

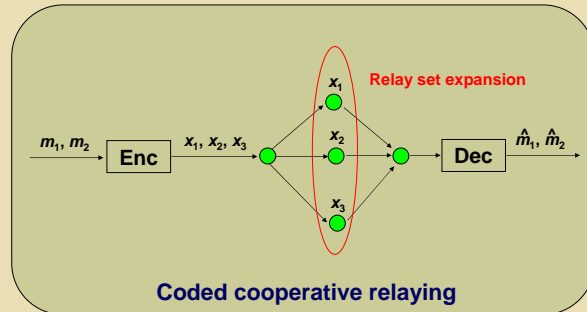
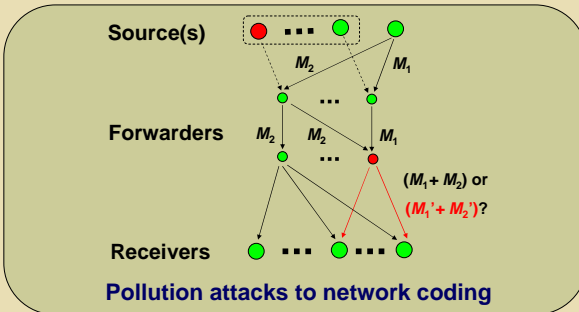
# Secure Network Coding & Coded Cooperative Relaying

Yong Guan, Ahmed Kamal and Sang Kim, Iowa State University, Ames, IA 50011.



## Pollution Attacks to Network Coding & Cooperative Relaying with Channel Coding

- Network coding is useful for maximizing network throughput. However, networks that utilize network coding technique are vulnerable to pollution attacks, where malicious nodes pollute or forge transmitted messages. We propose to design new schemes to secure networks using network coding against pollution attacks.
- Cooperative relaying uses multiple single-antenna relay nodes to realize MIMO systems. It can improve reliability, but may sacrifice data rate and limit the throughput improvement. We propose to combine cooperative relaying with channel coding to achieve significant coding gain without increasing bandwidth requirement.



This project aims at designing new efficient signature schemes for secure network coding against pollution attacks. By verifying the source signature attached to each message, the benign nodes can detect and filter polluted messages. We will also develop a bandwidth-efficient architecture combining channel coding and cooperative relaying to achieve significant energy savings. The redundancy introduced by the code are accommodated by expanding the relay set.

The proposed solutions focus on resource-constrained networks such as wireless sensor networks.

## Comparison to State of the Art

- |   |  |
|---|--|
| <p><b>Secure network coding</b></p> <ul style="list-style-type: none"> <li>• Reduce computation overhead</li> <li>• Accommodate more coding methods</li> <li>• Handle multiple &amp; malicious sources</li> </ul> | <p><b>Coded cooperative relaying</b></p> <ul style="list-style-type: none"> <li>• Reduce energy &amp; bandwidth of relay nodes</li> <li>• Simplify the hardware design of the relay nodes</li> <li>• Provide resilience against malicious attacks</li> </ul> |
|---|--|

## Comparison of Computation Overhead

	Pairing-based scheme	Homomorphic hashing scheme	New approach
Parameter setup	11.3 s	4.69 s	1.68 s
Hash calculation (per msg)	5.73 s	1.55 s	0.42 s
Verification (per msg)	17.59 s	2.33 s	1.58 s

### Homomorphic hashing scheme:

$$E = \sum_{i=1}^n \alpha_i M_i \Rightarrow h(E) = \prod_{i=1}^n h(M_i)^{\alpha_i}$$

### Pairing-based scheme:

- Calculating  $h(M_i) = \sum_{j=1}^m M_{i,j} r_j P_j$ ,

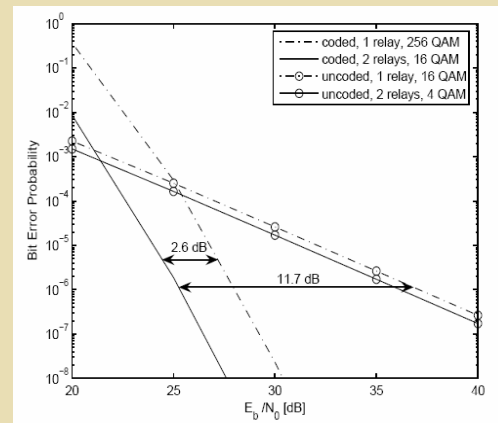
where  $P_j$  are q-tortion points on elliptic curves and  $M_{i,j}$  are codewords of  $M_i$ .

- Verifying  $e_q(h(E), Q) = \prod_{j=1}^m e_q(E_j P_j, r_j Q)$ ,

where  $e_q$  is a pairing function and  $E_j$  are code words of  $E$ .

**New approach:** Homomorphic hashing with more efficient hash calculation and message verification.

## Coding Gain



### Coded Cooperative Relaying:

- Achieving coding gain of 11.7 dB without requiring additional bandwidth compared to uncoded system such as Cooperative Spatial Multiplexing (C-SM).