
L. Pomante, M. Pugliese, S. Marchesani, F. Santucci

University of L’Aquila – ITALY
Center of Excellence DEWS
{luigi.pomante, stefano.marchesani, fortunato.santucci}@univaq.it,
marco.pugliese@ieee.org

IWCMC 2013, Cagliari, July 3rd
Outline

• Background & motivations
• A service-based modular architecture
• The WINSOME platform components
  – WIDS
  – TAKS/ECTAKS/TAKS2
• The WINSOME platform
• Conclusions and future work
Background & motivation

- **WINSOME** (Wireless sensor Network-based Secure system for structural integrity Monitoring and Alerting) provides secure monitoring services, supported by flexible and cheap systems, in areas where ordinary networks are unsuitable.

- Wireless Sensor Networks represent a promising technological solution but resource constraints and exposure to external attacks could limit their employment.
Background & Motivation

• In such a context, this work focuses on design and implementation issues of a security framework suitable for monitoring applications that rely on WSNs

• We have exploited the *Platform-Based Design* methodology to define a *Secure Platform*
  – Clear separation of functional and architectural aspects
A service-based modular architecture

- Secure Link Generation
- Anomaly Detection
- Node Authentication
- Data Processing
- other services

Application $A_1$, Application $A_2$, ..., Application $A_n$

e.g. data transmission

e.g. intrusion detection

e.g. system monitoring

underlying WSN
The WINSOME platform components

• Network security issues
  – System Availability
  – Data Confidentiality, Integrity and Authentication

• WINSOME solution through the following components
  – Intrusion Detection System (IDS)
    • Based on Weak Process Models (WPM)
  – Cryptographic Scheme (CS)
    • Based on Topology Authenticated Key Scheme (TAKS)
Intrusion Detection System

**WIDS**
- Misuse-based approach
- Threats are modeled with WPM
WIDS: WPM-based IDS

TAKS/ECTAKS/TAKS2

- Cryptographic scheme defined at DEWS and specifically designed for WSN because
  - Hybrid cryptography
  - Authentication and key generation are based on network topology, a key concept in WSN
    - Suited for dynamic network topologies
    - Suited for clustered WSN (gen. of clusterwise keys)
  - No need of a centralised Certification Authority
  - It does not need any key agreement protocol
The WINSOME Platform (1)

- Clustered WSN
- Functionality accomplished by
  - Static SW components (SWC) or
  - Dynamic SW components (DSWC) as mobile agents
- We have exploited the AGILLA middleware
  - Tuple Space
  - Neighbor List
  - Agent Migration
The WINSOME Platform (2)
The WINSOME Platform (3)

[Diagram showing the AGILLA Application Execution Environment (AAEE), Secure Platform, TinyOS, and WSN protocol stack with Mobile Agent A_1, Mobile Agent A_2, IRL/IRLA, Tuple Space, Neighbor List, AGILLA Manager, SW component, TAKS / ECTAKS, WIDS, TinySEC / TinyECC, and TinyOS.]
The WINSOME Platform (4)
The WINSOME platform (5)

• Performance evaluation
  – Cryptographic Scheme
    • Implementation on MicaZ with 128-bit keys using CBC, CBC-MAC with Skipjack as block cipher
    • Transmission phase: 15.42 ms
    • Reception phase: 8.34 ms
  – IDS
    • Estimation from data above on WPM modelling 3 types of threat
    • Score generation: 1-10 ms
Conclusions and Future Work

• We have presented an agent-based Security Platform for WSN Monitoring Applications (WINSOME)
  – Security functions are executed directly by nodes and complexity in IDS management is reduced due to the use of mobile agents and clustered tree topology
• Currently we are carrying on early experimentations on MicaZ and working on the full implementation of the proposed architecture

• WINSOME has been motivated and supported by the ESF-COST Action IntelliCIS
• The development of the middleware platform also fits in the frame of the Projects “Ricostruire” and “SMILING” supported by the Ministry of Economic Development to enhance technology transfer in the RIDITT framework.
Previous works related to WINSOME

About TAKS/ECTAKS/TAKS2


About WIDS


About WINSOME design and implementation

Thank you for the attention