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
- Key distribution
- Crypto
- MAC Frame Proposal
- 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 two-types of key-distributions (sensor- and coordinator-driven) are supported
- MAC has the interface to register security suites in addition to default suites that satisfy security guidelines

Simple Key Pre-distribution

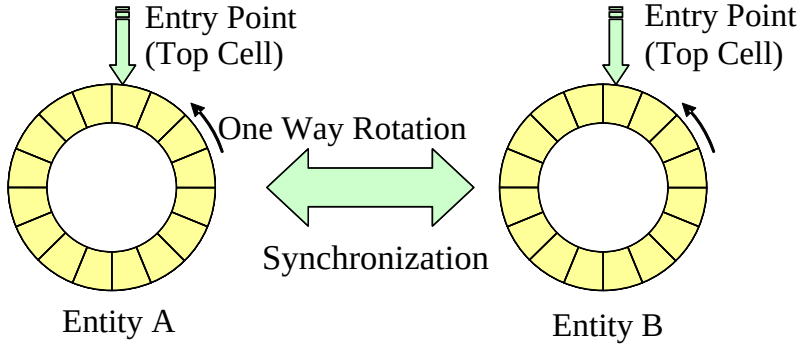
- Key seeds come not only from a backend but also from a sensor which gets data individuality directly from human body
- Both key distribution mechanisms need to be supported
  - Especially, generate a key using sensed data and not to exchange between a node and the coordinator

Less Traffic between Nodes

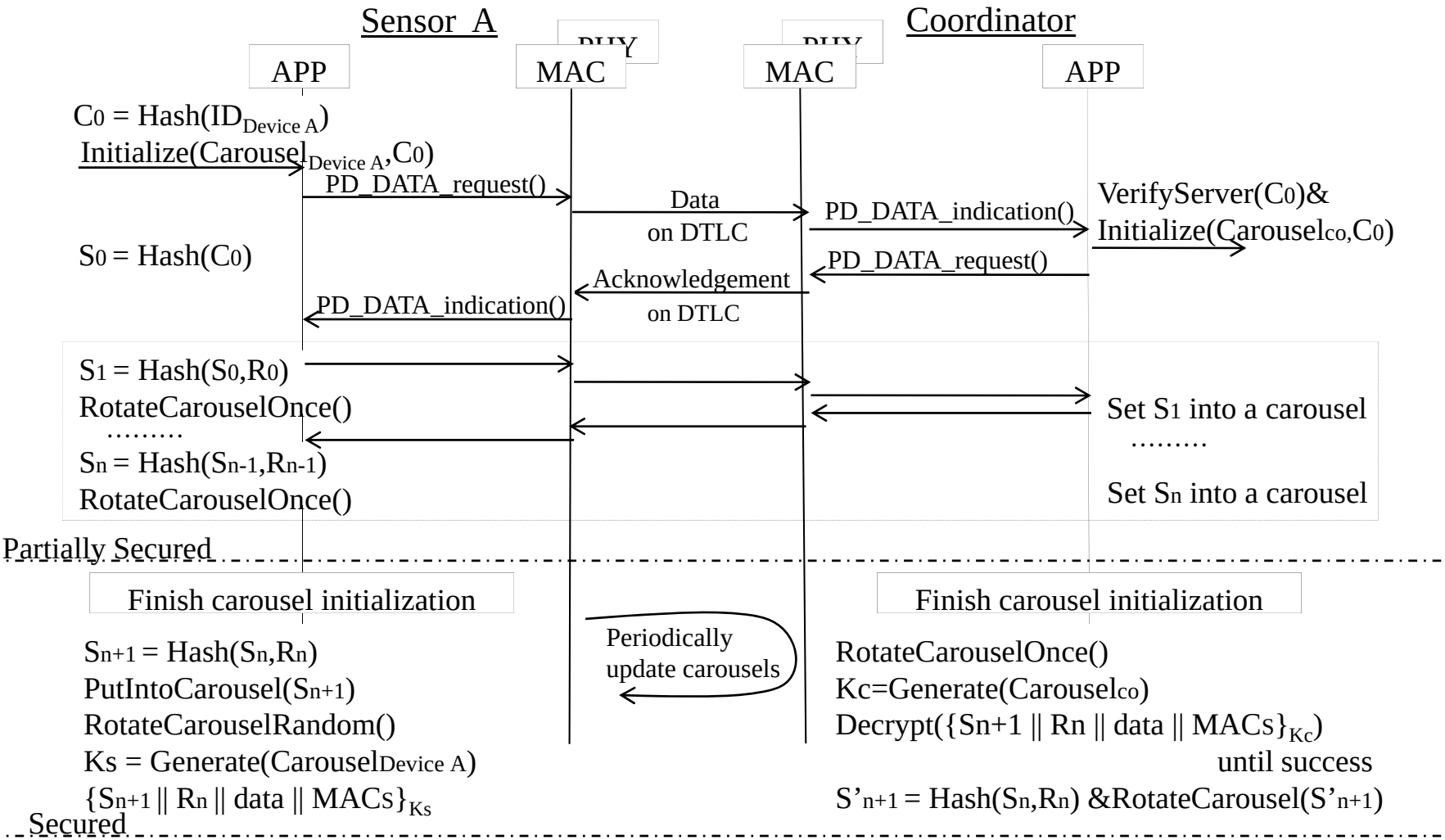
- Sensors consume much power during the receive-wait state and less wait state is expected
  - Intrinsic mutual authentication reduces extra communication/ computation for a sensor side

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

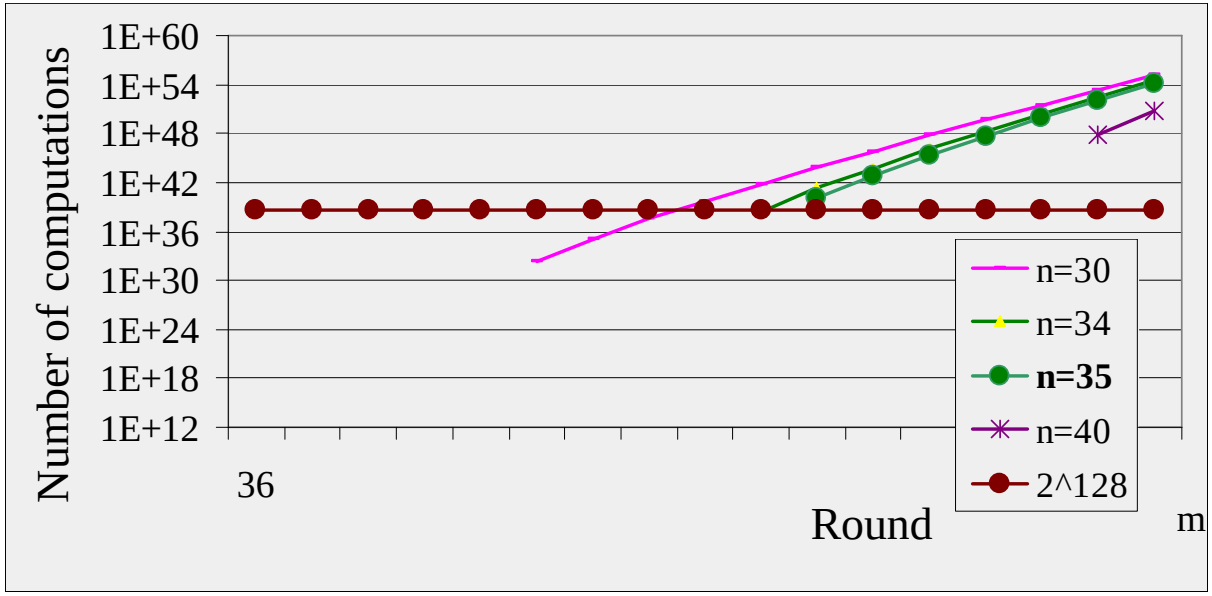


Key Initialization Protocol



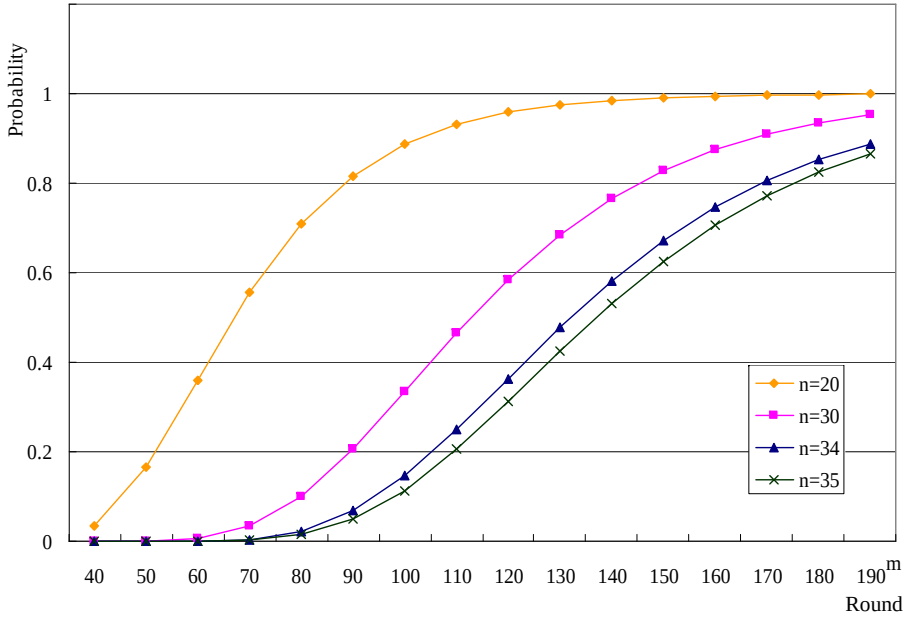
Carousel uncertainty

- The confidentiality level is 2^{128}
  - The key is sufficiently strong for current symmetric ciphers
  - A carousel containing at least 35 cells is sufficient to provide this confidentiality level



Probability of Carousel Duplication

- Probability that all cells of a carousel are filled with vital data after *m* rounds of data retrieval
  - An adversary needs to retrieve vital data along with the sensor/ coordinator more than 190 (>>*n*) rounds to have the same data in the carousel in the case *n* = 35
  - It is difficult for an adversary to duplicate a carousel both when *m* is small (*m* <35) and also when *m* is larger than *n* (*m*>*n*=35).



Evaluation

- Sensor-driven 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 2×10^{-4}
  - Verify almost the same error rate with MAC and PHY

Group Keying

- In a BAN, vital data be protected between a node and the coordinator
  - Group keying is complex and less computation peer-to-peer security is simple
  - Exposure of one vital data stream results in all data stream if group keying is wrongly used
  - FDLKH: Fully decentralized key management scheme on Logical Key Hierarchy
    - This extends the LKH (the Logical Key Hierarchy scheme) not to expect any central server but to use representative members of a group
    - On the FDLKH, the total variety of keys in a group is half of that of the LKH and the costs for a member join or leave keep the logarithmic order of the number of members

Crypto integration

- As a default, AES128-CBC is used
- In addition to it, Unified OTP Crypto with Authentication or others as long as Additional Cipher Suites Guideline for IEEE802.15.6 is satisfied (Need to define the requirement, the sample is from IEEE802.1 AE)

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.

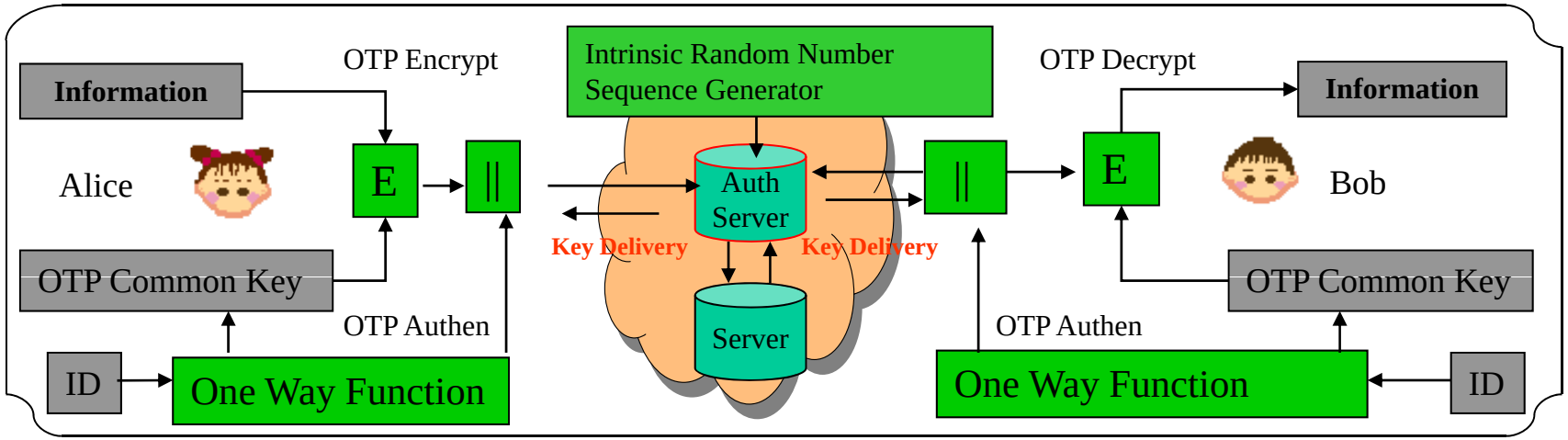
ii) If confidentiality is provided, the confidentiality mechanism has a publicly available proof of security in a model where the attacker has the ability to adaptively choose both plaintext and cipher text.

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.

Unified OTP* Crypto with Authentication

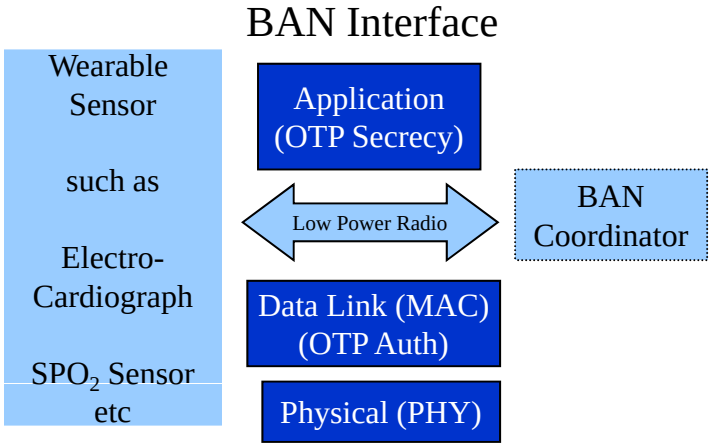
- The main algorithm of OTP is modulo arithmetic based on the intrinsic random sequence derived from the natural phenomenon and less computation in a sensor
- Unified OTP Cryptosystem for both Secrecy/Authentication in communication including the secret key delivery system from the initial to the subsequent 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

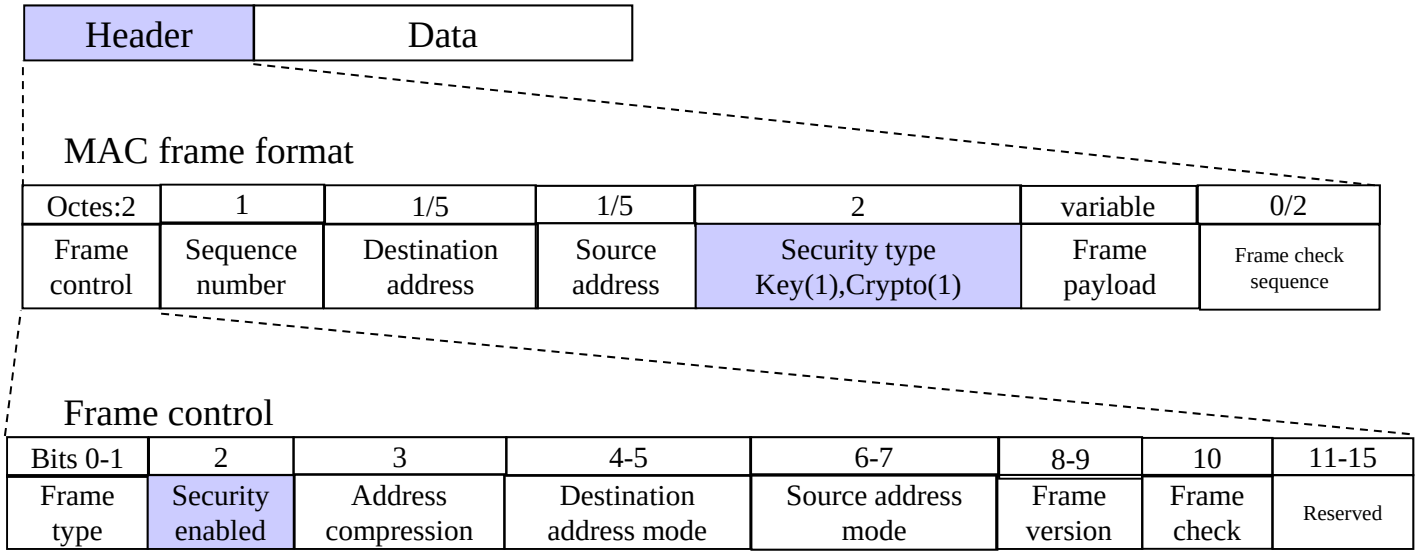
Implementation for OTP Authentication and Secrecy

- 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



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



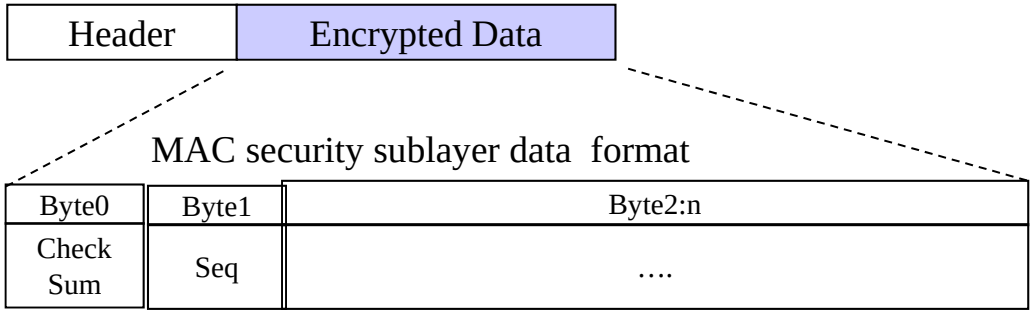
MAC Frame Proposal

- Security bit assignments in the frame control

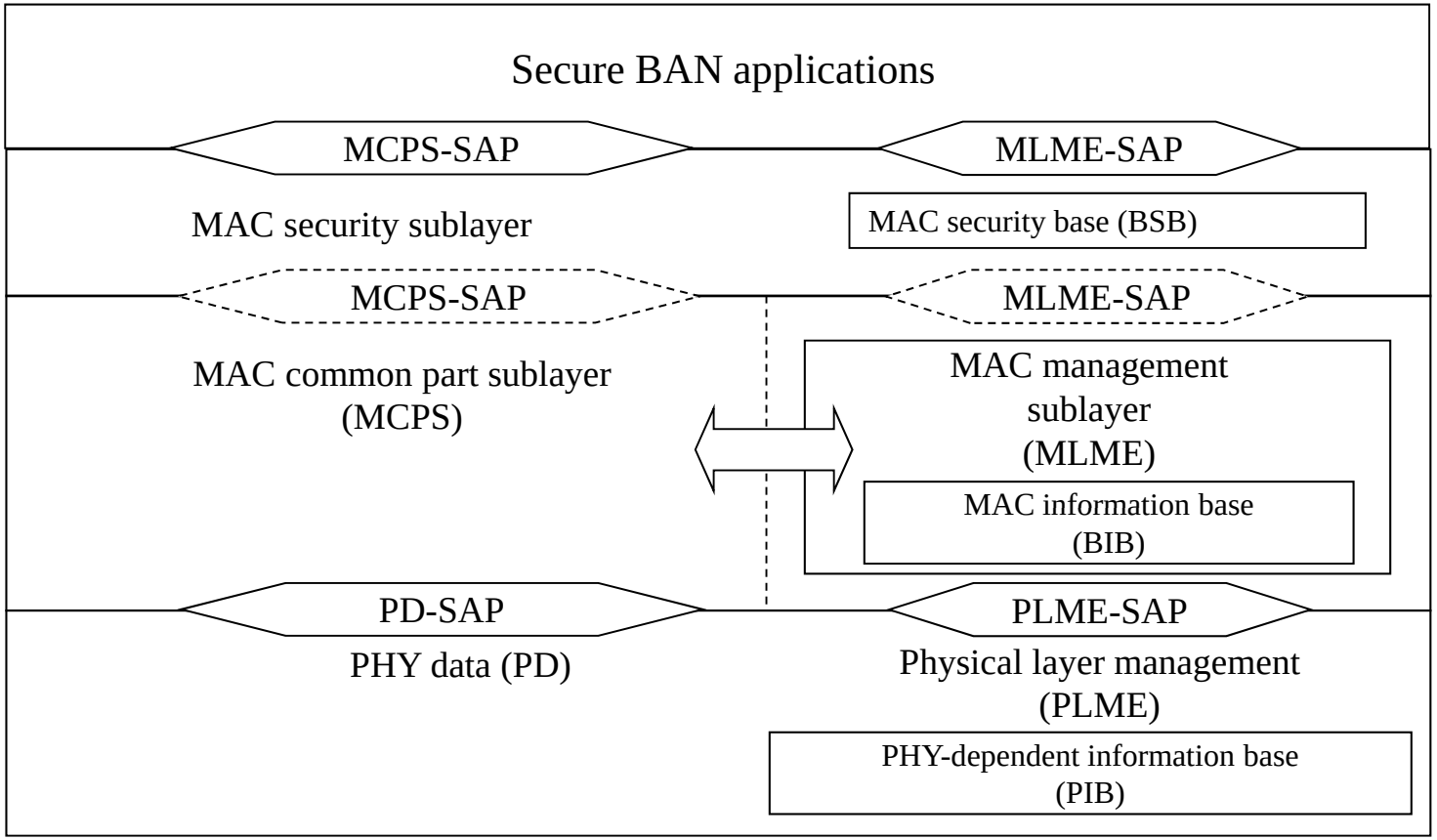
  Security enabled: 0x0, 0x1

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

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



Transparency of Security



Applications: Wearable Sensors and Secure BAN

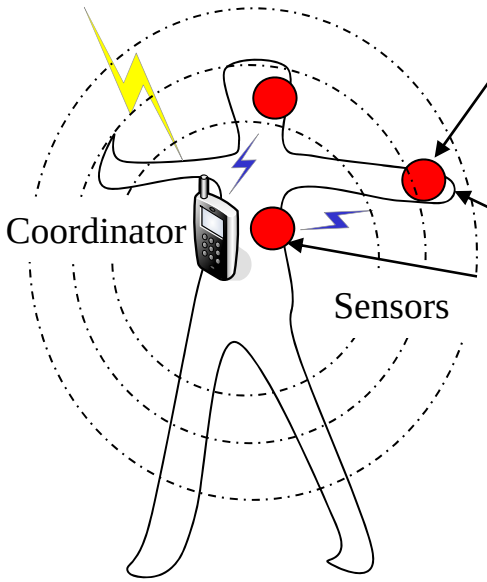
- Five wearable sensors for diseases
  - Electrocardiograph
  - Blood pressure
  - Breath
  - Percutaneous oxygen saturation (SpO2)
  - 3D-axes acceleration

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 Circulatory organs
Heart disease	○	○	△	△	△	Internal medicine Circulatory organs
Sleep apnea syndrome(SAS)	△	△	○	○	△	Respiratory Medicine Otolaryngology Circulatory organs 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



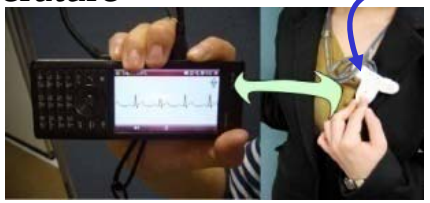
Wristwatch-type sphygmomanometer

Wristband-type stress meter

Ring(SpO2)

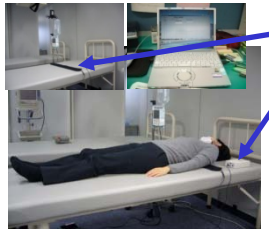
Wearable- or accessory-type (Electrocardiogram, Positioning, Temperature)

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



Wireless ECG with 3D-accel. and temp.

- •Breath



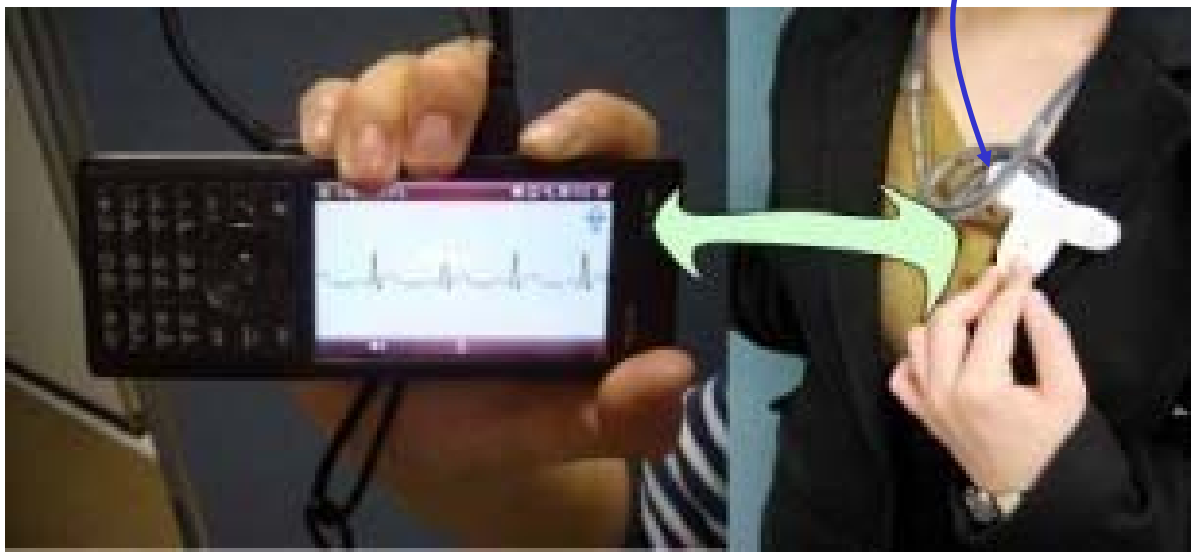
Breath sensor

Wireless controller

- •Blood pressure
- •Percutaneous oxygen saturation (SpO2)

Wireless SpO2 sensor

ECG Eample



Wireless ECG with 3D-accel. and temp.

Conclusion

- The data plane protocol defines the frame format for data encapsulation, encryption, and authenticity
- The security is configured depending on the use environment and two-types of key-distributions (sensor- and coordinator-driven) are supported
- MAC has the interface to register security suites in addition to default suites that satisfy security guidelines