Project: IEEE 802.15 Working Group for Wireless Personal Area Networks (WPANs)

Submission Title: [P802.15.4.e AFA provisioning : Proposal]
Date Submitted: [30 Jun., 2008]
Source: [Shusaku Shimada] Company [Yokogawa Co.]

Address [2-9-32 Nakacho-town Musashinoshi-city Tokyo, 180-8750 Japan]
Voice:[+81-422-52-5543], FAX: [+81-55-7311], E-Mail:[shusaku@ieee.org]

Re: [IEEE P802.15-08-0373-01-004e-call-for-proposals]

Abstract: [AFA(Adaptive Frequency Agility) provisioning for IEEE802.15.4 PHY/MAC.]

Purpose: [This submission is a proposal of MAC amendment responding to CFP of IEEE802.15 TG-4e.]

Notice: This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

Purposes of Proposal

Purposes include variety of aspects

AFA (cross layer multi-channel) functions,

using either PHR-extension or MHR-extension,
new MAC Primitives,
and NHL channel-coordination,

are able to provide,

(1) Collision Avoidance

(2) Frequency Agility and/or Selection

(3) Adaptive Channel Usage

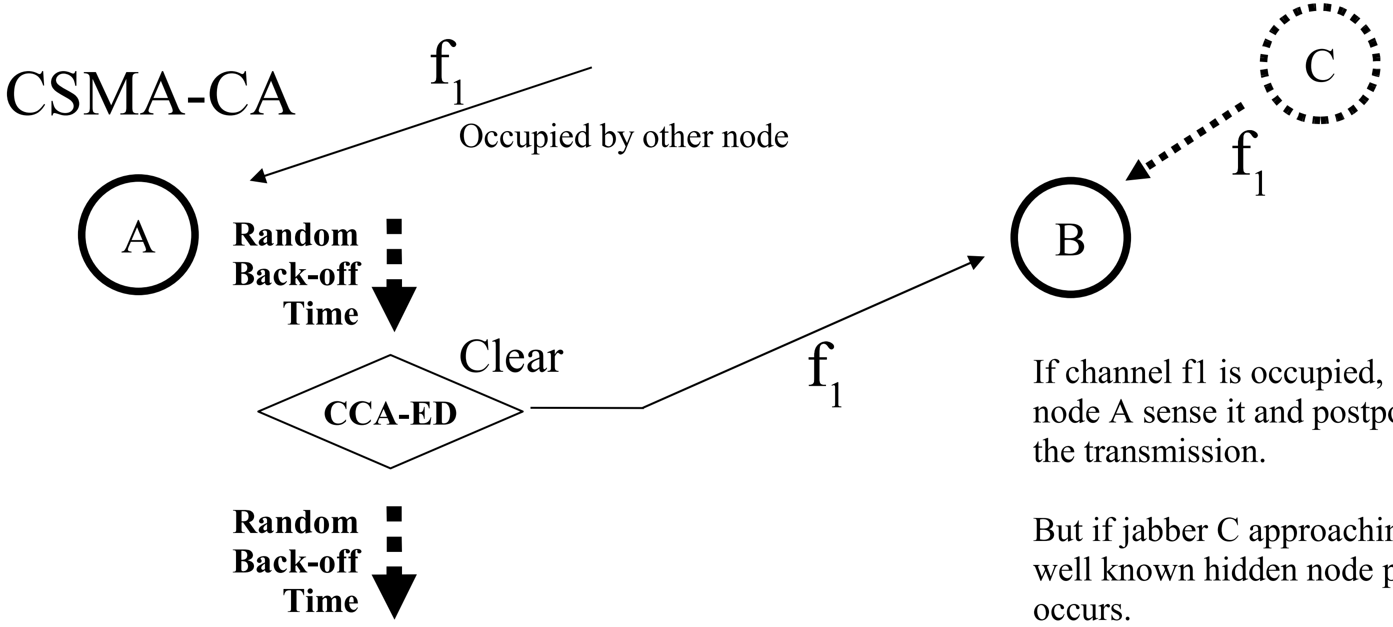
(4) Channel Blacklisting

(5) Fault localization and/or Isolation

Conventional 802.15.4 Mechanisms

Conventional Art (1)

Collision Avoidance by CSMA-CA



If channel f1 is occupied,
node A sense it and postpone
the transmission.

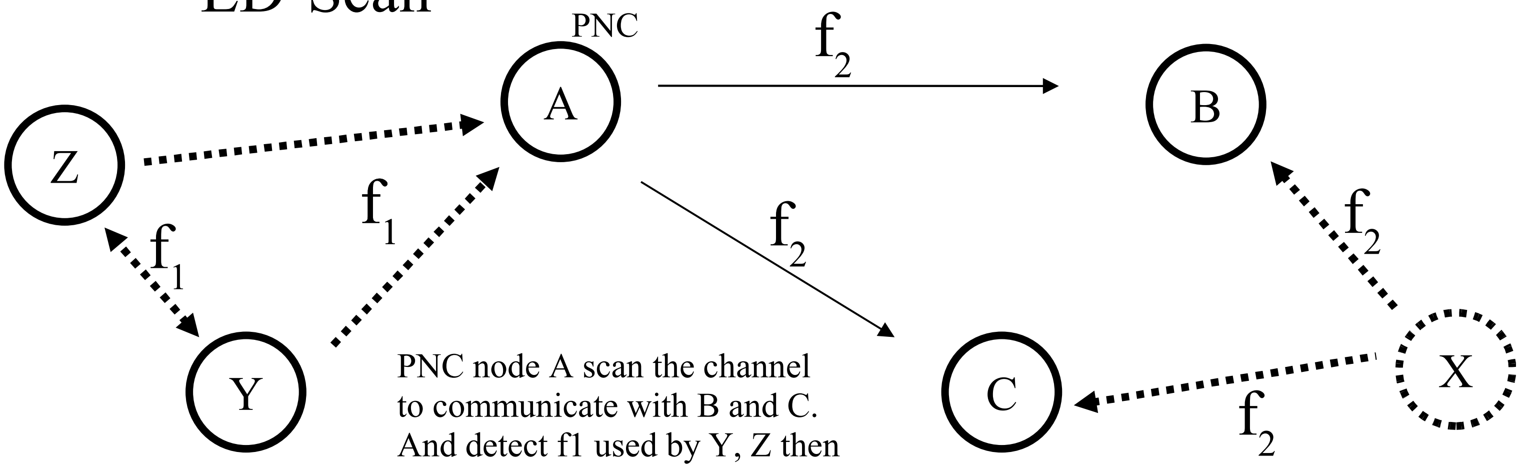
But if jabber C approaching B,
well known hidden node problem
occurs.

- Sufficiently effective mechanism if traffic is low enough.
- Time-critical, reliable and deterministic applications need more.

Conventional Art (2)

Frequency Channel Selection using ED-Scan

ED-Scan

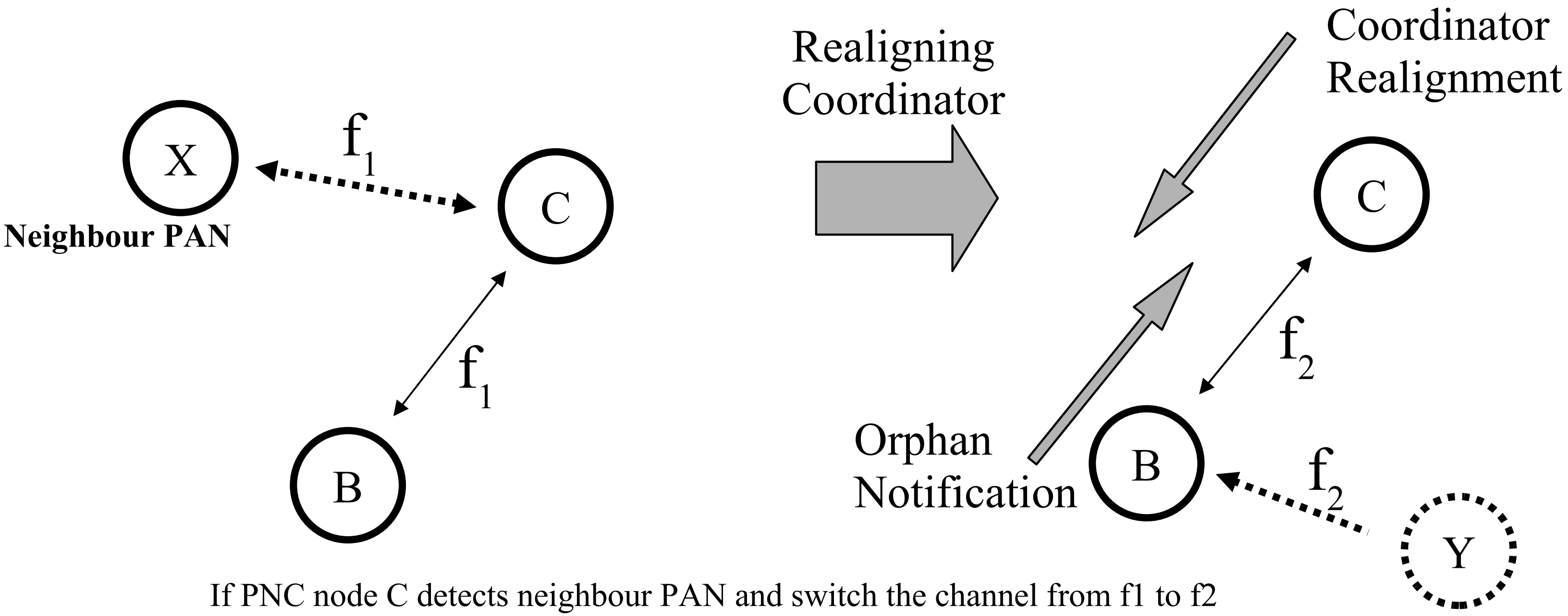


PNC node A scan the channel
to communicate with B and C.
And detect f1 used by Y, Z then
select f2.
But of course, there still hidden node
issue if jabber X is existing and using f2.

- Sufficiently effective mechanism if node density is sparse enough.
- Reliability Conscious applications need more to select channel.

Conventional Art (3)

Channel switching by Orphan Scan



If PNC node C detects neighbour PAN and switch the channel from f1 to f2
node B gets lost and Orphan scan mechanism is initiated.
But again if jabber Y is locating near node B, channel switching doesn't work properly.

- Sufficiently effective mechanism if altered channel is proper.
- Reliability Conscious applications prefer more to select channel.

Summary of Proposal

PHY Header Extension for AFA

< In the regulatory domains where AFA functionalities are recommended. >

or

MAC Header Extension for AFA

< In case of which MHR bits reflecting CCA result no security risks ajar. >

PHY Header Extension for AFA in case of 802.15.4 (Part 1)

Modification of PHR Length Field

Current : Length 7 bits + Reserved 1 bit
Modification : Length 7 bits + PHR Extension 1 bits

Addition in PHR structure

TX Channel Table

→ Length : 3 Octets + 1 Octet Control bits
→ 24 Entry for each 15.4 channels or sub-channels
including world-wide (2.4GHz) 5MHz channels
and US 915MHz 2MHz channels
and Japanese 200kHz 1mW/10mW sub-channels.
→ 1 bits for each entry
→ Value: 1bit, indicating
Clear/Busy , or AFA scheduled TX channel, or other

Favourable Usage

→ Inform status on other TX channels or TX schedule to Peer nodes

PHY Header Extension for AFA in case of 802.15.4 (Part 2)

		Octets				
		1		**3**	**1**	**variable**
Preamble	SFD	Frame length (7 bits) **(Extension Exist)**	Reserved (1 bit)	**TX Ch. Table** **24 Ch. x (1 bit)**	**Control bits** (8)	PSDU
SHR		PHR		**PHR Extension**		PHY payload

- Frame Length : Value "2" indicates the existence of PHR extension. c.f.
  Current minimum length is limited to 5 Octets (ACK).

- TX Channel Table : Channel and sub-channel number indicates each PHY on corresponding frequency bands as the way defined in 15.4 specifications, e.g. increasing number means increasing frequency.

Octet Number	1								2								3							
Sub-channel Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Clear/Busy	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit

- Control Field : Define the meaning of TX ch. Table, or other messages.

Std. Control field (1bit)	Control bits (6bit)	Reserved (Further Extension Exist)
0	Standard definition	(1 bit) Usually "0"
1	Reserved	

Control bits	Meaning
0	Channel clear/Busy
1	Scheduled TX
2	Acknowledged
3-63	Reserved

MAC Header Extension for AFA in case of 802.15.4 (part 1)

General MAC Frame Format

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/ 14	4	variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	**TX Ch. Table** (3 Octets) **Control bits** (1 Octet)	Frame Payload	FCS
		Addressing fields							
MHR								MAC Payload	MFR

Format of Frame Control field of MHR

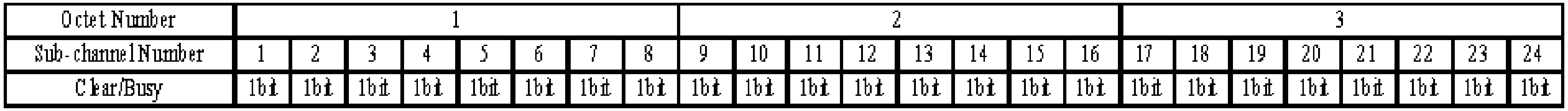
Bits: 0–2	3	4	5	6	7	8 –9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	Ack. Request	PAN ID Compression	**AFA Extension Enabled**	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

MAC Header Extension for AFA in case of 802.15.4 (Part 2)

General MAC Frame Format

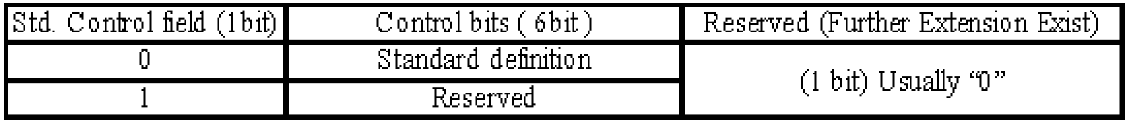
Octets: 2	**1**	**0/2**	**0/2/8**	**0/2**	**0/2/8**	**0/5/6/10/ 14**	**4**	**variable**	**2**
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	**TX Ch. Table** (24ch. x 1 bit) **Control bits** (8 bits)	Frame Payload	FCS
		Addressing fields							
MHR								MAC Payload	MFR

- TX Channel Table : Channel and sub-channel number indicates each PHY on corresponding frequency bands as the way defined in 15.4 specifications, e.g. increasing number means increasing frequency.

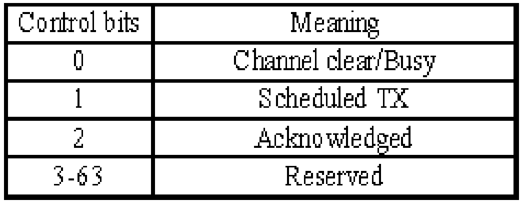


Octet Number	1								2								3							
Sub-channel Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Clear/Busy	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit

- Control Field : Define the meaning of TX ch. Table, or other messages.



Std. Control field (1bit)	Control bits (6bit)	Reserved (Further Extension Exist)
0	Standard definition	(1 bit) Usually "0"
1	Reserved	



Control bits	Meaning
0	Channel clear/Busy
1	Scheduled TX
2	Acknowledged
3-63	Reserved

Usage of PHR or MHR Extension for AFA

- Remote CCA

Result of multichannel CCA performed by peer node can be recognized and collected.

- Forecasting scheduled TX on peer node without CCA

If peer node is programmed to work in synchronous TX or TDMA without CSMA-CA scheme, PHR extension can be used to notify the channel may be occupied without CCA.

- Link layer Ack History

If a node have been performed successful transaction at least once, PHR extension can be used to indicate no fault of TRX on the channel. Adversely, indicating it have never performed acknowledged transaction, suggests a possible malfunction if Ack have been sent by peer nodes (observing nodes).

MAC Primitives for AFA

PHY Channel Coordination Functions

PHY Management Services

PLME-Peer-AFA-TX ; Perform CCA on each channel & TX on PHR-Ex
PLME-Peer-AFA-RX ; Collect AFA information in PHR on Peer frames

PIB

phyChannelsOccupied
→ Type: array ; Indicates CCA history of performed LBT
→ Value: Ratio and latest time stamp of Clearance

phyChannelsActivated
→ Type: array ; Indicates Transmitting Channel to Peer nodes
→ Value: Scheduled TX (including TDMA), Simulcast, Duplicate TX

phyCurrentChannel ; Currently using sub-channels
→ Type: array
→ Value: Arbitrary combination of channels, specified by number 1-24

MAC Primitives

MAC Management Service Primitive using PHR-Extension

MLME-CCA-Announce ; Perform CCA on each channel & inform peer nodes

.request (Type, CCAA_Chs, CCAA_Duration, ChPage, CCAA_Level, Persistence)

.confirm (StatusTxNumber, ChPage, CCAA_ResultListSize, CCA_ResultList)

MLME-Peer-CCA-Survey ; Collect CCA information on each CH & Peer

.request (Type, CCAS_Chs, CCAS_Duration, ChPage, Persistence)

.indication (StatusRxNumber, ChPage, ResultPeerListSize, CCA_ResultPeerList)

MLME-Scheduled-TX-Announce ; Inform peer nodes of scheduled TX-CH

.request (Type, STxA_Chs, ChPage, STxA_ListSize, STxA_List, STxA_Persist)

.confirm (StatusTxNumber, StxA_Chs, ChPage, STxA_PeerList)

MLME-Acked-CH-Announce ; Inform of Acknowledged Channels

.request (Type, AckA_Chs, ChPage, AckA_ListSize, AckA_List, AckA_Persist)

.confirm (StatusTxNumber, ChPage, AckA_ListSize, AckA_List)

MAC Primitives Appropriate Usage & Effects

MLME-CCA-Announce ; Issued by NHL to perform CCA on each channel and to inform peer nodes the status of CCA at specified detection level. MLME successively update CCA result during specified duration and confirm the result persist as the history of surrounding radio-sphere as long as the elapsed time of each CCA result is within the persistence limit.

MLME-Peer-CCA-Survey ; Issued by NHL to collect CCA information of each of peer on each channel and to organize the resulting Peer CCA table. MLME inform NHL of the organized result table through .indication. This result is persisting until and been updated by within specified persistence time. This effects during the specified duration of operation.

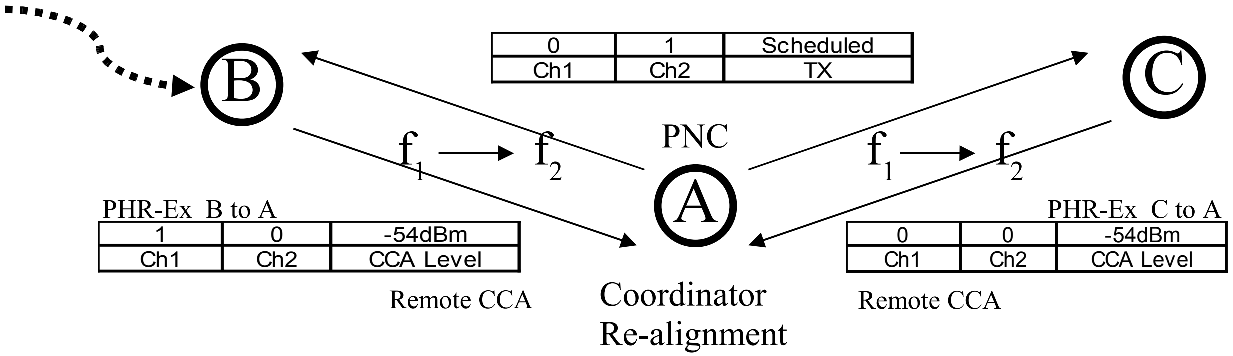
MLME-Scheduled-TX-Announce ; Issued by NHL to inform peer nodes of any of expected or scheduled transmission on each channel without CCA, which is resulted by Channel Switching, TDMA or Channel Hopper.

MLME-Acked-CH-Announce ; Issued by NHL to inform peer nodes of all of the channels which was recently acknowledged and the communication have been completed successfully. This confirm the health of both Tx & Rx and adversely possible asymmetry fault if permanent negative. The information have to be updated within appropriate time duration.

AFA Scenario

2 channel asynchronous AFA (Frequency Switching) Scenario

Node A, B, C are pre-defined to use Ch.1(f1), Ch.2(f2), and are using Ch.1, then switching to Ch.2 in this figure below.



0	1	Scheduled
Ch1	Ch2	TX

PHR-Ex B to A

1	0	-54dBm
Ch1	Ch2	CCA Level

PHR-Ex C to A

0	0	-54dBm
Ch1	Ch2	CCA Level

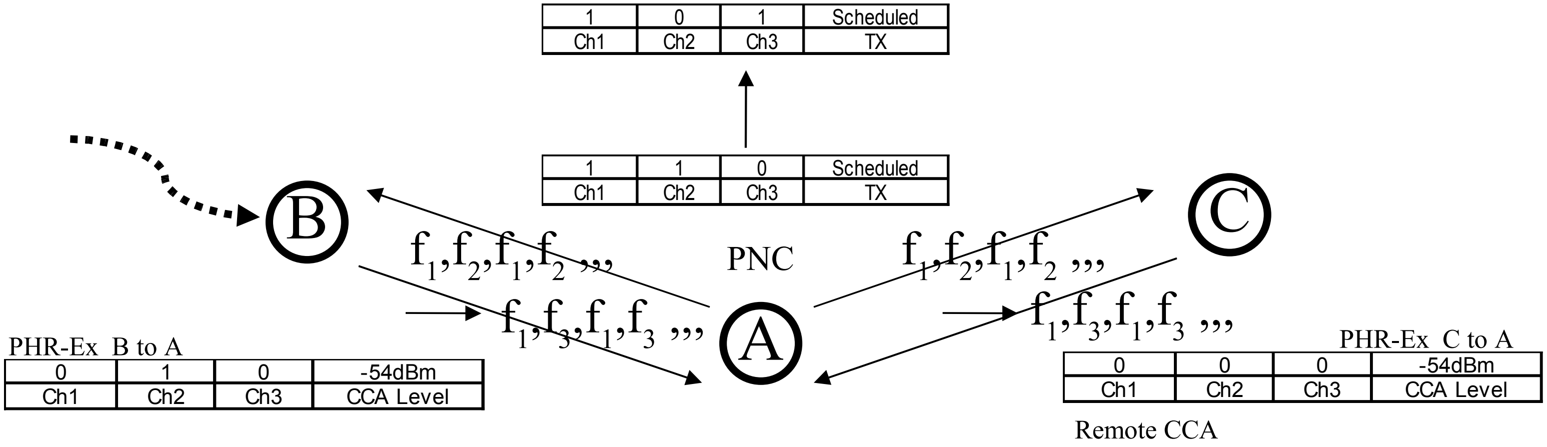
All node is using Ch.1 and node B is getting distracted due to interference, for example. PNC node A is collecting the remote CCA information from both node B and C periodically and detect the remote interferences at each node. If NHL decide to switch to alternate frequency channel of f_2 i.e. Ch.2, in this case, conventional Coodinator Re-alignment can work. Before this decision of channel switch, PNC can use AFA-Ex of scheduled TX on Ch.2.

Note: Before AFA, NHL can set the CCA level of each nodes

Multi-Channel asynchronous AFA Scenario

TX node may always transmits duplicate information on multiple channel redundantly.

All nodes are able to play the overlaid double Piconets and each leaf nodes can work either on Ch.1 or Ch.2.



1	0	1	Scheduled
Ch1	Ch2	Ch3	TX

1	1	0	Scheduled
Ch1	Ch2	Ch3	TX

PHR-Ex B to A

0	1	0	-54dBm
Ch1	Ch2	Ch3	CCA Level

PHR-Ex C to A

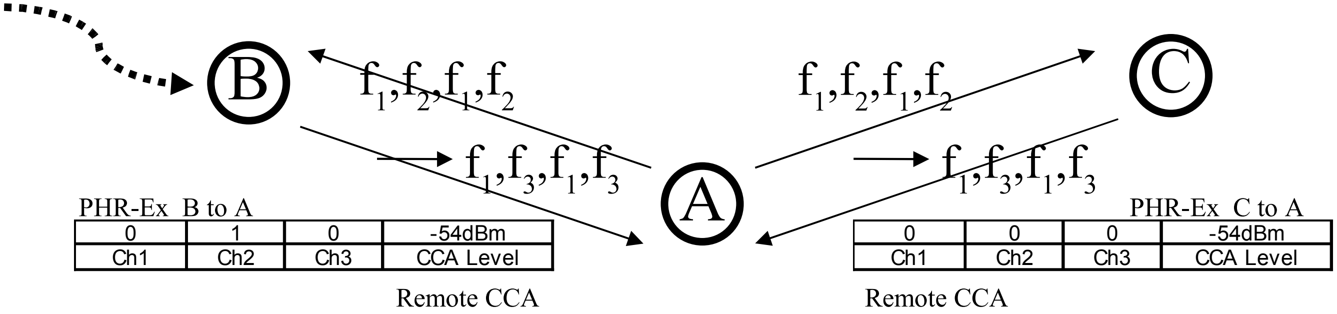
0	0	0	-54dBm
Ch1	Ch2	Ch3	CCA Level

Remote CCA

All nodes can take redundant opportunity to communicate on Ch.1 and Ch.2, and node B is getting interfered. PNC node A decides to switch channel by remote CCA and starts announcing the scheduled TX on Ch.1 and Ch.3. This alleviates the possibility of orphan generation.

2 channel synchronous AFA (Frequency Switching) Scenario

Node A, B, C are using f1 and f2 alternately, that is minimum multiple channels.



PHR-Ex B to A

0	1	0	-54dBm
Ch1	Ch2	Ch3	CCA Level

PHR-Ex C to A

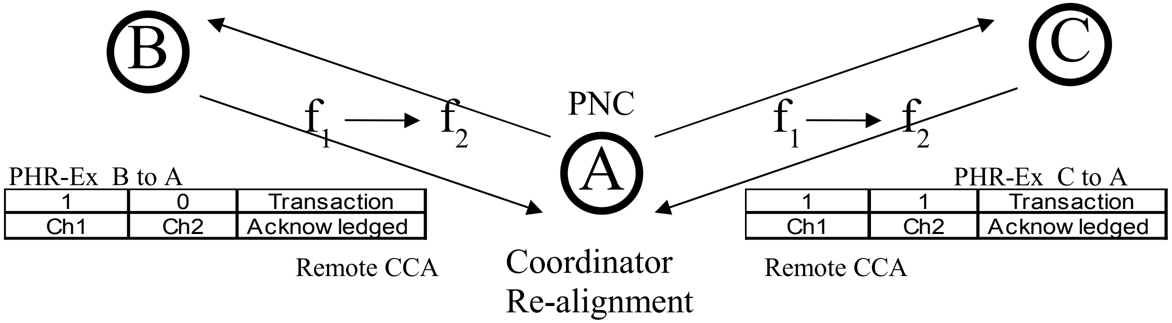
0	0	0	-54dBm
Ch1	Ch2	Ch3	CCA Level

All TX node must follow the pre-defined TX channel order to send, in this case, AFA means alternating order. PNC node A is collecting remote CCA information and detect remote busy of node B on Ch.2.

Simplest AFA can be the tactics of yielding the channel usage to avoid remote collision. If the remote CCA busy is sustaining, Ch.2 may be changed to and substituted by Ch.3, for example in this case.

Multichannel AFA (Fault Isolation) Scenario

NHL is able to have Acknowledged status on each leaf nodes
by receiving Ack'ed information on PHR-Ex.



PHR-Ex B to A

1	0	Transaction
Ch1	Ch2	Acknow ledged

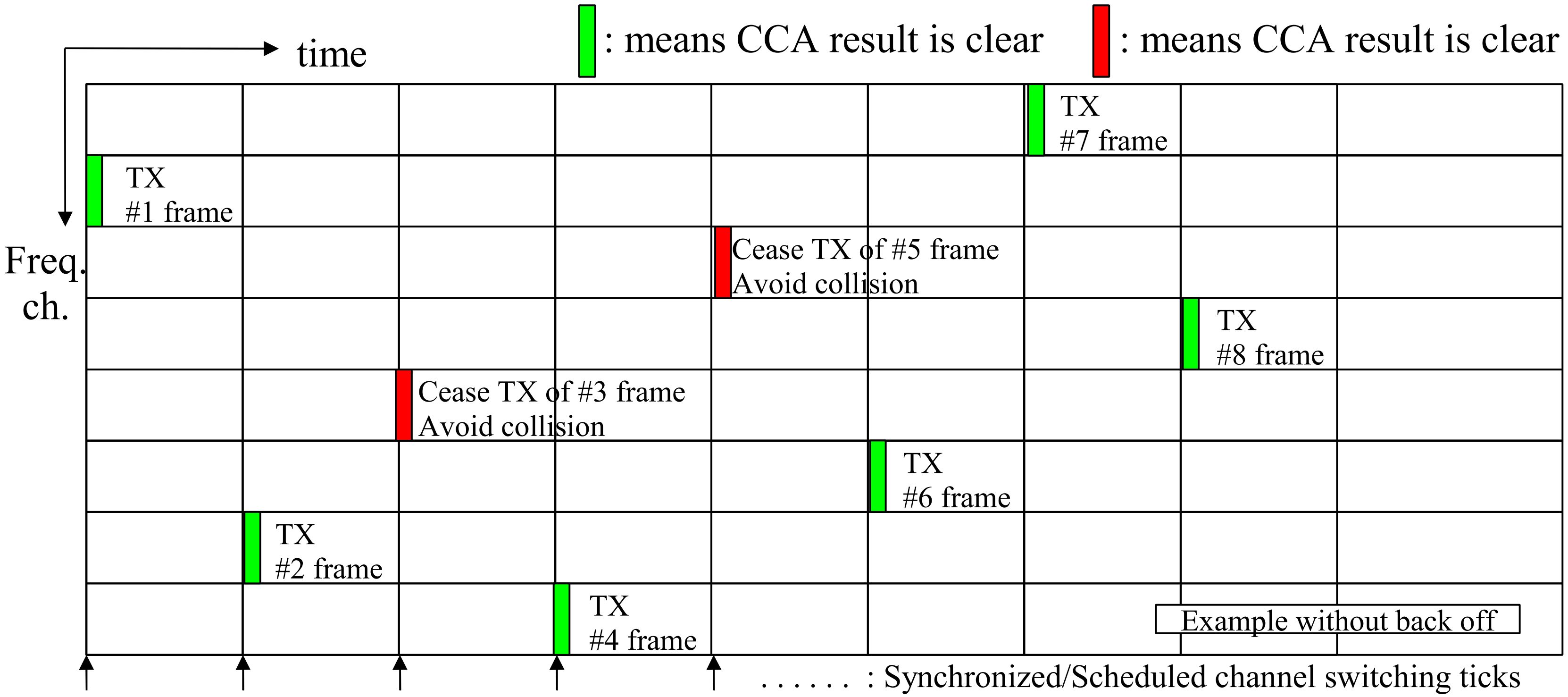
PHR-Ex C to A

1	1	Transaction
Ch1	Ch2	Acknow ledged

PNC is able to take action if sustaining No Acknowledged transaction on Node B. This may occur on a specific channel of Node B, or entire channel of Node B, and the information can be used to detect harmful Asymmetric Fault on the peer node.

AFA with distributed CCA in each time slot

TX node to decide the transmission of each channels using CCA.



time

Freq. ch.

🟩 : means CCA result is clear

🟥 : means CCA result is clear

TX #7 frame

TX #1 frame

Cease TX of #5 frame Avoid collision

TX #8 frame

Cease TX of #3 frame Avoid collision

TX #6 frame

TX #2 frame

TX #4 frame

Example without back off

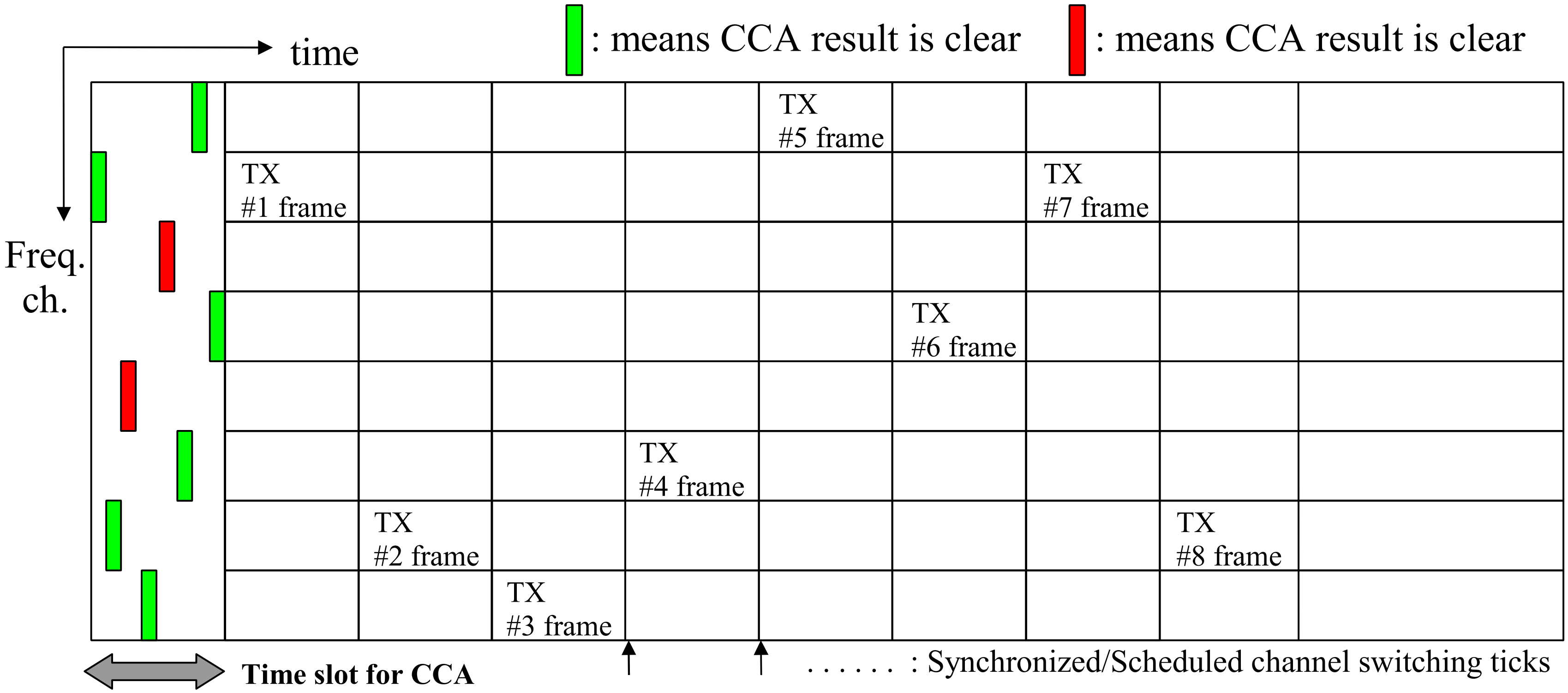
. . . . . . : Synchronized/Scheduled channel switching ticks

Then TX node must follow the pre-defined TX channel order to send. In this case, AFA means just CA, i.e., collision avoidance.

In case of the reliability conscious APP, it's better for TX node to inform the decision of transmission regarding entire channels to RX nodes.

AFA with congregated CCA in a designated time slot

TX node to decide the transmission of each channels and its order to send.



🟩 : means CCA result is clear 🟥 : means CCA result is clear

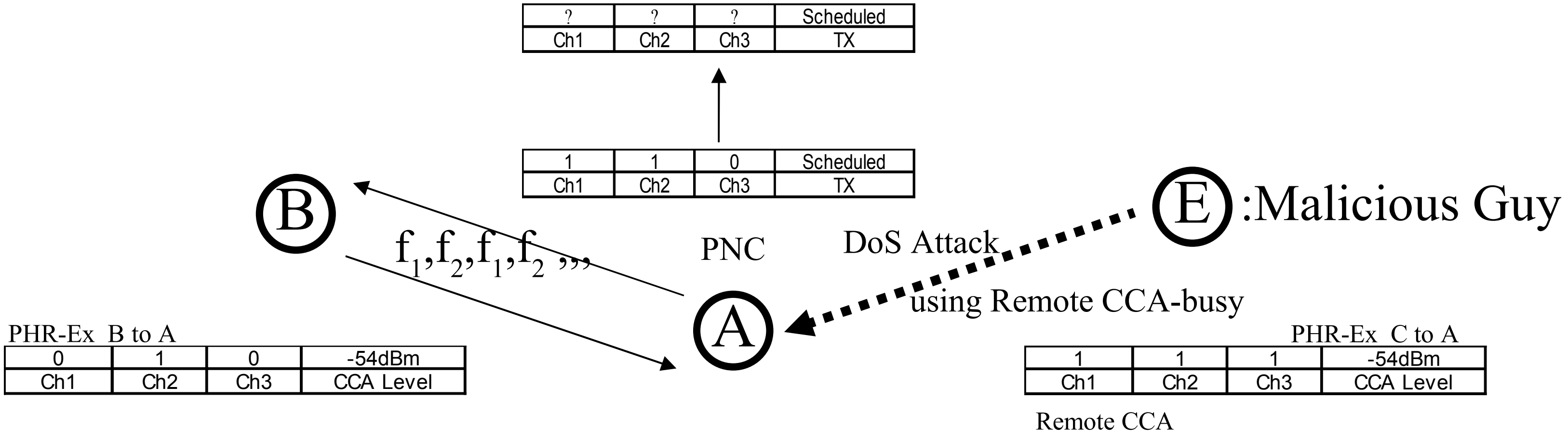
TX node must ensure at least a frame is following the previously scheduled channel and time slot unchanged to inform the new transmission channels and its order to send. Adaptive utilization of channels according to CCA is possible.

Security Considerations of AFA Extension

DoS Attack using PHR/MHR Extentsion for AFA

TX node may always exchange remote CCA information and may coordinate Tx channel scheduling.

Getting the first look at this PHR/MHR extension for AFA, DoS attacker seems to gain an additional mean to do their job.



?	?	?	Scheduled
Ch1	Ch2	Ch3	TX

1	1	0	Scheduled
Ch1	Ch2	Ch3	TX

PHR-Ex B to A

0	1	0	-54dBm
Ch1	Ch2	Ch3	CCA Level

PHR-Ex C to A

1	1	1	-54dBm
Ch1	Ch2	Ch3	CCA Level

Remote CCA

Although Node A and B can take account on node E's remote CCA busy, the credibility of node E itself and the authenticity of message pertaining this sort of remote busy may be verified through various ways, including simple statistical anomalies or usual masquerade detection.

This means no extra-vulnerability concerning DoS is introduced by AFA.

MHR CCA bit manipulation by Intentional Interference

Remote CCA information have to reflect the surrounding radio circumstance of sender.

MHR shall be included for MIC calculation of link layer keyed message authentication, ex., CBC-MAC of CCMP star.

MHR-Ex B to A

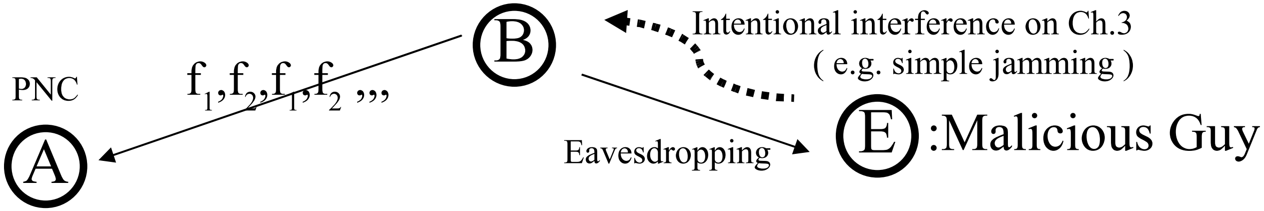
0	0	0	-54dBm
Ch1	Ch2	Ch3	CCA Level

Remote CCA

MHR-Ex B to A

0	1	1	-54dBm
Ch1	Ch2	Ch3	CCA Level

Remote CCA



B

Intentional interference on Ch.3 (e.g. simple jamming)

PNC

f_1,f_2,f_1,f_2 ,,,

A

Eavesdropping

E :Malicious Guy

Leaf node B communicating with PNC A may be intentionally interfered by node E with malicious intent and is possibly forced to retry TX and to indicate interfered channel situation in MHR extension field. This means MHR CCA bit can be manipulated by attacker who is going to collect message and its MIC information in order to crack MIC key. Of course this simple intervention is far trivial than other crucial mis-implementation or vulnerability, nevertheless a means to collect security ajar may be provided. In general, PHR extension is more secure than MHR when 15.4 security level other than 0 or 4 is employed.

References

- 15-08-0373-01-004e-call-for-proposals.doc
- 15-08-0030-01-004e-AFA-functionality-in-reliability-conscious-applications.pdf
- 15-08-0109-02-004d-WW-BPSK-with-AFA-provisioning.pdf
- ETSI EN 300 220-1
- ERC RECOMMENDATION 70-03 COMMISSION DECISION of 9 Nov. 2006 on harmonisation of the radiospectrum for use by short-range devices

END