Introduction to
Wireless Sensor Network Security

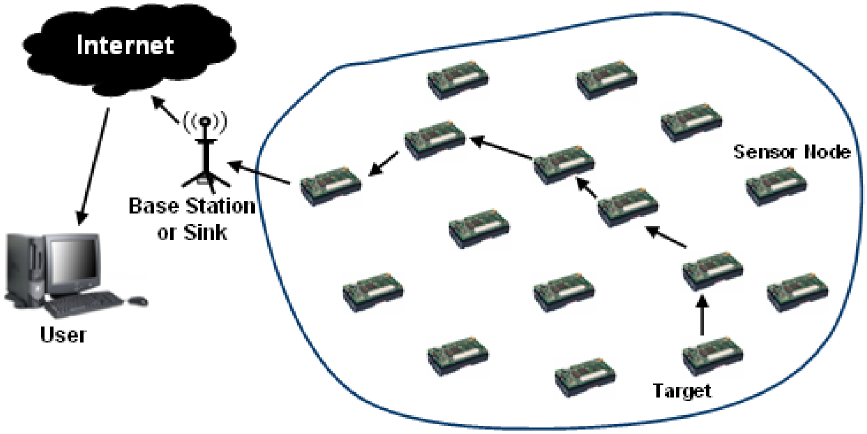
Presented By

Al-Sakib Khan Pathan
Department of Computer Science and Engineering
BRAC University, Bangladesh

Wireless Sensor Network

- Wireless networks consisting of a large number of motes
  - Self-organizing
  - Highly integrated with changing environment and network
  - Highly constrained resources
    - processing, storage, bandwidth, power
- Facilitate large scale deployment
  - Health care monitoring
  - Surveillance
  - Traffic monitoring
  - Military applications

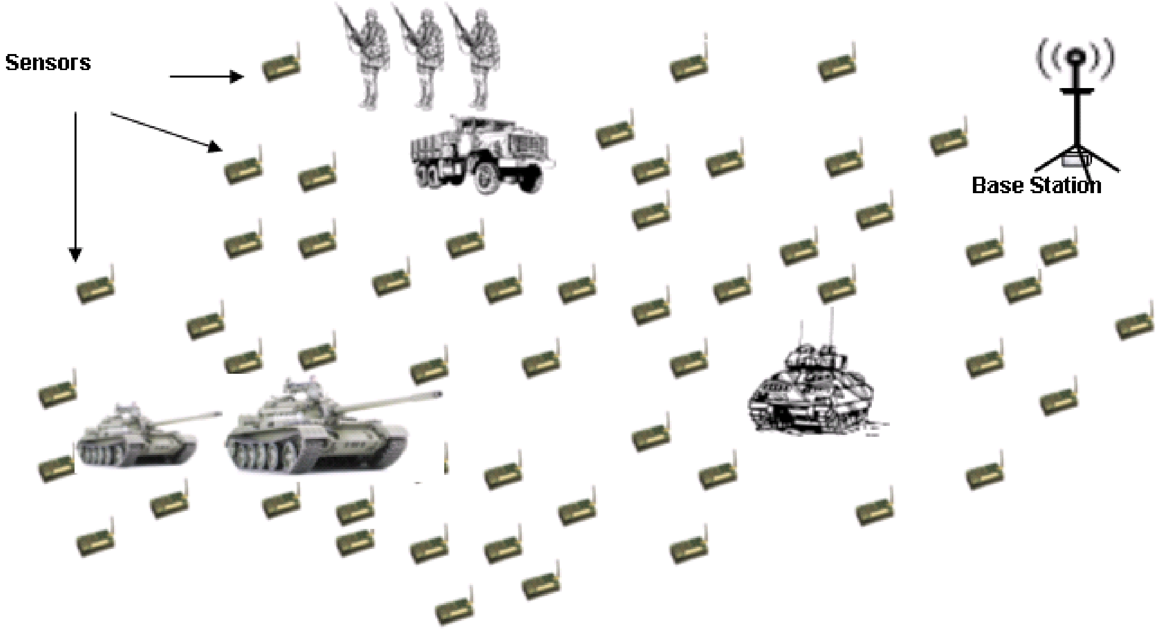
WSN!!



MICA2 Mote

- ATmega128L 8-bit processor at 8 MHz
- 128KB program memory (flash)
- 512KB additional data flash memory
- 433, 868/916, or 310 MHz multi-channel radio transceiver
- 38.4 kbps radio, 500-1000 feet outdoor range (depending on versions) with a size of only 58 x 32 x 7 (mm)
- Usually it is run by TinyOS operating system and powered by 2 AA sized batteries

An Application



WSN Security Angles

- Viewing Angle 1
  - (a) Key Management
  - (b) Secure Routing
  - (c) Secure Services
  - (d) Intrusion Detection Systems (IDS) [outsider, insider]
- Viewing Angle 2
  - (a) Physical security
  - (b) Deployment security (sparse or dense, etc.)
  - (c) Topological security (cluster/flat, hierarchy/tree, etc.)
  - (d) Wireless communication security
  - (e) Data security

WSN Security Angles

- Viewing Angle 3: Holistic Security
  - (a) Application layer security
  - (b) Transport layer security
  - (c) Network layer security
  - (d) Data link layer security
  - (e) Physical layer security

- **Holistic Security? – Still open research issue!**

DoS and DoS Attack

- Any kind of attempt of an adversary to disrupt, subvert, or destroy the network is a Denial of Service (DoS) attack
- In reality, any kind of incident that diminishes, eliminates, or hinders the normal activities of the network can cause a DoS situation
- Some examples include
  - Hardware failures
  - Software bugs
  - Resource exhaustion
  - Environmental conditions, or any type of complicated interaction of these factors

DoS and DoS Attack

- DoS (Denial of Service) is basically a given formal name of a particular condition of the network but when it occurs as a result of an intentional attempt of an adversary, it is called DoS attack
- In general, ‘Denial of Service (DoS)’ is an umbrella term that can indicate many kinds of events in the network in which legitimate nodes are deprived of getting the expected services (intentional attempts or unintentional incidents)

DoS Attack Categories

- DoS attacks can mainly be categorized into three types:
  - (1) Consumption of scarce, limited, or non-renewable resources
  - (2) Destruction or alteration of configuration information
  - (3) Physical destruction or alteration of network resources

Attacks Against Routing

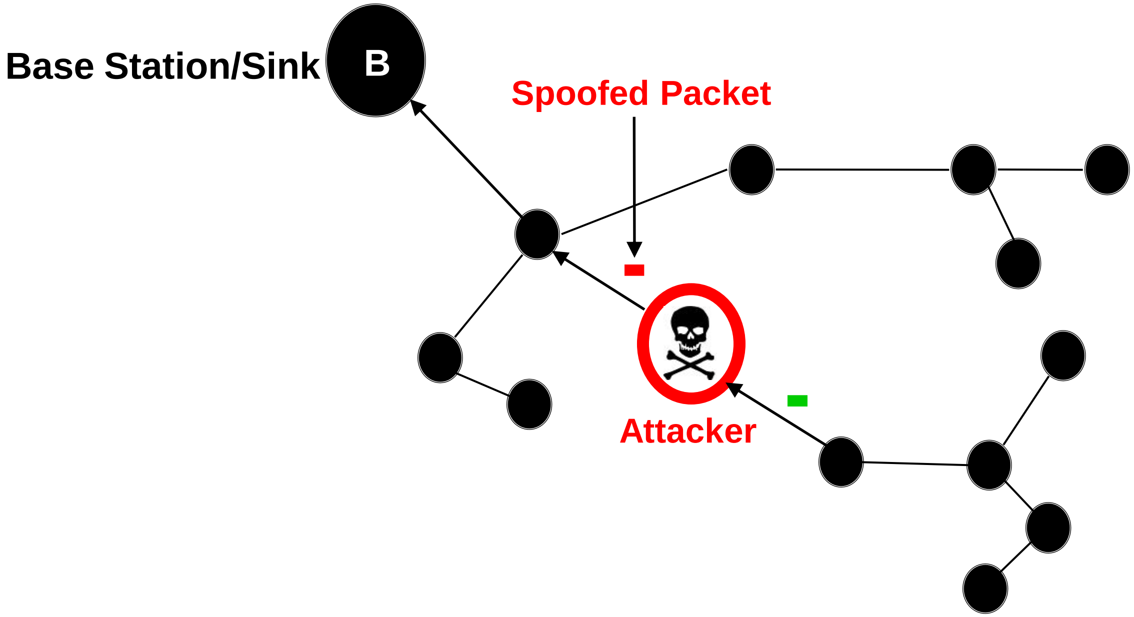
- Attacks on Information in Transit
- Selective Forwarding
- Blachole/Sinkhole Attack
- Sybil Attack
- Wormhole Attack
- HELLO Flood Attack
- Acknowledgement Spoofing

Information in Transit

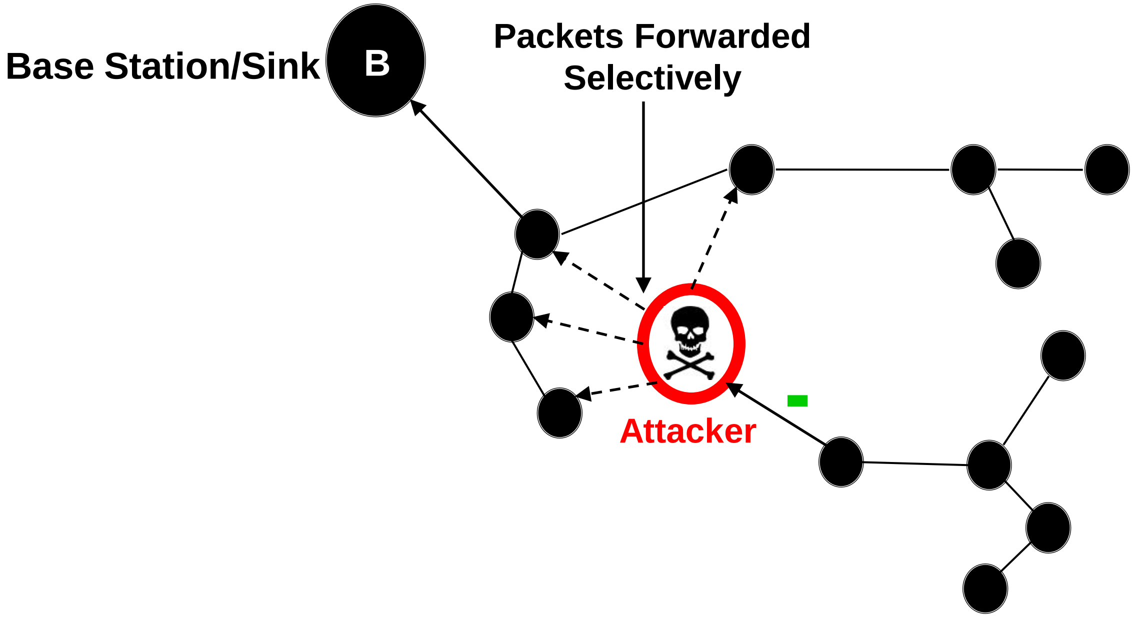
- Routing information can be spoofed, altered during transmission or replayed

- Thus adversaries might be able to
  - create routing loops
  - attract or repel network traffic
  - extend or shorten source routes
  - generate false error messages
  - partition the network
  - increase end-to-end latency

Information Spoofing



Selective Forwarding



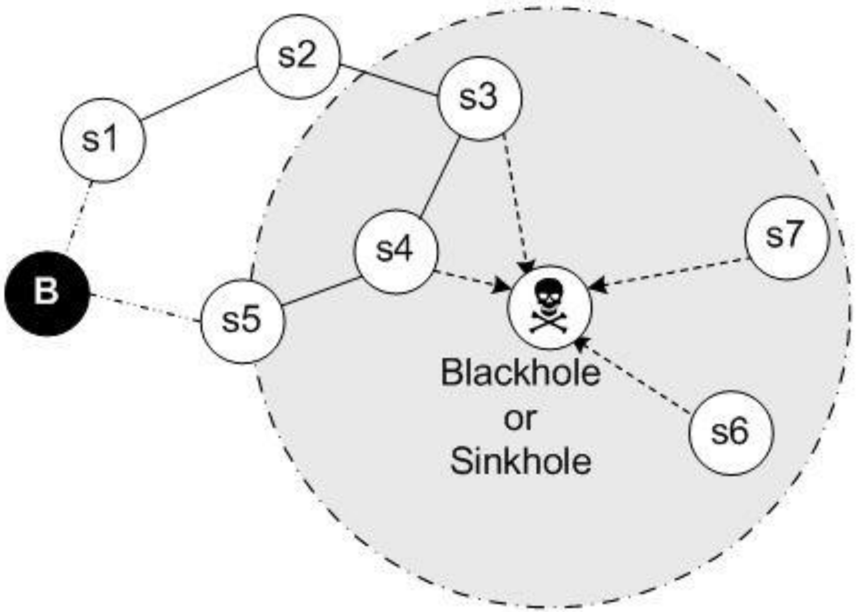
Harder to detect because selectively the packets are forwarded

Countermeasures?

- Intrusion Detection System or IDS
- Could be installed in the Base Station or Distributed IDS installed in each sensor node

Blackhole/Sinkhole Attack

- Flooding Based Protocols are vulnerable
- Malicious node inserts itself between the communicating nodes

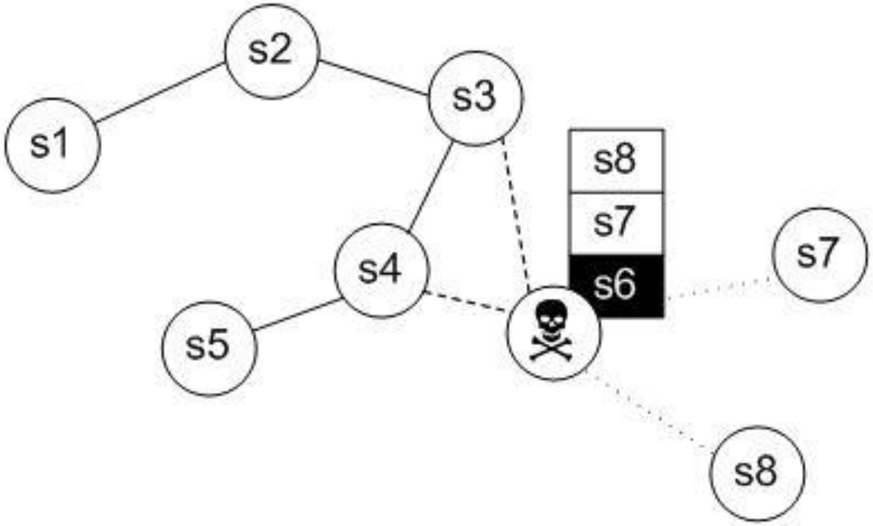


Countermeasures?

- Reward based system
- Intrusion Detection Systems (IDS) for Sensor Networks
- This attack might enable other attacks like selective forwarding; hence, IDS could be the solution

Sybil Attack

- A Node pretends to be more than one node at the same time
- Mostly affects geographical routing protocol

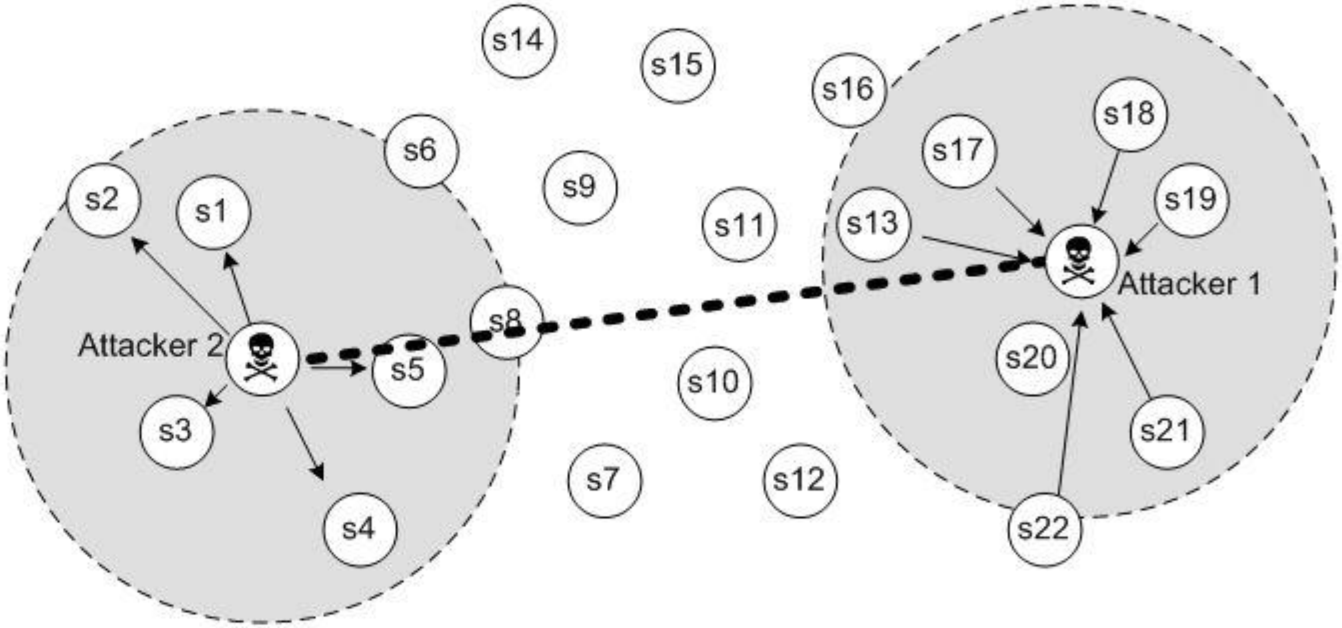


Countermeasures?

- Difficult to deal with
- Not many works are available or efficient mechanisms yet to be developed
- Radio resource testing
- Random key pre-distribution
- Others mechanisms like combinations of various schemes

Wormhole Attack

- Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location

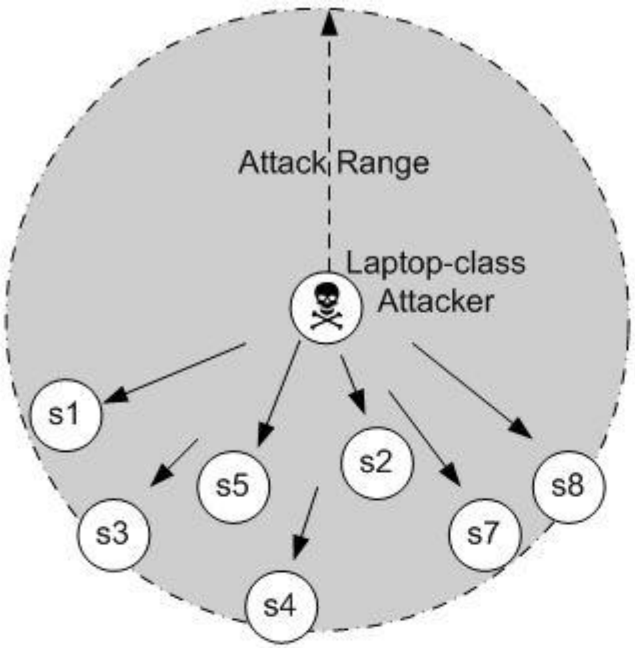


Countermeasures?

- Significant threat to Wireless Sensor Network
- It could be launched even in the neighbor discovery phase

Hello Flood Attack

- HELLO packets are used for this attack
- By sending the HELLO packet the adversary tries to be considered as the neighbor of a particular node
- With incoming packets attacker can do anything



Laptop-class attacker
Node-class attacker

Countermeasures?

- Bidirectional verification
- Multipath, multi-base routing

Acknowledgement Spoofing

- Some routing protocols use link layer acknowledgments
- Attacker may spoof acknowledgements
- This sort of attack convinces that weak link is strong or that dead node is alive
- Consequently weak link may be selected for routing; packets sent through that link may be lost or corrupted
- Countermeasures?
  - Link layer security architecture
  - Key Management mechanisms – numerous!!!

Approaches to Solutions

- Efficient key management schemes could provide proper authentication of nodes in the network
- Security for all the layers should be ensured however, this is an open research issue
- If sensed data could at least be sent to the base station using node-to-node authentication, it could deal with the rest
- Physical attacks cannot be prohibited without proper guarding mechanisms

Approaches to Solutions

- Critical Parameters in our Research are –
  - Computation Resource Utilization
  - Storage Utilization
  - Energy Utilization
  - Level of Security ??!!

- However there should be a trade-off among these parameters depending on the requirements and situation at hand

Approaches to Solutions

- A single mechanism cannot ensure security for all the levels

- Hence, there should be some sorts of co-operations among the various security measures applied to the sensors in a WSN

Our Approach (Cont.)

- Working areas I dealt with …
  - Storage-Efficient Security Schemes
  - Key Management Schemes
  - Increasing the level of security especially for military networks
  - Preventing **Homing** type DoS attacks using Key Management Schemes

- As in Military Networks, security is the Major issue we could consider a slight increase of the usage of the resources in the sensors

THANK YOU

Questions and Answers

spathan@ieee.org, spathan@bracu.ac.bd

???