Computer Networks 54 (2010) 558–572

Contents lists available at ScienceDirect

Computer Networks

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

A mobility management scheme for wireless mesh networks based on a hybrid routing protocol ☆

Zhenxia Zhang, Richard W. Pazzi, Azzedine Boukerche *

PARADISE Research Laboratory, SITE, University of Ottawa, Canada K1N 6N5

ARTICLE INFO

Article history:
Available online 10 September 2009

Keywords:
Mobility management
Wireless mesh networks
Handoff
Seamless roaming
Real-time application

ABSTRACT

Recent advances in wireless mesh networks (WMNs) have overcome the drawbacks of traditional wired networks and wireless ad hoc networks. WMNs will play a leading role in the next generation of networks, and the question of how to provide seamless mobility management for WMNs is the driving force behind the research. The inherent characteristics of WMNs, such as relatively static backbones and highly mobile clients, require new mobility management solutions to be designed and implemented.

In this paper, a hybrid routing protocol for forwarding packets is proposed: this involves both link layer routing and network layer routing. Based on the hybrid routing protocol, a mobility management scheme for WMNs is presented. Both intra-domain and inter-domain mobility management have been designed to support seamless roaming in WiFi-based WMNs. During intra-domain handoff, gratuitous ARP messages are used to provide new routing information, thus avoiding re-routing and location update. For inter-domain handoff, redundant tunnels are removed in order to minimize forwarding latency. Comprehensive simulation results illustrate that our scheme has low packet latency, low packet loss ratio and short handoff latency. As a result, real-time applications over 802.11 WMNs such as VoIP can be supported.

1. Introduction

Wireless mesh networks (WMNs) are an innovative network technology that has emerged in recent years. Compared to original wireless networks, WMNs have many advantages: dynamic self-organization, self-configuration, high scalability, low cost, and easy maintenance. These characteristics allow WMNs to play an important role in the next generation of wireless networks.

A comprehensive survey of WMNs is given in [2]. In summary, two types of nodes are involved in a WMN: mesh routers and mesh clients. Mesh routers are responsible for routing and maintaining the network topology. Mesh routers, also called access routers (ARs), provide a connection to the network for mesh clients. Certain special mesh routers also perform gateway functions. Mesh clients include mobile devices, such as laptops, PDAs and sensors. An example of a wireless mesh network is shown in Fig. 1.

Generally, there are three types of WMN architecture: infrastructure/backbone WMNs, client WMNs, and hybrid WMNs [2]. In infrastructure/backbone WMNs, mesh routers construct a backbone, and mesh clients can connect to each other by communicating with the mesh routers. Some mesh routers work as gateways that provide a connection to the Internet. The mobility of mesh clients is much greater than that of mesh routers; thus, a backbone composed of mesh routers is almost static. In client WMNs, there are no mesh routers in the network, and mesh clients provide routing, bridging and gateway functions by themselves. This architecture is similar to that of a conventional wireless ad hoc network. In hybrid WMNs, mesh clients

☆ This work is partially supported by NSERC, Canada Research Chairs Program, The Ontario Research Fund (ORF), ORNEC, The Early Ontario Researcher Award, The Ontario Centres of Excellence (OCE), and MRI Ontario Funds.

* Corresponding author. Tel.: +1 613 562 5800x6712.
E-mail address: boukerch@site.uottawa.ca (A. Boukerche).

1389-1286/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2009.08.020

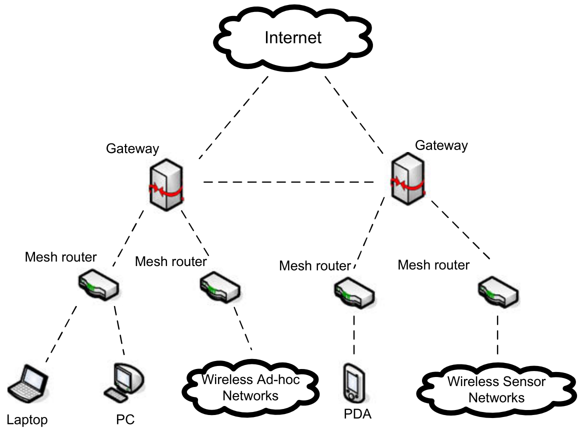

Fig. 1. An example of a wireless mesh network.

can communicate through both mesh routers and mesh clients. Infrastructure/backbone WMNs are the most popular type of architecture, and all of the WMNs discussed in this paper will be of this type.

The performance of WMNs is affected significantly by how the network manages the movements of mesh clients. Therefore, mobility management is one of the most important problems of WMNs. Although many existing mobility management solutions for conventional wireless networks can be applied to mesh networks, new mobility management solutions should be designed and implemented specifically for WMNs, considering their differences.

There are two kinds of roaming: *inter-domain roaming*, which refers to movement across different domains, and *intra-domain roaming*, which means movement among different access routers in the same domain. Accordingly, mobility management requires both inter-domain and intra-domain mobility management. This paper proposes an innovative scheme to provide both intra-domain and inter-domain mobility management within WMNs. The proposed solution uses a hybrid routing protocol, which integrates the network layer routing and link layer routing to forward packets and achieves easier handoff. For intra-domain handoff, our scheme avoids location update in the centralized location server, while also decreasing the time for re-routing after the handoff. In addition, our scheme can provide inter-domain handoff with low overhead by minimizing redundant tunnels. It provides seamless handoff with high scalability for real-time applications such as VoIP.

The remainder of this paper is organized as follows. Section 2 presents typical mobility management solutions for WMNs. The hybrid routing protocol is presented in Section 3, and our mobility management scheme is proposed in Section 4. Section 5 describes the simulation set-up and discusses the performance results. Finally, Section 6 summarizes our work and concludes this paper.

2. Related work

An extensive survey of mobility management in wireless networks is given in [1,3]. Mobility management includes location management and handoff management. With regard to location management, a mobile node updates its location information in a location database, and the system uses this location information to determine the mobile node's current position. Handoff management is responsible for establishing a new link when a mobile node changes its access router. Handoff is also referred to as handover. The access routers involved in the handoff may belong to the same domain (intra-domain handoff) or to two different domains (inter-domain handoff). Although many mobility management solutions over conventional wireless networks could be migrated to mesh networks, new mobility management solutions should be designed and implemented specifically for WMNs. In this section, some mobility management schemes that can be adopted in WMNs are reviewed.

2.1. Intra-domain mobility management

For conventional wireless networks, a variety of intra-domain solutions to reduce handoff latency have been proposed, such as HMIP [26], IDMP [19], MIP-RR [12], HAWAII [24], Cellular IP [8], and more [7]. However, these solutions are not suitable for WMNs. In this subsection, some intra-domain mobility management schemes that support seamless real-time applications for WMNs are reviewed. They can be classified within three groups: tunnel-based, routing-based, and multicast-based. Tunnel-based solutions always adopt a hierarchical architecture. The high-level agent encapsulates the low-level agent's address in an extra IP header, and forwards packets to the client's low-level agent first. The low-level agent, in turn, decapsulates the packets and sends them to the client. Routing-based solutions update routing tables in order to re-establish the connection after the handoff. The new multicast-based solution assigns the ARs of the same mesh client to two multicast groups; the multicast is then applied to support seamless mobility management.

2.1.1. Tunnel-based solutions

In [30], Wang et al. introduce Ant, a network-based intra-domain fast handoff scheme. When a mesh client begins handoff, the new access router sends a location update message to the location server. The former AR sets up a temporary tunnel with the new AR, and forwards the buffered packets. This former AR then informs the correspondent node's AR to set up a data path with the new AR for the mesh client. To decrease the delay that comes with establishing a temporary tunnel, all tunnels between the neighboring ARs are set up in advance. Updating the location information immediately in the handoff process is the main cost, while pre-establishing all bi-directional tunnels introduces other costs.

Huang et al. propose the hierarchically structured Mesh Mobility Management (M^3) in [13]. Three types of mesh routers are employed: gateways, superior routers, and access routers. When a handoff is activated, the prior AR adds a temporary routing entry to forward the packets to the new AR; then, the location information of the mesh client is updated at the superior router. The location information of the mesh client at the gateway is updated after a certain period to reduce the times of updating the database at the gateway. The hierarchical architecture decreases the delay when querying the client's location information at the gateway and increases the scalability of the mesh network. It also introduces the overhead of encapsulation and decapsulation.

2.1.2. Routing-based solutions

Navda et al. implement iMesh using a cross-layer mobility management scheme [20]. Every AR in the mesh network has a routing table containing the paths to all clients. Before handoff, a mesh client searches for new AR candidates in the link layer. It broadcasts a probe request message to all ARs in its vicinity. Upon receiving the probe response messages, the client selects the AR providing the best link quality, which is measured according to its signal-to-noise ratio, and then associates with this AR. A routing update is then triggered in the network layer. The OLSR [9] protocol is used in iMesh, and the overhead results from routing table updates after handoff. The overhead from the control messages in OLSR also increases with the number of mesh clients, and this limits iMesh's scalability.

MEMO (MEsh networks with MObility management) [25] adopts a cross-layer mobility management solution: MTMM (MAC-layer Triggered Mobility Management). The IP address of a mesh client is assigned by a simple hash function, and it remains within the domain during client roaming. When a mesh client decides to change its AR, the original AR notifies the correspondent node's AR to initiate route discovery for the mesh client. To lower overhead, a modified AODV protocol AODV-MEMO [25] is introduced for routing. However, routing table updates caused by handoff remain the main problem; this is also the case with iMesh.

2.1.3. Multicast-based solution

SMesh [5] is a seamless 802.11 wireless mesh network that supports fast handoff for Real-time applications. It uses the Spines messaging system [4,29] to provide communication between mesh nodes. In SMesh, every mesh client is associated with a multicast group, Client Data Group. All packets sent to a mesh client are forwarded to the Client Data Group, and the router in the Client Data Group then forwards the packets to the client. When handoff occurs, the new AR sends a gratuitous ARP [23] message with its MAC address to the mesh client, and the mesh client maps the new AR's MAC address to the default gateway IP address. Though the use of multicast groups of ARs ensures seamless handoff, group management is the main cause of overhead. Messages exchanged between ARs in order to maintain the Client Control Group and Client Data Group waste significant amounts of bandwidth.

2.2. Inter-domain mobility management

Unlike the case of intra-domain mobility management, fewer inter-domain mobility management solutions are proposed. Mobile IP [22] is one of the most significant solutions for inter-domain mobility management and it can be usefully adopted in WMNs. This solution eliminates the mobility problem through the use of tunnel technology. The original permanent IP address of the mobile node is referred to as the home address, which is administered by the home agent. When a mobile node moves to a foreign network, the foreign agent (usually a router) assigns a second temporary address known as a *care of address* to the mobile node. After receiving the *care of address*, the mobile node registers the secondary address to the home agent. All packets sent to the mobile node's home address are then tunneled, by the home agent, to the mobile node's *care of address* through IP encapsulation.

In [6], an inter-domain routing protocol is introduced to enhance the original SMesh [5] architecture, which can support inter-domain roaming. The idea is to incorporate a multicast group called Internet Gateway Multicast Group (IGMG), which is composed of Internet gateways, to provide transparent inter-domain handoff. TCP and UDP applications are considered separately.

In TCP communications, when an Internet gateway receives a SYN packet requesting the setup of a new TCP connection, it regards the new TCP connection as belonging to itself. When an Internet gateway receives a TCP packet, which is not a SYN packet, from a mobile client and the gateway does not have any entries regarding the TCP connection in its Network Address Translation (NAT) table [10], the Internet gateway multicasts the packet to the IGMG. The connection's owner subsequently receives the packet, forwards it to the Internet, and sends an owner notification message to the IGMG. All members in the IGMG are alerted to the ownership of this connection. Therefore, if any other gateways receive TCP packets from this connection, they forward the packets directly to the owner. With regard to UDP communications, when the gateway receives a new UDP packet from a mesh client, it relays the packet to both its destination and the IGMG. Moreover, the gateway sets a timer and waits for a response regarding the ownership of that UDP connection. After a timeout, the gateway indicates its ownership of the UDP connection and forwards the subsequent UDP packets to the Internet destination without forwarding them to the IGMG. However, if another gateway in the IGMG discovers that this UDP connection belongs to it before timeout, an owner notification is sent to the IGMG.

Moreover, to minimize re-routing delay for an inter-domain handoff, two routing protocol extensions are proposed: Pre-handoff discovery (PRD) for AODV [28] and FastSync for OLSR [27]. The principal idea behind PRD for AODV is to discover the route in the new wireless mesh network before the handoff is started. This extension could be integrated with Mobile IPv4 Fast Handovers [18] or FMIPv6 [17]. FastSync for OLSR decreases the time for updating routing information after inter-domain handoff. It enables mesh clients to determine the MPRs and to establish slinks quickly according to the network topology.

3. Hybrid routing

This section proposes our hybrid routing scheme for WMNs, which enables fast handoff. Three types of architectures for wireless mesh networks have been introduced in Section 1. In this paper, only the infrastructure/backbone mesh network is considered. The IEEE 802.11 protocol [14] is also used as the MAC layer protocol. Mesh clients can join and leave the mesh network at any time, and are able to roam in the network as well. When a client roams, the AR with which it associates changes because of the AR's limited transmission range. All packets sent to the Internet from mesh clients are routed to the gateway, and the gateway transmits these packets to the Internet destination using NAT.

In recent years, some link layer routing protocols have been designed to improve routing performance in WMNs [11,15]. In [11], a WDS-based link layer (layer 2) routing protocol for wireless mesh networks is proposed. This protocol introduces a layer 2 routing table which consists of the MAC address pairs that describe the routing information in the link layer. However, since the layer 2 routing tables in mesh routers and the centralized controller involved in this solution grow in proportion to the number of mesh clients, scalability is not well supported.

Our proposed mesh network adopts a hybrid routing protocol that involves both link layer (layer 2 in the OSI model [31]) routing and network layer (layer 3) routing. In essence, the mesh clients reply to an ARP message with their access router's MAC address. Therefore, packets forwarded among mesh routers can use link layer routing to decrease the encapsulation and decapsulation delay of IP datagrams, and the packets communicated between access routers and mesh clients can use network layer routing. This method avoids centralized control, so that the size of the layer 2 routing table is related to the number of mesh routers, and not the mesh clients. Thus, the layer 2 routing table will be small; the number of mesh routers in a domain is usually less than 100.

Algorithm 1. Pseudocode of layer 2 routing algorithm

```
Extract destination MAC address M
if M matches current router's MAC address then
    decapsulate the frame
    transmit the datagram to the network layer and use layer 3 routing
else if the table contains a specified route for M then
    forward the frame to the next-hop according to the layer 2 routing table
else
    report the layer 2 routing error
end if
```

An example of a routing table is shown in Table 1. In this example, if a mesh router wants to forward a frame to the destination with MAC address 00 15 58 83 DF 86, it searches the layer 2 routing table and finds that the MAC address of the next hop is 00 15 58 83 DF 88. The frame is then forwarded to 00 15 58 83 DF 88. The layer 2 routing table can be maintained with either a proactive routing method or a reactive routing method, such as the Hybrid Wireless Mesh Protocol (HWMP), which is specified in 802.11s [15]. Every mesh router knows the routing path to any other router.

Table 1
MAC address based routing table.

Destination MAC address	Next hop MAC address
00 15 58 83 DF 86	00 15 58 83 DF 88
......	......

The format of the 802.11 MAC frame header is shown in Fig. 2 [14]. The detailed information of the 11 subfields in the frame control field is given in Fig. 3 [14]. There are four address fields in the frame header. The different combinations of ToDS, FromDS and address fields are shown in Table 2 [14,11]. In the various combinations, the source address or destination address can be located in different address fields. In our mesh network, data frames are set by ToDS = 1 and FromDS = 1. The address 1 is the receiver address, which indicates the MAC address of the next hop. Address 2 is the transmitter address, which is the MAC address of the current node. The destination address and source address are in the fields of address 3 and address 4, respectively. This scheme enables the implementation of layer 2 routing in 802.11-based mesh networks.

When a mesh client joins the mesh network, it selects the AR that has the best link quality of all candidates. Many parameters can be used to measure the quality of links, such as signal-to-noise ratio, response delay, and so on. We adopt response delay as the link quality metric in our scheme. The mesh client then sends an association request message to the selected AR. Upon receiving the request, the AR obtains a private IP address from the DHCP server, and returns an association confirmation message with the client's IP address, the AR's MAC addresses, and the gateway's MAC address. Each AR maintains a table containing the IP address and MAC address pairs of all clients registered in it.

Two instances of communication are considered: communication between mesh clients, and communication between a mesh client and the Internet. In the first case, when a mesh client wants to transmit a packet to another client, and already knows the destination's MAC address, it constructs the packet and forwards it to its AR. Otherwise, the mesh client uses an ARP message to obtain the destination's MAC address (which is the MAC address of the destination's AR). The sender's AR then forwards the packet to the receiver's AR, based on the layer 2 routing path. When the receiver's AR receives the packet, it forwards this packet to the receiver, using the destination's IP address. In the second case, in order to send a packet to the Internet, the mesh client must forward the packet directly to the gateway, which transmits the packet to its destination. To send a packet to the mesh client, the gateway forwards the packet according to the layer 2 routing table, provided it knows the MAC address of the mesh client (the MAC address of the client's AR). Otherwise, it sends an ARP message to obtain the MAC address. The client's MAC address is maintained in the table temporarily. After a period of no communication between the mesh client and the Internet, the temporary entry is deleted. The pseudocode of the layer 2 routing is shown in Algorithm 1, and the pseudocode of the layer 3 routing is shown in Algorithm 2.

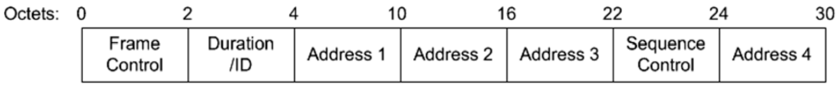

Fig. 2. IEEE 802.11 MAC frame header.

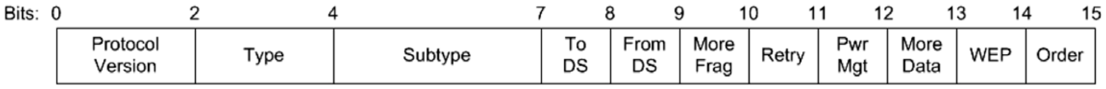

Fig. 3. Frame control field.

Table 2
To/from DS fields and address fields.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination address	Source address	BSSID	N/A
0	1	Destination address	BSSID	Source address	N/A
1	0	BSSID	Source address	Destination address	N/A
1	1	Receiver address	Transmitter address	Destination address	Source address

Algorithm 2. Pseudocode of layer 3 routing algorithm

```
Extract destination IP address D
if D matches any mesh client's IP address, which registers in this mesh router then
    map D to its MAC address
    encapsulate the MAC frame header for the datagram
    forward the datagram to its destination
else if the table contains a specified route for D then
    forward the datagram to the next-hop according to the layer 3 routing table
else
    report the layer 3 routing error
end if
```

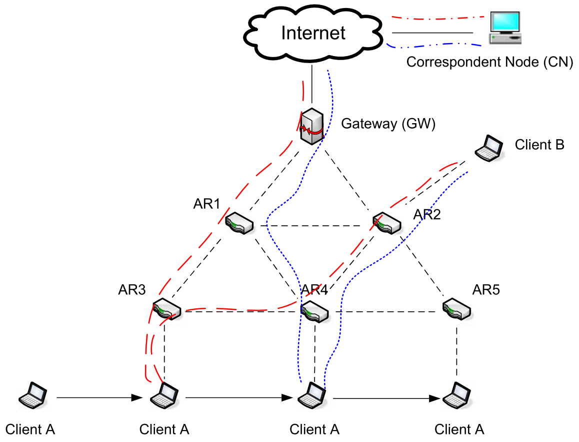

Fig. 4. Example scenario during intra-domain roaming.

3.1. Sample scenario

An example of our hybrid routing is described in this subsection. Table 3 shows the notation used in this paper. The topology of the mesh network is shown in Fig. 4. One gateway and five access routers construct the relay backbone in our scenario. When client A joins the mesh network, this client selects AR3 as its access router. All packets sent from client A should be sent to AR3; AR3 forwards these packets to the destination. Client A initially registers with AR3 and then obtains an IP address, denoted as IP_A. It also receives the MAC addresses of AR3 and the gateway, which are denoted as MAC_{AR3} and MAC_{GW}.

The following steps are taken when client A desires to send packets to client B. Suppose that A does not know B's MAC address, A sends an ARP message in order to determine it. AR2 then receives the ARP message and replies with its MAC address, MAC_{AR2}. Upon receiving this reply message, client A adds a mapping entry with IP_B and MAC_{AR2} into its mapping table. Using this approach, client A generates frames which are sent to client B, setting ToDS = 1, FromDS = 1, Address 1 = MAC_{AR3}, Address 2 = MAC_A, Address 3 = MAC_{AR2}, Address 4 = MAC_A, and forwards the frames to AR3. AR3 receives the packets, and finds that the destination is AR2. Then, AR3 searches the layer 2 routing table, which is shown in Table 4, to find the next hop. In this case, the next hop is AR4. AR2 therefore sets Address 1 = MAC_{AR4} and Address 2 = MAC_{AR3}. Be-

Table 3
Notation.

Notation	Description
AR*i*	access router *i*
A, B	mesh client A, mesh client B
CN	correspondent node
IP_n	the IP address of node *n*
MAC_n	the MAC address of node *n*
GW	gateway

Table 4
Layer-2 routing table of AR3.

Destination MAC address	Next hop MAC address
MAC_{GW}	MAC_{AR1}
MAC_{AR1}	MAC_{AR1}
MAC_{AR2}	MAC_{AR4}
MAC_{AR4}	MAC_{AR4}
MAC_{AR5}	MAC_{AR4}

cause the frames come from AR3's clients, AR3 sets Address 4 = MAC_{AR3}. In the next step, the frames are forwarded to AR4. Similarly, AR4 forwards the frames to AR2. After this, AR2 finds that the MAC address of the destination is the same as its own MAC address. Therefore, the frames are decapsulated and transmitted to the network layer. In the network layer, AR2 finds that the IP address of the destination is IP_B, determines that the MAC address of client B is MAC_B, sets the frame header as ToDS = 1, FromDS = 1, Address 1 = MAC_B, Address 2 = MAC_{AR2}, Address 3 = MAC_B, Address 4 = MAC_{AR2}, and transmits the packets to client B directly. In this way, client B can also send packets to client A. To do so, client B sets Address 3 = MAC_{AR3} in the frame header.

4. Mobility management scheme

In this section, we propose our mobility management scheme for IEEE 802.11 wireless mesh networks based on a hybrid routing protocol. Both intra-domain roaming and inter-domain roaming are considered in our scheme, which can provide seamless handoff for real-time applications.

4.1. Intra-domain mobility management

We begin by presenting our intra-domain mobility management scheme. When a mesh client roams in the mesh network, the AR that has the best link quality changes. Therefore, the mesh client has to associate with a new AR. The handoff is triggered by sensing that the response delay of the original AR is below a threshold. The mesh client then selects an AR that has the best link quality as its new AR. This probing process is done in all channels.

Next, the mesh client sends an association request message to the new AR, in which the client's IP address and MAC address pair are encapsulated. When the new AR receives this request, it adds the client's IP address and MAC address pair to its ARP table, and sends back an association confirmation message to the client. The new address pair is used to transmit packets to the client after the handoff. Upon receiving the confirmation message, the mesh client must reply to all of the ARP messages with the new AR's MAC address.

During the handoff, if communication exists between the mesh client and another client in the same domain, the mesh client sends a gratuitous ARP (GARP) message, to the correspondent node, with the new AR's MAC address. Upon receiving this gratuitous ARP message, the correspondent node maps the new AR's MAC address to the mesh client's IP address. All following packets are forwarded directly to the new MAC address without re-routing. The client then sends a disassociation message to the former AR with the new AR's MAC address. The former AR can therefore tunnel the following packets that are sent to the client to the new AR. This temporal tunnel is deleted when the original AR no longer receives any packets sent to that client. This entire handoff process is shown in Fig. 5.

Conversely, if a mesh client is communicating with an Internet destination, when the mesh client receives the association confirmation message, the gratuitous ARP message is sent to the gateway and not the correspondent node. Then the gateway maps the new AR's MAC address to the client's IP address, and the packets from the Internet can be correctly forwarded to the client after handoff. However, if a new correspondent node wishes to establish a connection with the mesh client right after handoff but before the gateway is informed of these changes, the connection may not be established. To address this problem, uplink traffic and downlink traffic are considered separately. In case of uplink traffic, the client may accurately send packets to the correspondent node, because the corre-

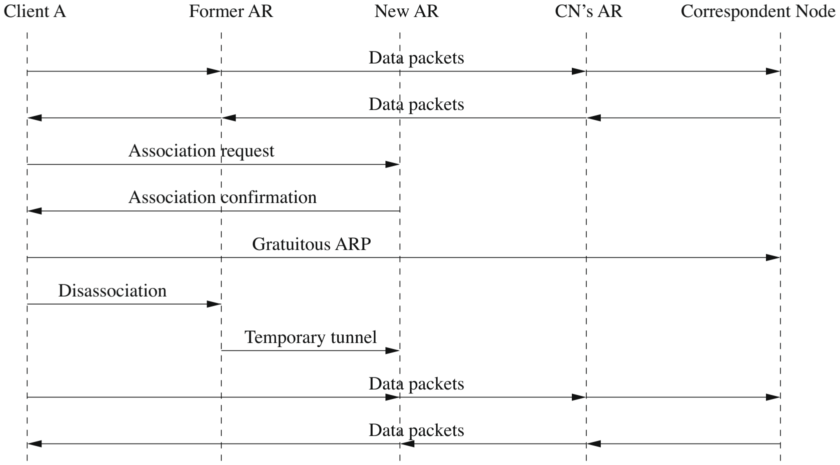

Fig. 5. Communication when handoff occurs if the mesh client has a connection in the same domain.

spondent node's address remains unchanged. For downlink traffic, if the correspondent node sends packets to the mesh client before the gateway has been informed of the changes, all packets received by the gateway will be forwarded to the old AR. And yet, because the prior AR receives the disassociation message which encapsulates the mesh client's new MAC address, the former AR will forward the packets to the new AR. In this way, the connection can still be established even if a new connection request is received before the gateway is informed of changes introduced by handoff. The handoff process in this situation is provided in Fig. 6.

In our solution, the IP address of the mesh client remains the same after handoff. Both UDP and TCP use a combination of IP address and port number to determine the destination. Therefore, the unchanged IP address permits both UDP and TCP communication to remain after handoff.

4.1.1. Sample scenario

We now consider the same topology of the mesh network, which is shown in Fig. 4. Client A is a mobile node, and it moves in the network following the arrows shown in Fig. 4. The dashed lines show the routing path before handoff, while the dotted lines show the routing path after handoff. As client A moves, it senses the signal strength of AR3 weakening. When the signal strength drops below a threshold, client A associates with a new mesh router. In this example, client A chooses to associate with AR4. Initially, client A sends an association request message with its IP address, IP_A, and MAC address, MAC_A, to AR4. AR4 replies with an association confirmation message containing the IP address and MAC address of AR4, IP_{AR4} and MAC_{AR4}. Client A then sends a gratuitous ARP message to client B with MAC_{AR4}, and client B maps the IP_A to MAC_{AR4}. All of the frames sent to client A are set by Address 3 = MAC_{AR4}. Finally, client A sends a disassociation message to AR3 for disconnection. The handoff process is finished, and the IP address of client A remains the same after handoff.

The main difference between communicating with a correspondent node (CN) through the Internet and communicating with a mesh client in the same domain is as follows. When the frame is generated, the field of Address 3 in the frame header is set to MAC_{GW}. Instead of sending a gratuitous message to the correspondent mesh client, when the handoff occurs, mesh client A sends the gratuitous ARP message to the gateway and claims that its new MAC address is MAC_{AR4}.

4.1.2. Comparison

A comparison of our proposed intra-domain solution with other solutions is shown in Table 5. Our solution has the following advantages:

- This solution does not require the central location database, and so does not incur the cost of updating and querying the location database is waived. All mesh clients use their ARs' MAC addresses as their MAC addresses; the locations of mesh clients can therefore be obtained according to clients' MAC addresses;

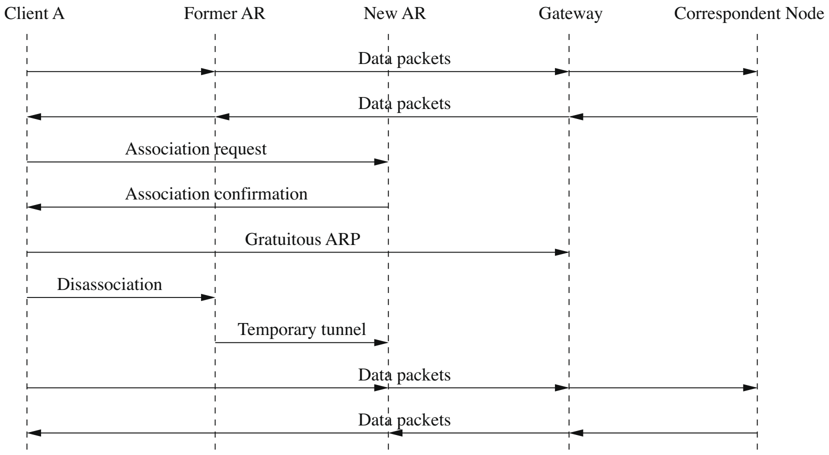

Fig. 6. Communication when handoff occurs if the mesh client has a connection through Internet.

Table 5
Comparison of our intra-domain mobility management solution and other solutions.

	M^3	Ant	iMesh	MEMO	SMesh	Our solution
Layer	layer 3	layer 3	layers 2 + 3	layers 2 + 3	layer 3	layers 2 + 3
Routing	Not mentioned	OLSR	OLSR	AODV-MEMO	Not mentioned	Hybrid routing
Location server	√	√	N/A	N/A	N/A	N/A
Routing update	N/A	N/A	√	√	N/A	N/A
Overhead reason	Hierarchical delay	Location update	Routing	Routing	Group management	Control traffic and GARP
Overhead level	Normal	Normal	High	High	Normal	Low

- The use of layer 2 routing can minimize the cost of packet relay among the mesh routers when compared with layer 3 routing. The delay of encapsulation and decapsulation of IP packets in the network layer is avoided. In addition, the IP address of mesh clients remains the same throughout domain roaming;
- Unlike traditional routing-based solutions, no routing table updating is necessary after handoff. The packets can be transmitted to the mesh client correctly by changing the MAC address of the mesh client;
- Unlike tunnel-based solutions, the tunneling overhead at each level of the hierarchy is removed.

4.2. Inter-domain mobility management

In this subsection, we focus on the inter-domain mobility management scheme. The inter-domain handoff is triggered when the mesh client switches to a AR in a different domain. As seen with intra-domain handoff, the mesh client broadcasts a probe message, gathers response messages, and selects the AR with the best signal strength as the new AR. An association request message is then sent to the new AR. Upon receiving the request, the new AR replies with an association confirmation message that contains the new AR's MAC address and the new gateway's IP address. The main difference between intra-domain roaming and inter-domain roaming is that the IP address of the mesh client changes, since the server in the new domain assigns a new private address to the mesh client. Therefore, in order to retain the existing data traffic after moving into a new domain, a temporary tunnel is established between the prior gateway and the new gateway through which data packets are forwarded.

After the new AR is selected, the mesh client sends a disassociation message, which includes the new gateway's information, to the prior gateway. The gateway maintains a tunnel list, which records temporary tunnels used to forward packets. For each temporary tunnel entry in the tunnel list the mesh client's address, paired with the new gateway's address, is used to represent a tunnel. When the old gateway receives the disassociation message, it registers the new tunnel in its tunnel list. Therefore, a temporary tunnel is established. All packets sent to the mesh client are then forwarded to the new gateway. Additionally, to maintain the tunnel list efficiently, a tunnel entry that is not used for a certain period will be removed. This inter-domain handoff process is illustrated in Fig. 7.

During inter-domain handoff, if the mesh client is communicating with the correspondent node of a former domain, further operations are required to guarantee that the correspondent node is able to find the new data path. In this case, a gratuitous ARP message is sent to the correspondent node by the mesh client before it moves to the new domain. The old gateway's MAC address is encapsulated in the gratuitous ARP message. When the correspondent node receives the gratuitous ARP message, it updates its ARP table and maps the mesh client's address to the gateway's MAC address. After that, according to our hybrid routing protocol, if the correspondent node wants to send packets to the mesh client, it will send packets to the gateway first; the gateway then forwards packets to the mesh client through the new gateway following the temporary tunnel. Fig. 8 shows this special inter-domain handoff process.

Moreover, when the mesh client moves across different domains, some redundant tunnels exist. To save network bandwidth and to reduce forwarding latency, these redundant tunnels should be removed. If a gateway receives data packets sent to a mesh client which moved to a new domain, it sends a notification message encapsulating the new gateway's IP address. The old gateway then updates its tunnel list and maps the mesh client's address to the new gateway's address. As a result, the data packets can directly be sent from the old gateway to the new gateway and redundant tunnels are merged.

4.2.1. Sample scenario

An example is shown in Fig. 9. Suppose that, mesh client M switches from domain A to domain B. It sends a disassociation message to gateway A (GWA) in which the informa-

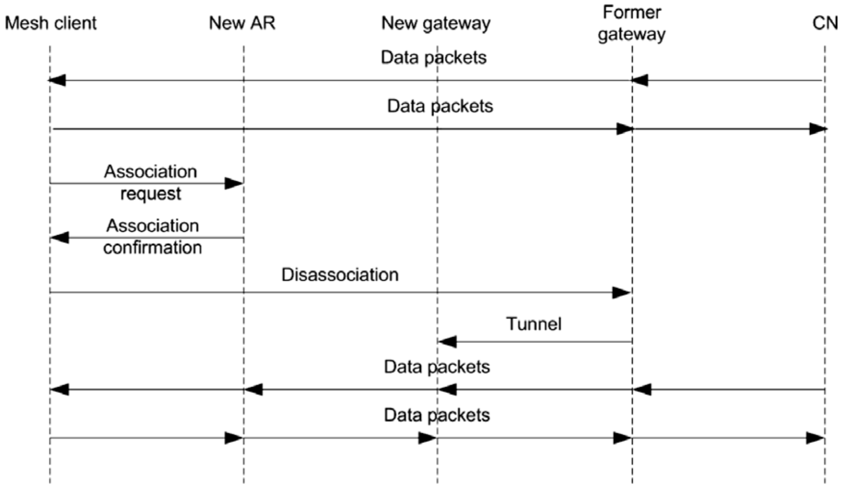

Fig. 7. Inter-domain handoff process.

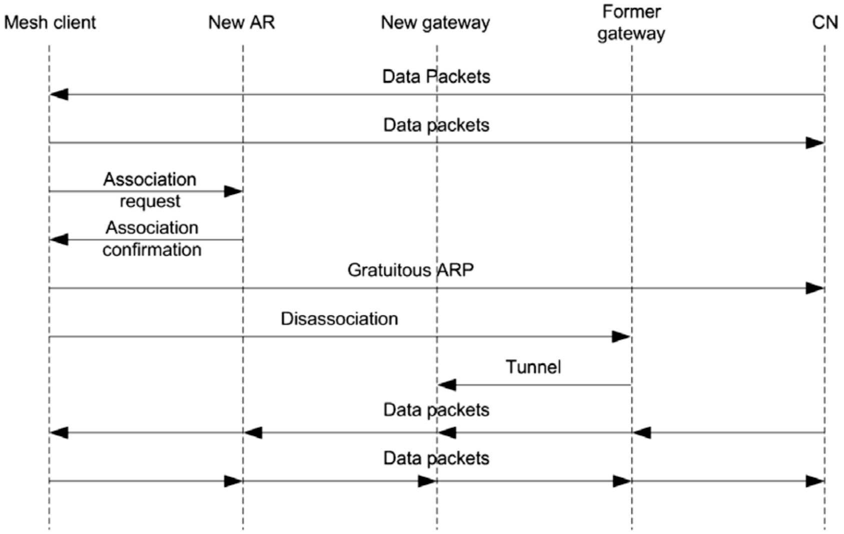

Fig. 8. Inter-domain handoff process when the mesh client has a communication in the prior domain.

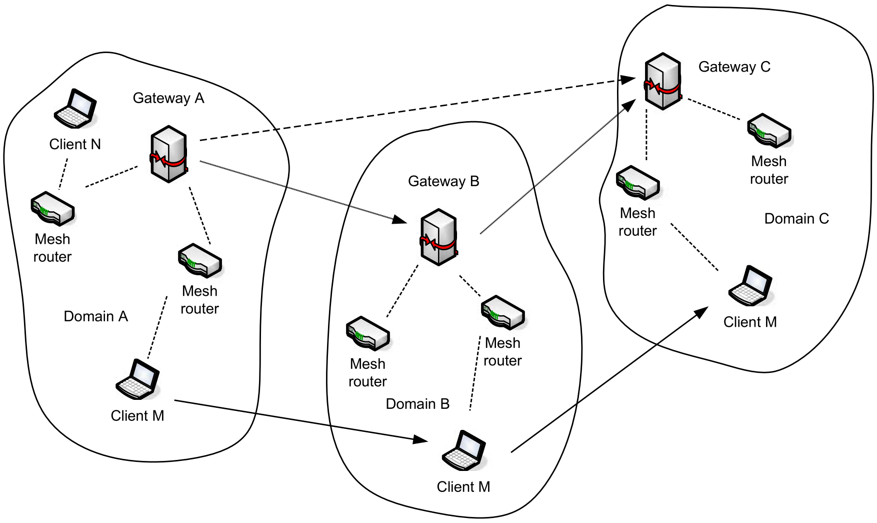

Fig. 9. An example of inter-domain handoff.

tion of gateway B (GWB) is encapsulated. A tunnel is established between GWA and GWB. Because M has a communication with correspondent node N, a gratuitous ARP message containing GWA's MAC address is sent to N. Upon receiving the gratuitous ARP message, N first forwards data packets to GWA; then GWA forwards packets to M through GWB. A new tunnel between gateway B and gateway C (GWC) is established to forward packets after M moves into domain C. The new data path is shown by dotted arrows in Fig. 9. GWA first forwards packets to GWB, and GWB then forwards packets to GWC. Though it appears two tunnels are needed to send packets from GWA to M, only one tunnel is truly needed. To reduce the number of tunnels, after M moves into domain C, GWB sends a notification message to inform GWA that the following packets sent to M can be forwarded to GWC directly. In Fig. 9, the new tunnel is represented by the dashed arrow. The old path $GWA \rightarrow GWB \rightarrow GWC$ is replaced by $GWA \rightarrow GWC$. As a result, the packet latency is reduced.

5. Performance evaluation

In this section, the simulation results are presented. The Network Simulator – ns2 (Release 2.31) [21] is used to simulate the proposed solution. Intra-domain roaming and inter-domain roaming are evaluated separately. To simulate a G.711 [16] encoded/decoded VoIP stream, a CBR flow, which sends a 160 byte UDP packet every 20 ms at a rate of 64 Kbps, is established between the mobile client and the correspondent node in our experiments. Mesh clients move according to four mobility models: Bounded Random Mobility Model (BRMM), Brownian Motion Mobility Model

Table 6
Simulation parameters.

Parameters	Value
Simulation time	400 s
CBR packet size	160 bytes
CBR packet interval	20 ms
Probe message interval	2 s
Radio range	250 m
Maximal velocity	5 m/s

(BMMM), Random Direction Mobility Model (RDMM), and Random Waypoint Mobility Model (RWMM). The general parameters are shown in Table 6. Other specific parameters are set as follows: in the case of BRMM, the incremental time interval is 1 s, the maximal angular change in direction is 90°, the maximum acceleration is 1 m/s^2, and in the case of RWMM, the pause between movements is 1 s.

5.1. Intra-domain roaming

The performance of our mobility management scheme during intra-domain roaming is discussed in this section. The mesh relay backbone is composed of 20 fixed mesh routers, and the mesh routers are deployed randomly in each simulation. However, we guarantee that all mesh routers are connected. There are 30 mobile nodes in our scenarios, and we establish one CBR flow between two mobile nodes. Moreover, for each mobility model, we ran 33 simulations.

5.1.1. Packet latency and loss ratio

In these experiments, the correspondent node sends the CBR packets every 20 ms to the mobile mesh client; therefore, 20,000 UDP packets can be sent in 400 s. The mobile client roams under a different mobility model and changes its access router. These experiments are used to test how our solution affects the data traffic. The average packet loss ratio and latency is shown in Table 7. According to the experimental results, although the mesh client changes its access router frequently, the loss ratio remains at a low level. The best results occur with the Random Direction Mobility Model, where the loss ratio is 0.085%. The worst results occur with the Brownian Motion Mobility Model with a loss ratio of 0.102%. As the table demonstrates in the simulations, the mesh client successfully changes its access router during the roaming process with a low loss ratio. Thus, our solution is proven to realize seamless handoff.

The relationship between packet latency and the associated access router, in a given simulation of each mobility model, is illustrated in Figs. 10–13. The left y axis shows the latency of each packet, and the right y axis represents the access router with which the mobile client associates. In Figs. 10–13, most packets arrive in time at the mobile client. However, some exceptions do occur, since, according to the CSMA/CA-based medium access approach in IEEE 802.11, the packets should be retransmitted when the mesh routers experience a collision. The average latency during intra-domain roaming is around 10 ms, and the average latency per hop is around 2.5 ms. The 95% confidence range of the average packet latency is shown in Fig. 14. We are 95% confident that the true packet latency will be between 8.73 ms and 11.57 ms.

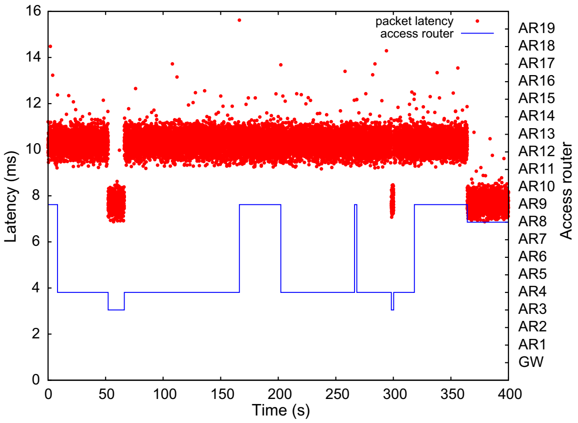

Fig. 10. Packets received in the case of BRMM during intra-domain roaming.

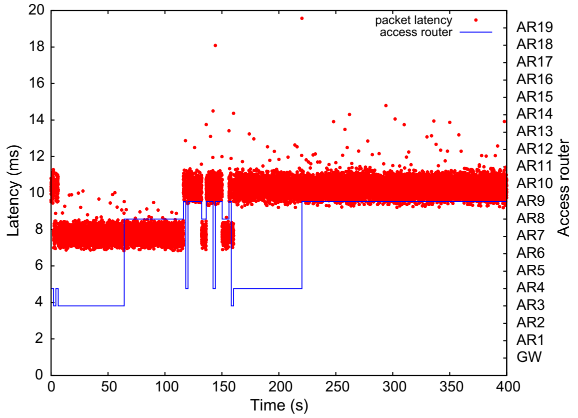

Fig. 11. Packets received in the case of BMMM during intra-domain roaming.

Table 7
Average packets-loss ratio and latency during intra-domain roaming.

Mobility model	Packets sent	Packets lost	Loss ratio (%)	Latency (ms)	Latency per hop (ms)
Bounded random mobility model	20,000	18.636	0.093	9.947	2.458
Brownian motion mobility model	20,000	20.394	0.102	9.936	2.423
Random direction mobility model	20,000	16.970	0.085	9.705	2.464
Random waypoint mobility model	20,000	19.788	0.099	10.633	2.530

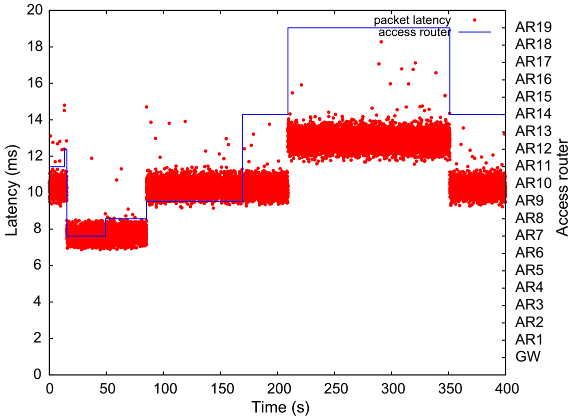

Fig. 12. Packets received in the case of RDMM during intra-domain roaming.

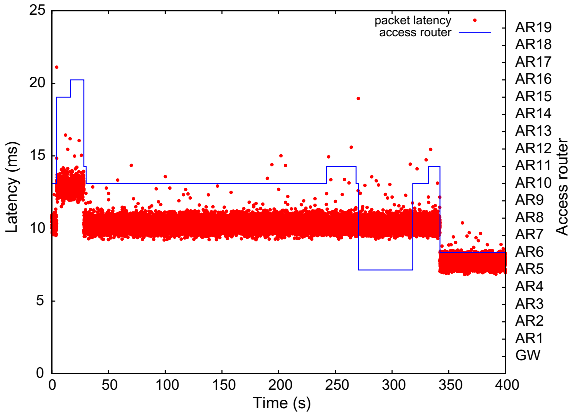

Fig. 13. Packets received in the case of RWPM during intra-domain roaming.

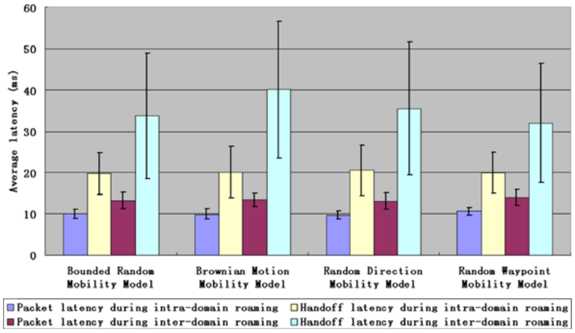

Fig. 14. Average packet and handoff latency.

5.1.2. *Handoff overhead and latency*

In intra-domain roaming, there are six kinds of overhead traffic which can be categorized into three groups:

1. *Link control.* There are two kinds of link control traffic: probe messages and reply messages. The mobile client broadcasts a probe message to all mesh routers in its neighborhood every 2 s, and waits for the reply messages to calculate the link quality of the mesh routers. The probe message and the reply message are both 40 bytes long. The link control traffic depends on the number of mesh routers in the mobile client's neighborhood.
2. *Association control.* Three types of messages are included: association request messages, association confirmation messages and disassociation messages. The 144-bytes request message is composed of the mobile client's IP address and MAC address, the old access router's IP address and MAC address, and the certification information. The confirmation message is used for the new AR authorizing the mesh client to connect. The size of a confirmation message is 144 bytes. The disassociation message is 64 bytes long. It includes the mobile client's IP address, and the new AR's IP address and MAC address. The association control overhead increases in accordance with the number of handoffs.
3. *Gratuitous ARP.* A gratuitous ARP message is 28 bytes long. The gratuitous ARP traffic grows with the number of handoffs and the number of correspondent nodes.

The average throughput rates for the three categories of overhead are shown in Table 8. The total overhead is quite low, and the negative impact on CBR traffic throughput is minimized. The link control traffic consumes the most bandwidth, which is around 1 Kbps per client. Association control traffic is only affected by the number of handoffs. For each handoff, the total overhead of association is 352 bytes. Thus, the maximum association traffic rate is 1.375 Kbps per mobile node. GARP traffic also consumes little bandwidth; even if the mesh client associates with a new AR every 2 s, the GARP traffic rate is 0.112 Kbps per CN. However, the GARP traffic grows linearly with the number of correspondent nodes; it is still quite small. Therefore, our solution has high scalability.

In addition, Fig. 15 presents a quantitative comparative study of intra-domain handoff overhead. Our scheme is compared with three other schemes: M^3 [13], MEMO [25] and SMesh [5]. These three schemes belong to different types. According to the simulation results, our scheme has the lowest overhead. MEMO, the routing-based solution, has the highest overhead. This is because routers need to update their routing tables during the handoff to find a new routing path for the mesh client. SMesh has to maintain multicast groups and M^3 needs to update the mesh client's location information on the location server; therefore, these two schemes introduce more overhead than ours.

Total intra-domain handoff latency consists of two parts: link layer handoff latency, which refers to the time for associating with the new AR in the link layer, and network layer handoff latency which is defined as the period that begins when the mobile client starts handoff and ends when the correspondent node receives the GARP message. However, link layer handoff latency cannot be controlled, because our solution works mainly on the network layer. The average link layer handoff latency should be around 40–50 ms [20,30]. The network layer latency of our solution is shown in Table 8, and the 95% confidence range of

Table 8
Average handoff overhead and network layer latency during intra-domain roaming.

Mobility model	Handoff number	Link (Kbps)	Reassociation (Kbps)	GARP (Kbps)	Total (Kbps)	Latency (ms)
Bounded random mobility model	11.545	1.017	0.079	0.006	1.102	19.682
Brownian motion mobility model	10.788	1.112	0.074	0.006	1.192	20.068
Random direction mobility model	5.273	0.970	0.036	0.003	1.009	20.496
Random waypoint mobility model	5.909	0.965	0.041	0.003	1.009	19.899

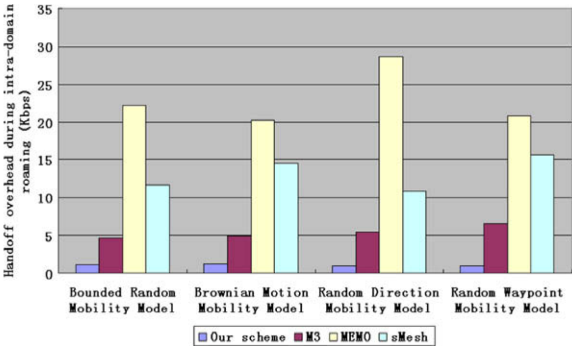

Fig. 15. Average handoff overhead during intra-domain roaming.

the average packet latency is shown in Fig. 14. In our multi-hop mesh networks, we are 95% confident that the true network layer handoff latency would be between 13.84 ms and 26.54 ms. Therefore, the total handoff latency would be around 53.84–76.54 ms. Fig. 16 illustrates the network layer intra-domain handoff latency of three schemes: our scheme, M^3 and MEMO. SMesh uses multicast to eliminate the handoff latency, and is not included in the figure. Our scheme and M^3 take a similar amount of time to complete handoff in the network layer, which is around 20 ms. And MEMO requires more time to complete the network layer handoff, which is around 45 ms.

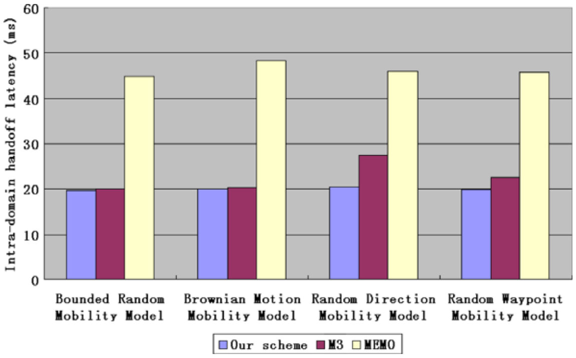

Fig. 16. Average intra-domain handoff latency in network layer.

5.2. Inter-domain roaming

In this section, the performance of our scheme during inter-domain roaming is illustrated. In these experiments, thirty access routers were deployed randomly and three domains were constructed by these mesh routers, and we changed the topology of the mesh network in each test. As with the intra-domain roaming scenario, there were thirty mobile nodes in each simulation experiment and we ran 33 simulations for each mobility model.

5.2.1. Packet latency and loss ratio

To evaluate our proposed scheme during inter-domain roaming, we randomly select two mobile nodes to establish a CBR flow between them, and both can move among different domains. In each simulation, 20,000 UDP packets were sent in 400 s. Table 9 shows the average packet loss ratio, latency and the 95% confidence range of the latency during inter-domain roaming. Although a few packets were lost due to handoffs and conflicts in wireless transmission, most of the packets were received by the nodes correctly. Compared to intra-domain roaming, inter-domain roaming has a high loss ratio, because paths typically require more hops, causing higher loss probability.

The average packet-forwarding latency during inter-domain roaming is still quite low. The best case occurs with the Random Direction Mobility Model, with a latency is 12.997 ms; and the worst case is that of the Random Waypoint Mobility Model, with a latency is 13.968 ms. In addition, we are 95% confident that the real packet latency throughout would be between 11.494 ms and 15.277 ms. The average packet latency is also greater here than in the case of intra-domain roaming, due to extra hops introduced by the tunnels.

5.2.2. Handoff overhead and latency

In these experiments, the average overhead during inter-domain roaming is assessed. We classify the overhead into three categories.

Table 9
Average packets-loss ratio and latency during inter-domain roaming.

Mobility model	Packets sent	Packets lost	Loss ratio (%)	Latency (ms)	Confidence range (ms)
Bounded random mobility model	20,000	107.317	0.536	13.236	11.186–15.287
Brownian motion mobility model	20,000	120.866	0.604	13.342	11.735–14.949
Random direction mobility model	20,000	105.960	0.529	12.997	11.023–14.971
Random waypoint mobility model	20,000	122.571	0.613	13.968	12.034–15.902

Table 10
Average overhead traffic and network layer handoff latency during inter-domain roaming.

Mobility model	Link (Kbps)	Handoff (Kbps)	Tunnel (Kbps)	Total (Kbps)	Handoff latency (ms)
Bounded random mobility model	1.023	0.102	0.002	1.127	33.682
Brownian motion mobility model	1.132	0.101	0.003	1.236	40.068
Random direction mobility model	0.997	0.118	0.003	1.118	35.496
Random waypoint mobility model	0.983	0.093	0.002	1.078	31.899

1. *Link control.* During inter-domain roaming, link control traffic is the same as during intra-domain roaming. Both the probe message and the reply message are 40-bytes long. The probe interval is still set to 2 s.
2. *Handoff overhead.* The handoff overhead includes both the intra-domain handoff overhead and inter-domain handoff overhead. The intra-domain handoff traffic includes association control traffic and GARP traffic, as discussed above. The inter-domain handoff traffic also includes association request messages, association confirmation messages, gratuitous ARP messages and disassociation messages. However, the association request message is 160 bytes, the association confirmation message is 176 bytes, and the disassociation message is 96 bytes long. The gratuitous ARP message is still 28 bytes long. When the number of the handoffs increases, the handoff overhead increases.
3. *Tunnel control.* To reduce the number of hops during inter-domain roaming, tunnel control messages are sent to remove redundant tunnels. A tunnel control message is 64 bytes long, and it costs the lowest amount of bandwidth in overhead.

Table 10 shows overhead traffic during inter-domain roaming under four mobility models. As with intra-domain roaming, link control traffic consumes the most bandwidth. The total overhead traffic is still very low. Figs. 17–20 show a comparison between CBR traffic throughput and the overhead traffic throughput in a simulation of each mobility model. In addition, the comparison of our scheme and SMesh [6] on handoff overhead is shown in Fig. 21. Our solution causes less overhead than SMesh.

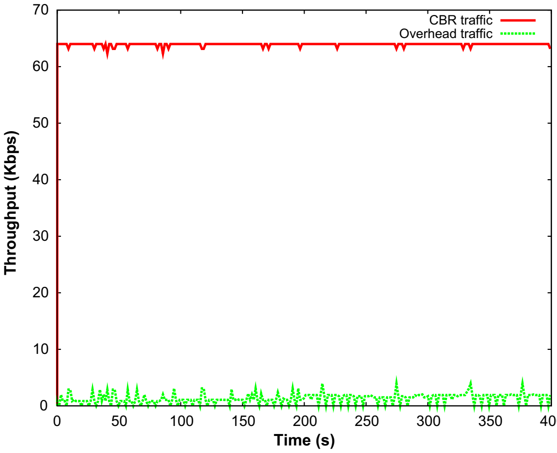

Fig. 17. Traffic throughput and overhead throughput in the case of BRMM during inter-domain roaming.

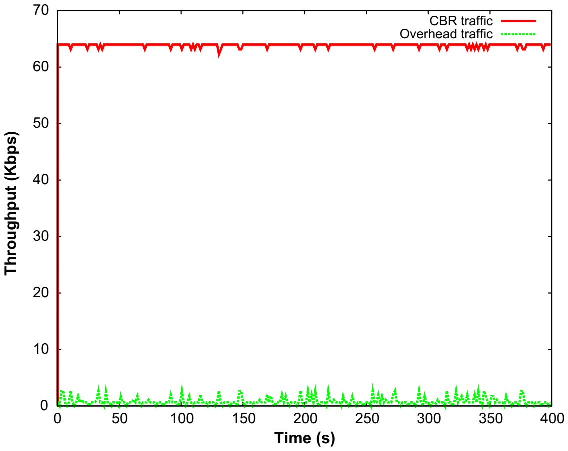

Fig. 18. Traffic throughput and overhead throughput in the case of BMMM during inter-domain roaming.

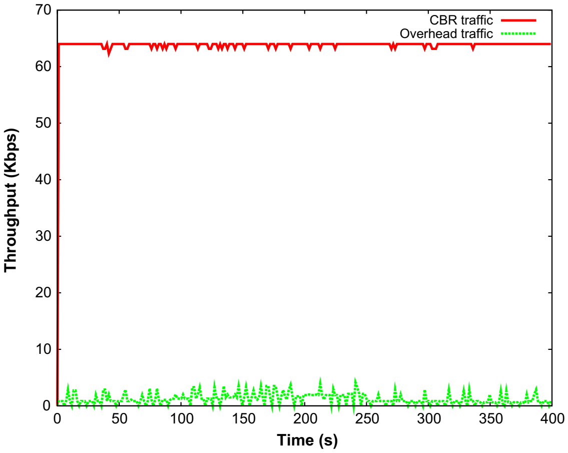

Fig. 19. Traffic throughput and overhead throughput in the case of RDMM during inter-domain roaming.

There are also two parts in the inter-domain handoff: link layer association and the network layer handoff. In our experiments, the network layer handoff is measured as the time period between the triggering of the association request by the mobile client and the establishing of a tunnel between the original gateway and the new gateway. Average network layer handoff latency under four mobility models is shown in Table 10, and the 95% confidence range of the network layer handoff latency is shown in Fig. 14. Moreover, Fig. 22 presents the comparison of our solution with SMesh on inter-domain handoff latency.

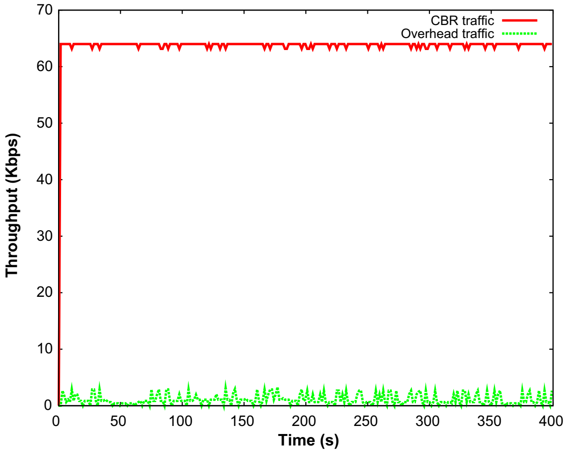

Fig. 20. Traffic throughput and overhead throughput in the case of RWPM during inter-domain roaming.

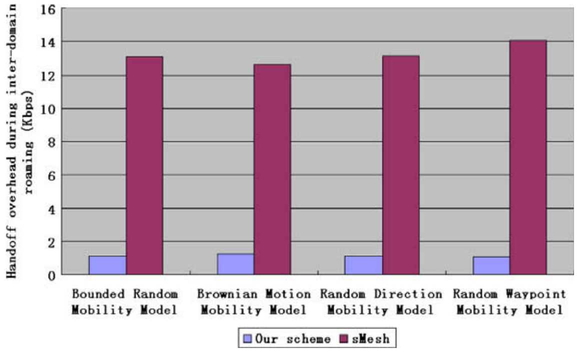

Fig. 21. Average handoff overhead during inter-domain roaming.

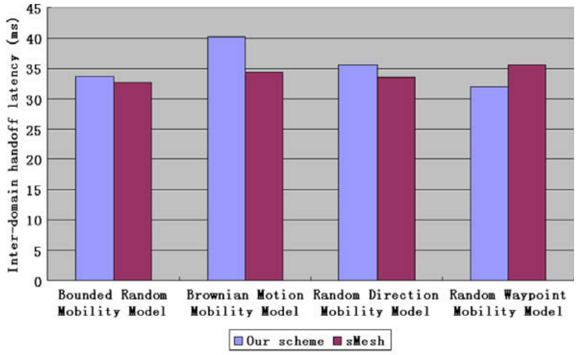

Fig. 22. Average inter-domain handoff latency in network layer.

According to our experiments, our scheme and SMesh perform similarly in terms of handoff latency. The inter-domain handoff latency is around 42.57–96.523 ms, and it successfully achieves the requirements of a real-time application, which is 120 ms. Thus, during inter-domain roaming, our scheme can still be used to support seamless real-time applications.

6. Conclusion

In this paper, existing mobility management solutions for WMNs have been reviewed. A hybrid routing algorithm, which routes with both a MAC address at the link layer and an IP address at the network layer, is introduced. With this routing algorithm, during the intra-domain handoff process, location updates in the centralized location server are avoided, and re-routing after the handoff is not required. Moreover, the inter-domain mobility management scheme is also realized in WMNs. According to the experiment results, seamless handoff can be achieved with a lower overhead cost, and with the packet latency and loss ratio remaining at a lower level in both intra-domain roaming and inter-domain roaming. Our scheme thus can be used to support seamless real-time applications. The issue of security and the question of how to balance security and performance would be an interesting direction for future research.

References

[1] I.F. Akyildiz, J. McNair, J.S.M. Ho, H. Uzunalioglu, W. Wang, Mobility management in next-generation wireless systems, Proceedings of the IEEE 87 (8) (1999) 1347–1384. August.

[2] I.F. Akyildiz, X. Wang, W. Wang, Wireless mesh networks: a survey, Computer Networks 47 (4) (2005) 445–487. March.

[3] I.F. Akyildiz, J. Xie, S. Mohanty, A survey of mobility management in next-generation all-IP-based wireless systems, IEEE Wireless Communications 11 (4) (2004) 16–28.

[4] Y. Amir, C. Danilov, June 2003. Reliable communication in overlay networks, in: Proceedings of the IEEE Dependable Systems and Networks, pp. 511–520.

[5] Y. Amir, C. Danilov, M. Hilsdale, R. Musaloiu-Elefteri, N. Rivera, June 2006. Fast handoff for seamless wireless mesh networks, in: Proceedings of the 4th International Conference on Mobile Systems, Applications and Services, pp. 83–95.

[6] Y. Amir, C. Danilov, R. Musaloiu-Elefteri, N. Rivera, An inter-domain routing protocol for multi-homed wireless mesh networks, in: IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2007, pp. 1–10.

[7] A. Boukerche, Handbook of Algorithms for Wireless Networking and Mobile Computing, Chapman & Hall/CRC, 2005.

[8] A.T. Campbell, J. Gomez, S. Kim, A.G. Valko, C.-Y. Wan, Z.R. Turanyi, Design, implementation, and evaluation of cellular IP, IEEE Personal Communications 7 (4) (2000) 42–49.

[9] T. Clausen, P. Jacquet, Optimized link state routing protocol (OLSR), October 2003. <http://www.ietf.org/rfc/rfc3626.txt,RFC-3626>.

[10] K. Egevang, P. Francis, The IP network address translator (NAT), May 1994. <http://www.ietf.org/rfc/rfc1631.txt,RFC-1631>.

[11] D. Gupta, J. LeBrun, P. Mohapatra, C.-N. Chuah, WDS-based layer 2 routing for wireless mesh networks, in: Proceedings of the 1st International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization, September 2006, pp. 99–100.

[12] E. Gustafsson, A. Jonsson, C.E. Perkins, Mobile IPv4 regional registration, June 2007. <http://www.ietf.org/rfc/rfc4857.txt,RFC-4857>.

[13] R. Huang, C. Zhang, Y. Fang, A mobility management scheme for wireless mesh networks, in: IEEE Global Telecommunications Conference, November 2007, pp. 5092–5096.

[14] IEEE Standard 802.11, 2007. IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements – part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications. <http://www.standards.ieee.org/getieee802/802.11.html>.

[15] IEEE Standard 802.11s, 2006. Draft amendment to standard IEEE 802.11: ESS mesh networking. <http://www.standards.ieee.org/getieee802/download/802.11g-2003.pdf>.

[16] ITU-T Recommendation G.711, 1989. <http://www.itu.int/rec/T-REC-G.711-198811-I/en>.

[17] R. Koodli, Fast handovers for mobile IPv6, July 2005. <http://www.ietf.org/rfc/rfc4068.txt,RFC-4068>.

[18] R. Koodli, C.E. Perkins, Mobile IPv4 fast handovers, October 2007. <http://www.ietf.org/rfc/rfc4988.txt,RFC-4988>.

[19] A. Misra, S. Das, A. Dutta, A. McAuley, S.K. Das, IDMP-based fast handoffs and paging in IP-based 4G mobile networks, IEEE Communications Magazine 40 (3) (2002) 138–145.

[20] V. Navda, A. Kashyap, S.R. Das, Design and evaluation of iMesh: an infrastructure-mode wireless mesh network, in: WoWMoM 2005, pp. 164–170.

[21] ns2, The network simulator – ns-2, 2008. <http://www.isi.edu/nsnam/ns/>.

[22] C.E. Perkins, IP mobility support for IPv4, January 2002. <http://www.ietf.org/rfc/rfc3220.txt,RFC-3220>.

[23] D.C. Plummer, An ethernet address resolution protocol or converting network protocol addresses to 48.bit ethernet address for transmission on ethernet hardware, November 1982. <http://www.ietf.org/rfc/rfc826.txt,RFC-826>.

[24] R. Ramjee, T.L. Porta, S.R. Thuel, K. Varadhan, S.-Y. Wang, HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks, in: Seventh International Conference on Network Protocols, November 1999, pp. 283–292.

[25] M. Ren, C. Liu, H. Zhao, T. Zhao, W. Yan, MEMO: an applied wireless mesh network with client support and mobility management, in: IEEE Global Telecommunications Conference, November 2007, pp. 5075–5079.

[26] H. Soliman, C. Castelluccia, K.E. Malki, L. Bellier, Hierarchical mobile IPv6 mobility management (HMIPv6), August 2005. <http://www.ietf.org/rfc/rfc4140.txt,RFC-4140>.

[27] S. Speicher, OLSR-FastSync: fast post-handoff route discovery in wireless mesh networks, in: IEEE 64th Vehicular Technology Conference, September 2006, pp. 1–5.

[28] S. Speicher, C.H. Cap, Fast layer 3 handoffs in AODV-based IEEE 802.11 wireless mesh networks, in: Third International Symposium on Wireless Communication Systems, September 2006, pp. 233–237.

[29] Spines, The spines overlay network, 2008. <http://www.spines.org>.

[30] H. Wang, Q. Huang, Y. Xia, Y. Wu, Y. Yuan, A network-based local mobility management scheme for wireless mesh networks, in: IEEE Wireless Communications and Networking Conference, March 2007, pp. 3792–3797.

[31] H. Zimmermann, OSI reference model – the ISO model of architecture for open systems interconnection, IEEE Transactions on Communications 28 (4) (1980) 425–432.

Zhenxia Zhang received his B.Sc. and M.Sc. in Computer Science from Zhejiang University, China, respectively in 2004 and 2006. He is now a Ph.D. student at PARADISE Research Laboratory at University of Ottawa. His current research interests are in the field of mobility management, handoff, wireless ad hoc and mesh networks, and wireless sensor networks.

Richard W. Pazzi received his B.Sc. and M.Sc. degrees in Computer Science from the Federal University of Sao Carlos, Brazil, respectively in 2002 and 2004. He received his Ph.D. degree from the University of Ottawa, Canada, in 2008. He is currently a Research Associate at the PARADISE Research Laboratory at the University of Ottawa. He was the recipient of Best Research Paper Awards from ICC 2009 and IWCMC 2009. He has been working with fault-tolerant protocols for wireless sensor networks and mobile computing. His research interests also include vehicular ad hoc networks, multimedia communications, networked 3D virtual environments, and computer graphics.

Azzedine Boukerche is a full professor and holds a Canada Research Chair position at the University of Ottawa (uOttawa). He is the founding director of the PARADISE Research Laboratory, School of Information Technology and Engineering (SITE), Ottawa. Prior to this, he held a faculty position at the University of North Texas, and he was a senior scientist at the Simulation Sciences Division, Metron Corp., San Diego. He was also employed as a faculty member in the School of Computer Science, McGill University, and taught at the Polytechnic of Montreal. He spent a year at the JPL/NASA-California Institute of Technology, where he contributed to a project centered about the specification and verification of the software used to control interplanetary spacecraft operated by JPL/NASA Laboratory. His current research interests include wireless ad hoc and sensor networks, wireless networks, mobile and pervasive computing, wireless multimedia, QoS service provisioning, performance evaluation and modeling of large-scale distributed systems, distributed computing, large-scale distributed interactive simulation, and parallel discrete-event simulation. He has published several research papers in these areas. He served as a guest editor for the Journal of Parallel and Distributed Computing (special issue for routing for mobile ad hoc, special issue for wireless communication and mobile computing, and special issue for mobile ad hoc networking and computing), ACM/Kluwer Wireless Networks, ACM/Kluwer Mobile Networks Applications, and Journal of Wireless Communication and Mobile Computing. He serves as an Associate Editor of IEEE Transactions on Parallel and Distributed systems, IEEE Transactions on Vehicular Technology, Elsevier Ad Hoc Networks, Wiley International Journal of Wireless Communication and Mobile Computing, Wileys Security and Communication Network Journal, Elsevier Pervasive and Mobile Computing Journal, IEEE Wireless Communication Magazine, Elsevier's Journal of Parallel and Distributed Computing, and SCS Transactions on Simulation. He was the recipient of the Best Research Paper Award at IEEE/ACM PADS 1997, ACM MobiWac 2006, ICC 2008, ICC 2009 and IWCMC 2009, and the recipient of the Third National Award for Telecommunication Software in 1999 for his work on a distributed security systems on mobile phone operations. He has been nominated for the Best Paper Award at the IEEE/ACM PADS 1999 and ACM MSWiM 2001. He is a recipient of an Ontario Early Research Excellence Award (previously known as Premier of Ontario Research Excellence Award), Ontario Distinguished Researcher Award, and Glinski Research Excellence Award. He is a cofounder of the QShine International Conference on Quality of Service for Wireless/Wired Heterogeneous Networks (QShine 2004). He served as the general chair for the Eighth ACM/IEEE Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, and the Ninth ACM/IEEE Symposium on Distributed Simulation and Real-Time Application (DS-RT), the program chair for the ACM Workshop on QoS and Security for Wireless and Mobile Networks, ACM/IFIPS Europar 2002 Conference, IEEE/SCS Annual Simulation Symposium (ANNS 2002), ACM WWW 2002, IEEE MWCN 2002, IEEE/ACM MASCOTS 2002, IEEE Wireless Local Networks WLN 03–04; IEEE WMAN 04–05, and ACM MSWiM 98–99, and a TPC member of numerous IEEE and ACM sponsored conferences. He served as the vice general chair for the Third IEEE Distributed Computing for Sensor Networks (DCOSS) Conference in 2007, as the program cochair for GLOBECOM 2007–2008 Symposium on Wireless Ad Hoc and Sensor Networks, and for the 14th IEEE ISCC 2009 Symposium on Computer and Communication Symposium, and as the finance chair for ACM Multimedia 2008. He serves as the General Co-Chair for the 11th IEEE International Symposium on a "World of Wireless, Mobile and Multimedia Networks" (WoWMoM 2010). He also serves as a Steering Committee chair for the ACM Modeling, Analysis and Simulation for Wireless and Mobile Systems Conference, the ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, and IEEE/ACM DS-RT.