School of Information Technologies

The University of Sydney

WSNSF: Wireless Sensor Networks Security Framework

A Malicious Node Detection by a Monitoring Mechanism

Tanveer Zia

INTERNATIONAL CONFERENCE ON NETWORK SECURITY & WORKSHOP

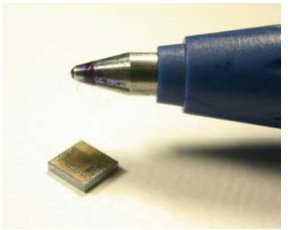
Jan 29-31 ,2007 Erode Sengunthar Engineering College ,Erode, Tamil Nadu, India

Outline

- WSN Applications
- Motes
- Why Security is different in WSN
- Challenges
- Attacks on WSN
- WSNSF
- Malicious Node Detection
- Analysis
- Questions

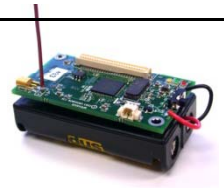
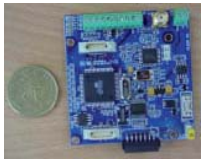
WSN Applications

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



Wireless Sensor nets – a promising future!

Motes…

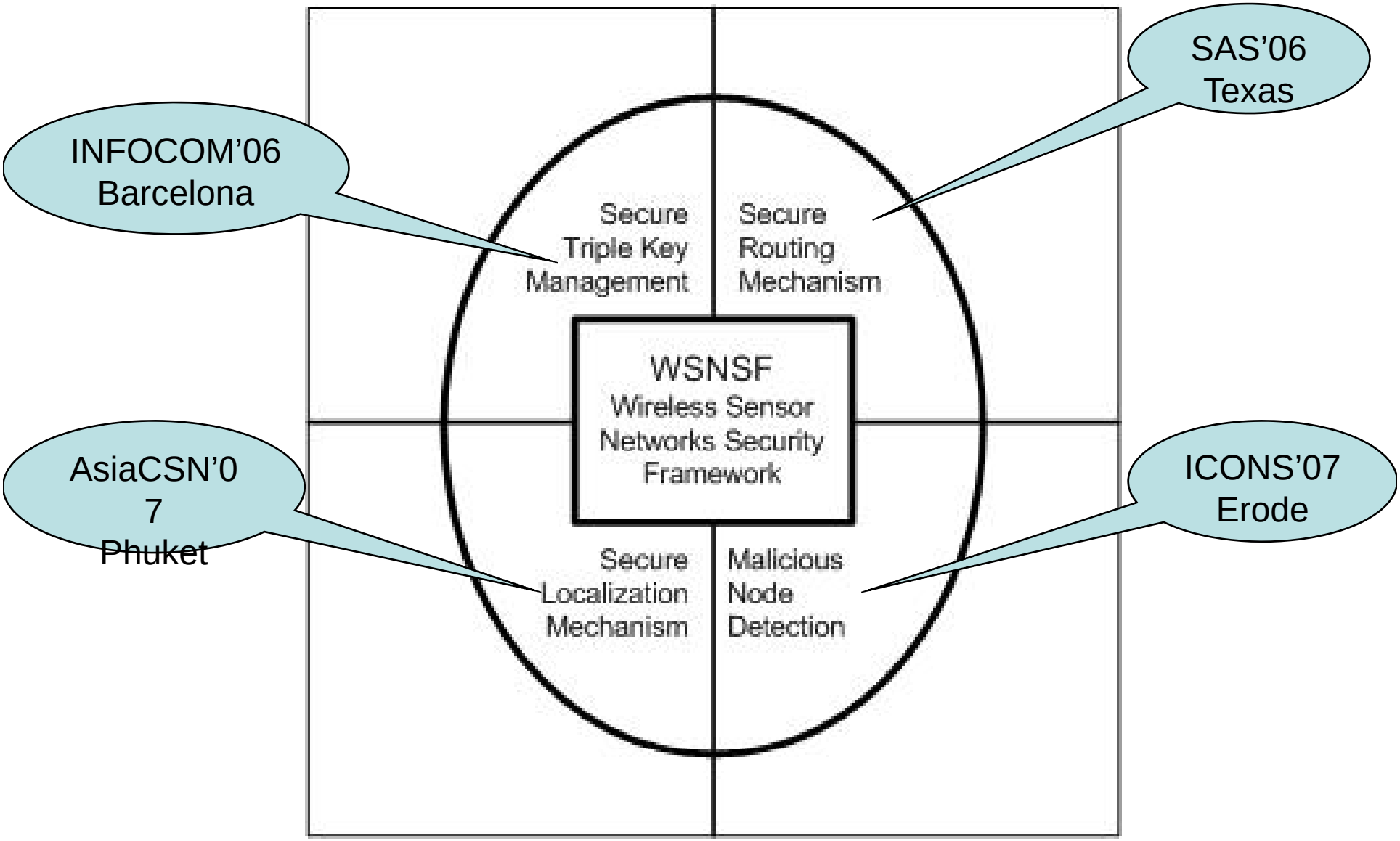
Specifications	BERKELEY'S MICA2 	CSIRO's FLECK 
Processor	8Mhz, Atmel ATMega128L	4Mhz, Atmel ATMega128L
Memory	128KB Program Flash and 4KB RAM	512KB Program Flash and 4KB RAM
External storage	512KB Serial Flash	1 MB (Fleck3)
Default power	2.7-3.3v 2xAA	1.3v – 5.3v includes solar charger circuit
Sleep mode	<15 microA	230 microA
Radio	916Mhz	433 Mhz
LEDS	3 led indicators	3 led indicators
Size	58 x 38 mm	60 x 60mm
Xm range	300m	500m
OS	TinyOS	TinyOS

Why Security is Different in WSN?

- Sensor Node Constraints
  - Battery (2xAA)
  - Processing power (8Mhz)
  - Memory (128-512KB Flash and <4KB RAM)
  - Energy Usage
    - 3V x (20 to 30)mA, 1.8V x (1 to 10)mA
- Networking Constraints
  - Wireless
  - Ad hoc
  - Unattended

Attacks on Sensor Nets

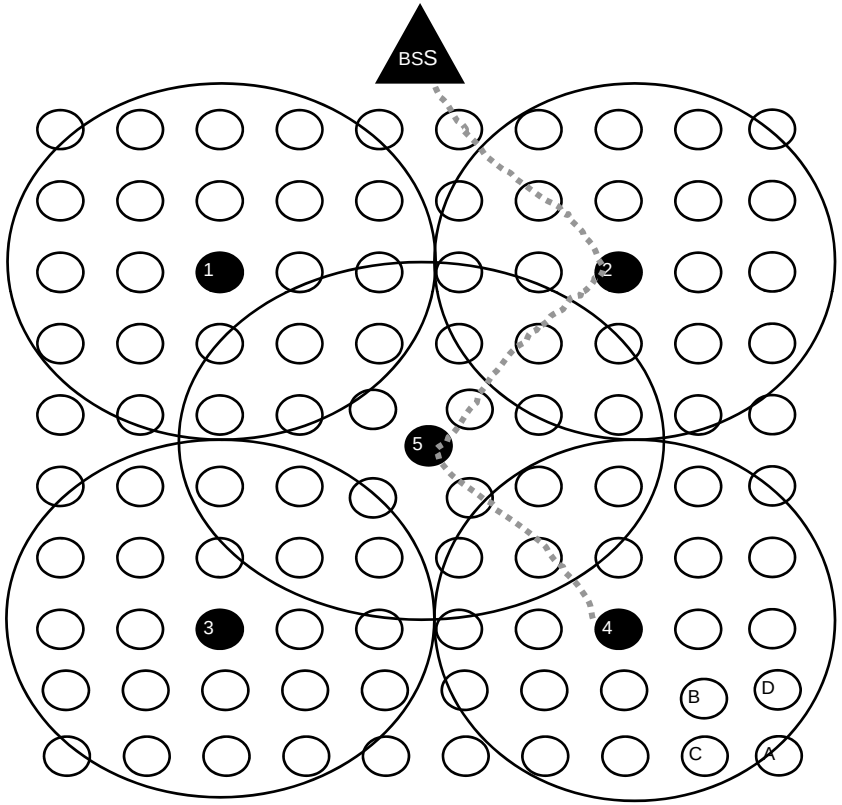
- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormhole attacks


INFOCOM'06
Barcelona
SAS'06
Texas
Secure
Triple Key
Management
Secure
Routing
Mechanism
WSNSF
Wireless Sensor
Networks Security
Framework
AsiaCSN'0
7
Phuket
ICONS'07
Erode
Secure
Localization
Mechanism
Malicious
Node
Detection

Malicious Node Detection (1)

- Node A sends message to Node B
- Node A converts itself into monitoring mode Am
- Am monitors the behaviour of Node B
- Am hears the message transmits by Node B and compares it with the Original message
- If the message transmitted by Node B is original, Am ignores it
- If there is difference in original and actual message, message is considered suspicious
- Node B is now considered as a suspicious node Bs

Malicious Node Detection (2)



Node Am (monitoring node) Bs (Suspicious node) and Nodes C & D neighboring nodes.

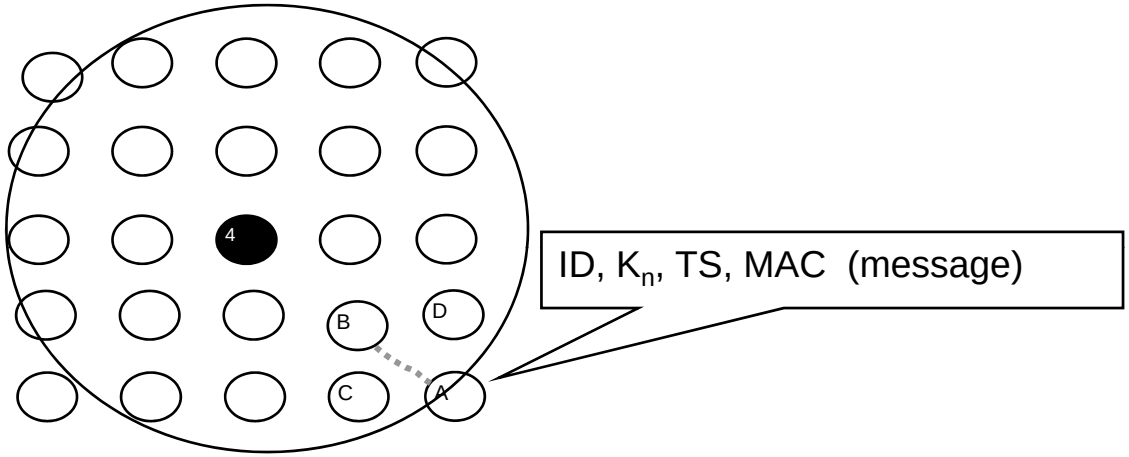
Node Suspicious Table

- Each node builds a node suspicious table containing the reputation of nodes in the cluster
- Modes update this table every time a suspicious node is identified by increasing suspicious count

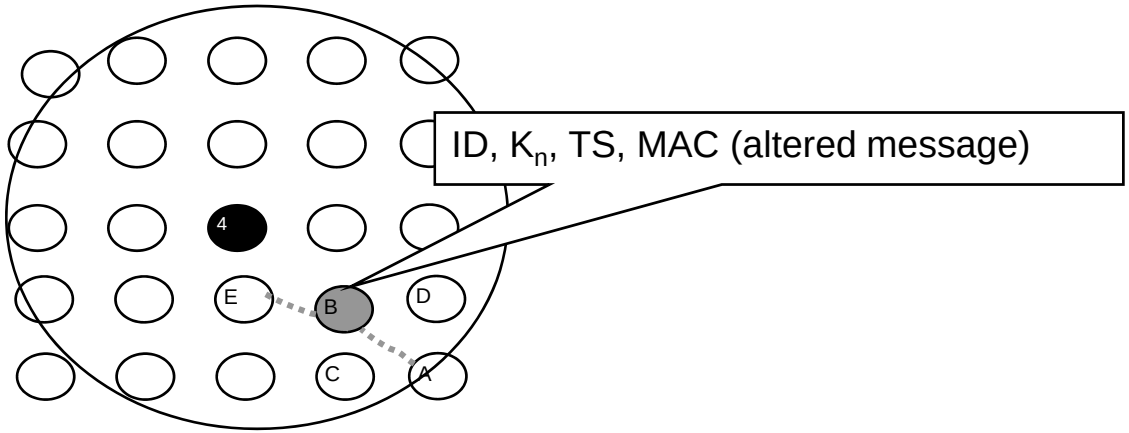
Node ID	Suspicious entries	Unsuspicious entries
ID	NS > 1	NU > 1

Malicious Node Detection (3)

(a) Message sent by Node A



(a) (b) Message altered by Node B:



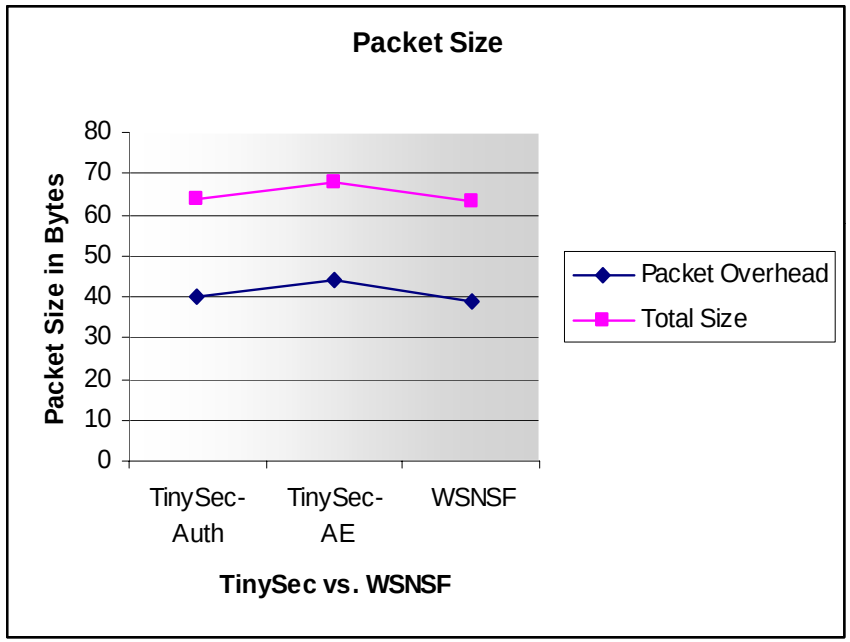
Malicious Node Detection (4)

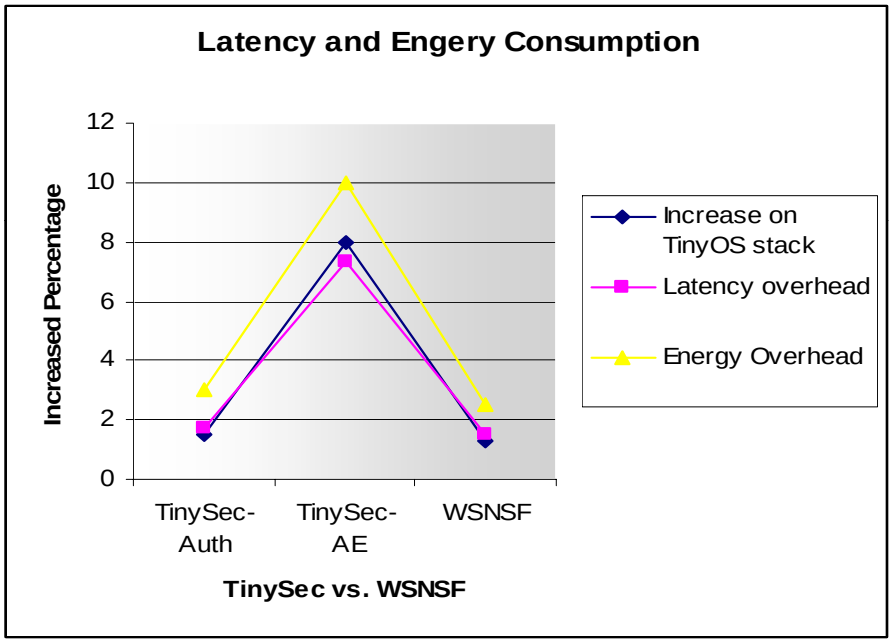
- Here ID is the node's unique identifier, *Kn* is the network key, *TS* is an encrypted time stamp, MAC is the message authentication code generated using *Kn* for message *m.*
- Node *Am* collects the replies from neighbors and updates its *node suspicious* table; it increases its own suspicious entry for *Bs* by one and the unsuspicious entries accordingly.
- Once the *suspicious* entries reach a threshold, node *Am* broadcasts that node *Bs* is a *suspicious* node and all the neighboring nodes update their *node suspicious* tables that a malicious node is present in the cluster.
- When the presence of a *suspicious* node message reaches a Cluster Leader, it isolates *Bs* by erasing *Bs* ID from its *nodes table* and discards any message coming from *Bs*. Cluster leader broadcasts the message that node *Bs* has been isolated, therefore any message originated from *Bs* is discarded by its neighboring nodes hence isolating node *Bs* from the network.

Analysis of the Proposed Mechanism (1)

	Application Data (b)	Packet Overhead (b)	Total Size (b)	Time to transmit (ms)	Increase over TinyOS stack	Latency Overhead	Energy Overhead
TinySec-Auth	24	40	64	26.6	1.5%	1.7%	3%
TinySec-AE	24	44	68	28.8	8%	7.3%	10%
WSNSF	24	39	63	25.9	1.3%	1.5%	2.5%

Analysis of the Proposed Mechanism (2)





"If you know the enemy and know yourself, you need not fear the result of a hundred battles"

Sun Tzu

Thank You

- Questions?
- Comments?
- Feedback?

About the Presenter

Tanveer Zia

- Tanveer is a part time lecturer in Information Systems at the University of Southern Queensland and University of Ballarat, Sydney affiliated campuses. Tanveer holds the degrees of BS Computer Sciences, Master of Business Administration, Master of Interactive Multimedia and is wrapping up his PhD at the School of Information Technologies, University of Sydney.
- Mobile: +6140 3393 090
- E-mail: tanzia@it.usyd.edu.au
- Web: http://www.it.usyd.edu.au/~tanzia