Vulnerabilities of Wireless Water Meter Networks

John McNabb
johnmcnabb@comcast.net
DEF CON 19
August 6, 2011

Background

- 13 years as an elected Water Commissioner
- 2 articles in NEWWA Journal on water infrastructure
- 10 years as lobbyist for Clean Water Action
- 6+ years as an IT Pro, mostly doing general tech support
- 2+ years as a security researcher, primarily interested in drinking water security & cyber security
- *Independent researcher*; no school, company, or grant support
- **DEF CON 18** last year - *Cyberterrorism & Security of the National Drinking Water Infrastructure*
- [March 2011 Hacker Japan article on my DC18 talk]
- **Shmoocon 2011** – *Hacking SmartWater Water Meters*

Importance of Water

- Water is essential for life.
- Water is a scarce commodity
- Water has been a source of conflict and war throughout human history.
- Water is a $400 billion global industry. Water has been called “the new oil.”
- Al Qaeda has repeatedly threatened to “poison” United States drinking water supplies.
- Water is a critical infrastructure.
- However, the American Society of Civil Engineers gives the nation’s drinking water infrastructure a D-grade and estimates that an investment of $255 billion is needed to bring the system to needed standards

Water Meter = Cash Register

- Water Bill based on the difference between “present reading” and “previous reading”, which is “usage”
- Usage x water rates = usage charge
- $40 billion – the annual income of US water utilities, mostly from meter information
- Average monthly water bill ranges from $34.29 a month in Phoenix compared to $65.47 in Boston for a family of four using 100 gallons per person each day.
- The revenue is very important to support day to day operations as well as capital replacement which nationally is billions behind schedule.

What could go wrong?

The June, 2011 audit of the Brockton, Mass. Water & Sewer Department found that :

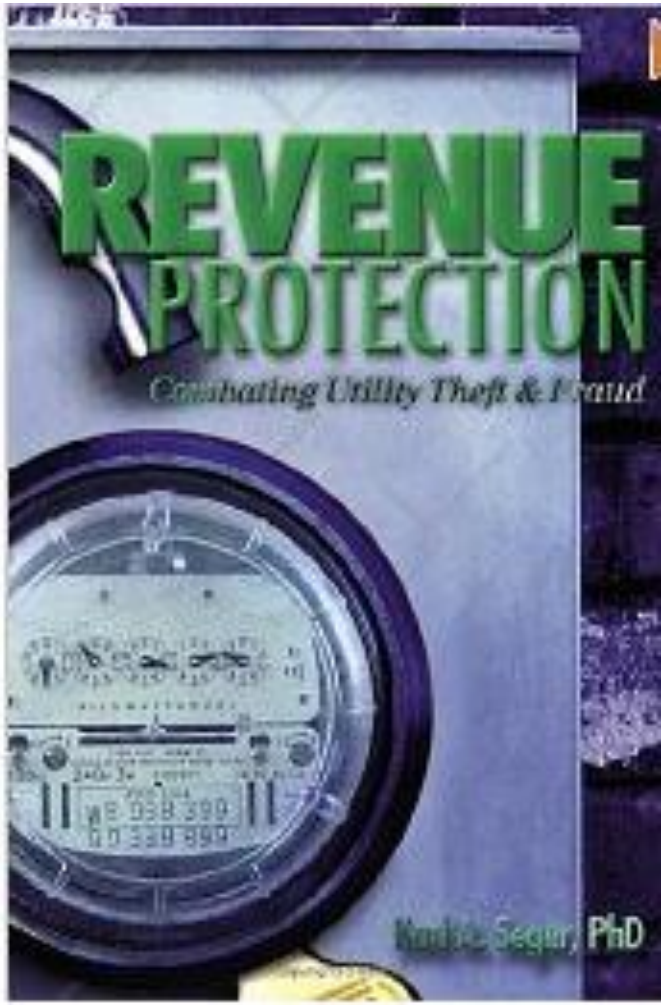
- most of the City's meters were 15 years or older,
- from FY2006 through FY2010 approximately 25% of the water bills were not based on reading the meter but were estimated readings, and that
- the billing staff did not have sufficient training in using the system.

The audit was called for by the City Council following the issuance of numerous retroactive bills to residents, resulting in one case of a water bill of $97,000 for one homeowner.

Brockton resident with **$92,439.35** water bill

Meter Tampering for Money

- Energy theft costs consumers billions of dollars every year in the United States alone
- Electric utilities assume 10% loss each year from theft
- “Theft of water by tampering with or bypassing water meters costs BWSC [Boston] thousands of dollars a year & .. imposes costs every paying customer.”



Water Meter Engineering

- How does the meter itself work?
- Displacement
  - Oscillating Piston
  - Nutating Disk
- Velocity
  - Single jet (Paddle wheel)
  - Multijet (Horizontal impeller)
  - Turbine
  - Propeller
- Ultrasonic meters measure the difference of the transit time of ultrasonic pulses propagating in and against flow direction

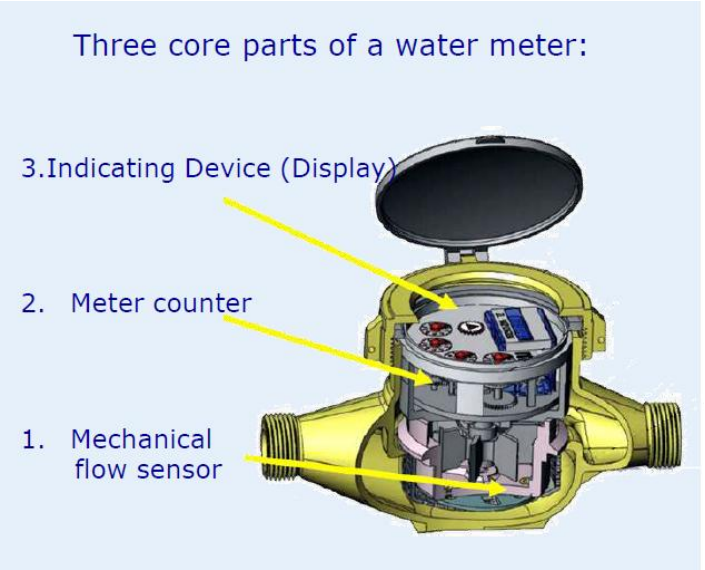
- Electromagnetic flow meters operate based upon Faraday's Law of induction, which states that a voltage will be induced in a conductor moving through a magnetic field.

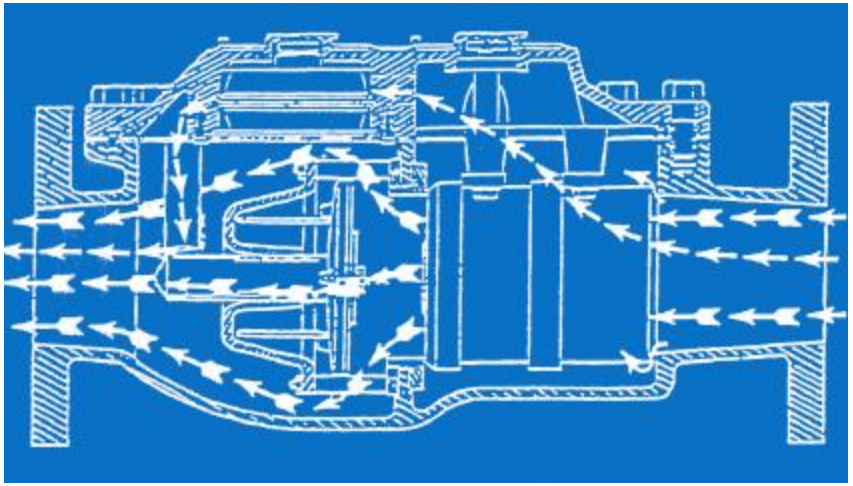
$$v = \frac{L}{2\ \sin(\alpha)}\ \frac{t_{up} - t_{down}}{t_{up}\ t_{down}} \text{ and } c = \frac{L}{2}\ \frac{t_{up} + t_{down}}{t_{up}\ t_{down}}$$

Faraday's Law: E=kBDV

Common types of water meters

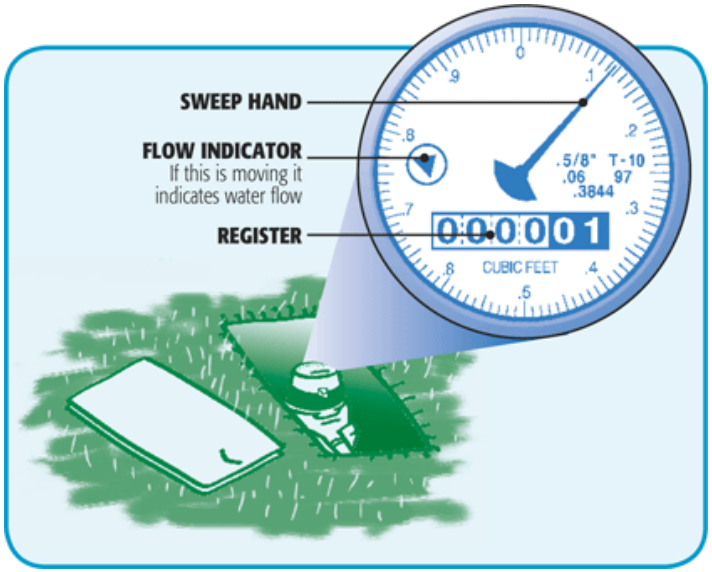
- Multi-jet Meter
- Single-jet Meter
- Positive Displacement Meter
- Turbine Meter
- Compound Meter
- Fire Meter
- Fire Hydrant Meter
- Electromagnetic or Mag Meter
- Ultrasonic Meter





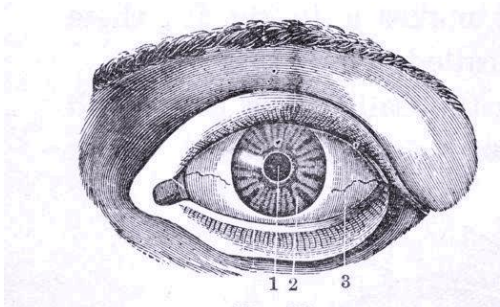
Data collection: Register

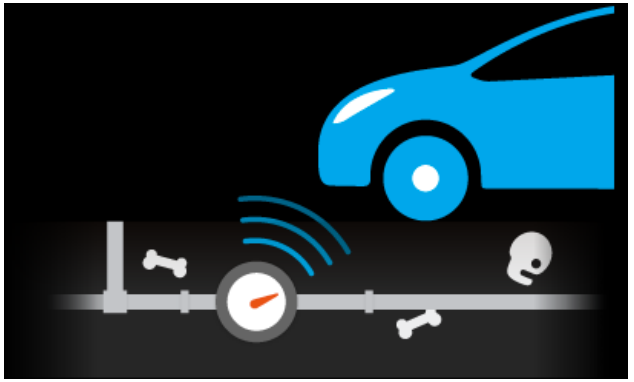
- Meters are data collection devices
- Data shown on “register”
- Data is total volume of water thru the meter since it was installed
- Interval readings turn it into information
- The less time between readings, the more information collected



Data Collection Methods

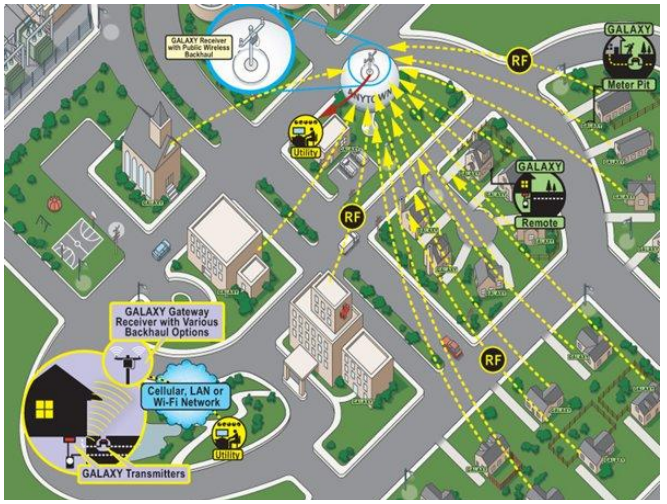
- **Eyeball.** This is the legacy method which requires a meter reader to physically enter the premises and read the meter, usually in the basement.
- **Walk-By.** The meter is connected with wires to a device located on the outside of the building, so even though a physical visit by a meter reader is still required he does not have to enter the building
- **Drive-By.** The meter is retrofitted with, or already comes with, a radio frequency transmitter, that is read by the meter reader in his vehicle as he drives past all the metered buildings on his route.





Data Collection – Fixed Network

- The fixed network is what we usually think of when we talk about Automatic Meter Reading or Smart Meter
- This takes the full capabilities of the wireless water meter and enables it to become a sensor network for the water utility that can allow <u>almost continuous water usage readings</u> (usually every 5-15 minutes).
- In the fixed network the signals from the single meter are transmitted and then collected in a central receiving station, if close enough, or to repeaters and then to the central receiving station.
- In most cases a star topology is used, but in some implementations a mesh topology is used to each meter can act as a repeater for any others within range.

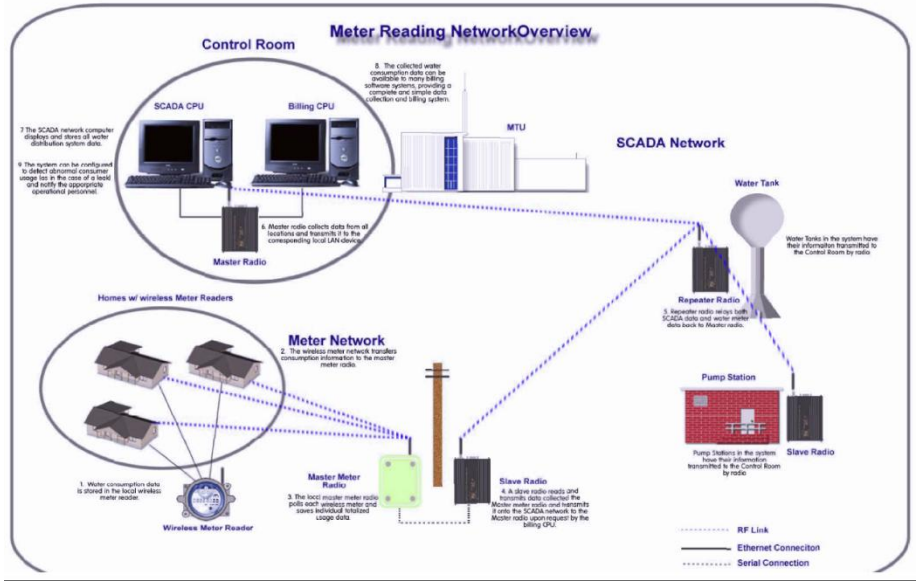


Evolution of the Smart Grid

Automated Meter Reading (AMR)	Advanced Metering Infrastructure (AMI)	Smart Metering and the Smart Grid
• One-way communications • Automated monthly meter reads	• Two-way communications • Frequent meter reads enable time-of-use billing • Utilities able to "talk" to the meters and control other devices	• Two-way umbrella communications across transmission and distribution • Enables intelligent control by utilities and the consumers • Provides ability for infrastructure to react in unison to changing market and demand needs

Basic Network Components

- Wireless transmitter or transceiver on the meter
- Collector, receiver or transceiver; (drive-by or static location)
- Central collector receiver/transceiver
- Billing office computer system



Wireless Water Meter is…

- Embedded device
- Node in Sensor network
- Information collection device
- Electronic cash register
- Regulator of availability of drinking water
- Water conservation device
- Big Brother?

Types of Wireless Water Meters

- No standards
- 25+ major manufacturers, each with small market share
- Data transmission:

- Phone lines
- Cable
- Power Lines
- Radio frequency
- Combination

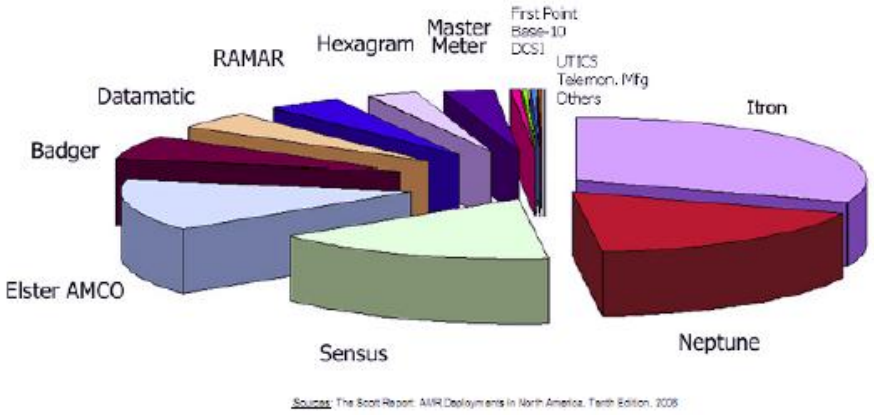
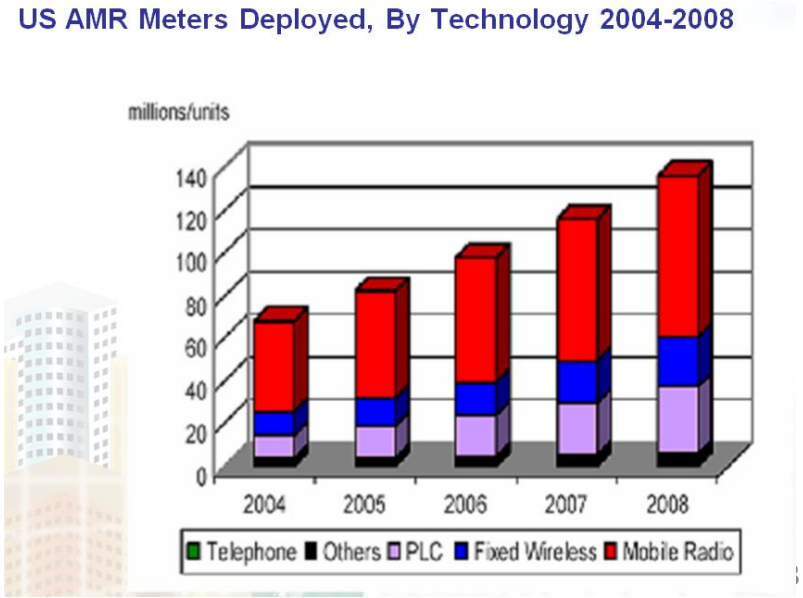
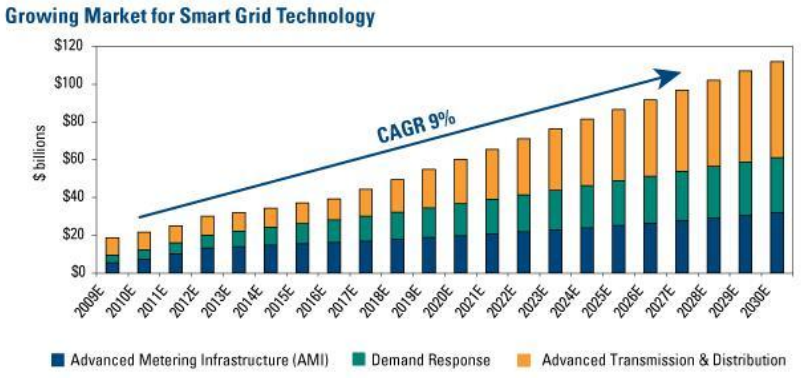


Figure 2. National Market Share of Water Meters



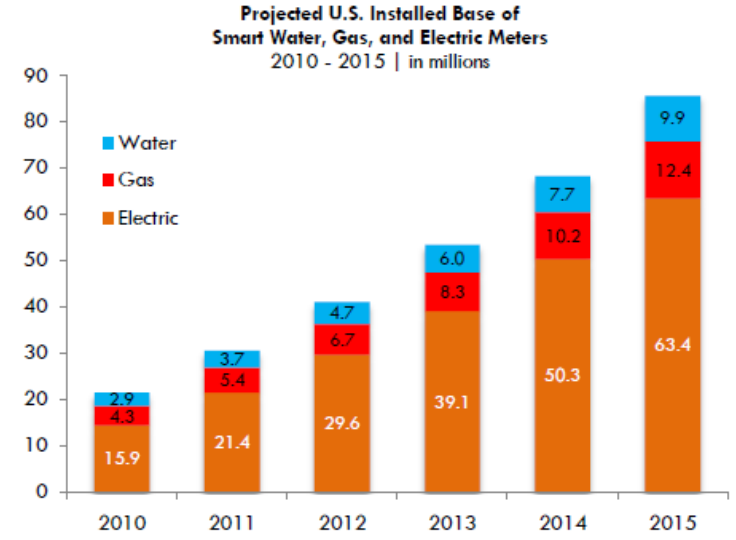
Growth of Smart Water Meters

- The U.S. advanced metering infrastructure (AMI) market [electricity+gas+water] will grow from $2.54 billion in 2010 to $5.82 billion in 2015 -- an 18% compound annual growth rate
- The world smart water meter market is expected to total $4.2 billion between 2010 and 2016.
- The worldwide installed base of smart water meters is expected to increase from 5.2 million in 2009 to 31.8 million by 2016.
- Most water meters in the US are read manually; only 28 percent of water utilities have AMR meters.
- About 50% of California water utilities have smart meters, driven by state mandate to cut water consumption 20% by 2020..



Source: Company data, FERC, EPRI, Brattle Group, IEA, Morgan Stanley Research.
E = Morgan Stanley Research estimates

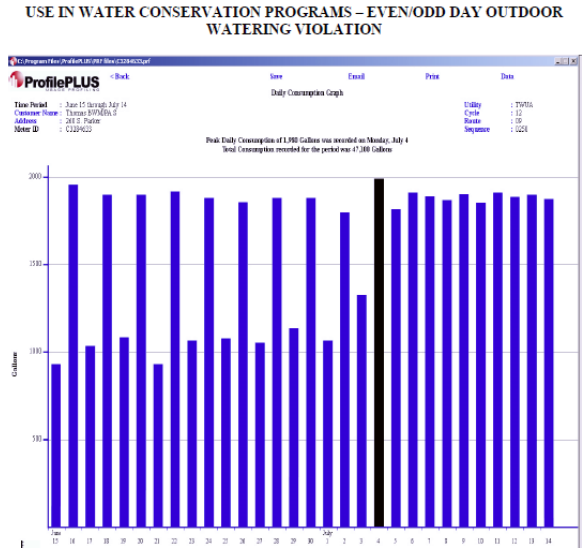
CAGR= Compounded Annual Growth Rate

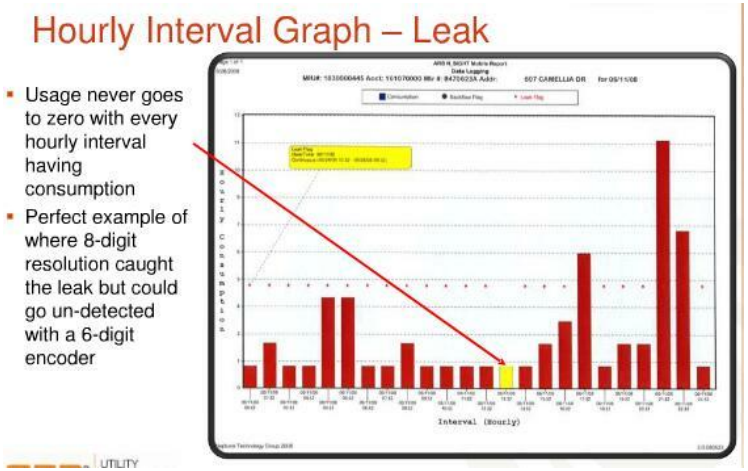


Source: Zpryme

Benefits of AMR/AMI to Utility

- Lower meter reading cost
- Better identify leaks
- Unaccounted-for water
- Detect evasion of water use restrictions
- Better accuracy
- Allows monthly billing
- Resolve bill disputes
- Customer service
- Water conservation



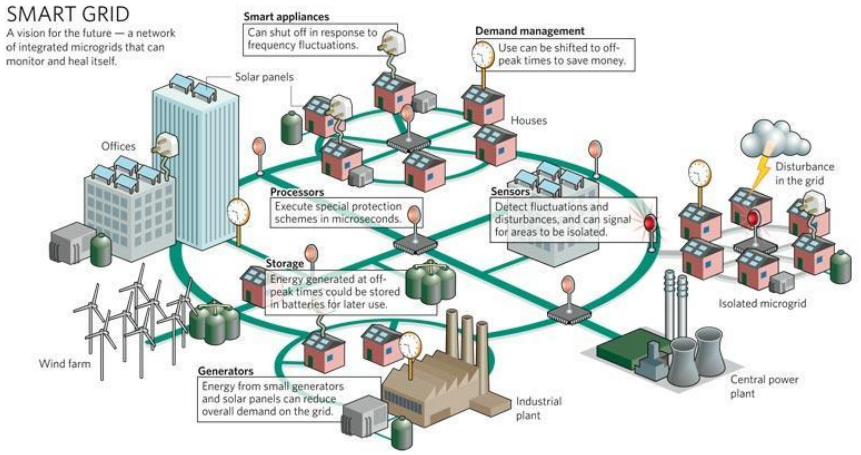


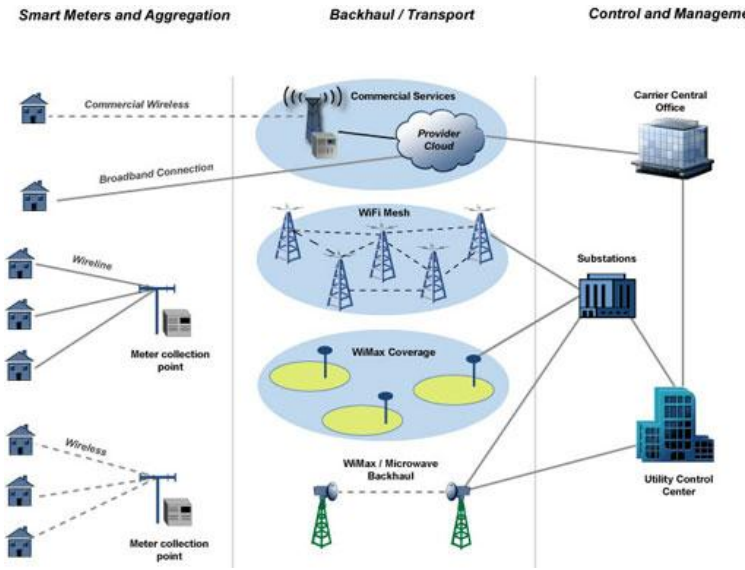
Water “Smart Grid” Real Benefits

The real benefits of the Smart Grid for Water lie in **aggregative, integrative, and derivative information**

A **meter read is not just a meter read**. It:

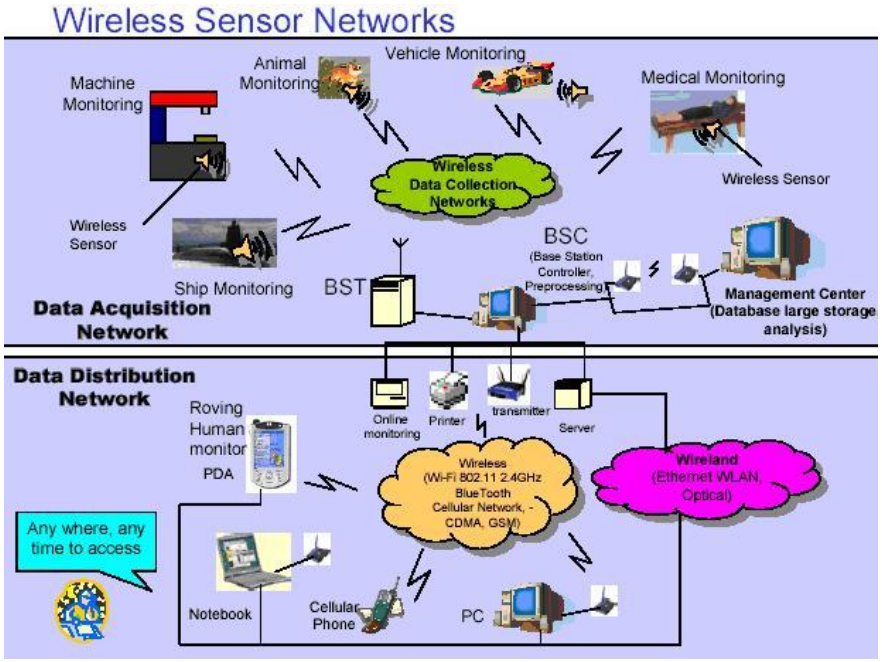
- forms a key part of the billing record;
- forms a fundamental part of the leak loss (pumped versus billed) analysis;
- establishes peak and average demand parameters;
- is a key measure of the performance of water conservation activities;
- forms the basis for feedback to the consumer directly on their impact on resources; and
- is the foundation for key reporting elements associated with regulatory requirements such as compliance with California’s 20 x 2020 Water Conservation Plan.”





Wireless Sensor Network

- A wireless water meter network is a kind of **Wireless Sensor Network**, which is defined as
- "a large network of resource-constrained sensor nodes with multiple preset function, such as sensing and processing… the major elements of a WSN are the sensor nodes and the base station."
- Each individual water meter is a "sensor node."
- **WSN Inherent Vulnerabilities:**
- the wireless medium itself,
- unattended operation,
- random topology, and
- hard to protect against insider attacks
- **Processor.** A typical sensor node processor is of 4-8 MHz, having 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency.
- **Energy:** Sensor nodes typically have a small form factor with a limited amount of battery power.
- **Memory:** Sensor nodes usually have a small amount of memory. Hence, sensor network protocols should not require the storage of a large amount of information at the sensor node.



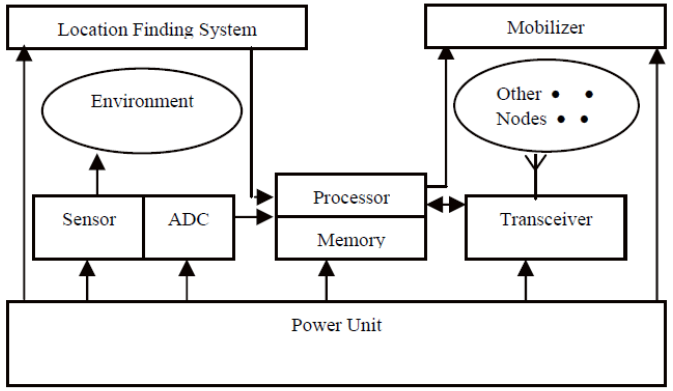


Figure 2. Sensor node architecture

Potential Attacks on WSN's

- Wireless Sensor Networks are subject to a wide range of potential attacks
- Active vs. Passive Attacks
- Outsider vs. Insider
- Mote class vs. Laptop class
- Interruption
- Interception
- Modification
- Replay attacks

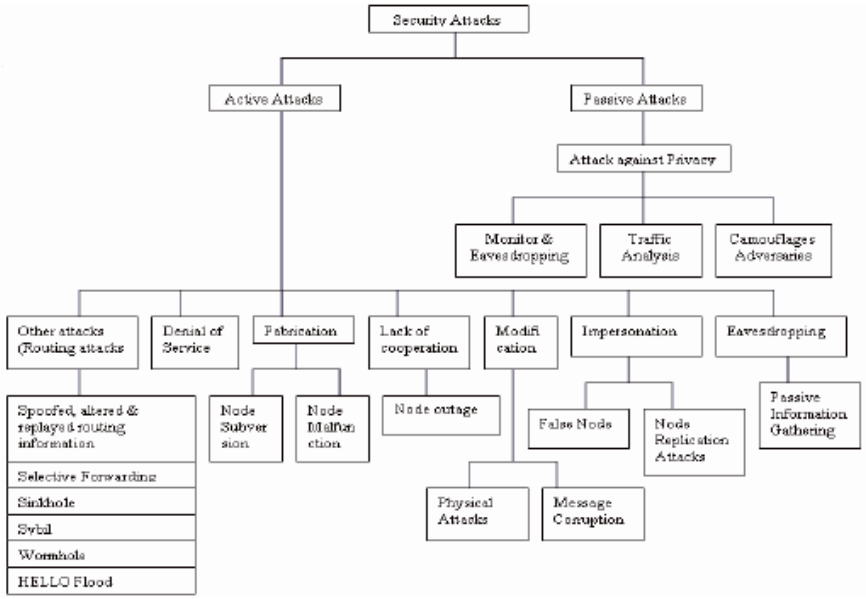


Figure 1. General Classification of Security Attacks

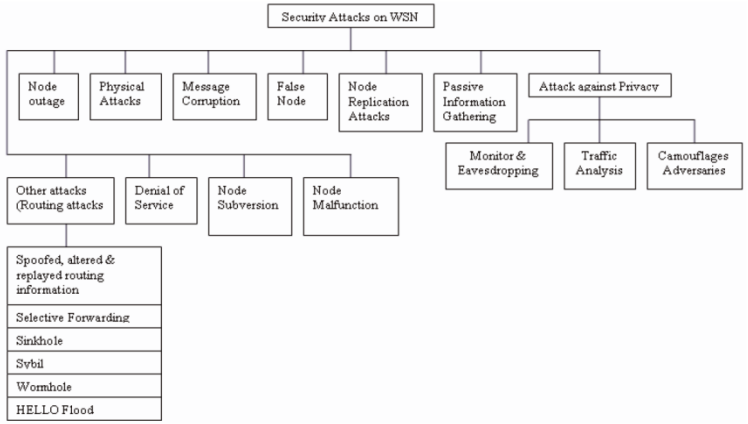
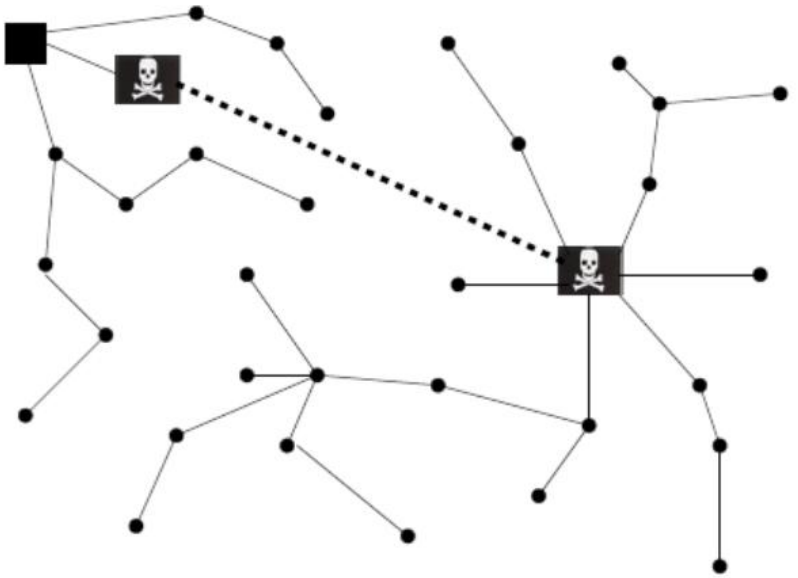


Figure 2. Classification of Security Attacks on WSN

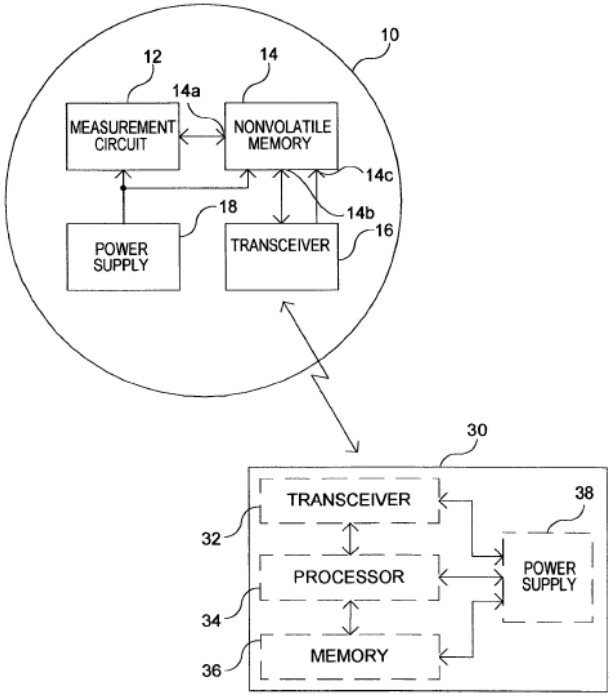
WSN Countermeasures

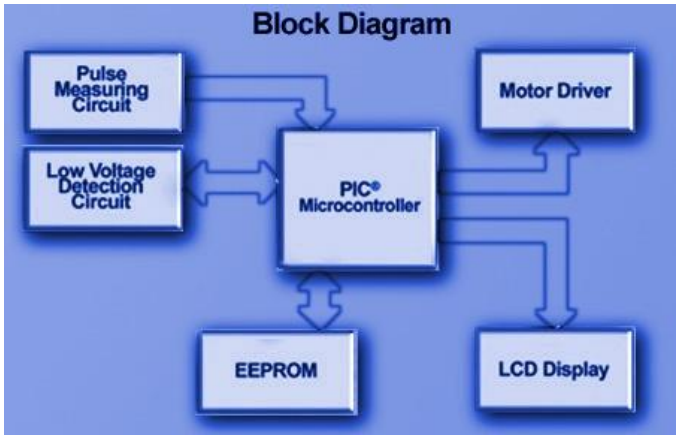
- Link layer encryption and authentication
- Multipath routing
- Identity verification
- Bidirectional link verification
- Authenticated broadcast



Wireless Meter Electronics

- Have off the shelf microcontrollers & transceivers
- Texas Instruments, Atmel, Microchip, etc.
- The trick is to find out which one is in a particular meter.
- Run on batteries, usually 5-20 yrs lifespan

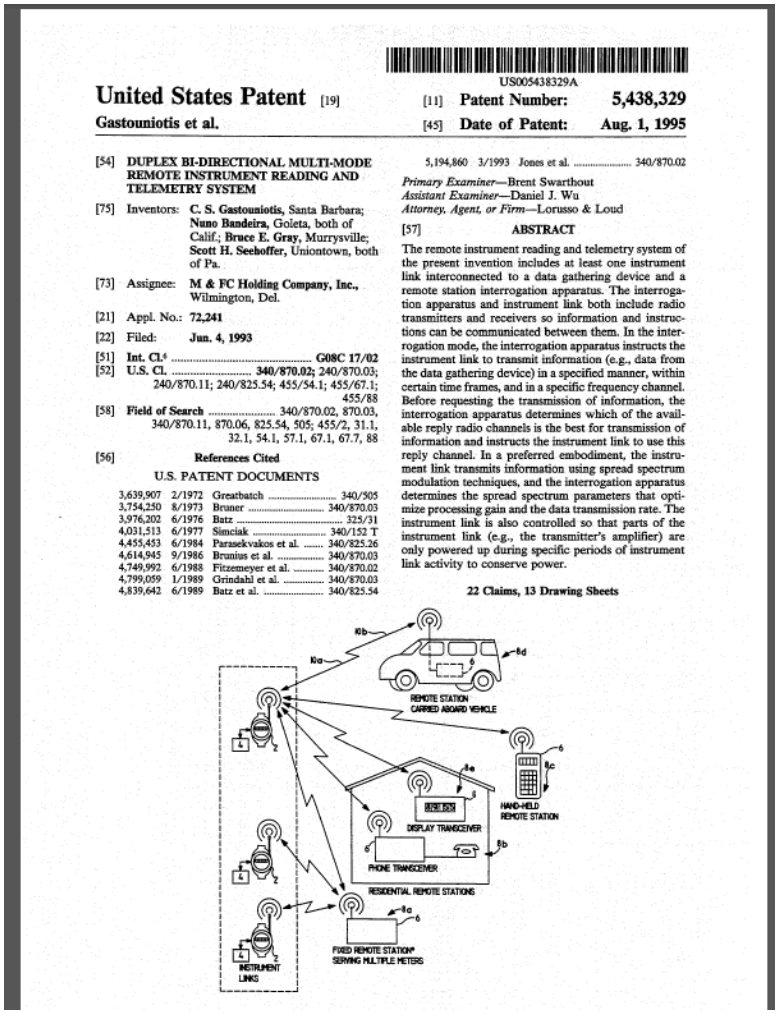




Design Description from Patent

Patent # 5,438,329, *Duplex Bi-Directional Multi-Mode remote Instrument Reading and Telemetry System*, August 1, 1995, the patent for the Sensus MXU Model 550 Meter Transceiver Unit (MXU) is very informative:

- "The instrument link 2 includes a microcontroller, such as an Intel 8051 family integrated circuit, to evaluate signals from the remote station and to control all the instrument link functions except those associated with the one second timer, the auto transmit counter, and the functions associated with those components."
- "The Electronically Erasable Programmable Read-Only Memory (EEPROM) interfaces with the microcontroller through a serial interface and provides one (1) kilobit (Kbit) of non-volatile storage. The EEPROM provides a means for storing configuration parameters and data that must be saved when the microcontroller is powered down (i.e. the instrument link sleep mode). For example, the EEPROM stores diagnostic data relating to the performance of the instrument link and a remote station. The EEPROM may be a Thompson 93C46 or equivalent."
- "An interrogation signal preamble is followed by a interrogation message that is preferably a Manchester encoded message at a data rate of 1 kbit per second. The interrogation message contains a variety of parameters including the interrogation mode (blind or geographic), instrument link ID with possible wild cards, reply window length, reply RF channel to be used, the pseudorandom code to be used for spread spectrum modulation, the reading cycle number, and the data to be transmitted (i.e. register reading or diagnostic information). Such a message is typically protected against transmission bit errors by a 16 bit CRC field."



US005438329A

United States Patent [19]
Gastouniotis et al.

[11] **Patent Number: 5,438,329**
[45] **Date of Patent: Aug. 1, 1995**

[54] **DUPLEX BI-DIRECTIONAL MULTI-MODE REMOTE INSTRUMENT READING AND TELEMETRY SYSTEM**

[75] Inventors: **C. S. Gastouniotis**, Santa Barbara; **Nuno Bandeira**, Goleta, both of Calif.; **Bruce E. Gray**, Murrysville; **Scott H. Seehoffer**, Uniontown, both of Pa.

[73] Assignee: **M & FC Holding Company, Inc.**, Wilmington, Del.

[21] Appl. No.: **72,241**

[22] Filed: **Jun. 4, 1993**

[51] **Int. Cl.**[5] **G08C 17/02**
[52] **U.S. Cl.** **340/870.02**; 240/870.03; 240/870.11; 240/825.54; 455/54.1; 455/67.1; 455/88
[58] **Field of Search** 340/870.02, 870.03, 340/870.11, 870.06, 825.54, 505; 455/2, 31.1, 32.1, 54.1, 57.1, 67.1, 67.7, 88

[56] **References Cited**
U.S. PATENT DOCUMENTS

3,639,907	2/1972	Greatbatch	340/505
3,754,250	8/1973	Bruner	340/870.03
3,976,202	6/1976	Batz	325/31
4,031,513	6/1977	Simciak	340/152 T
4,455,453	6/1984	Parasekvakos et al.	340/825.26
4,614,945	9/1986	Brunius et al.	340/870.03
4,749,992	6/1988	Fitzemeyer et al.	340/870.02
4,799,059	1/1989	Grindahl et al.	340/870.03
4,839,642	6/1989	Batz et al.	340/825.54
5,194,860	3/1993	Jones et al.	340/870.02

Primary Examiner—Brent Swarthout
Assistant Examiner—Daniel J. Wu
Attorney, Agent, or Firm—Lorusso & Loud

[57] **ABSTRACT**

The remote instrument reading and telemetry system of the present invention includes at least one instrument link interconnected to a data gathering device and a remote station interrogation apparatus. The interrogation apparatus and instrument link both include radio transmitters and receivers so information and instructions can be communicated between them. In the interrogation mode, the interrogation apparatus instructs the instrument link to transmit information (e.g., data from the data gathering device) in a specified manner, within certain time frames, and in a specific frequency channel. Before requesting the transmission of information, the interrogation apparatus determines which of the available reply radio channels is the best for transmission of information and instructs the instrument link to use this reply channel. In a preferred embodiment, the instrument link transmits information using spread spectrum modulation techniques, and the interrogation apparatus determines the spread spectrum parameters that optimize processing gain and the data transmission rate. The instrument link is also controlled so that parts of the instrument link (e.g., the transmitter's amplifier) are only powered up during specific periods of instrument link activity to conserve power.

22 Claims, 13 Drawing Sheets

Radio Frequencies

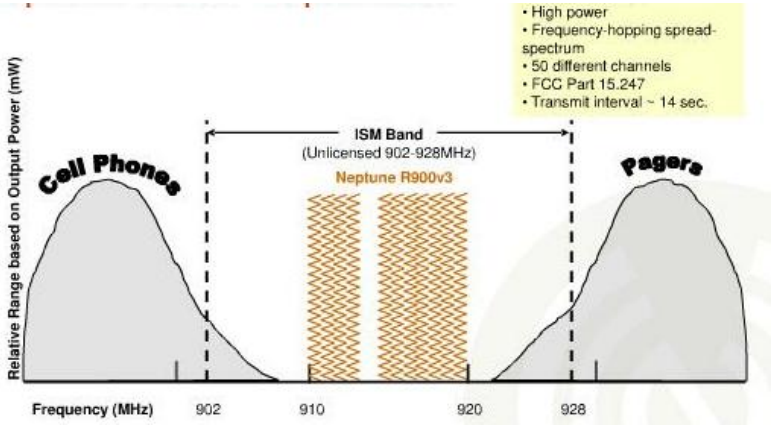
Manufacturer	Frequency	FHSS?	Security?
Aclara (Hexagram)	450 – 470		
Badger (Itron)	902 – 928		
Landis+Gyr (Cellnet)	902 – 928		
Datamatic	902 – 928	FHSS	
Elster AMCO (Severn)	902 – 928	FHSS	
Inovics	902 – 928	FHSS	
Itron	910 – 920		
Master Meter	902 – 928	DSSS	Encryption
Mueller (Hersey)	902 – 928	FHSS	
Neptune	900 – 950	FHSS	None
Performance	902 – 928	FHSS	
RAMAR	902 – 928		
Sensus	900 – 950	DSSS	Encryption

900 Mhz

- 900 MHz most commonly used for water meters in USA
- **Neptune Meter; Transmitter Specifications:**

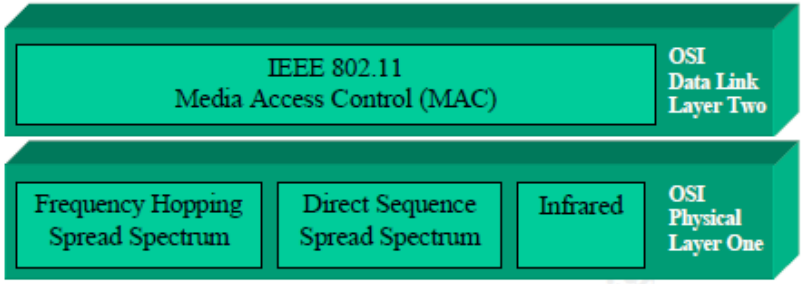
- Transmit Period - Every 14 seconds
- Transmitter Channels – 50
- Channel Frequency –

  910-920 MHz
- FCC Part 15.247 (802.15.247)
- Security? No encryption. FHSS



Frequency Hopping Spread Spectrum

- FHSS is a Layer One method of transmission
- "Some have expressed ideas that frequency hopping in FHSS may contribute to the security of 802.11, but these are invalid expectations—the hopping codes used by FHSS are specified by the standard and are available to anyone, thus making the expectation of security through FHSS unreasonable." Internet Protocol Journal, March 2002 Vol. 5 No. 1
- Touted by many as a security feature that makes encryption unnecessary
- While there are methods being researched to crack FHSS, it is still an obstacle to sniffing or eavesdropping
- However, researches have shown that FHSS can be cracked and should not be considered a security feature.

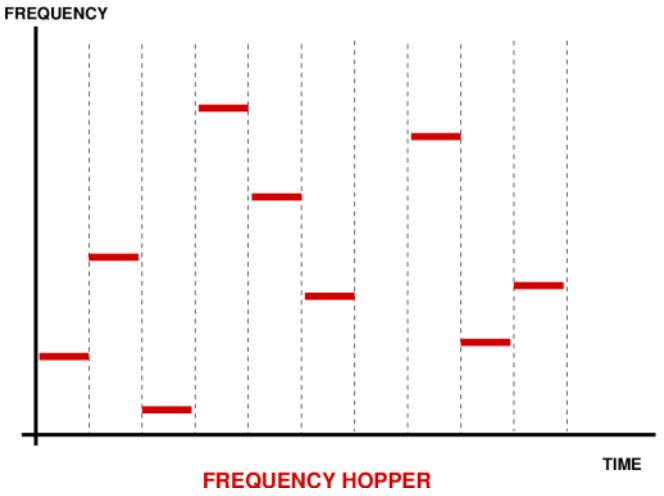


For China, North America and most of Europe:

x = {0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75} Set 1

x = {1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76} Set 2

x = {2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,74,77} Set 3



Why Hack Into Water Meters?

(1) Reduce water bill

(2) Steal water

(3) Evade water restrictions

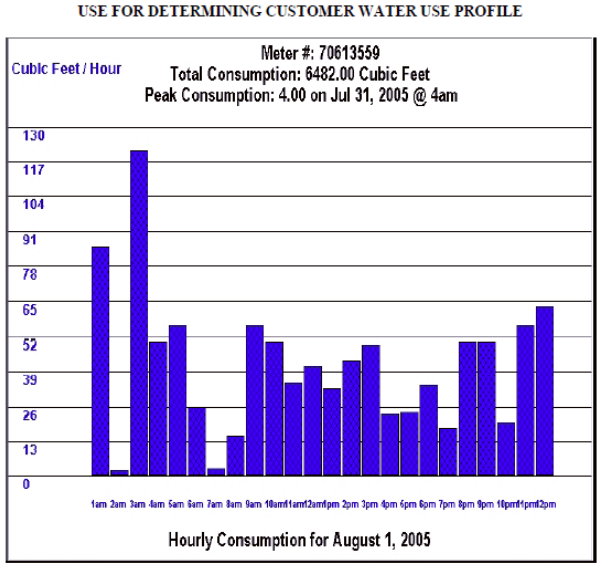
(4) Surveillance

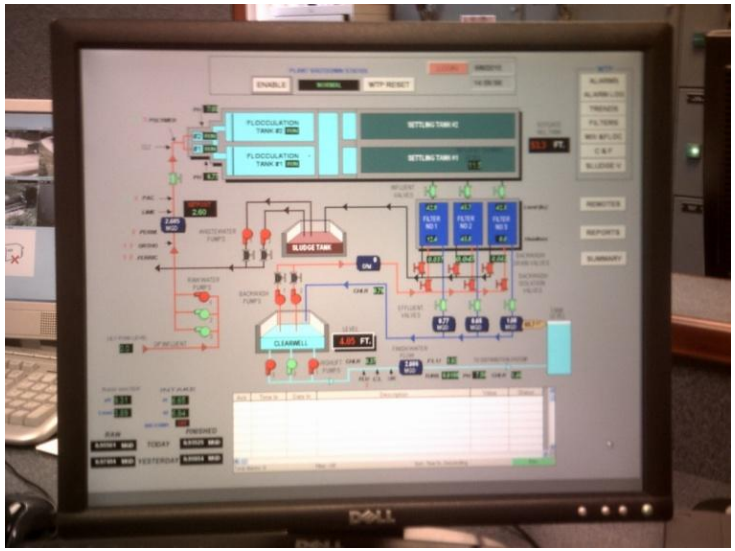
(5) Jack up other's water bills

(6) Route to introduce malware into water SCADA system(?)

(7) Get into other 'smartgrid' networks like electric grid

(8) Recon for potential attack?



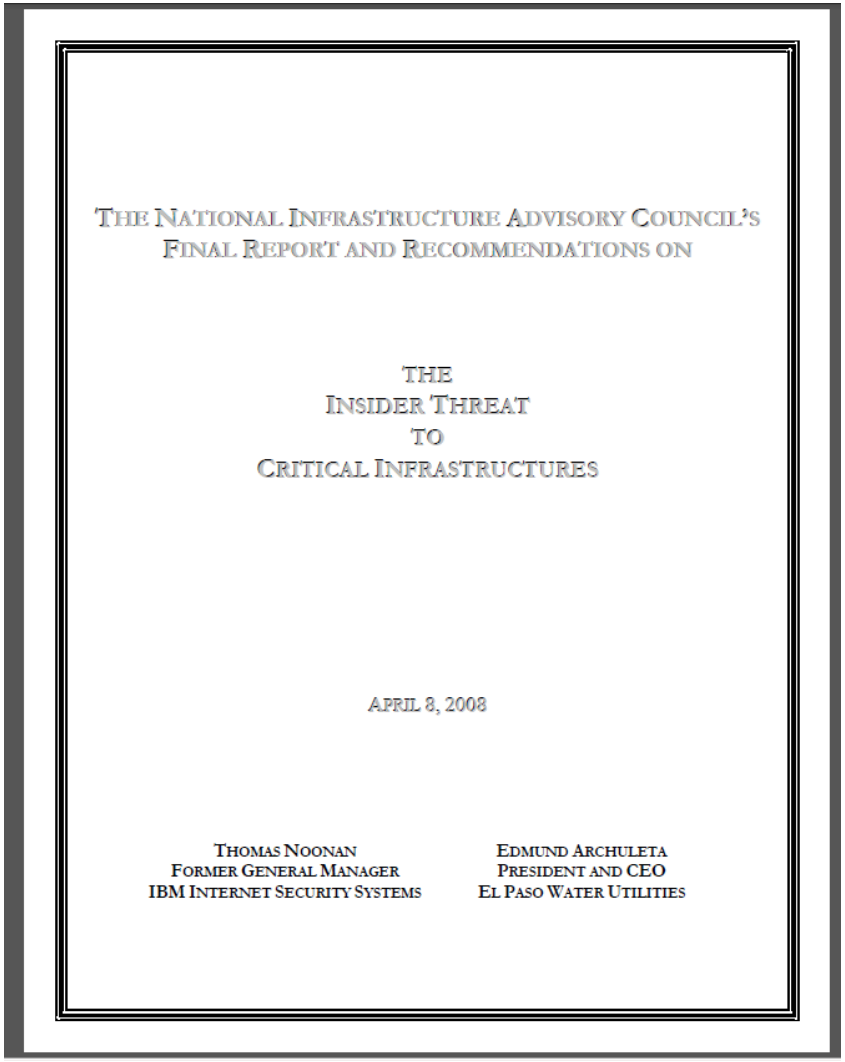


Evil Consumer

- Theft of services
- Build and distribute MITM boxes, like a pirate cable descrambler, or electricity theft device (being used in China), to lower reported usage, lowering water bills; stealing water & money.
- EFFECT: less revenue to water utility, leading to less maintenance of system and higher rates.

Evil Insider

- Insider threat: *one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.*
- "A new intelligence report from the Department of Homeland Security issued Tuesday, titled Insider Threat to Utilities, warns "*violent extremists have, in fact, obtained insider positions*," and that "*outsiders have attempted to solicit utility-sector employees" for damaging physical and cyber attacks*." ABC News, July 20, 2011
- The Maroochie incident in 2000, when a disgruntled former contractor used inside info to release 800,000 liters of sewage into the environment, using wireless network communications from his laptop, is an example of how insider threat could impact a wireless sensor network.


THE NATIONAL INFRASTRUCTURE ADVISORY COUNCIL'S
FINAL REPORT AND RECOMMENDATIONS ON

THE
INSIDER THREAT
TO
CRITICAL INFRASTRUCTURES

APRIL 8, 2008

THOMAS NOONAN
FORMER GENERAL MANAGER
IBM INTERNET SECURITY SYSTEMS

EDMUND ARCHULETA
PRESIDENT AND CEO
EL PASO WATER UTILITIES

Terrorist Attack

- **Recon.** Terrorist sends worm to intercept all signals to build hydraulic map of system for optimum results when inject poison into distribution system
- **Disruption.** Terrorist sends worm to shut off all water on certain date and time, coinciding with other attacks, updates firmware to keeps water turned off until utility can update them all.

Smart Grid is very “worm-able”

- Thanassis Giannetsos demonstrated a worm attack on wireless sensor networks with his SENSYS attack tool [BH Spain 2010]
- IOactive successfully ran a worm in a simulated city of 225,000 smart electric meters [BH USA 2009]
- Water smart grid could be just as vulnerable

Evil Water Utility: Big Brother?

- “Cary's citizens are right to be **concerned** about the information about our **private lives** that our Town staff will be able to collect if the Aquastar/AMI water meter system is implemented as planned.
- According to **Daniel Burrus**, a technology futurist and keynote speaker at the Autovation conference last September, "*As a utility, I could know exactly when you take a shower, exactly when you water the plants or wash the dishes*.
- *I could figure out how much water or electricity you are using at any point in time, and probably figure out what you are using it for*."

Are We Being Paranoid?

WHO WANTS SMART METER DATA?	HOW COULD THE DATA BE USED?[56]
Utilities	To monitor usage and load; to determine bills
Water conservation advisory companies	To promote water conservation and awareness
Insurance companies	To determine health care premiums based on unusual behaviors that might indicate illness
Marketers	To profile customers for targeted advertisements
Law enforcers	To identify suspicious or illegal activity
Civil litigators	To identify property boundaries and activities on premises
Landlords	To verify lease compliance
Private investigators	To monitor specific events
The press	To get information about famous people
Creditors	To determine behavior that might indicate creditworthiness
Criminals	To identify the best times for a burglary or to identify high-priced appliances to steal

Up the Ante: Hydrosense

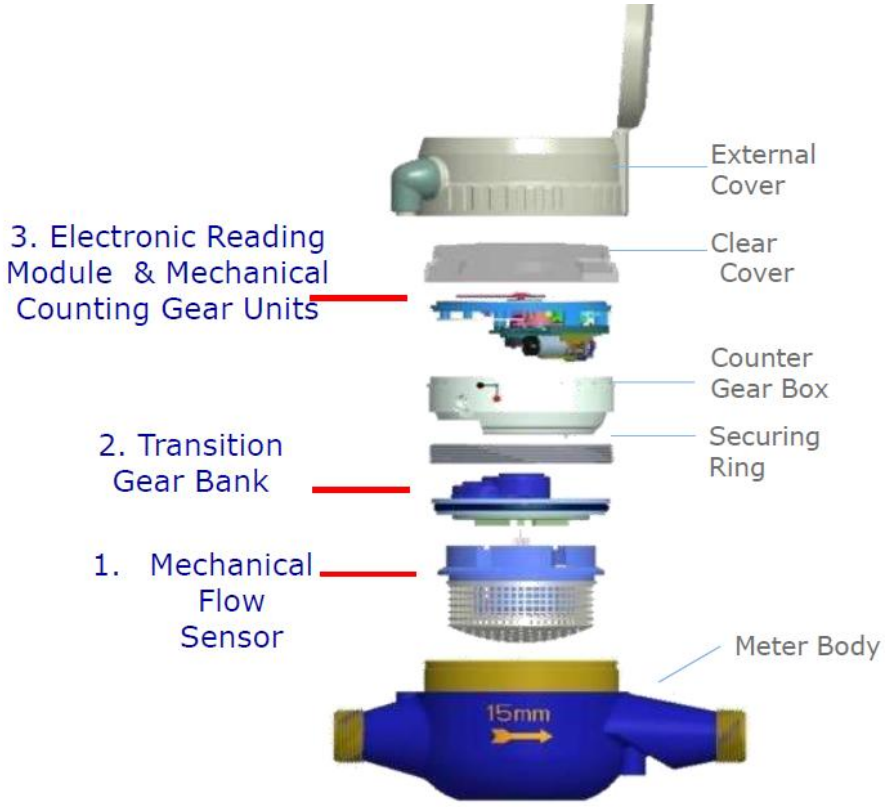
- HydroSense is a simple, single point, sensor of pressure of water in a building, which can give accurate information about when each water fixture is turned on and for how long.
- Hydrosense is a simple, screw-on device that doesn't require the services of a plumber. It operates on battery power, or uses WATTR, a self-powered version that uses the flow of water to power the device.
- Hydrosense measures the change in pressure and then to estimate the flow rate, which is related to pressure change via Poiseuille's Law,
- Poiseuille's Law is that the volumetric rate of fluid in a pipe Q is dependent on the radius of the pipe r, the length of the pipe l, the viscosity of the fluid μ and the pressure drop .
- The information is then sent via wireless – perhaps "backhauled" over the same wireless channel used by the water meter – to the water utility.

Vulnerabilities of Wireless Water Meters

- Some inherent vulnerabilities of the design – low onboard memory
- One vendor tells us what frequencies they transmit on, with no FHSS or encryption!
- Badger gives out its default network username, password and wireless key on web site
- Transceivers can be purchased on Ebay
- No encryption, FHSS, or DSSS on many of them
- However, more of them are coming out with encryption now

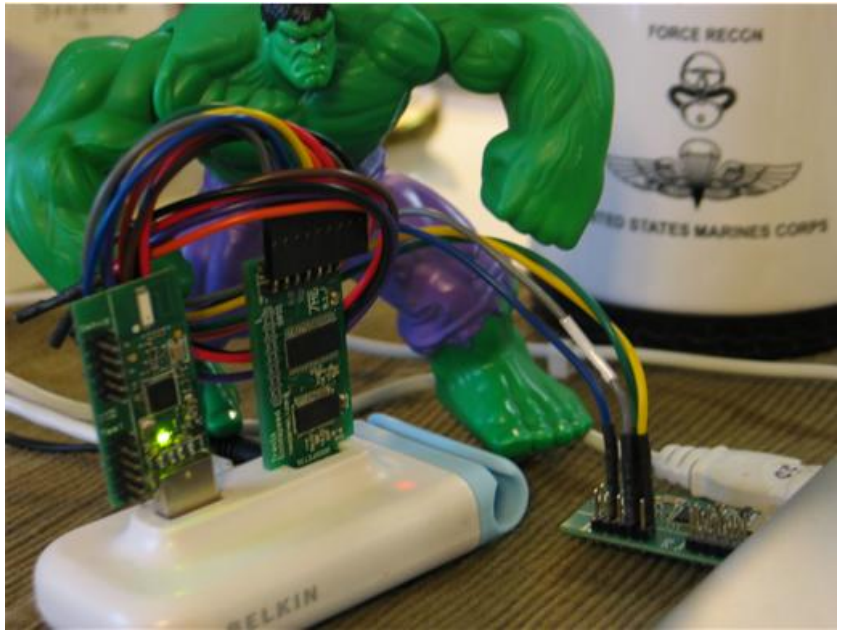
Design Advances in Water Meters

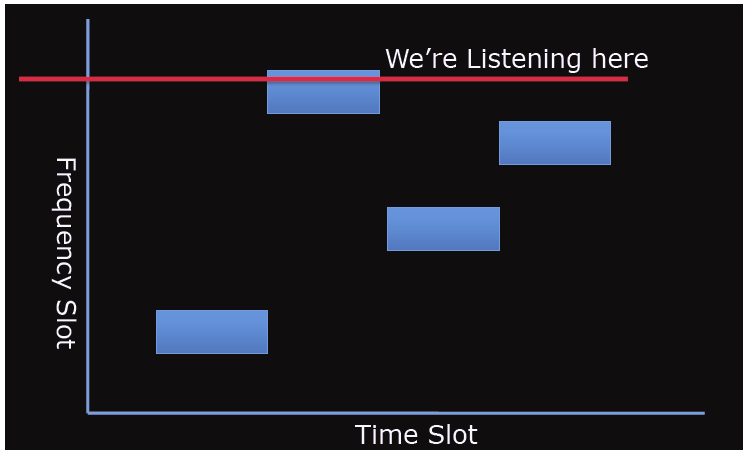
- "Third Generation" electronic water meters do not need batteries, have 99.9% accuracy.
- More wireless water meters are now being sold with encryption, such as AES 128 bit, 256 bit encryption



Sniffing FHSS Transceivers

- **atlas, cutaway & Q** – At Shmoocon 2011, atlas, cutaway & Q presented *Hop Hacking Hedy* and showed how FHSS was not inherently secure and how to crack it in 900 Mhz wireless devices using the CC1111EMK 868-915 Evaluation Module Kit programmed with Goodfet, using SmartRFstudio and python code they wrote.
- **Rob Havelt** - At Black Hat Europe 2009, in *Yes it is Too WiFi, and No It's Not Inherently Secure*, Rob Havelt discussed how he was able to crack Frequency Hopping Spread Spectrum (FHSS) in 2.4 GHz 802.11 using GNU radio and a USRP 2.0 and how it is not inherently secure. "*For legacy 802.11, it was possible to just use a USRP locked to a specific channel band, then feed the raw data into the BBN Adroit code - for kicks, you could set a file as the sniffer interface for Kismet or a tool like that to do analysis at each layer.*"





FAIL!

- I was hoping to supplement this talk with results of sniffing packets from my 900 MHZ FHSS wireless water meter.
- But, didn't have time or resources to do this before this talk, but the work is still ongoing.
- Tried Amtel RZ600, also FUNcube software radio peripheral, couldn't get them to work yet.

Ongoing Work

- **Atmel RZ600 Development Kit.** Has a 900 Mhz antenna and is advertised to be capable of being used as a development platform or just for packet sniffing. However, it did not work right out of the box. I am experimenting with some software to link it to Wireshark, but no success to date.
- **Texas Instruments CC1111 868-915 Mhz Evaluation Module Kit.** Will use to try to replicate the FHSS technique demonstrated by atlas, cutaway & Q, after making a working Goodfet. May also try Bus Pirate and a TI CC Debugger.
- **RFM DNT900DK.** The kit includes: two DNT900P radios installed in DNT900 interface boards, etc. Looks promising but haven't tried it yet.
- **FunCUBE Dongle Pro.** The FunCUBE Pro is advertised as a software defined radio that operates in the 64 – 1,700 Mhz range. I will see if I can use it to replicate Havelt's methodology.
- **IM-Me.** I am dying to replicate the uses of this pager which was demonstrated in "*Real Men Carry Pink Pagers*" by Travis Goodspeed and Michael Ossmann at ToorCon 2010, and see what other uses I can get out of it. I will try this if I have time.
- Breaking down wireless water meters and start to reverse engineer them.

Wrapping Up

- Water meters are an integral component of the national drinking water infrastructure
- Tampering with water meters, either mechanically or electronically, cost s money for local water systems
- Wireless water meters need to be better secured to prevent potential financial loss to water suppliers and to reduce potential security vulnerability to the water system.
- ***Thanks to:***
- Marc Maiffret
- Rob Havelt
- Travis Goodspeed
- atlas, cutaway, & Q
- Bob Johnston, CISSP, for his archived DHS Daily Infrastructure Reports (cited in my white paper)