TEXAS A&M UNIVERSITY

"Study on Security of Wireless Sensor Networks in Smart Grid“

Authors: Yufei Wang, Weimin Lin, Tao Zhang

Presented By: Jeff Jensen

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Roadmap

- A brief introduction
- Why wireless security?
- Past and relevant work
- So, what’s the problem?
- A suggested solution
- Further analysis
- My assessment
- The Future?
- References and Questions

Motivation = Smart Grid

- All encompassing grid < == > diverse landscape
- Devices need to talk to one another, not all devices connected easily by wire – network congestion problems
- Must merge traditional systems (SCADA, control networks, etc.) with emerging network technologies
- IT wiring doesn't currently go everywhere
- Wireless networks allow physical location to be nearly discretional
- ➔Application Specific Security

Wireless Sensor Networks (WSNs) and Security

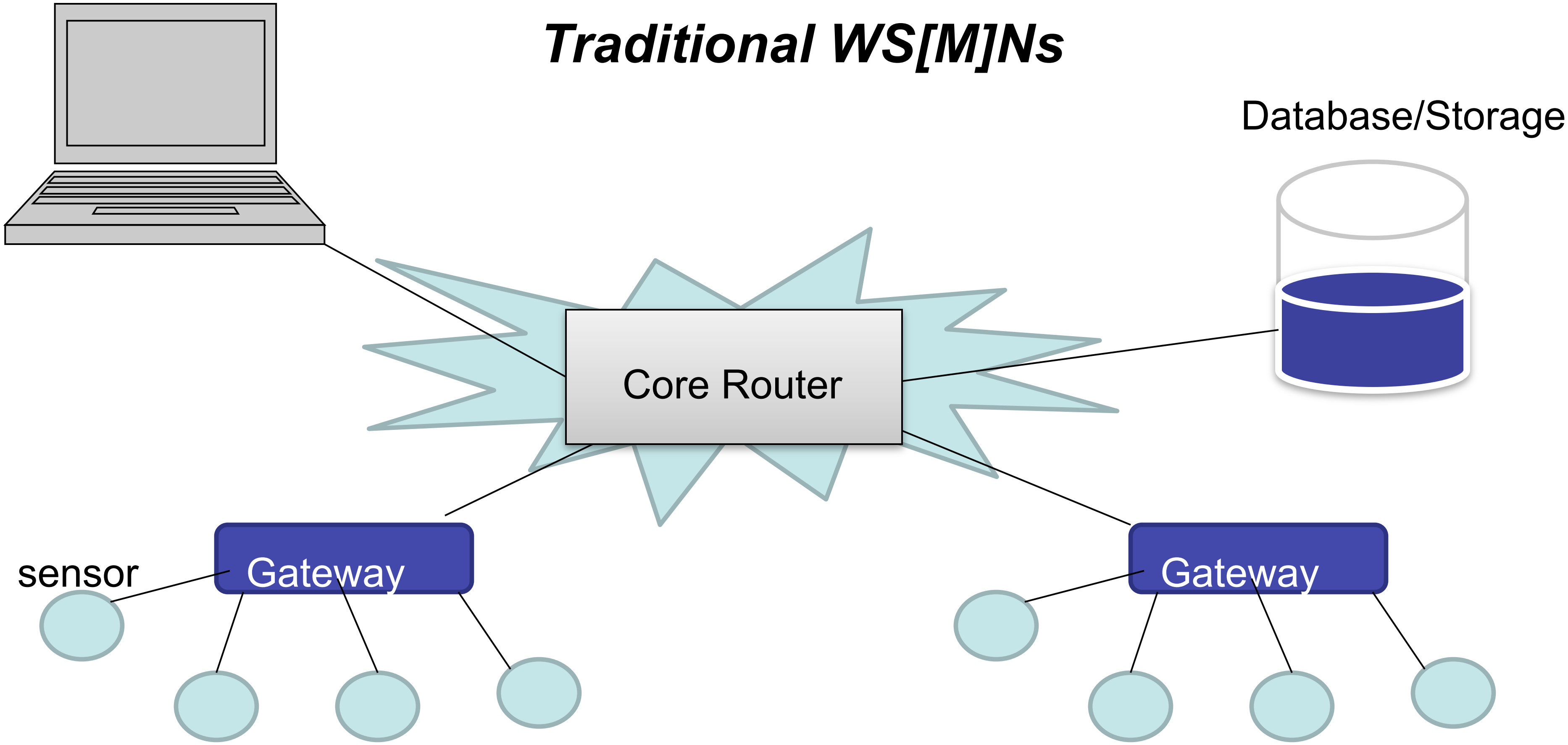
Wireless Sensor Networks (WSNs)

- Sensor networks capture valuable data for controlled networks, ***integral*** to smart grid development
- Wireless Multimedia Sensor Networks include various high-tech researched sensors, multimodal cameras (radiation detection, sunlight, wind, temperature, etc…)
- $Low Cost compared to wired counterparts (wiring cost included)
- Currently Utilized in military applications, environmental monitoring, commercial and human centric applications
- ➔ Smart Grid = Energy viewed as a necessity in society i.e. human centric applications
- Smart Grid is about information – sensors provide all the information

Traditional WS[M]Ns

- Rapidly interconnect with one another through distributed network nodes and interconnect protocols – one collection node down will not influence whole network
- Redundant sensors are deployed, densely populated for more accurate information
- Resources are constrained (processing power, communication range, communication bandwidth
- Multi-hop sensor node routing (not sensors themselves), intermediate nodes serve as routers
- Able to self heal from a node failure quickly
- Must have strong physical security, enough to prevent intrusion or data leak
- Application specific and data-centric (sensor networks gather information)

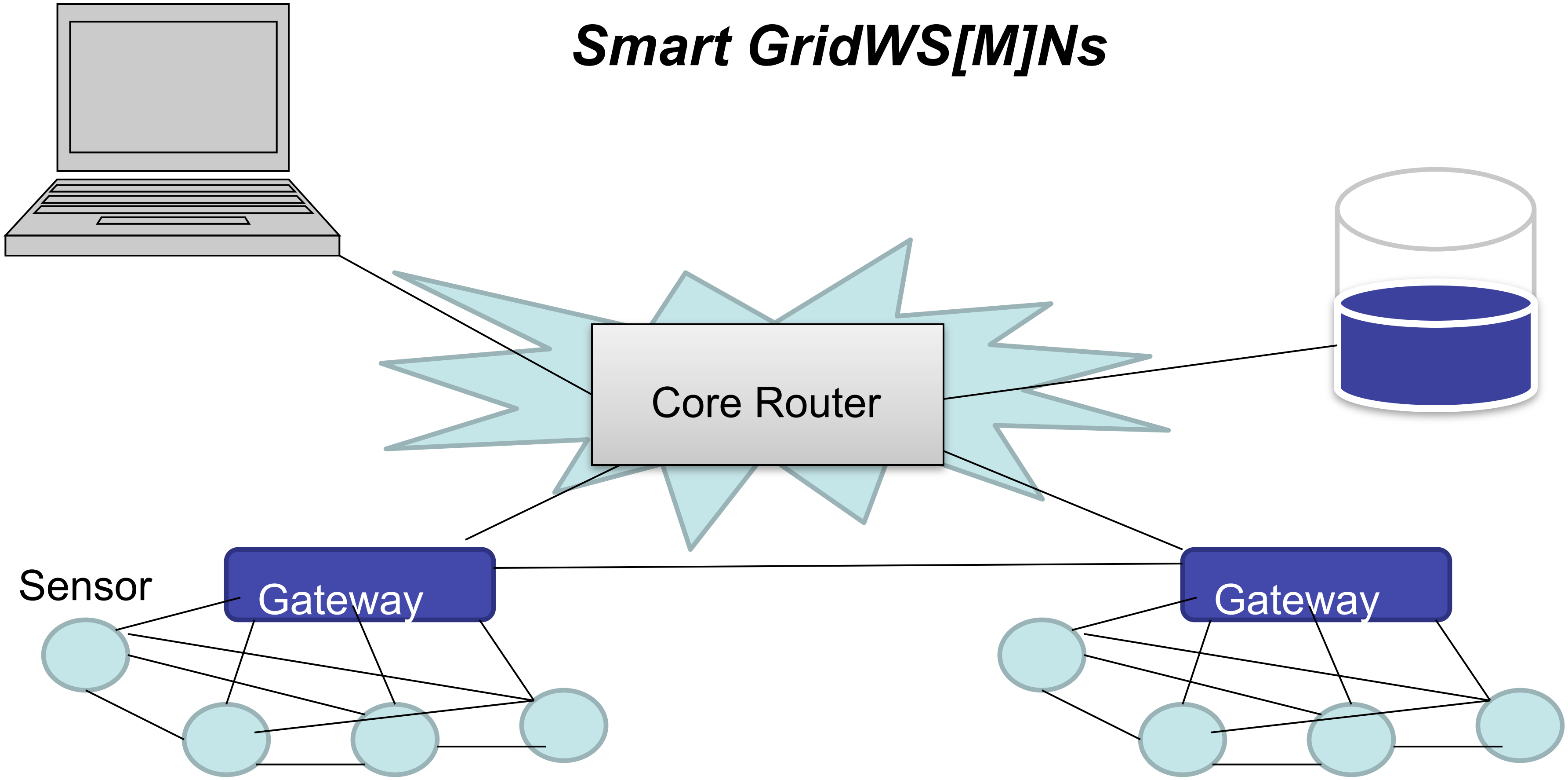
Traditional WS[M]Ns



Smart Grid WS[M]Ns

- Deployment topology will most likely not use a single hop to transmission gateway
- Data Processing – all data should be forwarded directly to control station
- Technology advancement in energy – less sensitive energy usage = less concern for protocols and algorithms because battery life significantly longer
- Remote maintenance and configuration
- Harsher electrical deployment environments
- Quality Of Service (QOS) for application specific WSNs becomes difficult to prioritize
- ➔High security requirements

Smart GridWS[M]Ns



Highlighting the Differences

Traditional WS[M]Ns	*Smart Grid WS[M]Ns*
One hop transmission from gateway	Multiple sensor hops before transmission
Physical Reconfiguration of devices	Remote Reconfiguration of devices
Relay data information through routers	Data processing, QOS and delivery highly important
Secure enough to prevent information leaks (reactive)	Highly secured, (proactive) security

Wireless Security

- ➔ Security is application specific, needed pillars for security structure
- Authors present 4 Concentrated Areas in wireless security:

  (1) Trust of Control Systems

  (2) Communication and Device Security

  (3) Privacy

  (4) Security Management
- Protect these to uphold benefits that WSNs provide the smart grid
- Each addresses a different aspect of the smart grid (Device, Consumer and Distributor)

Highlighting the Differences Again

Traditional WS[M]Ns	*Smart Grid WS[M]Ns*	
One hop transmission from gateway	Multiple sensor hops before transmission	*Control Systems*
Physical Reconfiguration of devices	Remote Reconfiguration of devices	*Devices and Comm*
Relay data information through routers	Data processing, QOS and delivery highly important	*Privacy*
Secure enough to prevent information leaks (reactive)	Highly secured, (proactive) security	*Security Management*

Relevant Security Threats

- To begin, Let’s talk C-I-A

Relevant Security Threats - Confidentiality

- "Secrecy is enforced while data resides on systems and devices within a sensor network throughout transmission"
- **My question for later – what qualifies secrecy?**
- **Someone should not be able to invade user's privacy, distributor's data**
- **Attacks on any layer of OSI model – collision attacks, exhausting attacks, unfair root-bridge selection and *(my suggestion an ntp attack)***

Relevant Security Threats- Confidentiality

- **Attacker physically accesses meter sensor through locks, begins running a sniffer and is able to inject data**
- **Attacker may be able to imitate other meters in the system**

Taken from
ettercap.sourceforge.net

Taken from wireshark.org

Relevant Security Threats - Integrity

- No unauthorized adjustment of data
- Man in the middle attack – No adjustment of data
- Differs from (ntp) attack because Integrity is changing data attack

Relevant Security Threats- Integrity

- Forward and Backward Secrecy
- A sensor cannot be placed into a network and find out past information
- Nor can a sensor be taken from a network and placed into a new network and send old information
- Attackers could insert sensors of their own which are “jail-broken” and gather information

Relevant Security Threats- Availability

- **Authors Present: Destroy communications links in WSNs, effectively make useless**
- **Can be DOS, jamming, jitter any QOS disruption – this affects Distributor, Customer and Devices**
- **Fairly easy attack to create…**

Relevant Security Threats- Availability

- How easy this is… (This is my own suggested example, hacking or tampering with meters is unlawful, I do not suggest or condone this action)
- Zigbee common RF device module for Home Area Networks (HANs) and WSNs
- 900 Mhz, Avg Power Output 100 mW
- My hack example - Create patch antenna and blare noise using software defined radio

Relevant Security Threats- Availability

- **Patch antenna is calculated based on wavelength and effective permitivity**

$$\lambda = \frac{2\pi}{k} = \frac{2\pi v}{\omega} = \frac{v}{f}$$

Depending on substrate permittivity, €, length of patch will vary slightly

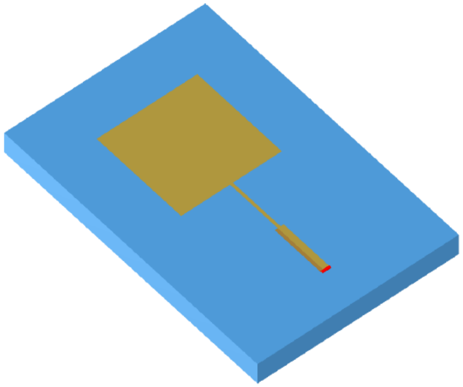


Image taken from: antennamagus.com

Relevant Security Threats- Availability

- USRP – Universal Software Radio Peripheral
- Allows injection and direct access to RTP packets
- Blare noise which drowns Zigbee signal out (this can also be an attack on Integrity)

Image taken from:
profheath.org

Other Relevant Security Threats

- Authentication and Authorization – communication among interstitial nodes is trustworthy i.e. the source and the receiving nodes verify one another's identity
- Non-repudiation – "A node cannot deny sending a message it has previously sent" – needed for retransmission in case of loss .. However – Freshness – "ensures key is recent and no adversary can replay old messages" [1]
- Foreseeable threat if attacker can continue to send old messages as "new data" - need to ensure that you can resend old data if needed
- Forward and Backward Secrecy – Forward: "sensor node should not be able to know any future messages once it leaves a network" Backward: "a new joining sensor should not be able to read or know previously sent messages" [1]
- These allow a hacker to install self made devices for data acquisition, systems need to be scalable and dynamic

Summing this Up

- New smart grid WSNs will vary from traditional WSNs
- Many security to issues to consider for various applications in the smart grid
- Attacks are relatively easy to create, can every one be counted for?
- Therefore, what problem comes from these analyses?

The Problem

- Although traditional WSN security systems are in place, new smart grid systems will be significantly more *APPLICATION SPECIFIC*
- Then, because everything is application specific, how does one normalize a security architecture for installation of different WSN topologies ???
- Security architecture must provide a process, implementation and a testing of a security system for an application specific instantiation
- I.E. Provide an overlying, holistic view of smart grid security architecture to cover such complex applications

The Proposed Solution

- Authors propose developing a security architecture of WSNs in the smart grid
- Consists of the following and is not limited to the following components:

  (1) Technology

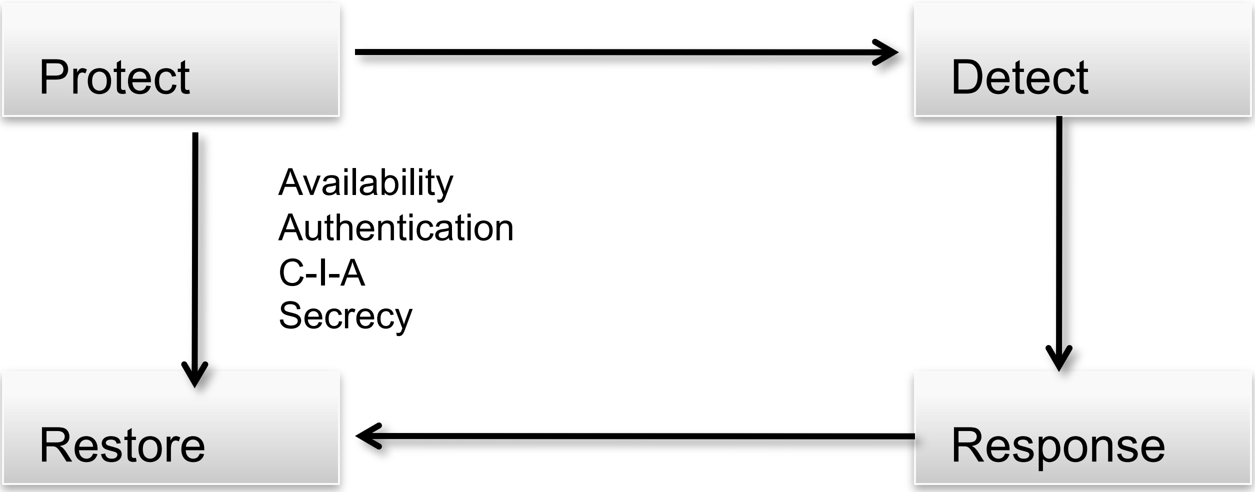
  (2) Management

  (3) Person and Organization

- Each section is broken into subcategories
- Although broad in scope, needs to be broad enough to try and be normalized for all WSN applications

The Proposed Solution- Technology

- **A security model for technology solutions is needed (PROACTIVE)**



The Proposed Solution-Technology

- Security Standards for WSNs in smart Grid

(1) Security Foundation Standards – security architecture, security technique specifications of applications and services (i.e. what measures need to be in place)

(2) Security Technique Standards – physical equipment for security, software for security

(3) Security Management Standards – delegation of security authority, establish personal roles for management professionalism

(4) Security Testing and Evaluation – What are the metrics that need to be met

The Proposed Solution-Technology

- Authors focus on Security Objectives for Supporting the “Security Techniques” portion of technology
- Establish Security Objectives within system

(1) Sensor Nodes and Terminals

(2) Communication Protocols (NTP, SMTP, HTTP(S), etc…)

(3) Data in its Life Cycle (generation, storage, usage and destroy)

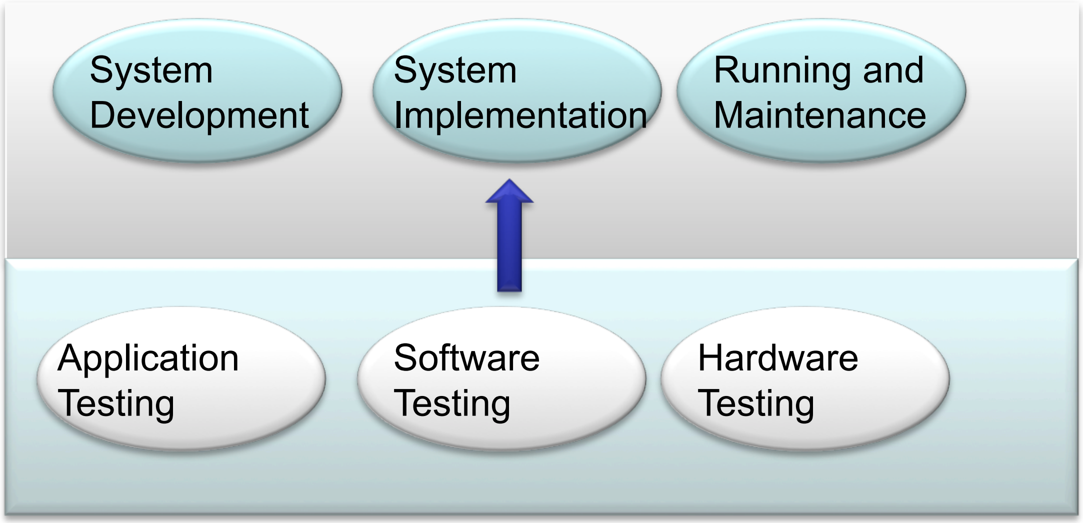
(4) Applications and Network Services

The Proposed Solution-Technology

- **Testing of applied technology should be done show below**

Stages of smart grid WSN Life Cycle

Security Testing and evaluation objectives



System Development

System Implementation

Running and Maintenance

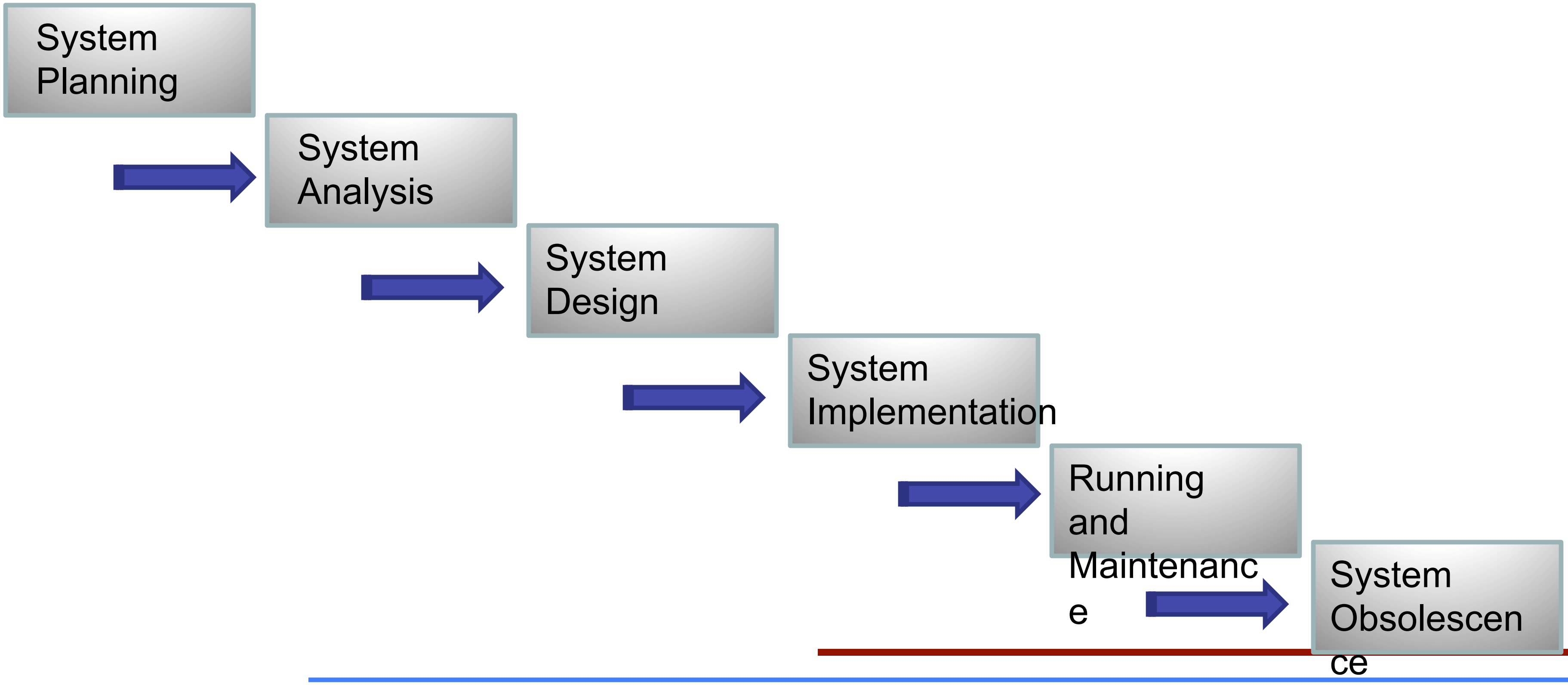
Application Testing

Software Testing

Hardware Testing

The Proposed Solution-Management

- **6 Stages to Management of Secure WSNs for the smart grid**



System Planning

System Analysis

System Design

System Implementation

Running and Maintenance

System Obsolescence

The Proposed Solution-Persons

- **Persons are integral for the management and development**
- **Essential to maintenance and upholding standards for deployment and establishment of WSN**

My Assessment

- Authors are too broad in scope and do not accurately depict a security strategy for the smart grid more so then just a regular wireless security network
- My own attack examples
- Emphasize Persons and Management, but no examples of clear leaders
- Emphasize application specific yet provide no background or examples to applications…
- Need to provide more proof of concept then speculate
- Good attempt to encapsulate a rather large subject area and provide guidelines

The Future

- **Develop more in depth security practices and protocols for future deployments**
- **In depth study of currently deployed WSNs**
- **Use newly developed security technologies**
- **New security research should produce newer technologies to help ameliorate problems and support suggested platform**

References

[1] Yufei Wang; Weimin Lin; Tao Zhang; , "Study on security of Wireless Sensor Networks in smart grid," Power System Technology (POWERCON), 2010 International Conference on , vol., no., pp.1-7, 24-28 Oct. 2010 doi: 10.1109/POWERCON.2010.5666729 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5666729&isnumber=5666013

[2] V.C. Gungor, et al., “Opportunities and Challenges of Wireless Sensor Networks in Smart Grid – A Case Study of Link Quality Assessments in Power Distribution System,” Industrial Electronics, IEEE Transactions on, vol. PP, pp. 1-1, 2010.

[3] T. Overman, R.W. Sackman, “High Assurance Smart Grid: Smart Grid Control Systems Communications Architecture”, CSIIRW , 2010.

[4] Alliance, ZigBee. *ZigBee Alliance Home*. Web. 13 Apr. 2011. <http://www.zigbee.org/>.

Questions

Thank You for Your Time