### Wireless Networks II: Performance & Cross-Layer Aspects

by Hans Peter Schwefel

<table>
<thead>
<tr>
<th>Mm1</th>
<th>Cellular Networks: GSM, GPRS, and UMTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mm2</td>
<td>Security aspects of wireless networks</td>
</tr>
<tr>
<td>Mm3</td>
<td>Security (cntd.), Header Compression</td>
</tr>
<tr>
<td>Mm4</td>
<td>Performance aspects/Quality of Service</td>
</tr>
<tr>
<td>Mm5</td>
<td>Reliability aspects</td>
</tr>
</tbody>
</table>

www.kom.auc.dk/~hps/WirelessNetworksII_Sp05/

### Last Lecture (MM2)

1. Security Requirements and basic cryptographic methods
   - Encryption, Authentication, Integrity Protection
   - Cryptographic Algorithms/Protocols, Key Exchange
2. IP Security (IPsec)
   - Functionality, modes, etc.
3. Security in GSM
   - Authentication, Encryption/Integrity Protection
4. Security in GPRS/UMTS
   - Authentication: UMTS-AKA
   - Encryption/Integrity Protection
   - Network Protection, Firewalls
5. Summary/Exercises (GPRS core network/Firewalling)

[Moved to MM3]
Part I: Security (cntd. From MM2)

1. Security mechanisms in cellular networks
   • GSM: Authentication, Encryption/Integrity Protection
   • GPRS/UMTS: Authentication, Encryption/Integrity Protection

2. Security in WLAN 802.11
   • WLAN Overview
   • Authentication
   • Wired Equivalent Privacy (WEP)

Part II: Header Compression

3. Header Compression
   • Motivation, Basic Principles & Algorithms
   • Robustness

4. Summary/Exercises

GSM security objectives

• Restrictions on GSM security
  – GSM was designed to be as secure as the fixed networks to which it would be connected
  – Protection against so-called active attacks which involved impersonating a network element was not believed necessary to address when GSM was designed
Security in GSM: Overview

- Security services
  - access control/authentication
    - user ⇔ SIM (Subscriber Identity Module): secret PIN (personal identification number)
    - SIM ⇔ network: challenge response method
  - confidentiality
    - voice and signaling encrypted on the wireless link (after successful authentication)
  - anonymity
    - temporary identity TMSI (Temporary Mobile Subscriber Identity)
    - newly assigned at each new location update (LUP)
    - encrypted transmission
- 3 algorithms specified in GSM
  - A3 for authentication ("secret", open interface)
  - A5 for encryption (standardized)
  - A8 for key generation ("secret", open interface)

SECRET:
- A3 and A8 available via the Internet
- network providers can use stronger mechanisms

Subscriber Identity Module (SIM)

- A smart card based security module which is inserted into the mobile
- All security functions (except encryption) at the user side are implemented on the SIM
- It contains all the identification data and cryptographic keys needed to make or receive a call
- Allows access control via PIN
- A smart card is used to prevent duplication of the subscription by maintaining secrecy of the authentication key
**GSM – authentication**

Kᵢ: individual subscriber authentication key  
SRES: signed response

---

**GSM - key generation and encryption**

---
GSM authentication and key derivation - security properties

- Entity authentication of the user to the network
- Mutual implicit key authentication between network and user
- Assurance of key freshness to the network
- Confidentiality of user identity related information on the interface between the user and the network (protection only against passive attacks)
- Establishment of a 64 bit cipher key Kc (which may be shortened by key derivation algorithm to 54 bits).

GSM: encryption mechanism

<table>
<thead>
<tr>
<th>MS/SIM</th>
<th>BS</th>
<th>MSC/VLR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Authentication and key agreement protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kc: Encryption key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A5: Algorithm for encryption / decryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MS/SIM: Mobile Station / Subscriber Identity Module</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BS: Base Station</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSC/VLR: Mobile Switching Centre / Visitor Location Register</td>
</tr>
</tbody>
</table>

Diagram:

- Ciphering and Deciphering
- Key Flows
- Synchronization
- Cipher key frame number
- Kc

Allocation and use of temporary identities

**MS/SIM**

- IMSI (for first time, or if data not available in current VLR)
- Subscriber authentication and ciphering
- TMSI (encrypted)

**MSC/VLR**

- Subsequent location updates:
  - TMSI\_old (unencrypted)
  - Subscriber authentication and ciphering
  - TMSI\_new (encrypted)

---

**GSM weaknesses**

- Problems with active attacks using false base stations
- Encryption keys and authentication data are transmitted in clear between and within networks
- Microwave links in access network are not protected
- Standardised algorithm A5/1 for encryption has been broken
- “Example” algorithm COMP128 for authentication and key derivation has been broken
- The encryption key length of max 64 bits has become too short
### UMTS Network Architecture

- **BSS (RAN/GERAN)**
  - BTS
  - BSC
  - Abis

- **RNS (UTRAN)**
  - Node B
  - lub
  - Iur

- **RNC**

- **PS Domain**
  - SGSN
  - GGSN
  - Gn
  - Gs
  - Gi

- **CS Domain**
  - CS-MGW
  - VLR
  - Nb
  - Mc
  - A
  - Gb

- **Network Domain**
  - G-E/Nc
  - Mb/Gi
  - Cx

### UMTS Security Domains

#### User Domain Security
- Secure access to terminal

#### Network Access Security
- Mutual authentication of user and network
- Confidentiality and integrity on the radio access link

#### Network Domain Security
- Secure exchange of signaling traffic between network elements
- Protection against attacks on the wireline network

#### Application Security
- Secure exchange of messages between applications in the user and provider domain
Overview of UMTS Security Mechanisms (R5)

- Mutual Authentication (UE–SGSN): UMTS AKA
- Encryption on air interface (data and signalling, UE–RNC)
- Integrity protection of signalling data on the air-interface
- Network protection (secure topologies, firewalls, etc.) up to operator
- Integrity protection and encryption of signalling traffic on external interfaces (Gp, Gi) via IPsec tunnels (ESP)

Air interface: Integrity Protection

![Integrity Protection Diagram]

Message Integrity Protecting (MAC-I)
- SENDER (UE or RNC)
  - COUNT-I
  - DIRECTION
  - MESSAGE
  - FRESH
  - Integrity Key IK
  - Integrity Function f9
  - MAC-I

Air Interface
- MESSAGE
- MAC-I

RECEIVER (UE or RNC)
- COUNT-I
- DIRECTION
- MESSAGE
- FRESH
- Integrity Key IK
- Integrity Function f9
- XMAC-I
**Air interface: Encryption**

![Air Interface Diagram]

**UMTS authentication and key agreement - security properties**

- Assurance of key freshness to the user
- Entity authentication of the network to the user
- Establishment of a 128 bit cipher key CK
- Establishment of a 128 bit integrity key IK
- Provision of a means to exchange authenticated information between Authentication Centre and USIM for management purposes
UMTS Authentication and Key Agreement (AKA)

- Based on long-term pre-shared key K on USIM and in HLR/AuC
- Authentication vector: Quintuplet (random number RAND, expected response XRES=f2(K,RAND), cipher key CK, integrity key IK, authentication token AUTN) generated in HLR/AuC using a sequence number SQN, RAND, and K
- VLR/SGSN downloads authentication vectors from HLR/AuC during Attach

**UMTS AKA: Message flow during Attach**

1. RRC Connection Request
2. RRC Connection Setup
3. RRC Connection Setup Complete
4. NAS: Attach Request
5. NAS: User Identity Request
6. NAS: User Identity Response
7. MAP: Authentication Data Request
8. MAP: Authentication Data Response
9. Storage of Authentication Vectors
10. Selection of the oldest AV
11. NAS: User Authentication Request
12. Verification of Authentication Token
13. Compute RES
14. Store KSI
15. NAS: User Authentication Response
16. RES = XRES?
17. Compute Cipher and Integrity Key
18. Select Cipher and Integrity Key
19. Decide allowed Integrity & Encryption Algorithms
20. RANAP: Security Mode Command
21. Reset START value to zero
22. Select UIA and UEA

Security Mode Setup Procedure continues at next page
**Ongoing developments in GSM and UMTS security**

- WLAN interworking security for GSM and UMTS subscribers
- Multicast/broadcast security
- Subscriber certificates
- Security for presence services
- PKI-based automated key management for core network signalling protection
- New cryptographic algorithms

**Topics not treated here**

- Intrusion Detection Systems (IDS)
- Transport Layer Security (TLS)
- Application Layer Security (HTTPs, sMIME, etc.)
- Authentication Protocols (Radius, Diameter)
- Security and network management
- SIP/IMS security
- Security in WLAN/ WPAN
- Electronic Payment Systems/digital cash
References: UMTS

3GPP specifications can be found under http://www.3gpp.org/.

- 3GPP TS 33.102: ‘Security architecture’
- 3GPP TS 33.200: ‘Network domain security; MAP application layer security’
- 3GPP TS 33.203: ‘Access security for IP-based services’
- 3GPP TS 33.210: ‘Network domain security; IP network layer security’
- 3GPP TS 35.201: ‘Specification of confidentiality and integrity algorithms: f8 and f9’
- 3GPP TS 35.205-35.208: ‘Specification of the MILENAGE Algorithm Set

For ongoing developments in 3G security refer to the meeting reports under ftp://ftp.3gpp.org/TSG_SA/WG3_Security/Reports/.

References (2): UMTS

Overview articles:

Content

Part I: Security (cntd. From MM2)
1. Security mechanisms in cellular networks
   • GSM: Authentication, Encryption/Integrity Protection
   • GPRS/UMTS: Authentication, Encryption/Integrity Protection

2. Security in WLAN 802.11
   • WLAN Overview
   • Authentication
   • Wired Equivalent Privacy (WEP)

Part II: Header Compression
3. Header Compression
   • Motivation, Basic Principles & Algorithms
   • Robustness

4. Summary/Exercises

WLAN: IEEE 802.11 standard

- 802.3 Ethernet
- 802.5 Token ring
- **802.11 WLAN**
- 802.15 WPAN

- Standards specify PHY and MAC, but offers the same interface to higher layers to maintain interoperability

<table>
<thead>
<tr>
<th>application</th>
<th>TCP</th>
<th>IP</th>
<th>LLC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>802.11 MAC</td>
</tr>
<tr>
<td>access point</td>
<td></td>
<td></td>
<td>802.11 PHY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>application</th>
<th>TCP</th>
<th>IP</th>
<th>LLC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>802.3 MAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>802.3 PHY</td>
</tr>
</tbody>
</table>

IEEE=Institute of Electrical and Electronics Engineers
### System architecture

**802.11 - Architecture of an infrastructure network**

- **Station (STA)**
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- **Basic Service Set (BSS)**
  - group of stations using the same radio frequency
- **Access Point**
  - station integrated into the wireless LAN and the distribution system
- **Portal**
  - bridge to other (wired) networks
- **Distribution System**
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

### MAC Frame Format & ‘standard security features’

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration/ID</th>
<th>Address1</th>
<th>Address2</th>
<th>Address3</th>
<th>Sequence Control</th>
<th>Address4</th>
<th>Frame Body</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Byte</td>
<td>2 Byte</td>
<td>6 Byte</td>
<td>6 Byte</td>
<td>2 Byte</td>
<td>6 Byte</td>
<td>0-2312 Byte</td>
<td>4 Byte</td>
<td></td>
</tr>
</tbody>
</table>

- 32bit CRC covering Header and Data → Protection against transmission errors
- 'Hidden' SSID (Service Set Identifier); to be provided by STA for association with AP
- MAC address filters (~Authentication)
- Encryption utilizing Wired Equivalent Privacy (WEP)
- Authentication
  - Open-System und Shared-Key
Encryption/Integrity Protection using WEP

- Based on shared Key K (40 or 104 bit)
- WEP activation indicated by header bit
- Integrity Protection: 4-Byte Integrity Check Value (CRC32) covering payload

WEP = 0:

802.11Hdr. Payload FCS

WEP = 1:

802.11Hdr. IV Payload ICV FCS

Encrypted

K (40/104 Bit)
IV (24 Bit)

RC4

S

P

C

IV

Discussion: WEP Integrity Protection

- ICV does not use Key K and ‘Linearity’ of Integrity Check Value ICV with respect to XOR operation
  
  \[
  \text{ICV}(P_1) \ XOR \ \text{ICV}(P_2) = \ \text{ICV}(P_1 \ XOR \ P_2)
  \]

- Attack:
  - Assume message P, which creates encrypted message C
    
    \[
    C = \text{RC4}(IV,k) \ XOR \ \langle P, ICV(P) \rangle
    \]
  
  - An attacker can now modify the message with some pattern A as follows
    
    \[
    C \ XOR \ \langle A, ICV(A) \rangle = [\text{RC4}(IV,k) \ XOR \ \langle P, ICV(P) \rangle] \ XOR \ \langle A, ICV(A) \rangle
    
    = \text{RC4}(IV,k) \ XOR \ \langle P \ XOR \ A, ICV(P) \ XOR \ ICV(A) \rangle
    
    = \text{RC4}(IV,k) \ XOR \ \langle P \ XOR \ A, ICV(P \ XOR \ A) \rangle
    \]
  
  which is still a ‘legal’ message

- Consequence: Messages can be arbitrarily modified (selected bits swapped), e.g. IP source/destination address modification (redirect attack)
Discussion: WEP Confidentiality

- Value of IV repeats (at the latest after $2^{24}$ Frames)
- If attacker intercepts two frames with same IV:

  \[
  C_1 = P_1 \ xor \ RC4(IV_1, k) \\
  C_2 = P_2 \ xor \ RC4(IV_1, k)
  \]

  \[
  C_1 \ xor \ C_2 = [P_1 \ xor \ RC4(IV_1, k)] \ xor \ [P_2 \ xor \ RC4(IV_1, k)] \\
  = P_1 \ xor \ P_2 \ xor \ RC4(IV_1, k) \ xor \ RC4(IV_1, k) \\
  = P_1 \ xor \ P_2
  \]

  \[\Rightarrow \text{ hence attackers knows Xor of two plaintexts}\]

  If attacker knows one pair $P_1, C_1$ (known plaintext attack), he can decrypt any frame that is encrypted with same IV value

Shared-Key Authentication (using WEP)

**Challenge:** random message $M$ (128 Byte)

**Response:** $<IV, M \ xor RC4(K, IV)>$, STA chooses value of IV
### Discussion: Shared-Key Authentication

- If Attacker listens to the authentication process he knows:
  - Un-encrypted Challenge M
  - Value of IV and corresponding cryptotext \( RC4(M,K) \) xor M

\[
\begin{array}{c}
K \ (40/104 \text{ Bit}) \\
IV \ (24 \text{ Bit}) \\
\end{array}
\]

\[
\begin{array}{c}
\text{RC4} \\
\text{S} \\
\text{C} \\
\text{IV} \\
\end{array}
\]

Consequence: Attacker knows random Bitstream \( S = RC4(M,K) \)
and can use that to
- Authenticate himself (for any challenge \( M' \))
- Encrypt correctly any message (however only with that specific IV)
- Decrypt messages sent with that IV

### Summary: WEP

**Advantages**
- Encryption of individual Frames, not sensitive to packet-loss/reordering
- Efficient encryption method (wrt. Processing time), pre-computation of RC4 bit-stream possible

**Drawbacks**
- Authentication is not secure
- Key-Management need to avoid repeated use of IV
- Integrity protection not secure

**Outlook:**
- Wireless Protected Access (WPA)
  - Authentication using EAP (Enhanced-Authentication-Protocol)
  - Encryption using TKIP(Temporal-Key-Integrity-Protocol)
- 802.11i standard
Content

Part I: Security (cntd. From MM2)
1. Security mechanisms in cellular networks
   • GSM: Authentication, Encryption/Integrity Protection
   • GPRS/UMTS: Authentication, Encryption/Integrity Protection
2. Security in WLAN 802.11
   • WLAN Overview
   • Authentication
   • Wired Equivalent Privacy (WEP)

Part II: Header Compression
3. Header Compression
   • Motivation, Basic Principles & Algorithms
   • Robustness
4. Summary/Exercises

Protocol Enhancements: Motivation

• Wireless links tend to show poor performance
  - Large delays
  - Low throughput
  - Bit errors / packet losses due to radio transmission
• Protocols in IP family not originally designed for such links
  - Increased volume due to headers
  - Deficiencies of TCP flow control
  - ... many more (e.g. applications HTTP→WAP)
• Protocol Enhancements are required, examples
  - Robust Header Compression (RoHC)
  - Enhancements for Wireless TCP
Header Compression (HC)

- Motivation
  - IP voice packets: header 40/60Bytes, average payload 25Bytes
  - TCP ACK packets: header 40/60 Bytes, payload often 0Bytes
- Data in many header fields …
  - … hardly ever changes e.g. source/destination address within same IP flow
  - … or changes in a regular pattern
- Idea: reduce header length by compression, e.g.
  - differential encoding of fields
  - and/or variations of Huffman compression
- Compression can be applied to several protocol headers, e.g. RTP/UDP/IP

Background: TCP Header

- Point-to-point, bi-directional connections (between end-systems)
- Reliable, in-order transport of byte–stream using
  - Sequence Numbers
  - Acknowlegements
- Flow/Congestion Control: Prevent flooding of
  - Receiver
  - Intermediate Systems

Selected Header Fields
- Sequence number: number of first data byte transmitted in the segment
- ACK number: number of next byte expected in the reverse data flow
- Window size: number of bytes host is willing to accept in reverse data flow
Background: UDP Header

- User Datagram Protocol UDP (RFC 768)
  - Connectionless
  - Unreliable
  - No flow/congestion control
- Functionalities
  - (De-)Multiplexing: Port Numbers
  - Simple additive checksum covering
    - UDP Header
    - UDP Payload
    - Pseudo IP Header
      - IP addresses & protocol type
      - Length of IP payload

UDP segment format

Real-Time Transport Protocol, RTP (RFC3550)

- Supports multi-party multimedia conferences
- Uses UDP and multicasting capabilities of IP
- Provides Time-stamps, sequence numbers
- Supports:
  - Codec description (in separate profile description, e.g. RFC3551)
  - synchronization
  - mixing & codec translation of multi-media streams
- Header

```
Ver P X CC M PTYPE Sequence Number
Timestamp
Synchronization Source Identifier
Contributing Source ID
...```

VERsion=2
P=Padding
X=Extension Header
CC=Source Count
M=Marker
PayloadTYPE
Header Structure: RTP/UDP/IP

Basic approach: HC and RoHC

Identify and reduce redundancy in header fields:
- **Intra-packet redundancy**: between header fields of the same packet (e.g. RTP/UDP/IP)
- **Inter-packet redundancy**: between header parts between different packets within a certain flow

Compression context (Base) required, when eliminating inter-packet redundancy
- Context transfer or re-establishment required in handover scenarios
- Packet loss/reordering can lead to de-synchronisation of compressor and decompressor → additional packet loss can result
- Additional methods for robustness introduced → RoHC
Classification of Header-Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Fixed</td>
</tr>
<tr>
<td>IP Header Length</td>
<td>Fixed</td>
</tr>
<tr>
<td>Type of service</td>
<td>Fixed</td>
</tr>
<tr>
<td>Total length</td>
<td>Inferred from Link layer</td>
</tr>
<tr>
<td>Identification</td>
<td>Fixed</td>
</tr>
<tr>
<td>Flags</td>
<td>Fixed</td>
</tr>
<tr>
<td>Fragment offset</td>
<td>Fixed</td>
</tr>
<tr>
<td>Time to Live</td>
<td>Fixed</td>
</tr>
<tr>
<td>Protocol</td>
<td>Fixed</td>
</tr>
<tr>
<td>Header checksum</td>
<td>Random</td>
</tr>
<tr>
<td>Source Address</td>
<td>Fixed</td>
</tr>
<tr>
<td>Destination address</td>
<td>Fixed</td>
</tr>
</tbody>
</table>

IP Header Variable

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>Fixed</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Fixed</td>
</tr>
<tr>
<td>Length</td>
<td>Inferred from Link layer</td>
</tr>
<tr>
<td>Check sum</td>
<td>Random</td>
</tr>
</tbody>
</table>

UDP Header Variable

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Fixed</td>
</tr>
<tr>
<td>Padding (P)</td>
<td>*</td>
</tr>
<tr>
<td>Extension (E)</td>
<td>*</td>
</tr>
<tr>
<td>CSRC Count (CC)</td>
<td>*</td>
</tr>
<tr>
<td>Marker</td>
<td>Random</td>
</tr>
<tr>
<td>Payload Type</td>
<td>Fixed</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>Delta</td>
</tr>
<tr>
<td>Time stamp</td>
<td>Delta</td>
</tr>
<tr>
<td>SSRC</td>
<td>Fixed</td>
</tr>
<tr>
<td>CSRC</td>
<td>*</td>
</tr>
</tbody>
</table>

RTP Header Variable

Different Header Compression schemes

- Compressed TCP – Van Jacobsen RFC 1144
  - only for TCP/IP
  - for wired networks
- Perkins
  - improvement of CTCP
- IPHC [RFC 2507]
  - only for IP
  - no feedback
- RFC2508
General Structure of Header Compressors

- Two entities: compressor and decompressor
- Compressor sends initial base
- Base is used by compressor and decompressor
- Compressor removes redundancy
- Decompressor adds removed information
- Proposed solution differ in a possible feedback channel

Robustness: Perkins’ scheme

- Robustness introduced by periodically repetition of full base information each N packets
- N packets define a frame
- All packets refer to the first packet of the frame
- Less compression due to higher delta values
Robust Header Compression (RFC3095)

- RTP/UDP/IP
- UDP/IP
- IP
- Uncompressed
- Current RoHC methods: 40 Bytes RTP/UDP/IP header \(\rightarrow\) on average 1 or 2 bytes

ROHC Modes

- Unidirectional (U) mode
- Optimistic (O) mode
- Reliable (R) mode

Feedback(O) Feedback(U) Feedback(R) Feedback(L)
**States of Compressor and Decompressor**

![Diagram showing the states of a compressor and decompressor: IR State, FO State, SO State, No Context, Static Context, Full Context.]

**Unidirectional**

![Diagram showing the unidirectional states: IR State, FO State, SO State, with transitions labeled as optimistic, timeout, and timeout/update.]

Wireless Networks II: Lecture 3, Spring05

Page 49

Hans Peter Schwefel
Decompressor

RoHC: Ongoing Work

- Application of RoHC methods for SIP compression
  - Compression of whole SIP messages
  - Goal: Reduction of call-setup delay
    (SIP message up to several thousand byte)

- Optimized use of Compression
  Trade-off: Data-Volume vs. Error Robustness on
  - Application Layer
  - RoHC Layer
  - Link-Layer
  → Optimization across whole protocol stack required
Summary

Part I: Security (cntd. From MM2)
1. Security mechanisms in cellular networks
   • GSM: Authentication, Encryption/Integrity Protection
   • GPRS/UMTS: Authentication, Encryption/Integrity Protection
2. Security in WLAN 802.11
   • WLAN Overview
   • Authentication
   • Wired Equivalent Privacy (WEP)

Part II: Header Compression
3. Header Compression
   • Motivation, Basic Principles & Algorithms
   • Robustness
4. Summary/Exercises

Exercises

A VoIP stream shows an average (RTP) payload of 40Bytes which is transported using RTP/UDP/IPv4 from one slave to another slave within a BT piconet using DH1 packets (1 slot, payload max 27 Bytes). The average inter-packet time is 20ms.

1. Compute the average utilization (fraction of used-timeslots) due to this VoIP stream, without header compression and when header compression is applied. Assume that header compression reduces the average header-length to 4 bytes (and use averages for your computation).

2. The BT link shows a bit-error rate (after utilizing FEC) of 1e-5. Assume independent errors. A simple RoHC mechanism is used that transmits first K full headers, and then (N-K) fully compressed headers (of assumed length 4 bytes). This sequence of N packets, called ‘cycle’, repeats afterwards. The decompressor is able to correctly reconstruct the full header from the compressed header of packet i, i>K, in the cycle if:
   • At least one of the K full headers at the beginning of the cycle was received correctly, AND
   • All fully compressed headers before packet i in the cycle were received correctly.

   For the following calculations, details of the access technology (BT) should not be considered.
   a) Compute and plot the average packet length of the compression mechanism, APL(N,K).
   b) Compute the probabilities, p_full and p_comp, that a full respectively compressed header is corrupted during transmission.
   c) Compute the probability p(i), that one of the K full headers in the beginning of the cycle was received correctly AND the i-th packet (i>K) is the first corrupted compressed header in the cycle.
   d) Compute the ‘additional packet loss’, APL, caused by correctly received compressed headers while incorrect base.
References: HC, RoHC

2. Casner & Jacobson, Compression IP/UDP/RTP Headers for Low-Speed Serial Links, RFC2508, Feb 1999
4. C.Bormann, et.al., Robust Header Compression (ROHC), RFC3095, July 2001

Acknowledgements

Security Part
• Lecture notes: Mobile Communications, Jochen Schiller, www.jochenschiller.de
• Student work (all TU Munich)
  – Alexander Schuster (Seminar)
  – Pascal Frantz (Seminar)
  – Michael Wolfgang (Seminar)
  – Mikhail Ryss (Seminar)
• Slide-Sets: Siemens ICM N, Siemens CT IC 3, UMTS Security
• Guenther Horn, Dirk Kroeselberg, Bernhard Petri, Siemens CT, ICM N

Header Compression:
• Lecture Slides: Wireless Systems, F. Fitzek (while at Uni Ferrara)