Outline

- Introduction
  - Broadcast Authentication
  - DoS Attacks against Broadcast Authentication
- Assumptions
- The proposed scheme based on PKC
- Simulation
- Conclusions
A denial of service (DoS) attack is an attempt to make a computer resource unavailable to its intended users.
A typical sensor network usually has one or more sinks (commanders). They broadcast commands to sensors, which act upon those commands.

Security is critical for sensor networks deployed in hostile environments, such as military battlefields and security monitoring.
Broadcast Authentication

One-way hash chain

- The sender first selects a random value $K_n$ as the last key in the key chain.
- Then repeatedly performs a one-way hash function, $F()$, to compute all the other keys.

$K_0 \xrightarrow{F} K_1 \xrightarrow{F} K_2 \xrightarrow{F} \ldots \xrightarrow{F} K_{n-1} \xrightarrow{F} K_n$

commitment
Introduction

- TESLA protocol provides efficient authenticated broadcast. However, TESLA is not designed for such limited computing environments.
- The TESLA-related part of the packet would be constitute over 50% of the packet.
- It is expensive to store a one-way key chain in a sensor node.
Introduction

- Public key cryptography (PKC), also known as asymmetric cryptography
  - Public key encryption
  - Digital signatures

A random number \( \rightarrow \) Key generation function

BS(sender)

Private key

Public key
Introduction

- Public key encryption

Only private key can decrypt this packet.

A packet encrypted with public key
Introduction

- Digital signatures
Signature verification using 160-bit elliptic curve keys on ATmega128, a processor used in Mica motes, may take as much as 1.6 seconds.

If every node verifies the incoming packets before forwarding them, there will be a long delay for remote nodes to obtain an authentic message.

- Authentication-first or forwarding-first
Introduction

- DoS attacks against broadcast authentication
Assumptions

- All nodes and attackers are **static**.
- Attackers can choose their locations, or take **multiple identities**.
- Their goal is to **exhaust the energy** of the nodes, and to **increase the response time**.
Assumptions

- Attackers do **not always** send fake messages. They can also forward authentic messages.
This paper presents a dynamic window scheme, where sensor nodes determine whether first to verify a message or first to forward the message by themselves.

Each node needs to maintain a parameter - authentication window size $\omega$. 
The proposed scheme based on PKC

If fake, $\omega = \omega/2$
Else $\omega = \omega + 1$
The proposed scheme based on PKC

4 > \( \omega \) → authentication first

3 ≤ \( \omega \) → forwarding first

1 ≤ \( \omega \) → forwarding first

If fake, \( \omega = \omega / 2 \)
Else \( \omega = \omega + 1 \)

If fake, \( \omega = \omega / 2 \)
Else \( \omega = \omega + 1 \)
Simulation

- **5000** sensor nodes are randomly deployed into an area of **200m × 200m**.
- The transmission range of sensor nodes set as **6m**.
- It takes **2 seconds** for a node to authenticate a message.
Simulation

![Graph showing the portion of nodes receiving and forwarding fake packets as a function of the ratio of fake messages to authenticated messages. The graph illustrates the decrease in the ratio of fake packets being received and forwarded as the ratio increases.]
Simulation

![Simulation Graph]

- Dynamic window scheme
- Authentication-first scheme
- Forwarding-first scheme

Average broadcast delay (sec)

ratio = numFakeMsg : numAuthMsg
Conclusions

- This paper presents a dynamic window scheme that allows each individual node to make its own decision on whether to forward a message first or verify it first.

- It can effectively contain the damage of DoS attacks to a small portion of the nodes.