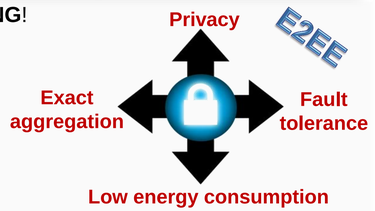
University of Pittsburgh
Computer Science Department

Privacy and Robustness for Data Aggregation in Wireless Sensor Networks

Marian K. Iskander, Adam J. Lee and Daniel Mossé

Introduction/Goals

- Sensors: limited **EVERYTHING**!
  - Bandwidth
  - Storage
  - Power
  - Computation
- Challenges:
  - Data Confidentiality
  - Fault Tolerance



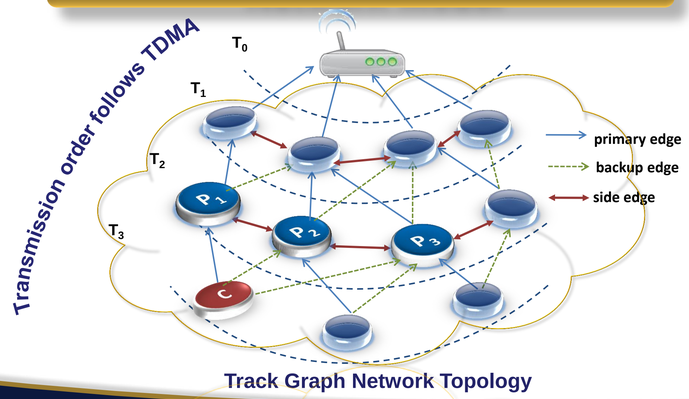
Building Blocks:

Privacy Preservation	Additively homomorphic stream cipher [1]
Robustness	Cascaded Ridesharing [2]

Applications

Collaborative sensing over shared infrastructure

Network Model



Track Graph Network Topology

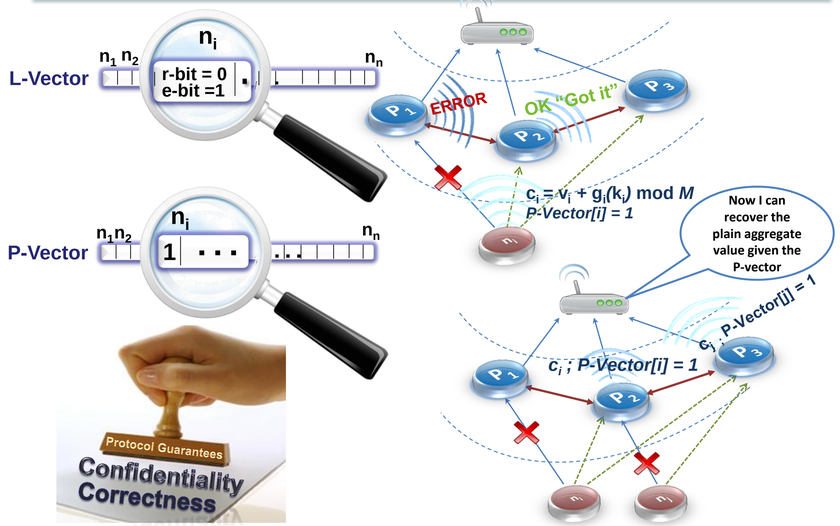
Attack Model

HONEST-BUT-CURIOUS
correctly aggregate, but eavesdrop

QUIET INFILTRATORS
stealthily infiltrate the network to eavesdrop

Protocol

1. Each sensor n_i encrypts its value v_i *as* $c_i = v_i + g_i(k_i) \bmod M$, and sets its corresponding bit in the *P*-Vector.
2. The resulting c_i values are aggregated using the Cascaded RideSharing protocol, which results in the sink receiving the value $C = \sum_i c_i \bmod M$.
3. The sink computes the aggregate key value $K = \sum_i g_i(k_i) \bmod M$ *for each* $i \in$ *P-Vector.*
4. The sink extracts the final aggregate value $V = \sum_i v_i = C - K \bmod M$.



Evaluation

Comparison of four protocols using the CSIM simulator [3]:

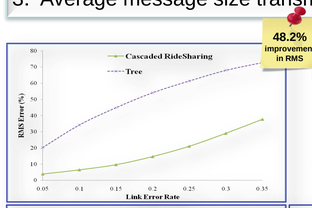
1. Spanning-tree: no fault tolerance, but efficient for power!
2. Cascaded RideSharing
3. Our confidentiality-preserving fault-tolerant aggregation protocol
4. Our protocol with state compression

Results

Comparison metrics :

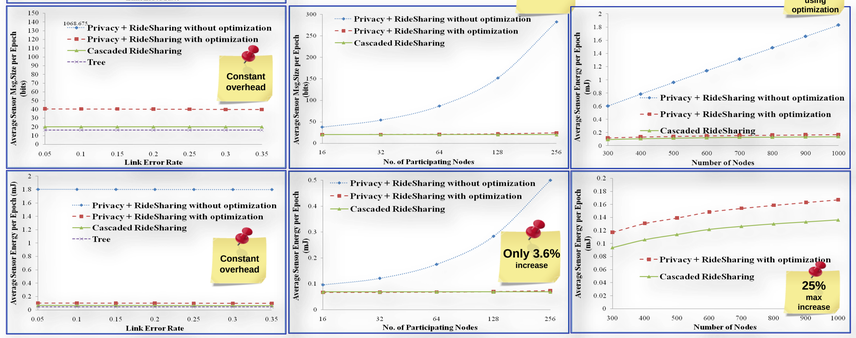
1. Average relative RMS error in aggregated results
2. Average energy consumed per node per epoch
3. Average message size transmitted per node per epoch

Mica2 mote



Simulation Parameters

Parameter	Value Ranges
Total number of nodes	300, 400, 500, . . . ,1000
Link error rate	0.05, 0.10, . . . , 0.35
Number of primary + backup parents	max(3)
Participation level (% of nodes reporting values)	1.5%, 2.5%, 5%, . . . , 25%



1- Effect of Link Error Rate | *2- Effect of Participation Level* | *3- Effect of Network Density*

Conclusions

- New privacy-preserving and fault tolerant in-network data aggregation protocol.
- Improvement of 48.2% in the root mean square (RMS) error of the final aggregate result over the spanning tree schemes (error rate up to 35%).
- Only 7.1% and 3.6% increases in the average message size and average power consumption over the RideSharing scheme.
- Maximum incurred power consumption overhead was 25% (with 100% node participation).

References

[1] C. Castelluccia, A. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks", ACM Transactions on Sensor Networks, Vol. 5, No. 3, Article 20, May 2009.
[2] S. Gobriel, S. Khattab, D. Moss´e , J. Brustoloni, and R. Melhem, "RideSharing: Fault tolerant aggregation in sensor networks using corrective actions", IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks,in SECON, 2006.
[3] "CSIM Simulator", http://www.mesquite.com/.

Appeared in 17th ACM Conference on Computer and Communications Security, CCS 2010