Security in the IoT

Professor Stephen Hailes
UCL

IoT

- IoT is coming – technologies to allow it to happen exist and are constantly reducing in price
  - wireless SoC ~ CC2538 is £2.98 in quantities of 2000
  - CISCO and others have identified markets with potential value of $trillions
- IoT has many properties, one of which is likely to be the longevity of attached devices. Another is (stable) networked control.

- Much of what takes to make it a commercial success can be represented as challenges that lie in:
  - **Engineering** – designing and building robust, secure, and extensible systems, and managing and adapting them over time
  - **Social acceptance** – gaining (or at least not abusing) the trust of end users –implies consideration of privacy and the perception of control
  - **Research** – much of which is in data processing, filtering, fusion, aggregation, modelling and presentation, and in control.
  - **Mixtures of the above** – issues like power saving for battery powered devices, localisation, and security/privacy are cross cutting

Net Result

- More intelligent sensing and control systems
- Greater connectivity
  - …giving greater availability of data and control
  - …which enables qualitatively different commercial opportunities
  - [Potentially] HUGE impact on society
  - BUT… scale and granularity of adoption → impact of system failure significant (people may die)
  - UIs will not be getting significantly better
  - Heterogeneity, adaptability, limited device capabilities and lack of clarity in management make it harder to ensure network availability
- Invisibility, heterogeneity → complex → autonomic response needed
  - No global management infrastructure, perimeter model not valid
  - Want systems to be self-configuring, adapting to context change
  - Need to understand trust (many levels) and to worry about privacy

…cont

- Assessing whether a (set of) fault(s) results from DoS is hard if node ‘failure’ rate high.
  - c.f. sensor nets for harsh environments
- Asymmetry between capabilities of attacker and attackee
- IDS related to DoS – what’s normal?

A warning (1)….

If you believe that encryption is the answer to your security problem, then you probably asked the wrong question.

- What on earth does 'security' mean anyway?
  - It's a state of being – everything is OK
- Security is about securing a **system**
- Security is a **process** NOT a product
- A sole focus on technology is blinkered and founded in ignorance

Security

- What changes in the IoT:
  - Resource poverty: relatively low processing power and energy stores
  - Asynchrony: your devices are switched off most of the time
  - Clock sync is not a given and is important
  - Mobility, the importance of location
  - Poor access to the hardware
  - Byzantine is the norm – things fail, but frequently not cleanly.
  - Cascading failure is the norm
  - Boundaryless security
    - Self protection
    - Intrusion detection
    - Many more points for information leakage
  - New DoS attacks
    - e.g. sleep deprivation
  - Actuators

…cont

- Security management
  - Policy
  - SW update
  - Who to tell? And in what way?
- Privacy
  - Whose data/information is it anyway? Can I opt out? When?
  - Associating information leakage with breach
- In Industrial Control Systems
  - Legacy Systems, COTS systems
  - Threats poorly understood
  - Risks very substantial
  - Almost no crossover in expertise between security engineers and control engineers

Threats (ISO 27005:2011 Appendix C)

- Physical damage
- Natural events
- Loss of essential services
- Disturbance due to radiation
- Compromise of information
- Technical failures
- Unauthorised actions
- Compromise of functions
- Hacker, cracker
- Computer criminal
- Terrorist
- Industrial espionage:
  - Intelligence, companies, foreign governments, other government interests
- Insiders:
  - poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees

Attacks on Industrial Control Networks

- **Target Selection**
  - Not Random
  - Clear objectives (Network, Process, System, Data, People, Environment)
- **Motivation**
  - Exfiltration
  - Sabotage
  - Extortion (halt the system & ransom)?
- **Organisation**
  - Different sets of skills, insiders, coordinated groups
  - Government agencies
- **Effort (Research and Preparation)**
  - System Infrastructure, people, behaviour, manuals, key certificates
- **Length of the attack**
  - Short-term to Long-term

Attacks on Industrial Control Systems

Location	Motivation	Target	Details
Europe	*Exfiltration*	*SCADA, PLC, DCS*	*HAVEX – a remote Access Trojan*
Global	*Exfiltration*	*Telvent OASyS SCADA Systems*	*Malware to steal SCADA logs*
Europe and Asia	*Exfiltration*	*Critical Infrastructure Systems*	*Duqu - Trojan*
USA	*Sabotage*	*South Houston Water Utilities Network*	*HMI (3-character password)*
USA	*Sabotage*	*California Canal System*	*Former employee installed malware*
Iran, Europe	*Sabotage*	*SIEMENS PLC*	*Stuxnet*

Maroochy: Water Services Breach (2000)


The Register
Biting the hand that feeds IT
DATA CENTRE SOFTWARE NETWORKS SECURITY BUSINESS HARDWARE SCIENCE BOOTNOTES
Hacker jailed for revenge sewage attacks
Job rejection caused a bit of a stink
31 Oct 2001 at 15:55, Tony Smith

- ❑ **Motivation**:
  - ❑ Revenge
  - ❑ (Insider: Disgruntled ex-employee)
- ❑ **Attack**: Attack on SCADA Control systems
  - ❑ Insecure radio communication between control centre and pumping stations
  - ❑ No SCADA system security
  - ❑ Using insecure radio communication & stolen SCADA configuration program to impersonate a legitimate machine to reconfigure pumping stations
- ❑ **Consequences**:
  - ❑ *"Marine life died, the creek water turned black and the stench was unbearable for residents," (Australian Environmental Protection Agency)*
  - ❑ 800,000 litres of raw sewage released into environment

Germany: Steel Plant (Dec, 2014)

- **Motivation**: Sabotage
- **Attack**(Details Unknown):
  - Spear-phishing techniques
  - Zero-Day Vulnerabilities
  - Escalated privileges (corporate network to production components)
- **Consequences:**
  - Brought the blast furnace under their control.
  - Massive Damage

BBC | Sign in | News | Sport | Weather | iPlayer | TV

NEWS TECHNOLOGY

Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Politics | Health | Education

22 December 2014 Last updated at 13:01

Share

Hack attack causes 'massive damage' at steel works

AFP

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

Stuxnet

Infection technique

Targeting SIEMENS SCADA
- Targeting only SIEMENS SCADA
- Under Windows & running WinCC/ Step-7 software

Including PLC rootkit
- Hide file copies to drives
- ⇒ Preventing user notifying infection before sharing drive

Subverting SIMATIC WinCC
- Sending malicious SQL code to WinCC database for execution
- Modifying view adding code

Attack strategy

Monitoring Profibus
- Identify targeted module
- ⇒ Communication with motor drives

Drives frequency changes
- 1410 Hz → 2Hz → 1064 Hz
- ⇒ Changing motor speed

"Man-in-the-Middle" attack
- Fake industrial process control sensor signals
- ⇒ Avoiding shutting down due to abnormal behaviour

Based on source: Symantec Corporation, 2011

Lifecycle of the Stuxnet Attack

Pre-Entry
- Define objectives
- Acquire skills and tools
- Design & Implement
- Testing

Entry (Initial Infection)
- Insiders
- Social Engineering
- Drive-by-download

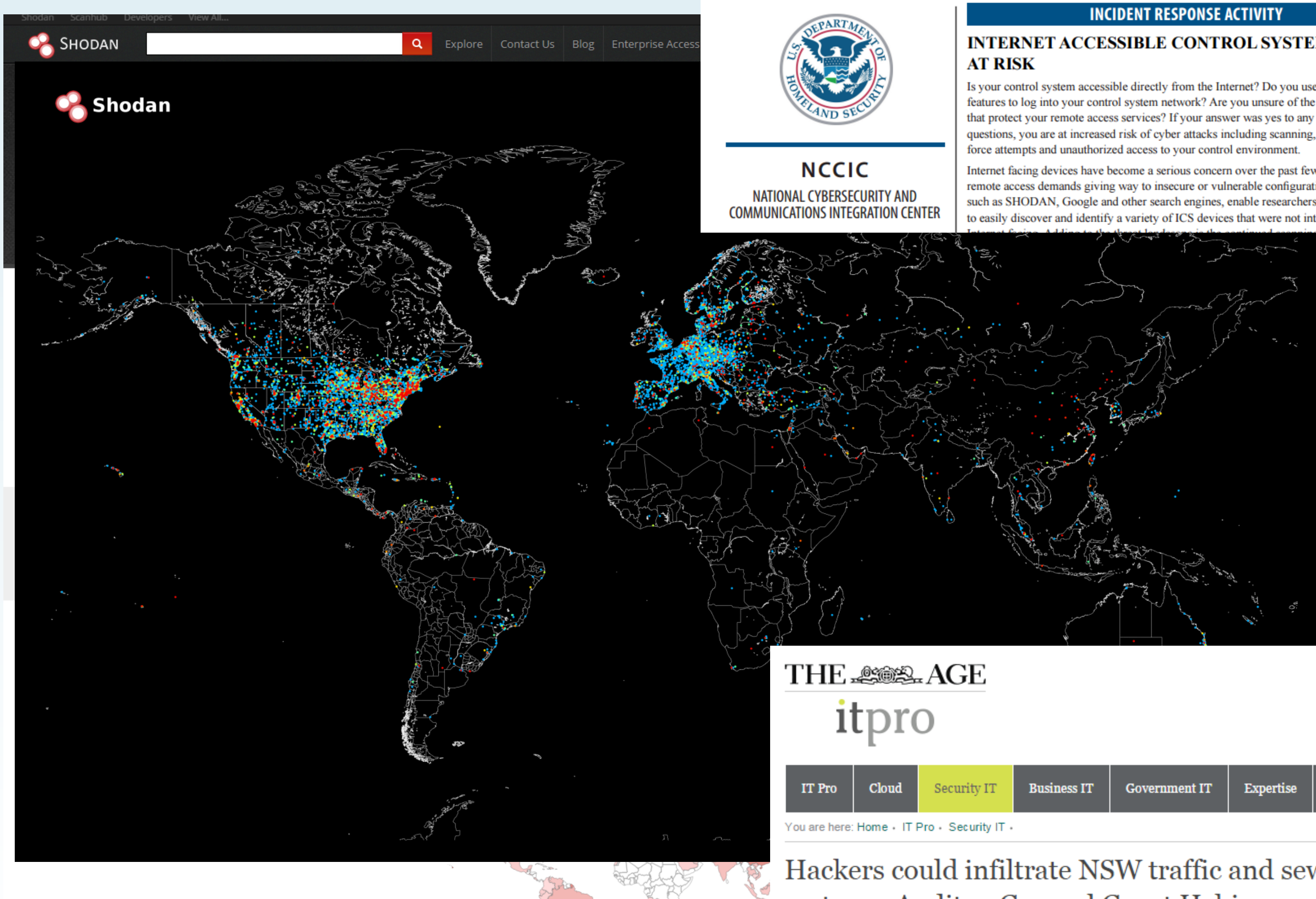
Propagation
- Internal Network Reconnaissance
- Escalate Privileges

Updates
- Peer to Peer Communication
- C&C Server

Operation
- Data Exfiltration
- Sabotage

Clean-Up
- Cover Tracks
- Remain Undetected

Shodan



ICS-CERT MONITOR

January – April 2014

NCCIC

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

INCIDENT RESPONSE ACTIVITY

INTERNET ACCESSIBLE CONTROL SYSTEMS AT RISK

Is your control system accessible directly from the Internet? Do you use remote access features to log into your control system network? Are you unsure of the security measures that protect your remote access services? If your answer was yes to any or all these questions, you are at increased risk of cyber attacks including scanning, probes, brute force attempts and unauthorized access to your control environment.

Internet facing devices have become a serious concern over the past few years with remote access demands giving way to insecure or vulnerable configurations. Tools, such as SHODAN, Google and other search engines, enable researchers and adversaries to easily discover and identify a variety of ICS devices that were not intended to be

THE AGE

itpro

IT Pro | Cloud | Security IT | Business IT | Government IT | Expertise | Opinion | IT J

You are here: Home • IT Pro • Security IT •

Hackers could infiltrate NSW traffic and sewage systems, Auditor-General Grant Hehir warns

January 25, 2015

Read later

Security

- Attributes that are worth thinking about:
  - Confidentiality
  - Integrity
  - Authenticity
  - Availability

- But how about
  - Credibility (= accuracy, repeatability, …)
  - Timeliness
  - Exclusivity

Challenges

- Trust/key establishment
- Secure community management
- Privacy
- Policy specification (from formal languages to HCI aspects to management)
- Power awareness
- Integrity
- Assurance of middleware/ components
- Secure control loops
- Perimeter devices in an open environment
- Secure routing
- Secure handoff (at many levels – network + service)
- Intrusion Detection – (who responds?, honeypots??)
- (For sensor nets) Secure data aggregation
- Monitoring of neighbouring devices
- New worms/viruses/spam(?)
- Feature interaction
- Standardisation: interoperable solutions
- Education

Security processes 1

- If we want to secure a system, then we need to follow a number of principles:
  - Prevention is *never* 100% effective – so:
    - Need defence in depth – several different mechanisms
    - Mechanisms for detecting and responding to attacks, preferably in real time, are essential:
      - – Detect – get to know you're being attacked.
      - – Localise – determine what's being attacked.
      - – Identify – determine who the attacker is.
      - – Assess – why are they doing this?
      - – Respond – depends on all of above.
      - – Recover – Have a plan better than 'go find a new job'

Security processes 2

- ❑ Compartmentalise – don’t put all of your data in one basket, use redundant (independently designed) control
- ❑ Start by securing the weakest link
- ❑ Take particular care with actuators – embed safety code and condition monitoring code
- ❑ Mediocre security now is better than great security never
- ❑ Involve stakeholders, devise training, quantify risks
- ❑ Have a strategy for dealing with change
- ❑ Be paranoid:
  - ❑ Give minimum privilege
  - ❑ Be vigilant – security is a 24/7 activity
  - ❑ (Watch the watchers -- 70% of all attacks are internal)

A warning (2)….

- Security has as much to do with people as technology
- It is a process, not a product.
- Beware of inductive logic “I can’t break it and I’m smart, therefore no smart person can break it”
- THERE IS NO SUCH THING AS CERTAINTY IN THIS WORLD

Conclusion

- Vision of the future
  - systems of huge scale,
  - with huge heterogeneity,
  - and a bigger impact on our lives than ever before
  - ‘perfect?’ Working would be good.
- Need R&D urgently to
  - think about what security means in these environments
  - understand threat models
  - understand potential impacts
- Need a public debate about impacts on society

Additional Slides

Covert Channels

- Covert Channels
  - *Any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy (Orange Book)*
- Types of Covert Channels
  - Timing Channels – changes in event timings
  - Network Storage Channels – hidden in the data
- Existing Research
  - Lack of research for wireless networks
  - Probability of detection low → channel capacity low

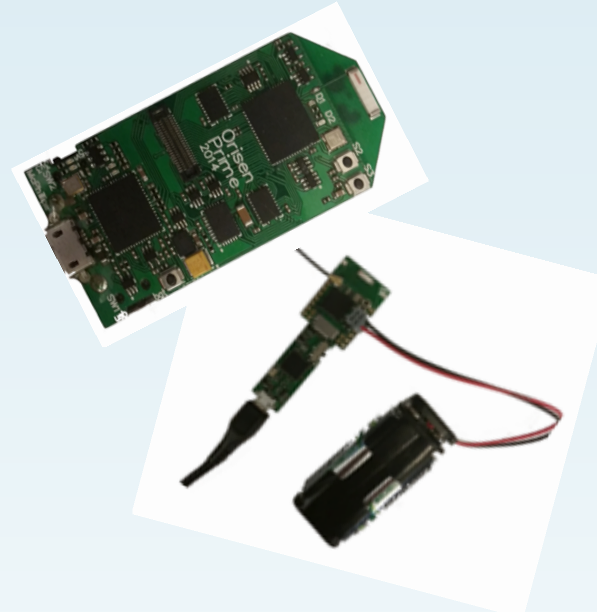
Proposed Covert Channels

1) Modulating Transmission Power
   - Impacts the RSSI (**Received signal strength indicator**) or LQI **(Link Quality Indicator**) signal at the receiver

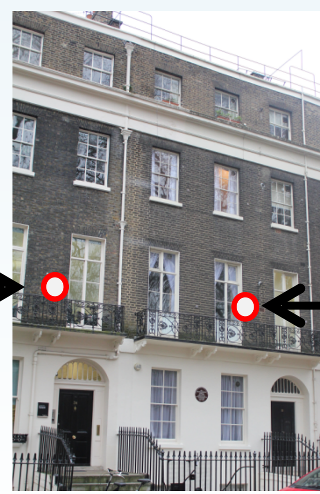
2) Modulating Sensor Data
   - In a way that can be seen in the encrypted form of that data

Devices and Testbed

- UCL's Orisen Devices
  - Freescale MC13224V chip (SoC)
  - IEEE 802.15.4 radio running at 250kbps
  - Chip antenna
  - -30dBm to +4dBm (power level 0 to 18)
- **Eve**: 12 dBi High Gain Directional Antenna
- Contiki OS



Eve



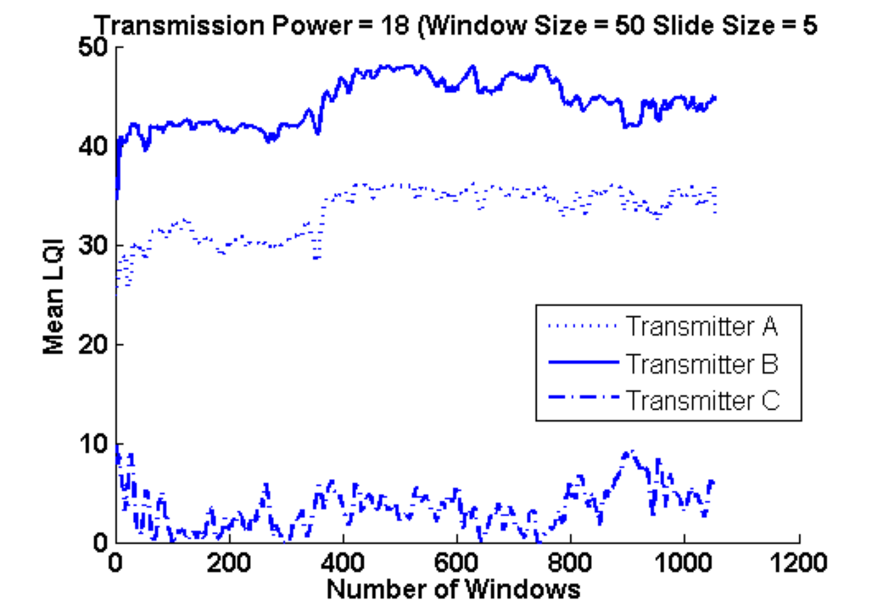
Distance: 7.5m

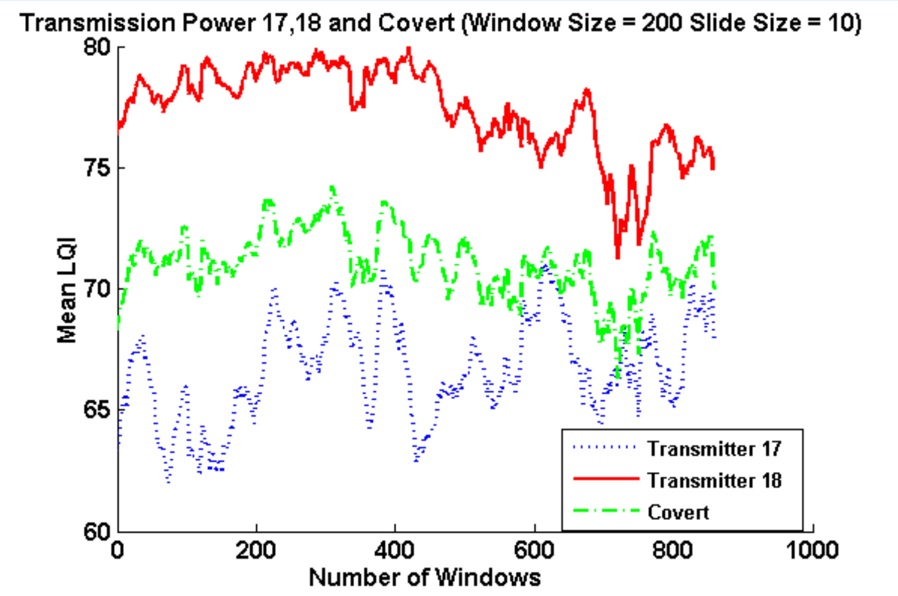
Alice

Mean Link Quality Indicator

Indoor to Indoor
(Transmission Power 18)

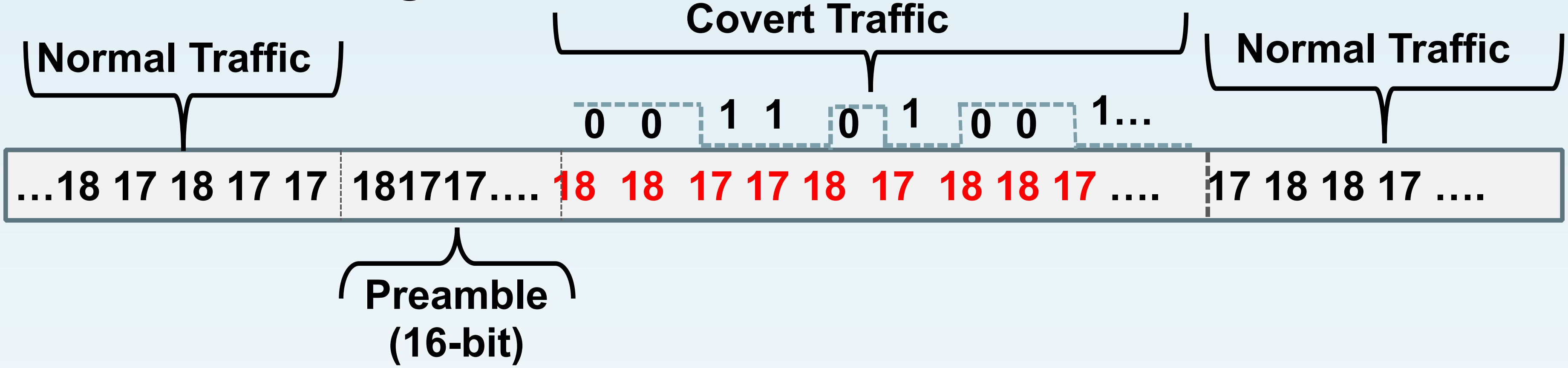
Outdoor to Outdoor
(Transmission 17, 18 and Random)



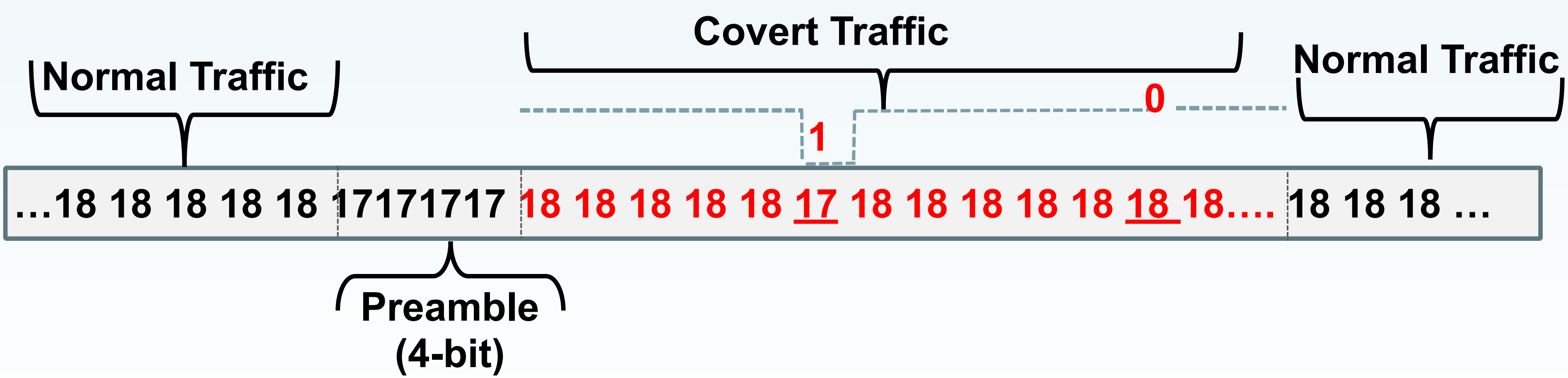


Covert Channel Based on Link Quality

1. ***Embedding in Random Traffic***



2. ***Embedding in Constant Traffic***



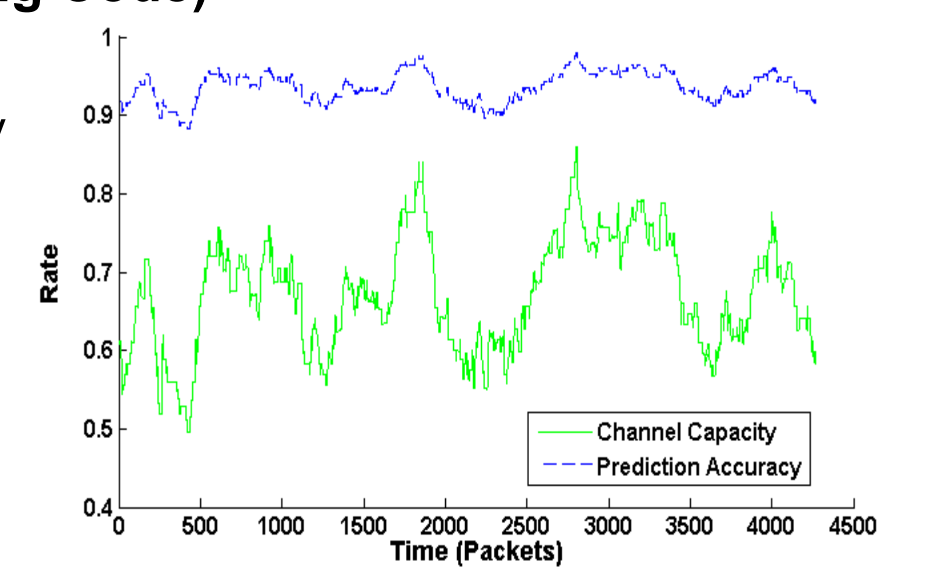
Results: Random

Dataset	1	2	3	4	5	6	7	8
Bits Remaining (128 Key)	***12***	***7***	***6***	***3***	***3***	***14***	***0***	***0***

- **LQI Threshold**
  - Exponentially-weighted moving average
  - Accuracy: ~90-98%
- **Error-Correcting Code (Hamming Code)**
- **Detection Analysis**
  - Two-sample Kolmogorov-Smirnov
  - Rejected Null Hypothesis

$$H_S = \sup_x | F(x) - S(x) |$$

  - where *F* and *S* are distribution functions



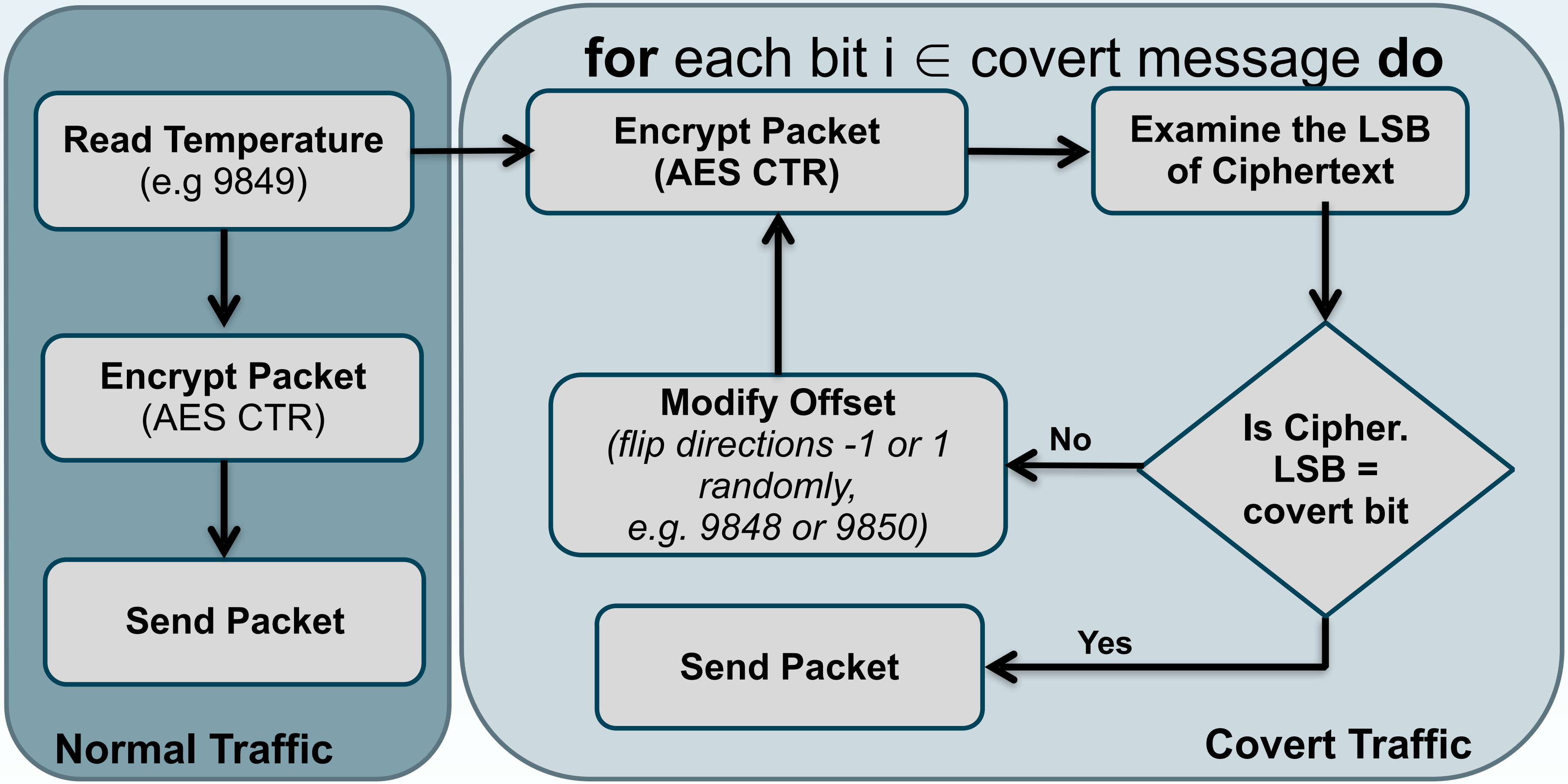
Results: Constant

Dataset	1	2	3	4	5	6	7
Bits Remaining (128 Key)	***11***	***8***	***10***	***2***	***18***	***2***	***8***

- **Accuracy:** ~86-98%
- **100% Accuracy ?**
  1. Longer Hamming Code, e.g. Reed-Sloman, Fountain Codes
  2. Transmit Covert Message Multiple Times (Bitwise Majority Voting)
  3. Key Search Strategy
     i. First change a single bit, then each pair of bits, and so on
     ii. Attempt decryption

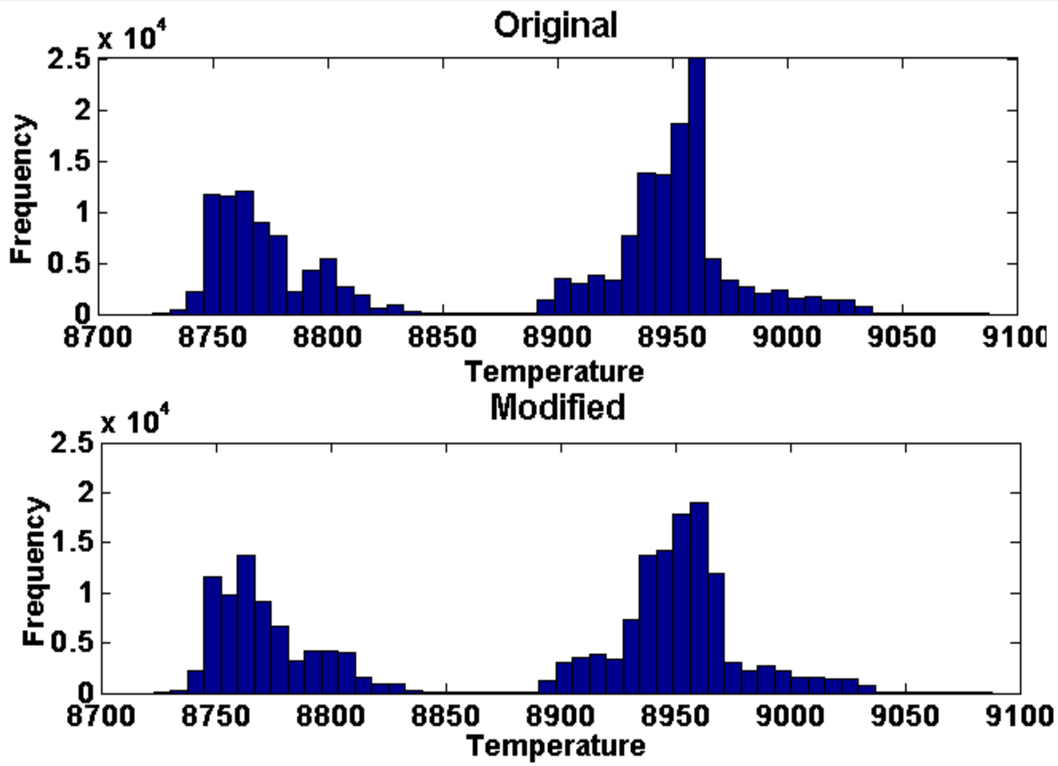
Sensor Covert Channel

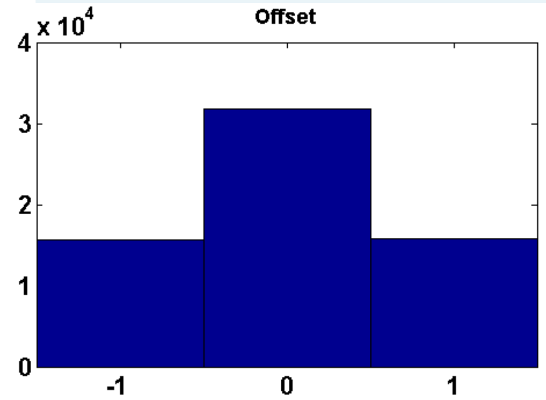
- ➢ Modulating Sensor Data (Temperature - ADC values)
  - ➢ Modified 1 in 3 packets



Results for Storage Covert Channel

- **Dataset Size:** 190,000
- **Two-sample Kolmogorov-Smirnov (KS2Test)**
  - Do not reject null hypothesis (i.e. the two data sets came from the same distribution)





Modified 16.76% of the readings
One Single ADC count
(±0.06 ºC) was sufficient

Conclusion

- First work to have explored use of the LQI or sensor readings in the design of covert channels
- Demonstrated the practicability of implementing such channels
- The regularity of sensor readings means that data can be leaked continuously
- Different modalities means higher bandwidth channels can be obtained by bonding together LQI and sensor data
- The same techniques can be used to receive control commands from outside