國立交通大學
資訊工程系
碩士論文

無線網狀網路中路由協定的效能量測

Performance Evaluation of the Routing Protocols in Wireless Mesh Networks

研究生:陶奎志

指導教授:王協源

中華民國九十四年六月

摘要

無線網狀網路(Wireless Mesh Network) 結合了 ad hoc 網路和 infrastructure 網路的兩者優勢，它是由多個網狀存取點(Mesh Access Point)和網狀客戶端(Mesh Client)組成。 在無線網狀網路裡 Mesh Access Point 可以使用 ad hoc 的介面來與其他 Mesh Access Point 溝通，而 Mesh Client 會透過 infrastructure 模式來與 Access Point 做連結。爲了幫助轉送從 Mesh Client 來的封包，Mesh Access Point 使用 ad hoc 路由協定來建立路由路徑。在 Access Point 中，主要是由“Wireless Mesh Routing”(WMR)來決定路由，如果在網狀網路裡的 WMR 採用一個沒有效率的路由協定，那無線網狀網路的可能將會獲得很差的效能且失去了擴充性，由此可見 WMR 對無線網狀網路而言是非常重要的。

在這篇論文裡， 我們使用 NCTUns 網路模擬器來模擬這些經常使用在無線網狀網路裡的路由協定，例如 OSPF，AODV 和 STP。 在比較這些路由協定的模擬結果之後，我們發現 OSPF 最適合用在無線網狀網路的路由協定，但是它仍然有一些問題存在，因此我們提出一個架構叫做 Multi-Gateway 且引入 RoofNet 的 ETX 來幫助 OSPF 的路由協定，進而改進無線網狀網路的效能。

Abstract

The wireless mesh network combines both the advantages of ad hoc networks and infrastructure networks. It is composed of multiple mesh access points and mesh clients. A mesh access point in the wireless mesh network uses an ad hoc mode wireless interface to communicate with other mesh access points, and mesh clients connect to its neighboring mesh access points by using the infrastructure mode wireless interface. In order to forward data packets from mesh clients, mesh access points use the wireless mesh routing protocol to construct the routing path. “Wireless Mesh Routing” (WMR) is the main component in an access point that decides how to route packets. The performance and the scalability of a wireless mesh network may be poor if WMR in the mesh network adopts an inefficient ad hoc routing protocol. Therefore, WMR is very important to wireless mesh networks.

In this paper, we used the NCTUns network simulator to evaluate several commonly used routing protocols in wireless mesh networks, such as OSPF, AODV and STP. After comparing the simulation results of these routing protocols, we find OSPF is the most suitable protocol for wireless mesh networks. However, it still has some problems. Therefore, we propose a multi-gateway architecture and apply the ETX metric to the OSPF routing protocol to improve the performance of the wireless mesh network.

致謝

首先感謝恩師王協源教授二年來對我的悉心指導，除了讓我在課業上進步良多之外，也教導了我許多待人處世的道理。

感謝各位口試委員撥冗來到交通大學進行口試，讓我知不足之處，使這篇論文更加完善。

最後感謝網路與系統實驗室的所有成員，因為有你們的陪伴以及彼此間的鼓勵，讓我在研究所二年不僅學到很多，生活也很充實快樂。在此特別感謝林志哲學長、陳志昌學長與徐明婉同學，你們的幫助讓這篇論文更形完善。

Table of Contents

List of Figures

1. Introduction

As wireless networks become more and more popular, users start to desire higher quality of wireless services, for example, higher bandwidth, greater coverage, and better reliability for wireless accesses. Recently, the wireless mesh network, a new type of wireless networks, emerges to be a better alternative solution to Internet accesses outdoors and in buildings because the infrastructure of the wireless mesh network is easy deployed and managed with low costs. Due to the advances of semi-conducting and SOC industries, the volume and manufacturing cost of a component in the infrastructure of the wireless mesh network is small nowadays. The wireless mesh network is composed of multiple mesh access points and mesh clients. A mesh client represents a device that a user uses to access the Internet via a mesh network, and a mesh access point acts as a router or a bridge in a fixed network to forward packets sent by mesh clients. In a wireless mesh network, mesh access points route packets without a centralized control unit. As such, the wireless mesh network eliminates the occurrence of “centralized failure” and provides self-healing, self-organized and self-configured.

In wireless mesh networks, a mesh client is required to attach to one of the access points operating in the IEEE 802.11 infrastructure mode, and an access point has to be capable of operating in the infrastructure and ad hoc modes simultaneously. An access point communicates with client nodes that are attached to it via the infrastructure mode and communicates with other access points via the ad-hoc mode. As such, access points in the wireless mesh network forms a type of Mobile Ad-hoc Network (MANET). Since the wireless mesh work shares many common features with the mobile ad hoc network, the routing protocols developed for the ad hoc network can be applied to the wireless mesh network. For example, Microsoft mesh networks and

RoofNet of the MIT are based on the DSR (Dynamic Source Routing) protocol, and many commercial products of wireless mesh networks adopt AODV (Ad hoc On-demand Distance Vector Routing) as the underlying routing protocols.

However, the wireless mesh network brings different challenges for ad hoc routing protocols because access points in the wireless mesh network are fixed and have unstable bit error rates of channels due to the interference and wireless natures. Therefore, traditional ad hoc routing protocols may not be suitable for the wireless mesh network because those ad hoc routing protocols assume that network nodes are mobile and thus may spend unnecessary overheads on detecting the movements of mesh access points. To address this problem, some wireless mesh networks adopt routing protocols used on fixed networks, such as OSPF (Open shortest path first routing protocol) [1] and so on.

It is interesting to know which routing protocol would have the best performances when it is applied to the wireless mesh network. In the literature, analyses about the performances of routing protocols in the wireless network are rare. So, in this thesis we compare the performances of the most commonly used routing protocols in wireless mesh networks, such as OSPF, AODV. The simulation results show that links among access points and the central access point (the central access point is the only node that connects to the Internet) are the bottlenecks of wireless mesh networks because multiple access points have to share the same channel to forward packets to a gateway. To further improve the performances of wireless mesh networks, we develop a multi-gateway system to distribute packets over multiple gateways to alleviate the interference and the contentions in those critical links. Finally, we use a more realistic physical layer model in our simulations to produce more accurate results. In addition, we implemented the ETX algorithm (the expected transmission count metric) [19] proposed in RoofNet [9] in OSPF, which outperforms other commonly used routing protocols in the wireless mesh network, to further improve the performances of OSPF.

2. Background

2.1. Architecture of Wireless Mesh Networks

There are two types of wireless architectures. One is the infrastructure network, and the other is the ad hoc network. The infrastructure network uses an access point to control and forward packets. It is the most popular architecture in the wireless network. An access points are usually fixed and the transmission range is limited. A mobile node which desires for the networking service must remain within the range. The ad hoc network is a kind of peer-to-peer network. In the ad hoc network, all mobile nodes share the same radio channel. Each node contends with each other and uses ad hoc routing protocol to make packets be correctly route in the network. Due to the limited transmission range of mobile nodes, packets in the ad hoc network usually traverse several nodes to reach their destination nodes. The ad hoc network is quite different from the infrastructure network, and it doesn't have any central node to manage and monitor the whole network. In this kind of networks, Mobile nodes will find the routing path by using the routing protocol. Nodes in the ad hoc network are equal, and they can spread freely and be disposed automatically.

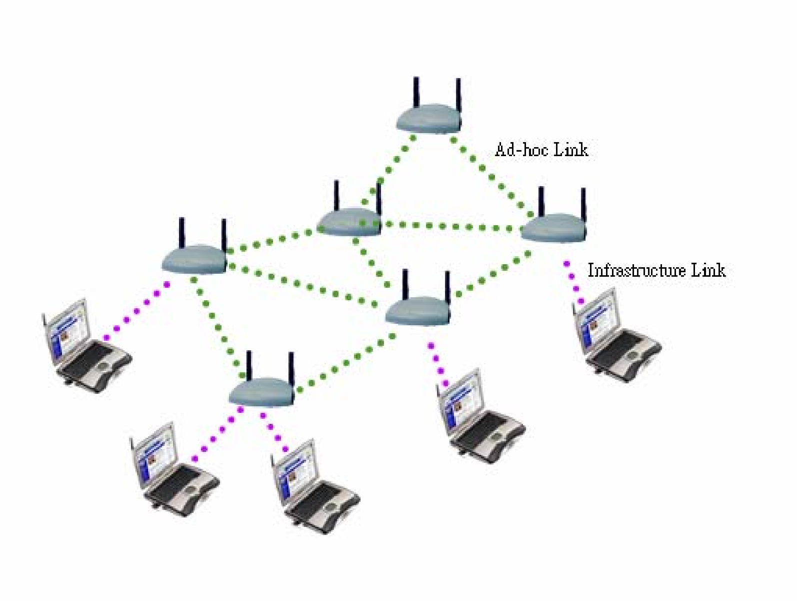

Figure 2-1 Mesh clients and mesh access points

The wireless mesh network combines the advantages of the ad hoc network and the infrastructure network. An access points in the wireless mesh network can be regarded as a forwarding node in the ad hoc network because in the wireless mesh network an access point uses an ad hoc mode radio channel to exchange packets with other access points. On the other hand, an access point also plays the role as a bridge for mesh clients. In the Figure 2-1 Mesh clients and mesh access points, the mobile nodes, called mesh clients, connected to the neighboring mesh access points at the beginning by using the infrastructure mode channel. Mesh access points use the wireless mesh routing protocol to construct routes for data packets of mesh clients with the ad hoc mode channels.

2.2. Characteristics of Wireless Mesh Networks

The main characteristics of the wireless mesh network are shown as follows:

- Self-routing – traditionally, the network administrator needs set up the static routing to tell the router how to route packets. Wireless mesh networks use wireless mesh routing protocols to route packet automatically. It makes the configuration of the routing for a network easier and the network disposed more convenient.

- Self-organized – in wireless mesh networks, mesh access point can use the routing protocol to form a group inside which all access points are connected. This simplifies the work of configuring and deploying a network for service providers.

- Self-healing – when a mesh access point malfunctions, it is easy to detect it and repair the routing paths that are broken due to this broken access point by choosing another forwarding access points.

3. Routing Protocols for Wireless Mesh Networks

3.1. Wireless Mesh Routing

"Wireless Mesh Routing" (WMR) is the main component in an access point that decides how to route packets. In the ad hoc network, throughputs experienced by end users are affected by hop counts of routing paths, the propagation loss, and the noise interference. The performances and the scalability of a wireless mesh network may be poor if WMR in the mesh network adopts an inefficient ad hoc routing protocol. Therefore, WMR are very important to wireless mesh networks.

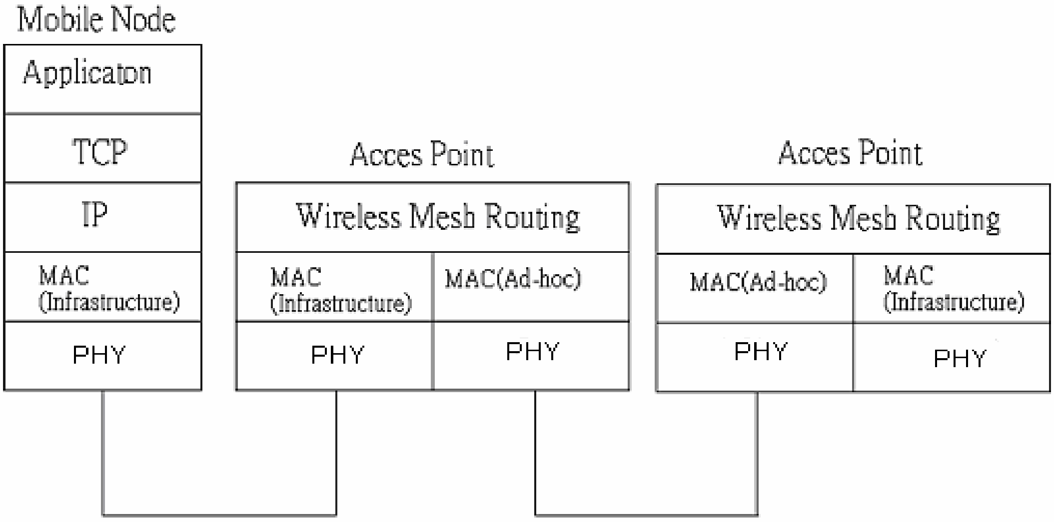

Figure 3-1 Protocol stacks of the wireless mesh routing

In the Figure 3-1, WMR is implemented on the mesh access points. When an application on the mobile node sends a data packet, the mesh access points will receive it from infrastructure interface and pass it to WMR. Then, WMR will forward packets to the ad hoc interface by IP address or MAC address of the packet.

3.2. Existing Routing Protocols

In this section, we first introduce currently-existed famous routing protocols for MANET and fixed networks. Routing protocols have been developed for many years. Since wireless mesh networks have the properties of the ad hoc network, there are lots of ad hoc routing protocols in the MANET. For example, AODV [5], DSR [3], and DSDV [4] are used in the MANET. In section 3.2.1, we briefly introduce routing protocols proposed for MANET, such as AODV. However, the mesh access points are fixed, so the high mobility is not major problems in wireless mesh networks. Mesh access points are just like the switches and routers in the wireless mesh networks. It can use the routing protocols running on switches and routers. In section 3.2.2, we describe how the spanning tree protocol works. In section 3.2.3, we introduce the two famous routing protocols used on the Internet backbone, RIP and OSPF. In addition, we also discuss the advantages and disadvantages of these protocols for the wireless mesh network.

3.2.1. MANET

There are two types of ad hoc routing protocols so far: (1) proactive (table-driven) (2) reactive (On-demand). These two kinds of routing protocols work in the distance manner.

3.2.1.1. Proactive (Table-driven) Protocols

The proactive protocols produce route control packets periodically between nodes. Every node needs to maintain a route table for all other nodes in the network. Each time the periodical route control packets are received by some nodes, this node must re-compute the route that can be derived from the control packets and updates the route table if needed. The drawbacks of proactive routing protocols are as follows. First, even in the low mobility environment, the route may not be changed over time. Nodes using proactive routing protocols still have to broadcast control packets periodically and thus waste bandwidth of the network. Furthermore, nodes may maintain a lot of routes never used. In such case, the messages exchanges for those unused routes will generate many unnecessary overheads. Although the table-driven protocol can build the routing path quickly, it wastes a lot of resource to keep the correctness of the route information. The overhead of the control packets is critical in the kind of bandwidth-critical networks.

3.2.1.2. Reactive (On-demand) Protocols

A reactive protocol triggers the routing path construction only when necessary. When a node wants to send a packet, it consults its route table to find a valid route to the destination of the packet. If one valid route is found, the routing protocol sends out the packet according to the found route. If not, this node initiates the route request process for the destination node indicated by the packet. The source node generates a corresponding valid route entry for this destination when it receives a response for this destination node. The validity of the route is determined by the lifetime. If the route is not used for some period, the route is considered to be no longer needed and is removed from the routing table. Before the route expired if the route is accessed, the lifetime of it is extended. Contrary to the proactive protocols, the reactive protocols maintain the route information when need to transmit packets. It reduces the unnecessary overheads at the cost of spending more time on finding a route.

Ad-Hoc on Demand Distance Vector (AODV) [5] routing protocol is a famous reactive protocol for ad hoc network. It is a representative of the reactive protocols in wireless networks. In AODV, the protocol operation is performed based on the packet demand. There will be no route maintained if there is no packet to be transmitted. So the route discovery process is initiated only when the source node tries to send a packet and there is no active route found in source node’s routing table. In the AODV routing protocol, the source node initiates the route discovery process by broadcasting the route request (RREQ) for the destination node. Each node excluding the destination node received the RREQ will forward the RREQ by re-broadcasting it. The dissemination of RREQ works in the flooding manner until the destination node is reached. The destination node received the RREQ will send back a route reply (RREP) to the source node through the reverse path of RREQ. The intermediate nodes on the reverse path will forward the RREP to the source node hop by hop. There is an alternative way to improve the response time of the route discovery process. If an intermediate node which has already route information for the destination node receives the RREQ, it can send back an RREP directly to the source node.

3.2.2. Spanning Tree Protocol

The spanning tree protocol was developed as a method for loop prevention on LANs. It allows bridges to exchange messages with each other, so they can create loop-free paths to other switches. Each bridge runs an algorithm which considers how loops can be prevented. STP prevents loops occurring in a network by blocking connections that could cause a loop. When a switch finds one of its ports may cause a loop in the network, it blocks this port to prevent a loop forming. STP elects a root bridge in the network. Then, each other bridge selects one of its ports with the least path cost to the root bridge. The least cost path is determined by STP’s looking at the bandwidth of a link. STP continually monitors the network to detect failures on switch ports and changes in the network topology. If STP detects any changes to the current topology, it quickly makes redundant ports available to make the network still connected and closes some other ports to ensure that the network is still loop-free if needed. In addition, STP uses a passive-learning method to avoid the wastes generated by the network detection procedure. It reconstructs the network each time when the network topology changes.

The root bridge on a LAN is selected by an election taking place. Each switch running STP exchanges its local information in a format called bridge protocol data units (BPDUs). When the priorities of all switches and bridges combined with their MAC addresses are all exchanged over the whole network, the bridge with the highest ID is selected as the root bridge. All ports on the root bridge are known as designated ports. On non-root bridges, only one port can be designated, all others are blocked. Designated ports forward MAC addresses of switches and bridges. Designated ports are selected after the bridge determines the lowest cost path to get to the root bridge. All designated ports are in what is known as forwarding state. A port with forwarding state is allowed to send and receive traffic. All of the other bridges are known as non-route bridges, they choose a port known as a root port to send and receive traffic. Using this method, the redundant links are closed down. A closed port can be opened again if there is a change to the network topology and that port is needed for recovering a link.

Because STP can do self-routing, self-organization, and self-healing, it’s easy to apply STP to the wireless mesh network. A traditional bridge/switch uses its ports to attach cables that connect to other bridges/switches. In the wireless mesh network, mesh access points use ad-hoc mode interfaces to exploit wireless channels for their communication. It’s obvious that an ad-hoc mode channel of a mesh access point in a wireless mesh network can be analogous to a port in a bridge/switch in a traditional fixed network. The details of STP in the wireless mesh work will be discussed in section 4.3

3.2.3. IP Routing Protocol

There are thousands and thousands of routers on internet. These routes are controlled by IP routing protocols. Routing protocols change information among routers to make the routing information fresh and correct for a network. Routers forward packets according to the routing tables maintained by IP routing protocols. The route information is usually divided into two types – the static routing and the dynamic routing. The static routing means that the routing entries in the routing tables are set up manually. The dynamic routing maintains the routing tables according to the network topology and various network conditions. The main advantage of the dynamic routing is that the router can choose another routing path to forward packets when the original routing path is broken. OSPF and RIP are two most popular dynamic routing protocols in the internet. Currently, these two protocols are standardized and widespread.

3.2.3.1. RIP

Route Information Protocol (RIP) is based on the distance-vector algorithm. Routers broadcast their own routing tables periodically and will calculate a shortest path based on the exchanged information to route packets. RIP is a simple routing protocol and cannot be used in a large network, because it has too many control messages and thus waste the network bandwidth.

3.2.3.2. OSPF

Open Shortest Path First (OSPF) is a routing protocol developed for IP network by IETF. OSPF was created because in the mid-1980s, the RIP was increasingly incapable of serving large, heterogeneous networks. OSPF is a link-state routing protocol that relies on flooding of link-state advertisements (LSAs) to all other routers within the same hierarchical area. Information including attached interfaces and other variables are included in OSPF LSAs. As an OSPF router accumulates link-state information, it uses the SPF algorithm to calculate the shortest path to all other nodes. Routers running the distance-vector algorithm, such as RIP, send all or a portion of their routing tables in routing-update messages to their neighbors. By contrast, OSPF only needs to flood updates on routing table sections which have changed. It does not send the entire routing table. OSPF uses logically segmented areas and networks to decrease the size of routing tables. Table size can be further reduced by using route summarization.

The Shortest Path First (SPF) algorithm is the basis for OSPF protocol. When an SPF router is powered up, it initializes its routing protocol data structures and then uses OSPF Hello protocol to acquire neighboring routers. The router sends hello packets to its neighbors and receives their hello packets. A hello packet used by OSPF not only carries the information of neighboring nodes but also acts as keep-alive to let routers know that other routers are still active and functional. On multi-access networks (networks supporting more than two routers), the Hello protocol elects a designated router and a backup designated router. The designated router is responsible for generating LSAs that describe the statuses of the links in its authorized area for the entire multi-access network. Designated routers allow a reduction in network traffic and in the size of the topological database.

Due to the success of OSPF on Internet, we choose it to compare to AODV and STP in wireless mesh networks. In section 4.4, we will discuss our implementation of OSPF in the wireless mesh network. All of the comparisons among the tree routing protocols will be listed in Chapter 5.

4. Design and Implementation

In this chapter, we will introduce the module system design in the NCTUns network simulation. Then we will explain the design and implementation of the tree routing protocols.

4.1. High Level System Design

4.1.1. Module Framework in the NCTUns network simulator

The following implementation and simulation will be held on NCTUns network simulator. The NCTUns is a high-fidelity and extensible network simulator capable of simulating various protocols used in both wired and wireless IP networks. The NCTUns network simulator provides a module-based platform for module developers to easily develop their modules and integrate them into our network simulator. A module may be a network protocol such as IEEE 802.3 MAC protocol. By developing and combining modules on this platform, we can create a special device node on NCTUns network simulator. Figure 4-1 depicts a network topology consisting of three nodes and the organization of each node.

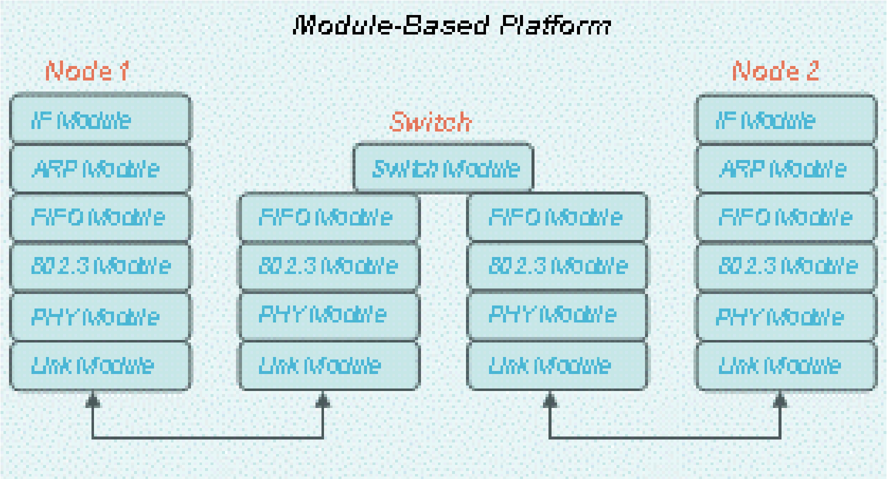

Figure 4-1 Module-based platform in the NCTUns

The NCTUns network simulator provides a basic module prototype. Every module inherits from this basic module prototype and implements some virtual functions of the module prototype. Figure 4-2 show such a prototype.

```
class NslObject {
            …… < deleted > ……
            MBinder         *recvtarget_;   /* to upper component */
            MBinder         *sendtarget_;   /* to lower component */
            NslObject(u_int32_t, u_int32_t, u_int32_t, char *);
            NslObject();
            virtual ~NslObject();

            virtual inline int          init();
            virtual inline int          recv(ePacket_ *);
            virtual inline int          send(ePacket_ *);
            virtual int                 get(ePacket_ *, MBinder *);
            virtual int                 put(ePacket_ *, MBinder *);
            virtual ePacket_            *put1(ePacket_ *, MBinder *);
            virtual inline int          command(int argc, char *argv[]);
            …… < deleted > ……
};
```

Figure 4-2 class NslObject

The most important virtual member functions of the module prototype are send() and recv(). If a node receives a packet, the *recv()* member function of all modules in the node will be called. As the Figure 4-3 shows, when an upon packet is received, the *recv()* functions in the module 3, module 2, and module 1 will be called in sequence. By using this method, income packets could be processed by every module on a node.

The *send()* function is contrary to the *recv()* function. Whenever a packet is sent, the *send()* function of the top module (module 1) will be called. After the process of the top module, the send() functions of the module 2 and module 3 will be called one by one. By continuously calling *send()* function in each module on a node, the outgoing packet can be processed on every modules to simulate packet transmissions.

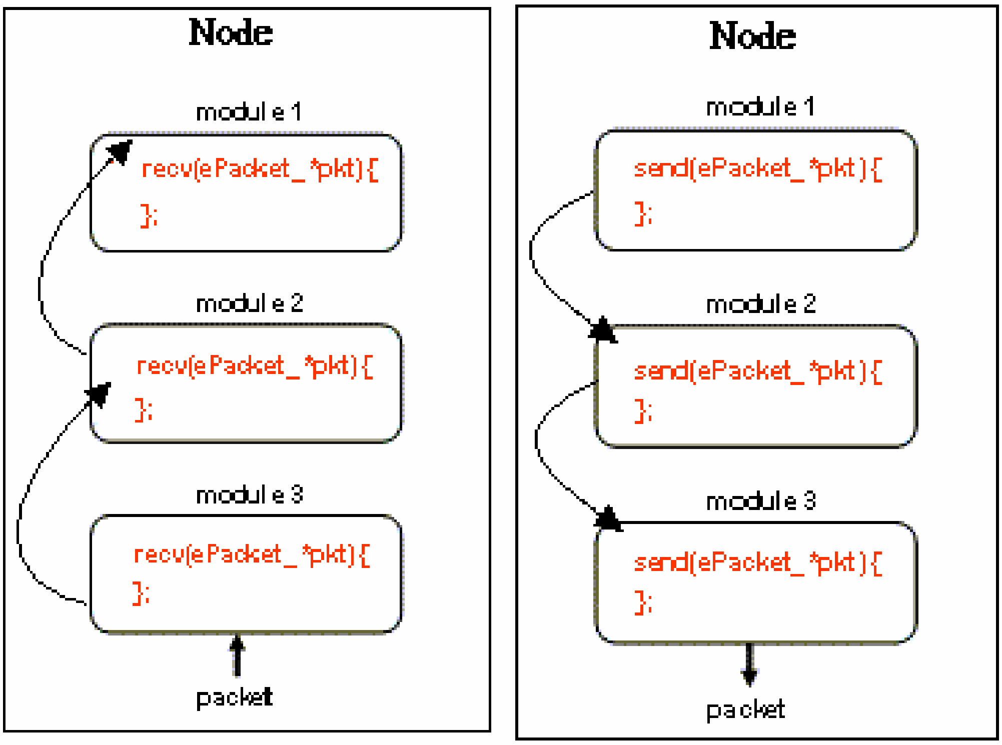

Figure 4-3 send() and recv() among modules

There are some other important member functions in the module prototype – *get()* and *put()*. As Figure 4-4 shows, the *put()* function is used in a module to push a packet to the module's next module. If this function is called, it will try to push a packet to a module or queue the packet in the mbinder. The get() function is used to dispatch packet to *send()* or *recv()* function in a module. Generally, this function is called by put() or put1() of a module's previous module. In this function, it will check a packet flag to see if the packet is an outgoing or incoming packet. If it is for outgoing, the *send()* is called. Otherwise, the *recv()* is called for the incoming packet.

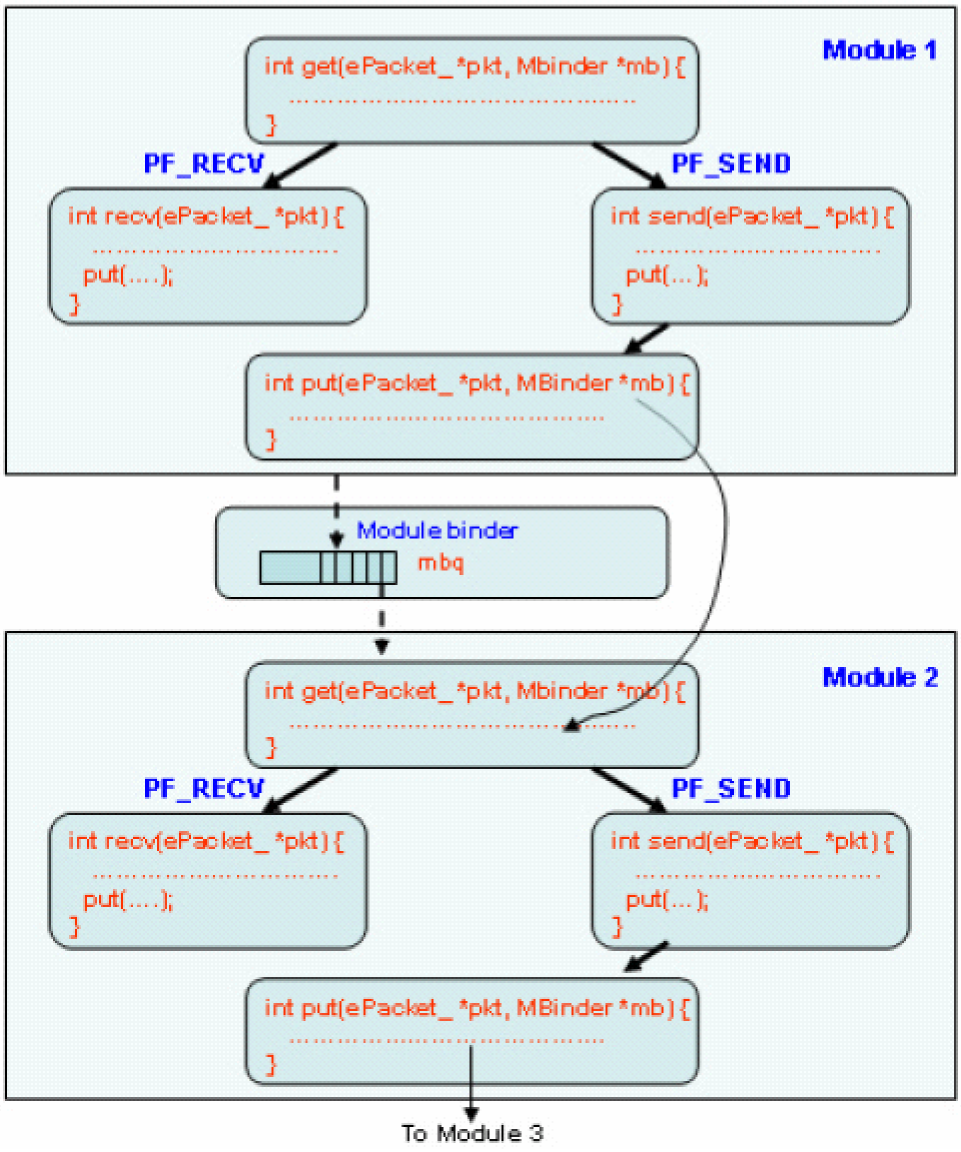

Figure 4-4 send(), recv(), get() and put() among modules

4.1.2. Access Point Node in the NCTUns network simulator

There is a kind of node called access point node in the NCTUns network simulator. As Figure 4-5 shows, it consists of two types of ports. One is wireless port which uses the 802.11 MAC module and Wphy module to simulate wireless network and has an AP module to simulate the behavior of an access point. Another is fixed port to connect to host, route or switch node. At the top of these ports, there is a Switch module to simulate the behavior of a switch.

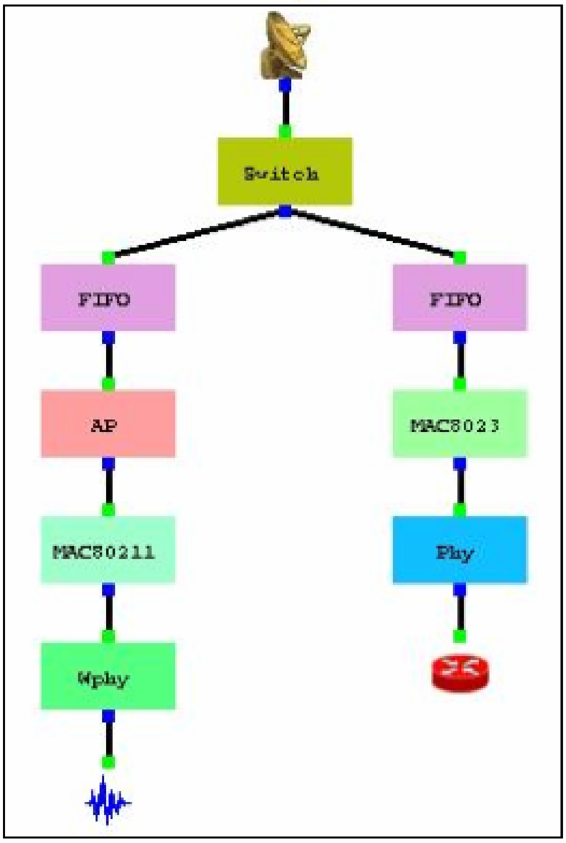

Figure 4-5 Protocol stack of the access point node

In the wireless mesh network, the mesh access point has two wireless interfaces. As Figure 4-6 shows, the mesh access point has two ports. The left port likes the infrastructure port in the old access point. The right port is also a wireless port to connect to the ad hoc network, but it changes the AP module to the MobileNode module (MNode) which can operate in the ad hoc mode. At the top of the two ports, there is a wireless mesh routing module which simulates routing protocol in the wireless mesh networks. Therefore, the implementation of wireless mesh networks in the NCTUns can be simplified to just implement the wireless mesh routing module. We choose three routing protocol to implement and simulate – AODV, STP, and OSPF. As mentioned above, in ad hoc networks, AODV is the most efficient routing protocol, so we choose it to stand for the ad hoc routing protocol. OSPF and spanning tree protocol are the most popular routing protocol in the Internet. Therefore, we use them to compare to the ad hoc routing protocol.

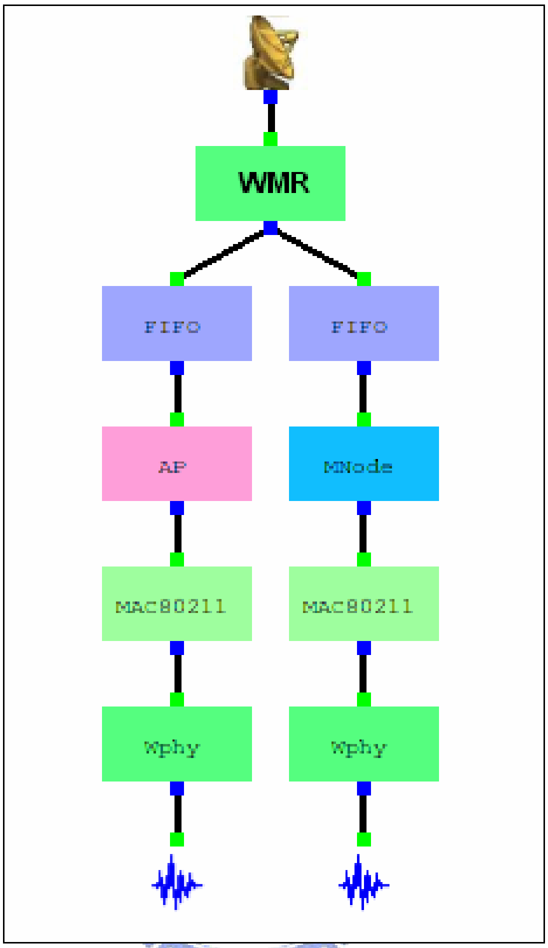

Figure 4-6 Protocol stacks of the mesh access point node

4.2. Implementation of AODV Routing Protocol

AODV is a complicated routing protocol and hard to implement. Fortunately, the NCTUns networks simulator already has the AODV module which simulates the AODV routing protocol and has been tested for years. Figure 4-7 shows the traditional mobile node with AODV routing protocol support. The AODV module will get the IP address of the mobile node from the Interface module and use the IP address for routing packets. When the AODV module routes a packet, it will filled the IP address of next node in the *rt_setgw()* member function of the packet. Then the

ARP module will fill the MAC address corresponding to the IP address into the Ethernet header for the MAC 802.11 module and the Wphy module to simulate the send process of the packet.

It is obviously that the AODV module can't be applied into the wireless mesh networks directly. Therefore, we replace the wireless mesh routing with the Interface module, the AODV module, the ARP module, and the Bridge module. As Figure 4-7 shows, The Interface module, the AODV module, and the ARP module are just the same as the original modules in the mobile node. We implement a new Bridge module to help the AODV module to support two interface routing. When a packet has been received from lower modules, the Bridge module will remember the coming port and the source MAC address of the packet and will put the send packet coming from upper module to the port which the destination MAC address corresponding to. By this method, AODV can work correctly in the wireless mesh network.

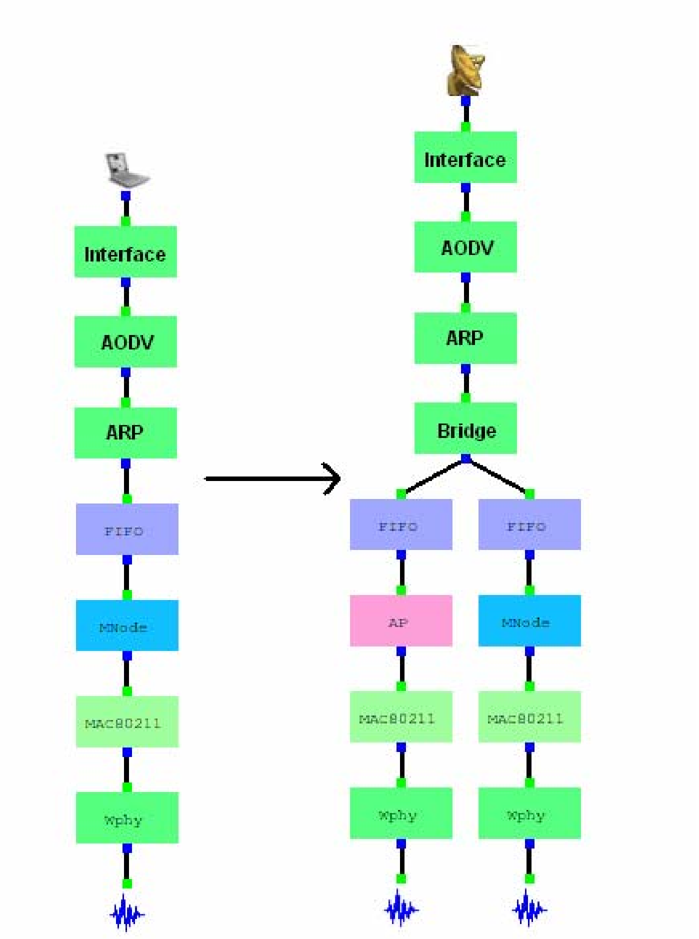

Figure 4-7 Left is the mobile node's protocol stacks, and Right is AODV mesh access point's protocol stacks.

4.3. Implementation of Spanning Tree Protocol

There is a Switch module which simulates the spanning tree protocol in the NCTUns network simulation. Each port of the Switch module has a port state to see if the port is opened or closed, and the switch module has a *SwPort* list to store the states of all ports. Spanning tree protocol will broadcast spanning tree information through these ports to other switches. We implement a MeshSW module to replace the Switch module by modifying the original Switch module. In wireless mesh networks, mesh access points can connect to its neighboring mesh access points. We take the connection between the mesh access points as a switch port and will give it a port state. Originally, the Switch module knows how many ports it has in the initiation, but the MeshSW module can’t get the information at the beginning. It use the *get()* function to check which connection the packets belong to and to see if the connection is in the *SwPort* list or add the connection into the *SwPort* list. When the MeshSW module routes packet in the *send()* function, it will find the corresponding connection which should be passed through and use the Ethernet tunneling to send the packet to the next access point. Consequently, the spanning tree protocol can work on the MeshSW module.

4.4. Implementation of OSPF Routing Protocol

Although there is an OSPF routing daemon in the NCTUns network simulator, it wasn’t implemented as a module. So we developed a simple protocol module, called MeshOSPF module, to support the basic functionalities of OSPF. The MeshOSPF module is different from the standard of OSPF routing protocol which can use designated routers to reduce the traffic. All of the MeshOSPF access points are in the same hierarchy. If a MeshOSPF access point broadcasts the LSA packet, all MeshOSPF access points will receive it. So we call the MeshOSPF module is a simple OSPF protocol module.

Initially, MeshOSPF access points will send hello packet to acquire neighboring access points. Then, all access points will send the LSAs to whole network and use the LSAs which have been received to build the shortest path tree and the routing table. The MeshOSPF access points have two kinds of neighbors – mobile node and access point. An access point neighbor is another MeshOSPF access point which will broadcast hello packet and LSAs. The MeshOSPF access point will use the hello packet to check if the access point neighbor is alive. A mobile node won’t send hello packet and could just only be seen by an access point. Therefore, the MeshOSPF access point updates the lifetime of the mobile node by packets come from it. If there is a LSA which comes from the other MeshOSPF access point and has a mobile node entry which is also its neighbor, the MeshOSPF access point will assume the mobile node has moved to the new MeshOSPF access point and remove it from the neighbor list.

However, when route the packets between the access points, the MAC 80211 module needs to know the MAC address of next hop access point. But the next hop access point also needs to know the original MAC addresses of the source node and destination node, we use Ethernet tunnel to preserve the original MAC addresses between the access points. When a mobile node sends a packet to the MeshOSPF access point, the access point will encapsulate the packet by Ethernet tunnel and forward it.

4.5. Design and Implementation of Multi-Gateway support

In wireless mesh networks, the scalability and the throughput are still problems. For multi-hop networking, it is well known that communication protocols suffer from scalability issues. When the size of network increases, the network performance degrades significantly. Routing protocols may not be able to find a reliable routing path, transport protocols may loose connections, and MAC protocols may experience significant throughput reduction. As a typical example, current IEEE 802.11 MAC protocol and its derivatives cannot achieve reasonable throughput as the number of hops increases to 4 or higher. The reason for low salability is that the end-to-end reliability sharply drops as the scale of the network increases.

In a real wireless mesh system, the most popular scenario is that all mesh clients connect to the internet through the gateway. If there is just only one gateway in the system, the system total throughput will be limited because all of the traffics will share the same bandwidth at the last hop to the gateway. Therefore, we propose a multi-gateway method to enlarge the scalability of the wireless mesh network.

As Figure 4-8 shows, when the mesh clients send the ARP request to ask the MAC address of the Gateway, the mesh access points will forward the ARP request to the gateway which has multiple interfaces. Then the gateway will check which interface the ARP request comes from and send the ARP replay which contains the MAC address of the interface to the mesh client. The ARP request of the mesh client may be received by the gateway more than once, so the gateway will use the interface which received the ARP request first to connect to the mesh client.

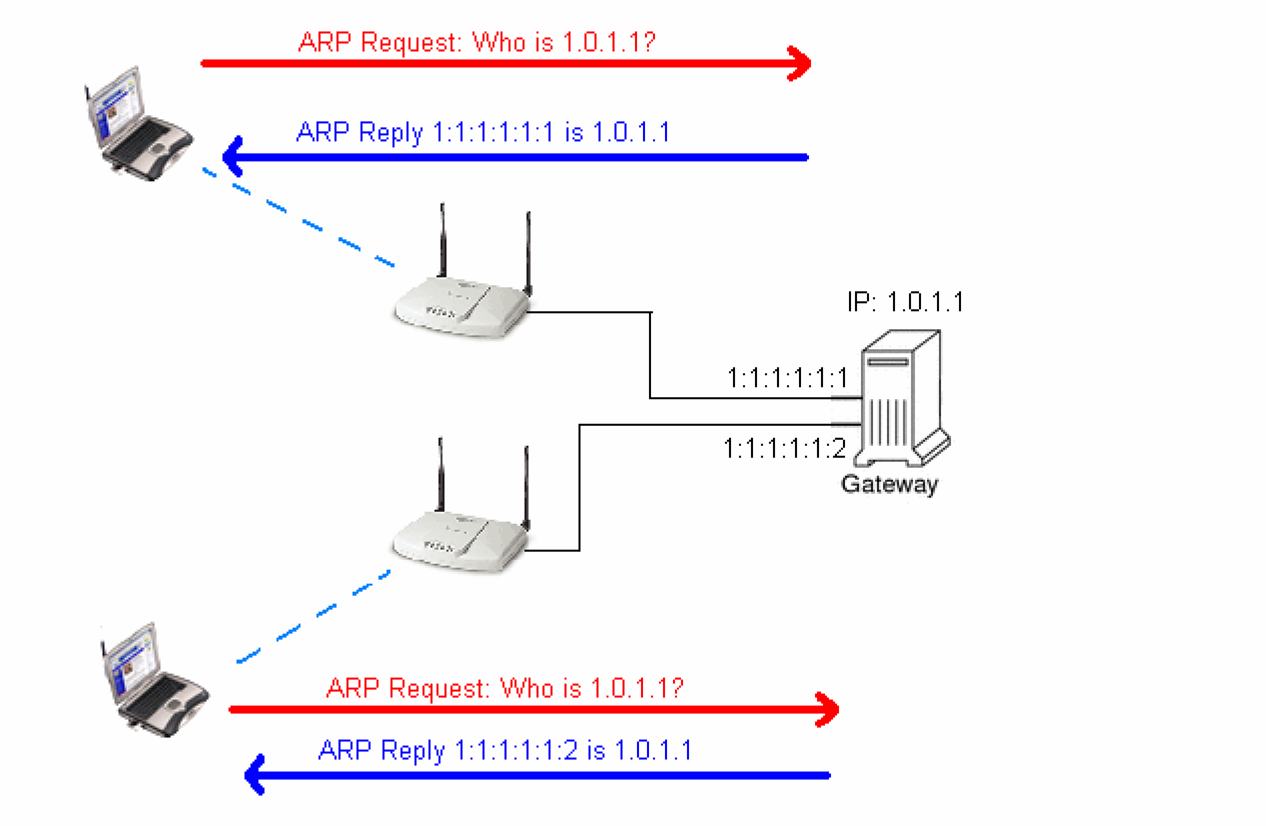

Figure 4-8 ARP request and reply in multi-gateway

We implement a MeshARP module to support multi-gateway in the wireless mesh network. The Figure 4-9 shows that the MeshARP module will connect to multiple interfaces and communicate with the normal ARP module on the mesh clients. Because they are independent from the wireless mesh routing, the MeshARP module can be implemented easily and clearly, and the policy of the multi-gateway can be stand alone.

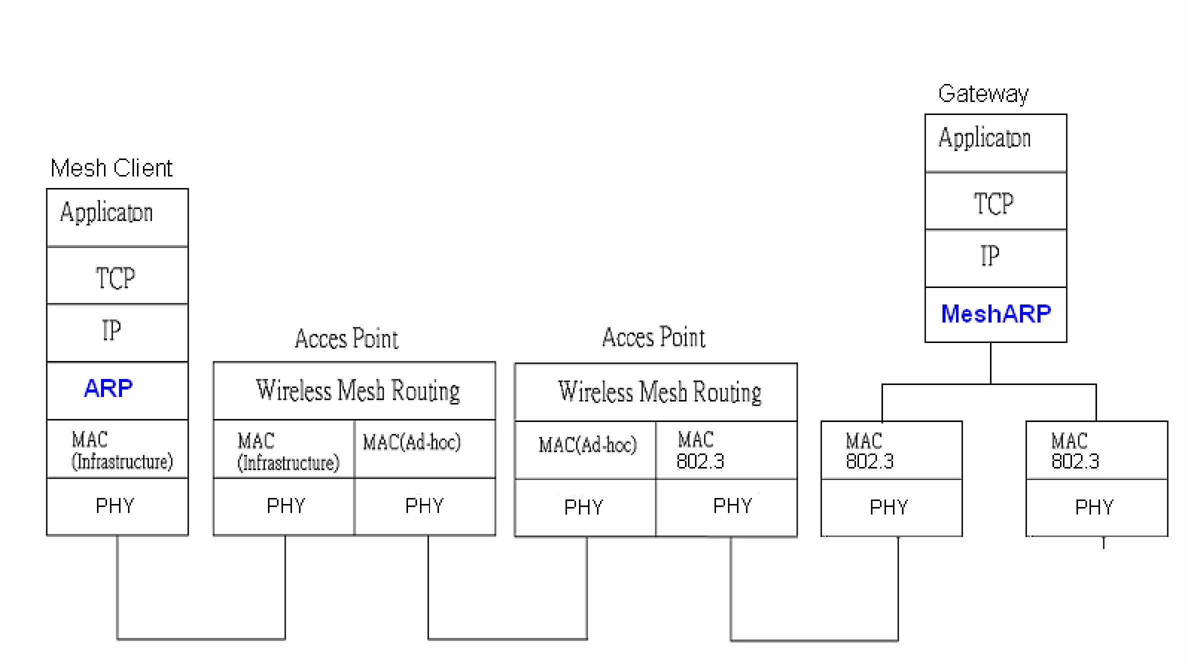

Figure 4-9 Protocol stacks of multi-gateway

We develop the MeshARP module by copy from the ARP module. Then we add the multiple ports support by using a table to store mapping of the MAC address and the ports. Initially, the MeshARP module will record the source MAC addresses and the source ports of the packets. When the MeshARP module fills the Ethernet header and want to send packet, it will use the destination MAC address to find the destination port. In the *arpReply()* function, the MeshARP module will find the port corresponding to the source MAC address and give the MAC address of the port in the ARP reply packet.

4.6. Design and Implementation of OSPF with ETX support

4.6.1. ETX Metric Design

ETX stands for expected transmission count metric. It's designed for RoofNet by MIT to enhance the performance of the ad hoc routing protocol. The ETX metric always chooses routing path with high end-to-end throughput. Using hop count as the metric without considering the delivery ratio may cause some destinations to be unreachable. As Figure 4-10 shows, sometimes the shortest hop may get low performance.

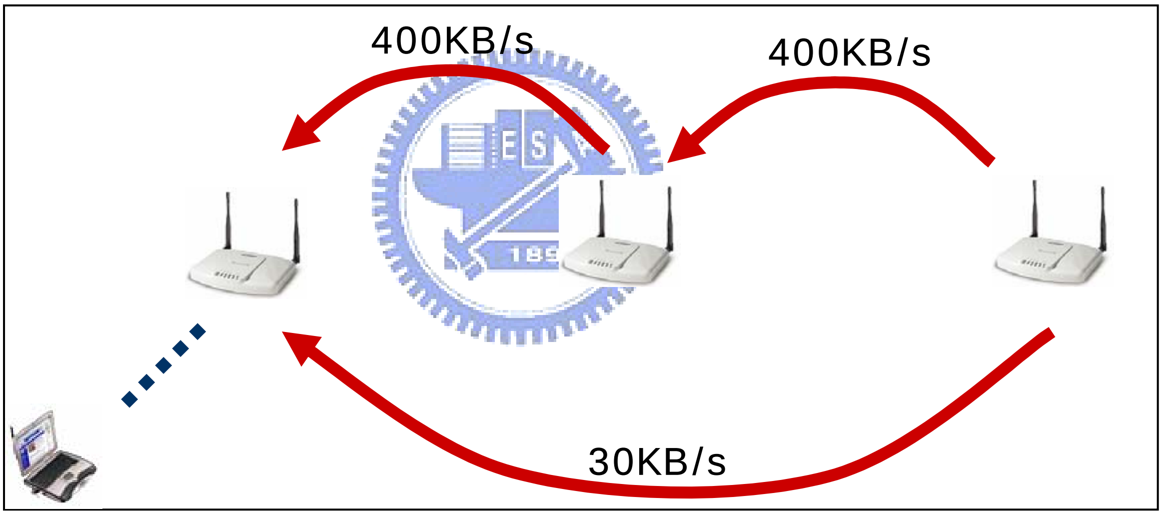

Figure 4-10 Less hop count with low throughput

The ETX of a link is the predicted number of data transmissions required to send a packet over that link. The ETX of a routing path is the sum of the ETX for each link in the routing path. For example, the ETX of a three hop counts routing path with perfect links is three, and the ETX of a one hop counts routing path with a 50% delivery ratio is two. The ETX of a link is calculated using the forward and reverse delivery ratios of the link. The forward delivery ratio, *df*, is the measured probability that a data packet successfully arrives at the recipient; the reverse delivery ratio, *dr*, is the probability that the ACK packet is successfully received. These delivery ratios can be measured as described below. The expected probability that a transmission is successfully received and acknowledged is $df \times dr$. The ETX of a link is:

$$ETX = \frac{1}{df \times dr}$$

The delivery ratio is measured by using the link probe packets. Every node in the ad hoc network will broadcast a fixed size probe packet at a period Γ and remember how many probes packet received during last *w* seconds. *Count(t-w,t)* is the number of probe packets have been received during time t-w to t. The delivery ratio at time *t* is

$$r(t) = \frac{count\ (t - w, t)}{w / \tau}$$

In the RoofNet, DSR and DSDV has been changed to work with ETX metric and prove that the ETX can improve the performance a lot. Because OSPF is also a hop-count routing protocol, it will get poor performance in the real world. Therefore, we modified OSPF routing protocol to support the ETX metric.

As mentioned above in the section 4.4, we implement the MeshOSPF module to support OSPF routing protocol. To support the ETX metric in the MeshOSPF module, first, the MeshOSPF module will count how many the hello packets it has received during a period and use it to calculate the delivery ratio of each neighbor. We add the delivery ratio into the LSAs packets to inform other access points the delivery ratios of our neighbors. As building the shortest path tree, originally, the MeshOSPF module drops the entry which has been inserted into the tree, because the hop count of the previous entry must be less than or equal to the new entry. In OSPF with ETX, the MeshOSPF module calculates the ETX of the routing path to the new entry and compares the new ETX and the old ETX. If the new entry has smaller ETX value, we remove the old entry and all of its child entry from the tree and insert the new entry to the tree. By this method, we can build a tree which has smallest ETX path and can use it to build a routing table which has high end-to-end throughput.

5. Performance Evaluation

5.1. Simulation Environment

All of the simulation will be performed over the NCTUns network simulator. Each case is simulated 20 times with different random positions and the average result is reported. The total simulation time is 200 seconds, but we just take the last 100 seconds to avoid the influence of the startup of the traffic flows (TCP slow start).

As Figure 5-1 shows, 25 mesh access points are deployed. They are placed in a 5x5 metric and the distance between neighboring access points is 200m. Each AP has two wireless 802.11b interfaces. One operates in ad-hoc mode (forward packets) while the other operates in infrastructure mode (serving mesh clients). The transmission and interference ranges of wireless NIC are set to be 250/550 meters. These NICs use different channels to avoid interferences. OSPF, STP or AODV is used among these access points. The access point at the center of the field connects to an Internet gateway using a 100 Mbps link. There are 25 mesh clients at random positions in the system. Each Client has a wireless 802.11b interface operating in infrastructure mode.

Figure 5-1 Simulation topology

5.2. Performance evaluation of Downlink TCP traffic

5.2.1. Topology

The most popular and widely used Internet applications are FTP, HTTP, email, etc. These Internet applications rely on Transmission Control Protocol to reliably transport data across heterogeneous networks and usually receive data from the internet through the gateway. Consequently, we make a downlink TCP traffic scenario. There is a TCP receiver (rtcp) in each mesh client. 25 TCP senders (stcp) run on internet gateway and send TCP traffic to each mesh clients. Therefore, there are 25 TCP traffic flows in the system. In the scenario, all mesh clients are fixed.

5.2.2. Simulation Results and Discussion

Figure 5-2 shows the system total throughput of the tree routing protocol in the wireless mesh network. We can observe that theses routing protocols have almost same performance. However, Figure 5-3 shows that almost all mesh clients can establish TCP connections to the gateway, but the stability of the connections has significant different between AODV and the other routing protocols. In Figure 5-3, the connection whose achieved throughput is greater than 0 KB/sec in more than 1/2 of the simulated duration is a stable connection.

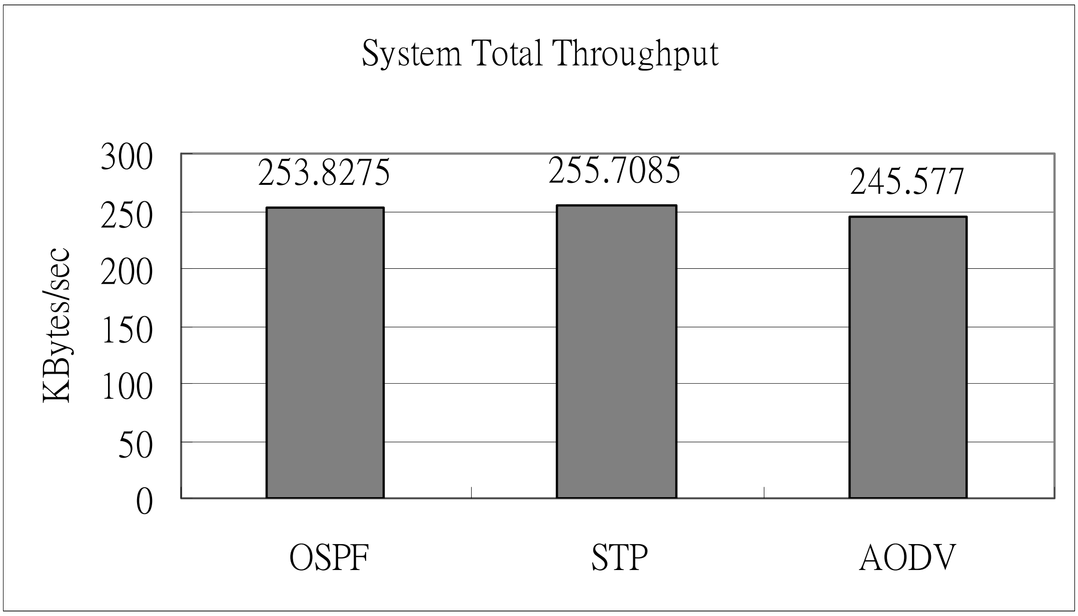

Figure 5-2 System total throughput of downlink TCP traffic

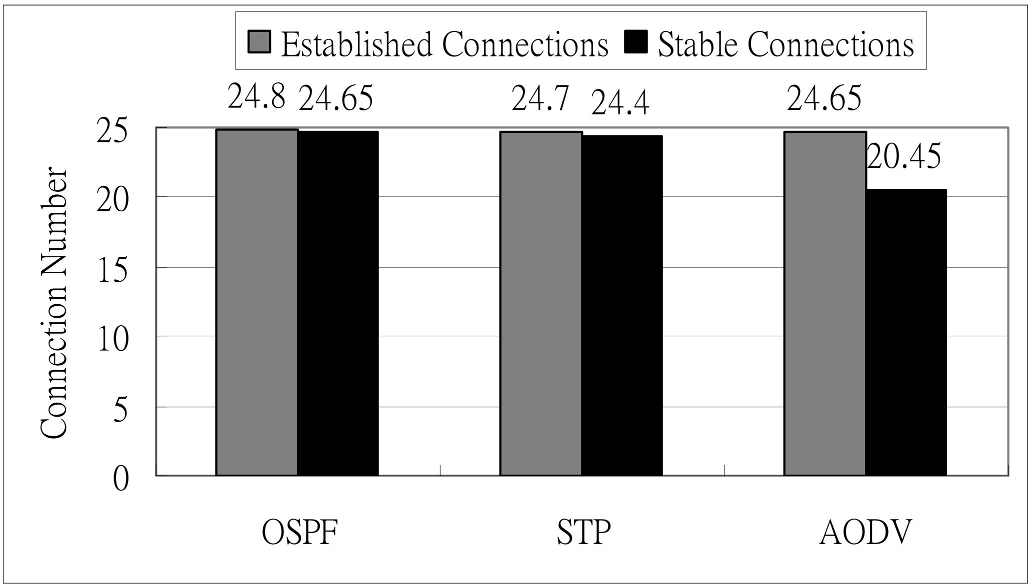

Figure 5-3 Connection number of downlink TCP traffic flows

OSPF, STP, and AODV have almost the same performance, but AODV have less stability. In a fully utilized system, the collisions may happen and active route timeout of AODV routing protocol may be triggered and mesh clients will send the RREQ to rebuild the route link. In wireless mesh network, it will cost a lot of time for AODV to build a route link and RREQ will flood to the whole system. If we increase the active route timeout of AODV, AODV can have almost the same performance as OSPF and STP. However, increasing the active route timeout will decrease the mobility of AODV routing protocol. In ad hoc networks, the mobile nodes usually have high mobility and need to do a lot of overhead to detect the mobility and repair the routing path. Therefore, the ad hoc networks, like AODV, may be not suitable for wireless mesh networks.

Figure 5-4 shows the relation between the hop count of the connection and the throughput in OSPF routing protocol. We can observe that as the hop count of connection decreases, the throughput of single mesh client increases. As Figure 5-5 shows, the more the number of the connections with less hop counts, the more performance could be achieved.

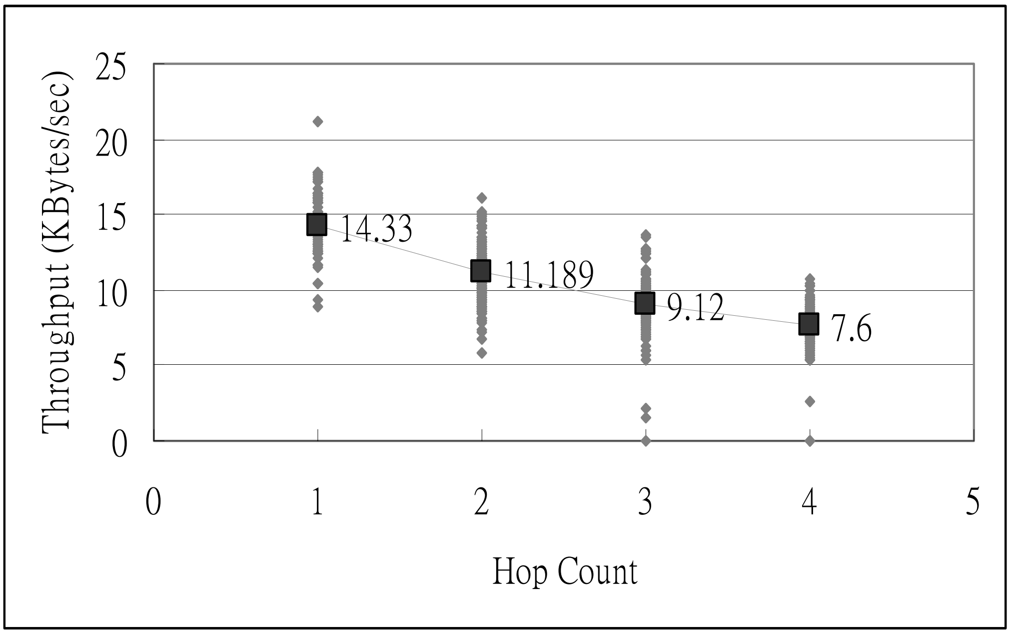

Figure 5-4 Relation between the hop count and throughput of each client

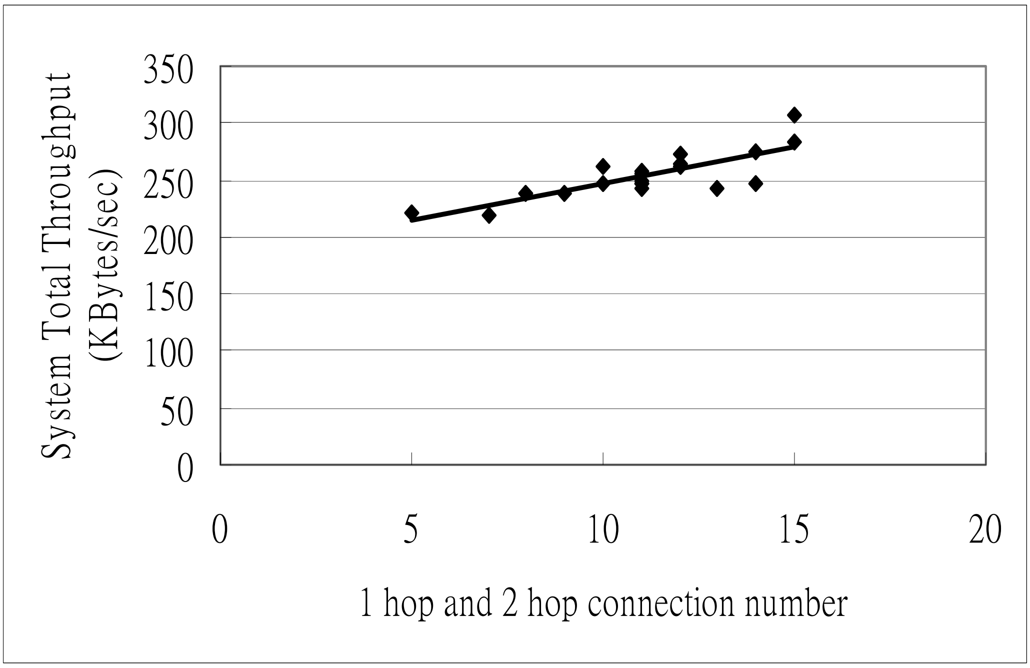

Figure 5-5 Relation between the hop count and system total throughput

5.3. Performance evaluation of Multi-to-Multi Clients TCP traffic

5.3.1. Topology

In recent years, the peer-to-peer applications are more and more popular. Especially the appearance of VOIP lets the application of peer-to-peer networks to be more important. We design a scenario that simulates the condition of peer-to-peer application. There are a TCP receiver (rtcp) and a TCP sender in each mesh clients. The sender and receiver won't be in the same mesh client. Therefore, there are 25 TCP traffic flows in the system. All mesh clients are fixed.

5.3.2. Simulation Results and Discussion

In Figure 5-6 and Figure 5-7 shows, OSPF has higher system throughput and more stability than the other routing protocols. As previously discussed, when the active timeout of the routing path happens, AODV needs to flood the RREQ to build the routing path, so it's less stable and has poor performance than OSPF routing protocol.

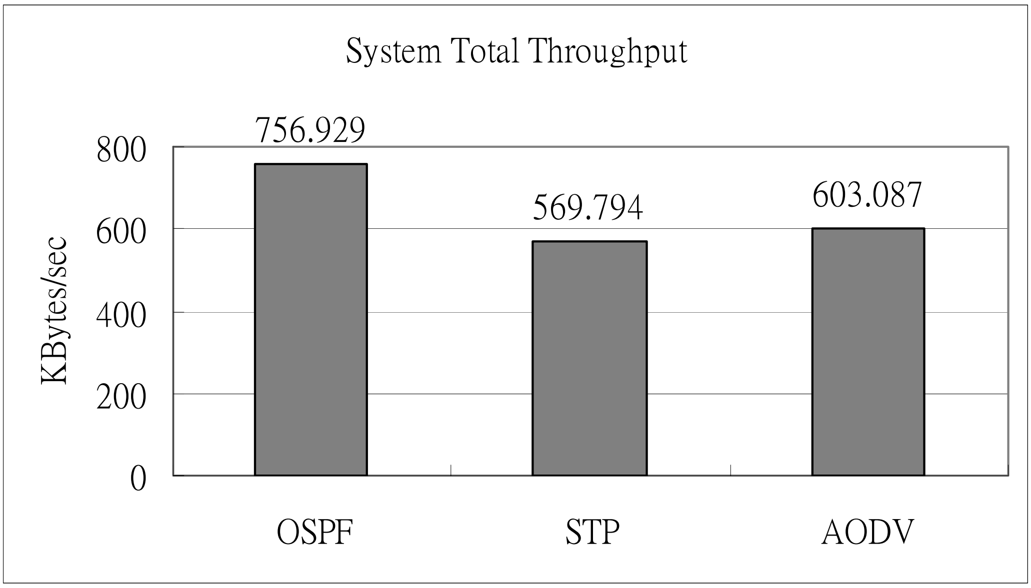

Figure 5-6 System total throughput of multi-to-multi clients TCP traffic

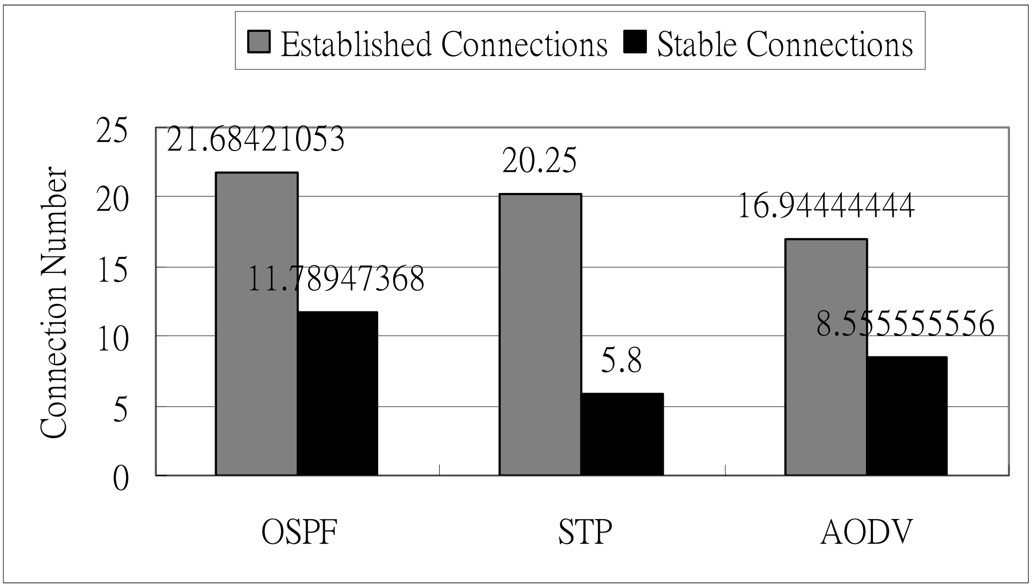

Figure 5-7 Connection number of multi-to-multi clients TCP traffic

As building the routing path, OSPF always use the shortest path to forward packet, but STP sometimes needs to route packets through the root access point and can’t use the shortest path. Because the routing path of STP is not always the shortest path, STP may use more hop counts to forwards packet than OSPF. In our simulation, STP needs 3.99 hop counts on average, but OSPF just only needs 3.45 hop counts on average.

5.4. Performance evaluation of Mobility Conditions

5.4.1. Topology

In the scenario, we simulate the wireless mesh network in mobility conditions. All configurations are the same as the downlink TCP traffic scenario, excluding that all mesh clients move randomly at 1 m/sec speed.

5.4.2. Simulation Results and Discussion

Figure 5-8 shows the system total throughput of the tree routing protocols. We can observe they have almost the same performance. But if we check the stability of the tree routing protocols which show in Figure 5-9, we can find that the mesh clients in AODV routing protocol can't have stable connection. When the mesh clients change active access point, the access points in the routing path will wait for routing path timeout and broadcast the RREQ to build a new routing path. However, In OSPF routing protocol, when the new access point get the association packet from the mesh client, it'll broadcast a LSA to inform the other access points. Then the access points will know the new position of the mesh client. STP has similar method to help mobility. When a STP access point get association packet, it can broadcast a packet to inform the access points at upper levels.

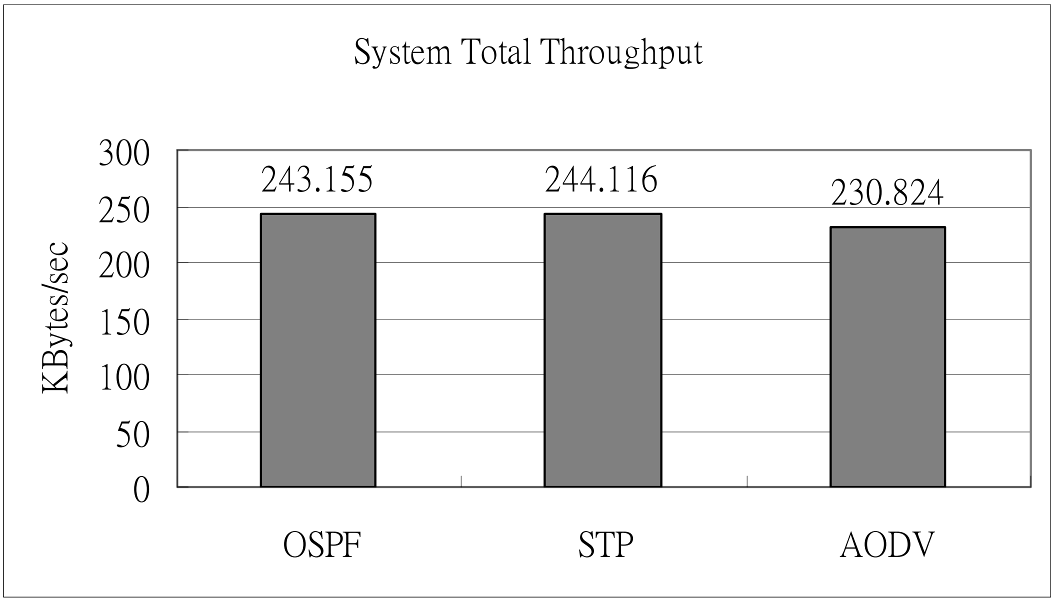

Figure 5-8 System total throughput of mobility conditions

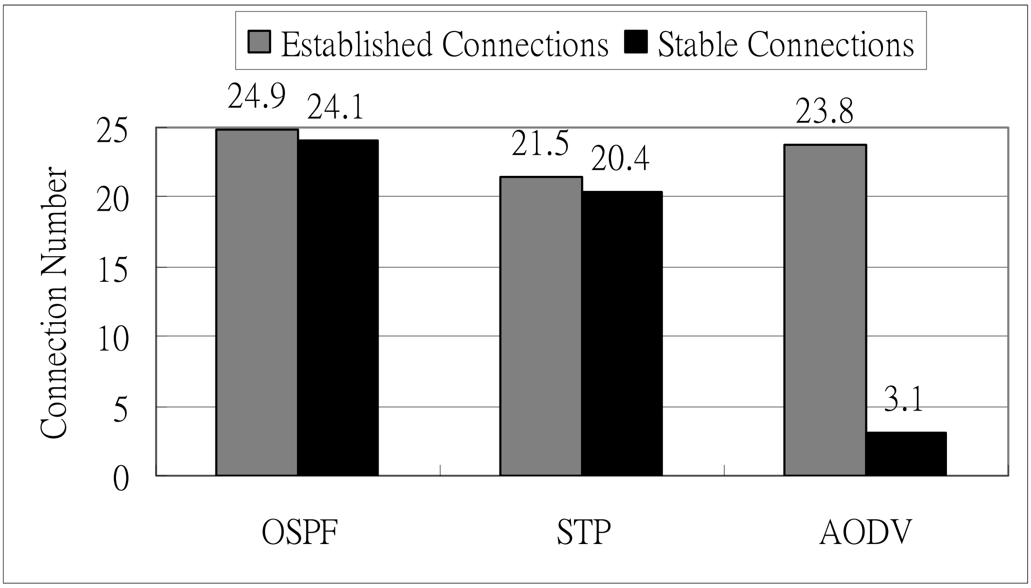

Figure 5-9 Connection number of mobility conditions

The stability of OSPF is still a little better than STP. It is because STP must wait for all of the access points which need to update the routing information getting the broadcast packet. Then it can forward packets correctly. As Figure 5-10 mobility condition in STP shows, when the mesh client move to the new access point, it will broadcast a packet to inform the upper level access points, and then the access points can route packets to the new access point.

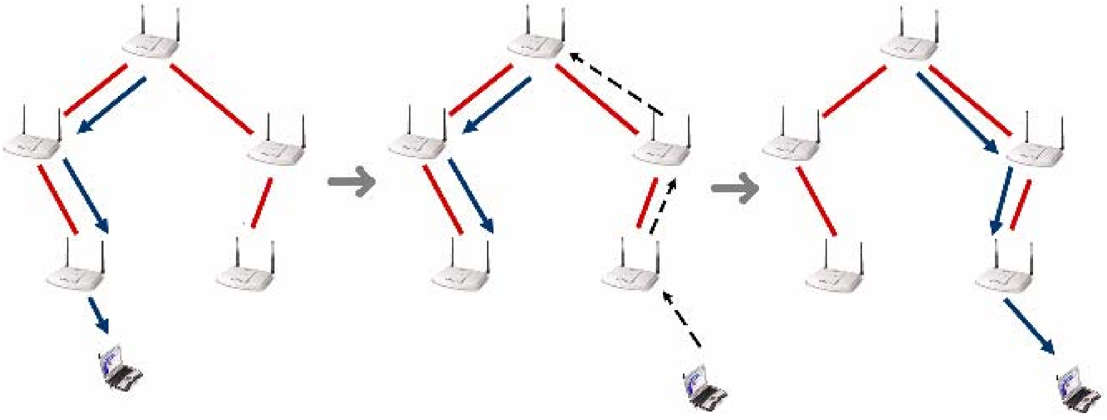

Figure 5-10 mobility condition in STP

However, OSPF can react more quickly in mobility condition. As Figure 5-11 mobility condition in OSPF shows, when the original access point get the LSA, it can help to route packets to the new access point immediately.

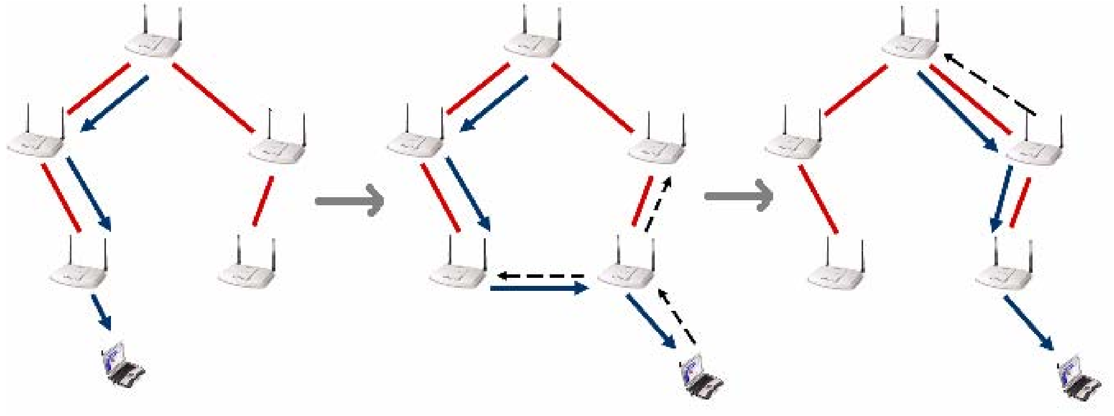

Figure 5-11 mobility condition in OSPF

5.5. Performance evaluation of Multi-Gateway Configurations

5.5.1. Topology

With the simulations above, we can conclude that OSPF is more suitable for wireless mesh networks. It can always use the shortest path to route packets to reduce the waste of the bandwidth in the multi-hop networks. It can react quickly in the mobility conditions. However, the low performance of wireless mesh networks is still a big problem. We implement the multi-gateway support on OSPF routing protocol and simulate the performance to compare to the original system. In the scenario of multi-gateway simulation, configurations are almost the same as the downlink TCP traffic scenario. But one interface of the gateway connects to the top right mesh access point and the other interface connects to the bottom left mesh access point. Figure 5-12 shows the topology of the multi-gateway.

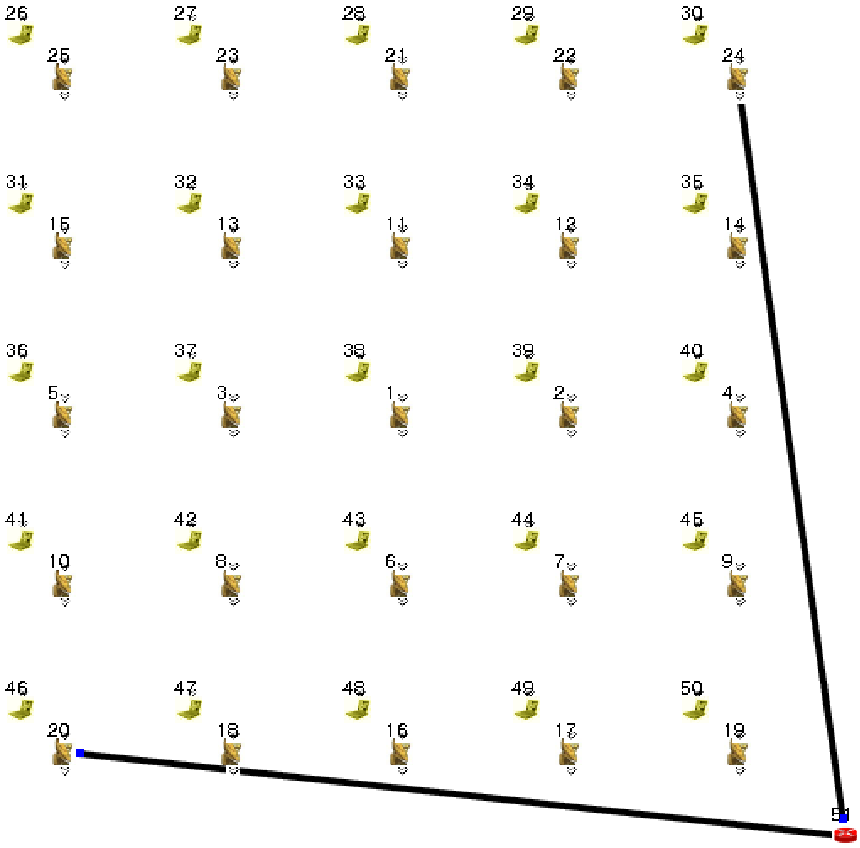

Figure 5-12 Simulation topology of multi-gateway

5.5.2. Simulation Results and Discussion

As Figure 5-13 shows, the multi-gateway can improve the performance a lot. By using multi-gateway, the interference of mesh access points can decrease. Originally, the bandwidth of the access point connect to the gateway is the bottleneck of the system performance. In the multi-gateway system, the bottleneck can be alleviated.

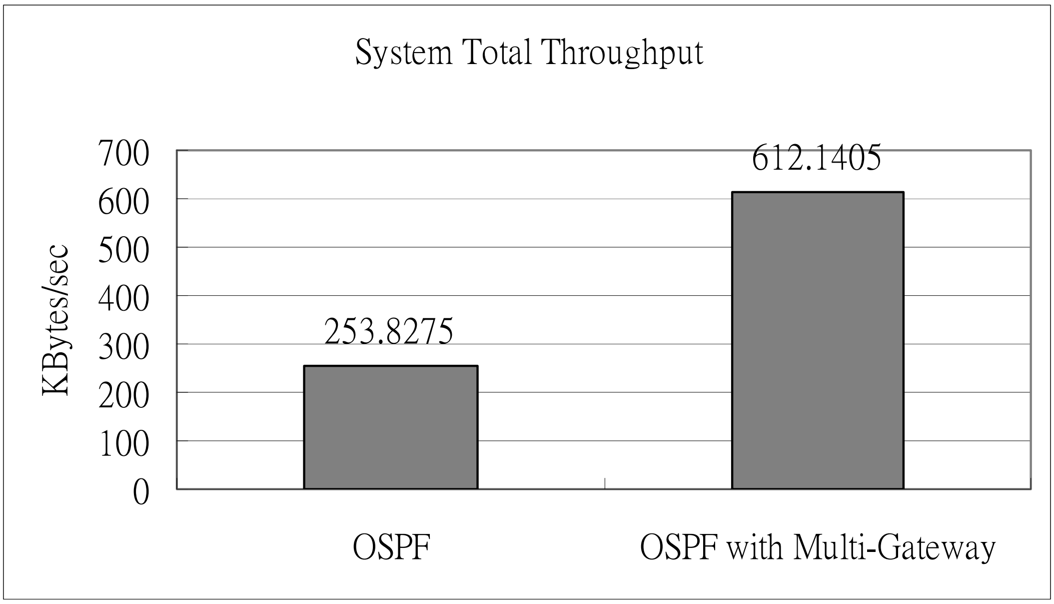

Figure 5-13 System total throughput of multi-gateway

In the simulation cases, the mesh clients are placed randomly. We analyze the 20 cases and find that the distribution of the mesh clients of two access points connected to the gateway is 12:13. But the actual distribution is 9.05:15.45. Although OSPF routing protocol should choose the shortest path randomly, the programming style will cause that OSPF routing protocol chooses some specific routing path frequently. We can conclude that the multi-gateway isn't absolutely fair. Even so, it still can ease off the loading of the access point connecting to the gateway significantly.

5.6. More realistic wireless channel simulation

5.6.1. Topology

The traditional Wphy module in NCTUns is very simple. It assumes that if the transmission range is less than 250m, the BER is 0 percent. There is another more realistic module in the NCTUns, called Awphy. It can simulate the propagation loss and the real BER in real world. We replace the Wphy module of the ad hoc link in the downlink TCP traffic scenario with the Awphy module and reproduce the simulation results. Then we do the simulation with the MeshOSPF with ETX again to compare to the original OSPF routing protocol.

5.6.2. Simulation Results and Discussion

As Figure 5-14 and

Figure 5-15 show, OSPF with ETX has less system total throughput, but it has more stability than original OSPF. Because the ETX metric can help OSPF routing protocol to choose a high throughput routing path for a single connection, connections with high hop counts in OSPF with ETX are more stable than in original OSPF. In original OSPF, theses connections may be dead after it has been established and the connections with less hop counts can get more bandwidth. Therefore, the system total throughput of the original OSPF can archive higher than OSPF with ETX, but OSPF with ETX can provide better service to the wireless mesh network.

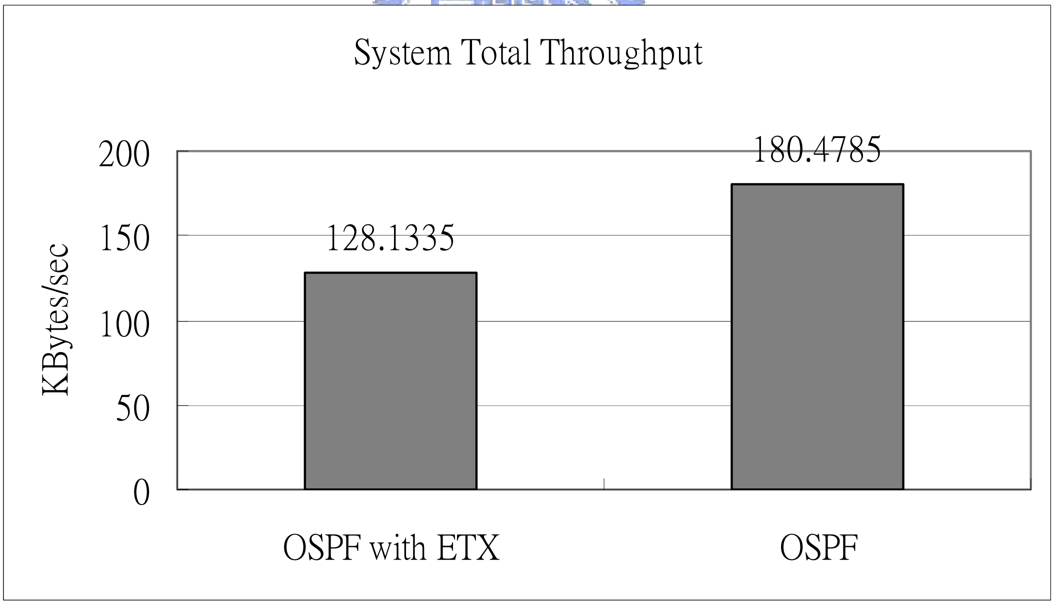

Figure 5-14 System total throughput of OSPF with ETX

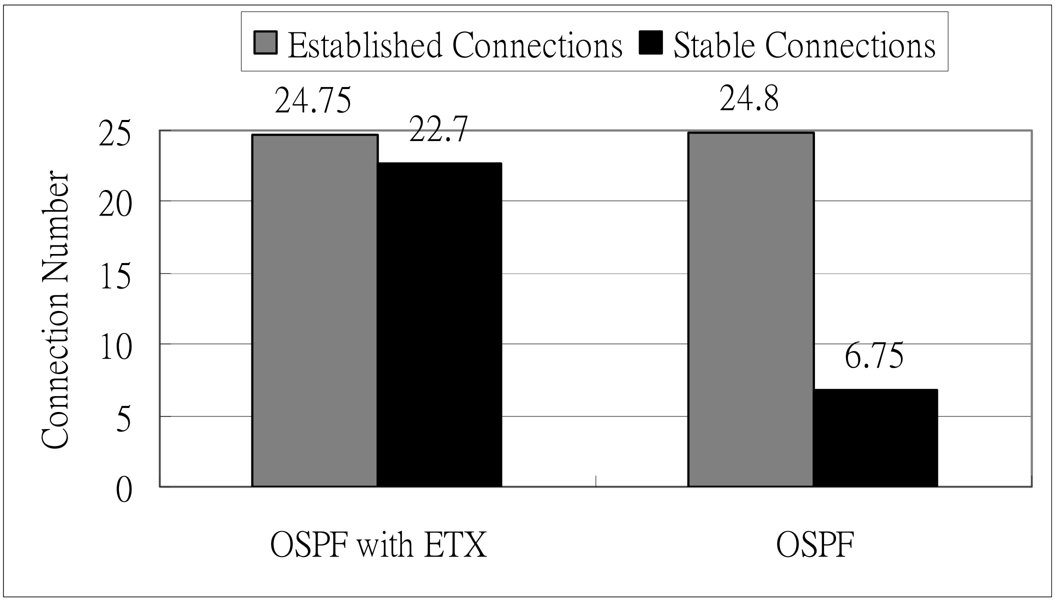

Figure 5-15 Connection number of OSPF with ETX

6. Future Work

In previous sections, we compare several routing protocols and show that the OSPF routing protocol with ETX and our proposed multi-gateway architecture is a better solution for constructing a wireless mesh network so far. In this chapter, we list several valuable and interesting tasks that are worthy to do in the future.

◆ **Port OSPF with ETX to linux**

When implementing the MeshOSPF module, we have to consider the portability issue. We divided the implementation of the MeshOSPF into two parts: the meshlib library and the MeshOSPF module.

The meshlib library has most functionalities of the OSPF routing protocol. These functionalities have been implemented as several functions, e.g., ospf_init(), ospf_helo(), ospf_flood_lsa(), ospf_build_tree(). We implemented these functions in C programming language without using any additional libraries or system calls. In NCTUns, these functions are implemented using the function calls provided by the simulation engine and the patched kernel. Therefore, when we want to port the meshlib library to a real Linux system, we need to replace the functions using the network system calls provided by NCTUns by using the standardized send() system call.

Because most of the functionalities of OSPF with ETX are implemented in the meshlib library, the MeshOSPF module is relatively simple. In the future, we can implement MeshOSPF functionalities on top of the meshlib library, which only requires several minor modifications for the Linux operating system.

◆ **Add the load-balancing support in MeshARP**

Our MeshARP module implements a simple load-balancing algorithm. It takes the input port of the first coming ARP request from a mesh client as the port to which a mesh client should connect. As described in section 5.5.2 , this load-balancing algorithm is not fair for all mesh clients. It is worthy to develop a more complex algorithm to support load-balancing with fair sharing of channel resources among mesh clients.

- **Enhance the security of the wireless mesh network**

Wireless mesh routing protocols usually assume that they works in non-hostile environments. Due to dynamically changing topology in a mobile network, a wireless mesh network usually has a decentralized architecture for security issue. It is still vulnerable with respect to the secure communications. Therefore, enhancing the security for the wireless mesh network is necessary and valuable.

- **Measure the performances of OSPF with ETX in real world**

In this paper, we have implemented OSPF with ETX and measured the performances with the simulation method. However, it still needs measurements in the field trials to evaluate the performances of OSPF with ETX in the real world.

7. Conclusion

Nowadays wireless LAN mesh networks use IEEE 802.11a/b/g networks as their underlying interconnection networks for access points. In the future it is very possible that the wireless mesh network starts to use other wireless radio technologies, such as UltraWideband, WiMAX, cellular, Bluetooth, and 802.15.4 Zigbee, as the underlying network. For example, the IEEE 802.16(WiMAX) is proposed to widen the coverage of the wireless services and provide more bandwidth. Wireless mesh routing can be used in wireless LANs to provide users with Internet accesses and communications among several heterogeneous networks. It can provide self-organization, self-configuration, and self-healing functions to reduce the costs and complexity of network deployment and maintenance.

WMR affects the scalability and the performances of the wireless mesh network a lot. Although some companies already have commercial wireless mesh network products for sale, results of field trials and experiments with existing wireless mesh networks show that the performances of routing protocols used by these wireless mesh networks are still far below what they expect to be. Therefore, we used the NCTUns network simulator to evaluate these routing protocols. From our simulation results, we found that OSPF is the most suitable protocol for wireless mesh networks. However, it still has the problem of limited scalability. In addition, OSPF cannot work well in the real world if it simply uses hop counts as the only metric for computing routing path. For this reason, we proposed a multi-gateway architecture to enlarge the network scale for our proposed mesh network system. Furthermore, we added the ETX metric into the shortest path first algorithm used by the OSPF routing protocol. Finally, we show that the performances of the wireless mesh work can be further improved with the above enhancements. OSPF with ETX and multi-gateway can be suitable for wireless mesh networks in the real world.

8. References

[1] J. Moy, “OSPF Version 2”, IETF RTC 2328, April 1998, http://rtg.ietf.org/rfc/rfc2328.txt

[2] IEEE 802.1D Standard Group Web Site. Available from: <http://www.ieee802.org/1/pages/802.1D.html >

[3] David B. Johnson, David A. Maltz, and Yih-Chun Hu. “The Dynamic Source Routing protocol for mobile ad hoc networks (DSR)”. Internet draft (work in progress), IETF, April 2003. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt.

[4] Charles E. Perkins and Pravin Bhagwat. “Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers.” In *Proc. ACM SIGCOMM Conference(SIGCOMM ’94)*, pages 234–244, August 1993.

[5] C. Perkins, E. Belding-Royer, S. Das, “Ad hoc on-demand distance vector (AODV) routing”. IETF RFC 3561, July 2003.

[6] G. Malkin, ”RIP Version 2”, IETF RTC 2453, November 1998, http://rtg.ietf.org/rfc/rfc2453.txt

[7] D. Jhonson and D.Maltz, “Dynamic Source Routing in Adhoc Wireless Networks”, Internet Draft, Dec. 1998.

[8] E.M. Royer and C-K Toh, “A Review of Current routing protocols for Ad-hoc mobile wireless networks”, IEEE Personal Communications, April 1999.

[9] D. Aguayo, J. Bicket, S. Biswas, D.S.J. De Couto, R.Morris, MIT Roofnet Implementation. Available from:<http://pdos.lcs.mit.edu/roofnet/design/>.

[10] BWN lab wireless mesh networks research project.Available from: <http://www.ece.gatech.edu/research/labs/bwn/mesh/>.

[11] J. Hauser, Draft PAR for IEEE 802.11 ESS Mesh, IEEEDocument Number: IEEE 802.11-03/759r2.

[12] IEEE 802.11 Standard Group Web Site. Available from: <http://www.ieee802.org/11/>.

[13] IEEE 802.16 Standard Group Web Site. Available from: <http://www.ieee802.org/16/>.

[14] Kiyon Autonomous Networks. Available from: <http://www.kiyon.com>.

[15] Microsoft Mesh Networks. Available from: <http://research.microsoft.com/mesh/>.

[16] Nortel Mesh Networks. Available from: <http://www.nortelnetworks.com/solutions/wrlsmesh/index.html>.

[17] Ian F. Akyildiz, Xudong Wang, and Weilin Wang. Wireless mesh networks: a survey. Computer Networks Journal (Elsevier), March 2005.

[18] Daniel Aguayo, John Bicket, Sanjit Biswas, Glenn Judd, Robert Morris, “Link-level Measurements from an 802.11b Mesh Network”, SIGCOMM 2004, Aug 2004

[19] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris, “A High-Throughput Path Metric for Multi-Hop Wireless Routing”, Proceedings of the 9th ACM International Conference on Mobile Computing and Networking (MobiCom ‘03), San Diego, California, September 2003.

[20] MeshDynamics structure Mesh. Available from:

<http://www.meshdynamics.com/>

[21] The LocustWorld Mesh, Available from: <http://www.locustworld.com/>