CWC Oulu CENTRE FOR WIRELESS COMMUNICATIONS
University of Oulu

Secure Remote Monitoring of Personal Medical Appliances

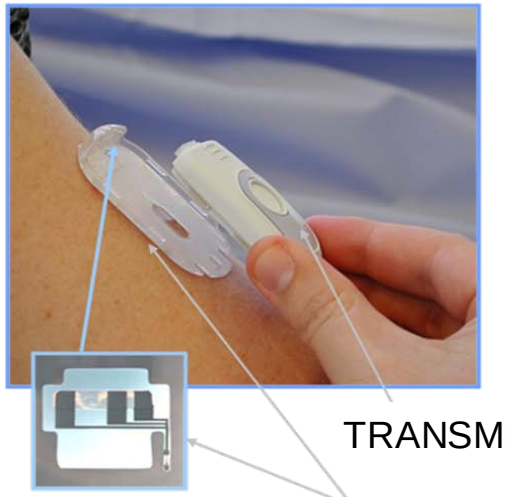
Professor Andrei Gurtov
Centre for Wireless Communications
University of Oulu, P.O. Box 4500, FI-90014 Oulu, Finland
gurtov@ee.oulu.fi

FRUCT'11, 26.4.2012
St. Petersburg, Russia

Motivation for Medical ICT

- Population gets older, high costs of medical care
- Insulin pumps, Implanted Cardio Defibrillators could be monitored remotely
- Threatening state of security in current medical devices
  - Demonstrated remote triggering of heart shock
- How to combine security with limited hardware and battery capabilities?

Secure Remote Monitoring of Personal Health Appliances (SEMOHealth)



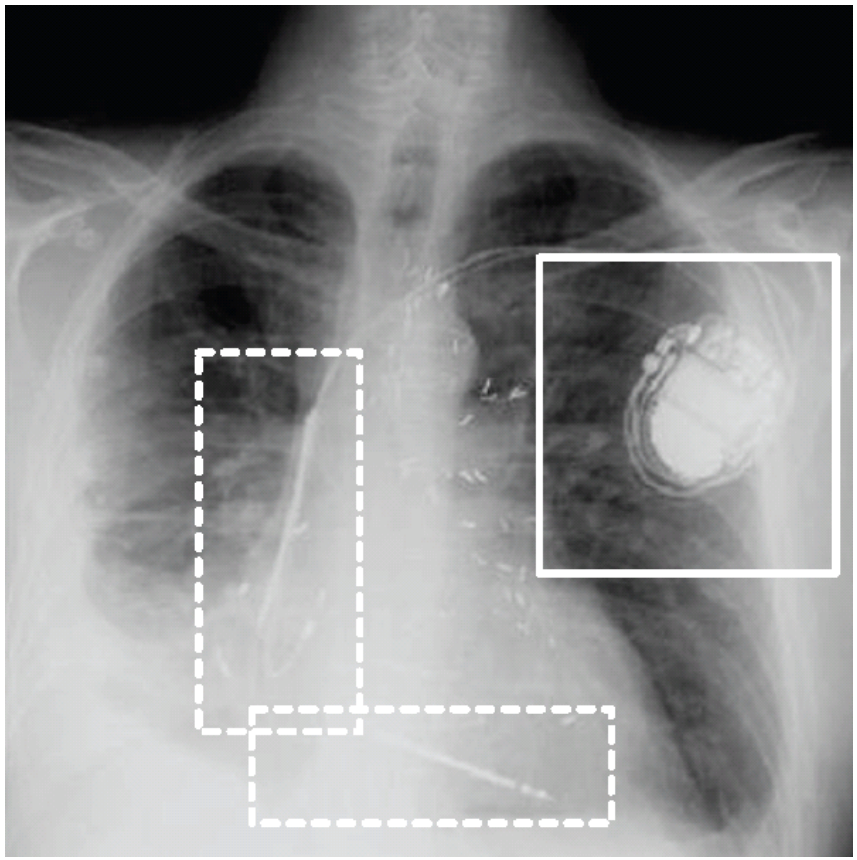
Overview of SEMOHealth Project

- Funded by Academy of Finland
- 1.1.2011-31.12.2013
- Main researchers: Ilya Nikolaevski, Dmitry Korzun
- Affiliated researchers: Dmitry Kuptsov, Boris Nechaev, Nie Pin, Juho Vähä-Herttua, Jani Pellikka
- Collaboration:
  - CWC, University of Oulu
  - Helsinki Institute for Information Technology HIIT
  - CSE, Aalto University
  - Philips Research
  - RWTH Aachen
  - FRUCT eHealth WG

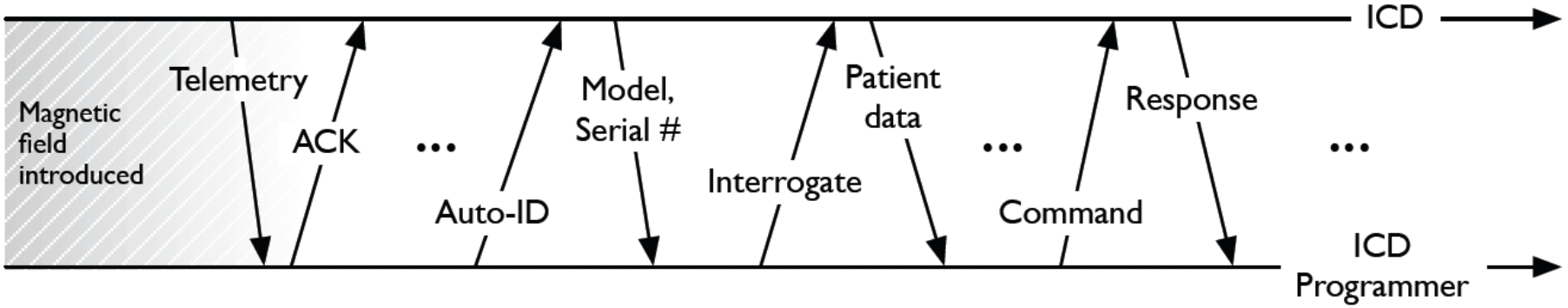
Demonstrated Attack on IMDs

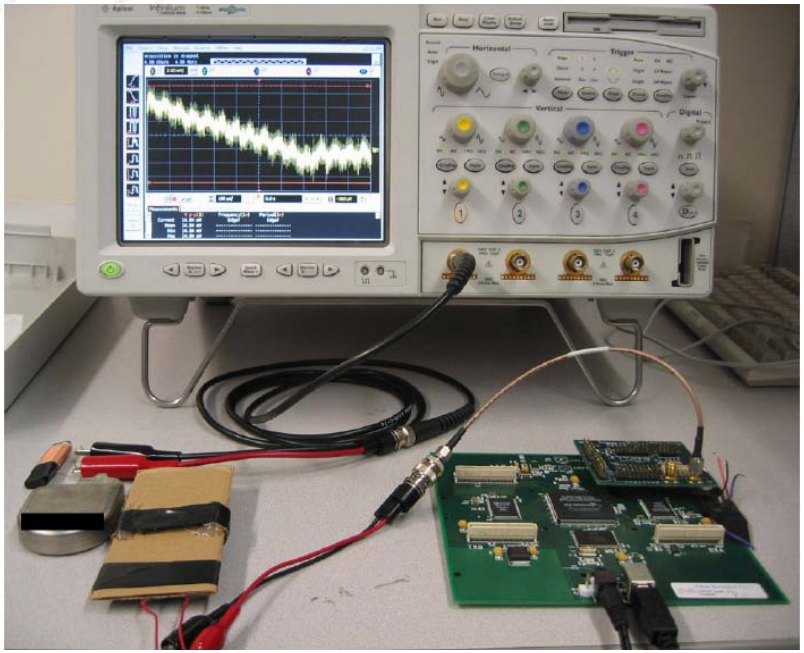
- **Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses**
  Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel
  IEEE Symposium on Security and Privacy, May 2008

(thanks for pictures!)



Decoded Plain-text Communication Protocol





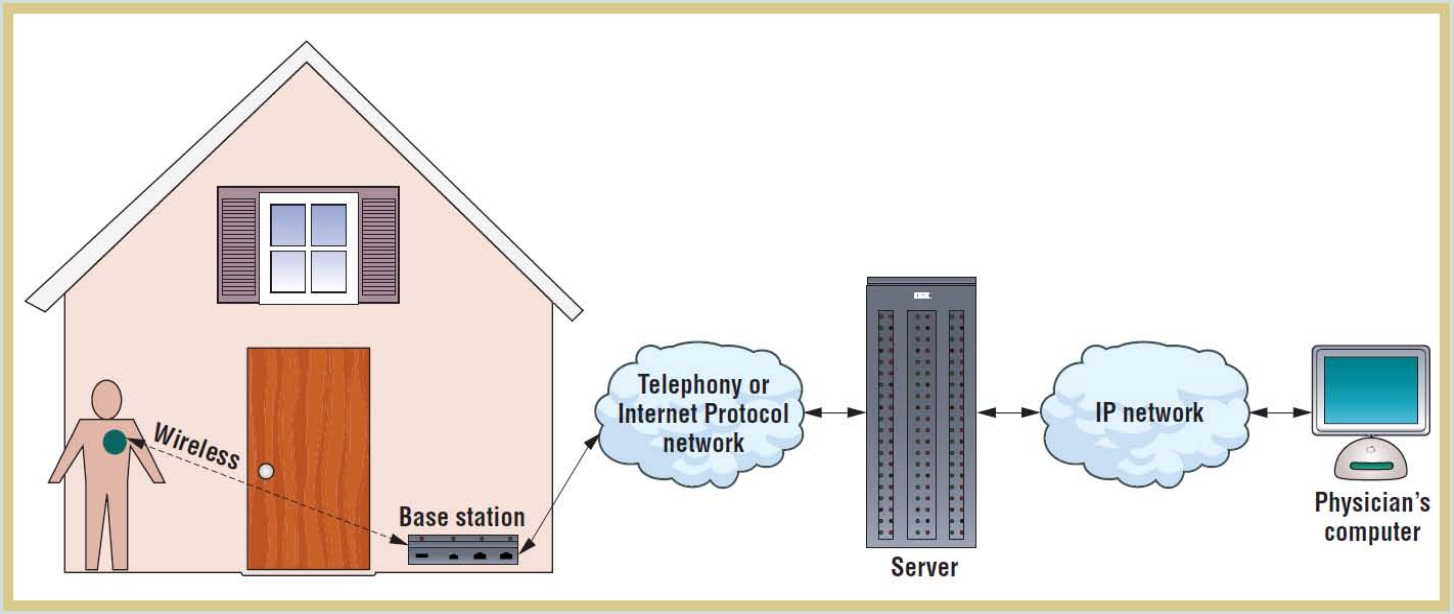
Demonstrated Attacks on Implanted Cardio Defibrillator

	Commercial programmer	Software radio eavesdropper	Software radio programmer	Primary risk
Determine whether patient has an ICD	✔	✔	✔	Privacy
Determine what kind of ICD patient has	✔	✔	✔	Privacy
Determine ID (serial #) of ICD	✔	✔	✔	Privacy
Obtain private telemetry data from ICD	✔	✔	✔	Privacy
Obtain private information about patient history	✔	✔	✔	Privacy
Determine identity (name, etc.) of patient	✔	✔	✔	Privacy
Change device settings	✔		✔	Integrity
Change or disable therapies	✔		✔	Integrity
Deliver command shock	✔		✔	Integrity

High-level Objectives of SEMOHealth

- High protection of the patient data
- Universal connectivity to patient
- Use of conventional mobile phones as a terminal
  - Sufficient range, needs to work e.g. in a shower
- Power efficiency
  - Battery must last 5-7 years
- Accessibility in case of emergency
  - Patient is unconscious
  - Traveling abroad
- Resilience to Denial-of-Service attack
- Operation over lossy wireless link
- Small packet size

Remote Monitoring Architecture



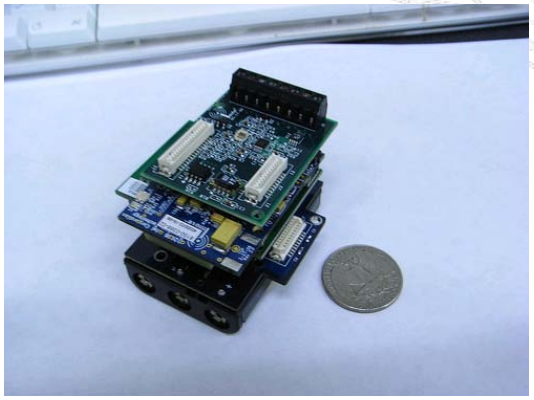
- Hybrid IPless/IP architecture based on Host Identity Protocol (HIP)
- Use of a mobile phone as a secure gateway for connecting personal devices to Internet
- No one knows yet how to exchange keys here!
- Trust management and revocation infrastructure
- Emergency access; Secure key storage; Preserving battery

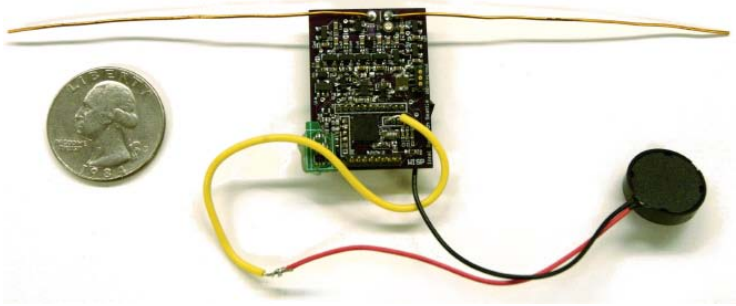
Expected Results and Contributions

- New energy-efficient security architecture for remote monitoring of personal medical devices
- Understanding the fundamental tradeoffs in security (preventing attacks) and accessibility in case of emergency
- New lightweight key exchange (e.g., using bivariate polynomials)
- Significant progress, even breakthroughs, are expected in the highly topical area of remote health monitoring
- At later phase, contribution to standards at IEEE 802.11.6 BodyNets and IETF Internet-of-things

Methodology

- Protocol and architecture design on paper first
- Analytical assessment of performance and scalability
- Prototyping and measurements on sensor platforms imote2 and Wireless Identification and Sensing Platform (WISP)
- Discussion with leading international experts on BodyNets and Internet-of-things
- Using Linux-based phone N900 as gateway
- Trial tests in collaboration with industry (Philips)





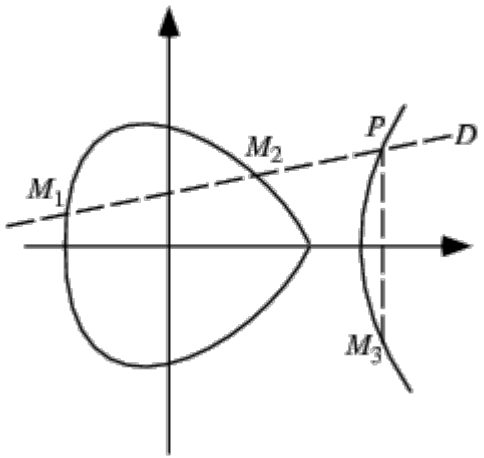
Host Identity Protocol (HIP) in a Nutshell

- HIP Base Exchange (BEX) – end-to-end key exchange protocol
- 4-way handshake (I1, R1, I2, R2 packets):
  - Mutual authentication with DSA/RSA signatures
  - Protection against DoS with puzzles
  - Key exchange with Diffie-Hellman (DH)
- HIP Diet Exchange (DEX) is a lightweight version
  - No signatures – fixed Elliptic curve DH (ECDH) keys are used instead
  - No hash functions

Duration of HIP Base Exchange (BEX)

- Basic HIP uses heavyweight RSA/DSA cryptography
- Association establishment can take up to a second even on regular PC
- Small devices have very restricted capabilities
- The use of Elliptic Curve Cryptography (ECC) is almost mandatory

Authentication	Session Key	BE
RSA1024	DH1536	275 ms
RSA1024	ECDH192	39 ms
ECDSA160	ECDH192	33 ms
RSA2048	DH2048	747 ms
RSA2048	ECDH224	187 ms
ECDSA224	ECDH224	129 ms



Security Properties of ECC and HIP BEX

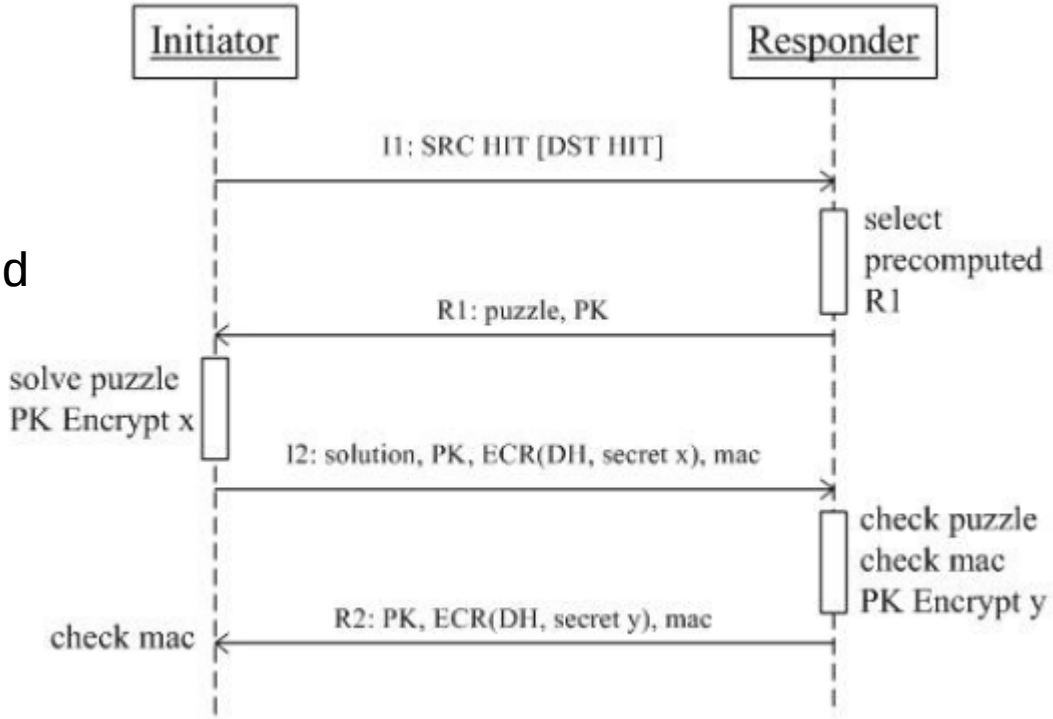
- ECC offers same cryptographic strength with almost order of magnitude less space
- HIP BEX requires signature operations and Diffie-Hellman key exchange

Security level	ECC	DSA/RSA
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Message	Initiator	Responder
I1	-	-
R1	verify, DH_compute_key	sign
I2	sign	verify, DH_compute_key
R2	verify	sign
CLOSE	sign	verify
CLOSE_ACK	verify	sign
Total	$2 \times T_{sign} + 3 \times T_{verify} + T_{dh}$	$3 \times T_{sign} + 2 \times T_{verify} + T_{dh}$
Only Base Exchange	$T_{sign} + 2 \times T_{verify} + T_{dh}$	$2 \times T_{sign} + T_{verify} + T_{dh}$

HIP Diet Exchange (DEX)

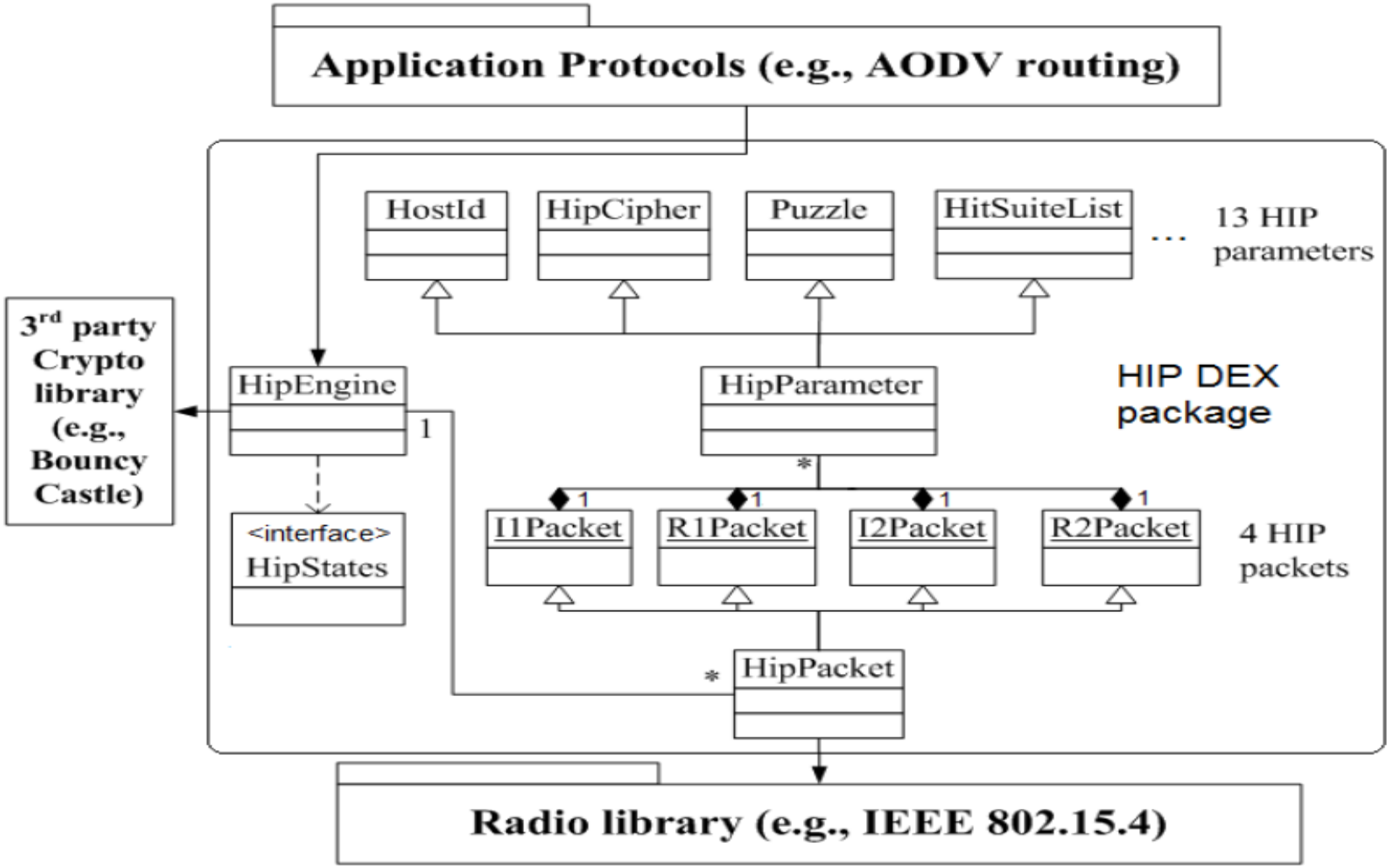
- Four-way handshake protocol proposed by Robert Moskowitz
- Packet size [40, 216)
  - Fragmentation needed
- Security primitives:
  - Puzzle
  - ECDH
  - AES encryption
  - CMAC



Security analysis of HIP DEX

- Protection against six attack models
  - Radio jamming: None
  - Packet DoS attack: Puzzle
  - Replay attack: Nonce + CMAC
  - Spoofing/Sybil attack: Password authentication
  - Message eavesdropping: AES encryption
  - Man-in-the-middleware/wormhole: ECDH

Implementation of DEX on Java SunSPOT



Experimental Results of DEX

- Energy & computing overhead of Initiator & Responder

	Energy consumption (10^{-3}mJ)	Computing latency (ms)
Puzzle generation and verification	17.95 (R)	227 (R)
Puzzle resolution	135.60 (I)	1297 (I)
ECDH handshake	143.12 (I+R)	498 (I+R)
CMAC calculation	0.44 (I+R)	4 (I+R)
Total cost	279.16 (I) 161.51 (R)	1799 (I) 729 (R)

- Different settings of puzzle difficulty and key length

	Energy consumption (10^{-3}mJ)	Computing latency (ms)
Puzzle resolution K=4,5,6,7,8,9,10	15.06, 24.16, 34.08, 68.41 135.61, 221.41, 540.39	155, 245, 338, 663 1297, 2099, 5085
ECDH handshake key=160,192,224	136.46, 208.98 301.59	498, 727 1072

Improvements

- Whitelist to store valid HITs during the network initialization phase
  - HIP NOTIFY (NEW_NODE) from the trusted base station
- Blacklist to ban abnormal HITs with excessive RSSI
  - Cross-layer design to evaluate signal strength
  - Use puzzle as a countermeasure
  - HIP NOTIFY (INVALID_HIT) to spread

Comparison DEX vs SSL/TLS

	HIP DEX	SSL/TLS
Overhead	Low (without puzzle)	Medial (without signatures)
Identity	Whitelist	ECDSA
Extensibility	Good	Rigid
Mobility	Yes	Limited
Scalability	High	Low
Maturity	Low	High

- Compatibility issue with legacy systems
- More efficient and flexible on WSNs
- Inherent support to the mobility of device/node
- No reference implementation and deployment

Model and Requirements for Medical Access

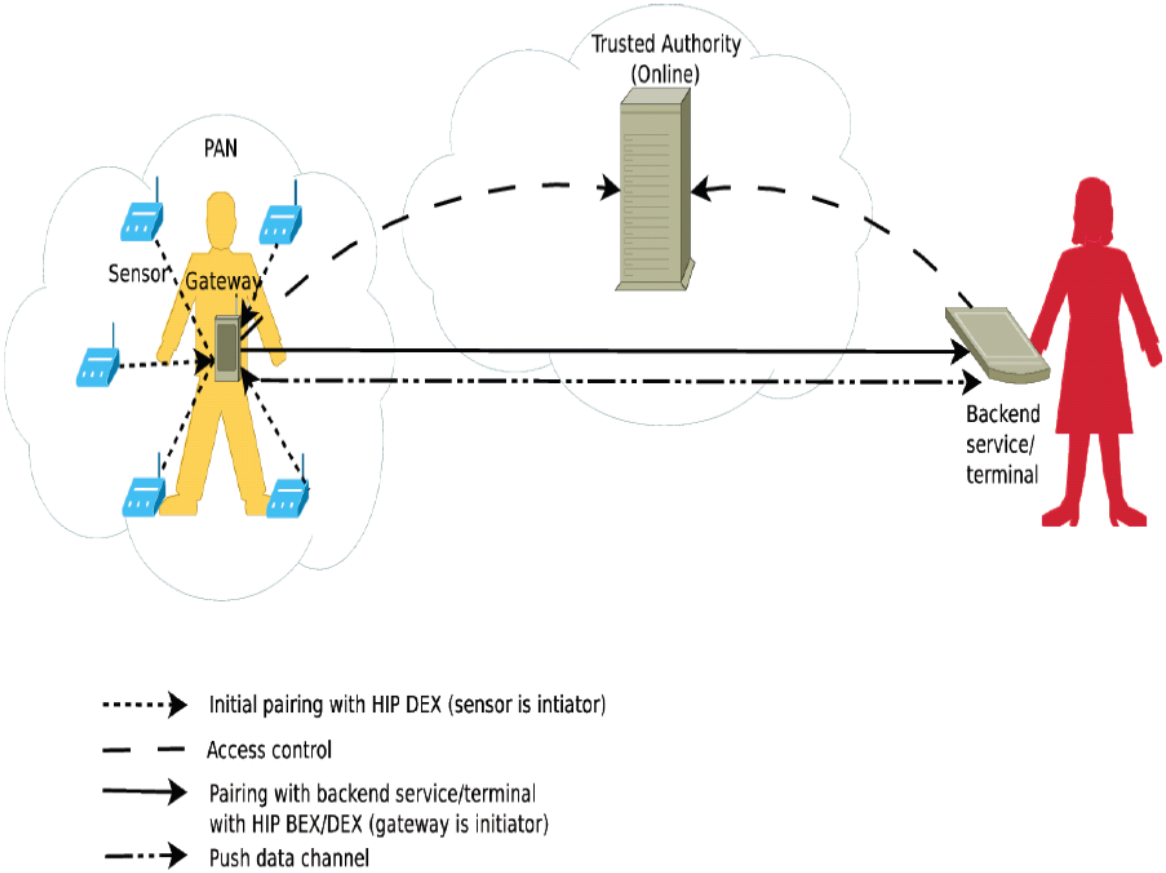
- Medical sensor network (MSN) comprises 2 subnetworks: Personal area network (PAN) and Backend area network (BAN)
- PAN sensors have limited battery and processing resources; BAN nodes don't
- PAN-to-PAN and PAN-to-BAN communication via PAN gateway
- PAN gateway manages security associations and enforces access control between the PAN sensors and BAN nodes
- A special trusted third party (TTP) exists and is trusted by all BAN nodes and PAN gateway
  - Manages identities and certificates
  - Provides means to build access control

Model and Requirements (cont'd)

- Two communication patterns:
  - PAN-to-PAN or PAN-to-Gateway
  - BAN-to-PAN Gateway
- PAN nodes perform initial pairing with gateway once after the deployment and store keying material permanently
- BAN nodes establish security associations with PAN gateway on demand

Architecture

- Sensor to gateway pairing
- Gateway to backend service pairing
- Backend terminal to gateway pairing
- Access control



Initial Pairing

- Occurs once after deployment of the PAN network
- Mutual authentication in HIP DEX is achieved with:
  - Preshared passwords
    - Secrets should be configured on both PAN gateway and PAN node prior to HIP handshake
  - Passwordless link-button approach:
    - Nodes perform HIP handshake within a small time window, e.g., within 5 seconds window after link button pressed on a gateway node

Initial Pairing (cont'd)

- Passwords can be preshared:
  - Using physical contact
  - Conveyed via visual channel (most convenient and secure method)
- Keys negotiated with HIP DEX are stored permanently on a gateway node and PAN node
- Procedure is repeated for all PAN nodes
- If the keys need to be rotated, initial pairing should be repeated

Gateway to Backend Service Pairing

- PAN node establishes security association with a backend service using HIP BEX
  - TTP signed certificates used for mutual authentication
  - RSA/DSA signatures for protecting DH keys
- PAN gateway initiates the communication and no other traffic is allowed

Backend Terminal to Gateway Pairing

- Imagine no Internet connectivity is available and emergency service needs to access the patient's PAN network
- Recall PAN gateway is configure to deny all communication but from the backend service
- PAN gateway triggers HIP BEX and waits for a legitimate answer (R1 containing valid certificate)
- Emergency service obtains a short time certificate prior to communication with PAN gateway (more on this in the next slide)

Access Control

- Patient's data is confidential
- Not all user's have equal rights to read/modify the configuration of patient's PAN
- BAN gateway should distinguish the revoked certificates
- Our proposal is to use 2 types of certificates:
  - Permanent membership certificate (PMC)
  - On-demand short term certificates (OSTC)
- PMCs are used by TTP as the bases for granting OSTCs
- PAN gateway accepts HIP BEX packet only with valid OSTCs (HIP BEX with PMCs are not allowed!)
  - Other HIP BEX packets are dropped

Evaluation of DEX and BEX on Imote2 Sensor

Protocol components	**Network types**		
	PAN	Internet	
	ECC HIP DEX	HIP BEX ECC	HIP BEX
Key exchange	Fixed ECDH	ECDH	DH
	160 bit	160 bit	1536 bit
Signatures	None	ECDSA	RSA
Certification method	None	ECDSA	RSA
Puzzle difficulty	0	≥ 10	≥ 10
MAC	CMAC (AES-CBC)	SHA-1	SHA-1
Message sizes (bytes)			
I1	40	40	40
R1	92	916	1544
I2	148	944	1568
R2	102	108	188
	DEX Duration (ms)	**BEX Duration (ms)**	
	72.396	151.26	1115.96
Energy (mj)			
For Initiator (I)	17.0	53.8	471.5
For Responder (R)	17.0	34.1	222.5
Total w/ transmission, I	26.14	73.74	560.1
Total w/ transmission, R	26.14	61.19	443.1

Implicit Certificates in HIP DEX

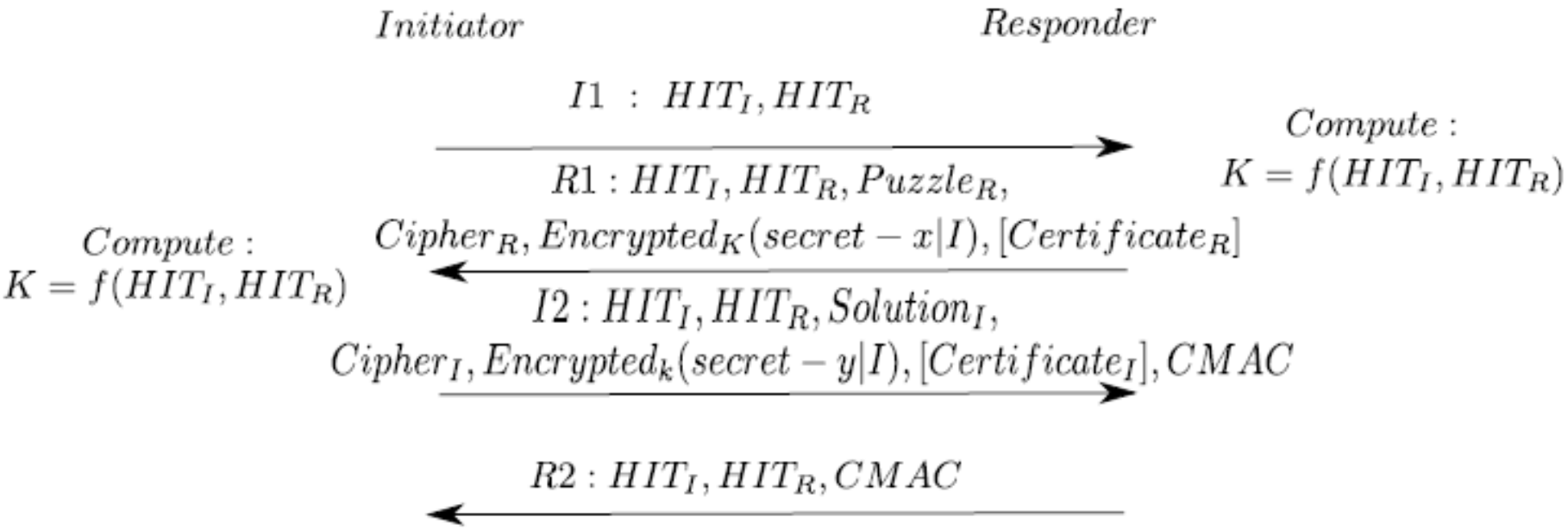
- Verification of implicit certificates is **extremely fast** compared with standard certificates with signatures and even ECDSA
  - Certificate verification is a CMAC run and a few elliptic curve polynomial operations (multiplication and addition)
  - **No signatures at all**
- If only HI is certificated **no need for transmitting X.509, SPKI, or any ASCII-structured documents in HIP signaling (not to mention processing them!) → smaller packet size and processing overhead**
  - Attribute certs require a more sophisticated format though
- Pseudonym HIs (public keys) certified by a 3rd party and bound to the static HIs and/or other relevant information
  - Yes, every host still maintains its own static host identity
  - Provides **host privacy** if certified CERTs encrypted (in I2 and R2)
    - Both Initiator and Responder can be protected
- Better **forward secrecy** due to use of ephemeral keys

Implicit Certificates in HIP DEX

- Implemented ECQV to HIP-DEX protocol
  - DEX carried out with disposable certified public keys (certified and bound cryptographically to the static HI and/or other relevant information by a 3rd party)
  - Conforms to "SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)", working draft Oct-2008, version 0.97
  - Exception: hash function *Hash* is CMAC function
    - Hash(BEU || I_U) → CMAC(BEU, I_U)
      - *BEU = negotiated (CA and host) random point in binary format, also know as the public-key reconstruction data*
      - *I_U = certified information about the host (e.g. HI, APN, NAI, …)*

Diet HIP with Polynomials

- New possible lightweight protocol for key exchange



Standardization Status

- New Task Group IEEE 802.15.9
  - Key management protocol for 802.15.4 and .7 links
  - HIP DEX, IKEv2, PANA, etc
  - Best Current Practice specification are expected within a year
- Internet Engineering Task Force (IETF)
  - Standards-track HIP RFCs
  - Developing DEX
- Internet Research Task Force (IRTF)
  - Published HIP experiment report
  - Related work on Internet-of-Things

Summary

- Current state of medical ICT security is scary
- A promising architecture and lightweight key management protocols are developed in SEMOHealth project
- Standard contributions to IEEE and IETF
- Future: zero power security with energy harvesting?