Security Issues in Wireless Networks

cshong@khu.ac.kr, Choong Seon Hong, KHU

Outline

- **Security Principles**
- **Security Terms**
- **General Classification of Attacks**
- **Wireless Attacks**
- **WSN Security**
  - Key Management
  - Secure Routing
  - Threats, attacks & Defenses
- **Wireless Mesh Networks**
- **3D Wireless Networks**
- Conclusions
- References

Security Principles

- We define security in the context of two groups: "**The good guys**" and "**The bad guys**".
- It doesn't matter if we are talking about people, robots or computers.
- In our definition, if there are no "**bad guys**", you are secure by default.
- Imagine a perfect world with no crime – there would be no need for a police force. Security tries to create such a perfect world, not globally but in a **controlled space**.
- It tries to create a bubble within which there are no bad guys at a given time. So it is as though the bad guys don't exist.

High-level look at **six principles** of security thinking (Philosophy of mistrust)

- Don’t talk to any one you don’t know
- Accept nothing without a guarantee
- Take everyone as an enemy until proved otherwise
- Don’t trust your friend for long
- Use well-tried solutions
- Watch the ground you are standing on for cracks

1. Don’t talk to any one you don’t know

- In the context of security, this means you must be 100% **certain** about the identity of a device or person before you communicate.
- It is the job of **security designers** to bring you as close to 100% as you need.

2. Accept nothing without a guarantee

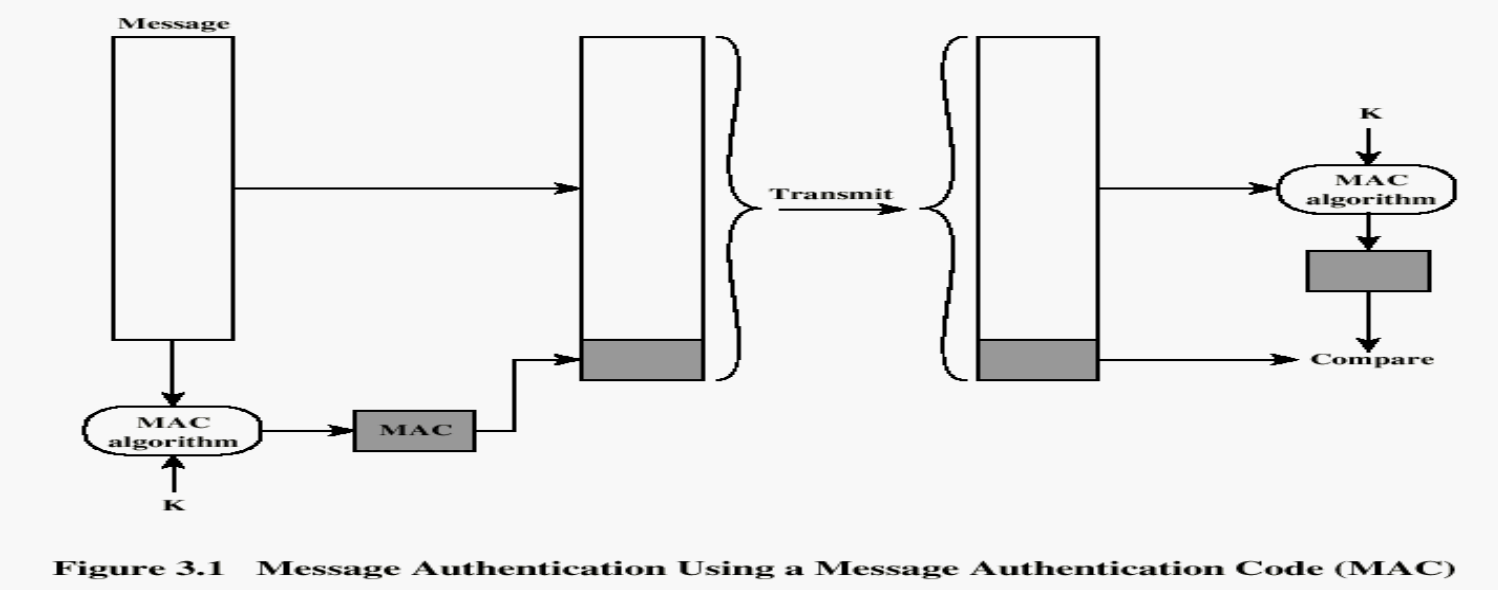


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

- Guarantee means a guarantee of **authenticity**.
- In other words, it is the "**proof**" that the message has not been changed (modified, delayed, or replaced).

3. Treat everyone as an enemy until proved otherwise

- Emphasis on the importance of not giving information to anyone until that person/device has proved identity.

4. Don’t trust your friend for long

- “Make new friends but keep the old”. The word “**keep**” implies an active process, a process of affirmation.

- So, the keys, passwords or certificates need to have a **limited life**. You should keep reaffirming the relationship by **renewing** the tokens.

5. Use well-tried solutions

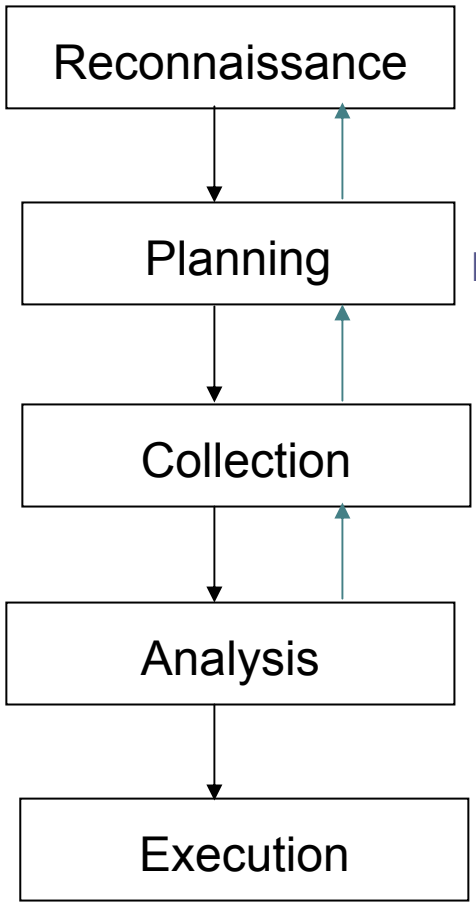
- Part of security psychology involves developing a **high level of mistrust** for anything new to see how this affects people's / device's attitude.

- For example, let's take **Encryption** as an example. The objective of encryption is to make the encrypted data look like perfectly random noise. Good algorithm will make it totally random. So no amount of analysis on the output stream would reveal any pattern.

6. Watch the ground you are standing on for cracks

- The challenge for hackers, of course, is to look for the little **cracks and crevices** that result from hidden assumptions.
- For example, a recent virus called "**Code Red**" (actually a worm) worked by exploiting the fact that when internal memory overflowed in a computer, information was accidentally left in memory in a place that was accessible from outside.
- The system designers made the **false assumption** that buffers do not overflow and that, if they do, the excess buffers are properly thrown away.
- Almost certainly this was a **subconscious assumption**; it was false and an attacker found it.

High-level Attacker Process



- Target Identification
- How you meet the goal
- Capture necessary information
- Analyze collected data
- Pick the time to join the network

Security Terms

- To set up a system in practice, we need to implement the **six principles** covered in the previous section using mechanisms that tend to be similar from one system to the next.
  - Threat Model
  - Security Protocol
  - Keys and passwords
  - Key entropy
  - Authentication
  - Authorization
  - Encryption

Security terms (cont'd)

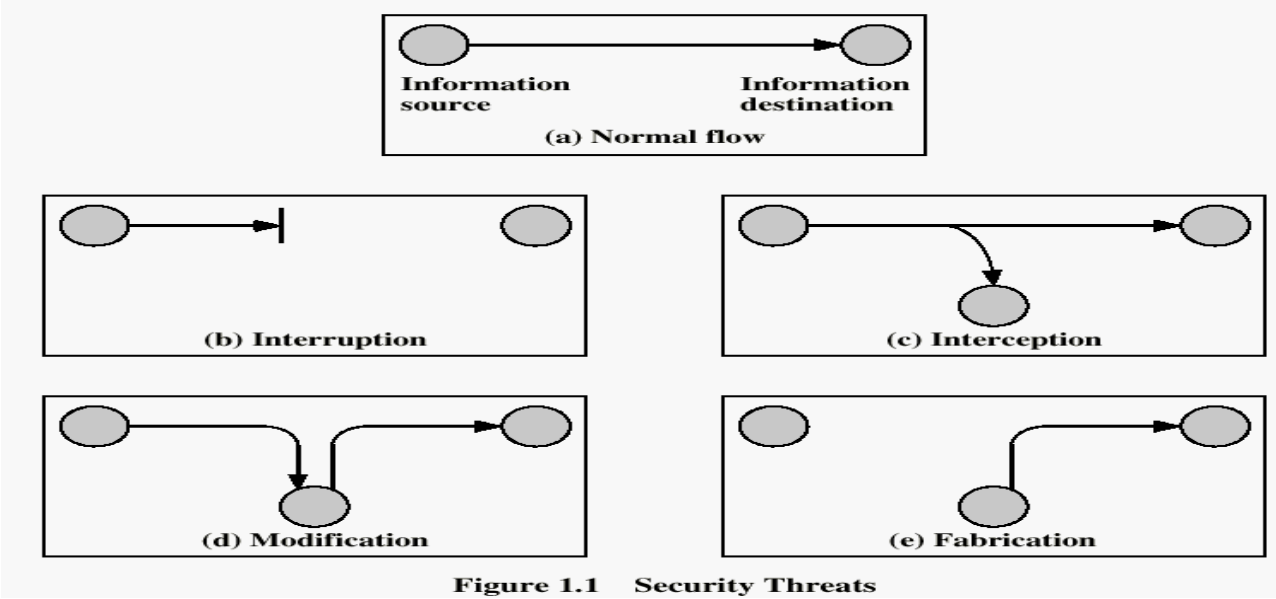


Figure 1.1 Security Threats

- **Threat Model**
  - We need a means to measure whether a security system meets its goal. One way to understand the security goals in a given situation is to make a list of all types of attack that are known.
  - This list is used to create the threat model, which is the basis for designing and evaluating security.

Security terms (cont'd)

- **Security Protocol**
  - Real security is provided by a set of processes and procedures that are carefully linked together.
  - It is important to realize that even of the most advanced encryption techniques are used, you have no security if they are used together in the wrong way.

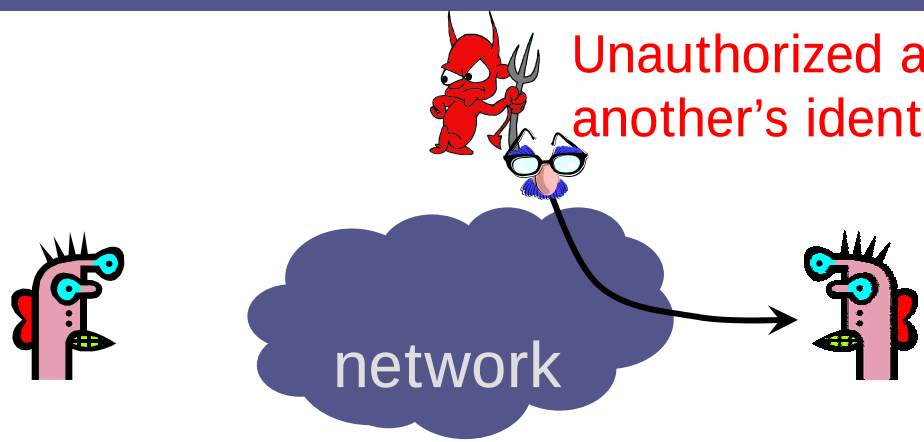
Security terms (cont'd)

- **Keys and passwords**
  - Both refer to a piece of information that is intended to be secret to two or more parties.
  - **Password:** Conventionally the term is used to refer to keys that are chosen by humans.
  - **Keys:** The term is more often used to describe information generated by machine that is usually not human readable.
    - You will often see the references to the **Length of Key**. For example, the original IEEE 802.11 had 40-bit keys, whereas most Wi-Fi WEP (Wired Equivalent Privacy) systems have 128-bit keys.

Security terms (cont'd)

- **Key entropy**
  - What is important about passwords and keys is the number of different possible values a key can take. Theoretically, a 40-bit key has 2^{40} possible values.
  - So, the number of possible key values determines the strength of the key and is known as the **Key Entropy**.

Security terms (cont'd)



- **Authentication**
  - The heart of security is the ability to distinguish the "**good guys**" from the "**bad guys**."
  - If you can't be sure whom you are talking to, you can't protect yourself against attack.
  - Two type:
    - **User Authentication** (you are talking to the person you are supposed to do so) and
    - **Message authentication** (Not tempered with delayed, altered or copied).

Security terms (cont'd)

- **Authorization**
  - The fact that you know who someone is (authenticate) doesn't mean you always want to give him access.
  - The decision to "**let him in**" is called authorization and always comes after **authentication**.

Security terms (cont'd)

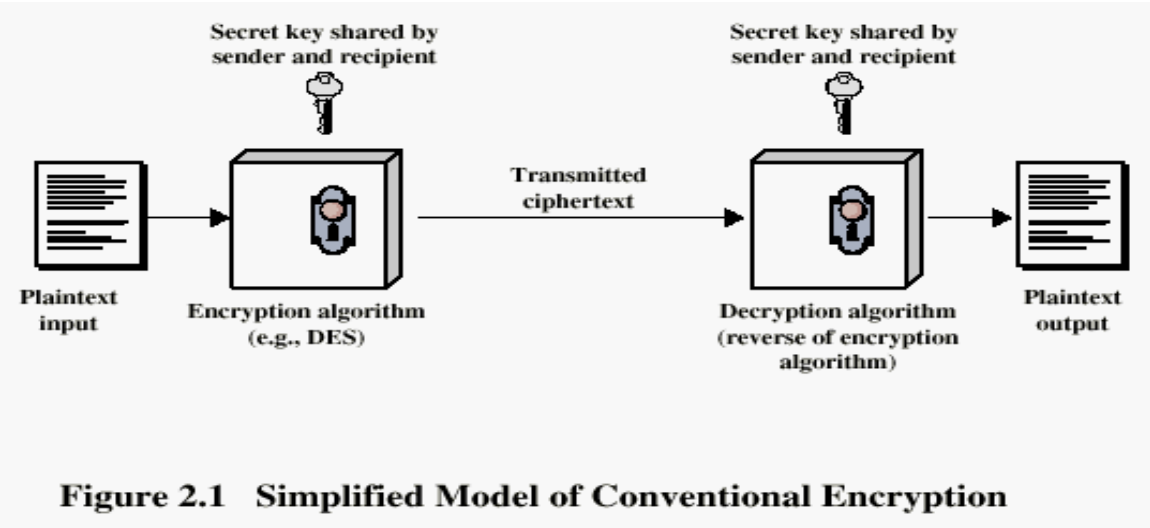


Figure 2.1 Simplified Model of Conventional Encryption

- **Encryption**
  - The process of combining a piece of data and a key to produce random-looking numbers is called Encryption.
  - It is useful only if a known key can be used to transform the random-looking numbers back to the original data.
  - Encryption algorithms are used to create security protocols.

General Classification of Attacks

- Snooping
- Modifications
- Masquerading
- Denial of Service

General Classification of Attacks (Cont'd)

- **Snooping**
  - Simply accessing **private information**. For example, getting company secrets, stock purchase decision, blackmail.
  - Encryption can be used to make snooping difficult where attacker needs to know the **secret encryption key** or to use some clever technique to recover the encrypted data.

General Classification of Attacks (Cont'd)

- **Modifications**
  - For example, if you can intercept a wireless transmission and change the destination address field (IP address) on a message, you could cause that message to be forwarded to you across the Internet, instead of its intended recipient.

General Classification of Attacks (Cont'd)

- **Masquerading**
  - When an attacking device impersonates a valid device.
  - If the device can successfully fool the target network into validating it as an authorized device, the attacker gets all the access rights that the authorized device established during log on.

General Classification of Attacks (Cont'd)

- **Denial of service (DoS)**
  - Usually blocks out everything, including the attacker
  - The objective of a DoS attack is to cause damage to the target by preventing operation of the network.

Wireless Attacks

- Wireless introduces a whole new set of opportunities for attackers trying to get **keys** because it is so easy to access the data stream, even though they may be encrypted.
- The problem for the attacker is that the data is encrypted and she needs the keys. Assuming you don't change the keys, he/she has much time as she wants to capture sample messages and analyze them.

Wireless Attacks (Cont'd)

- **To analyze the attacker to attack, let's look at some common terms**
  - Plaintext: The data before encryption – this is what we want to protect
  - Ciphertext: The encrypted version that the enemy can see over the radio link.
  - Keys: The secret value that is used to encrypt/decrypt the message
  - Cipher: The algorithm and rules used to perform the encryption and decryption.

  Ciphertext = Cipher (Key, Plaintext)

Attacker knows all three except the keys. Once they have all three components, they can attack on the keys

Wireless Attacks (Cont'd)

- **Attacking the keys through brute force**
- **Dictionary Attacks**
- **Algorithmic Attack**

Wireless Attacks (Cont'd)

- **Attacking the keys through brute force**
  - An attacker tries **every possible key** until he finds a match.
  - Given that he knows **ciphertext** and **cipher** (algorithm), he can decrypt the message and see whether it matches the plaintext.
  - The time taken for a brute force attack depends on the key size (**key entropy**).

Wireless Attacks (Cont'd)

- **Dictionary Attacks**
  - **The enemy uses a huge dictionary, or database, containing all the likely passwords.**

Wireless Attacks (Cont'd)

- **Algorithmic Attack**
  - **This approach is to try to break the algorithm, that is try to find the flaws in the way the encryption is performed that might expose the key value.**
  - **However understanding the weakness of a particular algorithm often requires that you are a cryptographic expert.**

What's different about sensor nets?

- Stringent resource constraints
- Insecure wireless networks
- No physical security
- Interaction with the physical environment

WSN Security

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

Why security?

- **Confidentiality**
  - Need the ability to conceal message from a passive attacker
- **Integrity**
  - Need the ability to confirm the message has not been tampered with
- **Authentication**
  - Need to know if the messages are from the node it claims to be from
- **Access Control**
  - Need the ability to determine if a node has the ability to use the resources

Why security is different in WSN?

- **Sensor Node Constraints**
  - Battery (2xAA)
  - Processing power (8Mhz)
  - Memory (<128KB 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

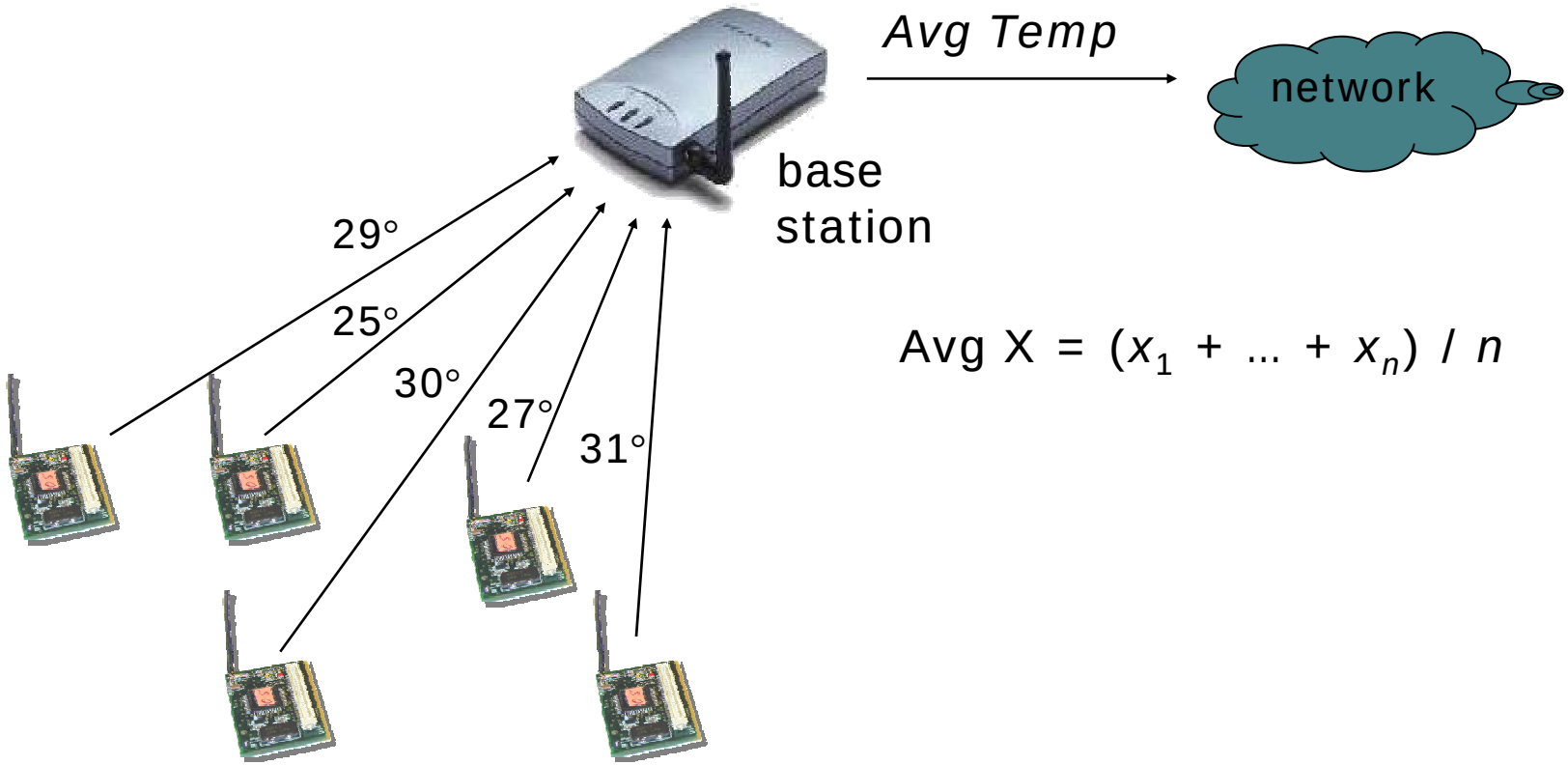
Challenges….

- **Must avoid complex key management**
  - Simple and must be super-easy to deploy
- **Crypto must run on wimpy devices**
  - We're not talking 2GHz P4's here!
  - Dinky CPU (4-8 MHz), little RAM ($\leq$ 256 bytes), lousy battery
  - Public-key cryptography? **NO**
  - **ECC**
- **Need to minimize packet overhead**
  - Radio is very power-intensive
    - 1 bit transmitted $\approx$ 1000 CPU ops
  - TinyOS packets are $\leq$ 28 bytes long

Attacks on sensor nets

Spoofed, altered, or replayed routing information	Create routing loop, attract or repel network traffic, extend or shorten source routes, generate false error messages etc
Selective forwarding	Either in-path or beneath path by deliberate jamming, allows to control which information is forwarded. A malicious node act like a black hole and refuses to forward every packet it receives.
Sinkhole attacks	Attracting traffic to a specific node, e.g. to prepare selective forwarding
Sybil attacks	A single node presents multiple identities, allows to reduce the effectiveness of fault tolerant schemes such as distributed storage and multipath etc.
Wormhole attacks	Tunneling of messages over alternative low-latency links to confuse the routing protocol, creating sinkholes etc.
Hello floods	An attacker sends or replays a routing protocols hello packets with more energy

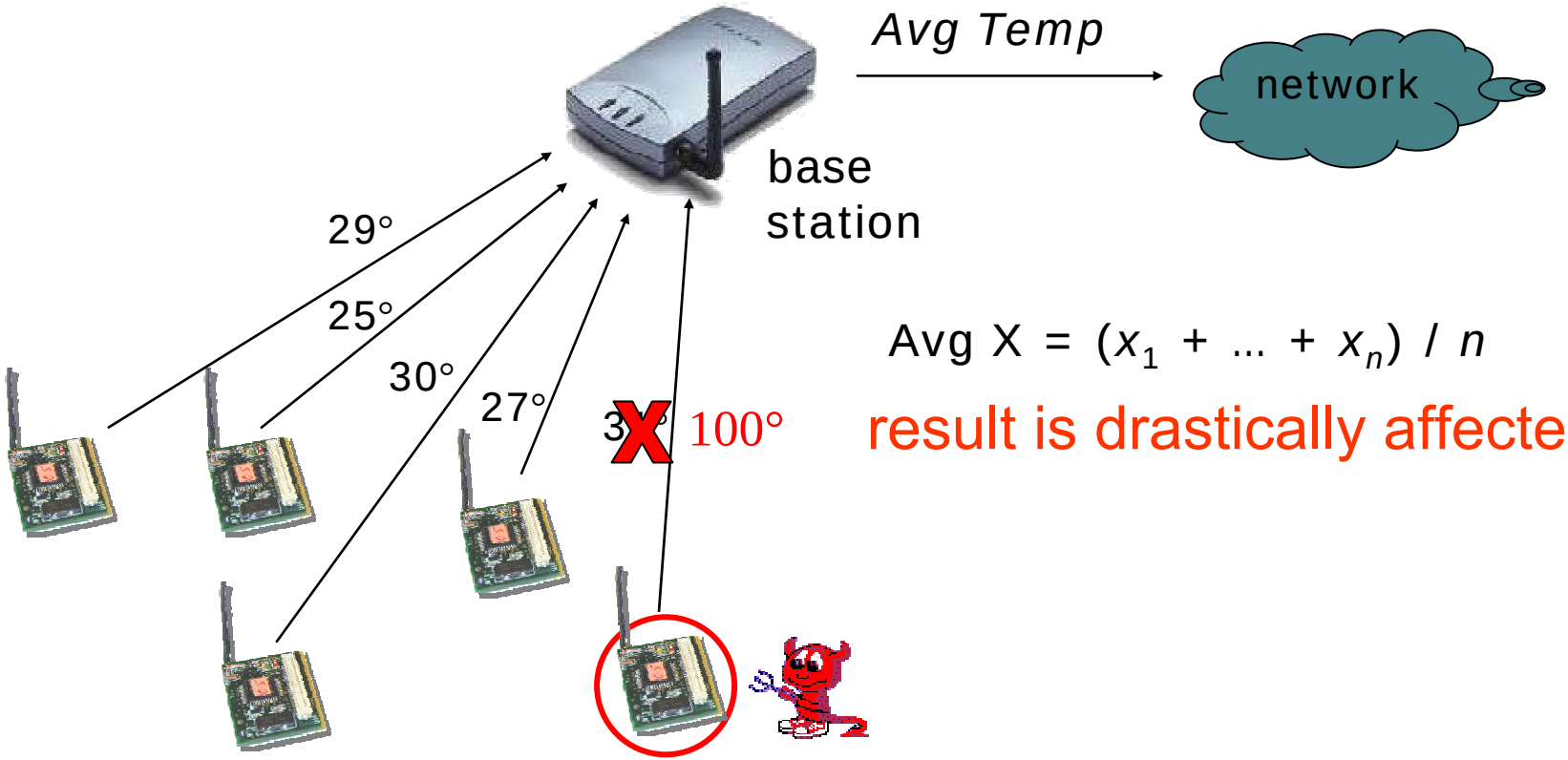
An Example (WSN application)



Avg X = $(x_1 + \ldots + x_n) / n$

Computing the average temperature

An Example + an attack



Avg X = $(x_1 + \ldots + x_n) / n$

result is drastically affected

Computing the average temperature

Cryptography

- **Secret key cryptography**
  - Faster
  - Consume much less computation energy
  - Key management is an issue
- **Public key cryptography**
  - Requires more computation power and memory
  - Cost more energy
  - Has been thought as impossible in WSNs
  - Key management is easier

Limitations of cryptography

- Can’t prevent traffic analysis
- Can’t prevent re-transmitted packets
- Can’t prevent replayed packets
- Can’t prevent delayed packets
- Can’t prevent packets from being jammed
- Can’t prevent malicious insiders, captured nodes

Crypto is not magic fairy dust

It won’t magically make insecure services secure.

Proper key management can help in a better way to protect sensory data

Key Management Goals

- The protocol must establish a key between all sensor nodes that must exchange data securely
- Node addition / deletion should be supported
- It should work in undefined deployment environment
- Unauthorized nodes should not be allowed to establish communication with network nodes

Key Management Schemes

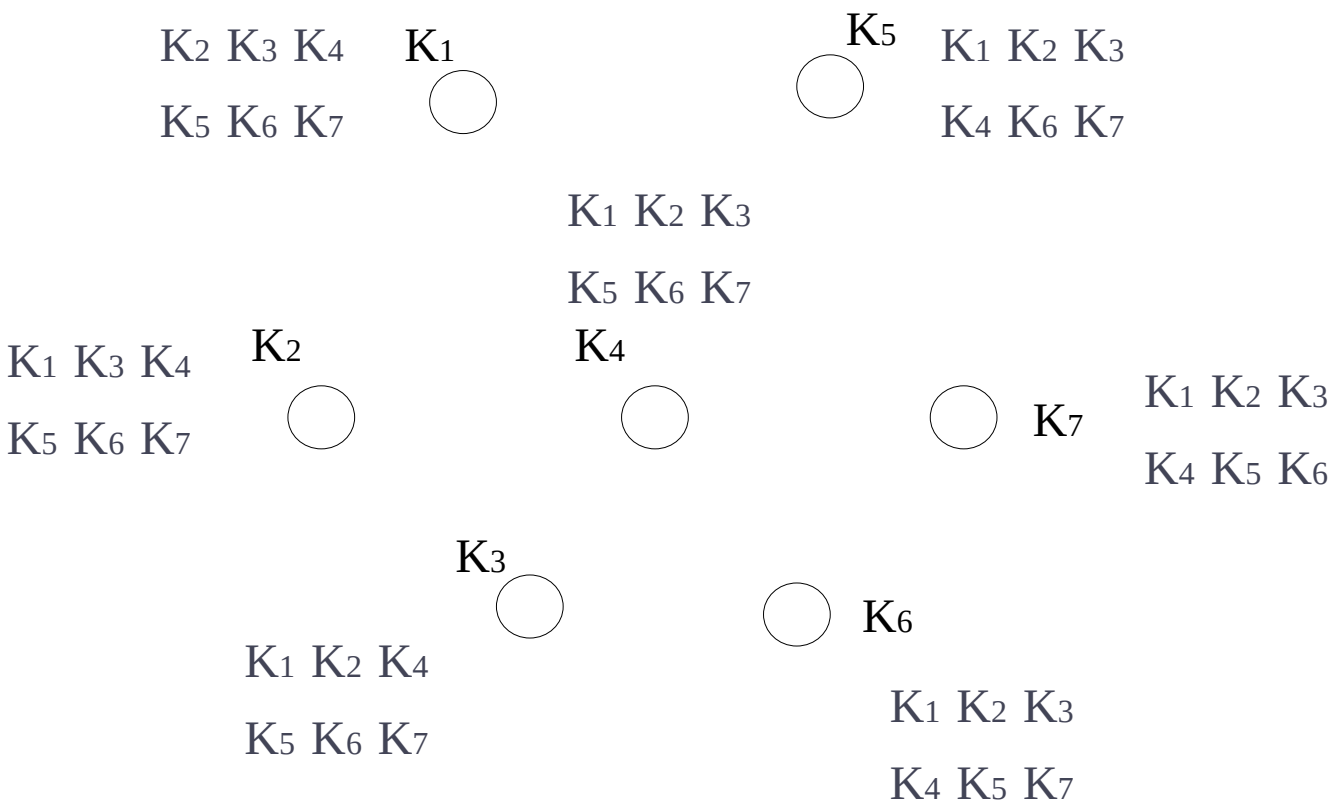
- **Trusted Server Scheme**
  - Depends on trusted server like Kerberos, no trusted infrastructure in WSN
- **Asymmetric (Public Key) Scheme**
  - Infeasible due to limited resources in WSN
- **Key Pre-Distribution Scheme**

Key pre-distribution

- **Master key approach**
  - Memory efficient but lack the security
  - All sensors use one master key to communicate with the rest of the sensor nodes
  - **Pros:** Efficient use of memory since the sensor only needs to save one key
  - **Cons:** Compromising one sensor node will compromise the whole network

- **Pair-wise key approach**
  - **N -1** keys for each node
  - Good security
  - Requires a lot of memory
  - Lack of scalability

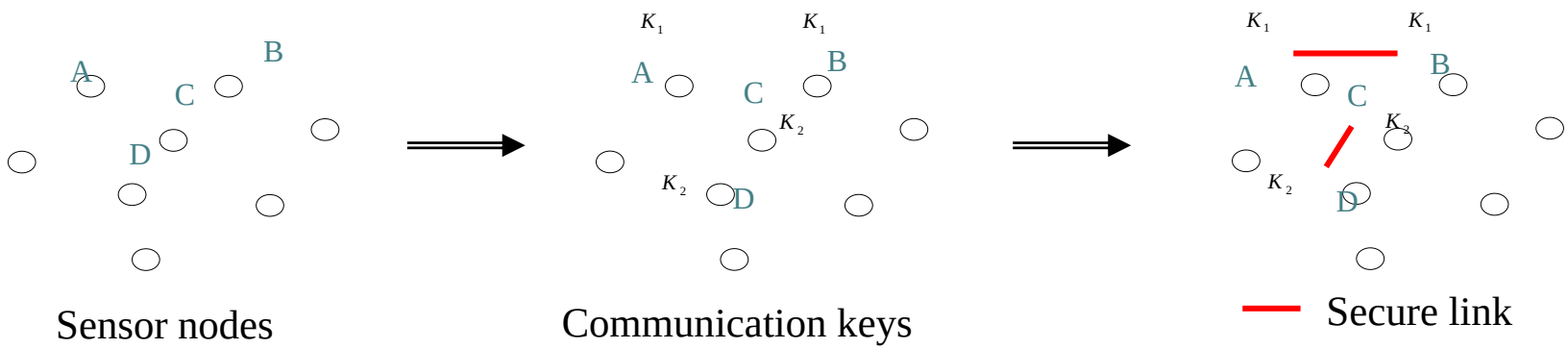
Key pre-distribution (Conventional Random Pair-wise scheme)



Requires a large storage space for keys in a large WSN

Key pre-distribution (Random Key Based basic Scheme)

- L. Eschenauer, V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *9th ACM Conference on Computer and Communication Security*, pp.41-47, November 2002. (CCS'02)
- Each node randomly picks *r* keys from a unordered key pool *S*.
- Use the common shared key to establish a secure link.
- Relies on probabilistic key sharing among the nodes of a random graph.



Shared key discovery: Each sensor node broadcasts a key identifier list and compares the list of identities received to the keys in their key chains. Note that more than one pair may share the same key

Key pre-distribution (Random Key Based basic Scheme)

- The probability that two key rings share at least a key is

  1 - Pr[two nodes do not share any key].

To compute the probability that two key rings do not share any key, we note that each key of a key ring is drawn out of a pool of ***P*** keys *without* replacement. Thus, the number of possible key rings is:

$$\frac{P!}{k!(P-k)!}$$

Pick the first key ring. The total number of possible key rings that do not share a key with this key ring is the number of key-rings that can be drawn out of the remaining ***P − k*** unused key in the pool, namely:

$$\frac{(P-k)!}{k!(P-2k)!}$$

Key pre-distribution (Random Key Based basic Scheme)

- Therefore, the probability that no key is shared between the two rings is the ratio of the number of rings without a match by the total number of rings.

- Thus, the probability that there is at least a shared key between two key rings is:

$$\frac{k!(P-k)!(P-k)!}{P!k!(P-2k)!}$$

Key pre-distribution (Random Key Based basic Scheme)

- Probability of sharing at least one key.

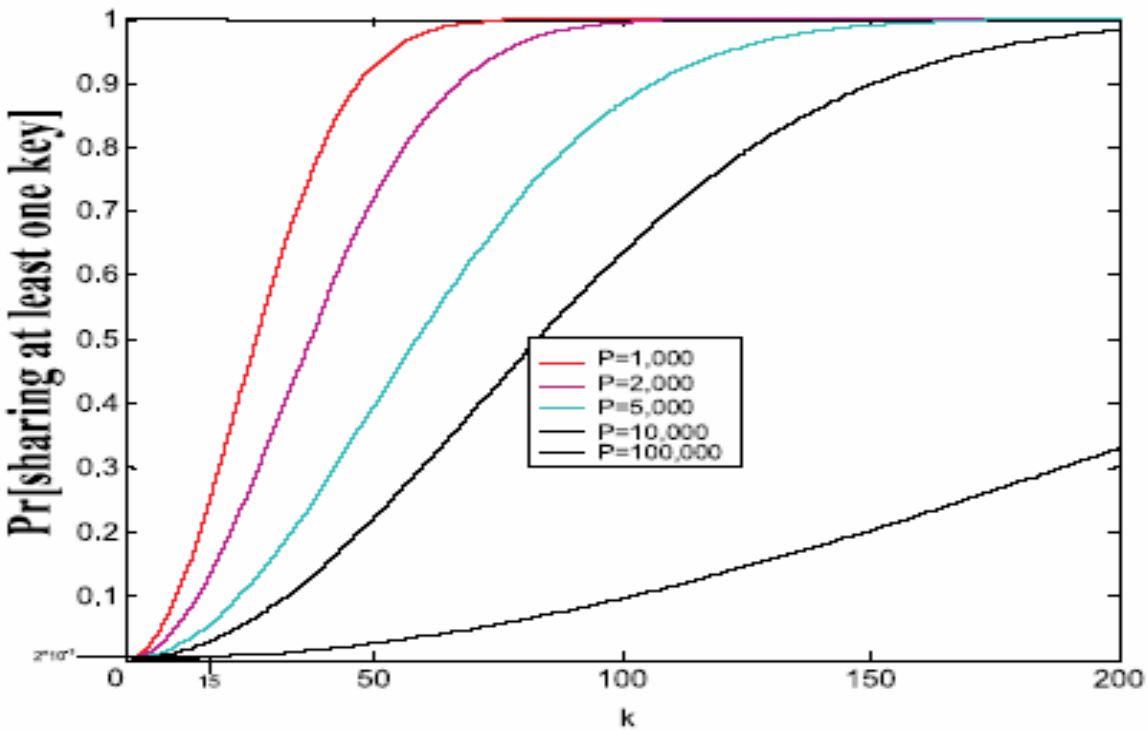


Figure 2: Probability of sharing at least one key when two nodes choose k keys from a pool of size P

Key pre-distribution (other approaches)

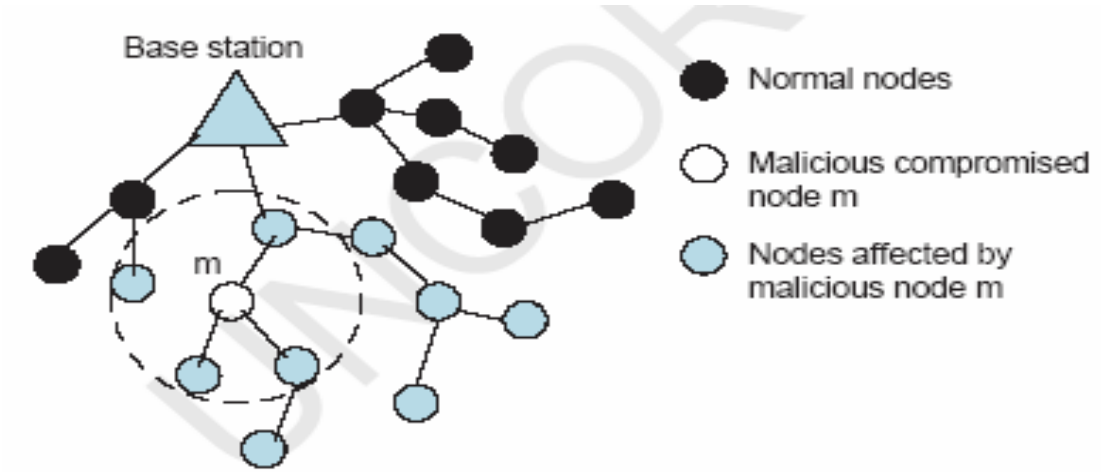
- **Key management**, *by Eschenauer et al. in ACM CCS'02.*
- **SPINS,** *by Perrig et al. in Wireless Networks Journal (WINE), 2002.*
- **Random Key Assignment,** *by pietro et al. in ACM SASN '03.*
- **Establishing Pairwise Keys,** *by Liu et al. in ACM CCS'03.*
- **LEAP,** *by Zhu et al. in proc. of ACM CCS'03.*
- **Pairwise Key Pre-distribution**, *by Du et al. in ACM CCS'03.*
- **Random Key Predistribution,** *by Chan et al. in IEEE S&P'03*
- **Deployment knowledge,** *by Du et al. in IEEE INFOCOM'04.*
- **TinySec**, *by Chris Karlof et al, UC Berkeley in SenSys'04*

Secure Routing (Attacks on routing)

Protocol	Relevant Attacks
TinyOS beaconing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods
Clustering based protocols (LEACH, TEEN, PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes
Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

Secure Routing (an example)

Problem



The typical tree-structured hierarchy of a wireless sensor network.

A malicious compromised node **m** can affect immediate neighbors as well as their downstream children.

Secure Routing (Cont'd)

Defense:

INSENS: Intrusion-tolerant routing for wireless sensor networks

Intrusion tolerance

- Limited broadcast using one way hash chains (OHCs): INSENS permits only base stations to initiate flooding of the network, e.g. to set up routing information.
- Multipath routing: multiple disjoint paths are set up from each sensor node
- Limited routing updates: Only the base station is allowed to update a node's data routing table.

Secure Routing (Cont'd)

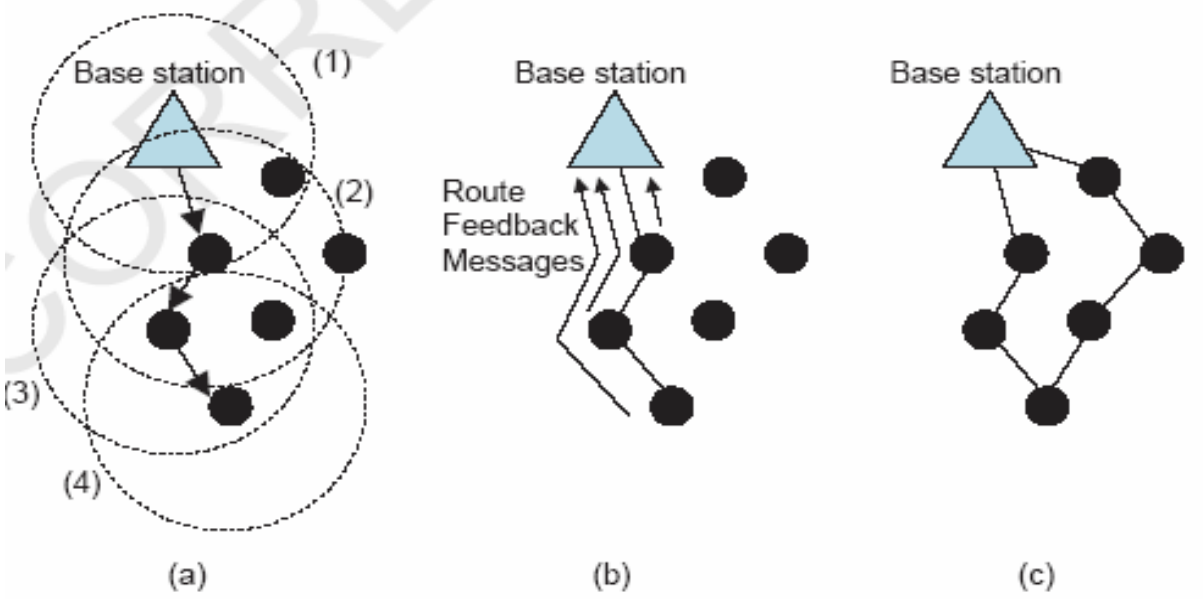
Defense:

INSENS: Intrusion-tolerant routing for wireless sensor networks

Adaptation to resource constraints

- Symmetric key cryptography is chosen to implement confidentiality and authentication between the base station and each resource-constrained sensor node.
- Complexity is pushed away from resource-poor sensor nodes and into the resource-rich base station
- lightweight **bidirectional verification** is applied to defend against the rushing attack. The nested message authentication code (MAC) is used as a countermeasure against the wormhole attack.
- **Multipath routing** to Multiple Base stations Schemes are presented to improve the tolerance of routing

Secure Routing (Cont'd)



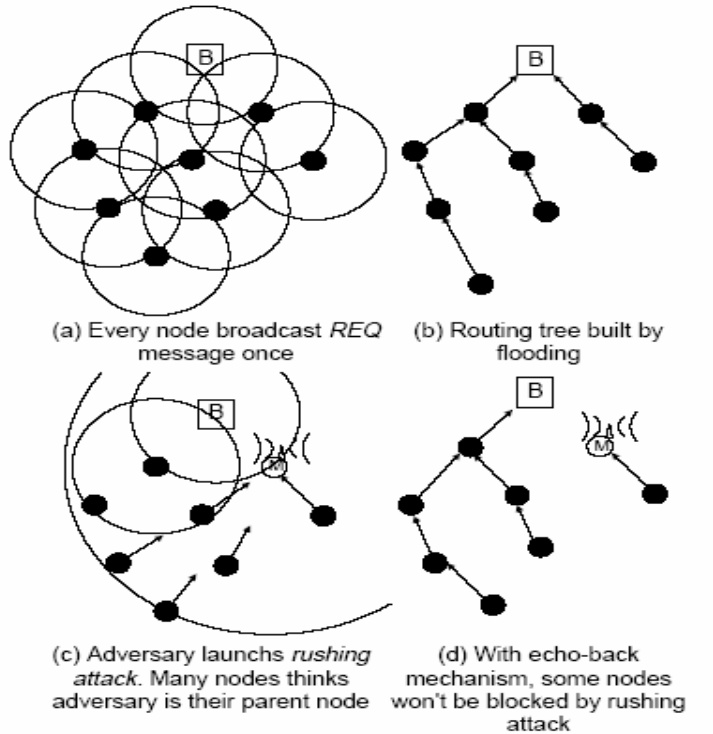
Three Phases of Basic INSENS:

- (a) **ROUTE REQUEST** is flooded from the base station (only one path is shown here).
- (b) **ROUTE REPLIES** are unicast back to the base station from each sensor node, containing neighborhood topology information.
- (c) A routing table is securely unicast to each node, in a breadth-first manner, establishing **multipath routing**.

Secure Routing (Cont'd)

simple echoback scheme

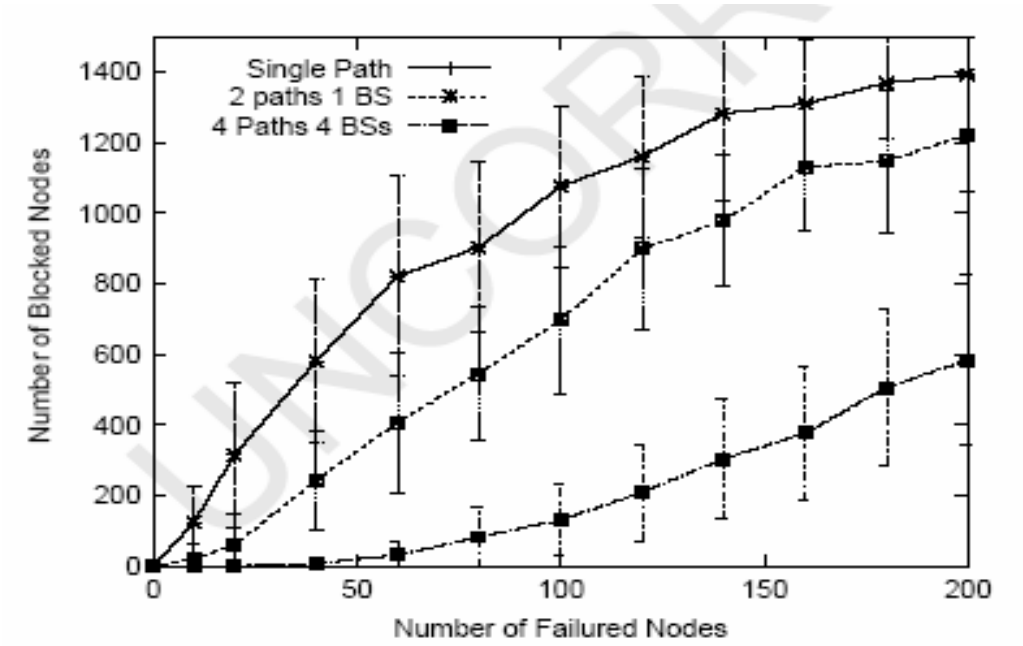
In this scheme, a node x only forwards the REQ messages for the nodes that can receive a message from x. Those nodes are termed x's reachable neighbors



Enhanced single-phase INSENS:

- (a) Secure REQ message flooding
- (b) Builds a secure routing tree.
- (c) A standard rushing attack
- (d) Rushing attack is blocked by the echo-back countermeasure.

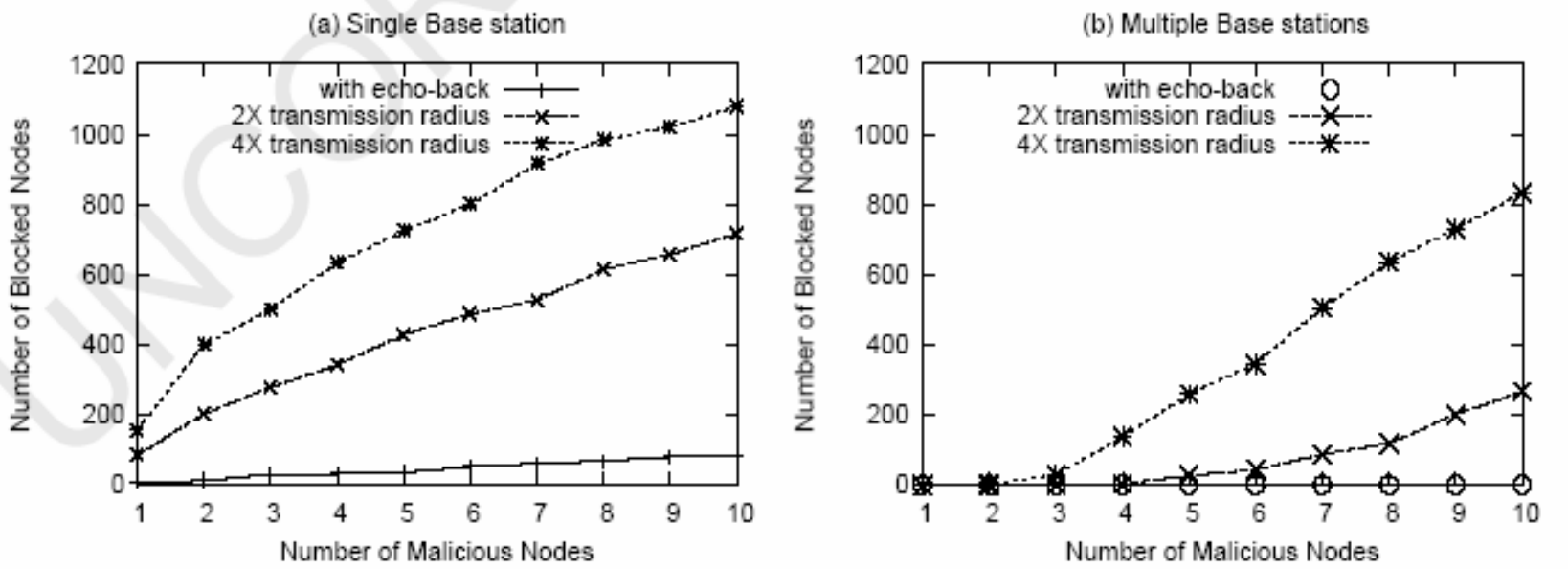
Secure Routing (Cont'd)



Effects of node failures.

- (a) INSENS builds **multiple paths** to bypass compromised nodes

Secure Routing (Cont'd)

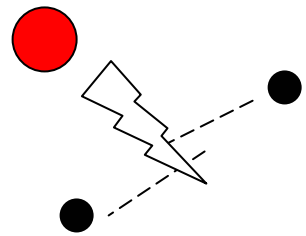


Effects of rushing attack during multipath routing setup (Single and multiple base stations).

- (a) The echo-back approach is very effective in limiting the rushing attack.

Threats, Attacks & Defenses

- **Physical layer**
  - **Jamming:** interference with radio frequencies used by a node's transceiver
    - Spread-spectrum communication
    - Priority messages
    - Lower duty cycle
    - Mode change
    - Jammed Area Mapping service
  - **Node tampering:** attack data confidentiality, robustness and survivability
    - Tamper-proofing: automatically erase sensitive cryptographic information
    - Hiding
    - Software algorithms for reducing revealed secret information



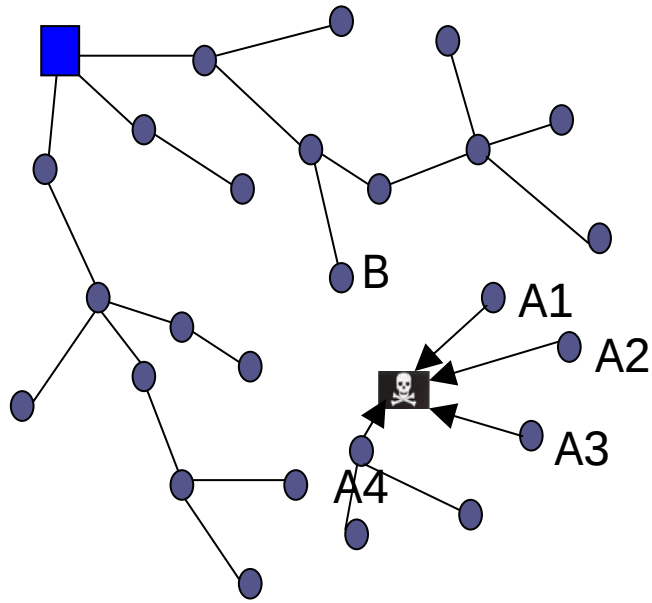
Jamming attack

Threats, Attacks & Defenses (Cont'd)

- **Link layer**
  - **Collision:** prevent nodes from successfully transmitting packets.
    - Error-correcting codes (partly)
  - **Exhaustion:** exhaustion of a network's battery power.
    - Rate limitation
  - **Unfairness:** induce unfairness in the priorities for granting medium access.
    - Use of small frames so that an individual node can capture the channel only for a short time.

Threats, Attacks & Defenses (Cont'd)

- **Network layer**
  - **Passive information gathering**
    - Strong encryption techniques need to be used
  - **False routing information**
    - Strong authentication techniques
  - **Selective forwarding:** malicious nodes may intentionally drop some packets and selectively forwards other packets.
    - Redundant routes
    - Redundant messages
    - IDS for sensor networks to detect malicious nodes.

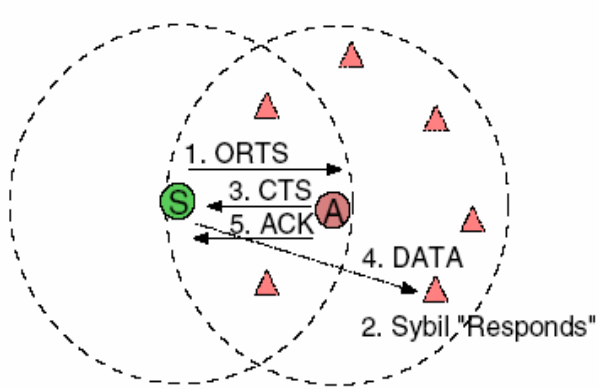


False Routing Information:

Example: captured node attracts traffic by advertising shortest path to sink, high battery power, etc

Threats, Attacks & Defenses (Cont'd)

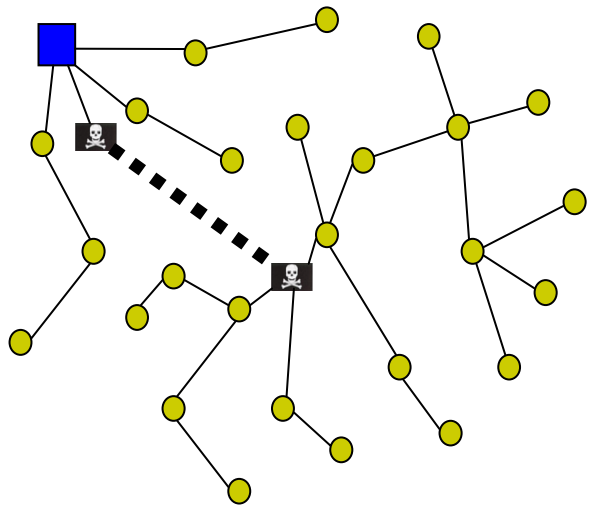
- **Network layer (Cont'd)**
  - **Sybil attack:** a single node claims to be other nodes in the networks.
    - Authentication and encryption techniques.
  - **Sinkhole attack:** tempt nearly all the traffic from a particular area through a compromised node, creating a metaphoric sinkhole with the adversary at the center.
    - Authentication and encryption techniques



Node ***A*** performs a Sybil attack against ***S***

Threats, Attacks & Defenses (Cont'd)

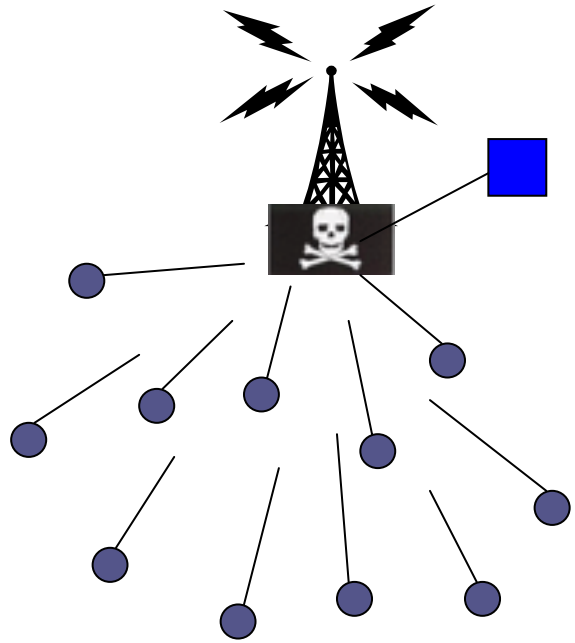
- **Network layer (Cont'd)**
  - **Wormhole attack:** an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part
    - No detecting technique is feasible for sensor networks
    - Avoid routing race conditions
    - Packet Leashes to defend against this attack



Wormhole attack

Threats, Attacks & Defenses (Cont'd)

- Network layer (Cont'd)
  - HELLO Flood Attack:
    - Many WSN routing protocols require nodes to broadcast HELLO packets after deployment, which is a sort of neighbor discovery based on radio range of the node
    - Laptop class attacker can broadcast HELLO message to nodes and then advertises high-quality route to sink
    - Defense: Authentication and verify the bidirectional link



Hello Flood Attack

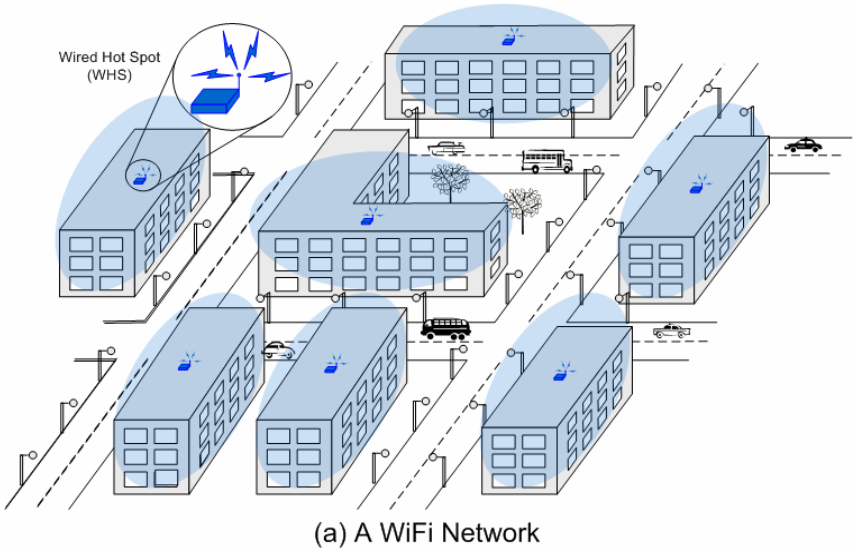
Attacks and Countermeasures at a glance

Layer	Attacks	Defense
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle; Region mapping, mode change
	Tampering	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network and routing	Spoofed, altered or replayed routing information	Egress filtering, authentication, monitoring
	Selective forwarding	Redundancy, probing
	Sinkhole	Authentication, monitoring, redundancy
	Sybil	Authentication, probing
	Wormhole	Authentication, packet leashes
	Hello flood attacks	Authentication, verify the bidirectional link
	Acknowledge spoofing	Authentication
Transport	Flooding	Client puzzles
	Desyncrhonization	Authentication

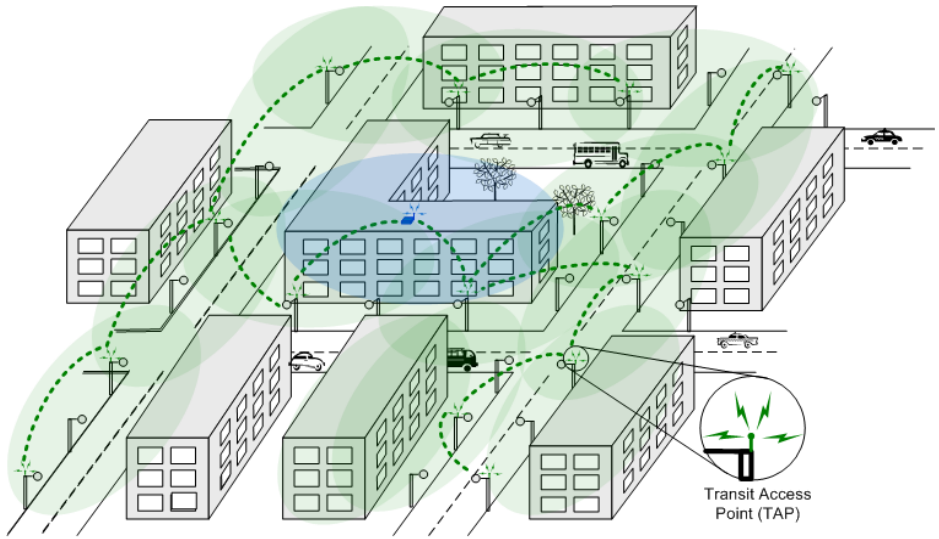
Wireless Mesh Networks

- **Introduction**
- **Challenges**
- **Attacks**
- **Observation**

Introduction



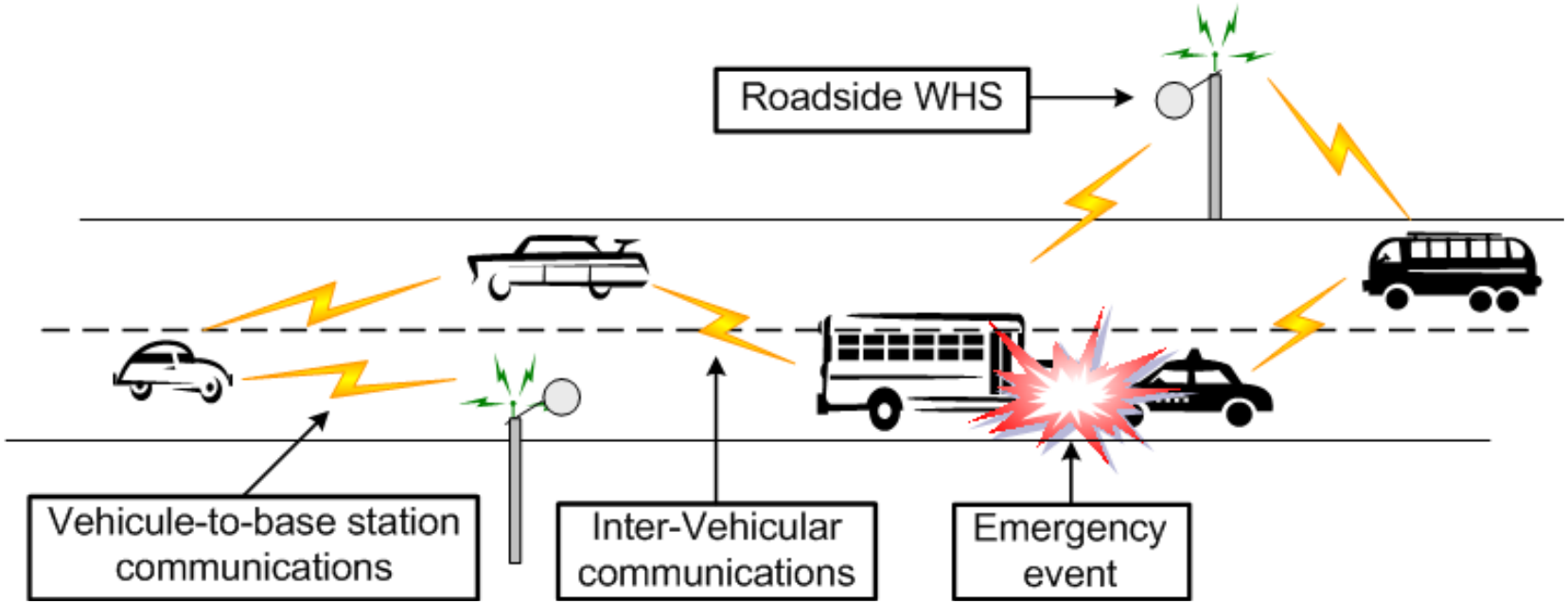
(a) A WiFi Network



(b) A Mesh Network

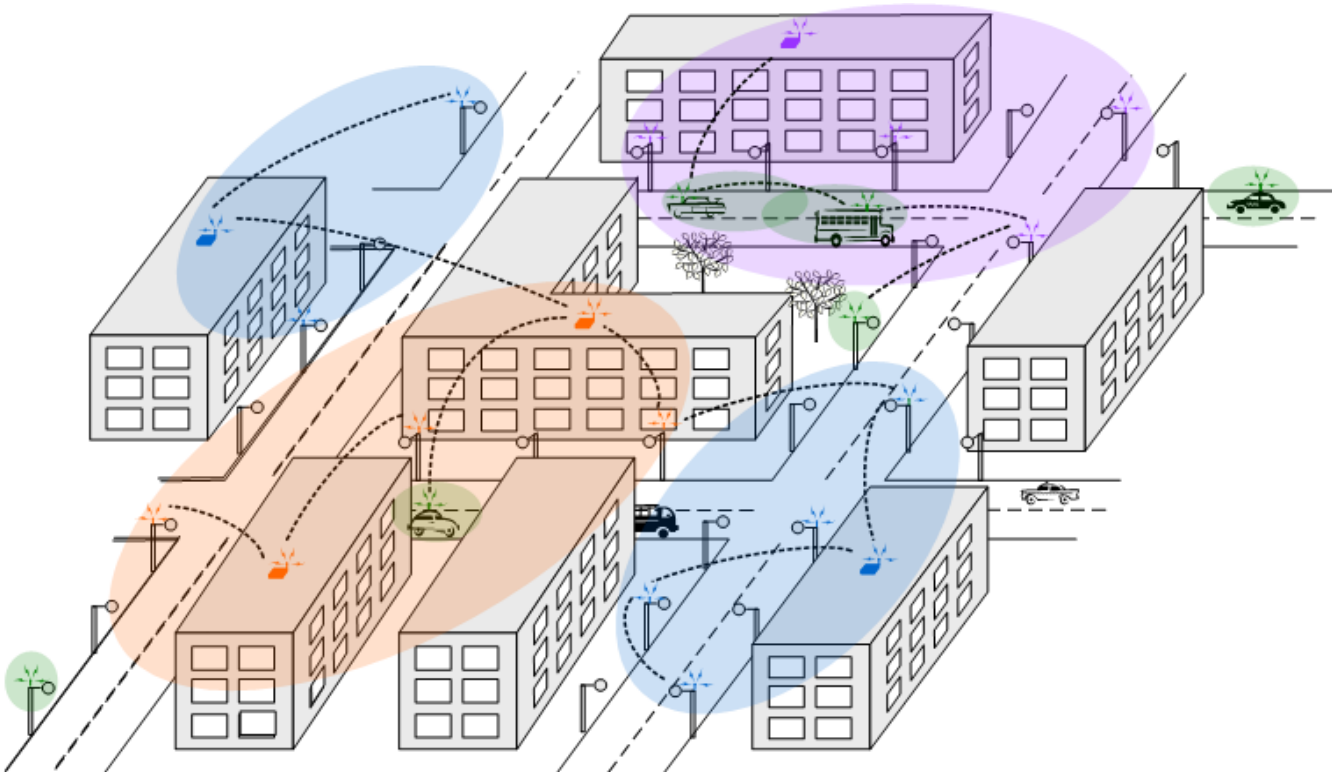
- **Two approaches to providing Internet connectivity**
  - **(a) WiFi Network:** several Wireless Hot Spots (WHSs) are needed to offer good coverage of a given area;
  - **(b) Wireless Mesh Network (WMN):** by using one WHS and several Transit Access Points (TAPs), it is possible to cover the same area as in (a); the TAPs rely on the WHS to transmit their traffic to and from the Internet.

Introduction…



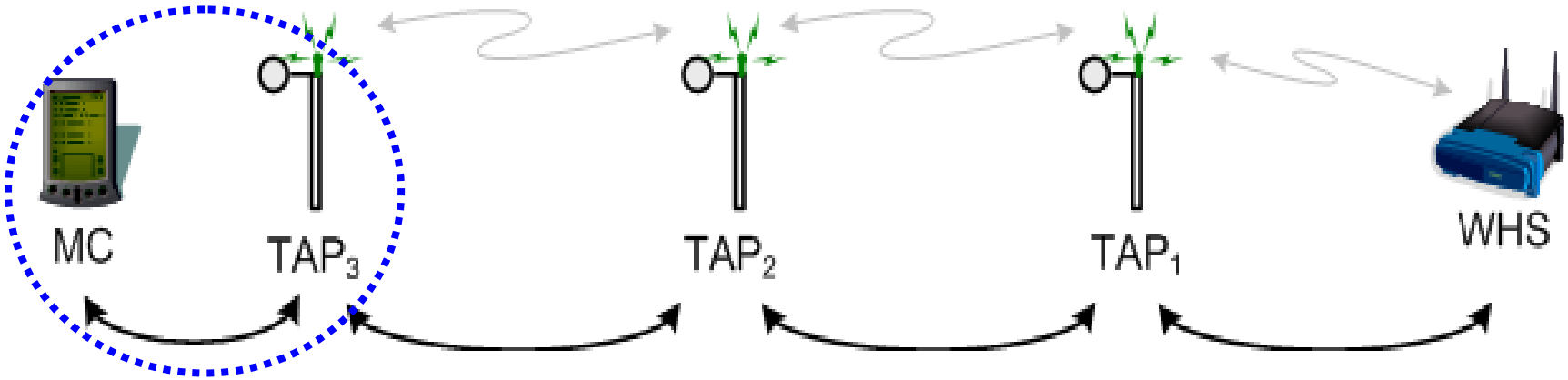
- **A very special WMN:** The Vehicular Network. It consists of a set of cars and roadside WHSs that exchange messages to report some important events or offer services to the drivers.

Introduction…



- **A multi-operator WMN:** In this example, three WMN operators (the devices managed by each of them are represented in different colors: blue, purple and orange) and one vehicular network operator (represented in green) coexist in the network.

Communication Scenario



The mobile client MC is within the transmission range of TAP3 and relies on TAP1 and TAP2 to relay its traffic to and from WHS.

Security challenges…

- Three critical security challenges
  - Detection of corrupt TAPs and mesh clients
  - Securing the routing mechanism and
  - Definition of a proper fairness metric to ensure a certain level of fairness in the WMN.

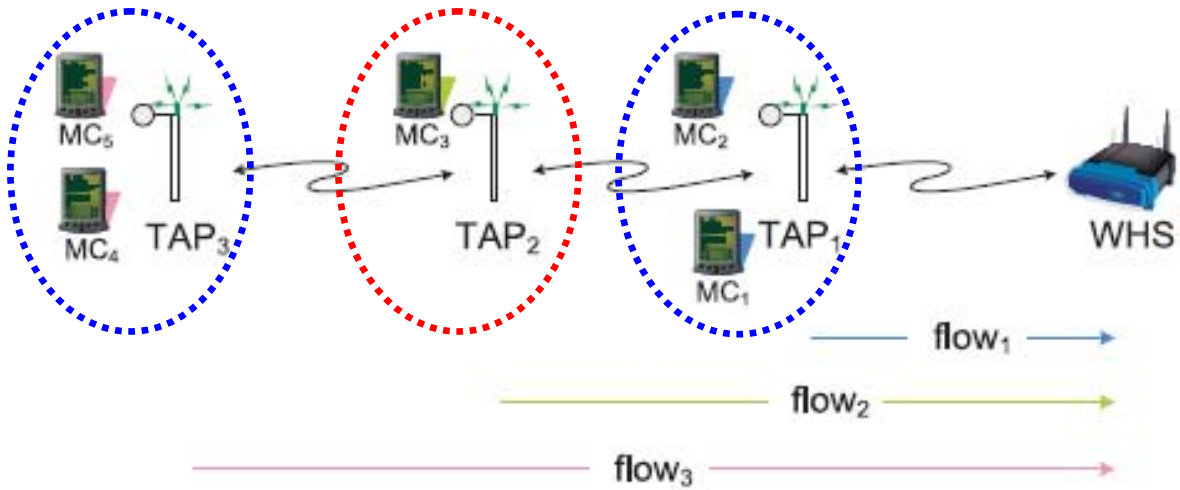
Attacks on TAPs

- Simple removal or replacement of TAPs in order to modify the network topology
- Accessing the internal state of the captured device without changing it
- Accessing and modifying the internal state to change the routing algorithm, secret data etc.
- Cloning the captured device and installing replicas at some strategically chosen locations to inject false data or to disconnect parts of the WMN.

Attacks on Routing Mechanism

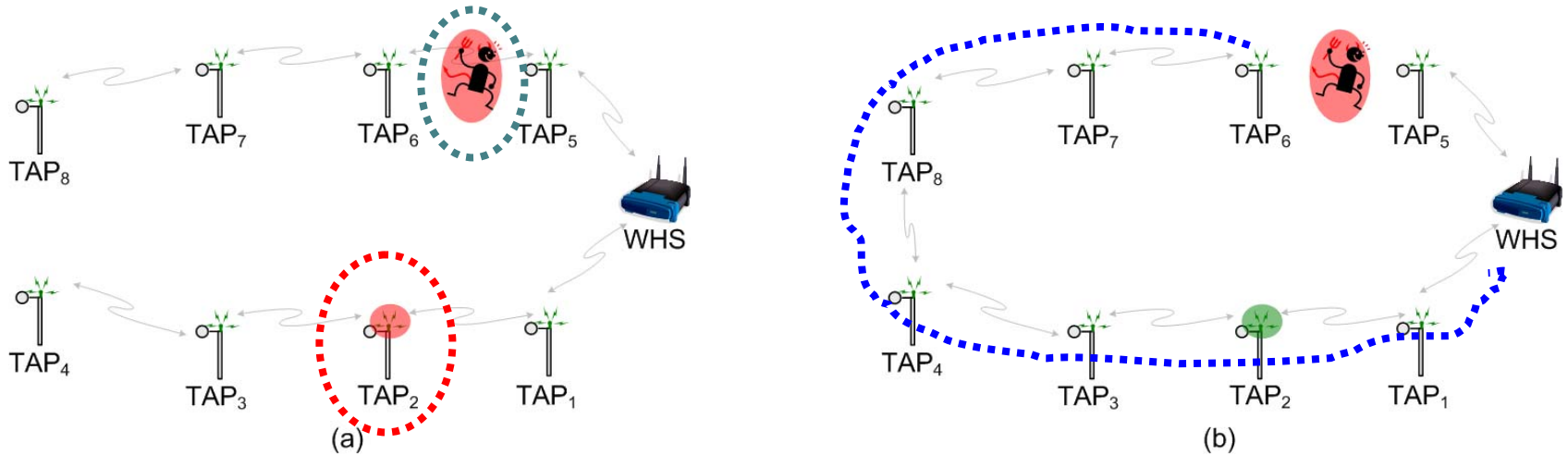
- Tamper with the routing messages
- Modify the state of one or several TAPs in the network
- Use replicated node(s) to perform DoS attacks

Fairness Problem



- In order to define the bandwidth sharing, it is important to take into consideration the number of mobile clients served by each of the TAPs.
- Flow 2 should thus have half as much as what flow 1 and flow 3 have, as TAP2 is serving only one client, whereas TAPs 1 and 3 are serving 2 clients each.
- Fairness is closely related to the # of hops b/w TAPs and WHS

Attack Example



- **Two attacks and the related countermeasures:**
- In (a), the adversary corrupted TAP2 and placed a jamming station between TAP5 and TAP6.
- As shown in (b), the detection of these attacks, if it is possible, leads to the reconfiguration of the WMN: the operator replaced the compromised TAP (the TAP circled in red in (a)) by an uncorrupted one (the TAP circled in green in (b)) and updated the routing.
- In this example, the reconfiguration leads to much longer routes for some TAPs (e.g., TAP6 was 2-hops away from the WHS and is now 7-hops away).

Observation

- **Key distribution**
  - Multi-hop, multi-operators having different entities (MC, MR, WHS)
- **Secure routing**
  - Needs different kinds of authentication (mobility)
- **Intruder detection** **For both mesh routers and mesh clients**
  - jamming (DoS) attack
  - malicious clients
- **Enforcement of a proper fairness metric**
  - To allow equal share of the resources

3 Dimensional Wireless Networks

- Introduction
- Deployment Strategy
- Routing
- Challenges

Introduction

- Although most wireless terrestrial networks are based on two dimensional (2D) design, in reality, such networks operate in three dimensions (3D).

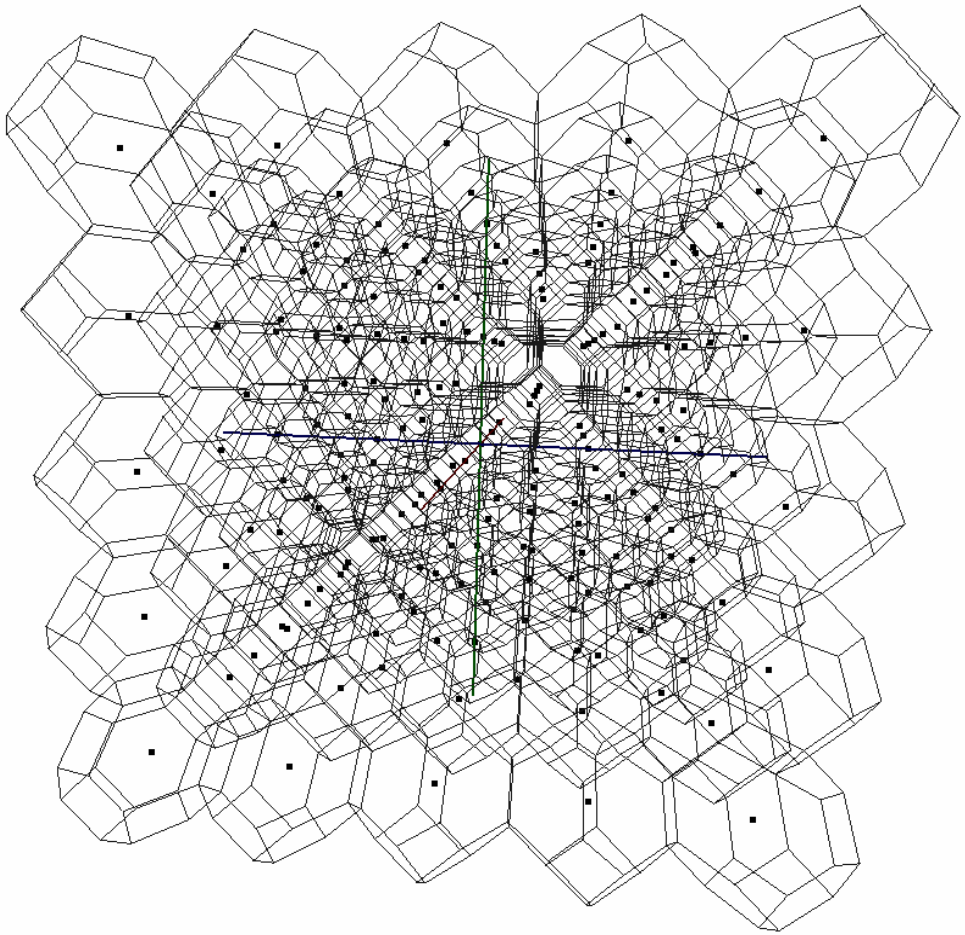
- Since most often the size (i.e., the length and the (width) of such terrestrial networks is significantly larger than the differences in the third dimension (i.e., the height) of the nodes, the 2D assumption is somewhat justified and usually it does not lead to major inaccuracies.

- However, in some environments, this is not the case; the underwater, atmospheric, or space communications being such apparent examples.

Introduction…

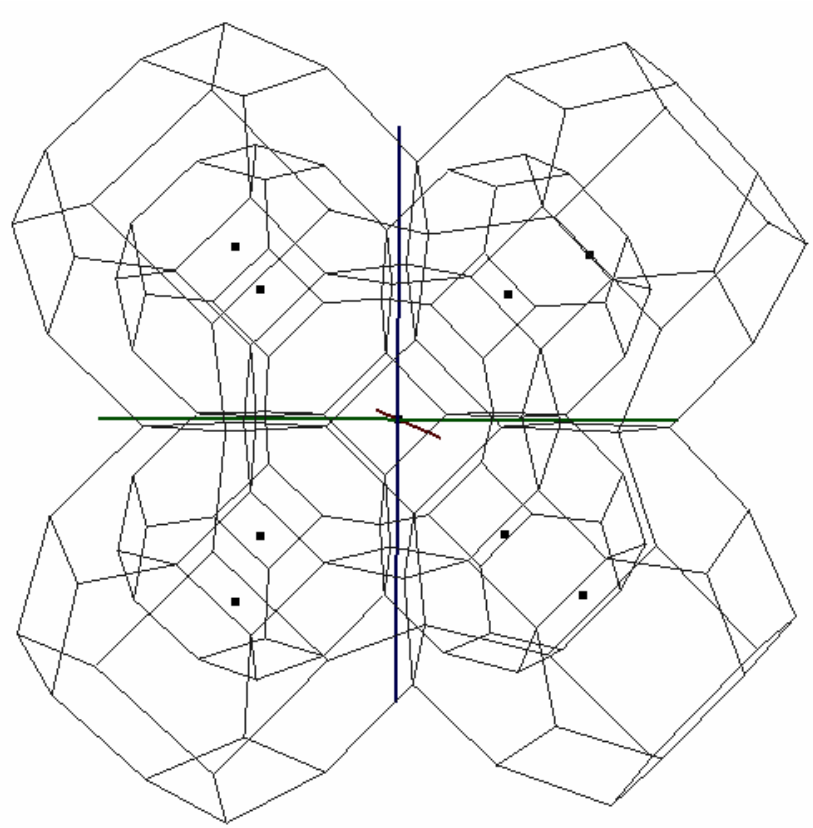
- The Air Force uses unmanned aerial vehicles with limited sensing range to form a 3D network for surveillance of an airspace.
- Similarly, the Navy can use a 3D network of underwater autonomous vehicles for surveillance of ocean

Deployment



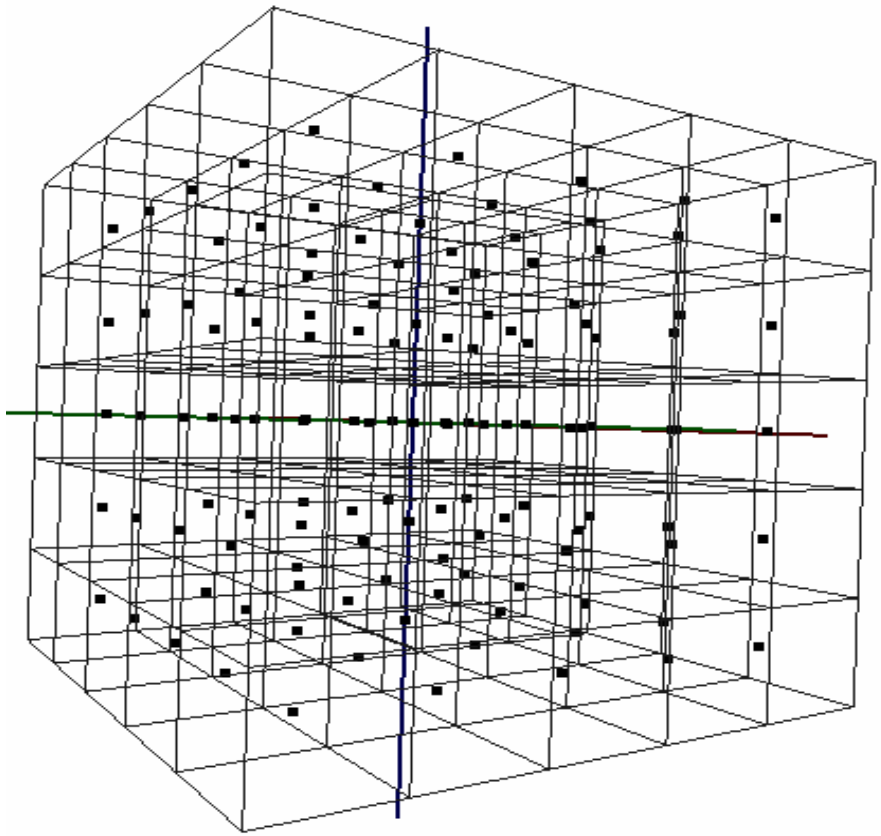
Truncated Octahedron placement strategy. 3D space is 20mx20mx20m and R=5m.

Deployment…



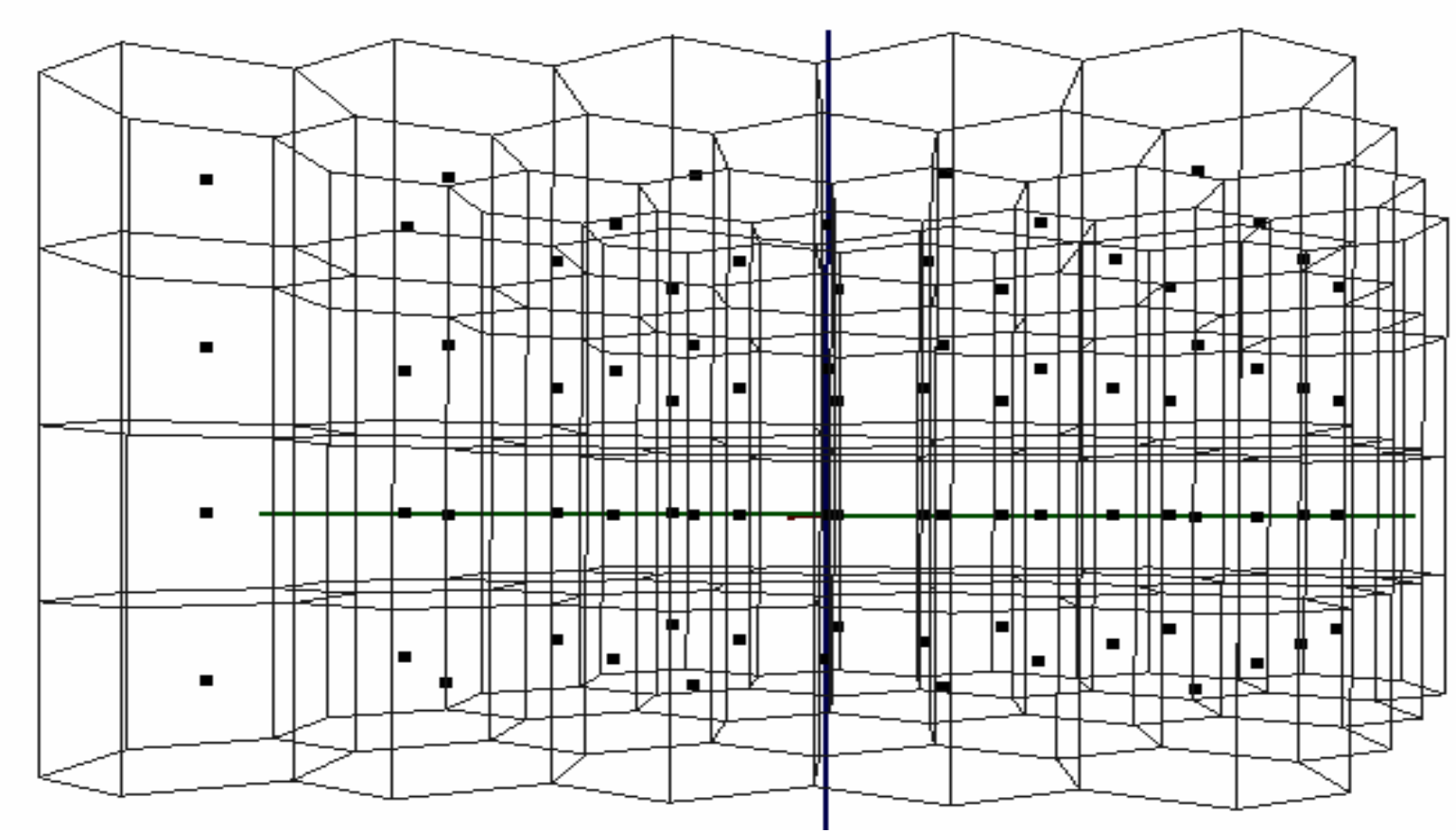
Truncated Octahedron placement strategy. 3D space is 15mx15mx15m and R=10m.

Deployment…



Node placement based on cube model

Deployment…



Hexagonal prism placement strategy

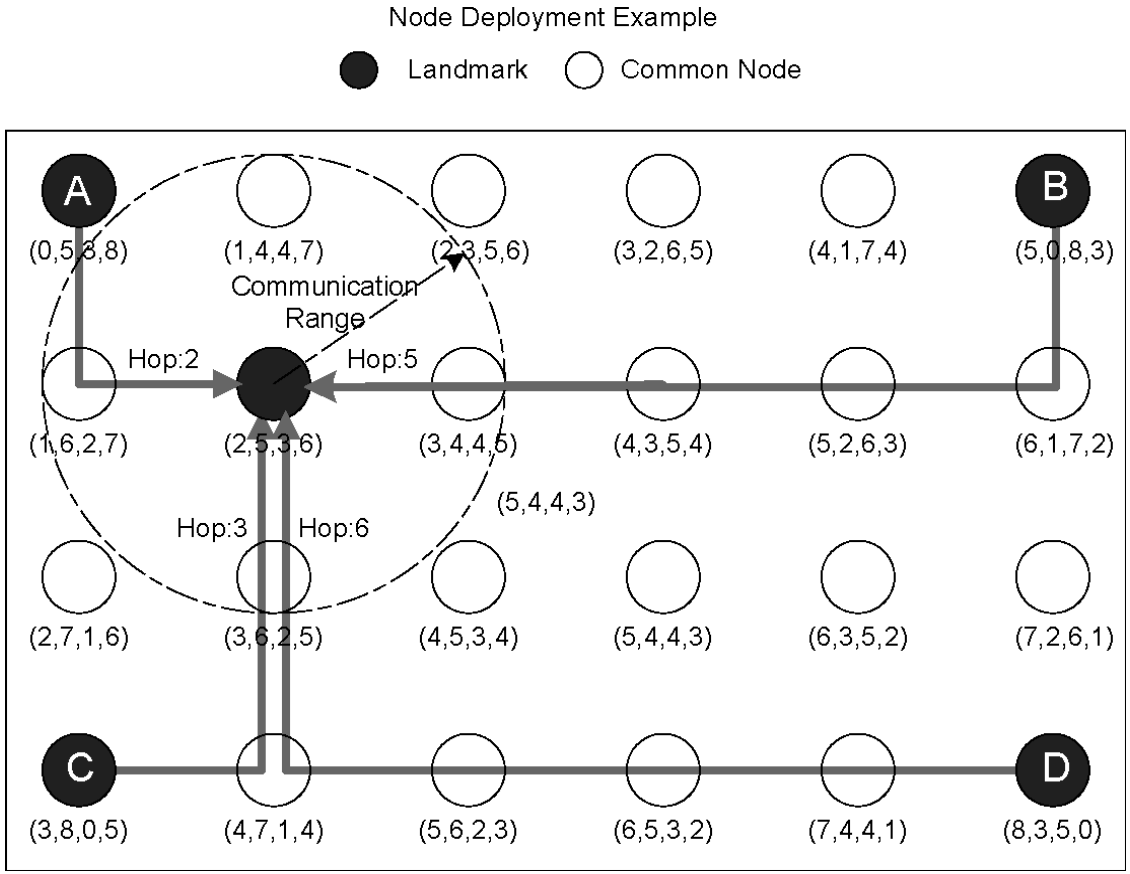
Routing

- **LCR:** Logical Coordinates based routing
- 3D Routing in Underwater Acoustic Sensor Networks
  - Delay-insensitive
  - Delay-sensitive

Logical Coordinates based routing

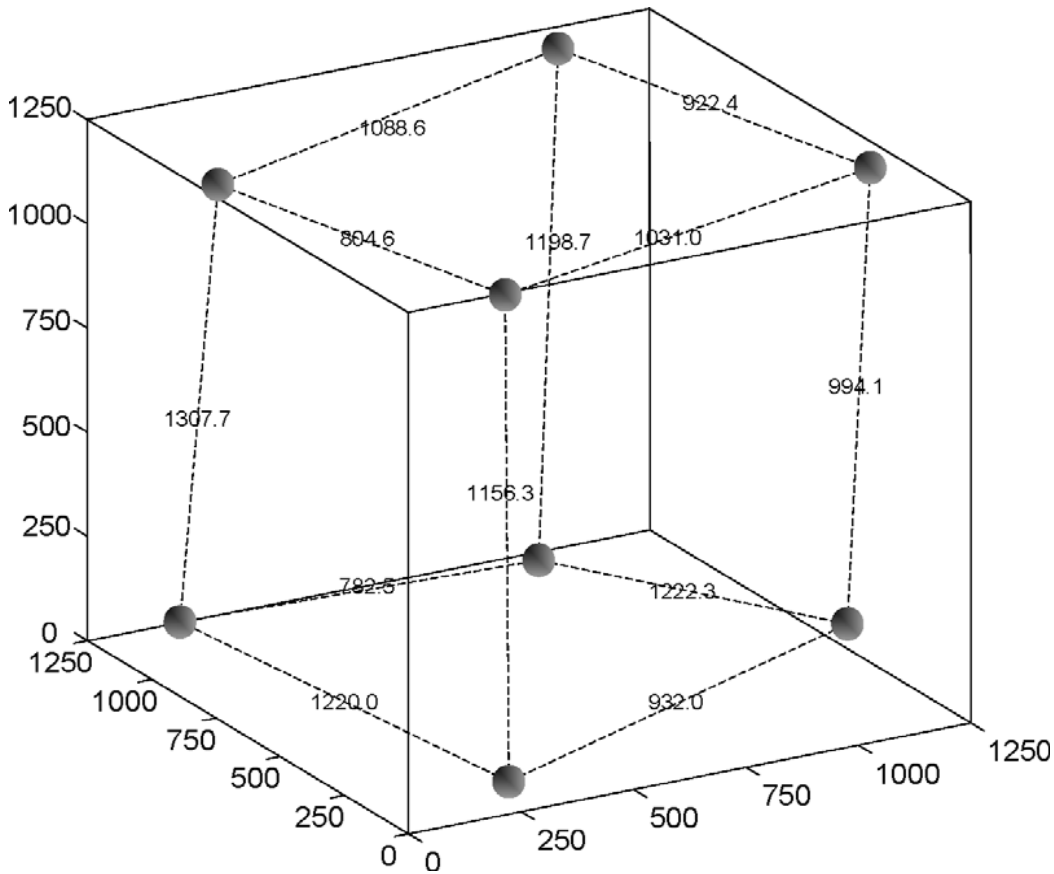
- LCR assigns each node a logical coordinate vector, and routes packets following these vectors.
-
- LCR demonstrates that LCR
  - guarantees packet delivery with a high probability
  - finds good paths
  - exhibits robust performance in the presence of network voids and node failures

An example for constructing logical coordinates



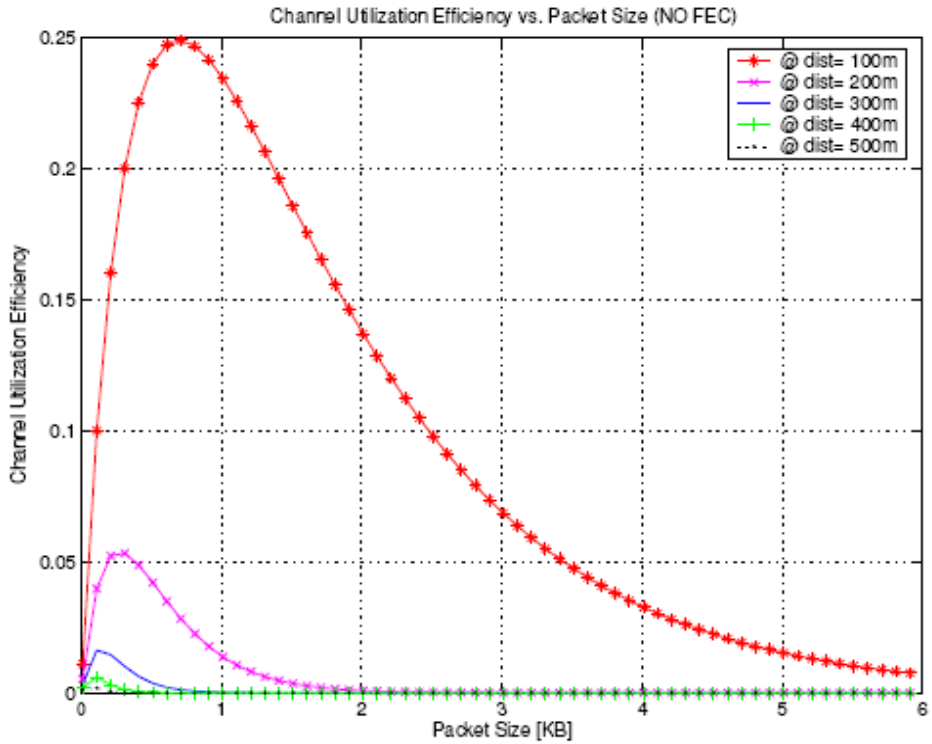
- For each node, the protocol only records its hop counts to a few reference nodes **(called *landmarks)***

Landmark election result in 3D space



- Since nodes are deployed three-dimensionally, in order to accurately characterize the topology, we choose 8 landmarks.

Under water channel efficiency



Underwater channel efficiency vs. packet size for different distances (100m-500m)

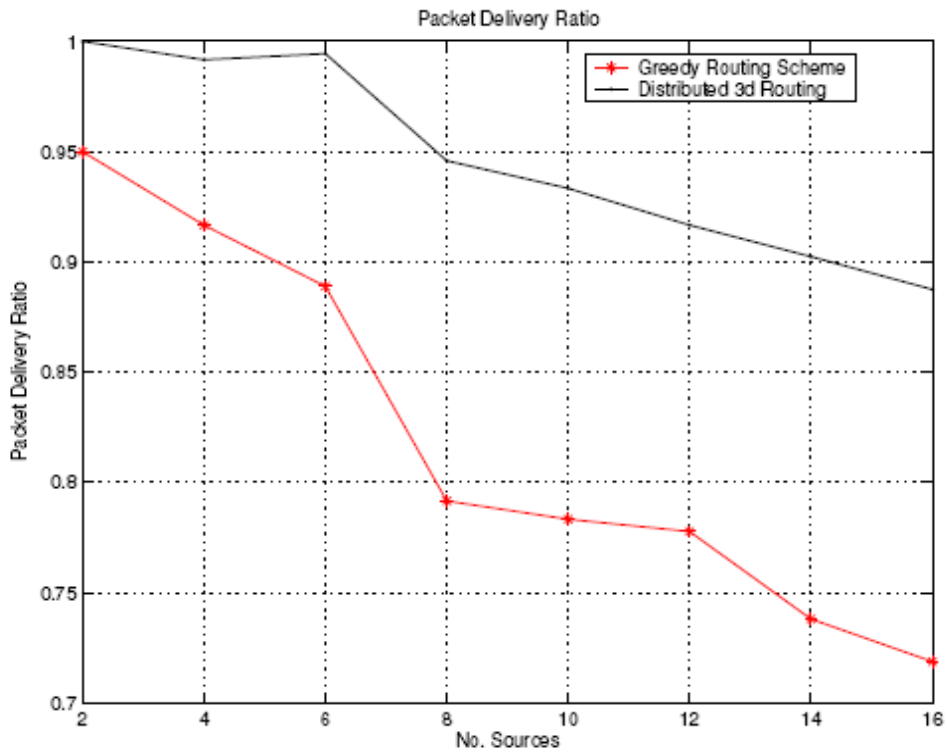
Under water routing

- **Delay-insensitive:**
  - The objective of our proposed solution is to efficiently exploit the channel and to minimize the energy consumption.
  - For this reason, we introduce the concept of **packet *train***. A packet train is a juxtaposition (side by side)of packets, which are transmitted back-to-back by a node without releasing the channel, in a single atomic transmission.
  - The corresponding node sends an ACK for each train. The ACK can either cumulatively acknowledge the whole train, i.e., all the consecutively transmitted packets, or it can selectively request the retransmission of specific packets, which are then included in the next train

Under water routing…

- **Delay-sensitive:**
  - The characteristics of the underwater environment, along with the requirements of delay-sensitive applications, suggest to devise solutions based on some form of centralized planning of the network topology and of the data paths, in order to optimally exploit the extremely scarce network resources.
  - For these reasons, ***virtual circuit*** routing techniques can be considered in UW-ASN for delay-sensitive applications, where multi-hop connections are established *a priori* between each source and sink, and each packet associated to a particular connection follows the same path.

Packet delivery ratio for a greedy routing scheme and the distributed 3D routing



Challenges

- What is the best way to place the nodes in three-dimension such that the number of nodes required for surveillance of a 3D space is minimized, while guaranteeing 100% coverage?
- What should be the minimum ratio of the transmission range and the sensing range of such a placement strategy?
- Routing (Secure routing)
- Key management

Security Conclusions

- No versatile security mechanism can solve all security issues in Sensor Network
- Each situation and application of sensor network with specific security requirements need distinct and specific solutions
- Security issues should be solved in each layer and there is a cooperation between those solutions
- Communication protocols: dealing with cryptographic algorithms used to achieve availability, confidentiality, integrity and authentication

Security Conclusions (Cont'd)

- Key management architectures: handling the complexities of creating and distributing keys used by communication
- Discovery of variety of attacks, threats and proper preventive methods
- Integrating research directions into complete security solutions for different kinds of sensor networks for different kind of application

References (**Key Management**)

[1] Chan, A. Perrig, and D. Song. **Random Key Predistribution Schemes for Sensor Networks**. IEEE Symposium on Security and Privacy (SP)

[2] Sencun Zhu, Sanjeev Setia, Sushil Jajodia. **LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks**. *In The Proceedings of the 10th ACM conference on Computer and communications security, 2003*.

[3] Pietro, R.D., L.V. Mancini, Y.W. Law, S. Etalle, and P. Havinga. **LKHW: A Directed Diffusion-Based Secure Multicast Scheme for Wireless Sensor Networks**. International Conference on Parallel Processing Workshops (ICPPW'03)

[4] Malan, D.J., Welsh, M., and Smith, M.D., "**A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography**", Proc. IEEE SECON 2004, 4-7 Oct. 2004, pp. 71 - 80.

[5] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. **SPINS: Security Protocols for Sensor Networks**. In The Seventh Annual International Conference on Mobile Computing and Networking (MobiCom 2001), 2001.

[6] Chris Karlof, Naveen Sastry, David Wagner. **TinySec: A Link Layer Security Architecture for Wireless Sensor Networks**. ACM SenSys 2004, November 3-5, 2004.

[7] L. Eschenauer, V. D. Gligor, "A **Key-Management Scheme for Distributed Sensor Networks**," 9th ACM Conference on Computer and Communication Security, pp.41-47 .

[8] Gaurav Jolly, Mustafa C. Ku çu, Pallavi Kokate, and Mohamed Younis, "**A Low-Energy Key Management Protocol for Wireless Sensor Networks".** Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03)

References (**Attacks and Counter Measures**)

[1] Chris Karlof David Wagner. **In Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures**.

[2] J. R. Douceur, "**The Sybil Attack**," *in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002*.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson, "**Wormhole detection in wireless ad hoc networks**," *Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002*.

[4] JYih-Chun Hu, Adrian Perrig, David B. Johnson, "**Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks**," Technical Report TR01-384, December 17, 2001

[5] Y. Hu, A. Perrig, and D. Johnson, "**Rushing attacks and defense in wireless ad hoc network routing protocols**", Second ACM Workshop on Wireless Security (WiSe'03), San Diego, CA, USA, 2003.

References (**Secure Routing**)

[1] J. Deng, R. Han, and S. Mishra. **INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks**. Poster paper. In the 23rd IEEE International Conference on Distributed Computing Systems (ICDCS 2003), Providence, RI (May 2003).

[2] J. Deng, R. Han, and S. Mishra. **A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks.** In the 2nd IEEE International Workshop on Information Processing in Sensor Networks (IPSN 2003), Palo Alto, CA (April 2003).

[3] Anthony D. Wood, Lei Fang, Tian He, "**SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks"** *SASN'06,* October 30, 2006, Alexandria, Virginia, USA.

[4] P. Papadimitratos and Z. Haas. **Secure routing for mobile ad hoc networks**. In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, Jan. 2002.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: **a secure on-demand routing protocol for ad hoc networks**. In *Proceedings of the Eighth Annual International Conference on Mobile computing and Networking*, pages 12–23, Sept. 2002.

[6] Y.-C. Hu, D. B. Johnson, and A. Perrig. **Secure efficient distance vector routing in mobile wireless ad hoc networks**. In *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pages 3–13, June 2002.

[7] *K. Akkaya, M. Younis, **A survey on routing protocols for wireless sensor networks**, To appear in Journal of Ad Hoc Networks.*

[8] J. Deng, R. Han, S. Mishra, **Inrusion tolerance and anti-traffic analysis strategies in wireless sensor networks**, In IEEE International Conference on Dependable

References (**Wireless Mesh Networks**)

1. N.B.Salem, H.P. Hubaux, "*Securing wireless mesh networks*," IEEE Wireless Communications, April, 2006. pp. 50-55.
2. Y. Zhang, Y. Fang, "*ARSA: An attack resilient security architecture for multihop wireless mesh network*," IEEE Journal on Selected Areas in Communications, vol.24. no.10, October, 2006. pp. 1916-1928.
3. X.Wu , N. Li, "*Achieving privacy in Mesh Networks*", in proceedings of SASN'06, pp-13-22, Oct. 30, 2006.
4. W. Taojun, X. Yuan and Y.Cui, "*Preserving traffic privacy in Wireless Mesh Networks*," in prod of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06).
5. P. Tague, R.Poovendran "*Modeling Node Capture Attacks in Multi-hop Wireless Networks*," Ad Hoc Networks, vol. 5 issue 6, August 2007, pp. 801- 814.
6. Santhanam, L., Nandiraju, D., Nandiraju N., Agrawal D.P., "*Active Cache Based Defense against DoS Attacks in Wireless Mesh Network*," 2nd International Symposium on Wireless Pervasive Computing, ISWPC '07, 5-7 Feb. 2007, pp. 419-424.
7. I. F. Akyildiz, X. Wang, and W. Wang, "*Wireless Mesh Networks: A Survey*," Computer Networks (Elsevier), 47(4), 2005, pp. 445-487.

References (3D Wireless Networks)

1. S. M. Nazrul Alam and Zygmunt Haas, "*Coverage and Connectivity in Three-Dimensional Networks*," in Proc of ACM MobiCom, 2006.
2. Akyildiz, I.F., Pompili, D., Melodia, T., "*Underwater Acoustic Sensor Networks: Research Challenges*," Ad Hoc Networks Journal, (Elsevier), March 2005.
3. V. Ravelomanana, "*Extremal properties of three-dimensional sensor networks with applications*," IEEE Transactions on Mobile Computing 3 (3), 2004, pp. 246–257.
4. M. Bahramgiri, M. Hajiaghayi., and V. S. Mirrokni, "*Fault-Tolerant 3-Dimensional Distributed Topology Control Algorithms in Wireless Multi-hop Networks*," in Wireless Networks, vol. 12, no.2, pp. 179-188, April, 2006, Springer Netherlands.
5. P. Gupta and P.R. Kumar, "*Internet in the Sky: The Capacity of Three Dimensional Wireless Networks*," Comm. in Information and Systems, vol. 1, pp. 33-49, 2001.
6. J. Carle, J.F. Myoupo, and D. Semé, "*A Basis for 3-D Cellular Networks*," in Proc. of the 15th International Conference on Information Networking, 2001.
7. Catherine Decayeux and David Semé, "*A New Model for 3-D Cellular Mobile Networks*," in Proc. Of ISPDC/HeteroPar 2004.

Thanks !