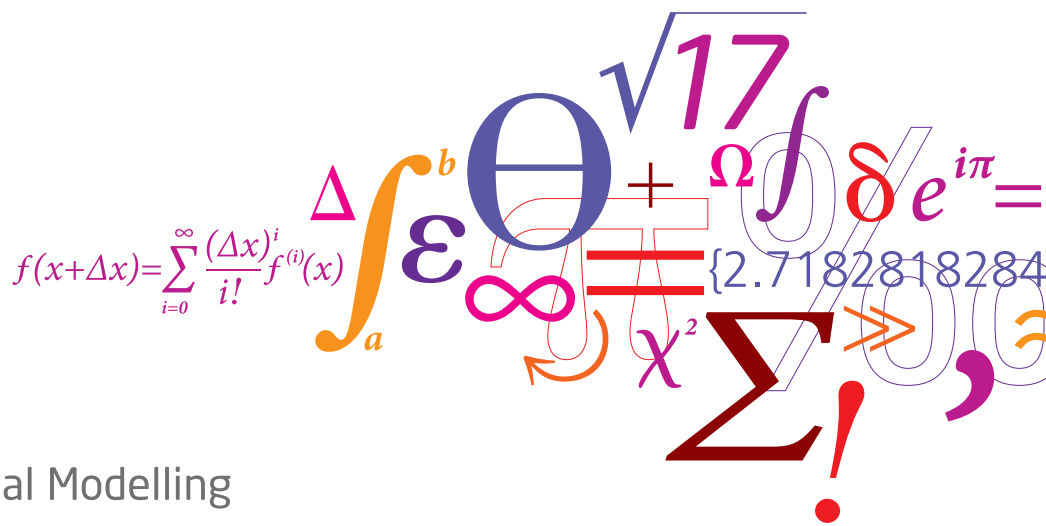
Security in Wireless Sensor Networks – Course 02234

Threats and common attacks

Alessio Di Mauro
Davide Papini

DTU Informatics



DTU Informatics
Department of Informatics and Mathematical Modelling

Outline

Security goals

Attacker types

Passive attacks

Active attacks

Outline

Security goals

Attacker types

Passive attacks

Active attacks

Security goals

Security has many different aspects, common goals are:

- Authentication (Identity verification and validation)
- Access Control (Granting access only to allowed resources)
- Confidentiality (Forbid access to unwanted third parties)
- Privacy (Prevent retrieval of private information, also implicitly!)
- Integrity (Data is exchanged without malicious alteration)
- Non-repudiation (Data can always be linked to its true owner)
- Freshness (Prevent identical copies of the same message to be sent)
- Availability (Service has to be always available)

Outline

Security goals

Attacker types

Passive attacks

Active attacks

Attacker types

- An attacker can be active or passive (and so are the attacks performed)
- An attacker can be an insider or an outsider
- An attacker can be fixed or mobile
- An attacker can be stealthy or non-stealthy
- Multiple attackers can coexist in the same system, furthermore they can join forces to perform more complex attacks

Outline

Security goals

Attacker types

Passive attacks

Active attacks

Passive attacks

These techniques don’t cause direct harm to a system, hence the name.

Passive attacks

These techniques don't cause direct harm to a system, hence the name.

Eavesdropping

Radio frequency is an ubiquitous medium. Potentially everybody can overhear unprotected (and protected) transmissions if the protocol is known.

Passive attacks

These techniques don't cause direct harm to a system, hence the name.

Eavesdropping

Radio frequency is an ubiquitous medium. Potentially everybody can overhear unprotected (and protected) transmissions if the protocol is known.

Traffic analysis

By analyzing the traffic (e.g. sender, recipient, number of messages exchanged) useful information can be inferred such as the network topology and a node role. Different levels can be observed.

Passive attacks

These techniques don't cause direct harm to a system, hence the name.

Eavesdropping

Radio frequency is an ubiquitous medium. Potentially everybody can overhear unprotected (and protected) transmissions if the protocol is known.

Traffic analysis

By analyzing the traffic (e.g. sender, recipient, number of messages exchanged) useful information can be inferred such as the network topology and a node role. Different levels can be observed.

Often used as starting points to perform aimed attacks to key elements (e.g. DoS around the sink).

Outline

Security goals

Attacker types

Passive attacks

Active attacks

- Physical
- Camouflage, replay and message modification
- Denial of service
- Cryptographic attacks

Active attacks

Cause direct harm and disrupt the normal functioning of the system.

Most common active attacks are:

- Physical
- Camouflage, replay and message modification
- Denial of service
- Cryptographic attacks

Physical

Nodes could be easily accessible to physical attackers

Physical

Nodes could be easily accessible to physical attackers

Destruction

One or more nodes are simply destroyed and removed from the network.

Physical

Nodes could be easily accessible to physical attackers

Destruction

One or more nodes are simply destroyed and removed from the network.

Tampering

Nodes are analyzed and/or altered in different ways:

- Firmware dump
- Node reprogramming
- Cloned nodes
- Cryptographic keys dump
- ...

Camouflage, replay and message modification

Camouflage

A node pretends to be another node. Global identification is not always used in WSN. Reactive protocols (as opposed to routing based protocols) can be easily fooled.

Camouflage, replay and message modification

Camouflage

A node pretends to be another node. Global identification is not always used in WSN. Reactive protocols (as opposed to routing based protocols) can be easily fooled.

Replay

Successfully camouflaged nodes can replay the same message over and over again (e.g. logging in without username and password).

Camouflage, replay and message modification

Camouflage

A node pretends to be another node. Global identification is not always used in WSN. Reactive protocols (as opposed to routing based protocols) can be easily fooled.

Replay

Successfully camouflaged nodes can replay the same message over and over again (e.g. logging in without username and password).

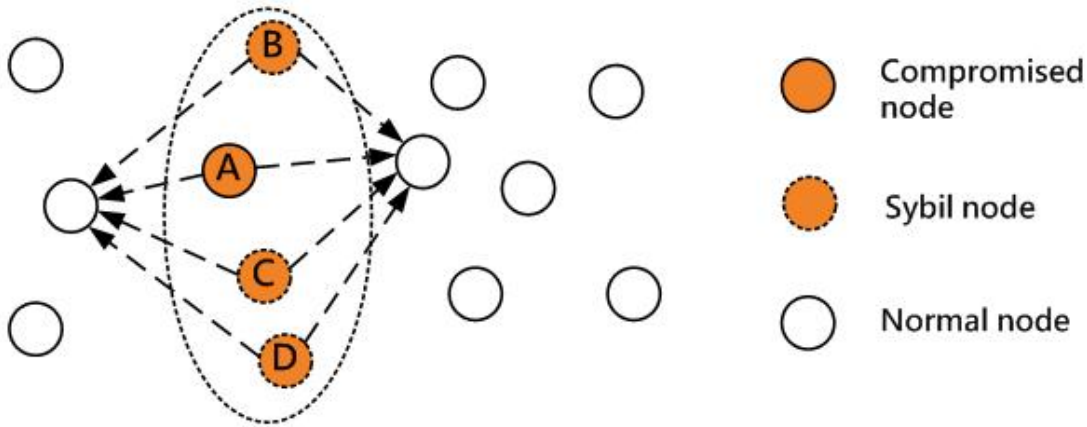
Message modification

Message could be modified before being replayed or forwarded (e.g. the temperature is ~~above~~ within normal values).

Camouflage, replay and message modification – cont

Sybil

A node relates to the rest of the network using multiple different identities. Aggregate data could be altered and routing path invalidated.



Denial of Service

Denial of Service attacks undermine the availability of the service provided by the system. DoS can be performed on different layers. However, different types of DoS tend to overlap.

Denial of Service – Physical layer

Jamming

RF signal can be jammed by using overlapping signals that can reduce the S/N ratio below the accepted threshold. Jamming can be performed remotely and selectively.

Denial of Service – Physical layer

Jamming

RF signal can be jammed by using overlapping signals that can reduce the S/N ratio below the accepted threshold. Jamming can be performed remotely and selectively.

Destruction and Tampering

These two attacks can be performed in such a way to cause DoS within the system.

Denial of Service – MAC and Link layer

These are attacks that exploit protocol specific information

Denial of Service – MAC and Link layer

These are attacks that exploit protocol specific information

Intentional Collision

- Sending colliding CTS packets whenever a RTS is received
- Jamming of active periods
- Fake long transmissions
- ...

Denial of Service – MAC and Link layer

These are attacks that exploit protocol specific information

Intentional Collision

- Sending colliding CTS packets whenever a RTS is received
- Jamming of active periods
- Fake long transmissions
- . . .

Resource exhaustion

Nodes usually have a limited amount of energy (i.e. a battery). Prolonged intentional collisions attacks can produce a quicker power depletion, permanently removing the attacked nodes from the network.

Denial of Service – Network Layer

The aim of these attacks is to disrupt the normal delivery of network level packets or to cause resource exhaustion by sending fake data.

Denial of Service – Network Layer

The aim of these attacks is to disrupt the normal delivery of network level packets or to cause resource exhaustion by sending fake data.

Hello flood

Powerful signals are used to broadcast HELLO packets where the attacker pretends to be a neighbor of all the other nodes. Messages sent to the attacker won't reach their destination.

Denial of Service – Network Layer

The aim of these attacks is to disrupt the normal delivery of network level packets or to cause resource exhaustion by sending fake data.

Hello flood

Powerful signals are used to broadcast HELLO packets where the attacker pretends to be a neighbor of all the other nodes. Messages sent to the attacker won't reach their destination.

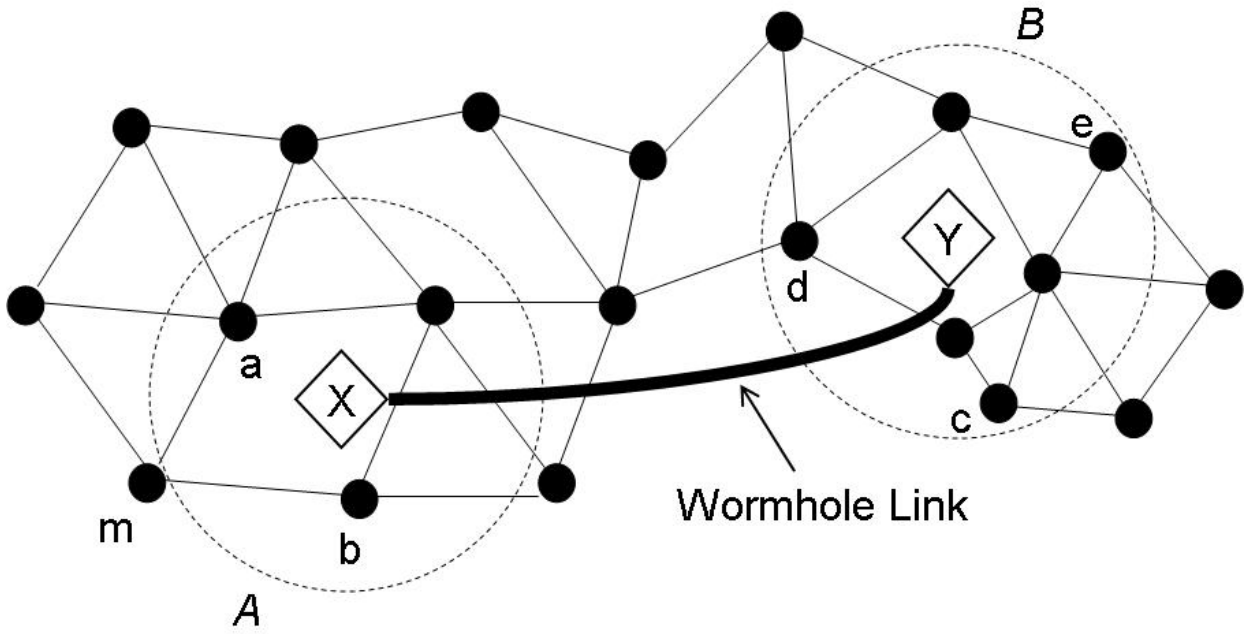
Detour

Sub-optimal routes may be forced (for example by adding virtual nodes) so that more energy is used to relay packets. Furthermore loops can be created.

Denial of Service – Network Layer – cont

Wormhole attack

Two malicious nodes can collude to forward messages from one to the other using a low latency OOB channel. Neighborhood tables are invalidated and regular packets are dropped for reaching their TTL.



Denial of Service – Network Layer – cont

Sink hole attack

A malicious node presents itself as a good routing choice and becomes a hub for the messages going to the base station. These messages can then be dropped or used for further attacks.

Denial of Service – Network Layer – cont

Sink hole attack

A malicious node presents itself as a good routing choice and becomes a hub for the messages going to the base station. These messages can then be dropped or used for further attacks.

Black hole attack

A node starts dropping all the traffic that it receives. If the node is also a sink the attack is much more effective.

Denial of Service – Network Layer – cont

Sink hole attack

A malicious node presents itself as a good routing choice and becomes a hub for the messages going to the base station. These messages can then be dropped or used for further attacks.

Black hole attack

A node starts dropping all the traffic that it receives. If the node is also a sink the attack is much more effective.

Selective forwarding (or gray hole attack)

Only a particular type of packets are dropped by the node either for its own advantage or in order to avoid detection.

Denial of Service – Transport layer

SYN flooding

A node sends multiple SYN packets to other nodes with a spoofed return address, never completing the 3WHS. This causes lots of half-opened connections to be stored by the victims the eventually won't be able to accept new legit connections.

Session hijacking

An attacker replaces the victim after the session setup time (when credential are exchanged) and continues the communication undetected from the other node.

Cryptographic attacks

Cryptography is commonly used to produce security and cryptographic primitives are frequently targeted.

Cryptographic attacks

Cryptography is commonly used to produce security and cryptographic primitives are frequently targeted.

Pseudo-random generators

Pseudo-random numbers are used for many tasks (e.g. nonce, IVs). However they're usually designed for statistical purposes and the seed could be obtained if enough numbers have been observed. Only secure PRG should be used for security purposes.

Cryptographic attacks

Cryptography is commonly used to produce security and cryptographic primitives are frequently targeted.

Pseudo-random generators

Pseudo-random numbers are used for many tasks (e.g. nonce, IVs). However they're usually designed for statistical purposes and the seed could be obtained if enough numbers have been observed. Only secure PRG should be used for security purposes.

Signatures

Crypto schemes use digital signatures to authenticate messages. Depending on the scheme known signed messages could be replayed, old signatures could be appended to forged messages.

Cryptographic attacks

Cryptography is commonly used to produce security and cryptographic primitives are frequently targeted.

Pseudo-random generators

Pseudo-random numbers are used for many tasks (e.g. nonce, IVs). However they're usually designed for statistical purposes and the seed could be obtained if enough numbers have been observed. Only secure PRG should be used for security purposes.

Signatures

Crypto schemes use digital signatures to authenticate messages. Depending on the scheme known signed messages could be replayed, old signatures could be appended to forged messages.

Key management

Cryptographic keys could be unsafely handled during their generation, sharing, storage etc. Attacks aimed to obtain the keys could be performed in these phases (No central trusted authority in WSN).

Project Ideas – $1/3$

Attacks survey

Choose one class of attacks and write a small technical survey. The report should explain the attacks in detail, discuss about suitable WSN systems where to deploy the attacks, discuss about real application instances and known countermeasures.

- Choose a class of attacks
- Research work using available literature
- Write a final report

Project Ideas – $2/3$

Ideas for attack countermeasure

Familiarize yourself with one of the presented attacks and write a small technical report focused on a possible new idea on how to prevent and/or detect that attack. The report should explain the attack and your idea in detail, discuss about suitable WSN systems where to deploy the attack, discuss about real application instances and compare your idea to known countermeasures.

- Choose one of the attacks
- Research work using available literature
- Think about a new technique on how to counter such attack
- Write a final report

Note: if the idea is good there are possibilities to further develop it. (MSc Thesis!).

Project Ideas – $3/3$

Energy harvesting WSN

Write a small technical report that examines one class of the presented attacks, in the EH-WSN scenario. How do the attacks change compared to regular WSN? Which attacks make sense? Which don't? For example Taddeo *et al.* (2010) presented a dynamic algorithm that decreases the message security depending on the available energy. Messages are also delayed if it's not possible to fulfill their minimal security requirements. By exhausting the resources of a node and then analyzing if it is transmitting or not it is possible to know if important messages are being sent and if is worth further attacking the node.

- Choose a class of attacks
- Research work using available literature
- Further research work specialized in the Energy Harvesting context
- Write a final report

Project Ideas - $3/3$ – cont

Note: project 2 and 3 could be combined together. If you have an idea we can talk about it.

Requirements and rules

- Be sure to include all (an hopefully only) the useful material
- Any material which you include in your report, and that is not your own personal work, must be clearly marked. Furthermore, you must give a reference to its source
- The first page of the report must contain the project title, the academic year, your name and your student number
- The report should be around 10 to 15 pages long and should follow the common layout for a scientific paper (more on this in the next lecture)

References

- Erdal Cayirci and Chunming Rong, *Security in Wireless Ad Hoc, Sensor and Mesh Networks*, John Wiley & Sons, 2009, ISBN 978-0-470-02748-6.
- Teodor-Grigore Lupu. Main types of attacks in wireless sensor networks. *In Proceedings of the 9th WSEAS international conference on signal, speech and image processing, and 9th WSEAS international conference on Multimedia, internet & video technologies (SSIP '09/MIV'09)*. World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, Wisconsin, USA, 180-185.
- Antonio Vincenzo Taddeo and Marcello Mura and Alberto Ferrante, QoS and Security in Energy-harvesting Wireless Sensor Networks *In Proceedings of ICETE SECRYPT 2010*