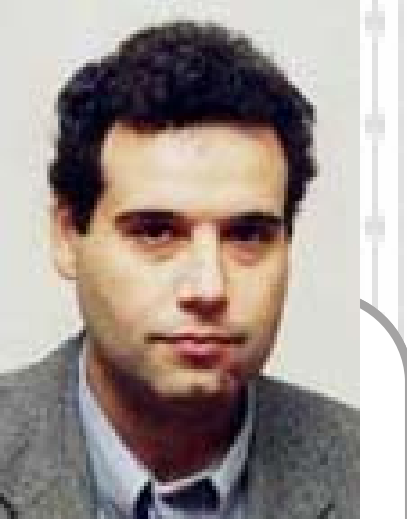


Broadcast/Multicast Security in Multi-User Wireless Sensor Network

Wenjing Lou and Berk Sunar
ECE, Worcester Polytechnic Institute

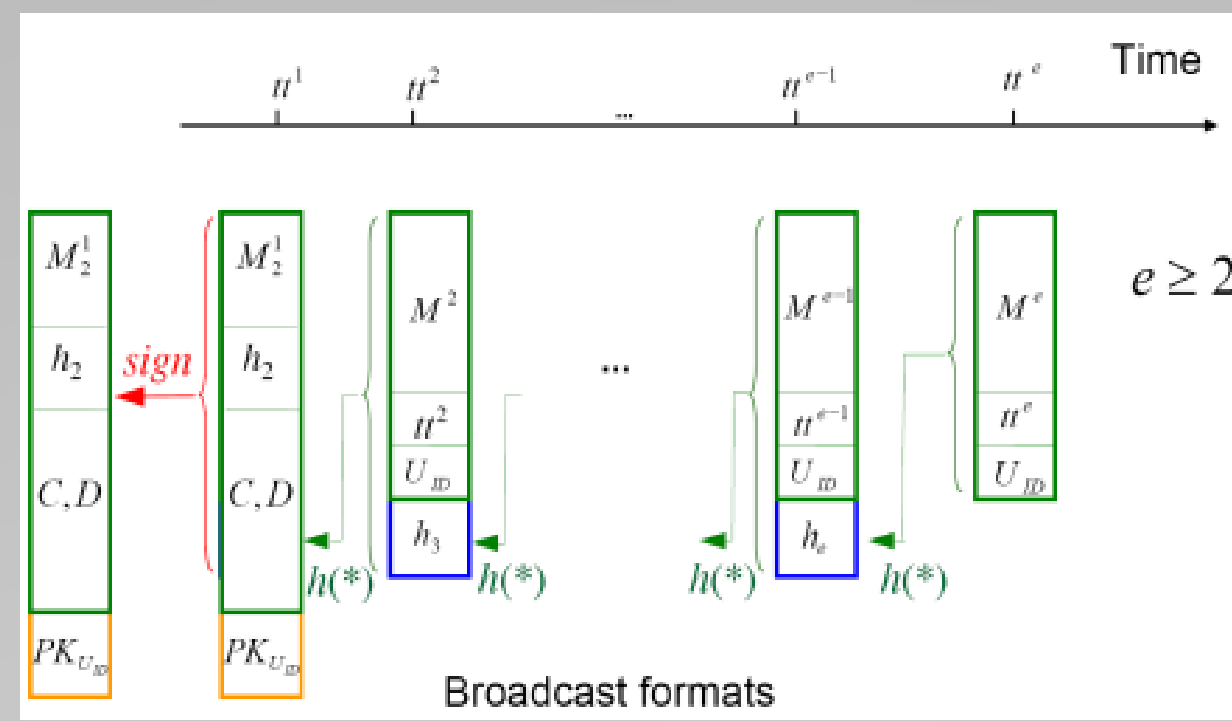
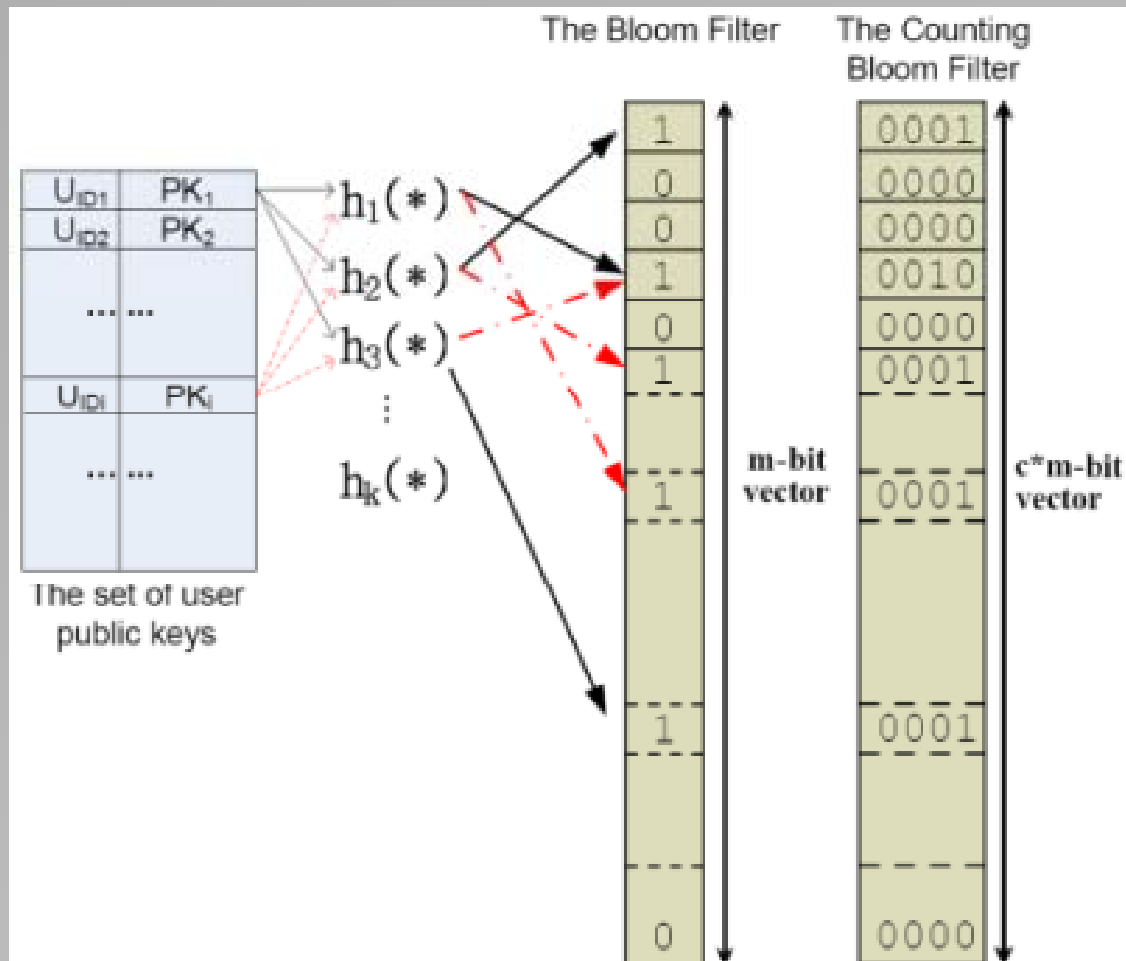
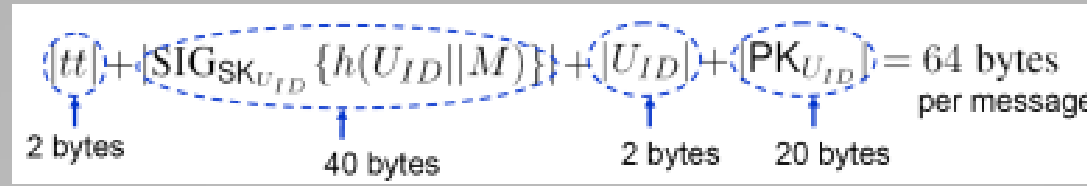
NSF Grant CNS- 0716306



Multi-User Broadcast Authentication

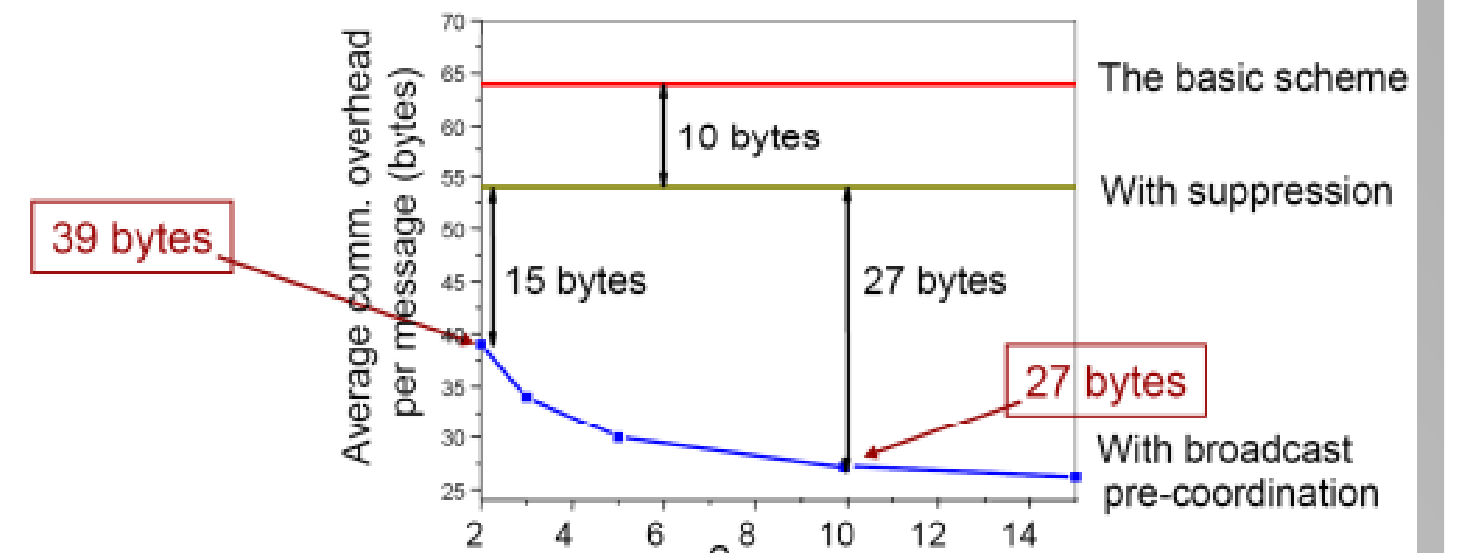
- Problem: provide effective, efficient, scalable, and secure broadcast authentication mechanisms that support a large number of mobile users to broadcast to a multi-hop wireless sensor network anytime from anywhere in the network
- Approach: integrate efficient cryptographic building blocks with public key operations to minimize the overall computation and communication overhead and achieve higher security strength for various application scenarios.

- Immediate Broadcast Authentication
- Memory efficiency: Bloom filter based
- Communication efficiency: partial message recovery, pre-coordinate broadcast messages



Communication overhead:

- Assume that SHA1 is used: $|h_i| = 20$ bytes



Computational overhead:

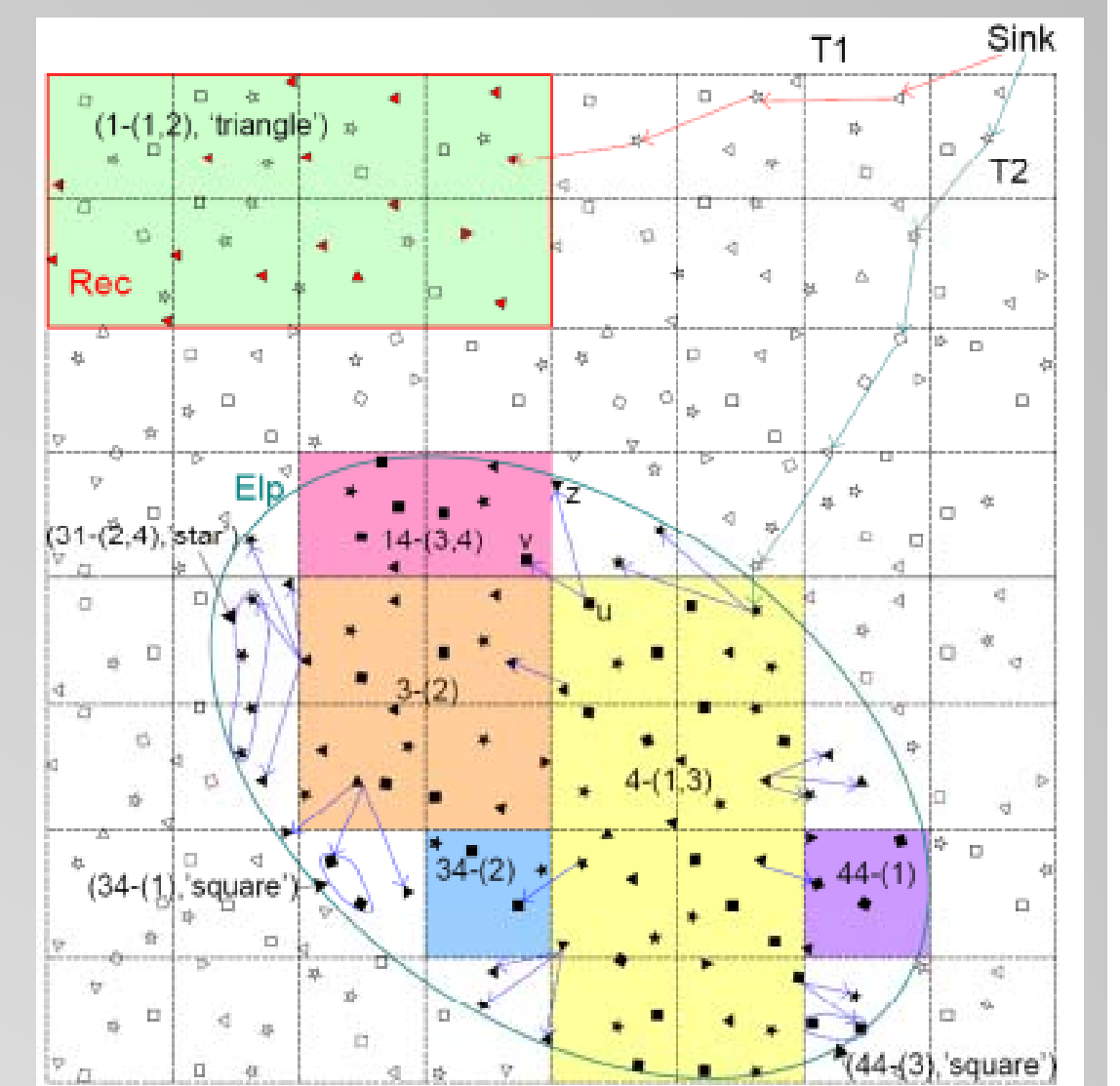
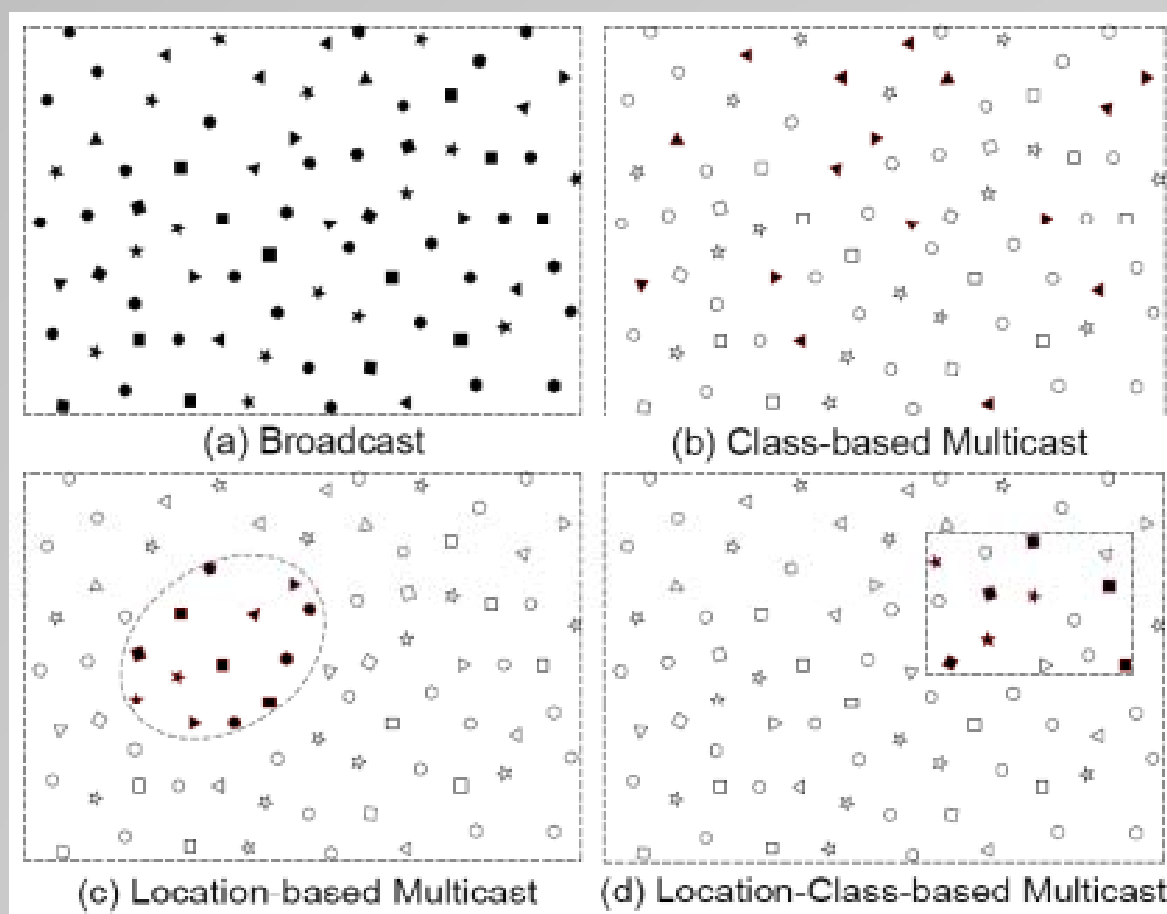
- $1/e$ signature verification per message on average!

Semantic-based Dynamic Multicast Encryption

- Problem: support dynamically forming and changing multicast groups.
- Approach:

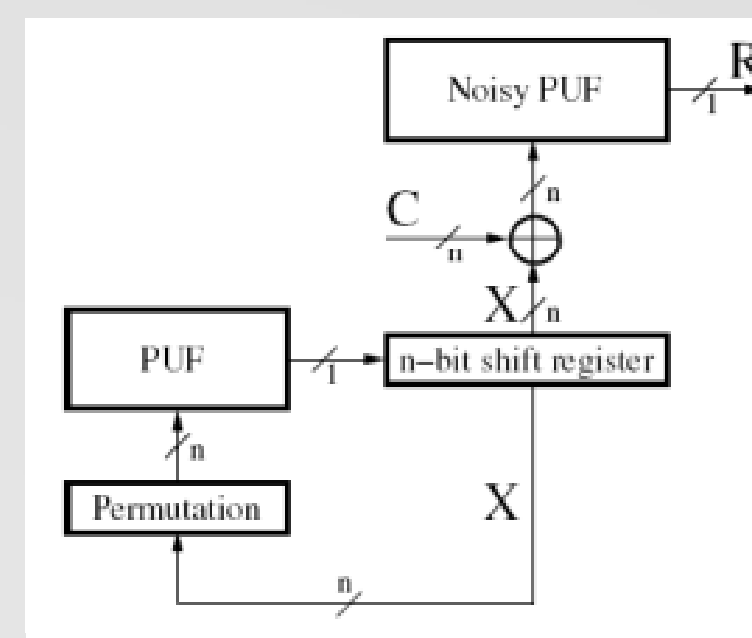
- Semantic-based elementary group concept:** allow the dynamic formation of a multicast group from a more scalable number of elementary groups rather than a large number of independent sensor nodes.
- Quadtree-based location-based group key management:** Each node belongs to multiple location-based elementary groups; the location information of each node is embedded into its keys so that the damage caused by node compromise is minimized.
- Key distribution:** global partition local diffusion, and energy-efficient geographical multicast routing techniques

- Impact:
 - New direction and new methods on secure group communication: dynamically forming new groups.



Low-cost Tamper-proof Authentication for Pervasive Devices

- Problem: cryptographically strong protection for low cost devices (RFIDs, sensor nodes etc.)
- Approach:
 - Use time delay based physically unclonable functions (PUFs) for cheap tamper-resilience.
 - No expensive cryptographic functions: Reuse noisy PUF output to achieve threshold authentication.
 - Eliminate PUF database by forming linear model generated via learning algorithms.
 - Statistically well behaving $\{0,1\}^n \rightarrow \{0,1\}^n$ function from PUF: PUF in feedback mode with random permutation gives nearly ideal random walk in lattice.
- Impact:
 - Tiny footprint: Ideal to protect low-cost high volume applications.
 - Tamper-resilience: Node compromise is no longer a problem.
 - Increased sensitivity: Threshold authentication allows a higher degree of tamper-resilience without sacrificing reliability.



Protocol 1: PUF Enrollment

- S initializes X^0 inside P to a random value
- S collects (X^j, R) pairs from P and uses the values to model the system
- S disables the X^j reading logic

Protocol 2: PUF Authentication

- S picks a random C
- P receives the challenge C, iterates X^j
- P calculates $\tilde{C} = C \oplus X^{j+1}$,
- P enters \tilde{C} into the Noisy PUF circuit
- P sends $R = \text{PUF}(\tilde{C})$ to S
- S accepts P if the number of errors in R is not more than expected from the noisy PUF circuit.