

**Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)**

**Submission Title:** [A Traffic-based Secure MAC Protocol for WBAN with Bridging Function]

**Date Submitted:** [May, 2009]

**Source:** [Kyungsup Kwak<sup>1</sup>, Sana Ullah<sup>1</sup>, Xizhi An<sup>1</sup>, M. A. Ameen<sup>1</sup>, Jingwei Liu<sup>1</sup>, Bumjung Kim<sup>1</sup>, Hyungsoo Lee<sup>2</sup>, Jaeyoung Kim<sup>2</sup>]

Company [Inha University<sup>1</sup>, Electronics and Telecommunications Research Institute (ETRI)<sup>2</sup>]

Address [428 Hi-Tech, Inha University, 253 Yonghyun-dong, Nam-gu, Incheon, 402-751, Republic of Korea]<sup>1</sup>, [ETRI, 161 Gajeong-dong, Yuseong-gu, Daejeon, 305-700, Republic of Korea]<sup>2</sup>

Voice: [], FAX: [],

E-Mail: [kskwak@inha.ac.kr (other contributors are listed in “Contributors” slides)]

**Re:** []

**Abstract:** [ Inha MAC Proposal to TG6]

**Purpose:** [To be considered in IEEE 802.15.6]

**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.

**Release:** The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15.

## Contributors

Name	E-mail	Affiliation
Kyungsup Kwak	kskwak@inha.ac.kr	Inha University
Sana Ullah	sanajcs@hotmail.com	Inha University
Xizhi An	anxizhi@inhaian.net	Inha University
M. A. Ameen	m.ameen@hotmail.com	Inha University
Jingwei Liu	j_w_liu@hotmail.com	Inha University
Bumjung Kim	ufopoint@gmail.com	Inha University
Hyungsoo Lee	hsulee@etri.re.kr	ETRI
Jaeyoung Kim	jyk@etri.re.kr	ETRI

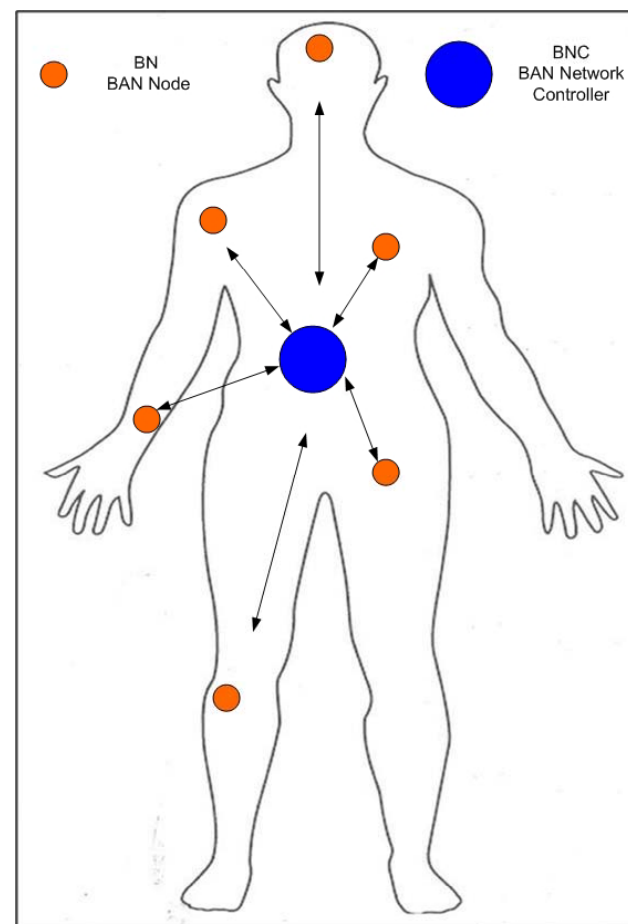
# Outlines

- **WBAN Overview**
- **Power –efficient Scheduling with Wakeup Solutions**
  - **Wakeup by Traffic-based Patterns**
  - **Wakeup by Radio**
- **MAC Frame Structure with Security Specifications**
- **Single MAC with Multiple Bands/PHYs**
  - **Bridging Function**
- **Performance Results**
- **Conclusion**

# WBAN Overview

# WBAN Major Characteristics

- A network consists of low-power invasive and non-invasive BAN Nodes (BNs) .
- BNs can be
  - **Full functional:** When deal with Multi-Phys.
  - **Reduced functional:** Mostly in the in-body networks.
- One WBAN device is selected as a BAN Network Coordinator (BNC).
- One-hop coverage range is around 3m.
- The traffic characteristics vary from low to high with periodic and non-periodic intervals, and vice versa.
- The dynamic natures of BNs does not urge synchronized periodic wake-up periods
  
- Communication flows:
  - Normal Traffic:
    - BNs  $\longleftrightarrow$  BNC
  - Emergency Traffic:
    - BNs  $\longleftrightarrow$  BNC
  - On-Demand Traffic:
    - BNC  $\longleftrightarrow$  BNs
    - BNs  $\longleftrightarrow$  BNs



## WBAN Devices Setting: Typical

<b>Device</b>	<b>Freq. Band</b>	<b>Data Rate</b>	<b>Power Supply</b>	<b>Function</b>
Out-Body Device	Unlicensed ISM/UWB Band	High	High-Capacity Battery	Monitoring, Multimedia
On-Body (wearable) Device	Unlicensed ISM/UWB Band or Licensed Medical Band*	Medium	High / Moderate Battery	Monitoring, Connecting implant node and out-body node
In-Body (implant) Device	Licensed Medical Band*	Low	Limited Battery	Medical, Monitoring

\* Medical band: MICS, WMRS, WMTS

## WBAN MAC Major Issues(1)

- Heterogeneous Traffic
  - Normal, On-demand, and Emergency traffic
- Interoperability
  - Multiple frequency bands and correspondingly multiple PHY techniques
  - Connecting different devices working on different bands/PHYs
- Scalability
  - Variable data rate: Kbps ~ Mbps
  - Variable number of devices
- Energy Saving
  - Synchronous or asynchronous
  - Beacon or preamble
  - Different periods of wake up and sleep

## WBAN MAC Major Issues(2)

- Energy waste in Sensor Networks
  - Idle Listening
  - Collision
  - Overhearing
  - Over-emitting
  - Others
- Suitable wake-up mechanisms can save significant amount of energy in WBAN and increase the network lifetime.
  - Device wake-ups only when necessary, otherwise it sleeps thereby saving energy.

Radio State	Power Consumption (mW)
Transmit	81
Receive/Idle	30
Sleep	0.003

- Coordinated and controlled data transmission can reduce energy consumption.



## WBAN Device Classification(1)

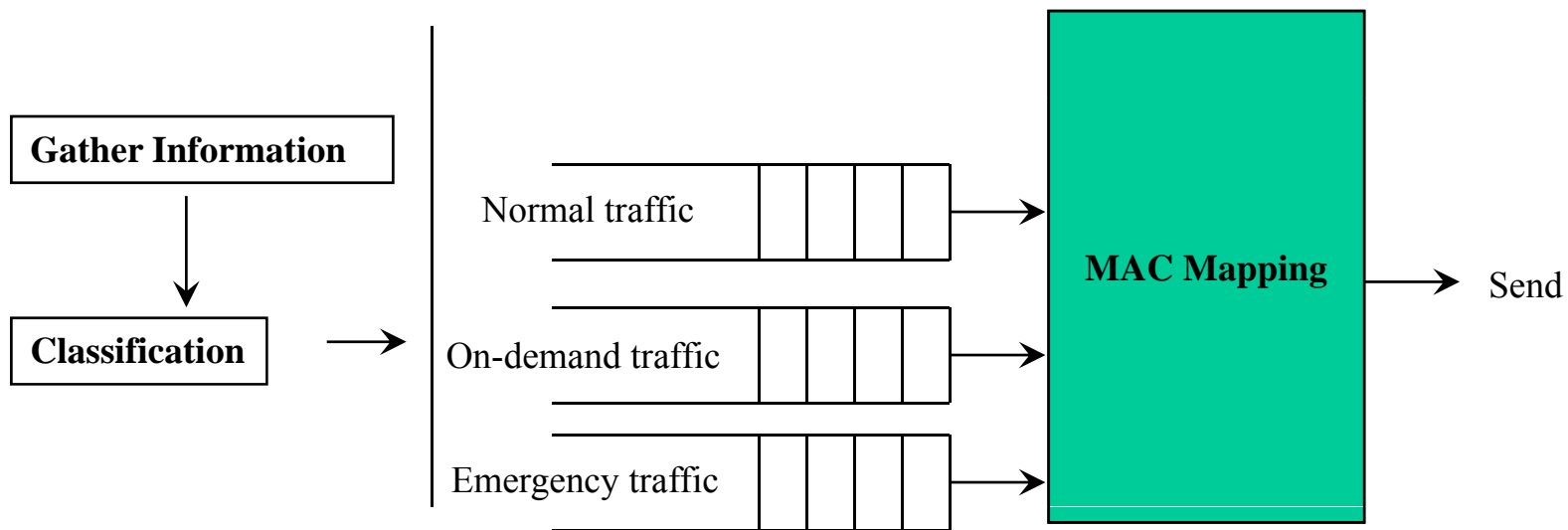
- BNC: BAN Network Coordinator
  - On AC power supply
    - It can wake-up all the time.
    - It can support normal, emergency, and on-demand traffics.
  - On battery power supply
    - It has certain limitations and should adopt low-power scavenging techniques.
    - It should calculates its own wakeup pattern based on the BN's wake-up patterns.
    - It should maintain the traffic-based wake-up table.
- BN: BAN Node(Device)
  - They are operating on limited power and support a default normal wake-up state.
    - Wake-up and sleep according to traffic-based wake-up table.
    - BN wake-ups upon receiving an 'on demand' request from a BNC.
    - BN wakes-up by itself to handle emergency events.

## WBAN Device Classification(2): Function

- Full Function Device (FFD)
  - Beaconing function
  - Bridging function
    - Have Multiple PHYs
  - Control functions
  - Generally, it can act as a BNC.
  
- Reduced Function Device (RFD)
  - Only support one band / one PHY for a specific application
  - Often in-body device due to very limited power and capacity

# WBAN Traffic Classification

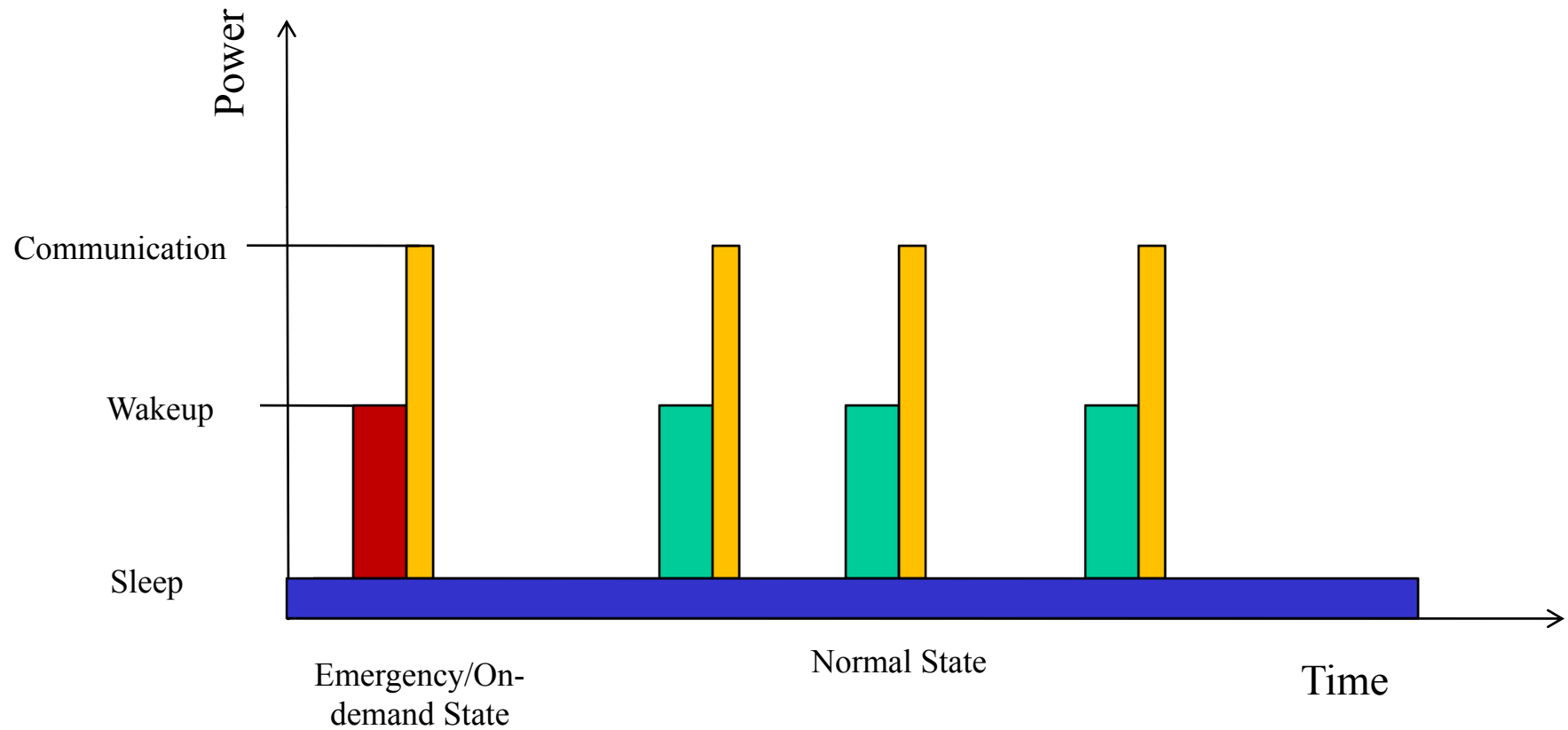
- Data traffic in a WBAN is classified into:
  - **Normal traffic:** Based on normal operation between BN and BNC using a defined patterns.
  - **On-demand traffic:** Initiated by BNC to know certain information.
  - **Emergency traffic:** In case of critical condition.



## States of WBAN Device (1)

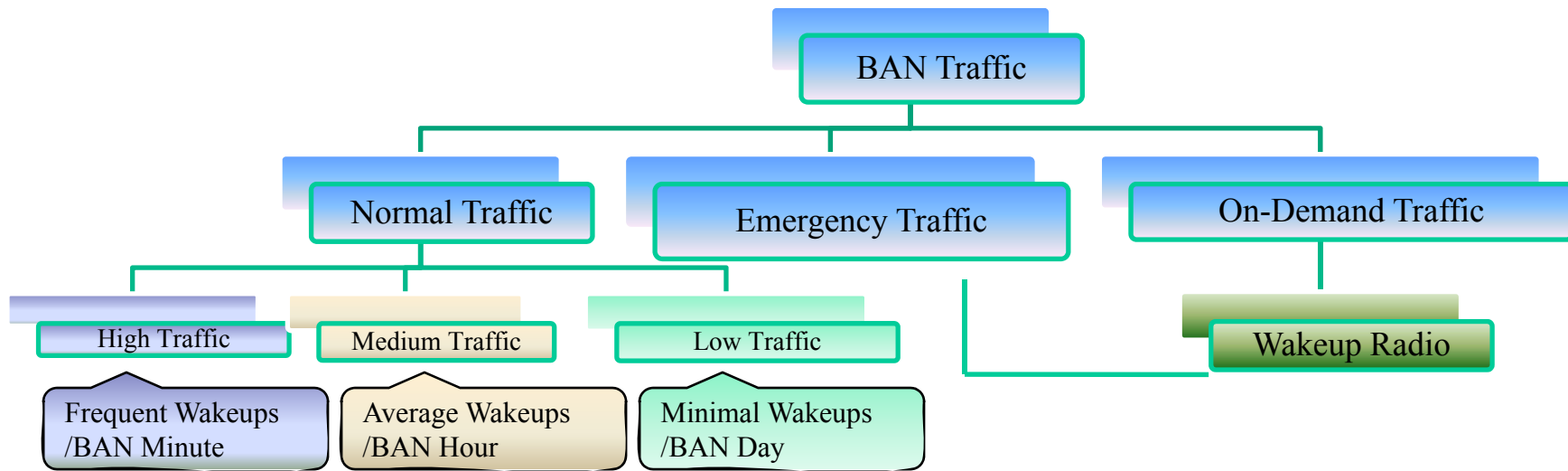
- Sleep State:
  - Default state of BNs.
- Wake-up State: intermediate state from Sleep to Data transmission
  - Normal Wake-up State
    - Based on the wakeup patterns maintained by the BNC.
  - On-demand Wake-up State
    - To handle on-demand requests.
    - BNC can wake up any BN with an on-demand request instead of waiting for its wake-up pattern.
  - Emergency(Self) Wake-up State
    - To handle time critical events
- Communication State
  - Data communication between BNs and BNC.

# States of WBAN Device (2)



# Wakeup by Traffic-based Pattern for Normal Traffic

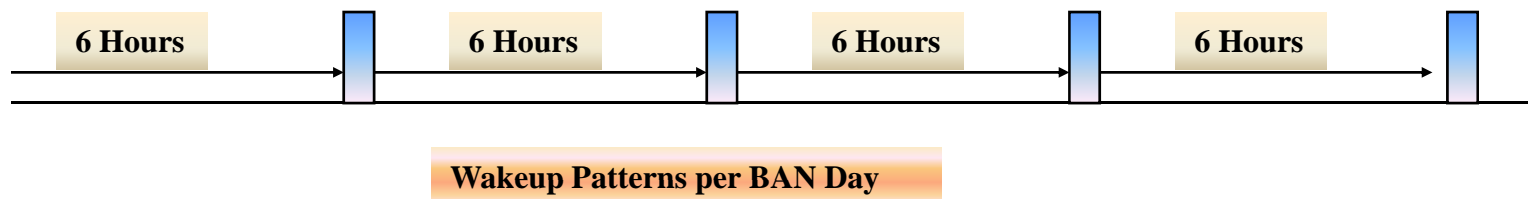
# Traffic Level Patterns



	Normal Traffic	On-demand Traffic	Emergency Traffic
BNs(BAN Nodes)	Send data based on the <u>Traffic-based Wake-up Table</u>	Receives a <u>Wake-up Radio</u> from the BNC and respond	BNs are triggered when exceeds a predefined threshold and Send a <u>Wake-up Radio</u>
BNC(BAN Network Coordinator)	Send data based on the <u>Pattern-based Wake-up Table</u>	Send a <u>Wake-up Radioto</u> BNs	Receives a <u>Wake-up Radio</u> and respond

## Traffic-based Wakeup Patterns (1)

- In normal case, the operation of each BN is based on a wakeup pattern.
- The initial wakeup pattern is pre-defined (by the company) or created and modified (by the BNC).
- The wakeup patterns are repeated per BAN **Day**, BAN **Hour**, BAN **Minutes**, BAN **Seconds**, and BAN **Milliseconds**.
  - This allows simple representation of the traffic levels (depends on the application requirements)
  - High traffic node sends data  $x$  times per BAN Minute or BAN Millisecond
- The BNC can change the traffic levels from Low to High (vice-versa) by simply changing the wakeup patterns.



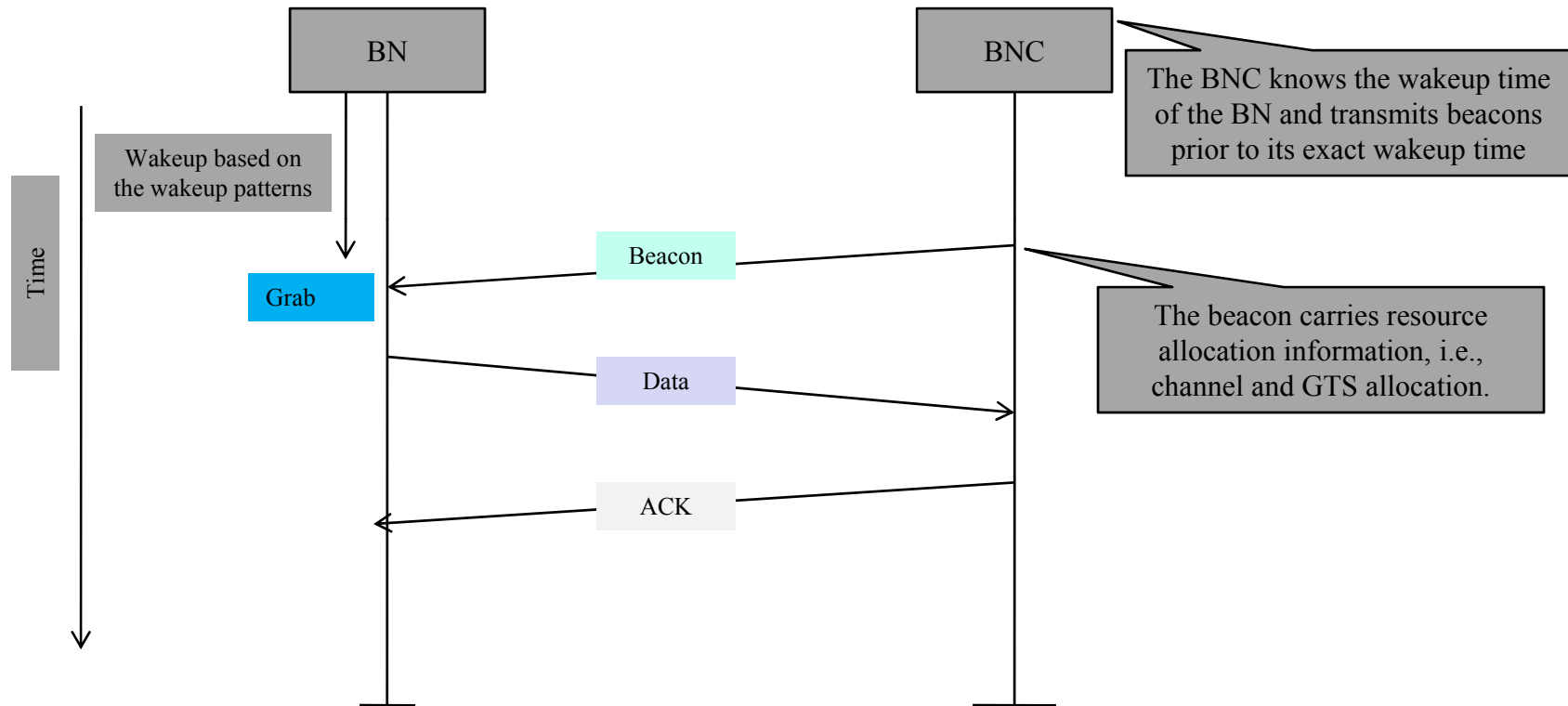


## Traffic-based Wakeup Patterns (2)

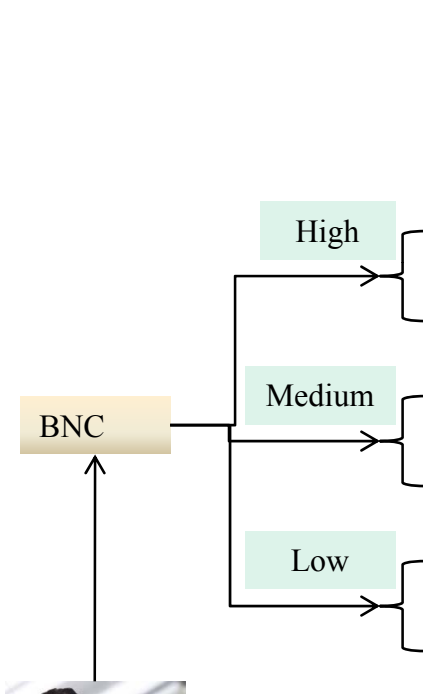
- The BNC creates and manages a traffic-based wakeup table with High, Medium, and Low priorities.
- The BNC continuously transmits the beacons to the BN prior to its wakeup time .
- After wakeup, the BN grabs the beacon that contains information about:
  - Synchronization
  - Channel allocation
  - GTS allocation depends on the traffic load
  - Priority Information
- BNs having same wakeup patterns are assigned channel and time slot based on the their priorities.
- The transmission starts when a GTS slot is allocated to the BN.

# Data Transfer Model: Normal Traffic

- From BN to BNC



# Traffic-based Pattern Table at BNC



	BAN Nodes	BAN Day	BAN Hour	BAN Minute	BAN Seconds	BAN Milli second
High	Endoscope	-	-	-	-	<i>i</i>
	ECG	-	-	-	<i>j</i>	-
Medium	Insulin Sensor	-	-	<i>k</i>	-	-
	Glucose Sensor	-	<i>l</i>	-	-	-
Low	Blood Pressure	<i>m</i>	-	-	-	-
	EMG	<i>n</i>	-	-	-	-



Two parameters allow doctor to change the traffic levels of BNs, i.e, BAN Unit (Day, Hour, Minute, Second, and Millisecond) and patterns.

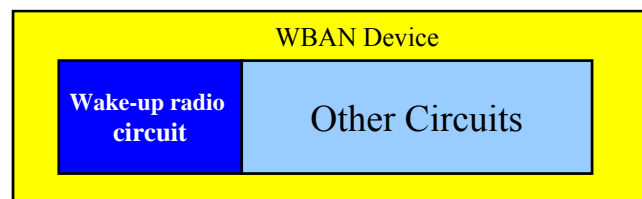
Endoscope and ECG sends data with *i millisecond* and *j second* interval

# Wakeup by Radio

## for On-demand & Emergency

## Wake-up Radio Concept

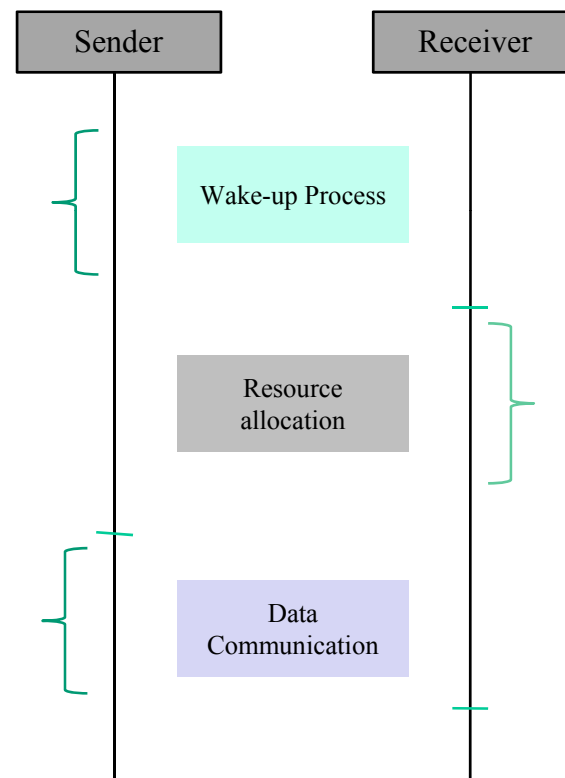
- Wake-up Radio Concept
  - Radio-triggered hardware component in sensor devices.
  - Wake-up radio signal contains enough energy to trigger a wake-up process [1].
  - Hardware Implementation
    - Extremely low-power detection circuit in WBAN devices.
    - Wake-up radio circuit is on all the time, while all other circuits can be switched off when sensor device is sleeping.



- Wake-up radio can be adopted in a WBAN.

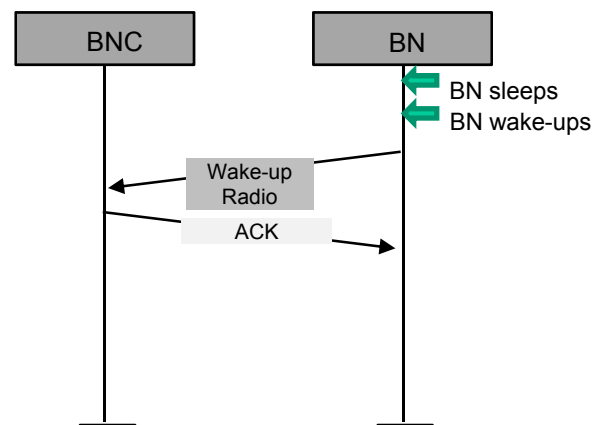
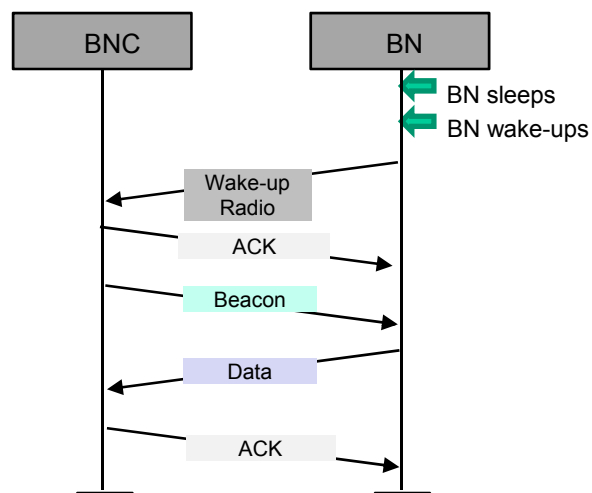
# Communication Process by Wakeup Radio

- Wake-up Procedure
  - BNC sends wake-up radio signal to BN.
- Resource Allocation Procedure
  - BNC allocates Channel and Time slots
  - BN sends an ACK to BNC
- In final step, data communication takes place.



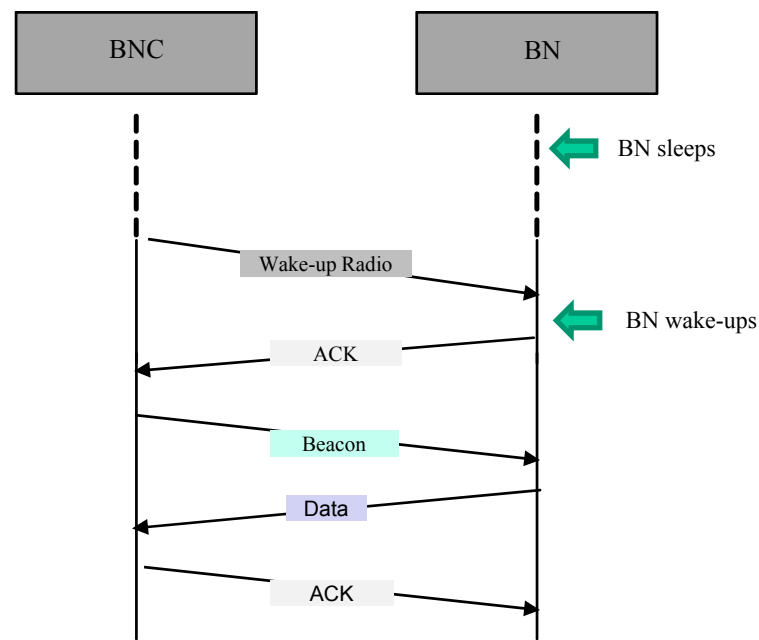
## Data Transfer Model: Emergency Traffic

- Self wake-up of a BN in emergency case
  
- Two situations
  - Emergency health problems sensed by BN
    - A BN triggers itself to wake-up.
    - BN sends a wake-up signal to the BNC.
    - BNC sends an ACK
  - Low Battery problem at BN
    - Battery is dying.
    - BN sends a wake-up signal to the BNC.
    - BNC sends an ACK



## Data Transfer Model: On-demand Traffic

- BNC wake-ups a BN on-demand
  - BNC needs data from BN.
  - Instead of waiting for BN’s normal wakeup pattern, BNC wakes up the BN with wake-up radio.
  - BNC sends a wake-up signal to wake-up a BN and waits for ACK.
  - BN wakes up and sends ACK.

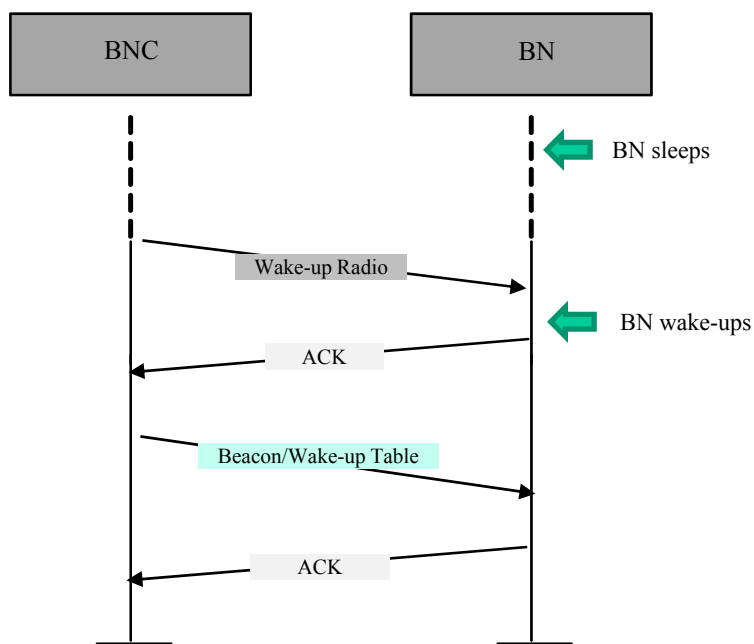




# Data Transfer Model: Updating Wakeup Table

□ **Pattern table is updated by the BNC**

- ◆ **BNC wakes up BN**
- ◆ **BN wakes up and send ACK**
- ◆ **BNC sends new pattern to BN**
- ◆ **BN sends ACK**



## Secured Wake-up Scheme

The steps of 2-stage secure wake-up scheme:

Step 1: BNC sends a wake-up packet to BN.

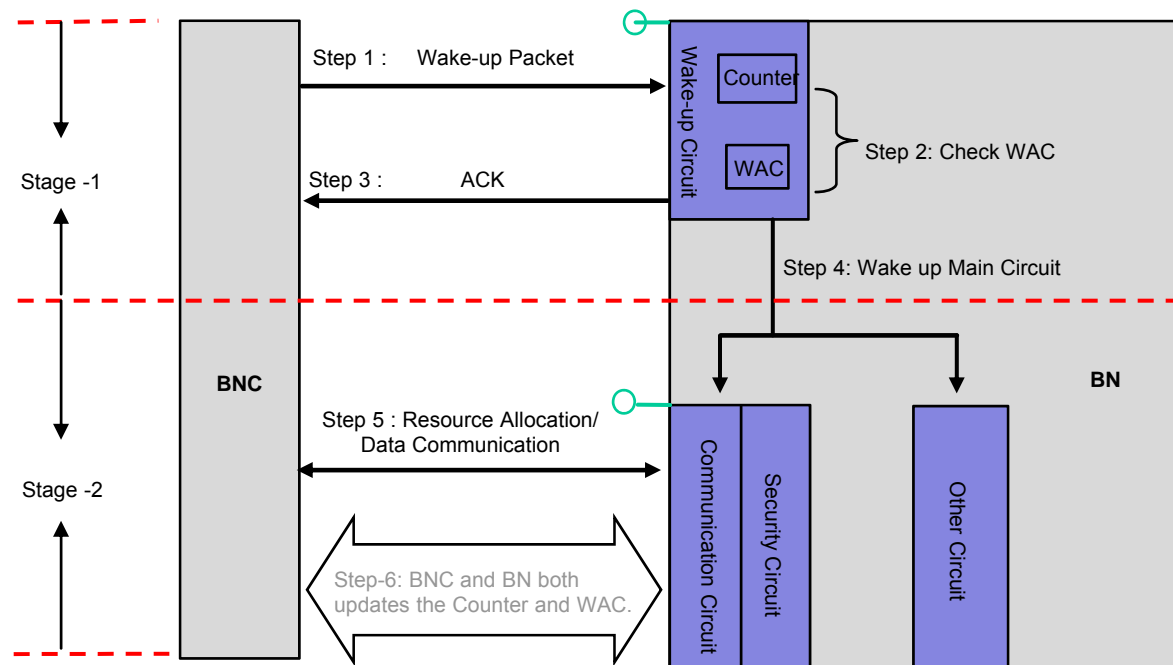
Step 2: BN checks if the received WAC matches with the stored WAC.

Step 3: Wake-up Circuit wakes up Main Circuit.

Step 4: Main Circuit of BN sends ACK to BNC.

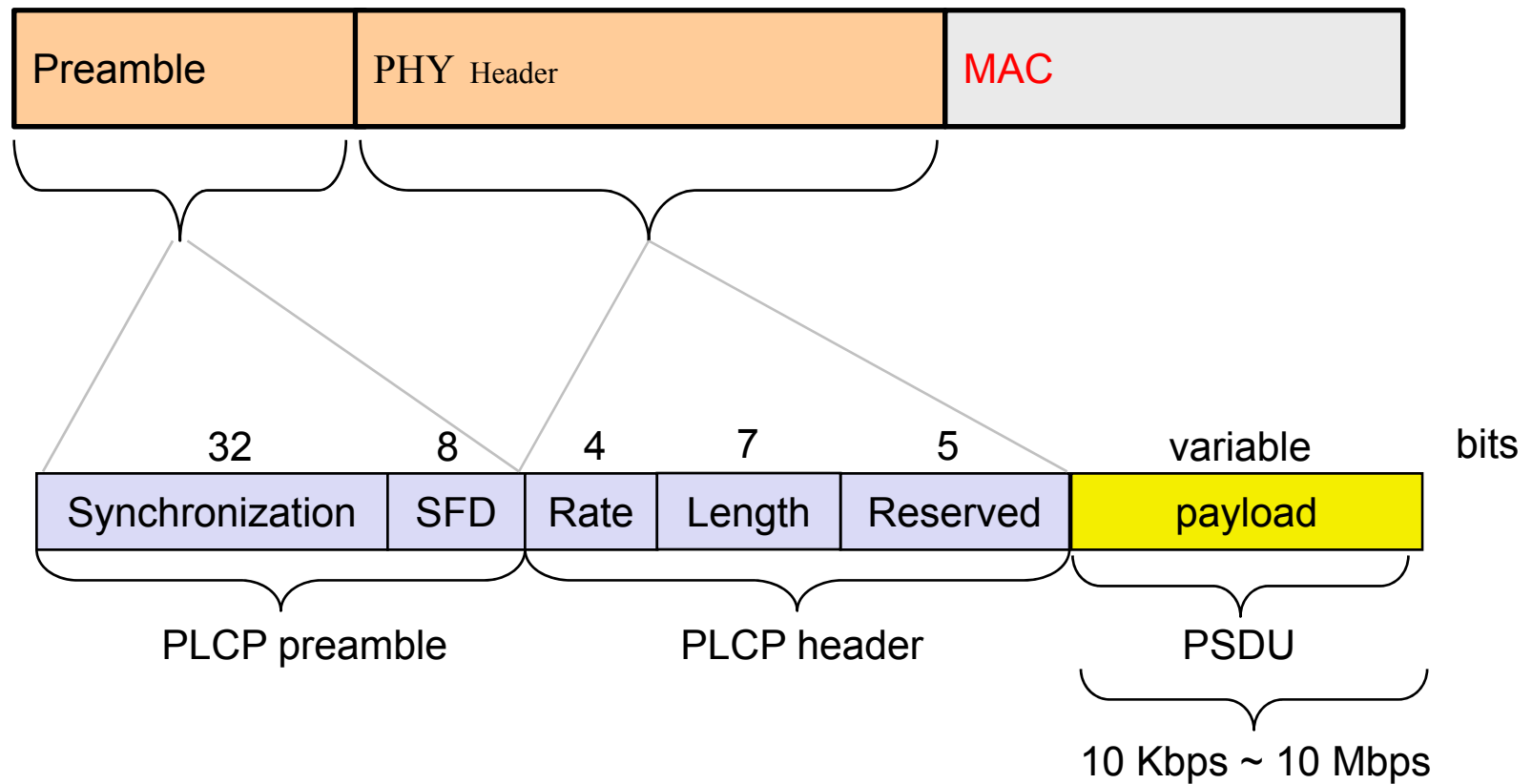
Step 5: Resource Allocation/ Data Communication

Step 6: BNC and BN both updates the Counter and WAC.

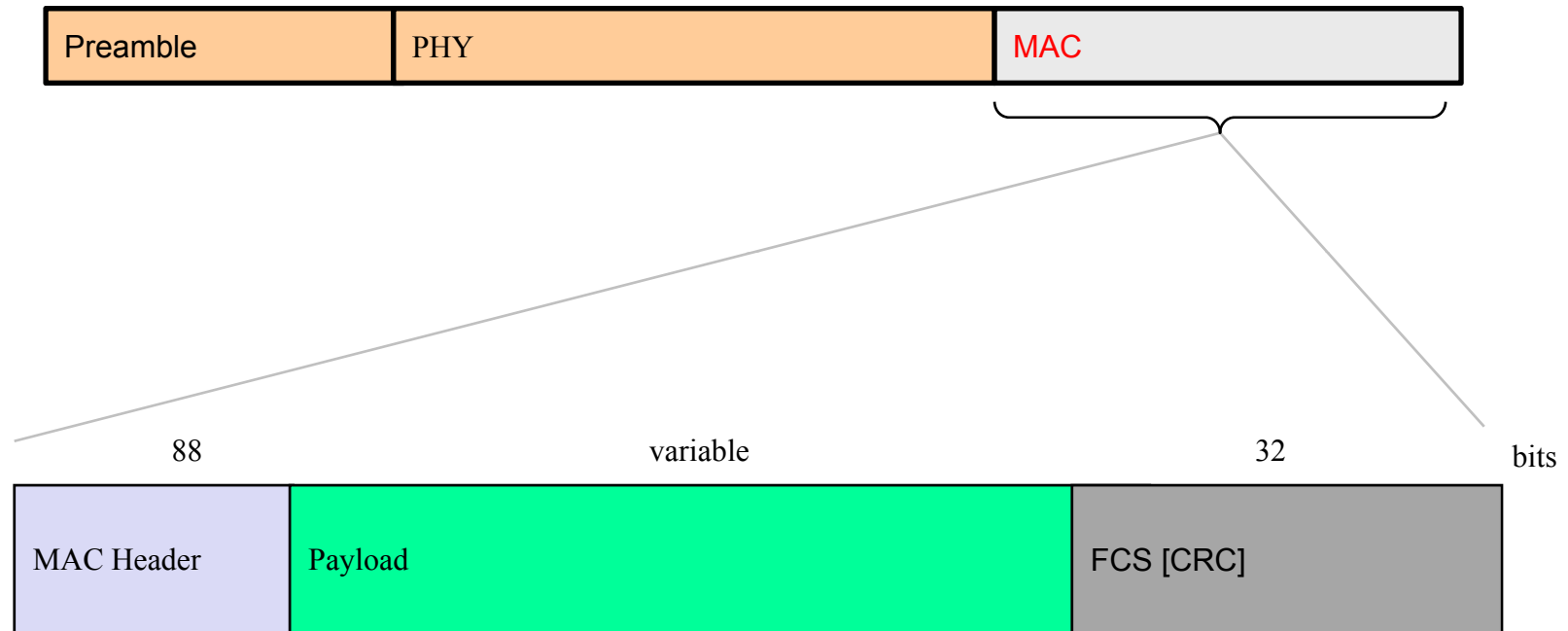


# MAC Frame Structure with Security Specification

# General PHY/MAC Frame Format

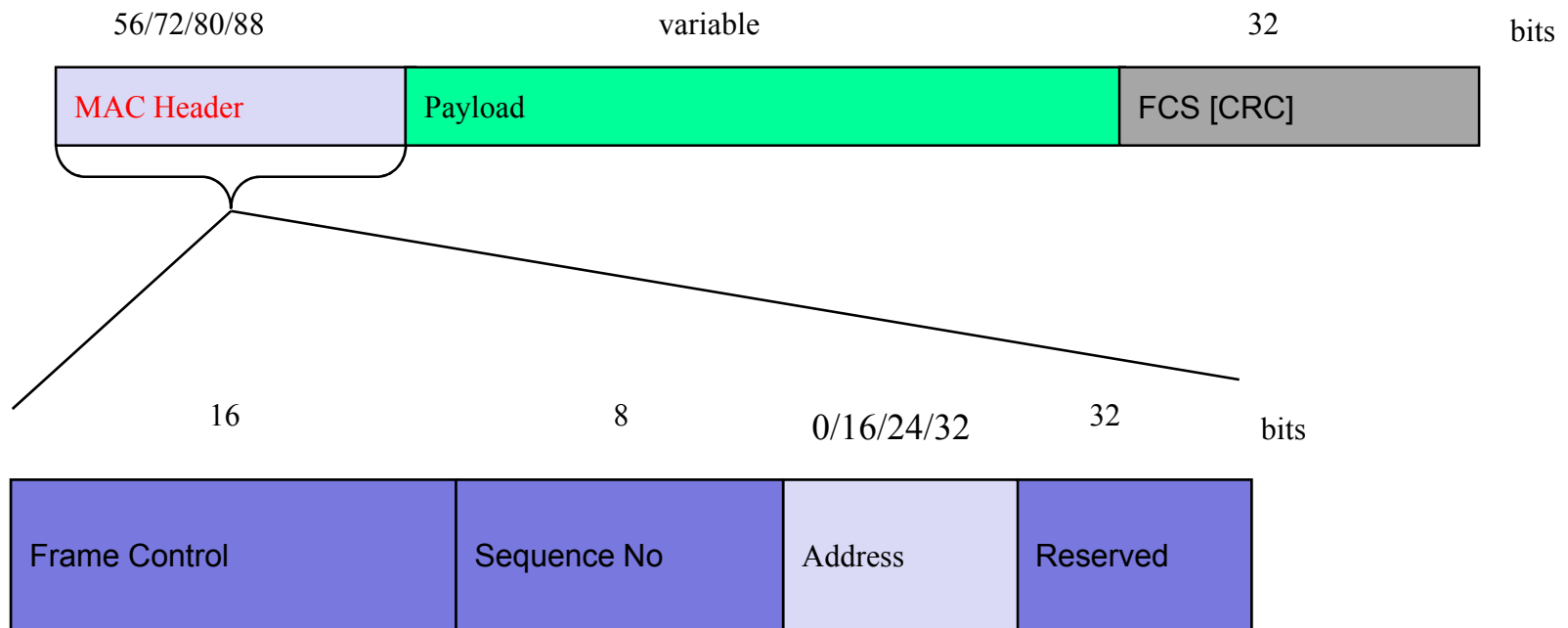


# MAC Frame Structure



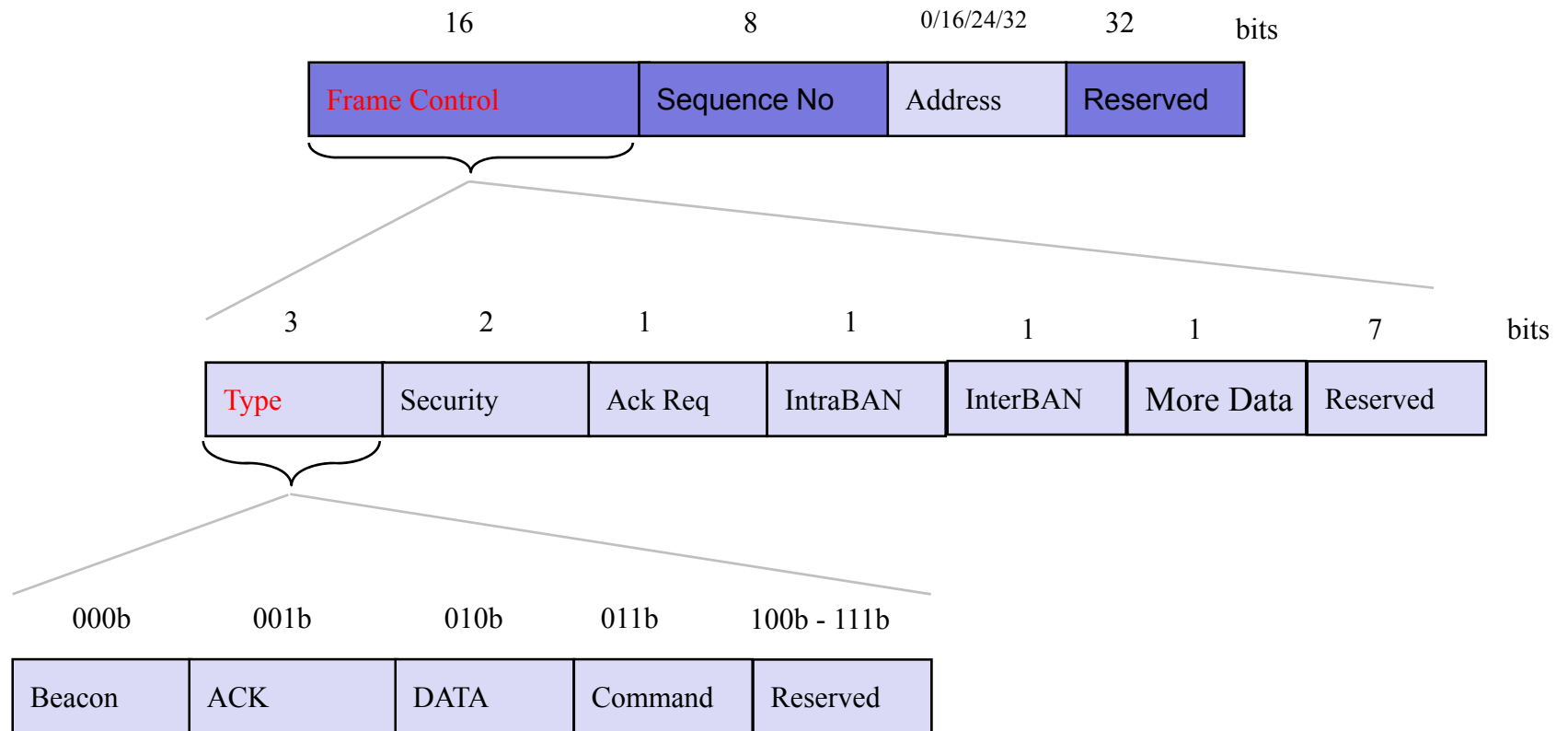
**MAC Frame length:  $88+32+\text{variable payload} = 120 \text{ bits} + \text{payload} = 15 \text{ octets} + \text{payload}$**

# MAC Header

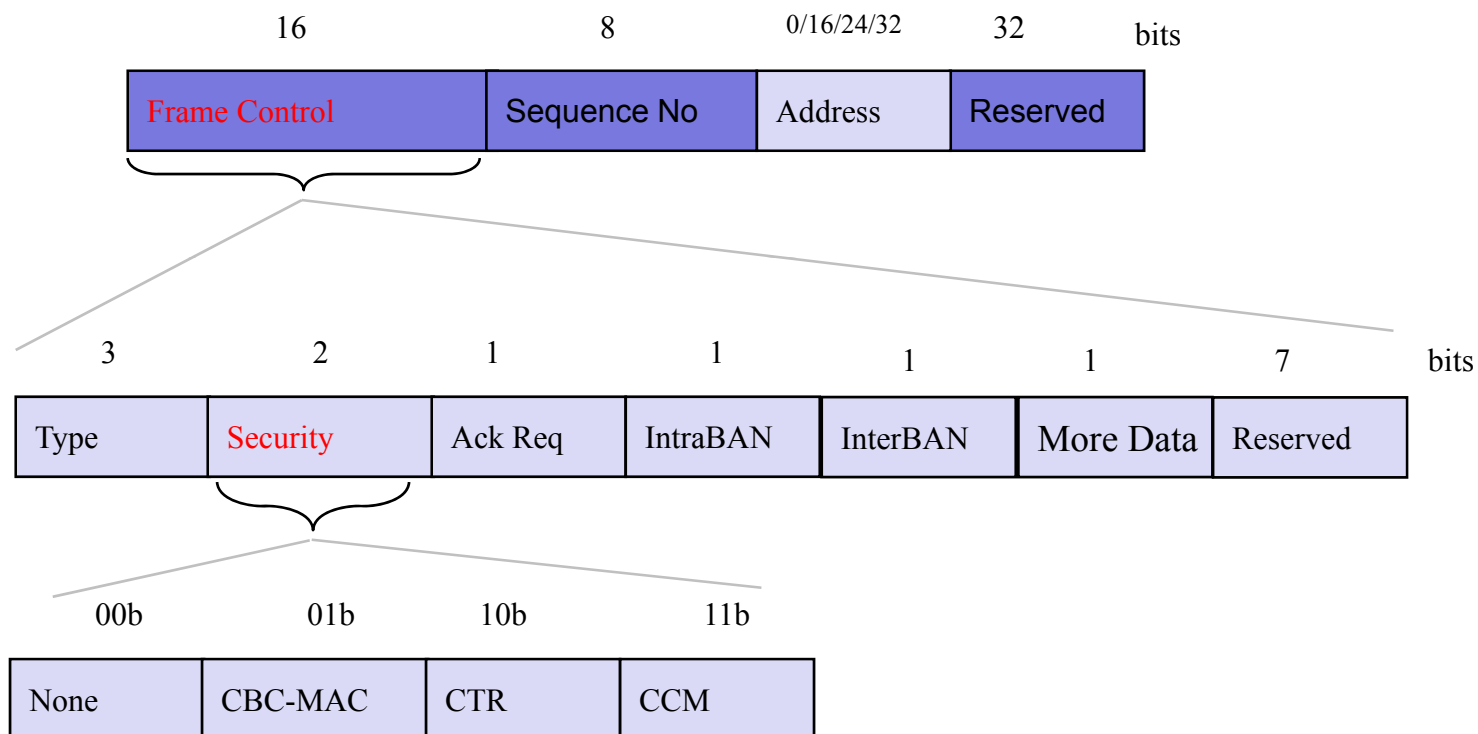


**Length: 56/72/80/88 bits = 7/9/10/11 octets**

# Frame Control: Type field

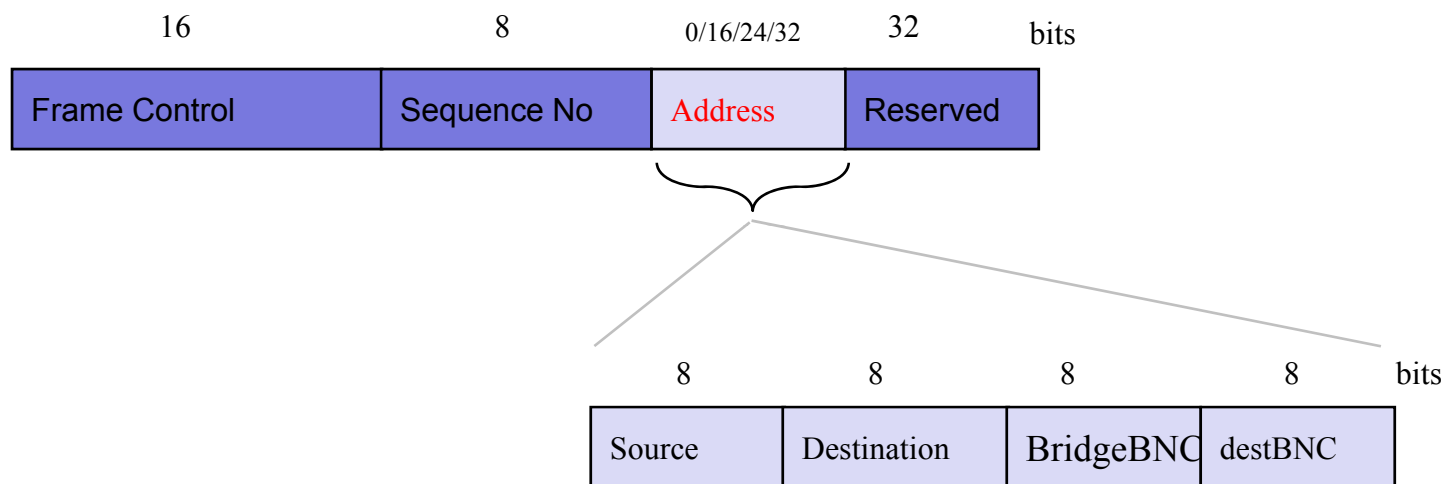


# Frame Control: Security field



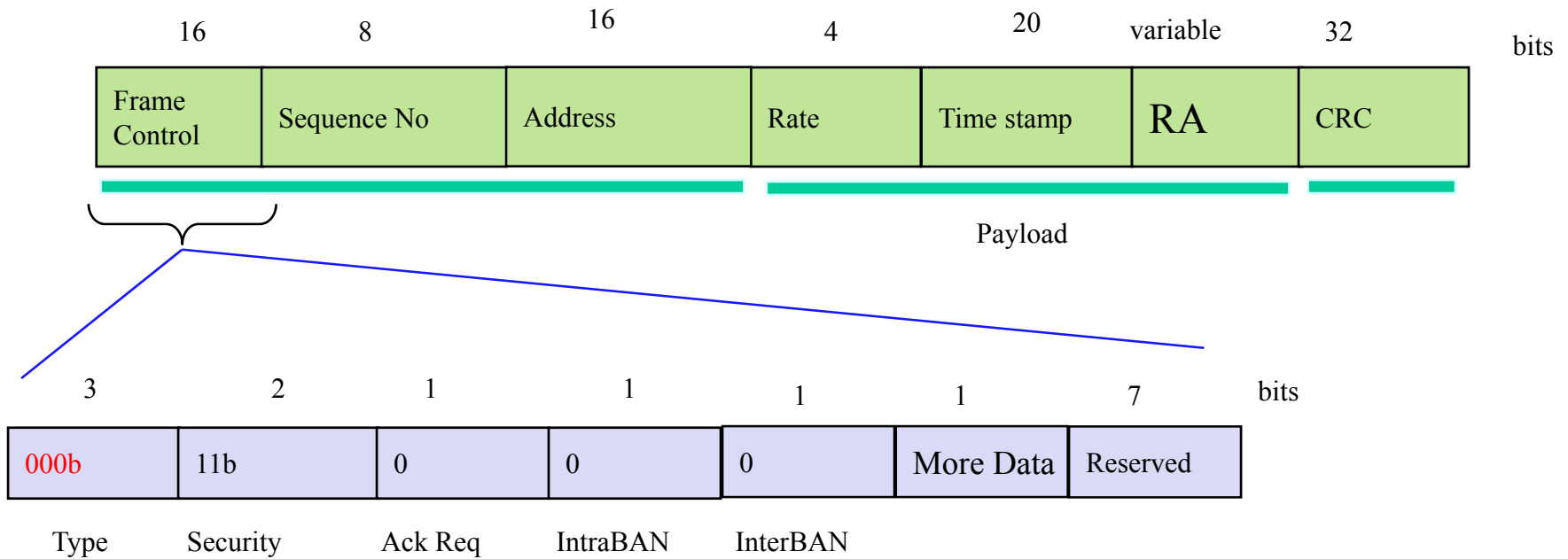


# Address Field



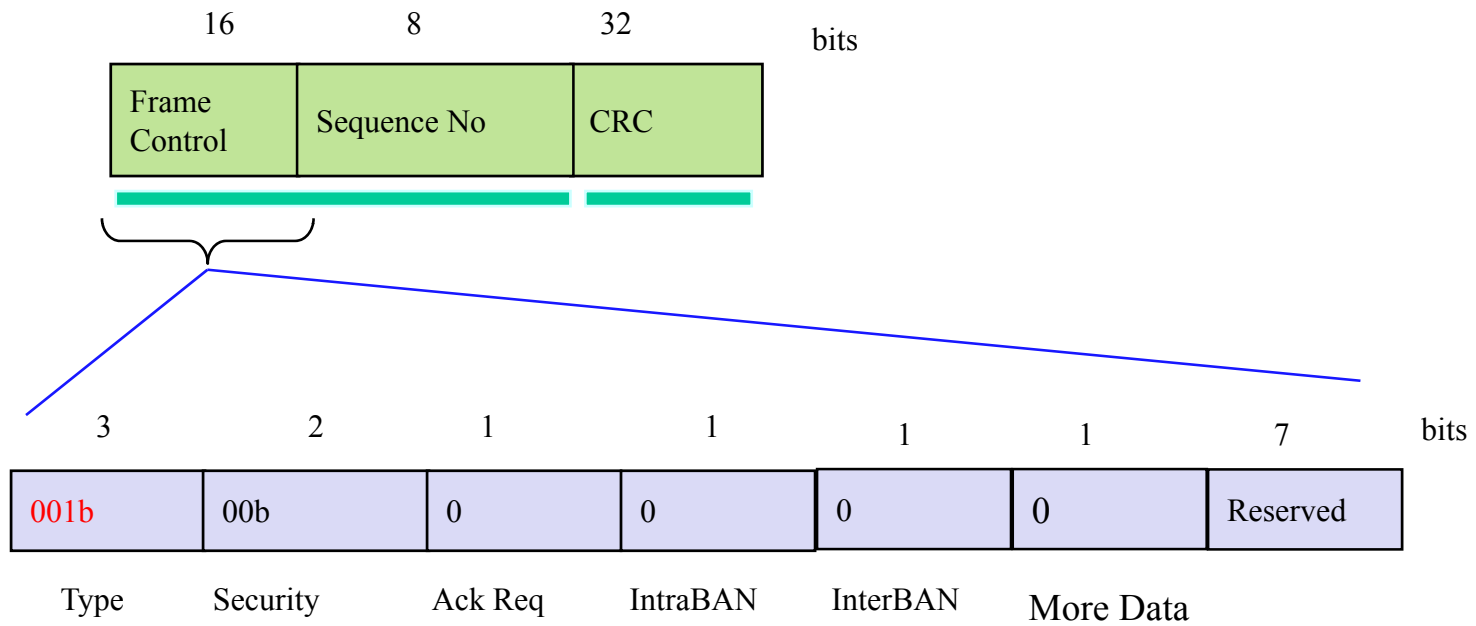
- Length: 0/16/24/32 bits = 0/2/3/4 octets
- Ack frame has no address field = 0 octet
- Beacon frame has 2 address fields = 2 octet
- Command frame has 2 address fields = 2 octets
- Data frame without bridging has 2 address fields = 2 octets
- Data frame with bridging in intra-BAN communication has 3 address fields = 3 octets
- Data frame with bridging in inter-BAN communication has 4 address fields = 4 octets

# Beacon frame



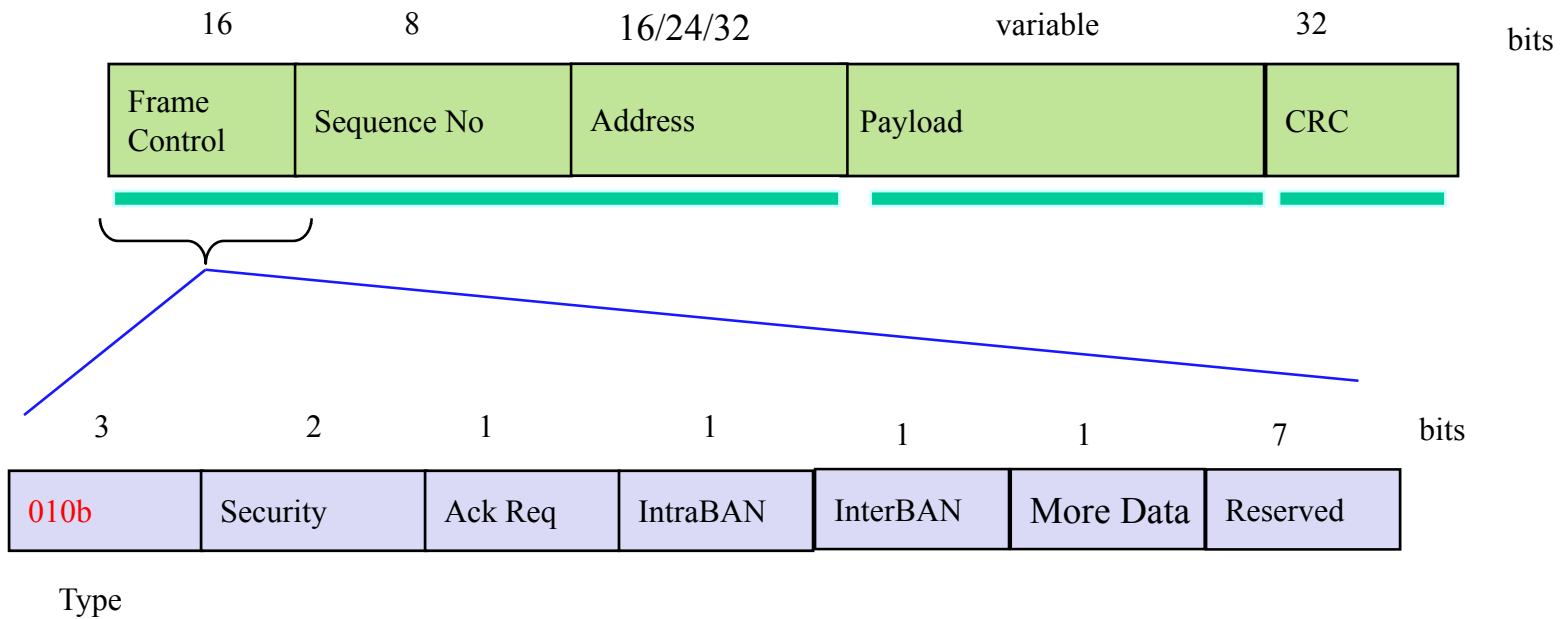
**Length: 96 bits + variable = 12 octets + variable**

# Acknowledge frame



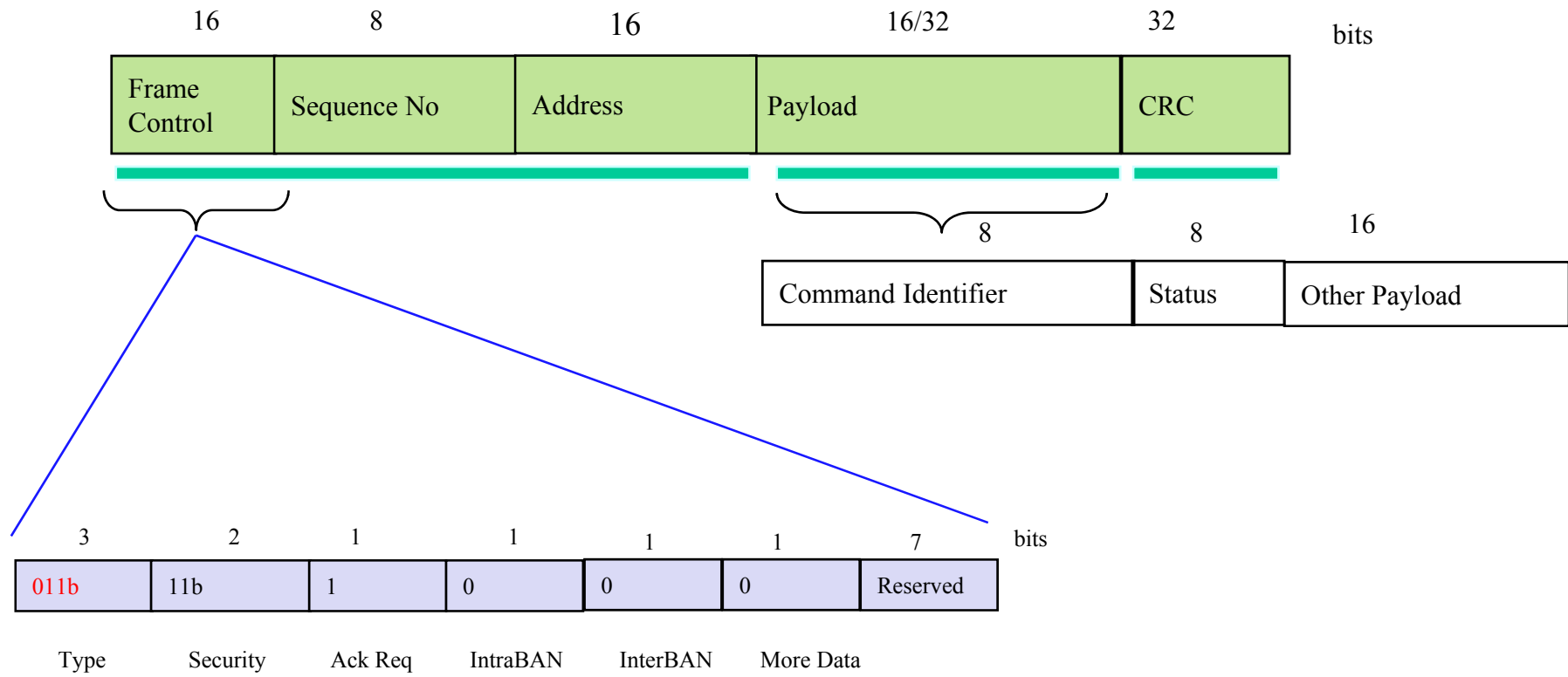
**Length: 56 bits = 7 octets**

# Data frame



**Length: 72//80/88 bits + variable = 9 /10/11 octets+ variable**

# Command frame



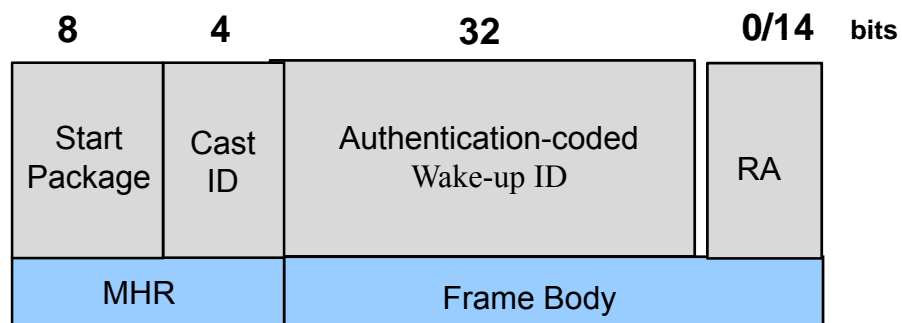
**Length: 88 /104 bits =11/13 octets**

## MAC Commands

Commands	Initiated by BNC	Initiated by BN
Device Status check	X	
Security check	X	
Association request		X
Association response	X	
Disassociation notification		X
Data request	X	X
BAN id Conflict	X	

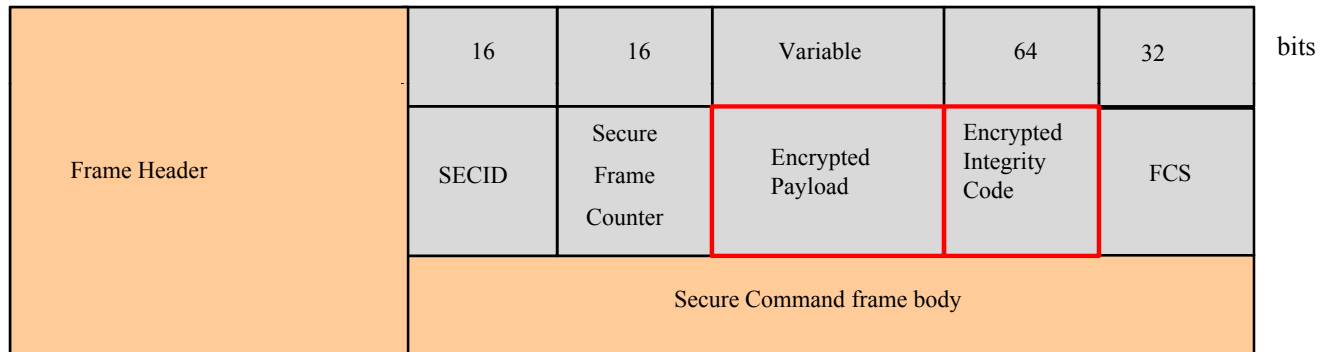
# Wake-up Frame

## Wake-up frame with Wake-up Authentication Code (WAC)



Cast ID	000b	0001b	0010b	0011b	0100b	0101b	0110b	0111b	1000b	1001b	1010b	1011b	1100b	1101b	1110b	1111b
Type	UC	MC1	MC2	MC3	MC4	MC5	MC6	MC7	MC8	MC9	MC10	MC11	MC12	MC13	MC14	BC

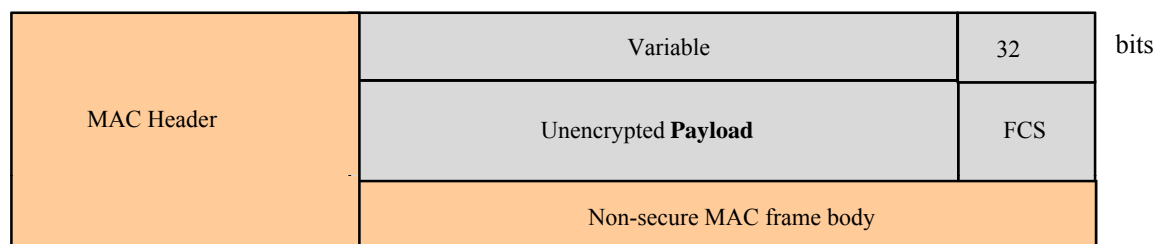
# MAC Frame with Security (1)



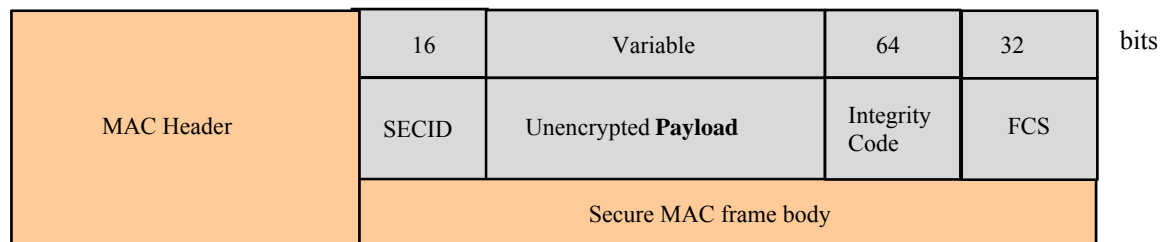


## MAC Frame with Security (2)

MAC frame without Security – Level 0 ( None)

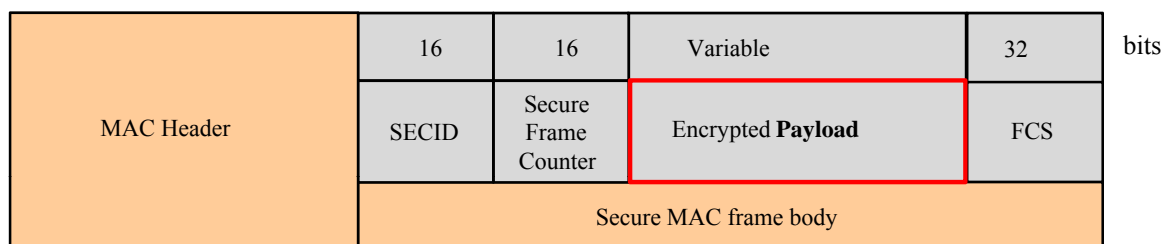


MAC frame with Security – Level 1 ( AES-CBC-MAC Mode)

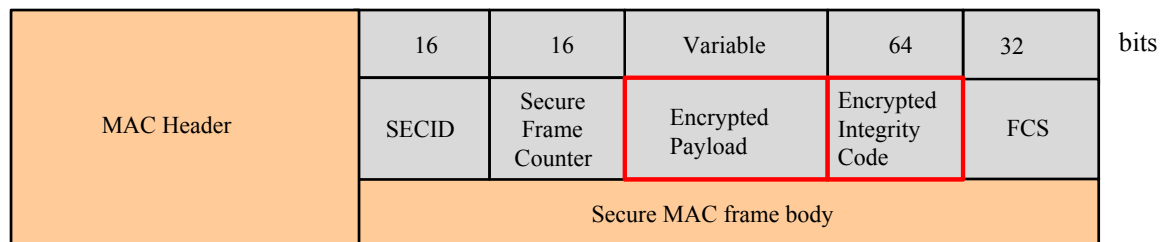


## MAC Frame with Security (3)

### MAC frame with Security – Level 2 (AES-CTR Mode)



### MAC frame with Security – Level 3 (AES-CCM Mode)



## Security Suites Specifications

- Security suites may be used when a device is operating in secured mode.
- A security suite consists of a set of operations to perform on MAC frames that provide security services.
- The security suite name indicates the symmetric cryptography algorithm and mode.

Identifier	Security Suite Name	Security Services		
		Data Encryption (Variable)	Frame Integrity (64 Bits)	Sequential Freshness
0x00	None			
0x01	AES-CBC-MAC		√	
0x02	AES-CTR	√		√
0x03	AES-CCM	√	√	√

## Channel and GTS slots Allocation Table

Channel and GTS slots Allocation Table are maintained at BNC.

RA field showing channel allocation:

<b>BN Address (8 bits)</b>	<b>Channel ID (4 bits)</b>	<b>Slot indicator ( 10 bits)</b>
--------------------------------	--------------------------------	--------------------------------------

BNC maintains the following table to keep record of channel and GTS slots use.

	BN Address (8 bits)	Channel ID (4 bits)	Slot indicator ( 10 bits)
BNC	00000001	0011	0100000000
	...	...	...
	...	...	...

In the above table, the example shows that the BN (with address 00000001) has been allocated channel 4 (0011b) and GTS slot 2 (0100000000b).

## Channel and GTS slots Allocation Table

BNC maintains the following table to keep record of channels.

Channel (4 bits)	Channel	1	2	3	4	5	6	7	8	9	10
	Channel ID	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001
*Use flag (1 bit)		0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1

\* Use flag: 0 – not in use, 1 – in use

BNC maintains the following table to keep record of GTS slots.

GTS slot Channel		1	2	3	4	5	6	7	8	9	10
1	Use flag	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1
...											
...											
...											
10	Use flag	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1

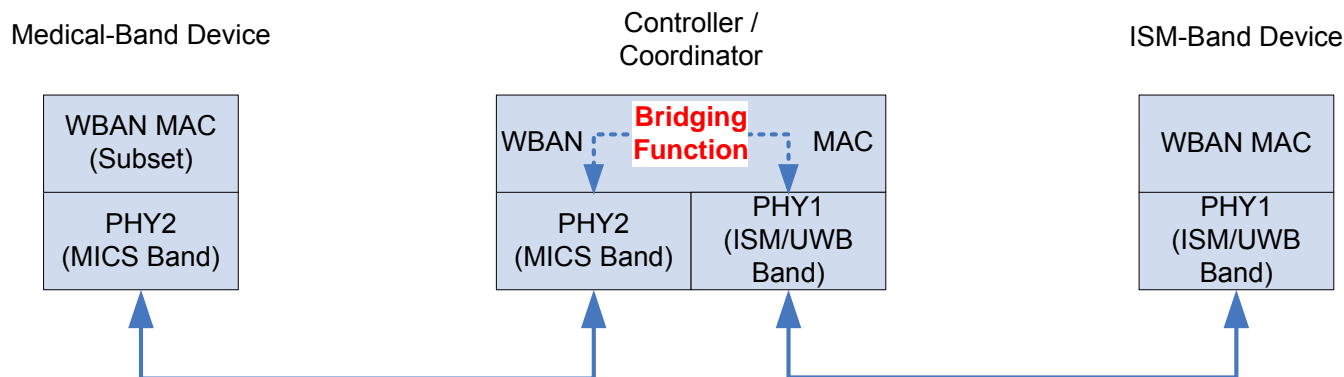
# One MAC with Multi-PHY/Bands: Bridging Function

# Single MAC with Multiple Bands/PHYs

- Multiple Bands, Multiple PHYs
  - For MICS, ISM and UWB bands, each respectively may have its own suitable PHY technique.
  - One such combination of Band and PHY can be regarded as a “Channel” from the viewpoint of MAC.
  - Devices with the same Band and PHY specifications share the same Channel by using some MAC scheme.
- “One MAC”: A Common Hybrid MAC Framework
  - Different Channels may adopt one common MAC framework.
    - One Channel is corresponding to one MAC entity.
    - The basic structure of all MAC entities is the same.
    - The MAC entity of one Channel could have minor adjustments (different values of parameters) within this framework to meet its specific requirements.
  - Hybrid Multiple Access Methods within Superframe
    - Beacon Period (+ Resource Allocation Period) + Contention Access Period + Contention Free Period + Inactive Period

# Bridging Function

- The Bridging Function connects two or more Channels by forwarding frames between them.
  - MAC transparency: support multiple PHYs
    - Setup logic connections across Channels and among devices with different PHYs.
    - Let all devices see each other as if they are of the same kind.
  - Link-layer MAC Frame (or MPDU) Relay
    - Store (data from one channel) and then forward (data to another channel)
  - Example Protocol Stack of Bridging Function

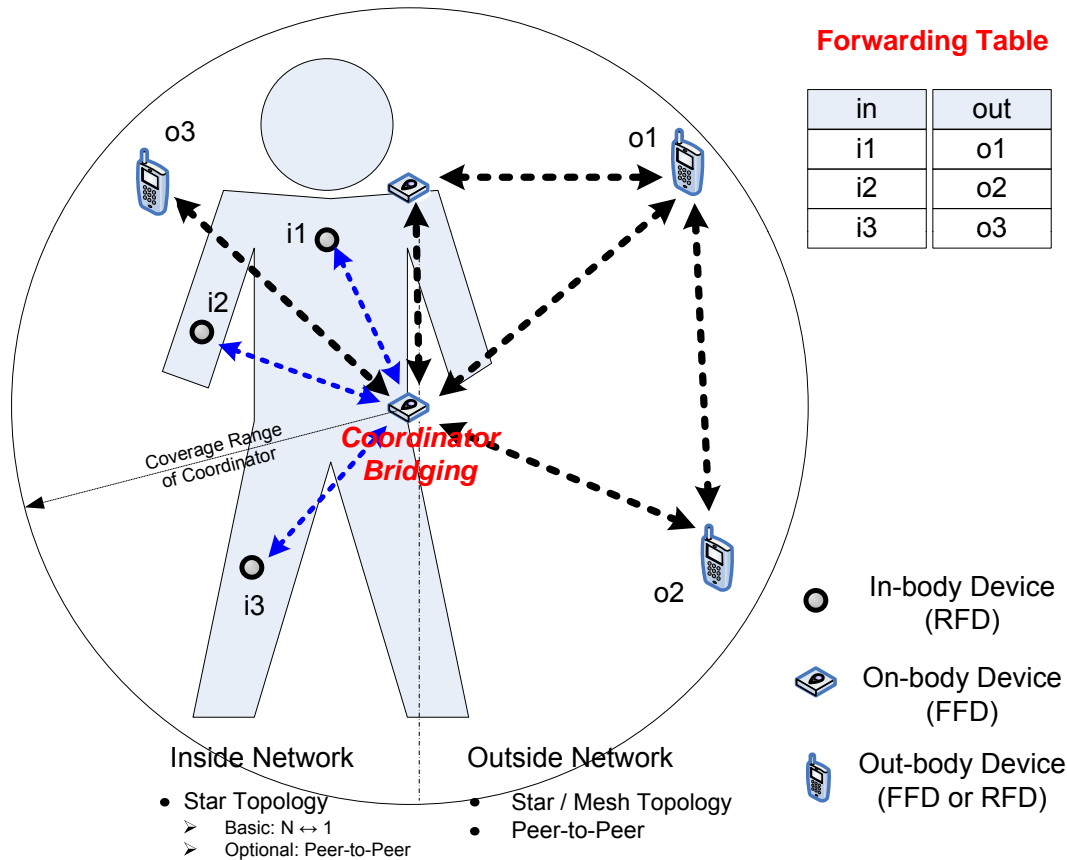




## Bridging Function in Detail

- The node implementing bridging function (in short, bridge) has two or more physical (radio) interfaces.
  - A bridge receives frames from one Channel, review the MAC address of the frame to determine if it should be forwarded to the other Channel(s) it is connected to, and retransmits the frame following the standard protocol rules for the systems it is connected to.
  - Frame Processing: integrity check, frame address filtering and mapping, encrypt/decrypt, physical layer header conversion
- A bridge has enough memory that allows it to store and forward frames between Channels.
- A bridge contains a frame address-forwarding table that it uses to determine if the frames should be forwarded between Channels.
  - Manually configurable
  - Self-learned: bridge monitors the frame traffic in the network to continually update its frame-forwarding table.
- Bridges primarily operate at the physical layer and link layers of the OSI reference model.

# WBAN Scenario with Bridging Function

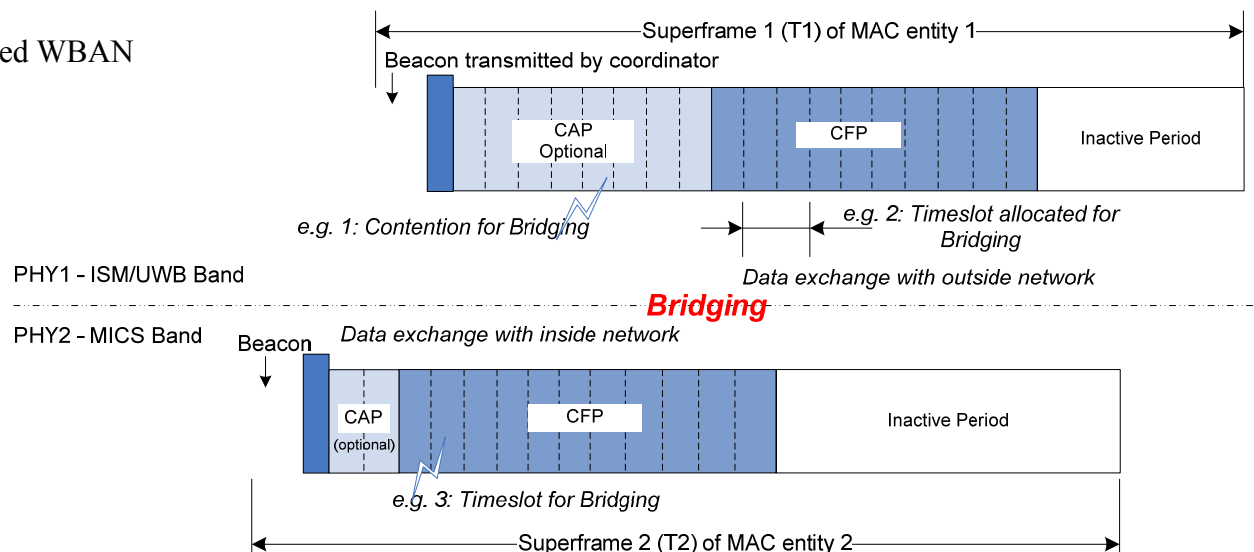


# One Comprehensive MAC

- One MAC
  - Common Beacon
    - The BNC that can support multiple PHY's broadcasts common beacon on all channels.
    - Provide universal timing/synchronization among all channels.
  - Each channel has suitable media access method.
    - Resource Allocation
      - Scheduled Resource Allocation
    - Contention Access Period
      - Slotted Aloha
    - Contention Free Period
      - TDMA
    - Inactive Period
      - Sleeping to save energy
- Bridging Function
  - Setup connection across channels.
  - Mapping: let device see all the others as if they are in the same channel.

# Scheme 1: Two Independent Superframes

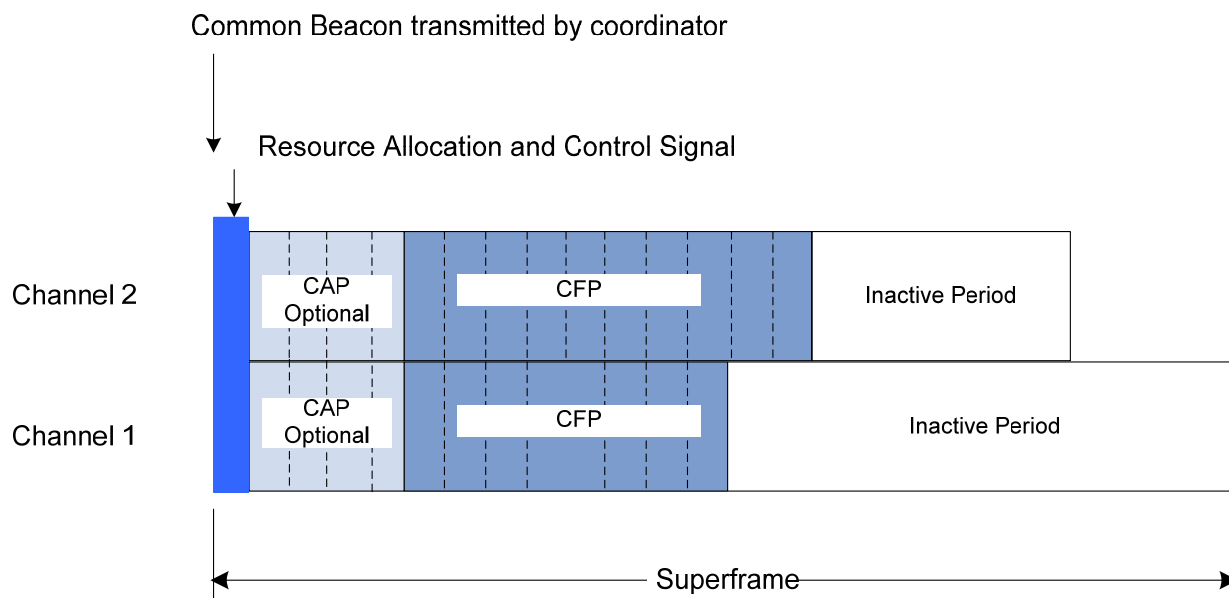
- Synchronized WBAN



- The network of ISM/UWB devices has superframe 1.
  - Timeslot for Bridging may have the highest priority.
- The network of MICS devices has superframe 2.
  - T2 may be a multiple of T1.
  - Different wake up and sleeping period.
- Bridging function works in a store-and-then-forward manner.
  - The device doing bridging function belongs to both networks at the same time.
  - In each network, the bridging device can obey current MAC settings of that network, independent of another network.

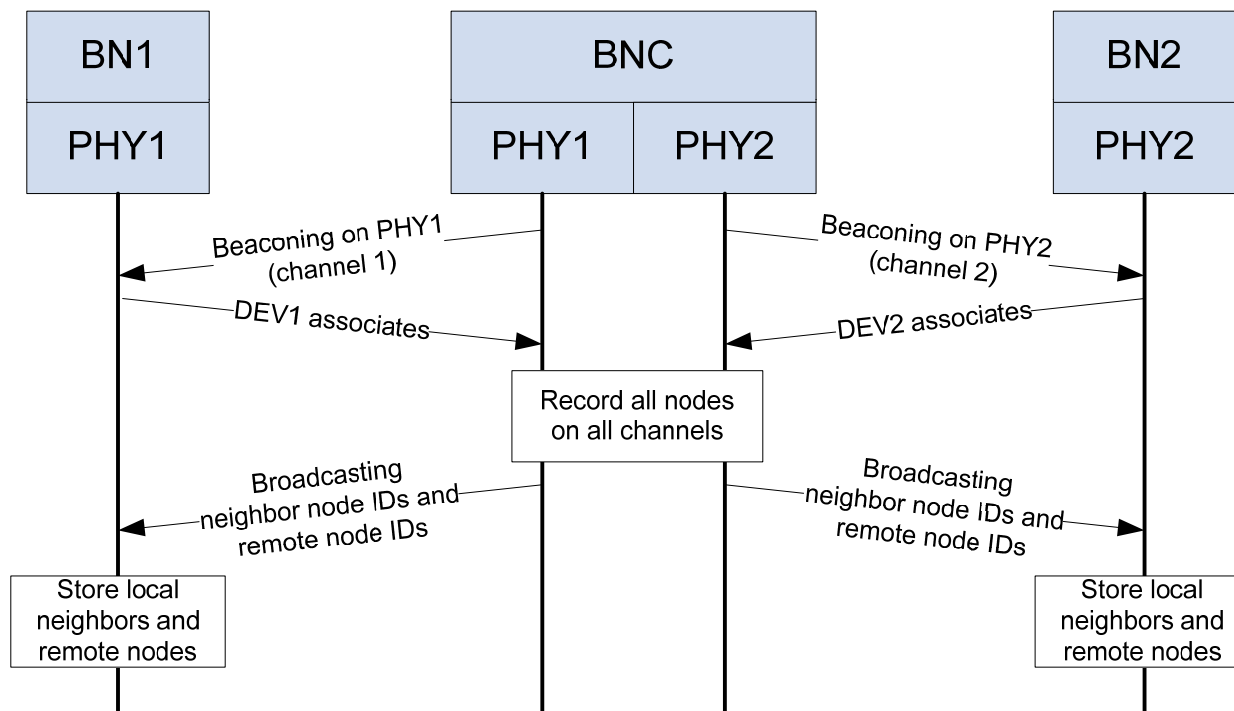
## Scheme2: One Common Beacon

- Hybrid Multiple Access
  - Among channels: Common Beacon and Timing + Bridging Function
  - Within each channel: TDMA, CSMA, Aloha, slotted-Aloha, *etc.*



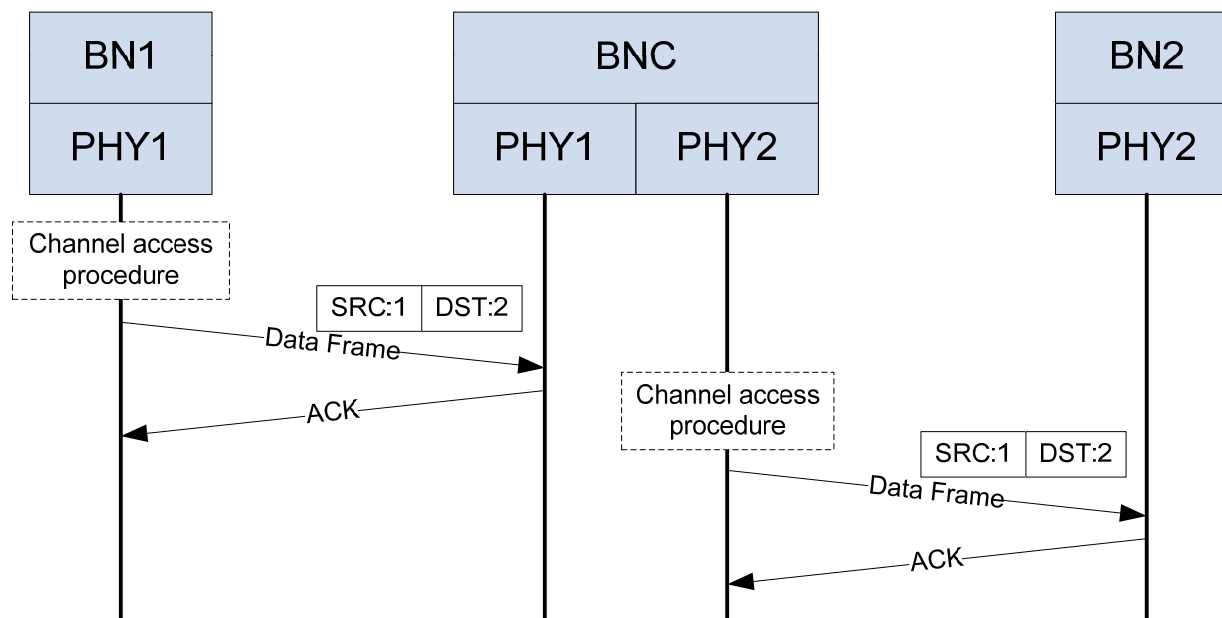
# Bridging Function Flowchart: Initialization

- Initialization



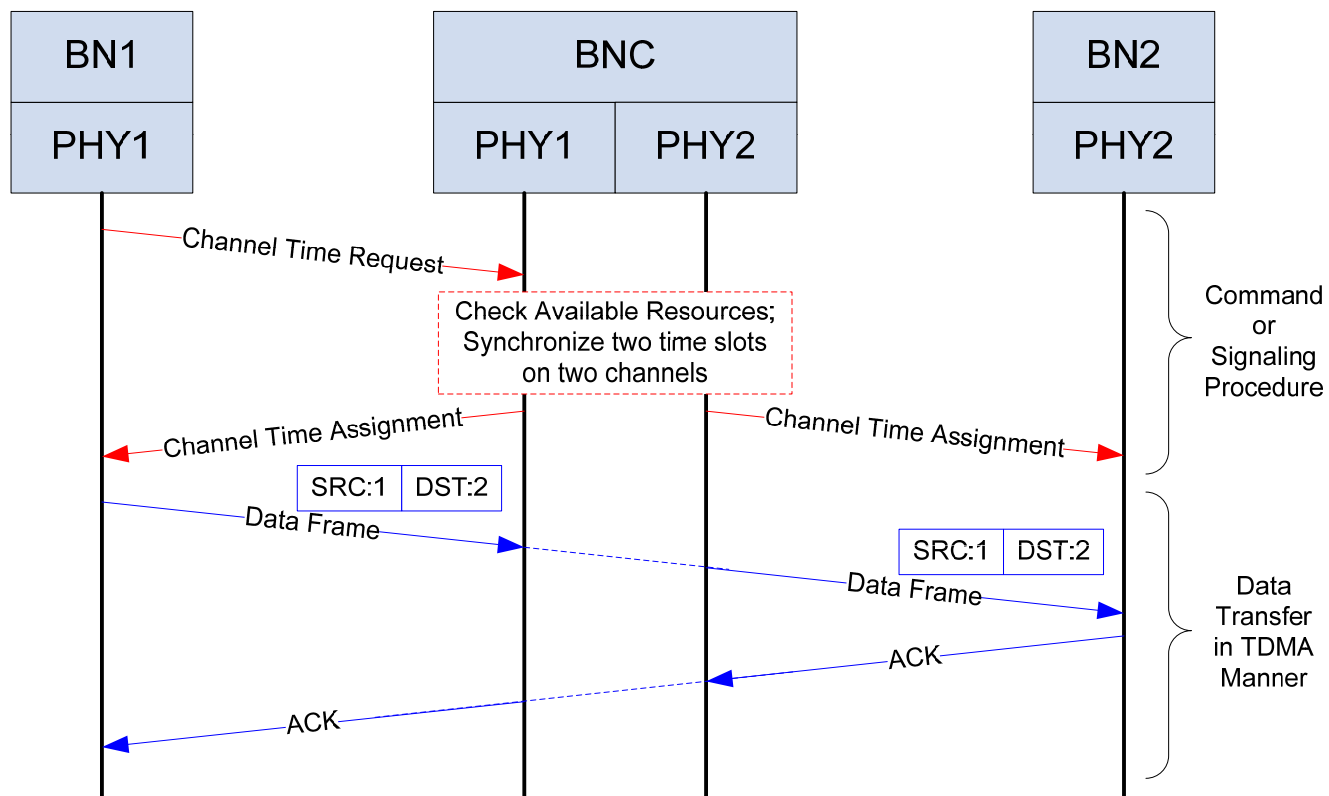
# Bridging Function Flowchart: Non-real-time

- Data transfer – Best effort



# Bridging Function Flowchart: Real-time

- Data transfer – Real-Time





## Bridging function: Discussion

- Advantages
  - Bridging function is useful, especially for in-body devices.
    - It can collect or dissipate data from or to (low-rate) in-body devices in a whole so that the transmission efficiency can be higher.
    - In-body devices can have longer sleeping period, so energy is saved.
    - The design of BN can be simplified.
  - Devices working on different bands/PHYs can transmit simultaneously.
    - Interconnection between different devices is realized logically in MAC.
    - Bridging function makes PHYs transparent to MAC.
- Questions and Answers
  - Does it result in larger delay?
    - Ans.: The extra delay could be controlled in a tolerable range.
  - Is it more complex?
    - Ans.: Interconnection problem itself is very complex. WBAN shall cooperate with existing (medical) devices working on different bands, so this design of one MAC over multiple PHYs becomes reasonable.
  - Is it necessary or not?
    - Ans.: Direct communication between in-body devices and out-body devices may encounter extremely high path loss (low transmission power may even worsen the situation) and the low data rate of in-body devices may slow down the whole network throughput.

# Performance Results

## Traffic Environment: Normal Traffic

- Model transition delays between transceiver states and power consumption in each state
- Transceiver states
  - Sleep– The BN is in sleeping mode
  - Listening State – The BN is waking up
  - Active States
    - RX – The BN is receiving data from BNC
    - TX – The BN is transmitting data to BNC

## Radio Model

- $T_s$  – the setup time required to turn on the transceiver from sleep state into the RX or TX state
- $T_T$  – the turn-around time required to switch the transceiver between RX and TX
- $P_s, P_R, P_T$  – power consumed, respectively, in the Sleep, RX, and TX states
- Average packet inter-arrival time at BN is  $L = N/\lambda$
- Data packet duration is  $T_D$
- Control frames (Beacon and ACK) duration is  $T_c$
- Assume low traffic conditions

$$1/\lambda \gg T_D + T_T + T_c$$

## System Parameters: Normal Traffic

- Average Power Consumption during transmission is:

$$(P_s + P_R (T_c + T_s) + P_T (T_D + T_T) + P_T (T_c + T_T)) / L$$

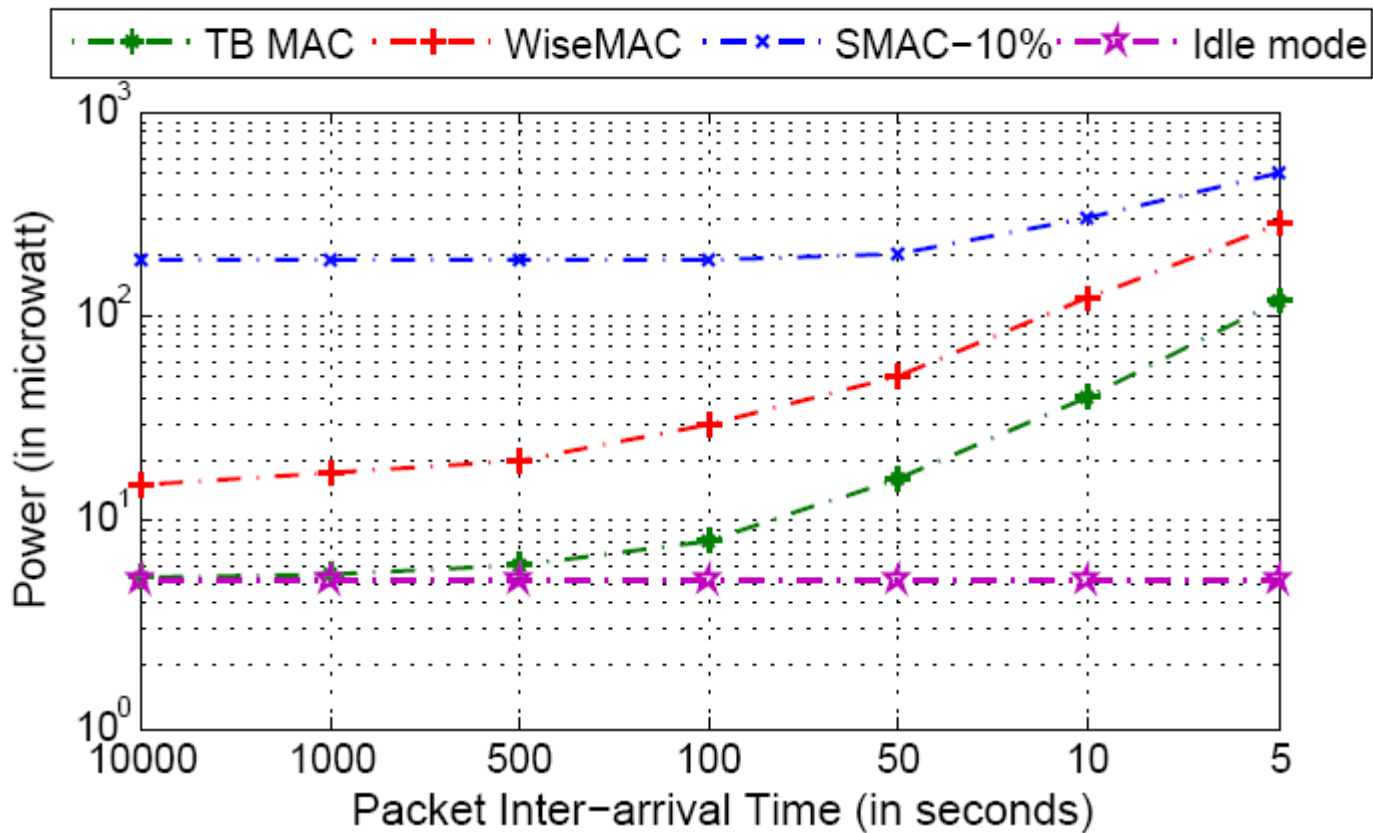
Where L is the Average packet arrival rate at the BN and is equal to  $N/\lambda$ .

Parameter	Value
$P_s$	5
$P_R$	1.8mW
$P_T$	27mW
$T_s$	0.8ms
$T_T$	0.4ms
$T_D$ (50 bytes)	16ms
$T_c$ (10 bytes)	3.2ms

Average delay: The time to transmit the beacon, the time to transmit data, and the time to receive ACK.

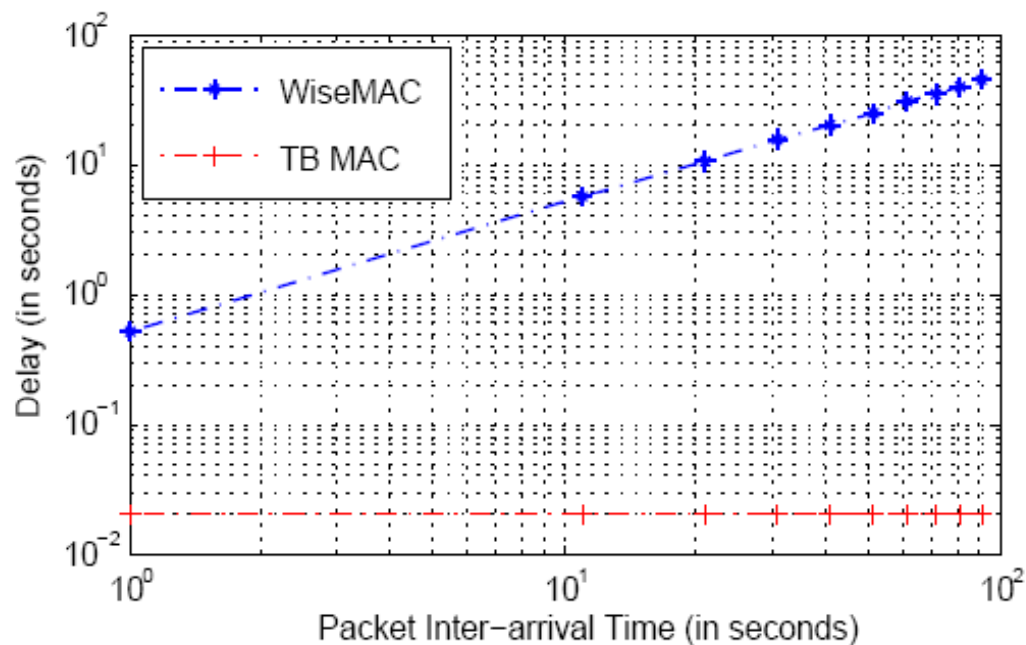
$$2T_c + 2T_T + T_D$$

### Average Power Consumption vs. Packet Arrival Time

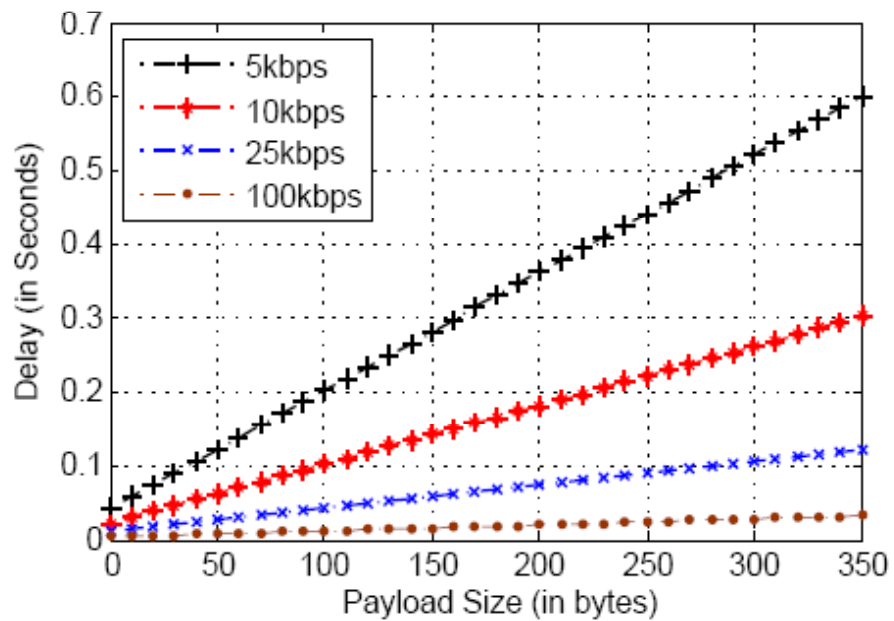


TB MAC – Traffic Based MAC Protocol

# Delay Vs. Packet Arrival Time

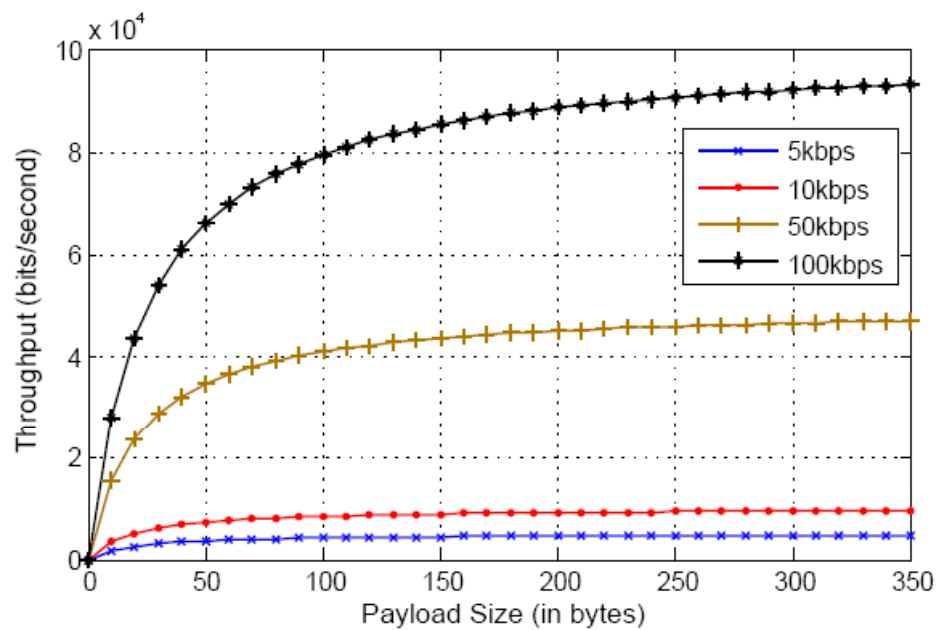


# Delay vs. Payload Size





# Throughput vs. Payload Size



# Conclusion

## Conclusions

- The WBAN traffic is classified into Normal, On-demand, and Emergency traffic.
- Two wakeup scheme proposed
  - In normal case, wakeup by traffic-based patterns
  - In on-demand and emergency cases, wakeup by radio
- The BNC creates and modify the traffic-based wakeup table
- A 2-stage secure wakeup scheme is proposed to ensure secure communication.
  - Why not use wakeup for normal traffic?
- We further presented MAC frame structure that includes beacon, data, command frames formats.
- A bridging function is proposed to allow communication between different devices working on different bands/PHYs.
- Our performance results show that the traffic-based wakeup patterns save significant amount of energy.