Hiroshima City University

An Impersonation Attack Detection Method Using Bloom Filters and Dispersed Data Transmission for Wireless Sensor Networks

Noriaki Tanabe, Eitaro Kohno, Yoshiaki Kakuda

Graduate School of Information Sciences,
Hiroshima City University

Agenda

- ◆Background
- ◆Impersonation attacks
- ◆Overview of our proposed method
  - Bloom Filters
  - Secret Sharing Scheme-based dispersed data transmission
- ◆Proposed method
- ◆Experiments and Discussions
- ◆Conclusions

Background

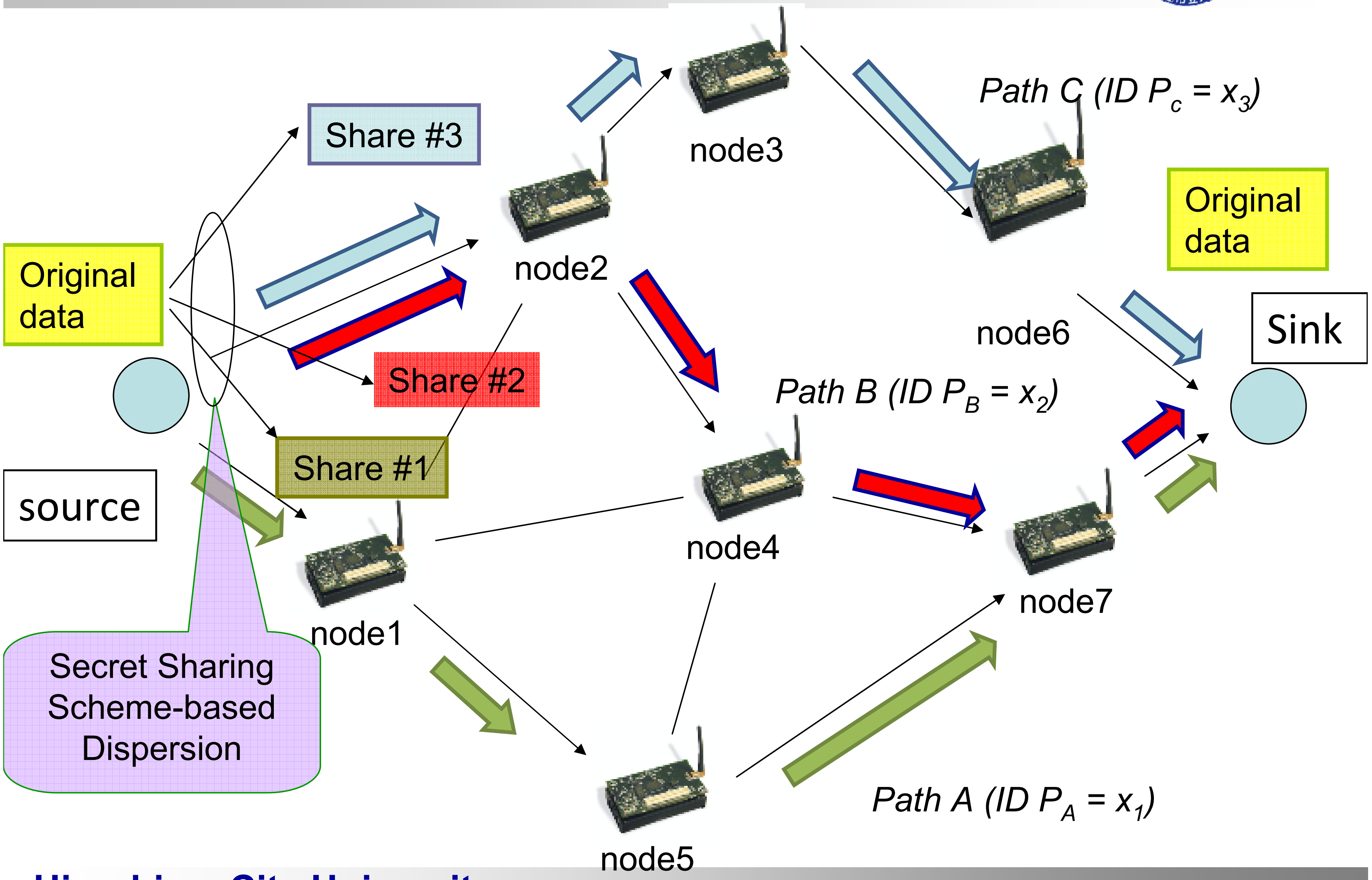
- Usage of Wireless Sensor Networks (WSNs)
  - Climate observation
  - Crime prevention, Disaster response
  - Healthcare

Requires for confidentiality when transferring data

- Dispersed Data Transmission
  - Secret Sharing Scheme-based dispersion
  - Weak against impersonation attacks

Countermeasure to impersonation attacks

Dispersed Data Transmission



Background (cont.)

- With Wireless Sensor Networks, sensor nodes and sink nodes communicate using multihop communication function.
- Multihop communication
  - <u>Intermediate node can steal relaying data</u>

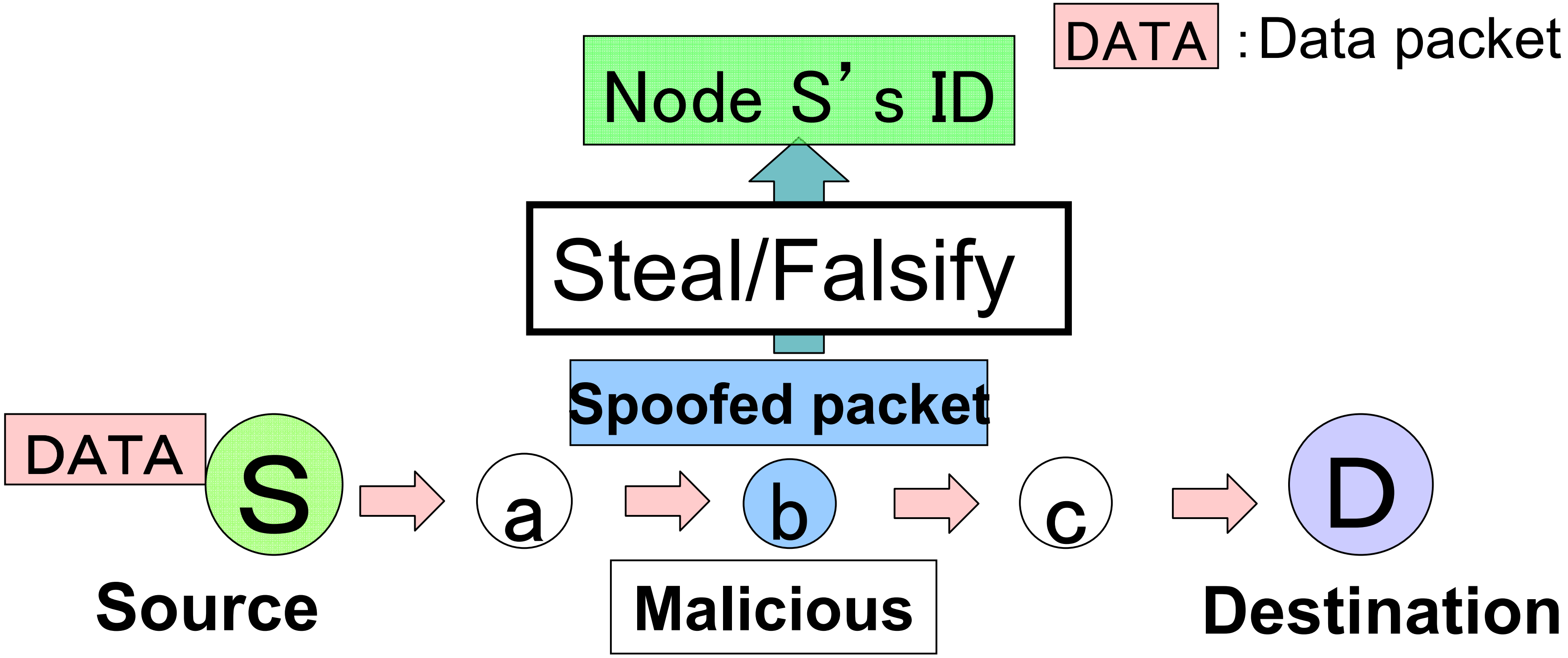
Possibility to be in danger of being attacked

- Falsification and eavesdropping of data packets
- **Impersonation (attacks)**

Impersonation attacks

【Actions of a malicious mode】

1. Steal/Falsify the source node’s ID
2. Sends crafted packets to destination node



Overview of our proposed method

Detection and Prevention Impersonation Attacks by Malicious Node

【Feature 1. **Authentic Identity**】

- Bloom Filters to stores adjacent node ID's of source node

【Feature 2. **Packet Transmission**】

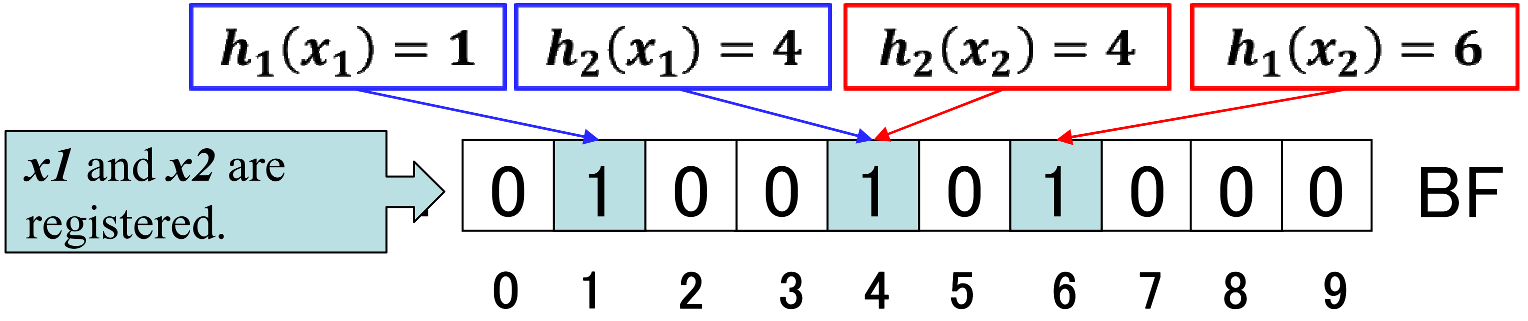
- Secret Sharing Scheme-based dispersed data transmission

Bloom Filters (BFs)

- Data structures that are bit sequences
- Capable of registering multiple data
- Procedures to register data
  1. Acquire hash values to resist data
  2. Set “1” of each hash values

***x_1, x_2*:**
Data to be registered

***$h_1()$, $h_2()$*:**
Hash functions



$h_1(x_1) = 1$ $h_2(x_1) = 4$ $h_2(x_2) = 4$ $h_1(x_2) = 6$

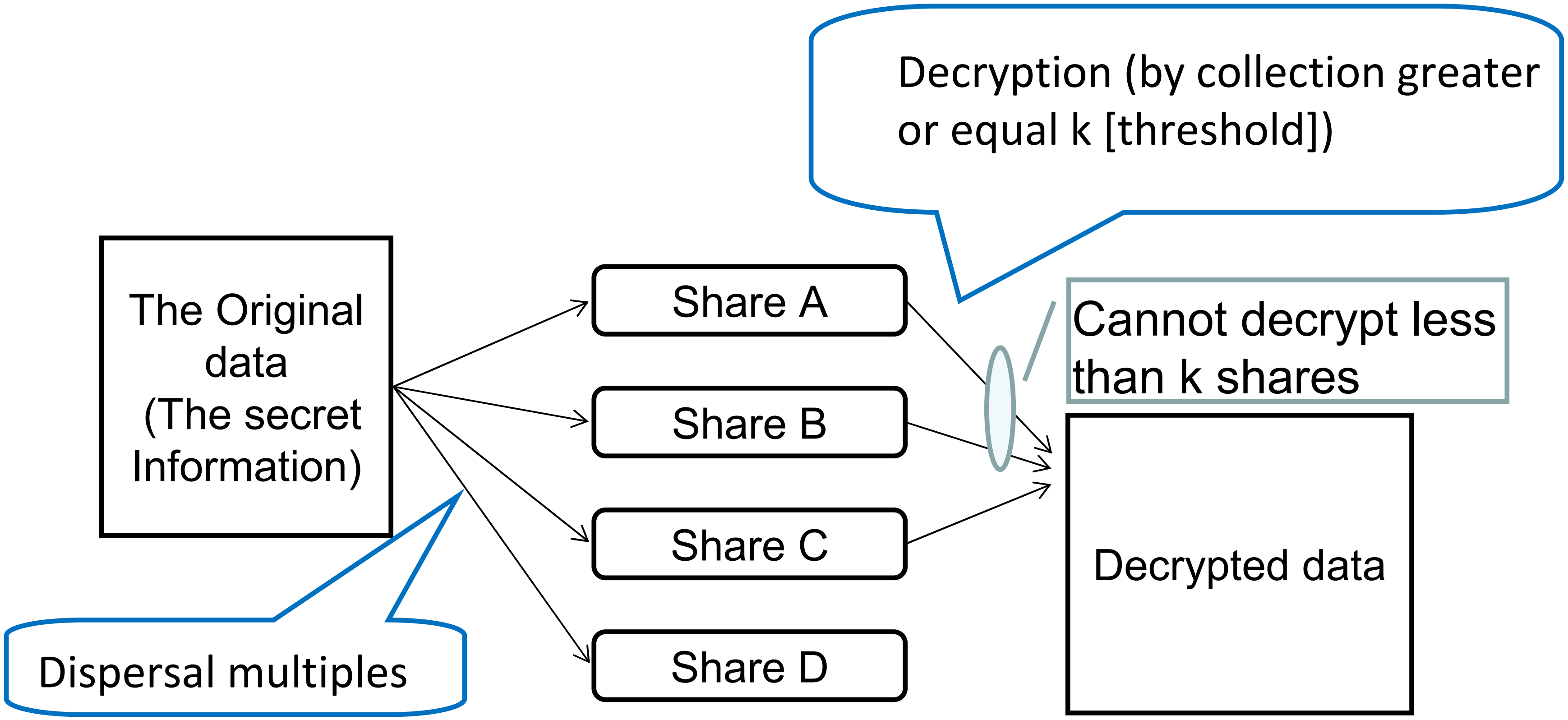
x1 and *x2* are registered.

0	1	2	3	4	5	6	7	8	9
0	1	0	0	1	0	1	0	0	0

BF

BFs can be captured, but the function cannot be reversed.

Secret Sharing Schemes



Decryption (by collection greater or equal k [threshold])

The Original data (The secret Information)

Share A

Share B

Share C

Share D

Cannot decrypt less than k shares

Decrypted data

Dispersal multiples

Conceptual diagram of Secret Sharing Scheme

This diagram called as a (k,n) threshold schemes.

Secret Sharing Scheme

■Method to create multiple shares from the original data for storing safely.

Protect authentic information against malicious node’s attacks

【Characteristics】

■The original data can be decrypted by collecting shares

- ・# of shares ≧ threshold: possible to decrypt
- ・# of shares < threshold ：impossible to decrypt

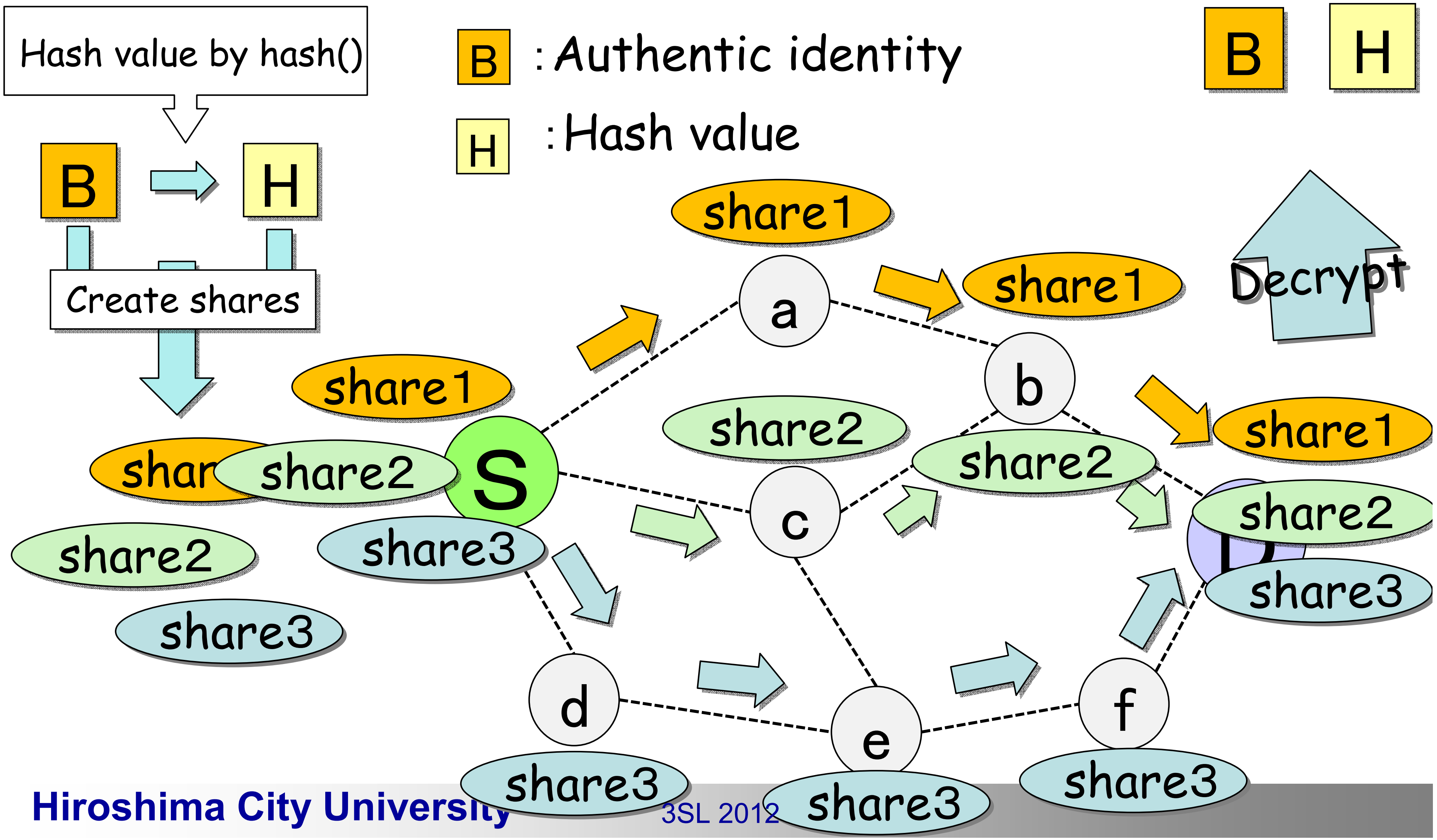
Procedures of our proposed method

1.Transmission of authentic identity

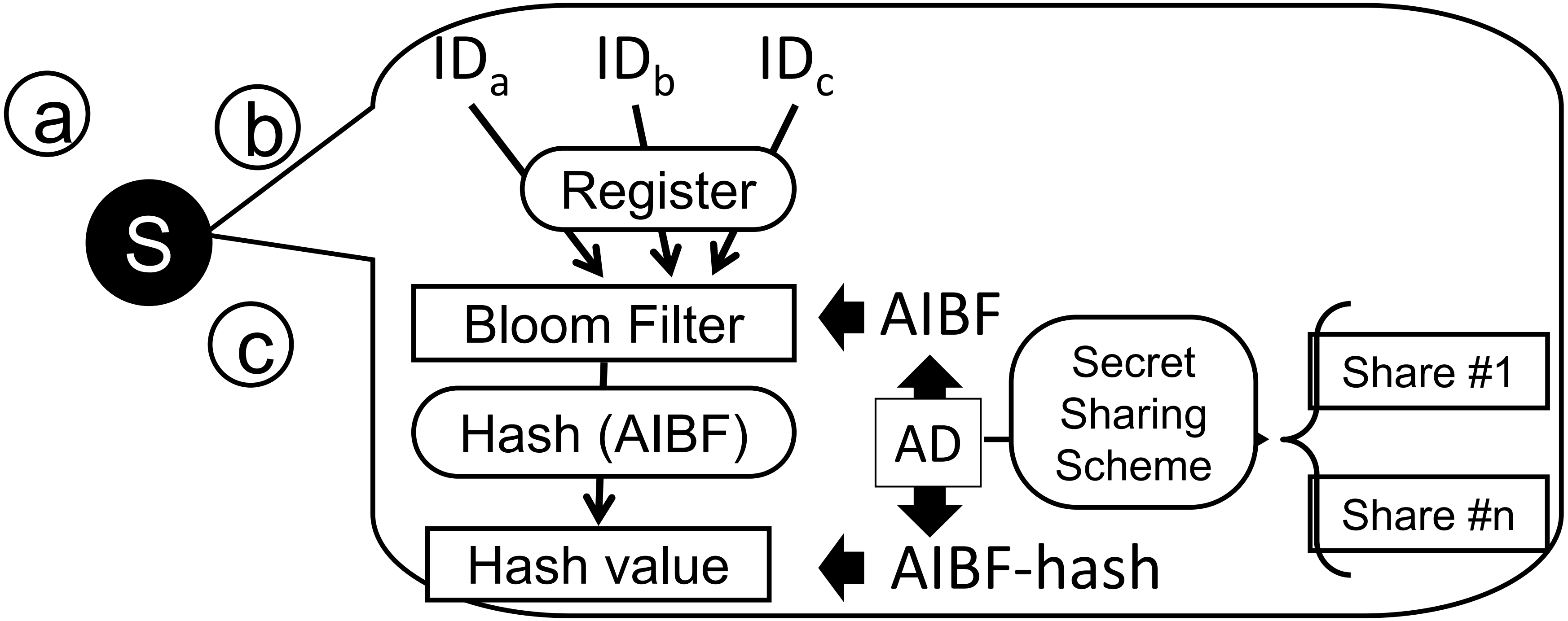
2. Using authentic identity to detect falsification

3. Detection of impersonation attacks

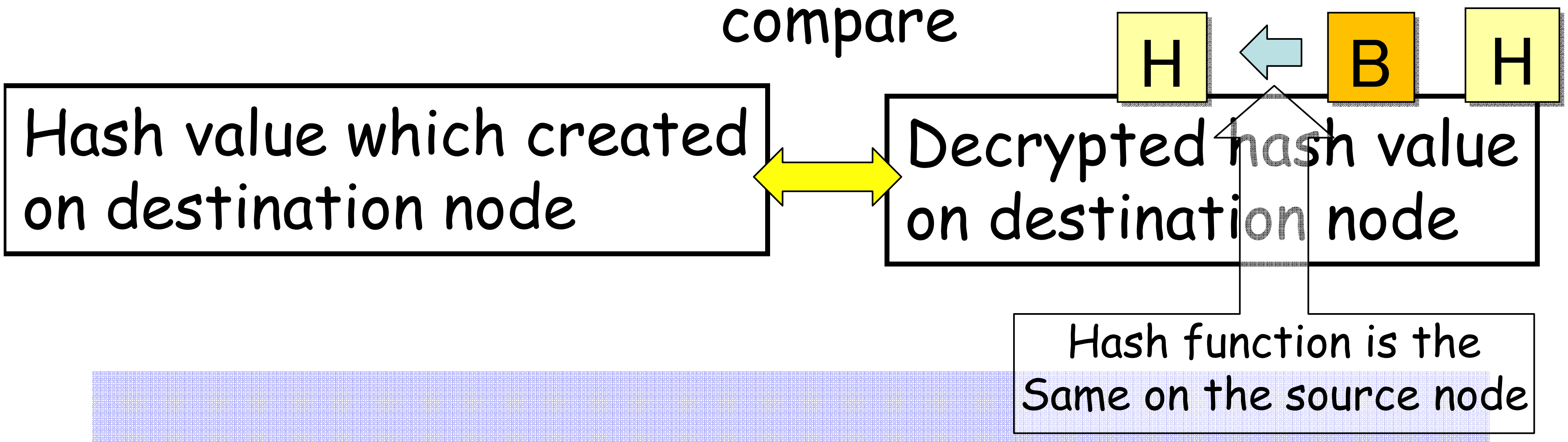
1.Transmission of authentic identity



Procedures on source node



2. Using authentic identity to detect falsification



compare

Hash value which created on destination node

Decrypted hash value on destination node

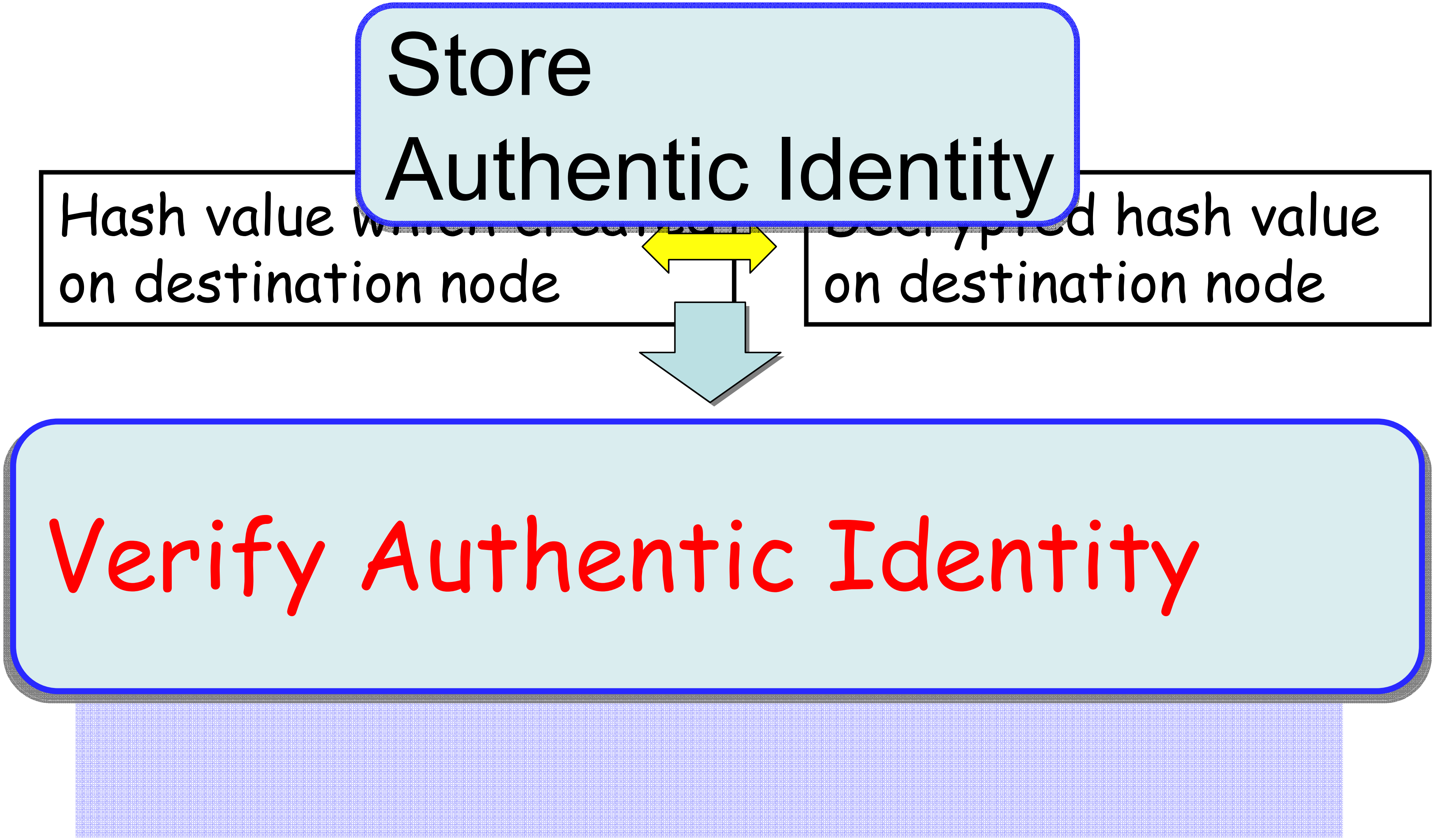
Hash function is the Same on the source node

identical: no falsified

different: falsified

(falsified during transmission)

2. Using authentic identity to detect falsification (cont.)



Store Authentic Identity

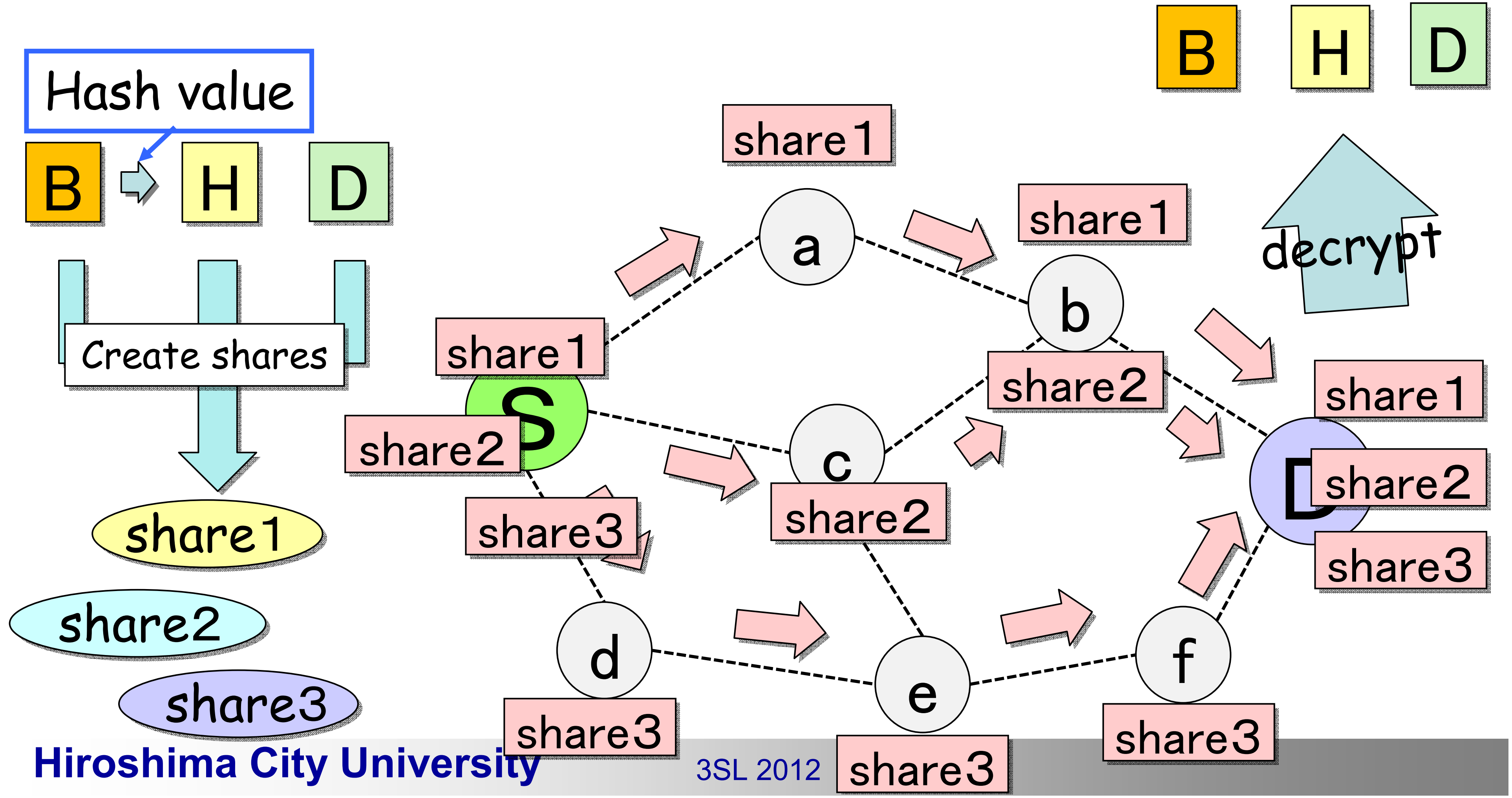
Hash value which created on destination node

Decrypted hash value on destination node

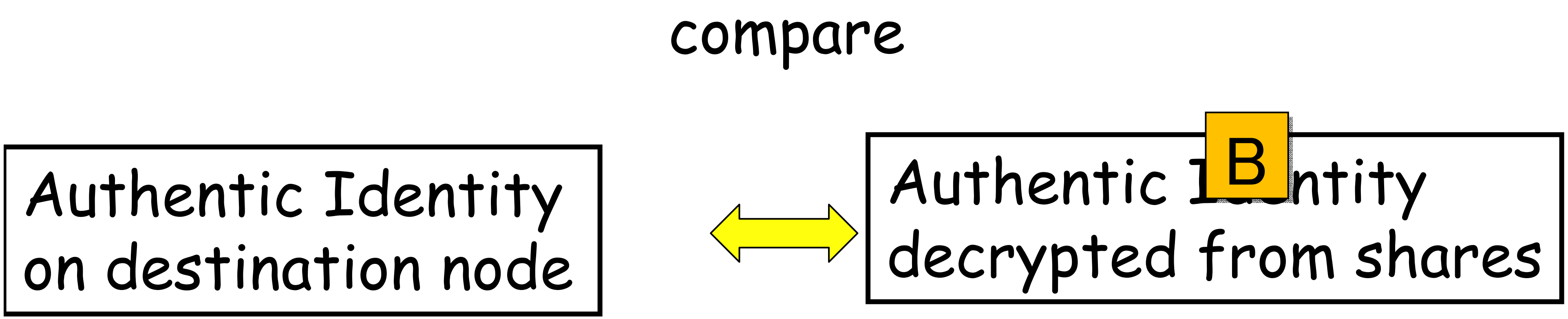
Verify Authentic Identity

3. Detection of impersonation attacks

B	:Auth. Info.
H	:Hash value
D	:Original data
share	:share which includes data



3. Detection of impersonation attacks (cont.)



identical : The source node is S.

different : Impersonation attacks exist

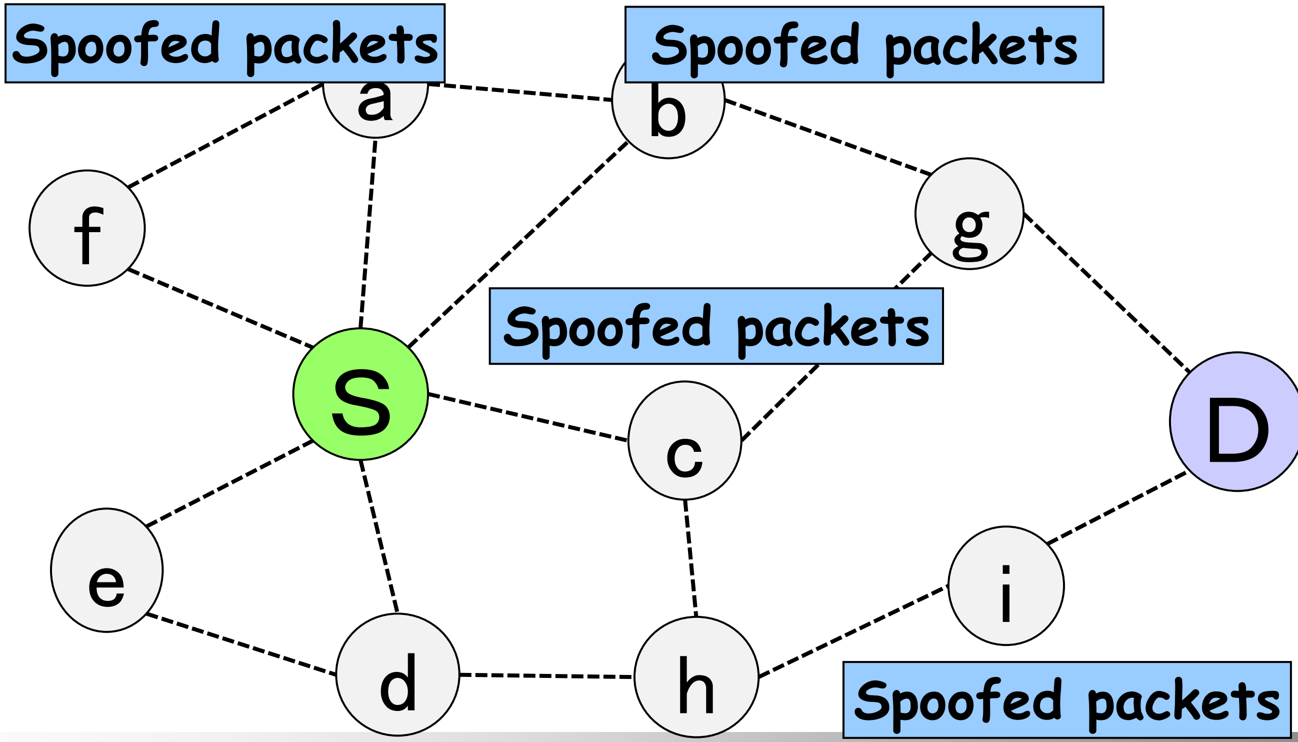
(The source node is not S.)

Simulation parameters

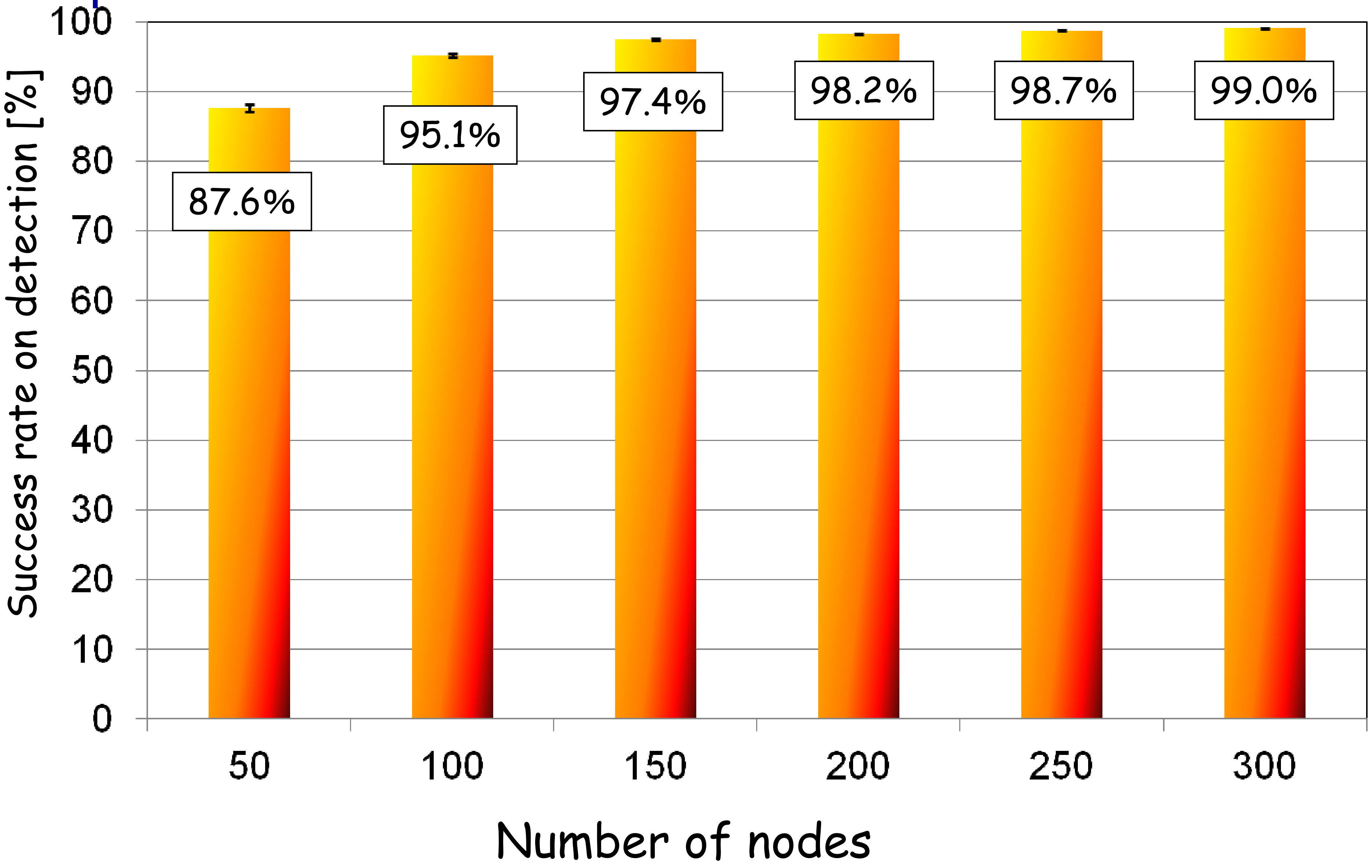
Simulator	QualNet ver.5.0
Routing protocol	SRIDR
Number of nodes	50,100,150,200,250,300
Field size (m x m)	1100 x 1100
Source and destination pairs	10
Interval of data packets (sec)	0.4
Radio area (m)	250
Hash function	Salted SHA-1
Length of Bloom Filter (bit)	128
Number of simulation run	50
MAC layer protocol	IEEE802.11b (PHY-ABSTRACT)
Node distribution	RANDOM

Scenarios of experiments

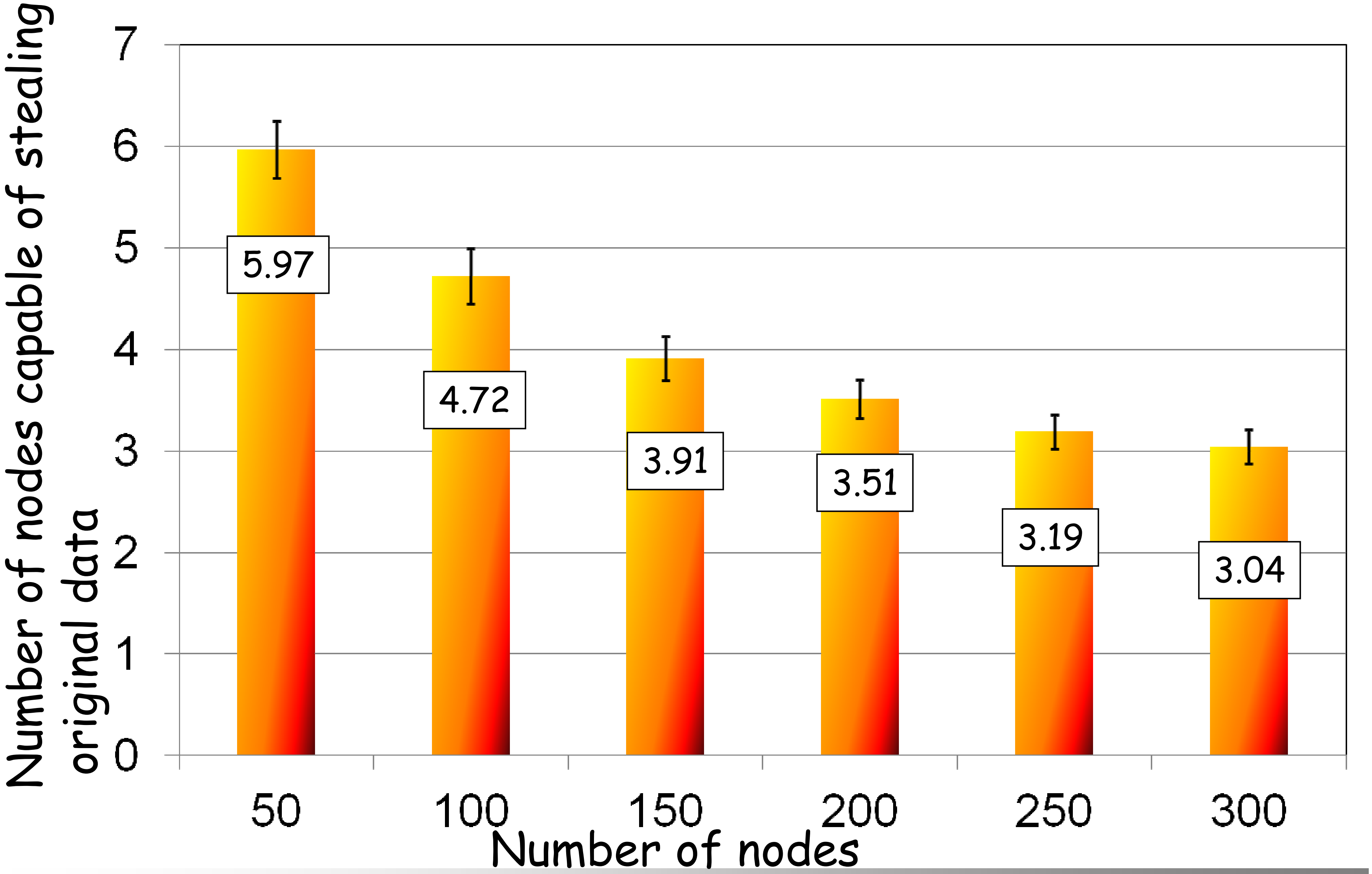
1. Performs proposed method
2. Malicious nodes creates spoofed packets and transmits them.
3. Destination nodes try to detect impersonation



Results of the success rate on detection of impersonation attacks



Number of nodes capable of stealing original data



Conclusion

- We have proposed a new detection method for impersonation attacks on WSNs.
  - Bloom Filter

    +
  - Secret Sharing Scheme-based secure dispersed data transmission
- Our proposed method can detect impersonation attacks.
- In addition, our proposed method has been effective as the number of nodes in the networks grows.