Emerging Paradigms in Sensor Network Security

Department of Electrical Engineering
Texas A&M University

Prof. Deepa Kundur, Ph.D.
Sensor Media Algorithms & Networking for Trusted Intelligent Computing (SeMANTIC) Group

- Dr. Deepa Kundur

Ph.D. Students
- Anli Chen
- Alexandra Czarlinska
- Chuhong Fei
- William Luh
- Nebu Mathai
- Unoma Ndili
- Samer Al-Kiswamy

Undergrad Researchers:
Ashly Kirkland, Jim Griffin, Kyle Marshall, Scott Savage, Peter Mehl, Zuber Abdella
What is a Sensor Network?

- **Well-known definition:**
  - communication + computation + inference + actuation

- **Applications:**
  - Environmental monitoring, “smart” spaces, collaborative media interfaces
  - Military, civilian and industrial surveillance, unmanned aerial and ground vehicles
Properties of Sensor Networks

- Redundant
- Collaborative
- Data-centric
- Actuating
- Application-specific
- Ad hoc
- Untethered
- Autonomous
- Hierarchical
Sensor Nets and Security

- Resource Constraints
- Wireless communications

- Collaborative Processing/Aggregation
- Interaction with Physical Environment
  - Sensing
  - Actuation
Security Strategies

- Establish Trust
- Limit Trust
- Distribute Trust
- Discriminate Trust
Limiting Trust.
Secure Aggregation

BASE STATION

SMALL SCALE MOBILE AGGREGATION

LARGE SCALE STATIC AGGREGATION
Secure Aggregation

- Statistical Disclosure Control
  - Used by Census Bureaus to modify raw data yet preserve statistical properties for later processing
  - Di -> P[Di]
  - Homomorphic Property:
    \[
    \text{AGG}[D_1, D_2, \ldots, D_n] = \text{AGG}[P[D_1], P[D_2], \ldots, P[D_n]]
    \]
Secure Aggregation

- Secure Multiparty Computation
  - Cooperative computation among two or more parties in which no party discloses its input to the others or can have it estimated from the computation result
  - Result known to Aggregator: \( E[\text{AGG}[D_1, D_2, \ldots, D_n]] \)

- Keying information is not employed for aggregation, so attacker is forced to apply a severe DoS attack
Multimedia

- Secure Scalable Coding
  - Scalable coding + progressive encryption
  - (Wee & Apostolopoulos, 2001)
- Watermarking/Steganography
  - Transparent passive security
  - Authentication, copy control, ...
Distributing Trust.
Threshold Secret Sharing

- Separate a secret into $w$ parts such that at least $t$ of them are required to reconstruct the secret
  - (Shamir, 1979)
- Visual cryptography
  - (Naor, Shamir, 1994)
INSIDER ATTACK!
Visual Secret Sharing

PERCEPTUALLY INSECURE!

Courtesy of William Luh
Visual Secret Sharing

- Perceptual security considerations
- Computational security considerations
- Energy considerations
Discriminative Trust.
Encryption and Compression

- **Encryption** → **Compression** → **secured content**
- **content** → **Encryption** → **Compression** → **secured content**
- **compromise** → **Cmpr I** → **Encryption** → **Cmpr II** → **secured content**
- **poor compression** → **incompatible format**
Selective Encryption

I B B P B B I B B P B B B

Group of Pictures (GoP)

Spanos and Maples (1996)
I-frame Coding

8x8 Blocking → Transform eg., DCT, DWT → Quantization Q(.) → Entropy Coding

Metadata (Huffman tables, headers, synchronization information, etc.)

Entropy Decoding → De-quantization → Inv Transform eg., IDCT, IDWT → Block Recomposition

Metadata (Huffman tables, headers, synchronization information, etc.)
Selective Encryption

- **Scramble:**
  - Coefficient order (zigzag scan)
  - Signs of coefficients
Sign Scrambling (Shi and Bhargava, 1998)
Sign Scrambling  (Shi and Bhargava, 1998)
Sign Scrambling (Shi and Bhargava, 1998)
Conclusion

- Intelligent networking security paradigms are embracing multimedia processing
MM Security Achievements

- Provide finer granularity of access control
- Facilitate sophisticated content adaptation in the face of security
- Enable resilience to insider attack
MM Security Inadequacies

- Obfuscation must have a decent definition of trust
  - Avoid security by obscurity
- Perceptual and computational security must synergize
- Security is made “softer” to account for error/adaptation
  - Implications to strength of protection?
Contact Info:

- deepa@ee.tamu.edu
- http://www.ee.tamu.edu/~deepa