

## A Simple Sufficiency Security Protocol for Wireless Sensor Network

### Introduction

- Increasing trend of WSN usage esp. Medicare
- Need for WSN security
- Not many security protocols WSN
- Limitation in WSN
  - most of the effective security algorithms available these days are greedy energy consumption
- Idea of a sufficient security protocol for WSN

### WSN characteristics

- ultra low power consumption
- small size
- limited computational capability
- low cost device

### Security vs WSN

- Most wireless systems are sensitive to security problems due to its exposure characteristic
- in WLAN: WEP and WPA
- In WSN
  - TinySec
  - SNEP
  - SPIN

### WSN Mote & HW security Support

- WiseNet – not support
- Mica2: Not support
- MicaZ – Zigbee support 128 bit AES
  - Average lifetime 350 days @1% duty cycle (not include encryption)
- Telos - support 128 bit AES
  - Average lifetime 900 days @1% duty cycle (not include encryption)

### Security Concept

- Availability
  - the readiness for correct service
- Confidentiality\*\*\*
  - the absence of unauthorized disclosure of information
  - Achieved by Encryption techniques
- integrity
  - absence of improper system alterations

## Encryption techniques

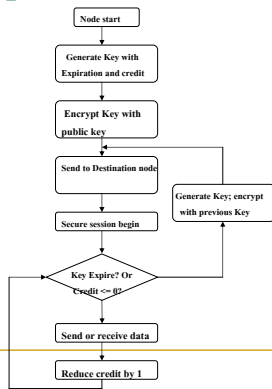
- Key establishment and trust setup
  - A variety of protocols have been proposed over several decades – not suitable for WSN
- Symmetric key cryptography
  - Easy to use
  - Less complexity
  - Require an effective key distribution
  - E.g. RC4, RC5, DES, 3DES, and AES
- Asymmetric key cryptography
  - High complexity
  - Hard to be broken
  - E.g. PKI, PGP, Diffie-Hellman

## A Simple Sufficiency Security Protocol for WSN (SSSP)

- Sufficiency security requirement
- Low power consumption
- Low complexity
- Ease of implementation

## An Example of SSSP

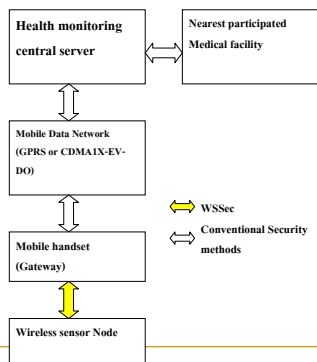
### ■ WSSec



## WSSec summary

- Simple
- No need for key distribution
- Provide sufficient security – key expiration and credit
- Energy efficient by using smaller key size but changing key more frequent
- Ease of deployment

## Health Monitoring Scenario



THANK YOU