Annual review FLORENCE 2013

WP4 – Network: prototypes

WP4 prototypes

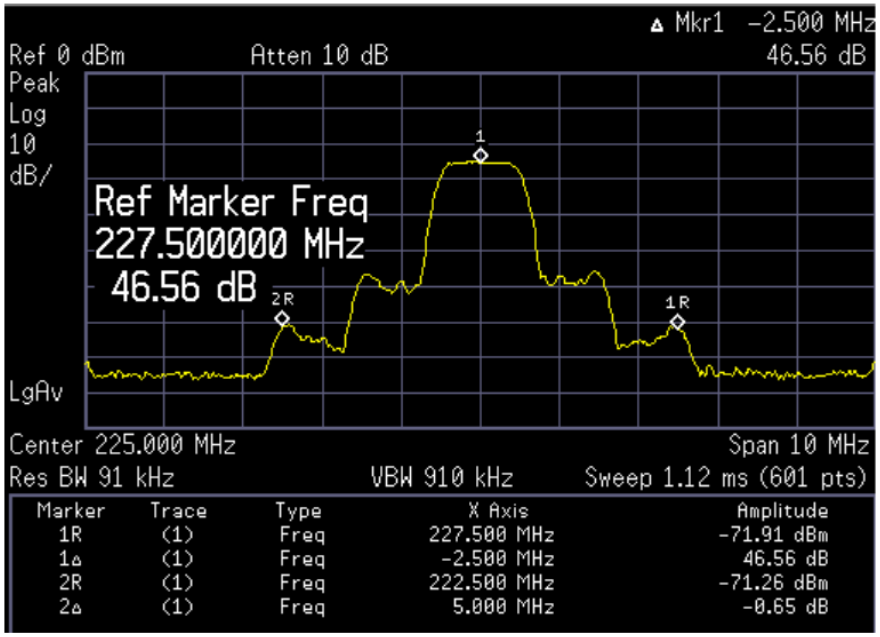
- Task 4.1 Smart SPD driven transmission
  - P1: SPD-driven Smart Transmission Layer
- Task 4.2 Distributed self-x models
  - P2: Recognizing and Mitigating DoS Attacks
  - P3: Model-based Framework for Dependable Distributed Computation
- Task 4.3 Reputation-based resource management technologies
  - P4: Reputation-based Secure Routing
  - P5: Intrusion Detection System
- Task 4.4 Trusted and Dependable Connectivity
  - P6: Link Layer Security
  - P7: Network Layer Security
  - P8: Access Control in Smart Grid Networks

nSHIELD

SPD-driven Smart Transmission Layer (1)

- Test bed prototype consists of:
  - 2 SDR-capable nSHIELD Power Nodes (OMBRA v2)
  - 2 SE HandHeld devices
  - Auxiliaries

SPD-driven Smart Transmission Layer (2)

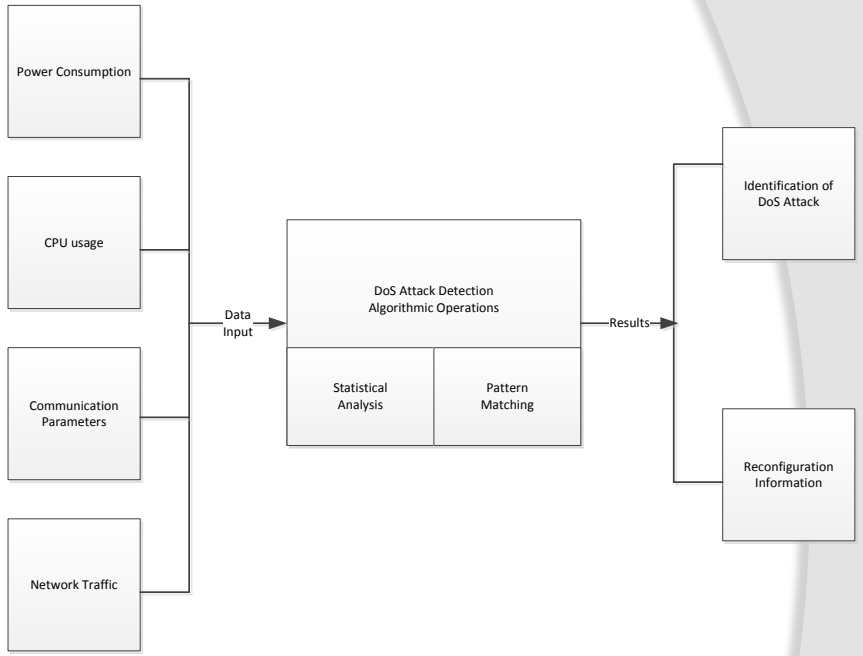


- Four functionalities have so far been implemented and studied:
  - Remote control of the radio
  - Waveform analysis
  - Interference detection
  - Spectrum sensing

nSHIELD

Recognizing DoS attacks (1)

- Statistical analysis and pattern matching algorithms analyze power consumption, CPU usage and network status
- Correlation of all inputs can detect abnormal situations (DoS attack notification)
- Correlated Patterns can be matched to database of normal and abnormal scenarios



- The main output of the algorithm is the detection alarm but reconfiguration commands can be issued with proper training

nSHIELD

Recognizing DoS attacks (2)

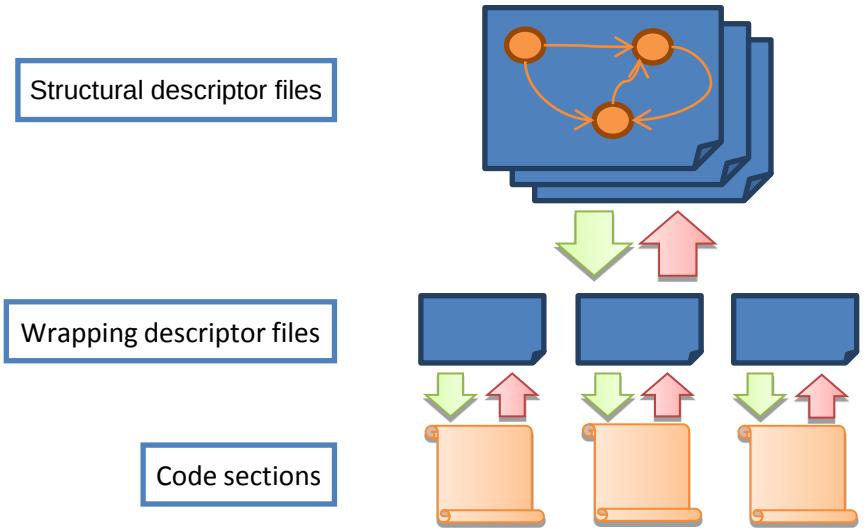
	CPU abnormalities	Power abnormalities	Traffic abnormalities
Detection Accuracy	70%	60%	50%
False positives	15%	20%	15%

- Algorithms and network simulated in OMNET++ and MiXiM platforms
- Initial simulations point to a good detection accuracy although real world implementation needed
- Porting to the BeagleBone family of platforms under way

nSHIELD

Model-based framework for dependable distributed computation (1)

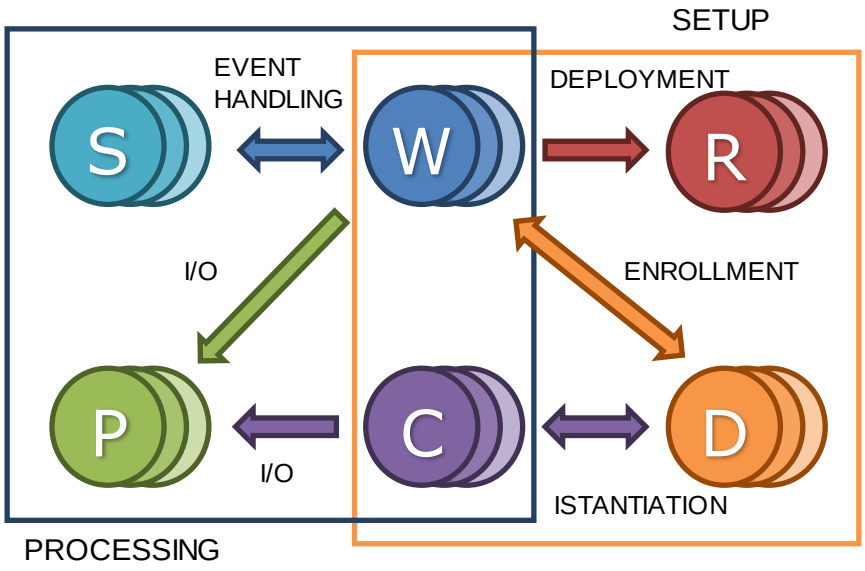
- Abstracts an application using a dataflow metamodel
- Enables mixed-language mixed-architecture distributed processing
- Simplifies safe component reusal



nSHIELD

Model-based framework for dependable distributed computation (2)

- There exist multiple *roles*, with possibly multiple nodes taking each one
- The worker (W) role is taken by embedded devices
- All roles except the client (C) may be taken by server(s)



Reputation-based Secure Routing (1)

- Distributed ad-hoc systems: each entity depends on its neighbors to accomplish full communication among all participants.
- Trust and Reputation: important mechanisms for correct routing behavior
- Counter action against several routing attacks: Black-Hole, Gray-Hole, Bad mouthing

Reputation-based Secure Routing (2)

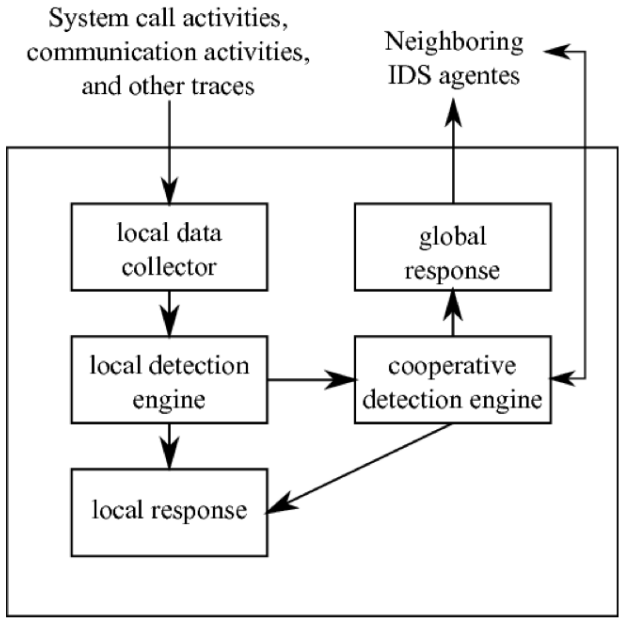
- Hardware Platform: Memsic IRIS
- Operating System: TinyOS 2.x
- Routing Protocol: Greedy Perimeter Stateless Routing
- Trust Module: configurable SPD Level

SPD Level	Nano
1 (lowest)	-
2 (low)	DT (Direct Trust)
3 (medium)	Weighted DT (Direct Trust) + ID (Indirect Trust)
4 (high)	Weighted DT + ID + Beta distribution

nSHIELD

Intrusion Detection System (1)

- Local detection uses Specification-based and Reputation and Trust detection techniques
- Cooperative detection uses Reputation and Trust techniques only.



- Reputation and Trust techniques use direct (first-hand) and indirect (second-hand) information.
- Using a Bayesian model for Reputation and Trust management.

nSHIELD

Intrusion Detection System (2)

- A considered IDS is based on nodes' cooperation in a fully distributed environment

REPUTATION TABLE		
Node ID	α	β
⋮	⋮	⋮
Node ID	α	β

FIRST-HAND INFORMATION TABLE		
Node ID	α	β
⋮	⋮	⋮
Node ID	α	β

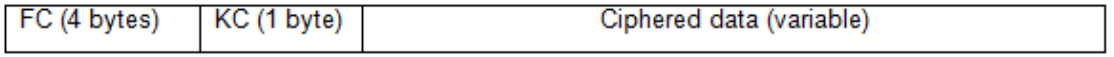
TRUST TABLE		
Node ID	α	β
⋮	⋮	⋮
Node ID	α	β

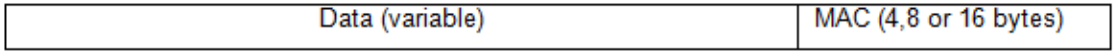
- Proposed IDS prototype consists of a number of wireless sensors sending information to the base station via gateway
  - Platform of choice is Zolertia Z1 running Contiki

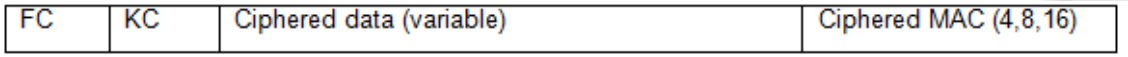
nSHIELD

Link layer security (1)

- 802.15.4 provides four basic security services:
  - Access control
  - Message integrity
  - Message confidentiality
  - Replay protection
- Security algorithms supported
  - CTR
  - CBC-MAC
  - CCM

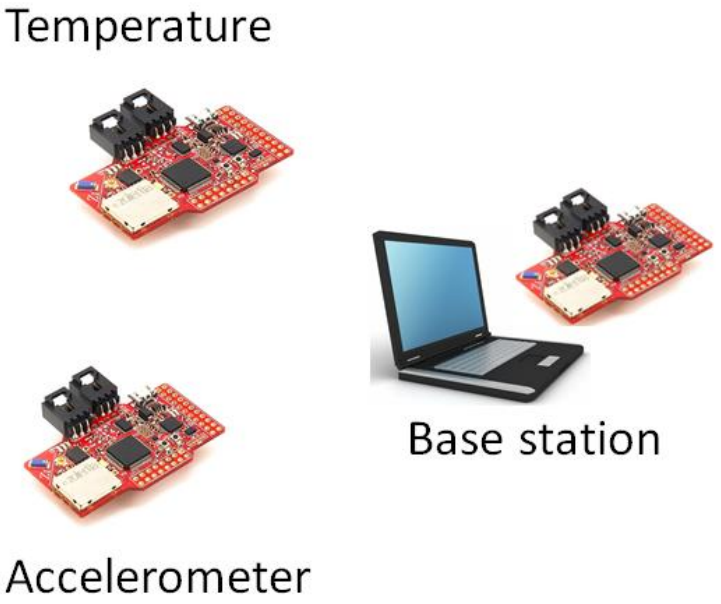


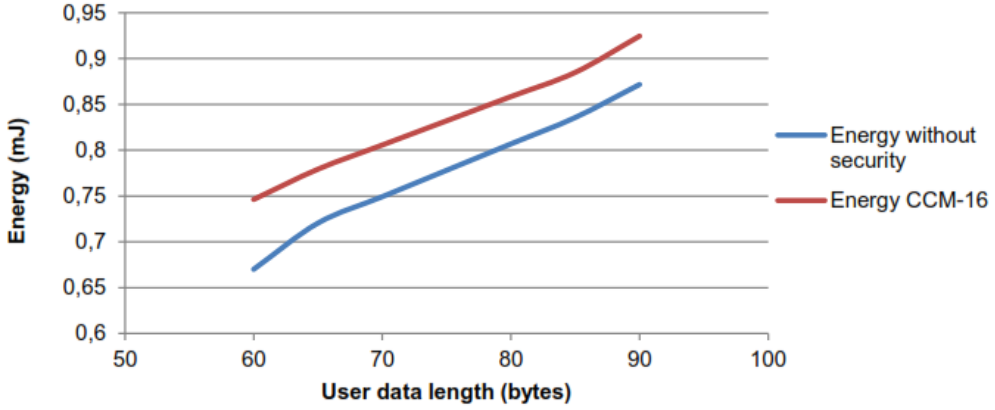




Link layer security (2)

- Two sensors sending information to the base station
  - Without security
  - TinyOS hardware security CCM-16



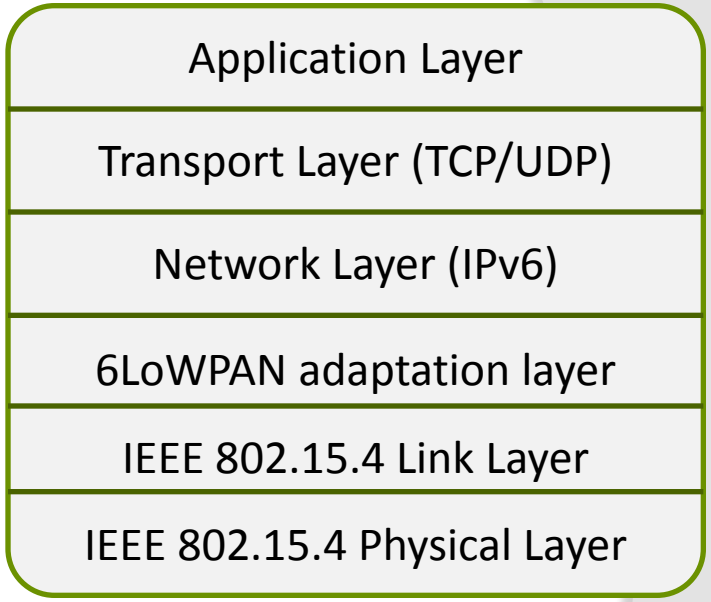


Network layer security (1)

- IPSEC can be the solution for securing messages at the IP layer for
  - Routing protocols
  - End-to-end security where DTLS would not apply, e.g. TCP-based cross-boundaries communications
  - Any application
- IPSEC provides:
  - Confidentiality
  - Message authentication
  - Message integrity

Network layer security (2)

- 6LoWPAN adaptation layer
  - requires **header encoding**
- IPsec utilizes underlying AES_CCM* (found on IEEE802.15.4 chips)
  - CCM (Counter with CBC-MAC) is an **authenticate-and-encrypt** block cipher mode
  - Authenticated ESP. No need for AH overhead
  - Also provides encryption-only and integrity-only capabilities



nSHIELD

Access control in Smart Grid Networks

- Smart grids – fundamental infrastructure for energy distribution across cities

- Access control and encryption are studied in order to ensure security in network layer within low voltage domain

nSHIELD

The END

That’s all folks!

ARTEMIS