IEEE 802.16 메쉬 네트워크에서의 SN-Protected 네트워크 엔트리 프로세스

준회원 임 립 상*, 정회원 유 상 조**

SN-Protected Network Entry Process for IEEE 802.16 Mesh Network

Lin Lixiang* *Associate Member*, Sang-jo Yoo** *Regular Member*

ABSTRACT

The workgroup of IEEE 802 proposed the IEEE 802.16 standard, also known as WiMAX, to provide broadband wireless access (BWA). The standard specifies two operational modes, one is popular PMP mode, and the other is optional mesh mode. In the mesh mode, the network entry process-NetEntry is the pivotal procedure for mesh network topology formulation and thus, influences the accessibility of whole mesh network. Unfortunately, the NetEntry process suffers from the hidden neighbor problem, in which new neighborship emerges after a new node comes in and results in possible collisions. In this paper, we propose a new SN-protected NetEntry process to address the problem. Simulation results show that the new proposed NetEntry process is more stable compared with the standard-based NetEntry process.

Key Words : IEEE 802.16, Broadband Wireless Access, WiMAX, Mesh Network, Network Entry

Ⅰ. Introduction

With the development of wireless communication technology, great success has been achieved to provide voice service for users. To meet the increased need of users' demand, the development of next-generation broadband communication network targets at providing user with high speed, high bandwidth, and low delay and low packet loss rate. To develop standards and recommend practices to support the development and deployment of broadband wireless access (BWA) in wireless metropolitan area (WMAN) networks, the IEEE 802.16 workgroup was established. The alternative in Europe is the standard High Performance Radio Metropolitan Area Network (HIPERMAN) developed by the European Telecommunications Standards Institute (ETSI). The equivalent standard in Korea is the Wireless Broadband (WiBro)[1].

Wireless mesh network (WMN) has been attracting much attention in recent years due to its inherent advantages, such as high throughput, quick deployment, easy maintenance, low cost, self-organization, self-configuration and self-correction. Originally, wireless mesh network was developed to meet the challenge in military communication, including high-bandwidth transmission, IP for point to point, accurate position without GPS equipped.

※ This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2010-C1090-1011-0007)

* 인하대학교 정보통신대학원 멀티미디어통신망 연구실 (linlixiang@hotmail.com)
** 인하대학교 정보통신대학원 (sjyoo@inha.ac.kr)

논문번호 : KICS2009-09-400, 접수일자 : 2009년 9월 10일, 최종논문접수일자 : 2010년 6월 30일

These days, the mesh network for wireless local area (WLAN) has come out, in which the wireless route can achieve 5km transmission range. Thus, it is possible to apply the wireless mesh technology in WMAN communication system. Under these circumstances, the workgroup of IEEE 802.16 includes mesh mode in the IEEE 802.16 standard[2] as the extension of point-to-multipoint (PMP) mode. In the mesh mode, direct communication between subscriber stations (SSs) is defined in the MAC layer. Therefore, nodes can communicate with each other via multihop routing or forwarding without the aid of the BS node. One BS can support more SSs in the mesh mode compared with the PMP mode. Besides, mesh networks are able to be extended quickly, simply by adding more SSs.

In the IEEE 802.16 mesh mode, a new node, referred to as the node that expects to join the mesh network, is supposed to finish the network entry (NetEntry) process before it becomes a regular active mesh node in the network. Therefore, the NetEntry process is a pivotal procedure for an IEEE 802.16 mesh network[1]. Moreover, the performance of the NetEntry process plays an important role in the operations of IEEE 802.16 mesh networks because all nodes need to complete this step when joining the network. However, according to our research, the NetEntry process may suffer from the hidden neighbor problem where some new neighborships emerge after a new node comes in and leads to collision, which results in some new nodes taking a long time to finish the NetEntry process. A few nodes even fail to finish the NetEntry process. In this paper, we propose a new NetEntry process, so-called SN-protected NetEntry process, to solve the problem.

The paper is organized as follows. Section II shows an overview of the IEEE 802.16 mesh mode. Section III provides the problem statement and proposes the SN-protected NetEntry process. Section IV presents the performance evaluation of our solution by simulation results. Finally, Section V concludes the paper.

Ⅱ. Mesh Mode Overview In WiMAX

2.1 Network Architecture

In the PMP mode, the SS has direct link connected to the BS. This architecture is exactly similar to celluar networks. On the contrary, there is no separate downlink and uplink in the mesh mode. As shown in Fig. 1, every SS can directly communicate with its neighbors without the help of BS, and the SS act as the wireless relay to forward others's traffic toward the central mesh BS. In typical installation, one or several nodes act the role of BS to connect with the external backhaul link, e.g., Internet or telecommunication networks. Such nodes are referred to as mesh BS and the other nodes are called mesh SS[1]. A node can choose the links with the best quality to transmit data, and with an intelligent routing protocol, the traffic can be routed to avoid the congested area.

The other three important terms of Mesh mode are neighbour, neighborhood and extended neighbourhood. The station with which a node has direct links are called neighbors. Neighbors of a node shall form a neighborhood. A node's neighbors are considered to be "one hop" away from the node. An extended neighbourhood contains, additionally, all

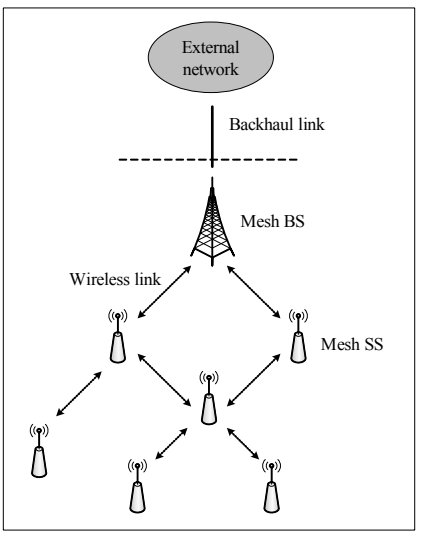


Fig. 1. The IEEE 802.16 mesh network architecture

the neighbors of the neighborhood[2].

2.2 Frame Format

Fig. 2 presents the frame format in the IEEE 802.16 mesh mode. In this mode, network accesses are in a manner like TDMA. The network bandwidth is divided into frames, and each frame consists of control subframe and data subframe. The control subframe is defined for the transmission of signalling messages, which is fixed as (MSH_CTRL_LEN*7) OFDM symbols. The parameter MSH_CTRL_LEN is advertised in the Network Descriptor IE (information element). The control subframe is composed of a few transmission opportunities in terms of different time slots.

As shown in Fig. 1, two types of control subframes exist, a network control subframe and a schedule control subframe. After one periodic network control subframe, the following 4*Scheduling_Frame (SF) frames are the schedule control subframes followed by the next frame with network control subframe. The SF parameter value is defined in the Network Descriptor IE.

The network control subframe is used primarily for new nodes in gaining access to a WiMAX mesh network and then joining the network. As mentioned before, the network subframe contains a few transmission opportunities, the first transmission opportunity (TxOpp) serves only for new nodes to transmit network entry messages (MSH-NENT) in the NetEntry process. The remaining transmission opportunities are used for function nodes to transmit network configuration messages (MSH-NCFG), which are used for advertising the network configuration information of a mesh network.

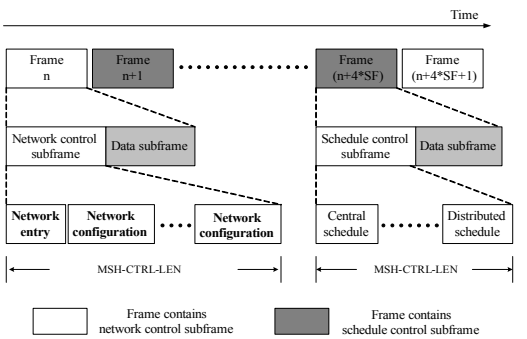


Fig. 2. Frame format in IEEE 802.16 mesh mode

The schedule control subframe is used to allocate resource in a common medium, where the first part is for transmitting centralized scheduling messages (MSH-CSCH/MSH-CSCF) and the second part is for transmitting distributed scheduling messages (MSH-DSCH). The parameter MSH_DSCH_NUM in the Network Descriptor indicates how many distributed scheduling messages may occur in the schedule subframe. This suggests that the first (MSH_CTRL_LEN- MSH_DSCH_NUM) TxOpps are allocated for MSH-CSCH and MSH-CSCF.

The data subframe is mainly used to transmit data, which consists of a fixed number of minislots, up to 256 depending on the physical layer profile employed[3].

2.3 Distributed Election Scheduling

In the IEEE 802.16 mesh mode, the transmission timing of MSH-NCFG (also MSH-DSCH) is based on distributed election-based scheduling, and each node is supposed to determine the next transmission opportunity of MSH-NCFG during last transmission time based on distributed scheduling algorithm. This distributed scheduling ensures no collisions occur within the extended two-hop neighborhood of each node and works without central control[4].

To explain the distributed election-based scheduling, we first introduce some important definitions. The first one is holdoff time (HT). According to the standard, after one transmission of MSH-NCFG, the node is supposed to wait for at least a holdoff time before next transmission. The second definition is eligible transmission interval (ETI). Once the node determines next transmission opportunity (TxOpp) by election algorithm, it will not broadcast the exact TxOpp but only the interval of series transmission opportunities to save network resources, which is referred to as ETI.

The distributed election-based scheduling contains two primary parameters: Xmt_Holdoff_Exponent (exp) and Next_Xmt_Mx. With the Xmt_Holdoff_Exponent, holdofftime(HT) is derived as

$$HT=2^{(base+exp)} \quad (1)$$

in which base value is defined as 4 in the standard.

During each transmission time, a node calculates the next TxOpp based on the following 3 steps: 1) setting the Temp_Xmt_Time equal to the first TxOpp after the HT, 2) determining competing nodes list in Temp_Xmt_Time, 3) running the Mesh Election algorithm, which is defined in the IEEE 802.16 standard. If the specific node generates the biggest value accoding to Mesh Election algorithm, it wins the competition and sets Temp_Xmt_Time as next TxOpp. Otherwise, the specific node loses the competition in this slot. The node sets the Temp_Xmt_Time to the next slot and executes the same steps untilit finally wins as shown in Fig.3. After determining the next TxOpp, the node calculates appropriate Next_Xmt_Mx(MX) together with Xmt_Holdoff_Exponent parameter to broadcast in the MSH-NCFG message. Therefore, neighbor nodes are able to aware ETI of the specific node, which is derived as

$$2^{exp}*MX<ETI<2^{exp}*(MX+1) \quad (2)$$

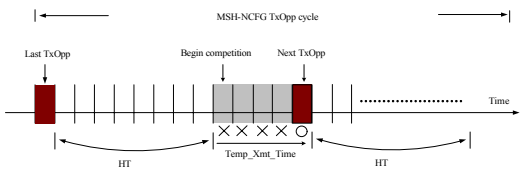


Fig. 3. Overview of distributed election-based election

2.4 NetEntry Process

Fig. 4 provide an example that a new node appears in network, where the new node has 3 one-hop neighbor nodes and 3 two-hop neighbor nodes in the scenario. In the IEEE 802.16 mesh mode, any new node needs to complete the network entry process when joining the mesh network. The entire NetEntry can be divided into the following procedures[2]:

- · synchronization and obtain network parameters
- · opening sponsor channel
- · negotiation, authentication and registration
- · closing NetEntry process.

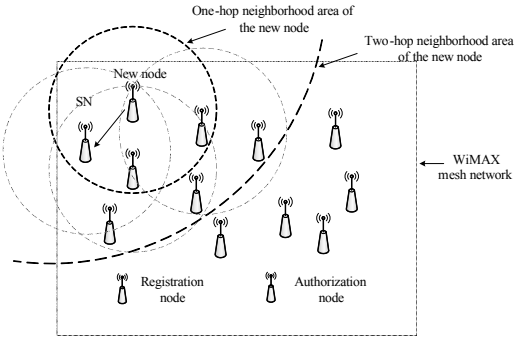


Fig. 4. A case for a new node's NetEntry process

Fig. 5 depicts the control message exchange overview in each procedure of the whole NetEntry process. After being powered on, a new node shall perform scanning and search for network configuration message (MSH-NCFG) to acquire coarse synchronization with the mesh network. MSH-NCFG message is broadcasted in network to advertise the basic network configuration. Once the PHY has achieved coarse synchronization, the node should attempt to acquire network parameters and build a physical neighbor list based on received MSH-NCFGs. In particular, the new node shall continually monitor MSH-NCFG messages at least until it receives the MSH-NCFG from the same node twice. Then, the new node will select a sponsor node (SN) from the physical neighbour list and send out a MSH-NENT:NetEntryRequest by contending for a network entry transmission

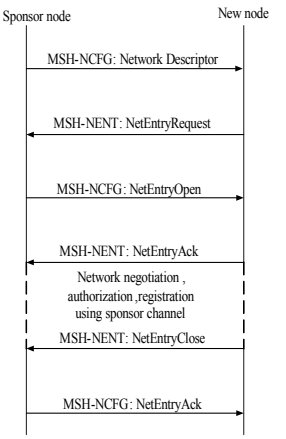


Fig. 5. Message exchange overview of the NetEntry process

opportunity.

Upon receiving the request message, the SN will evaluate the request. If the SN is not capable to serve this request, it will send back a MSH-NCFG:NetEntryReject, or if the SN accepts the request, it will send out a MSH-NCFG: NetEntryOpen, which contains a temporary schedule that could be used for the new node during the next negotiation, authentication and registration procedure. Once the new node has received MSH-NCFG:NetEntryOpen, it acknowledges the acceptance by replying a MSH-NENT:NetEntry and begins to perform negotiation, authentication and registration using the temporary schedule.

After the above procedures have been completed, the new node closes the NetEntry process by sending a MSH-NENT:NetEntryClose to the SN to cancel the temporary schedule. Last but not least, the SN acknowledges the closure of sponsorship by sending a MSH-NCFG:NetEntryAck.

Unfortunately, the standard based NetEntry process does not work well in some dense network according to our research. Some hidden node problems happen during the NetEntry process, which may effect on the performance of the NetEntry process. For example, some new nodes taking a long time to finish the NetEntry process and a few nodes even fail to finish the NetEntry process in some extreme cases. Aiming at improving the stability of the NetEntry process in IEEE 802.16 mesh network, a new NewEntry process is proposed in this paper.

Ⅲ. Related Work

In this section, related work on research for the IEEE 802.16 mesh network is reviewed. So far, a lots of papers in this field have been published, in which most papers focus on the data transmission phase. As mentioned in Section II, resources in data subframe are allocated by either the centralized scheduling or the distributed scheduling. In the centralized scheduling field,[5-8] focus on the centralized scheduling algorithm. In the distributed scheduling field, Claudio et al. [3] analysed the performance of the mesh election procedure by means of extensive simulations. In [4], Bayer et al. analyses the distributed election-based scheduling and propose that constant base value is not optimal and need decrease. In [9], Cao et al. theoretically investigated the performance of distributed election-based scheduling, and a stochastic model for the distributed scheduler of the mesh mode was proposed. In [10], Bayer et al. proposed a dynamic holdoff time setting scheme to improve the performance of the distributed scheduling mode.

On the other hand, our paper is focus on initialization phase of IEEE 802.16 mesh network. Wang et al.[11] first identified the hidden terminal problem in the NetEntry process, and proposed the relevant solution, in which neighbors of a new node shall include the SN in their competing node list all the time to reduce the possible collision. Although their scheme improved the success rate of NetEntry process, it has two disadvantages. First, their scheme still can not ensure 100% success rate. Second, their scheme does not consider the delay of whole NetEntry process. In another paper of Wang et al. [12], they proposed that the neighbors of a new node shall use large holdoff time during whole NetEntry process to remedy the hidden terminal. However, this scheme is not able to guarantee transmission efficiency when the network in stable state. Aiming at solve the limitations of previous two paper, we proposed a new SN-protected NetEntry process.

Ⅳ. Problem Statement

As mentioned in Section I, the performance of the NetEntry process plays an important role in the operations of the IEEE 802.16 mesh network. Unfortunately, when the IEEE 802.16 mesh standard is implemented, the so-called hidden neighbor problem[11], first identified by Wang et al., may occurs in the NetEntry process. As a result, some new nodes may take a long time to finish the NetEntry process and certain new nodes even fail to complete the NetEntry process and thus, can not join the mesh network successfully.

Fig. 6 shows a typical case of the hidden neighbor problem in the IEEE 802.16 mesh network.

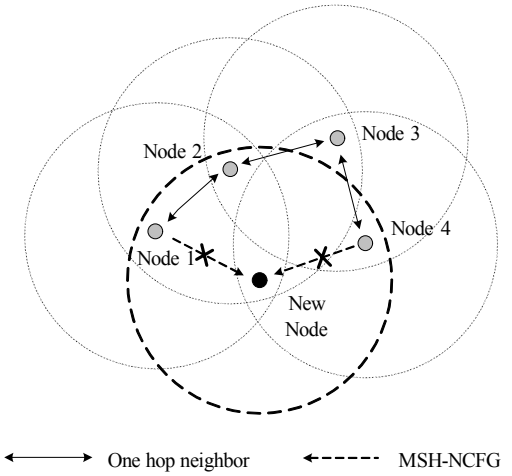


Fig. 6. A hidden neighbor case in the IEEE 802.16 mesh network.

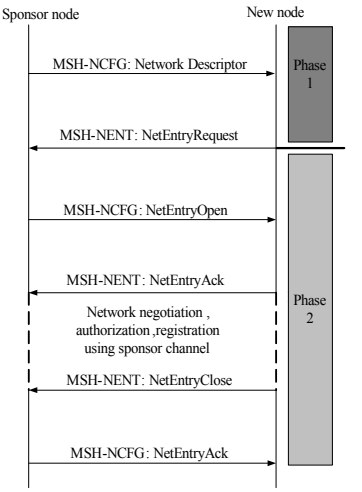


Fig. 7. Two-phase hidden neighbor problem in the NetEntry process.

Before the new node being powered on, we assume that there are only four function nodes (Node 1, 2, 3, 4) that exist in the network. Node 1 and Node 2 are one-hop neighbors of each other, so as Node 2 and Node 3, Node 3 and Node 4. Therefore, Node 3 is two-hop neighbor of Node 1 and Node 4 is two-hop neighbor of Node 2, and vice versa. The neighborship of these four nodes are stable. In particular, Node 1 and Node 4 have no neighborship with each other.

Now, the new node appears and tries to join the network. Node 1 and Node 4, together with Node 2, will become one-hop neighbor of the new node, which makes Node 1 and Node 4 become the so-called "hidden neighbor" of each other. Due to lack of neighborship, the MSH-NCFG messages sent by the hidden neighbor pair are likely to be blocked by each other which might influence the performance of the NetEntry process.

As shown in Fig. 7, the hidden neighbor problem in the NetEntry process can be divided into 2 phases. In phase 1, the new node is monitoring the MSH-NCFG messages from all its one-hop neighbors. In the case of Fig. 3, since the MSH-NCFG from Node 1 might be blocked by Node 4, the new node probably takes more time to accumulate MSH-NCFG messages from Node 1. In particular, it is even possible that the new node fails to obtain any MSH-NCFG from Node 1 in case that all neighbors of the new node transmit MSH-NCFG with a small interval (exp=0,1).

In phase 2, the new node has finished obtaining network parameters from all its one-hop neighbors and selects one node as SN. Unfortunately, if the SN has any hidden neighbor as Node 1 or Node 4 in our case, the two important MSH-NCFG: (NetEntryOpen or NetEntryAck) from the SN to the new node can also be blocked and thus need retransmissions. Timeout T25 is defined in standard for the new node to receive relevant MSH-NCFG and retransmission is triggered after T25. After several timeouts, if the new node still can not receive relevant MSH-NCFG, it shall find a new SN to restart the same process, which delays the whole NetEntry process and wastes network resources.

Ⅴ. The Proposed SN-protected NetEntry Process

5.1 SN-protected NetEntry Process

To ease the hidden neighbor problem and enhance the performance of the NetEntry process in the IEEE 802.16 mesh network, we propose a new SN-protected NetEntry process.

First, when a new node just begins the NetEntry process, all its one-hop neighbors shall employ

relative large exp value, which increases the MSH-NCFG transmission interval and thus reduces the probability of MSH-NCFG message collision between hidden neighbor pairs. Note that the new node can notify its appearance by a short message in the network entry TxOpp. After the new node has successfully finished accumulating MSH-NCFGs from all one-hop neighbors and obtaining network parameters, all its one-hop neighbors decrease their exp value by overhearing MSH-NCFG: NetEntry-Request indicating the end of phase 1. In the following NetEntry process, the hidden neighbor problem belongs to phase 2 and only happens on SN as we explained in part A. Therefore, all one-hop neighbors could employ a small exp value to improve transmission efficiency.

As mentioned in Section III, Wang et al. have proposed a similar scheme[12], in which large exp value is used by neighbors during the whole NetEntry process. In fact, it is only suitable for the case that whole network is in initialization phase. On the other hand, we focus on a different case in which the network is stable and transmission efficiency must be considered. Therefore, we propose all one-hop neighbors of a new node use a large exp value only in phase 1 instead of the whole NetEntry process.

Seond, after successfully accumulating MSH-NCFGs from neighbors and selecting the SN, the hidden neighbor problem proceeds to phase 2. As mentioned in part A of this Section, two important MSH-NCFG messages from the SN to the new node, MSH-NCFG:(NetEntryOpen or NetEntryAck), have the possiblityof being blocked due to hidden neighbors which thus, influences the NetEntry process. To deal with this problem, the concept “SN-protected interval” is introduced, which means the SN‘s eligible interval for two important MSH-NCFG: (NetEntryOpen or NetEntryAck). As depicted in Fig. 8, on receiving MSH-NENT: (NetEntryRequest or NetEntryClose) transmitted by the new node, the SN shall reply with MSH-NCFG:(NetEntryOpen or NetEntryAck) in its next MSH-NCFG eligible interval, which is the “SN-protected interval”.

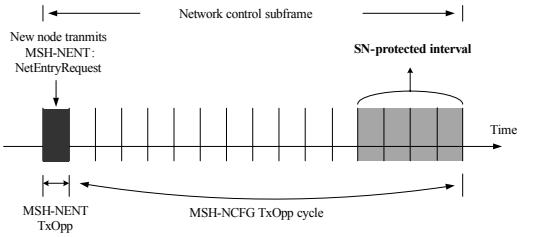


Fig. 8. SN-protected interval of the proposed NetEntry process.

As we mentioned in part B of Section II, a mesh node determines its next MSH-NCFG TxOpp during last MSH-NCFG TxOpp and broadcasts the eligible interval to neighbors. Thus, a new node can be aware of the next MSH-NCFG eligible interval of SN by overhearing the last MSH-NCFG from SN. Therefore, in our proposed method, when a new node transmits MSH-NENT:(NetEntryRequest or NetEntryClose), the new node shall indicate the next MSH-NCFG eligible interval of SN, which is the protected interval, through MSH-NENT message. To achieve that, a new node needs to take out two fields from the latest MSH-NCFG from SN, Next_Xmt_Mx and Xmt_Holdoff_Exponent, and then add into MSH-NENT:(NetEntryRequest, NetEntryClose). Fig 9 illustrates the revised MSH-NENT:(NetEntryRequest or NetEntryClose) message format. Thus, all the one-hop neighbors of the new node are informed of the SN-protected interval after overhearing the two above MSH-NENT messages.

Syntax	Size	Notes
MSH-NENT_Message_Format(){		
Management Message Type = 40	8 bits	
Type	3 bits	0x2 NetEntryRequest 0x3 NetEntryClose
Sponsor Node ID	16 bits	
Next Xmt Mx (SN)	3 bits	
Xmt Holdoff Exponent (SN)	5 bits	
Xmt Power	4 bits	
Xmt Antenna	3 bits	
If (Type=0x2)	variable	
MSH-NENT_Request_IE()		
}		

Fig. 9. Revised MSH-NENT:(NetEntryRequest or NetEntryClose) message format.

In addition, the time consumed for the SN to evaluate a sponsorship request is referred to as the process time. Fig. 11 shows an example that the next MSH-NCFG eligible interval of the SN might be too close to MSH-NENT:NetEntryRequest, which results in the SN not having enough process time to respond in its next MSH-NCFG eligible interval. Therefore, we also propose that a new node shall evaluate the time between MSH-NENT:NetEntry-Request and the next MSH-NCFG eligible interval. If the time is longer than the process time, the SN-protected interval should be added into MSH-NENT:NetEntryRequest, and if the time is shorter than the process time, a new node shall add SN-protected interval into a new defined MSH-NENT:SN_ProtectedInterval message, by making use of the reserved MSH-NENT format (type 0x0). Fig 10 shows the message format of the new defined MSH-NENT:SN_ProtectedInterval. After gerenates MSH-NENT:SN_ProtectedInterval message, the new node shall select the first MSH-NENT transmission opportunity after the process time to broadcast.

After receiving the revised MSH-NENT:NetEntry-Request or MSH-NENT: SN_ProtectedInterval, the mesh node (e.g. node A) performs the following procedures as shown in Fig. 12. First, Node A checks whether the SN, which is indicated in SponsorNodeID field in MSH-NENT: NetEntry-Request, is already in its whole extended neighbors list. If the SN is in node A's neighbor list, Node A keeps performing the original process because no collision will happen between node A and SN. If the SN is out of node A's neighbor list, it means that node A and SN are hidden neighbors of each other. Then, node A checks whether itself can win any TxOpp during the SN-protected interval. If node A indeed wins a TxOpp during the SN-protected interval, it will check whether the winning TxOpp is just for sending normal a MSH-NCFG or for sending important MSH-NCFG: (NetEntryOpen or NetEntryAck), in which node A could also be a SN to help another new node entering network. If node A is just to send normal MSH-NCFG, we propose node A keeps quiet in the winning TxOpp to avoid collision with the SN. Note that before the wining TxOpp, if node A has received MSH-NENT: NetEntryAck indicating that MSH-NCFG: NetEntry-Open has reached to the new node successfully, then node A is allowed to transmit in the wining TxOpp.

Syntax	Size	Notes
MSH-NENT_Message_Format(){		
Management Message Type = 40	8 bits	
Type	3 bits	0x0 Reserved
Sponsor Node ID	16 bits	
Next Xmt Mx (SN)	3 bits	
Xmt Holdoff Exponent (SN)	5 bits	
Xmt Power	4 bits	
Xmt Antenna	3 bits	
}		

Fig. 10. New MSH-NENT:SN_ProtectedInterval message format

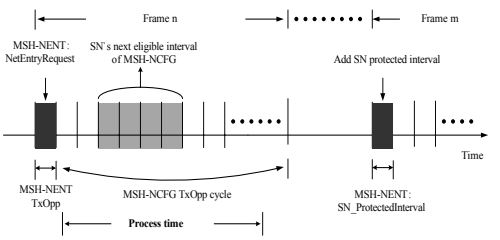


Fig. 11. An example shows the process time

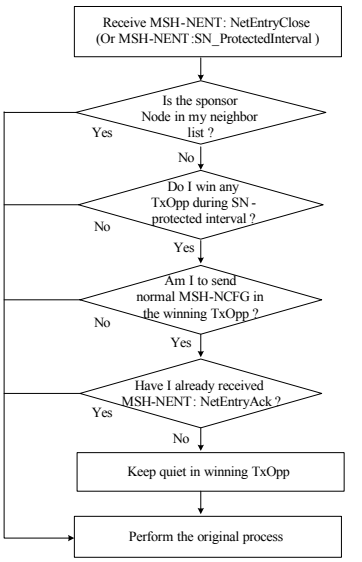


Fig. 12. Neighbor node behaviour in the SN-protected NetEntry process (1)

Futhermore, when mesh nodes receive MSH-NENT: NetEntryClose, similar procedures are repeated as shown in Fig. 13. Thus, our proposed SN-protected NetEntry process prevents two important MSH-NCFG of the SN from the collision problem as illustrated in Fig. 14.

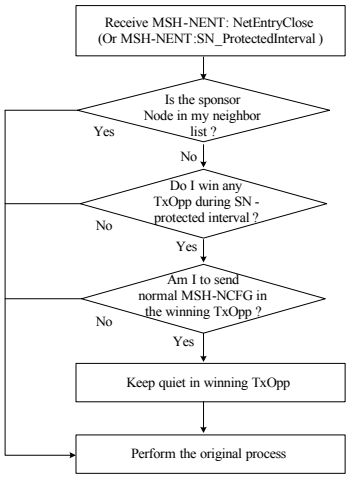


Fig. 13. Neighbor node behaviour in the SN-protected NetEntry process(2)

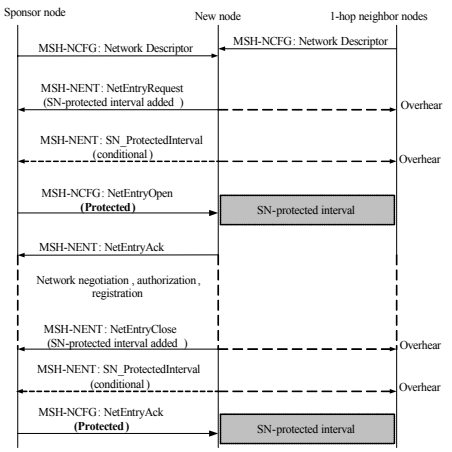


Fig. 14. Message exchange in the SN-protected NetEntry process

5.2 Discussion on the Impact of the Proposed Solution

As mentioned in the previous part, when it is necessary, a certain mesh node needs to keep quiet in the winning MSH-NCFG TxOpp during SN-protected interval. This behaviour might have some impact on the efficiency of MSH-NCFG transmission in the network.

In the example of Fig. 15, node A (exp=2) wins the 2th, 70th and 158th MSH-NCFG TxOpp based on distributed election-based scheduling, and node B is node A's one-hop neighbor. In 2th TxOpp, node A broadcasts its next eligible interval, which is from 68th to 71th. From the view of node B, the next eligible interval of node A changes to (68th,71th) and the earliest subsequent TxOpp of node A is start from 132th as in Fig.16. In 70th TxOpp, node A follows the proposed process and finds that it shall keep quiet in 70th TxOpp. As a result, from the view of node B, the schedule information of node A keeps same as shown in Fig. 17. In contrast, if node A obeys the IEEE 802.16 mesh standard, it shall transmit in 70th TxOpp to broadcast its next eligible interval as (157th,160th). On receiving the MSH-NCFG from node A, node B updates the schedule information as depicted in Fig. 17, where the next eligible interval of node A changes to (157th,160th) and the earliest subsequent TxOpp of node A is start from 221th. In the following TxOpp, node B utilizes the updated schedule information of node A on distributed scheduling algorithm, leading

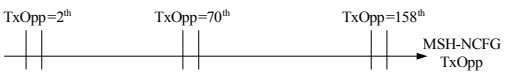


Fig. 15. Example: winning TxOpp of node A.

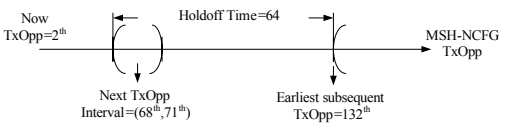


Fig. 16. Example: the schedule information of node A from node B's view in 2th TxOpp.

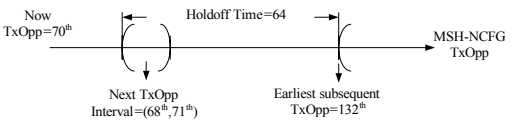


Fig. 17. Example: the schedule information of node A from node B's view in 70th TxOpp (the proposed NetEntry process).

to more efficient calculation. For example, node A will not be added into the competing node list between TxOpp (132th,157th) according to Fig. 18. In contrast, if the schedule information (proposed NetEntry process case) as in Fig. 17 is used, node A shall be added into the competing nodes list after 132th TxOpp in the distributed scheduling algorithm, causing superfluous calculation.

Despite some impact on efficiency of MSH-NCFG transmission, the advantage of the proposed solution is notable. As shown by later simulation work, our proposed solutions considerably improved the performance of NetEntry process.

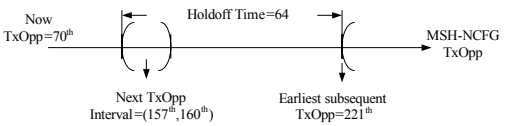


Fig. 18. Example: the schedule information of node A from node B's view in 70th TxOpp (the standard-based NetEntry process)

Ⅵ. Performance Analysis

To analyze the performance of the proposed SN-protected NetEntry process, some experimental simulations are conducted. We compare the proposed SN-protected NetEntry process with the WiMAX mesh standard-based NetEntry process.

6.1 Simulation Environment

In order to conduct a simulation study, we realized distributed election based scheduling and a mesh network platform. Table 1 illustrates the main parameters used in this simulation, which are compliant with the IEEE 802.16 standard[2]. In this simulation, only one channel is used to control subframe transmission, and we do not consider data traffic because the research is only focused only on the control subframe.

To represent different network density, two cases (50 nodes within 1500x1500 square meters area and 100 nodes within 2500x2500 square meters area) are simulated. In each case, mesh nodes are randomly distributed within the defined area, and we repeat

Table 1. Simulation Parameters

Parameter	Value
Scenario	Random-50, 100 nodes
Simulation Duration	100s
Frame Duration	10ms
Max. transmission range	500m
MSH_CTRL_LEN	8
Scheduling_Frames (SF)	2
Standard-based NetEntry (exp)	1
Proposed NetEntry - phase 1 (exp)	3
Proposed NetEntry - phase 2 (exp)	1

the simulation runs until 50 different connected network topology samples are generated. In each topology sample, we implement both the standard-based NetEntry process and the proposed SN-protected NetEntry process for comparison, and the total simulation time is 100 seconds. Finally, we collected 50 comparisons of the NetEntry consumed time.

6.2 Simulation Results

Based on simulation results and theory estimation, we first set the threshold for the NetEntry consumed time as 20 seconds in this simulation, and the NetEntry consumed time means how much time needed for a new node to finish the whole NetEntry process or to become a functional node in network. In the real commercial market, this NetEntry consumed time is a critical criterion for quality of service. Another new definition is introduced for comparison - the ratio of normally entering nodes, which means the ratio of those nodes who can enter the network within the threshold NetEntry time over all simulation cases.

Fig. 19 shows the comparison of the ratio of normally entering nodes. In 50-node case, the ratio is 86% for standard-based NetEntry process while the proposed SN-protected NetEntry process achieves 100% ratio. In 100-node case, the ratio for standard-based NetEntry process is only 72% while the SN-protected NetEntry process still ensures a

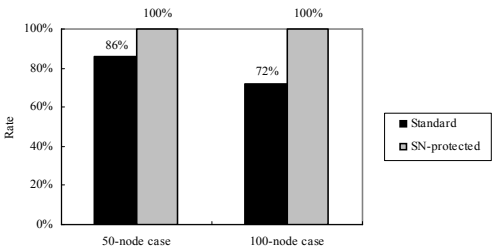


Fig. 19. The ratio of normally entering nodes.

100% ratio.

Fig. 20 compares the consumed time of standard NetEntry process and our proposed SN-protected NetEntry process for 50-node case. According to the simulation result, there are around 38 samples where the proposed NetEntry process requires a little more time to finish and the reason is the hidden neighbor problem does not occur or just has a small impact on the NetEntry process in those samples. Since neighbor nodes employ large exp value in phase 1 of our proposed NetEntry process, a new node takes little more time to finish accumulating MSH-NCFG messages from neighbours, which makes the proposed NetEntry process require a little more time. However, in the remaining 12 samples, the advantage of our proposed SN-protected NetEntry process stands out. We can see that the standard NetEntry consumed more time and even failed in one sample. The reason is the hidden neighbor problem seriously effect the total consumed time of NetEntry process due to MSH-NCFG retransmission and restarting process. In contrast, by solving the hidden neighbor problem, the proposed SN-protected NetEntry is more stable. Although it takes more time in phase 1, the time saved in phase 2 dominates. Therefore, in spite of small excess consumed time in some cases, our proposed NetEntry process is more stable than the standard NetEntry process overall.

Fig. 21 compares the consumed time of Wang's NetEntry process [11] and our proposed SN-protected NetEntry process for 50-node case. As we can see, Wang's solution ease the influence caused by hidden node problem compared with standard NetEntry process. However, since Wang's NetEntry process can not totally solve the problem, there are still several extreme cases exist. On the other hand, our proposed NetEntry process is more stable.

Fig. 22 and Fig. 23 present the comparison for 100-node case, which have similar behaviors with 50-node case. The result shows that the hidden neighbor problem occurs more severely in dense network. As we can see from Fig. 22, compared with 50-node case of Fig. 21, there are more samples in the 100-node case where the standard NetEntry process consumes more time than the proposed NetEntry process, and there are two nodes that fail to complete the standard NetEntry process. In contrast, by following the proposed SN-protected NetEntry process, the unnecessary delay can be reduced considerably. Fig. 23 shows the comparsion

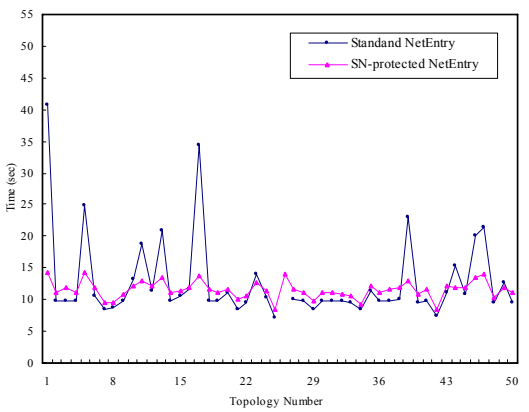


Fig. 20. Standard Entry VS SN-protected Entry in NetEntry consumed time (50-nodescase).

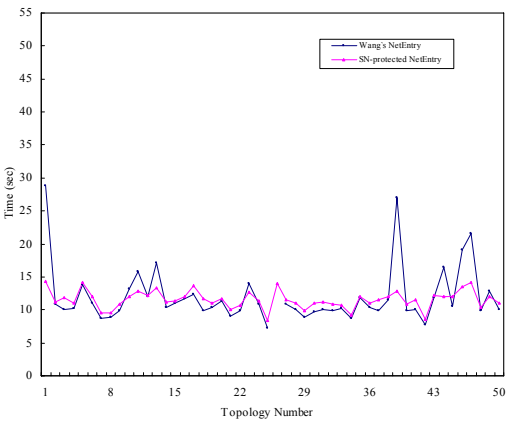


Fig. 21. Wang's Entry VS SN-protected Entry in NetEntry consumed time (50-nodescase)

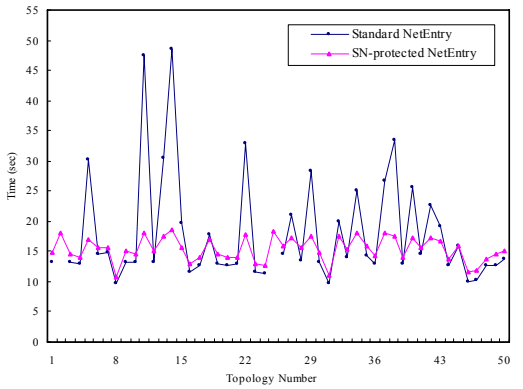


Fig. 22. Standard Entry VS SN-protected Entry in NetEntry consumed time (100-nodescase).

between Wang's NetEntry process and our proposed SN-protected NetEntry process, as same as previous situation, our proposed SN-protected NetEntry process outstands in stability.

To sum up, regardless of different network topologies, our proposed methods provide steady NetEntry consumed time compared with other methods and thus improve the stability of the NetEntry process in WiMAX mesh network.

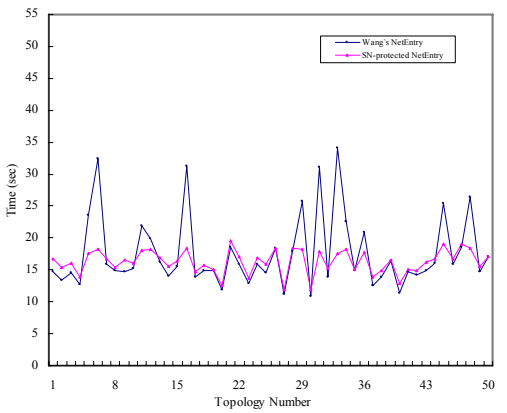


Fig. 23. Wang's Entry VS SN-protected Entry in NetEntry consumed time (100-nodescase).

Ⅶ. Conclusions

IEEE 802.16 mesh mode is a promising network to provide wireless broadband access (BWA). In the mesh mode, the network entry process (NetEntry) is the pivotal procedure for mesh network topology formulation and thus, influences the accessibility of whole mesh network.

In this paper, we describe the hidden neighbor problem, in which new neighborship emerges after a new node comes in and results in possible collisions, in the network entry process (NetEntry) of the IEEE 802.16 mesh mode. To overcome the problem, we first separated the problem into 2 phases. In the phase 1, the new node may fail to accumulate MSH-NCFG messages from neighbors. In the phase 2, two important MSH-NCFG messages sent to the new node from the SN may be blocked by its hidden neighbor. Thus, we proposed the so-called SN-protected NetEntry process, in which the two message MSH-NCFG messages are protected from possible collisions.

Simulation results show that our proposed solutions successfully address the hidden neighbor problem. Regardless of different network topologies, the consumed time of the proposed NetEntry process is more steady compared with the standard-based NetEntry process and thus the enhance the stability of the NetEntry process in IEEE 802.16 mesh networks.

References

[1] Y. Zhang, J. J. Luo, H. L. Hu, "Wireless Mesh Networking," Auerbach Publication, 270 Madison Avenue, New York, USA.

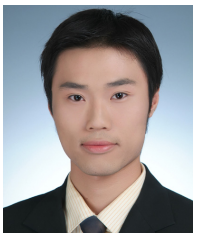
[2] IEEE Std 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks-Part 16: Air Interface for Fixed Broadband Wireless Access System," 2004.

[3] C. Cicconetti, A. Erta, L. Lenzini, and E. Mingozzi, "Performance evaluation of the mesh election procedure of IEEE 802.16/WiMAX," in Proc. ACM MSWiM, Chania, Crete Island, Greece, pp.323-327, Oct.22-26, 2007, .

[4] N. Bayer, D. Sivchenko, B. Xu, V. Rakocevic and J. Habermann, "Transmission timing of signaling messages in IEEE 802.16 based mesh networks," in Proc. Eur. Wireless, Athens, Greece, Apr. 2006.

〔5〕 S.-M. Cheng, P. Lin, D.-W. Huang, and S.-R. Yang, “A study on distributed/centralized scheduling for wireless mesh network,” in Proc. IWCMC, Vancouver, BC, Canada, pp.599-604, Jul.3-6, 2006.
〔6〕 M. Cao, V. Raghunathan, and P.R. Kumar, “A tractable algorithm for fair and efficient uplink scheduling of multihop WiMAX mesh networks,” in Proc. 2nd IEEE Workshop WiMesh, Reston, VA, pp.101-108, Sep. 25, 2006.
〔7〕 D. Kim and A. Ganz, “Fair and efficient multihop scheduling algorithm for IEEE 802.16 BWA systems,” in Proc. 2nd Int. Conf. IEEE Broadnets, Boston, MA, pp.833-839, 2005.
〔8〕 H. Shetiya and V. Sharma, “Algorithms for routing and centralized scheduling to provide QoS in IEEE 802.16 mesh networks,” in Proc. 1st ACM Workshop WMuNeP, Montreal, QC, Canada, pp.140-149, Qct. 2005.
〔9〕 M. Cao, W. Ma, Q. Zhang, X. Wang, and W. Zhu, “Modelling and performance analysis of the distributed scheduler in IEEE 802.16 mesh mode,” in Proc. 6th ACM Int. Symp. MobiHoc, Urbana-Champaign, IL, pp.78-89, May 25-27, 2005.
〔10〕 N. Bayer, B. Xu, J. Habermann, and V. Rakocevic, “Improving the performance of the distributed scheduler in IEEE 802.16 mesh networks,” in Proc. IEEE VTC-Spring, Dublin, Ireland, pp.1193-1197, Apr. 2007.
〔11〕 S. Y. Wang, C. L. Lin, K. H. Fang, adn T. W. Hsu, “Facilitating the network entry and link establishment processes of IEEE 802.16 mesh networks,” in Proc. IEEE WCNC, Hong Kong, pp.1842-1847, Mar. 11-15, 2007.
〔12〕 S. Y. Wang, C. C. Lin, H. W. Chu, T. W. Hsu, and K. H. Fang, “Improving the Performances of Distributed Coordinated Scheduling in IEEE 802.16 Mesh Networks,” in IEEE Transactions on Vehicular Technology, Vol.57, No.4, pp.2531-2547, 2008.

임 립 상 (Lin Lixiang) 준회원



2007년 6월 East China Normal University 정보통신공학과(공학사)
2008년 3월~2010년 2월 인하대학교 정보통신공학과(공학석사)

유 상 조 (Sang-Jo Yoo) 정회원

1988년 2월 한양대학교 전자통신학과(공학사)
1990년 2월 한국과학기술원 전기 및 전자공학과(공학석사)
2000년 8월 한국과학기술원 전자전산학과(공학박사)
1990년 3월~2001년 2월 KT 연구개발본부
2001년 3월~현재 인하대학교 정보통신대학원 정교수
<관심분야> 초고속 통신망, 무선 MAC 프로토콜, 인터넷 QoS, Cross-layer 프로토콜 설계, Cognitive Radio Network