CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Secure Sensor Network SUM Aggregation with Detection of Malicious Nodes

Sunoh Choi, Gabriel Ghinita, and Elisa Bertino
Department of Computer Science, Purdue University

Motivation

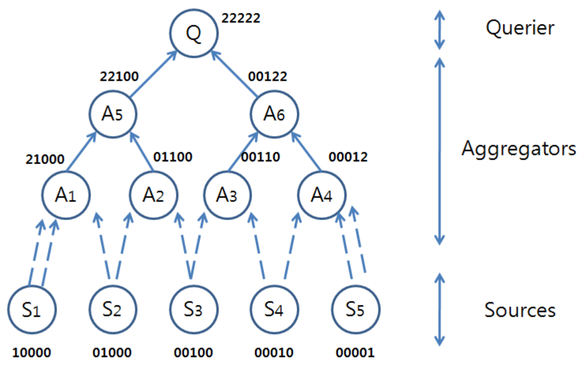
- Secure computation of sums
  - Additively Homomorphic Encryption
- Identify malicious nodes
  - Partial sum
  - Reliable and Efficient communication
  - Divide and Conquer

Bitmap Dissemination Method (BDM)

- Counting Bitmap F_i
  - $F_i = (B_i \mid C_i \mid MAC_i = E(B_i \mid SS_i, K, K_i, p))$
- Aggregation of Counting Bitmaps
  - $F' = (B' = B_i \vee B_j \mid C' = C_i \cdot C_j \mid MAC_i + MAC_j)$
- Authentication of Counting Bitmaps
  - Compute $\sum B_i$ from B' and C'
  - Check $MAC' = E(\sum B_i \mid \sum SS_i, K, \sum K_i, P)$

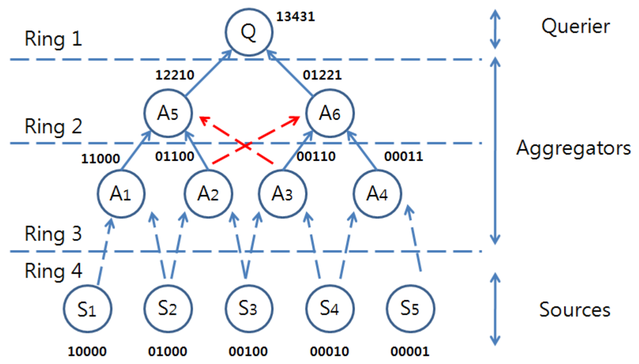
Flexible Aggregation Structure (FAS)

- Each sensor node has *m* parent nodes
- Each aggregator gives counting bitmap for partial sum



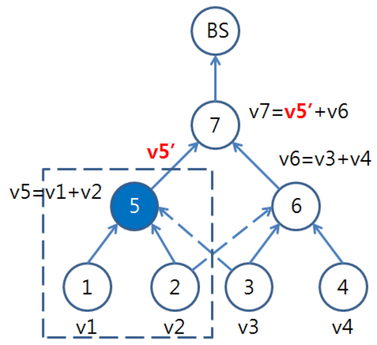
Advanced Ring Structure (ARS)

- All nodes have *m* parent nodes
- Each aggregator gives counting bitmap for multipath

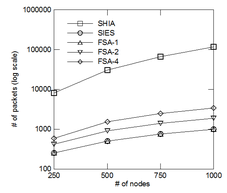


Divide and Conquer Algorithm (DAC)

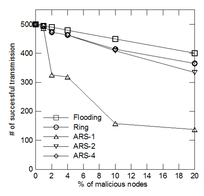
- When a partial sum of a node is not correct, BS requests partial sums of the node's children using FAS and ARS.



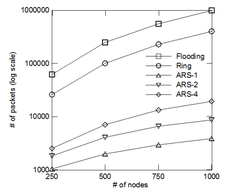
Experimental Results



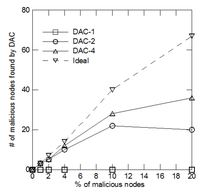
Communication Overhead in Aggregation



Successful Transmission



Communication Overhead in ARS



Performance of DAC

CERIAS

Discovery Park e-Enterprise Center