Methoden zum Schutz von Verkehrsdaten in Funknetzen

Problembeschreibung

Peilung und Ortung in Funknetzen

Das „Direct Sequence Spread Spectrum“ Sendeverfahren

Erzeugen der PN-Codesequenz (Schlüsselaustausch)

Bewertung

Entspreizung an vertrauenswürdiger Stelle

Informationstechnische Kapselung der BTS

Zusammenfassung

Hannes Federrath
Jürgen Thees

Technische Universität Dresden
Institut für Theoretische Informatik
01062 Dresden

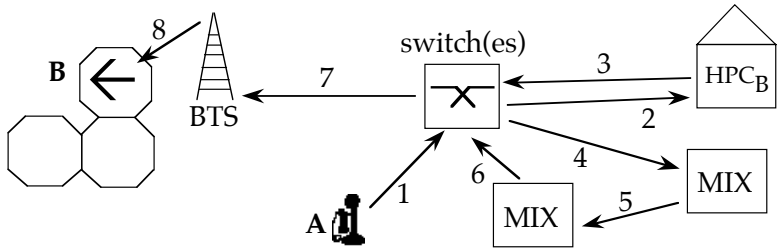
Problembeschreibung

Ziel:

- **Erstellungsmöglichkeit von Bewegungsprofilen in zellularen Mobilfunknetzen verhindern**
- **Schutz des Aufenthaltsortes eines Funkteilnehmers als Teil des Schutzziels Vertraulichkeit**

Voraussetzung:

- **Vertrauenswürdige Speicherung (notwendiger) Lokalisierungsinformation**



Betrachtungsgegenstand:

- **Physikalisch bedingte Peil- und Ortbarkeit von Mobilfunkstationen verhindern oder erschweren**
  - **Funktechnische**
  - **Informationstechnische**

Peilung und Ortung in Funknetzen

Wie Peilung elektromagnetischer Wellen erschweren?

Ausnutzen von Störungen:

- **Inhomogenitäten und Diskontinuitäten im Ausbreitungsmedium**
- **Überlagerungen von Wellen**
- **Rauschen**

Ansatz:

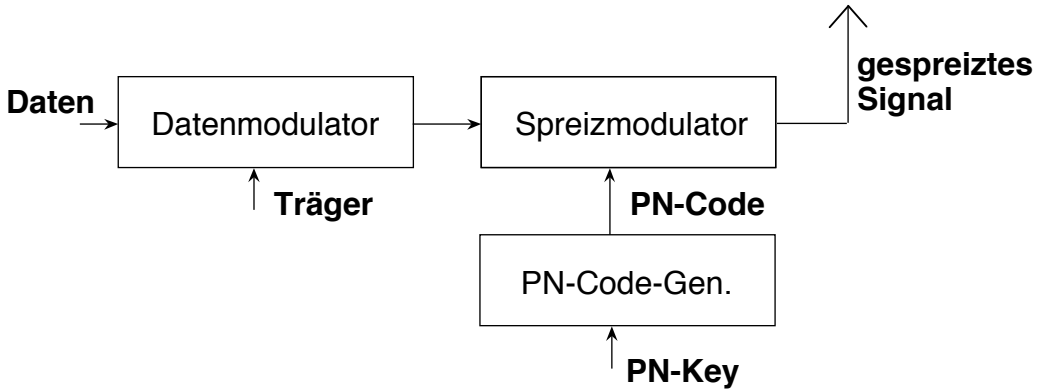
- **Modulationsverfahren verteilt die Signalenergie so breit, daß sie wesentlich kleiner als die Rauschleistungsdichte ist**

Spread Spectrum Systems:

- **Frequency Hopping Spread Spectrum**
- **Direct Sequence Spread Spectrum (DS/SS)**

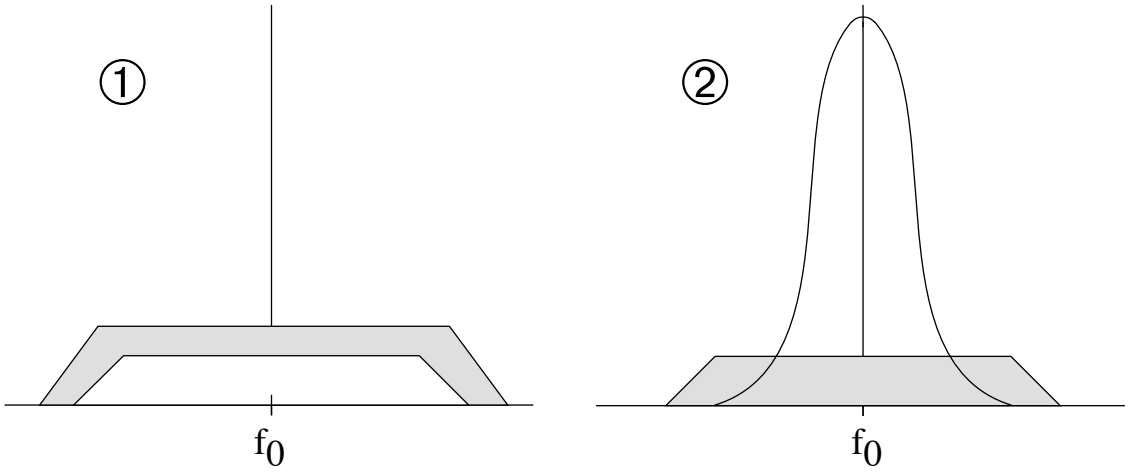
Das „Direct Sequence Spread Spectrum“ Sendeverfahren

Kontinuierliche Verteilung der Signalleistungsdichte auf ein Spektrum:



- **Spreizfaktor**
- **Pseudo-Noise-Codesequenz**
- **PN-Key zur Erzeugung der PN-Codesequenz**
- **Orthogonale Codes zur Mehrfachnutzung des Spektrums**

Einfluß von Störungen:



Nutzsignal

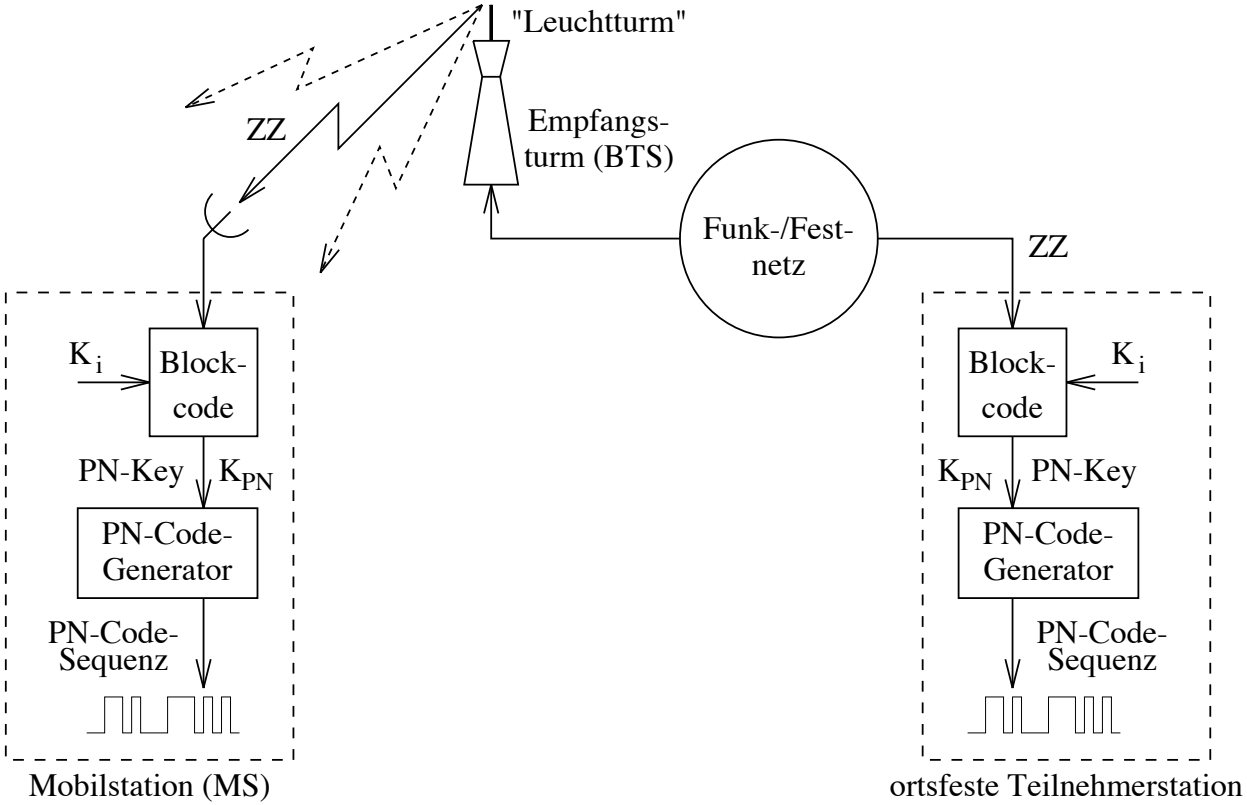
Störung

① **Empfangenes Signal mit breitbandiger Störung**

② **Signal nach Rücknahme der Spreizung**

Erzeugen der PN-Codesequenz (Schlüsselaustausch)

Gespreizte Verbindungsaufnahme...



bei mobile terminated call

- **Unnötig, da Standorte der BTS gewöhnlich bekannt**

bei mobile originated call

- **MS sollte möglichst immer gespreizt senden**
- **PN-Codesequenz bei Sender und Empfänger nötig**
- **Wie PN-Codesequenz erzeugen?**
  - **per Leuchtturm ZZ verteilen**
  - **Zeitbasis verwenden**

Bewertung

Sicherheitsbetrachtung:

- **Jeder, der PN-Code besitzt, kann peilen und orten**

→ **PN-Codesequenz muß vertraulich sein**

→ **PN-Codesequenz muß nach kryptographischen Gesichtspunkten gebildet werden**

Bewertung aus Sicht mehrseitiger Sicherheit:

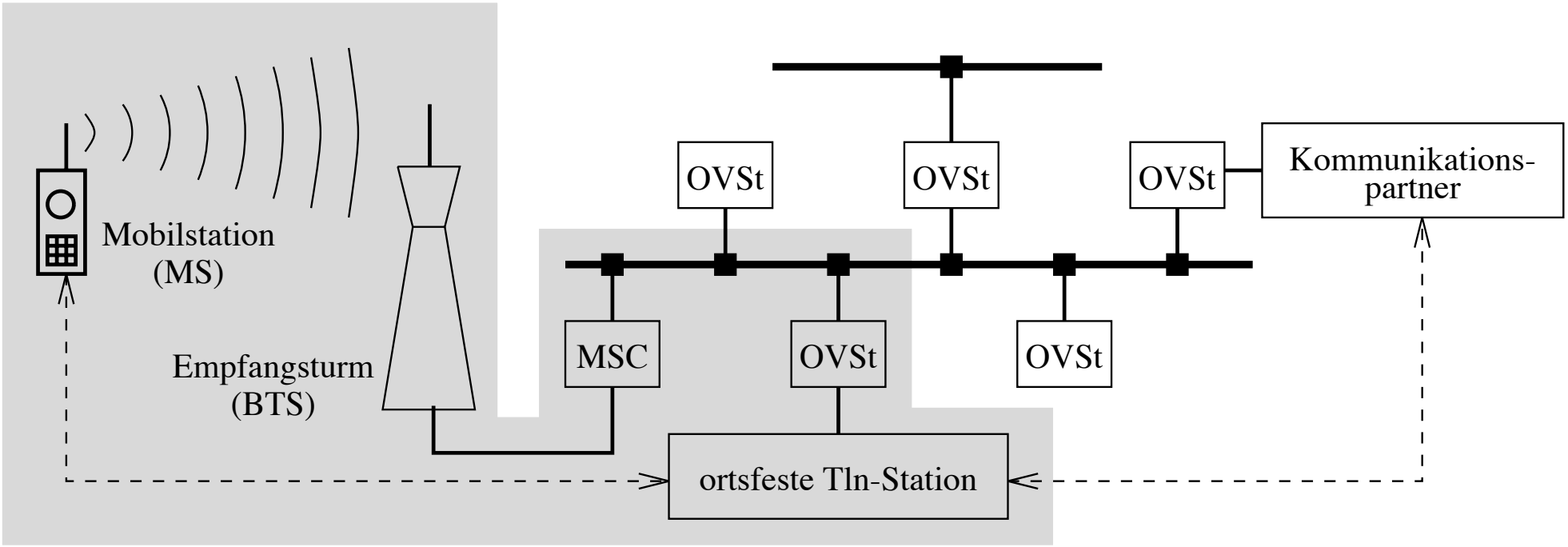
- **Schutz vor Outsidern des Kommunikationsnetzes → erfüllt**
- **Schutz vor Insidern → *nicht* erfüllt**

Konsequenz: weitere Maßnahmen notwendig — Vorschläge:

1. **Entspreizung an vertrauenswürdiger Stelle (ortsfeste Heimstation, Home Personal Computer HPC)**
2. **Entspreizung in informationstechnisch gekapselter Base Transceiver Station (BTS)**

1. Möglichkeit: Entspreizung an vertrauenswürdiger Stelle

- **Sehr hoher Bandbreitebedarf im Festnetz, insbesondere im Teilnehmeranschlußbereich**
- **Bei Vermittlung: Schutz der Kommunikationsbeziehung zwischen BTS und HPC nötig**



mit PN-Code geschützter(gespreizter) Bereich

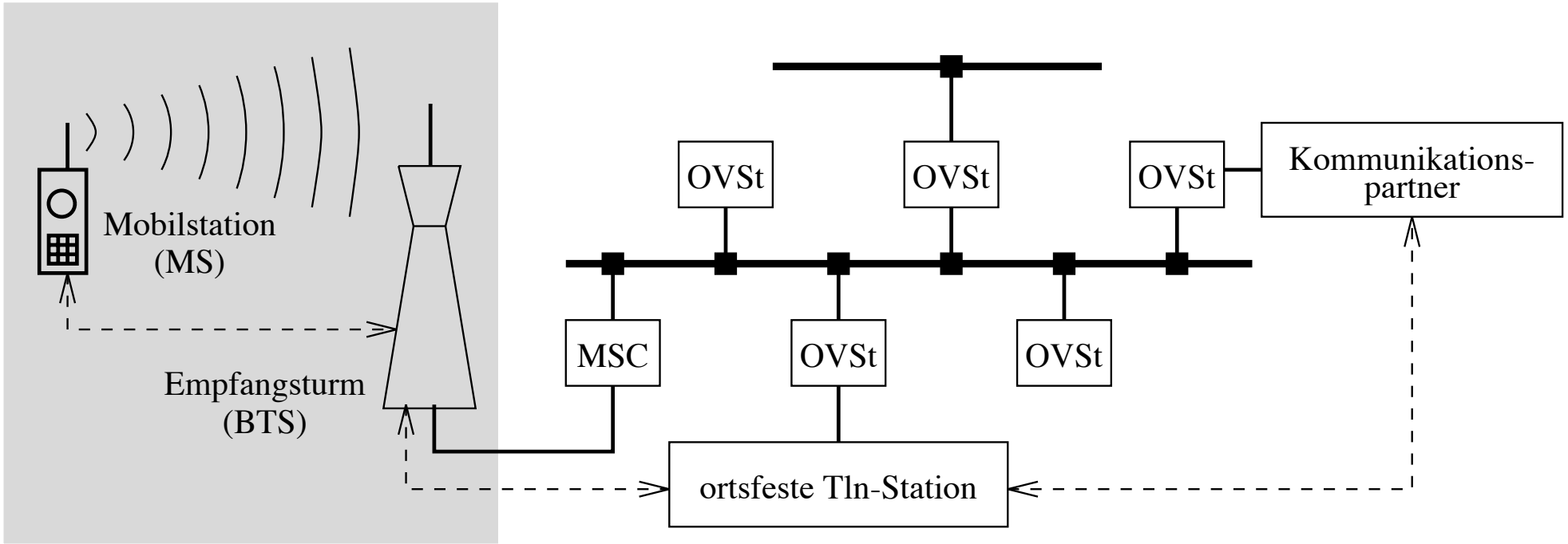
Informationsfluß

MSC Mobilvermittlungsstelle

OVSt Ortsvermittlungsstelle

2. Möglichkeit: Informationstechnische Kapselung der BTS

- **BTS aus sicherheitstechnischer Sicht vertrauenswürdig konstruieren**
- **Schutz der Kommunikationsbeziehung zwischen BTS und HPC nötig**



mit PN-Code geschützter(gespreizter) Bereich

Informationsfluß

MSC Mobilvermittlungsstelle

OVSt Ortsvermittlungsstelle

Zusammenfassung

Verhindern der Ortung von sendenden Mobilunkstationen

- **Mit DS/SS und weiteren informationstechnischen Maßnahmen erreichbar**
- **Gute Selbstortungsmöglichkeit (durch ortsfeste Station) – z.B. im Notfall**

Realisierbarkeitsprobleme:

- **Auf bisherigen GSM-basierten Netzen Modifikation der Multiplexgestaltung der Funkkanäle nötig**
- **Entspreizung in ortsfester Station setzt heute noch nicht überall vorhandene Festnetzinfrastruktur voraus (Breitbandverkabelung im Teilnehmeranschlußbereich)**

Weitere Effizienzsteigerungsmöglichkeit: Ungespreiztes Senden

- **Wann ungespreizt senden, um Aufwand zur Schlüsselverteilung zu verringern? (z.B. Einbuchen, Call Setup)**
- **Evtl. jedoch wieder neue Angriffsmöglichkeiten**