A FORWARDING CACHE VLAN PROTOCOL (FCVP) IN WIRELESS NETWORKS

Tzu-Chiang Chiang[1,3], Ching-Hung Yeh[1], Yueh-Min Huang[1] and Fenglien Lee[2]
Department of Engineering Science, National Cheng-Kung University, Taiwan, ROC[1]
National Center for High-Performance Computing Taiwan, ROC[2]
Department of Information Management, Hsing-Kuo University, Taiwan, ROC[3]

ABSTRACT

The Virtual Local Area Network (VLAN) technology is one of the hottest areas of networking systems. A VLAN is a logical connection rather than physical that allows network devices to be combined as "virtual LANs". The VLAN technology functions by logically segmenting the network into different broadcast domains so that packets can only delivered between ports with the same VLAN identity (group member). By using this characteristic of VLAN there is a very flexible mechanism to group the physical ports together. Wireless networks also need the flexibility to collect more than two devices equipped with wireless communication and networking capability. In recent years, wireless network has been attracting a lot of attention due to wireless devices have enjoyed a tremendous rise in popularity. In order to communicate among some groups of wireless devices without the convention concept of clusters we propose a novel model to form the multiple-domain or the multiple-group as "virtual LANs" according to the logical connection in ad hoc networks. In this paper we also propose a novel forwarding cache VLAN protocol (FCVP) for ad hoc networks to simulate the behavior of VLAN in ad hoc network. For our purpose, each node in ad hoc networks records the nodes of the same VLAN identity in a cache table to keep the information of the VLAN identification for forwarding the packets. We simulate the proposed protocol in ad hoc network environment between 50 and 80 nodes with different size of VLANs groups. The result shows that the throughput of our protocol delivering packets to all nodes in the same VLAN group is more than 84% of the case. Furthermore, we compared to the flooding, the efficiency of communication improves up to 68% on our FCVP.

KEYWORDS: Virtual Local Area Network, wireless networks, ad hoc networks, multiple-group.

This research is supported by NICI IPv6 Infrastructure Development Division, Taiwan (Grant #I-0400).

1. Introduction

In recently years, almost every industry and every type of application, data is tremendous changed presentation through images, videos rather than text. A few of the applications are absorbing greater amounts of bandwidth. Therefore today's corporations routinely buy the fastest computers on the market and want those machines to run on the fastest safest network possible [1][2][3]. The network switch was invented to assist networks to accomplish these precise properties. The LAN switch network permits users to be combined into as "Virtual LANs." A VLAN is a logical, rather than a physical, collection of network devices. In the router-based network devices are recognized by their physical location in the network. This is indicated in a network-layer address, which inform the router physical segment where must send data to. A VLAN acts like an ordinary LAN, but connected devices don't have to be physically connected to the same segment. The VLAN allows a flexible mechanism, simply grouping physical ports together, or can combine existing hubs, routers and FDDI backbone with dedicated switched ports, wide area networks, and more. While clients and servers may be located anywhere on a network, they are grouped together by VLAN technology, and broadcasts are sent to devices within the VLAN.

An ad hoc wireless network [4] represents a system of wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary network topology; each node relies on its neighbors to forward packets to destinations not directly in its transmission range. I.e. The mobile modes equipped with wireless communication and networking capability can collect to form an ad hoc wireless network temporarily. Such nodes can communicate with another node that is immediately within their radio range or one that is outside their radio range. A communication occurs when two or more devices (but not all nodes in an ad hoc network) are communicating among themselves and they are composed in a group. Many communications occurs in same ad hoc network meaning that many groups propagate packets simultaneously. By the broadcasting protocol, these packets will be received in all groups (nodes) even they do not require them. However these processes involve broadcasting over the wireless network, which results in wasteful bandwidth and an increase in overall network control traffic. So an ad hoc wireless network needs to be parted into multiple-domain or multiple-group as “virtual LANs” to reduce redundant transmission and ensure reasonable performance. In this paper we propose a forwarding cache VLAN protocol. By employing forwarding cache table in each node progress a VLAN mechanism to improve the performance for multiple-group communication in ad hoc networks.

The rest of the paper is organized as follows. We describe the Virtual Local Area Network in Section 2. Section 3 in detail for forwarding cache VLAN protocol, Section 4 compares the efficiency to original broadcast. Finally, section 5 provides our concluding remarks and future works.

2. Virtual Local Area Network

In a local area network, data link-layer broadcast and multicast traffic is delivered to all devices, but this traffic cannot go beyond the LAN boundary. In the past, shared cabling or hubs were the boundaries for LANs. A VLAN is an administratively configured LAN or broadcast domain. VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of moves, adds, and changes in members of these groups [5]. VLANs configured by using Media Access Control addresses can recognize when a device has been moved to another port on a switch. VLAN management software can then automatically reconfigure that device into its appropriate VLAN without the need to change the device's MAC or IP address. Traffic between VLANs is restricted. Bridges forward unicast, multicast and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs. So the packets are only switched between ports that are designated for the same VLAN. By confining packet broadcast on a particular LAN only to the LANs within the same VLAN, switched virtual network avoid wasting bandwidth, a fault in traditional switched network where packets are often forwarded to LANs that even do not require them. Hence offers benefits in term efficiency use of bandwidth, flexibility, performance and security.

The IEEE 802.1Q [5] standard defines the operation of VLAN Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure. The IEEE's 802.1Q standard was developed to address the problem of how to break large networks into smaller parts so broadcast and multicast traffic would not grab more bandwidth than necessary. The mechanisms support VLAN in Bridged LAN environment including the frame format and how the frames are relayed to destinations. Any frame has a VLAN-tagged to associate with the incoming port’s VID (VLAN ID). The Filtering Database (FDB) stored addressing information and frame-filtering information in the form of Mac addresses and VLAN entries.

Switches are one of the core components of VLAN communication. Switches provide the intelligence to make filtering and forwarding decisions by packet and to communicate to other switches and routers within the network. 802.1Q-compliant switch ports can be configured to transmit tagged or untagged frames. The switch implementing the standard is as following typical operations:

First, when a frame enters the switch it is checked for errors. An error-free frame will be associated with a VID as described above so that frame’s learning and forwarding is relative to the VLAN it belongs to. If the Ingress Filtering set to enable and the incoming port is not a member of this VALN, the frame will be rejected.

Second, an accepted frame will be submitted to the forwarding process to be relayed to other ports, and at the same time the switch observes its source MAC address, source port, VID associated and other necessary addressing information and automatic using them to update the FDB. The process of forwarding uses the MAC address and VID of the frame to index into the FDB to find out where the frame shall be relayed. And eventually the frame is sent through those corresponding outbound ports if not filtered out by Egress Filter, which also decide whether the outgoing frame should carry a VID. The logical interrelationships are illustrated in Figure 1.

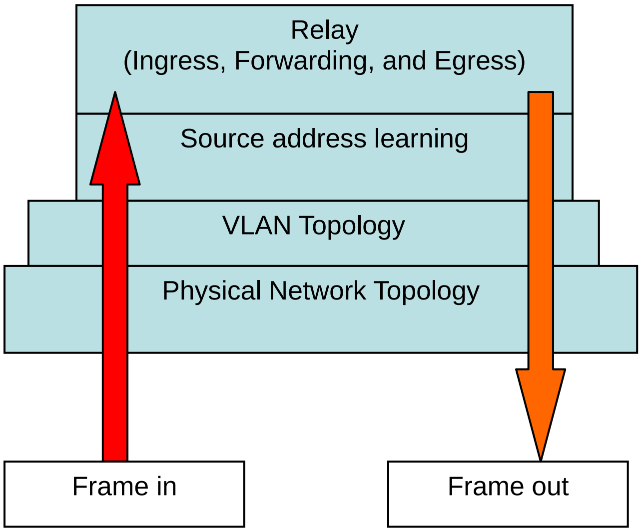

Fig 1: The VALN logical interrelationships

It is obvious that LANs switches afford essential improvement in performance and dedicated bandwidth across the networks, with the intelligence necessary for VLAN segmentation.

3. Forwarding Cache VLAN Protocol (FCVP) in Ad Hoc Networks

A wireless ad hoc network has no fix infrastructure available, so no fixed device can serve as LAN's switch. Hence we propose forwarding cache VLAN protocol which utilizes forwarding cache table to progress a VLAN mechanism and improves the performance for VLAN communication in ad hoc networks. In FCVP we have three basic elements to server as fundamentals.

First, packet header should include VID to identify which VLAN it belongs to. If the VID is null then the packet is a normal packet.

Second, each node has a cache table functioning as filter to store the VID which can forward.

Third, each node stores a VID into cache table through a cache request (CREQ) packet to obtain the VID.

The fields in the forwarding cache table show in the table 1. The table 2 presents the CREQ format. The field of packet type used to differentiate from data packet.

Table index	VID field

Table 1: forwarding cache table

Packet type	VID field

Table 2:CREQ format

According the three elements, FCVP can be achieved by the following four phase:

Initiating phase:

VLAN can be freely formed in the network topology. The nodes of the same VLAN identify each other and decide VID using a protocol such as flooding. As the same time, VLAN's nodes exchange routing information to find the minimum hop nodes that can reach all members. Then send the CREQ to these hop nodes.

Maintaining phase:

Each VLAN's nodes broadcast a CREQ to neighboring nodes in a period time. Each node deletes the VID from the cache table when neither received the CREQ nor forward packet that belongs to the VID in a period time. The objective is to ensure that cache table is up-to-date. When nodes keep moving away original position and exceed the radio range, the original neighboring nodes do not need to forward packet, so deletes the VID from the cache table and newly neighboring nodes need to be recorded the VID into their cache table.

Transmission phase:

Every node can initial a communication (such as a source node) to the VLAN it belongs to. When node received packet, three results will be process, by the following algorithm:

Begin
  If the packet never received before **then**
  / each node checks packet sequence number to avoid forwarding loop. */*
    If the VID in the receiving packet = the VID of receiving node **then**
      {Accept and forward the packet;
       Reply ACK packet to the source node
      }
    Else-if VID in the receiving packet exist in the cache table of receiving node **then**
        Forward the packet
      Else
  */*VID in the receiving packet not exist in the cache table of receiving node */*
        Drop the packet
      End-if
    End-if
  End-if
End

The algorithm can be simplified by the flow chart as figure 2:

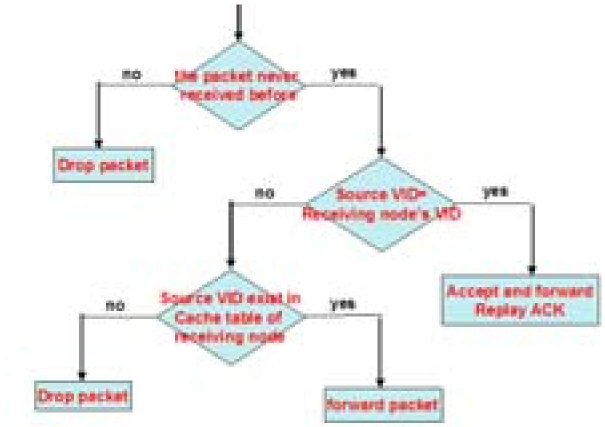

Fig 2: The decision flow chart

Re-routing phase:

Source node checks with ACK packet. If anyone node of the VLAN did not replay the ACK packet, then the node lost hop nodes. The source node initiates "router discovery" using a uni-cast algorithm such as AODV [6] or DSR [7] to find the routing path. Then resend the packet to the un-received node and send CREQ to the hop nodes in the path.

As an example, Fig 3 shows the network topology graph. After initiating phase, there are three VLAN red, blue and black. The node color present which VLAN it belong to. The red VLAN has 5 nodes, blue VLAN has 5 nodes, and black VLAN has 6 nodes. In the red VLAN, the blue node 5, 3, 1 and black node 6 are the hop nodes to reach each red member and store VID "*red*" in their cache table. The forwarding cache table of blue node 3 stores the VID "*red*" and "black" as the table 3.

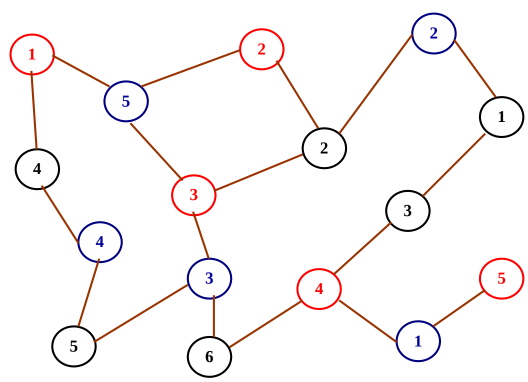

Fig 3: Three VLAN network topologies

Table 3: forwarding cache table of blue node 3

Table index	VID field
1	red
2	black

When the red node 5 moves toward the black node 1, by CREQ broadcast the black node 1 and 3 store VID "*red*" in their cache table. This let red node 5 still reachable in red VLAN. Fig 4 shows the network topology graph.

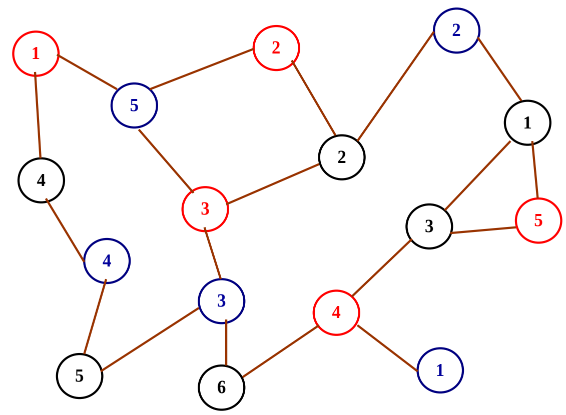

Fig 4: The network topology after red node 5 moving

Assume red node 1 initiates a communication to red VLAN and the black node 3 does not work, then the red node 5 will be unreachable and will not reply ACK to red node 1. After the ACK inspection, red node 1 initiates "router discovery" and find the either path representation with green line in Fig 5. Then the blue node 2 finally will store VID "*red*" in cache table, becomes forwarding node of red VLAN.

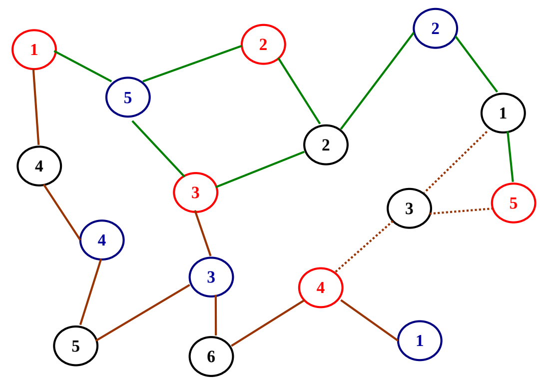

Fig 5: The block node 3 does not work

According above description, the other VLANs will do the same behavior. Therefore, FCVP utilizes the forwarding cache table to reduce redundant transmissions by efficiently inspecting the status of received packet of each node before the relaying process. FCVP can very efficiently forwarding packet when the VID in the cache table. The other nodes will reject the packet and reduce the overhead in the network. As a consequence, the FCVP incurs very little overhead with propagation of the packet and reduce resource consumption with each hop of the VLAN.

4. Compare to Flooding With FCVP Using Computer Simulation

We compare the efficiency of the processed FCVP methods to Flooding using computer simulation. Networks are randomly generated within 600m x 600m grid. There are n nodes in the grid with k VLANs and nodes can communicate each other within transmission range. Each VLAN is formed with randomly members. The re-routing adapts the AODV algorithm. In the simulation study, we turn n and k to compare how the network sizes and VLAN sizes affect the efficiency.

Figure 6 shows similar results for network sizes from 50 nodes to 80 nodes with 5 to 8 VLANs. As a consequence of the greater node density, the FCVP is sufficient to deliver packets to all nodes in a VLAN group. There are some nodes moving out of transmission range which can not re-route successfully. It shows that the percentage up to 84% in the 80 nodes existing 8 VLANs by the FCVP. In the same condition, original flooding achieves only 80%. The main impact of the improvement is that FCVP re-routes successfully before nodes moving out of transmission range, original flooding has too many redundant transmissions (control packet flood) to reach destination in time.

Similar results for the percentage of the overhead of FCVP and original flooding in Fig. 7. We assign the flooding overhead to be 100% for comparing basis. It shows that the overhead of FCVP in 5 VLANs is from 50% to 39% when nodes number from 50 nodes to 80 nodes. And the overhead of FCVP in 8 VLANs is from 39% to 32% when nodes number from 50 nodes to 80 nodes. It give a clear result that the overhead improves up to 68% in the 80 nodes existing 8 VLANs. Furthermore, compared to different sizes of VLAN, FCVP was still efficient when the sizes of VLAN changing.

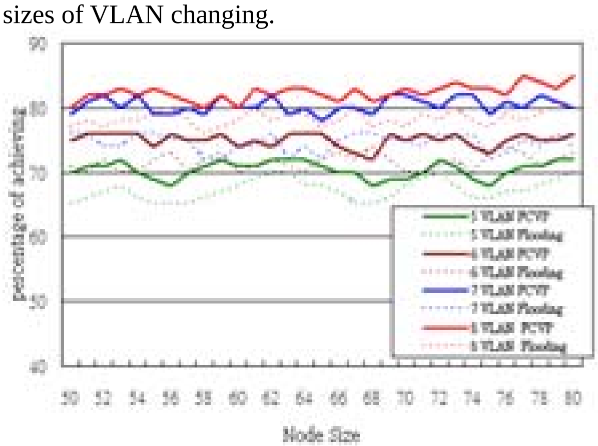

Fig 6: the percentage of successful deliver packets

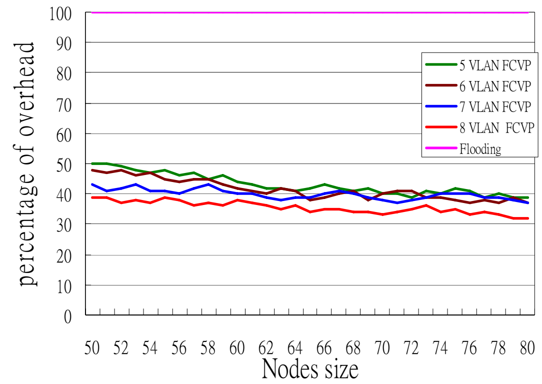

Fig 7: The percentage of the overhead of FCVP and original flooding

The results present in this session quantify the improvement in FCVP that results from the use forwarding cache table to reduce redundant transmissions. However, if the network increases greater nodes density, the improvement increases more obviously.

5. Conclusions and Future Research

In this paper, we have described the forwarding cache VLAN protocol (FCVP) for ad hoc networks. The main objective of our protocol is efficient to progress the behavior of VLAN in ad hoc networks. By the forwarding cache table likes the Filtering Database (FDB) to make filtering and forwarding decisions, the re-routing mechanism prevent hop nodes un-working. Since the forwarding decision are computed locally, no complex distributed data structure needs to be recomputed during the transmitting process. FCVP can improve the performance for behavior of VLAN in ad hoc network.

Simulation results show that our protocol is more efficient than original flooding. The network with greater nodes density is more properly to adopt FCVP.

We plan to identify the suitable cache table refreshing mechanism on the proposed FCVP method in the future works. We will also generalize the clustering method to progress the behavior of VLAN so that they can be applied in ad hoc wireless networks.

References

[1] Rajaravivarma, V.; “Virtual local area network technology and applications,” Proceeding of the Twenty-Ninth Southeastern Symposium on , 9-11 March 1997 Pages:49 - 52

[2] N. Kavak, “Data Communications in ATM Networks,” *IEEE Network*, vol.9, no.3,May/June 1995.

[3] A. Gupta and D. Ferrari, “Resource Partitioning for Real-time Communication,” *IEEE/ACM Trans. on* Networking,Vol. 3, No. 5, Oct 1995, pp. 501–518.

[4] J. Jubin and J.D. Tornow, “The DARPA Packet Radio Network Protocols,” Proceeding of the IEEE, Vol.75, no. 1, Jan. a987, pp. 21-32.
[4] J. Jubin and J.D. Tornow, “The DARPA Packet Radio Network Protocols,” Proceeding of the IEEE, Vol.75, no. 1, Jan. a987, pp. 21-32.
[5] IEEE Std 802.1Q, 2003 Edition. IEEE standards for local and metropolitan area networks. Virtual bridged local area networks.

[6] C. E. Perkins and E. M. Royer. Ad-hoc On-Demand Distance Vector Routing. In *The Second IEEE workshop on Mobile Computing System and applications*, New Orleans, LA, USA, Feb. 1999.

[7] J. Broch and D. B. Johnson. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. IETF Internet Draft, October 1999.

[8] Yueh-Min Huang and Tzu-Chiang Chiang ,“A Sequence and Topology encoding for Multicast Protocol (STMP) in wireless Ad Hoc Networks”, The Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, China,(PDCAT'03), 8/2003.