ITU-T Meeting SG17: Security – Tutorial
ITU, Geneva, Switzerland

Two-way Authentication for Tiny Devices

Corinna Schmitt, Burkhard Stiller
Department of Informatics IFI, Communication Systems Group CSG,
University of Zürich UZH
[schmitt | stiller]@ifi.uzh.ch

April 15, 2015

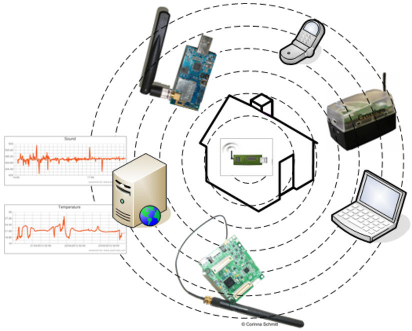
Universität Zürich[UZH]

CSG
Communication Systems Group

ifi

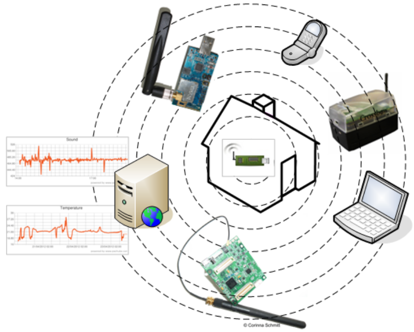
Content

- SecureWSN
  - Research motivation
  - SecureWSN architecture
  - Hardware
- Two-way Authentication Solutions
  - TinyDTLS
  - TinyTO
- Conclusion



Content

- SecureWSN
  - Research motivation
  - SecureWSN architecture
  - Hardware
- Two-way Authentication Solutions
  - TinyDTLS
  - TinyTO
- Conclusion



Research Motivation

- Internet connectivity rises → Internet of Thing (IoT)
  – All kind of devices that use IP communications.

- IoT is not limit to notebooks and servers anymore
  → Includes also constraint devices (e.g., mobiles, sensors)
  → Special case: Wireless Sensor Networks (WSNs)

Research Motivation

- Internet connectivity rises → Internet of Thing (IoT)
  - All kind of devices that use IP communications.

- IoT is not limit to notebooks and servers anymore
  → Special case: Wireless Sensor Networks (WSNs)
  → Constraint devices

- Constraints in memory, power, and computational capacity
  - Research is challenging
  - Not limited to architecture issues
  - Includes security aspects and solution design
    → Building trust in the network
    → Support privacy

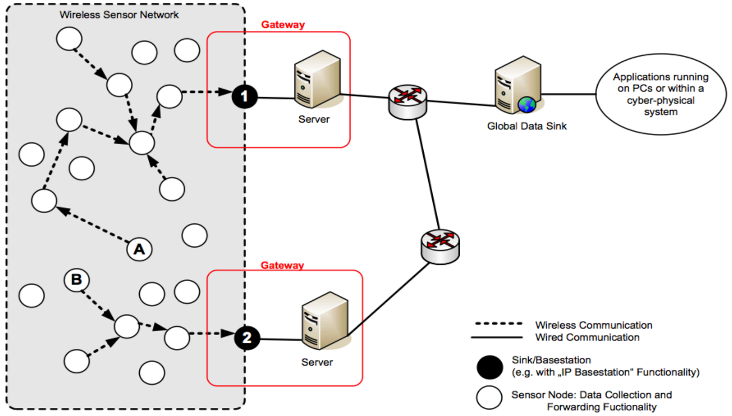
- Any data includes sensitive information

Wireless Sensor Network

- WSN consists of different sensor nodes.
- Nodes are from different vendors with different equipment.
  - Memory, energy, sensors
- Usually WSNs using IEEE 802.15.4 and UDP as transmission protocol of choice.
- WSN destination has parser and gateway functionality.

- Goals:
  - Efficient data transmission
    → limit redundancy, pre-processing
  - Secure transmissions

- Idea:
  - Use standards from IP networks.
  - Optimize data transmission in order to save resources.



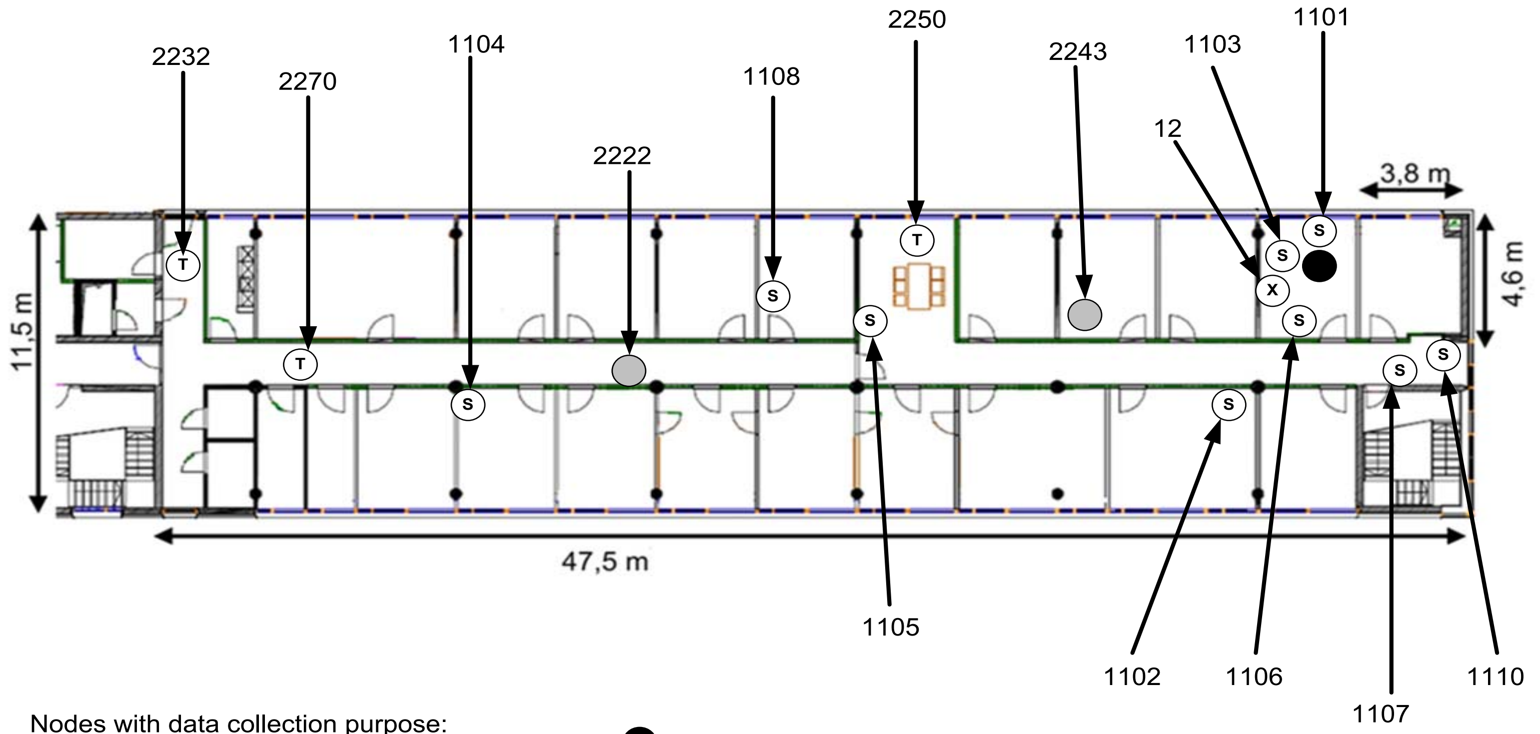
Constraint Devices (RFC 7228)

Name	data size (e.g., RAM)	code size (e.g., Flash)
Class 0, C0	<< 10 KiB	<< 100 KiB
Class 1, C1	~ 10 KiB	~ 100 KiB
Class 2, C2	~ 50 KiB	~ 250 KiB

Table 1: Classes of Constrained Devices (KiB = 1024 bytes)

- **Class 0 devices**
  - Sensor-like nodes
  - Usually pre-configured
  - In general are not able to communicate directly and secure with the Internet.
- **Class 1 devices**
  - Unable to talk easily to other Internet nodes employing a full protocol stack (*e.g.*, HTTP, TLS, or security protocols).
  - Are able to provide support for security functions required on large networks
  - Can be integrated as fully developed peers into an IP network.
- **Class 2 devices**
  - Can support mostly same protocol stacks as used on notebooks or servers.

SecureWSN Scenario



Nodes with data collection purpose:

(S) IRIS with mts300 or mts400

(T) TelosB with activated sensors

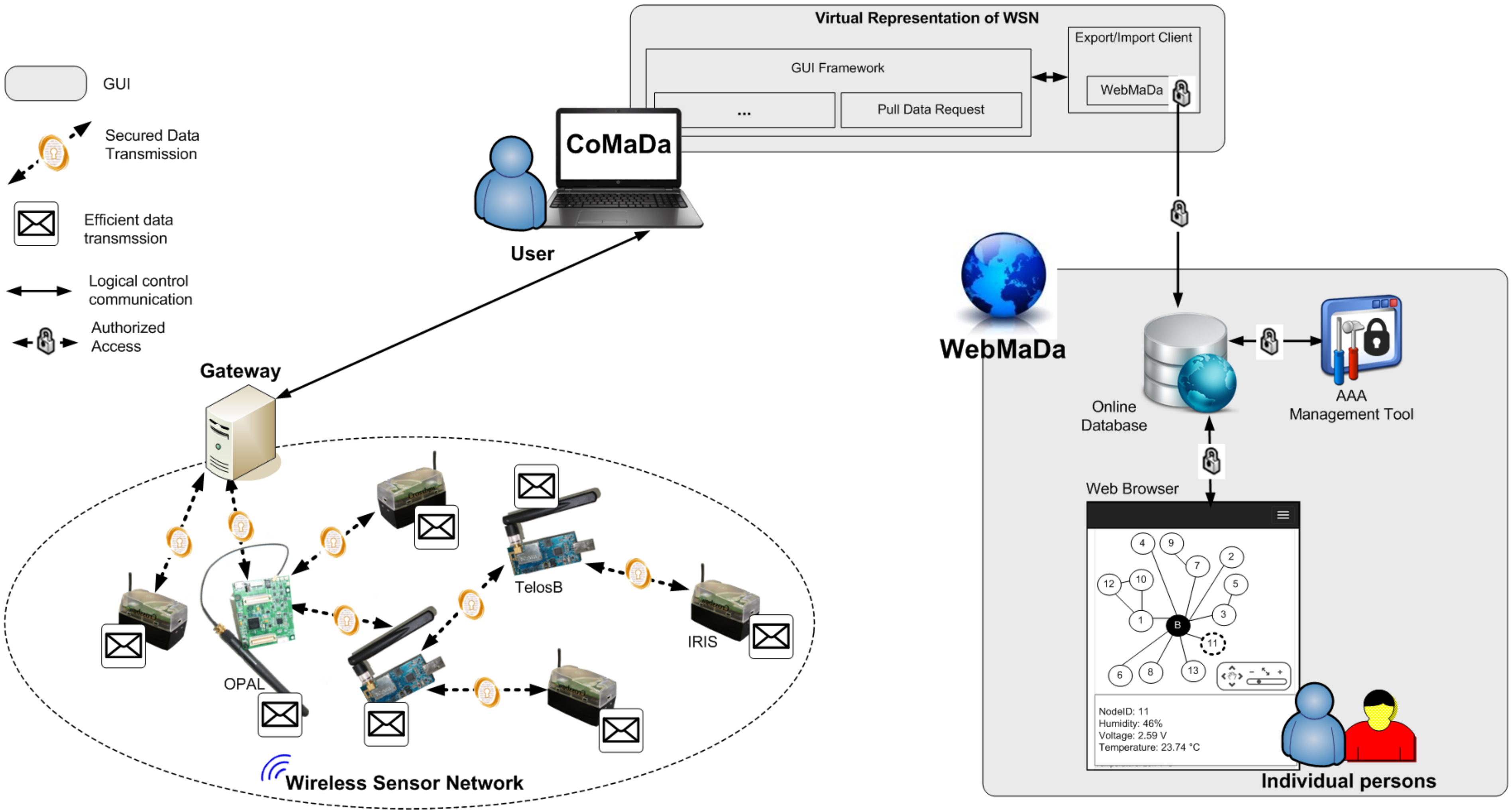
Gateway (TelosB)

TelosB with aggregation purpose

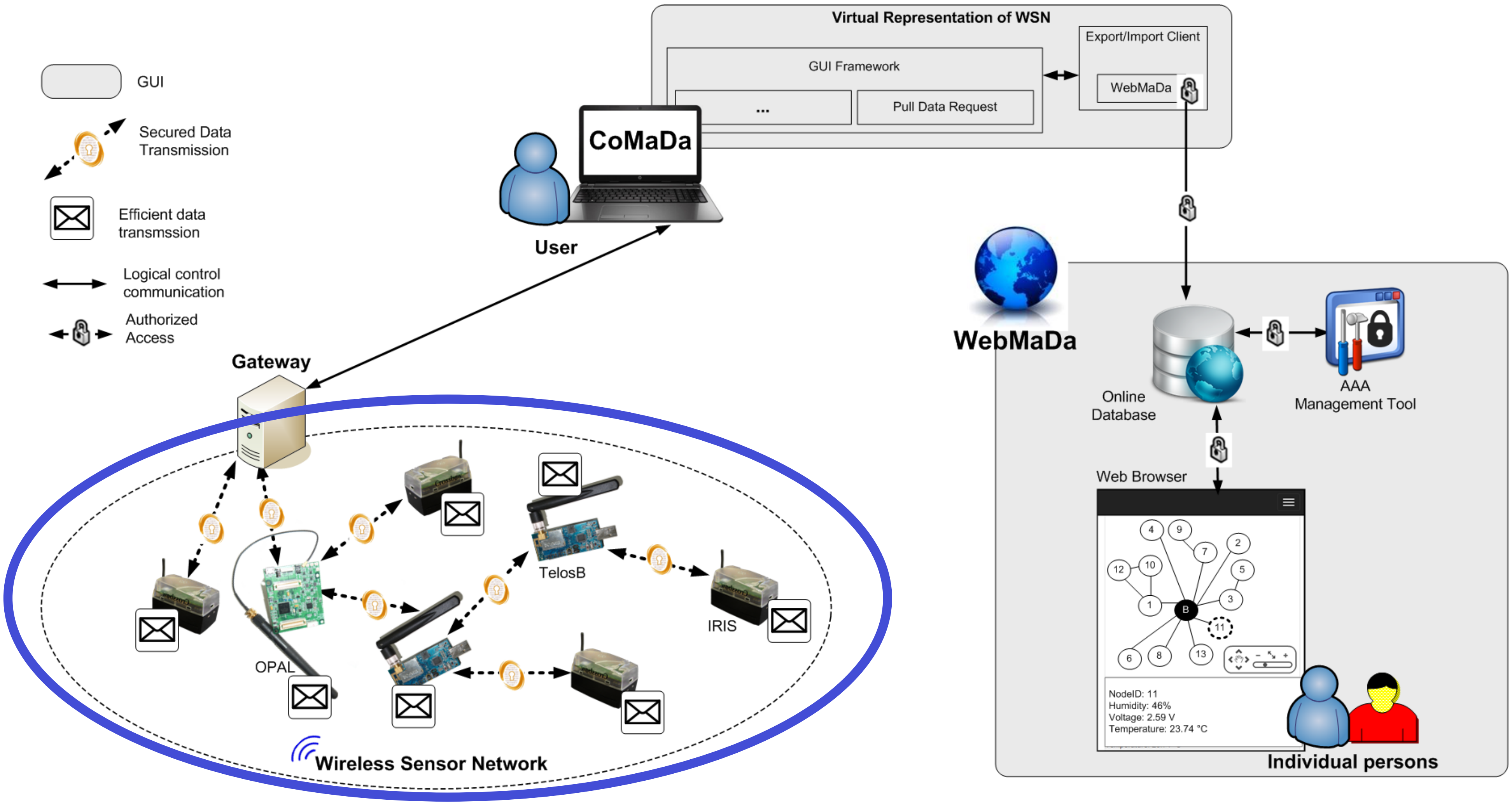
(X) Opal

ifi

SecureWSN Component Overview



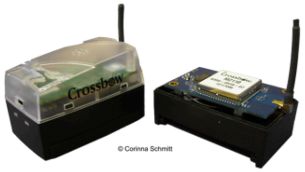
SecureWSN Component Overview



Two-way authentication

Hardware & Functionalities

IRIS (MTS300, MTS400) from Crossbow Inc. (XBOW)

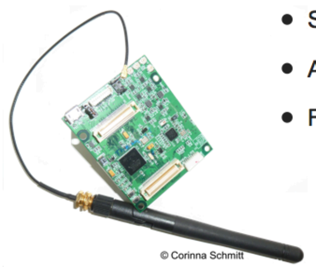


- Data collection - TinyIPFIX
- Forwarding

TelosB of type CM5000-SMA from ADVANTIC SISTEMAS Y SERVICIOS S.L.

- Aggregation - TinyIPFIX
- Data collection - TinyIPFIX
- Forwarding
- Security support: TinyTO, TinySAM

OPAL from Commonwealth Scientific and Industrial Research Organisation (CSIRO)

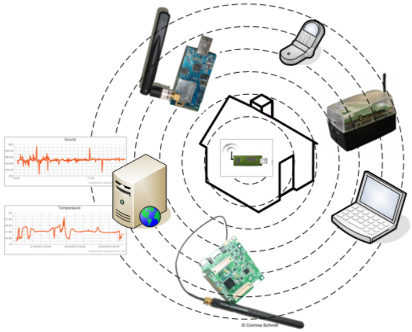


- Security support: TinyDTLS
- Aggregation - TinyIPFIX
- Forwarding

	IRIS	TelosB	OPAL
Chip	ATMega1281	TPR2400CA	Atmel Cortex SAM3U4E
Program Flash Memory	128 kB	48 kB	256 kB
Measurement (Serial) Flash	512 kB	1024 kB	n.n.
RAM	8 kB	10 kB	52 kB
Configuration EEPROM	4 kB	16 kB	n.n.
Power Source	2 AA	USB 2 AA	microUSB B 3 AA
Processor Current Draw	Active: 8 mA Sleep: 0.008 mA	Active: 1.8 mA Sleep: 0.051 mA	Active: 30 mA Sleep: 0.0025 mA
RF Transceiver Current Draw	Receive: 16 mA	Receive: 23 mA Idle: 0.021 mA Sleep: 0.001 mA	Receive: 16 mA
Size [mm]	58 x 32 x 7	65 x 31 x 5	60 x 50 x 10
Weight [g]	18	23	40
Sensors & Features	Light, Temperature, GPS, Humidity, Acoustic actuator, Acoustic, Barometric pressure, Seismic, Magnetometer	Light, Humidity, Temperature	Trusted Platform Module (TPM)
Manufacturer	Crossbow Inc.	Advantic Sistemas Y Servicios S.L., Crossbow Inc.	CSIRO

Content

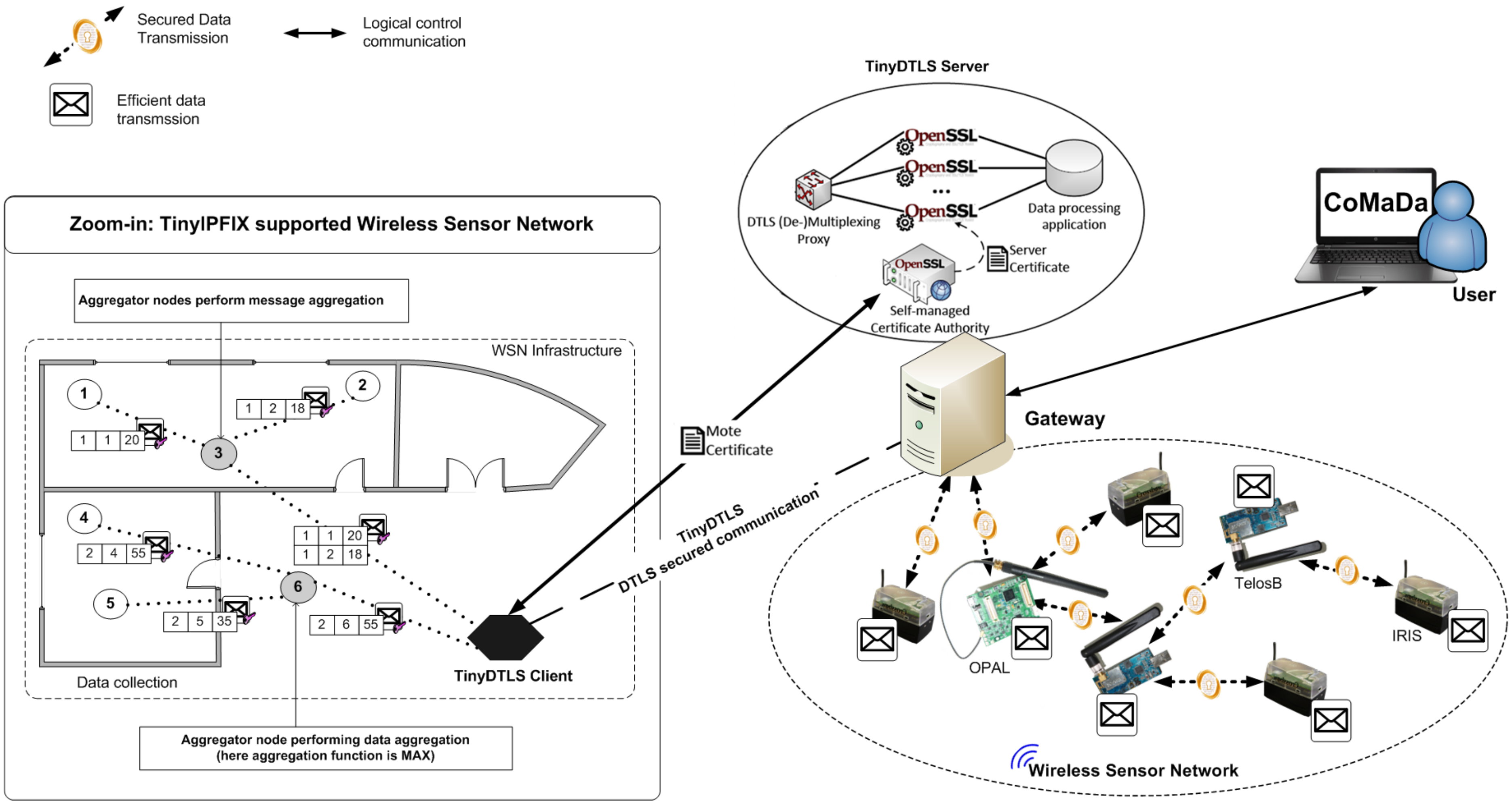
- SecureWSN
  - Research motivation
  - SecureWSN architecture
  - Hardware
- Two-way Authentication Solutions
  - TinyDTLS
  - TinyTO
- Conclusion



Two-way Authentication Solutions in SecureWSN

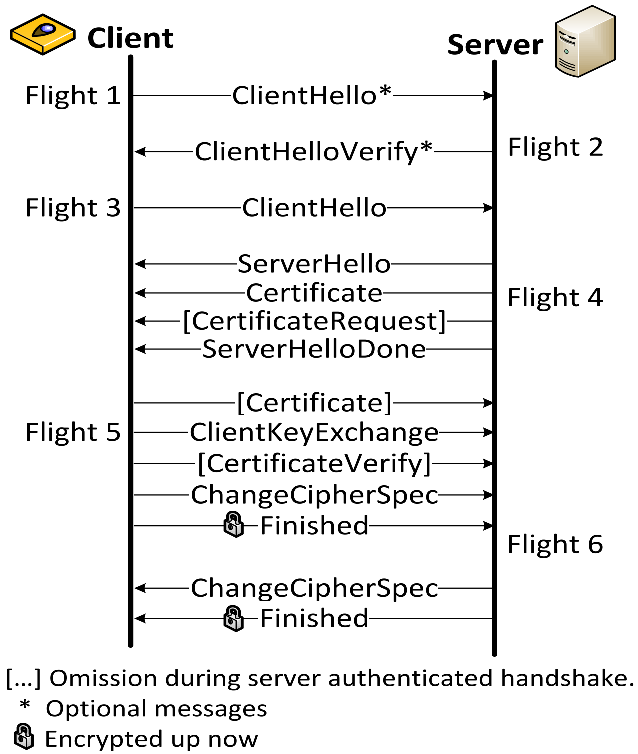
- **TinyDTLS**
  - DTLS solution using OPAL clusterhead supporting message aggregation
  - Requirements
    - Class 2 devices or higher
    - External infrastructure – Certificate Authority
    - X.509 certificates
- **TinyTO**
  - Bellare-Canetti-Krawczyk (BCK) with pre-shared master key
  - Requirments
    - Class 1 devices
    - Pre-shared master key
- Requirement: Support of efficient data format TinyIPFIX and aggregation.

Updated Architecture for TinyDTLS



TinyDTLS - Handshake

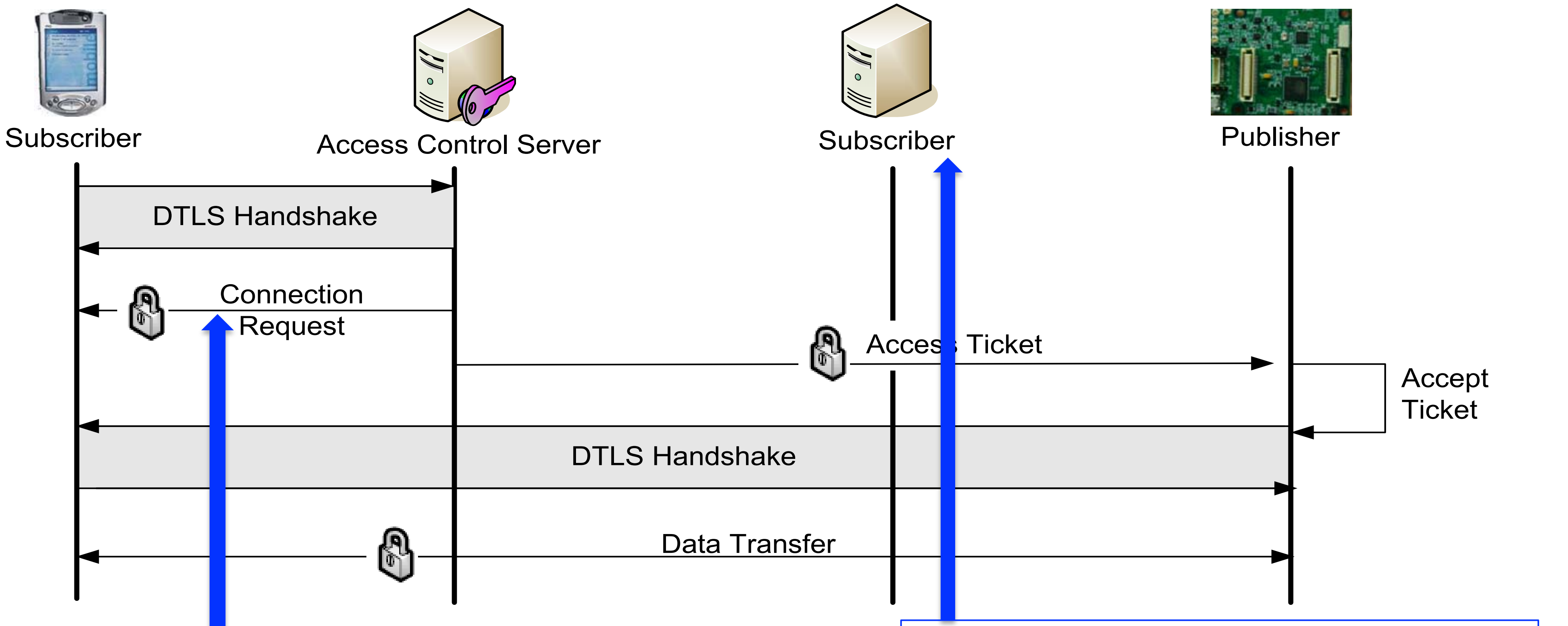
- Solution:
  - DTLS client supports server authentication
  - DTLS client supports fully authenticated DTLS handshakes.
- Handshake
  - Secured by RSA X.509 certificates
  - Server and client negotiate hash algorithm and cipher in handshake
  - Different authentication possible
- DTLS server implementation is based on OpenSSL 1.0.0d
  - Padding for RSA signature verification uses PKCS#1.
  - Client has to sign a SHA1 hash instead of concatenation of a MD5 and SHA1 hash.



TinyDTLS - Functionality

- Supported cipher suite:
  - RSA for key exchange
  - AES-128-CBC for encryption
  - SHA1 for hashing
- Cluster head with TPM
  - Provides tamper proof generation
  - Storage of RSA keys
  - Hardware support for the RSA algorithm.
- Nodes without TPM:
  - Authentication via the DTLS pre-shared key cipher-suite is supported.
    - Chose of small number of random Bytes Preload to the publisher before deployment
    - Derivate the actual key.
  - New established secret must also be available for the ACS
    - Disclose the key to devices with sufficient authorization.

TinyDTLS - Data Exchange



Subscriber asks for connection to publisher and receives a connection request (copy of access ticket) back.

= Gateway with forwarding functionality and format conversion of data between IP network and WSN.

TinyDTLS - Evaluation

Memory consumption

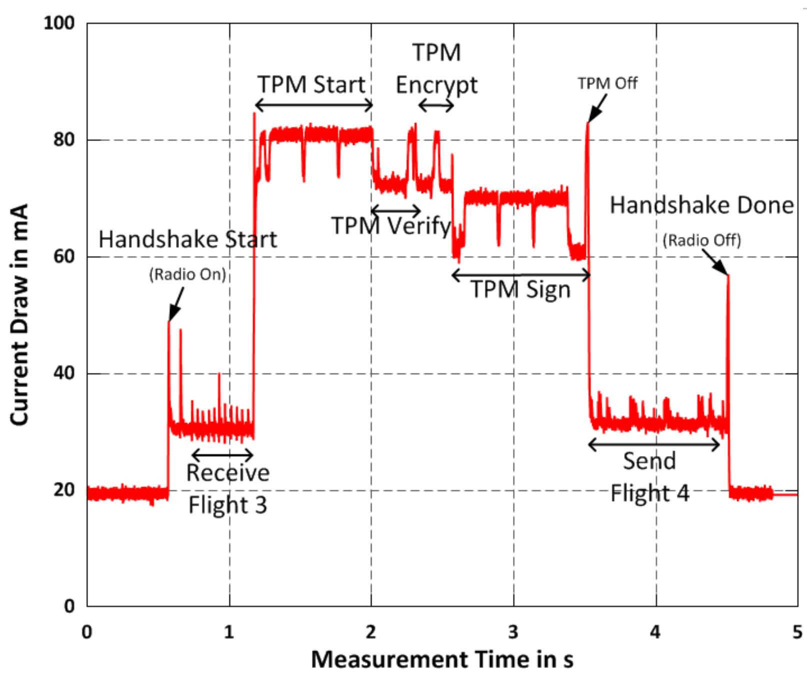
Component	RAM [bytes]	ROM [bytes]
Cryptography	537	10635
DTLS Messages	1348	4204
DTLS Network	3614	3104
TPM	4356	6406
BLIP	5968	6868
Application	98	2488
System	1306	27907
Sum (total)	**17,839**	**63,383**

Assumption: 2048-bit RSA key

Action	Current [mA]	Fully Authenticated Handshake		Server Fully Authenticated Handshake	
		Time [ms]	Energy [mJ]	Time [ms]	Energy [mJ]
Computation	30	35	4.18	33	3.95
Radio TX	18	242	17.4	70	5.03
TPM Start	52.2	836	174.46	836	174.5
TPM TWI	43.6	688	120.0	476	83.0
TPM Verify	51.8	59	12.2	56	11.6
TPM Encrypt	51.8	39	8.07	40	8.28
TPM Sign	52.2	726	151.5	-	-
Sum	299.6	2625	487.8	1511	286.4

Transaction time and energy consumption

TPM energy consumption



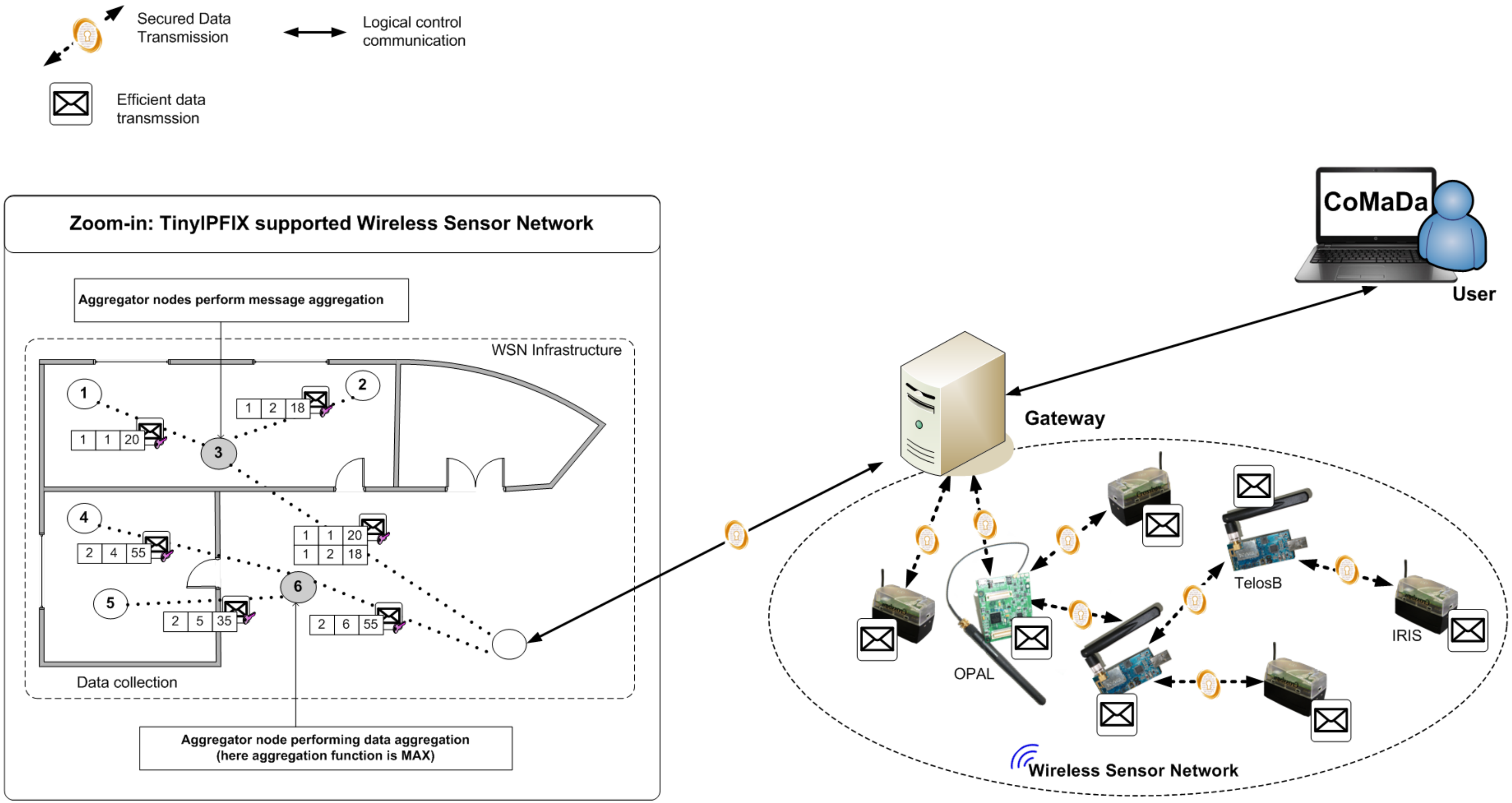
TinyDTLS - Drawbacks

- TinyDTLS
  - Very resource consuming → needs class 2 device
  - X.509 certificates
  - External infrastructure required

→ More light-weighted solution required

→ Requests
  → Support two-way authentication
  → Same security level support (e.g., keying material)

Architecture for TinyTO

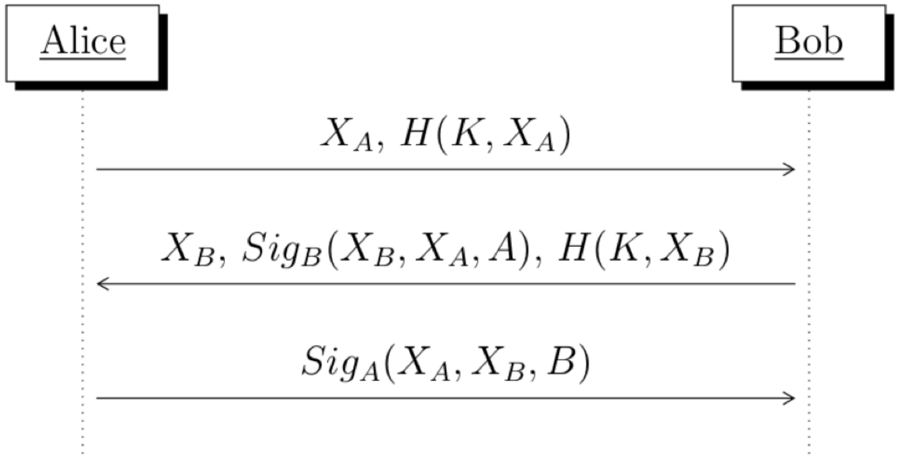


TinyTO - Handshake

- **T**wo-way Authentication Protocol for **Tiny** Devices (**O**ptimization)
- Modified Bellare, Canetti, Krawczyk (BCK) with Pre-shared Keys (PSK)
  - Defense against a man-in-the-middle attack
  - Additional authorization of different communication parties

- Elliptic Curve Cryptography used
  - For key generation
  - For key exchange
  - For signatures
  - For encryption

- Key sizes
  - 192-bit ECC key
  - Comparable to the security levels of RSA keys in range of 1024-bit to 2048-bit

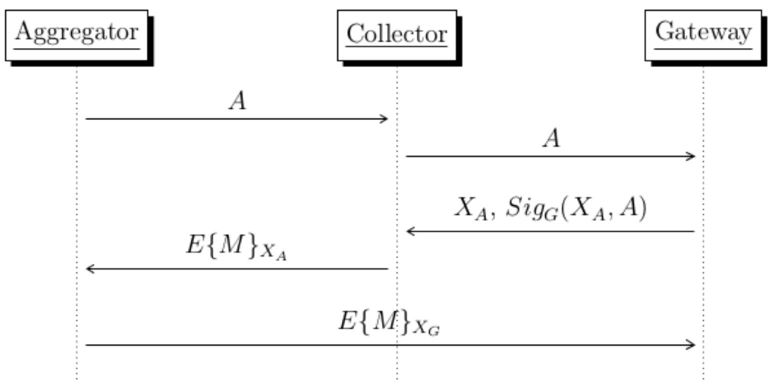


X_A : Public Key Alice
X_B : Public Key Bob
K : Pres-Shared Key

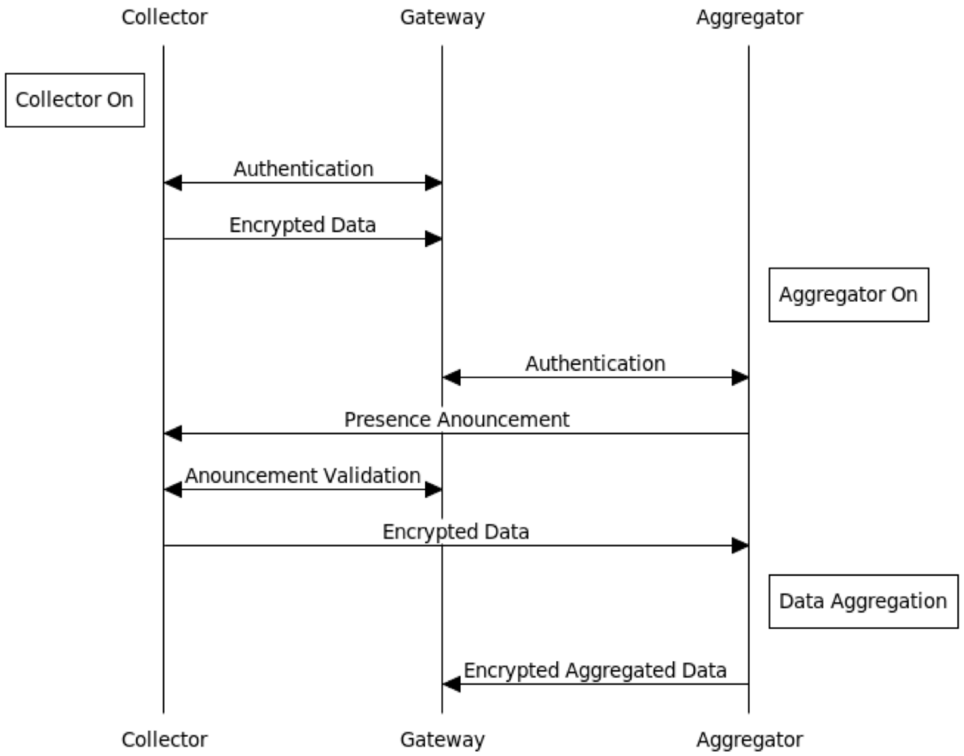
Sig_A : Signature by Alice
Sig_B : Signature by Bob
H : Hash

TinyTO – Handshake for Aggregation

- Aggregation support



A : Identity Aggregator
X_A : Public Key Aggregator
Sig_G : Signature by Gateway
$E\{M\}_P$: Encryption with P



TinyTO - Evaluation

Memory Consumption for Collector and Aggregator

Collector		
Component	**RAM [bytes]**	**ROM [bytes]**
Cryptography	406	9378
Handshake	612	1138
Data Collection	5478	31344
RPL	1498	6228
Sum (total)	**7994**	**48114**

Aggregator		
Component	**RAM [bytes]**	**ROM [bytes]**
Cryptography	406	11406
Handshake	602	1636
Data Aggregation	6964	26904
RPL	498	6270
Sum (total)	**8470**	**46216**

Operation	Collector [s]	Aggregator [s]
EC Key Generation	8.77 ± 0.17	4.77 ± 0.14
SHA-1	< 0.1	< 0.1
ECDSA Sign	9.28 ± 0.18	5.14 ± 0.19
ECDSA Verify	18.51 ± 0.19	10.20 ± 0.19
ECIES Encrypt	9.41 ± 0.18	5.98 ± 0.15
ECIES Decrypt	-	4.96 ± 0.19

Operation	Time [s]
Handshake for Aggregator	20.89 ± 0.18
Handshake for Collector	36.79 ± 0.18
Aggregator Verification	19.44 ± 0.19
Message Aggregation (doa = 2)	15.90 ± 0.53

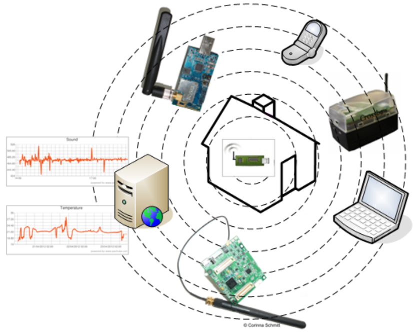
Execution Times for individual ECC Operations

Energy Consumption of Different Cryptographic Operations

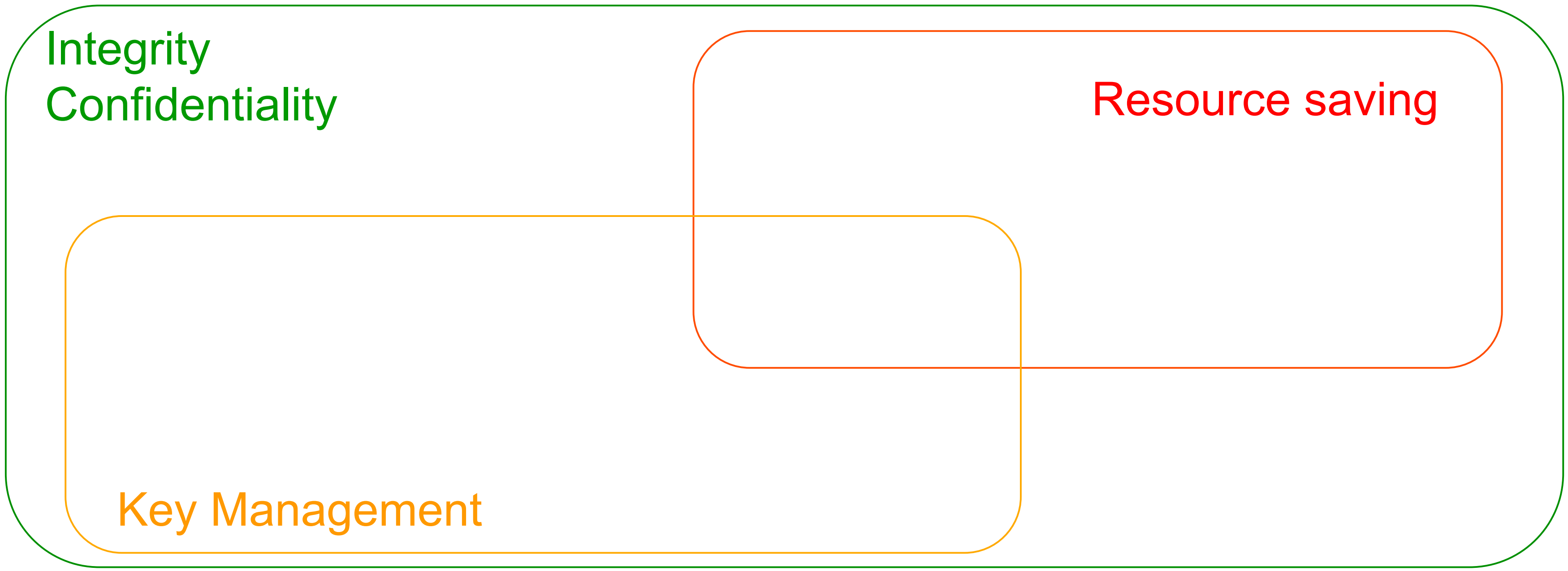
Operation	Collector		Aggregator	
	Time [s]	Energy [mJ]	Time [s]	Energy [mJ]
EC Key Generation	4.77 ± 0.14	25.77 ± 0.03	8.77 ± 0.17	56.34 ± 0.13
ECDSA Sign	5.14 ± 0.19	27.75 ± 0.19	9.28 ± 0.18	50.10 ± 0.16
ECDSA Verify	10.20 ± 0.19	55.08 ± 0.19	18.51 ± 0.19	99.96 ± 0.19
ECIES Encrypt	5.98 ± 0.15	32.28 ± 0.06	9.41 ± 0.18	49.23 ± 0.16
ECIES Decrypt	4.96 ± 0.19	26.79 ± 0.19	-	-

Content

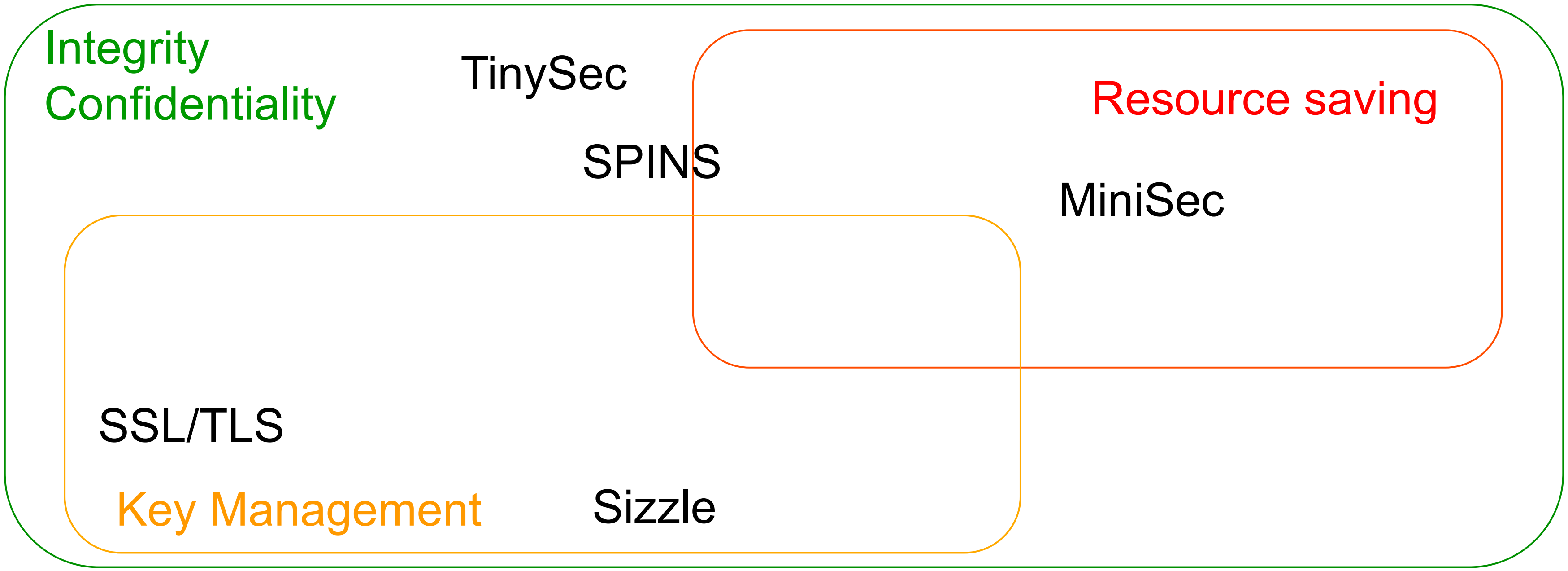
- SecureWSN
  - Research motivation
  - SecureWSN architecture
  - Hardware
- Two-way Authentication Solutions
  - TinyDTLS
  - TinyTO
- Conclusion



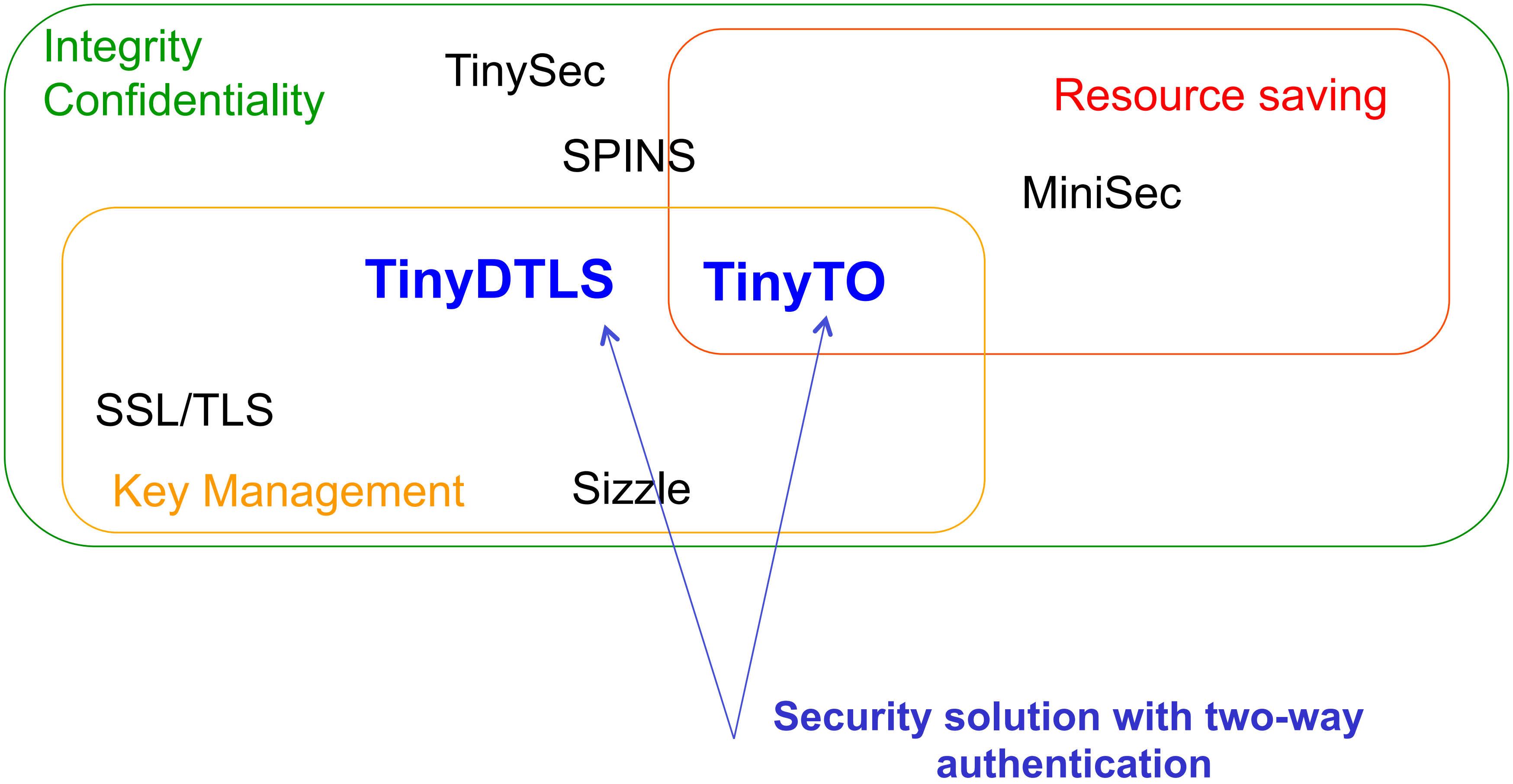
Security Comparison



Security Comparison

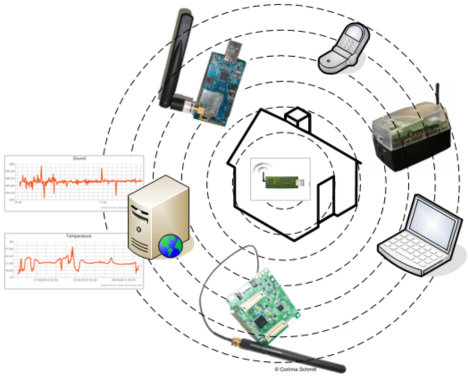


Security Comparison



Conclusion

- Secure communication is general requirement for trust.
  - Sensitive data linked every where
  - Support of security fundamentals
- Additionally, two-way authentication becomes essential
  - TinyDTLS and TinyTO for constraint devices
  - Selection depends on application and hardware resources
  - Standard-based solutions
  - Optimization possible
- Security support also required outside the WSN
  - Throughout the whole process of data publishing
  - Especially, mobile access



Publications

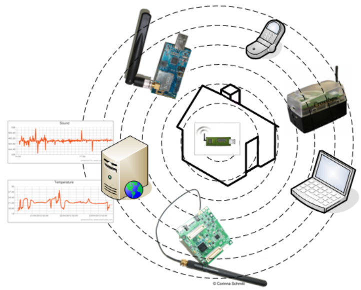
- C. Schmitt, M. Noack, W. Hu, T. Kothmayr, B. Stiller: Two-way Authentication for the Internet-of-Things. Securing the Internet of Things through Progressive Threat Detection and Management, Editors: H. Alzaid, B. Alomair, S. Almotiri, N. Nasser, Book Series on Advances in Information Security, Privacy, and Ethics (AISPE), IGI Global, ISSN: 1948-9730, Approved on March 30, 2015, in press
- C.Schmitt, B.Stiller: Two-way Authentication for IoT, IETF Internet Draft, Standards Track, ACE, Version 01, draft-schmitt-ace-twowayauth-for-iot-01, URL: http://tools.ietf.org/html/draft-schmitt-ace-twowayauth-for-iot-01,December 2015
- Martin Noack: Optimization of Two-way Authentication Protocol in Internet of Things; Universität Zürich, Communication Systems Group, Department of Informatics, Zürich, Switzerland, August 2014, URL: https://files.ifi.uzh.ch/CSG/staff/schmitt/Extern/Theses/Martin_Noack_MA.pdf
- C. Schmitt, T. Kothmayr, B. Ertl, W. Hu, L. Braun, G. Carle: TinyIPFIX: An Efficient Application Protocol For Data Exchange In Cyber Physical Systems, Journal Computer Communications, DOI: 0.1016/j.comcom.2014.05.012, June 2014
- R.Garg, C.Schmitt, B.Stiller: Investigating Regulative Implications for User-generated Content and a Design Proposal, PIK - Praxis der Informationsverarbeitung und Kommunikation. Vol. 36, No. 4, pp. 1-11, ISSN (Online) 1865-8342, DOI: 10.1515/pik-2013-0042, December 2013
- T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, G. Carle: DTLS based security and two-way authentication for the Internet of Things. Journal Ad Hoc Networks, ELSEVIER, Vol. 11, Issue 8, pages 2710-2723, DOI: 10.1016/j.adhoc.2013.05.003, November 2013
- C.Schmitt: Secure Data Transmission in Wireless Sensor Networks, Dissertation, Series Network Architectures and Services (NET), Chair for Network Architectures and Services, Technische Universität München, ISBN: 3-937201-36-X, ISSN: 1868-2634 (print), ISSN: 1868-2642 (electronic), DOI: 10.2313/NET-2013-07-2, NET 2013-07-2, Series Editor: Georg Carle, Technische Universität München, Germany, July 2013

- More under https://corinna-schmitt.de/publications.html

Acknowledgement

http://www.smartenit.eu

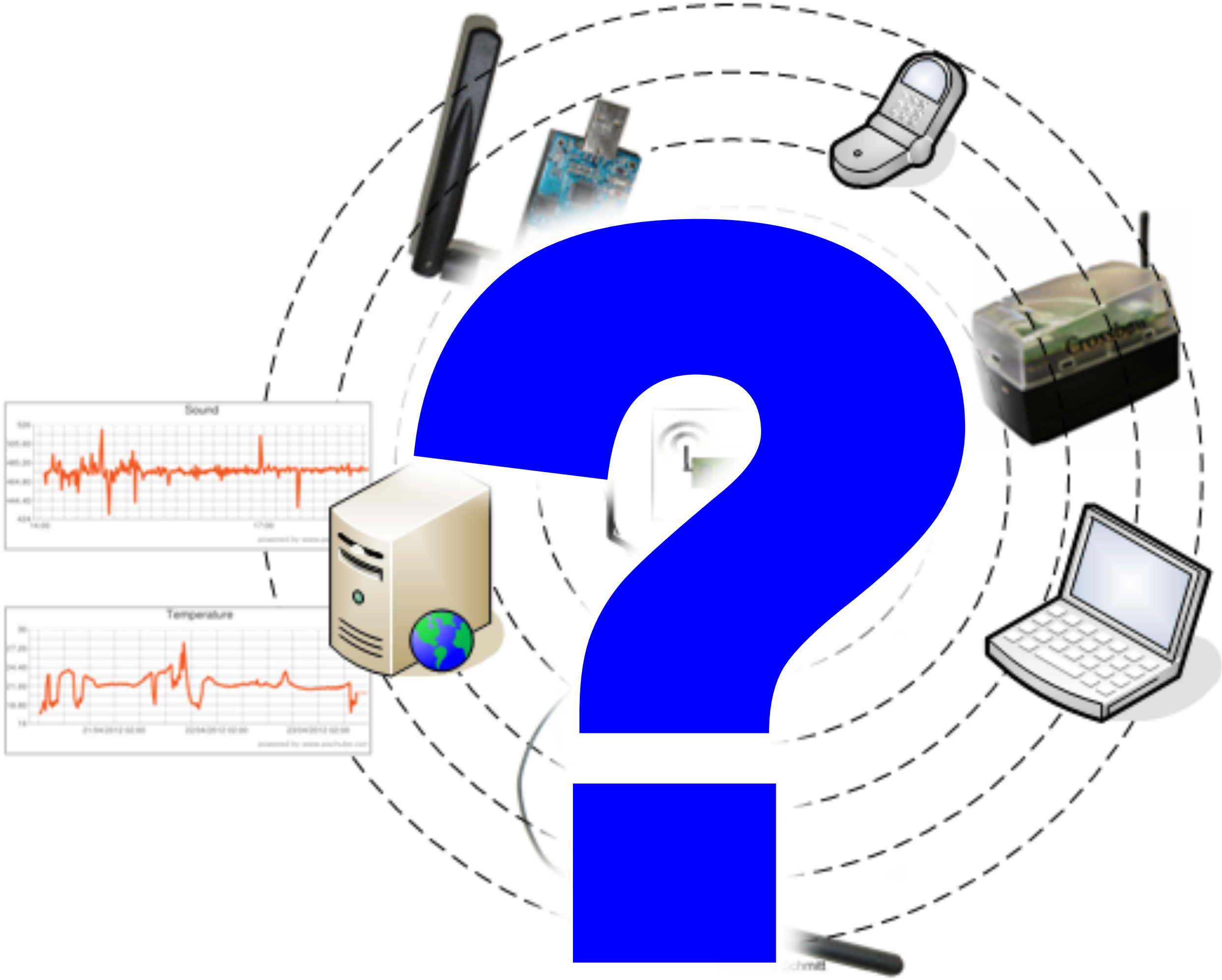
http://www.fp7-flamingo.eu



Thomas Kothmayr and Martin Noack

all@CSG
all@SecureWSN

Thanks ...



http://www.csg.uzh.ch/research/SecureWSN.html