Faculty of Electrical Engineering - Skopje

Securing communication in WSN trough use of cryptography

Ace Dimitrievski
Biljana Stojkoska
Kire Trivodaliev
Danco Davcev

NATO-ARW, Suceava, September 4-8, 2006

{ace, biljana.stojkoska, kire.trivodaliev, etfdav}@etf.ukim.edu.mk

1. Introduction

- **What is Wireless Sensor Network (WSN)?**

  WSN consists of hundreds or thousands of low-power nodes, that are able to sense real phenomena and communicate with each other. The data collected by the nodes is transferred to central device called Sink where sensor information are accumulated and processed.

- **Why do we need security in WSN?**

  WSNs are becoming increasingly popular for military and industry use. Because of this we cannot accept “security through obscurity” thus we need concrete protection against intruders.

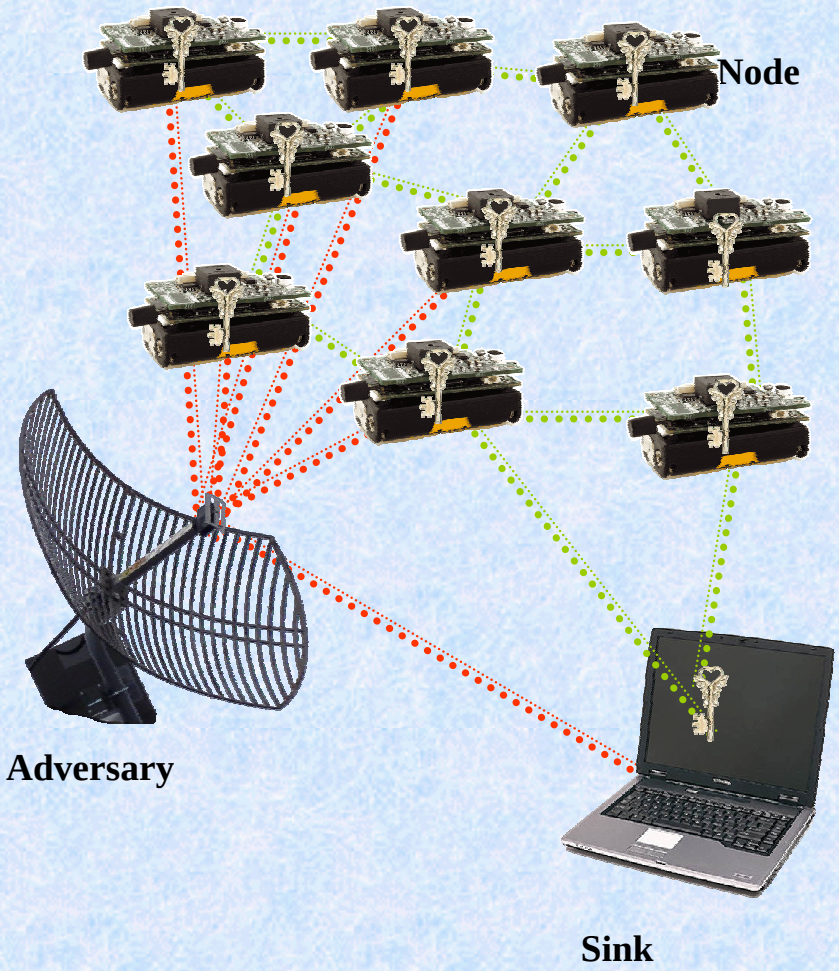
- **Security issues**

  Several factors make WSN susceptible to security threats. Those factors include the use of wireless medium, limited processor, memory and power resources, physical exposure of the nodes to the adversary, and the ad-hock infrastructure.

  We identify several possible scenarios of attacking the WSN and we use adaptive holistic approach to investigate the use of cryptography to provide level of security against the identified attacks.

2. Security threats in WSN

- Most attacks on WSN are based on the "man in the middle" scenario.
- Types of attack
  - Sniffing
  - Data integrity
  - Energy drain
  - Black hole
  - Hello flood
  - Wormhole

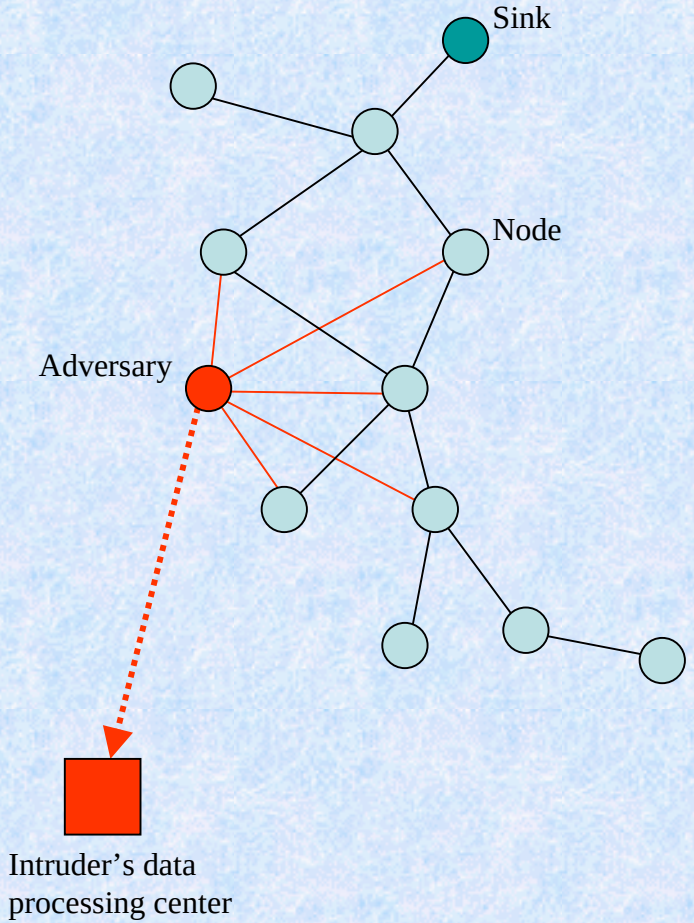


2.1. Security threats in WSN – Sniffing attack

• Sniffing attacks are done when a note is placed in the proximity of the sensor grid and data is captured by it. The collected data is transferred to the intruder by some means.

• The attack is based on the inherit vulnerability of the wireless networks of having unsecured and shared medium.

• The goal of this attack is to gather valuable data from the sensors. Often this attack is related to military or industrial espionage.



2.2. Security threats in WSN – Data integrity attacks

• Data integrity attacks compromise the data traveling among the nodes in WSN by changing the data contained within the packets.

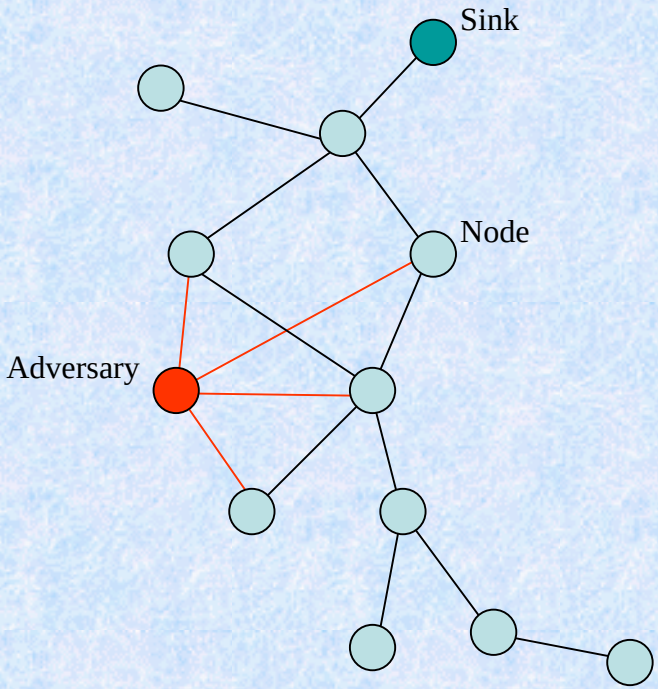
• The attack is possible because of the protocols used in WSN for data exchange and route discovery. The attacker node must have processing, memory and power capabilities far greater than the sensor nodes.

• The goals of this attack can be:

  • To falsify sensor data and by doing so compromise the victim's research

  • To falsify routing data in order to disrupt the sensor network's normal operation, possibly making it useless. This is considered DoS attack.

  • To use known vulnerabilities in the network stack in order to hack the node's software.



2.3. Security threats in WSN – Energy drain attacks

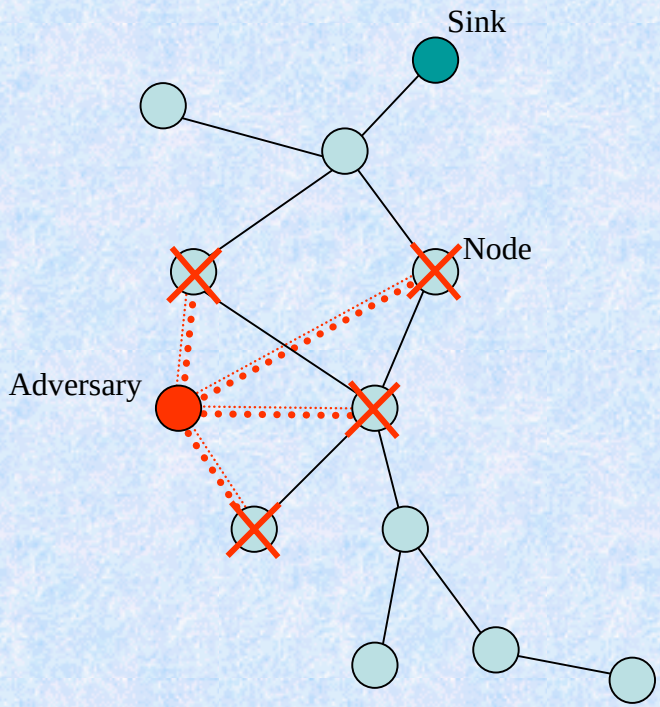
• Energy drain attack is conducted when an adversary node radiates large amount of traffic and requires other nodes to respond.

• The power scarcity of the WSN nodes and the fact that radio transmissions plays a huge part in energy spending makes this attack possible. However the attack is possible only if the intruder's node has enough energy to transmit packets at a constant rate. The routing algorithms can compensate for this attack so it is necessary for the attacker to has greater transmission range to be able to compromise a large section or the entire network.

• The goals of this attack can be:

  • To destroy the capabilities of the WSN

  • To split the network grid and consequently take control of part of the sensor network by inserting a new Sink node.



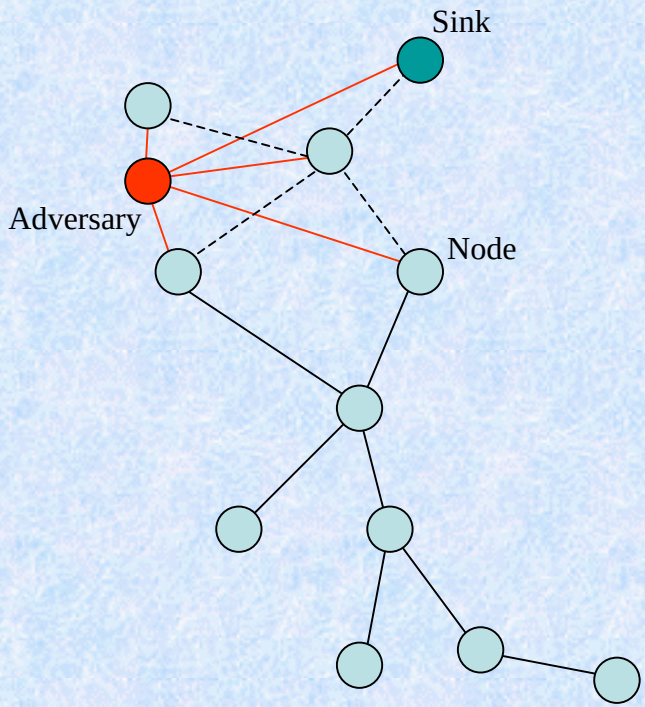
2.4. Security threats in WSN – Black hole attack

• The black hole attack consists of positioning a node in range of the sink and attract the entire traffic to be routed thrugh it by advertising itself as the shortest route.

• The routing protocols that are responsible for the survival of the network as long as possible present the possibility for this attack. The attacker is faced with the issues of greater radio coverage and data throughput and consequently the issue of energy resources.

•The goals of this attack can be:

- To provide a better ground for lunching other attacks like data integrity or sniffing.
- To block the traffic to the sink



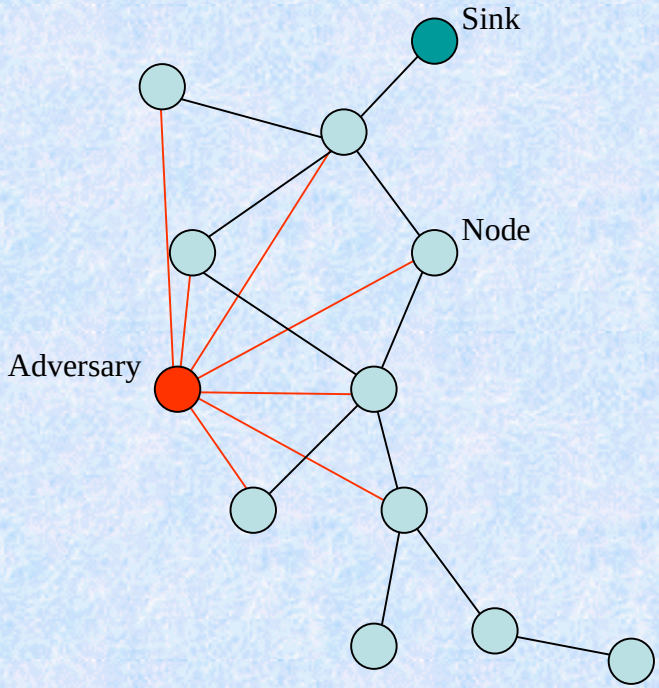
2.5. Security threats in WSN – Hello Flood Attack

• In hello flood attack HELLO packets are used to establish the attacker as a neighbor to the sensors located in wire area thus fooling them to send the data destined for the base station through it.

• This attack is similar in nature to some of the previously described attacks and it also requires large energy spending and long range radio coverage by the adversary.

•The goals of this attack can be:

- To be an alternative to the black hole attack
- To control the data flow in the WSN
- To be combined with some of the other attacks



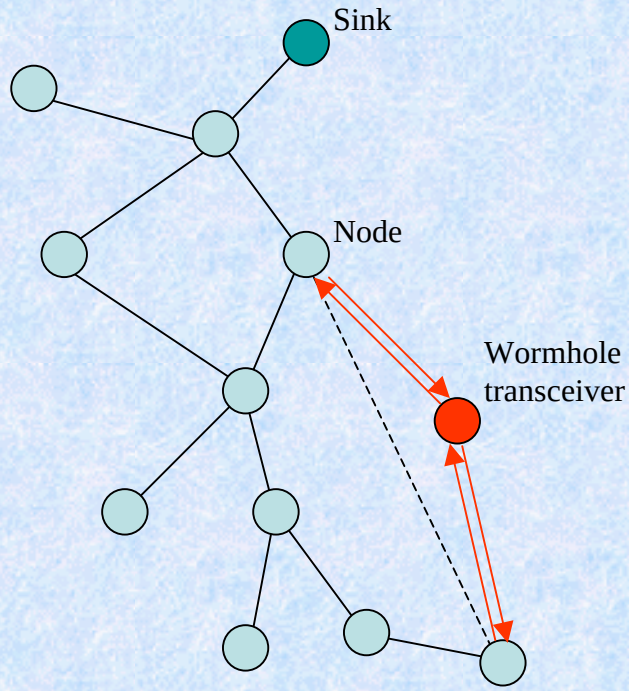
2.6. Security threats in WSN – Wormhole Attack

• Wormhole attack is a layer 1 attack. It is done by the intruder node acting as a repeater between two or more nodes. In doing so the attacker creates a virtual wormhole so the victim nodes discover each other as neighbors.

• This is by far the hardest attack to protect against since it is committed on level 1 of the network stack and only the data channel is affected. Our research has not yet came up with cost effective solution for this attack using cryptography. Complex routing protocols could present a solution. This issue is interesting research challenge.

•The goals of this attack can be:

- To undermine cryptography protection
- To confuse the sensor's protocols and disrupt normal functioning



3. Application of cryptography in WSN

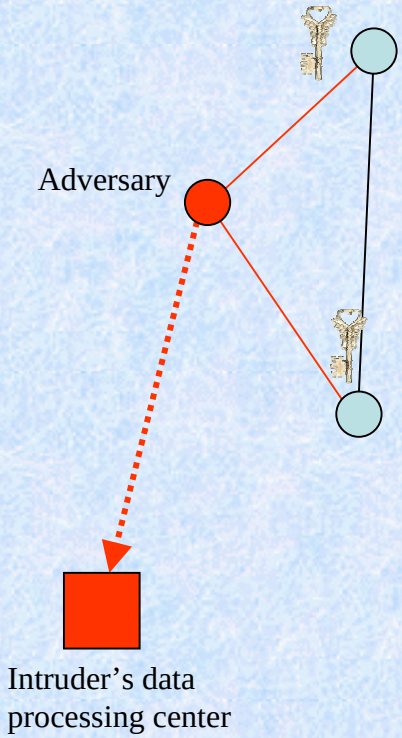
- Identify cryptographic goals
  - Confidentiality
  - Data integrity
  - Authentication
  - Non-repudiation
    (little interest to WSN)
- Identify protection schemes
    - Identify constraints
- Identify cost
- Adaptive holistic approach

3.1.1. Application of cryptography in WSN - Confidentiality

• Confidentiality is a service used to keep the content of information from all but those authorized to have it.

• Confidentiality is used to handle the sniffing attacks. The packets could be captured by the adversary but it won't be intelligible for to be used in any way.

• Confidentiality can be achieved by using cryptography. Either symmetric or asymmetric key can be used to protect the data from exposure to the adversary.

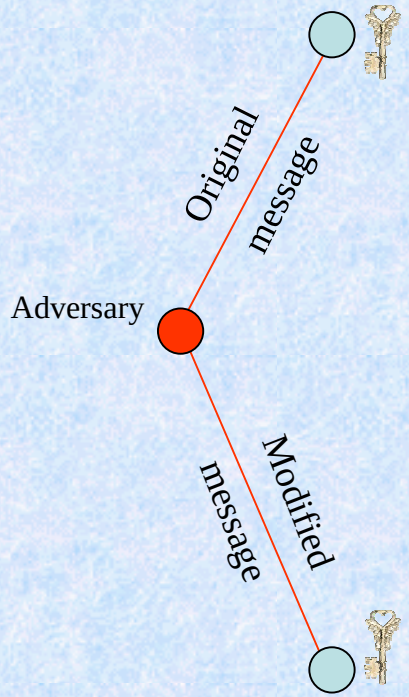


3.1.2. Application of cryptography in WSN – Data integrity

• Data integrity is a service that prevents or identifies unauthorized alteration of data.

• By providing data integrity we are able to solve the Data integrity attacks.

• Data integrity is achieved by means of signing the data content. If the adversary changes the message then the receiving node can identify the modification and disregard the message.



3.1.3. Application of cryptography in WSN - Authentication

• Authentication is a service that provides that the parties involved in communication are authorized and to confirm their identity.

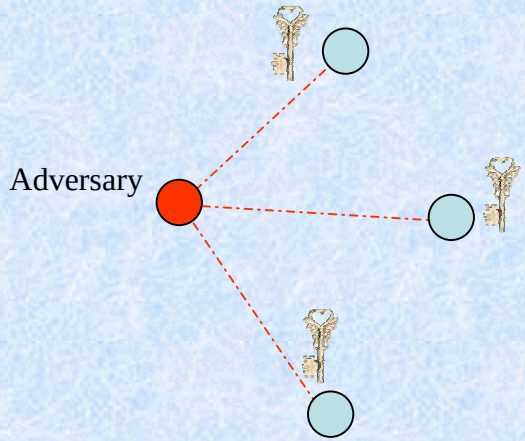
• This cryptographic goal can be used to prevent data integrity, energy drain, black hole and hello flood attacks.

• *Authentication* is accomplished by providing cryptographic means of identifying each node.

• *Data integrity* attacks can be handled using authentication. When a node is not successfully identifies the intruder's node the node does not become a part of the network so data from that node is disregarded.

• *Energy drain* and *black hole* attacks depend on the nodes talking to the adversary. This can be prohibited by preventing the nodes from sending messages to unauthorized nodes.

• In the *hello flood* attacks the enemy nodes are not able to advertise themselves as neighbors because they are also required to authenticated.



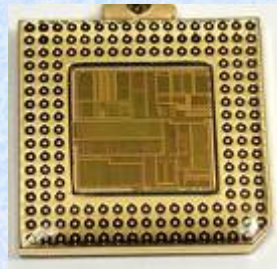
3.2. Application of cryptography in WSN - Constrains

- Memory constrains

  The are two types of memory constrains in WSN for implementing cryptography. First is limited RAM memory and the second is limited code memory.

- Processor constrains

  Cryptography is processor demanding activity. Especially public key cryptography is processor demanding since to achieve good security longer keys are required.



- Energy constrains

  Nodes are battery powered and thus for them to achieve longer live and functioning must save energy. Most of the energy is spend by the radio transmission.

3.2. Application of cryptography in WSN – Costs and benefits

Costs

- Public key
  - Large keys require more processing time especially if implemented at a lower layer of the OSI stack.
- Symmetric key
  - Complicated key distribution

Benefits

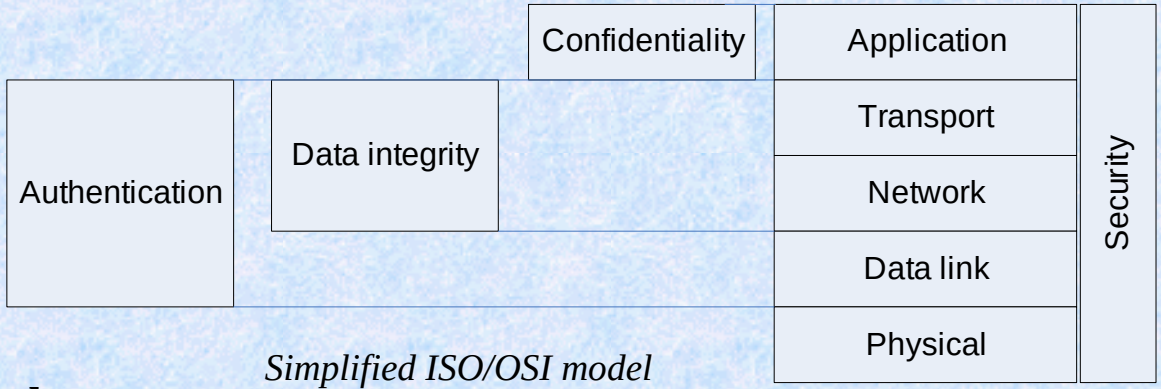
- Public key
  - Solves key distribution problem
- Symmetric key
  - Lower processor cost

Discussion of possible combined model

At cases where it is feasible to implement more than one algorithm a combination of public key cryptography for key distribution and symmetric key for data encryption could be used by the following algorithm.

4. Adaptive holistic approach

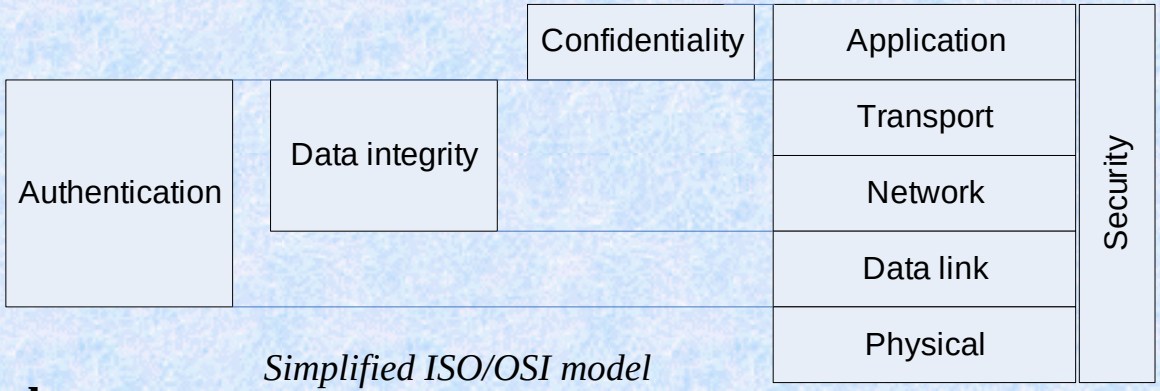
- **Holistic approach**
  - Security at all layers



Simplified ISO/OSI model

- **Our adaptive holistic approach**
  - We use adaptive approach to provide security through cryptography in WSN. The adaptive approach focuses on partial implementation of cryptographic goals at certain layers of the ISO/OSI model to provide low cost solution while maintaining the level of security found in the full holistic approach. The concrete selection of the goals would be made based on required specific adaptation. The proposal can be discussed and improved based on the needs and level of protection required.
  - Confidentiality most often would show best results if used at the application layer. Protocols used at lower layer are usually publicly available and hiding them from the adversary would not offer benefits but would greatly increase the overhead and slow down the routing protocols.

4. Adaptive holistic approach



Simplified ISO/OSI model

- **Our adaptive holistic approach**

  - Data integrity is proposed to be implemented at the transport level to establish reliable end-to-end communication. It can be used to defend against intruders but also against unreliable transmission environment. In addition it can be implemented at the network layer to protect against attacks aimed at the routing protocols.

  - Authentication provides protection against the majority of attacks aimed at compromising the normal operation of the WSN. Therefore we propose, depending on specific needs, that this goal be implemented at the Data link, Network and Transport layer. Most often data link authentication will prove sufficient except in cases where the adversary is able to physically capture one or more nodes.

5. Conclusion

- WSN require security but demand lower cost for providing it.
- We explore the possible attacks on WSN and elaborate possible protection schemes using the main cryptographic goals.
- Using adaptive holistic approach we propose cost saving implementations of each cryptographic goal by implementing the algorithms on specific layers of the ISO/OSI model to provide the best effect.
- Future work will include testing various models experiment with our WSN equipment to obtain empirical evidence for the proposed models.