Institute of Operating Systems
and Computer Networks

Technische
Universität
Braunschweig

Secure communication based on noisy input data

Feature extraction from audio contexts

Stephan Sigg

May 17, 2011

Overview and Structure

- Classification methods
- Feature extraction
  - Features from audio
  - Features from RF
- Fuzzy Commitment
- Fuzzy Extractors
- Authentication with noisy data
- Error correcting codes
- Entropy
- Physically unclonable functions

Outline

Aspects of the mobile radio channel

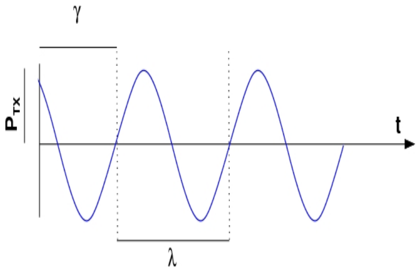
RF transmission

- Electromagnetic signals
- Transmitted in wave-Form
- Omnidirectional transmission
- Speed of light
  - $c = 3 \cdot 10^8 \frac{m}{s}$

Aspects of the mobile radio channel

RF signal

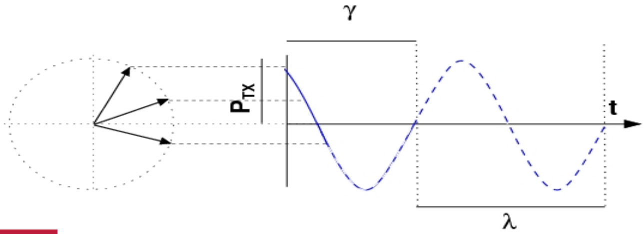
- Transmission power:
  - $P_{TX}[W]$
- Frequency:
  - $f[\frac{1}{sec}]$
- Phase offset:
  - $\gamma[\pi]$
- Wavelength:
  - $\lambda = \frac{c}{f}[m]$



Aspects of the mobile radio channel

RF signal

- Real part of rotating vector
  - $\zeta = \Re\left(e^{j(ft+\gamma)}\right)$
- Instantaneous signal strength:
  - $\cos(\zeta)$
- Rotation Speed: Frequency f



Aspects of the mobile radio channel

Noise

- In every realistic setting, noise can be observed on the wireless channel
- Typical noise power:[1]

$$P_N = -103dBm$$

- Value observed by measurements

[1] 3GPP: 3rd generation partnership project; technical specification group radio access networks; 3g home nodeb study it... t (release 8). Technical Report 3GPP TR 25.820 V8.0.0 (2008-03) (March)

Aspects of the mobile radio channel

Noise

- Thermal noise can also be estimated analytically as

$$P_N = \kappa \cdot T \cdot B$$

- $\kappa = 1.3807 \cdot 10^{-23} \frac{J}{K}$: Boltzmann constant
- T: Temperature in Calvin
- B: Bandwidth of the signal.

Aspects of the mobile radio channel

Example

- GSM system with 200kHz bands
- Average temperature: 300K
- Estimated noise power:

$$\begin{aligned} P_N &= \kappa \cdot T \cdot B \\ &= 1.3807 \cdot 10^{-23} \frac{J}{K} \cdot 300K \cdot 200kHz \\ P_N &= -120.82dBm \end{aligned}$$

Aspects of the mobile radio channel

Path-loss

- Signal strength decreases while propagating over a wireless channel
- Order of decay varies in different environments
- Impact higher for higher frequencies
- Can be reduced by antenna gain (e.g. directed)

Location	Mean Path loss exponent	Shadowing variance σ^2 (dB)
Apartment Hallway	2.0	8.0
Parking structure	3.0	7.9
One-sided corridor	1.9	8.0
One-sided patio	3.2	3.7
Concrete Canyon	2.7	10.2
Plant fence	4.9	9.4
Small boulders	3.5	12.8
Sandy flat beach	4.2	4.0
Dense bamboo	5.0	11.6
Dry tall underbrush	3.6	8.4

Aspects of the mobile radio channel

Path-loss

- For analytic consideration: Path-loss approximated
- Friis free-space equation:

$$P_{TX} \cdot \left(\frac{\lambda}{2\pi d}\right)^2 \cdot G_{TX} \cdot G_{RX}$$

Aspects of the mobile radio channel

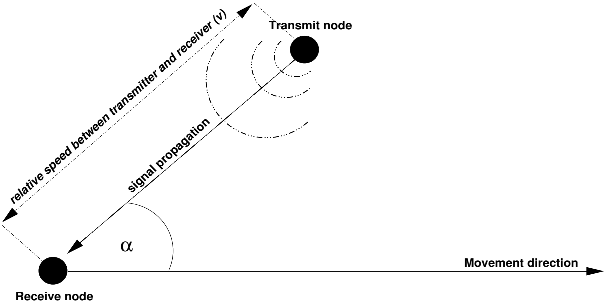
Path-loss

$$P_{RX} = P_{TX} \cdot \left(\frac{\lambda}{2\pi d}\right)^2 \cdot G_{TX} \cdot G_{RX}$$

- Utilised in outdoor scenarios
  - Direct line of sight
  - No multipath propagation
- d impacts the RSS quadratically
- Other values for the path-loss exponent α possible.
- Path-loss:

$$PL^{FS}(\zeta_i) = \frac{P_{TX}(\zeta_i)}{P_{RX}(\zeta_i)}$$

Aspects of the mobile radio channel



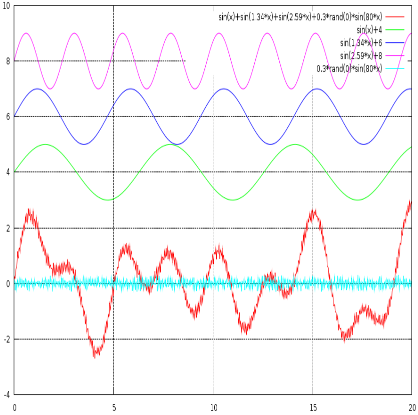
Doppler Shift

- Frequency of a received signal may differ to the frequency of the transmitted signal
- Dependent on relative speed between transmitter and receiver
- $f_d = \frac{v}{\lambda} \cdot \cos(\alpha)$

Aspects of the mobile radio channel

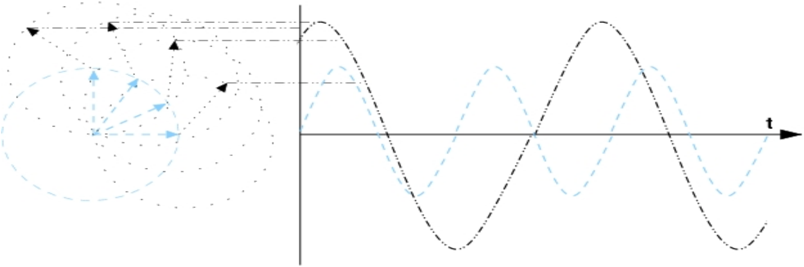
Superimposition of RF signals

- The wireless medium is a broadcast channel
- Multipath transmission
  - Reflection
  - Diffraction
  - Different path lengths
  - Signal components arrive at different times
- Interference



$$\zeta_{\text{sum}} = \sum_{i=1}^{\iota} \Re\left(e^{j(f_i t + \gamma_i)}\right)$$

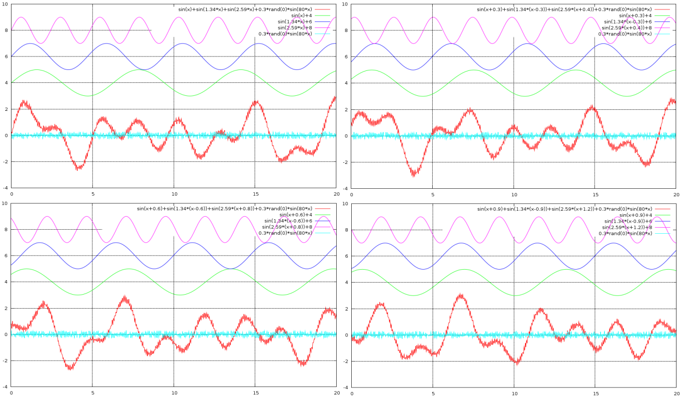
Aspects of the mobile radio channel



Superimposition of RF signals

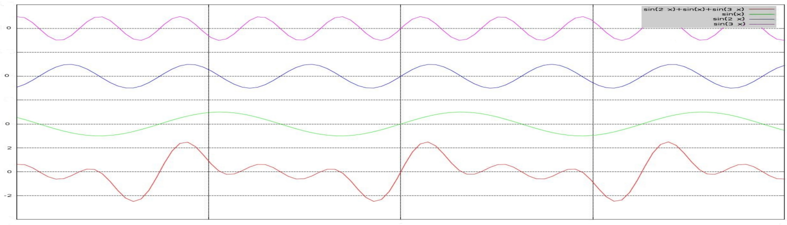
- At a receiver, all incoming signals add up to one superimposed sum signal
- Constructive and destructive interference
- Normally: Heavily distorted sum signal

Aspects of the mobile radio channel



- Channel conditions are dependent on time and location
- Independent channel conditions typically expected in a distance of $\frac{\lambda}{2}$

Aspects of the mobile radio channel



Interference

- Signal components arrive from more than one transmitter
- Neighbouring nodes generate interference:

$$\zeta_{\text{sum}} = \sum_{i=1}^{\iota} \Re\left(e^{j(f_i t + \gamma_i)}\right)$$

Aspects of the mobile radio channel

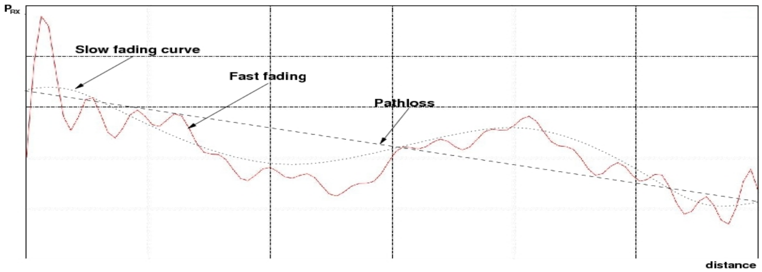
Interference

- A radio system typically requires a specific minimum signal power over interference and noise level:

$$SINR = \frac{P_{\text{signal}}}{P_{\text{noise}} + P_{\text{interference}}}$$

- Concepts to reduce interference:
  - Clustering (cellular networks)
  - Spread spectrum techniques (Code divisioning)

Aspects of the mobile radio channel



Fading

- Signal quality fluctuating with location and time
- Slow fading
- Fast fading

Aspects of the mobile radio channel

Slow fading

- Result of environmental changes
- Temporary blocking of signal paths
- Changing reflection angles
- Movement in the environment
  - Trees
  - Cars
  - Opening/closing doors
- Amplitude changes can be modelled by log-normal distribution

Aspects of the mobile radio channel

Fast fading

- Signal components of multiple paths
- Cancellation of signal components
- Fading incursions expected in the distance of $\frac{\lambda}{2}$
- Channel quality changes drastically over short distances
- Example: Low radio reception of a car standing in front of a headlight is corrected by small movement
- Stochastic models are utilised to model the probability of fading incursions
  - Rice
  - Rayleigh

Aspects of the mobile radio channel

Fast fading

- Fast fading weakened when direct signal component observed

- Density of amplitude distribution modelled by Rice distribution:

$$f(A) = \frac{A}{\sigma^2} e^{-\frac{A^2+s^2}{2\sigma^2}} I_0\left(\frac{As}{\sigma^2}\right)$$

- s: Dominant component of received signal
- σ: Standard deviation
- Modified Bessel function with order 0:

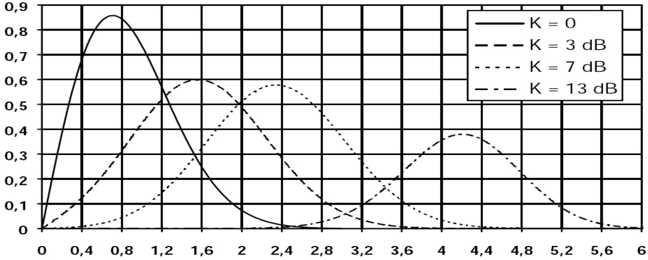
$$I_0(x) = \frac{1}{2\pi} \int_0^{2\pi} e^{x\cos(\Psi)} d\Psi$$

Aspects of the mobile radio channel

- Ricean factor:

$$K = \frac{s^2}{2\sigma^2}$$

  - Impacts probability density function of Rice distribution
  - Most probable outcome impacted

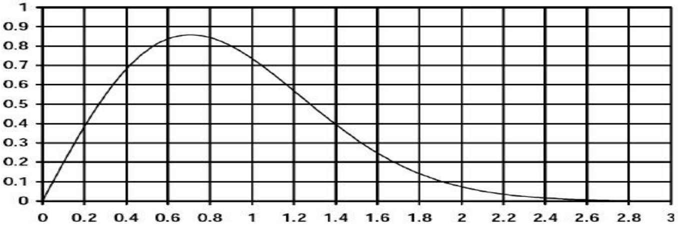


Aspects of the mobile radio channel

- For $K = 0$, Rice distribution migrates to Rayleigh distribution:

$$
\begin{aligned}
\lim_{K\to 0} f(A) &= \lim_{K\to 0} \frac{A}{\sigma^2} e^{-\frac{A^2}{2\sigma^2}-K} I_0\left(\frac{A\sqrt{2K}}{\sigma}\right) \\
&= \lim_{K\to 0} \frac{A}{\sigma^2} e^{-\frac{A^2}{2\sigma^2}-K} \frac{1}{2\pi} \int_0^{2\pi} e^{\frac{A\sqrt{2K}}{\sigma}\cos(\Psi)} d\Psi \\
&= \frac{A}{\sigma^2} e^{-\frac{A^2}{2\sigma^2}-0} \frac{1}{2\pi} \int_0^{2\pi} e^{\frac{A\sqrt{2\cdot 0}}{\sigma}\cos(\Psi)} d\Psi \\
&= \frac{A}{\sigma^2} e^{-\frac{A^2}{2\sigma^2}}
\end{aligned}
$$

Aspects of the mobile radio channel



Rayleigh distribution

- Probability density function of received sum signal for $n \gg 1$
- Assumption:
  - No direct signal component exists
  - Received signal components of approximately equal strength
- Example: Urban scenarios with dense house blocks

Aspects of the mobile radio channel

- With large K, Rice distribution evolves to Gauss distr.:

$$
\begin{aligned}
I_0(x) \quad & \rightarrow_{x\gg 1}\rightarrow \quad \frac{e^x}{\sqrt{2\pi}} \\
\Rightarrow f(A) \quad & \rightarrow_{x\gg 1}\rightarrow \quad \frac{A}{\sigma^2} e^{-\frac{A^2}{2\sigma^2}-K} \frac{e^{\frac{A\sqrt{2K}}{\sigma}}}{\sqrt{2\pi\frac{A\sqrt{2K}}{\sigma}}} \\
f(A) \quad & = \quad \frac{A}{\sigma^2\sqrt{\frac{2\pi}{\sigma}}\sqrt{A\sqrt{2K}}} e^{-\frac{A^2}{2\sigma^2}-\frac{s^2}{2\sigma^2}} e^{\frac{A\sqrt{2K}}{\sigma}} \\
& = \quad \frac{A}{\sigma^2\sqrt{\frac{2\pi}{\sigma}}\sqrt{A\sqrt{2K}}} e^{-\frac{A^2+s^2-2As}{2\sigma^2}} \\
& = \quad \sqrt{\frac{A}{s}} \frac{1}{\sigma 2\pi} e^{-\frac{1}{2}\left(\frac{A-s}{\sigma}\right)^2}
\end{aligned}
$$

Aspects of the mobile radio channel

- The term

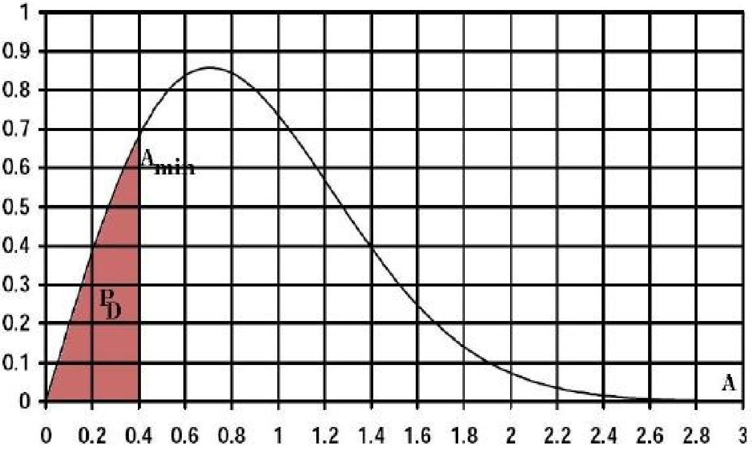
$$\sqrt{\frac{A}{s}}\frac{1}{\sigma 2\pi}e^{-\frac{1}{2}\left(\frac{A-s}{\sigma}\right)^2}$$

- differs from the Gauss distribution in $\sqrt{\frac{A}{s}}$:

$$f_{Gauss}(x) = \frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{1}{2}\left(\frac{A-s}{\sigma}\right)^2}$$

- With $\sqrt{\frac{A}{s}} \approx 1$, Rice distribution can be approximated by Gauss distribution

Aspects of the mobile radio channel



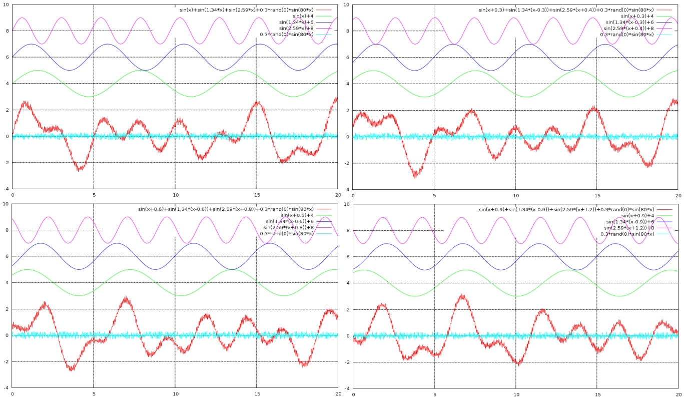
Aspects of the mobile radio channel

Simulation of frequency selective channels

- After signal transmission, the signal contour can be heavily distorted
  - Intersymbol interference
  - Fading
  - Interference
  - Noise
- In order to improve the signal reception, further signal processing is required

Aspects of the mobile radio channel

Simulation of frequency selective channels



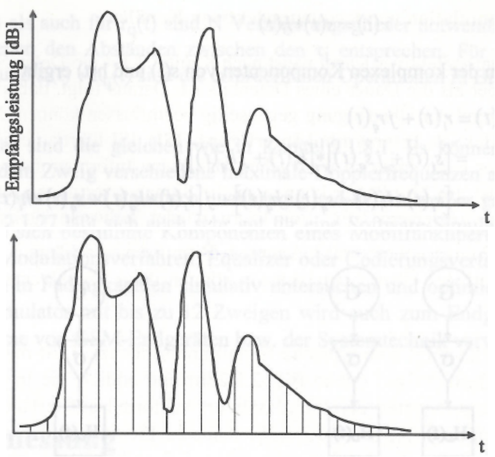
Aspects of the mobile radio channel

Simulation of frequency selective channels

- A common approach is to estimate he channel impulse response during a known training bit-sequence
- When the channel impulse response is known, signal distortions can be corrected
  - When the time axis is divided in discrete parts
  - We can derive discrete impulses for the energy in each of these parts

Aspects of the mobile radio channel

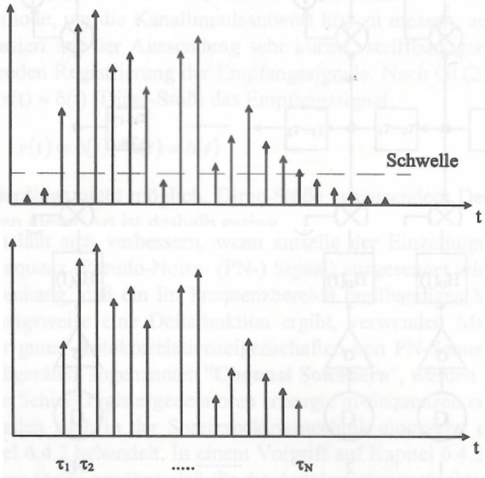
Simulation of frequency selective channels[2]



[2] ...er, Digitale Mobilfunksysteme, Teubner, 1996

Aspects of the mobile radio channel

Simulation of frequency selective channels



Aspects of the mobile radio channel

Simulation of frequency selective channels

- Each component of the impulse response possesses a phase ϕ_i and a value a_i
- The impulse response in the complex basis band is defined as

$$h(t) = \sum_{i=1}^{N} a_i e^{j\phi_i} \delta(t - \tau_i) = h_i(t) + jh_q(t)$$

- The complex components are

$$h_i(t) = \sum_{i=1}^{N} a_i \cos \phi_i \delta(t - \tau_i)$$

$$h_q(t) = \sum_{i=1}^{N} a_i \sin \phi_i \delta(t - \tau_i)$$

Aspects of the mobile radio channel

Simulation of frequency selective channels

- The received signal $r(t)$ is described as

$$r(t) = s(t) \cdot h(t)$$

- By considering the complex components also, we obtain

$$\begin{aligned}
r(t) &= r_i(t) + jr_q(t) \\
&= [s_i(t) + js_q(t)] \cdot [h_i(t) + jh_q(t)] \\
&= [s_i(t) \cdot h_i(t) - s_q(t) \cdot h_q(t)] + j\left[s_(t) \cdot h_q(t) + s_q(t) \cdot h_i(t)\right]
\end{aligned}$$

Aspects of the mobile radio channel

Channel estimation

- The easiest approach to estimate $h(t)$ works in the time domain
- Based on sending very short impulses
- And registering the received signals
- The approach can be improved by utilising a pseudo-noise sequence instead of single identical impulses
- The inverse of the estimated impulse response is correlated $\overline{h(t)^{-1}}$ with the received signal:

$$r(t) \cdot \overline{h(t)^{-1}} = s(t) \cdot h(t) \cdot \overline{h(t)^{-1}} \approx s(t)$$

Outline

Features of the RF channel

Features specific for the RF-channel

- Wlan Access points
- Signal Strength
- Signal to noise ratio
- Fluctuation in signal strength
- Energy on several frequency bands
- Active Bluetooth devices
- GSM base stations/GSM active set
- ...

Outline

Properties of the RF channel

Secure communication based on RF-channel information

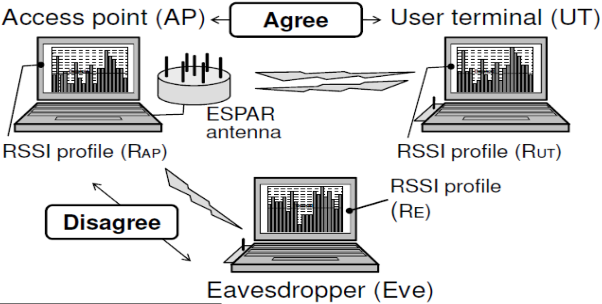
- The communication channel for a communication among two nodes is spatially sharp concentrated[3]
- This channel symmetry can be exploited to derive secure keys among two devices

[3] Smith, A direct derivation of a single-antenna reciprocity relation for the time domain, IEEE Transactions on A[illegible]gation, Vol. 52, no. 6, 2004.

Features of the RF channel

Secure communication based on RSSI measurements[4] [5]

- Utilisation of a variable directional antenna (ESPAR)
  - Increases the fluctuation of channel characteristics based on relative location



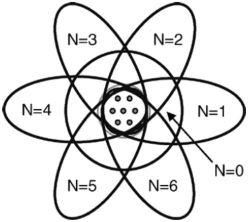
[4] Yasukawa, Iwai, Sasaoka, A secret key agreement scheme with multi-level quantisation and parity check using fluctuation of radio channel property, ISIT, 2008

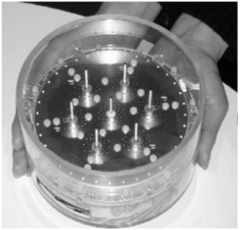
[5] Aono, Higuchi, Ohira, Komiyama, Sasaoka, Wireless secret key generation exploiting reactance-domain scalar ... fading channels, IEEE Transactions on Antennas and Propagation, Vol. 53, No. 11, 2005.

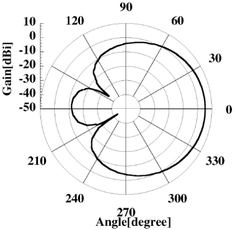
Features of the RF channel

Secure communication based on RSSI measurements

- Utilisation of a variable directional antenna (ESPAR)
  - Variable-directional array antenna
  - Single central active radiator
  - parasitic elements loaded with variable reactors
  - By altering the dc voltage to varactor diodes in the parasitic elements, antenna beam can be formed



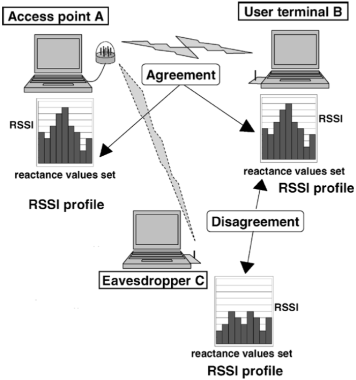




Features of the RF channel

Secure communication based on RSSI measurements

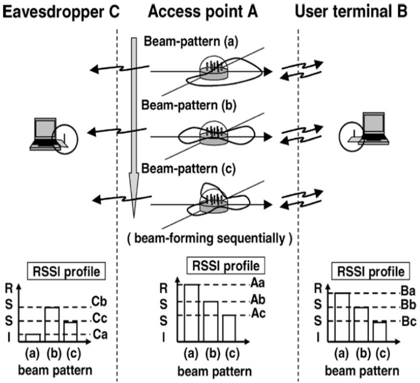
- Secret-key generation and agreement principle
  - Repeated transmission of beam patterns
  - Due to the ESPAR antenna, channel characteristics to spatially separated nodes differ
  - Binary keys are created from the RSSI-sequence according to a threshold value



Features of the RF channel

Secure communication based on RSSI measurements

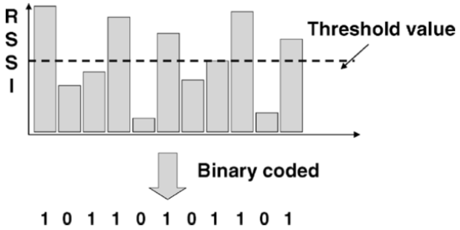
- Secret-key generation and agreement principle
  - Repeated transmission of beam patterns
  - Due to the ESPAR antenna, channel characteristics to spatially separated nodes differ
  - Binary keys are created from the RSSI-sequence according to a threshold value



Features of the RF channel

Secure communication based on RSSI measurements

- Secret-key generation and agreement principle
  - Repeated transmission of beam patterns
  - Due to the ESPAR antenna, channel characteristics to spatially separated nodes differ
  - Binary keys are created from the RSSI-sequence according to a threshold value



Features of the RF channel

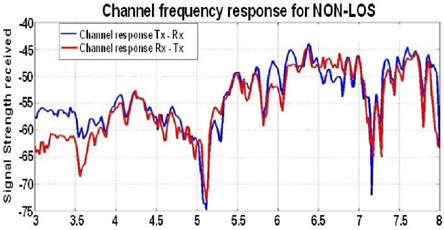
Secure communication based on RSSI measurements

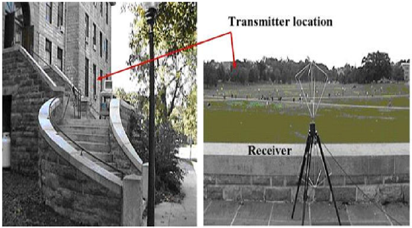
- Discussion
  - Special antenna required to increase spatial fluctuation of channel characteristics
  - Security measure dependent on channel fluctuations

Features of the RF channel

Secure communication based on deep fades in the SNR[6]

- Communication partners agree on a threshold value
- Bot nodes transmit repeatedly and alternately
- Channel characteristics are transformed to bit sequence
  - Signal envelope below threshold in timeslot: 1, else 0
- No specialised hardware required
  - Only threshold detectors which are already present in transceivers



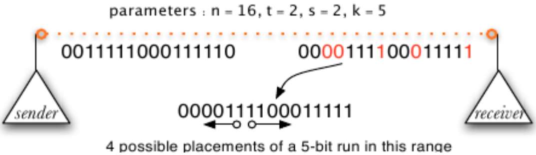


[6] Azimi-Sadjadi, Kiayias, Mercado, Yener, Robust Key Generation from Signal Envelopes in Wireless Networks, CCS,

Features of the RF channel

Secure communication based on deep fades in the SNR

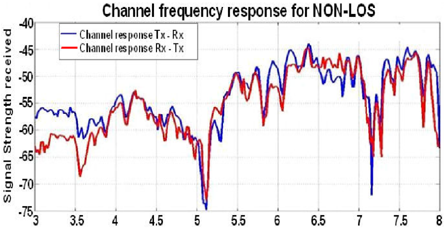
- Key generation
  1. Sender and receiver sample bit sequences
  2. Sender transmits key verification information to receiver
  3. Receiver decides on correct key by scanning through all possible error vectors



Features of the RF channel

Secure communication based on deep fades in the SNR

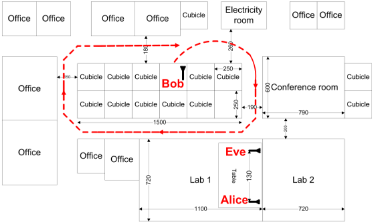
- Discussion
  1. Computationally cheap approach
  2. No special hardware required
  3. Probably uneven distribution of 0 and 1 (Dependent on Channel characteristics and time slot)
  4. Key generation in the presence of noise not optimal

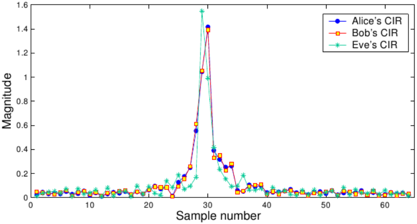


Features of the RF channel

Secure communication based on the CIR[7] [8]

- Utilise Channel impulse response as secure secret
  - Utilise magnitude of CIR pain peak
  - Transformed to binary sequence via Threshold
  - Error correction method required in order to account for noise in the binary sequences



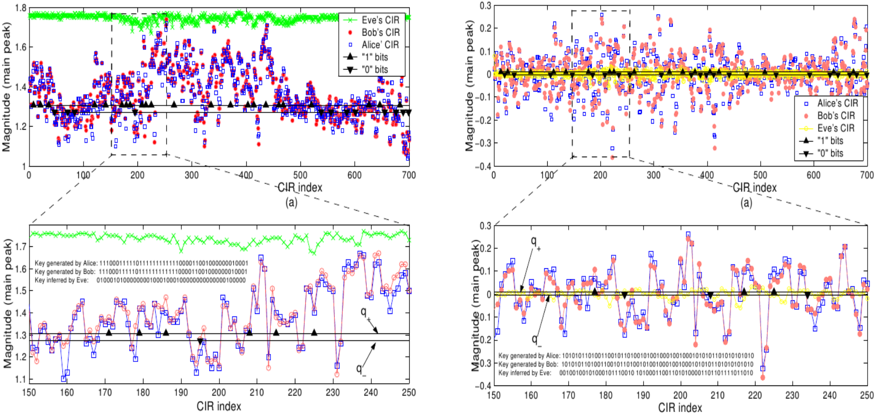


[7] Mathur, Trappe, Mandayam, Ye, Reznik, Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel, MobiCom, 2008

[8] Tmar, Hamida, Pierrot, Castelluccia, An adaptive quantisation algorithm for secret key generation using radio ...nts, NTMS, 2009

Features of the RF channel

Secure communication based on the CIR



Outline

Questions?

Stephan Sigg
sigg@ibr.cs.tu-bs.de

Literature

- C.M. Bishop: Pattern recognition and machine learning, Springer, 2007.
- P. Tulys, B. Skoric, T. Kevenaar: Security with Noisy Data – On private biometrics, secure key storage and anti-counterfeiting, Springer, 2007.
- R.O. Duda, P.E. Hart, D.G. Stork: Pattern Classification, Wiley, 2001.