A Security Framework for Wireless Sensor Networks

Tanveer Zia

Prof. Albert Zomaya

School of Information Technologies

University of Sydney

IEEE Sensors Applications Symposium (SAS06),
February 7-9, 2006 , Houston, Texas

Outline

- An overview of Wireless Sensor Networks
  - MICA motes
  - Applications
- Security in Wireless Sensor Networks
  - Why security is different in WSN
- Our security Framework
  - Cluster formation
  - Secure triple-key management scheme
  - Secure routing
- Summary and Future work

An Overview of WSN

- MICA Motes
- Applications

MICA Motes

- Processor: 8Mhz
- Memory: 128KB Flash and 4KB RAM
- External storage: 513KB
- Default power: 2xAA
- Radio: 916Mhz and 40Kbits/second.
- Transmission range: 100 Feet
- Bandwidth: 10 Kilobits/sec
- Available code space: 4500bytes
- OS: TinyOS

WSN Applications

- Battle field and homeland security
  - Enemy movement (tanks, soldiers, terrorists etc)
- Environmental monitoring
  - Habitat monitoring
  - Early bush fire detection
- Hospital tracking systems
  - Tracking patients, doctors, drug administrators.
- Traffic congestions monitoring
  - Traffic flow and jams

WSN Security

- Why security?
- Why security is different in WSN?

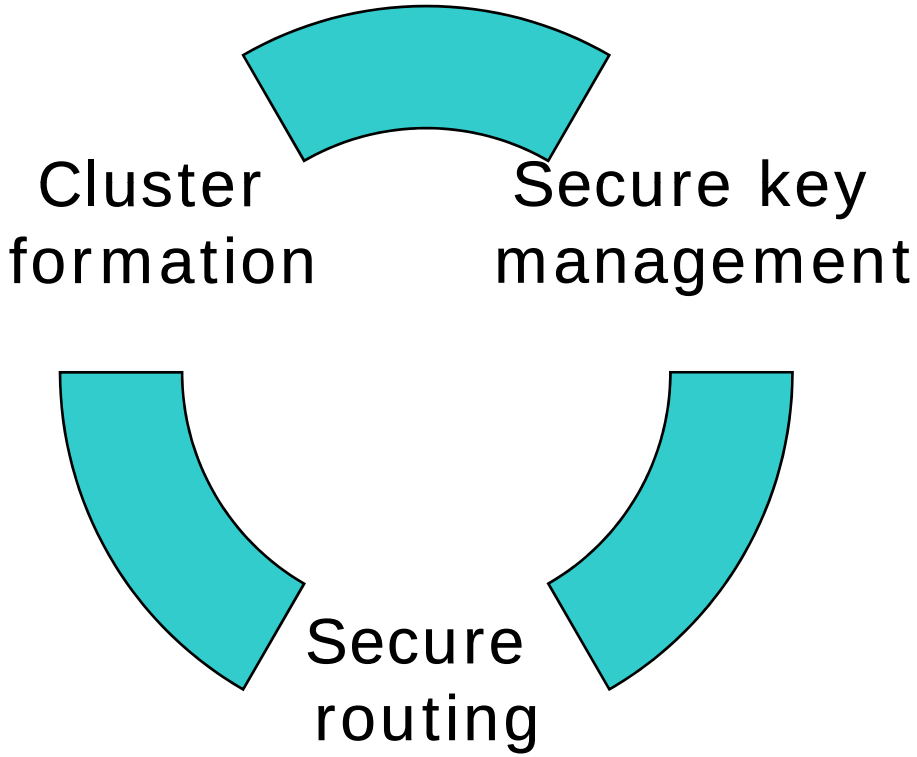
Why Security?

- CIA
  - Confidentiality, Integrity, and Availability
- Broadcast nature of transmission
- Physically insecure sensor nodes

Why security is different in WSN?

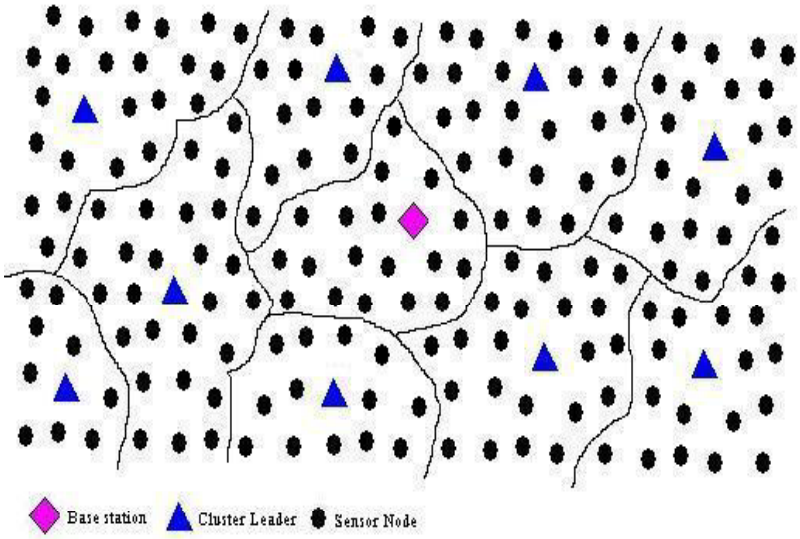
- Sensor Node Constraints
  - Battery
  - Processing power
  - Memory
- Networking Constraints and Features
  - Wireless
  - Ad hoc
  - Unattended

Our Security Framework



Cluster Formation

- Nodes deployment
- Message broadcast
- Leader election
- Data aggregation
- Multi-hop clustering model



Key Management Schemes

- Trusted Server Scheme
  - Depends on trusted server like Kerberos, no trusted infrastructure in WSN
- Asymmetric (Public Key) Scheme
  - Infeasible due to limited resources in WSN
- Key Pre-Distribution Scheme

Key Pre-Distribution

- Pre-Deployment of keys – loading the keys into sensor nodes prior to deployment
- Challenges:
  - Energy efficiency
  - Security – compromised nodes
  - Scalability – addition of new nodes

Current solutions in key pre-distribution

- Master key approach
  - Memory efficient but lack the security
  - Tamper resistant hardware, cost?
- Pair-wise key approach
  - N-1 keys for each node
  - Good security
  - Requires a lot of memory
  - Lack scalability

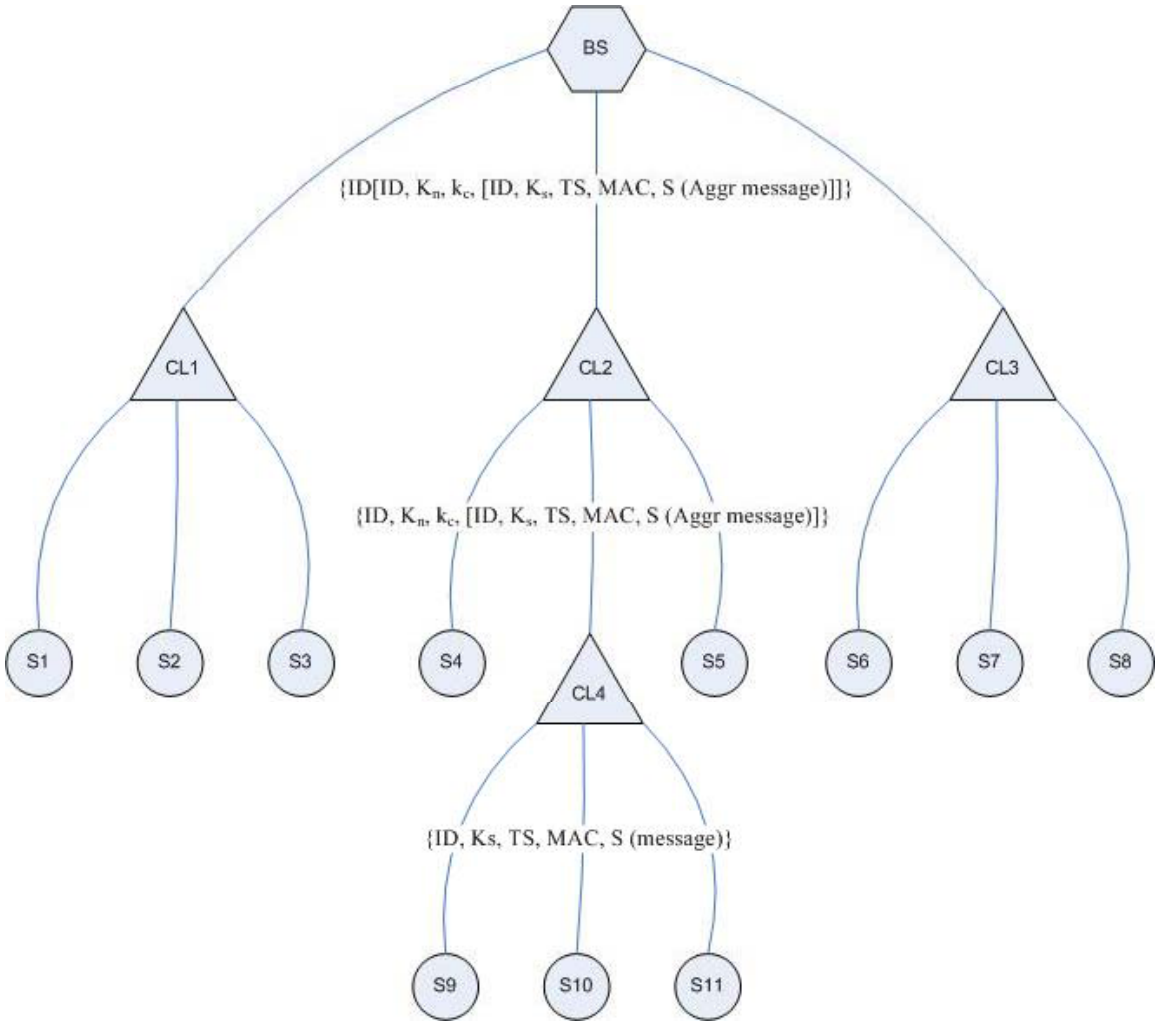
Our secure triple key management scheme

- Proposed secure keys
  - K_n (network key)
    - Generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. Nodes use this key to encrypt the data and pass onto next hop
  - K_s (sensor key)
    - Generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. Base station uses this key to decrypt and process the data and cluster leader uses this key to decrypt the data and send to base station.
  - K_c (cluster key)
    - Generated by the cluster leader, and shared by the nodes in that particular cluster. Nodes from a cluster use this key to decrypt the data and forward to the Cluster Leader

Key calculation

- Base station to node key calculation
- Nodes to cluster leader key calculation
- Cluster leader to cluster leader key calculation
- Cluster leader to base station key calculation

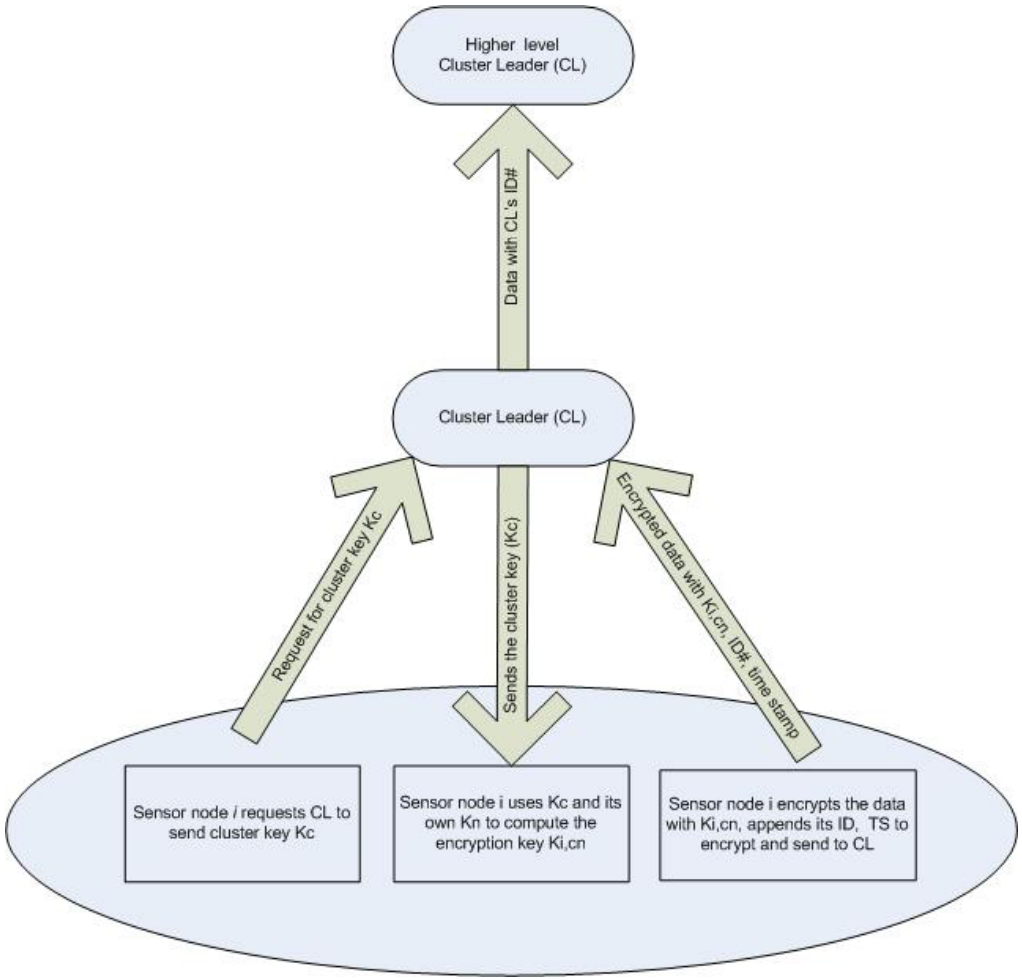
Key calculation



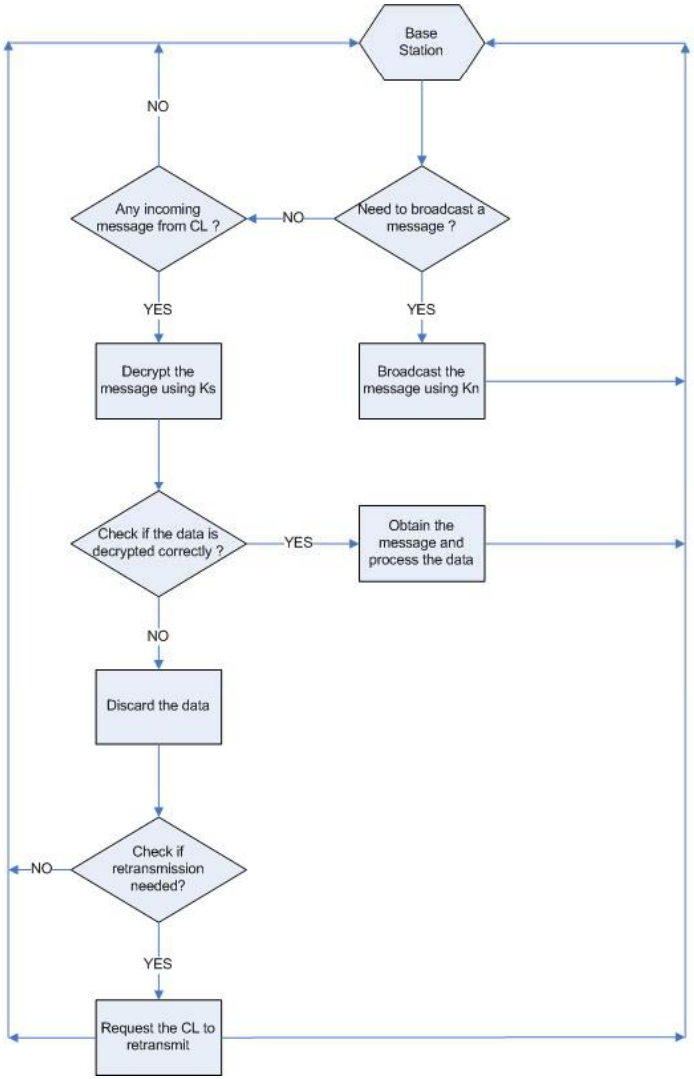
Routing algorithms

- Nodes to base station routing algorithm
- Base station to nodes routing algorithm

Nodes to base station routing



Base station to nodes routing



Analysis of proposed security framework

ID	Keys	TS	S	Data	MAC
3	3	1	1	0..31	4

This gives us 44 bytes of data packet to transmit. Taking into account 128K program memory of ATmega128L MICA2Dot our framework can be best implemented in a network of up to 3000 sensor nodes.

Analysis of proposed security framework (continue..)

- Advantages
  - Good security - CIA
  - Better usage of limited energy
  - Scalability
- Trade off
  - Limited number of nodes

Summary and future work

- WSN – future of many applications
- Resource constrained
- Unique security challenges
- Security framework
- Future work:
  - Implementing our security framework in Berkeley's MICA motes
  - A node "monitoring" mechanism to identify malicious nodes in WSN

Questions/Feedback?