Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)

Submission Title: [Secure SDS-TWR Sequence]
Date Submitted: [23 August, 2005]
Source: [Lars Menzer] Company [Nanotron Technologies GmbH]
Address [Alt-Moabit 61, D-10555 Berlin, GERMANY]
Voice:[+49303999540], FAX: [+4930399954288], E-Mail:[l.menzer@nanotron.com]

Re: [802.15.4a.]

Abstract: [Discusses security issues on ranging and proposes methods and a secure ranging sequence]

Purpose: [Promote discussion 15.4a PHY/MAC requirements]

Security Issues

- Security in this context means that range and location cannot
  - **be manipulated**
  - **acquired by unauthorized devices**

Potential Applications

- Military
- Law enforcement
- Asset tracking
- But even simple applications with liability of operators or manufacturers (e.g., range aware garage door opener, range aware key-less entry systems)

Manipulation

- Attackers can disturb or change information on transmitted messages (node IDs, time stamps, crystal offsets, etc.)
- Attackers can transmit fake ranging messages
  - Replay attacks (record a valid ranging message & replay it)

Unauthorized Acquisition

- Decoding of ranging information (time stamps, crystal offsets, range) from ranging messages
- Transmit initiating messages
  - Easily getting response messages with all information
  - Replay attacks
- Passive TOA measurement on ranging as well as **non-ranging** message sequences
  - Ranging response time attack*
- Active TOA measurement on **non-ranging** message sequences
  - Ranging response time attack*

* see next slide

*Response Time Attack

- Response time of message sequences (DATA-ACK, CTRL-ACK) can vary per 15.4 standard definitions, **but**:
- In CFP and non-beacon enabled networks variation is not guaranteed
- Precise response time behavior of devices is known or can be found out by characterization (manufacturer can be identified by MAC address), probably $\mathbf{t_{ack}}$ does vary in coarse steps only (resulting offsets on range can be identified and eliminated: e.g., 15 m .. 315 m .. 615 m)
- In CAP variation in coarse steps due to slot alignment likely
- Response time can vary equally distributed within a known time range due to clock drift, then averaging over several sequences is possible
- TOA accuracy can be improved further by measurement of several sequences and averaging
- Crystal errors can be eliminated by measurement of symmetrical message exchange (SDS-TWR, Doc: 15-05-0002-01-004a)

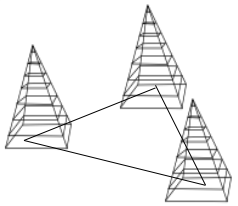
Definitions

- Robustness
  - Ranging information can be protected against noise and disturbers
- Security*
  - Ranging can be protected against attackers, which could try to manipulate a system
- Privacy
  - Range can be kept as a secret within a closed group, 3rd parties shouldn't be able to find out range and/or location

* Security is the general term as well

Security Measure

- Protect ranging against an attacking 15.4a device with a typical antenna
- Protect ranging against noise, disturbers & attackers
- Protection against heavy equipment or other methods is partly possible to impossible:
  - Parabolic antennae (AOA method)
  - Infrastructure / anchor nodes (TDOA)
  - Other searching methods



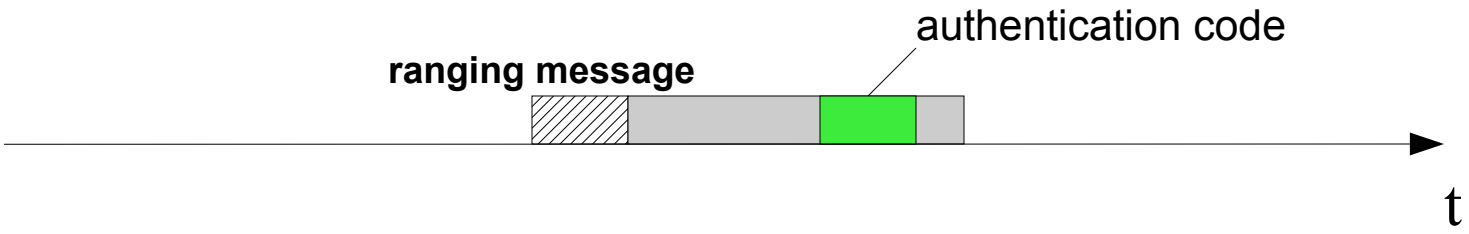
Security on Ranging

- ***Don't:***
  - Transmit unprotected ranging information
  - Cooperate in ranging without authorization/authentication checks
  - Use ranging information without authentication checks
  - Response after a deterministic, publicly known or fixed turnaround time in ranging message sequences as well as **data message sequences** (response time attacks)
  - Utilization of the non-atomic* authentication mechanism only

*see next slides

Atomic Authentication

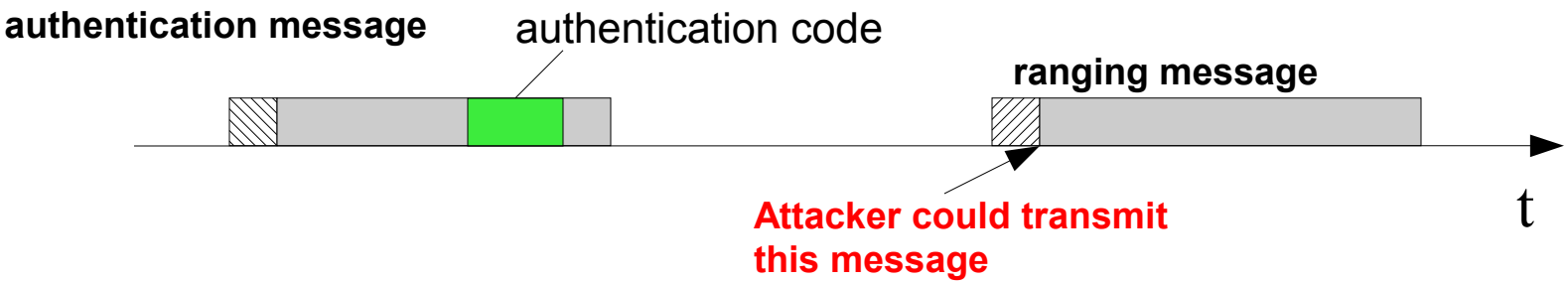
- Authentication code is embedded into the ranging messages
- No additional messages required



- Ranging message authenticates itself

Non-Atomic Authentication

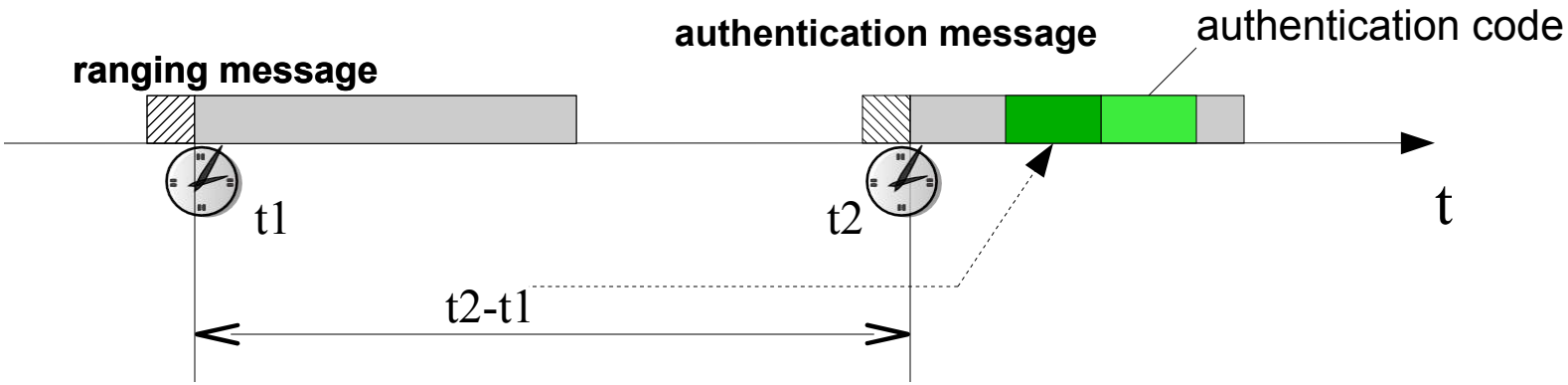
- Authentication code is not embedded into the ranging messages
- Utilization of additional authorization message



- **Secure identification of ranging message is not possible**

Semi-Atomic Authentication

- Utilization of an additional authentication message with references (e.g., time references) to the ranging message



- Ranging message can be identified securely

Security Capabilities 15.4 PHY/MAC

- **PHY**
  - Is not able to check the correctness of a ranging message nor to protect ranging information
  - Does not know unique identifiers
- **MAC**
  - Checks for bit errors, correctness (FCS)
  - Knows unique identifiers (MAC addresses, sequence numbers)
  - Can encrypt payloads
  - Supports authorization/authentication methods
  - Does not support control of response time to allow guaranteed non-deterministic response time behavior

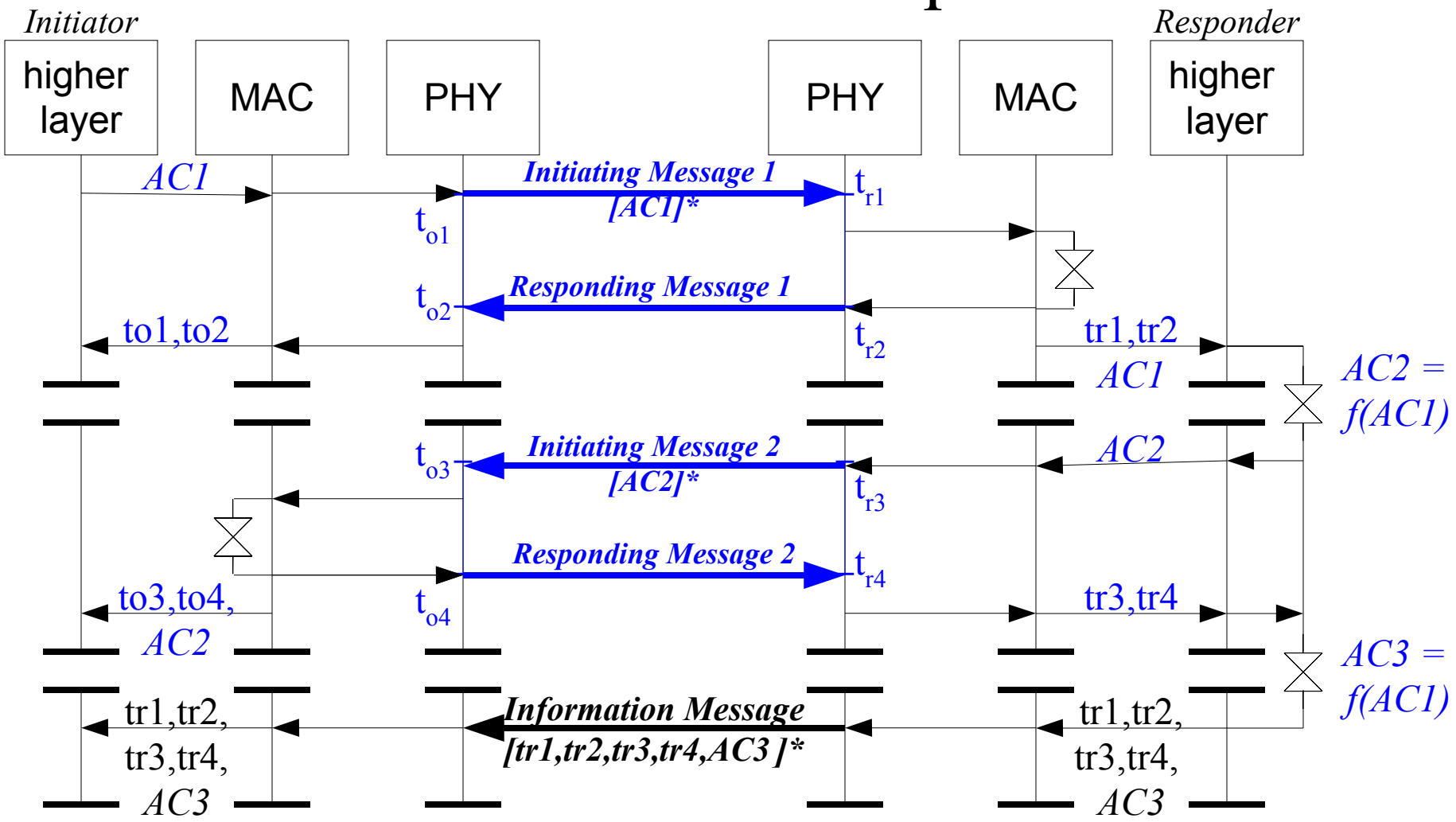
Security Support by Higher Layer

- Can implement security mechanisms as an option
- Needs minimum support from PHY/MAC
  - Uses existing MAC features (e.g., encryption)
  - Avoids ranging security extensions in MAC and potential security flaws in low layer standard
- Security mechanisms can be made as complex as required and don't have to be very fast

Additional Feature Required in PHY/MAC: Response Time Control

- Guaranteed non-deterministic response time behavior of sequences to avoid response time attacks
- Introduce additional PHY and/or MAC controls
- Response time has to be varied in a secure way to avoid averaging and correlation attacks, but this can be controlled by higher layer
- This feature is mandatory for data message sequences

Secure SDS-TWR Sequence



ACx = Authentication Code *encrypted payload

Secure SDS-TWR Sequence (cont.)

- *AC1* authenticates *Initiating Message 1*
- *AC2* authenticates *Initiating Message 2* (*AC2* was generated from *AC1*)
- *AC3* authenticates *Information Message* (*AC3* was generated from *AC1*)
- Originator checks authenticity of *Responding Messages 1* by comparison of $(t_{r3}\text{-}t_{r2})$ with $(t_{o3}\text{-}t_{o2})$ and *Responding Messages 2* by comparison of $(t_{r4}\text{-}t_{r1})$ with $(t_{o4}\text{-}t_{o1})$
- *Initiating Message 1* can be protected further by one-time-pads or validity dates to avoid replay attacks (e.g., optional real time clock on higher layer)

Secure SDS-TWR Sequence (Summary)

- All messages can be authenticated securely, by atomic and semi-atomic mechanisms
- Prior authentication is not necessary
- Sequence uses available MAC functions: encryption, payload/non-payload message sequence (DATA-ACK-like sequences could be applied for ranging)
- Additional feature required in PHY/MAC: response time control, but mandatory against response time attacks
- Authentication procedures are not critical in timing
- Higher layer can implement authentication mechanisms