An Authentication Framework for Wireless Sensor Networks using Identity-based Signatures

Rehana Yasmin
R.Yasmin@cs.bham.ac.uk

Co-authors: Dr Guilin Wang, Dr Eike Ritter
University of Birmingham
Outline of the Presentation

- Introduction
- Challenges
- Existing Approaches in WSN
- Problem Definition
- Proposed Authentication Framework
- Comparison with Existing Schemes
- Conclusion & Future Work
Introduction: Wireless Sensor Networks

- Composed of small low cost resource constrained sensor nodes (motes)
- Monitor and report certain phenomenon
- Adversary can inject false data packets, modify original data packets
- Adversary can also compromise sensor nodes
Introduction: Authentication

- Countermeasure: Authentication
  - Verify claimed message sender
  - Contents of a message

Authentication in Wireless Sensor Networks

- Base station to sensor nodes
- Sensor node to other sensor nodes
- Outside user to sensor nodes
  - Session key establishment
  - Access control enforcement
Challenges

Why not use conventional authentication mechanisms?

• Sensor nodes are resource constrained devices
  ❖ Low processing capability
  ❖ Low battery power
  ❖ Low storage
  ❖ Low bandwidth

• Hurdle in applying strong cryptographic based authentication schemes e.g., digital signatures

• Compromised sensor nodes do not allow Message Authentication Code
Existing Approaches: $\mu$-TESLA


Issues with $\mu$-TESLA based Schemes

- Base station to other sensor nodes authentication
- Sensor node broadcasts through base station only
- Not suitable for real time applications
- Delayed authentication
- Denial of Service (DoS) attack
- Multiple senders broadcast turn by turn during predefined time intervals
- Support only limited number of broadcast senders
Existing Approaches: Digital Signature
[Ren 2007, Cao 2008]

Issues with Digital Signature based Schemes

• Public key and certificate management
  ❖ Send public key and certificate with every message
    ❑ Low bandwidth
    ❑ Two signature verifications per message
  ❖ Store public key of each sender
    ❑ Storage overhead
    ❑ Reduces scalability
  ❖ User authentication also suffer from the same problem

• Message signing expensive in terms of time and energy consumption
Problem Definition

• Authentication mechanism which provides
  
  ❖ Broadcast or multicast without the involvement of base station
  ❖ Quick broadcast of real time messages
  ❖ Authentication of messages
  ❖ Authentication of any outside user

• Public key and/or certificates management
Proposed Authentication Framework

- An authentication framework which utilizes
  - Identity-based signatures
    AND
  - Online/Offline signature schemes
Proposed Authentication Framework

Identity-based Signatures

[Shamir84, ...]

- User can use his identity information as his public key

- Corresponding private key generated by a private key generator (PKG)

- Eliminates the need of a certificate
Proposed Authentication Framework

Online/Offline Signatures

[Even 1989, …]

- Message signing is divided into two phases:
  - **Offline** phase
  - **Online** phase

- Offline phase performed by a resourceful device

- Suitable for resource constrained signer
Proposed Authentication Framework

The proposed authentication framework

• Comprised of two authentication schemes
  ❖ Sensor Broadcast Authentication
  ❖ Outside User Authentication

• Utilizes
  ❖ ID-based online/offline signature (IBOOS) for sensor broadcast authentication
  ❖ ID-based signature (IBS) for outside user authentication
Sensor Broadcast Authentication Scheme

- Base station, a resourceful and trustworthy entity, plays the role of PKG
- First two phases are performed before the deployment

1. **System Initialization**
   - Base station computes:
     - msk $SK_{PKG}$, mpk $PK_{PKG}$, system parameters $SP$

2. **Key Generation**
   - Base station computes:
     - private keys $D_{ID}$ corresponding to user ID
   - ID, $D_{ID}$, $PK_{PKG}$ and SP are stored on sensor nodes before deployment
Sensor Broadcast Authentication Scheme

3. Message Broadcast
   • Offline phase: performed on base station (before hand)
     \[ S \leftarrow \text{OffSign}(D_{ID}, SP) \]
   • Online phase: performed on sensor node
     \[ s \leftarrow \text{OnSign}(m, S, TS) \]

4. Authentication
   • On receiving a message, sensor node
     ❖ Verifies time stamp \( TS \)
     ❖ Verifies signature using signer’s ID and system parameters
     \[ 0/1 \leftarrow \text{Ver}(m, ID, s, SP) \]
Outside User Authentication Scheme

• Base station, a resourceful and trustworthy entity, plays the role of PKG

1. System Initialization
   Same as in first scheme

2. Key Generation
   Same as in first scheme

3. User Registration
   • Performed every time when a new user is registered with the system
   • Base station computes:
     - private key $D_{ID}$ corresponding to user ID
   • User U receives $ID_U$, $D_{ID_U}$, $PK_{PKG}$ and SP from base station through a secure channel
Outside User Authentication Scheme

4. User Request
   • User U signs his request and sends to sensor node N

   \[ U \rightarrow N: \{RM, TS, ID_U, \sigma\}, \text{ where} \]
   \[
   \sigma \leftarrow \text{Sign} \left( (RM, TS, ID_U), D_{ID_U} \right)
   \]

5. User Authentication
   • On receiving a user request, sensor node
     - Verifies time stamp \( TS \)
     - Verifies signature using user’s ID and system parameters

     \[ 0/1 \leftarrow \text{Ver} \left( m, ID_U, \sigma, SP \right) \]
Outside User Authentication Scheme

6. Session Key Establishment

- We propose to use ID-based one-pass session key establishment protocol.
- During authentication phase, user also sends his ephemeral key $E_U$.
- After successful user authentication, sensor node computes session key using $E_U$.
- The only message exchanged is signed by the user, verified by the sensor node.
- Designed our own new ID-based one-pass key establishment protocol.
## Comparison with Existing Schemes

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Signature Schemes</th>
<th>Energy Cost (Offline) mW</th>
<th>Energy Cost (Online) mW</th>
<th>Computation Time (Online) s</th>
<th>Storage Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Existing Broadcast Authentication Schemes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAS [Ren2007]</td>
<td>ECDSA</td>
<td>0</td>
<td>26.96</td>
<td>0.89</td>
<td>-</td>
</tr>
<tr>
<td>DAS [Ren2007]</td>
<td>ECDSA</td>
<td>0</td>
<td>26.96</td>
<td>0.89</td>
<td>22N = 1.2MB</td>
</tr>
<tr>
<td>IDS [Ren2007]</td>
<td>Pairing based</td>
<td>0</td>
<td>87.09</td>
<td>3.47</td>
<td>-</td>
</tr>
<tr>
<td>IMBAS [Cao2008]</td>
<td>BNN</td>
<td>0</td>
<td>72.90</td>
<td>2.43</td>
<td>-</td>
</tr>
<tr>
<td><strong>Proposed Sensor Broadcast Authentication Scheme</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposed</td>
<td>IBOOS [Ren2008]</td>
<td>φ*</td>
<td>5.62</td>
<td>0.19</td>
<td>-</td>
</tr>
<tr>
<td>Proposed</td>
<td>IBOOS [Xu2005]</td>
<td>48.60</td>
<td>ε*</td>
<td>ε*</td>
<td>-</td>
</tr>
</tbody>
</table>

N = 50,000, φ* shows the cost of underlying signature scheme and ε* shows negligible cost

Rehana Yasmin

## Comparison with Existing Schemes

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Signature Schemes</th>
<th>Energy Cost (mW)</th>
<th>Verification Time (s)</th>
<th>Storage Overhead (Bytes)</th>
<th>Session Key</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Existing User Authentication Schemes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RRUASN [Benenson2004]</td>
<td>ECDSA</td>
<td>106.84</td>
<td>3.54</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>DP²AC [Zhang2009]</td>
<td>RSA</td>
<td>14.05 + TE</td>
<td>0.47 + TT</td>
<td>10*T</td>
<td>No</td>
</tr>
<tr>
<td><strong>Proposed User Authentication Scheme</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposed</td>
<td>IBS [Cao2008]</td>
<td>72.90</td>
<td>2.43</td>
<td>0</td>
<td>Yes</td>
</tr>
</tbody>
</table>

TE = Transmission Energy  
TT = Transmission Time  
T = Used Tokens
Importance of Work and Advantages

• First attempt to handle the problem of authenticated broadcast by sensor nodes
• First application of online/offline signature to wireless sensor networks

• Primary advantages of the proposed authentication framework:
  💣 Reusability
  💣 Efficiency
  💣 Public keys and certificates management
  💣 Scalability
Conclusion & Future Work

- **Proposed authentication framework**
  - Efficient in terms of computation time and energy consumption
  - Solves the problem of public keys and certificates
  - Provides scalability

- **In future,**
  - Implementation on real sensor nodes
  - Access control
References

Existing Approaches

μ-TESLA [Perrig 2002]

- Micro Timed Efficient Stream Loss-tolerant Authentication
- Message Authentication Code (MAC)
- Symmetric cryptography introduces asymmetry
- Base station to sensor nodes broadcast authentication
Existing Approaches

μ-TESLA (continued)

Sender Setup

- One-way hash key chain

- Key commitment $K_0$ stored on every receiver

- Time divided into $n$ equal parts

- Each key from key chain assigned to one time slot

![Diagram of key chain and time slots]

$K_3 \quad K_4 \quad K_5 \quad K_6 \quad K_7$

$t_3 \quad t_4 \quad t_5 \quad t_6 \quad t_7 \quad t$
Existing Approaches

μ-TESLA (continued)

Broadcasting Authenticated Packets

- In time interval $i$, the sender uses key $K_i$ to compute MAC
- Same MAC key for all packets in that interval
- In time interval $(i + \delta)$, the sender reveals key $K_i$
- $\delta$ depends on round trip time between the sender and the receivers
Existing Approaches

μ-TESLA (continued)

Authenticating Broadcast Packets

- Sender and receivers need to be loosely time synchronized
- Receivers need to know the key disclosure schedule
- A packet verification involves three steps
  - First, to see if packet is safe
  - Second, to verify the received MAC key
  - Third, to verify MAC using verified MAC key