Routing und Sicherheit in drahtlosen Sensor-Netzwerken (DSN)

Dipl.-Ing. Frank Reichenbach

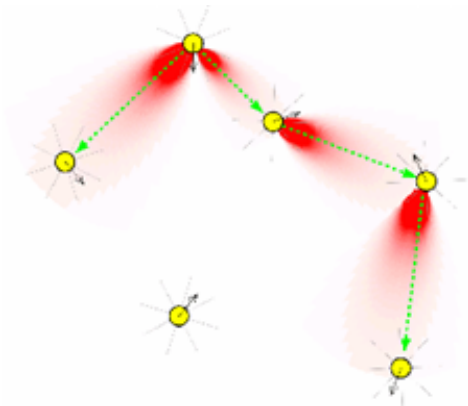
Universität Rostock
Fakultät für Informatik und Elektrotechnik
Institut MD

Agenda

- Routing
  - Grundlagen
  - Protokolle
    - Destination-Sequenced Distance-Vector Routing (DSDV)
    - Clusterhead Gateway Switch Routing (CGSR)
    - Dynamic Source Routing (DSR)
    - Ad-Hoc On-Demand Distance Vector Routing (AODV)
  - Fazit
- Sicherheit
  - Grundlagen
  - Angriffe
  - Gegenmaßnahmen
  - Fazit
- Referenzen

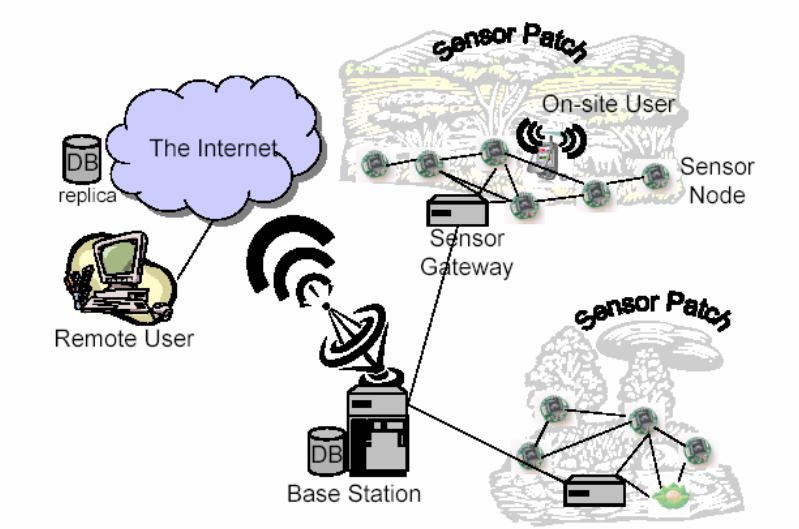
Routing in drahtlosen Ad-Hoc Netzwerken

Grundlagen



Ad-Hoc vs. Drahtlose Sensor Netzwerke (DSN)

- Größe der Knoten
- Ressourcenarmut (Energie)
- Aufgaben (Messen)
- Mobilität
- Interfaces
- Menge der Knoten



Einführung

- Routing = Art der Wegfindung durch ein Netzwerk
- Laut RFC 1983: *„Routing ist der Prozess der Auswahl der richtigen Schnittstelle und des nächsten Hops für Pakete, die weitergeleitet werden sollen.“*
- ISO/OSI Modell – Network Layer (logische Adressen vorhanden)

Englischer Sprachgebrauch

- Routed-Protokoll:
  - Weiterleitung durch den Router
  - Weiterleitung von Benutzerinformationen
  - Router muss in der Lage sein, die Informationen, die durch das Routed-Protokoll gegeben sind, zu interpretieren
  - Bsp.:
    - Internetprotokoll (IP)
    - Internetwork Packet Exchange (IPX) Protokoll von Novell

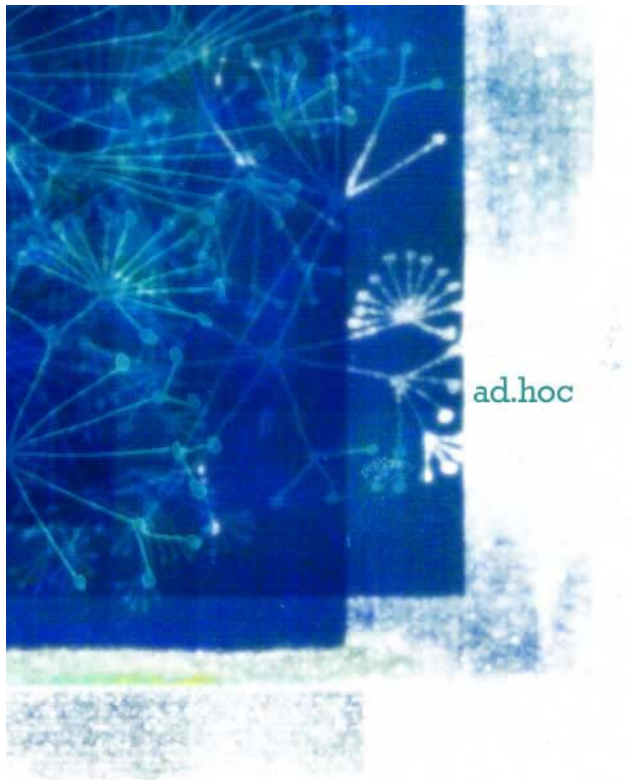
- Routing-Protokoll:
  - Ermöglichen die Wegewahl durch spezielle Routing-Algorithmen
  - Nur Weiterleitung von Tabellen mit Informationen, die die Weitergabe der Benutzerinformationen unterstützen, jedoch keine Benutzerinformationen

Traditionelles Routing einfach übernehmen?

- Traditionelle Routing-Verfahren aus Festnetzen arbeiten nicht effizient genug oder versagen komplett!
  - Hohe Dynamik
  - Mobilität
  - Asymmetrische Verbindungen
- „Verbindung“ zwischen zwei Knoten im klassischen Sinne (z.B. mit bestimmten Qualitätsgarantien) gibt es hier nicht

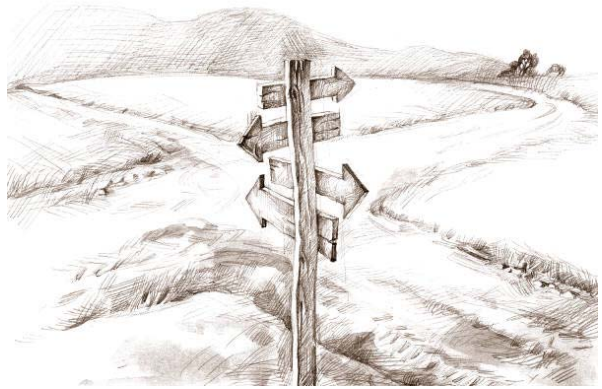
Anforderungen an Routing Protokolle

- Performanz
  - Optimaler Weg
  - Geringe Latenz
- Energieverbrauch
- Netzabdeckung
- Sicherheit
- Robustheit
- Skalierbarkeit
- Schleifenfreiheit
- Quality of Service (Priorisierung der Pakete)

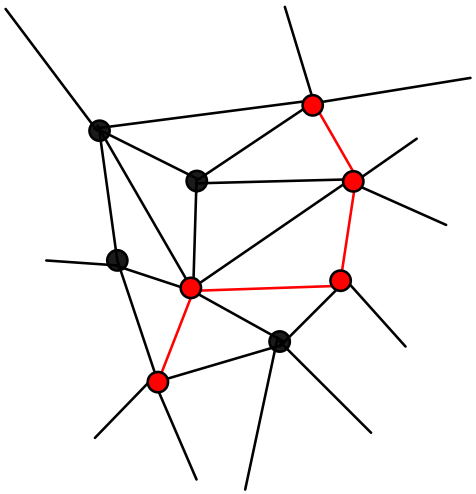


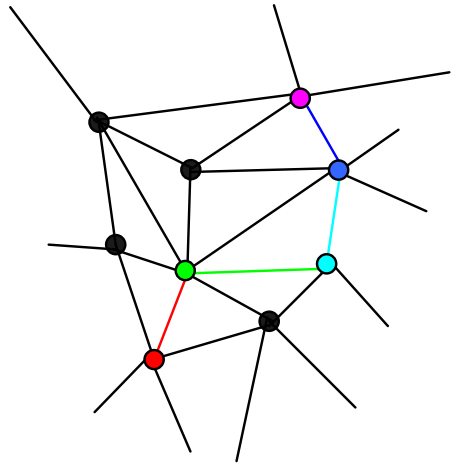
Routing

Protokolle



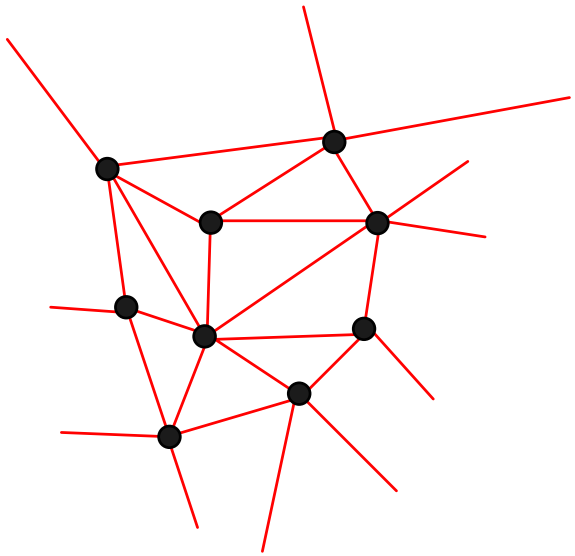
Klassifikation von Routing Protokollen

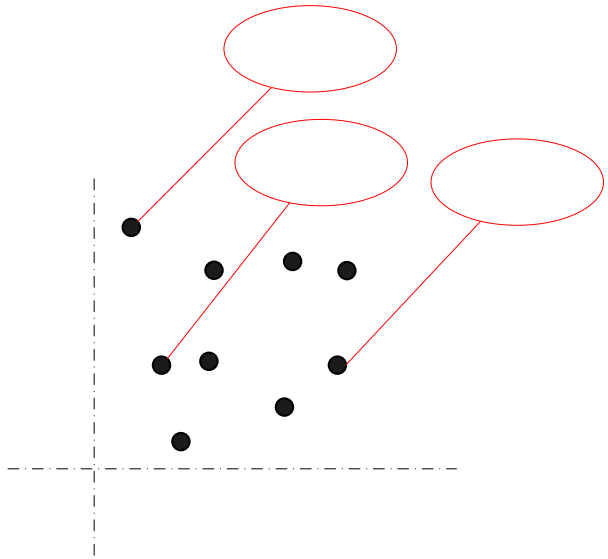




Source Path Routing	vs.	Destination Routing
• Startknoten übergibt komplette Route • Route im Header des Paketes enthalten • Zwischenknoten leiten passiv weiter		• Startknoten übergibt nur die Zieladresse • Zwischenknoten entscheiden nächsten Hop • Zwischenknoten leiten aktiv weiter

Klassifikation von Routing Protokollen





Topologiebasiert	vs.	Geografisch
• Informationen sind Netzwerkverbindungen • Abgelegt in Routingtabellen • Ständige Aktualisierung der Routingtabellen erforderlich		• Position der Knoten bekannt • Wegbestimmung über Koordinaten • Ständige Aktualisierung der Position erforderlich

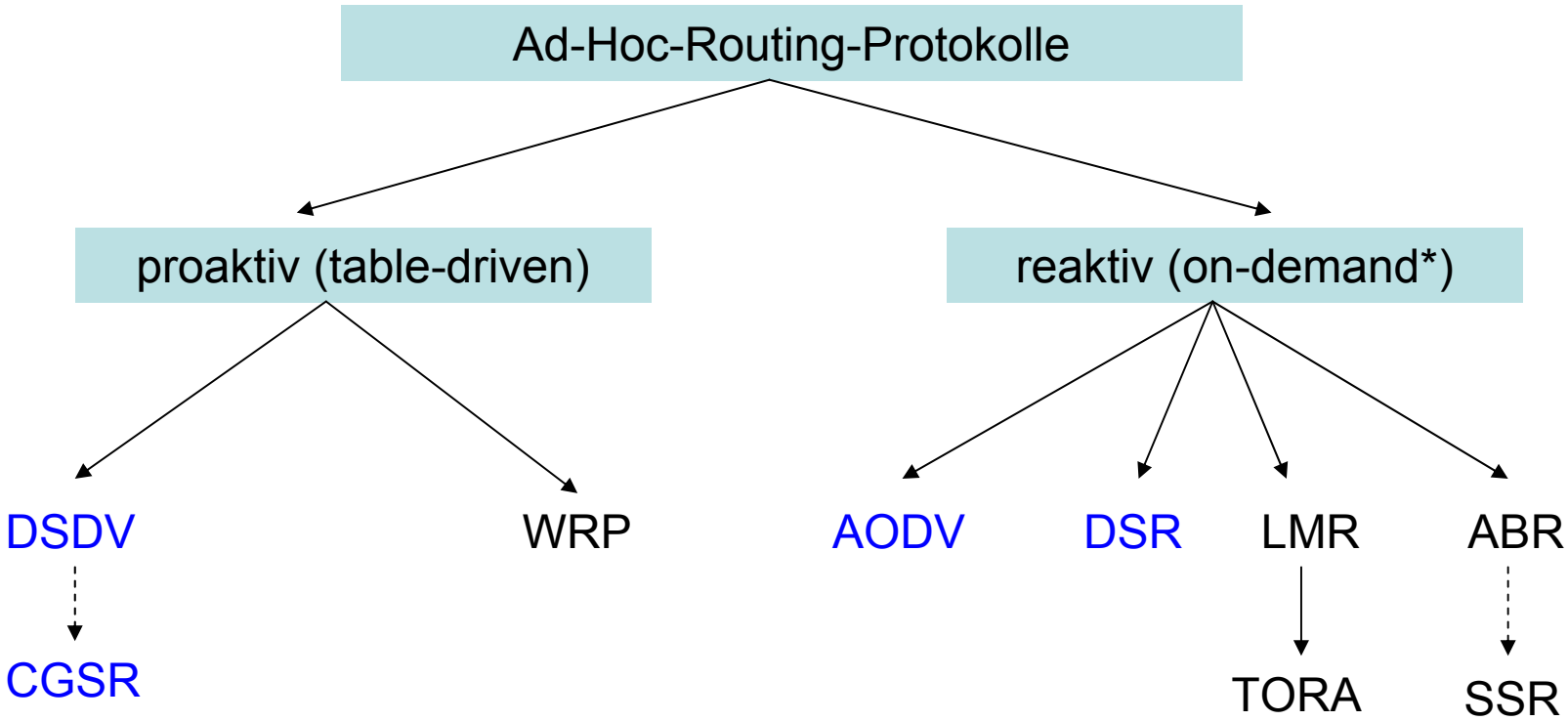
Klassifikation von Routing Protokollen

Proaktives Routing (table-driven)	vs.	Reaktives Routing (on-demand)
• Jeder Knoten kennt alle sich auf das Netz beziehende Routinginformationen – „global state“ • Ständige Aktualisierung der Informationen erforderlich • Auch bei Nichtnutzung oder für die Zukunft („pre-fetching“) • Vorteil: optimale Wegbestimmung sofort durchführbar • Nachteil: hoher Aktualisierungsaufwand		• Ermittlung der Route erst vor Paketversendung • Cachetabellen (gelernte Routen) • „Route Discovery“ – Wegsuche durch „Flooding“ • „Route Maintenance“ – Routen Updaten • Vorteil: geringe Bandbreitenutzung • Nachteil: höhere Latenzzeiten

Bezeichnungen

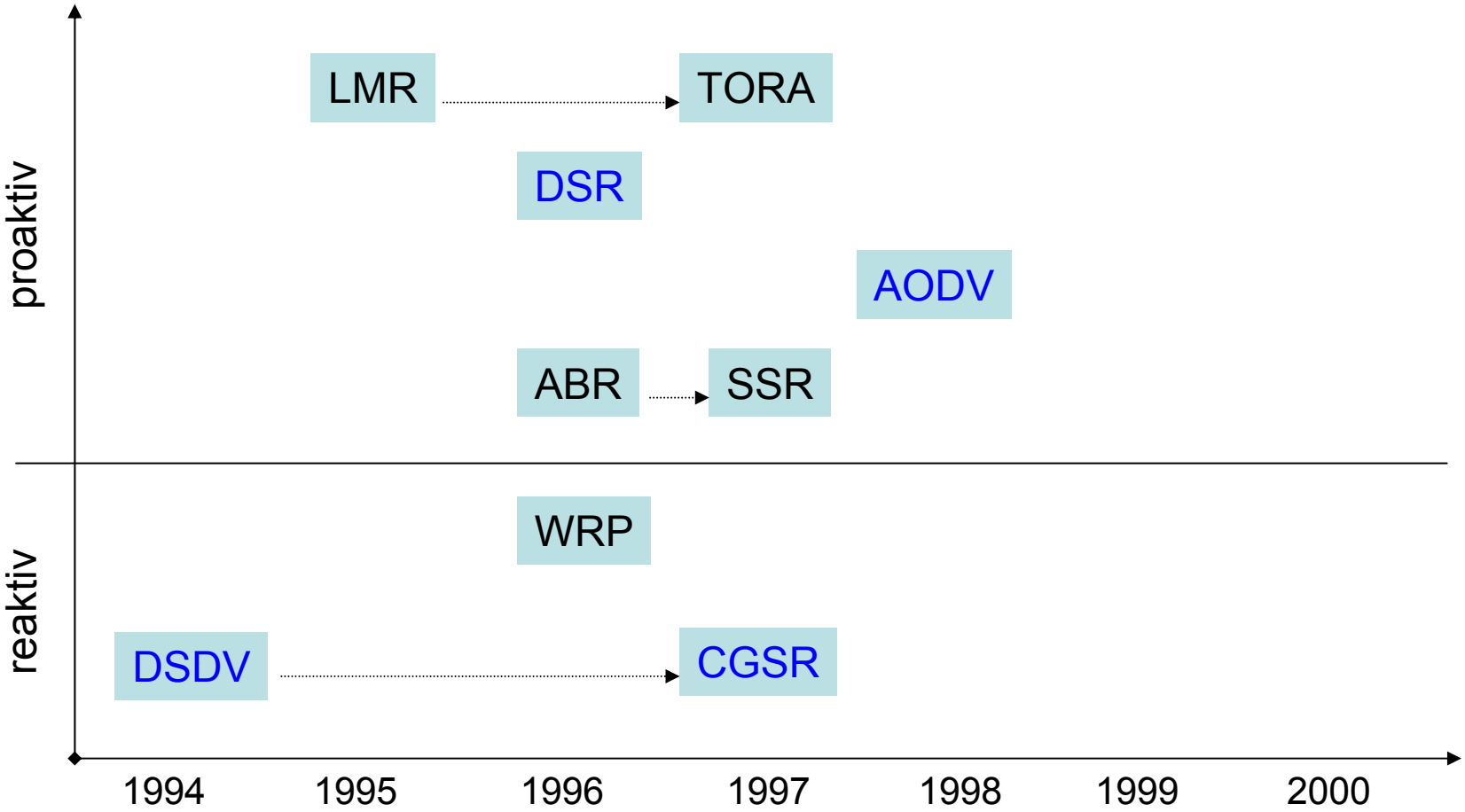
- DSDV = Destination-Sequenced Distance-Vector Routing (1994)
- CGSR = Clusterhead Gateway Switch Routing (1997)
- WRP = Wireless Routing Protocol (1996)
- AODV = Ad-Hoc On-Demand Distance-Vector Routing (1997)
- DSR = Dynamic Source Routing (1996)
- LMR = Lightweight Mobile Routing (1995)
- TORA = Temporally Ordered Routing Algorithm (1997)
- ABR = Associativity-Based Routing (1996)
- SSR = Signal Stability Routing (1997)

Strukturierung der Protokolle



* auch: Source-initiated on-demand

Zeitliche Einordnung



1. DSDV (Proaktiv)

- Destination-Sequenced Distance-Vector Routing
  - C. Perkins 1994
  - Proaktiv (table driven)
  - Auch bekannt als „Distributed Bellman-Ford Algorithm“ (Grundlage für „Routing Information Protokoll“ (RIP))


Charles Perkins, Nokia

- Funktionsweise
  - Jeder mobile Knoten des Netzwerkes unterhält eine Routing-Tabelle
  - R.-Tabelle enthält alle möglichen Zielknoten und die Anzahl der Teilstrecken (Hops) zum Ziel
  - Routing-Tabellen-Updates werden regelmäßig ausgesendet

1. DSDV – Routing Tabelle

Destination	Next	Metric	Seq. Nr	Install Time	Stable Data
A	A	0	A-550	001000	Ptr_A
B	B	1	B-102	001200	Ptr_B
C	B	3	C-588	001200	Ptr_C
D	B	4	D-312	001200	Ptr_D

- Enthält alle verfügbaren Zielknoten
- **Sequence number**: Erstellt durch den Zielknoten (spiegelt Aktualität wieder; ZielknotenID + aufsteigende Anzahl)
- **Install Time:** Zeit der Erzeugung der Eintragung (genutzt zum Löschen alter Werte)
- **Stable Data:** Pointer zu einer Tabelle, die angibt, wie stabil die Route ist (genutzt um Fluktuation im Netzwerk zu dämpfen)

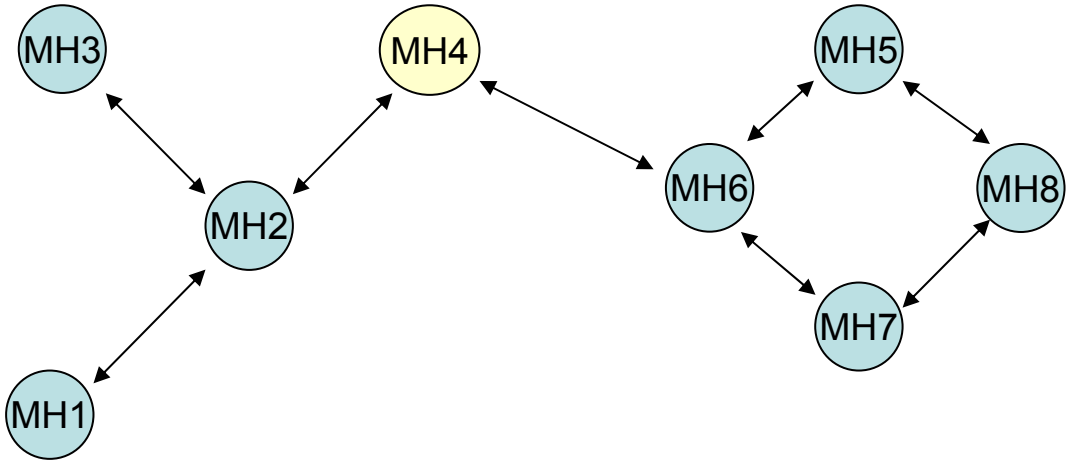
1. DSDV – Übertragung der Route-Informationen

- Routing-Tabellen-Updates (Broadcasts)
  - *full dump*
    - Vollständige Routing-Information eines Knotens wird gesendet
    - Wird selten durchgeführt, da viele Daten zu senden
    - Kann mehrere PDUs umfassen (Protocol Data Unit)
  - *incremental*
    - Überträgt nur die Routing-Informationen, die sich seit dem letzten *full dump* geändert haben
    - Sollte in eine PDU passen

1. DSDV – Wahl der Route

- New-Route-Broadcasts enthalten
  - Zieladresse
  - Sequenznummer der Information, die den Broadcast ausgelöst hat
  - Sequenznummer des Broadcast
- Es wird immer die Route mit der neuesten Sequenznummer gewählt
- Bei Gleichheit wird die Route mit der kleinsten Metrik gewählt
- Knoten beobachten Einschwingzeit von Routen...
  - Durch Verzögerung von Routen-Updates

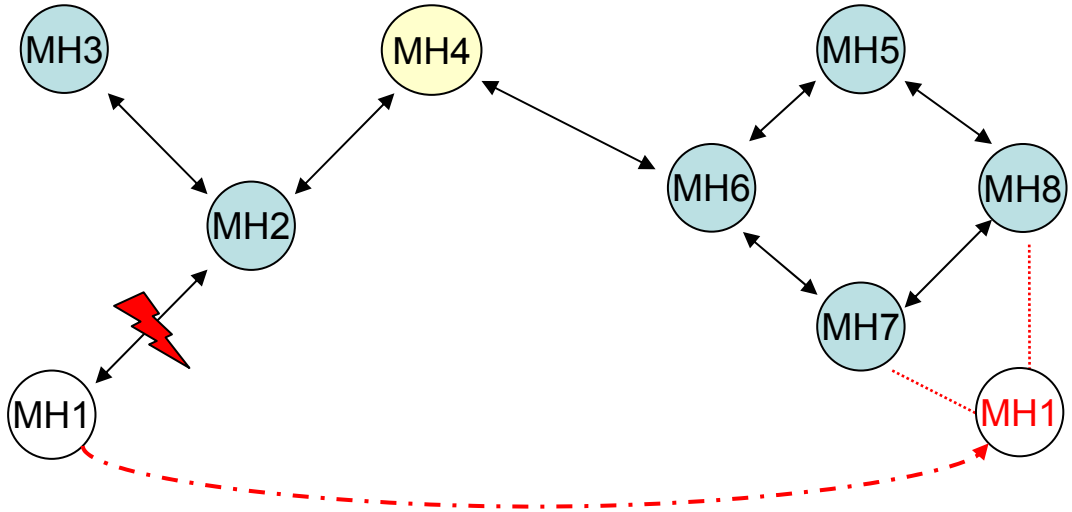
1. DSDV – Beispiel – Knotenbewegung



Destination	Next Hop	Metric	Seq. Nr.	Install	Stable_Data
MH1	MH2	2	S406_MH1	T001_MH4	Ptr1_MH1
MH2	MH2	1	S128_MH2	T001_MH4	Ptr1_MH2
MH3	MH2	2	S564_MH3	T001_MH4	Ptr1_MH3
MH4	MH4	0	S710_MH4	T001_MH4	Ptr1_MH4
MH5	MH6	2	S392_MH5	T002_MH4	Ptr1_MH5
MH6	MH6	1	S076_MH6	T001_MH4	Ptr1_MH6
MH7	MH6	2	S128_MH7	T002_MH4	Ptr1_MH7
MH8	MH6	3	S050_MH8	T002_MH4	Ptr1_MH8

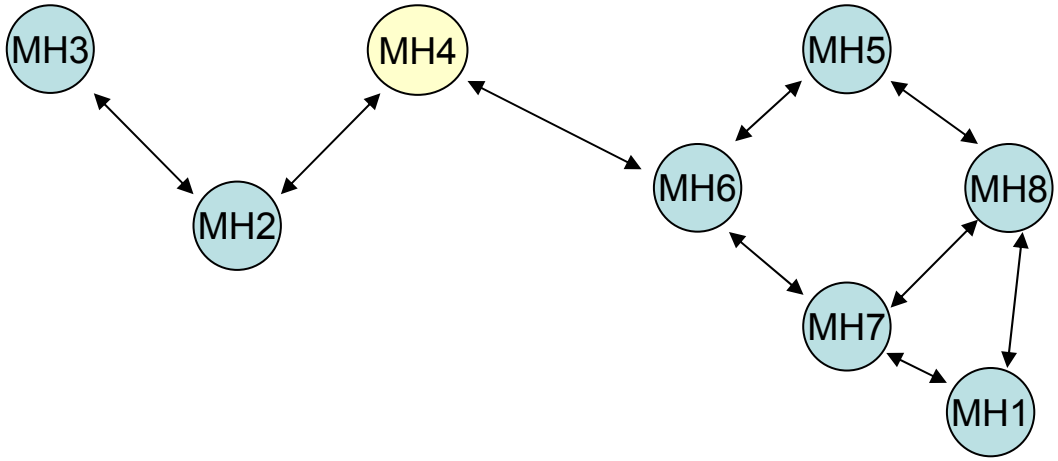
MH4 Routing-Tabelle

1. DSDV – Beispiel – Knotenbewegung



- Update wird von MH1 ausgelöst → Broadcast zu MH7 und MH8
- MH2 bemerkt das fehlende Vorhandensein von MH1 → Incremental Update von MH2 mit ungerader Sequenznummer und unendlicher Metrik
- Updates durchsetzen das gesamte Netz

1. DSDV – Beispiel – Knotenbewegung



Destination	Next Hop	Metric	Seq. Nr.	Install	Stable_Data
MH1	MH6	3	S516_MH1	T810_MH4	Ptr1_MH1
MH2	MH2	1	S128_MH2	T001_MH4	Ptr1_MH2
MH3	MH2	2	S564_MH3	T001_MH4	Ptr1_MH3
MH4	MH4	0	S710_MH4	T001_MH4	Ptr1_MH4
MH5	MH6	2	S392_MH5	T002_MH4	Ptr1_MH5
MH6	MH6	1	S076_MH6	T001_MH4	Ptr1_MH6
MH7	MH6	2	S128_MH7	T002_MH4	Ptr1_MH7
MH8	MH6	3	S050_MH8	T002_MH4	Ptr1_MH8

MH4 Routing-Tabelle

1. DSDV - Bewertung

- Pro:
  - Effiziente Berechnung
  - Einfache Implementierung
  - Geringe Latenz
- Contra:
  - Schlechte Skalierung bei Zunahme von Knoten
  - Schnelle topologische Veränderungen bereiten Probleme
  - Zwei große Tabellen erforderlich
  - Periodische Updates erforderlich:
    - Hoher Netzwerkverkehr
    - Verkehr auch bei unveränderter Netztopologie
    - Nie genutzte Routen werden auch aktualisiert
- Fazit:
  - DSDV eignet sich für kleinere, wenig mobile Netze sehr gut!

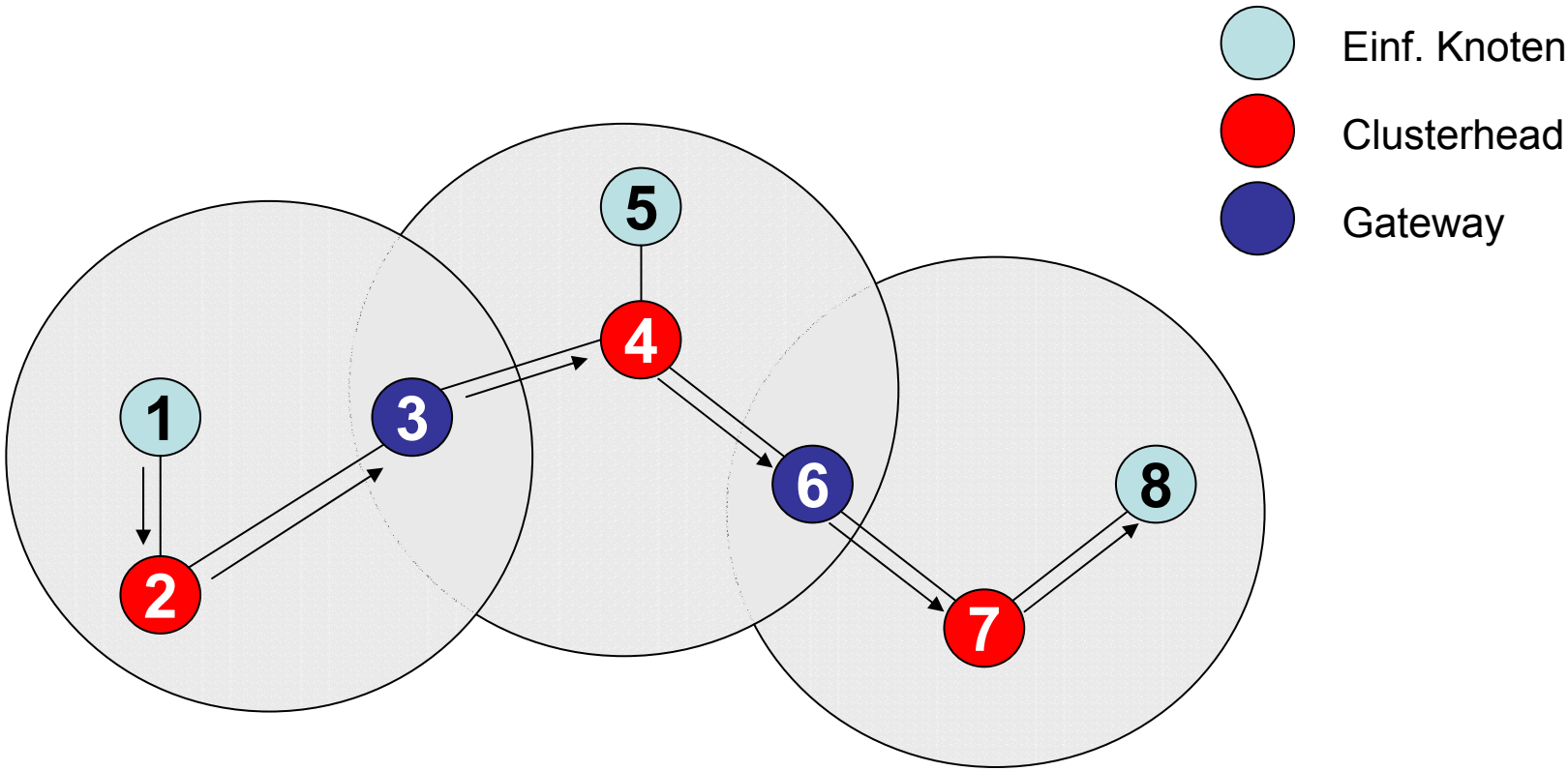
2. CGSR (Proaktiv)

- Clusterhead Gateway Switch Routing (proaktiv)
  - Basiert auf DSDV, aber statt flachem Netzwerk
    → Gruppierung von Knoten zu Clustern
  - Unterschiede:
    - Adressierung
    - Netzwerkorganisation
  - Einzelne Knoten werden zu Clusterheads bestimmt
    - Gibt die Rahmenbedingungen für die Kommunikation zwischen den Clustermitgliedern vor
  - Cluster sind über Gateways verbunden
  - Gateway-Knoten sind im Einzugsbereich mehrerer Clusterheads

Mario Gerla, UCLA

2. CGSR - Beispielroute

- Routing von Knoten 1 zu Knoten 8



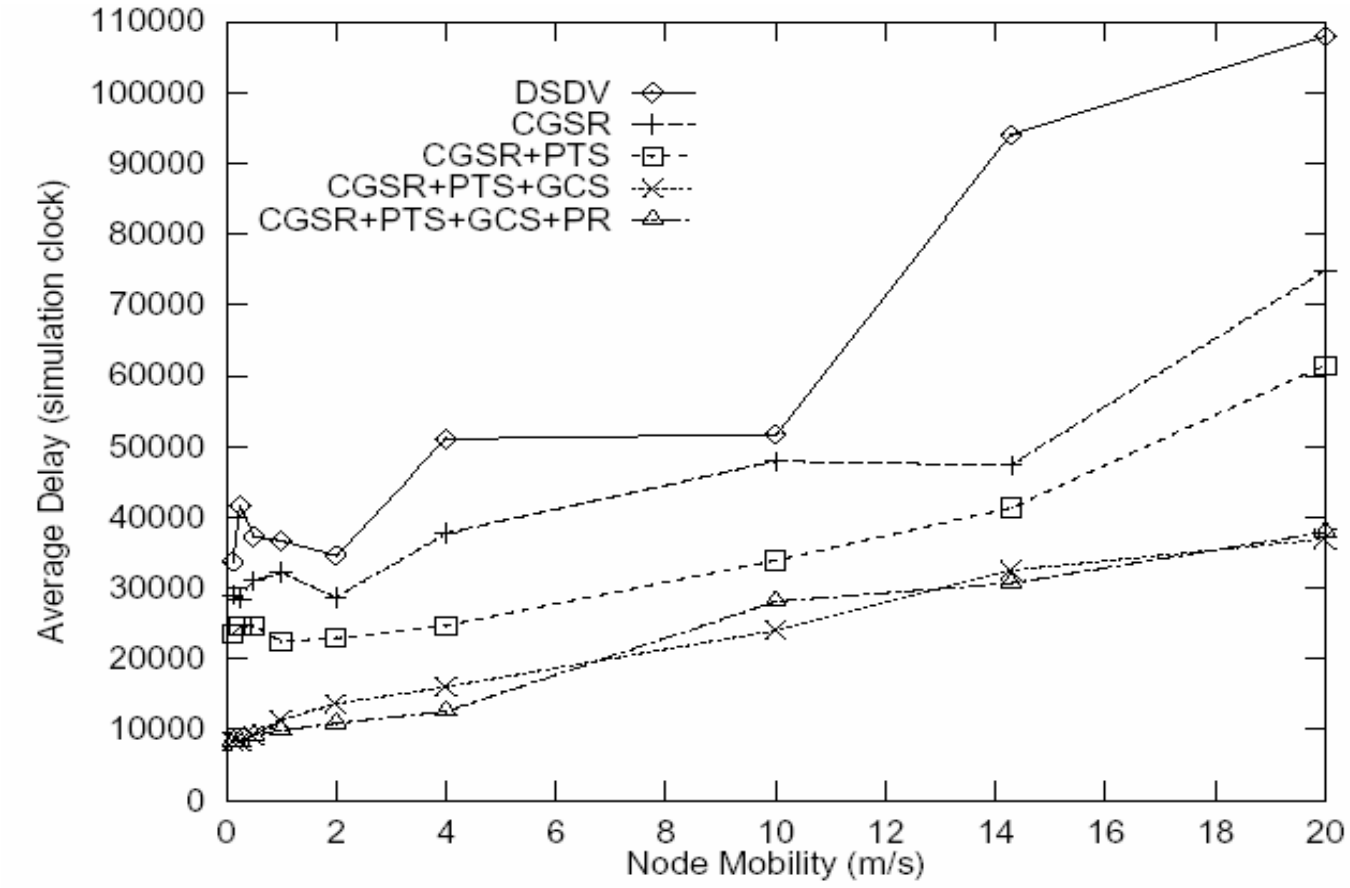
2. CGSR - Funktionsweise

- Ein Paket, das ein **Knoten** aussendet, wird zuerst zum **Clusterhead** geroutet
- Vom Clusterhead wird das Paket über einen **Gateway** zum nächsten Clusterhead weitergeleitet
- Der letzte Schritt wird solange wiederholt, bis der **Clusterhead** des Zielknotens erreicht wird
- Das Paket wird schließlich zum **Zielknoten** geroutet
- Jeder Knoten muss „Cluster Member Table“ unterhalten

2. CGSR - Bewertung

- Pro:
  - Bessere Performance durch hierarchische Netzwerkorganisation
- Contra:
  - Overhead durch Clusterbildung
  - Ständige Suche des optimalen Clusterheads
    - Verbesserung:
      - Clusterhead wird nur geändert:
        - » Falls er in die Reichweite eines Anderen kommt
        - » Wenn ein Knoten aus der Reichweite aller Clusterheads wandert
        - → LCC (Least Cluster Change)

Vergleich DSDV - CGSR



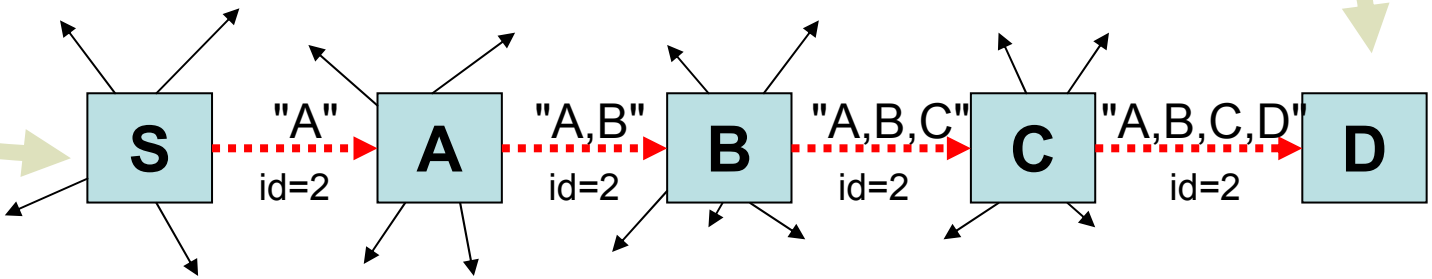
3. DSR (Reaktiv)

- Dynamic Source Routing
  - *Source Routing*: Datenquelle kennt die komplette Route zum Empfänger
  - Datenpakete tragen komplette Route im Header
  - Grundlegende Mechanismen:
    - **„Route Discovery“:** wird veranlasst, wenn Knoten S zu Knoten D senden will und keine Route kennt
    - **„Route Maintenance“:** wenn Knoten S erkennt, dass Route zu D nicht mehr funktioniert und versucht eine Ausweichroute zu finden
  - Eigenschaften:
    - Alle Operationen des Protokolls sind „on-demand“
    - Keine periodischen Routingpakete
    - Änderungen der Topologie beeinflussen nur betroffene Knoten

David B. Johnson

3. DSR - Route Discovery

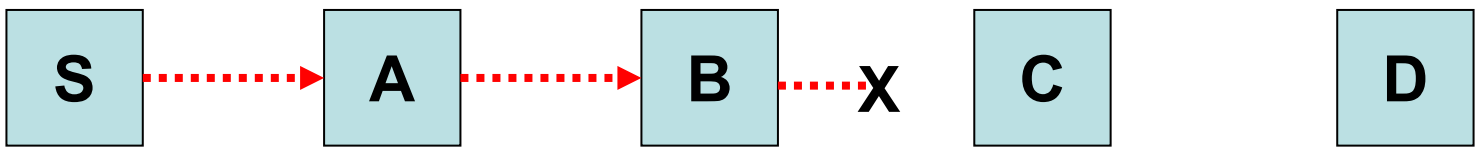
- Möchte S ein Paket an D versenden, schaut S zunächst in seinen Route Cache
- Wenn keine Route im Cache vorhanden → *Route Discovery*
- Bezeichnungen
  - S = Initiator des *Route Discovery*
  - D = Ziel des *Route Discovery*



  - D sendet *Route Reply* zurück an S

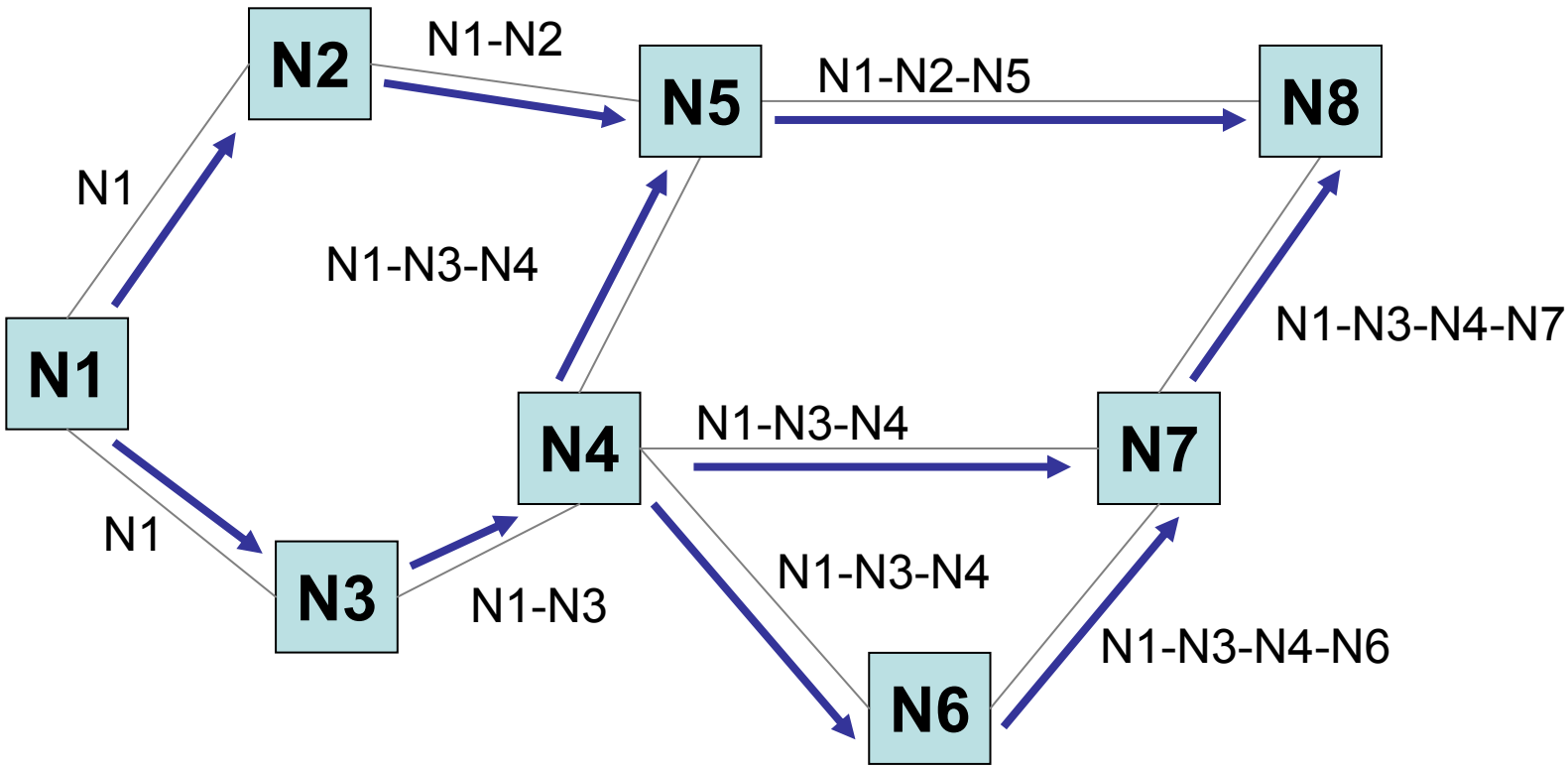
3. DSR - Route Maintenance

- Jeder Knoten entlang einer Route ist dafür verantwortlich, dass ein Paket den nächsten Knoten der Route erreicht
- Im Beispiel: Knoten B wird so lange versuchen, das Paket zu C zu übertragen, bis eine **maximale Versuchszahl** erreicht wird
- Anschließend wird eine *Route Error*-Nachricht an S zurückgesendet
- S entfernt den toten Link aus seinem Route Cache und sucht nach einer **Alternativroute**
- Falls Alternativroute im Cache → Route wird gewählt
- Wenn keine Alternativroute im Cache → S startet **neuen Route Request**



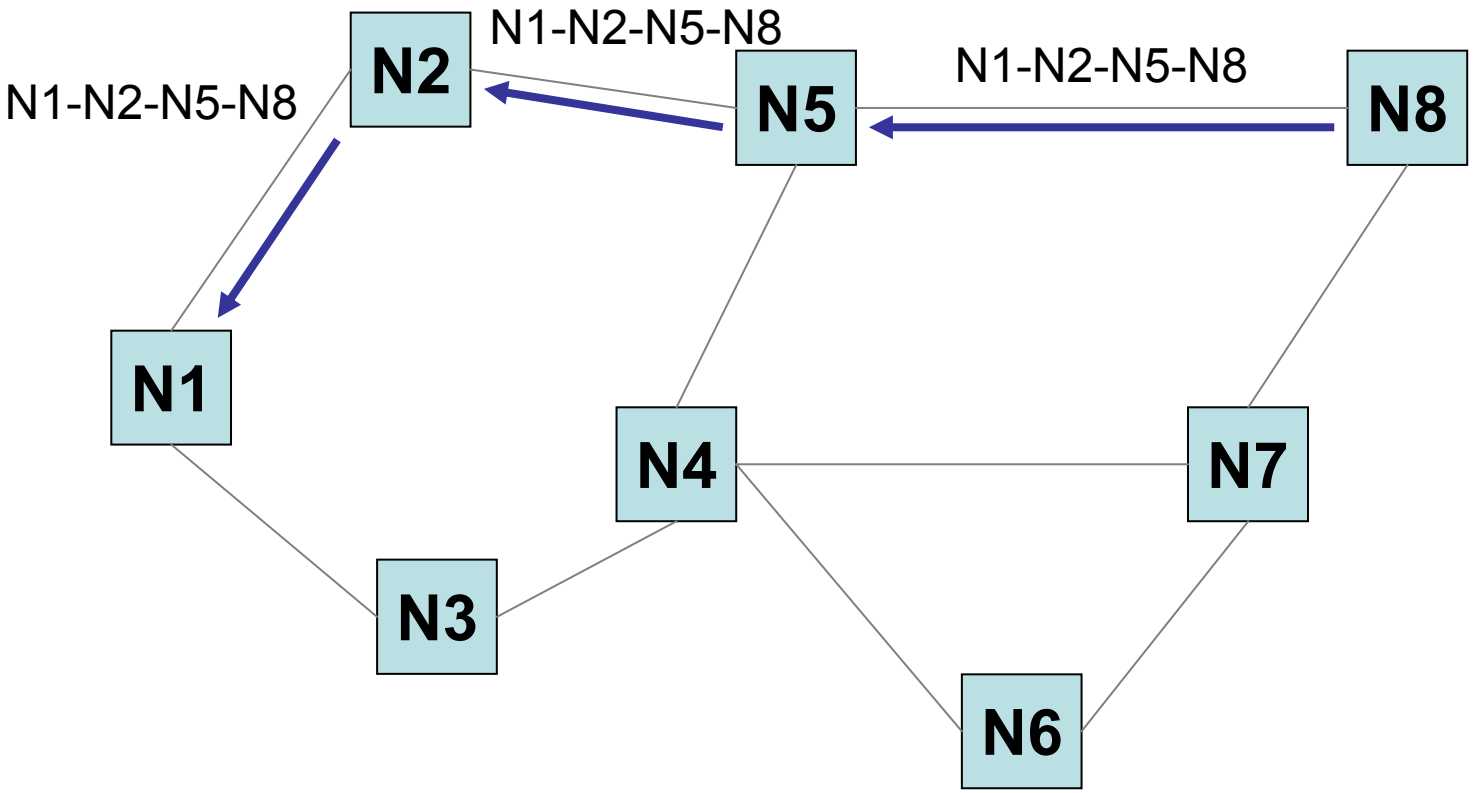
3. DSR - Route Discovery

- Beispiel mit mehreren möglichen Routen S = N1 zu D = N8



3. DSR – Route Replay

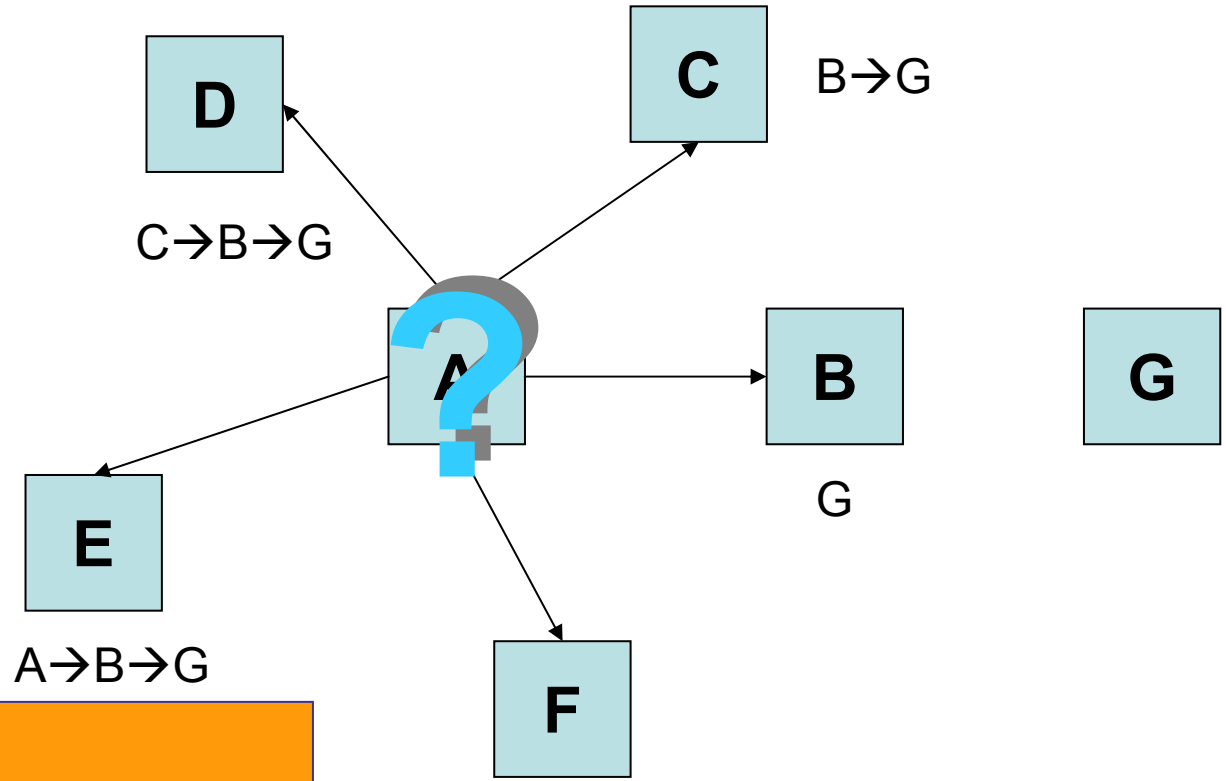
- Beispiel mit mehreren möglichen Routen S = N1 zu D = N8



3. DSR - Zusätzliche Eigenschaften des Route Discovery

- **Cachen von belauschten Routing-Informationen**
  - Ein Knoten, der ein Paket weiterleitet, kann die Routinginformationen dieses Paketes seinem eigenen Route Cache hinzufügen
- **Zwischenknoten antworten auf Route-Requests**
  - Erhält ein Knoten ein Route-Request und ist nicht der Zielknoten, kann er, wenn er die gewünschte Route im Cache hat, ein Route-Reply an den Initiator des Route-Request zurücksenden
- **Verhindern von Route-Reply-Stürmen**
  - Zwischenknoten verzögern Route-Reply
- **Route-Request Hop-Limits**
  - Route Requests, die Hop-Limit überschreiten werden verworfen

3. DSR - Route-Reply-Sturm



- A sucht Route nach G
- B, C, D, E, F erhalten Route Request
- Alle antworten quasi-gleichzeitig mit Route aus dem Route-Cache
  → Kollision!

3. DSR – Route Maintenance Eigenschaften

- **Paket-Rettung (Packet-Salvaging)**
  - Rettet Paket, das einen Route-Error verursacht hat
- **Cachen von Negativ-Informationen**
  - Tote Links werden nicht aus Route-Cache gelöscht, es wird stattdessen ein Hinweis gespeichert, dass der Link z.Zt. nicht existiert.
- **Verstärkte Ausbreitung von Route-Error-Nachrichten**
  - Der Quellknoten einer Nachricht, die einen Route-Error verursacht hat, sendet einen Broadcast darüber an seine Nachbarn

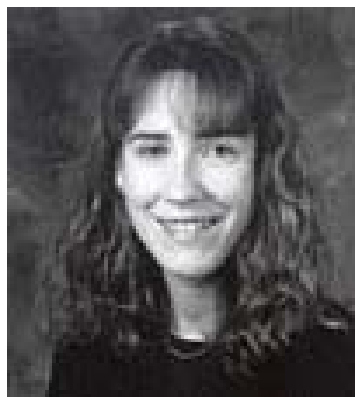
3. DSR - Bewertung

- Pro:
  - Wenig überflüssiger Netzwerkverkehr
  - Erhöhte Sicherheit durch Source Routing
- Contra:
  - Größere Latenz

4. AODV (Reaktiv)

- Ad-Hoc On-Demand Distance Vector Routing
  - Basiert auf DSDV
  - *Problem bei DSDV:* Topologieveränderung erzwingt netzweiten Broadcast → Traffic
  - *Jetzt:* Nur Knoten auf einem aktiven Pfad tauschen Informationen aus
  - Routen werden nur noch bei Bedarf ermittelt
  - Routingtabellen werden unterhalten
  - Bei unbekannter Route → *Route Discovery*
  - Datenquelle sendet RREQ-Paket per Broadcast
  - Datensenke antwortet mit RREP-Paket entlang der gefundenen Route

Charles Perkins, Nokia

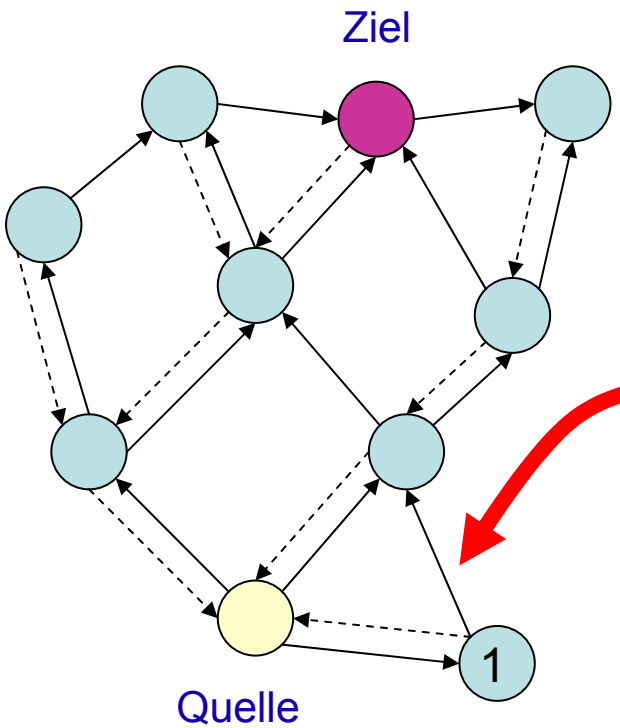


Elizabeth M. Royer, UCSB

4. AODV – Route Discovery

- Annahme: Knoten S möchte Paket an Knoten D senden
- Route in Routing-Tabelle von S?
- Nein → Route Discovery wird gestartet
  - S erzeugt RREQ-Paket mit Zieladresse, Seq.-Nummer und Broadcast-ID
    → Broadcast
  - Erhält ein Zwischenknoten das RREQ-Paket, schaut er nach, ob er es schon kennt, wenn ja → RREQ-Paket wird verworfen
  - Hat der Zwischenknoten eine aktuelle Route zu D, sendet er ein RREP-Paket an S
  - Falls kein Zwischenknoten eine Route zu D kennt, dann sendet schließlich D ein RREP an S

4. AODV - Route Discovery Beispiel



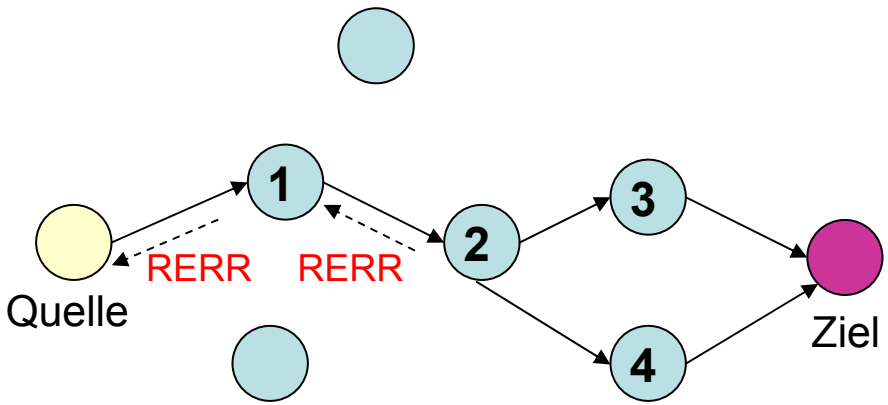
Ausbreitung des Route Request

Reverse Route Eintrag

Jeder Zwischenknoten erzeugt nur dann einen Reverse-Route-Eintrag, wenn er ein RREQ-Paket zum **ersten** mal erhält.

4. AODV - Route Maintenance

- Falls ein toter Link entdeckt wird → Route Error (RERR) wird an Datenquelle gesendet
- RERR enthält eine Liste mit allen Zielknoten, die nun nicht mehr erreichbar sind



4. Bewertung

- Pro:
  - Geringe Latenz
  - Wenig überflüssiger Netzwerkverkehr
- Contra:
  - ?

Vergleich DSR/AODV

- Gemeinsamkeiten
  - Reaktiv (Routen werden nur bei Bedarf ermittelt)
  - Route Discovery basiert auf Request- und Reply-Zyklen
  - Routing-Informationen werden auch in Zwischenknoten gespeichert
- Unterschiede
  - DSR hat Zugriff auf größere Menge von Routing-Informationen (Cache vs. Routing-Table)
  - DSR antwortet auf alle Requests, die einen Zielknoten erreichen (Quelle lernt alternative Routen)
  - AODV-Routing-Tabelle kennt dagegen nur einen Eintrag je Ziel
  - DSR kennt keinen Mechanismus, um veraltete Routen zu erkennen (obwohl einige veraltete Routen von RERR-Paketen gelöscht werden)

Fazit

- Anwendungsszenario bestimmt stark die Wahl des optimalen Algorithmus
- Routing-Protokolle in Ad-Hoc Netzwerken unterliegen strengen Anforderungen
- Bisher keine Quality of Services implementiert
- Zusätzliche Parameter, wie z.B. Ortsinformationen sollten genutzt werden

- Außerdem: Keine Berücksichtigung von Sicherheit!

Sicherheit in drahtlosen Ad-Hoc Netzwerken

Grundlagen

Was bedeutet Sicherheit?

- Risikomanagement
- Aufdecken, Erkennen von
  - Bedrohungen
  - Schwachstellen
  - Angriffen
- Abschätzen von
  - Angriffswahrscheinlichkeiten
  - Kosten
- Entwicklung von vorbeugenden Schutzmaßnahmen
- Entwicklung von Gegenmaßnahmen

Ad-Hoc Netzwerk - Charakteristik

- Weit gefächertes drahtloses Netzwerk von mobilen und statischen Knoten
- Keine feste Infrastruktur oder zentrale Administration
- Kein Provider vorhanden
- Spontane Kommunikationsbeziehungen zwischen benachbarten Knoten
- Jeder Knoten profitiert von Diensten der Nachbarknoten
- Mobilität durch drahtlose Kommunikation
- Kooperation zwischen Knoten erforderlich
- Dynamische Netzwerktopologie (unstabile Routen und Verbindungen)
- Routing und Mobilitätsmanagement wird vom Power Management beeinflusst
- Accesspoints zum drahtgebundenen Netz

Arten der Sicherheit

- Sicherheitsanforderungen an Ad-Hoc Netzwerke sind vergleichbar mit denen an drahtgebundene Netzwerke
  - Vertraulichkeit (Nachricht unbekannt für Dritte)
  - Integrität (Daten nicht durch Dritte verändert)
  - Verfügbarkeit (Ständige Erreichbarkeit von Services)
  - Authentifizierung (Überprüfung einer vorgegebenen Identität)
  - Anonymität (Keine Weitergabe von privaten Informationen an Dritte)

- ABER!
  - Existierende Sicherheitslösungen drahtgebundener Netzwerke sind nicht ohne erneute Untersuchung auf Ad-Hoc Netzwerke übertragbar

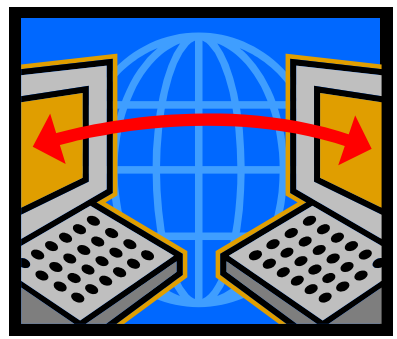
- Warum?
  - Die Sicherheitsprobleme sind aufgrund der besonderen Eigenschaften von Ad-Hoc Netzwerken andersartig als in drahtgebundenen Netzwerken

Drahtgebundene vs. Drahtlose Netzwerke

- Drahtgebundene Netze:
  - Router übernehmen Packet-Forwarding und werden gesichert
  - „Sniffing“ des Übertragungskanals schwierig (Optisches Kabel)

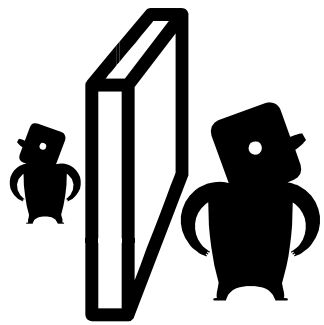
- Drahtlose Netze:
  - Jeder Knoten ist ein Router
  - Übertragungskanal ist zugänglich für legitimierte Nutzer und Angreifer
  - Kein definierter Ort für Netzverkehr-Monitoring oder Zugriffskontrollmechanismen
  - Verschwommene Grenze zwischen internem Netzwerk und externer Welt
  - Existierende Routing-Protokolle (AODV,DSR,wMAC) setzen trusted, cooperative Umgebung voraus

- Folgen:
  - Angreifer wird zum Router und stört das Netzwerk
  - Keine „klare“ Verteidigungslinie!



Ansätze zur Sicherung

- Proaktiv:
  - Versuch Attacken des Angreifers vom „ersten Platz“ zu verhindern (kryptografische Techniken)
- Reaktiv:
  - Detektion von Bedrohungen a posteriori und sofortige Reaktion
- Optimale Lösung:
  - Integration beider Ansätze
  - Prävention, Detektion und Reaktion



ABER: Sicherheit ist nicht umsonst!

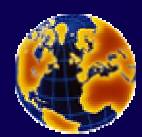
- Erhöhter Aufwand an:
  - Rechenleistung
  - Kommunikation
  - Management
- Sensornetzwerke sind ressourcenarm!
- Tradeoff:
  - Netzwerkperformance ←→ Sicherheitsstärke

Sicherheitsaufgaben

Application Layer	Detektion und Erkennung von Viren, Würmern, fremder Code, Missbrauch
Transport Layer	Authentifizierung und Sicherung der end-to-end Kommunikation durch Datenverschlüsselung
Network Layer	Schützen des Ad-Hoc-Routings und der Forwarding-Protokolle
Link Layer	Sicherung des wMAC-Protokolls und Anbieten Link-Layer Sicherheitssupport
Physical Layer	Verhinderung von Denial of Service Attacken

- Hauptaufgabe: Sicherung der Multihop-Connectivity!
  - *Link-Layer:* Sicherung von Onehop-Konnektivität durch Protokolle (MAC)
  - *Network-Layer:* Erweiterung der Konnektivität zu Multihops durch Routing und Data-Forwarding-Protokolls

DoS (Denial of Service) oder DDoS (Distributed Denial of Service) sind Angriffe auf Server mit dem Ziel sie bzw. einen oder mehrere ihrer Dienste arbeitsunfähig zu machen. Erfolgt der Angriff von vielen verteilten Systemen aus, wird von einem Distributed Denial of Service Attack (DDoS) gesprochen.



Sicherheit in drahtlosen Ad-Hoc Netzwerken

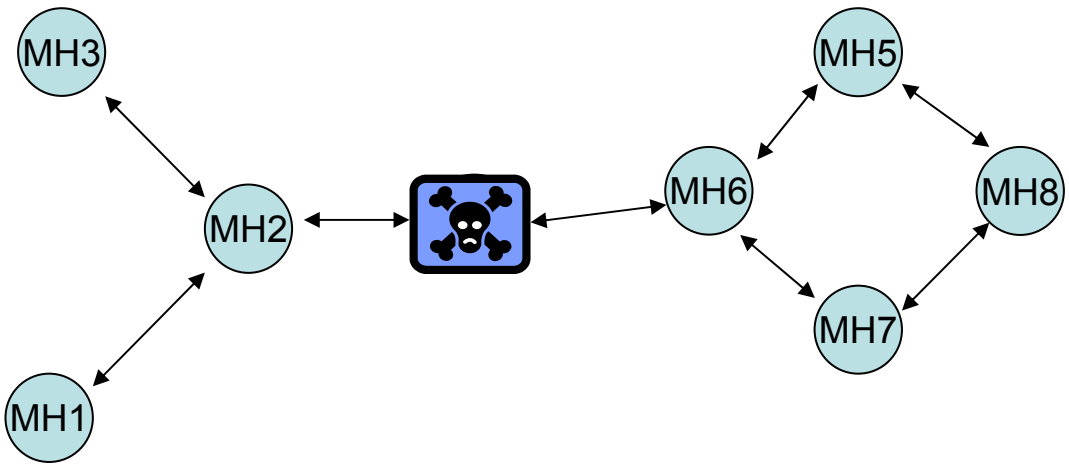
Angriffe

Allgemein: Angriffe auf Routing-Protokolle

- Umleitung des Netzverkehrs zu einer bestimmten Lokation unter Kontrolle
- Erzeugung erhöhtem Netzverkehrs in bestimmten Regionen
- Kanalkonkurrenz
- Weiterleitung von Paketen über eine nicht existierende oder nicht optimale Route
- Erstellung von Routing-Loops
- Verhinderung einer Routenfindung zum Zielknoten
- Partitionierung des Netzwerkes

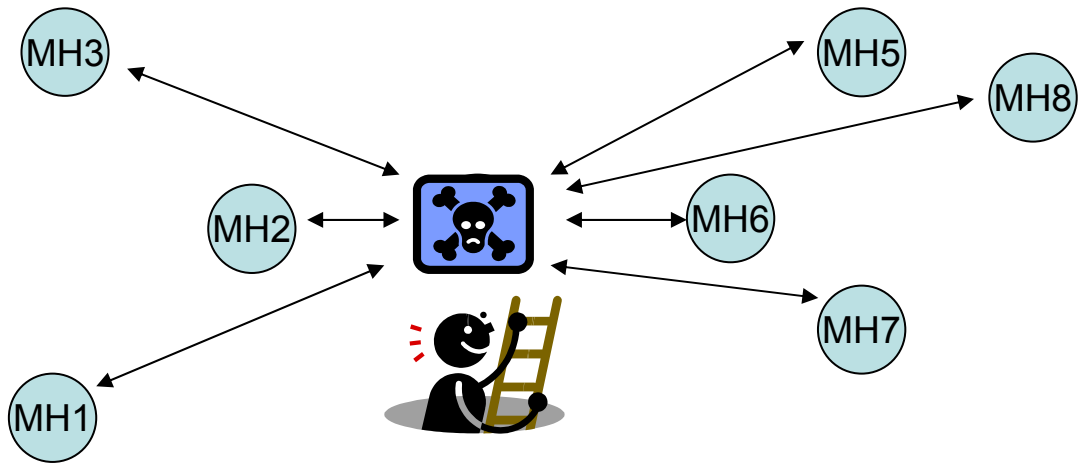
„Selektive Forwarding“

- *Annahme:*
  - Unverfälschte Weitergabe der Information über alle Knoten
- *Angriffstrategie:*
  - „falschen“ Knoten im Netz einschleusen
  - Kein Weiterleiten oder Manipulation der Informationen
  - Allerdings: Schnell durch Nachbarknoten aufzudecken
  - Also: selektives Weiterleiten oder Manipulieren



„Sinkholes“

- *Annahme:*
  - Manipulation eines Knotens
- *Angriffsstrategie:*
  - Anlocken des Verkehrs aus der Umgebung:
    - Leistungsstarker Transceiver
    - Vorgaukeln einer geringen Entfernung zur Basisstation
- *Effekt:* „Schlucken“ aller Nachbarinformationen
- *Grundlage für:*
  - „Selektive Forwarding“

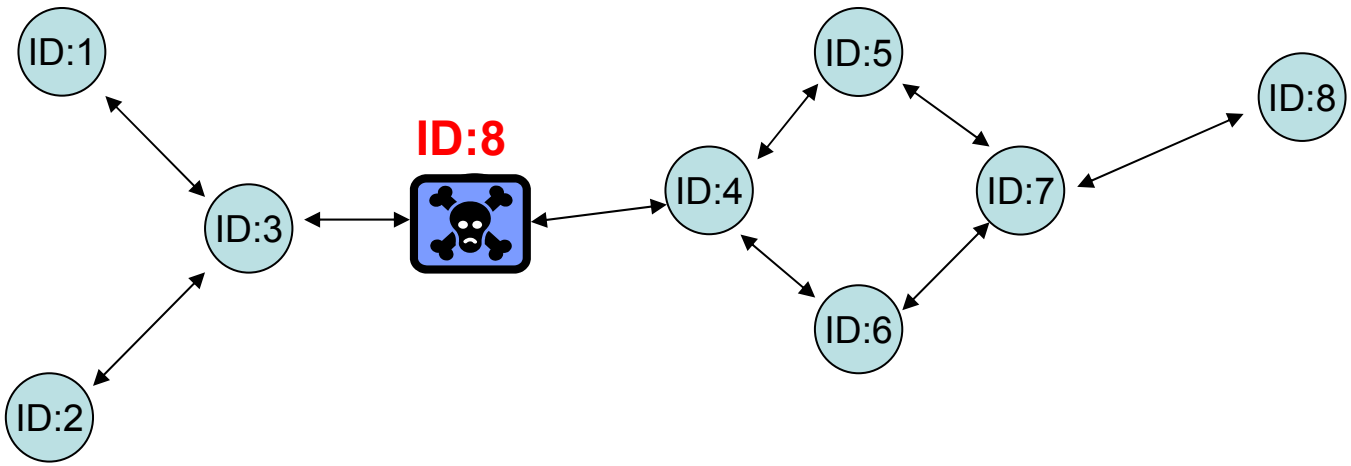


„Wormholes“

- *Annahme:*
  - Manipulation von mindestens zwei Knoten
- *Angriffsstrategie*:
  - Weiterleitung an einen weit entfernten Knoten
  - → Wormhole durch z.B.:
    - drahtgebundenes Netz (Unsichtbares Netz)
    - Erhöhte Sende-, Empfangsleistung zweier Knoten
  - „Ausspucken“ des Paketes in das Netzwerk
- *Effekt:*
  - Tunnelung der Informationen durch deutlich kürzerer Verbindungen
- *Vorteil:*
  - Funktion auch mit verschlüsselten oder authentifizierten Paketen
- *Grundlage für:*
  - „Sinkholes“
  - „Selektive Forwarding“
  - Kontrolle großer Netzwerkteile

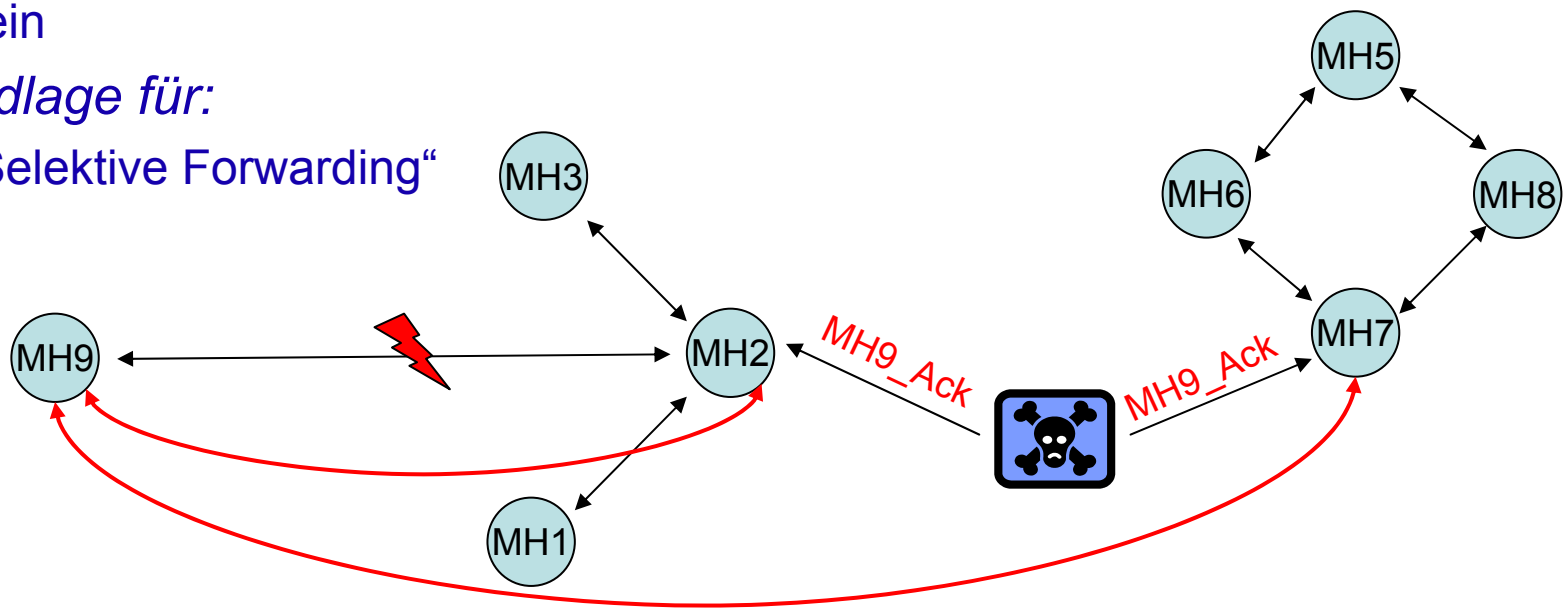
„Sybil-Angriff“

- *Annahme:*
  - jede NodeID existiert einmalig im Netz
- *Angriffstrategie:*
  - „feindlicher“ Knoten verwendet existente ID‘s und „schluckt“ Pakete
- *Grundlage für:*
  - “Selektive Forwarding“
  - Zerstörung von Strukturen geografischer Routingprotokolle



„Acknowledgement Spoofing“

- *Annahme:*
  - Ack-Pakete dienen als Steuerbefehle
- *Angriffstrategie:*
  - Versendung falscher Ack-Pakete
  - Nicht- oder schwer erreichbare Knoten scheinen vollständig aktiv zu sein
- *Grundlage für:*
  - „Selektive Forwarding“



„Flooding“

- *Annahme:*
  - „feindlicher“ Knoten besitzt hohe Sendeleistung und genügend Energie
- *Angriffsstrategie:*
  - Versendung des Hello-Paketes zur Anmeldung am Netzwerk
- *Effekt:*
  - Durch sehr häufiges Versenden → DoS-Attacke
  - Durch Versenden mit hoher Sendeleistung → Bekanntmachung als Nachbarn bei sehr vielen weit entfernten Nachbarn
- *Vorteil:*
  - Versuch eines Nachbarn an „richtigen“ Nachbarn zu senden schlägt ebenfalls fehl, weil dieser auch an den falschen Knoten weiterleitet → Dominoeffekt

Beispiele

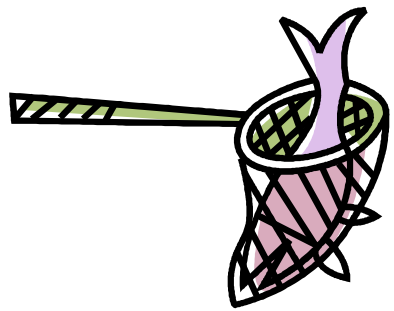
- Einführung von Routing-Updates, welche nicht der Spezifikation folgen

1. DSR
   - Veränderung der Originalroute
   - Gespeichert in RREQ oder RREP-Paketen
   - Löschen eines Knotens, Vertauschung der Reihenfolge oder Einführung eines neuen Knotens

2. AODV
   - Veränderung der Route durch Einführung kleinerer Metrik
   - Routing Updates mit einer hohen Sequenznummer und dadurch Neutralisierung aller gültiger Nachbarupdates

Sicherheit

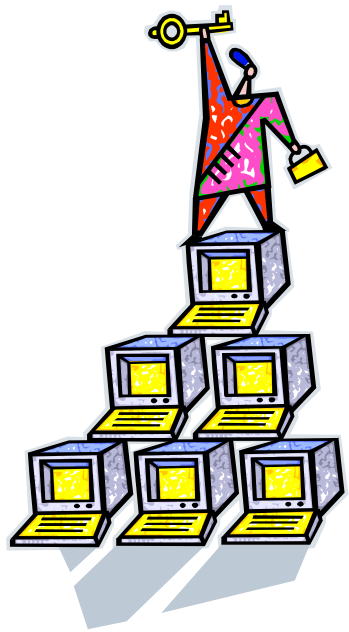
Gegenmaßnahmen



Global bekannter symmetrischer Schlüssel

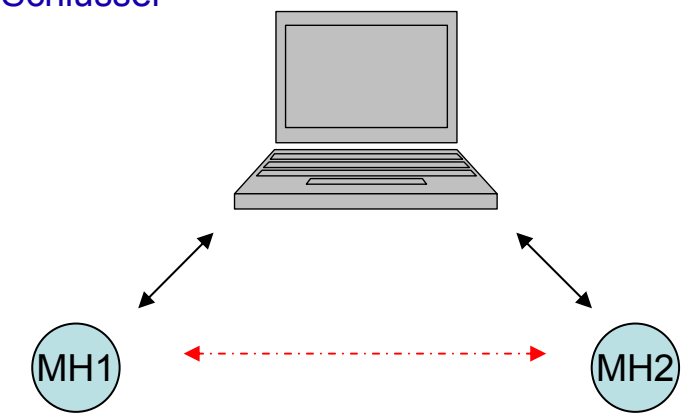
- „Link Layer“ Verschlüsselung und Authentifizierung
  - Verschlüsselung des gesamten Nachrichtenverkehrs
  - Angreifer haben nunmehr keinen Zugriff auf die Daten

- HOHER Schutz:
  - Gegen „Forwarding“ and „Sinkholes“
- WENIG Schutz:
  - Gegen „Flooding“ und „Wormholes“
- KEIN Schutz:
  - Gegen „Insider“



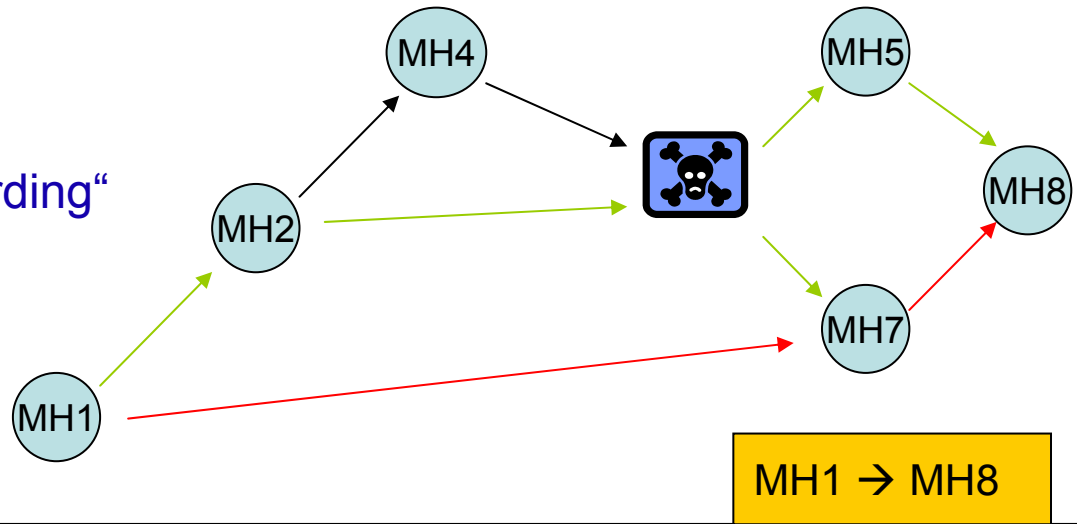
Basisstation mit geteilten Schlüsseln

- *Ansatz:*
  - *Vertrauenswürdige* Basisstation teilt mit jedem Knoten im Netzwerk einen gemeinsamen Schlüssel
  - Jeder Knoten verifiziert Pakete der Basisstation (Integrität, Authentizität, Geheimhaltung)
  - Sicherheit zwischen zwei Knoten:
    - Aushandelung eines Schlüssels mithilfe der Basisstation
    - Gegenseitige Bestätigung der Identität
- *Effekt:*
  - Überprüfung der Identität eines Knotens
  - Angreifer ist abhängig von Anzahl der „gestohlenen“ Schlüssel
  - Basisstation limitiert Anzahl der Nachbarknoten
- HOHER Schutz:
  - Gegen „Sybil“ und „Flooding“
- MITTEL Schutz:
  - Gegen „Wormholes“
  - Gegen „Insider“



Multipath Routing

- *Ansatz:*
  - Nutzung mehrerer Pfade
  - Auswahl eines Pfades durch Zufall
- *Effekt:*
  - Angreifer kann sich nicht einfach entlang eines bestimmten Pfades platzieren
- HOHER Schutz:
  - Gegen „Selektive Forwarding“



Packet Leashes

- Leash → Angehängte Information an ein Paket
- *Ansatz:*
  - Beschränkung maximaler Entfernung des Paketes

1. Geografischer Leash
   - Sender fügt eigene Position und Zeitpunkt des Versendens an
   - Empfänger berechnet maximale Entfernung des Paketes aus:
     - Eigene Position
     - Ankunftszeit
     - Maximalgeschwindigkeit eines Sensorknotens
     - Zeitabweichung
   - Wenn Empfänger außerhalb des Bereichs:
     → „Wormhole“ detektiert!

Packet Leashes

2. Zeitlicher Leash
   - Paket bekommt begrenzte Lebenszeit
   - Hohe Uhrensync. Nötig
   - Empfänger vergleicht Ankunftszeit mit Sendezeit

- *Nachteil:*
  - „falscher“ Knoten überspringt einfach Überprüfung

- MITTLERER Schutz
  - Gegen „Wormholes“

Digitale Signatur (Elektronische Unterschrift)

- *Grundlage:*
  - Asymmetrisches Kryptosystem (RSA)
- *Angriff:*
  - Angreifer verfälscht Dokument (Integrität, Authentizität in Gefahr)
- *Abwehrstrategie:*
  - Unterzeichner besitzt geheimen (privaten) Schlüssel
  - Empfänger besitzt bekannten (öffentlichen) Schlüssel
  - Empfänger überprüft Unterschrift
- *Bsp.:*
  - PGP (E-Mail), S/MIME

Das RSA-Kryptosystem ist ein asymmetrisches Kryptosystem, d.h. es verwendet verschiedene Schlüssel zum Ver- und Entschlüsseln. Es ist nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman benannt.

Digitale Signatur - Bewertung

- Pro:
  - Nachweis über Integrität und Authentizität
  - Jeder Knoten kann mit den öffentlichen Schlüsseln verifizieren
  - Benötigte Schlüsselanzahl bei Nutzung von paarweise geteilten Schlüsseln:

$$2n$$

- Contra:
  - Gehört der öffentliche Schlüssel dem Unterzeichner?
  - Anfällig gegenüber DoS-Angriffen (falsche Dokumente spammen)
  - Aufwand: Signieren/Entschlüsseln, Verifizieren/Verschlüsseln
  - Jeder Knoten benötigt „Certificate Revocation List“

Fazit

- Derzeitig existierende Routing Protokolle sind weitestgehend ungeschützt
- Notwendigkeit von einfachen, rechenarmen Konzepten
- Standards müssen entwickelt werden
- Sicherheit erfordert immer zusätzliche Belastung des Energieverbrauchs

Referenzen

- Stajano, Frank: *Security for Ubiquitous Computing.* Wiley Series in Communications Networking & Distributed Systems; 2002
- Fischer, Lars: *Routing in MANETS.* Seminar „Sicherheit in Ad-Hoc Netzen: Protokolle und Anwendungen“, TU Darmstadt
- Yang, Hao: *Security In Mobile Ad Hoc Networks: Challenges And Solutions.* IEEE Wireless Communications
- Karlof, Chris; Wagner, David: *Secure routing in sensor networks: Attacks and countermeasures.* In SNPA, 2003
- http://www.cwc.oulu.fi/~hernia/linkit.html

Vielen Dank!

Gibt es Fragen?