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

Submission Title: **MedWiN MAC and Security Proposal – Part 2 of 2**
Date Submitted: May 4, 2009

Source: David Davenport [1], Neal Seidl [2], Jeremy Moss [3], Maulin Patel [4], Anuj Batra [5], Jin-Meng Ho [5], Srinath Hosur [5], June Chul Roh [5], Tim Schmidl [5], Okundu Omeni[6], Alan Wong [6]

(1) GE Global Research, davenport@research.ge.com, 518-387-5041, 1 Research Circle, Niskayuna, NY, USA

(2) GE Healthcare, neal.seidl@med.ge.com, 414-362-3413, 8200 West Tower Avenue, Milwaukee, WI, USA

(3) Philips, j.moss@philips.com, +44 1223 427530, 101 Cambridge Science Park, Milton Road, Cambridge UK

(4) Philips, maulin.patel@philips.com, 914-945-6156, 345 Scarborough Road, Briarcliff Manor, NY, USA

(5) Texas Instruments, {batra@ti.com, 214-480-4220}, {jinmengho@ti.com, 214-480-1994}, {hosur@ti.com, 214-480-4432}, {jroh@ti.com, 214-567-4145}, {schmidl@ti.com, 214-480-4460}, 12500 TI Blvd, Dallas, TX, USA

(6) Toumaz Technology, {okundu.omeni@tomuaz.com, +44 1235 438950}, {alan.wong@toumaz.com, +44 1235 438961}, Building 3, 115 Milton Park, Abingdon, Oxfordshire, UK

Re: Response to IEEE 802.15.6 call for proposals

Abstract: This presentation illustrates the major MAC aspects of a joint MAC and security proposal detailed in an accompanying normative text document doc. IEEE 802.15-09-0327-00-0006.

Purpose: To submit a joint proposal on MAC and security to the IEEE 802.15.6 task group

MedWiN MAC and Security Proposal

Part 2 of 2 – Security

GE Global Research:	David Davenport
GE Healthcare:	Neal Seidl
Philips:	Jeremy Moss, Maulin Patel
Texas Instruments:	Anuj Batra, Jin-Meng Ho Srinath Hosur, June Chul Roh Tim Schmidl
Toumaz Technology:	Okundu Omeni, Alan Wong

Outline

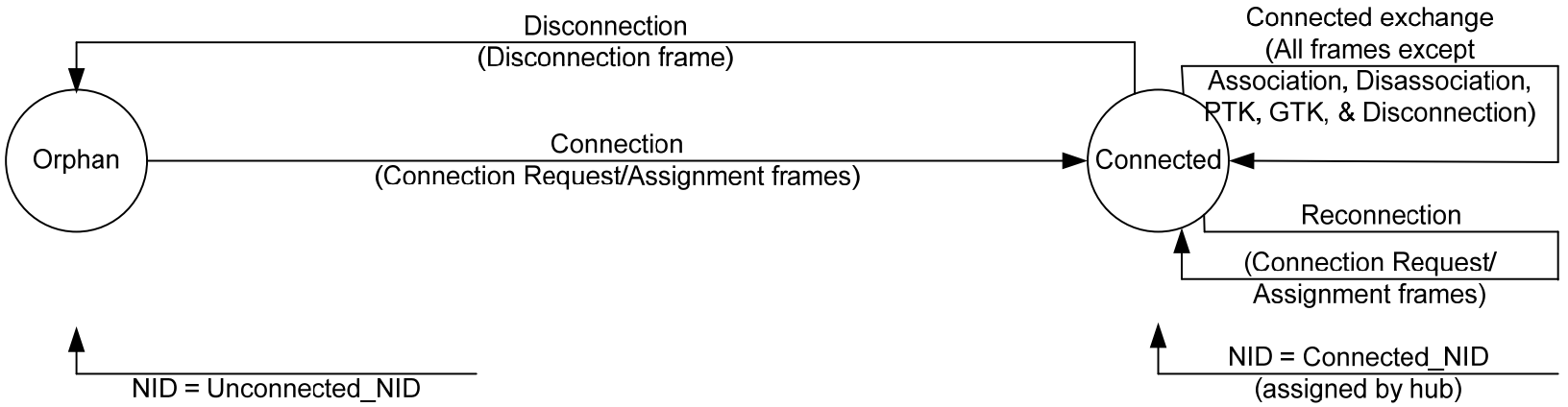
- Motivation
- Access state diagrams & Security hierarchy
- Security services
  - Security fields
  - AES-128 CCM input blocks
  - AES-128 CBC authentication
  - AES-128 CTR mode encryption/decryption
  - Replay filtering
- Security keys
  - Temporal key (TK) creation/distribution
    - Pairwise temporal key (PTK) creation for unicast protection
    - Group temporal key (GTK) distribution for multicast/broadcast protection
  - Master key (MK) generation protocols provided
    - ✓ MK preinstalled association
    - ✓ Unauthenticated association
    - ✓ Public key hidden association
    - ✓ Password authenticated association
    - ✓ Display authenticated association
- Implementation Estimates

Motivation

- Security needs to be built into the system from the start, not as an after thought
- Patient data usually requires protection from casual eavesdropper
  - Data confidentiality → Encryption
- Integrity of data also needs to be provided → Authentication
- Message source authentication
- Applications which do not require security don't turn it on

Access State Diagram 1 – No Security

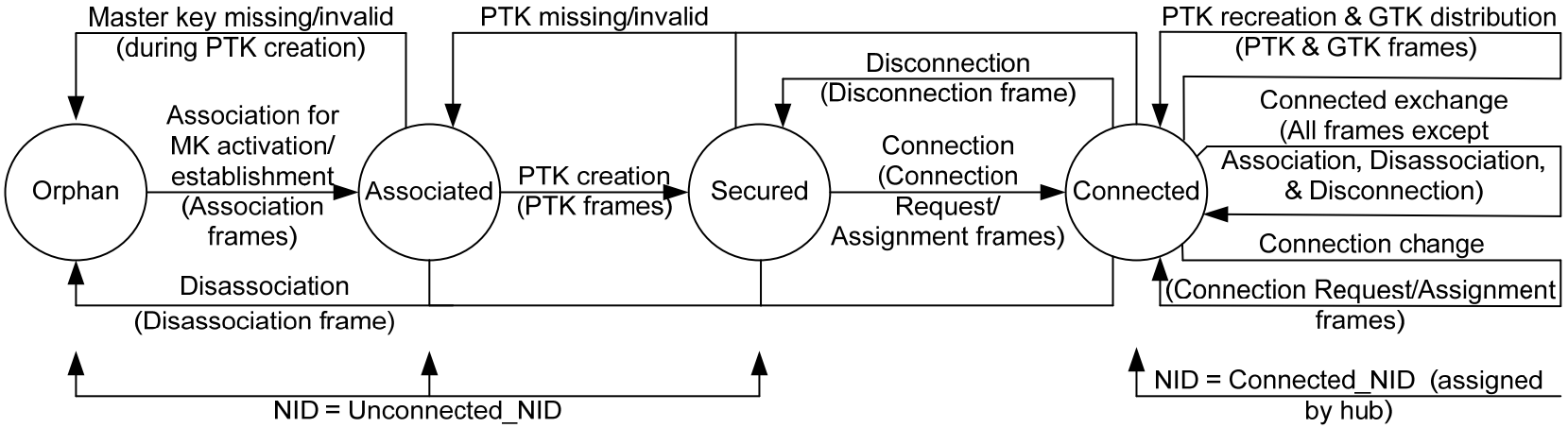
- Orphan state – node not connected to hub. Can only send connection request message
- Connected state – node connected to hub. Can send all unsecured messages



(a) Unsecured communication

Access State Diagram 2 – Security Enabled

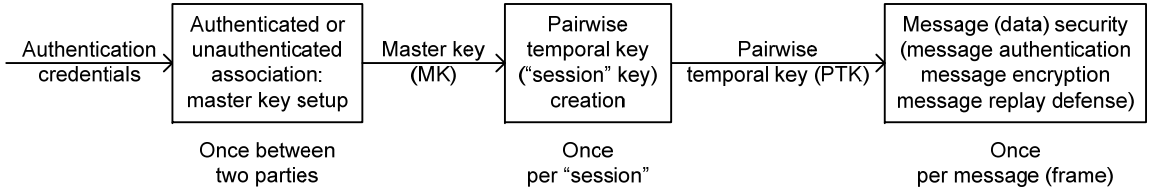
- Associated state – Master keys activated or generated
- Secured state – PTK created
- Connected state – connected to hub. Can send only secured messages



(b) Secured communication

Security Hierarchy

- A PTK (session key) is needed for data security
  - PTK (data) → security check sum → data authenticity & integrity
  - PTK (data) → encryption →data confidentiality & privacy
  - PTK (data) + security sequence # → security checksum → replay defense
- A master key (MK) is needed for PTK creation
  - The master key is not used as a session key for security reasons
  - Compromise of a PTK does not break the master key
- Association is needed for MK setup
  - How can two devices establish a secret MK—even with attackers around?
  - How can a device reject a MK setup with an unauthorized device?
  - How can a device allow a MK setup with a "rescuer" in an emergency?

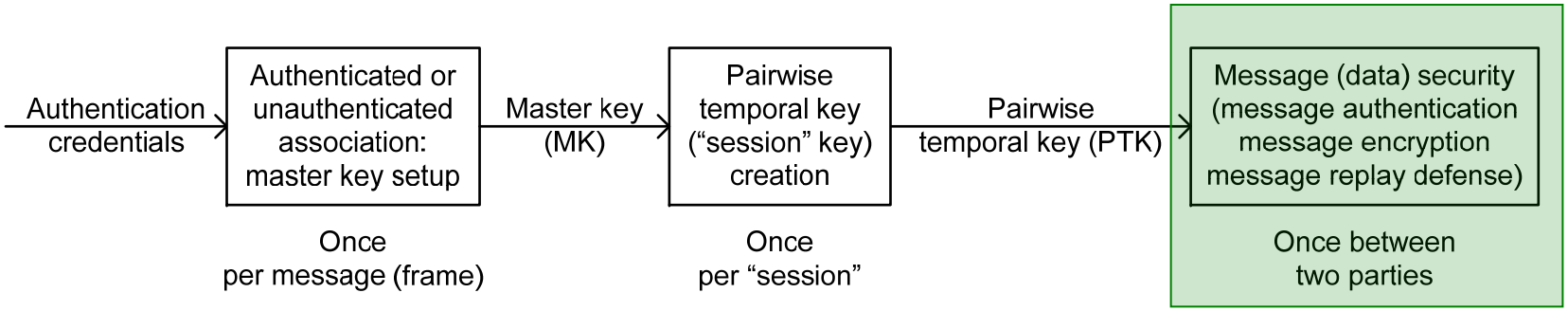


Connection Time

- Made up of the following components
  - Time to find Hub's channel
  - Time to get contention interval or poll from Hub
  - Time to exchange association & PTK creation frames (in secured connection)
    - Only required when joining for the 1st time
  - Time to exchange connection frames
- Also depends on the beacon period and frequency of channel hopping of the hub

Security Services

- Security indication
  - Security fields in MAC header and frame body
- Authentication, encryption, and decryption
  - Format of AES-128 CCM blocks
  - Authentication, encryption, and decryption operation
- Replay filtering
  - Security sequence number

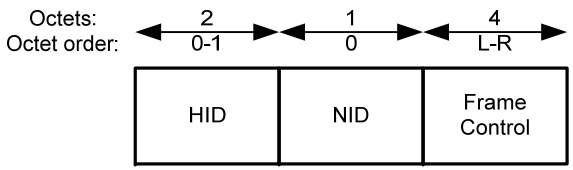


Security Fields in MAC Header

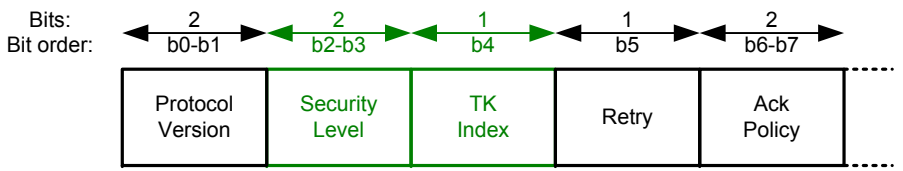
- Security Level
  - Indicates the security level of the current frame
- TK Index
  - Indicates the pairwise temporal key (PTK) or group temporal key (GTK) being used to secure the current frame
  - Provided for PTK or GTK change

Table 1 — Security Level field encoding

Field value b2 b3	Security level of current frame
00	Level 0 – frame not secured
10	Level 1 – frame authenticated but not encrypted
01	Level 2 – frame authenticated and encrypted
11	Reserved



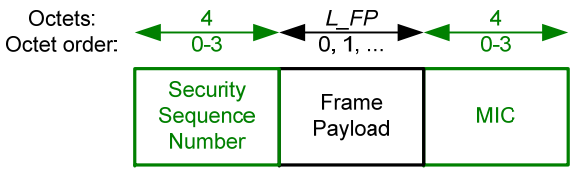
MAC Header format



Frame Control format

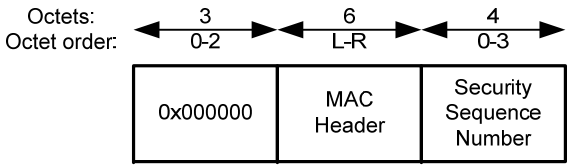
Security Fields in MAC Frame Body

- Security Sequence Number
  - Increments by every frame transmission or retransmission secured with the same PTK or GTK
  - Provided for nonce construction and replay detection
- MIC
  - Set to a keyed message authentication check computed based on AES-128 CCM
  - Provided for preserving the authenticity and integrity of the current frame

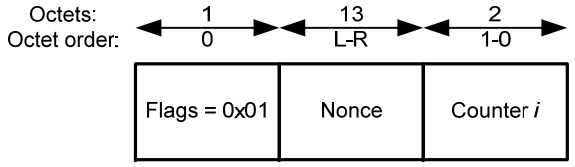


MAC Frame Body format

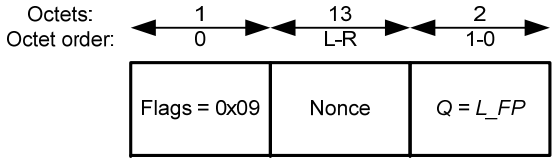
AES-128 CCM Input Blocks



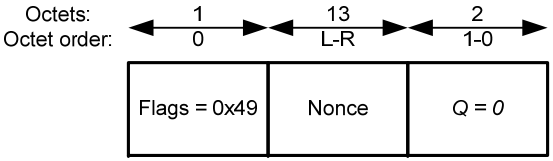
Nonce format



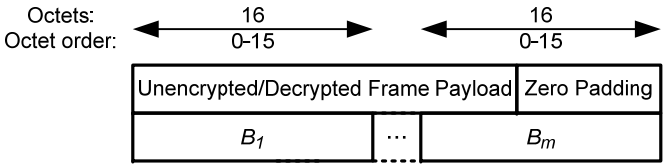
Ctr_i format



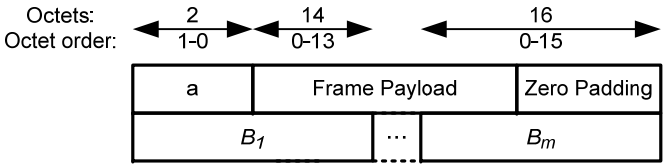
B_0 format (frame payload encrypted)



B_0 format (frame payload not encrypted



$B_1, \ldots, B_m$ format (frame payload encrypted)

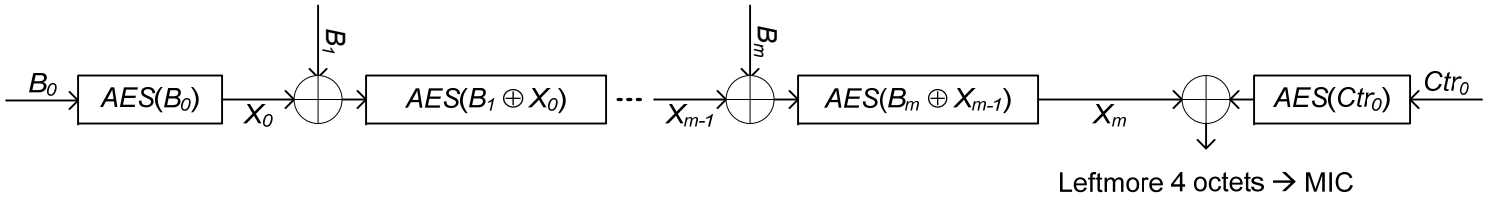


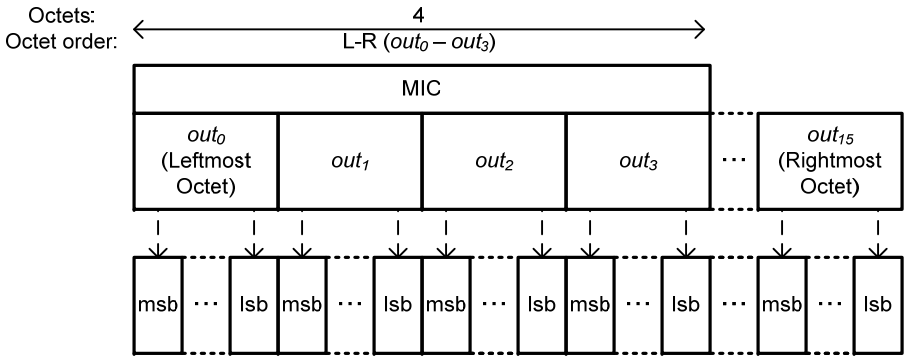
$B_1, \ldots, B_m$ format (frame payload not encrypted)

AES-128 CBC Authentication

$$X0 = AES(B0),\ Xi = AES(Bi \oplus Xi\text{-}1),\ i = 1, \ldots, m$$

$$MIC = LMB\_n(M),\quad M = AES(Ctr0) \oplus Xm$$





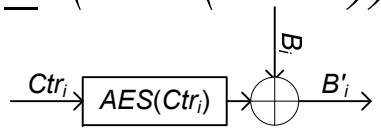
msb = most-significant bit lsb = least-significant bit

MIC calculation and transmit order

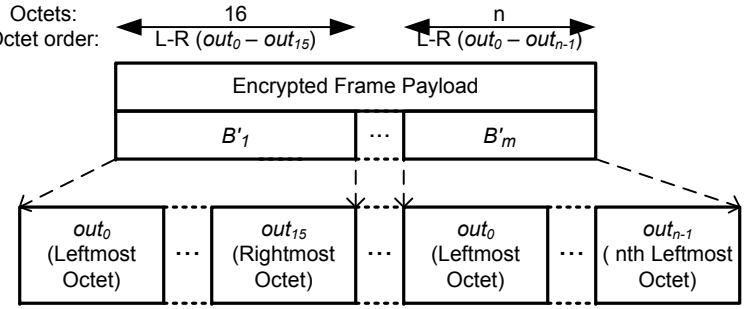
AES-128 CTR Mode Encryption/Decryption

$$B'i = Bi \oplus AES(Ctri),\ i = 1, \ldots, m\text{-}1$$

$$B'm = L\_n(Bm) \oplus L\_n(AES(Ctrm))$$



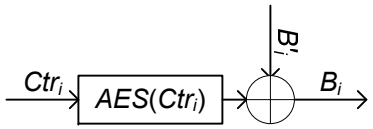
Cipher text generation



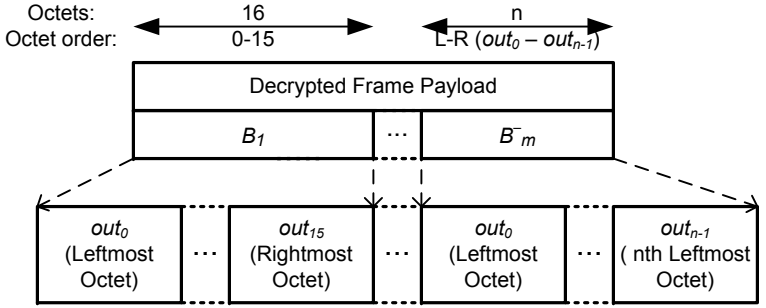
Encrypted Frame Payload format

$$Bi = B'i \oplus AES(Ctri),\ i = 1, \ldots, m\text{-}1$$

$$B^{-}m = B'm \oplus L\_n(AES(Ctrm))$$



Plain text recovery



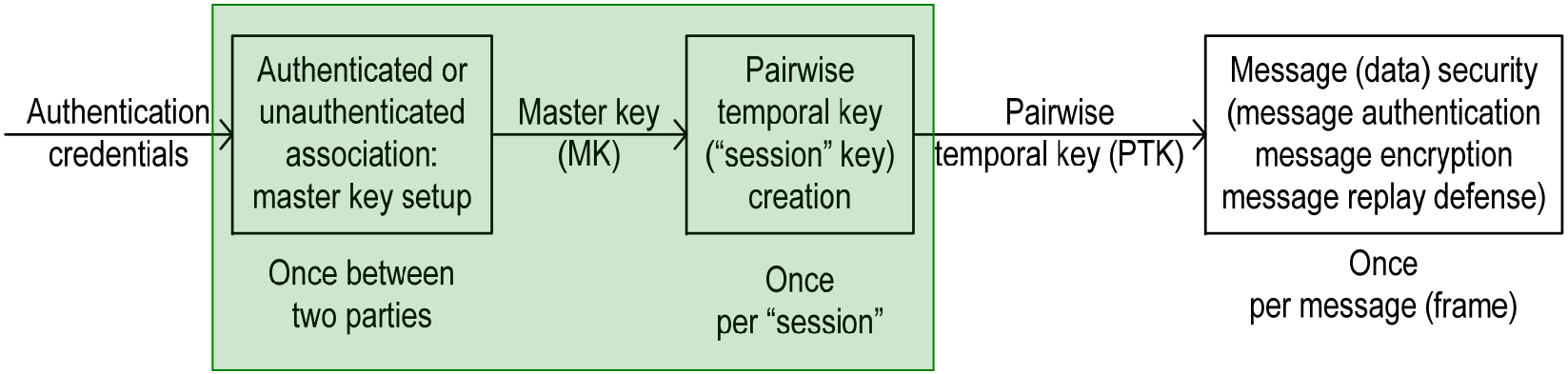
Decrypted Frame Payload format

Replay Filtering

- Security sequence number setting on transmission
  - Set to 1 in a frame secured with a new PTK or GTK
  - Incremented by one for each successive frame transmission or retransmission secured with the same PTK or GTK
- Replay filtering on reception
  - Accept a MIC-valid frame secured with a new PTK
  - Accept a MIC-valid frame with a security sequence number > the security sequence number contained in the last accepted frame secured with the same PTK
  - Discard a frame with a security sequence number ≤ the security sequence number contained in the last accepted frame secured with the same PTK

Security Keys

- PTK creation & GTK distribution
  - PTK creation based on a master key
  - GTK distribution based on a PTK
  - A "Session" as indicated below can be for as many as 2^{32} data frame transactions which would usually be the lifetime of a node
- MK setup
  - Done only once between a node and a hub
    - By running an association protocol
    - Five association protocols provided



PTK Creation

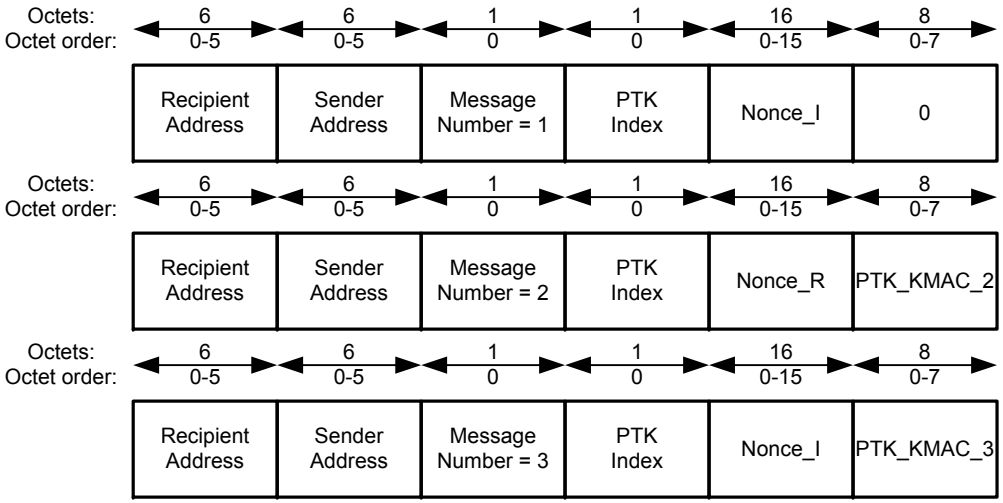
- MK → PTK
  - PTK compromised → MK NOT compromised → One-way hash
  - Freshness → both parties have a say in PTK creation → Nonces combined

PTK = CMAC(MK, Address_I || Address_R || Nonce_I || Nonce_R || PTK_Index)

KCK = CMAC(MK, Address_R || Address_I || Nonce_R || Nonce_I || PTK_Index)

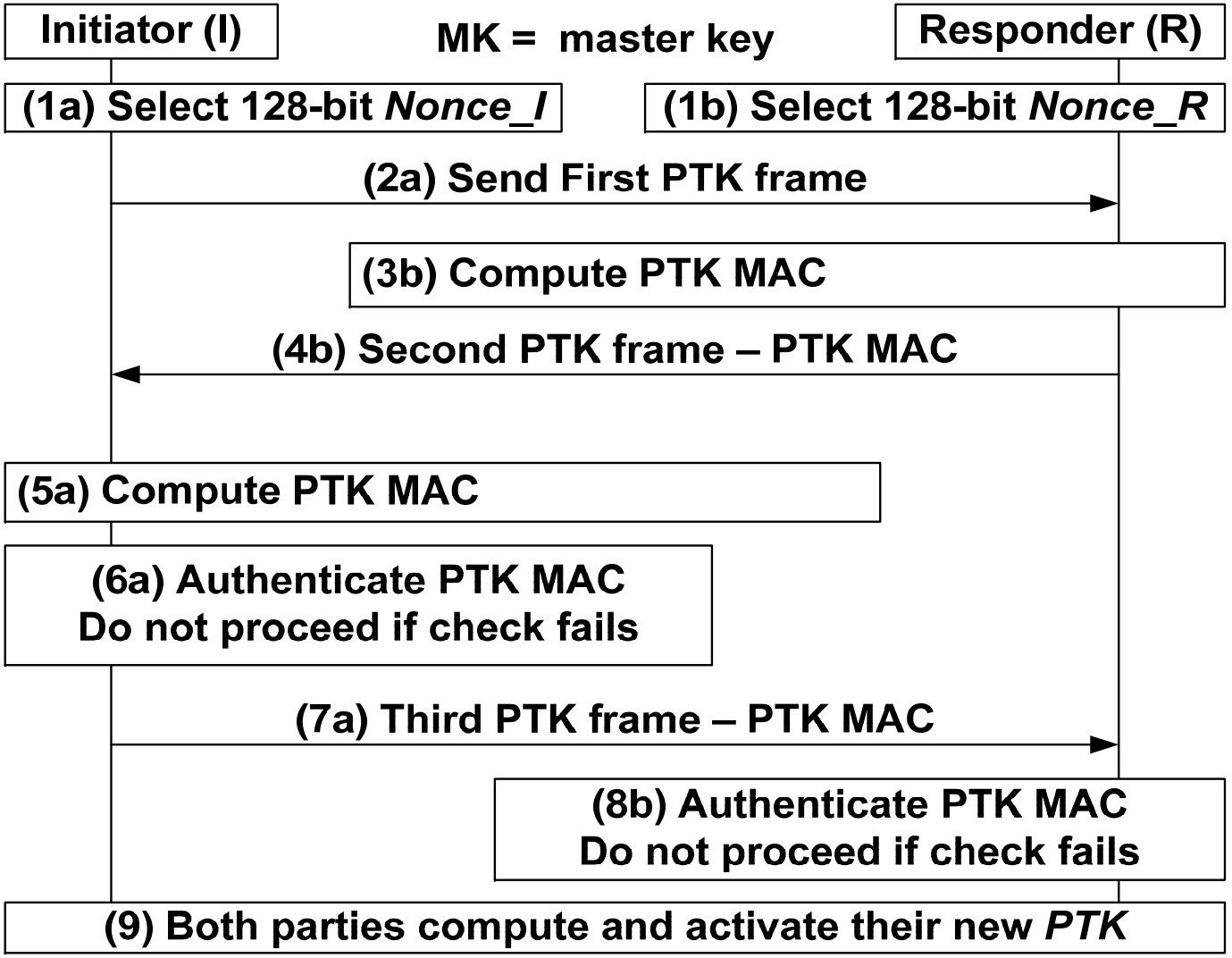
PTK_KMAC_2 = LMB_64(P), PTK_KMAC_3 = RMB_64(P)

P = CMAC(KCK, Address_I || Address_R || Nonce_R || Nonce_I || PTK_Index)



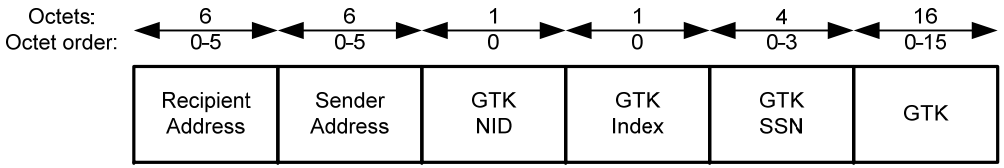
Frame Payload format for PTK frames

PTK Creation – Flowchart



GTK Distribution

- PTK → GTK
  - For securing broadcast & multicast
  - GTK contained in a frame encrypted & authenticated by the PTK



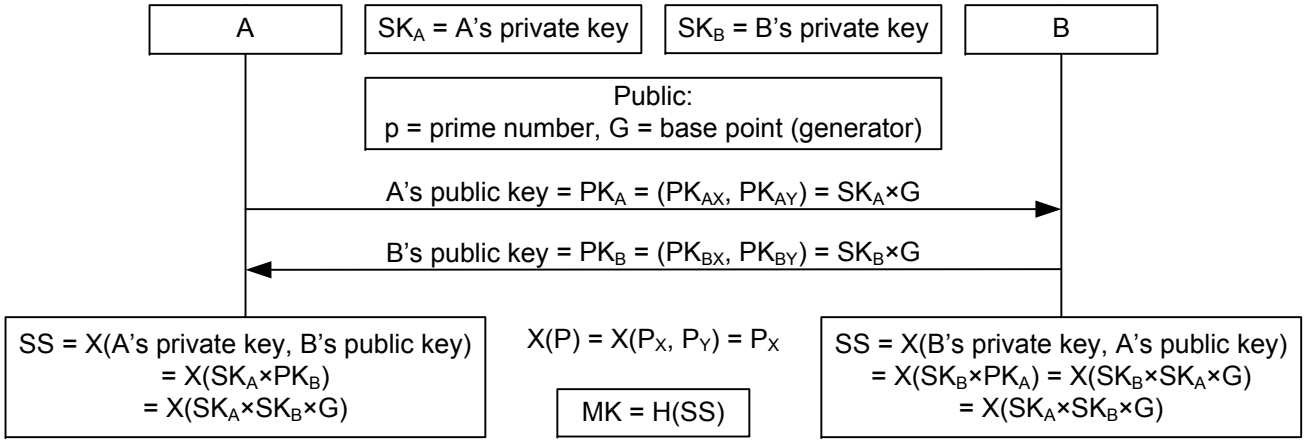
Frame Payload format for GTK frames

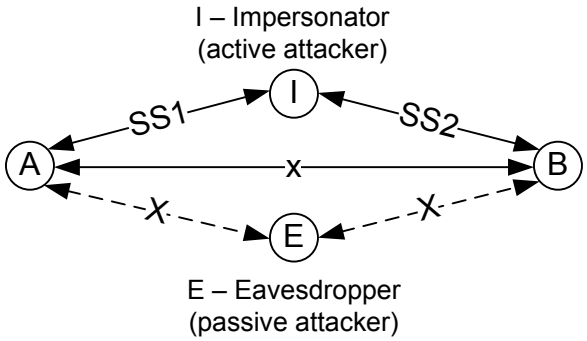
Diffie-Hellman Key Exchange

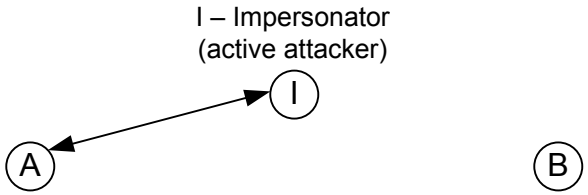
- 2 common methods:
  - Modular Exponentiation (traditional Diffie Hellman)
  - Elliptic Curve
- Both based on discrete logarithm – mathematically hard → resistant to eavesdropping
- Subject to impersonation & man-in-the-middle attacks → authentication needed
- Elliptic curve based implementation requires significantly fewer bits for same level of security, and so lower complexity implementation e.g. 192-bits versus 1536-bits for modular exponentiation

Diffie-Hellman Key Exchange (2)

$$y^2 = x^3 + ax + b \pmod{p},\ a,b \in GF(p),\ 4a^3 + 27b^2 \neq 0$$

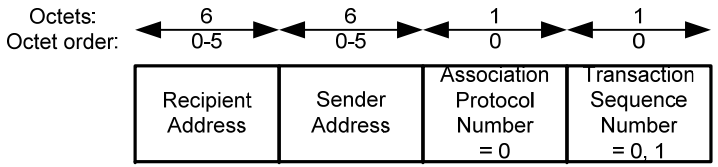




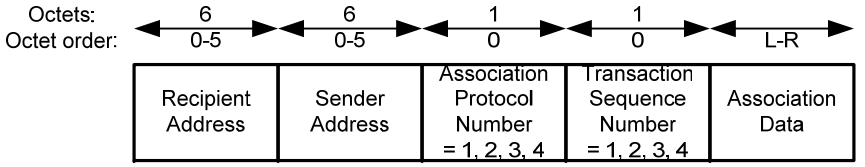


Association frames

- Exchanged to set out a pre-shared master key (MK) or set up a new MK
- Same general framework for different association protocols



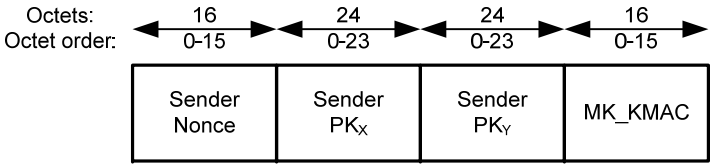
Frame Payload format for Association frames – master key pre-shared association protocol



Frame Payload format for Association frames – unauthenticated association, public key hidden association, password authenticated association, and display authenticated association

Table — Association Protocol Number field encoding

Field value decimal	Association protocol
0	Master key pre-shared association
1	Unauthenticated association
2	Public key hidden association
3	Password authenticated association
4	Display authenticated association
5-255	Reserved



Association Data format for association protocols 1-4

$DHKey = X(SK_A \times PK_B) = X(SK_B \times PK_A)$

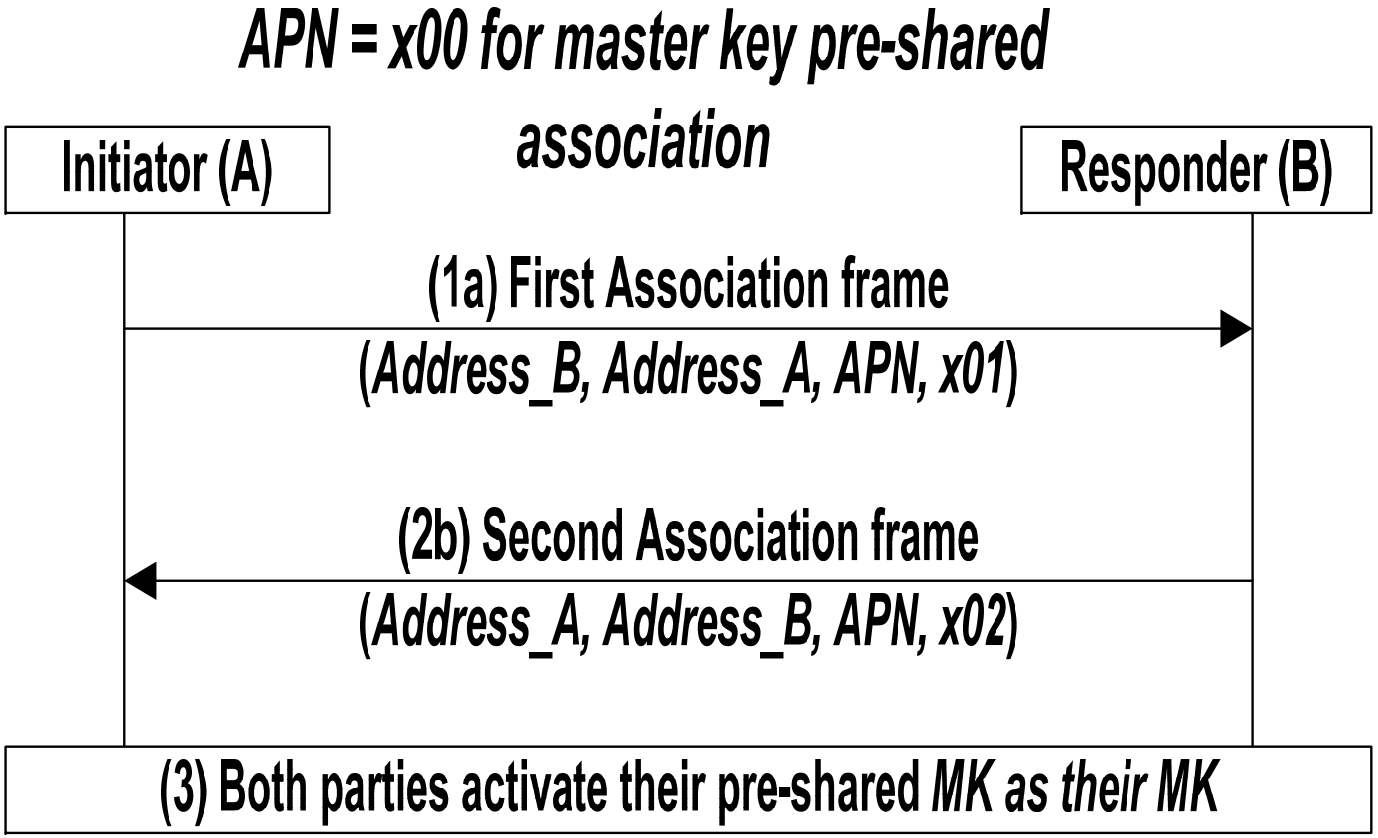
MK_KMAC_2 = CMAC(DHKey, Address_A || Address_B || Nonce_A || Nonce_B)
MK_KMAC_3 = CMAC(DHKey, Address_B || Address_A || Nonce_B || Nonce_A)

H = CMAC(DHKey, Address_A || Address_B || Nonce_A || Nonce_B)
D = RMB_16(H), D_A = BS2DI(D), D_B = BS2DI(D)
Commitment = CMAC(Nonce_A, Address_A || Address_B || PK_{AX} || PK_{AY})

MK = CMAC(DHKey, Nonce_A || Nonce_B)

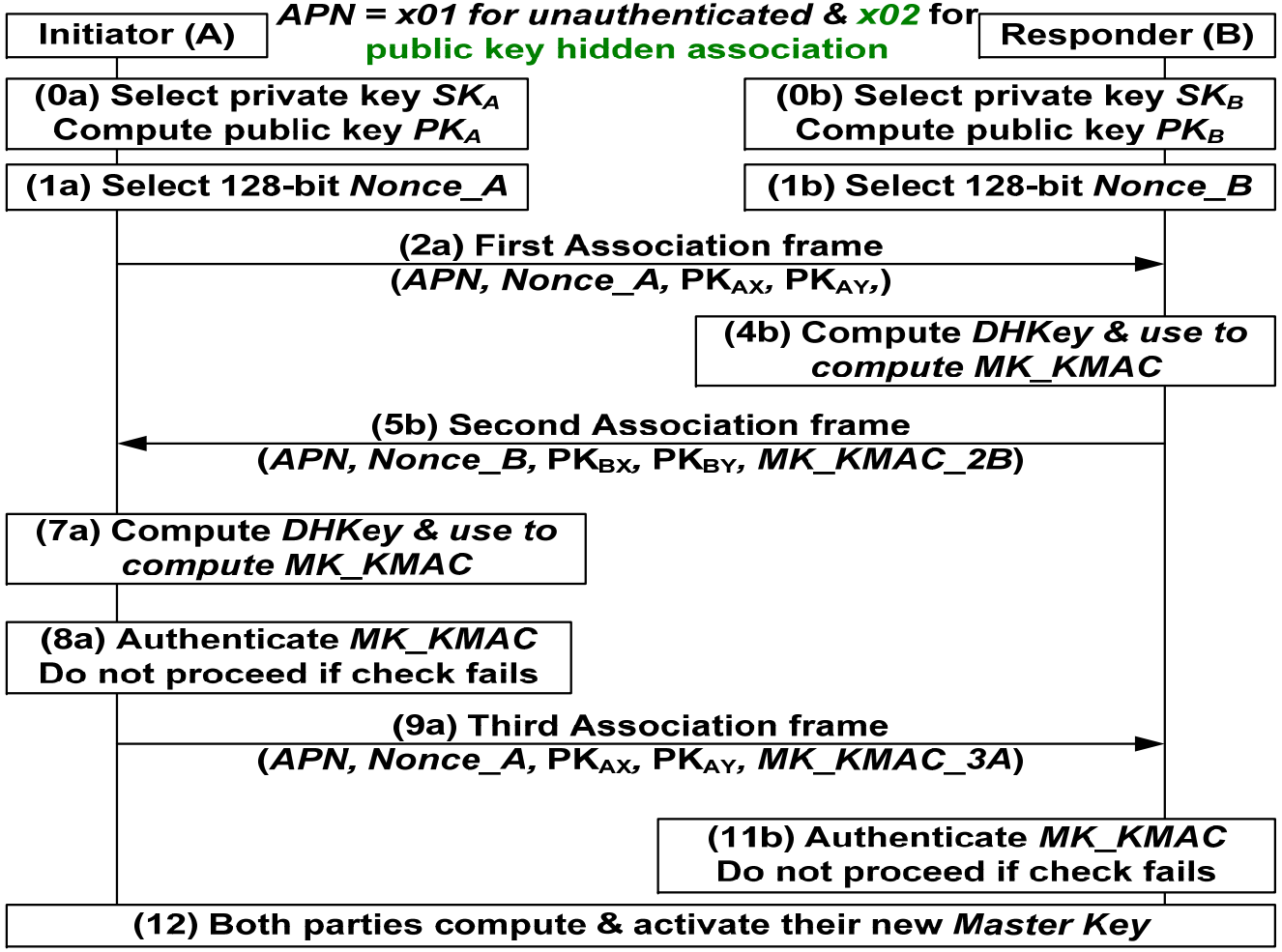
Master Key Pre-shared Association

- A simple two-way handshake to set out, i.e., activate, the pre-shared MK
- Loss of the MK list at the hub could expose all the data sent earlier or later
- Cannot "automatically" generate a new MK if the existing MK is compromised



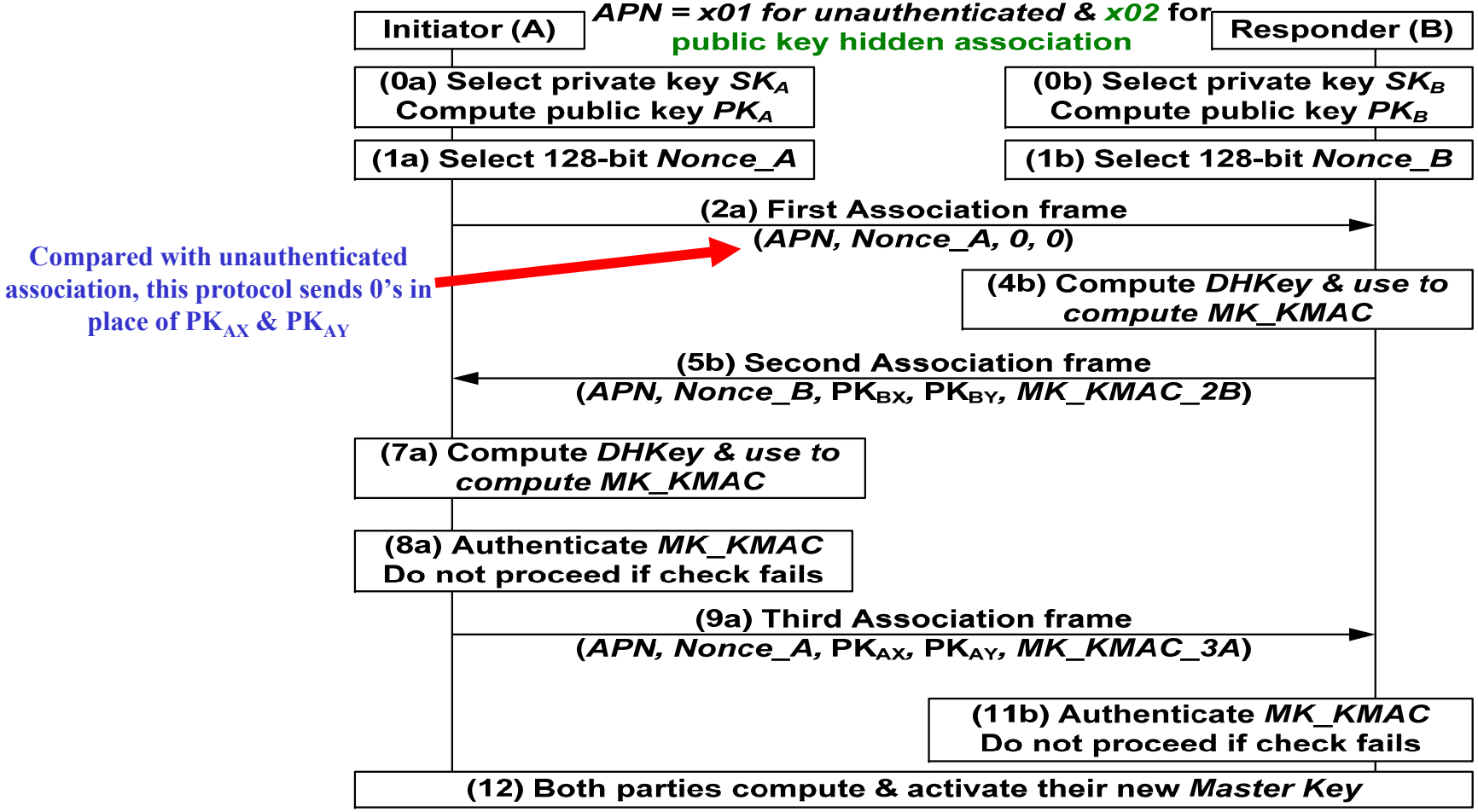
Unauthenticated Association

- May be used in a controlled environment with no active attacks expected
- Requires no authentication credentials or special user interfaces for verification



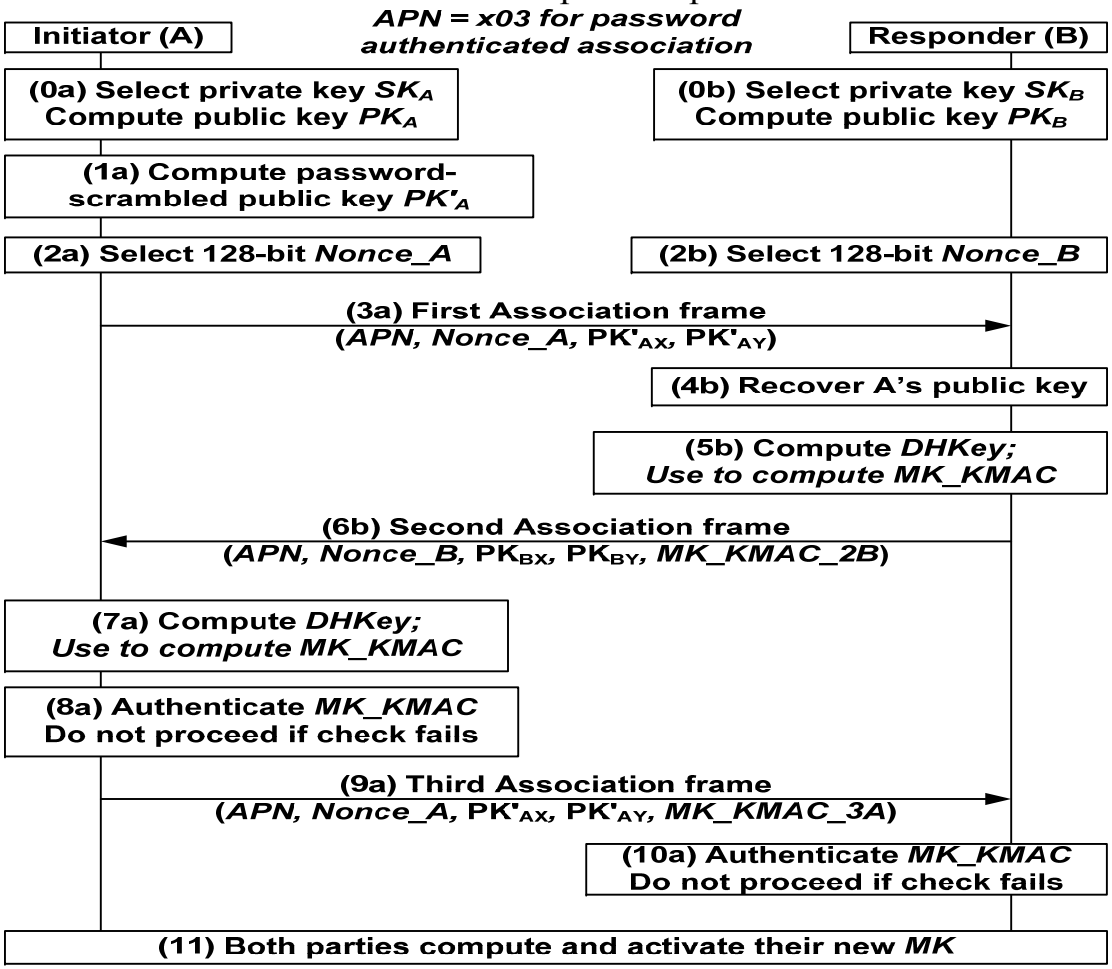
Public Key Hidden Association

- Node's public key transferred to hub in a secure out-of-band channel in advance
- Improbable over-the-air active (impersonation & MITM) attacks
- Lost of the public key list at the hub would NOT compromise previous data



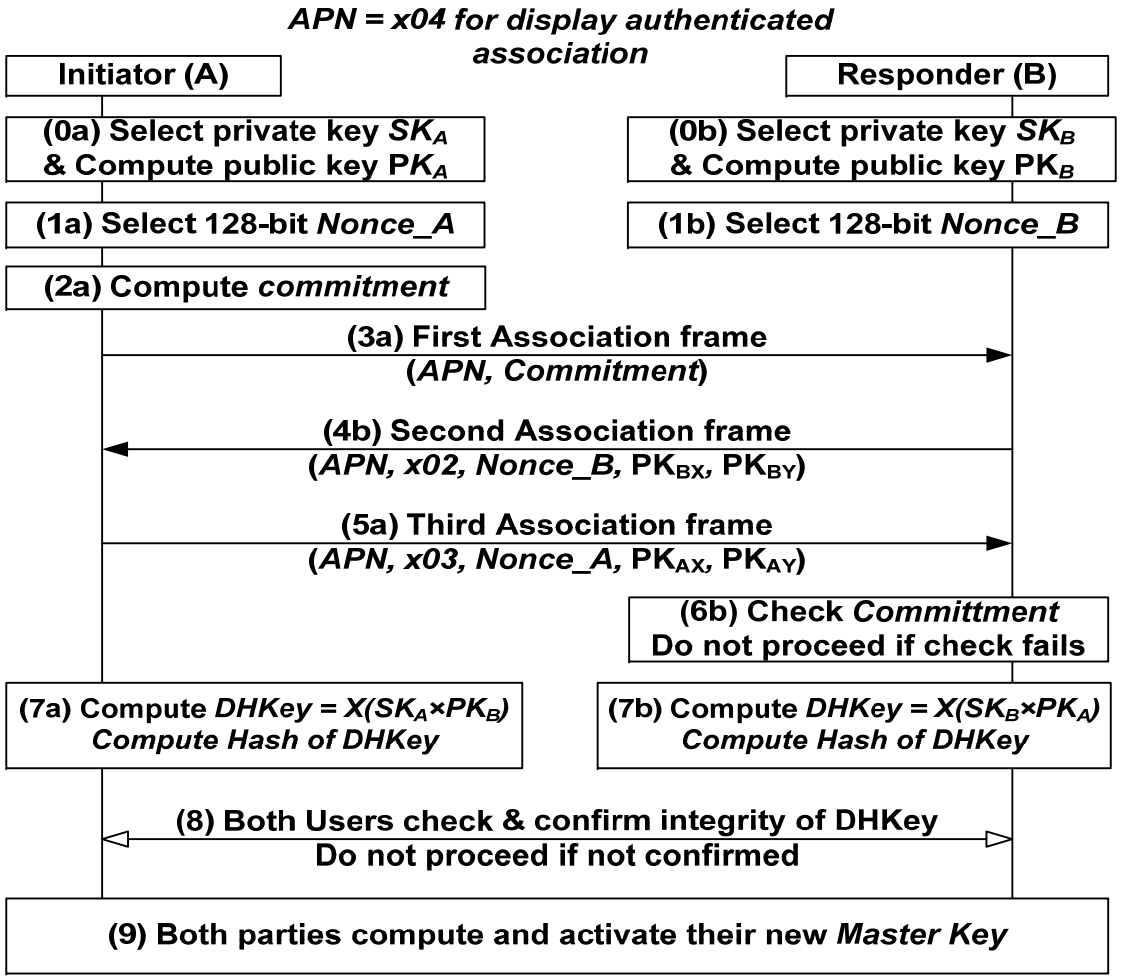
Password Authenticated Association

- Node & hub have a shared password in advance
- Improbable over-the-air active (impersonation & MITM) attacks possible
- Lost of the password list at the hub would NOT compromise previous data



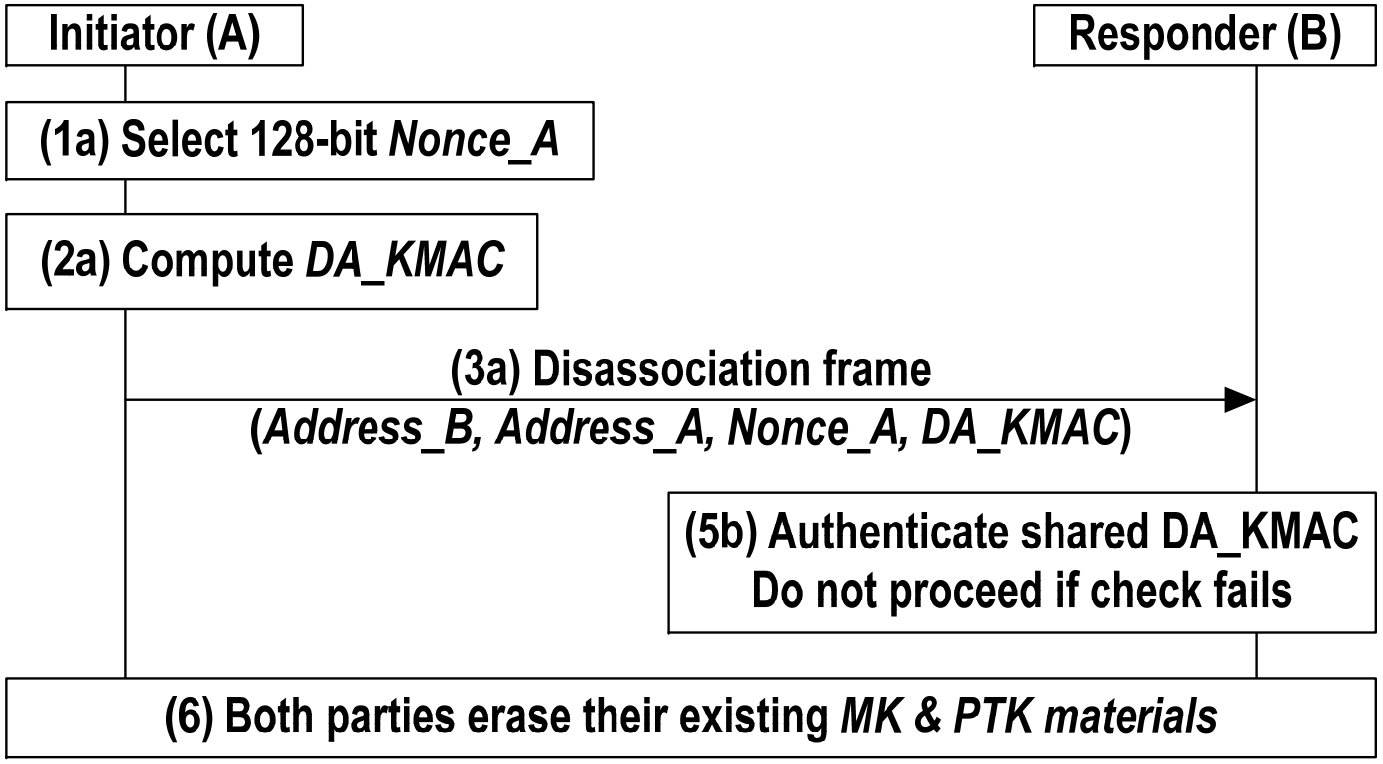
Display Authenticated Association

- Node & hub have a visible display of 5-digit decimal numbers
- Improbable over-the-air active (impersonation & MITM) attacks possible



Disassociation

- To void an existing association, i.e., to repeal a shared master key



Implementation Estimates

- AES-128 CCM requires around 10kgates for a hardware implementation
- Master Key pre-shared association protocol doesn't have additional implementation requirements
- Other association protocols require the ECDH key exchange algorithm
  - Software implementation takes around 20 KB of memory (program and data) on a 16-bit processor running at 8MHz. Run time is a few seconds [1]
  - Hardware implementation requires between 100-200k gates. At the same 8 MHz clock, it would take around under 100 ms [2,3]
    - This time can be halved if the public key computation is done in advance.
  - The references were designed with a goal of high throughput, so for this implementation, we expect we can optimize for area and get this down to between 10-20k gates. At 8 MHz a key exchange would then take around 1 second (or 500 ms if public key computation is done in advance)
- Total implementation area for the entire security functionality should be between 20-30kgates
  - 10kgates if keys are pre-shared

MedWiN Security Proposal Summary

- Access state diagrams & security hierarchy – defined and described
- Security services – (specified in normative text)
  - Relevant mechanisms defined and illustrated
- Security keys – (specified in an annex)
  - Temporal key (TK) creation/distribution
  - Master key (MK) generation
    - Provided protocols illustrated & described
- Implementation Estimates outlined

Details including references are provided in the accompanying normative text doc. IEEE 802.15-09-0327-00-00006.

Comparison Criteria

Criteria	Proposed Capability
1. Regulatory	Compliant with TG6 regulatory document in multiple frequency bands
2. Raw PHY data rate	100 kbps to 1 Mbps supported between node and hub
3. Transmission distance	PER and link budget shown to support 10% PER for 255 octet PSDU at 3 meters within all operating frequency bands proposed.
4. Packet error rate	
5. Link budget	
6. Power emission level	-10 dBm / -16 dBm maximum EIRP
7. Interference and coexistence	MAC: Channel hopping, Beacon shifting, Acknowledgements, Poll/Post for additional retransmission if necessary. PHY: Channelization ≥ 10 channels, same channel bandwidth for all modulations at each frequency band, low sidelobes of selected modulation
8. Security	**MAC provides 3 levels of security (none, authentication, authentication + encryption) based on AES-128. Association protocols provided for master key setup.**
9. Reliability	Acknowledged traffic, guard time and node synchronization to beacon provided. Unique identifications used to distinguish between collocated BANs. Link margin sufficient given TG6 channel models variations.
10. Quality of Service	MAC: Time to join a network ~ 63 msec for message exchange. Fast (<1 sec) channel access available via prioritized CSMA/CA random access as well as scheduled or improvised access mechanisms.
11. Scalability	PHY: Scalable data rate from common symbol rates. MAC: Multiple nodes supported via m-periodic scheduled, improvised and random access methods. Prioritized QoS and beacon configuration.
12. MAC transparency	MAC transparent across multiple frequency bands proposed
13. Power Efficiency	MAC: Sleep and Hibernate modes. PHY: ≤ 3.1 mW (active), 50 μW (standby), 250/125 nW (deep sleep)
14. Topology	Star topology, broadcast beacon supported. Maximum number of nodes supported via multiple access mechanisms.
15. Bonus Point	**Merged proposal focused on satisfying needs of medical BAN applications as defined by TG6 PAR.**

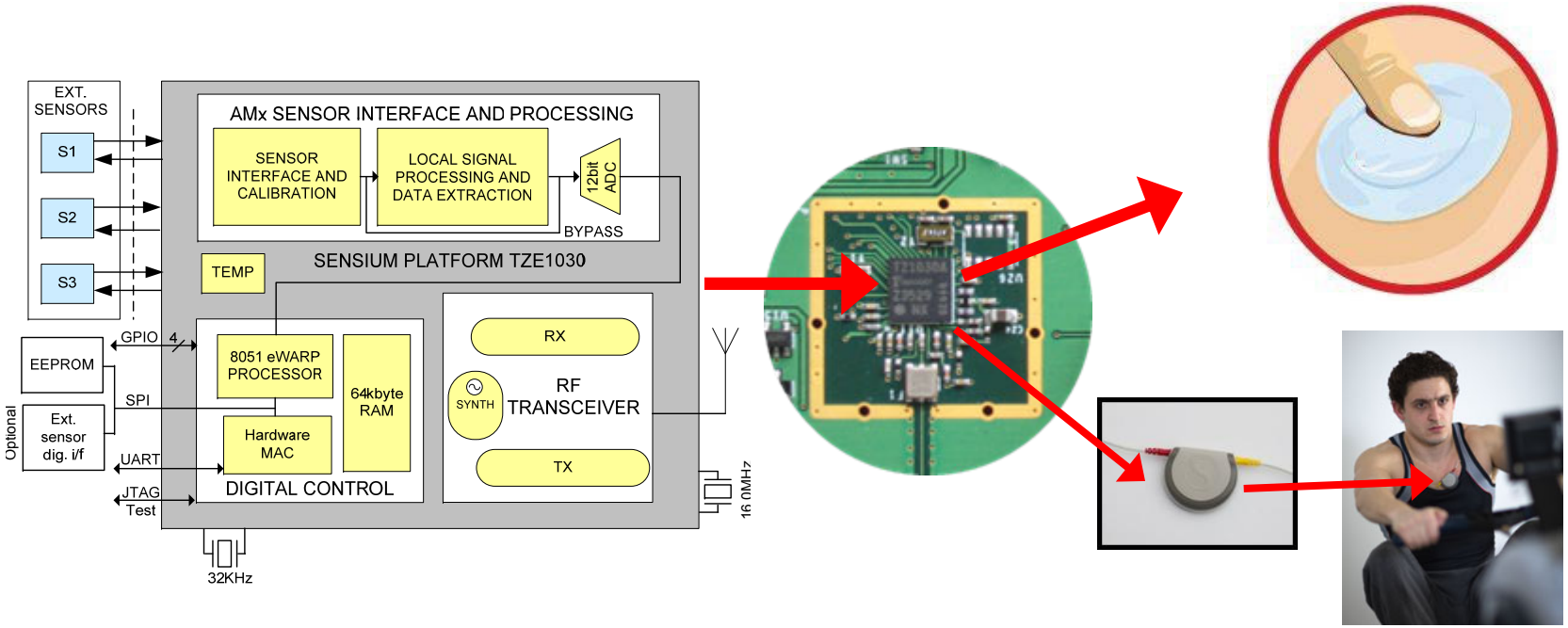
Additional References

[1] http://discovery.csc.ncsu.edu/pubs/ipsn08-TinyECC-IEEE.pdf

[2] S. B. Ors, L. Batina, B. Preneel, J. Vandewalle, "Hardware Implementation of an Elliptic Curve Processor over *GF*(*p*)", Proceedings. IEEE International Conference on Application-Specific Systems, Architectures, and Processors, 2003

[3] "Certicom® Suite B Public Key IP Core™", http://www.certicom.com/images/pdfs/ds-suiteb-pk-ipcore.pdf

MedWiN Know-How (1)



130nm CMOS Production SoC for Biotelemetry WBAN: µP, hardware MAC & wireless transceiver*

- Supply voltage 1-1.5V - Maximum SoC current < 3mA - WBAN Range > 3m
- Full custom hardware MAC: Star topology, TDMA, FDMA (only 35µW for full link/network management)
- Sensor Interface: ADC, Sensor interface circuitry, Sensor signal BW 100 Hz

**A. Wong, D. McDonagh, G. Kathiresan, O. Omeni, O. El-Jamaly, T. Chan, P. Paddan, A. Burdett, "A 1V, Micropower System-on-Chip for Vital-Sign Monitoring in Wireless Body Sensor Networks," Proc. ISSCC, Feb. 2008.*

MedWiN Know-How (2)

GE Healthcare Monitoring Solutions is an experienced industry leader in the development of seamless, wired and wireless connectivity and information distribution products and systems.

ApexPro CH Ambulatory telemetry system operating in the WMTS.

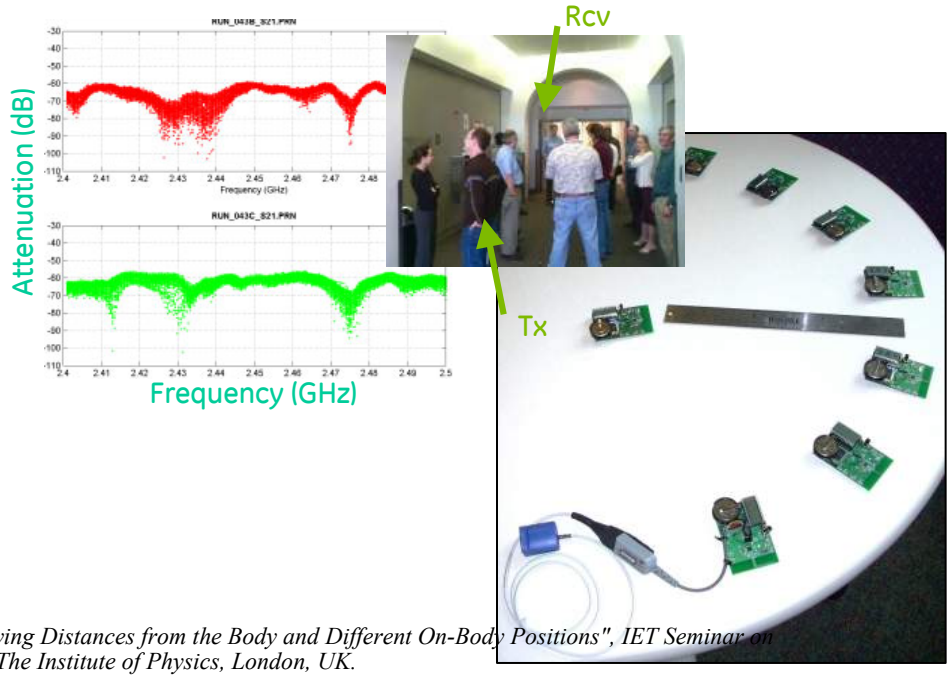
ApexPro FH Frequency-hopping ambulatory telemetry system operating in the WMTS.

DASH patient monitor Delivers basic vital signs to ICU monitoring units with built-in wireless LAN.

Web and Mobile Viewer Provides clinician access to patient data via wireless LAN or cell phone.

Enterprise Access Multi-use wireless infrastructure (600 MHz – 6 GHz) extends clinical, voice and business application access throughout the enterprise.

GE Global Research propagation measurements, hardware and protocol prototypes leveraging time / frequency diversity for Medical Body Area Networks

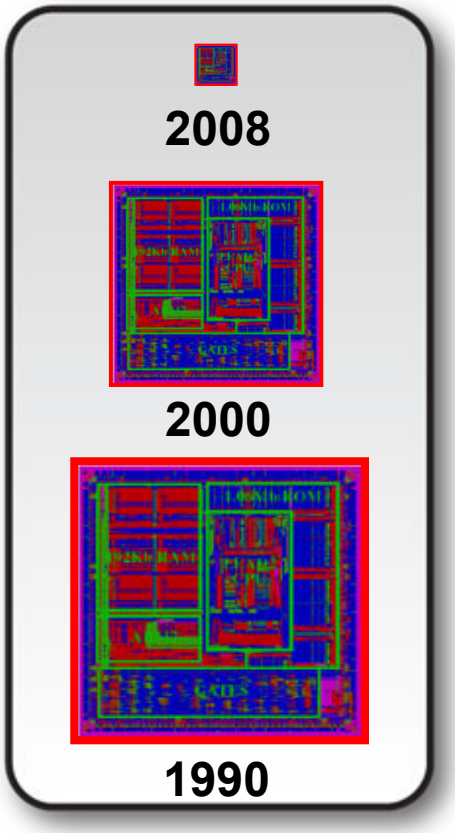


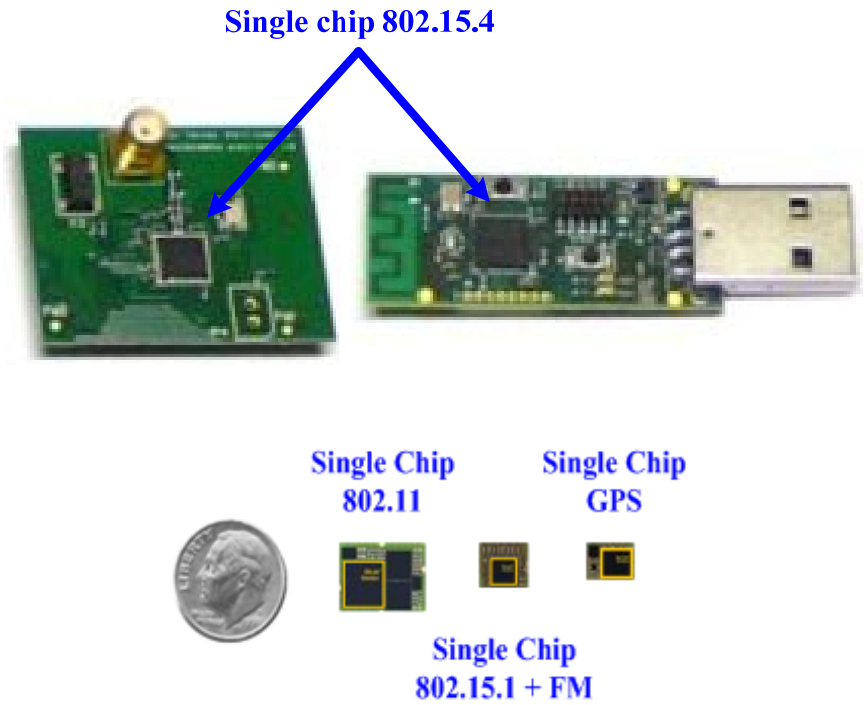
A. Alomainy, Y. Hao, D. Davenport, "Parametric Study of Wearable Antennas with Varying Distances from the Body and Different On-Body Positions", IET Seminar on Antennas and Propagation for Body-Centric Wireless Communications, 24 April 2007, The Institute of Physics, London, UK.

D. Davenport, B.. Deb, F. Ross, "Wireless Propagation and Coexistence of Medical Body Sensor Networks for Ambulatory Patient Monitoring," accepted for publication, Proc. Body Sensor Networks 2009, June 2009.

GE Healthcare Petition for Rule Making to Create Medical Body Area Network Service, FCC ET Docket 08-59, http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-08-953A1.pdf.

MedWiN Know-How (3)





Ultra Low power single chip wireless systems for supporting body sensor systems

"System Architecture Of A Wireless Body Area Sensor Network For Ubiquitous Health Monitoring", Journal of Mobile Multimedia, Vol. 1, No.4 (2006) 307-326

MedWiN Know-How (4)

Philips Patient Monitoring is an industry leader providing seamless wireless connectivity

IntelliVue Smart-Hopping (SH) Telemetry in WMTS and ISM, a cognitive radio technology.

IntelliVue Patient Monitor family delivers optimized monitoring based on patient acuity over WLAN and SH technologies.

IntelliVue WTAAP, enhanced vital and telemetry monitoring with Short Range 802.15.4 radio technology, a wireless link between telemetry and bedside monitors.

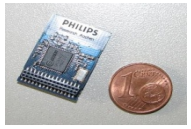
Philips Mobile Patient Access, Provide enhanced web services and near real-time patient data.

Philips Healthcare support filings for Rule Making to Create Medical Body Area Network Service, FCC ET Docket 08-59

Philips Research has an outstanding reputation in the field of body sensor networks for many years:

Co-organizer *BSN platform* *Open innovation*

Body Sensor Networks BSN 2007



AQUIS GRAIN

MyHeart

BASUMA

Book, journal, conference contributions

T. Falck, J. Espina, O. Garcia et al., "Towards easy-to-use, safe, and secure wireless medical body sensor networks", In: P. Olla and J. Tan (Eds.): "Mobile health solutions for biomedical applications", IGI Global, 2009

T. Falck, J. J. Garcia: "Quality of service for IEEE 802.15.4-based wireless body sensor networks", In: Proc. WiPH 2009

J. Espina, J. Mühlsteff, T. Falck et al., "Wearable body sensor network towards continuous cuff-less blood pressure monitoring", In: Proc. BSN 2008

D. Cavalcanti, R. Schmitt, A. Soomro, "Performance analysis of 802.15.4 and 802.11e for body sensor network applications", In: Proc. BSN 2007

J. Espina, T. Falck, O. Mülhens:, "Network topologies, communication protocols, and standards", In: G.-Z. Yang (Ed.): "Body sensor networks", Springer, 2006

T. Falck et al.: "On-body sensors for personal healthcare", In: G. Spekowius, T. Wendler (Eds.): "Advances in healthcare technology", Springer, 2006

T. Falck, J. Espina et al., "BASUMA – A body sensor system for telemedicine", In: Proc. EWSN 2006