Non-root-based Hybrid Wireless Mesh Protocol for Wireless Mesh Networks

Madhusudan Singh[1], Song-Gon Lee[2*] and HoonJae Lee[2]

[1]*Samsung Mobile Display, Korea*
[2]*Department of Ubiquitous IT, Division of Computer & Information Engineering, Dongseo University, Busan- 617-716, Korea*
sonu.dsu@gmail.com, nok60@dongseo.ac.kr, hjlee@gdsu.dongseo.ac.kr
[*]*Corresponding Author*

Abstract

Wireless mesh networks (WMNs) are wireless networks that are composed of mesh routers and mesh clients. Mesh routers have minimal mobility and form the backbone of WMNs. IEEE 802.11s-based WMNs have a default routing protocol, namely, a hybrid wireless mesh protocol (HWMP). In tree-based proactive mode, HWMP is completely centralized and constrained by the root node, which causes a bottleneck at the root node. In reactive mode, HWMP always initiates path discovery message broadcasting, which uses unnecessary power resources. In this paper, we propose a new routing protocol for WMNs based on HWMP. This protocol, which we refer to as the decentralized hybrid wireless mesh protocol (DHWMP), provides a different root for different transmissions. We also perform simulations to compare the performance of the proposed scheme with existing routing protocols, including HWMP, ad hoc on-demand distance vector (AODV) routing, and optimized link state routing (OLSR).

Keywords: *IEEE802.11s, HWMP, AODV, OLSR, Performance analysis*

1. Introduction

Wireless mesh networks (WMNs) combine the advantages of wireless connections and a mesh topology to provide better mobility, a lower cost of deployment, easier network expansion, and robust connections. WMNs extend the coverage of wireless local area network (WLAN) technology to other areas. However, the problem with the use of WMNs is the wired connection between the access points (APs). Wired links often increase the complexity and deployment cost of WLAN technology [1]. Therefore, it is desirable to connect the APs via wireless links and to create a WLAN mesh. WMNs can use different wireless technologies for the provision of backhaul multi-hop connectivity and an easy access link between mesh clients and mesh routers. For example, IEEE 802.11 [2], IEEE 802.15 [3], and IEEE 802.16 [4] are currently used for wireless connections.

WMNs are suitable for many applications, such as broadband home networking, enterprise networking, community networking, building automation systems, and health and medical systems [5-6]. There has been a substantial amount of research on WMNs [7~9].

The standard name for WLAN technology is IEEE 802.11, and the WMN standard for 802.11 is IEEE 802.11s [10]. IEEE 802.11s technology provides a cost-effective and simple method for wireless networking. In these WMNs, APs turn into mesh APs (MAPs). MAPs provide backhaul connection services for WMNs and access services for mobile station access. Mobile stations are sometimes referred to as mesh clients. The IEEE 802.11s standard draft introduces a third class of nodes called mesh points (MPs). MPs and MAPs forward

packets on behalf of other nodes to extend the wireless transmission range. Mesh clients can associate with MAPs but not with MPs. Mesh portals (MPPs) are MAPs that provide connectivity to other networks, thus acting as a gateway for mesh networks. Figure 1 shows an example of an IEEE 802.11s mesh network.

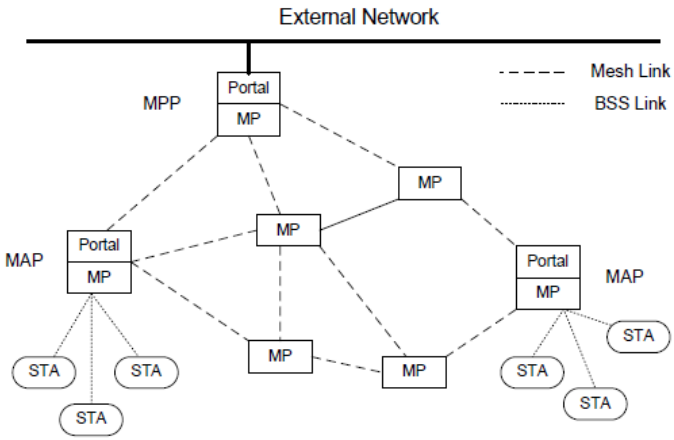


Figure 1. Example of an IEEE 802.11s WMN

In WMNs, routing protocols are classified as proactive, reactive, or hybrid [11]. As the name suggests, the proactive routing protocol maintains routes before a route is needed. This protocol attempts to maintain up-to-date information. A reactive protocol finds a route only when a node wants to communicate with another node. Hybrid routing protocols are a combination of the above two methods. Some routes to the destination are maintained proactively, while others are created on demand. Ad hoc on-demand distance vector (AODV) routing (RFC 3561) is a well-known reactive routing protocol for wireless ad hoc networks [12]. This protocol offers quick adaptation to dynamic link conditions, low processing overhead, and low memory overhead. Optimized link state routing (OLSR) is a proactive protocol that is based on table-driven techniques [13]. The proactive nature of the protocol allows it to maintain routes to all of the nodes in the networks by a frequent exchange of topology information with other nodes in the networks. OLSR adopts the multipoint relay (MPR) mechanism to reduce the routing overhead caused by the flooding of control information in the networks.

The default routing protocol for IEEE 802.11s-based WMNs is the hybrid wireless mesh protocol (HWMP) [10]. HWMP contains both reactive and proactive routing components. This protocol has adapted the AODV specifications as its reactive mode protocol, radio metric (RM)-AODV. While AODV works on layer 3 with Internet protocol (IP) addresses and uses the hop count as a routing metric, RM-AODV was redesigned to use media access control (MAC) addresses and a radio-aware path selection metric for path selection at the data link.

In the existing HWMP, the proactive tree-based routing has been completely centralized and constrained by the root node. HWMP still cannot support route optimization between two MPs [14]. The reactive routing (on-demand routing) protocol always initiates the path discovery process, which causes some broadcasting and wastage of power resources. In this paper, we introduce non-tree based root nodes in a proactive routing protocol and attempt to solve the difficulties in the reactive routing protocol.

This paper is structured as follows. Section 1 provides an introduction, and Section 2 provides an overview of HWMP. Section 3 specifies the proposed HWMP, and Section 4 presents the performance analysis. Section 5 concludes our proposal.

2. Overview of HWMP

IEEE 802.11s defined HWMP as a basic routing protocol for a WMN. It is a hybrid routing protocol that combines a reactive mode and a proactive mode. The protocol's reactive mode operation is based on AODV, and the proactive mode operation is based on tree-based routing. HWMP is located on layer 2; therefore, it uses MAC addresses instead of IP addresses for routing message communications. In addition, the term 'path selection' is used instead of 'routing' in layer 2 routing. The main purpose of the on-demand routing protocol is to support mesh points that work for mobility, while the proactive routing protocol supports the fixed nodes. The airtime metric is a default routing metric that is used to measure the link quality. In HWMP, on-demand routing and proactive routing can work simultaneously.

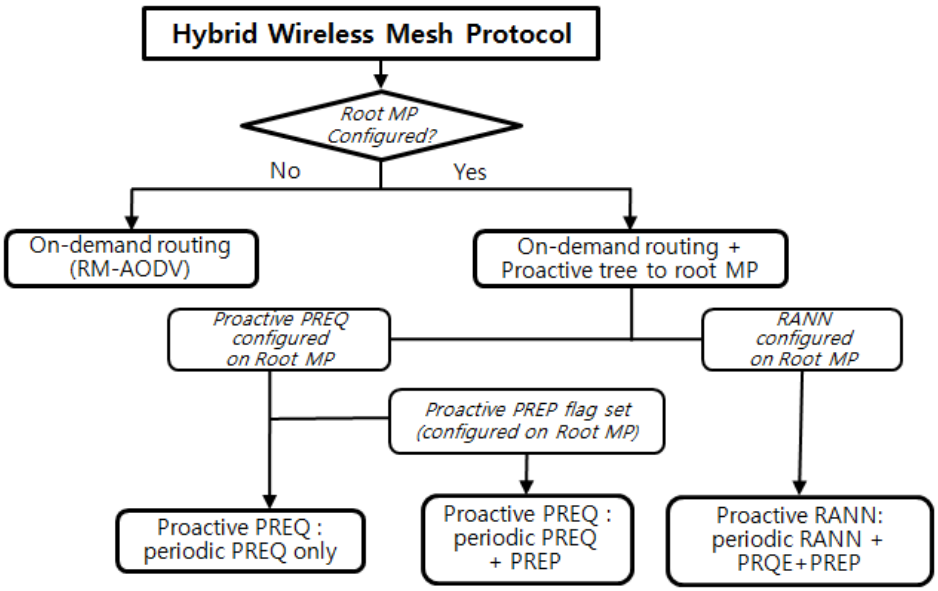


Figure 2. Configuration Cases for HWMP

Figure 2 shows the configuration cases for HWMP. If the root MP is not configured, then on-demand path setup is achieved by a path discovery mechanism, RM-AODV. If an MP needs a path to a destination, then it broadcasts a path request message (PREQ) into the mesh network. The intermediate MPs will rebroadcast the updated PREQ whenever the received PREQ corresponds to a newer or better path to the source. Similarly, the requested destination MP will respond with a path reply message (PREP) whenever a received PREQ corresponds to a newer or better path to the source. Intermediate MPs that already have a valid path to the requested destination can respond with a PREP.

HWMP sets up an MP as a root MP to build the proactive tree. Three different methods for proactive tree building in HWMP are shown in Figure 2. If an MP is configured to be a root MP and to use the proactive PREQ mechanism, then it will periodically broadcast a proactive PREQ with increasing sequence numbers. Any intermediate MPs that receive

a proactive PREQ will process it in a manner similar to the way in which a PREQ performs on-demand path discovery.

The proactive PREP flag in the PREQ controls whether the PREP is sent in response to a proactive PREQ. The setting of the flag is configured at the root MP. If the flag is not set, then no PREP is sent in response to the reception of a proactive PREQ. This situation is called the non-registration mode. In this mode, a path tree from all of the MPs to the announced root MP is established, but the MPs are not registered proactively at the root MP. If a source MP wants to have a bidirectional communication with the root MP, the source MP can send a gratuitous PREP before the first data frame to register its address with the root MP. The non-registration mode makes a lightweight creation and maintains the proactive paths to the root MP.

If the proactive PREP flag is set, then the MP must send the PREP in response to the reception of a proactive PREQ. This situation is called the registration mode. In this case, MPs register with the root MP by sending a PREP in response to the proactive PREQ.

If an MP is configured to be a root MP and to use the proactive root announcement (RANN) mechanism, then it will broadcast a RANN with an increasing sequence number periodically. The RANNs are only used to propagate path metrics to the root MP and to all of the MPs in the mesh network, but they will not create or update any paths in the routing table. If the MP must create or update a path to the root MP, then it will send a unicast PREQ to the root MP. The processing of the unicast PREQ and the response with a PREP are performed in a manner similar to that used to process a PREQ during on-demand path discovery. This method establishes a forwarding tree for each MP toward the root MP. Multiple root MPs can be configured in a mesh network that is running HWMP, which means that multiple proactive tree scan be built simultaneously by the different root MPs.

The hybrid routing event occurs when a root MP is configured and a registration mode is set. When a source MP wants to send data to a destination MP but has no path to the destination in its routing table, the source can send the data frames to the root MP. Because the mesh network is in registration mode, the root MP knows that the destination is inside the mesh network. It forwards the data frame to the destination together with an indication that both the source and destination are in the same mesh. This data frame activates the destination MP to initiate a path discovery for the destination. This procedure will establish the optimal path between the source and destination MPs. The subsequent data frames will be forwarded on this path.

3. Proposed Decentralized Hybrid Wireless Mesh Protocol (DHWMP)

3.1 Decentralized Proactive Routing Mechanism

In proactive routing, the source MP generates PREQ for the destination MP and sends it to MPP. MPP is a fixed part of the network and maintains two routing tables. The first routing table stores information about PREQ, such as the source MP address, source address, destination address, and hop count, and it maintains the neighbor query. In the second routing table, the MPP stores source path details, such as the source MP address, destination MP address, intermediate MPs addresses, and root IDs. The root is found based on the calculation of the neighbors' information. The common MP between the source and destination is assigned to be a root, and the MPs that compose the shortest path are the intermediate MPs. Some common information elements (IEs), such as the element ID (to be defined (TBD)), hop count (the number of hops from the originator to the MP transmitting the request), time to live (TTL, maximum number of hops allowed for this IE), and metric (the cumulative metric from

the originator to the MP transmitting the PREQ) are used in proactive mechanisms. A modified proactive mechanism is defined below.

When a source MP wants to send data to a destination MP, the source MP checks its routing table as to whether there is a path to the destination. If there is no path, then the source MP will discover a new route to the destination MP with the help of PREQ. The source MP is also known as the originator.

The IE contained in PREQ is shown in Figure 3. In our proposal, PREQ has a destination address, source address, and MPP address, which contains the address of the specific MPP that was sent by the source PREQ for the destination MP. The destination sequence number (DSN) field has the sequence number of the destination, and the source sequence number (SSN) field has the sequence number of the source MP. We have added the MPP address as a new information element in our proposed schemes.

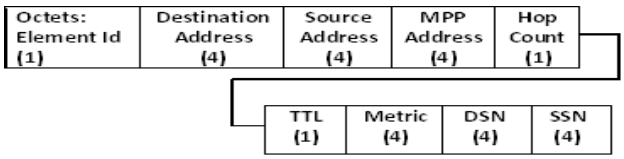


Figure 3. PREQ Element Fields Sent by the Source Node to the MPP

After receiving the proactive PREQ from the source MP, the MPP will store all of the information about the source, such as the destination address, source address, and neighbors' addresses, and then, the MPP will generate a neighbor query "neighbors" address of each node in the network. This query will broadcast to all of the nodes. In Figure 3, we show the neighbor query. In the MP address field, we store the address of the specific MP that sends the neighbors' information to the MPP. The neighbors' query element is added into the MPP PRQE message for the neighbor information. The length shows the distance between the nodes, and other IEs are the same as the previous PREQ IE. The IE of the neighbors' PREQ is specified in Figure 3.

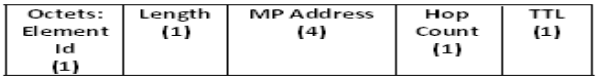


Figure 4. PREQ Element Fields Sent by the MPP with the Neighbor Query

Neighbor information is a new information element. We used this element to obtain the neighbors' information. Upon receiving a neighbor query from the MPP, each MP will send the information on the neighbors to MPP, which will maintain the information in its routing table. It will search for a common feasible neighbor between the source and destination and will define that node as a root. The complete information about the source and destination has been sent to that specific node so that it can prepare itself to work as a root. MPP sends a neighbor query and receives neighbor information from all of the existing MPs. In Figure 5, we show the PREP from MPs to MPP. Each MP replies to a neighbor query request with information about its own neighbors' details, such as the neighbors' addresses, neighbor link metric, and lifetime (the time for which MPs receive the PREQ considering the forwarding information to be valid).

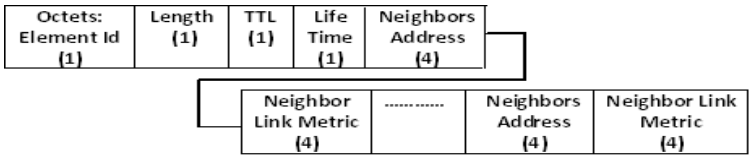


Figure 5. PREP with Neighbor Information for MPP

In Figure 6, the PREP from the MPP to the source node has the information of the element ID, length (L), destination address, sources address, and path information (information about the root address and all intermediate node addresses). Its size depends on the total number of intermediate node addresses. In this IE, we added new path information details.

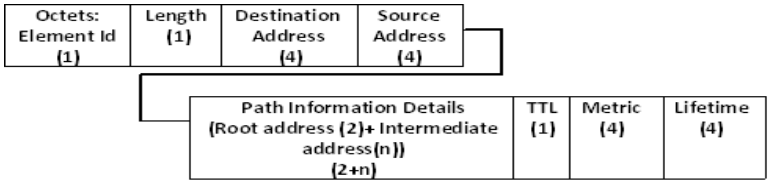


Figure 6. PREP by the MPP to the Source Node with Path Information for the Path Details

In the proactive routing protocol, the MPP will announce common neighbors of source-destination pairs as roots in the network. For each node, after receiving neighbor information, the MPP finds the common neighbors between the source and destination MPs. If it has any common neighbor, then it announces that node as a root. If more than one common node has been found between the source and destination MPs, then the MPP attempts to define the less weighted node as the root. If both common nodes have the same weight, then MPP announces the root based on its priority.

If the source MP changes in a network, then a new source MP always sends PREQ through a new path to MPP, and MPP again provides the new path according to the source and destination neighbors. The complete details of that path are stored in the second routing table for future use.

When any new node is added to the network, then the new node sends a hello message to the neighbors. Then, the neighbors store information about that new node in their table and send the details to the MPP. Then, the MPP updates its own table.

Each MP maintains its table by providing information about the node address, neighbor details, and path details (if the MP plays any role between the source and destination, then the details of the path were maintained by the MPP). In Figure 7, we have shown the elements of the root announcement, such as the source address, destination address, and root address (an address of a node that has been announced as a root between the source and destination by the MPP). The IE of RANN is defined in Figure 7.

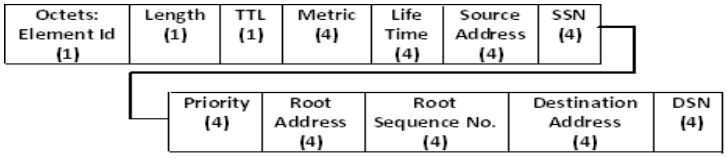


Figure 7. Root Announcement Field Elements

3.2 Proposed Reactive Routing Protocol

When a source MP needs a path to the destination MP, then the first source MP will check its proactive routing table and find its path, which has been provided by the MPP and stored in the source MP. Then, the source node sends a hello message to the next MP. If a node is found to be in a sleeping mode, then after receiving the hello message, that node becomes activated in preparation for action. If any node has been found to be busy in any other transmission, then that node receives the information that one more action is waiting to be processed. The airtime link metric is always initialized to zero in reactive routing. Whenever an MP forwards a hello message, the MP updates the metric field to reflect the cumulative metric of the path. After activating the path of the source node, the destination MP unicast PREP goes back to the source node.

When the source receives the PREP, it transmits data frames to the destination. If the destination receives further hello messages with a better metric, then the destination updates its path for the new path and sends the PREP to the source along the updated path. It uses little energy compared with an existing PREQ message because in existing systems, reactive routing always broadcasts the PREQ to all MPs in the network for the path and waits for a PREP and then searches for a better path option. However, in our proposal, the source MP finds the path from the proactive routing table and starts communicating with the help of a hello message. If the source MP does not obtain any path information from its proactive routing table, then the reactive routing can work as an existing system that initiates with the PREQ. Thus, our proposal saves energy during reactive routing.

In this paper, we introduce reactive routing path initialization (RRPI) protocol messaging, and the message format is shown in Figure 8. The RRPI has a source address, destination address, next MP address (which it receives from the proactive routing table and the size of which depends on the predefined path (n)), hop count, TTL, and metric.

Octets: Element Id (1)	Source Address (4)	Destination Address (4)	Next MP Address (according to proactive table) (n)	Hop Count (1)	TTL (1)	Metric (4)

Figure 8. Reactive Routing Path Initialization IE

4. Performance Analysis

We have used the simulation scenarios of NS-2 to analyze the performance results on the aggregate throughput, which is shown below. The system parameters for the simulation have been set as shown in Table 1. The simulation area was 1,000×1,000 m^2. The packet size is set to 512 bytes, and the packet transmission rate is set to 10 packets/s. The Wi-Fi radio mode is set to 802.11b, and the radio range is set to 50 m. The radio bandwidth is 2 Mbps. The total number of nodes is 100. We employed a constant bit rate (CBR) source for the traffic scenario. We also used a single radio system for WMNs, which means that the same radio is used for access and wireless backhaul.

Table 1. System Parameter Metrics for Simulation in NS-2

Parameter	Value
Simulation area	1,000 ×1,000 m^2
Total no. of nodes	100
Simulation Time	500 s
Packet size	512 bytes
Bandwidth	2 Mbps
Packet rate	10 pkts/s

Four different performance metrics were used for the performance comparison: the channel capacity [ref], packet delivery ratio, end-to-end (ETE) delay, and routing overhead. In this scenario, the performance of the DHWMP protocol is evaluated and compared with OLSR, AODV, and HWMP as a function of the number of nodes. Figures 9, 10, 11, 12, and 13 depict the channel capacity of each node, channel capacity of the entire network, packet delivery ratio, ETE delay, and routing overhead, respectively.

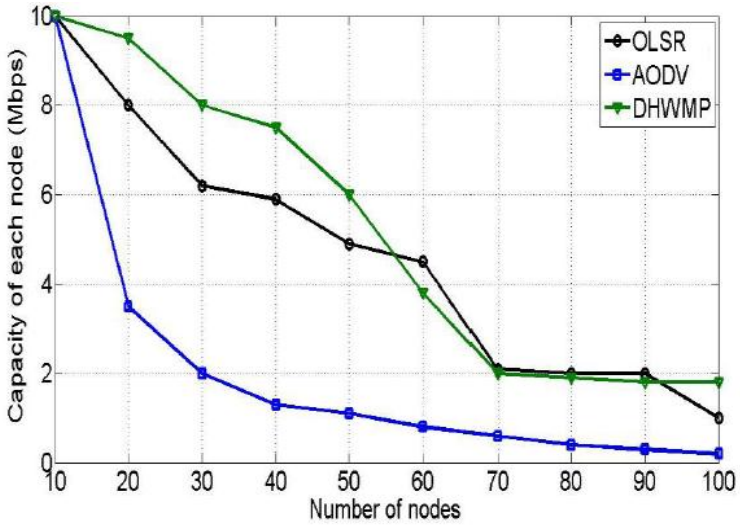


Figure 9. Comparison of Each Node's Channel Capacity in the WMN

Figure 9 compares the channel capacity performances of OLSR, AODV, and DHWMP in each node for a single radio. The DHWMP outperforms OLSR and AODV. In the beginning of the simulation, all three routing protocols start from the same point with fewer nodes. However, as the number of nodes increases, the capacity performance of all protocols decreased due to network congestion and collision. DHWMP still outperforms AODV and OLSR. When the number of nodes is 30, the difference between DHWMP and AODV is the highest, with a difference of almost 6 Mbps. The maximum (almost 2 Mbps) and minimum (0.01 Mbps) differences between OLSR and DHWMP occur with 30 and 70 nodes, respectively.

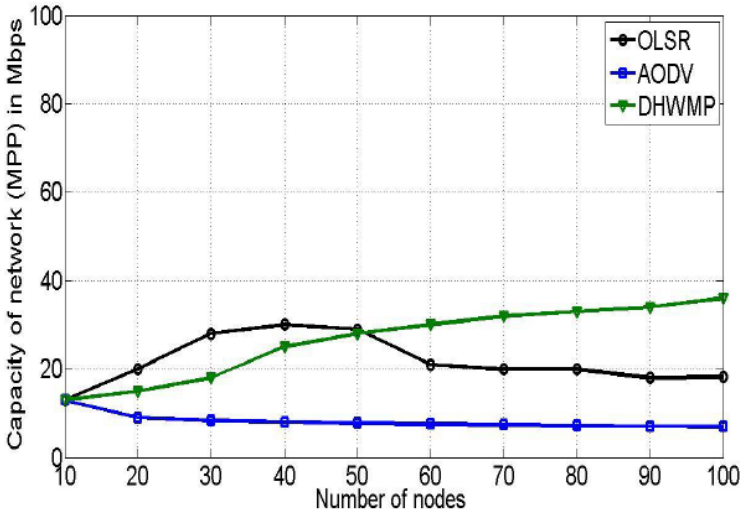


Figure 10. Comparison of the Network Channel Capacity in a WMN

The simulation results in Figure 10 compare the channel capacity performance for the entire network for the proposed DHWMP and the other existing routing protocols (AODV and OLSR). At the beginning of the simulation, the capacities of all of the routing protocols were similar. However, as the numbers of nodes increased, the performance of AODV decreased while the capacities of OLSR and DHWMP increased. In the figure, until the number of nodes is 50, DHWMP does not perform better than OLSR. When there are more than 50 nodes, DHWMP outperforms OLSR. In a large-scale network, DHWMP outperforms OLSR and AODV in terms of channel capacity.

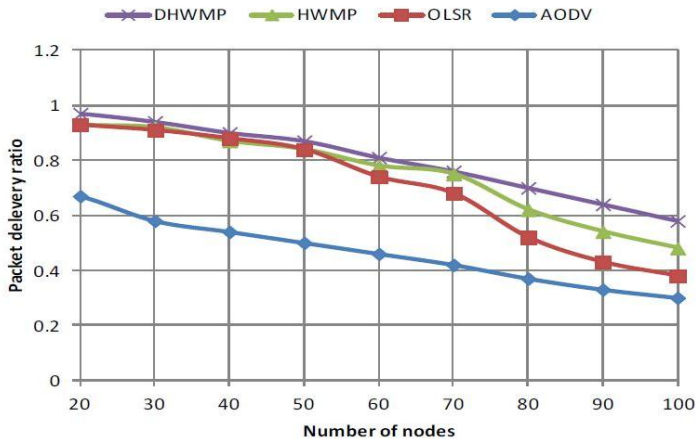


Figure 11. Packet Delivery Ratio as a Function of the Number of Nodes

The packet delivery ratio (PDR) denotes the ratio of the total packets that were received at the destination to the total packets that were sent by the source during the entire simulation, which reflects the efficiency of the routing. The PDR is used to determine the optimal number of delivery paths under different circumstances. It is also used to determine the suitability of different clustering algorithms to support multipath routing. The more packets that are received, the better the performance is.

In other words,

$$PDR = \frac{\Sigma Pr}{\Sigma Ps} \tag{1}$$

where PDR denotes the PDR during the entire simulation, Pr denotes the number of packets received by the destination, and Ps denotes the number of packets sent by the source.

Figure 11 shows the PDR of DHWMP, which is higher than those for HWMP, OLSR, and AODV. Although there is better performance using a single channel, when there are more nodes transmitting packets through the network, the performance begins to degrade. However, from Figure 11, we can see that the PDR of DHWMP with an increasing number of nodes is better than for those for AODV, OLSR, and HWMP.

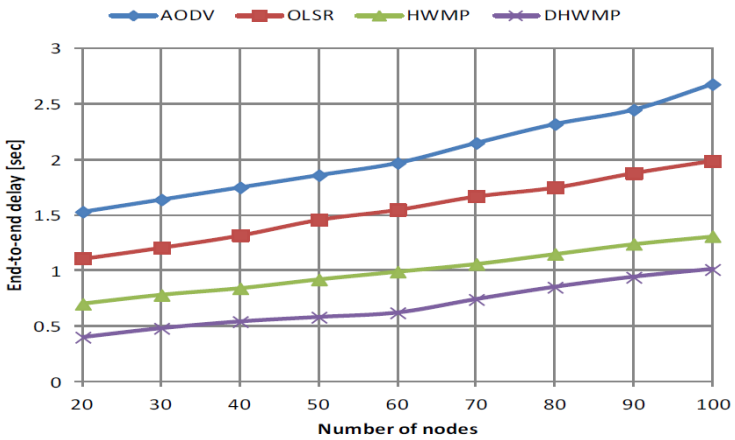


Figure 12. ETE Delay as a Function of the Number of Nodes

The data transmission time from a source to destination is known as ETE delay. The unit of delay is seconds. The ETE is the total transmission time between the source and destination, including the time delay that is caused by the cache during the discovery phase, the queue waiting time, and the transmission time over the links. The lower the ETE delay, the better the performance. The ETE delay is defined as follows:

$$ETE\ delay = \frac{\Sigma(T_R - T_S)}{\Sigma N_P} \tag{2}$$

where T_R denotes the time to receive the packets, T_S denotes the time to send the packets, and N_P denotes the number of packets. The delay time increases as the number of nodes increases. Figure 12 presents the ETE delay as a function of the number of nodes. DHWMP has the lowest ETE delay compared to that of the existing HWMP, OLSR, and AODV. In this result, DHWMP has the lowest ETE delay compared to other routing protocols. The ETE delay of DHWMP at 20 nodes is 0.4 s. After that, it increases slightly as the numbers of nodes increases. The ETE delay of DHWMP at 100 nodes is 1 s, whereas the AODV, OLSR, and HWMP ETE delays are 2.7 s, 2 s, and 1.8 s, respectively.

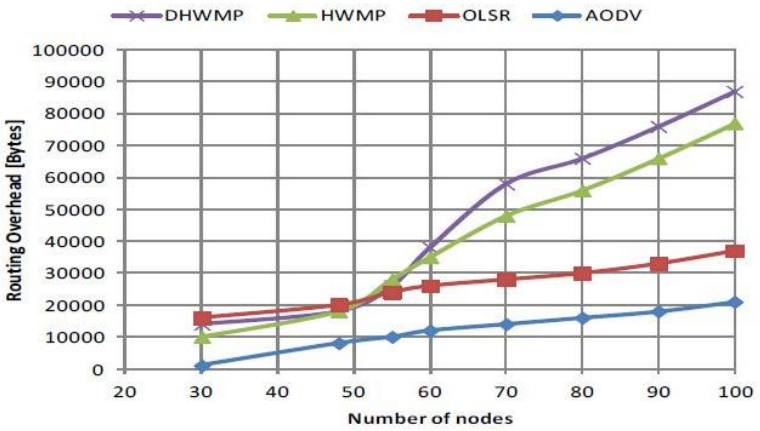


Figure 13. Routing Overhead as a Function of the Number of Nodes

Routing overhead is the total number of routing packets transmitted over a network during the simulation time of 200 s. Figure 13 indicates that the routing overhead of DHWMP is less than that of OLSR until there are 55 nodes. After 55 nodes, the overheads of HWMP and DHWMP increase rapidly due to node congestion and collisions, but the overhead of HWMP is still less than that of DHWMP. AODV, HWMP, and OLSR have less overhead than HWMP. When there are only a few nodes, DHWMP performs slightly better than OLSR. DHWMP and HWMP have almost the same overhead when there are 48-56 nodes. In a practical case, 50 nodes would be a common deployment. Thus, DWHPM is a valid option for WMN routing.

5. Conclusions

HWMP is the default routing protocol for IEEE 802.11s-based WMNs. HWMP combines both reactive and proactive techniques. However, the existing systems have many drawbacks. For example, HWMP has a root bottleneck problem in the proactive mode and a power wastage problem in the reactive mode. To overcome these problems, the proposed scheme uses different roots for different transmissions in the proactive routing protocol. In the existing HWMP, during reactive routing, if any node needs to transmit data, it initiates with a PREQ message. However, our scheme simply sends a hello message to start the data communications. Therefore, we can improve upon the drawbacks of an existing HWMP.

We have measured the performance of DHWMP with respect to the channel capacity, PDR, ETE delay, and routing overhead. DHWMP outperforms the existing protocols in terms of channel capacity, PDR, and end-to-end delay, but it requires large routing overhead compared to other routing protocols. However, if we consider a practical WMN case in which the number of nodes is fewer than 50, routing overhead is not a serious problem.

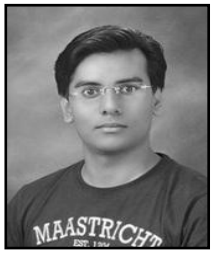
Acknowledgements

This research was supported by Basic Science Research Program though the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Grant number: 2012-0002273 and 2012-0008447).

References

[1] M. Singh and S. -G. Lee, "Decentralized Hybrid Wireless Mesh Protocol", Proceedings of Fourth International Conference on Computer Sciences and Convergence Information Technology, **(2009)** November, pp. 824-829; Seoul, Korea.
[2] IEEE Standards Association, "IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", **(2007)** June.
[3] IEEE Standards Association, "IEEE Std 802.15.1-2005 – Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)", **(2011)** June.
[4] "The IEEE 802.16 Working Group on Broadband Wireless Access Standards", http://grouper.ieee.org/groups/802/16/.
[5] Akyildiz, F. Ian, X. Wang and W. Wang, "Wireless Mesh Networks: a Survey", Computer Networks and ISDN Systems, vol. 47, **(2005)**, pp. 445-487.
[6] U. Varshney, "Pervasive Healthcare and Wireless Heath Monitoring", Mobile Network and Applications, vol. 12, **(2007)**, pp. 113-127.
[7] C. M. Oh, H. J. Kim, G. Y. Lee and C. K. Jeong, "A Study on the Optimal Number of Interfaces in Wireless Mesh Network", International Journal of Future Generation Communication and Networking (IJFGCN), vol. 1, no. 1, SERSC, **(2008)**, pp. 59-66.
[8] Z. Hu, P. Verma and J. Sluss Jr., "Routing in Degree-constrained FSO Mesh Networks", International Journal of Hybrid Information Technology (IJHIT), vol. 2, no. 2, SERSC, **(2009)**, pp. 71-80.
[9] P. Xiao, J. He and Y. Fu, "Distributed Group Key Management in Wireless Mesh Networks", International Journal of Security and Its Applications (IJSIA), vol. 6, no. 2, SERSC, **(2012)**, pp. 115-120.
[10] Draft STANDARD for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements – Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE P802.11s / D4.01, **(2010)**.
[11] S. Waharte, R. Boutaba, Y. Iraqi and B. Ishibash, "Routing protocols in wireless mesh networks: challenges and design considerations", Multimed Tools Appl ., vol. 29, **(2006)**, pp. 285–303.
[12] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF RFC 3561, **(2010)**.
[13] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", IETF RFC 3626, **(2003)**.
[14] X. Wang and A. O. Lim, "IEEE 8002.11s wireless Mesh networks: Framework and challenges", Ad Hoc Networks, vol. 6, **(2008)**.
[15] Belair Networks, "Capacity of Wireless Mesh Networks", white paper, BDMC00040-C02, **(2006)**.

Authors



Madhusudan Singh received his Ph.D. degree in the Dept. of Ubiquitous IT, from Dongseo University (DSU), Busan, South Korea in 2012. M. Tech. degree in Dept. of IT with spec. in Software Engineering from Indian Institute of Information Technology, Allahabad (IIIT-A), India in 2008 and his Master degree in the Dept. of Computer Application from UP Technical University(UPTU), Lucknow, India in 2006. Bachelor degree is the Dept. of Computer Applications from VBS Purvanchal University, Jaunpur, India. Dr. Singh was a visiting research scholar at University of the Pisa, Italy in 2010. Currently, he is a senior engineer, at Samsung Research Group at Samsung Display, South Korea. His fields of research interests are Wireless Mesh Networks, Information Security, Wireless Sensor Networks, Signal System, Image Processing, and Software Engineering.

Sang-Gon Lee received his BEng, MEng, and PhD degree in electronics engineering from Kyungpook National University, Korea, in 1986, 1988, and 1993, respectively. He is a professor at the Division of Computer & Information Engineering, Dongseo University. He was a visiting scholar at QUT, Australia from 1993 to 1994. His research areas include information security, network security, wireless mesh/sensor network and future internet.

HoonJae Lee received his BS, MS, and PhD degrees in electronic engineering from Kyungpook National University, Daegu, Korea in 1985, 1987, and 1998, respectively. He is currently a professor in the School of Computer & Information Engineering at Dongseo University. From 1987 to till date, he was a research associate at the Agency for Defense Development (ADD). He has more than 150 national/international technical publications as well as about 50 patents. His current research interests include developing secure communication system, secure Wireless Sensor Network, and Side-Channel Attack.