SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks

Yi Yang, Xinran Wang, Sencun Zhu, Guohong Cao

Why Data Aggregation?

- ✓ **Sensor Networks**
  - ❖ **Functions**
    - – **Sensing**
    - – **In-network Processing**
    - – **Ad-hoc Communication**
  - ❖ **Applications**
    - – **Military Surveillance**
    - – **Homeland Security**

- ✓ **Without Aggregation**
  - ❖ **Data Redundancy**
  - ❖ **Communication Cost**
  - ❖ **Energy Expenditure**
- ➢ **Reporting Raw Data is Unnecessary!**
- ✓ **Aggregation Reduces Overhead in Data Collection!**

Security Challenges

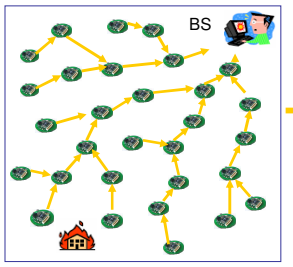
- ✓ **A Lossy Data Compression Process**
- ✓ **Compromised Intermediate Nodes Change Aggregated Data**
- ✓ **BS cannot Verify Results without Knowing Original Readings**
- ➢ **How can BS Obtain a Good Approximation of Aggregation Result with a Fraction of Compromised Nodes?**

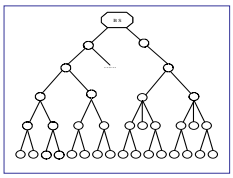
Our Solutions

Divide and Conquer

– **Partition Aggregation Tree into Multiple Logical Groups of Similar Sizes**

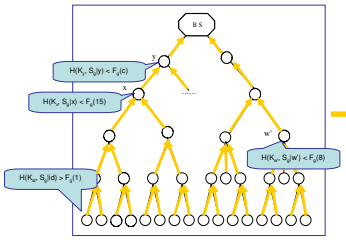
Tree Construction & Query Dissemination

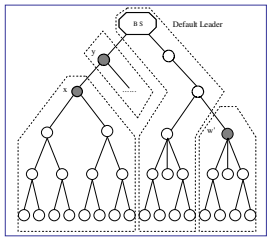




- – **An Unbalanced Tree Rooted at BS**
- – **Data are Aggregated Hop by Hop**
- – **Each Aggregate is (Value, Count)**
- – **Every Node Forwards Only One Copy**

Probabilistic Grouping & Data Aggregation

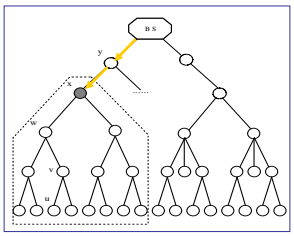


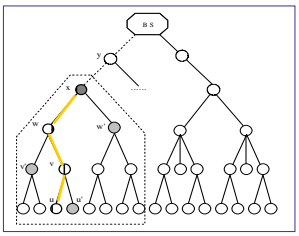


Commit and Attest

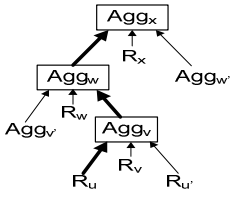
– **Each Group Generates a Commitment that cannot be Denied Later**
– **BS Identifies Abnormal Groups from Set of Group Commitments based on a Bivariate Multiple Outlier Detection Grubbs' Test**
– **Groups under Suspicion Prove Correctness of Submitted Commitments to BS by Probabilistic Path Selection**
– **BS Discards Commitments from Groups Failing to Support Previous Values when Computing Final Aggregates**

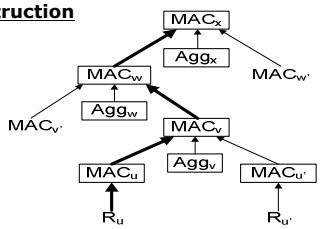
Group Attestation





BS Reconstruction





Security Analysis and Performance Evaluation

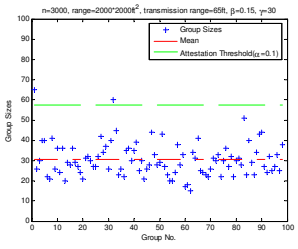
❖ Zero False Positive Rate

– **Attack-free Groups will Pass Grubbs' Test anyway**

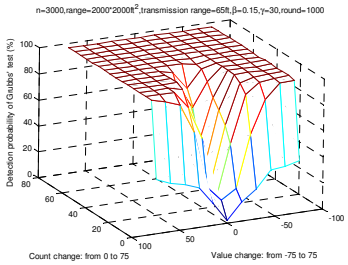
❖ Grouping Function

– $F_g(c)=(1-e^{-\beta c})^{\gamma}(0<\beta\le 1,\gamma\ge 1)$

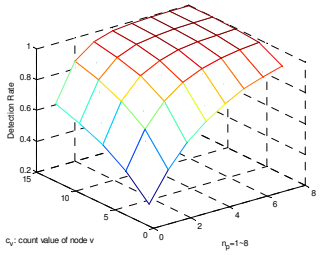
Grouping Result



Detection Capability of Grubbs' Test



Detection Capability of Group Attestation



Message Overhead in Packet*Hop