Purdue Research Foundation

Secure Embedded Wireless Networks

Prof. Saurabh Bagchi
School of Electrical & Computer Engineering, Purdue University

September 10, 2008

Purdue Research Foundation

Product / Service

- Communication protocol that can fit within the constraints of embedded wireless devices
- Secure $\Rightarrow$ No eavesdropping, no masquerading, no compromised nodes

www.otc.purdue.edu OFFICE OF TECHNOLOGY COMMERCIALIZATION

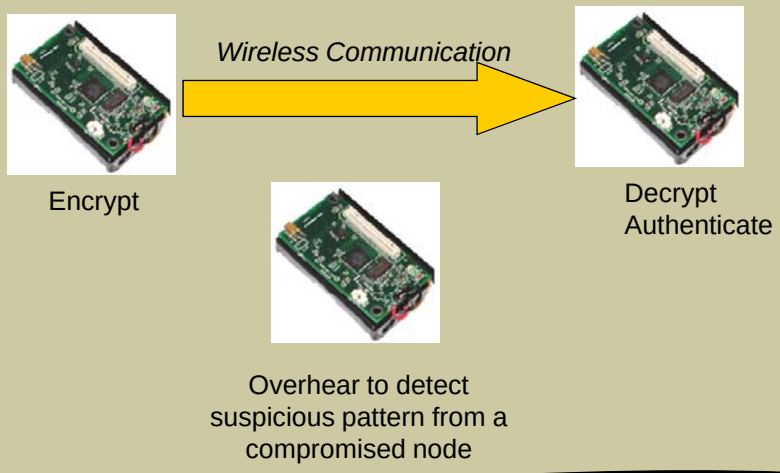
Purdue Research Foundation

Advantages

- Based on Advanced Encryption Standard (AES) protocol already widely used and National Security Agency (NSA) approved
- Fastest AES encryption method available
- Provides secure communication; even when a node has been compromised (local monitoring)
- Science novelty:
  - Software optimizations, including compiler
  - Distributed software requiring no central controller
- Cost effective and easily modified since it is software-based

Purdue Research Foundation

Schematic of Solution



www.otc.purdue.edu OFFICE OF TECHNOLOGY COMMERCIALIZATION

Purdue Research Foundation

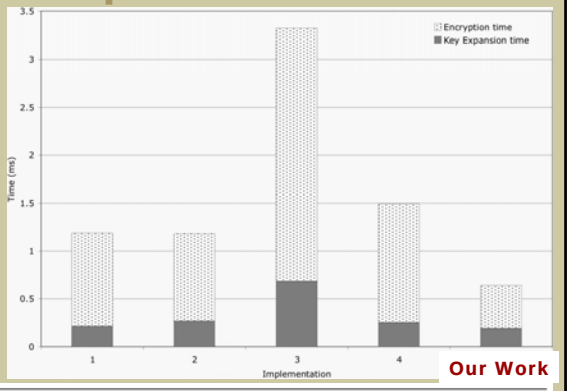
Experiment

- Softbaugh DZ1611 Zigbee Demo Board
- ROM (Code) Size
  - msp430-objdump
- RAM (Memory) Usage
  - msp430-gdb printing stack pointer
- Execution Time
  - Set I/O line on start, clear on end
  - Measure on oscilloscope

Purdue Research Foundation

AES Comparison

- Improved both speed and code size (RAM unknown)
- Note that our measurements seem to have varied significantly from published numbers in some cases

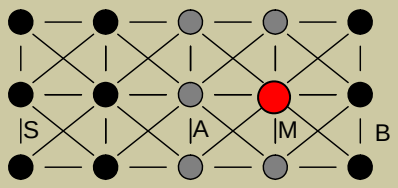


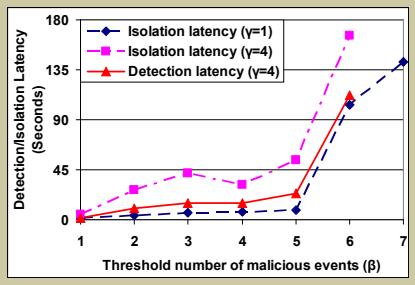
Our Work

Implementation	Reference paper	Measured ROM Usage	Published ROM Usage
1	[6]	5968 bytes	n/a
2	[12]	6780 bytes	12616 bytes
3	[14]	6848 bytes	3322 bytes
4	[10]	n/a	n/a
5	Our implementation	5160 bytes	n/a

Purdue Research Foundation

Internal Malicious Node Detection





- Malicious node *M* – has all the cryptographic keys – thwarting communication to base node *B*

Purdue Research Foundation

Applications

- Military/Homeland Security
  - Secure ad-hoc networking
  - Secure wide area networking
  - Emergency/disaster communications
- Corporate entities where secure wireless communication is a concern
- Hospitals/pharmacies
- E-commerce

www.otc.purdue.edu OFFICE OF TECHNOLOGY COMMERCIALIZATION

Purdue Research Foundation

Team

- Faculty principal investigator:
  Prof. Saurabh Bagchi
- Technical staff: Aaron Ault
- Students: Shammi Didla (undergraduate), Rajesh Panta, Matthew Tan Creti

Purdue Research Foundation

Next Steps

- Patents pending
- Development timelines:
  - Prototype developed & tested, including comparative evaluation
  - Commercial viability = ~1 man year
- Future plans for development
  - Software for the two parts (secure communication, detection of compromised nodes) needs to be ported to a common platform

www.otc.purdue.edu OFFICE OF TECHNOLOGY COMMERCIALIZATION

Purdue Research Foundation

Summary

- Secure communication between nodes using AES that is faster than the wireless network speed
- Detection and isolation of internal compromised node through decentralized protocol

Purdue Research Foundation

Opportunity

- Licensing or start-up opportunity
  - Contact Hilton Turner, Technology Manager
  - 765-496-7539
  - haturner@prf.org