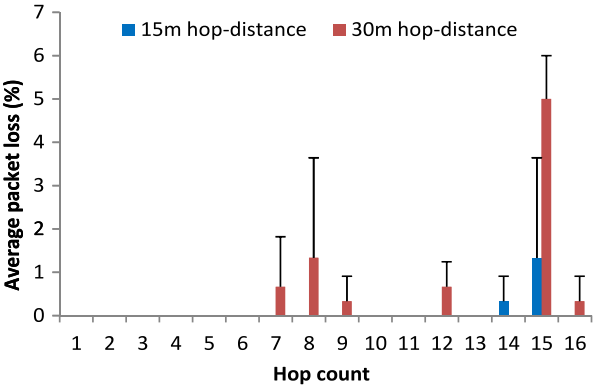

Fig. 12. Maximum packet loss in outdoor tandem networks.

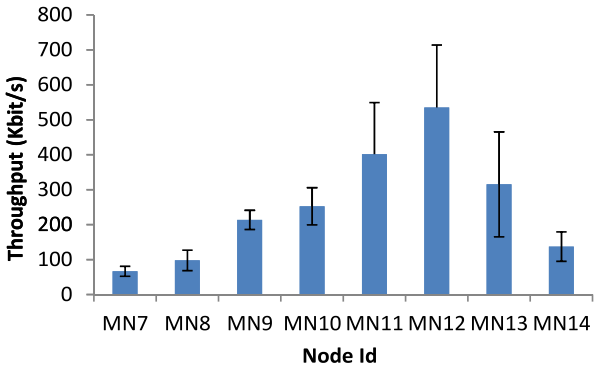

Fig. 13. Throughput in the outdoor tree-based network when nodes concurrently transmit the data.

reached a network with 20 hops. Meanwhile, for another half of the day, the 16th hop was reached in the 30 m hop-distance network (but some links have disconnected during the evaluation). For most nodes, the packet loss is in the range of 1–2% which is acceptable in an intermittent outdoor wireless environment. Even the largest packet loss at node 15 is only 5%, which is small enough and acceptable for VoIP services and web browsing which are the main targeted services of this work.

In addition to the tandem topologies, the tree-based network (Fig. 7b) is useful for verifying the network's usability when an intermediate node serves several clients. In this deployment, the hop-distance was set to 30 m, while nodes at the same level (same number of hops to the root) are close to each other (about 2 m). In this experiment, we have evaluated the throughput at level-3, i.e., the leaf nodes, when they sent data to MN0 concurrently. It should be noted that this experiment was conducted at ISU in an outdoor environment. We did not evaluate RTT and packet loss because previous experiments (e.g., Fig. 11) demonstrated that they are minimally affected for short paths.

The experiment was conducted three times and the average values are plotted in Fig. 13. The results reveal that the total throughput is around 2 Mbps which is similar to the throughput at hop 3 in the 30 m hop-distance tandem network as shown in Fig. 11 b. Since no fairness mechanism has been employed in TDRAN, throughput is different at different nodes. However, the lowest throughput (around 100Kbps) is adequate for web browsing. If a relevant fairness mechanism is integrated, the proposed approach would be more robust.

5.5. Usefulness of the CST approach

CST practicality in re-configuring disconnected links has been evaluated: two nodes (among 20 nodes) in the 15 m hop-distance tandem network were disconnected and a network administrator was asked to find and fix those disconnections. It took him 17 min to complete the task by moving around (starting from the farthest node) to check from node to node. When he was allowed to use CST, it took him only 8 min to finish the task since he could find out exactly which nodes have been disconnected by looking at the CST at the farthest node. The time he needed was for physically moving to the disconnected nodes. Of course, in a real situation the link will re-established automatically when the user moves closer to a VAP.

It should be noted that, in the 15 m hop-distance network, the CSTs were always correctly updated according to the network connectivity status. However, in the 30 m hop-distance counterpart, the CSTs sometimes could not update correctly in a real-time, especially for the farther-away nodes, located 7 or more hops away from the IGW. The reason is higher packet loss, which leads to lost CST notifications. Consequently, improving the reliability of CST notification will be considered in future work.

5.6. Verification under real Internet-based services

We also have verified several actual Internet-based services, namely text-based web surfing; video streaming (on YouTube); text, voice, and video chats using Skype on the deployed topologies to reveal the usefulness of the proposed approach to disaster recovery. Concretely, the above services were verified on both the tree-based network shown in Fig. 7b, and the tandem networks. For the tandem networks, both the indoor (50 m hop-distance at IPU shown in Fig. 9) and outdoor (30 m hop-distance at ISU) settings were verified. In these experiments, rather than capturing performance values such as throughput, RTT, packet loss as in Section 5.4, we asked participants for their perceived delay, jitter or any abnormal effects of these services when they used them. Qualitative results are summarized in Table 3.

As shown in Table 3, all of the aforementioned services worked smoothly in the tree-based network since this topology is just a combination of short (in terms of hop count) chain-based topologies. For the tandem networks, the services worked well when the path length is less than 9 hops in the indoor 50 m hop-distance

Table 3
User-perceived quality of Internet-based service.

Application	Topology		
	Tree-based network	Tandem network (Indoor-50 m, IPU)	Tandem network (Outdoor-30 m, ISU)
Web site surfing/Textual chat using Skype	Smoothly (no perceived delay/jitter)	Smoothly	Smoothly
Video streams (YouTube)	Smoothly	Smoothly when the path is less than 9 hops. From MN10, there is some perceived delay.	Smoothly when the path is less than 15 hops. From MN16, there is some perceived delay.
Video chat (Skype) (between MNi and MN0)	Smoothly	Smoothly when the path is less than 9 hops. From MN10, some jitter occurs.	Smoothly when the path is less than 15 hops. From MN16, some jitter occurs.

experiments at IPU and 15 hops in the outdoor 30 m hop-distance experiments at ISU, respectively. When the number of hops is larger, some small jitter occurred on video streams (Skype video chat). However, the higher delays are short and can be ignored, especially in the case of disaster recovery. As the network can be extended to 20 hops by 15 m-distance and 16 hops by 30 m-distance networks, which result in 300 m and 480 m (respectively) in radius or about 1 km in diameter, while providing acceptable user-perceived Internet-based services, we conclude that this approach is practical for disaster recovery, specifically around the evacuation centers.

6. Conclusion

The focus of this article was on providing **Internet connectivity** to disaster victims in the fastest and simplest way. The novel **wireless multihop communication abstraction** (WMCA) concept and the practical **tree-based disaster recovery network** (TDRAN) scheme utilizing the **software-based access node** (SAN) approach were proposed to hide the complexity of multihop network establishment and configuration. As a result, the network can be quickly set up using on-site available commodity mobile devices without any requirement for deployment of additional equipment. Users can easily access the Internet via TDRAN, as if they were connected to conventional APs, and automatically contribute to the network extension. This trait provides a seamless "self-support" feature from local communities for effective emergency response. The proposed approach also benefits network programmers and administrators because it decouples software development and network operations for multihop wireless networks.

Our field experiments with medium-size networks demonstrated the feasibility of on-site configured wireless access networks for disaster recovery. The effectiveness and scalability of the proposed network abstraction and protocols were thoroughly evaluated and analyzed. The results show that the proposed techniques can quickly establish an access network that covers a large area, around 1 km in diameter, which is suitable for emergency response and evacuation centers. Finally, existing Internet services, including audio and video streaming, worked well over these networks.

Acknowledgments

We would like to express our gratitude to Professor Shingo Minato and Professor Michiharu Masui at Ishinomaki Senshu University for their valuable support in terms of facilities and man power for our field experiments. We would also like to thank Dr. Matthias Herlich from the Computer Science and Mathematics Department, Faculty of Electrical Engineering, Universitat Paderborn, Germany who provided us with comments regarding the analysis of the experimental data.

References

[1] M. Portmann, A.A. Pirzada, Wireless mesh networks for public safety and crisis management applications, IEEE Internet Comput. 2 (1) (2008) 18–25.

[2] R.A. Lawson, Tsunami detection systems for international requirements, OCEANS07, Vancouver, Canada, September 2007, pp. 1–7.

[3] TohokuEarthquake, Great East Japan Earthquake (March 2011), URL: http://www.mext.go.jp/english/incident, accessed Nov., 2014.

[4] T.M. Quang, K. Nguyen, E. Kamioka, S. Yamada, Tree-based disaster recovery multihop access network, in: 19th Asia-Pacific Conference on Communications (APCC13), Bali, Indonesia, August 2013, pp. 415–420.

[5] T.M. Quang, K. Nguyen, S. Yamada, DRANs: resilient disaster recovery access networks, in: First IEEE International Workshop on Future Internet Technologies (IWFIT 2013), in Conjunction with IEEE COMPSAC 2013, Kyoto, Japan, 22–26 July, 2013, pp. 754–759.

[6] T.M. Quang, K. Nguyen, B. Cristian, S. Yamada, On-the-fly establishment of multihop wireless access networks for disaster recovery, IEEE Commun. Mag. 52 (10 (October)) (2014) 60–66.

[7] R. Chandra, P. Bahl, Multinet: connecting to multiple IEEE 802.11 network using a single wireless card, IEEE INFOCOM Hong Kong, March 2004, pp. 882–893.

[8] N. Uchida, K. Takahata, Y. Shibata, Proposal of never die network with the combination of cognitive wireless network and satellite system, in: The 13th International Conference on Network-Based Information Systems (NBiS2010), Gifu, Japan, September 2010, pp. 365–370.

[9] N. Uchida, K. Takahata, Y. Shibata, N. Shiratori, Never die network extended with cognitive wireless network for disaster information system, in: The Fifth International Conference on Complex, Intelligent and Software Intensive Systems, Seoul, Korea, June 2011, pp. 24–31.

[10] H. Okada, H. Oka, K. Mase, Network construction management for emergency communication system SKYMESH in large scale disaster, in: IEEE Fourth International Workshop on Management of Emerging Networks and Services, California, US, December 2012, pp. 875–880.

[11] K. Fall, A delay-tolerant network architecture for challenged internets, in: Proceedings of the ACM SIGCOMM'03, NY, USA, 2003, pp. 27–34.

[12] D. Amit, A.V. Vasilakos, Backpressure-based routing protocol for DTNs, Proceedings of the ACM SIGCOMM'10, New Delhi, India, August 2010, pp. 405–406.

[13] Y. Song, L. Liu, H. Ma, A.V. Vasilakos, A biology-based algorithm to minimal exposure problem of wireless sensor networks, IEEE Trans. Netw. Serv. Manage. 11 (3) (September 2014) 417–430.

[14] L. Liu, Y. Song, H. Zhang, H. Ma, A.V. Vasilakos, Physarum optimization: a biology-inspired algorithm for the Steiner tree problem in networks, IEEE Trans. Comput. 64 (3) (March 2015) 818–831.

[15] P. Li, S. Guo, S. Yu, A.V. Vasilakos, Reliable multicast with pipelined network coding using opportunistic feeding and routing, IEEE Trans. Parallel Distrib. Syst. 25 (12) (December 2014) 3264–3273.

[16] T. Meng, F. Wu, Z. Yang, G. Chen, A.V. Vasilakos, Spatial reusability-aware routing in multi-hop wireless networks, IEEE Trans. Comput. PP (99) (2015) 1–13.

[17] X.Y. Liu, Y. Zhu, L. Kong, C. Liu, Y. Gu, A.V. Vasilakos, M.Y. Wu, CDC: compressive data collection for wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 26 (8) (August 2015) 2188–2197.

[18] X. Xu, R. Ansari, A. Khokhar, A.V. Vasilakos, Hierarchical data aggregation using compressive sensing (HDACS) in WSNs, ACM Trans. Sens. Netw. 11 (3) (March 2015) 1–25.

[19] M. Youssef, M. Ibrahim, M. Abdelatif, C. Lin, A.V. Vasilakos, Routing metrics of cognitive radio networks: a survey, IEEE Commun. Surv. Tutorials 16 (1) (2014) 92–109.

[20] L. Peng, G. Song, Y. Shui, A.V. Vasilakos, Codepipe: an opportunistic feeding and routing protocol for reliable multicast with pipelined network coding, in: Proceedings IEEE INFOCOM'12, Florida, USA, 2012, pp. 100–108.

[21] IEEE Std 802.11sTM, Amendment 10: Mesh Networking, September 2011.

[22] C.C. Ricardo, M.S.C. Luiz, S.M.C. Debora, A.N.V. Celio, IEEE 802.11s multihop MAC: a tutorial, IEEE Commun. Surv. Tutorials 13 (1) (2011) 52–66.

[23] S.C. Yang, M.K. Yoon, D.H. Kim, J.D. Kim, Implementation of a multi-radio, multi-hop wireless mesh network using dynamic WDS based link layer routing, in: Seventh International Conference on Information Technology, Nevada, USA, April 12–14, 2010, pp. 908–913.

[24] V. Bahl, R. Chandra, P.P.C. Lee, V. Misra, J. Padhye, D. Rubenstein, Y. Yu, Opportunistic use of client repeaters to improve performance of WLANs, in: ACM CoNEXT 2008, Madrid, Spain, December 10–12, 2008, pp. 1–12.

[25] D. Camps Mur, A. Garcia, P. Serrano, Device to device communications with wi-fi direct: overview and experimentation, IEEE Wireless Commun. Mag. 20 (3) (June 2013) 96–104.

[26] Emergency Management Applications for the LAN-Cell 3G/4G Cellular Router. URL: http://www.proxicast.com/emergency/emergency-dr.htm, accessed Nov., 2014.
[27] D. Abusch-Magder, P. Bosch, T.E. Klein, P.A. Polakos, L.G. Samuel, H. Viswanathan, 911-NOW: a network on wheels for emergency response and disaster recovery operations, Bell Labs Tech. J. 11 (4) (2007) 113–133.
[28] T. Sakano, Z.M. Fadlullah, Thuan Ngo, H. Nishiyama, M. Nakazawa, F. Adachi, N. Kato, A. Takahara, T. Kumagai, H. Kasahara, S. Kurihara, Disaster resilient networking—a NEW vision based on movable and deployable resource units (MDRUs), IEEE Netw. 27 (4) (July/August 2013) 40–46.
[29] Y. Al-Hazmi, H. De Meer, Virtualization of 802.11 interfaces for wireless mesh networks, in: Eighth International Conference on Wireless On-Demand Network Systems and Services (WONS), Bardonecchia, Italy, January 26–28, 2011, pp. 44–51.
[30] H. Wirtz, T. Heer, R. Backhaus, K. Wehrle, Establishing mobile ad hoc networks in 802.11 infrastructure mode, Sixth ACM Workshop on Challenged Networks (CHANTS '11), New York, NY, USA, ACM, 2011, pp. 49–52.
[31] M.H. Sarshar, P.K. Hoong, I.A. Abdurrazaq, Nodesjoints: a framework for tree-based MANET in IEEE 802.11 infrastructure mode, in: 2013 IEEE Symposium on Computers & Informatics (ISCI), Langkawi, Malaysia, April 7–9, 2013, pp. 190–195.
[32] A.J. Nicholson, S. Wolchok, B.D. Noble, Juggler: virtual net-works for fun and profit, IEEE Trans. Mobile Comput. 9 (1) (January 2010) 31–43.
[33] Defining I/O Control Codes. URL: http://msdn.microsoft.com/en-us/library/windows/hardware/ff543023(v=vs.85).aspx, accessed Nov., 2014.
[34] Translated and Routed Connection. URL: http://technet.microsoft.com/en-us/library/cc754703(v=ws.10).aspx, accessed Nov., 2014.
[35] Y. Yanjun, C. Qing, A.V. Vasilakos, EDAL: an energy-efficient, delay-aware, and lifetime-balancing data collection protocol for wireless sensor networks, in: IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems, Hangzhou, China, 2013, pp. 182–190.
[36] K. Nguyen, T.M. Quang, S. Yamada, A software-defined networking approach for disaster-resilient WANs, in: IEEE 22nd International Conference on Computer Communications and Networks (ICCCN), Nassau, Bahamas, 2013, pp. 1–5.
[37] FPing, URL: http://www.kwakkelflap.com, accessed Nov., 2014.
[38] Iperf, URL: http://iperf.fr, accessed Nov., 2014.
[39] Connectify, URL: http://www.connectify.me, accessed Nov., 2014.

Quang Tran Minh is a lecturer at Faculty of Computer Science and Engineering, Ho Chi Minh City University of Technology, Vietnam and a visiting researcher at Shibaura Institute of Technology, Tokyo, Japan. He has been a researcher at Network Design Department, KDDI R&D Laboratories, Saitama, Japan (2014–2015) and a researcher at Principles of Informatics Research Division, National Institute of Informatics, Tokyo, Japan (2012–2014). His research interests include mobile and ubiquitous computing, network design and traffic analysis, disaster recovery systems, data mining, and ITS. He received his Ph.D. in Functional Control Systems from Shibaura Institute of Technology. He is a member of IEEE.

Yoshitaka Shibata received his Ph.D. in Computer Science from the University of California, Los Angeles (UCLA), USA in 1985. From 1985 to 1989, he was a research member in Bell Communication Research (former AT&T Bell Laboratory), USA, where he was working in the area of high-speed information network and protocol design for multimedia information services. From 1989 to 1998, he was with Information and Computer Science Department in Toyo University, Japan as a professor, where he conducts an intelligent multimedia network laboratory. Since 1998, he is working for Iwate Prefectural University, Japan as an executive director of Media Center and a professor of Faculty of Software and Information Science in the same university. Currently he is a vice president of Iwate Prefectural University. His research interests include Disaster Information Networks, Wireless Adhoc Networks, Cognitive Networks, New Generation Networks. He is a member of IEEE, ACM, Information Processing Society of Japan (IPSJ) and Institute of Electronic and Communication Engineering in Japan (IEICE).

Cristian Borcea is an associate professor in the Department of Computer Science at New Jersey Institute of Technology, Newark, NJ, USA. He is also a visiting associate professor at the National Institute of Informatics, Tokyo, Japan. 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 IEEE, ACM, and Usenix.

Shigeki Yamada is a professor and director in the Principles of Informatics Research Division at National Institute of Informatics, Tokyo, Japan. 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 senior member of IEEE, and a member of IEICE and IPSJ.