Sensor Networks – Hop-by-Hop Authentication

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 24)

Introduction

- Sensor networks are subject to false data injection attacks
  - Deployed in unattended environments
  - Goal may be to deceive base station or deplete resources on relaying nodes
- Interleaved hop-by-hop authentication scheme guarantees detection of injected false data packets
  - If no more than t nodes are compromised

Application Scenario

- Military application of sensor networks for reconnaissance of the opposing forces
- Deploy a cluster of sensor nodes around each area of interest
  - Tank movements, ship arrivals, munition plant
  - Deploy a base station in a secure location to control the sensors and collect data
- An adversary may compromise several sensor nodes
  - Inject false data into the network
  - Traditional authentication not good since adversary knows all the keying material possessed by the compromised nodes
- Goal of research - address false data injection attack
  - Base station verifies the authenticity of report
  - Filter out false data packets injected by compromised nodes

Proposed Solution

- Hop-by-hop authentication scheme in which at least t+1 nodes have to agree upon a report before sending it to the base station
- All nodes in the path from the source to the base station participate in authenticating the report in an interleaved fashion
- Guarantees detection subject to a security threshold
  - No more than t nodes are compromised

Assumptions

- Sensor nodes are organized in clusters (at least t+1 nodes)
- Cluster head role may be rotated
- Network links are bidirectional
- Every node shares a master key with BS
- Each node establishes a pairwise key with its one-hop neighbors
  - One could use LEAP to achieve this
  - Also, a node can establish pairwise keys with other nodes
- All nodes within a cluster are equally trusted
- Base station has a mechanism to authenticate broadcast messages (μTesla)
- BS will not be compromised

Design Goals

- When there are no more than t compromised nodes
  - BS should be able to detect any false data packet injected by a compromised node
  - No. of hops before an injected data packet is detected and discarded is small
  - Scheme should be efficient in computation and communication
  - Scheme should be robust to node failures

Definition of Association

- Two nodes ui and uj on the path from CH to BS are associated if their difference = t+1
- If i – j = t+1, ui is upper associated node of uj and uj is lower associated node of ui
- A node that is less than t+1 hops away from BS doesn't have an upper associated node
- An intermediate node may have multiple lower associated nodes
  - If it has multiple child nodes leading to multiple clusters
- A node ui that is less than t+1 hops away from CH has one of the cluster nodes as lower associate
- CH is associated with u(t+1)

Scheme Overview

- The security scheme has 5 phases
  - Node initialization and deployment
  - Association discovery
  - Report endorsement
  - En-route filtering
  - Base station verification

Node Initialization and Deployment

- Key server loads every node with a unique id and necessary keying material
  - Preloads node u with an individual key Ku shared with the BS
  - From Ku, node u derives its authentication key
- Node u then establishes pairwise keys with its neighbors using LEAP or any other protocol
- In summary, node u discovers its 1-hop neighbors and establishes pairwise keys

Association Discovery

- It is done in a two-way fashion
- It is needed to discover the id's of a node's associates
- First step is Base station Hello (discover upper associate)
- Second step is Cluster ACK (discover lower associate)
- If the path is static, this is a one-time investment
- Otherwise, you have to do an incremental association (whenever the path from CH to BS changes)
- Since ACK is critical for a node to maintain correct association, ACK may be done in an authenticated manner (using MACs)

Report Endorsing

- Sensor nodes generate a report when triggered by a special event
- The scheme requires that at least t+1 nodes agree on the report for consideration
- This means that if t > 0, an adversary cannot cause a false report by compromising just one sensor node

Report Endorsement Steps

- Node v first sends endorsement report to CH using two MACs
  - When a node v agrees on event E, it computes a MAC for event E using its authentication key derived from the BS (Individual MAC)
  - In addition, it computes another MAC using the pairwise key with its upper associate (pairwise MAC)
- CH collects endorsements from t+1 nodes including itself
- Compresses the t+1 individual endorsements into one XMAC (by ex-oring) after authenticating each one of them
- Final report R to be sent consists of E, a list of id's of the endorsing nodes, XMAC, t+1 pairwise MACs
- R is authenticated with the pairwise key between CH and the next node in the path to the BS

En-route Filtering

- Node u upon receiving R from downstream node, first verifies authenticity of R (using its pairwise key)
- It then checks the no. of different pairwise MACs in R
- If node u is s (s < t+1) hops away from BS, it should see s MACs, otherwise, t+1 MACs
- It then verifies the last MAC in the list based on the pairwise key shared with its lower associate
- Node u will drop the report if any of the above checks fails
- If u is more than t+1 hops away from BS, it proceeds to compute a new pairwise MAC over E using its upper associate's pairwise key
- It then removes the last MAC from the MAC list and inserts the new MAC
- It then forwards the report to its upstream node
- Each node is thus able to verify one pairwise MAC (lower associate) in the report independently in addition to MAC computed by its direct downstream node

Base Station Verification

- Base station BS only needs to verify the compressed MAC
- It computes the t+1 MACs over E using the authentication keys of the nodes in the id list, then XOR the MACs to see if it matches the one in the report
- BS is assumed to know the location of the cluster nodes
  - After reading the report (authenticated), it can react to the event coming from the clusters
  - If the verification fails, BS will discard the report

Security Analysis

- Ability of the BS to detect a false report and ability of the en-route nodes to filter false reports
  - Base station detection – guaranteed as long as no more than t nodes try to forge a report (scheme compresses t+1 individual MACs and this compression is secure)
  - En-route filtering – analysis shows that both cluster insider attacks and en-route insider attacks can be detected and false packets can be dropped

References

- Sencun Zhu, Sanjeev Setia, Sushil Jajodia, Peng Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks", *Proceedings of IEEE Symposium on Security and Privacy (S&P'04),* Oakland, California, May 2004