Sicherheit in Ad-hoc-Netzen

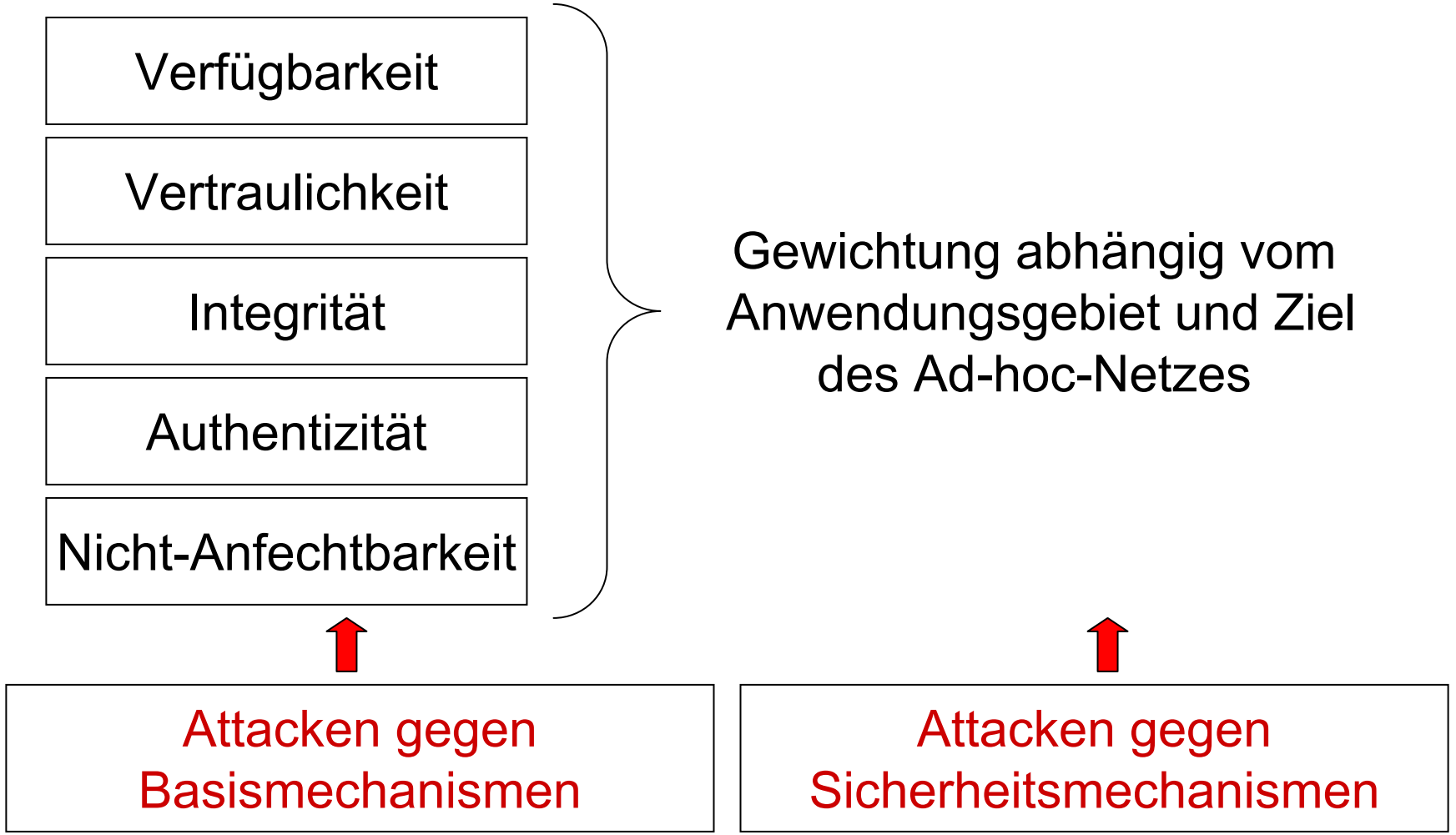
KM-/VS-Seminar

Wintersemester 2002/2003

Betreuer: Stefan Schmidt

TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.ibr.cs.tu-bs.de http://www.ibr.cs.tu-bs.de

Sicherheitsprobleme



Attacken gegen Sicherheitsmechanismen

- Diebstahl
- Interferenzen
  - Lauschen
  - aktives Senden von Störsignalen
- Medienzugriff (MAC)
  - Nichteinhaltung der Richtlinien
- Routing
  - node selfishness
  - Publikation falscher Routinginformationen

Attacken gegen Basismechanismen

- Austausch von public keys
- Ausspionieren von private keys
- Eindringen in Trust bzw. Key Server
- Vortäuschen einer anderen Identität

- Attacken nicht auf Ad-hoc Netze beschränkt

- Sicherheitsmaßnahmen jedoch Ad-hoc-Netz spezifisch

Schutz der Basismechanismen (Hardwareschutz)

- SMART-Cards gegen Diebstahl und Manipulation
- SMART-Card / Sicherheitschip für Medienzugriff

  Upgrade der Software?

Schutz der Basismechanismen (Routing 1)

- watchdog (versucht unkooperative nodes zu erkennen)
  - enthält für jeden Nachbarknoten einen Zähler über nicht weitergeleitete Pakete
  - bei Überschreitung eines Schwellwertes Meldung an Sender
- pathrater (versucht alternative Route zu finden)
  - bewertet einzelne Knoten und bildet Bewertung für Routen
  - Startwert: 0,5
  - erfolgreiche Weiterleitung: +0,01 (alle 200ms) (max.=0,8)
  - Verbindungsabbruch: -0,5
  - Watchdogmeldung: -100

Schutz der Basismechanismen (Routing 2)

- Problem: **alte** oder **falsche** Routinginformationen?
- alte Routinginformationen durch Teilnehmermobilität sind nicht unterscheidbar von böswillig ausgesendeten falschen Routinginformationen
- alternative Routen bei Verbindungsabbrüchen
- diversity coding
  - Senden von redundanten Infos zur Fehlerkorrektur über alternative Routen
- geographic routing
  - Routen von Daten mit Hilfe geografischer Positionen

TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.tu-bs.de http://www.ibr.cs.tu-bs.de

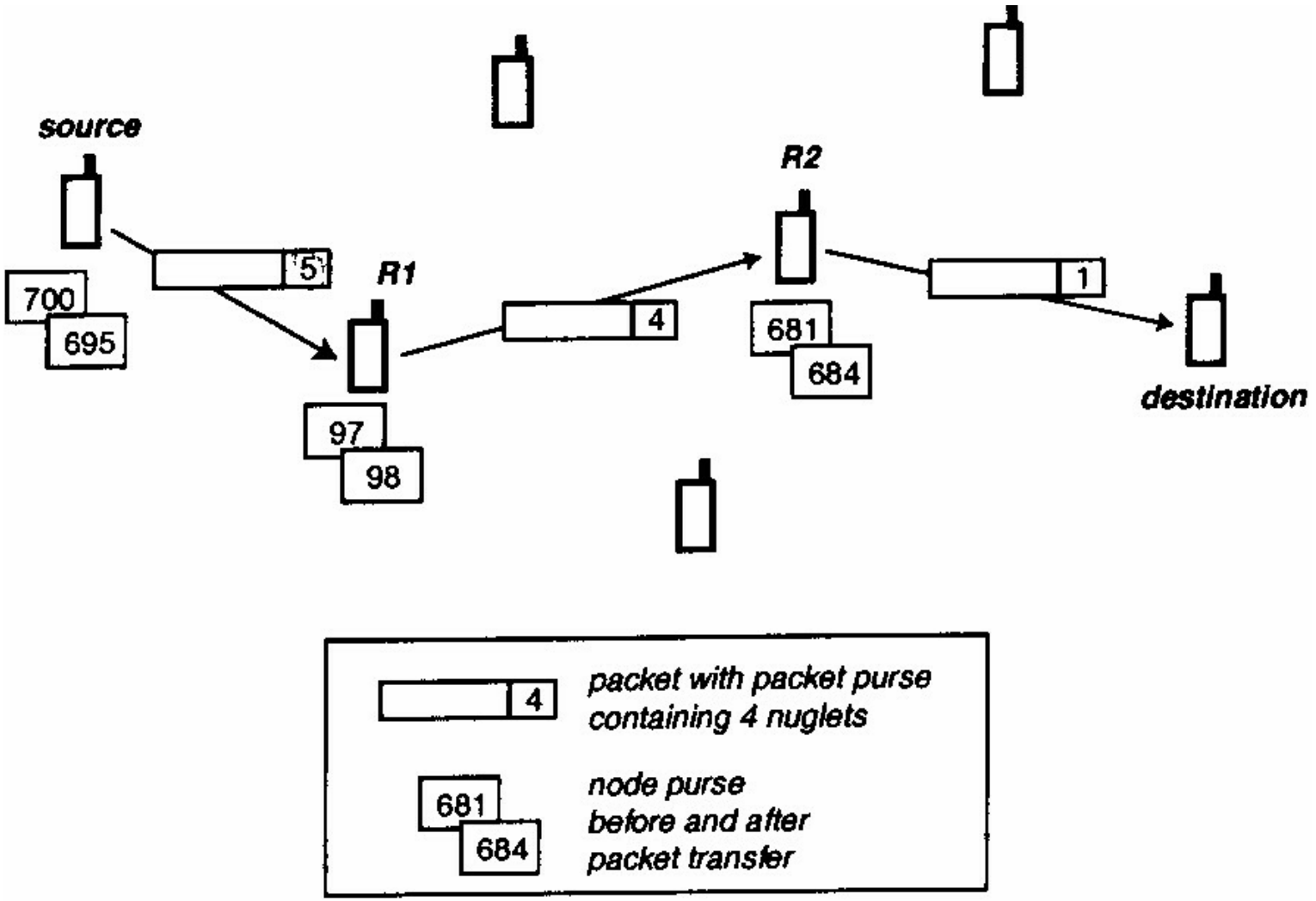
Schutz der Basismechanismen (Routing 3)

- Problem: Kooperation beim Routing?
- - Anreiz zum Kooperieren
- - Abhalten vom Überladen des Netzes

- Virtuelle Währung: **nuglet**
- Packet Purse Model (Sender bezahlt für Transport)
- - Sender gibt Paket x nuglets mit und versendet es
- Packet Trade Model (Empfänger bezahlt für Transport)
  - Nodes kaufen sich Pakete gegenseitig ab und verkaufen sie weiter

TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.tu-bs.de http://www.ibr.cs.tu-bs.de

Schutz der Basismechanismen (Routing 4 - PPM)



Schutz der Sicherheitsmechanismen

- Datenübertragung
  - symmetric key cryptography
  - asymmetric key cryptography

- Key-Etablierung (Übertragung der Schlüssel)
  - key agreement
  - key transport

Schutz der Sicherheitsmechanismen (asymmetric key cryptography)

- public/private key Paar
- public key öffentlich, private key geheim
- Verschlüsselung mit public key des Empängers
- Entschlüsselung nur mit zugehörigem private key möglich

- Möglichkeit: Übertragung eines symmetrischen Schlüssels und nachfolgender Wechsel der Verschlüsselung

- Problem der Authentizität des public keys bleibt bestehen!

Schutz der Sicherheitsmechanismen (key agreement)

- Gruppenkommunikation
- Wahl eines Passwortes oder einfachen Schlüssels
- Übertragung an alle teilnehmenden Personen
- password-authenticated key exchange

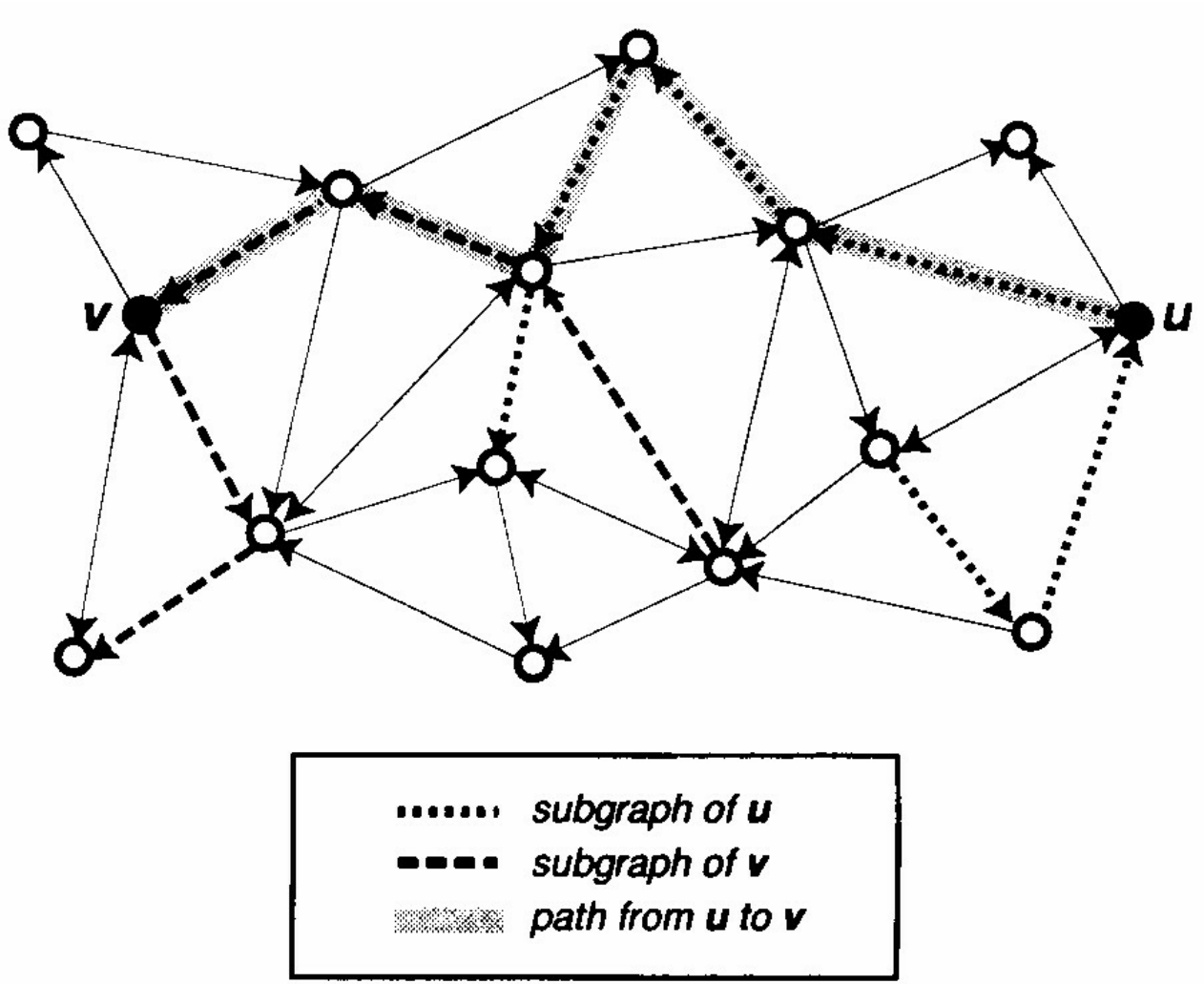
Schutz der Sicherheitsmechanismen (self organized public-key infrastructure)

- Bildung von Zertifikatketten zur Übertragung des public keys
- public key Zertifikat:

  Datenstruktur in welcher ein public key, durch die digitale Signatur des Besitzers des Zertifikates, an eine Identität gebunden wird.

- Zertifikate stellen Vertrauensbeziehungen dar
- Nodes besitzen eine gewisse Anzahl von public keys vertrauensvoller Nodes
- Mischen mit Empfängerzertifikaten zur Kettenbildung möglich

Schutz der Sicherheitsmechanismen (self organized public-key infrastructure)



Schutz der Sicherheitsmechanismen (key managment service)

- Emulierte Autorität (CA) übernimmt Schlüsselmanagment
  - kennt alle public keys
  - update Nachrichten
  - query Anfragen
  - auf mehrer Nodes verteilt (Server)
  - jeder Server enthält einen Teil des CA private keys
  - generiert Teilsignatur
  - combiner bildet aus Teilsignaturen eine vollständige CA-Signatur

Zusammenfassung

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Authentizität
- Nicht-Anfechtbarkeit

Was ist gelöst?
Was ist nicht gelöst?
Weitere Attacken?