Containing Denial-of-Service Attacks in Broadcast Authentication in Sensor Networks

MobiHoc 2007

Chi-Han Lin

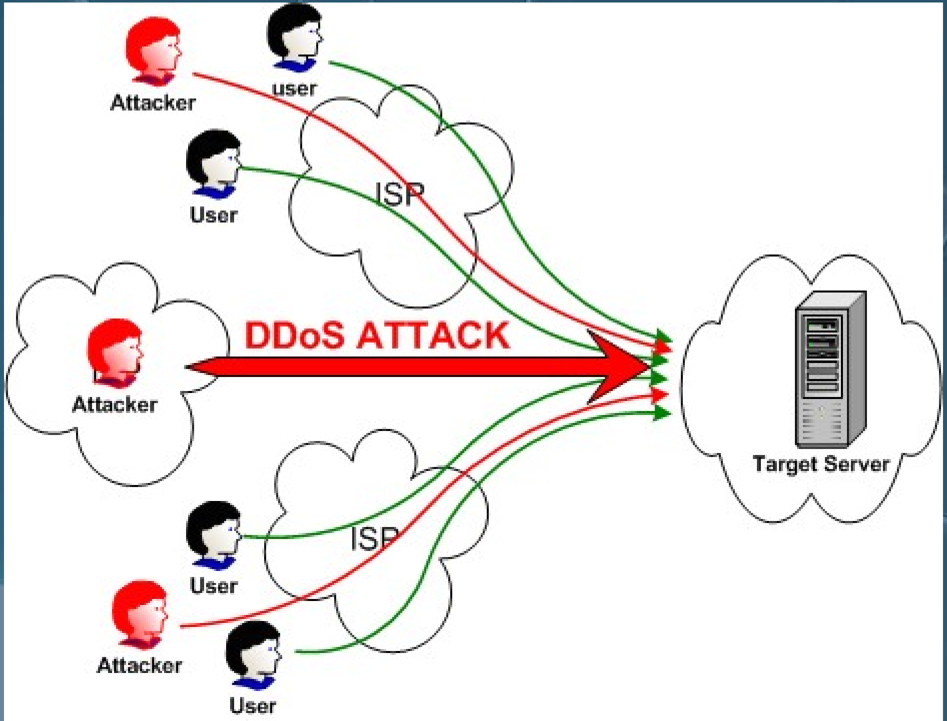
Jul. 31, 2008

Outline

- Introduction
  - Broadcast Authentication
  - DoS Attacks against Broadcast Authentication
- Assumptions
- The proposed scheme based on PKC
- Simulation
- Conclusions

Introduction

- A denial of service (DoS) attack is an attempt to make a computer resource unavailable to its intended users.



Introduction

- 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.

Introduction

- 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.

$$\boxed{K_0} \xleftarrow{F} K_1 \xleftarrow{F} K_2 \xleftarrow{F} \dots \xleftarrow{F} K_{n-1} \xleftarrow{F} K_n$$

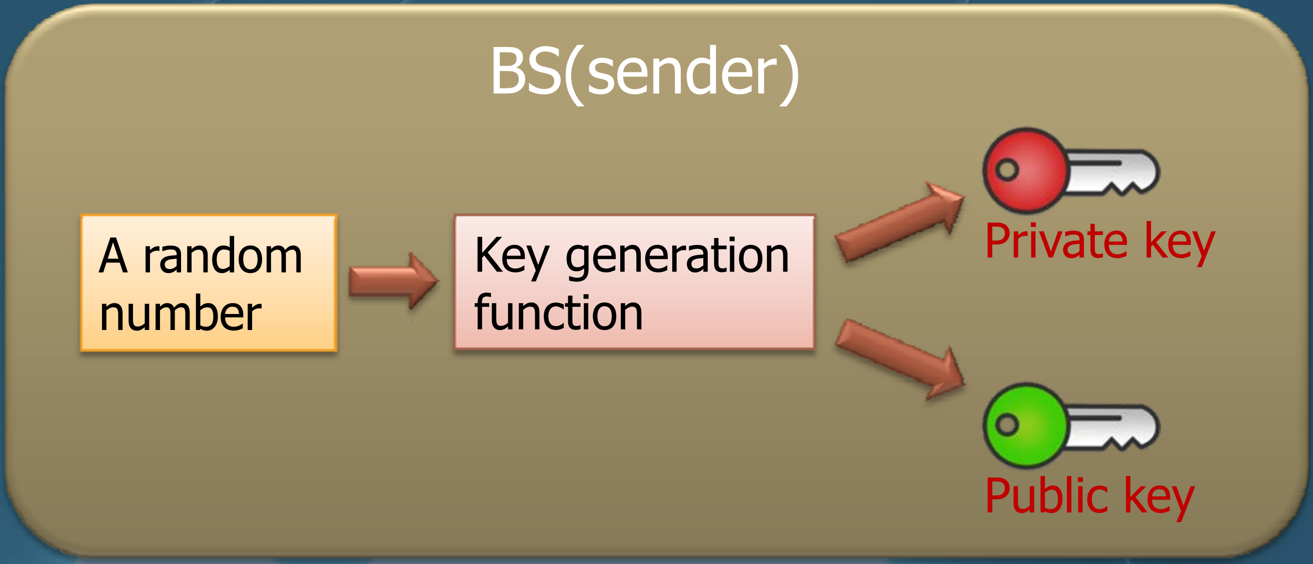
commitment

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



BS(sender)

A random number

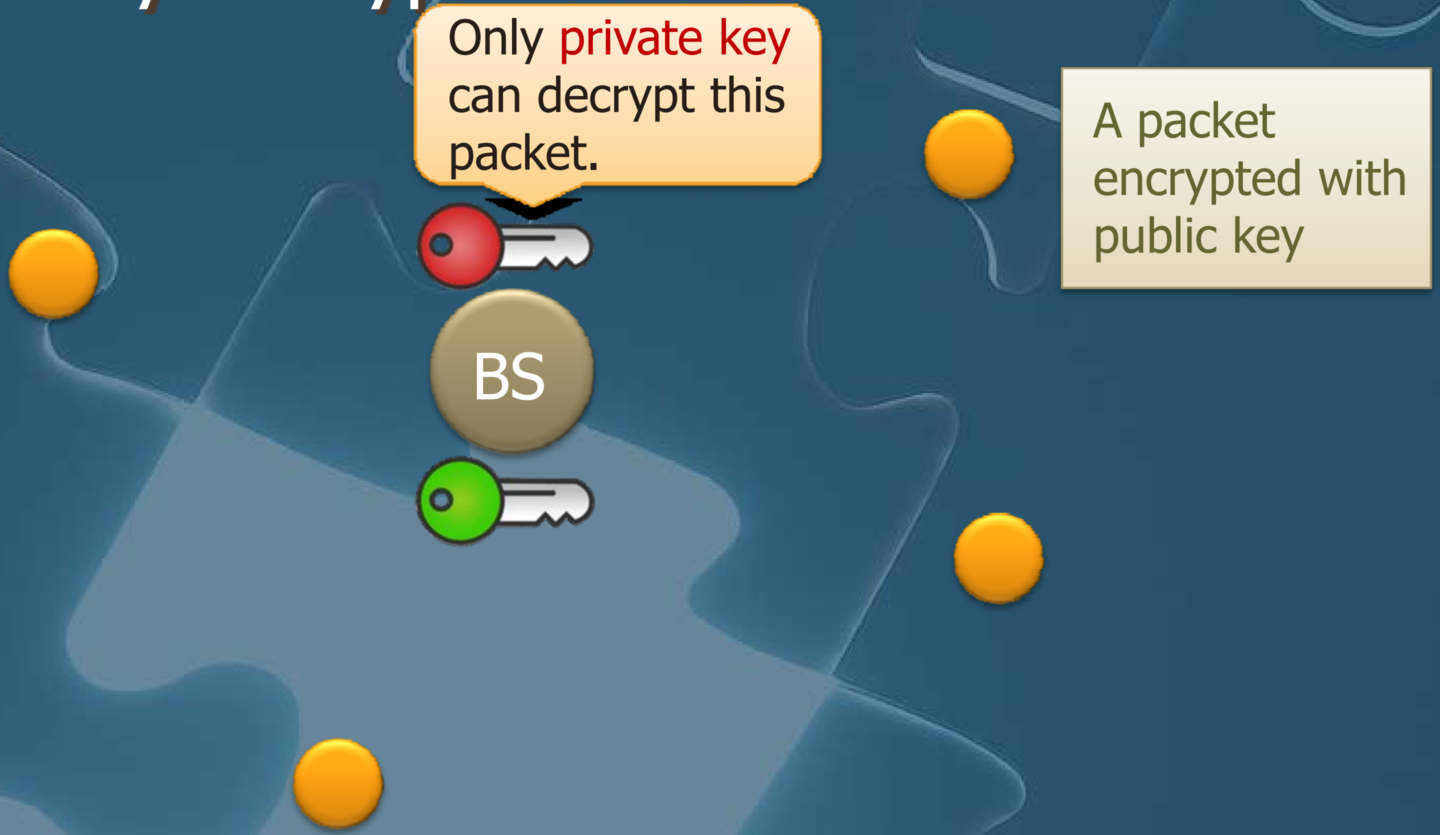
Key generation function

Private key

Public key

Introduction

- Public key encryption

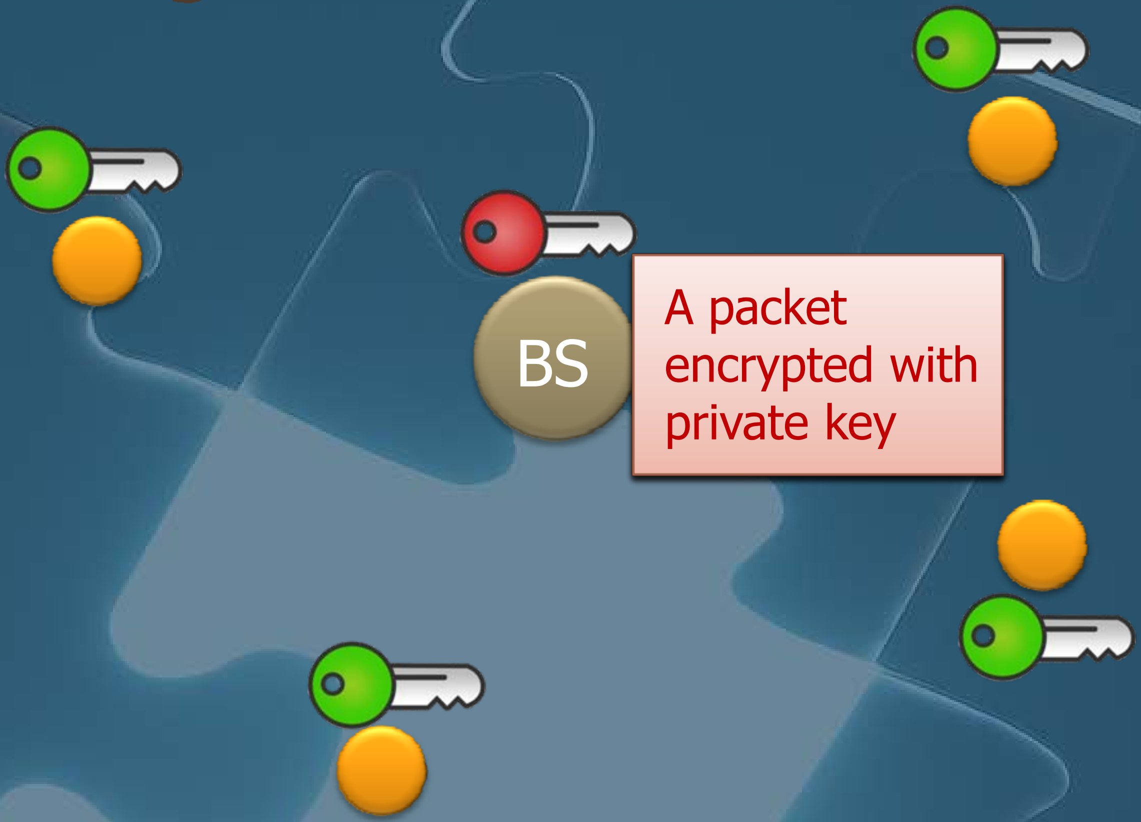


Only private key can decrypt this packet.

A packet encrypted with public key

Introduction

- Digital signatures



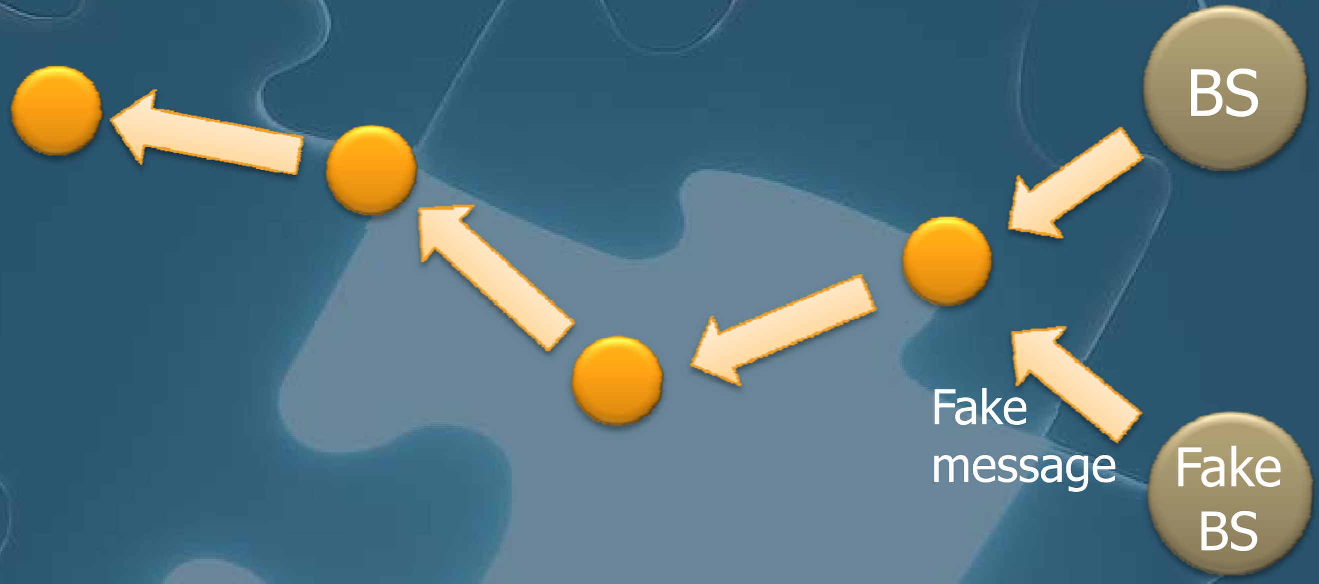
A packet encrypted with private key

Introduction

- 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

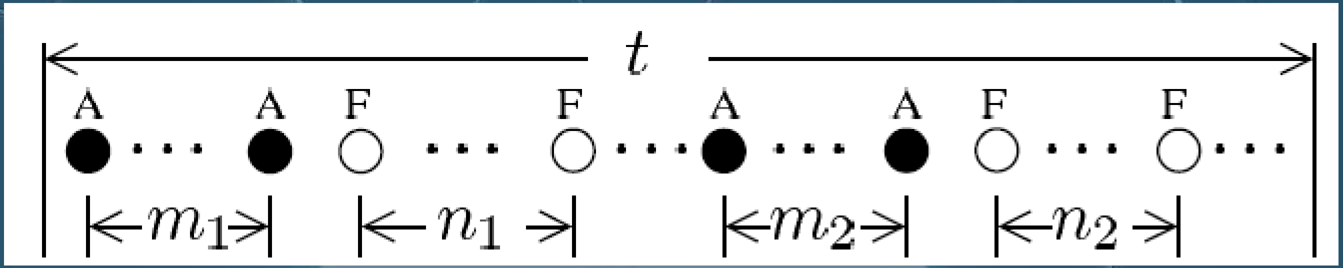


Assumptions

- 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

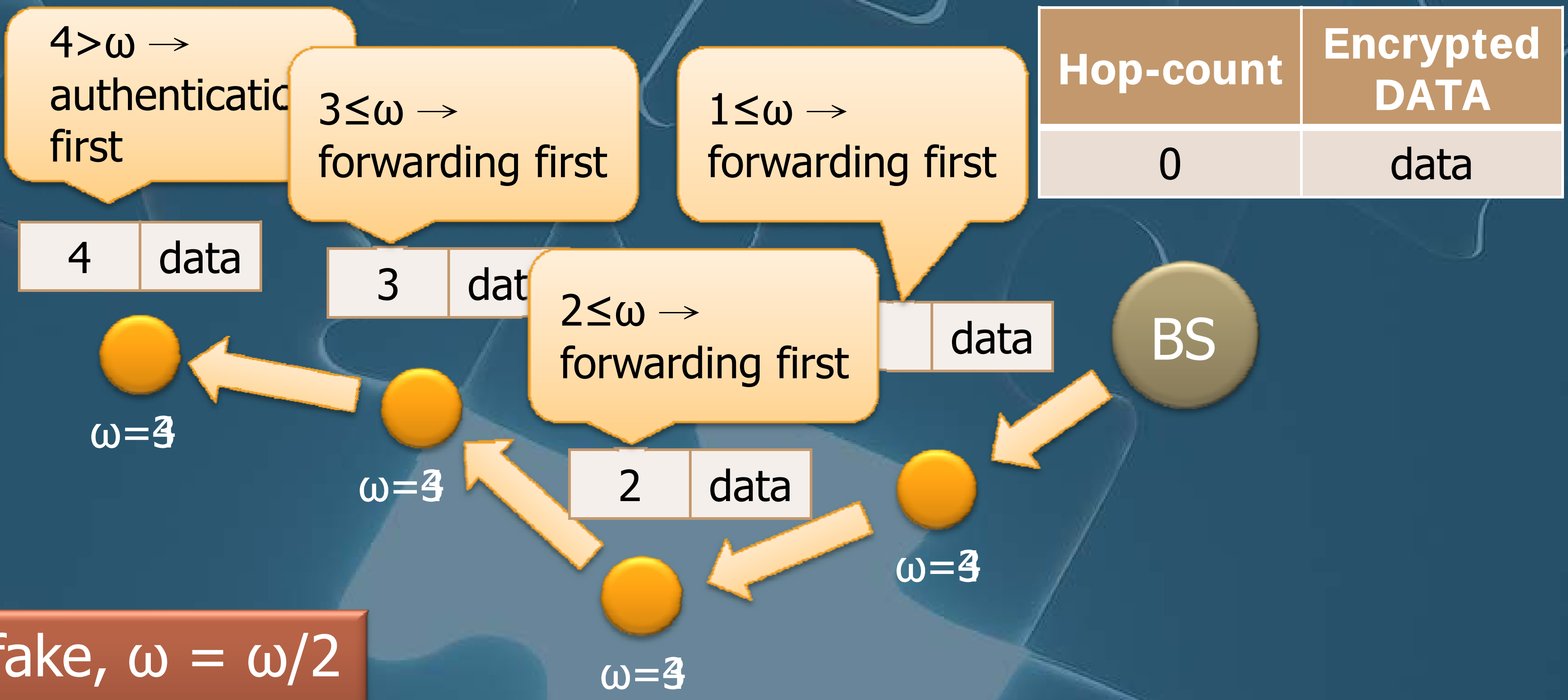
- Attackers do not always send fake messages. They can also forward authentic messages.



The proposed scheme based on PKC

- 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 ω.

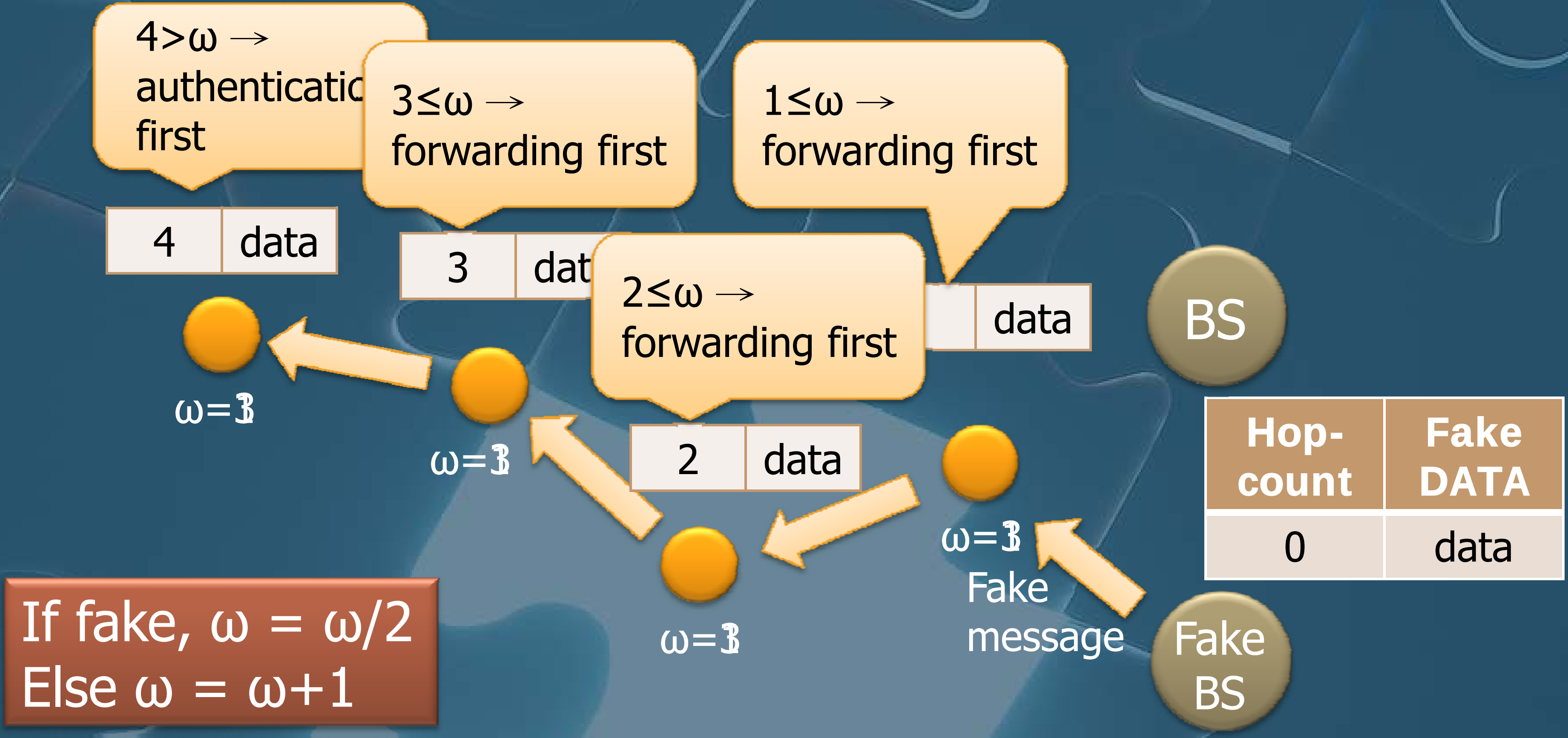
The proposed scheme based on PKC



Hop-count	Encrypted DATA
0	data

If fake, ω = ω/2
Else ω = ω+1

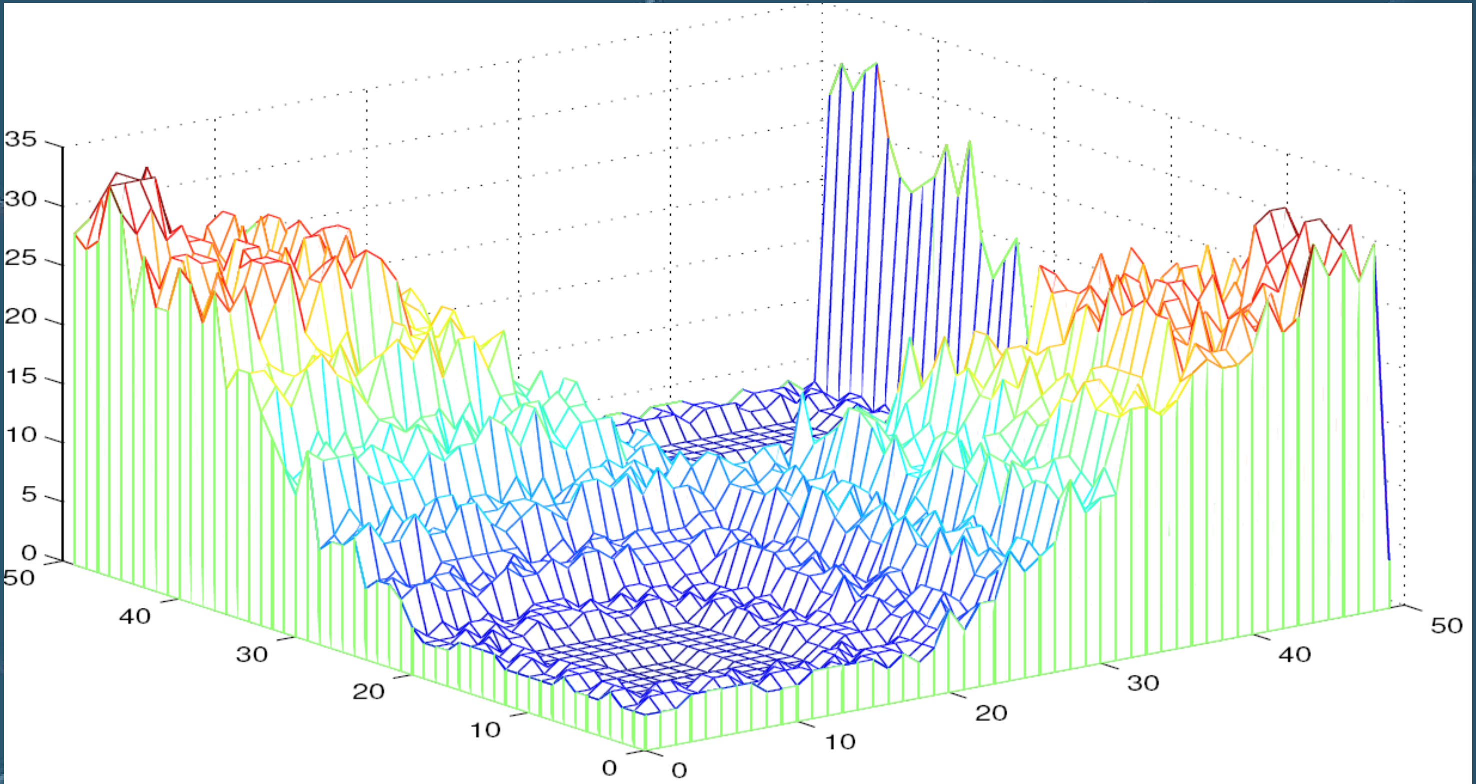
The proposed scheme based on PKC



Hop-count	Fake DATA
0	data

If fake, ω = ω/2
Else ω = ω+1

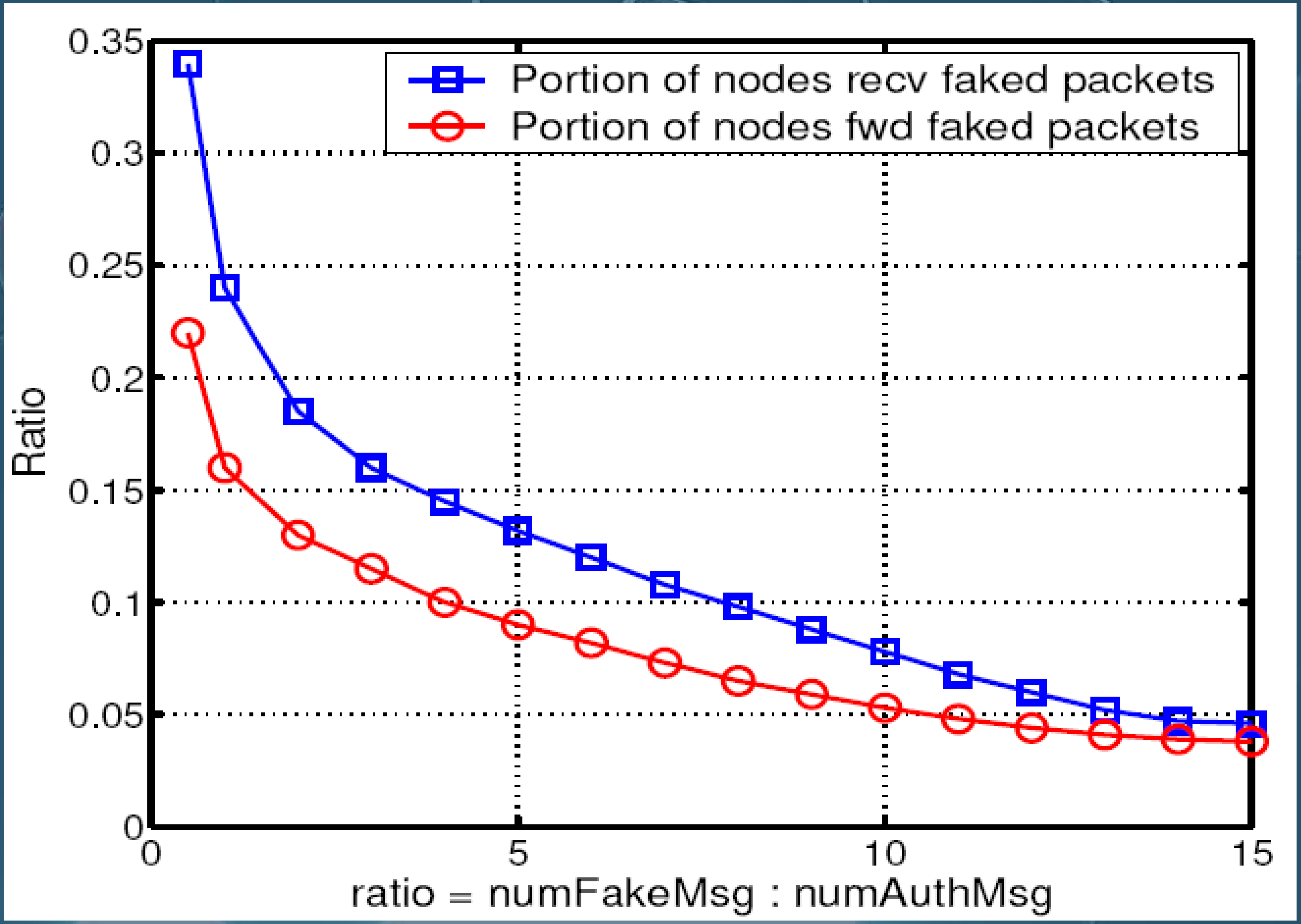
Simulation



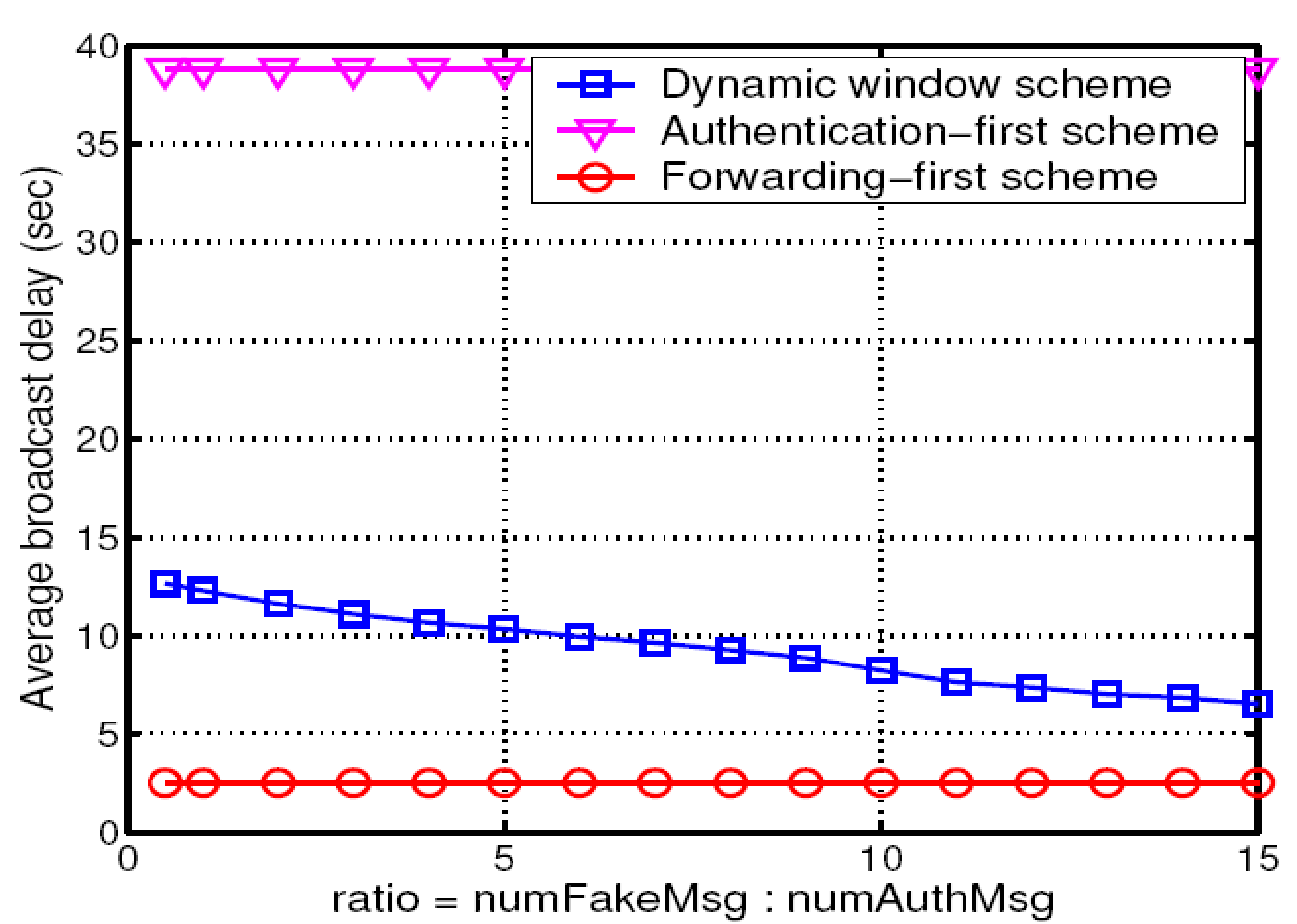
Simulation

- 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

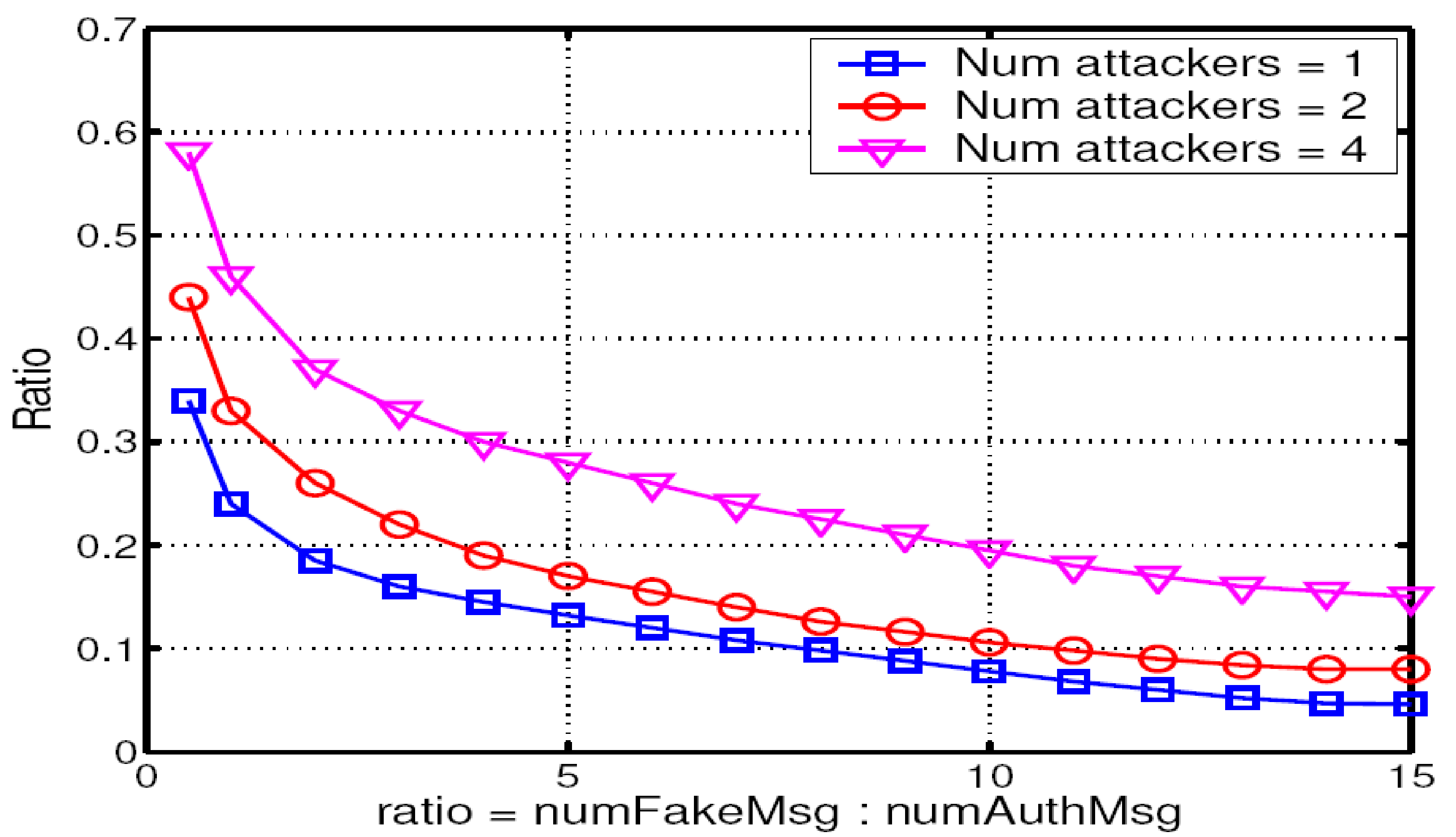

Portion of nodes recv faked packets
Portion of nodes fwd faked packets
Ratio
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0
5
10
15
ratio = numFakeMsg : numAuthMsg

Simulation



Dynamic window scheme
Authentication–first scheme
Forwarding–first scheme
Average broadcast delay (sec)
40
35
30
25
20
15
10
5
0
0
5
10
15
ratio = numFakeMsg : numAuthMsg

Simulation


Num attackers = 1
Num attackers = 2
Num attackers = 4
Ratio
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
5
10
15
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.