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

**Submission Title:** [Secure MAC Proposal for Body Area Network]
**Date Submitted:** [15 November, 2009]

**Source:** [Masahiro Kuroda, Osamu Atsumi, Ryuji Kohno] Company [NICT, Sangikyo]
Address [4-2-1 Nukui-Kitamachi, Koganei, Tokyo, Japan ]
Phone:[+81-42-327-6886], FAX: [+81-42-327-5519],
E-Mail:[marsh@nict.go.jp, atsumio@sangikyo.co.jp]

**Abstract:** [This document describes security requirements and a proposal for MAC security to the TG6 group]

**Purpose:** [Discussion in 802.15.6 Task Group ]

# Secure MAC Proposal for Body Area Network

Masahiro Kuroda, Osamu Atsumi, Ryuji Kohno

NICT, Sangikyo

# Outline

- Summary
- Motivation
- Requirements
- Proposals
- BAN security references
- Conclusion

# Summary

- The data plane protocol defines the frame format for data encapsulation, encryption, and authenticity
- The security is configured depending on the use environment and MAC has the interface to register security suites in addition to default suites that satisfy security guidelines

# Motivation

- Both user requirements and efficient security requirements need to be satisfied in Secure BAN

# User Requirements and Efficient Security Requirements

- User requirements
  1. Easy setup not to disturb users, such as a medical staffs
  2. Power efficient not to add extra hand works for medical staffs
  3. A patient who wears a BAN needs to know the first-level (brief) analysis of sensed data as the primary user
- Efficient security requirements
  1. Flexible cipher integration with less computation
  2. Simple key pre-distribution with re-keying to maintain strong security
  3. Less traffic authentication/encryption between nodes and the coordinator
  4. Protection from attacks under restricted power supply
  5. A coordinator has an interface to looked at data received (from above 3.)

# Flexible Cipher Integration

- BAN is an extremely power-efficient network and expects compact and power-efficient ciphers, such as OTP (One Time Pad cipher) and others  in addition to AES-128 CBC as long as they satisfy security suites requirements
- Cipher integration is transparent to MAC, because the purpose of cipher is to protect user data. MAC, on the other hand, takes care of protection from wireless related attacks

# Simple Key Pre-distribution

- Key seeds come from not only a backend but also a sensor which gets individuality data directly from human body
- Both key distribution mechanisms need to be supported

# Less Traffic between Nodes

- Sensors consume much power during the receive-wait state
- Embedded mutual authentication reduces extra protocols/computation in a sensor

# Protection from Unintentional Attacks

- MAC takes care of external threats for wireless communication. MAC monitors false BAN traffic and others relate to other layers
  1. Eavesdropping (MAC)
     - Adversaries place a wireless device in a monitor mode, record BAN traffic, and use the data to infer valuable BAN information
  2. Traffic injection (MAC)
     - Adversaries attempt to inject false BAN traffic to cause a disruption of BAN services
  3. RF interference
     - Interference/jamming from external factors is a serious threat to BAN services availability
  4. Physical threats
     - BAN devices have the risk of physical damages, vandalization ,and so on

# Coordinator Decrypts Received Data

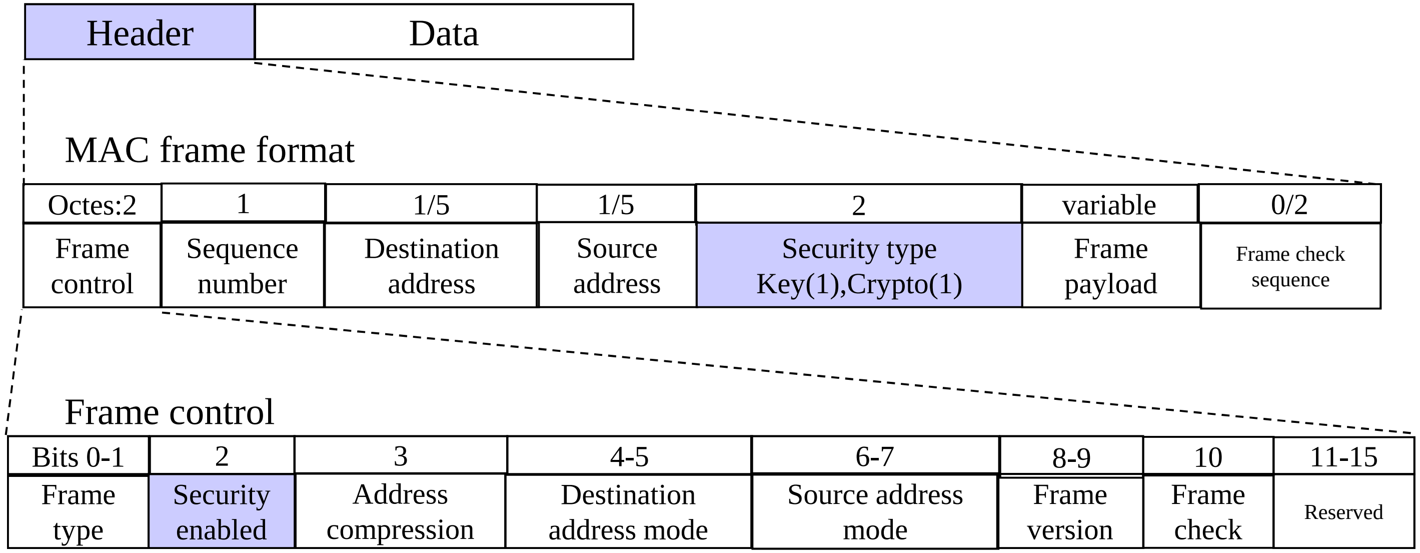
- The person who wears a BAN first knows whether serious trouble or not before sending vital information to remote sites
- For this purpose, a coordinator gathers vital data securely and decrypts it for the first-level analysis
- Two security models, one for a BAN and the other for backend system, exist in a coordinator

# Requirements for Secure MAC

1. MAC has an interface to plug-in ciphers as long as thy satisfy security suites guideline
2. MAC has an interface to implement various types of key distribution mechanisms and defines message formats for the protocol
3. MAC has protections from attacks
4. MAC security is not transparent to backend networks

# MAC Frame Proposal

- MAC frame format and frame control
  - MAC frame format consists of frame control field, sequence number, destination/source addresses, security type, and frame payload with frame check sequence
  - The frame control consists of frame type. security enabled, address compression, destination/source address mode, frame version, and frame check
  - When the security enabled bit is set, registered application level security is used by referencing the security type in the header



MAC frame format

| Octes:2 | 1 | 1/5 | 1/5 | 2 | variable | 0/2 |
|---|---|---|---|---|---|---|
| Frame control | Sequence number | Destination address | Source address | Security type Key(1),Crypto(1) | Frame payload | Frame check sequence |

Frame control

| Bits 0-1 | 2 | 3 | 4-5 | 6-7 | 8-9 | 10 | 11-15 |
|---|---|---|---|---|---|---|---|
| Frame type | Security enabled | Address compression | Destination address mode | Source address mode | Frame version | Frame check | Reserved |

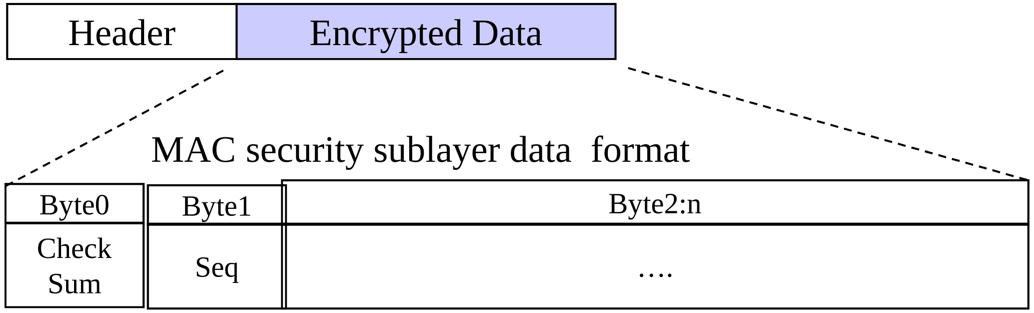
# MAC Frame Proposal

- Security bit assignments in the frame control

Security enabled: 0x0, 0x1

Security type: Key: 0x00 = reserved, 0x01 = carousel-type key, 0x02 = reserved

Crypto:0x00 = reserved, 0x01 = AES128-CBC, 0x02 = reserved

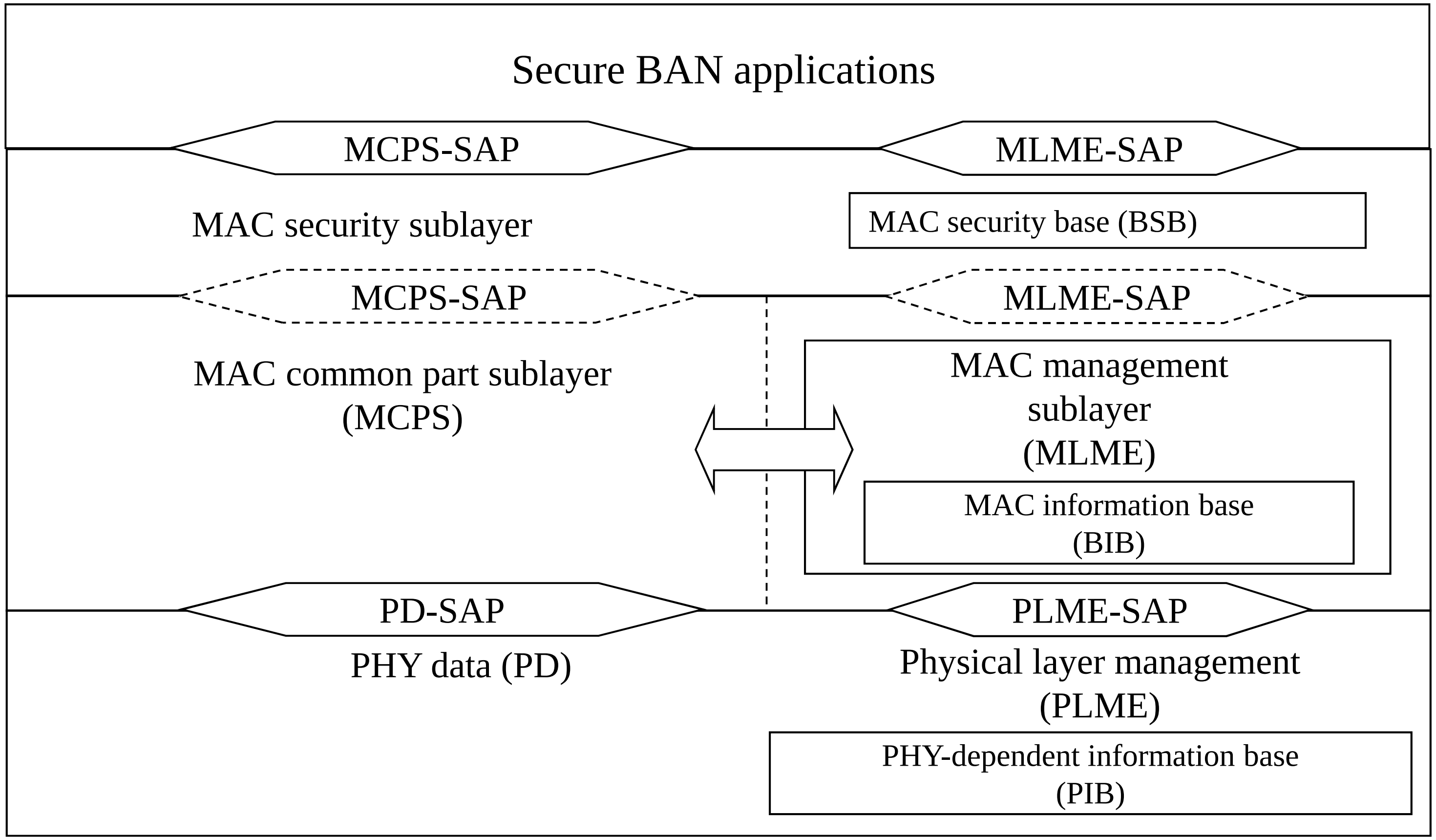


| Header | Encrypted Data |
|---|---|

MAC security sublayer data format

| Byte0 | Byte1 | Byte2:n |
|---|---|---|
| Check Sum | Seq | …. |

# Transparency of Security

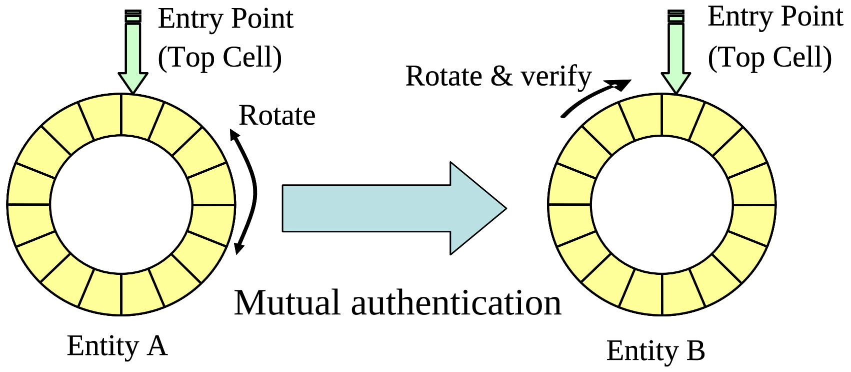


# BAN Security References

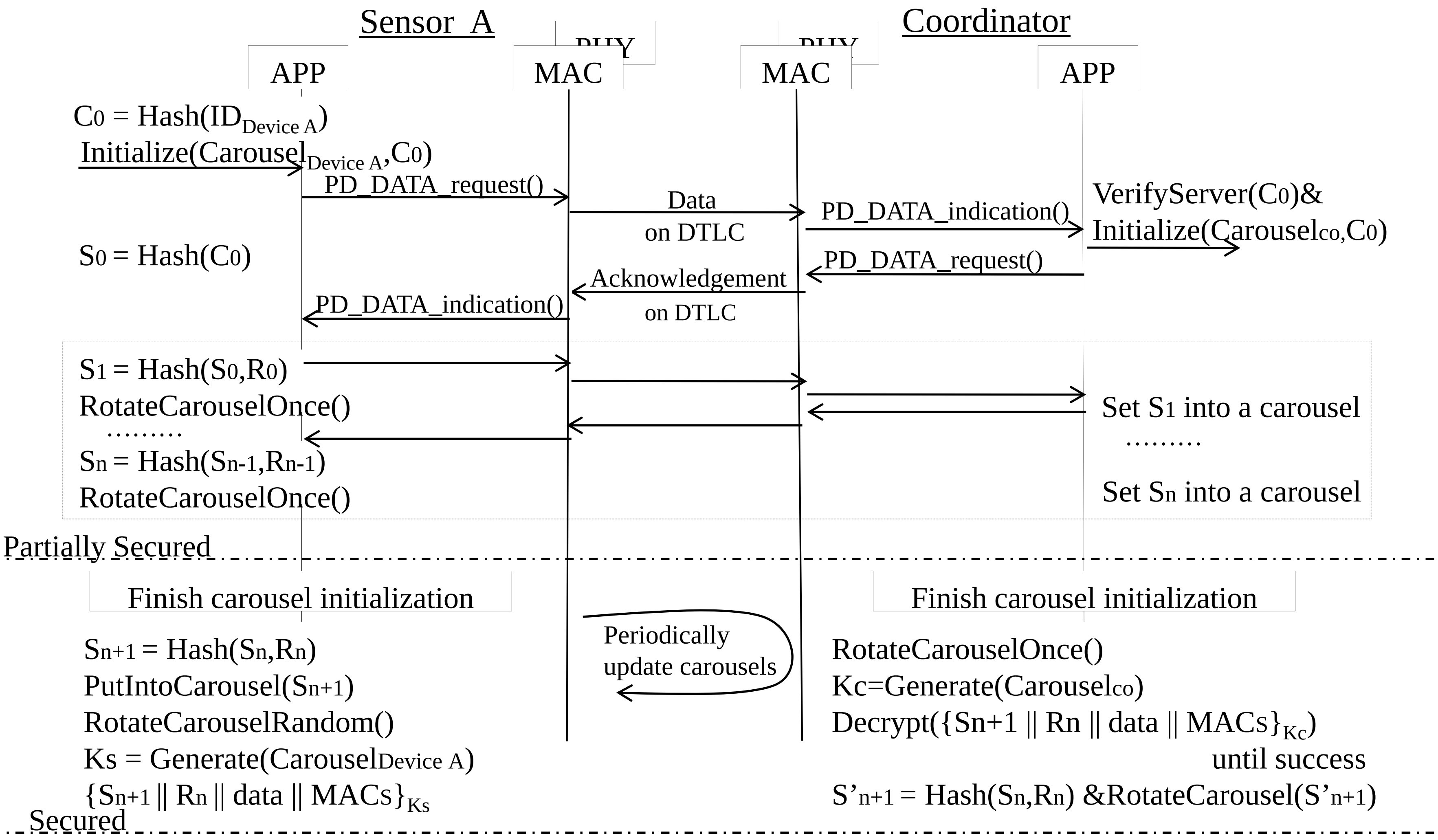
1. Sensor-driven Carousel-type Key Generation
2. Wearable Sensors and Secure BAN
3. Unified OTP Crypto with Authentication
4. Additional Cipher Suites Guideline from IEEE802.1 AE

# Sensor-driven Carousel-type Key Generation

- A carousel is a data structure that is a circular list of cells, with each cell capable of containing information regarding a trail, such as the trail of a user movement and/or ECG data
- When new information is entered into the carousel, it is placed in the entry point cell, and the carousel is then rotated by a random number of cells
- Whenever there is superseded information stored at the entry point, it is overwritten by new information
- Both a sensor and the coordinator share a carousel corresponding to the varying behavior/vital data
- Generate a key from this carousel at both sides



# Key Initialization Protocol



Sensor A

Coordinator

PHY

APP

MAC

PHY

MAC

APP

$C_0$ = Hash($ID_{Device\ A}$)

Initialize($Carousel_{Device\ A}$,$C_0$)

PD_DATA_request()

Data on DTLC

PD_DATA_indication()

VerifyServer($C_0$)&

Initialize($Carousel_{co}$,$C_0$)

$S_0$ = Hash($C_0$)

PD_DATA_request()

Acknowledgement on DTLC

PD_DATA_indication()

$S_1$ = Hash($S_0$,$R_0$)

RotateCarouselOnce()

………

$S_n$ = Hash($S_{n-1}$,$R_{n-1}$)

RotateCarouselOnce()

Set $S_1$ into a carousel

………

Set $S_n$ into a carousel

Partially Secured

Finish carousel initialization

Finish carousel initialization

Periodically update carousels

$S_{n+1}$ = Hash($S_n$,$R_n$)

PutIntoCarousel($S_{n+1}$)

RotateCarouselRandom()

Ks = Generate($Carousel_{Device\ A}$)

$\{S_{n+1} \| R_n \|$ data $\|$ MACs$\}_{Ks}$

RotateCarouselOnce()

Kc=Generate($Carousel_{co}$)

Decrypt($\{Sn+1 \| Rn \|$ data $\|$ MACs$\}_{Kc}$)

until success

$S'_{n+1}$ = Hash($S_n$,$R_n$) &RotateCarousel($S'_{n+1}$)

Secured

# Evaluation

- Sensor-based key generation in addition to coordinator-based one
- Intrinsic mutual authentication by generating a key separately in both sides
- Less computation key generation
  - 67.8 hours continuous operation
  - 220 mAh, 3 grams battery
- The secure MAC works on an small ECG and other sensors
  - The MAC/PHY and AES128-CBC with the key generation consumes 29KB ROM and 2 KB RAM on an 8-bit CPU
  - More than 8 ECG sensors associate with the same secure BAN and they operate properly
- 32 bytes data transfer
  - Approximate error rate in PHY is $2 \times 10^{-4}$
  - Verify almost the same error rate with MAC and PHY

# Wearable Sensors and Secure BAN

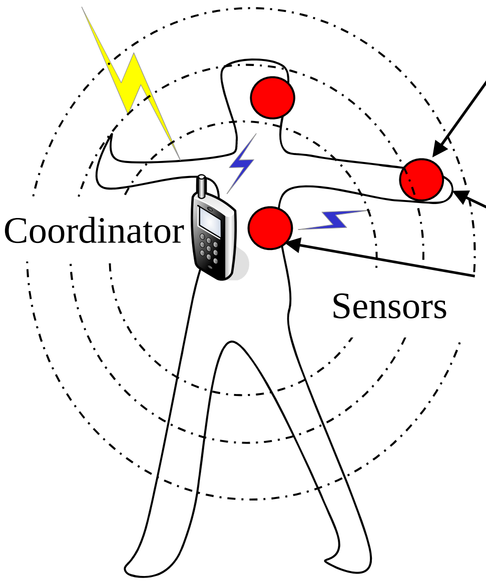
- Five wearable sensors for diseases
  - Electrocardiograph
  - Blood pressure
  - Breath
  - Percutaneous oxygen saturation (SpO2)
  - 3D-axes acceleration

| Disease & condition | ECG | Blood pressure | Breath | SpO2 | 3D Accel. | Related department of diagnosis and treatment |
|---|---|---|---|---|---|---|
| High blood pressure (related to cerebral infarction, apoplexy, kidney disease, and diabetic) | △ | ○ | △ | △ | ○ | Internal medicine<br>Circulatory organs |
| Heart disease | ○ | ○ | △ | △ | △ | Internal medicine<br>Circulatory organs |
| Sleep apnea syndrome(SAS) | △ | △ | ○ | ○ | △ | Respiratory Medicine<br>Otolaryngology<br>Circulatory organs<br>Internal medicine |
| Chronic obstructive pulmonary disease (COPD) | △ | △ | ○ | ○ | △ | Respiratory Medicine |

○: Required, △: Better to wear

From Dr. Yamasue, Medical School, Yokohama City University

# Wearable Sensors and Secure BAN



Coordinator

Sensors

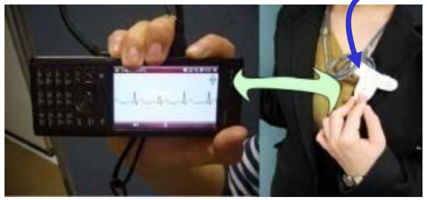
Wristwatch-type sphygmomanometer

Wristband-type stress meter

Ring(SpO2)

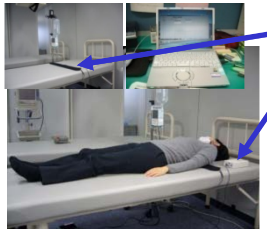
Wearable- or accessory-type (Electrocardiogram, Positioning, Temperature)

- Electrocardiogram (ECG)
- 3D-acceleration
- Temperature



Wireless ECG with 3D-accel. and temp.

- Breath



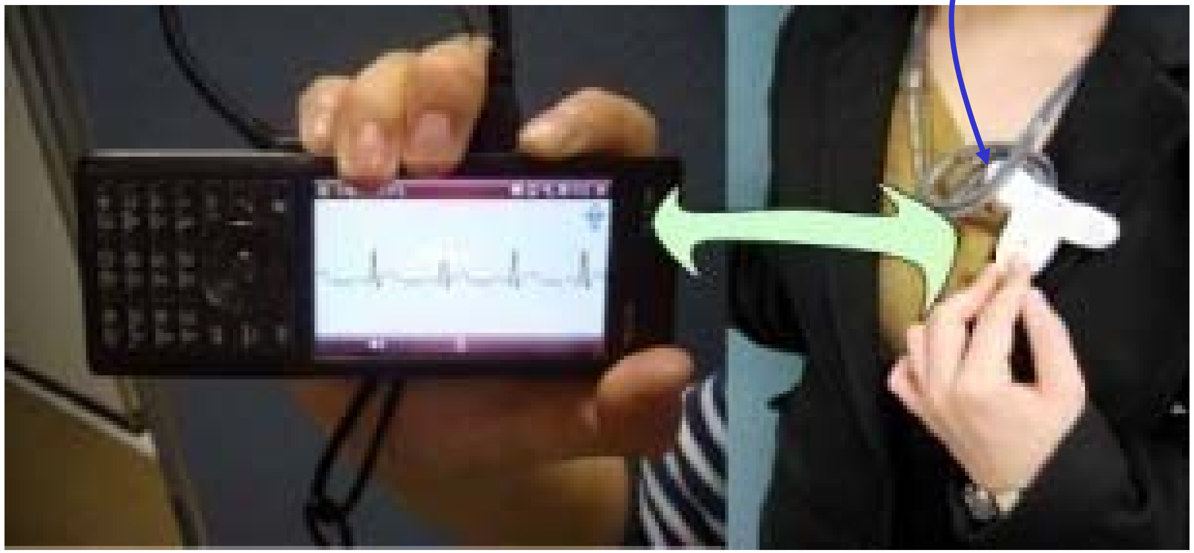
Breath sensor

Wireless controller

- Blood pressure
- Percutaneous oxygen saturation (SpO2)

Wireless SpO2 sensor

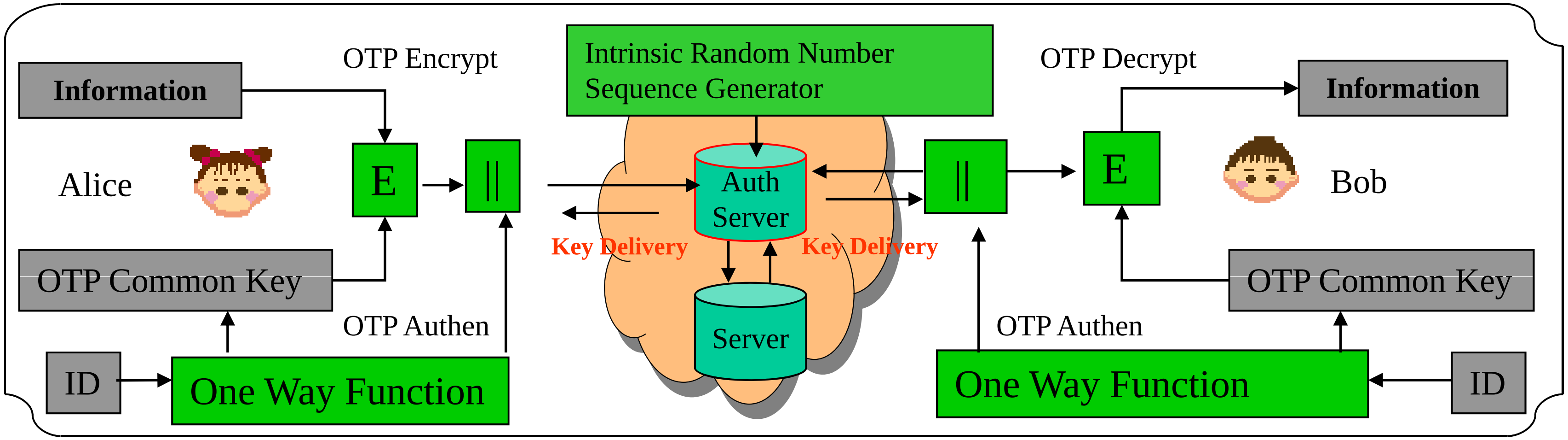
# ECG Eample



**Wireless ECG with 3D-accel. and temp.**

# Unified OTP* Crypto with Authentication

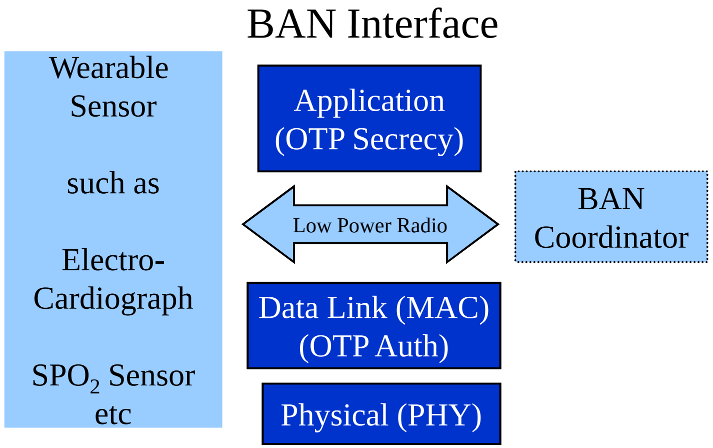
- The main algorithm of OTP is modulo arithmetic based on the intrinsic random sequence derived from the natural phenomenon and less computation in a sensor
- Unified OTP Cryptosystem for both Secrecy/Authentication in communication including the secret key delivery system from the initial to the subsequent stages of the communication without depending on mathematical methodology except modulo arithmetic
- Secure initial key delivery is not opened yet.



OTP*: One Time Pad cipher whose encryption key is disposable on one time pad basis

# Implementation for OTP Authentication and Secrecy

- Both OTP authentication and secrecy are stream cipher
- The size of a key for OTP Authentication is proposed as 64bits or 128bits and that of the key for OTP Secrecy is dependent on the amount of data transfered



# Additional Cipher Suites Guideline from IEEE802.1 AE

a) Algorithms chosen have an effective key length of at least 128 bits. In schemes built on block ciphers, the underlying block cipher has a block width of at least 128 bits

b) If serviced by separate algorithms, the properties of the authentication and confidentiality mechanisms are combinable in accordance with well-established security results. Either the encryption happens before authentication, or the encryption is performed through keystream generation.

c) Either of the following holds true:

1) The underlying cryptographic cipher is approved by either a national or international standards body or a government agency; or

2) The following conditions i) through iv) apply:

i) The Cipher Suite provides message authentication using a message authentication algorithm with a publicly available proof of security against forgery attacks, even in a model where the attacker has the ability to choose messages for the sender.

ii) If confidentiality is provided, the confidentiality mechanism has a publicly available proof of security in a model where the attacker has the ability to adaptively choose both plaintext and cipher text.

iii) Mechanisms for confidentiality and message authentication are used in a way that is consistent with their proof of security. For example, if using the Cipher Block Chaining (AES-CBC) mode of operation the IV is performed through keystream generation.

iv) Mechanisms for confidentiality and message authentication are used in a way that is consistent with their proof of security. For instance, if using the Cipher Block Chaining (AES-CBC) mode of operation, the IV is randomly selected with each message, and not sequentially.

# Conclusion

- The data plane protocol defines the frame format for data encapsulation, encryption, and authenticity
- The security should be configurable satisfying security suites requirement depending on the use environment, such as medical/healthcare and entertainment
- There are candidates for power-efficient authentication and secrecy for BAN and BAN has its security domain which is not transparent from backend security systems