Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?

Cristina Alcaraz, Pablo Najera, Javier Lopez, Rodrigo Roman

Presented by Alexander Witt and Aniket Shah

Overview

- Introduction
- Security Integration Challenges
- Integration Approaches
- Demystifying the TCP/IP solution issues
- Case Study
- Technical Overview
- Conclusion
- Critical Review

Introduction

- WSN – an important element in IoT paradigm; facilitates collaboration of heterogeneous information systems and services
- Many companies have bought into the above idea, working to find solutions. E.g. : A Smarter Planet by IBM, CeNSE by HP Labs
- Integration with the Web; 6LoWPAN uses IPv6 for web services such as SOAP and REST
- Many challenges associated with this sector such as security, physical and virtual connections; especially between WSN and the Internet, etc.

Security Integration Challenges

- WSN in IoT raises security challenges; paper focuses on connections at network level
- Security needs to be considered at a global perspective, not just local
  - Ensures the curbing of additional requirements to integrate local nodes on a global scale
- Security is an important factor as it helps user perceive control over information and not vice versa
- Data privacy is another important feature
  - Segregation of shared and private data
  - Confidentiality in business scenarios

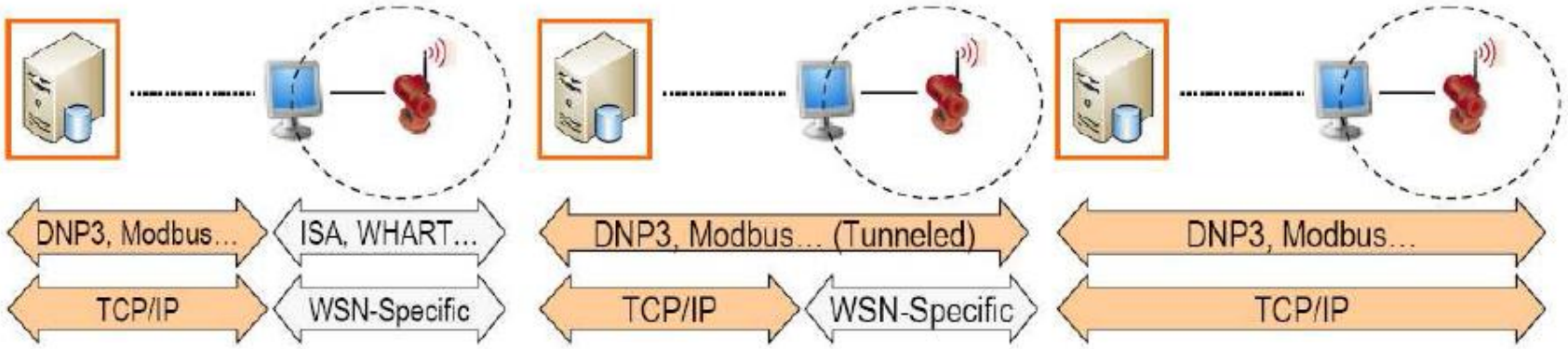
Security Integration Challenges

- Another significant aspect under consideration is Component security
  - Security protocols at network level
  - Interaction between objects and services
- Objects and infrastructures of an IoT network should be able to handle several identification and security mechanisms in a transparent and scalable way
- Need to reach equilibrium point in secure interactions is an interesting problem

Integration Approaches

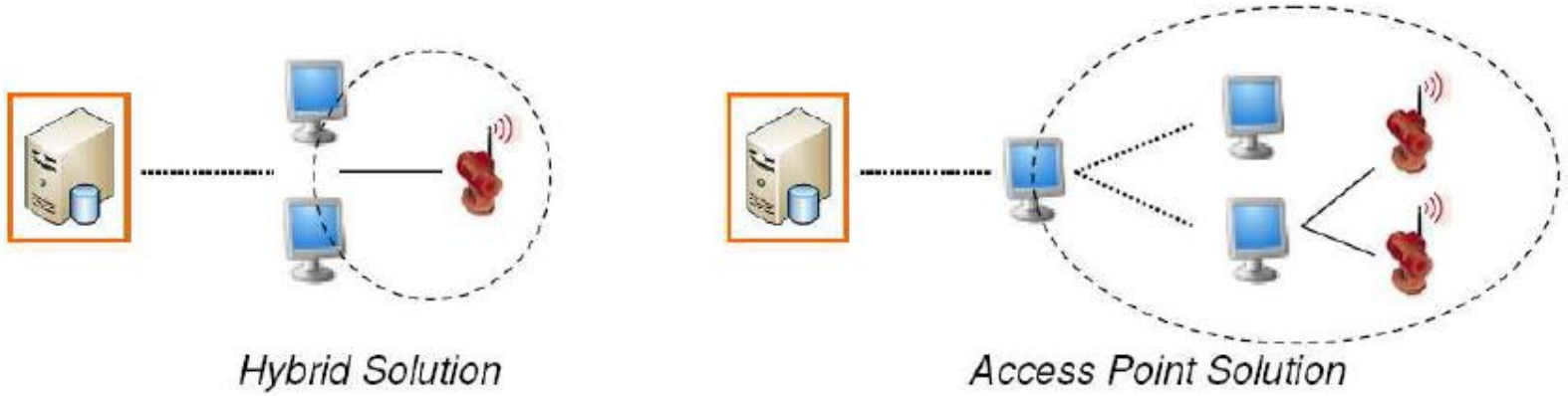
- For network design, it is necessary to know the integration approaches to connect to both infrastructures of WSN and the Internet
  - Classification: Stack based or Topology based
- Stack based: integration level depends on similarities between network stacks of WSN and Internet
  - Classification: Front End, Gateway or TCP/IP
- Topology based: integration level depends on actual location of nodes
  - Classification: Hybrid or Access Point

Integration Approaches



Stack-Based Approaches

[Fig. 1]



Topology-Based Approaches

Stack-based Classification

- *Front-end solution*: WSN independent from the Internet
  - Implements its own protocols
  - All interaction managed by a centralized base station
- *Gateway solution*: WSN can exchange information with Internet hosts
  - Internet hosts and sensor nodes can address each other indirectly through a gateway
  - Base station acts as application layer gateway; translating lower layer protocols and routing information
- *TCP/IP solution*: WSN shares a compatible network layer protocol
  - Sensor nodes implement TCP/IP (or 6LoWPAN) to become a part of the Internet
  - Sensor nodes may not be able to use specific WSN protocols

Topology-based Classification

- *Hybrid solution*: Dual sensor nodes located at root of the WSN
  - A set of nodes located at the edge can access the Internet directly and become base stations
  - This approach provides redundancy and network intelligence
- *Access Point solution*: Backbone of devices that allow sensing nodes to access the Internet in a single hop
  - WSNs become unbalanced tree with multiple roots (sensor nodes with Internet enabled nodes)
  - Increases capabilities of nodes in the backbone network
- In most cases, Topology based networks are combined with Stack based classification except for the TCP/IP solution

Demystifying the TCP/IP solution issues

- TCP/IP provides best solution to integrate WSN and the Internet
  - External system can access node information directly
  - Nodes can query Internet for services
- Multiple factors to be considered for complete integration
  - Existing issues may affect WSN whose nodes are completely integrated into the Internet
  - More challenging to assure security of WSNs that make use of the TCP/IP solution

Factors determining integration approach

- *Resilience*: Security mechanisms to increase robustness against attacks (such as Denial of Service)
- *User Authentication and Authorization*: Permission storage; consider implementing single sign-on systems
- *Communication Security*: Analyze other secure communication channels (e.g. TLS); study different key exchange mechanisms
- *Accountability*: Be able to record interactions with user; will help recreate security incidents and abnormal situations

Factors determining integration approach

- *Functionality*: Some nodes need not be aware of the Internet due to limited functions (tasks)
- *Hardware*: Certain nodes may not connect to the Internet directly due to memory constraints of security mechanisms
- *Inherent weakness*: Decide whether certain applications should isolate nodes from the Internet; filtering traffic at the network edge
- *Network redundancy*: Necessary to develop mechanisms in TCP/IP environments to deal with exceptions such as unreachable nodes
- *Protocol optimization*: Most protocols allow a network to self-heal and optimize internal behavior; yet to be found for 6LoWPAN networks

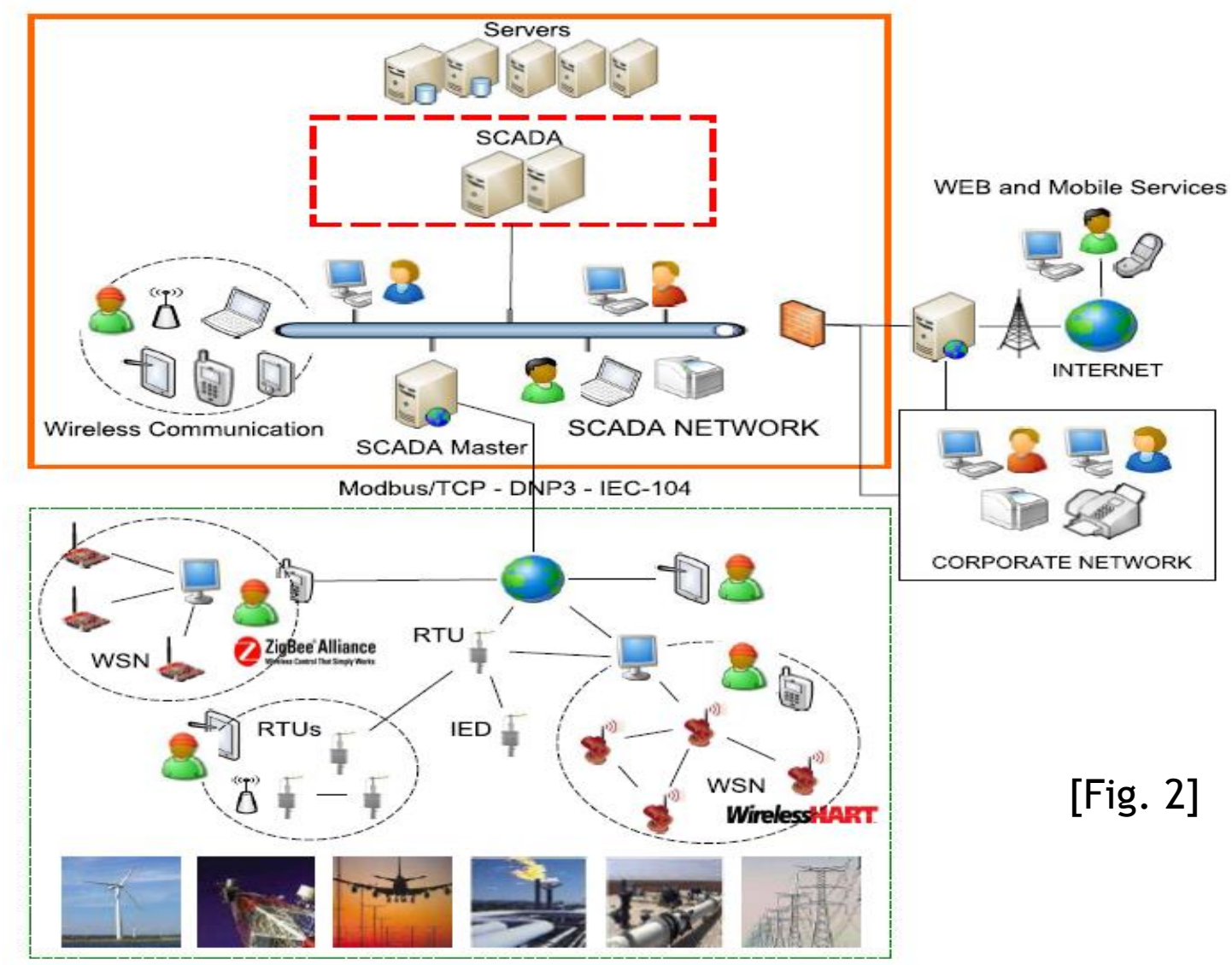
Case Study – SCADA Systems and First Responders

- Pure TCP/IP integration solution has certain limitations, especially in terms of security
- Application requirements determine the type of integration solution
- Two sensor network applications analyzed:
  - WSN enabled SCADA system
  - First Responder system

SCADA Systems

- SCADA – Supervisory Control and Data Acquisition system
- Uses new technology to monitor many critical infrastructures in real time
- Main elements of a SCADA system:
  - Central control systems – remote monitoring of infrastructures by humans
  - Remote subsystems – located within the infrastructure; provides data/ information from various elements of the infrastructures

SCADA Network Architecture



[Fig. 2]

SCADA Systems

- Migration to IP for automation has increased with TCP/IP real time monitoring and communication
- Led to development of hybrid technologies (e.g. Bluetooth, Wi-Fi, Zig-Bee, WSNs, etc.)
- WSNs considered as key technology
  - Smart and autonomous
  - Auto-configuration
  - Self monitoring and self-healing
  - Anomaly detection and tracking

SCADA Systems

- Industrial applications have led to various products
  - MeshNetics nodes (Zig-Bee) launched SensiLink Integration platform
  - Cooper Power Systems' wireless Outage advisor for Electric power systems
  - Sensus' FlexNet SmartPoints for power systems
- Interoperability of products is based on industrial standards such as ZigBee, WirelessHART and ISA100.11a (based on the IEEE 802.15.4-2006 standard) which specifies the PHY and MAC layers of WPANs
- Main goal of these standards
  - secure connectivity
  - energy saving using a wireless mesh network
  - interoperability with other systems
  - data reliability

First Responder Systems

- Sensor networks play disaster response roles such as monitoring, tracking, triage etc. Hence the name first responder systems
- Creates and maintains information structure when other communication and support system not available
  - Reason: Dynamic and autonomous nature of WSN
- Many advantages of WSN-base first responder system integration with the Internet
  - Network at disaster location helps visualize distant evets
  - Global view of disaster situation
  - Interaction with centralized situation to optimize task distribution

Analysis

INTEGRATION SOLUTIONS AND APPLICATIONS

	Overview	SCADA	FIRST RESPONDERS
TCP/IP	→ Distributed mechanisms × Device overhead × Weak to external attackers ✓ Resilient to device failure ✓ Direct access to the devices	→ Long lifetime: must support multiple protocols → Devices do not need to be Internet-aware × Critical Environment × SCADA-specific protocols provide extra properties	✓ Short lifetime: deployment-specific protocols ✓ Devices can take advantage of Internet-awareness
FRONT-END	→ Centralized management × Single point of failure ✓ Store and Forward, Redundancy	→ Increase access points to improve robustness ✓ Isolation of the sensor devices	→ No need for redundancy → Extra access points might not be available × Node Isolation might be counterproductive
GATEWAY	→ Mixed Architecture × Single point of failure ✓ Application-Layer access	→ Increase access points to improve robustness → Some intelligence should be pushed to the devices	→ Extra access points might not be available

[Table 1]

Analysis

- For SCADA systems, benefits of pure TCP/IP solution don't warrant complete integration of WSN with the Internet
- Increase in network traffic can become problematic for WSN nodes due to their limited capabilities
- Existence of a central entry point makes the Gateway solution vulnerable against availability attacks. This can be solved by using the Hybrid and Access Point solutions
- TCP/IP solution for First responders works well as there is limited overhead on nodes
- Benefits associated with Front-end and Gateway solutions for First responder systems are not so important in these emergency scenarios

Technical Overview

- Different technologies used to protect a WSN
  - Cryptographic primitives (ECRYPT Stream Ciphers, PKC ECC, Rabbit)
  - Attestation and detection systems
  - Key management systems
- Security technologies being developed
  - Secure routing
  - Time synchronization
  - Trust management
  - Secure middleware
- Essential for protection to nodes (in nodes or inside routers / base stations)

Conclusion

- Full integration at the network level may not be necessary
- Some applications should not connect their nodes directly to the Internet
- There are more security issues when integrating WSN with the IoT:
  - Integration of security mechanisms & services
  - User acceptance
  - Management of data privacy

Critical Review

- Good indication of tradeoffs existing in different approaches to integration
- Do not impose a doctrine for good IoT security but discuss security attributes
- Discuss attributes of the environment that may influence scheme selection
- The paper is organized well but could explain certain sections better
- Discuss TCP/IP connectivity to the Internet
  - Do not mention if battery life is a constraint to consider (are WSNs wired or not)
- Good bearing on the value of cryptographic primitives in IoT
  - Lightweight Simon & Speck block cipher undergoing standardization

Thank You