Freie Universität Berlin

Summer Term 2008

PS Telematik Projekt: Embedded Sensor Web

Attacker

Outline

1. introduction
2. theoretical background
3. implementation
4. (results)
5. problems
6. conclusion

1 - introduction

- wireless networks are vulnerable for numerous potential 'villains'
- no possibility to make a wireless network immune
  - neither to intentional nor to unintentional attacks
- but:
  - there are a few possibilities to make an attack difficult
- in general:
  - especially for safety relevant information it must be guaranteed, that no third person is able to get it

1 - introduction

- there won't be safety relevant information in this wireless network
- nevertheless:
  - ‚The HomeAutomationCompany™‘ is interested in a robust and stable network, so that it needs a big effort to jam the network
- my task:
  - find some possibilities to disrupt the network in order to get to know, how the network will react

2 - theoretical background

General problem in every wireless network:

- everyone who is in range is able to receive sent data in the network
  - it does not matter, if someone who receives data, is allowed to receive data or if he is not
- therefore there are some cornerstones a serious network should meet:
  - *confidentiality*
  - *integrity*
  - *availability*
  - *authenticity*
  - *accountability, non-repudiation*

2 - theoretical background

Conveying some ideas for jamming the WSN from cornerstones

Before:

- passive attacks
- active attacks

2 - theoretical background

passive attacks

- tapping network traffic
- analysing tapped network traffic

active attacks

- occupying the network
- manipulating the network after analysing
  - sending changed data
  - sending duplicated data
- manipulating network structure
  - I am one of them
  - everyone is the same
  - routing changed
- manipulating the hardware

3 – implementation

Tapping the network – my first sniffer!

- every data packet sent in the network logged
- analysing it …?
  - there were a lot of packets of type 80 and 81 … ;-)
  - no chance to get really useful information for manipulation

Occupying the network

- which channel does the network currently use
- send data for a time period without interuption
- scanning the channel again

3 – implementation

Gadgetries …

Manipulating the hardware using the possibilities of scatterweb

- How will the WSN react, when every node has the same id?
- What will happen, when the transmit power of every node is 0?

4 – (results)

5 - problems

Needed effort for analysing the network traffic is enormous!

- routing ?
- content of data packets ?

Therefore:

- most of the possible mechanisms were simply too hard to implement
- occupying the network is an option, but it‘s not the smartest one

- attacking at the given network structure is another option

6 - conclusion

In this project there are still many possibilities to jam the network.

A lot of them are not obvious, because the hacker does not belong to the top 5 … ;-)

But for one, who has enough time to study and analyse the network traffic, it is not too hard to manipulate the Wireless Sensor Network.

Some more safety arrangements should be integrated.

Ideally the network would use an secure encryption while sending, as it is almost standard in a wireless network, but everyone knows, that this would have gone beyond the scope of our project.