A Distributed Authentication Scheme For A Wireless Sensing System

Kevin Bauer and Hyunyoung Lee
Department of Computer Science
University of Denver
{kbauer, hlee}@cs.du.edu

2nd International Workshop on Networked Sensing Systems
San Diego, CA June 28, 2005
Presentation Outline

- Introduction and Background
- System Model
- Explanation of our proposed scheme
- Analysis and Proof of Correctness
- Conclusion and Questions
Introduction (1)

- The broadcast nature of wireless network transmissions presents a significant security vulnerability.

- Popular public-key cryptographic schemes such as RSA and shared secret key exchange protocols such as Diffie-Hellman are particularly vulnerable in wireless networks to:
  - Impersonation attacks
  - Man-In-The-Middle (MITM) attacks
Introduction (2)

- Further complications in sensor networks:
  - Limited CPU, main memory, battery and other resources make most public-key cryptographic schemes too expensive
  - Symmetric key schemes are vulnerable to attack by a more computationally sophisticated device like a mobile laptop computer
Introduction (3)

Therefore, we introduce a unique approach to security in wireless sensor networks to address node authentication.

Informally, authentication is the degree to which one communicating party can prove the valid identity of another party in the network.

Our approach is:
- Efficient: Practical for wireless sensors
- Fault-tolerant: Resilient to a given threshold of corrupt (Byzantine faulty) processes
- Distributed: Every node can make local decisions
- Randomized: Guarantees that corrupted parties cannot influence the authentication protocol.
Background

- Our authentication scheme employs:
  - Secret Sharing Cryptography
    - A “secret” $D$ is partitioned into $n$ “shares,” $D_0, D_1, D_2, \ldots, D_{n-1}$ and distributed to each trustee $t_i \in T$
    - At least $k$ shares $D_i$ (for $k = |R|$, $R \subseteq T$) must be present to compute $D$
  - Randomized Group Consensus
    - A method for achieving agreement among distributed processes in an asynchronous communication environment
    - A “COIN_FLIP” operation provides randomized inputs to overcome the Fischer, Lynch, Paterson impossibility result with high probability
Pictorial System Model

Subgroup A

Sensor Nodes

Wired Communication link

Subgroup B

Base Station

Processing Center (PC)

Subgroup C

Base Station
Abstract System Model

We abstractly model a wireless sensor network $S$ by the tuple $\langle N, T, M \rangle$ where:

- $N$ is the set of sensors in the network
- $T \in N$ is the "target" node in $S$ to be authenticated
- $M$ is the set of message channels between an arbitrary sensor and its base station
Processing Center (PC)

- The Processing Center (PC) has the following duties:
  - Assign each node a unique identification (ID) number from the set of natural numbers
  - Inform node $t_i$ of its logical ring successor, $t_{i+1}$ and its predecessor, $t_{i-1}$
  - Maintain a secret for each node
  - When necessary compute shares of a particular secret and distribute to the trustee set
Proposed Scheme - Initialization

1. A target $T$ is chosen for authentication

2. $T$ notifies the PC that it must be authenticated

3. The PC computes $|N| - 1$ $s_i$ shares of $T$'s secret and broadcasts to each trustee $t_i \in N \setminus \{T\}$ a $s_i$ share
Select Challengers

Every non-target node $u \in N \setminus \{T\}$ selects its logical ring successor $v$ to be a challenger with a probability, $p$

For $p = 1/a \ (\log_2 (a + 1))$, with $a = |N| - 1 / 2k + 1 \geq 1$

- **COIN_FLIP() = TAIL**
  - $v$ is not elected
    - Do nothing

- **COIN_FLIP() = HEAD**
  - $v$ is elected:
    1. $u$ broadcasts “$v$ is a challenger” message
    2. $t_i$ sends its share to $v$
    3. $u$ keeps track of $v$
Receive & Reconstruct Secret

- For each node \( v \in N \setminus \{T\} \) elected to the challenger set:
  - Receive a share from every \( t_i \in N \setminus \{T\} \) and store it locally
  - Reconstruct the secret from the shares, \( \text{secret} \)
  - Request \( T \)'s secret, \( T\text{secret} \)
  - If \( T\text{secret} = \text{secret} \), then broadcast "true"
  Else broadcast "false"
Decide Authenticity

- Upon receiving a “true” or “false” message:
  - $\forall v \in challengers$
    - Receive each challenger’s vote and keep track of the number of “true” votes (as local variable $true\_counter$)
  - If $true\_counter > \frac{1}{2}(|N| - 1)$ then
    - $T$ is authentic
  - Else
    - $T$ is not authentic

- The PC must refresh $T$’s secret and redistribute new shares to the trustees
Analysis Overview

- Our scheme:
  - Selects challenger nodes fairly
  - Selects challenger nodes with a probability \( p = \frac{1}{a} \left( \log_2 (a + 1) \right) \), for \( a = |N| - 1 / 2k + 1 \geq 1 \)
  - Requires:
    \( \mathcal{O}(|N| \log_2 |N|) \) secure messages
    \( \mathcal{O}(\log_2 |N|) \) broadcast messages
    \( \theta(b_{secret} |N| \log_2 |N|) \) bits in total*

*Using Shamir's polynomial interpolation secret sharing
Proof of Correctness (1)

Probability $p$ as a Function of the Number of Nodes
(Localized Trend)

$|N| - 1$

$p$

$k = 1$

$k = 2$
Proof of Correctness (2)

Probability $p$ as a Function of the Number of Nodes
(Generalized Trend)

$|N| - 1$

$k = 1$
$k = 2$
Concluding Remarks

- Our primary contribution is a unique authentication scheme that is:
  - Efficient
  - Fault-tolerant
  - Distributed
  - Randomized
  and, therefore, well-suited to the resource constraints of wireless sensor networks

- Future work: Simulation as verification of the analytical result
The End

Questions & comments