Wireless Sensor Network Security

Dr. Ashok Kumar Das

IEEE Senior Member
Associate Professor
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*
Homepage: http://www.iiit.ac.in/people/faculty/ashokkdas
Personal Homepage: https://sites.google.com/view/iitkgpakdas/

Overview of Wireless Sensor Networks

Overview of Wireless Sensor Networks

- In a sensor network, many tiny computing nodes called sensors are scattered in an area for the purpose of sensing some data and transmitting data to nearby *base stations* for further processing.
- A sensor node, also known as a *mote*, is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. The transmission between the sensors is done by short range radio communication.
- The base station is assumed to be computationally well-equipped whereas the sensor nodes are resource-starved.
- The sensor nodes are usually scattered either randomly or manually in a *sensor field* (i.e., deployment area or target field).
- Data are routed back to the base station by a multi-hop infrastructure-less architecture through sensor nodes.

Overview of Wireless Sensor Networks

Ad hoc Networks

- An ad hoc network is a group of mobile, wireless hosts which co-operatively and spontaneously form a network independently of any fixed infrastructure or centralized administration.
- In particular, an ad hoc network has no base stations: a host, also called node, communicates directly with nodes within its wireless range and indirectly with all other destinations using a multi-hop route through other nodes in the network.

Overview of Wireless Sensor Networks

Differences between sensor networks and ad hoc networks

- The number of nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network may change frequently.
- Sensor nodes are limited in power, computation capacities as well as memory.
- Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.

Overview of Wireless Sensor Networks

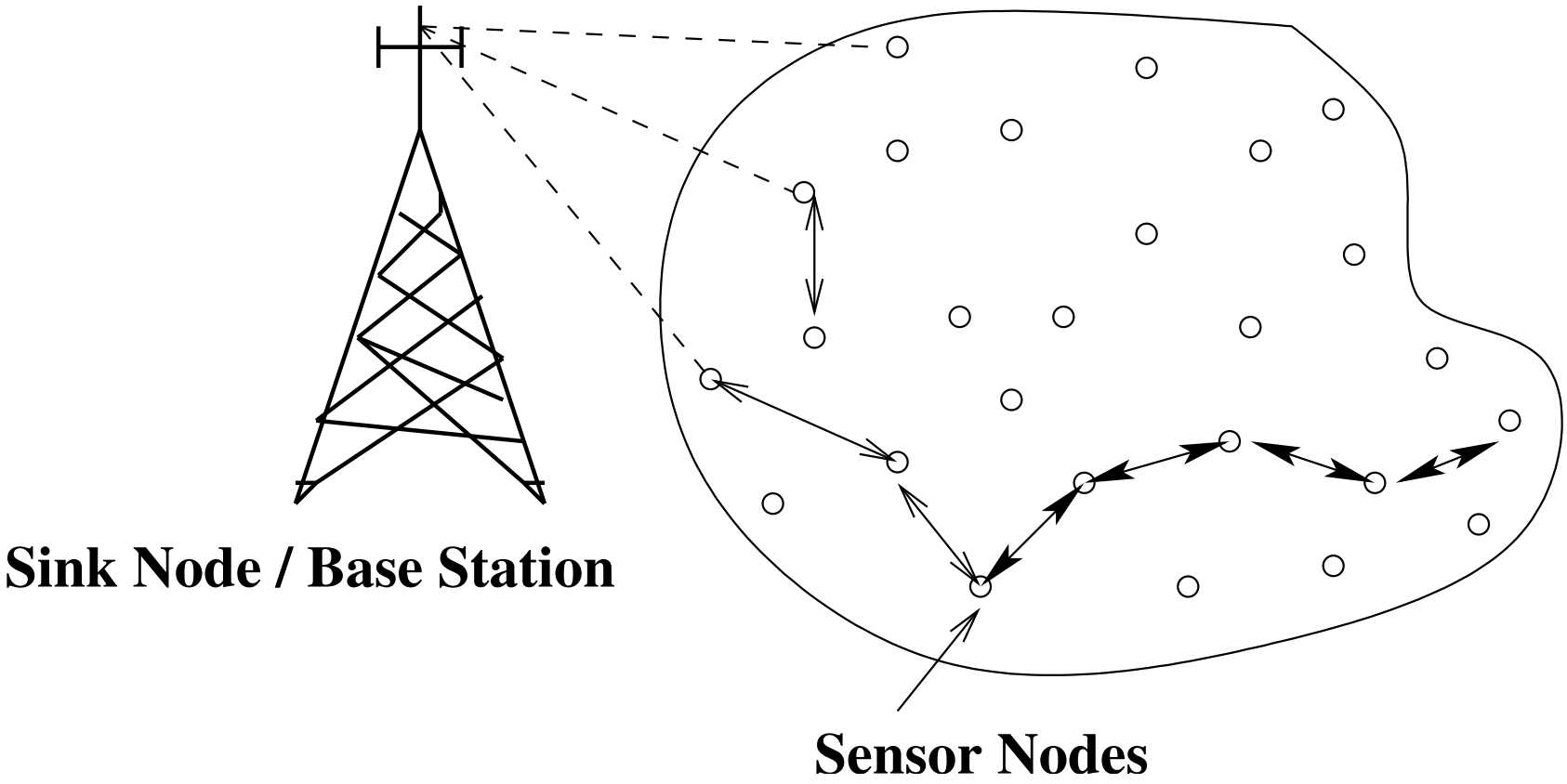


Figure: A distributed wireless sensor network (DWSN)/homogeneous architecture.

Overview of Wireless Sensor Networks

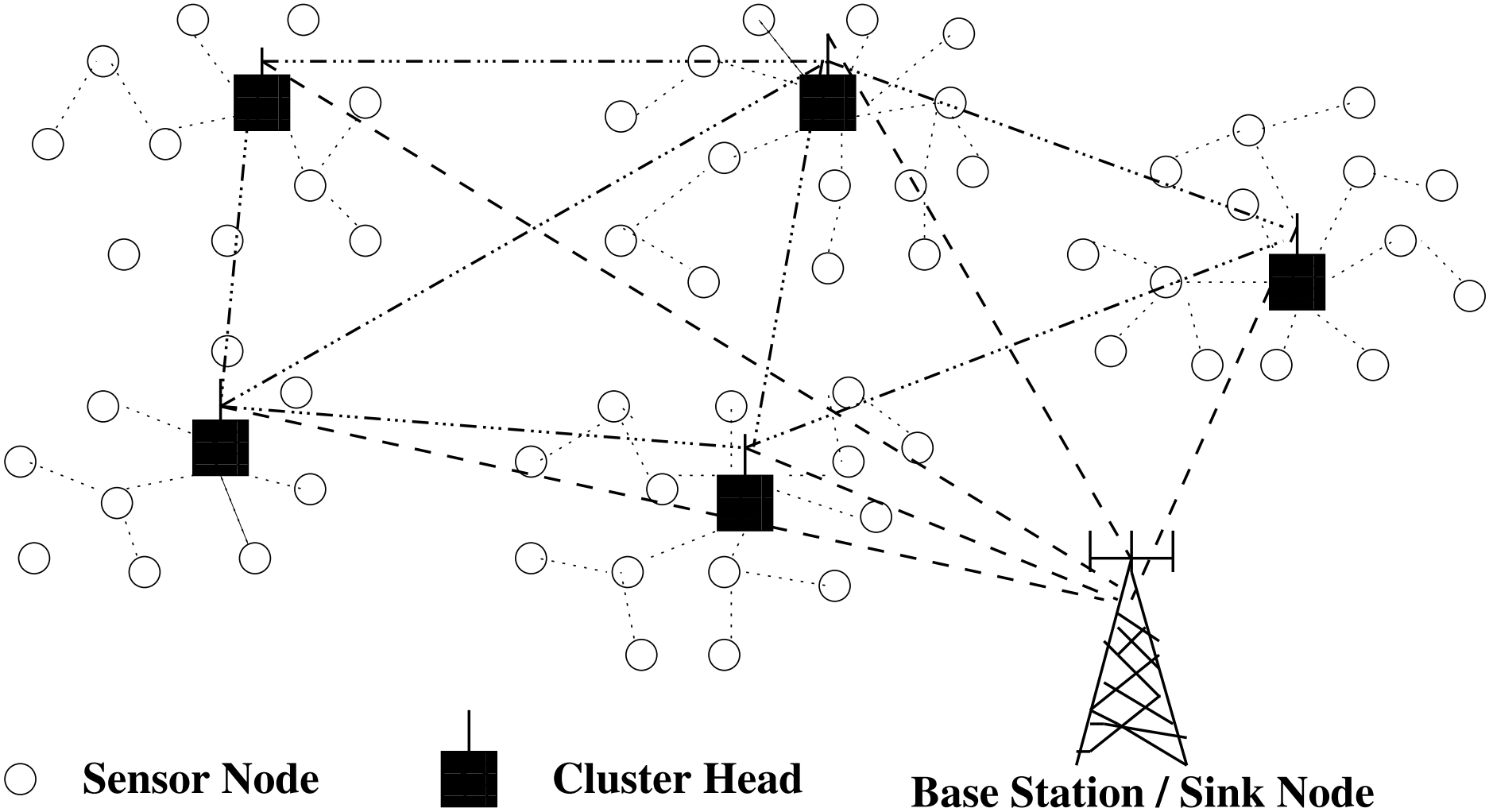


Figure: A hierarchical wireless sensor network (HWSN)/heterogenous architecture.

Overview of Wireless Sensor Networks

Hardware constraints

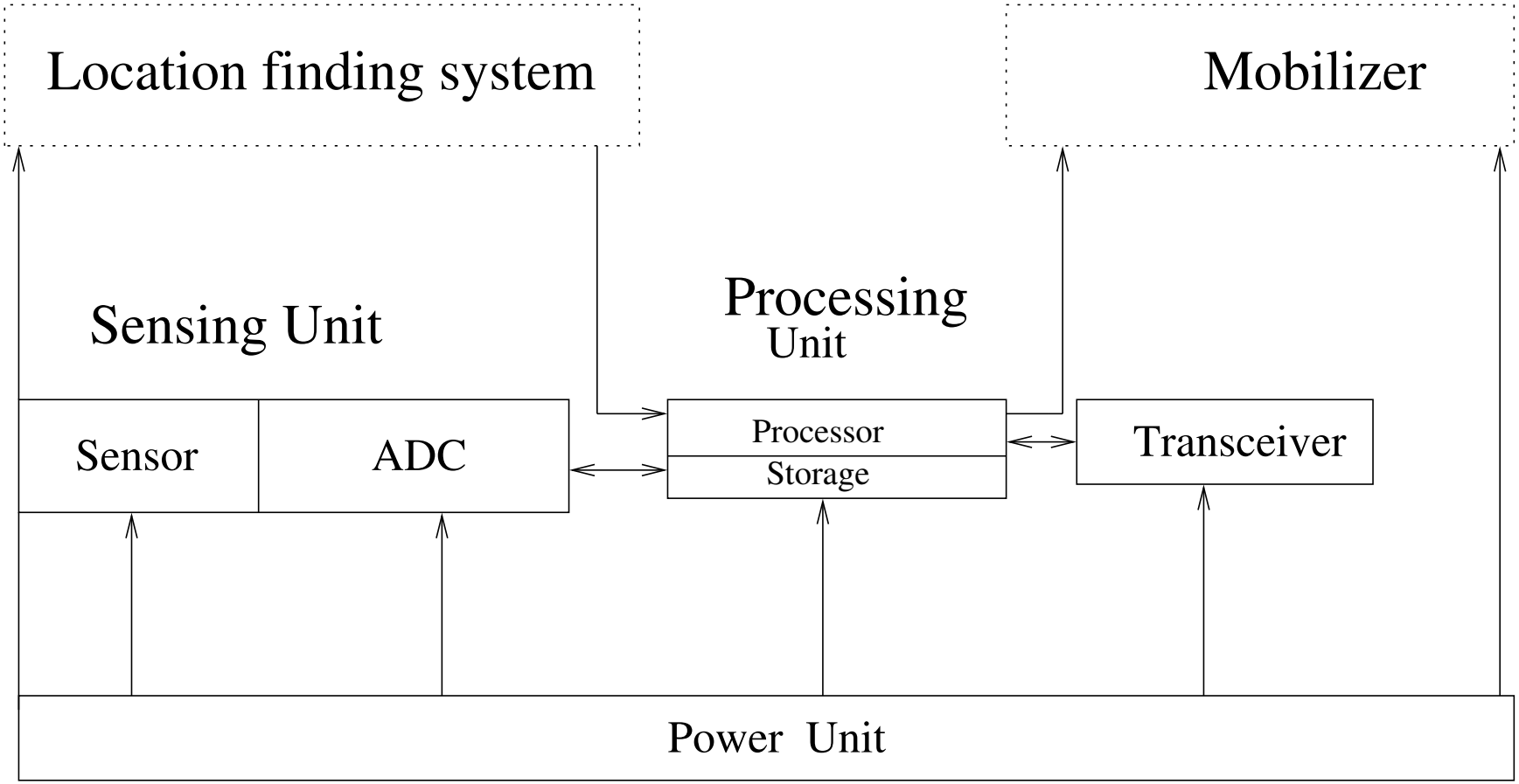


Figure: The components of a sensor node.

Overview of Wireless Sensor Networks

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Table: Basic characteristics of typical MICA2 and MICA2-DOT motes

	MICA2	MICA2-DOT
Processor	8-bit 7.7 MHz Atmega 128	8-bit 4 MHz Atmega 128
RAM	4K bytes	4K bytes
ROM	128K bytes	128K bytes
EEPROM	512K bytes	512K bytes
Data rate	38.4K baud	38.4K baud
Default packet size (under TinyOS)	29 bytes	29 bytes
Power supply	2 AA batteries	1 coin cell battery

Overview of Wireless Sensor Networks

Sensor network topology

- ***Pre-deployment and deployment phase:*** Sensor nodes can be deployed in mass or placed one by one in the sensor field (target field).
- ***Post-deployment phase:*** The topology of a sensor network can change after deployment due to sensor nodes' available energy, mobility of nodes, etc.
- ***Redeployment of additional nodes phase:*** Additional sensor nodes can be redeployed at any time to replace the faulty or compromised sensor nodes.

Overview of Wireless Sensor Networks

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Applications of sensor networks

- Military applications
- Environmental monitoring
- Classroom/home
- Health monitoring
- Habitat monitoring
- Detecting and monitoring car thefts
- Vehicle tracking and detection
- Practical application of WSNs (Vehicular Ad Hoc Networks, VANETs)

Overview of Wireless Sensor Networks

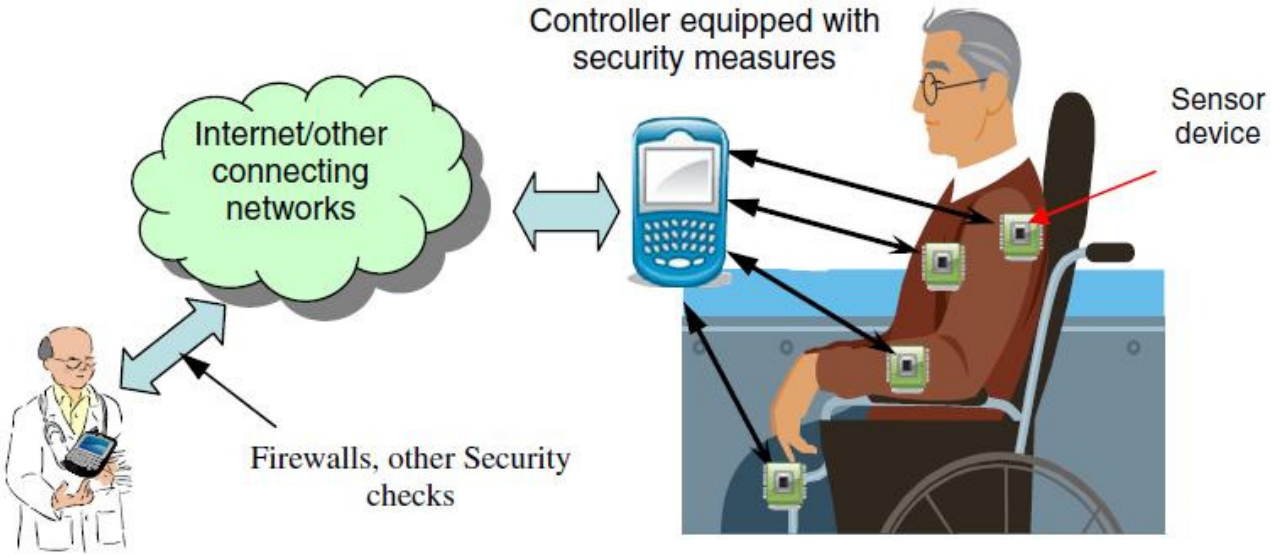
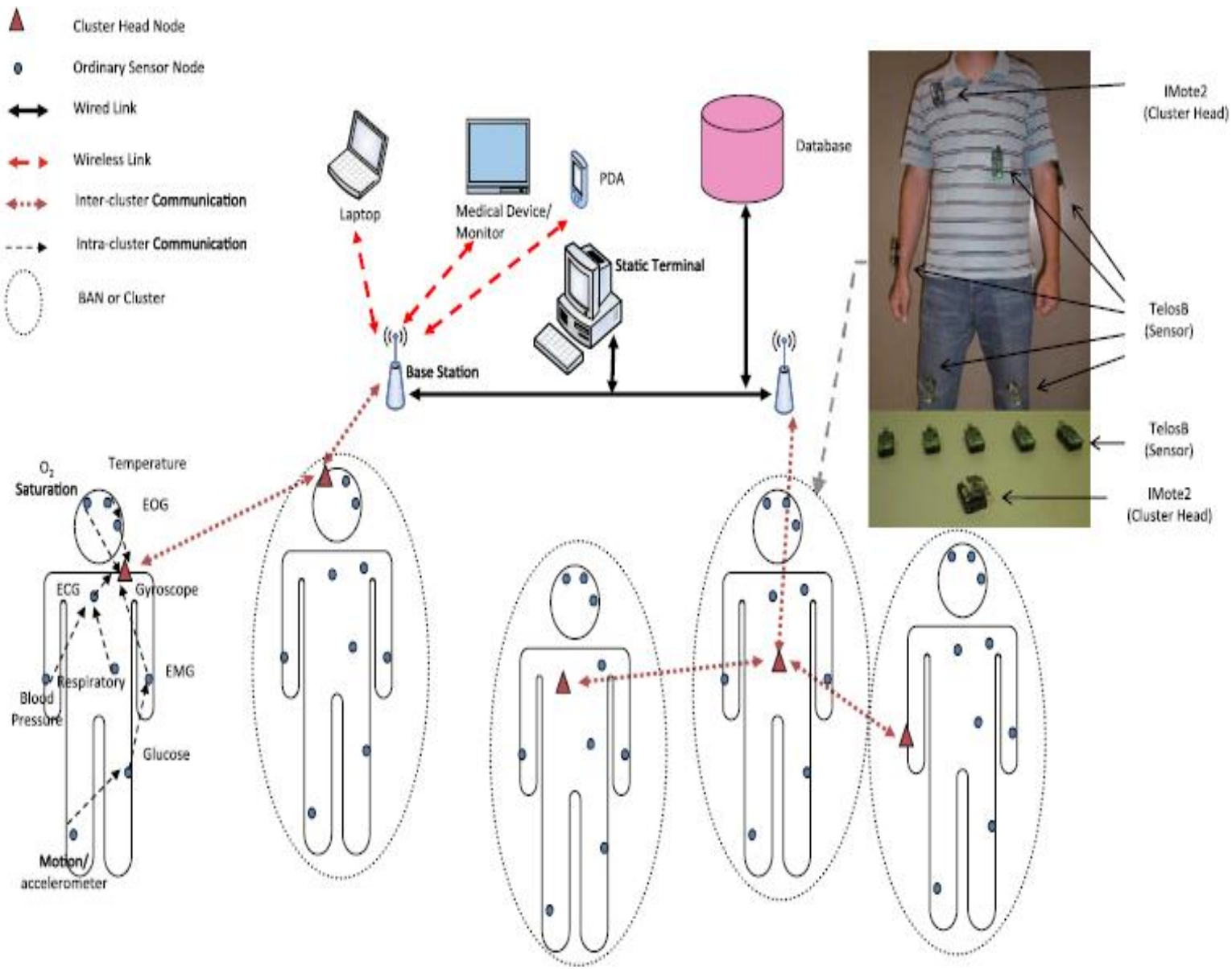


Figure: Application in wireless body area networks.

A hierarchical WBAN with the clustering heads



Battlefield surveillance

- A large number of sensor nodes are rapidly deployed in a battlefield via airplanes or trucks.
- Each individual sensor node monitors conditions and activities in its surrounding after deployment in the battlefield and then reports these sensing observations to the nearby base stations via wireless communications with its neighbor sensor nodes.
- The base station then conducts a more accurate detection on the activities (for example, possible attacks) of the opposing force after collecting a large number of sensing observations from the sensor nodes.
- Thus, the appropriate decisions as well as responses can be made quickly in the battlefield.

Overview of Wireless Sensor Networks

References on Wireless Sensor Networks Surveys

- I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A Survey. Computer Networks, Vol. 38, No. 4, pp. 393-422, 2002.
- H. Alemdar and C. Ersoy. Wireless sensor networks for healthcare: A survey. Computer Networks, Vol. 54, No. 15, pp. 2688-2710, 2010.

Overview of Wireless Sensor Networks

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

General security requirements

- ***Authentication:*** authenticating other sensor nodes, cluster heads, and base stations before granting a limited resource, or revealing information.
- ***Integrity:*** ensuring that message or the entity under consideration is not altered.
- ***Confidentiality:*** providing privacy of the wireless communication channels to prevent eavesdropping.
- ***Availability:*** ensures that the desired network services are available even in the presence of denial of service attacks.
- ***Non-repudiation:*** preventing malicious nodes to hide their activities.
- ***Authorization:*** ensures that only the sensor nodes those who are authorized can be involved in providing information to network services.
- ***Freshness:*** ensures that the data is recent and no adversary can replay old messages.

General security requirements (Continued...)

We also need to consider the forward and backward secrecy as new sensors are deployed in the network and old sensors fail due to energy problems.

- ***Forward secrecy:*** When a sensor node leaves the network, it must not read any future messages after its departure.
- ***Backward secrecy:*** When a new deployed node joins in the network, it must not read any previously transmitted message.

Sensor network limitations

- *Limited resources in sensor nodes:* Each sensor node has a primitive processor featuring very low computing power and only small amount of programmable memory.
- *Limited life-time of sensor nodes:* Each sensor node is battery-powered. So, after several weeks or months of operation, some nodes in the network may exhaust their power and as a result, the security protocols used must be energy efficient.
- *Limited communication abilities of sensor nodes:* Sensor nodes have the ability to communicate with each other and the base stations using short range wireless radio transmission at low bandwidth.

Sensor network limitations

- *Lack of knowledge about deployment configuration:* In most applications, the post-deployment network configuration is not possible to decide a prior. As a result, it may not be always possible to use security algorithms that have strong dependence on locations of sensor nodes in a sensor network.
- *Issue of node capture:* Wireless sensor networks often operate in an unattended environment. An adversary may physically capture some sensors to compromise their stored sensitive secret data and codes from their memory as they are not generally equipped with tamper-resistant hardware.

Securing Wireless Sensor Networks

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

- Key management
- User authentication
- Access control
- User access control
- Intrusion detection

Key management

- In this method, the practical approach is to preload a set of keying information before the deployment of sensor nodes in the target field.
- After deployment, they discover their neighbor nodes and then establish the secret keys between them using the preloaded keying information.
- Neighbor sensor nodes then use the established secret keys for their future secure communications.

User authentication

- In a user authentication in WSN, a legitimate user is allowed to query and collect the real-time data at any time from a sensor node or cluster head of the network as and when he/she demands for it.
- As most of the applications in wireless sensor network (WSN) are real-time based, so users are generally interested in accessing real-time information.
- This is possible if the users (called the external parties) are allowed to access the real-time data directly from the nodes inside WSN and not from the base station *BS*.
- Usually, the information from nodes are gathered periodically in the *BS* and so, the gathered information may not be real-time.
- In order to get the real-time information from the nodes, the user needs to be first authorized to the nodes as well as the *BS* so that illegal access to nodes do not happen.

Access control

- An access control scheme consists of two tasks: *node authentication* and *key establishment*.
- In *node authentication*, a deployed node needs to prove its identity to its neighbor nodes and also to prove that it has the right to access the existing sensor network.
- On the other hand, in *key establishment*, the secret shared keys need to be established between a deployed node and its neighbor nodes to protect secure communications among them.

User access control

- User access control mechanism provides the access rights for the correct information and resources for different services in wireless sensor network.
- Using user access control, an authorized user can access only those information for which he/she is permitted to access.
- In WSNs, specially in case of WBAN, for accessing of medical data, there exist different groups of users.
- In medical applications, different types of information belonging to various security levels can be generated by all kinds of sensors.
- With the proper access privilege, selected types of the authorized users should access proper data. This means that accessibility of a particular type of data to users is based solely on necessity.

Intrusion detection

- **External versus internal attacks:**
  - In the normal flow of the network, the nodes are honest and cooperative entities, whereas attacker nodes are precluded from the network and have no access to the network.
  - The external attacks can be launched only from the outside of the scope of the network. So, the impact of these attacks is limited especially in case of WSN.
  - The attacker can physically capture a sensor node and extract useful information such as its identity, secret key, etc. from that node, and can deploy some fake sensor nodes by using that extracted information. In this way an internal attack can be performed.
  - Internal attacks such as blackhole, misdirection, wormhole, sinkhole, etc. are very harmful in nature as they cause severe damage to the performance of the network.

Attacks on the different layers of WSN stack

Table: Layer-wise attacks on WSN stack

Layer	Attacks
Physical Layer	Tampering, Sybil attack, Jamming, Interception
Data Link Layer	Sybil attack, Collision, Exhaustion, Replay attack, Spoofing and altering routing attack, Traffic analysis and monitoring
Network Layer	Selective forwarding attack, Blackhole attack, Sybil attack, Hello flood attack, Spoofing attack, Internet smurf attack, Wormhole attack, Misdirection attack
Transport Layer	Desynchronization, Flooding attack
Application Layer	False data injection, Spoofing and altering routing attack

Summary of some network layer attacks
Blackhole attack

- A blackhole attack occurs when an intruder captures and re-programs a set of nodes in the network to block the packets that they receive instead of forwarding them towards the base station.
- As a result, any information that enters in the blackhole region is compromised by an attacker.
- This attack is easy to constitute and it is capable of undermining network effectiveness by partitioning the network such that the important event information do not reach the base station.
- The network performance parameters such as throughput and end-to-end delay are affected in the presence of the blackhole nodes.

Blackhole attack scenario

- A blackhole attack scenario is shown in Figure. In this case, there are three sources S_1, S_2 and S_3, which send data to the destination D. However, in the presence of blackhole attacker node X, the packets do not reach to the destination D because they are captured by X.

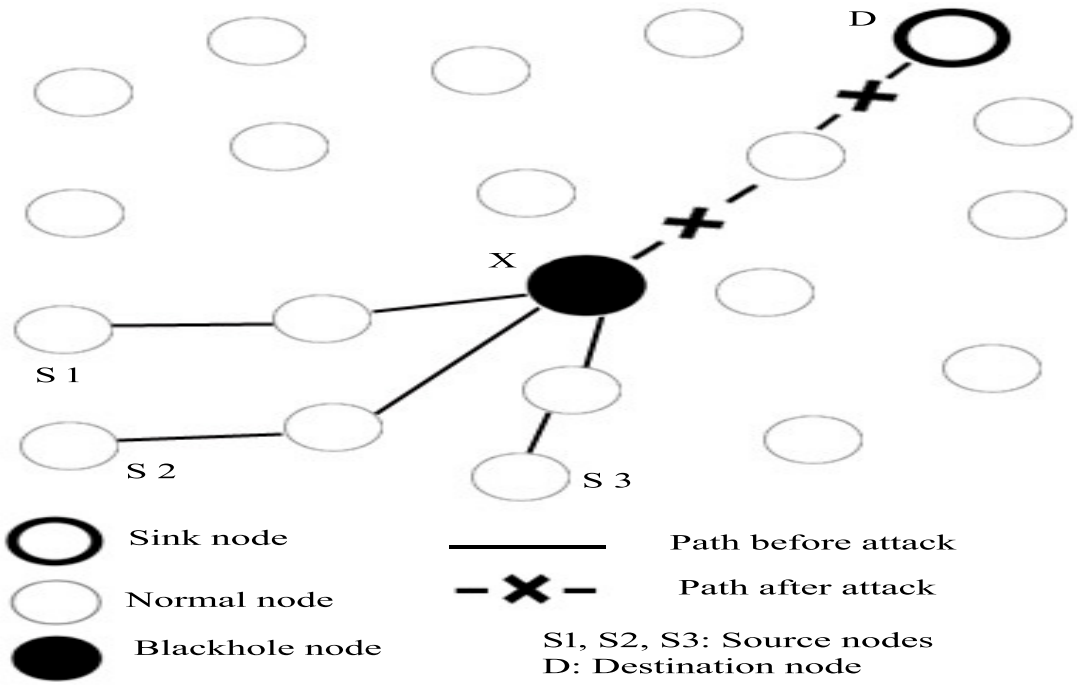


Figure: An example of a blackhole attack in WSN

Misdirection attack

- In a misdirection attack, an attacker routes the packets from its neighbors to other distant nodes, but not necessarily to its legitimate destination nodes.
- This produces a long delay in packet delivery and decreases throughput of the network. Under this attack, packets reach to the destination, but from a different route which further produces long delay and thus, also decreases throughput of the network.

Misdirection attack scenario

- There are two scenarios: one for the normal flow and other for the misdirection attack.
- Nodes S and R communicate via intermediate nodes A and D. Let node A be a misdirection attacker node. A then forwards the messages to a node, which is far away from the destination.
- Thus, the messages reach to the node R, but from a different path $\langle S, A, B, C, D \rangle$ that further increases the delay.

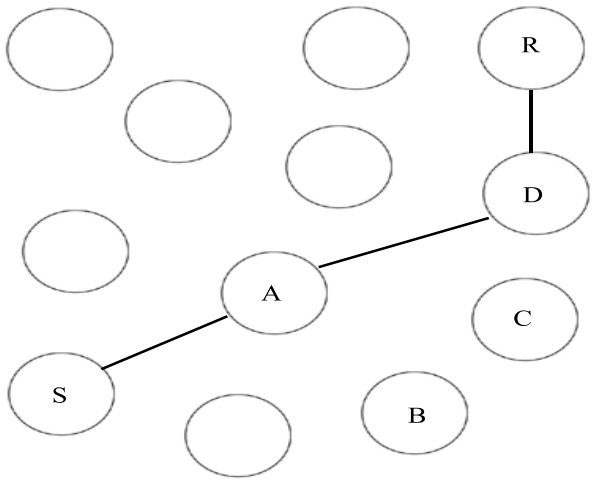


Figure: Normal flow

Misdirection attack scenario cont..

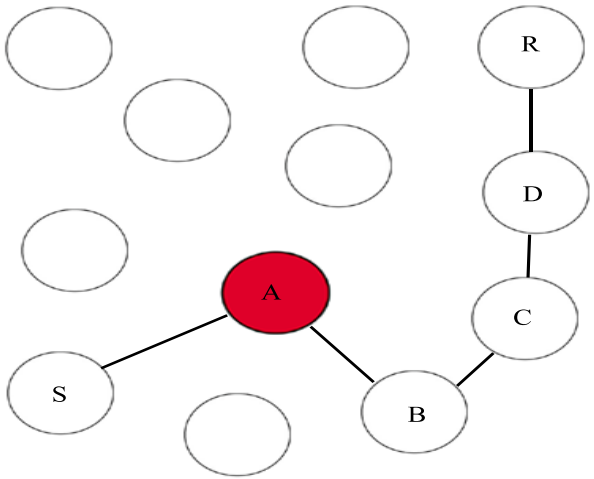


Figure: Under misdirection attack

Wormhole attack

- In a wormhole attack, an attacker can tunnel the packets between two distant locations in the network through an in-band channel or out-of-band channel. In this case, a wormhole tunnel is formed by a pair of attackers.
- The wormhole tunnel gives two distant nodes a misapprehension that they are close to each other.
- The existing wormhole can attract and bypass a large amount of network traffic, and thus the wormhole node can easily get the network traffic and perform the manipulation.
- The attacker is able to launch a variety of attacks including the sniffing, modification and dropping.

Wormhole attack scenario

- Figure depicts a scenario for the wormhole attack. Source node *A* sends the packets to a sink node *E* via intermediate nodes *B*, *C*, and *D*.
- At the same time, a wormhole node, say *WH*1 advertises a path with less hop distance so that node *A* attracts towards that path and it starts sending the packets via *WH*1 and *WH*2, where *WH*2 is the colluded node of the wormhole node *WH*1.

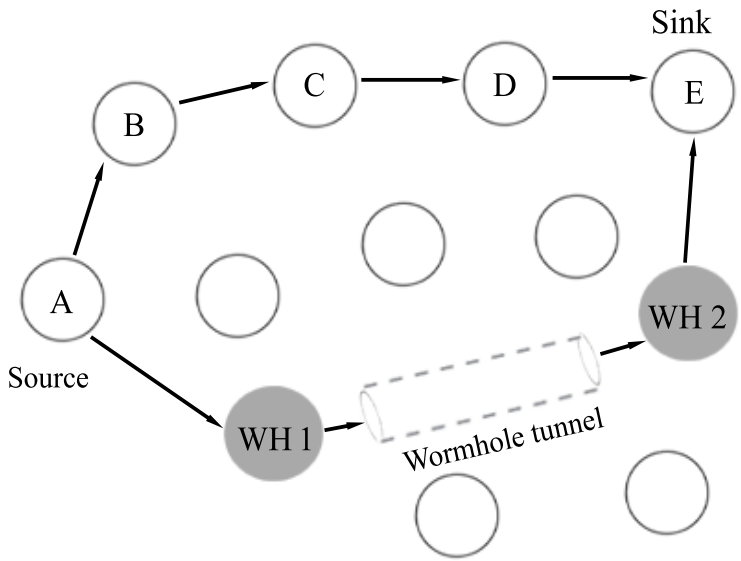


Figure: An example of wormhole attack

Sinkhole attack

- In a sinkhole attack, a malicious (sinkhole) node advertises a best possible route to the base station which misguides its neighbors in order to use that route more frequently.
- The malicious node thus gets an opportunity to tamper with the data, damage the regular network operations.
- In a sinkhole attack, the attacker node utilizes a compromised node to launch the attack in which a route with the less hope distance is advertised to misguide its neighbors.
- This assures the neighbors to forward all the traffic through such an advertised route.
- The route not only captivates the neighbors of the sinkhole, but also it captivates other nodes that are closer to the sinkhole than to the base station.

Sinkhole attack scenario

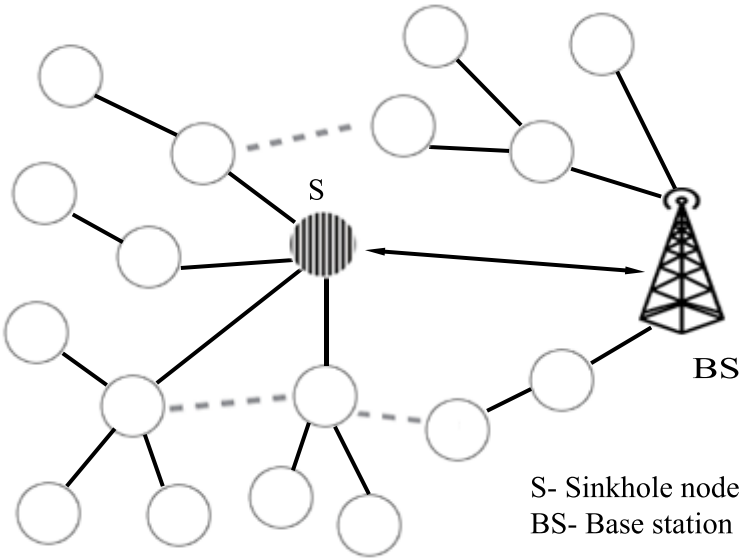


Figure: An example of sinkhole attack

Sinkhole attack scenario cont..

- The sinkhole attack can also be conducted using the wormhole attack, where a malicious node first captures the packets from its neighbors and utilizes a secret tunnel (wormhole tunnel) to send the packets to another colluded node.
- The colluded node eventually delivers the packets to the base station.
- The two ends of the wormhole tunnel can be at a longer distance as compared with other routes, but still it can prevent the source from discovering other routes greater than two hops away from the base station.

Sinkhole attack scenario cont..

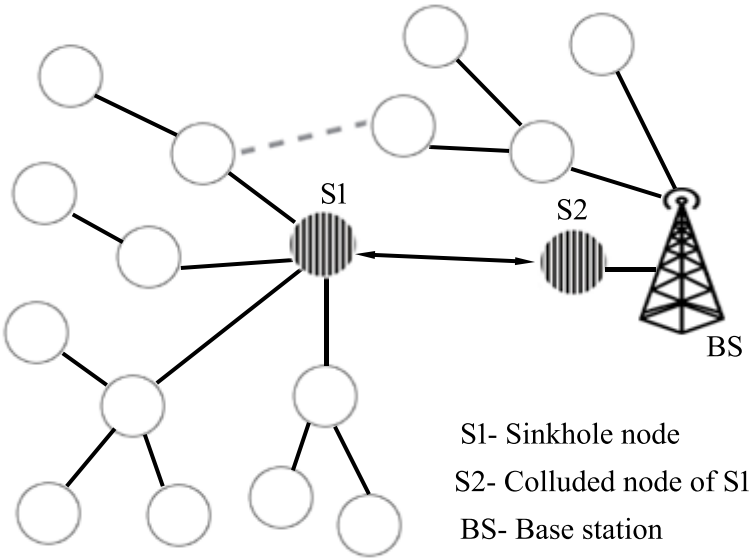
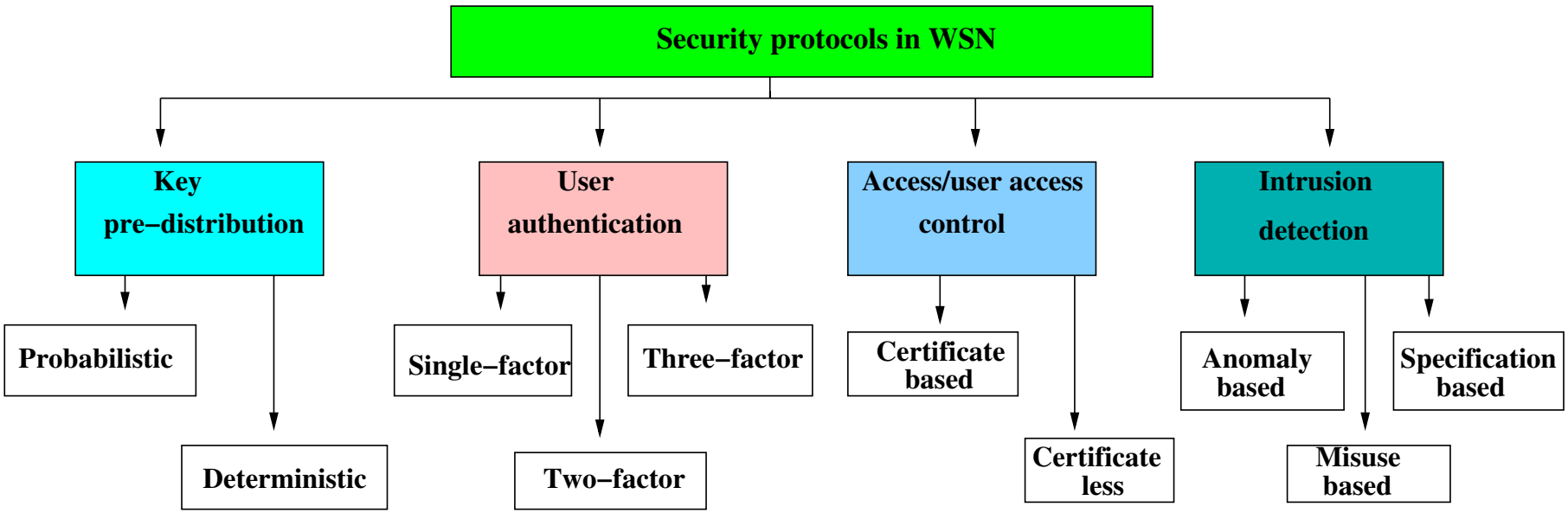


Figure: An example of sinkhole attack using wormhole tunnel

Hybrid anomaly

- In WSN, multiple attacks can be launched at a time.
- Hybrid anomaly is a type of anomaly that contains different types of attacker nodes, such as blackhole nodes, misdirection nodes, etc.
- Hybrid anomaly has the ability to degrade the network performance rapidly, and it can also trouble the attack specific detection mechanism.

Security protocols in WSNs: a taxonomy



Thank you