UNIVERSITÀ DI PISA

FACOLTÀ DI INGEGNERIA

LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA

Dynamic Adaptation of the Distributed Election Procedure in IEEE 802.16 WMNs

Candidato:	Mirko Marino
Relatori:	Prof. Luciano Lenzini Prof. Enzo Mingozzi Ing. Claudio Cicconetti

ANNO ACCADEMICO 2007/2008

Contents

List of Figures and Tables

1 Introduction

"Commit to the LORD whatever you do,
and your plans will succeed."
— *Proverbs 16:3 (NIV)*

Wi-Fi has changed the way people navigate the Internet, and in record time. The technology, which is used to create wireless networks in small areas such as homes, offices, and parks, allows millions to move about freely while they surf the Web with laptops and PDAs. Today, the customers require the same services, but in a large scale, to access internet anywhere. WiMax responds to this need, but is more than just a faster version of Wi-Fi.

The industry trade group WiMAX ForumTM [6] has defined WiMAX as a "last mile" broadband wireless access (BWA) alternative to cable modem service, telephone company Digital Subscriber Line (DSL) or T1/E1 service.

What makes WiMAX so exciting is the broad range of applications it makes possible but not limited to broadband internet access, T1/E1 substitute for businesses, voice over Internet protocol (VoIP) as telephone company substitute, Internet Protocol Television (IPTV) as cable TV substitute, backhaul for Wi-Fi hotspots and cell phone towers, mobile telephone service, mobile data TV, mobile emergency response services, wireless backhaul as substitute for fiber optic cable.

WiMax IEEE 802.16 include a mesh mode operation. Wireless mesh networks (WMNs) are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity. WMNs are comprised of two types of nodes: mesh routers and mesh clients. Other than the routine capability for gateway/bridge functions as in a conventional wireless router, a mesh router contains additional routine functions to support mesh networking.

Through multi-hop communications, the same coverage can be achieved by a mesh router with much lower transmission power. To further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. Mesh routers have minimal mobility and form the mesh backbone for mesh clients. Thus, although mesh clients can also work as a router for mesh networking, the hardware platform and software for them can be much simpler than those for mesh routers. In addition to mesh networking among mesh routers and mesh clients, the gateway/bridge functionalities in mesh routers enable the integration of WMNs with various other networks. Thus, WMNs will greatly help users to be always-on-line anywhere, anytime.

The characteristics of WMNs are outlined below, where the hybrid[1] architecture is considered for WMNs, since it comprises all the advantages of WMNs:

- WMNs support ad hoc networking, and have the capability of self-forming, self-healing, and self-organization.
- WMNs are multi-hop wireless networks, but with a wireless infrastructure/backbone provided by mesh routers.
- Mesh routers have minimal mobility and perform dedicated routing and configuration, which significantly decreases the load of mesh clients and other end nodes.
- Mobility of end nodes is supported easily through the wireless infrastructure.
- Mesh routers integrate heterogeneous networks, including both wired and wireless. Thus, multiple types of network access exist in WMNs.
- Power-consumption constraints are different for mesh routers and mesh clients.
- WMNs are not stand-alone and need to be compatible and interoperable with other wireless networks.

In this work, we propose two algorithms (AIMD[2] and MIAD[3]) to dynamically adapt the Mesh Election Procedure of a Wireless Mesh Network using IEEE 802.16 mesh. The

[1] Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients.

[2] Additive Increase Multiplicative Decrease

aim is to allows a more complete self-configuration of the mesh routers. Therefore the two algorithms are deeply analyzed to test the effective functioning and to evaluate the performance through exhaustive simulations. We proposed two algorithms due to the results obtained from the AIMD's simulations that led us to develop MIAD.
Finally we analyze the behaviour through simulations with bursty traffic.

[3] Multiplicative Increase Additive Decrease

2 Standard IEEE 802.16

> "Do not let this Book of the Law depart from your
> mouth; meditate on it day and night, so that you
> may be careful to do everything written in it.
> Then you will be prosperous and successful."
> — *Joshua 1:8 (NIV)*

Commonly referred to as *WiMAX* or less commonly as *WirelessMAN™* or the *Air Interface Standard*, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (*MANs*). Published on April 8, 2002, the standard defines the use of bandwidth between the licensed 10GHz and 66GHz and between the 2GHZ and 11GHz frequency ranges and defines a MAC layer that supports multiple physical layer specifications customized for the frequency band of use and their associated regulations. 802.16 supports very high bit rates in both uploading to and downloading from a base station up to a distance of 30 miles to handle such services as VoIP, IP connectivity and TDM voice and data.

As currently defined through IEEE Standard 802.16, a wireless MAN provides network access to buildings through exterior antennas communicating with central radio base stations (*BSs*).

The stations with which a station has direct links are called neighbours and shall form a neighbourhood. A node's neighbours are considered to be "one hop" away from the node. A two-hop extended neighbourhood contains, additionally, all the neighbours of the neighbourhood.

The wireless MAN offers an alternative to cabled access networks, such as fiber optic links, coaxial systems using cable modems, and digital subscriber line (DSL) links. Because wireless systems have the capacity to address broad geographic areas without the costly infrastructure development required in deploying cable links to individual sites, the technology may prove less expensive to deploy and may lead to more ubiquitous broadband access. WirelessMAN technology bringing the network to a building, users inside the building will connect to it with conventional in-building networks such as, for data, Ethernet (*IEEE Standard 802.3*) or wireless LANs (*IEEE Standard 802.11*). However, the fundamental design of the standard may eventually allow for the efficient extension of the WirelessMAN networking protocols directly to the individual user.

The standard is intended to allow for multiple vendors to produce interoperable equipment. However, it also allows for extensive vendor differentiation.

Development of IEEE Standard 802.16 and the included WirelessMAN™ air interface, along with associated standards and amendments, is the responsibility of IEEE Working Group 802.16 on *Broadband Wireless Access* (*BWA*) Standards [1].

Historically, the 802.16 activities were initiated at an August 1998 meeting called by the National Wireless Electronics Systems Testbed (N-WEST) of the U.S. National Institute of Standards and Technology.

2.1 MAC (Medium Access Control)

The IEEE 802.16 MAC protocol was designed for point-to-multipoint broadband wireless access applications. It addresses the need for very high bit rates, both uplink (to the BS) and downlink (from the BS). Access and bandwidth allocation algorithms must accommodate hundreds of terminals per channel, with terminals that may be shared by multiple end users. The request-grant mechanism is designed to be scalable, efficient, and self-correcting.

The MAC includes S*ervice-Specific Convergence Sublayers* (*CS*) that interface to higher layers, above the core MAC common part sublayer that carries out the key MAC functions.

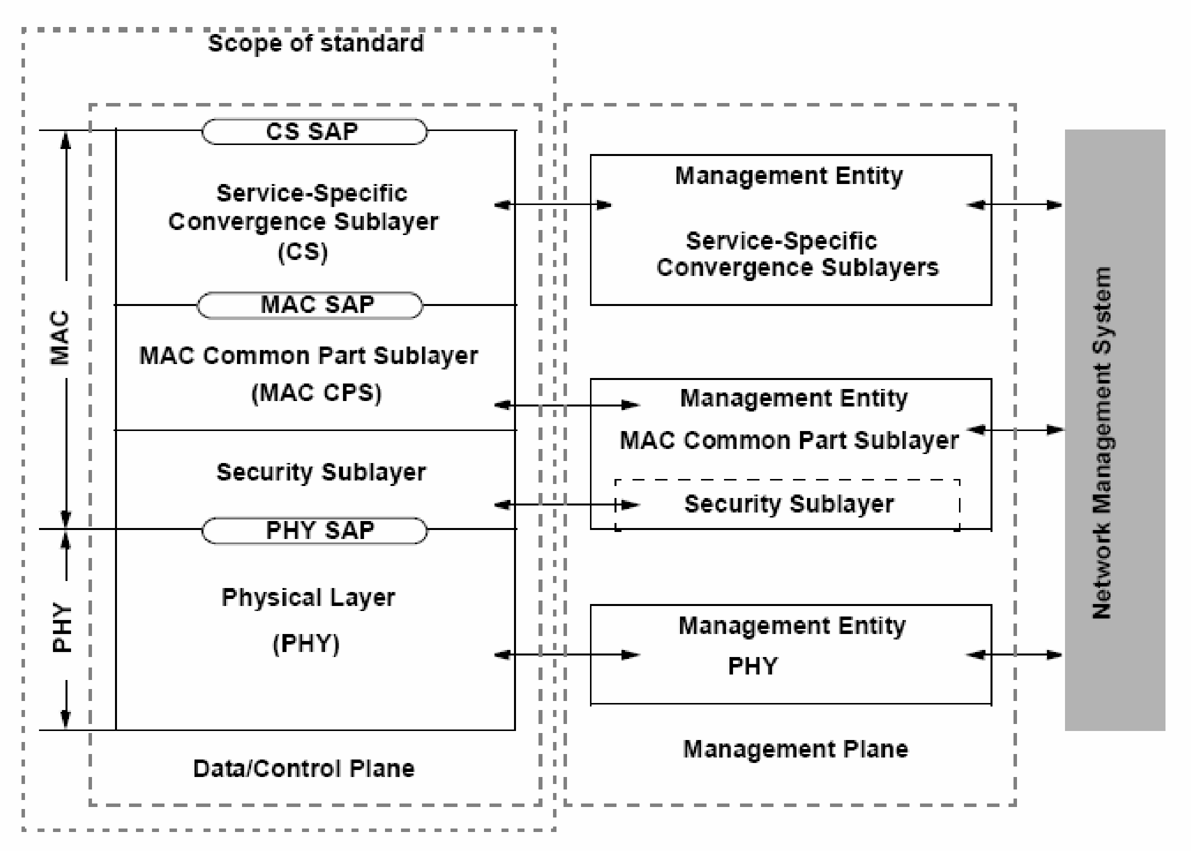


FIGURE 2.1 – IEEE STD 802.16 PROTOCOL LAYERING.

The Service-Specific Convergence Sublayer provides any transformation or mapping of external network data, received through the *CS Service Access Point* (*SAP*), into *MAC*

SDUs received by the *MAC Common Part Sublayer* (*CPS*) through the MAC SAP. This includes classifying external network *Service Data Units* (*SDUs*) and associating them to the proper MAC *Service Flow Identifier* (*SFID*) and C*onnection Identifier* (*CID*). It may also include such functions as P*ayload Header Suppression* (*PHS*). Multiple CS specifications are provided for interfacing with various protocols. The internal format of the CS payload is unique to the CS, and the MAC CPS is not required to understand the format of or parse any information from the CS payload.

The MAC CPS provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance. It receives data from the various CSs, through the MAC SAP, classified to particular MAC connections.

IEEE Standard 802.16 defines two general service-specific convergence sublayers for mapping services to and from 802.16 MAC connections:

- *ATM convergence sublayer*: it is defined for ATM services.
- *Packet convergence sublayer*: it is defined for mapping packet services such as IPv4, IPv6, Ethernet, and virtual local area network (*VLAN*).

The primary task of the sublayer is to classify service data units to the proper MAC connection, preserve or enable QoS, and enable bandwidth allocation. The MAC also contains a separate security sublayer providing authentication, secure key exchange, and encryption.

CS provides a mechanism for requesting bandwidth, associating QoS and traffic parameters, transporting and routing data to the appropriate convergence sublayer, and all other actions associated with the contractual terms of the service.

Connections are referenced with 16-bit connection identifiers and may require continuously granted bandwidth or bandwidth on demand.

Each SS has a standard 48-bit MAC address, but this serves mainly as an equipment identifier, since the primary addresses used during operation are the CIDs. Upon entering the network, the SS is assigned three management connections in each direction. These three connections reflect the three different QoS requirements used by different management levels.

The PHY definition includes multiple specifications, each appropriate to a particular frequency range and application.

2.1.1 Service-Specific CS

The service-specific CS resides on top of the MAC CPS and utilizes, via the MAC SAP, the services provided by the MAC CPS.

The CS performs the following functions utilizing the services of the MAC:

- Accepting higher-layer *Protocol Data Units* (*PDUs*).
- Performing classification of PDUs into the appropriate connection.
- Processing (if required) the PDUs based on the classification.
- Suppression of payload header information (optional).
- Delivering CS PDUs to the appropriate MAC SAP associated with the service flow for transport to the peer MAC SAP.
- Receiving CS PDUs from the peer entity.
- Rebuilding of any suppressed payload header information (optional).

The sending CS is responsible for delivering the MAC SDU to the MAC SAP. The MAC is responsible for delivery of the MAC SDU to peer MAC SAP in accordance with the QoS, fragmentation, concatenation, and other transport functions associated with a particular connection's service flow characteristics. The receiving CS is responsible for accepting the MAC SDU from the peer MAC SAP and delivering it to a higher-layer entity.

The packet CS is used for transport for all packet-based protocols such as *Internet Protocol* (*IP*), *Point-to-Point Protocol* (*PPP*), and *IEEE Std 802.3* (*Ethernet*).

2.1.2 MAC SDU Formats

Once classified and associated with a specific MAC connection, higher-layer PDUs shall be encapsulated in the MAC SDU format as illustrated in Figure 2.2. The 8-bit

Payload Header Suppression Index (*PHSI*) field shall be present when a *Payload Header Suppression* (*PHS*) rule has been defined for the associated connection.

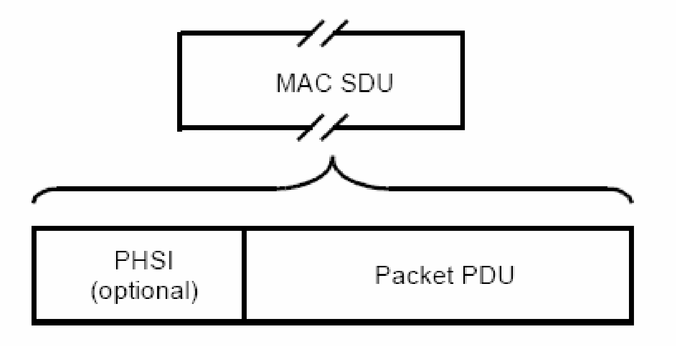


FIGURE 2.2 – MAC SDU FORMAT.

MAC SDU is mapped onto a particular connection for transmission between MAC peers. The mapping process associates a MAC SDU with a connection, which also creates an association with the service flow characteristics of that connection. This process facilitates the delivery of MAC SDUs with the appropriate QoS constraints.

2.1.3 MAC PDU Formats

The MAC PDU is the data unit exchanged between the MAC layers of the BS and its SSs.

A MAC PDU consists of:

- A fixed-length *MAC header*.
- A variable-length *payload*. If present, the payload shall consist of zero or more subheaders and zero or more MAC SDUs and/or fragments thereof. The payload information may vary in length, so that a MAC PDU may represent a variable number of bytes. This allows the MAC to tunnel various higher-layer traffic types without knowledge of the formats or bit patterns of those messages.
- An optional C*yclic Redundancy Check* (CRC).

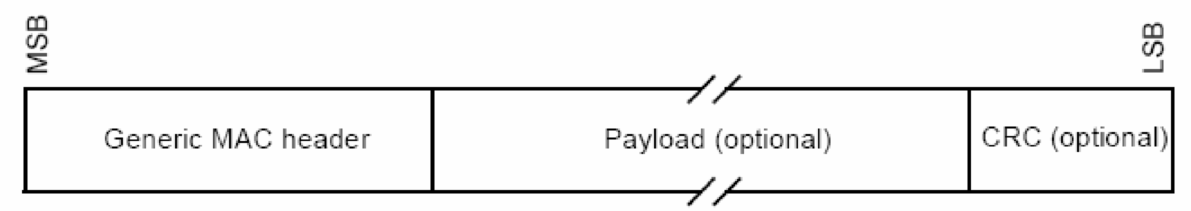


FIGURE 2.3 – MAC PDU FORMAT.

Fields specified as SDUs or SDU fragments (for example, MAC PDU payloads) are transmitted in the same order of bytes as received from upper layers.

Multiple MAC PDUs may be concatenated into a single transmission in either the uplink or downlink directions. Figure 2.4 illustrates this concept for an uplink burst transmission.

Since each MAC PDU is identified by a unique CID, the receiving MAC entity is able to present the MAC SDU (after reassembling the MAC SDU from one or more received MAC PDUs) to the correct instance of the MAC SAP. MAC Management messages, user data, and bandwidth request MAC PDUs may be concatenated into the same transmission.

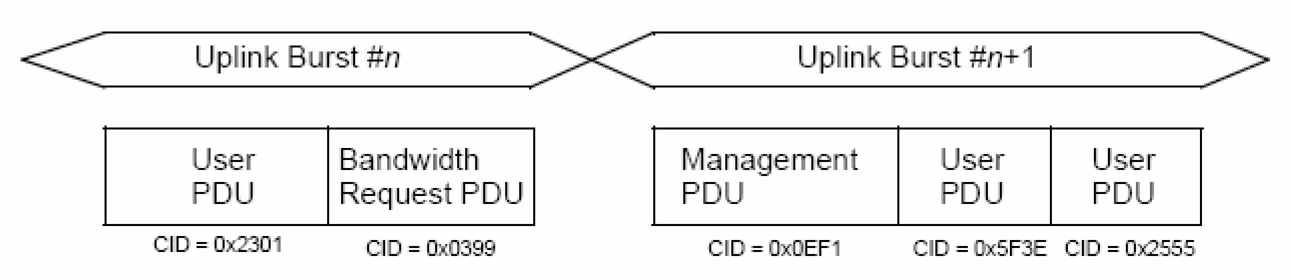


FIGURE 2.4– MAC PDU CONCATENATION SHOWING EXAMPLE CIDS.

2.2 MAC Common Part Sublayer

A network that utilizes a shared medium (the space through which the radio waves propagate) shall provide an efficient sharing mechanism. The 802.16 standard specifies two modes for sharing the wireless medium: *point-to-multipoint* (*PMP*) and *mesh* (optional).

2.2.1 PMP (Point-to-MultiPoint)

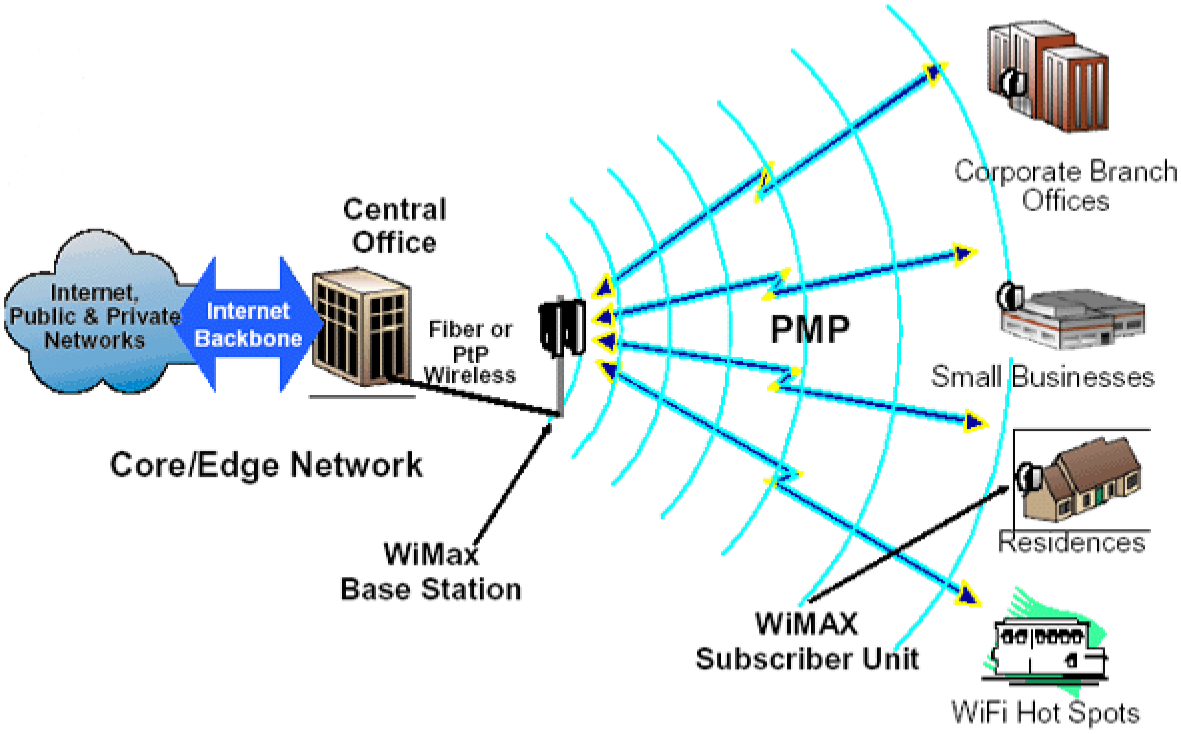


FIGURE 2.5 – POINT TO POINT AND POINT TO MULTIPOINT CONFIGURATIONS.

One base station can service hundreds of dissimilar subscribers in terms of bandwidth and services offered.

With PMP, the BS serves a set of SSs within the same antenna sector in a broadcast manner, within a given frequency channel and antenna sector, all stations receive the same transmission, or parts thereof. Transmissions from SSs are directed to and centrally coordinated by the BS.

The BS is the only transmitter operating in downlink, so it transmits without having to coordinate with other stations, except for the overall *time division duplexing* (*TDD*) that may divide time into uplink and downlink transmission periods.

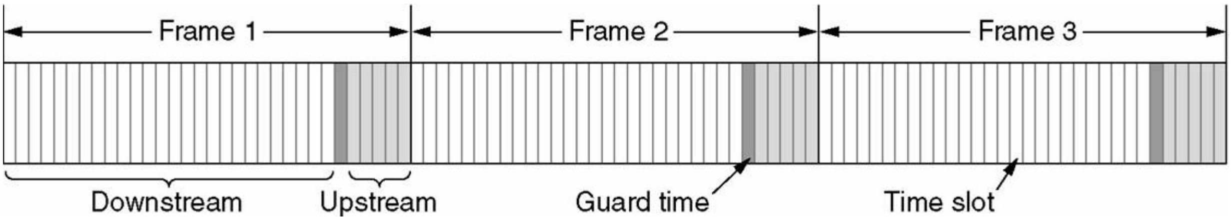


FIGURE 2.6 – TIME DIVISION DUPLEXING.

In the downlink (from BS to SS) subframe, the BS transmits a burst of MAC protocol data units (PDUs). Since the transmission is broadcast, all SSs listen to the data transmitted by the BS. In cases where the *DL-MAP* does not explicitly indicate that a portion of the downlink subframe is for a specific SS, all SSs capable of listening to that portion of the downlink subframe shall listen. The SSs check the CIDs in the received PDUs and retain only those PDUs addressed to them.

In the uplink (from SS to BS) any SS transmits a burst of MAC PDUs to the BS in a *time-division multiple access* (*TDMA*) manner. Based on measurements at the physical layer, any SS adapts over time the *Interval Usage Code* (*IUC*) in use, that is, modulation, rate, and *Forward Error Correction* (*FEC*) scheme, for both downlink (downlink *IUC*, *DIUC*) and uplink (uplink *IUC*, *UIUC*) transmissions.

Downlink and uplink subframes are duplexed using one of the following techniques:

- *Frequency-division duplex* (*FDD*) is where downlink and uplink subframes occur simultaneously on separate frequencies.

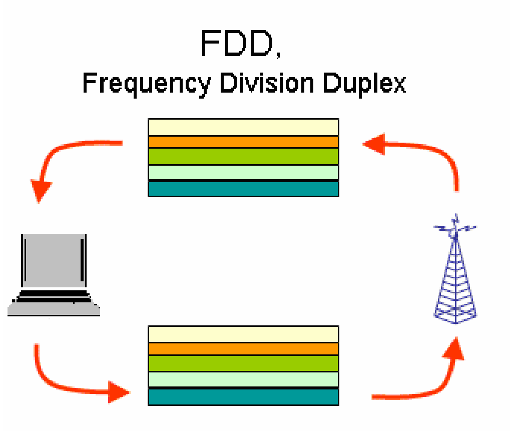


FIGURE 2.7 – FDD.

- *Time-division duplex* (*TDD*) is where downlink and uplink subframes occur at different times and usually share the same frequency.

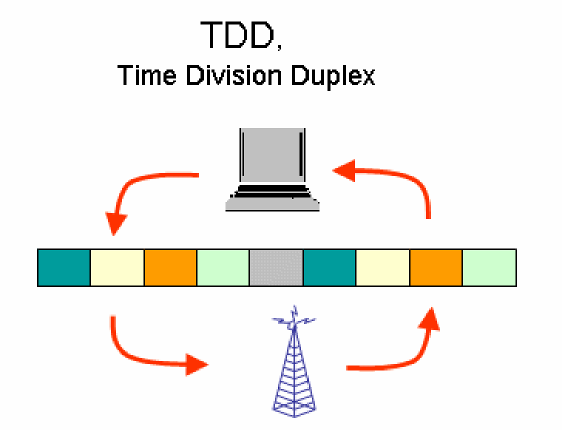


FIGURE 2.8 – TDD.

Sometimes FDD and TDD are simultaneously. Both TDD and FDD alternatives support adaptive burst profiles in which modulation and coding options may be dynamically assigned on a burst-by-burst basis.

SSs can be either *full duplex* (i.e., they can transmit and receive simultaneously) or *half-duplex* (i.e., they can transmit and receive at nonoverlapping time intervals).

The MAC protocol is connection-oriented: all data communications, for both transport and control, are in the context of a unidirectional connection.

At the start of each frame, the BS schedules the uplink and downlink grants in order to meet the negotiated QoS requirements. Each SS learns the boundaries of its allocation within the current uplink subframe by decoding the *UL-MAP* message.

The downlink subframe starts with a frame control section that contains the *DL-MAP* for the current downlink frame; this message contains the timetable of the downlink grants, as well as the UL-MAP for a specified time in the future.

DL-MAP and UL-MAP are transmitted by the BS at the beginning of each downlink subframe for both FDD and TDD modes.

The downlink map specifies when physical layer transitions (modulation and FEC changes) occur within the downlink subframe. The downlink subframe typically contains a TDM portion immediately following the frame control section.

In FDD systems, the TDM portion may be followed by a TDMA segment that includes an extra preamble at the start of each new burst profile. This feature allows better support of half-duplex SSs. In an efficiently scheduled FDD system with many half-duplex SSs, some may need to transmit earlier in the frame than they receive. Due to their half-duplex nature, these SSs lose synchronization with the downlink; the TDMA preamble allows them to regain synchronization.

The SSs transmit in their assigned allocation using the burst profile specified by the *Uplink Interval Usage Code* (*UIUC*) in the UL-MAP entry granting them bandwidth.

The downlink subframe is shown in Figure 2.9 and the uplink subframe is show in Figure 2.10.

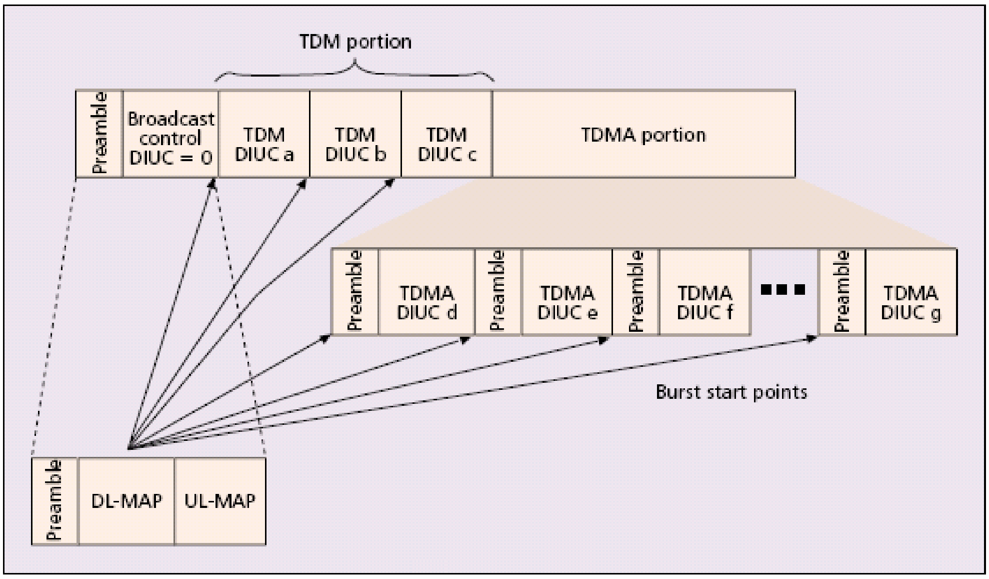


FIGURE 2.9 – DOWNLINK SUBFRAME STRUCTURE.

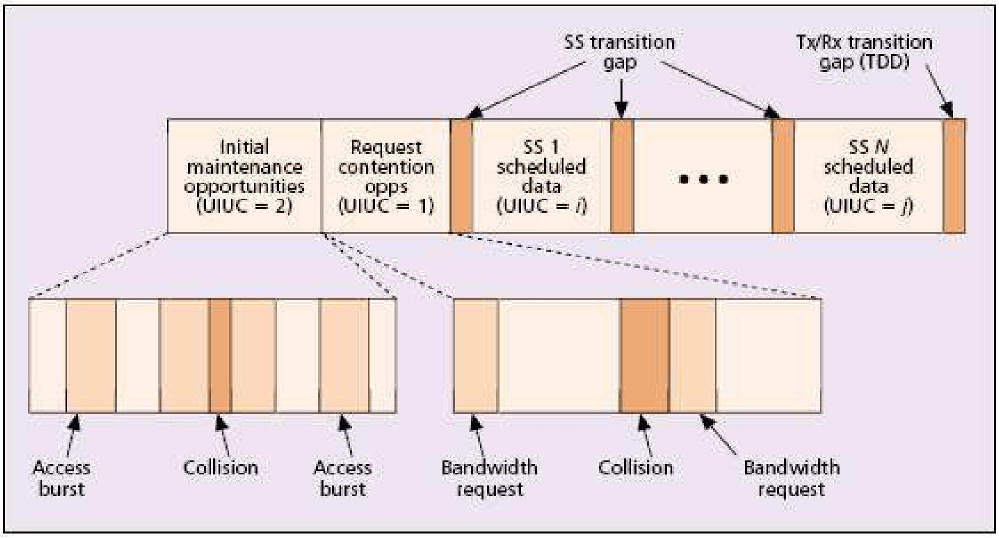

SS transition gap
Tx/Rx transition gap (TDD)
Initial maintenance opportunities (UIUC = 2)
Request contention opps (UIUC = 1)
SS 1 scheduled data (UIUC = i)
SS N scheduled data (UIUC = j)
Access burst
Collision
Access burst
Bandwidth request
Collision
Bandwidth request

FIGURE 2.10 – UPLINK SUBFRAME STRUCTURE.

For the purposes of mapping to services on SSs and associating varying levels of QoS, all data communications are in the context of a connection. Service flows may be provisioned when an SS is installed in the system. Shortly after SS registration, connections are associated with these service flows (one connection per service flow) to provide a reference against which to request bandwidth.

Additionally, new connections may be established when a customer's service needs change. A connection defines both the mapping between peer convergence processes that utilize the MAC and a service flow. The service flow defines the QoS parameters for the PDUs that are exchanged on the connection.

The concept of a service flow on a connection is central to the operation of the MAC protocol. Service flows provide a mechanism for uplink and downlink QoS management. An SS requests uplink bandwidth on a per connection basis (implicitly identifying the service flow). Bandwidth is granted by the BS to an SS as an aggregate of grants in response to per connection requests from the SS.

Since the BS controls the access to the medium in the uplink direction, bandwidth is granted to SSs on demand. For this purpose, a number of different bandwidth-request mechanisms have been specified:

- *Unsolicited granting*: a fixed amount of bandwidth on a periodic basis is requested during the setup phase of an uplink connection. After that phase, bandwidth is never explicitly requested.
- *Unicast poll*: consists of allocating to a polled uplink connection the bandwidth needed to transmit a bandwidth request. If the polled connection has no data awaiting transmission or if it has already requested bandwidth for all of its backlog, it will not reply to the unicast poll, which is thus wasted.
- *Broadcast polls*: are issued by the BS to all uplink connections. The main drawback in this mechanism is that a collision occurs whenever two or more uplink connections send a bandwidth request by responding to the same poll, in which case a truncated binary exponential backoff algorithm is employed.
- *Piggybacked on a PDU*: this mechanism is effective only if the connection has some backlog for which bandwidth reservation has already been issued.

The 802.16 MAC specifies four different scheduling services in order to meet the QoS requirements of multimedia applications:

- *Unsolicited grant service* (*UGS*).
- *Real-time polling service* (*rtPS*).

- *Non-real-time polling service* (*nrtPS*).
- *Best effort* (*BE*).

Each scheduling service is characterized by a mandatory set of QoS parameters, which is tailored to best describe the guarantees required by the applications.

Each SS shall have a 48-bit universal MAC address; this address uniquely defines the SS from within the set of all possible vendors and equipment types. It is used during the initial ranging process to establish the appropriate connections for an SS. It is also used as part of the authentication process by which the BS and SS each verify the identity of the other.

Connections are identified by a 16-bit CID. The message dialogs provide three CID values. The same CID value is assigned to both members (uplink and downlink) of each connection pair. The use of a 16-bit CID permits a total of 64K connections within each downlink and uplink channel.

The CID can be considered a connection identifier even for nominally connectionless traffic like IP, since it serves as a pointer to destination and context information. Requests for transmission are based on these CIDs, since the allowable bandwidth may differ for different connections, even within the same service type. The type of service and other current parameters of a service are implicit in the CID; they may be accessed by a lookup indexed by the CID.

At SS initialization, two pairs of management connections (uplink and downlink) shall be established between the SS and the BS and a third pair of management connections may be optionally generated. The three pairs of connections reflect the fact that there are inherently three different levels of QoS for management traffic between an SS and the BS.

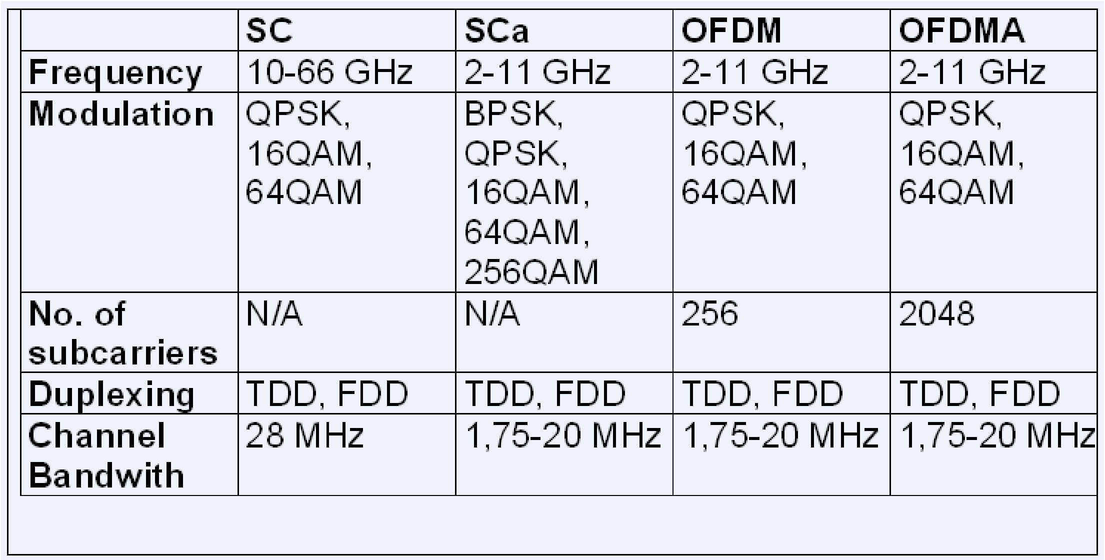
- *Basic connection*: is used by the BS MAC and SS MAC to exchange short, time-urgent MAC management messages.
- *Primary management connection*: is used by the BS MAC and SS MAC to exchange longer, more delay-tolerant MAC management messages.

- *Secondary management*: *connection* is used by the BS and SS to transfer delay tolerant, standards-based messages:
    - *Dynamic Host Configuration Protocol* (*DHCP*).
    - *Trivial File Transfer Protocol* (*TFTP*).
    - *SNMP*.
    - Etc.

  These messages are carried in IP datagrams and they may be packed and/or fragmented.

Air interface specifications are:

- *WirelessMAN-SC2*: uses a single-carrier modulation format.
- *WirelessMAN-OFDM*: uses orthogonal frequency-division multiplexing with a 256-point transform. Access is by TDMA. This air interface is mandatory for license exempt bands.
- *WirelessMAN-OFDMA*: uses orthogonal frequency-division multiple access with a 2048-point transform. In this system, multiple access is provided by addressing a subset of the multiple carriers to individual receivers.



	SC	**SCa**	**OFDM**	**OFDMA**
Frequency	10-66 GHz	2-11 GHz	2-11 GHz	2-11 GHz
Modulation	QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM, 256QAM	QPSK, 16QAM, 64QAM	QPSK, 16QAM, 64QAM
No. of subcarriers	N/A	N/A	256	2048
Duplexing	TDD, FDD	TDD, FDD	TDD, FDD	TDD, FDD
Channel Bandwith	28 MHz	1,75-20 MHz	1,75-20 MHz	1,75-20 MHz

FIGURE 2.11 – AIR INTERFACE SPECIFICATIONS.

Use of the secondary management connection is required only for managed SS.
For the SCa, OFDM, and OFDMA PHY layers, management messages shall have CRC.

Connections, once established, may require active maintenance. The maintenance requirements vary depending upon the type of service connected.

Finally, connections may be terminated. This generally occurs only when a customer's service contract changes. The termination of a connection is stimulated by the BS or SS.

2.2.2 MESH Networks

In mesh mode, traffic can be routed through other SSs and can occur directly among SSs. Access coordination is distributed among the SSs. Depending on the transmission protocol algorithm used, this can be done on the basis of equality using distributed scheduling, or on the basis of superiority of the Mesh BS, which effectively results in centralized scheduling, or on a combination of both.

Distributed scheduling:
All the nodes including the Mesh BS shall coordinate their transmissions in their two-hop neighborhood and shall broadcast their schedules (available resources, requests and grants) to all their neighbors. Optionally the schedule may also be established by directed uncoordinated requests and grants between two nodes. Nodes shall ensure that the resulting transmissions do not cause collisions with the data and control traffic scheduled by any other node in the two-hop neighborhood. There is no difference in the mechanism used in determining the schedule for downlink and uplink.

Centralized scheduling:
Resources are granted in a more centralized manner. The Mesh BS shall gather resource requests from all the Mesh SSs within a certain hop range. It shall determine

the amount of granted resources for each link in the network both in downlink and uplink, and communicates these grants to all the Mesh SSs within the hop range. The grant messages do not contain the actual schedule, but each node shall compute it by using the predetermined algorithm with given parameters.

All the communications are in the context of a link, which is established between two nodes. One link shall be used for all the data transmissions between the two nodes. QoS is provisioned over links on a message-by-message basis. No service or QoS parameters are associated with a link, but each unicast message has service parameters in the header. Traffic classification and flow regulation are performed at the ingress node by upper-layer classification/regulation protocol. The service parameters associated with each message shall be communicated together with the message content via the MAC SAP.

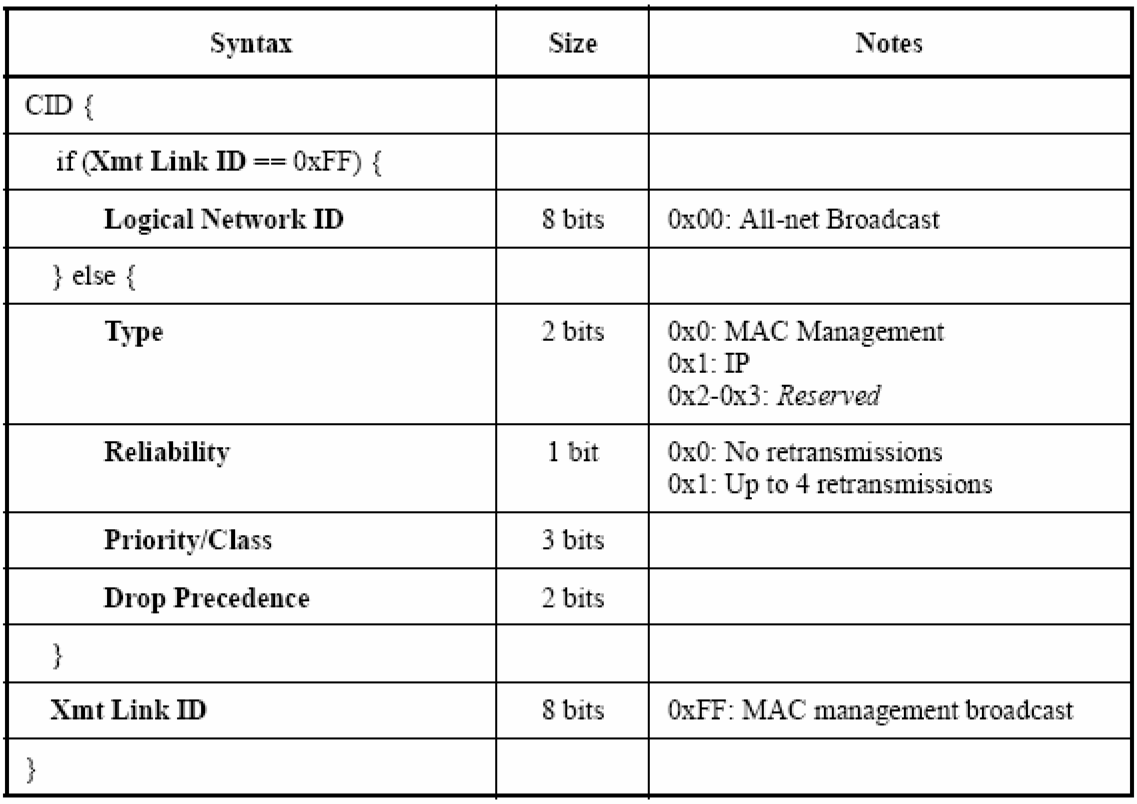
Mesh systems typically use omnidirectional antennas, but can also be co-located using sector antennas. At the edge of the coverage area of the Mesh network, where only a connection to a single point is needed, even highly directional antennas can be used.

Each node shall have a 48-bit universal MAC address, as defined in IEEE Std 802-2001. The address uniquely defines the node from within the set of all possible vendors and equipment types. This address is used during the network entry process and as part of the authorization process by which the candidate node and the network verify the identity of each other.

When authorized to the network the candidate node shall receive a 16-bit node identifier (*Node ID*) upon a request to the Mesh BS. Node ID is the basis for identifying nodes during normal operation. The Node ID is transferred in the Mesh subheader, which follows the generic MAC header, in both unicast and broadcast messages.

For addressing nodes in the local neighbourhood, 8-bit link identifiers (*Link IDs*) shall be used. Each node shall assign an ID for each link it has established to its neighbours. The Link IDs are communicated during the Link Establishment process as neighbouring nodes establish new links. The Link ID is transmitted as part of the CID in the generic MAC header in unicast messages. The Link IDs shall be used in distributed scheduling to identify resource requests and grants. Since these messages are broadcast, the receiver nodes can determine the schedule using the transmitter's Node ID in the Mesh subheader, and the Link ID in the payload of the *MSH-DSCH* (*Mesh Mode Schedule with Distributed Scheduling*) message.

The Connection ID in Mesh mode is specified as shown in Table 2.12 to convey broadcast/unicast, service parameters, and the link identification.



Syntax	Size	Notes
CID {		
if (Xmt Link ID == 0xFF) {		
Logical Network ID	8 bits	0x00: All-net Broadcast
} else {		
Type	2 bits	0x0: MAC Management 0x1: IP 0x2-0x3: *Reserved*
Reliability	1 bit	0x0: No retransmissions 0x1: Up to 4 retransmissions
Priority/Class	3 bits	
Drop Precedence	2 bits	
}		
Xmt Link ID	8 bits	0xFF: MAC management broadcast
}		

TABLE 2.12 – MESH CID CONSTRUCTION.

- *Priority/Class*: priority field indicates message class.
- *Drop Precedence*: messages with larger Drop Precedence shall have higher dropping likelihood during congestion.

2.3 MAC Management messages

MAC Management messages shall be carried in the payload of the MAC PDU. All MAC Management messages begin with a *Management Message Type* field and may contain additional fields. MAC Management messages on the Basic, Broadcast, and Initial Ranging connections shall neither be fragmented nor packed. MAC Management messages on the Primary Management Connection may be packed and/or fragmented.

For the SCa, OFDM, and OFDMA PHY layers, management messages carried on the Initial Ranging, Broadcast, Basic, and Primary Management connections shall have CRC usage enabled. The format of the Management message is given in Figure 2.13.

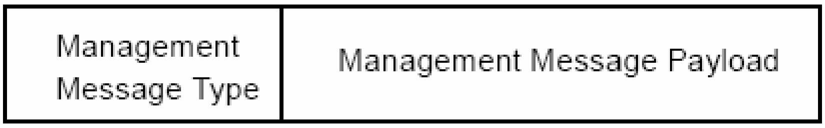
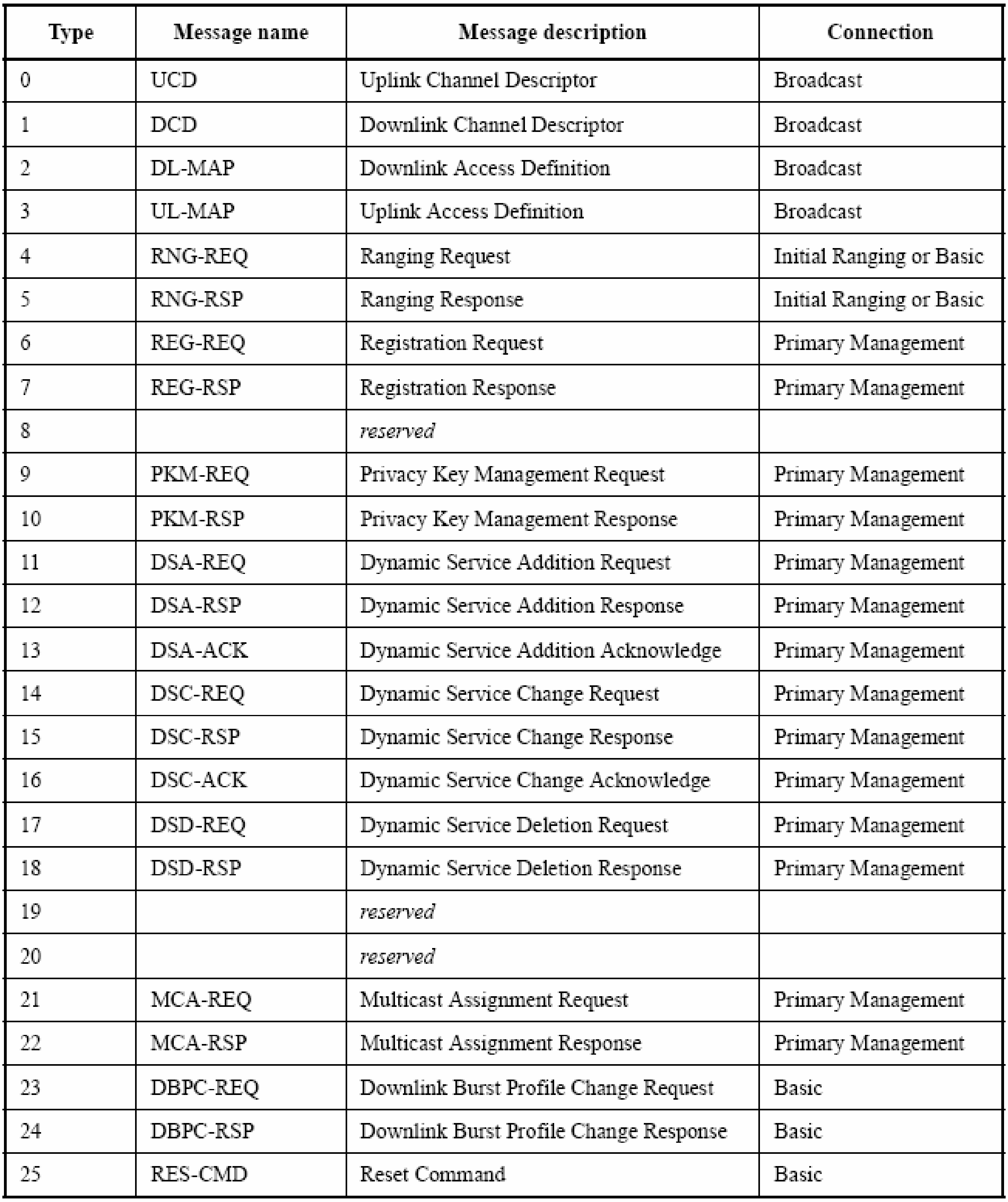


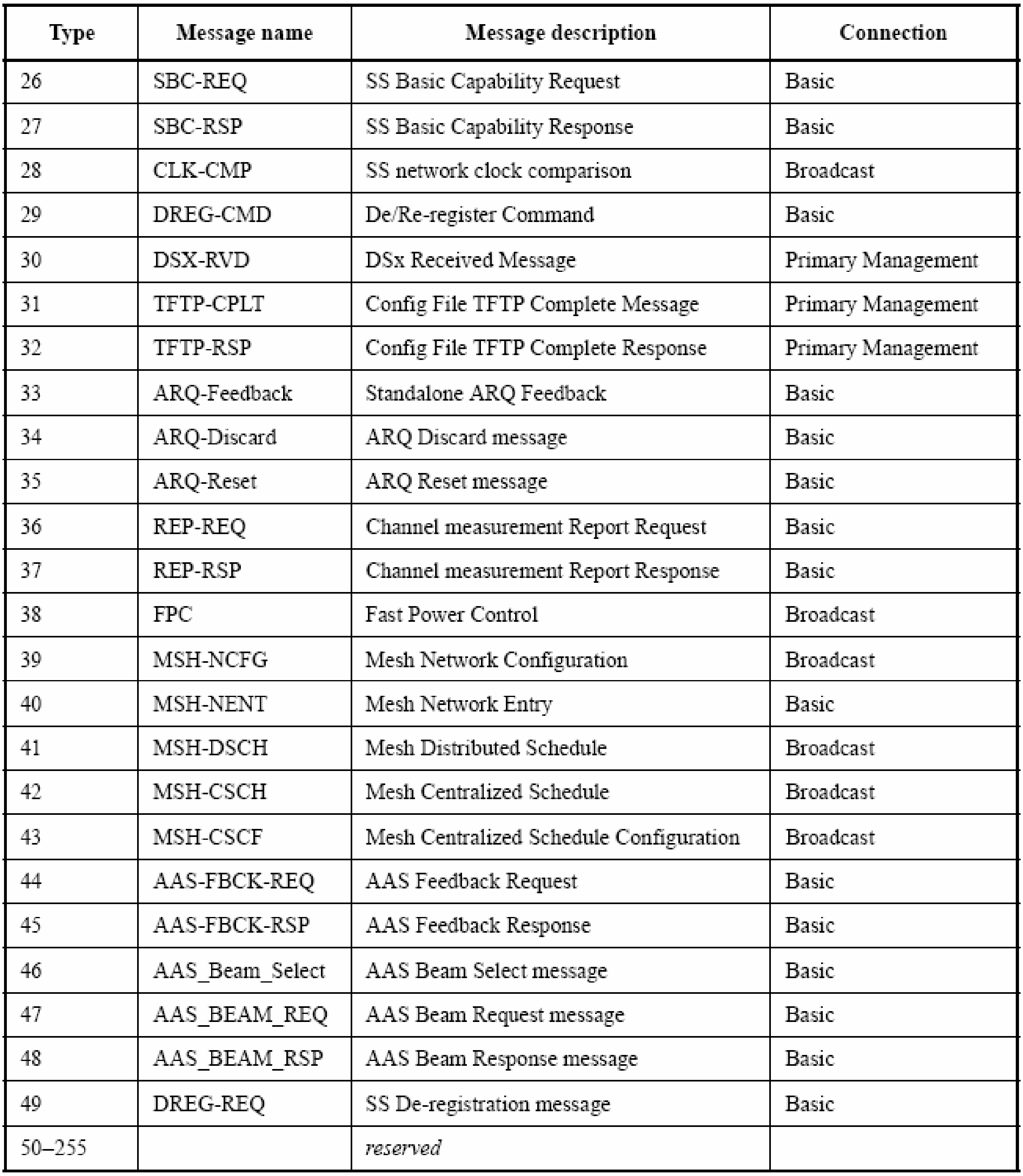
FIGURE 2.13 – MAC MANAGEMENT MESSAGE FORMAT.

The encoding of the Management Message Type field is given in Table 2.14 and 2.15.



Type	Message name	Message description	Connection
0	UCD	Uplink Channel Descriptor	Broadcast
1	DCD	Downlink Channel Descriptor	Broadcast
2	DL-MAP	Downlink Access Definition	Broadcast
3	UL-MAP	Uplink Access Definition	Broadcast
4	RNG-REQ	Ranging Request	Initial Ranging or Basic
5	RNG-RSP	Ranging Response	Initial Ranging or Basic
6	REG-REQ	Registration Request	Primary Management
7	REG-RSP	Registration Response	Primary Management
8		*reserved*	
9	PKM-REQ	Privacy Key Management Request	Primary Management
10	PKM-RSP	Privacy Key Management Response	Primary Management
11	DSA-REQ	Dynamic Service Addition Request	Primary Management
12	DSA-RSP	Dynamic Service Addition Response	Primary Management
13	DSA-ACK	Dynamic Service Addition Acknowledge	Primary Management
14	DSC-REQ	Dynamic Service Change Request	Primary Management
15	DSC-RSP	Dynamic Service Change Response	Primary Management
16	DSC-ACK	Dynamic Service Change Acknowledge	Primary Management
17	DSD-REQ	Dynamic Service Deletion Request	Primary Management
18	DSD-RSP	Dynamic Service Deletion Response	Primary Management
19		*reserved*	
20		*reserved*	
21	MCA-REQ	Multicast Assignment Request	Primary Management
22	MCA-RSP	Multicast Assignment Response	Primary Management
23	DBPC-REQ	Downlink Burst Profile Change Request	Basic
24	DBPC-RSP	Downlink Burst Profile Change Response	Basic
25	RES-CMD	Reset Command	Basic

TABLE 2.14 – MAC MANAGEMENT MESSAGES.

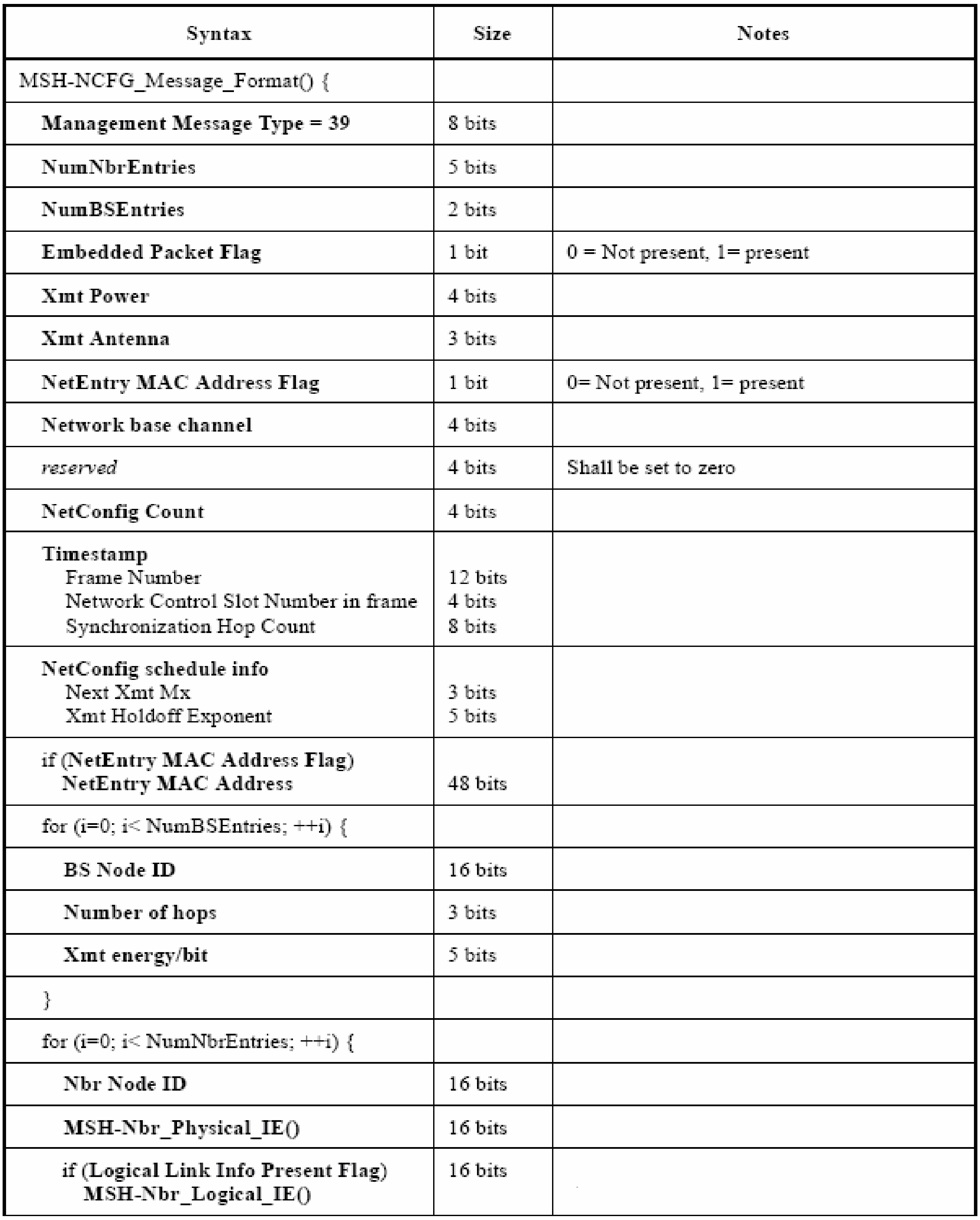


Type	Message name	Message description	Connection
26	SBC-REQ	SS Basic Capability Request	Basic
27	SBC-RSP	SS Basic Capability Response	Basic
28	CLK-CMP	SS network clock comparison	Broadcast
29	DREG-CMD	De/Re-register Command	Basic
30	DSX-RVD	DSx Received Message	Primary Management
31	TFTP-CPLT	Config File TFTP Complete Message	Primary Management
32	TFTP-RSP	Config File TFTP Complete Response	Primary Management
33	ARQ-Feedback	Standalone ARQ Feedback	Basic
34	ARQ-Discard	ARQ Discard message	Basic
35	ARQ-Reset	ARQ Reset message	Basic
36	REP-REQ	Channel measurement Report Request	Basic
37	REP-RSP	Channel measurement Report Response	Basic
38	FPC	Fast Power Control	Broadcast
39	MSH-NCFG	Mesh Network Configuration	Broadcast
40	MSH-NENT	Mesh Network Entry	Basic
41	MSH-DSCH	Mesh Distributed Schedule	Broadcast
42	MSH-CSCH	Mesh Centralized Schedule	Broadcast
43	MSH-CSCF	Mesh Centralized Schedule Configuration	Broadcast
44	AAS-FBCK-REQ	AAS Feedback Request	Basic
45	AAS-FBCK-RSP	AAS Feedback Response	Basic
46	AAS_Beam_Select	AAS Beam Select message	Basic
47	AAS_BEAM_REQ	AAS Beam Request message	Basic
48	AAS_BEAM_RSP	AAS Beam Response message	Basic
49	DREG-REQ	SS De-registration message	Basic
50–255		*reserved*	

TABLE 2.15 – MAC MANAGEMENT MESSAGES (CONTINUED).

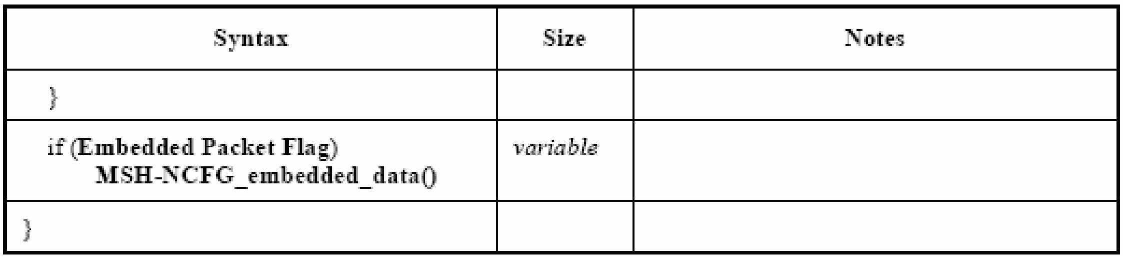
2.3.1 MSH-NCFG message

MSH-NCFG messages provide a basic level of communication between nodes in different nearby networks whether from the same or different equipment vendors or wireless operators. All the nodes (BS and SS) in the Mesh network shall transmit MSH-NCFGs.



Syntax	Size	Notes
MSH-NCFG_Message_Format() {		
Management Message Type = 39	8 bits	
NumNbrEntries	5 bits	
NumBSEntries	2 bits	
Embedded Packet Flag	1 bit	0 = Not present, 1= present
Xmt Power	4 bits	
Xmt Antenna	3 bits	
NetEntry MAC Address Flag	1 bit	0= Not present, 1= present
Network base channel	4 bits	
reserved	4 bits	Shall be set to zero
NetConfig Count	4 bits	
Timestamp Frame Number Network Control Slot Number in frame Synchronization Hop Count	 12 bits 4 bits 8 bits	
NetConfig schedule info Next Xmt Mx Xmt Holdoff Exponent	 3 bits 5 bits	
if (**NetEntry MAC Address Flag**) **NetEntry MAC Address**	 48 bits	
for (i=0; i< NumBSEntries; ++i) {		
BS Node ID	16 bits	
Number of hops	3 bits	
Xmt energy/bit	5 bits	
}		
for (i=0; i< NumNbrEntries; ++i) {		
Nbr Node ID	16 bits	
MSH-Nbr_Physical_IE()	16 bits	

if (Logical Link Info Present Flag)
MSH-Nbr_Logical_IE()
	16 bits	



Syntax	Size	Notes
}		

if (Embedded Packet Flag)
MSH-NCFG_embedded_data()
	variable	

}		

TABLE 2.16 – MSH-NCFG MESSAGE FORMAT.

- *NumNbrEntries*: number of neighbors reported on in the message. The number of neighbors reported on may be a fraction of the whole set of neighbors known to this node. A node can report on subsequent subsets of neighbors in its subsequent MSH-NCFG transmissions.
- *N270umBSEntries*: number of Mesh BS neighbors reported on in this message.
- *XmtAntenna*: the logical antenna used for transmission of this message.
- *Network base channel:* the base channel being used in this node's network, which is the logical number of the physical channel, shall be used to broadcast schedule control information. A subset of the possible physical channel numbers is mapped to logical channels in the Network Descriptor.
- *Netconfig count*: counter of MSH-NCFG packets transmitted by this node. Used by neighbors to detect missed transmissions.
- *Synchronization hop count:* counter used to determine superiority between nodes when synchronizing the network.
- *XmtHoldoffExponent*: the XmtHoldoffTime is the number of MSH-NCFG transmit opportunities after NextXmtTime (there are MSH-CTRL-LEN – 1 opportunities per network control subframe), that this node is not eligible not transmit MSH-NCFG packets.
- $XmtHoldoffTime = 2^{(XmtHoldoffExponent + 4)}$
- *NextXmtMx*: NextXmtTime is the next MSH-NCFG eligibility interval for this neighbor and computed as the range:
- $2^{XmtHoldoffExponent} NextXmtMx < NextXmtTime \leq 2^{XmtHoldoffExponent} (NexXmtMx+1)$
- *NetEntry MAC Address*: indicates presence or sponsorship of new node.

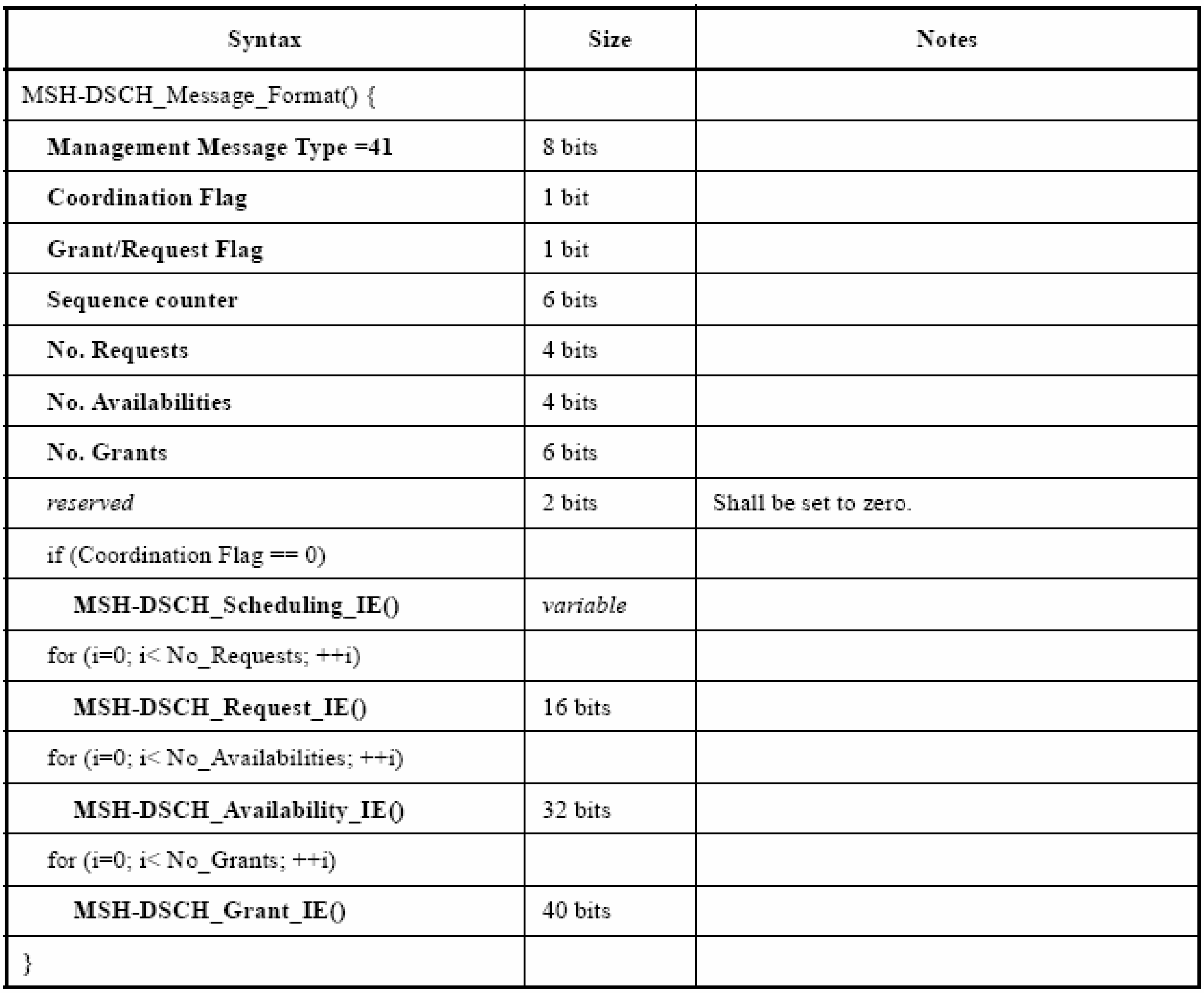
- *Number of hops*: number of hops between the reporting node and the reported Mesh BS node.
- *Xmt energy/bit factor*: indication of energy/bit needed to reach Mesh BS through this node.
- *Nbr node ID*: node ID of the neighbor node reported on.

2.3.2 MSH-DSCH message

A Mesh Schedule with Distributed Scheduling (MSH-DSCH) message shall be transmitted in a mesh mode when using distributed scheduling. In coordinated distributed scheduling, all the stations (BS and SS) shall transmit a MSH-DSCH in a PMP fashion at a regular interval to inform all the neighbours of the schedule of the transmitting station.

The MSH-DSCH message shall be used in parallel also to convey resource requests to the neighbours. Each station shall regularly transmit its MSH-DSCH message in a collision-free manner within its extended neighbourhood. In uncoordinated distributed scheduling, the stations shall transmit the MSH-DSCH in a directed fashion to an intended neighbour.

The MSH-DSCH message format is given in Table 2.17.



Syntax	Size	Notes
MSH-DSCH_Message_Format() {		
Management Message Type =41	8 bits	
Coordination Flag	1 bit	
Grant/Request Flag	1 bit	
Sequence counter	6 bits	
No. Requests	4 bits	
No. Availabilities	4 bits	
No. Grants	6 bits	
reserved	2 bits	Shall be set to zero.
if (Coordination Flag == 0)		
MSH-DSCH_Scheduling_IE()	*variable*	
for (i=0; i< No_Requests; ++i)		
MSH-DSCH_Request_IE()	16 bits	
for (i=0; i< No_Availabilities; ++i)		
MSH-DSCH_Availability_IE()	32 bits	
for (i=0; i< No_Grants; ++i)		
MSH-DSCH_Grant_IE()	40 bits	
}		

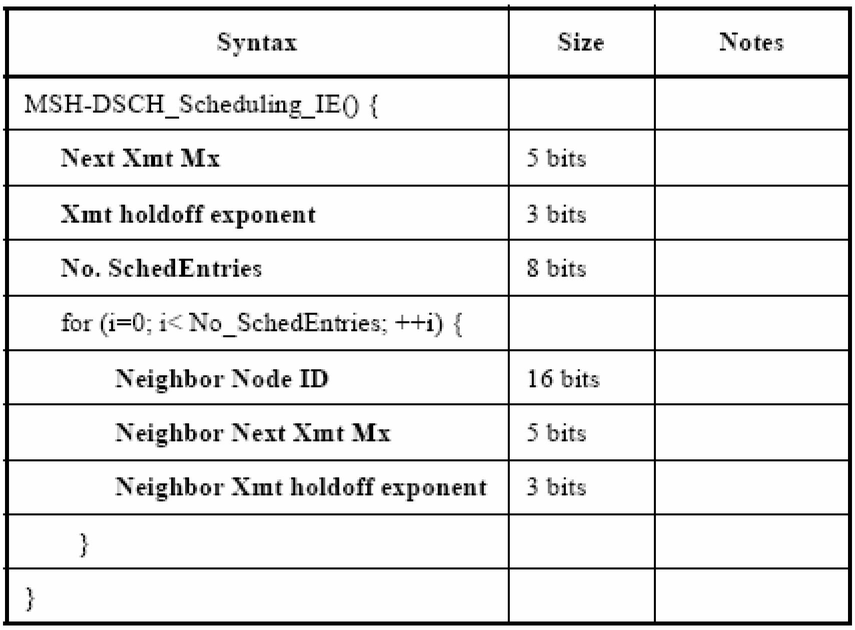
TABLE 2.17 – MSH-DSCH MESSAGE FORMAT.

- Coordination Flag
  - 0: Coordinated (take place in the control subframe).
  - 1: Uncoordinated (take place in the data subframe).
- Both the cases require a three-way handshake (Request, Grant, and Grant confirmation) to establish a valid schedule. Uncoordinated scheduling may only take place in minislots that cause no interference with the coordinated schedule.
- Grant/Request Flag
  - 0: Request message
  - 1: Grant message (also used as Grant confirmation)

- The Request Type indicates that a new Request is made of one or more other nodes. The message may also contain Availabilities and Grants. The Grant Type indicates that one or more Grants are given or confirmed. The message may also contain Availabilities and Requests. Requests in this type of message indicate pending demand to the indicated node, but do not solicit a Grant from this node. This flag is always set to 0 for coordinated distributed scheduling.
- Sequence Counter: in coordinated scheduling, it allows nodes to detect missed scheduling messages. Independent counters are used for the coordinated and uncoordinated messages.
- No. Requests: number of Request IEs in the message.
- No. Availabilities: number of Availability IEs in the message. The Availability IEs are used to indicate free minislot ranges that neighbors could issue Grants in.
- No. Grants: number of Grant IEs in the message.

MSH-DSCH Scheduling IE

The Coordinated distributed scheduling information carried in the MSH-DSCH message shall be used to distribute information needed to determine transmission timing of the MSH-DSCH messages with coordinated distributed scheduling. Each node shall report the two related parameters both of its own and all its neighbors.



Syntax	Size	Notes
MSH-DSCH_Scheduling_IE() {		
Next Xmt Mx	5 bits	
Xmt holdoff exponent	3 bits	
No. SchedEntries	8 bits	
for (i=0; i< No_SchedEntries; ++i) {		
Neighbor Node ID	16 bits	
Neighbor Next Xmt Mx	5 bits	
Neighbor Xmt holdoff exponent	3 bits	
}		
}		

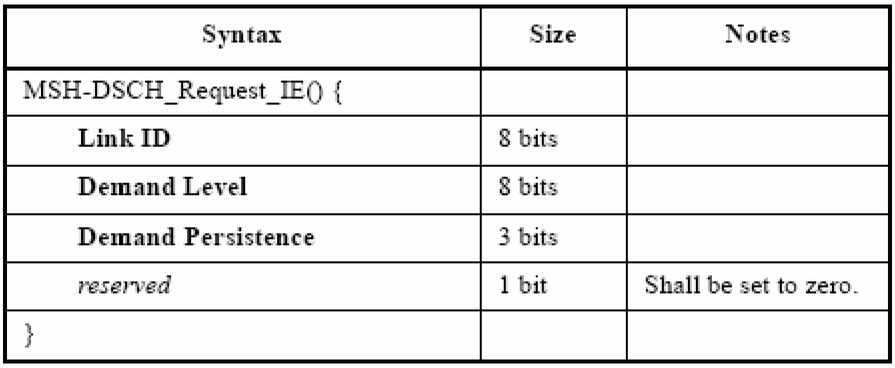
FIGURE 2.18 – MSH-DSCH SCHEDULING IE.

- NextXmtMx: NextXmtTime: is the next MSH-DSCH eligibility interval for this node and computed as the range: *2XmtHoldoffExponent NextXmtMx < NextXmtTime ≤ 2XmtHoldoffExponent (NextXmtMx+1)*
- NeighborNextXmtMx: advertises the NextXmtMx as reported by this neighbor.
- XmtHoldoffExponent: the XmtHoldoffTime is the number of MSH-DSCH transmit opportunities after NextXmtTime (there are MSH-CTRL-LEN –1 opportunities per network control subframe,) that this node is not eligible to transmit MSH-DSCH packets. *XmtHoldoffTime = 2(XmtHoldoffExponent+ 4)*
- NeighborXmtHoldoffExponent: advertises the XmtHoldoffExponent as reported by this neighbor.

- No. SchedEntries: number of Neighbor MSH-DSCH Scheduling Entries in the message.

MSH-DSCH Request IE

The Requests carried in the MSH-DSCH message shall convey resource requests on per link basis.



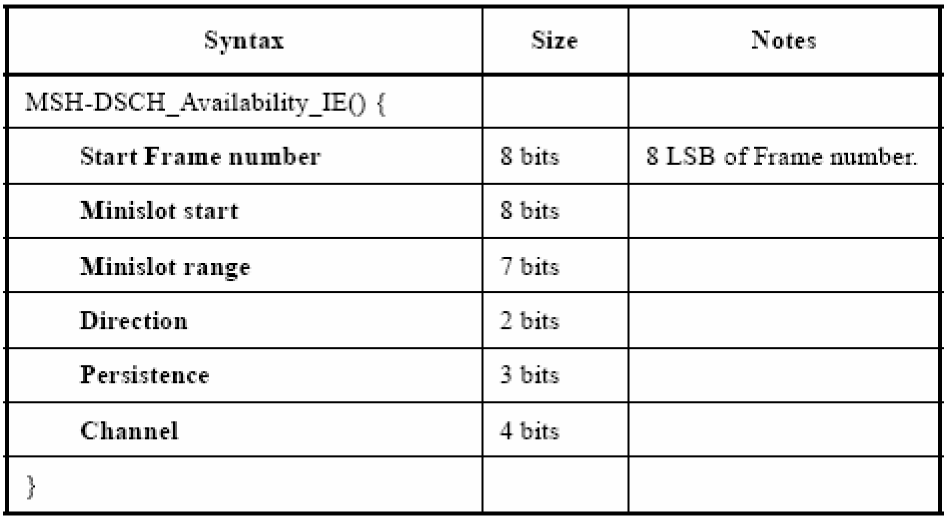
Syntax	Size	Notes
MSH-DSCH_Request_IE() {		
Link ID	8 bits	
Demand Level	8 bits	
Demand Persistence	3 bits	
reserved	1 bit	Shall be set to zero.
}		

TABLE 2.19– MSH-DSCH REQUEST IE.

- *Link ID*: the ID assigned by the transmitting node to the link to this neighbor that this request involves.
- *Demand Level*: demand in minislots assuming the current burst profile.
- *Demand Persistence*: number of frames wherein the demand exists.
    - 0: cancel reservation.
    - 1: single frame.
    - 2: 2 frames.
    - 3: 4 frames.
    - 4: 8 frames.
    - 5: 32 frames.
    - 6: 128 frames.
    - 7: good until cancelled or reduced.

MSH-DSCH Availabilities IE

The Availabilities carried in the MSH-DSCH message shall be used to indicate free minislot ranges that neighbors could issue Grants in.



Syntax	Size	Notes
MSH-DSCH_Availability_IE() {		
Start Frame number	8 bits	8 LSB of Frame number.
Minislot start	8 bits	
Minislot range	7 bits	
Direction	2 bits	
Persistence	3 bits	
Channel	4 bits	
}		

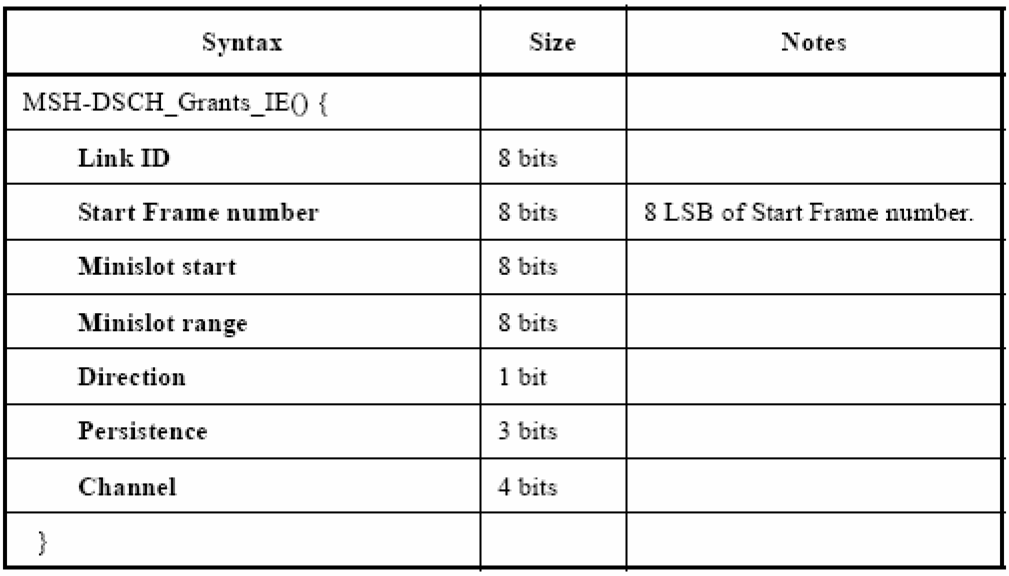
Table 2.20– MSH-DSCH Availability IE.

- *Start Frame number*: indicates lowest 8 bits of frame number in which the availability starts.
- *Minislot start*: the start position of the availability within a frame.
- *Minislot range*: the number of minislots free for grants.
- *Direction*
    - 0: minislot range is unavailable.
    - 1: available for transmission in this minislot range.
    - 2: available for reception in this minislot range.
    - 3: available for either transmission or reception
- *Persistence*: number of frames over which the Availability is valid.
    - 0: cancel reservation.
    - 1: single frame.
    - 2: 2 frames.
    - 3: 4 frames.
    - 4: 8 frames.
    - 5: 32 frames.

    - 6: 128 frames.
    - 7: good until cancelled or reduced.
- *Channel*: logical number of the physical channel. A subset of the possible physical channel numbers is mapped to logical channels in the Network Descriptor.

MSH-DSCH Grants IE

The Grants carried in the MSH-DSCH message shall convey information about a granted minislot range selected from the range reported as available. Grants shall be used both to grant and confirm a grant.



Syntax	Size	Notes
MSH-DSCH_Grants_IE() {		
Link ID	8 bits	
Start Frame number	8 bits	8 LSB of Start Frame number.
Minislot start	8 bits	
Minislot range	8 bits	
Direction	1 bit	
Persistence	3 bits	
Channel	4 bits	
}		

TABLE 2.21 – MSH-DSCH GRANTS IE.

- *Link ID*: ID assigned by the transmitting node to the neighbor that this grant involves.
- *Start Frame number*: indicates lowest 8 bits of frame number in which the schedule is granted.
- *Minislot start*: the start position of the reservation within a frame.
- *Minislot range*: the number of minislots reserved.

- *Direction*
    - 0: from requester (i.e., to granter).
    - 1: to requester (i.e., from granter).
- *Persistence*: number of frames over which the grant is allocated.
    - 0: cancel reservation.
    - 1: single frame.
    - 2: 2 frames.
    - 3: 4 frames.
    - 4: 8 frames.
    - 5: 32 frames.
    - 6: 128 frames.
    - 7: good until cancelled or reduced.
- *Channel*: logical number of the physical channel. A subset of the possible physical channel numbers is mapped to logical channels in the Network Descriptor.

2.4 Scheduling Services

Scheduling services represent the data handling mechanisms supported by the MAC scheduler for data transport on a connection. Scheduling is performed by negotiating minislot ranges and associated channels within the data subframe. Schedule is adaptive, based on the traffic demand for each link.

There are 3 scheduling mechanisms.

- *Coordinated centralized scheduling*: uses scheduling packets transmitted in a collision-free way within scheduling control subframes; this scheduling is coordinated by the mesh BS. And is the best for links supporting persistent traffic streams

- *Coordinated distributed scheduling*: uses scheduling packets transmitted in a collision-free way within scheduling control subframes. It uses the same distributed scheduling algorithm used for MSH-NCFG packets and it uses some or the entire control portion of each frame to regularly transmit its own schedule and proposed schedule changes on a PMP basis to all its neighbors. Within a given channel all neighbor stations receive the same schedule transmissions. All the stations in a network shall use this same channel to transmit schedule information in a format of specific resource requests and grants.

  Coordinated distributed scheduling ensures that transmissions are scheduled in a manner that does not rely on the operation of a BS, and that are not necessarily directed to or from the BS.

  Within the constraints of the coordinated schedules (distributed or centralized), uncoordinated distributed scheduling can be used for fast, ad-hoc setup of schedules on a link-by-link basis.

- *Uncoordinated distributed scheduling*: is the best for scheduling over links with occasional or brief traffic needs. This is established by directed requests and grants between two nodes, and shall be scheduled to ensure that the resulting data transmissions (and the request and grant packets themselves) do not cause collisions with the data and control traffic scheduled by the coordinated distributed nor the centralized scheduling methods.

Both the coordinated and uncoordinated distributed scheduling employ a three-way handshake.

- *MSH-DSCH Request*: is made along with MSH-DSCH Availabilities, which indicate potential slots for replies and actual schedule.

- *MSH-DSCH Grant*: is sent in response indicating a subset of the suggested availabilities that fits, if possible, the request. The neighbours of this node not involved in this schedule shall assume the transmission takes place as granted.

- *MSH-DSCH Grant*: is sent by the original requester containing a copy of the grant from the other party, to confirm the schedule to the other party. The neighbours of this node not involved in this schedule shall assume the transmission takes place as granted.

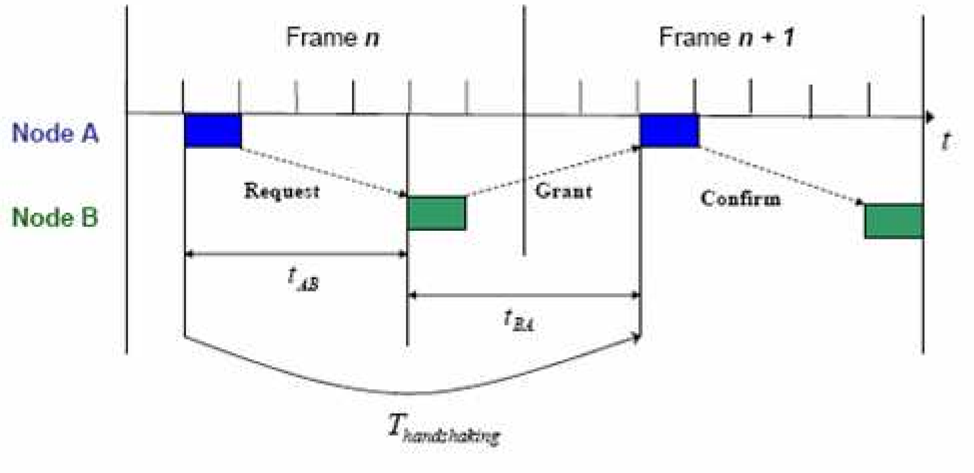


FIGURE 2.22 – 3 WAY HANDSHAKE.

Differences between coordinated and uncoordinated distributed scheduling:

- *Coordinated case*: the MSH-DSCH messages are scheduled in the control subframe in a collision free manner.

- *Uncoordinated case*: MSH-DSCH messages may collide. Nodes responding to a Request should wait a sufficient number of minislots of the indicated Availabilities before responding with a grant, such that nodes listed earlier in the Request have an opportunity to respond. The Grant confirmation is sent in the minislots immediately following the first successful reception of an associated Grant packet.

2.5 Physical layer for mesh networks

The system uses a frame of 0.5, 1, or 2 ms; this frame is divided into physical slots.

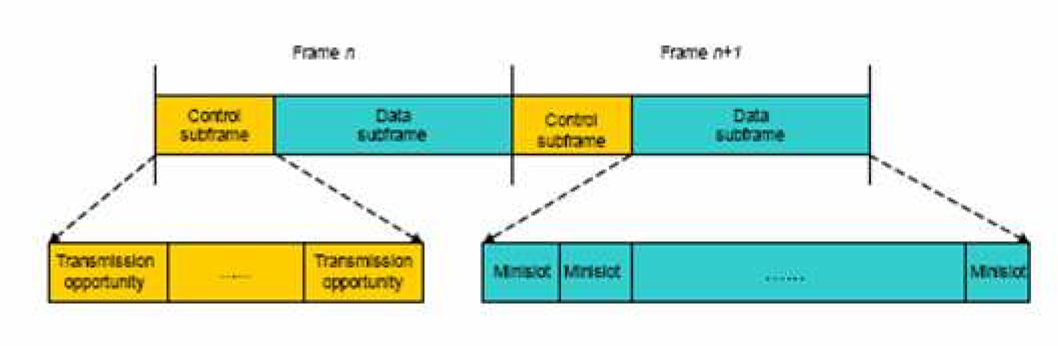


FIGURE 2.23 – FRAME STRUCTURE.

Mesh frame Structure:

- *Control subframe*: there are two type of control subframe:
  - *Network control*: create and maintain the cohesion between the different systems.
  - *Schedule control*: coordinated scheduling of data-transfers between systems.

  There are sixteen *Transmission Opportunities* (*TO*) and one TO is equal to seven OFDM symbols.
- *Data subframe*: the basic unit is the minislot. Data subframe reservation scheme is unspecified in the standard

Only TDD is supported in Mesh mode where there are no clearly separate downlink and uplink subframes. Stations shall transmit to each other either in scheduled channels or in random access channels. The frame structure is described in Figure 2.24.

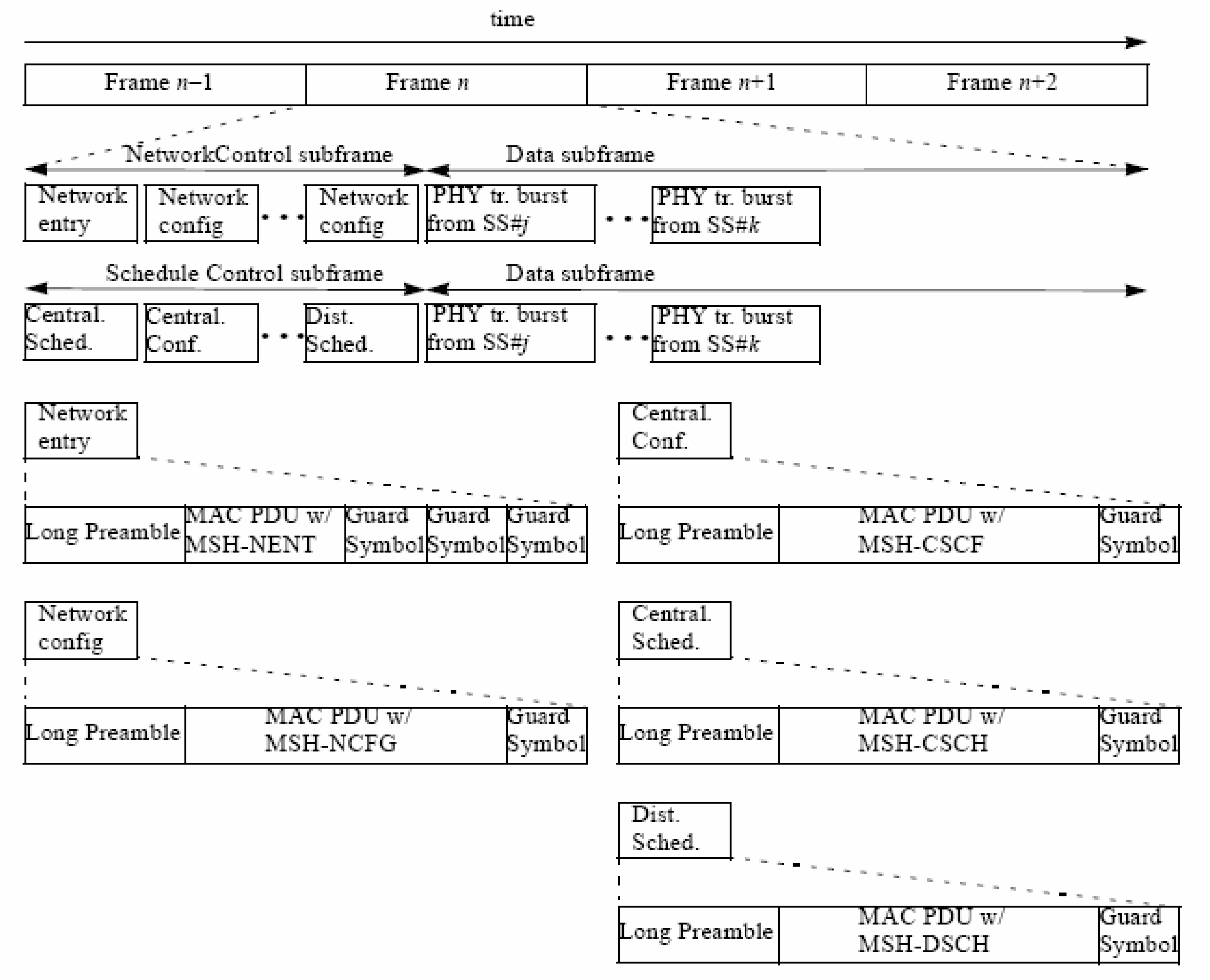


FIGURE 2.24 – MESH FRAME STRUCTURE.

Frames with a network control subframe occur periodically, as indicated in the Network Descriptor. All other frames have a schedule control subframe.

The length of the control subframe is fixed and of length *MSH-CTRL-LEN * 7* OFDM symbols, with *MSH-CTRL-LEN* indicated in the Network Descriptor.

During a network control subframe, the first seven symbols are allocated for network entry, followed by *MSH-CTRL-LEN – 1* sets of seven symbols for network configuration.

During a schedule control subframe, the Network Descriptor indicates how many (*MSH-DSCH-NUM*) Distributed Scheduling messages may occur in the control subframe.

The first *(MSH-CTRL-LEN – MSH-DSCH-NUM) * 7* symbols are allocated to transmission bursts containing MSH-CSCH and MSH-CSCF PDUs, whereas the remainder is allocated to transmission bursts containing MSH-DSCH PDUs.
Distributed Scheduling messages (using the long preamble) may further occur in the data subframe if not in conflict with the scheduling dictated in the control subframe.

All transmissions in the control subframe are sent using QPSK ½ with the mandatory coding scheme. The data subframe is divided into minislots, which are, with possible exception of the last minislot in the frame, of size ceiling *[(OFDM symbols per frame – MSH-CTRL-LEN * 7) / 256]*. A scheduled allocation consists of one or more minislots.

All the basic functions like scheduling and network synchronization are based on the neighbour information that all the nodes in the Mesh network shall maintain. Each node (BS and SS) maintains a physical neighbourhood list with each entry containing the following fields:

- *MAC Address*: 48-bit MAC address of the neighbour.
- *Hop Count*: indicates distance in hops of this neighbour from the present node. If a packet has been successfully received from this neighbour it is considered to be 1 hop away.
- *Node Identifier*: 16-bit number used to identify this node in a more efficient way in MSH-NCFG messages.
- *XmtHoldoffTime*: the minimum number of MSH-NCFG transmit opportunities that no MSH-NCFG message transmission is expected from this node after NextXmtTime.
- *NextXmtTime*: the MSH-NCFG transmit opportunity(ies) when the next MSH-NCFG from this node is expected.
- *Reported Flag*: Set to TRUE if this NextXmtTime has been reported by this node in a MSH-NCFG packet. Else set to FALSE.

- *Synchronization hop count*: this counter is used to determine superiority between nodes when synchronizing the network. Nodes can be assigned as master time keepers, which are synchronized externally. These nodes transmit Synchronization hop count of 0. Nodes shall synchronize to nodes with lower synchronization hop count, or if counts are the same, to the node with the lower Node ID.

When using coordinated distributed scheduling all the stations in a network shall use the same channel to transmit schedule information in a format of specific resource requests and grants in MSH-DSCH messages.

A station shall indicate its own schedule by transmitting a MSH-DSCH regularly. The MSH-DSCH messages shall be transmitted during the control portion of the frame. MSH-DSCH messages are transmitted regularly throughout the whole Mesh network to distribute nodes' schedules and (together with network configuration packets) provide network synchronization information.

An SS that has a direct link to the BS shall synchronize to the BS while an SS that is at least two hops from the BS shall synchronize to its neighbor SSs that are closer to the BS.

The control portion of every *[Schedule Frames + 1]* frames is reserved for communication of MSH-NCFG and MSH-NENT packets.

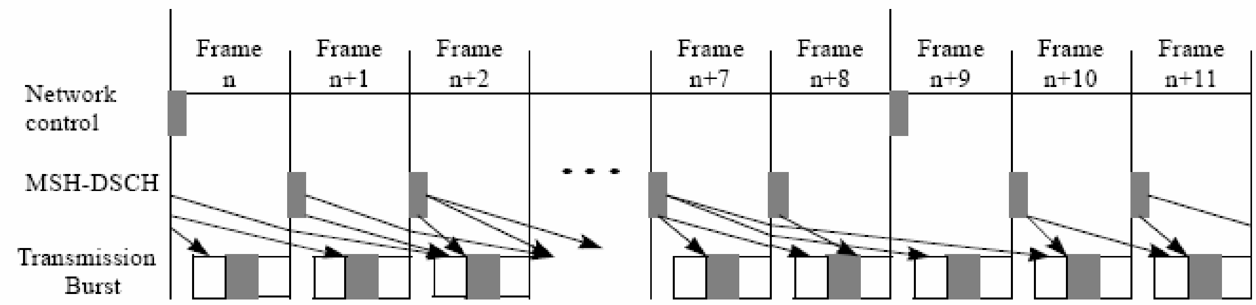


FIGURE 2.25 – TIME RELEVANCE EXAMPLE OF MSH-DSCH IN DISTRIBUTED SCHEDULING.

Network configuration (*MSH-NCFG*) and network entry (*MSH-NENT*) packets provide a basic level of communication between nodes in different nearby networks whether

from the same or different equipment vendors or wireless operators. These packets are used to synchronize both centralized and distributed control Mesh networks.
This communication is used to support basic configuration activities such as:

- Synchronization between nearby networks used.
- Communication and coordination of channel usage by nearby networks.
- Discovery and basic network entry of new nodes.

MSH-NCFG, MSH-NENT, and MSH-DSCH can assist a node in synchronizing to the start of frames. For these messages, the control subframe, which initiates each frame, is divided into transmit opportunities. The MSH-NCFG messages also contain the number of its transmit opportunity, which allows nodes to easily calculate the start time of the frame.

MSH-NCFG and MSH-NENT packets are scheduled for transmission during control subframes. To ensure that all nearby nodes receive these transmissions, the channel used is cycled through the available channels in the band, with the channel selection being based on the Frame number.

During the current XmtTime of a node (i.e., the time slot when a node transmits its MSH-NCFG packet), the node uses the following procedure to determine its NextXmtTime:

- Order its physical neighbor table by the NextXmtTime.
- For each entry of the neighbor table, add the node's NextXmtTime to the node's XmtHoldoffTime to arrive at the node's EarliestSubsequentXmtTime.
- Set TempXmtTime equal to this node's advertised XmtHoldoffTime added to the current XmtTime.
- Set *success* equal to false.
- While *success* equals false do:
    - Determine the eligible competing nodes, which is the set of all nodes in the physical-neighbor list with a NextXmtTime eligibility interval that includes TempXmtTime or with an EarliestSubsequentXmtTime equal to or smaller than TempXmtTime.

- Hold a *Mesh Election* among this set of eligible competing nodes and the local node using TempXmtTime and the list of the Node IDs of all eligible competing nodes as the input: *MeshElection (TempXmtTime,MyNodeID,CompetingNodeIDsList [ ])*
- If (this node does not win *Mesh election)*

  Set TempXmtTime equal to next MSH-NCFG opportunity.

Else:

  Set *success* equal to true.

  Set the node's NextXmtTime equal to TempXmtTime.

The *Mesh Election* procedure determines whether the local node is the winner for a specific TempXmtTime among all the competing nodes. It returns TRUE, if the local node wins, or otherwise FALSE.

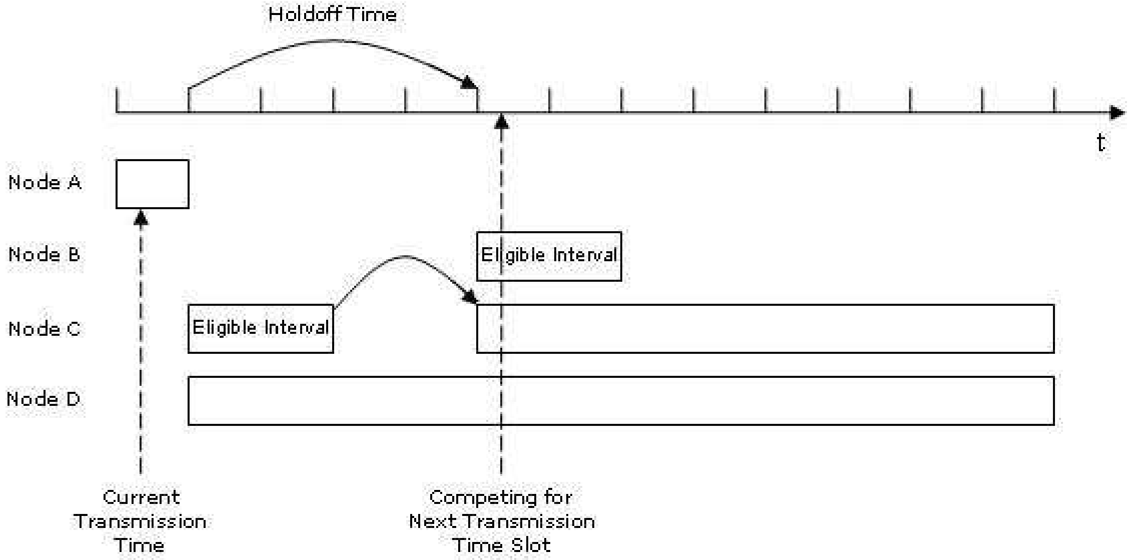


FIGURE 2.25 – CONTENTION MECHANISM.

The NetEntry scheduling protocol provides the upper-layer protocol an unreliable mechanism to access the NetEntry slot(s), so that new nodes, which are not yet fully-functional members of the network, can communicate with the fully-functional members of the network.

In the NetEntry slots, new nodes shall transmit MSH-NENT messages using the following two step procedure:

- The initial MSH-NENT packet with request IE is sent in a random, contention-based fashion in a free network entry transmission slot immediately following MSH-NENT transmission opportunity after the targeted sponsor sends a MSH-NCFG with sponsored MAC address 0x000000000000.
- After the sponsor advertises the new nodes MAC Address in a MSH-NCFG message, the new node may send a MSH-NENT immediately following MSH-NENT transmission opportunity.

When a MSH-NCFG packet is received from a neighbour, the following is performed:

- The hop count field in the Physical Neighbourhood List for the neighbour itself is set to 1.
- The hop count field for other nodes listed in the MSH-NCFG message is set to *HopstoNeighbor+2* unless they are already listed with a lower hop count.
- The NextXmtTime and XmtHoldoffTime of the transmitting node and all reported nodes are updated.
- The "Reported Flag" for each entry in the Physical Neighbour Table, that was modified, is set to FALSE.

A new node entering the Mesh network obeys the following procedures.

1. <u>Scan for active network and establish coarse synchronization with the network</u>.

    On initialization or after signal loss, the node shall search for MSH-NCFG messages to acquire coarse synchronization with the network. Upon receiving a

MSH-NCFG message the node acquires the network time from the *Timestamp* field of the message. The node may have non-volatile storage in which all the last operational parameters are stored and shall first try to re-acquire coarse synchronization with the network. If this fails, it shall begin to continuously scan the possible channels of the frequency band of operation until a valid network is found. Once the PHY has achieved synchronization, the MAC shall attempt to acquire network parameters. At the same time the node shall build a physical neighbour list.

2. Obtain network parameters from MSH-NCFG messages.

From the established physical neighbor list, the new node shall select a potential *Sponsoring Node* out of all nodes having the *Logical Network ID* of the node for which it found a suitable *Operator ID*. The new node shall then synchronize its time to the potential sponsor assuming 0 propagation delay after which it shall send a *MSH-NENT:NetEntryRequest* including the Node ID of the potential sponsor.

Until the node has obtained an unique Node ID, it shall use *temporary Node ID* (0x0000) as *Transmitter's Node ID* in all transmissions.

Once the *Candidate Node* has selected a Sponsoring Node, it shall use the Sponsoring Node to negotiate basic capabilities and to perform authorization. For that purpose the Candidate Node shall first request the Sponsoring Node to open *Sponsor Channel* for more effective message exchange.

3. Open Sponsor Channel.

The process is initiated by the Candidate Node, which transmits a *MSH-NENT:NetEntryRequest* message to the Sponsoring Node. Upon reception of the MSH-NENT:NetEntryRequest message with the Sponsor Node ID equal to Node

ID of its own, the candidate Sponsoring Node shall assess the request and either opens the Sponsor Channel or rejects the request.

If the candidate Sponsoring Node does not advertise the Candidate Node's MAC address in the sponsor's next MSH-NCFG transmission, then the procedure is repeated. If these attempts all fail, then a different Candidate Sponsoring Node is selected and the procedure repeated (including re-initializing coarse network synchronization).

If the selected candidate Sponsoring Node does advertise the Candidate Node's MAC address, it shall continue to advertise this MAC address in all its MSH-NCFG messages until the sponsorship is terminated.

Once the Candidate Node has received a positive response (a *NetEntryOpen* message) in from the candidate Sponsoring Node in the MSH-NCFG message, it shall acknowledge the response by transmitting a *MSHNENT:NetEntryAck* message to the Sponsoring Node at the first following network entry transmission opportunity.

If the Sponsoring Node accepts the request and opens a Sponsor Channel, the channel is ready for use immediately after the transmission of the acknowledgment message. At the same time, the candidate Sponsoring Node becomes the Sponsoring Node.

Figure 2.26 displays the message transfer sequence during a successful network entry without repetitions or timeouts.

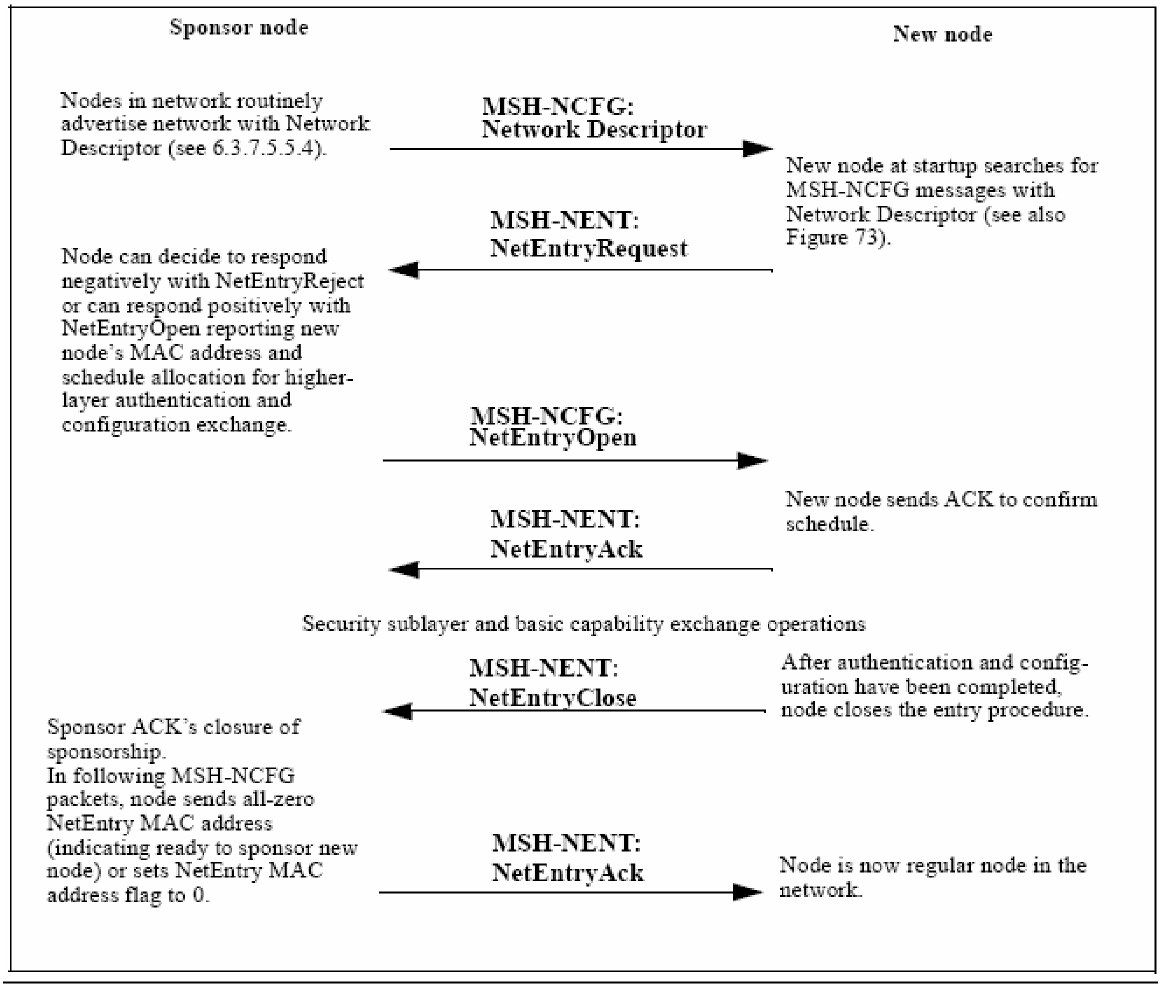

Sponsor node
New node
Nodes in network routinely advertise network with Network Descriptor (see 6.3.7.5.5.4).
MSH-NCFG: Network Descriptor
New node at startup searches for MSH-NCFG messages with Network Descriptor (see also Figure 73).
MSH-NENT: NetEntryRequest
Node can decide to respond negatively with NetEntryReject or can respond positively with NetEntryOpen reporting new node's MAC address and schedule allocation for higher-layer authentication and configuration exchange.
MSH-NCFG: NetEntryOpen
New node sends ACK to confirm schedule.
MSH-NENT: NetEntryAck
Security sublayer and basic capability exchange operations
MSH-NENT: NetEntryClose
After authentication and configuration have been completed, node closes the entry procedure.
Sponsor ACK's closure of sponsorship. In following MSH-NCFG packets, node sends all-zero NetEntry MAC address (indicating ready to sponsor new node) or sets NetEntry MAC address flag to 0.
MSH-NENT: NetEntryAck
Node is now regular node in the network.

FIGURE 2.26 – SUCCESSFUL NETWORK ENTRY MESSAGE EXCHANGE.

4. Node authorization.

5. Perform registration.

   Registration is the process where a node is assigned its Node ID.

6. Establish IP connectivity.

   The Node shall acquire an IP address using DHCP.

7. Establish time of day.

8. Transfer operational parameters.

After successfully acquiring an IP address via DHCP, the Node shall download a parameter file using TFTP.

The 48-bit universal MAC address assigned during the manufacturing process is used to identify the node to the various provisioning servers during initialization and whenever performing authentication with a neighbor node.

After entering the network, a node can establish links with nodes other than its sponsor by following the secure process that uses the *MSH-NCFG:Neighbor Link Establishment IE*.

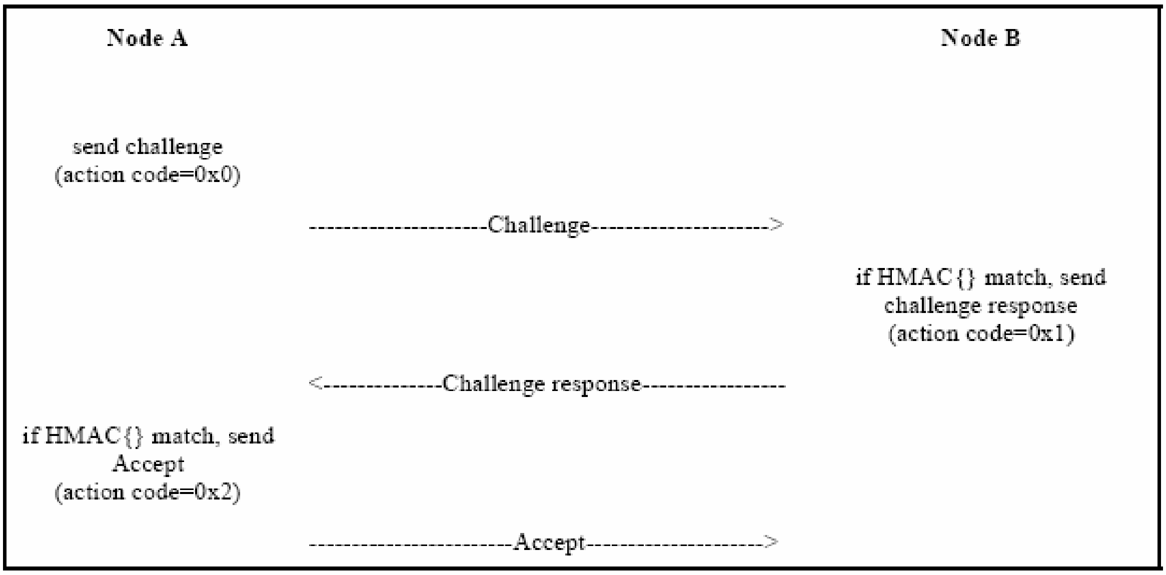

Node A
Node B
send challenge
(action code=0x0)
---------------------Challenge--------------------->
if HMAC{} match, send
challenge response
(action code=0x1)
<--------------Challenge response-----------------
if HMAC{} match, send
Accept
(action code=0x2)
------------------------Accept-------------------->

FIGURE 2.27 – ESTABLISHING LINK CONNECTIVITY.

- Node A sends a challenge (action code = 0x0) containing:
  HMAC{Operator Shared Secret, frame number, Node ID of node A, Node ID of node B}
  - *Operator Shared Secret*: is a private key obtained from the provider (which is also used to enter the network).

    - *Frame number*: is the last known frame number in which Node B sent a MSH-NCFG message.

- Node B, upon reception, computes the same value compute by Node A and compares. If the values do not match, a rejection (action code = 0x3) is returned. If a match is achieved, Node B sends, implicitly accepting the link, a challenge response (action code=0x1) containing:

  HMAC{Operator Shared Secret, frame number, Node ID of node B, Node ID of node A}

    - *Frame number*: is the frame number in which Node A sent the MSH-NCFG message with challenge.

  It also randomly selects and includes an unused link ID, which shall from this point forward indicate the link from node B to node A.

- Node A, upon reception, computes the same value compute by Node B and compares. If the values do not match, a rejection (action code = 0x3) is returned. If a match is achieved, Node A sends an *Accept*. It also randomly selects and includes an unused link ID, which shall from this point forward indicate the link from Node A to Node B.

2.6 Wireless MAN-OFDM PHY

Mesh networks use OFDM modulation that is based on OFDM modulation and designed for NLOS operation in the frequency bands below 11 GHz.

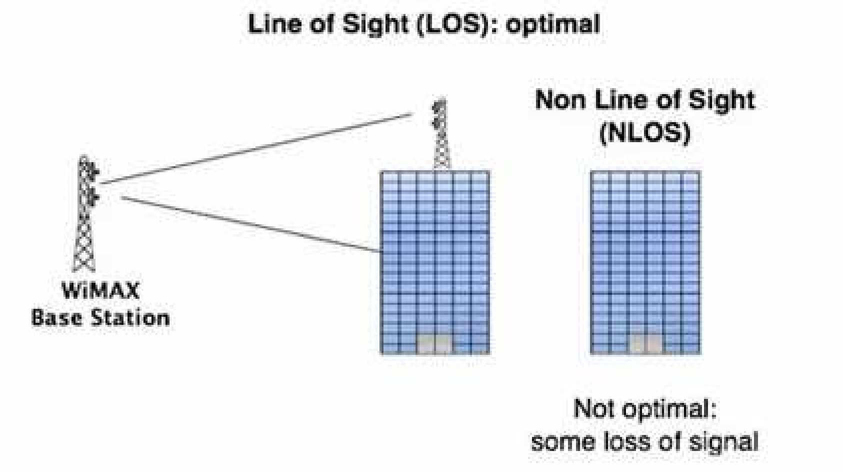

Line of Sight (LOS): optimal
Non Line of Sight (NLOS)
WiMAX Base Station
Not optimal: some loss of signal

FIGURE 2.28 – LOS AND NLOS.

Inverse-Fourier-transforming creates the OFDM waveform; this time duration is referred to as the useful symbol time T_b. A copy of the last T_g of the useful symbol period, termed *CP*, is used to collect multipath, while maintaining the orthogonality of the tones.

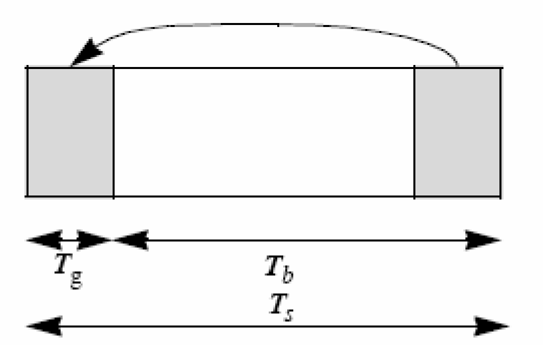


FIGURE 2.29 – OFDM SYMBOL TIME STRUCTURE.

Cyclic extension provides multipath immunity as well as a tolerance for symbol time synchronization errors.

On initialization, an SS should search all possible values of CP until it finds the CP being used by the BS. The SS shall use the same CP on the uplink. Once a specific CP duration has been selected by the BS for operation on the downlink, it should not be changed. Changing the CP would force all the SSs to resynchronize to the BS.

2.7 Data modulation

After bit interleaving, the data bits are entered serially to the constellation mapper. BPSK, Gray-mapped QPSK, QAM 16, and QAM 64 shall be supported, whereas the support of QAM 64 is optional for license-exempt bands. The constellations shall be normalized by multiplying the constellation point with the indicated factor *c* to achieve equal average power.

Per-allocation adaptive modulation and coding shall be supported in the downlink. The uplink shall support different modulation schemes for each SS based on the MAC burst configuration messages coming from the BS.

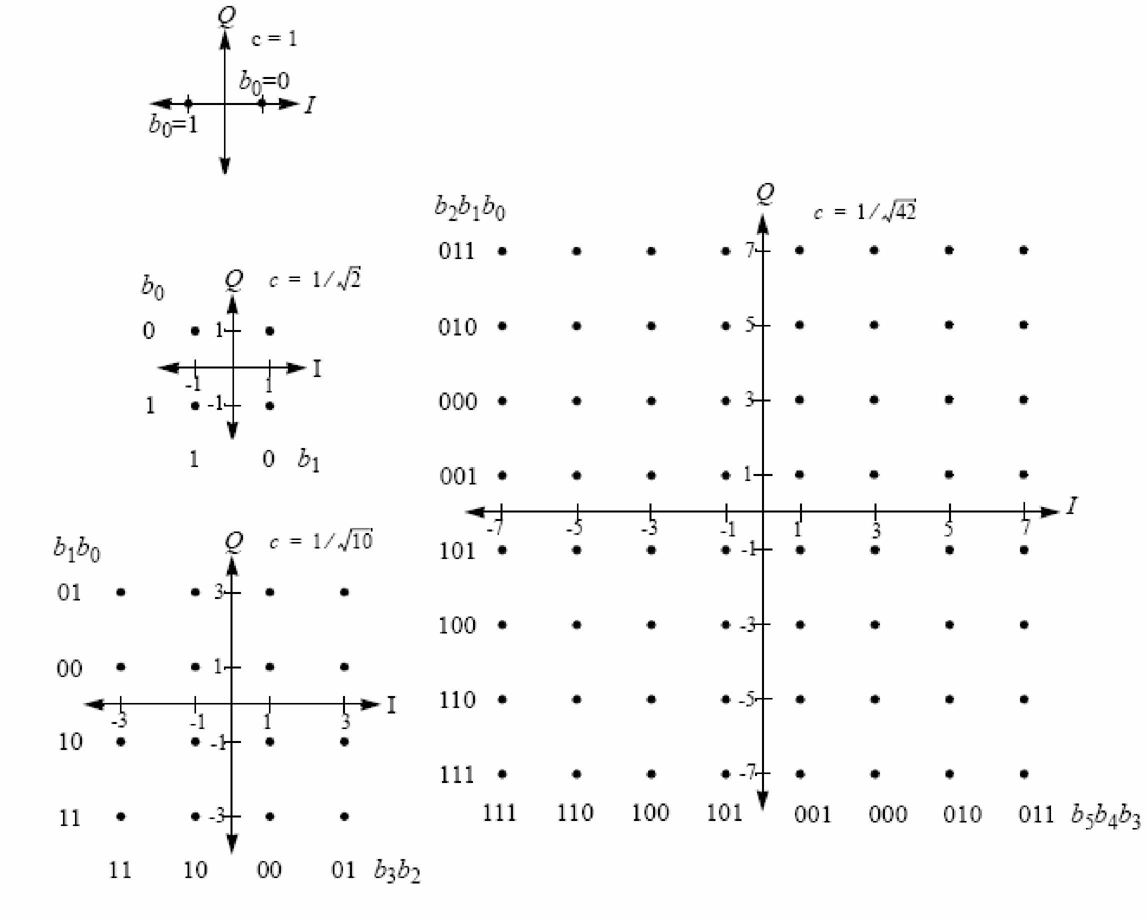


FIGURE 2.30 – BPSK, QPSK, 16-QAM, AND 64-QAM CONSTELLATIONS.

2.8 Preamble structure and modulation

All preambles are structured as either one of two OFDM symbols. The OFDM symbols are defined by the values of the composing subcarriers. Each of those OFDM symbols contains a cyclic prefix, which length is the same as the CP for data OFDM symbols.

The first preamble in the downlink PHY PDU, as well as the initial ranging preamble, consists of two consecutive OFDM symbols. The first OFDM symbol uses only subcarriers the indices of which are a multiple of 4. As a result, the time domain waveform of the first symbol consists of four repetitions of 64-sample fragment, preceded by a CP. The second OFDM symbol utilizes only even subcarriers, resulting in time domain structure composed of two repetitions of a 128-sample fragment, preceded by a CP. The time domain structure is exemplified in Figure 2.31. This combination of the two OFDM symbols is referred to as the *long preamble*.

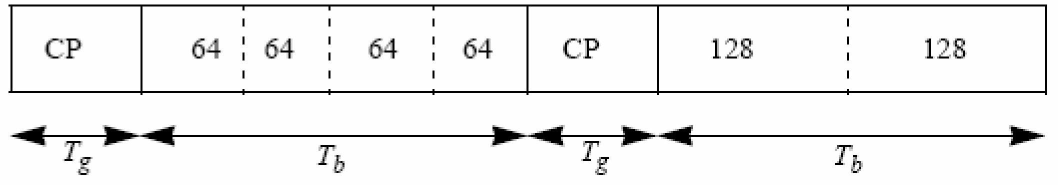


FIGURE 2.31 – DOWNLINK AND NETWORK ENTRY PREAMBLE STRUCTURE.

In the uplink, when the entire 16 subchannels are used, the data preamble, as shown in Figure 2.32 consists of one OFDM symbol utilizing only even subcarriers. The time domain waveform consists of 2 times 128 samples preceded by a CP.

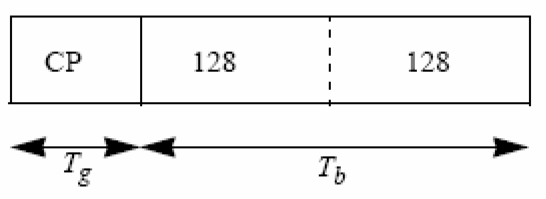


FIGURE 2.32 – UPLINK PREAMBLE STRUCTURE.

In mesh mode, bursts sent in the control subframe shall start with the long preamble. In the mesh data subframe, the bursts shall be default start with the long preamble, but neighbors may negotiate to use the *short preamble* by setting the preamble flag in the NeighborLinkInfo field.

3 Mesh Networks

“If you are willing and obedient,
you will eat the best from the land”
— *Isaiah 1:19 (NIV)*

Mobile ad hoc networks are collections of mobile nodes connected together over a wireless medium. These nodes can freely and dynamically self-organize into arbitrary and temporary ad hoc network topologies, allowing people and devices to continuously internetwork in areas with no preexisting communication infrastructure (e.g., disaster recovery and battlefield environments). The ad hoc networking concept is not new, having been around in various forms for over 30 years.

Mesh networks are built on a mix of fixed and mobile nodes interconnected via wireless links to form a multihop ad hoc network where users’ devices are an active part. They dynamically join the network, acting as both user terminals and routers for other devices, so that extending network coverage.

Several emerging and commercially interesting applications have been deployed based on wireless mesh network architecture. Public transportation companies, government agencies, and research organizations are looking for viable solutions to realize intelligent transport systems (i.e., integrated public transportation systems that are built to be safe, cost effective, efficient, and secure). Wireless mesh could be the flexible solution to implement the information delivery system required to control transportation services.

An example for this application scenario is the *Portsmouth Real-Time Travel Information System* (*PORTAL*), a system that, as part of a citywide public transportation communications network, aims at providing real-time travel information to passengers. This system is realized by equipping more than 300 buses with mesh technology provided by MeshNetworks Inc. The wireless mesh network allows anybody to display, at more than 40 locations throughout the city, real-time information on transportation services, such as where his/her bus is, its ultimate destination, and when it is scheduled to arrive. The same system is also expected to be used to address and alleviate transportation congestion problems, control pollution, and improve transportation safety and security.

Solutions based on cellular technologies have been used, but they have proved to be unsatisfactory in many aspects. In particular, cellular data networks promise near ubiquitous coverage and allow high-mobility speeds, but data rate is limited and the network infrastructure is extremely costly. Furthermore, wireless mesh networks appear to be the natural solution to address the needs of law enforcement agencies and city governments. For instance, the *San Matteo Police Department* in the *San Francisco Bay Area* has equipped all its patrol cars with laptops, and motorcycle and bicycle patrols with PDAs, employing standard 802.11b/g wireless cards for communications.

Internet service providers (*ISPs*) are seeking integrated solutions to implement public Internet access, so there are a growing number of small and big ISPs based on Wi-Fi technologies to provide broadband wireless Internet access. The wireless mesh networks are the ideal solution to provide both indoor and outdoor broadband wireless connectivity in urban, suburban, and rural environments without the need for extremely costly wired network infrastructure.

An example of this is the metro-scale broadband city network activated on April 2004 in the city of Cerritos, California, operated by *Aiirmesh Communications Inc.*, a wireless ISP (*WISP*) company.

This significant reduction of network installation costs ensures rapid deployment of a metropolitan broadband network that is cost effective even with a limited potential subscriber base, as found in rural or scarcely populated urban areas.

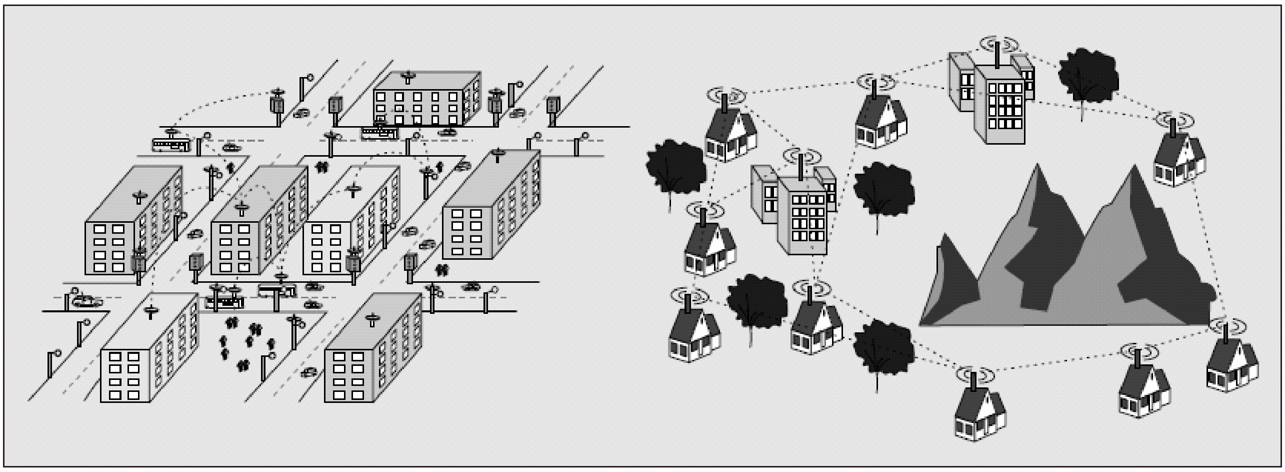


FIGURE 3.1 – EXAMPLES OF MESH NETWORKS.

Wireless mesh has been envisioned as the economically viable networking paradigm to build up broadband and large-scale wireless commodity networks.

A wireless mesh network is a fully wireless network that employs multihop communications to forward traffic to and from wired Internet entry points. A mesh network introduces a hierarchy in the network architecture with the implementation of dedicated nodes (called *wireless routers*) communicating among each other and providing wireless transport services to data traveling from users to either other users or *access points* (access points are special wireless routers with a high-bandwidth wired connection to the Internet backbone).

The network of wireless routers forms a wireless backbone (tightly integrated into the mesh network), which provides multihop connectivity between nomadic users and wired gateways. The meshing among wireless routers and access points creates a *wireless backhaul communication system*, which provides each mobile user with a low-cost, high-bandwidth, and seamless multihop interconnection service with a limited number of Internet entry points and with other wireless mobile users. Backhaul is used to indicate the service of forwarding traffic from the originator node to an access point from which it can be distributed over an external network. Specifically in the mesh case, the traffic is originated in the users' devices, traverses the wireless backbone, and is distributed over the Internet network.

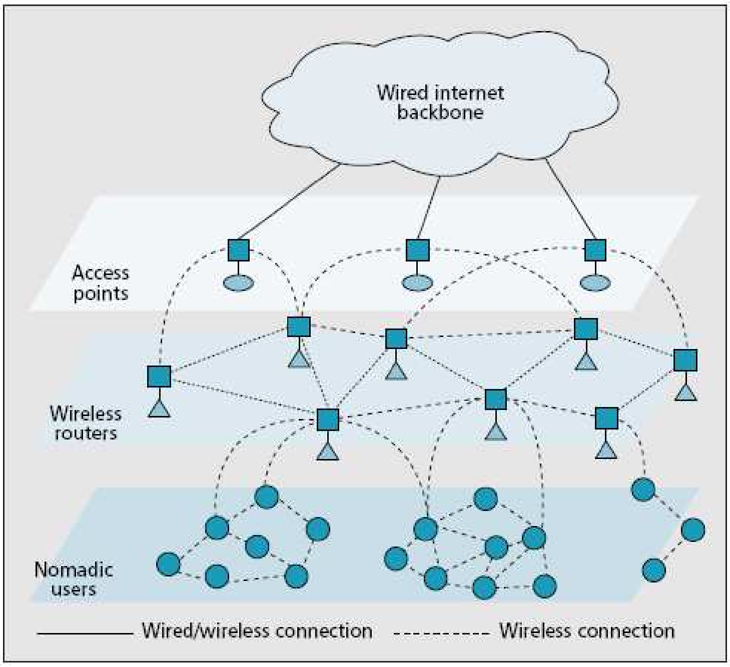


FIGURE 3.2 – A THREE-TIER ARCHITECTURE FOR WIRELESS MESH NETWORKS.

Wireless networks are highly scalable and cost effective, offering a solution for the easy deployment of high-speed ubiquitous wireless Internet.

Benefits of wireless mesh networks:

- *Reduction of installation costs*: currently, one of the major efforts to provide wireless Internet beyond the boundaries of indoor WLANs is through the deployment of *Wi-Fi hot spots*. Basically, a hot spot is an area that is served by a single WLAN or a network of WLANs. To ensure almost ubiquitous coverage is necessary to deploy a large number of access points because they covered a limited distance so the hot spot architecture is costly, unscalable, and slow to deploy. A mesh wireless backbone, however, enormously reduces the infrastructural costs because the mesh network needs only a few points of connection to the wired backbone.

- *Large-scale deployment*: WLAN technologies increased data rates have been achieved by using more spectrally efficient modulation schemes. However, for a specific transmit power, shifting toward more efficient modulation techniques reduces coverage.

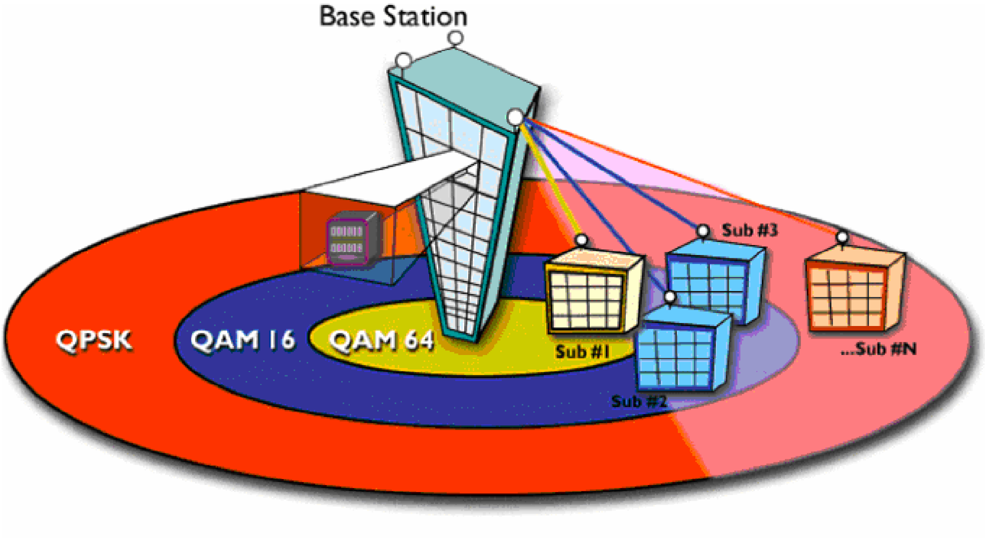


FIGURE 3.3 – MODULATION RANGE.

Moreover, for a fixed total coverage area, more access points should be installed to cover small-size cells. Obviously, this picocellularization of WLANs further hinders the scalability of this technology, especially in outdoor environments, but multihop communications offers long distance communications via hopping through intermediate nodes. Since intermediate links are short, these transmissions could be at high data rates, resulting in increased throughput compared to direct communications. The wireless backbone can realize a high degree of spatial reuse and wireless links covering longer distance at higher speed than conventional WLAN technologies.

- *Reliability*: the wireless backbone provides redundant paths between each pair of endpoints, significantly increasing communications reliability, eliminating single points of failure and potential bottleneck links.

- *Self-management*: the adoption of peer-to-peer networking to build a wireless distribution system provides all the advantages of ad hoc networking, such as self-configuration.

In the mesh architecture network setup is automatic and transparent to users. For instance, when adding additional nodes in the mesh, these nodes use their meshing functionalities to automatically discover all possible wireless routers and determine the optimal paths to the wired network. In addition, the existing wireless routers reorganize, taking into account the new available routes. Thus, the network can easily be expanded, because the network self-reconfigures to assimilate the new elements.

3.1 Techniques for implementing wireless mesh networks

Several IEEE standard groups are actively working to define specifications for wireless mesh networking techniques.

In particular, special task groups have been established to define the requirements for mesh networking in *wireless personal area networks* (*WPANs*), *WLANs*, and *wireless metropolitan area networks* (*WMANs*).

The following standards may be identified.

3.1.1 IEEE 802.15.5

This project is devoted to the definition of PHY and MAC specifications for establishing short-range wireless connectivity for small groups of fixed, portable, and moving computing devices, such as PCs, PDAs, peripherals, cell phones, pagers, and consumer electronics. In November 2003 the IEEE P802.15.5 Mesh Network Task Group was formed to determine the necessary mechanisms that must be present in the PHY and MAC layers of WPANs to enable mesh networking. The use of mesh networking in the WPAN environment is motivated by the power limitations of mobile devices.

3.1.2 IEEE 802.11S

The IEEE 802.11 Working Group contains several standards committees developing technologies for the WLAN environment. Relevant to the mesh networking paradigm is the extension under development by the P802.11s ESS Mesh Networking Task Group. The scope of this TG is to extend the IEEE 802.11 architecture and protocol for providing the functionality of an *Extended Service Set* (*ESS*) mesh with access points capable of establishing wireless links among each other to enable automatic topology learning and dynamic path configuration. The idea behind this proposed amendment is to extend the IEEE 802.11 MAC protocol to create an IEEE 802.11 wireless distribution system that supports both broadcast/multicast and unicast delivery at the MAC layer using radio-aware metrics over self configuring multihop topologies.

3.1.3 IEEE 802.16A

In 1999 the 802.16 Working Group was established to address the "first-mile/last-mile" connection in WMANs, working toward *Local Multipoint Distribution System* (*LMDS*) architectures for broadband wireless access. The WMAN network, as specified in the 802.16 standard, employs a *point-to-multipoint* (*PMP*) architecture where each base station serves a number of subscriber stations in a particular area. A PMP system is a star-shaped network where each subscriber connects to the same central hub. The BS transmits on a broadcast channel to all the SSs, while the SSs have point-to-point links with the BS. At the high frequencies *line-of-sight* (*LOS*) communications are needed because the system can tolerate a limited amount of multipath interference. The need for reliable *non-LOS* (*NLOS*) operations, together with the opportunity to expand the system scope to license-exempt bands, has led to the development of the IEEE 802.16a standard. The adoption of NLOS operations allowed 802.16a standard mesh extensions to be included in the standard. It is useful to consider how the time division multiple access (TDMA)-based MAC layer of a 802.16a system supports this optional mesh mode. In mesh mode all SSs may have direct links with other SSs, and the data traffic directly between SSs. Communications in the direct links can be controlled by either a centralized or distributed algorithm. In centralized scheduling, the BS determines the flow assignment from the resource requests of the SSs. Subsequently, the SSs determine the actual schedule for their neighbors (i.e., the SSs to which they have direct links) from these flow assignments by using a common algorithm. In distributed scheduling, all the nodes including the BS shall coordinate their transmissions in their two-hop neighborhood and broadcast their schedules (available resources, requests, and grants) to all their neighbors.

Wireless links can easily be added to the existing network to either expand the network or introduce additional capacity in the wireless backbone. Consequently, WiMAX products can offer low-cost flexible alternatives for building the wireless backbone in outdoor scenarios.

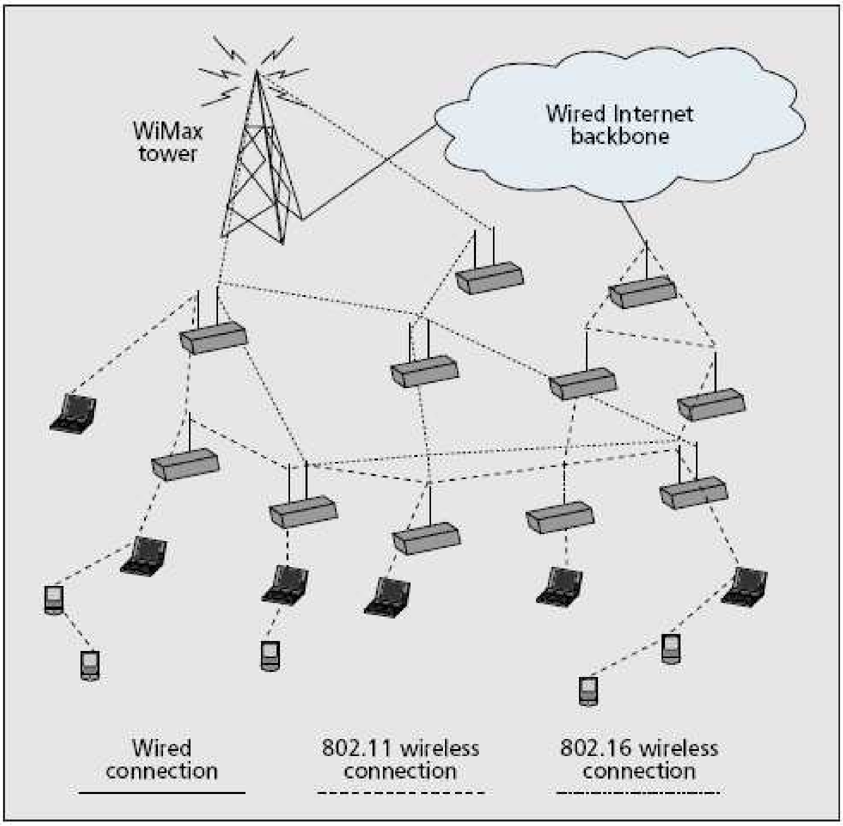


FIGURE 3.4 – INTEGRATION OF WIMAX AND WI-FI TECHNOLOGIES IN LARGE-SCALE WIRELESS MESH NETWORKS.

3.1.4 IEEE 802.20

802.20 systems are intended to provide ubiquitous mobile broadband wireless access in a cellular architecture (e.g., macro/micro/picocells), supporting the mesh networking paradigm (i.e., NLOS communications) in both indoor and outdoor scenarios.

802.16e and 802.20 standards will both specify new mobile air interfaces for wireless and mobile broadband services; there are some important differences between them. 802.16e will add mobility in the 2–6 GHz licensed bands, while 802.20 aims for operation in licensed bands below 3.5 GHz. Moreover, 802.16e is looking at the mobile user walking around with a PDA or laptop, while 802.20 addresses high-speed mobility issues (speeds up to 250 km/h). More important, the 802.16e specification will be based on an existing standard (802.16a), while 802.20 is starting from scratch.

3.2 Scalability of the network architecture and protocols

One of the major problems to address while building a multihop wireless backhaul network is the scalability of both the network architecture and protocols. There are several research efforts to improve the capacity of wireless mesh networks by exploiting such alternative approaches.

- *Multiple radio interfaces*: multiple channels and/or radio interfaces could increase network capacity by exploiting the independent fading across different frequencies or the orthogonality of frequency bands.

- *Multiple-input multiple-output techniques (MIMO)*: systems employing multiple antennas for both transmitting and receiving improve the capacity and reliability of wireless backbones by exploiting antenna diversity and spatial multiplexing. Diversity provides the receiver with several (ideally independent) replicas of the transmitted signal and is therefore a powerful technique to combat fading and interference. Spatial multiplexing divides the channel into multiple "*spatial channels*" through which independent data streams or signals can be coded and transmitted simultaneously.

  As a consequence, diversity techniques make the channel less fading, which is of fundamental importance for wireless backbones, where deep fades can occur and the channel changes slowly, causing fades to persist over a long period of time.

- *Beamforming antennas*: nevertheless, when strong interference is also present, diversity processing alone cannot improve the signal. To cope with interference, smart antennas or adaptive array processing can be utilized to enhance both the energy efficiency and multiple access interference rejection capability of the high-throughput wireless backbone. The key idea is to exploit the beamforming capability of the transmit/receive antenna arrays. The exploitation of directional transmissions could suffice to ensure a wireless backbone with high speed and a high degree of spatial reuse.

Although the use of multiple antennas at the wireless routers in combination with signal processing and coding is promising in providing a high-capacity wireless backhaul system, it is not enough to achieve a scalable wireless backbone. For instance, it is well known that as the number of users increases, random MAC protocols suffer from increased contention in the network. Moreover, users' traffic traversing the wireless backbone does not have a unique fixed destination, but rather can be delivered to any wired access point. In addition, several paths may exist at the same time to reach a given access point; path capacity and channel bandwidth could be highly variable. New scalable and distributed scheduling and routing protocols have to be designed to efficiently manage data traffic. These algorithms must be aware of the characteristics of the physical channel, which leads to the need for cross-layer design among physical and networking functions.

- *Opportunistic channel selection*: the literature focusing on cross-layering to optimize networking functions exploits multi-user diversity, that is, the condition when, in a system with many users, different users experience peaks in their channel quality at different time instants. For instance, in this case it is proved that the scheduler should allocate transmission opportunities to users with the most favorable channel conditions. The mesh network environment adds further degrees of freedom in the scheduling process, because the scheduling policies could exploit additional types of diversity such as spatial diversity and frequency diversity to enhance throughput. The design of scheduling policies for a multichannel, multihop, and multidestination system is extremely challenging because opportunistic selection of the high-quality channel cannot be performed locally in the single wireless router, but should be coordinated among all the wireless routers forming the backbone network. Consequently, the scheduling process in a wireless mesh network is intrinsically distributed, where the coordination among wireless routers is achieved via the exchange of messages containing information on channel conditions and traffic demands.

The MAC and PHY layers play a crucial role in providing the scalability and performance optimization required for wireless mesh networking. Most of the current routing protocols for multihop communications typically choose optimized (in the sense of minimum hop count, maximum lifetime of the route, or maximal residual power in the nodes along the route) paths without taking link quality into account. Therefore, several research efforts are devoted to the definition of novel routing metrics that correctly account for the loss rate and channel bandwidth of each link forming the path.

The routing protocol for a wireless backbone needs to be redesigned not only to deal with the path diversity, but also to address the distinct nature of the wireless backbone network with respect to a general ad hoc network. The user traffic to the Internet does not need to follow the same path, but could be forwarded to any of the Internet egress points in the multihop wireless backhaul network. Consequently, the routing protocol should opportunistically select the "*best wire*" toward any wired access point. The routing protocol could effectively benefit from the existence of nonmobile powered wireless infrastructure to exploit hybrid ad hoc routing that combines both proactive and reactive techniques.

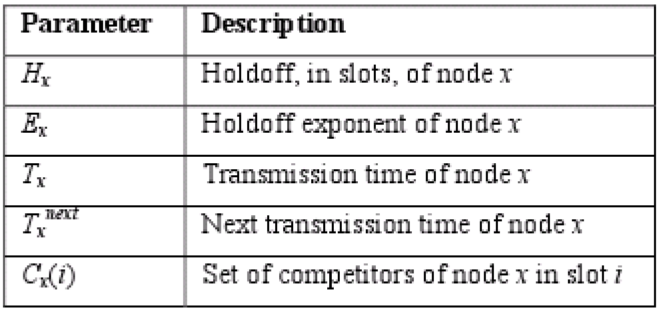
In the wireless backbone formed by stationary wireless routers, it is reasonable to envision that a link-state routing protocol analogous to a traditional wired routing protocol such as *Open Shortest Path First* (*OSPF*) could be used.

4 Mesh election procedure

“Delight yourself in the LORD,
and he will give you the desires of your heart.
Commit your way to the LORD;
trust in him, and he will act.”
— *Psalm 37:4-5 (ESV)*

In this section we take the concepts previously viewed relate to the “Mesh Election Procedure” to introduce the topic of the simulations that we’ll investigate later.

To describe the mesh election procedure we first introduce the notation that will be used, which is reported in Table 4.1 for a generic node *x*.



Parameter	**Description**
H_x	Holdoff, in slots, of node x
E_x	Holdoff exponent of node x
T_x	Transmission time of node x
T_x^{next}	Next transmission time of node x
$C_x(i)$	Set of competitors of node x in slot i

TABLE 4.1 – NOTATION.

We will not distinguish between the BS and SSs and we will refer to both as *nodes*, which is the common name in the literature for WMNs. In IEEE 802.16, a *logical link* (hereafter *link*) is set up between any two nodes, called *one-hop neighbors* (or *neighbors*), provided that they can communicate directly with each other. A link establishment procedure is provided for this purpose. Moreover, we define *two-hop neighbors* as nodes that have at least one common neighbor, but are not neighbors themselves.

As already introduced, the mesh election procedure is used to coordinate the access to the control slots in a distributed collision-free manner. To this aim a node refrains from transmitting in control slots reserved by one- and two-hop neighbors. The latter are referred to as *competitors* of that node. Specifically, each node resolves a *virtual* contention by exploiting the information collected in control messages sent by its neighbors during previous control slots. The mesh election procedure enforces a strict precedence among the competitors, i.e. only one competitor is the winner of the contention. A node contends through virtual contention at each slot until it wins.

Note that collision-free access is guaranteed under the assumption that collision only happens at the receiving node if two or more neighbors transmit at the same time. In other words, the overall interference due to transmissions of nodes two or more hops away from the receiving node is assumed to be negligible. This assumption is motivated by the fact that, in a WMN backbone, nodes are considered to be fixed and links stable, and therefore mutual interference can be controlled by carefully planning the network topology [2].

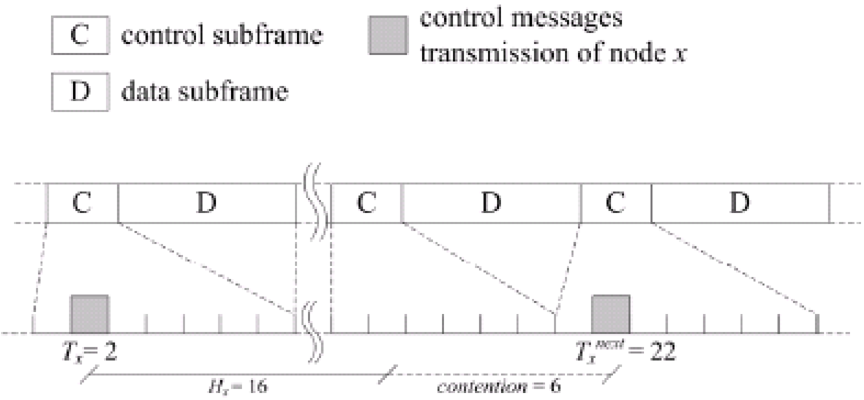


FIGURE 4.2 – CONTROL SLOT ACCESS OF NODE X.

We now illustrate how nodes access control slots by means of a simple example, depicted in Fig. 4.1. First of all, note that from the mesh election procedure standpoint, control sub-frames can be seen as a continuous sequence of control slots. Furthermore, we assume without loss of generality that slots are numbered in ascending order.

The IEEE 802.16 standard specifies that node *x* must defer its transmission by a holdoff time, namely H_X , in units of slots (e.g. 16 in Fig. 4.1), before contending again for transmitting since its last access to a control slot. This constraint must be taken into account by any node *x* when computing its next slot to transmit control information through the virtual contention. We refer to the next slot selected by node *x* for control access as T_X^{next}. The latter is the first slot in which node *x* is the winner of the virtual contention. In the example in Fig. 4.1, node *x* runs the mesh election procedure right before transmitting on slot T_X (i.e. slot 2). First, node *x* skips H_X=16 slots (solid line) from slot T_X=2 before virtually contending according to the holdoff time constraint. Then it competes for access in each subsequent control slot, losing the virtual contention for 6 slots (dashed line), until it wins on slot 22, which is thus selected as T_X^{next}.

Therefore, to compute T_X^{next}, node *x* has to verify whether it is the winner of the virtual contention on a given slot T_X or not. This is performed as follows. First, node *x* derives the set C_X (*i*) of one- and two-hop neighbors that need be considered as competitors for each slot subject to virtual contention, i.e. $i \geq T_X + H_X$. It then applies a pseudo-random function, specified by the IEEE 802.16 standard, to sort the set of nodes C_X *(i) U {x}*. The exact procedure that node *x* uses to derive C_X (*i*) is reported in the IEEE 802.16 standard. The earliest slot where node *x* is the winner of the contention, i.e. it has the highest priority according to the pseudo-random function, is selected as T_X^{next}. It is worth noting that the pseudo-random function guarantees that every node will *eventually* win the contention for some slot *i*. The interested reader can find the formal definition of the pseudo-random function in subsection 6.3.7.5.5.6 of the IEEE 802.16 standard [3].

As specified by the IEEE 802.16 standard, the holdoff time H_X is equal to:

$$E_X = 2^{4+E_X}$$

where $E_x \in [0, 7]$ is a system parameter called *XmtHoldoffExponent* which can be configured on a per node basis. Thus, as mentioned earlier, two consecutive slot accesses by the same node are separated by at least 16 slots, when $E_x = 0$.

4.1 Dynamic Adaptation of the Holdoff Time

A node x must take into account the holdoff time H_X when computing its next slot to transmit control information through the virtual contention. The value of the holdoff exponent E_X (that determines the holdoff time H_X) is set manually by an administrator of the network. This procedure is not trouble-free, because must take into account the topology of the network and the amount of competitors. In addition this procedure needs on every node.

We want that every node can calculate the own optimum holdoff time automatically and communicate it to the on-hop neighbors.

4.2 AIMD (contention time based)

The first algorithm[4] implemented to obtain a dynamic adaptation of the holdoff time is based on the time of contention to get the next opportunity for transmission (T_x^{next}). The figure 4.3 show the algorithm.

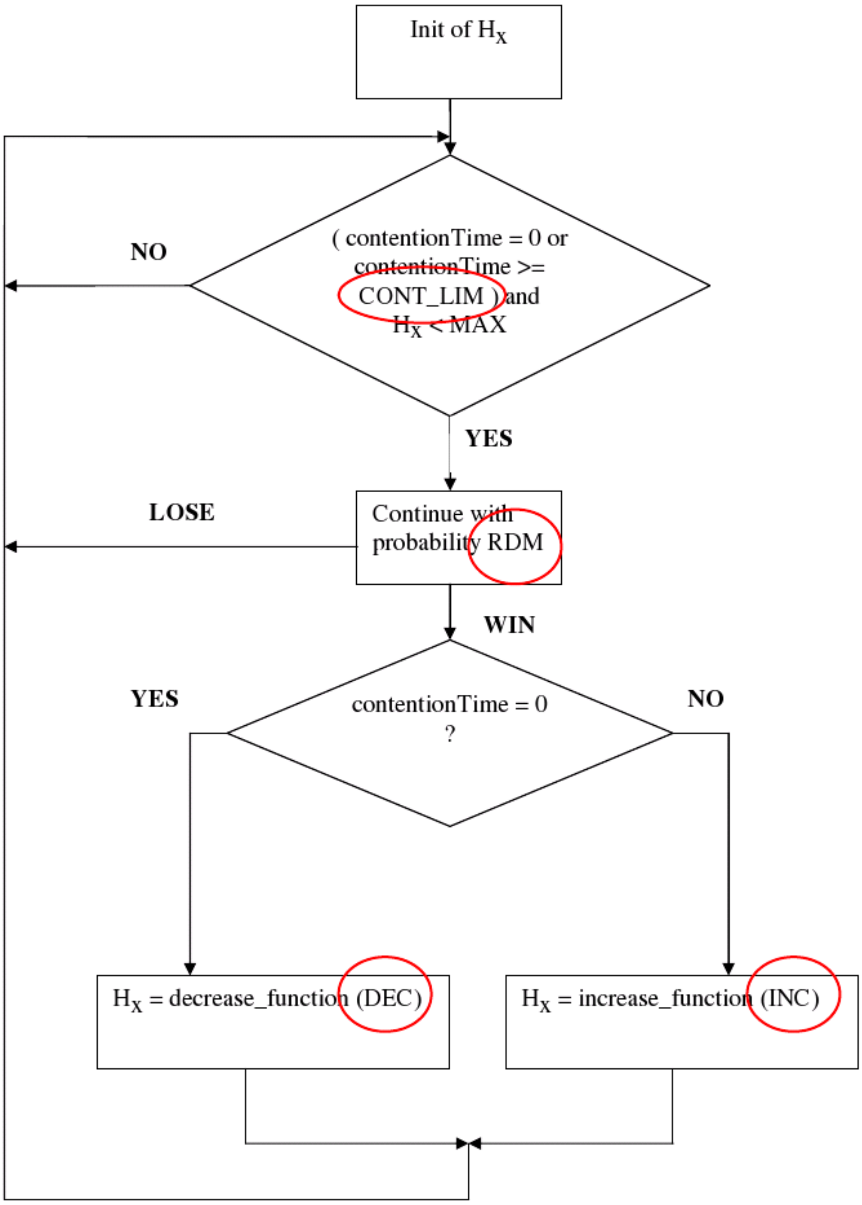

Init of H_X
NO
(contentionTime = 0 or contentionTime >= CONT_LIM) and H_X < MAX
YES
LOSE
Continue with probability RDM
WIN
YES
contentionTime = 0 ?
NO
H_X = decrease_function (DEC)
H_X = increase_function (INC)

FIGURE 4.3 – AIMD ALGORITHM.

[4] AIMD means Additive Increase Multiplicative Decrease

Each transmission of DSCH message, the node check the contention time (indeed check the average contention time from the last holdoff time change) and decides whether to increase or decrease the holdoff time. Specifically increase the holdoff time if the contention time exceed *CONT_LIM* (contention limit) and decrease if the contention time is equal to zero. Otherwise, if contention time is between zero and *CONT_LIM,* the holdoff time is considered optimum.

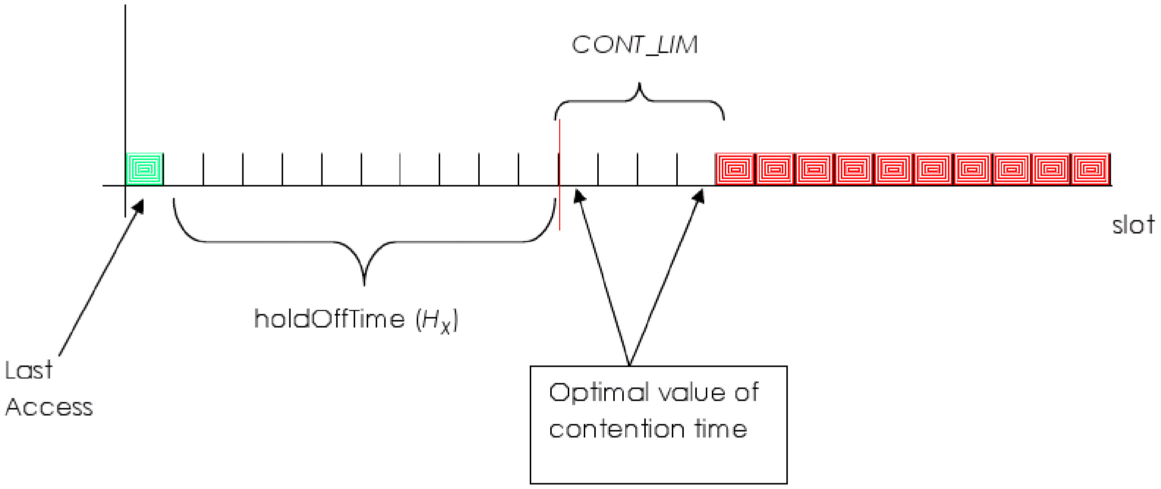


FIGURE 4.4 – AIMD SLOT ACCESS.

When the node decides that the holdoff time must be changed, the change occurs with probability *RDM.*

DEC and *INC* are the constant passed to the relative function which determine the value of decrement or increment.

The code of the two functions is written below:

```
int decrease_function (DEC){
    return (unsigned int)ceil(holdOffTime * DEC);
}

int increase_function (INC){
    return (unsigned int)floor(holdOffTime + (contention_avg *
           INC));
}
```

So the increment is additive and the decrement is multiplicative.

CONT_LIM is calculate as

$$tolerance * H_x$$

where *tolerance* is a parameter to set properly.

4.3 MIAD

This algorithm was created consequently of the results obtained in section 5.1.

It[5] approach the problem in a radical different way as shown in figure 4.5.

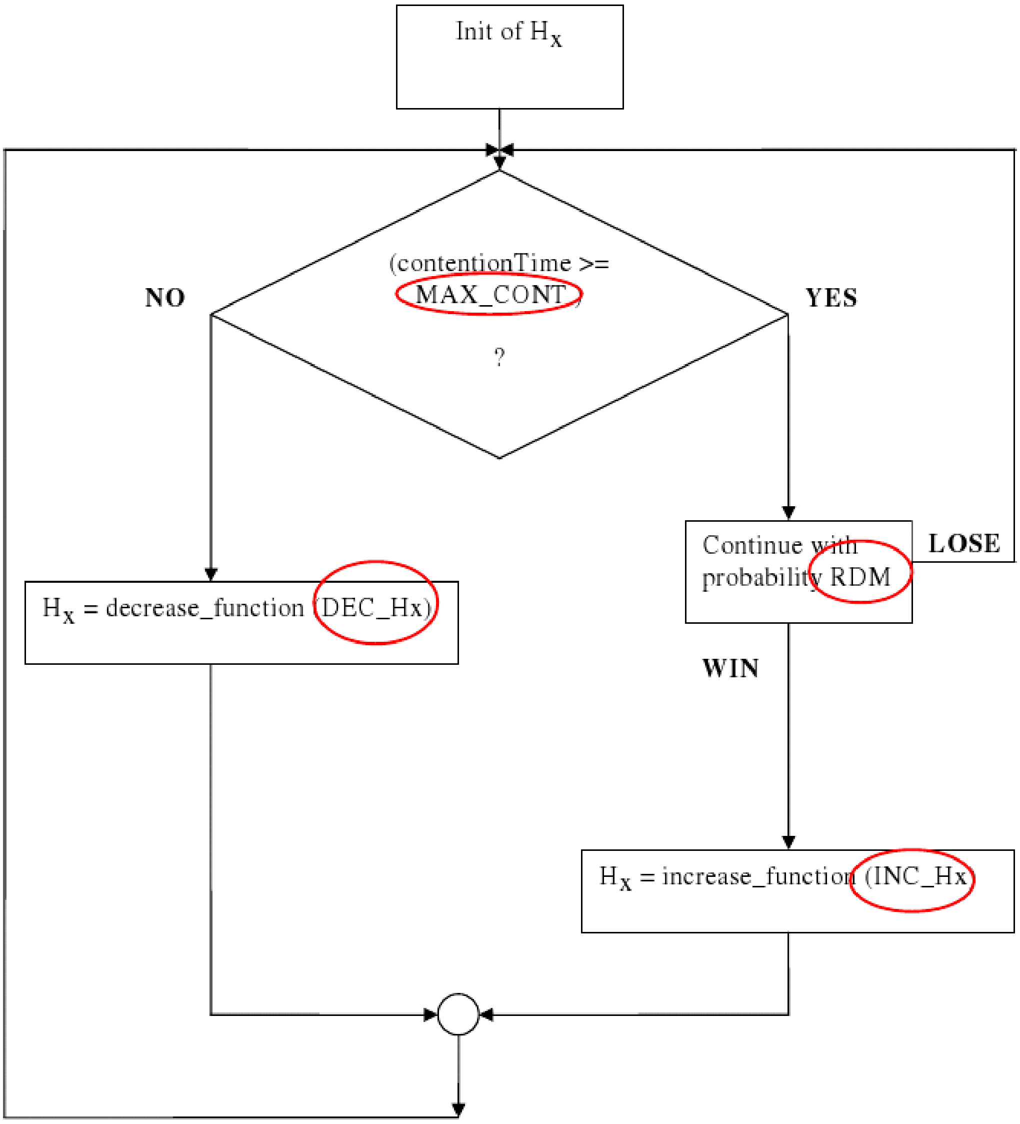


FIGURE 4.5 – MIAD ALGORITHM.

[5] MIAD means Multiplicative Increase Additional Decrease

Specifically, it doesn't minimize the contention time, but decrease the holdoff time at every control slot access except when the contention time exceed *MAX_CONT* . In this case the node increase the holdoff time with probability *RDM*.

The code of the functions *increase_function()* and *decrease_function()* is written below:

```
int decrease_function (DEC_Hx){
    return holdoffTime - (unsigned int)ceil(holdOffTime *
    DEC_Hx);
}

int increase_function (INC_Hx){
    return (unsigned int)ceil(holdOffTime * INC_Hx);
}
```

and MAX_CONT is calculate as

$$tolerance * H_x$$

where *tolerance* is a parameter to set properly and, unlike the AIMD algorithm, now can assume values greater than 1.

5 Performance evaluation

“But he was pierced for our transgressions,
he was crushed for our iniquities;
the punishment that brought us peace was upon him,
and by his wounds we are healed.“
— *Isaiah 55:3 (NIV)*

The parameters used in simulations are not totally compliant with the IEEE 802.16 standard [3] because we introduce the possibility to use an holdoff time less than 16 (2^{4+E_x}). The frame duration is 4 ms because depend on the channel bandwidth which is 10 MHz. According to the standard, only one channel is used to transmit control information, thus the use of multiple channels is not considered. Furthermore, there is no data traffic, since the latter does not impact on the transmission in control slots.

The main performance index that have been considered in order to assess the distributed election procedure performance. is the *access interval* (*in time units*) which is defined as the time interval between two subsequent control message transmissions of a node.

We implemented the coordinated distributed mode of IEEE 802.16 mesh in the *ns2* network simulator [4]. The simulation output analysis was carried out using the method of independent replications.

The duration of each simulation run varied depending on how the specific system was configured.

5.1 Performance evaluation of AIMD

In this scenario we evaluate the performance of the mesh election procedure implementing the algorithm described above with respect to the following system parameters:

- Frame duration, 4 ms;
- Number of control slot per frame, 8;
- Number of MSH-DSCH frames between two consecutive MSH-NCFG frames, 32;
- XmtHoldoffExponent of nodes, unused;
- *DEC* (decrease factor), 0.5;
- *INC* (increase factor), 0.5.

To this aim we consider a network of 21 nodes, with an increasing number of neighbour (Branches) for each node, from 2, i.e. the connectivity graph is a *ring,* to 20, i.e. the connectivity graph is a *clique*. Note that this scenario is hardly of interest for current deployments of WMSs. Nonetheless, it allows us to derive the impact of the parameters above on the system performance with varied node density.

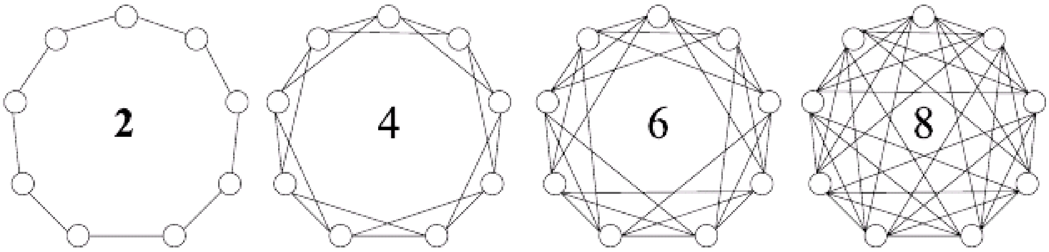


FIGURE 5.1 – MULTIRING (FROM RING TO CLIQUE)

For a better understanding of the graphics we report a notation table:

Parameter	**Description**
Randomness	*RDM*
Tolerance	Parameter used to calculate *CONT_LIM*
Legacy	Standard IEEE 802.16

TABLE 5.2 – NOTATION.

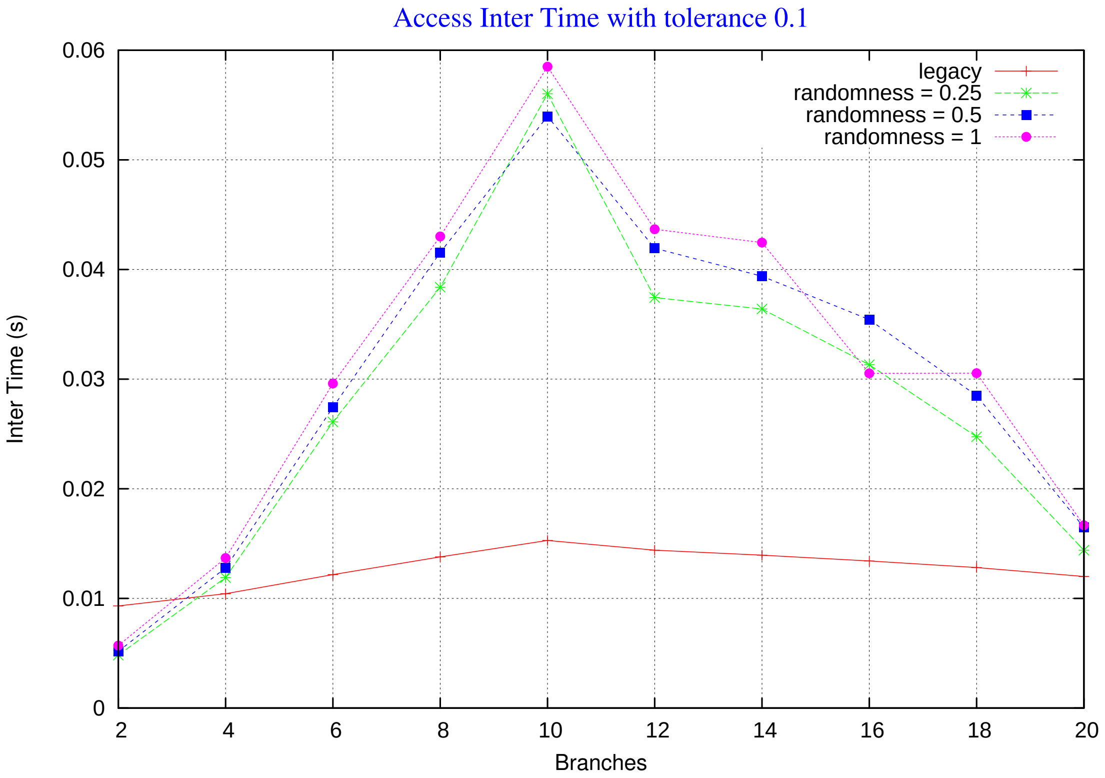


FIGURE 5.3 – AIMD ACCESS INTER TIME WITH TOLERANCE 0.1.

In figure 5.3 we report the average access interval (in time units) versus the number of neighbor, with fixed *tolerance* (constant to determine *CONT_LIM*). As can be seen the average access interval in the legacy mode is much lower regardless of *randomness* (*RDM*).

In figure 5.4 we set *randomness* to 0.5 (the best result in the previous graph considering the worst case, i.e. 10 branches) and we analyze the performance by vary *tolerance* . As shown in the figure, the greater the value of *tolerance*, the smaller the average access interval.

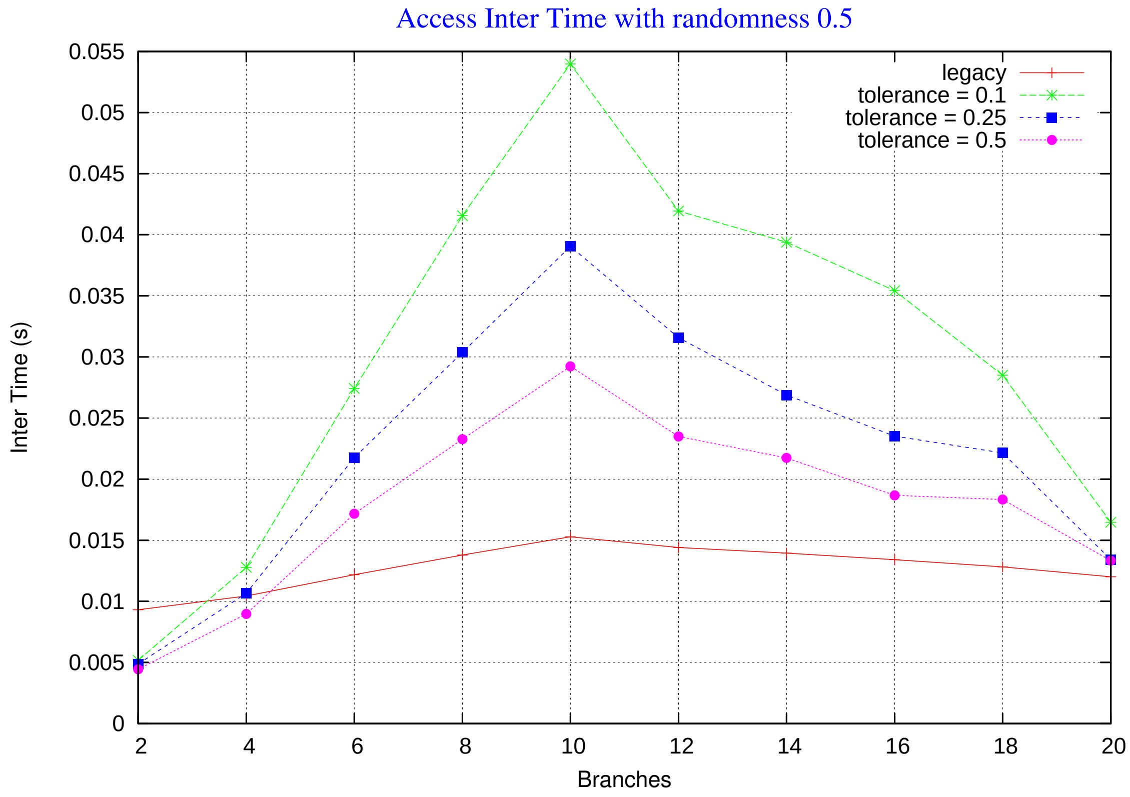


FIGURE 5.4 – AIMD ACCESS INTER TIME WITH RANDOMNESS 0.5.

Concluding, the greater the value of *tolerance*, the greater the value of *CONT_LIM* therefore understand that we must act less on the holdoff time to reach the legacy performance. This means that the first algorithm we have implemented don't approach the problem in the correct way.

This does not mean that the algorithm don't work.

Figure 5.5 shows the number of slots in which the node competes to win the virtual contention setting randomness to 0.25. As can be seen the contention slots are lower with the new algorithm compared to the legacy, achieving the goal of the algorithm. But this behavior don't permit to obtain a decrease of the average access interval because the algorithm tend to increase the holdoff time to decrease the contention time, but the increase is bigger of the advantage obtained by the decrease[6]. So, the same accesses are done in a bigger interval of time.

[6] The Next Transmission time is determinate by the Holdoff Time plus the Contention Time.

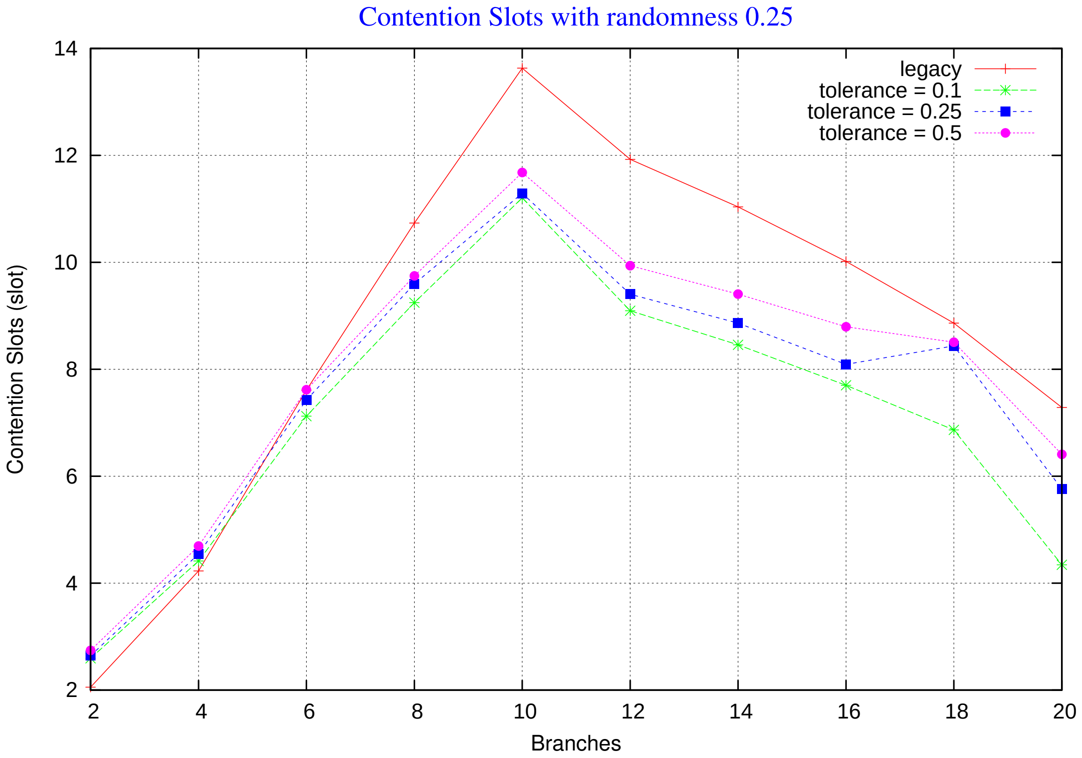


FIGURE 5.5 – AIMD CONTENTION SLOTS WITH RANDOMNESS 0.25.

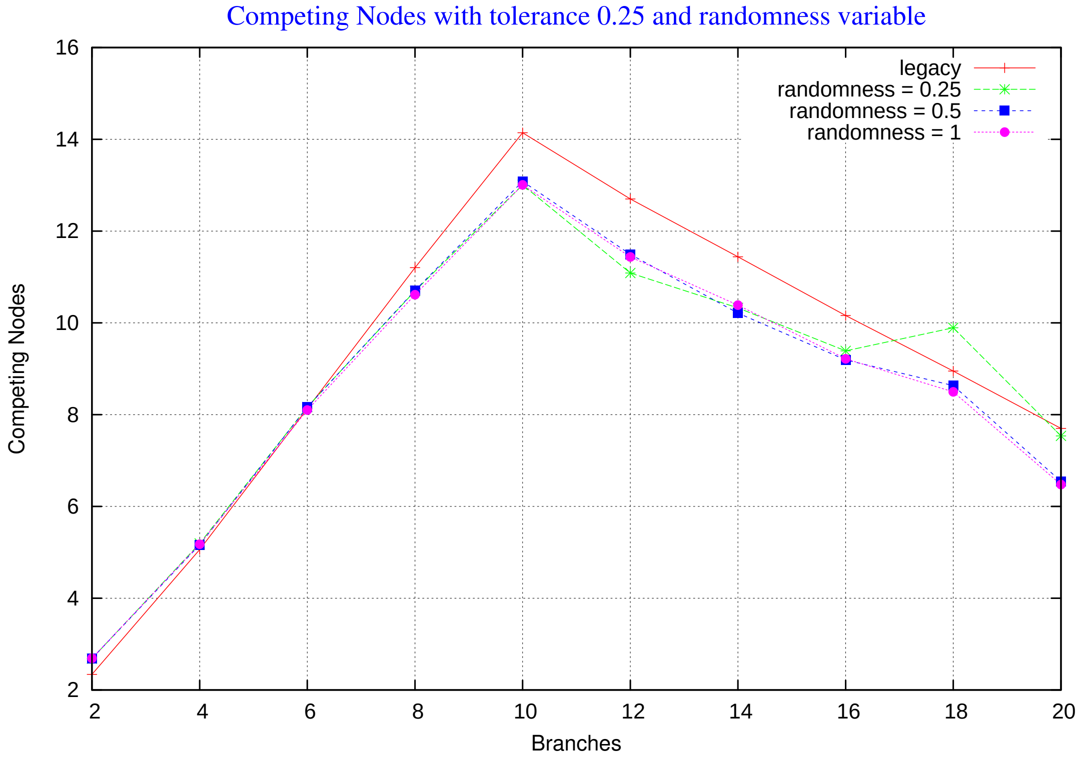


FIGURE 5.6 – AIMD COMPETING NODES WITH TOLERANCE 0.25.

Figure 5.6 shows the average number of nodes competitor in the virtual contention setting *tolerance* to 0.25. The competitors are less with the algorithm implemented and this confirms what we have said. The nodes competitors are less because the same number of nodes access the control channel in a longer time.

5.2 Performance evaluation of MIAD

In this scenario we evaluate the performance of the mesh election procedure implementing the MIAD algorithm with respect to the following system parameters:

- Frame duration, 4 ms;
- Number of control slot per frame, 8;
- Number of MSH-DSCH frames between two consecutive MSH-NCFG frames, 32;
- XmtHoldoffExponent of nodes, unused;
- *DEC* (decrease factor), 0.05;
- *INC* (increase factor), 2.

For a better understanding of the graphics we report a notation table:

Parameter	**Description**
Randomness	*RDM*
Tolerance	Parameter used to calculate *MAX_CONT*
Increase factor	INC_Hx
Decrease factor	DEC_Hx
Legacy	Standard IEEE 802.16

TABLE 5.7 – NOTATION.

To evaluate the performance we use a multi ring topology, already shown in figure 5.1, with 21 nodes and growing number of neighbour (from 2 to 20).

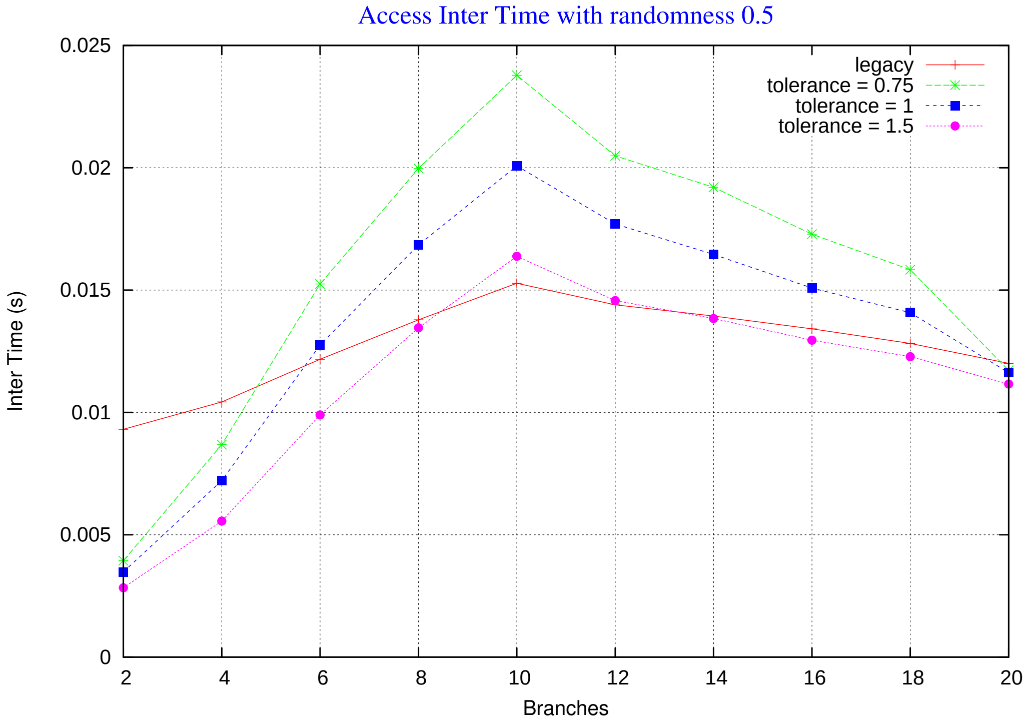


FIGURE 5.7 – MIAD ACCESS INTER TIME WITH RANDOMNESS 0.5.

Figure 5.7 shown the average access interval setting randomness (*RDM*) to 0.5 with *tolerance* ∈ { 0.75, 1, 1.5 }. As can be seen the performance of the legacy mode are still better in the worst case, but the curve with tolerance 1.5 has a lower access inter time before and after the worst case.

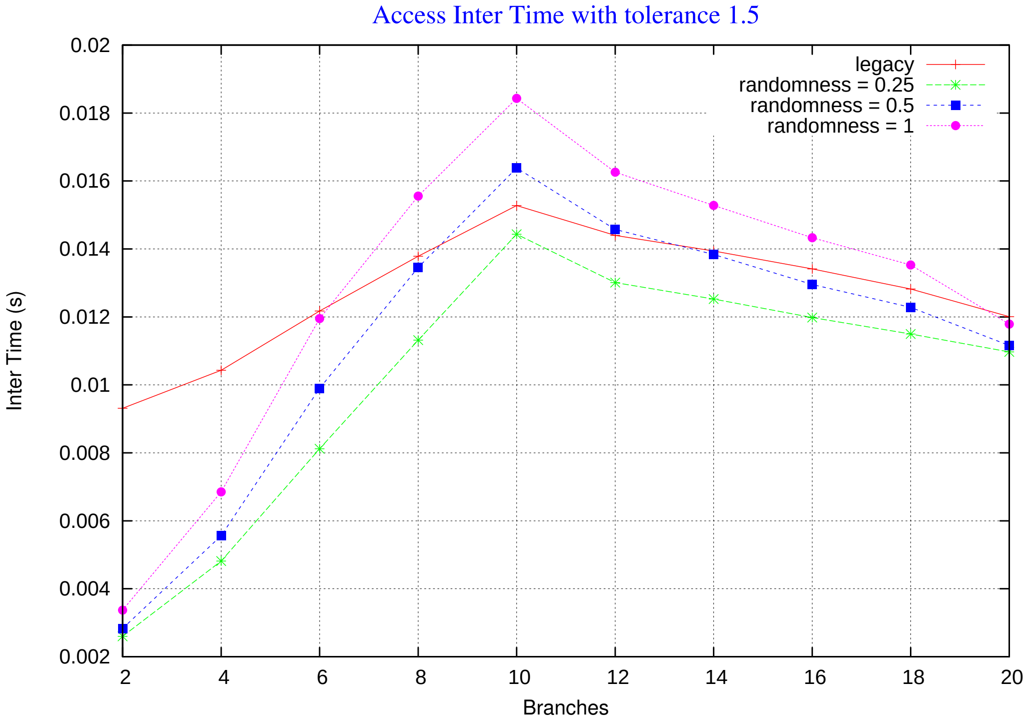


FIGURE 5.8 – MIAD ACCESS INTER TIME WITH TOLERANCE 1.5.

Setting tolerance to 1.5 (the curve with best performance seen in figure 5.7) and changing randomness we see, in figure 5.8, that the curve with randomness 0.25 has better performance than the legacy mode.

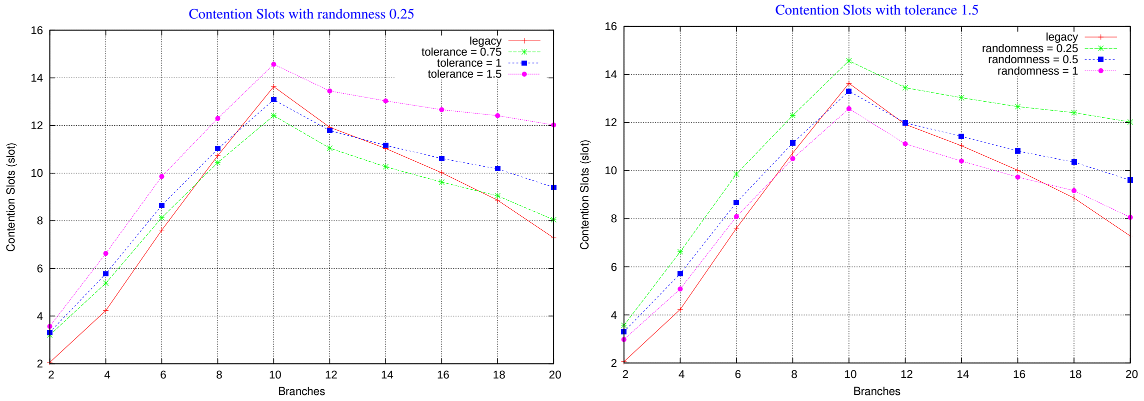


Figure 5.9 – MIAD Contention Slots with randomness 0.25 and with tolerance 1.5.

Figure 5.9 confirms that contention time is not proportional to the average access interval, because the curve that has the best performance in terms of average access interval (tolerance = 1.5 and randomness = 0.25), has the worst performance in terms of contended slots. This is due to the best use of the channel because the same number of nodes access the control channel with a lower average time.

5.2.1 Dimensioning

Found that the MIAD algorithm work properly, we want to dimension RDM, DEC_Hx, INC_Hx, MAX_CONT (tolerance), to get the best performance.

To do this, we use the same simulation environment described above but with a multi ring topology formed by 61 nodes and 30 branches, because we want do the simulations in a pessimistic situation.

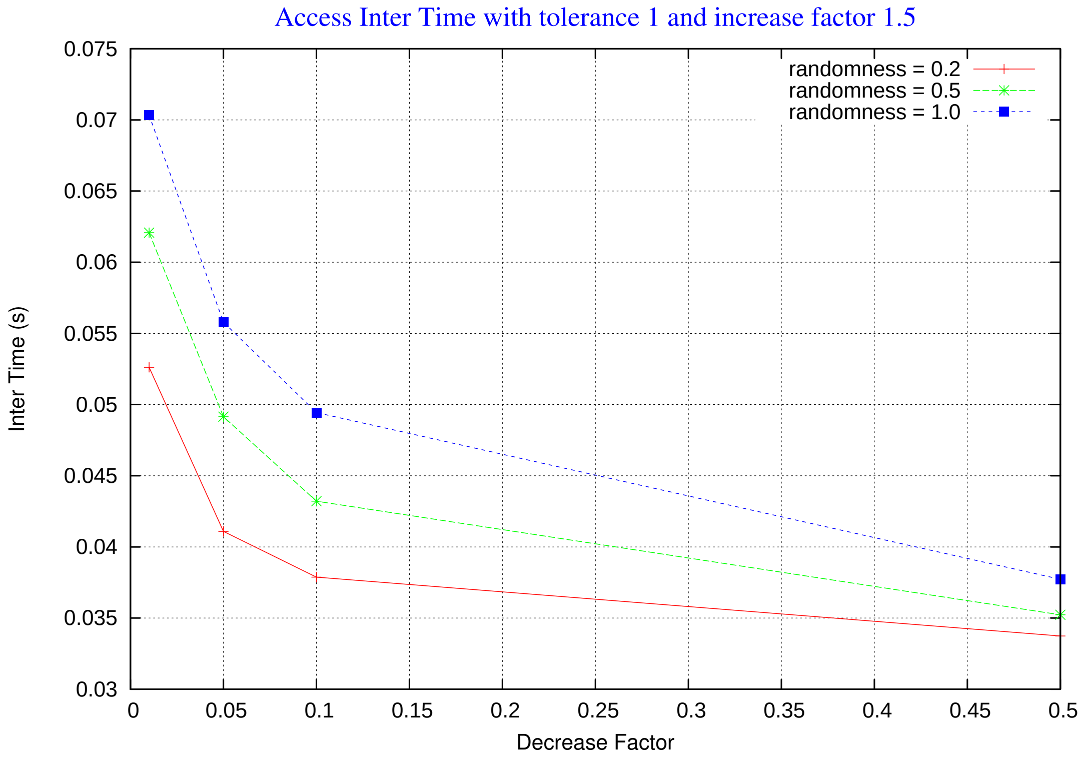


FIGURE 5.10 – ACCESS INTER TIME WITH TOLERANCE 1 AND INCREASE FACTOR 1.5.

In figure 5.10 we set tolerance to 1 and the increase factor to 1.5 varying randomness and the decrease factor from 0.2 to 1 and from 0.01 to 0.5 respectively. As can be seen, we have the best performance in terms of average access interval with randomness = 0.2.

Starting from the previous result we fix the parameter with the best performance to find the others.

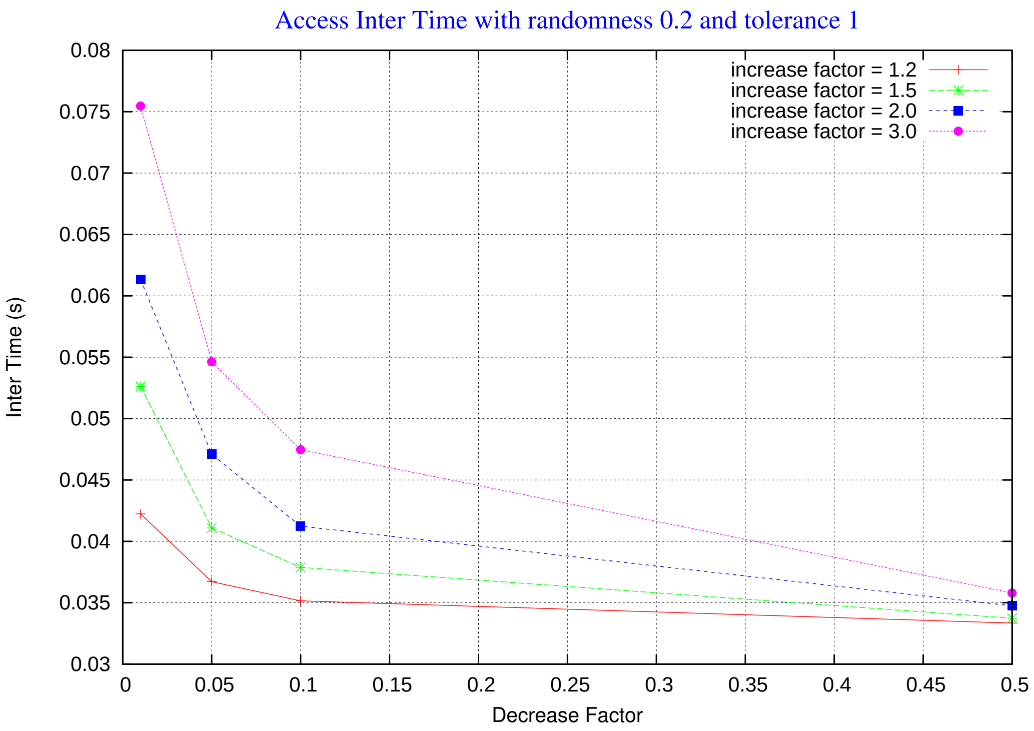


FIGURE 5.11 – ACCESS INTER TIME WITH RANDOMNESS 0.2 AND TOLERANCE 1.

Figure 5.11 illustrate the curves with different increase factor setting randomness to 0.2 and tolerance to 1. This graphic show that when we use an increase factor = 1.2 we have a lower average access interval.

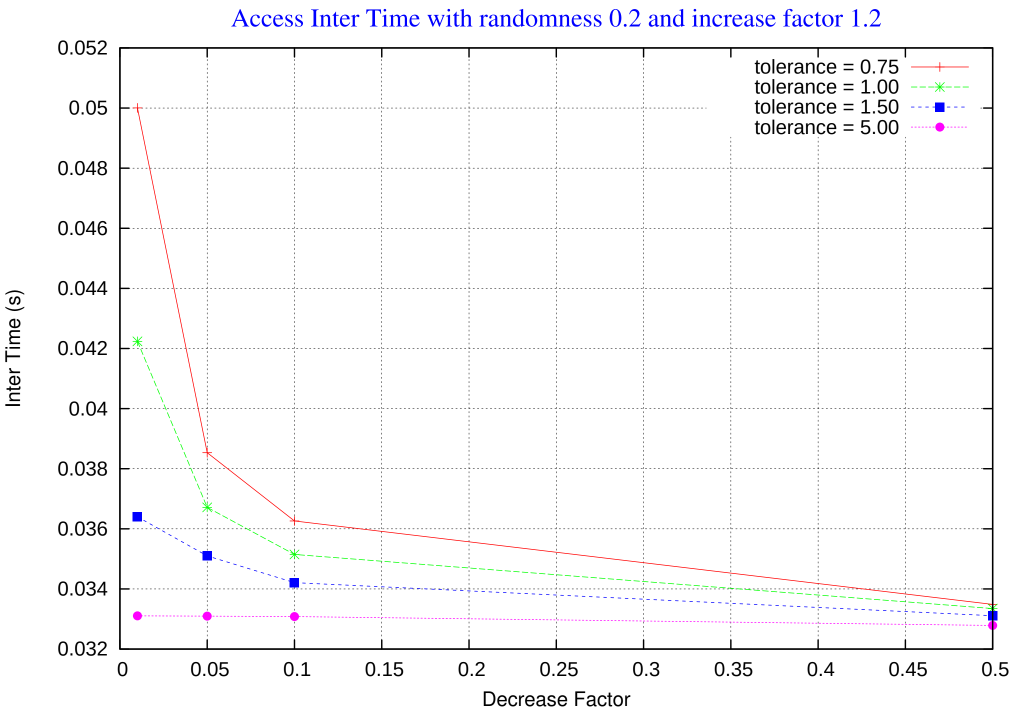


FIGURE 5.12 – ACCESS INTER TIME WITH RANDOMNESS 0.2 AND INCREASE FACTOR 1.2.

Now we have two parameters to fix: randomness 0.2 and increase factor 1.2. Figure 5.12 report the average access inter time varying tolerance. As can be seen, with tolerance = 5 we obtain the best performance.

The three graphics analyzed say that greater decrease factor is preferable (decrease factor = 0.5).

In summary we have the best performance of the algorithm with the following parameters:

- Randomness = 0.2 (lower)
- Increase factor = 1.2 (lower)
- Decrease factor = 0.5 (greater)
- Tolerance = 5 (greater)

Recall that, in MIAD, lower randomness and increase factor, and grater tolerance and decrease factor, means a lower holdoff time. The curves in graphics 5.10, 5.11, 5.12 seems that still fall and this means that a lower holdoff time is preferred. To ascertain this behaviour we need simulations with static holdoff time.

.

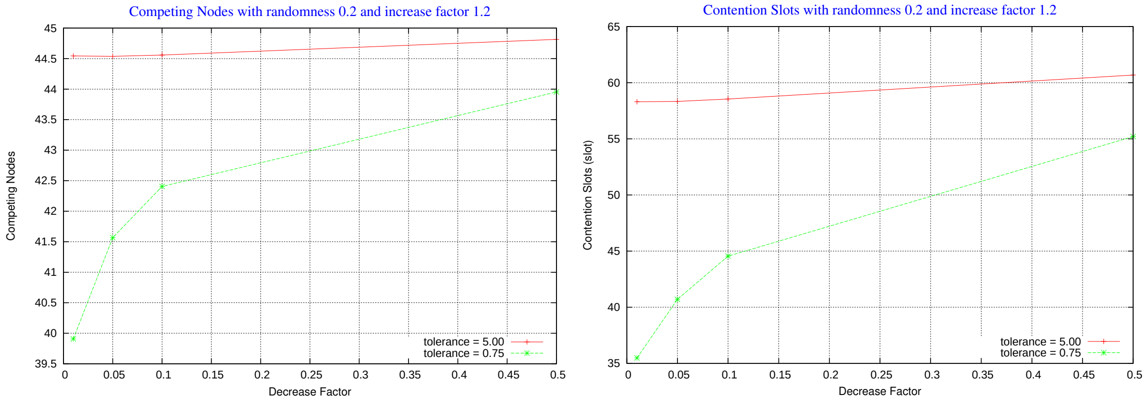


FIGURE 5.13 – COMPETING NODES AND CONTENTION SLOTS WITH RANDOMNESS 0.2 AND INCREASE FACTOR 1.2.

Finally, figure 5.13 show the competing nodes and the contention slots of two simulations with different tolerance and the same randomness and increase factor. As can be seen, the curve with tolerance = 5, which has the best performance in terms of average access interval, has a greater number of competing nodes and compete the virtual contention for a long time. The cause has already been analyzed previously in the same paragraph.

5.2.2 Static Holdoff time

We now estimate the average access interval when the graph of the network is a multi ring with 101 nodes and 50 branches, hence hypothetically the worst condition to have a low holdoff time. This simulations allow as to understand if there is a minimum holdoff time that offer lower access inter time different than holdoff time = 1.

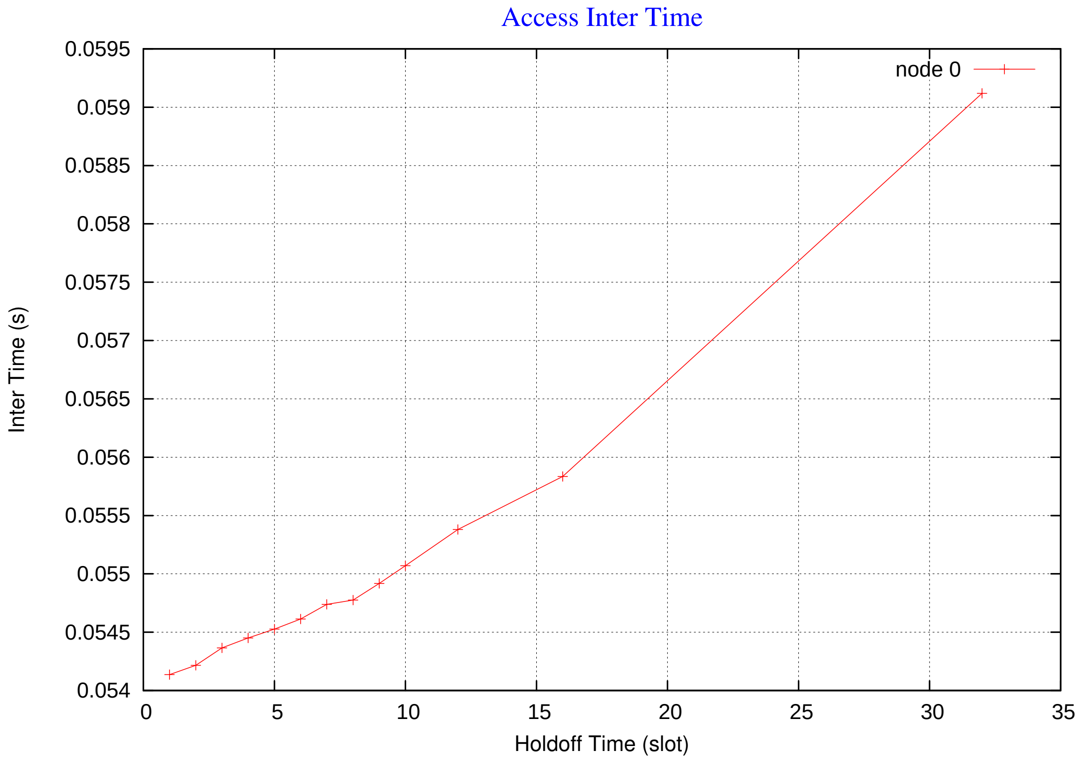


FIGURE 5.14 – ACCESS INTER TIME WITH GROWING HOLDOFF TIME.

Figure 5.14 show the average access interval of a generic node with growing holdoff time (from 1 to 32). We can see that the minimum access inter time corresponds to holdoff time = 1. This is an important result, because obtained with a relevant number of nodes. Probably we can obtain a minimum access inter time with holdoff time greater than 1, increasing the number of nodes moreover, but is not relevant for real application.

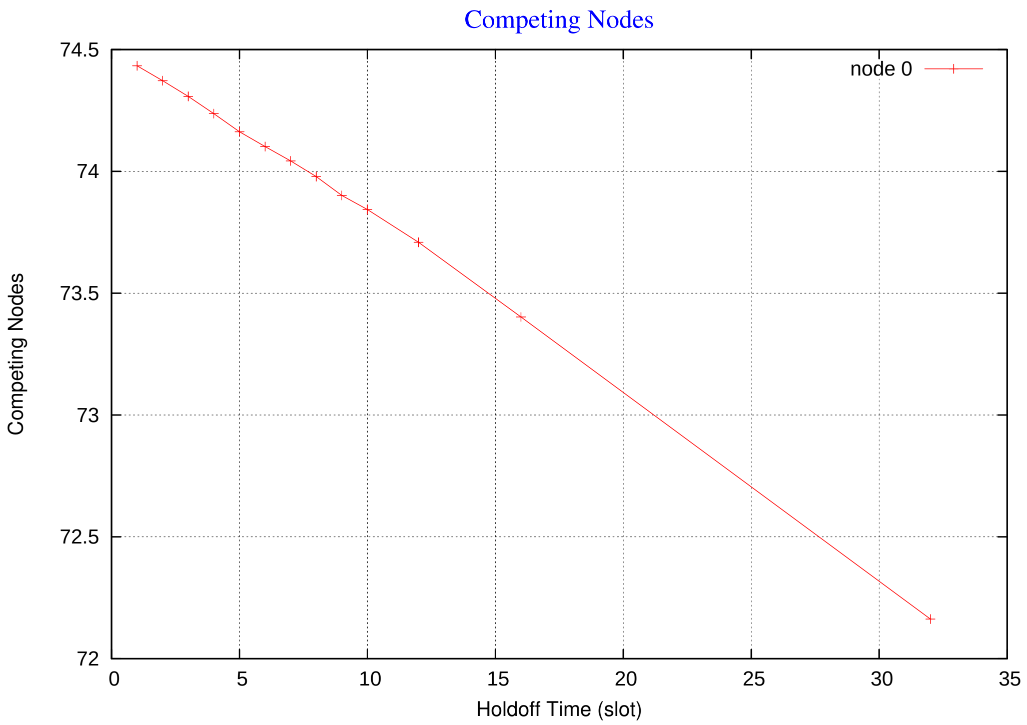


FIGURE 5.15 – COMPETING NODES WITH GROWING HOLDOFF TIME.

As we can guess the number of nodes competitors in the election procedure is inversely proportional to the holdoff time and this is confirmed by figure 5.15.

5.2.3 Star topology

In this paragraph we discuss the performance in terms of average access inter time when the graph of the network is a star.

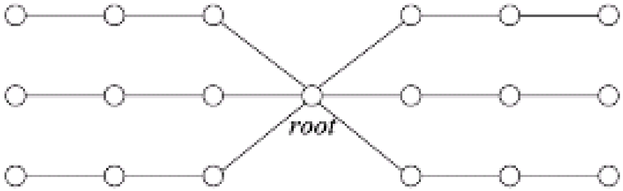


FIGURE 5.16 – STAR TOPOLOGY.

Specifically we collect the statistics from the root growing the number of braches of the star from 1 to 80 with holdoff time constant to the value 1 or 16 (minimum value of holdoff time in the standard IEEE 802.16).

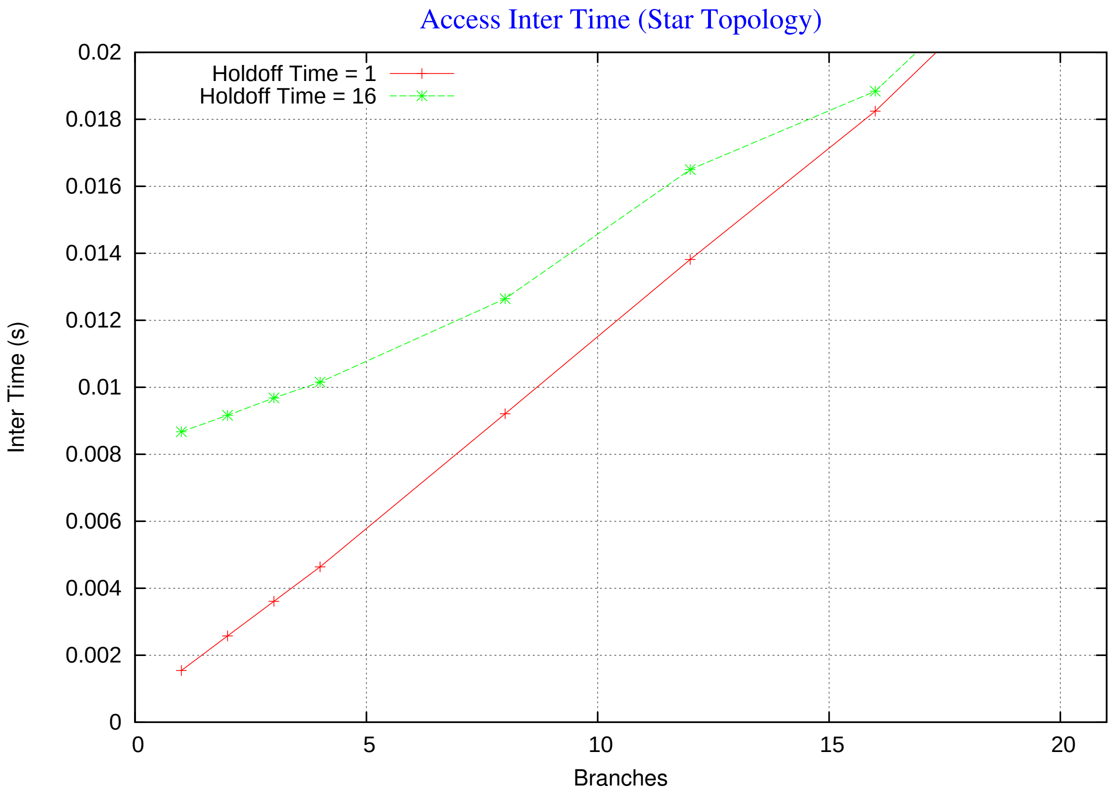


FIGURE 5.17 – ACCESS INTER TIME (STAR TOPOLOGY)

Figure 5.17 show the result of the simulation until 20 branches. As can be seen the average access interval with holdoff time = 1 is always under the same curve with holdoff time = 16. The results confirm the previous simulations.

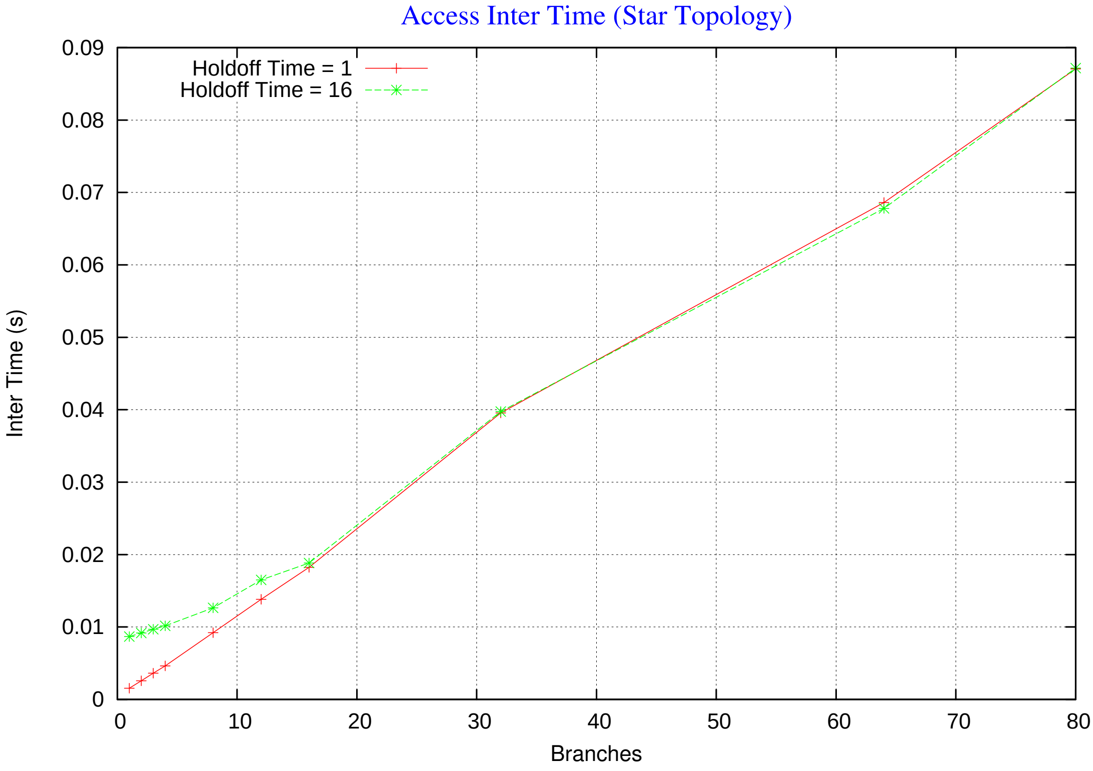


FIGURE 5.18 – ACCESS INTER TIME UNTIL 80 BRANCHES (STAR TOPOLOGY).

From figure 5.18 we see which increasing the braches the two curves collide together, but a network with so many branches is not of interest to applications.

In conclusion, we can say that an holdoff time = 1 give the lower average access inter time in every common real application.

5.2.4 Simulations with traffic

We now evaluate the performance of the network with bursty traffic, in terms of the average throughput, average end-to-end delay and average access interval. Specifically, we define the end-to-end delay (or *delay*) of a packet as the time interval between the arrival time of this packet at the network layer of the sender node, and the time when this packet is completely delivered to the network layer at the destination node. Packet generation of each traffic flow is based on the procedure proposed in [7] as the reference traffic model for characterizing the performance of IEEE 802.16 networks: a best-effort traffic flow is built from the super-imposition of four Interrupted Poisson Processes (IPPs), generating packets with a constant size of 192 bytes. The average offered load for each traffic source is about 125kb/s.

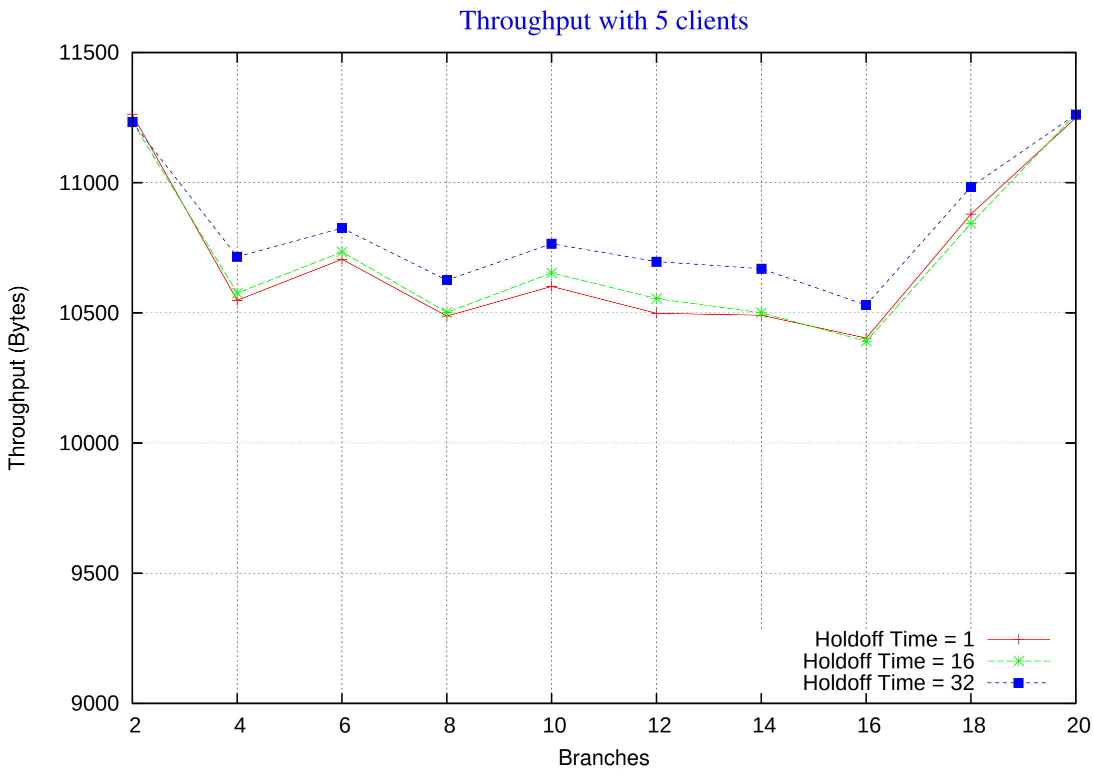


FIGURE 5.19 – THROUGHPUT WITH 5 CLIENTS.

The network consists of 21 nodes interconnected as a multi ring (fig. 5.1) where the number of branches grown from 2 to 20.

Figure 5.19 shown the average end to end throughput when the traffic is the aggregation of 5 clients (served by mesh routers). As can be seen, when holdoff time = 1 we haven't the best performance in terms of throughput (even if it does not differ too much). Figure 5.20 confirms that an holdoff time = 1 give the lower average access inter time. But this doesn't means that the throughput is higher too.

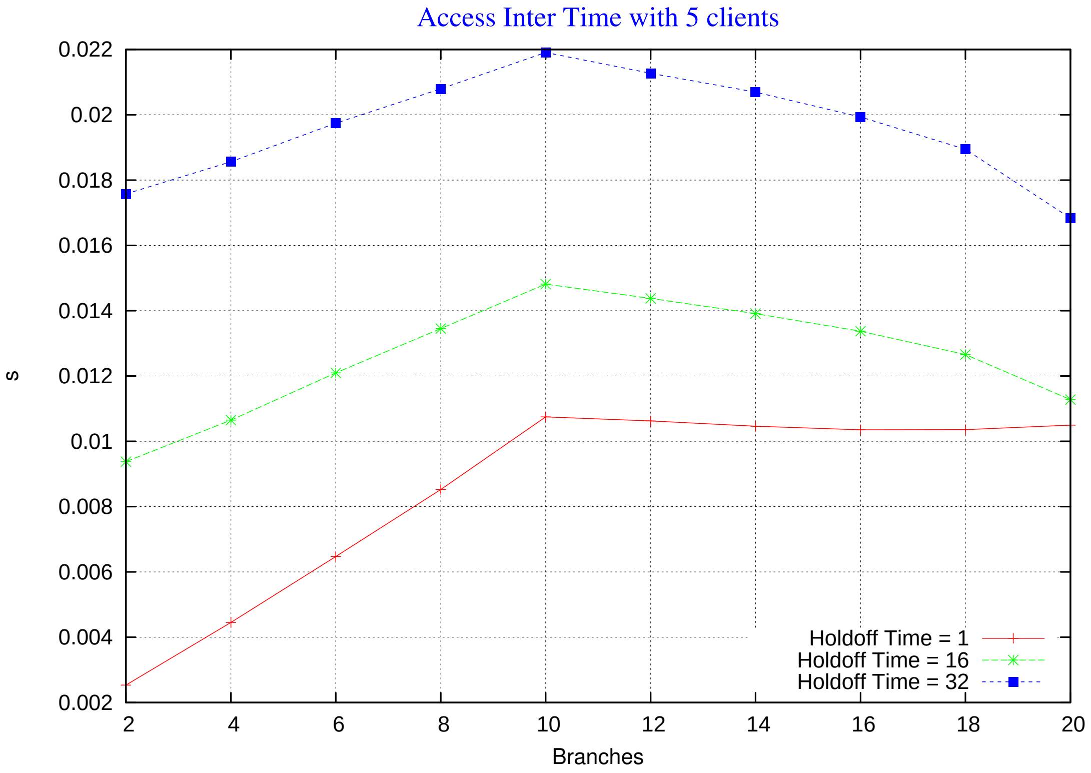


FIGURE 5.20 – ACCESS INTER TIME WITH 5 CLIENTS.

The reason is that the advantage of a faster access of the control channel is less than the disadvantage of more three way handshake. But an holdoff time = 1 makes the network more dynamic. Specifically, as shown by figure 5.21, the average end-to-end one way delay with holdoff time = 1 decrease, because every node access the control channel faster facilitating multi-hop transmissions.

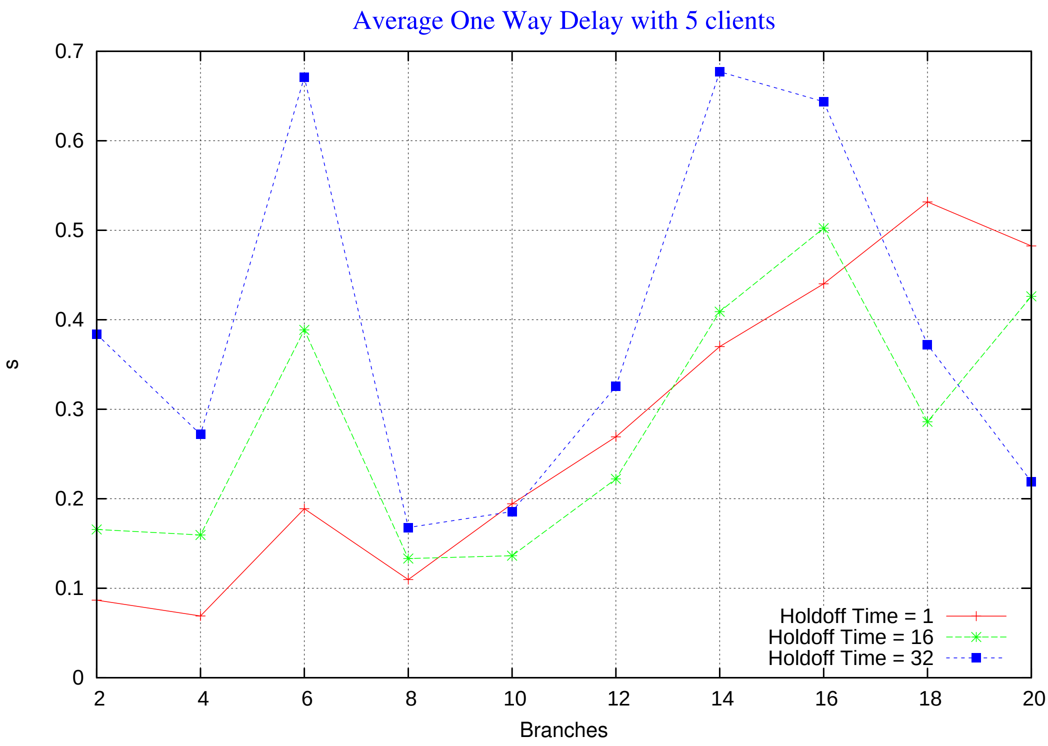


FIGURE 5.21 – AVERAGE ONE WAY DELAY WITH 5 CLIENTS.

Figure 5.22 and 5.23 show the same results of figure 5.19 and 5.20 respectively, but with a traffic aggregate of 10 clients (network heavily loaded) for a more complete analysis.

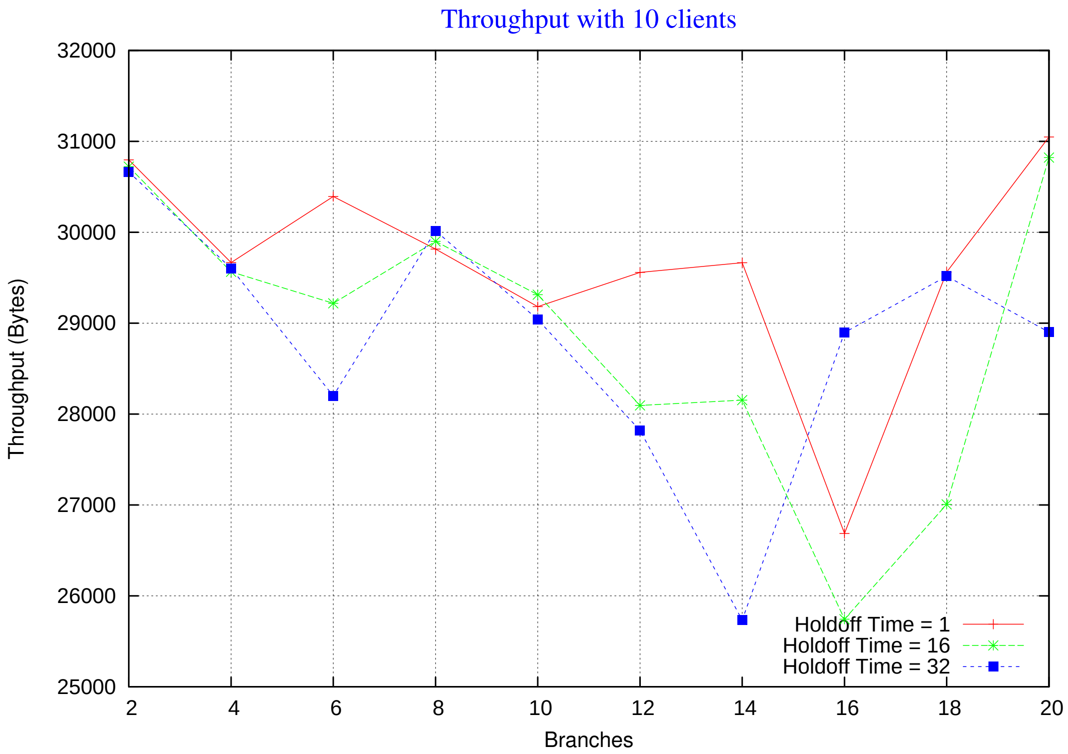


FIGURE 5.22 – THROUGHPUT WITH 10 CLIENTS.

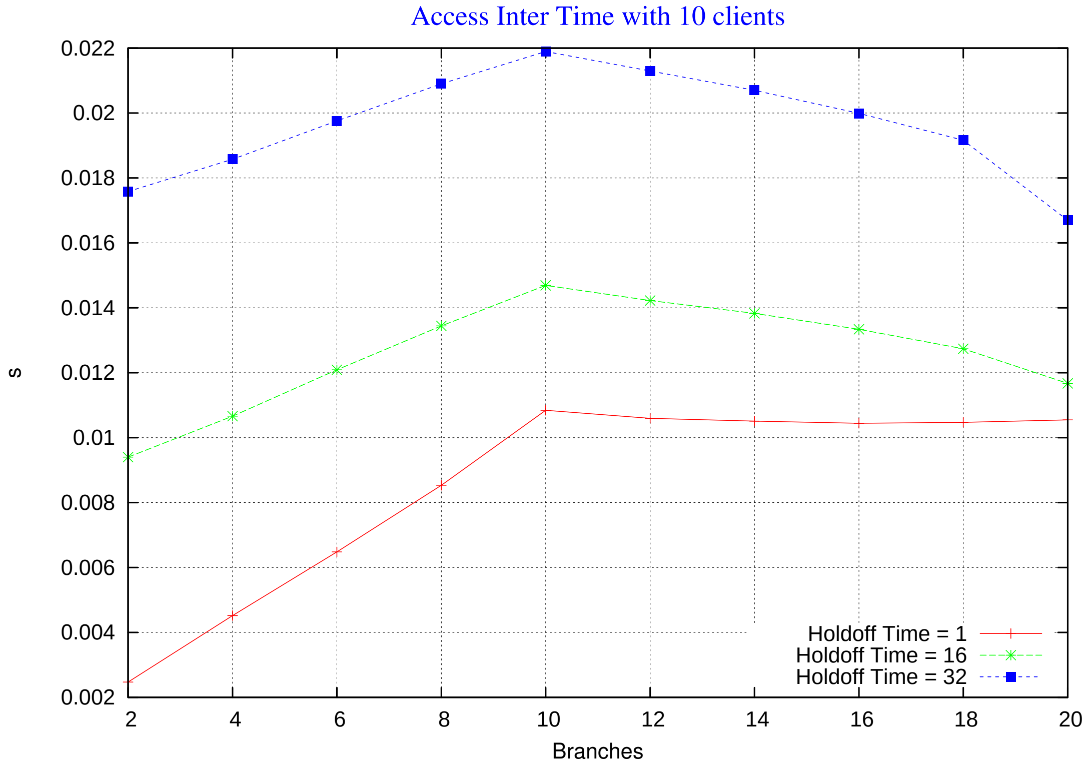


FIGURE 5.23 – ACCESS INTER TIME WITH 10 CLIENTS.

As be seen, figure 5.23 and 5.20 presents the same curves, because the average access inter time does not depend on the type of traffic.

6 Conclusions

> “If anyone acknowledges that Jesus is the Son of God,
> God lives in him and he in God.”
> — *1 John 4:15 (NIV)*

In this work we have proposed two algorithms, AIMD and MIAD, to adapt dynamically the Distributed Election Procedure in IEEE 802.16 mesh.

Specifically AIMD adapt the holdoff time of each mesh router based on the average number of contented slots, calculated from the last change of holdoff time, to access the control channel in the virtual contention. Instead MIAD approach the problem in a radical different way consequently of the results obtained from the performance evaluation of the AIMD algorithm. In particular it constantly decrease the holdoff time until the average number of contended slots exceed an established limit. If so, the node drastically increase the holdoff time and than restart to decrease it slowly.

We evaluated the system performance under different scenarios with both the algorithms. Our analysis showed that AIMD, despite worked properly, doesn’t yield the expected results in terms of average access inter time to the control channel. In the other hand, MIAD, yielded excellent results, achieving better performance compared to the standard IEEE 802.16 mesh.

Further analysis made it possible to find that a holdoff time of 1 gives the faster access to the control channel in every realistic situation of application of mesh networks.

Finally, we evaluated the throughput and the end-to-end delay under scenarios with bursty traffic, proving that using an holdoff time of 1 we have similar performance in terms of throughput compared to the standard, but end-to-end delay drastically lower.

Bibliography

[1] http://WirelessMAN.org

[2] Akyildiz, I. F. and Wang, X. A survey on Wireless Mesh Networks. *IEEE Commun. Mag.*, vol. 43, no. 9, Sep. 2005, pp. 23–30.

[3] IEEE 802.16-2004. IEEE standard for Local and Metropolitan Area Networks – Part 16: Air interface for Fixed Broadband Wireless Access systems. Oct. 2004.

[4] http://www.isi.edu/nsnam/ns/ , last version 2.31, Mar. 2007.

[5] http://www.wimax.com

[6] http://www.wimaxforum.org

[7] C. R. Baugh, J. Huang, R. Schwartz, and D. Trinkwon, "Traffic model for 802.16 TG3 MAC/PHY simulations," IEEE 802.16 Broadband Wireless Access Working Group, Tech. Rep., Mar. 2001.

[8] C. Cicconetti, I. F. Akyildiz, L. Lenzini. "Bandwidth balancing in multi-channel IEEE 802.16 wireless mesh networks," proc. *IEEE INFOCOM 2007*, Anchorage, Alaska, USA, May 6–12, 2007.

[9] N. Bayer, D. Sivchenko, B. Xu, V. Rakocevic, J. Habermann. "Transmission timing of signaling messages in IEEE 802.16 based mesh networks," proc. *European Wireless 2006*, Athens, Greece, April 2–5, 2006.

[10] Lichun Bao, J.J. Garcia-Luna-Aceves, "A new approach to channel access scheduling for ad hoc networks", in the seventh annual international conference on *Mobile Computing and Networking* 2001, pp. 210-221.

[11] Cicconetti, C., Akyildiz, I.F., and Lenzini, L., "FEBA: A Bandwidth Allocation Algorithm for Service Differentiation in IEEE 802.16 Mesh Networks," submitted for journal publication, August 2007.

[12] C. Cicconetti, A. Erta, L. Lenzini, E. Mingozzi, "Performance evaluation of the mesh election procedure of ieee 802.16/wimax", pp. 323 - 327 , 2007.

[13] B. Li Y. Xue and K. Nahrstedt, Price-based resource allocation in wireless ad hoc networks, Tech. Rep. UIUCDCS-R-2003-2331, Univ. of Illinios at Urbana-Champaign, 2003.