Wireless Sensor Network Security — Moving on to PhD from Master's

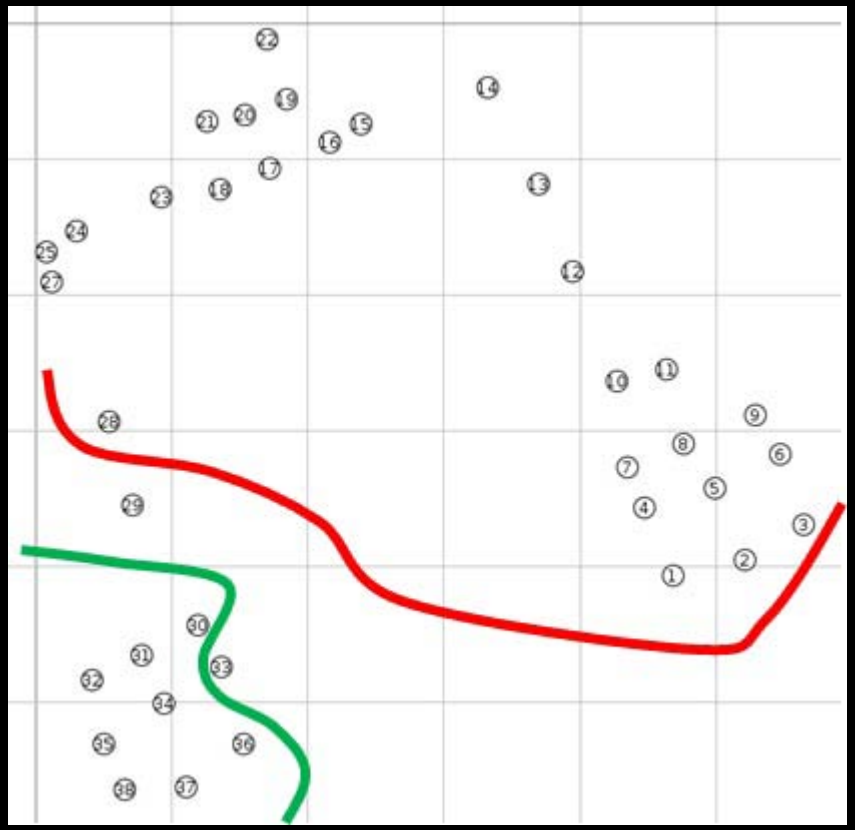
My Master’s Project

- To detect intrusions using a signature of time when updating to new software version
- Network-wide knowledge quantified as 'Intrusion Warning Score' (IWS)
- Higher the IWS, the higher is the probability of intrusion

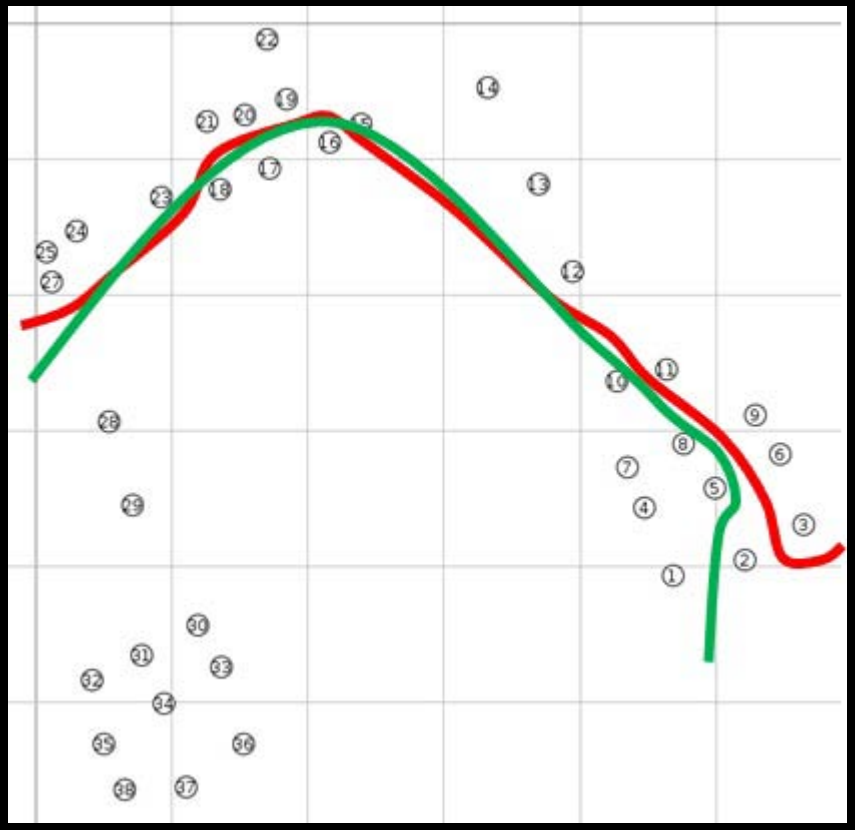
Insight from the Technique

- Anomalies in software update patterns
- Identification of point of intrusion
- Idea of zoning
  - GREEN: Low IDS score, needs physical protection
  - GREY: False pos/neg, needs augmentation
  - RED: Effectively guarded
- Rank possible combinations of parameters based on intrusion vulnerability

Owheo WSN Network



50% TX Power



100% TX Power

Insight from the Technique

- Anomalies in software update patterns
- Identification of point of intrusion
- Idea of zoning
  - GREEN: Low IDS score, needs physical protection
  - GREY: False pos/neg, needs augmentation
  - RED: Effectively guarded
- Rank possible combinations of parameters based on intrusion vulnerability
- Detect node relocations, node repudiation and node compromise

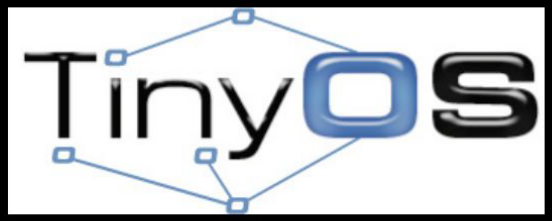
Weakness of the Project

- It is carried out in simulations
- Various assumptions made:
  - Sensors cannot be physically compromised (they must be physically protected to be realistic)
  - Network-wide information cannot be forged
  - Attackers are not able to modify protocols in a uncompromising sensor

Key Researchers leaving WSN

- Jonathan Hui (Deluge & IPv6/6LoWPAN)
- David Culler (DARPA Network Embedded Systems Technology project)
- Philip Levis (TinyOS, RPL)

*From Philip Levis' talk (OSDI-2012)



- Tremendously successful academic project
  - Started as Perl scripts used by a handful of academics
  - Now ~100 downloads a day, hundreds of thousands of nodes
  - Has a worldwide community of hundreds of contributors
- But it could have been more so
  - Missed being a platform for simple sensing apps (Arduino)
  - Missed being a platform for the Internet of Things (Contiki)
  - "Applications" became "hard applications"
  - Should have focused on the simple as much as the complex (the island syndrome)

41

Choices for PhD Project

A. Extending my existing work
B. Other avenue / disjoint field

Extending – Investigating Security

- Distributed approach with multiple sinks
- Role based deployment of heterogeneous nodes (silent nodes)
- Monitoring nodes (reputation based trusted routing path or wired backbone)
- Honey-pot trap

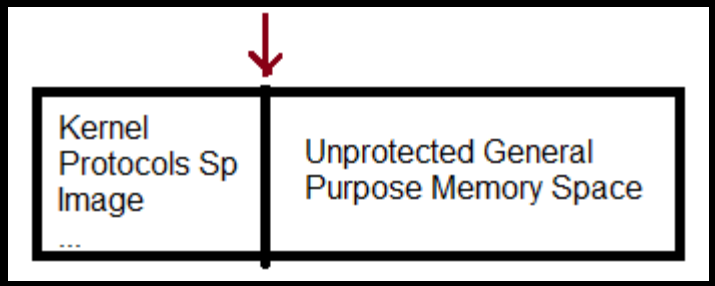
Need to Introduce New Devices

Desired properties:

- Update protocol/security codes housed in protected space
- Devices are able to protect the integrity of stored secrets
- Adversary cannot retrieved/cloned secrets in memory
- Tampered device must fail to authenticate to the network
- Protected space can only be programmed physically (needs to follow specific security routines)

Need to Introduce New Devices

- Managing Protected Storage in Embedded Device
  - Use of multi-factor funtion
    - Signature from compiler/publisher/program
    - Assigned Unique Identifier from the Programmer
    - Hardware dependent uncloneable feature (e.g., crystal frequency?)
  - Protects part of the memory space (how is not known yet)



- Executable Address Randomisation

Feedback