



AWISSENET



Security & Trust in Wireless Sensor Networks

Theodore Zahariadis

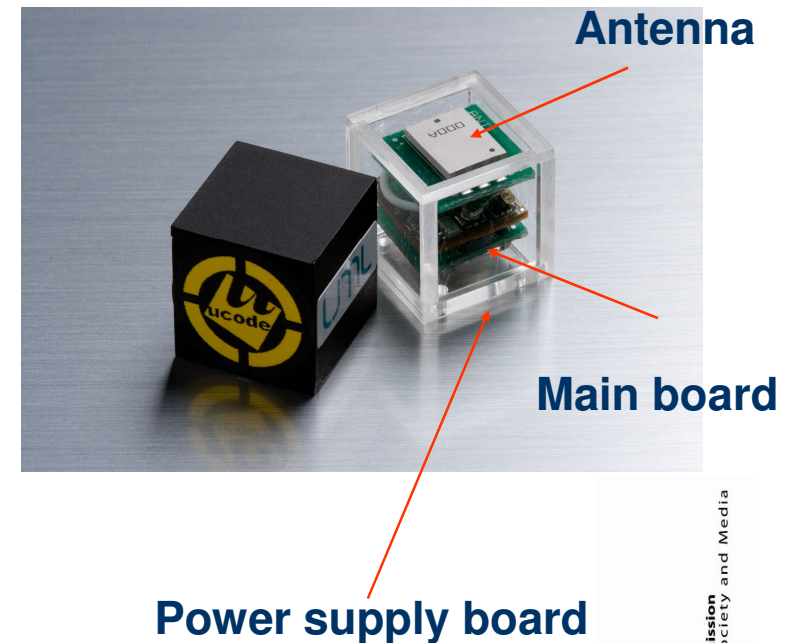


European Commission
Information Society and Media



Ultra-wide-band Sensor Node

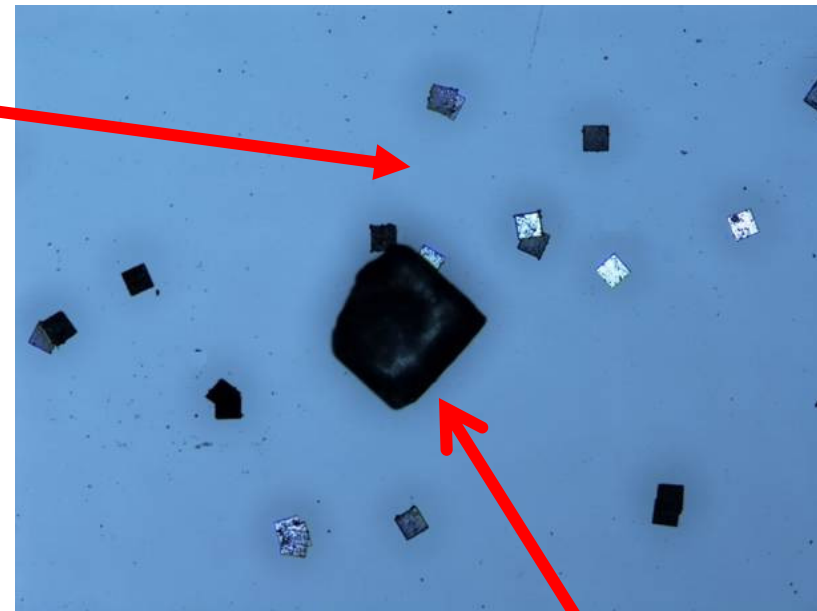
- **Ultra small sensor node**
 - The smallest UWB sensor node in the world: 10mm×10mm×10mm
 - On board temperature sensor
- **Ultra low power**
 - Low power communication: 3nW/bps
 - More than 9 years battery life using button cell (CR-2032)
(Communication every five minutes)
- **High speed communication**
 - From 250kbps to 10Mbps



Chips will be invisible

Newly developed ultra
small μ -Chip, size of 50
 μm x 50 μm
Thickness 7.5 μm

For sensors
directly embedding
into paper



Compared with crystal of granulated sugar

Wireless Sensor Networks

- Are expected to:
 - form an integral part of the foreseen Future Internet (of Things)
 - play a key role in the vision of offering mobile, personalised services, whenever and wherever needed
 - Support applications with broadband, wireless connectivity anytime and anywhere.
- **Applications:** environmental surveillance, asset management, physical phenomenon monitoring, creation of smart, interactive and immerse spaces
- However, they face essential security and resilience limitations, especially across insecure, heterogeneous and multi-administration domains

Security and Operational Requirements

- **Privacy/Confidentiality**: ensures that the data is well protected and remains secret from unauthorized parties
- **Data Integrity**: ensures that any received data has not been altered or modified
- **Data Freshness**: data is recent and old messages are not replayed.
- **Non-repudiation**: ensure that a node cannot deny sending of a message that it originated.
- **Availability of services and information**: services and information can be accessed at the time they are required, despite of the presence of attacks.
- **Network reliability**: is the capability to keep the functionality even if some nodes fail and is tightly coupled to resilience.
- **Authentication-survivability**: is the capability to verify that the data received was really sent by a trusted sender and not by an adversary that injected data in the network.
- **Self-Organization and self-healing**: is the ability to mitigate adverse situations as well as frequent nodes movement.
- **Secure Localization**: is the ability to accurately locate each sensor.
- **Scalability**: is the ability to support a large number of wireless sensor nodes.

Sensor Node Constraints

- **Energy Limitation.** Every security measure taken in order to mitigate attacks has an impact on energy consumption (encryption, hashing, overhead bits).
- **Transmission Range.** The transmission range of wireless ad-hoc/sensor nodes is limited in order to conserve energy thus allowing the nodes to restrict their transmission range.
- **Limited memory and storage capacities.**
 - TelosB: 16-bit, 8 MHz RISC CPU, 10K RAM, 48K Program Memory, 1024K FLASH
 - Mica mote2: 4 MHz 8-bit CPU, 4 KB of RAM, 128K Program memory, 512KFLASH.
- **Unattended Operation.** The nodes may be deployed in an environment open to adversaries, interference, harsh environmental conditions, etc. The likelihood that a node suffers a physical attack is much higher than in another typical network which is located in a secure place and mainly faces attacks from a network.

Network Constraints

- **Mobility and Hierarchy.** During the network mission, the composition of the network and its routing topology may change.
- **Data Rate and Packet Size.** Both data rate and packet size affect the overall sensor node energy consumption. Packet sizes are relatively small, while data rates are relatively low.
- **Unreliable Communications.** Normally the packet-based routing is connectionless and thus inherently unreliable. Furthermore, the unreliable wireless communication channel also results in damaged packets.
- **Conflicts.** Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network.
- **Latency.** The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among nodes.

AWISSENET Summary

- AWISSENET optimisations focus on four key principles:
 - **Discovery, evaluation and selection of trusted routes** based on multiple security metrics and trust measuring methods.
 - **Secure Service Discovery**, providing network-level security framework, which will protect service discovery messages inside the sensor network, when crossing unknown domains or when interacting with public service providers.
 - **Intrusion detection and intruder identification** based on distributed trust to provide security against malicious attacks.
 - **Highly Secure sensor nodes** against attacks from malicious users having actual access to the sensor nodes.
- The AWISSENET results will be packed in a security toolbox, which will be prototyped and validated in a large trial of more than 100 sensor nodes.



AWISSENET



Thank you

**Theodore Zahariadis
Synelixis Ltd**

zahariad@synelixis.com



European Commission
Information Society and Media



TRUST MODELING

Direct Trust

Forwarding (E1)	# of Success	# of Failures
Network-ACK (E2)	# of Success	# of Failures
Packet precision- Integrity (E3)	# of Success	# of Failures
Authentication (E4)	# of Success	# of Failures
Cryptography-Confidentiality (E5)	# of Success	# of Failures
Reputation RES (E6)	# of Response	# of no Response
Reputation Validation (E7)	Value	
Remaining Energy (E8)	Value	
Network ACK History Log (E9)	1 0 1 1 0 1 0 0 1 1 0 1 0 1 1 1	
Number of Interactions (E10)	Value	
Distance to the sink node (E11)	Value	

$$T_i^{A,B} = \frac{a_i S_i^{A,B} - b_i F_i^{A,B}}{a_i S_i^{A,B} + b_i F_i^{A,B}}$$

$$T_8^{A,B} = \frac{a_8 V_{now} - b_8 V_{initial}}{a_8 V_{now} + b_8 V_{initial}}$$

$$C^{A,B} = 1 - \frac{1}{noi + a_{10}}$$

$$DT^{A,B} = C^{A,B} \left(\sum_{i=1}^k W_i * T_i^{A,B} \right)$$

TRUST MODELING: Indirect & Total Trust

Direct Trust Value of responding node DT^{A, N_j}	Value	
Reputation RES	# of Response	# of no Response
Reputation value of responding node $DT^{N_j, B}$	Value	
Reputation Correctness History Log	1 0 1 1 0 1 0 0 1 1 0 1 0 1	

$$IT^{A,B} = \sum_{j=1}^n W(DT^{A, N_j}) DT^{N_j, B}$$

Total Trust

$$TT^{A,B} = W(DT^{A,B}) DT^{A,B} + W(IT^{A,B}) IT^{A,B}$$