Toward Commodity Wireless Multihop Access Networks

Quang Tran Minh (1)(2), Kien Nguyen(1), Shigeki Yamada (1)
(1) National Institute of Informatics, Tokyo, Japan
(2) Hochiminh City University of Technology, Hochiminh City, Vietnam
{quangtran, kienng, shigeki}@nii.ac.jp

Abstract—Wireless multihop access network is an appropriate approach to providing Internet access to applications such as last-mile and rural area communications, disaster recovery, etc. However, the realization of the existing wireless access networks is still limited. The main reasons are that they require particular hardware and software to be installed at pre-defined locations, or it is costly to deploy enough density nodes in a vast area for network formation. This paper proposes a novel approach to automatically set up multihop access networks, bringing Internet connectivity to users by leveraging their commodity mobile devices. In this work, a single WiFi interface equipped mobile device is transformed into a virtual access point (VAP) using wireless virtualization. As a result, each node works in both the station (STA) and the VAP modes to connect with each other forming tree-based networks which extend the Internet connectivity. Users can access Internet through the proposed network easily as if they are connected to the conventional access points (APs) and unconsciously contribute to the network extension. A prototype has been implemented and evaluated to confirm the feasibility as well as the effectiveness of the proposed approach.

Index Terms - Commodity access network, multihop, tree-based topology, wireless virtualization.

I. INTRODUCTION

Internet access is a vital factor in the modern life. It affects almost every activity from education, business, governmental execution, to entertainment, health care, or even emergency relief. Unfortunately, many people still cannot access Internet in their daily activities or even in very critical situations such as in disasters or health-care service requests. Concretely, providing Internet access to rural areas is still challenging to both academia and industry. In addition, in severe disasters, main parts of the communication infrastructures might be damaged, disconnecting people from the outside world, making the situation more serious [1].

Wireless mesh network (WMN) [2] is one of the possible solutions for last-mile Internet access [3]. Infrastructure-mesh network consisting of a set of mesh-routers (MRs) and Internet gateways (IGWs) to form the mesh backbone and provide Internet access to mobile nodes (MNs) is the most commercial interest approach. The most significant impact of this technology is that it provides Internet access to the areas where wired infrastructure is not viable (e.g., difficult or economically infeasible to deploy). As a result, this approach can be applied for last-mile or rural areas Internet access in some extents. However, the realization of such infrastructure-mesh networks is still limited since they need dedicated hardware (e.g., MRs), complicated routing protocols, and more important the whole system must be installed and deployed in advance at particular areas.

One of the solutions for the aforementioned issue is to devise a scheme whereby access networks can be automatically set up using commodity mobile devices. The newly established network is extended through multihop communication to reach viable communication infrastructures, such as still-alive access points (APs) in disaster areas or APs at the edges of a backbone network (wired networks or WMN) in last-mile and rural area Internet access situations. This work aims at quickly setting up multihop access networks to extend Internet connectivity from these APs to users. As the network is created from commodity mobile devices without any requirement for additional hardware, the access network becomes a commodity one (i.e., can be used without interference to their daily activities). To achieve this goal, these networks must be established transparently to users, as ordinary users cannot be expected to perform complicated set-up operations. The main contributions of this work can be summarized as follow:

(i) Transform commodity mobile devices into virtual access points (VAPs) using wireless virtualization technology.
(ii) Bring the Internet connectivity to users by establishing tree-based networks of VAPs. Automatic configuration of IP addresses and DNS resolution for smooth Internet connectivity are also addressed.
(iii) A simple yet effective mechanism for failover in tree-based topology is devised.
(iv) A preliminary prototype on Windows-based laptops has been built and tested to confirm the feasibility and effectiveness of the proposed scheme. The prototype provides an essential benchmark for developing commodity wireless multihop access networks.

The rest of the paper is organized as follows: Section II presents literature review on related work. The proposed approach on commodity wireless multihop access network is addressed in Section III. Section IV presents the preliminary prototype while the feasibility and the effectiveness of the proposed approach are evaluated in Section V. Section VI concludes this work and draws out the future work directions.

II. RELATED WORK

Wireless multihop ad hoc network such as wireless backhaul mesh network (WMN) [2], mobile ad hoc network (MANET) [4], and delay/disruption tolerant network (DTN) [5] has been an active research field in the last decade. These researches focus on providing communication means in the
areas where wired infrastructure networks cannot be deployed because of technically and/or economically infeasible. Several works have been dedicated to last-mile communications [3], rural area Internet access [6], and continuously Internet connectivity for emergency responses [7]. Although these approaches are potential, there are still fundamental barriers such as complexity of network configurations, dedicated hardware (MRs) and software (routing protocols) requirements, complexity in allocating and managing ID, etc., that hinder their real-world realization.

The emerging IEEE 802.11s standard [8] provides a new framework for mesh network, reducing the network establishment difficulties. However, IEEE 802.11s compliant network interface cards (NICs) are required and the number of nodes in this technology is limited to 32. WiFi Direct [9] is closely related to our proposal where each node can work in both the STA (i.e., client) mode for Internet access, and software-based AP mode for serving other nodes. However, the feasibility of multihop-based Internet connectivity sharing on WiFi Direct has not been addressed. On-demand deployment of Internet connected WiFi APs or cellular base stations, which are carried by emergency vehicles, is a common solution in disaster recovery [10]. SkyMesh [11] applied the same approach by attaching MRs to balloons to form mesh-backbones on the sky. The merit of the SkyMesh is that the WMN is deployed on the sky to alleviate the line-of-sight effect so that transmission range can be significantly extended. Obviously, these solutions are expensive, and are still stuck in the inherent issues such as the mesh network must be established in advance at the places where constructors can reach and requires special equipments like MRs and vehicles/balloons. Consequently, these approaches are not fully suitable for last-mile/rural area Internet access and disaster recovery Internet connectivity.

Arguably, MANET [4] can resolve the aforementioned issues since it can be configured using client devices. In fact, many issues related to the real deployment (not merely simulation verifications) of MANETs still remain unsolved. For instance, similar to WMN, special network auto-configuration software (NAS) including multihop routing protocols such as AODV [12], OLSR [13], etc., must be installed in each MN beforehand. In addition, it is too complicated to ordinary users to configure and change their mobile devices into ad-hoc mode for MANET establishment.

Different from the existing technologies, our scheme establishes a multihop access network using commodity WiFi-equipped devices which are always available on-site, and the network can be extended to an arbitrary number of nodes. This work complements existing solutions with a free and fast approach to bring Internet access to the users.

III. COMMODITY MULTIHOP ACCESS NETWORK

A. Overall Architecture

Figure 1 shows the overall architecture of the proposed scheme that extends the Internet connectivity to users who were left disconnected because of backbone network failures or unreachable (e.g., last-mile communication). Here, the devices which are close to the active AP (e.g., the surviving AP in a disaster which has Internet connectivity), such as mobile nodes MN1 and MN5, try to associate to this AP (step 1). The AP initiates network establishment by asking these MNs to download the necessary network auto-configuration software, NAS (step 2). This software transforms associated nodes into virtual access points (VAPs), thus extending Internet access to farther nodes (step 3). Consequently, the NAS will be uploaded to any node that associates with a VAP making every intermediate mobile node a VAP. These iterations create a tree-based network bringing Internet connectivity to farther users (e.g., MN3, MN4).

As illustrated, the proposed scheme utilizes on-site commodity mobile devices such as laptops, tablets, smart phones, to set up on-demand wireless access networks. This approach is not only cost effective, but also fast in providing broadband Internet access to areas where wired infrastructure is either difficult or economically infeasible to deploy. Specifically, the proposed scheme is applicable for last-mile/rural area communications or Internet connectivity for quick emergency response.

B. Network Design

As mentioned, the NAS is the heart of the proposed scheme. It is assumed that a network controller on the backbone network activates the NAS-trigger on the reachable APs so that every node that connects to it is forced to download the NAS as shown in step 2 in Fig. 1. The NAS including a NAS-trigger can also be installed on user mobile devices (e.g., volunteer devices) to transform them into VAPs a priori. As a result, any mobile node that connects to a VAP is forced to download the NAS and transforms itself into a VAP, thus the Internet access is extended. The main functionalities of NAS are illustrated in Fig. 2 and described as follows:

![Functionalities of the NAS](image)

Figure 2. NAS’s main functionalities

1. Access network node transformation

Each intermediate node must maintain two modes, namely STA and VAP, to connect to two networks concurrently. The STA mode connects the MN to the upstream AP (or VAP) for Internet access, while the VAP mode shares this Internet connection to the vicinity. The simplest way to realize this

![Image 329x576 to 535x682](image)

Figure 1. Multihop access network for Internet connectivity extending based Internet connectivity bringing broadband Internet access to areas where wireless infrastructure is either difficult or economically infeasible to deploy.
functionality is having multiple wireless interfaces at each node. However, this is not a realistic requirement. Switching between these modes using a single built-in wireless interface is an alternative. Nevertheless, the switchover time is long enough to significantly degrade the network performance, reducing multihop communication capability/coverage. To solve this issue, this work leverages wireless virtualization [14] to abstract a single physical wireless interface into two logical interfaces: one is used for STA mode (WIF1), and the other for VAP mode (WIF2). In order to transform a commodity mobile node into a VAP, we use a software-based AP approach [15].

2. Multihop communication simplification

Routing is one of the key challenges in wireless multihop communications. Several researches focus on multi-hop routing protocols such as AODV [12] and OLSR [13] which are the two most successful and representative for reactive and proactive approaches, respectively. However, implementing these protocols faces on several difficulties in severe environments like disasters. Concretely, they must be installed and appropriately configured in each MN in advance. These requirements are impractical in real-world applications since ordinary users are not expected to have enough technical skills to configure the networks.

As shown in Fig.1, our approach is different as the proposed scheme quickly establishes a tree-based network which simplifies the routing tasks since routing for Internet communication is done along this tree. As a result, the network establishment is simplified minimizing routing overhead 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. Finally, the packets reach the actual AP where a traditional routing protocol is implemented to route the packets in the Internet. It should be noted that communication is always initiated by mobile nodes which are not directly reachable from the Internet as they use private IP addresses as described in the following subsection.

3. IP address management and DNS resolution

For Internet connectivity, IP address allocation and duplication avoidance as well as DNS resolution are needed. Each MN has two logical wireless interfaces (WIF1 and WIF2), thus each one must be assigned an individual IP address. The difficulty is how to automatically assign the IP addresses to them considering IP address duplication avoidance. It should be noted that there is no centralized entity such as a centralized DHCP server for serving this task.

In the proposed scheme, the VAP on WIF2 serves as a network gateway for the associated nodes, WIF2's IP address is in the form of 192.168.x.1. In order to create such an IP automatically, x is computed from the MAC address of the physical WIF (e.g., using a hash function). A DHCP server is installed on this VAP, thus any node that associates with it is assigned (to the node's STA interface) an IP in the form of 192.168.x.2 to its WIF1. Here, z is in the range of 2 to 254 as determined by the DHCP server. It should be noted that IP addresses of the two interfaces (WIF1 and WIF2) in the same node cannot belong to the same subnet (192.168.x.0/24). Since, the WIF1's IP address is automatically assigned by the DHCP server on its upstream VAP, the node cannot control this process. However, the node can avoid the aforementioned confliction by checking the automatically generated value for the third octet of its WIF2's IP (i.e., x) to assure that this value is different from the third octet in its WIF1's IP. The procedure for creating WIF2's IP on the considered node is described in Fig. 3.

```
Procedure IPAllocation()
    int x = Hash(WIF1's MAC address);
    int y = third octet of the WIF1's IP;
    if x = y {
        x++;
    }
    Assign 192.168.x.1 as WIF2's IP
```

As each VAP implements its own DHCP server for assigning local/private IP addresses to its STAs/clients, network address translators (NATs) are needed at each VAP in order to communicate over the Internet. NATs also support a simple layer 3 routing mechanism over the 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 an intermediate node identifies to which client the data should be forwarded. In addition, since each VAP serves as a default network gateway, it supports DNS resolution for the associated nodes. Accordingly, any node that requires an Internet access just asks for DNS resolution by sending a DNS query to the default gateway. Intermediate nodes forward the queries to their default gateways until they reach the AP and finally resolved.

Figure 3. Automatic IP address allocation on the VAP's interface

Figure 4. Internet access through the proposed network
Figure 4 illustrates the procedure that allows a common node (MN2) to connect to a VAP (at MN1) for Internet access and extending this Internet connectivity. After associating (steps 1 and 2) with the surviving VAP, MN2 is forced to download NAS from the associated VAP (step 3). This software transforms MN2 into a VAP (step 4) using its second logical wireless interface, while the first logical interface works as a common client. Consequently, MN2’s VAP brings the Internet connectivity to its vicinity. As shown, the IP addresses of the two logical interfaces at MN2 are accordingly assigned. After having Internet connection, MN2 can raise a DNS query (step 5) for HTTP request (step 7). The DNS query is sent to its default gateway, namely the VAP on the MN1 (step 5). This intermediate node continues forwarding the query to its default gateway, namely the actual AP (step 5.1), where the query is finally resolved.

The simplicity in network establishment and routing (by directly forwarding packets to the next hop) in the tree-based topology is the most important feature that makes the realization of the proposed approach more feasible. However, because of this simplicity, the proposed scheme does not manage the whole topology information (each node just knows about its directly connected nodes, namely its parent and children), the network cannot automatically reconfigure when failures occur. Our target is not to make the network auto-healing but, instead we provide a user friendly approach for manual network reconfiguration under a simple yet effective connectivity status notification mechanism.

4. Connectivity status notification

In the proposed scheme, each user/node just knows about its direct parent (i.e., upstream VAP), therefore it cannot know about any failure at any farther link in the path to the actual AP. As a result, a user cannot understand the reason why while its connection to the VAP is still active and is in a good quality but he/she cannot access to the Internet. Consequently, he/she cannot know where to the network failure occurs to fix. To solve this issue, each node should manage a connectivity status table (CST) which contains the status of all the links from the node to the actual AP. This table is managed by the "connectivity status management" component implemented on the NAS as shown in Fig. 2. An example of the connectivity status and CTS is depicted in Fig. 5.

![Figure 5](image)

Here a link describes a connection between a node and an AP/IGW (or VAP) in a network represented by a SSID (e.g., link A<>B is represented by SSID2). The status of a link can be connected ("C") or disconnected ("D"). A link can be failed (disconnected) because of battery shortage or node moves. A link can up (connected) again when the failure is recovered (i.e., the disconnected node (re-)connects to its previous associated VAP or to a new VAP). Each node manages a CST whose each row represents the status of a particular upstream link (from the node to the actual AP/IGW). The structure of this table is "SSID, Status, hop_count" where the hop_count is the number of hops from the node to the AP/IGW. Obviously, with this table, user can know why he/she cannot access to the Internet even though the current connection to the upstream VAP is still alive, and where (at what link) the connectivity has been failed to conduct a network reconfiguration.

In order to update a CST, the connectivity status is notified from the upstream node (VAP) to downstream nodes (STAs) under following principles: (i) when a link downs or ups, the corresponding up/down link notification is automatically notified (by the immediate connected nodes) and propagated (by downstream nodes) to any node in the path until the notification reaches the leaf nodes. This notification is conducted by broadcasting; (ii) a node can raise a CST request (manually) to update its CST. According to the CST request, a CST response is replied. The CST request and CST response are paired with each other and sent by unicaicing. It should be noted that, in every notification (CST request, up/down link notification, CST propagation), the whole CST of the notifying node is sent (unicast or broadcast) to downstream nodes. As mentioned, 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 protocol (unicast or broadcast). The packet formats and their corresponding fields are described in detail as follow and in Table I, respectively.

- CST request(SrcIP, DestIP, TransID, Type)
- CST response(SrcIP, DestIP, TransID, Type, CST_Content)
- CST propagation(SSID, TransID, Type, CST_Content)

TABLE I. FIELDS IN CONNECTIVITY STATUS NOTIFICATION MESSAGES

<table>
<thead>
<tr>
<th>Field</th>
<th>Size (Bytes)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcIP</td>
<td>4</td>
<td>IP address of the requester (children node)</td>
</tr>
<tr>
<td>DestIP</td>
<td>4</td>
<td>IP address of the receiver (parent node)</td>
</tr>
<tr>
<td>TransID</td>
<td>2</td>
<td>Transaction ID (used for avoid looping)</td>
</tr>
<tr>
<td>Type</td>
<td>1</td>
<td>The message type (1 means CST request, 2 CST response, 3 CST propagation)</td>
</tr>
<tr>
<td>SSID</td>
<td>20</td>
<td>SSID of the notification broadcasting node</td>
</tr>
<tr>
<td>CST_Content</td>
<td>Variable</td>
<td>The content of CST. Its length is variable depending on the number of rows in CST</td>
</tr>
</tbody>
</table>

The CST_Content on the CST_response and CST_propagation presented in Table I is a variable length field with following format.

CST_Content (<SSID, status, hop_count>{<next row>})

The CST_Content is the content of the CST table of a node sent to its clients (under a request or auto notification). Each
row of this table is a triple of <SSID, Status, hop_count> as mentioned previously.

IV. PROTOTYPE

This section presents the preliminary prototyping of the proposed scheme using commodity mobile devices. An experimental network topology is illustrated in Fig. 6. Here, intermediate nodes with the NAS deployment (i.e., can serve as both STA and VAP modes) are ASUS U24A-PX3210 laptops with 4GB memory, corei5 2.5 Ghz CPU, Atheros AR9002WB - 1NG WiFi Network Adapter, running on Windows 7. As shown, any WiFi equipped mobile device such as smart phone, laptop, etc., can easily access to the Internet through our proposed network as if it is connected to a conventional AP. The implementation details are described as follows.

1. Wireless virtualization and VAP transformation: This step virtualizes the single built-in WiFi NIC into 2 logical NICs and transforms the commodity mobile devices into a VAP using the second logical NICs (WIF2). These two tasks are performed using the command shown below (line (1)), where <ssid> is the SSID of the newly-set VAP and <passPhrase> is the password used for associating with this VAP. The established VAP is activated by the command in line (2).

   (1) Netsh Wlan set hostedNetwork Mode=allow
       SSID=<ssid> Key=<passPhrase> keyUsage=persistent
   (2) Netsh Wlan start hostedNetwork

2. Deploying DHCP server and NAT on the established VAP: This step installs the DHCP and NAT functionalities on the newly built VAP. Windows provides the Internet Connection Sharing (ICS) utility to share the Internet connection of a particular node. This utility includes DHCP and NAT functionalities to be utilized for our purpose. Accordingly, ICS is used to share the current wireless connection at the primary logical interface (WIF1) with the secondary interface (WIF2) at the VAP. As a result, the VAP is ready to accept any association, assign IP addresses, and deal with DNS resolution for new connected clients.

V. EVALUATION

The main purpose of this evaluation is to verify the feasibility of the proposed network in terms of bringing Internet connectivity to farther users. The network performance in terms of delay, throughput as well as the feasible accessibility to real Internet-based services, such as voice chat on Skype and video streaming on YouTube, on a multihop topology and multiple users has been evaluated.

Several field experiments have been conducted in Iwate Prefectural University, Japan. Iwate is the prefecture that has been significantly affected by the Great East-Japan Earthquake. A tandem and a tree based network topologies were created as shown in Fig. 7 and Fig. 8, respectively. Here, the distance between any pair of nodes (in any link) was 50m. MN0 was connected to the real AP/GW, while MNi (i=1...6) was connected to the Internet via the deployed network.

![Figure 7. A tandem multihop access network with link-distance of 50m](image)

![Figure 8. A tree-based multihop access network whose link-distance is 50m](image)

As expected the network configuration procedure works correctly at each node, where the single wireless NIC was abstracted into 2 logical NICs with appropriate IP addresses. Table II shows an example observed from the tandem network in Fig. 7. This network was also used for evaluating of the network performance in terms of delay and throughput for a multihop topology, since this network shows the worst case in terms of hop counts from the node to the actual AP.

<table>
<thead>
<tr>
<th>Node</th>
<th>STA (WIF1) IP</th>
<th>VAP (WIF2) IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>MN0</td>
<td>192.168.137.141</td>
<td>192.168.137.1 (default GW for MN1)</td>
</tr>
<tr>
<td>MN1</td>
<td>192.168.137.2</td>
<td>192.168.124.1 (default GW for MN2)</td>
</tr>
<tr>
<td>MN2</td>
<td>192.168.124.50</td>
<td>192.168.97.1</td>
</tr>
<tr>
<td>MN3</td>
<td>192.168.97.35</td>
<td>192.168.133.1</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Figure 9 shows the average round trip time (RTT) and the throughput between MNi (i=1...6) and MN0 of the tandem network shown in Fig. 7. Although the RTT has higher values when the number of hops increases, the RTT is still low, namely less than 200ms, even for the longest path. The
throughput decreases with the number of hops, but it still reaches an acceptable value, 1.6Mbps, in the worst case. Thus, we can conclude that the overhead (especially that of wireless virtualization) doesn’t impact much the network delay and throughput. These network performance parameters are acceptable for smooth VoIP services and for web browsing.

![Graph showing the relationship between hop count and throughput](image)

**Figure 9.** Round trip time latency and Throughput in the proposed network

We also verified several actual Internet-based services, namely text-based web surfing; video streaming (on YouTube); text, voice, and video chat using Skype on both the tandem and tree-based networks illustrated in Fig. 7, and Fig. 8, respectively. These services worked smoothly even in the worst scenario (i.e., video chat from MN6 in the tandem network) as shown in Table III.

<table>
<thead>
<tr>
<th>Application</th>
<th>Tree-based network</th>
<th>Capacity</th>
<th>Tandem network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web site surfing</td>
<td>Smoothly</td>
<td>Smoothly</td>
<td>Smoothly</td>
</tr>
<tr>
<td>Video streams (YouTube)</td>
<td>Smoothly</td>
<td>Smoothly</td>
<td>Smoothly</td>
</tr>
<tr>
<td>Video chat (Skype)</td>
<td>Smoothly</td>
<td>Smoothly</td>
<td>Smoothly</td>
</tr>
</tbody>
</table>

**VI. CONCLUSION AND FUTURE WORK**

This article proposed a novel approach to on-site establishment of multihop wireless access networks which can be utilized for last-mile communication, rural area Internet access of keeping Internet connectivity for disaster recovery. The main novelty of this approach is that Internet connectivity is moved close to the users using commodity mobile devices. It is not only cost effective but also transparent to ordinary users since they can connect to the network as easily as they are connected to conventional APs. Moreover, when connected users naturally contribute to the network extension.

A real prototype has been built and tested in an area that was widely affected by the Great East-Japan Earthquake in 2011. Experiments conducted with multihop wireless access networks have demonstrated the feasibility and the effectiveness of the proposed approach. Concretely, they show that the proposed scheme is practical and ready to be realized in real-world applications. Nevertheless, the tree-based topology in the proposed approach also consists of inherent weakness in its connectivity sensitivity. Although the connectivity status notification mechanism has been proposed to support for easily fixing up the network, in order to make the network more robust, issues related to mobility and failover, load balancing must be resolved. Network with multiple and heterogeneous IGWs (Wifi APs, 3G base stations,...) is an interesting research direction for the future work.

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

**REFERENCES**


