Sicherheit in drahtlosen Umgebungen

2. Deutsche KuVS Summer School: Sicherheit in Netzen und verteilten Systemen

Dirk Westhoff
NEC-Europe Ltd.

zusammen mit…

Krishna Paul (IIT Bombay), *Andre Weimerskirch*, (Uni Bochum), *Ingo Riedel* (Uni Bochum), *Marc Plaggemeier* (Uni Bonn), *Joao Paulo Barraca* (Uni Avero), *Joao Francisco de Lima Lobo Girao* (Uni Avero), Amer Aijaz (Uni Stuttgart), *Bernd Lamparter* (NEC-E Ltd.)

Projekt…

IPonAir NEXT GENERATION WIRELESS INTERNET

http://www.iponair.de

Agenda…

Zellulare Netzwerke

- Paketurheberverifikation am Zugangsrouter

Ad Hoc Netzwerke

- Kooperation in Ad Hoc Netzwerken
  - Wert
  - Detektion vs. Motivation
  - ein motivationsbasierter Ansatz
  - Empfehlungen zum Einsatz dig. Signaturen

Sensor Netzwerke

- ‘Zero-Common Knowledge’ Authentikation

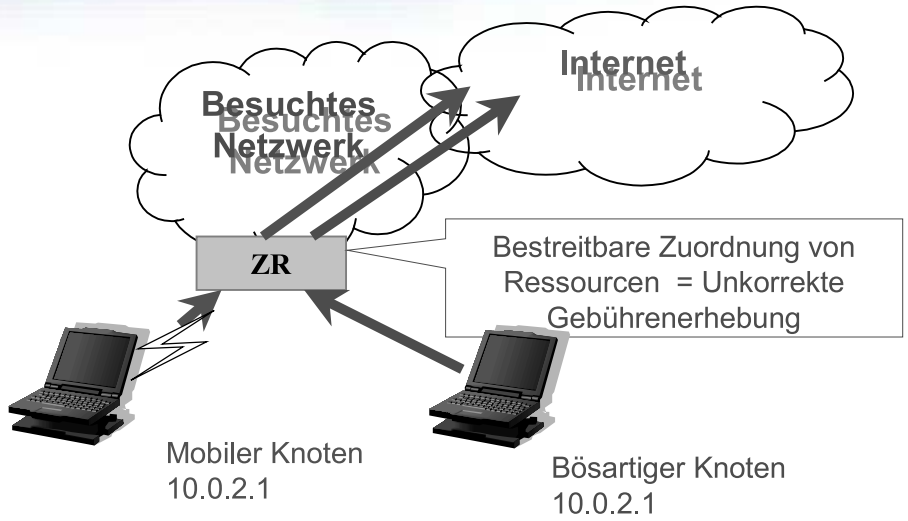
Agenda…

Zellulare Netzwerke

- Paketurheberverifikation am Zugangsrouter
- Kooperation in Ad Hoc Netzwerken
  - Wert
  - Detektion vs. Motivation
  - ein motivationsbasierter Ansatz
  - Empfehlungen zum Einsatz dig. Signaturen
- ‘Zero-Common Knowledge’ Authentisierung

Paket-Urheberverifikation am Zugangsrouter

Szenario und Problem:



- „IP-Catching“: IP-Adresse kann auf dem drahtlosen Medium gelesen werden
- Knoten können kostenfrei Daten senden

Paket-Urheberverifikation am drahtlosen Zugangsrouter

Problemformulierung:

Finde ein Daten-Authentisierungsverfahren, das

- (begründbar) sicher,
- robust,
- kostengünstig,
- geeignet für verschiedenste drahtlose Zugangstechnologien

ist.

Kontakt: NEC Europe Ltd. Mobile Internet Group

Paket-Urheberverifikation am drahtlosen Zugangsrouter

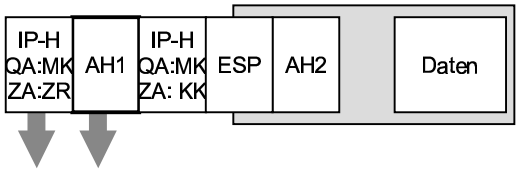
Kandidaten:

- L 2: - E.g. IEEE 802.11 a/b WEP: Stromchiffrat: RC4+IV
  - ETSI HIPERLAN/2: Blockchiffrat: DES-OFB+CRC optional und leicht zu brechen [Borisov et. al]

  => zu unsicher
- L3: IPsec verursacht 12-59% Datenüberschuss bei Echtzeitverkehr

  => folgende Folie

L3 IPsec Ansatz:



Datenüberschuss von bis zu 59% der Paketgrösse

- L4: SSH,SSL,TLS überträgt IP-Adresse in Klartext

  => kein Schutz gegenüber Quell- und Zieladresse

Allgemein: Automatische Schlüsselverteilung problematisch...

Paket-Urheberverifikation am drahtlosen Zugangsrouter

Unsere Lösung:

- Kostengünstige Paket-Urheberverifikation

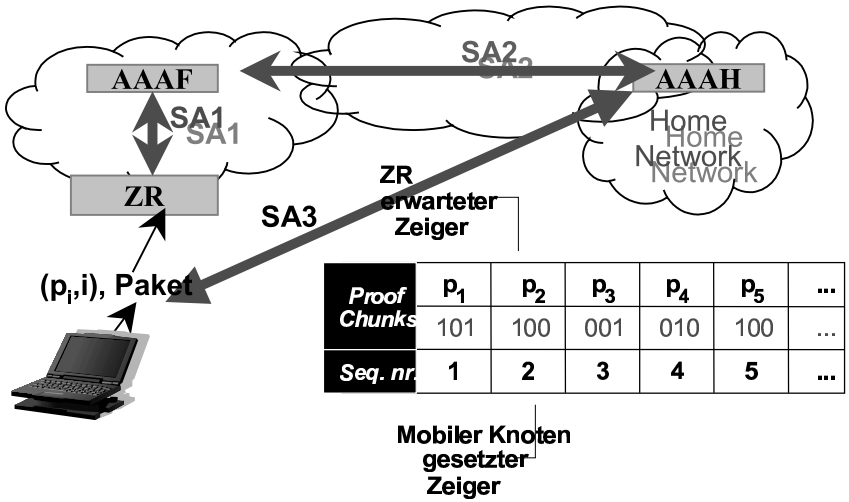
  - verursacht weit weniger Überschuss als IPsec Tunnel Modus
  - erweiterbar zu volumen-basierter Datenzuordnung am ZR
  - unterstützt Zuordnung auch im Falle von zell-abhängigen Wechsel der IP-Adresse (MIP + IPsec ESP)

⇒unterstützt Echtzeitverkehr über verschiedene Zugangs-technologien

Paket-Urheberverifikation am drahtlosen Zugangsrouter

Unvorhersehbare Bits:

- Bei initialer Geräte-Authentisierung AAAH:
  stellt MK und ZR Zufalls Bit-Strom
  $r=b_1,\ldots,b_n$
  bereit
- MK:
  generiert für das *i*-te Paket
  -Beweis $p_i := b_{(i-1)|p|+1},\ldots,b_{i|p|}$
  -Reihenfolgenummer *i*
- Zugangsrouter (ZR):
  - braucht (p_i,i) nicht zu entschlüsseln. Nur ein kostengünstiger Vergleich von p_i ist notwendig.
  - nach Vergleich Zeiger |p| Positionen weiter.



Kontakt: NEC Europe Ltd. Mobile Internet Group

Paket-Urheberverifikation am drahtlosen Zugangsrouter

Eigenschaften (1):

- Betrugsaufdeckung:
  böswillige Modifikation resultiert in zusätzlichem Vergleich auf dem gegenwärtigen Beweis p_i (an ZR)

- Robustheit:
  - ZR behandelt Paketverlust durch *explizites* lesen von *i* nach einem einzelnen negativen Vergleich (i muss sich immer erhöhen!!)
  - zwei negative Vergleiche decken Betrug auf
  - auch dem Verlust eines Bündels von Paketen kann so begegnet werden

Paket-Urheberverifikation am drahtlosen Zugangsrouter

Eigenschaften (2):

- Korrektheit:
  Wahrscheinlichkeit erfolgreich böswillig Pakete zu senden:

  - einzelnes Paket: $Pr(E_i) = 2^{-|p|}$

  - *m* sequentielle Pakete: $Pr(E_{i+1} \wedge, \ldots, \wedge E_{i+1}) = 1/2^{|p|m}$

Beispiel: **p=1/2B, m=10**

ein Paket: Pr()=1/16,
sequentielle Pakete $Pr() = 10^{-11}$

Paket-Urheberverifikation am drahtlosen Zugangsrouter

Eigenschaften (3):

„Hop-by-Hop“ Erweiterungs-Kopf:

Next Header	Length =0r	Opt. Type =x	Opt. Len. =0	Opt. Data **={pi},i**	PadN. =1i	Length =1	Value= 0

Reihenfolge-Nummer und Beweis:

	‚Spitzen' Paketverlust							
Verlust rate	2	3	4	5	6	i_{max}	|i|	|p|
$3*10^{-1}$	0.09	0.027	0.0081	0.00243	0.00072	>6	4	4
$2*10^{-1}$	0.04	0.008	0.0016	0.00032	-	>5	4	4
10^{-1}	10^{-2}	10^{-3}	-	-	-	>3	3	5
10^{-2}	10^{-4}	-	-	-	-	>2	3	5
10^{-5}	10^{-10}	-	-	-	-	2	2	6

- Kosten:
  - geringer Kopf-Überschuss von 8 Byte,
  - Verifikation per ‚Vergleich‘ günstiger als Berechnung

Gewinn:

	Paketlänge [Byte]			
	108	160	200	512
IPsec [%]	59.0	40.0	32.0	12.0
Unvorher. Bits [%]	8.3	5.6	4.5	1.7
Gewinn [Punkt]	50.7	34.4	27.5	10.3

Kontakt: NEC Europe Ltd. Mobile Internet Group
© Dirk Westhoff (dirk.westhoff@ccrle.nec.de)

Paket-Urheberverifikation am drahtlosen Zugangsrouter

Grenzen und Erweiterungen:

- DoS: böswilliger Knoten kann Re-Authentisierung erzwingen
- Pseudo-Zufallszahlen-Generator für MK und ZR:
  -nur initiale Bits anstatt Zufallsbitstrom über das drahtlose Medium

Ergebnisse:

- Patent (Japan, USA, Deutschland)
- prototypische Implementation unter Linux
- Publikationen: ITR, ICQT‘03

Agenda…

- Paketurheberverifikation am Zugangsrouter

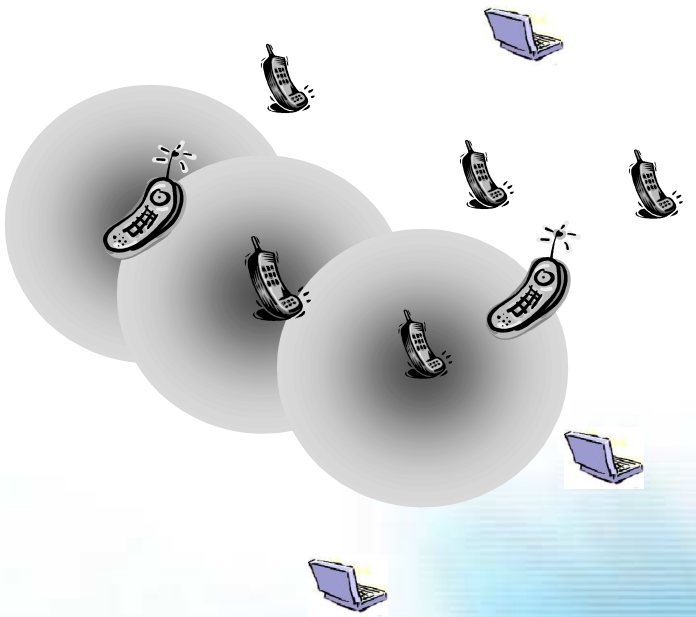
Ad Hoc Netzwerke

- Kooperation in Ad Hoc Netzwerken
  - Wert
  - Detektion vs. Motivation
  - ein motivationsbasierter Ansatz
  - Empfehlungen zum Einsatz dig. Signaturen
- ‘Zero-Common Knowledge’ Authentisierung

Ad Hoc Netzwerke...

- selbst-organisierend
- Knoten senden, empfangen und/oder **leiten weiter**
- drahtloses Medium
- Knoten migrieren

=> Kooperation !!!



Kontakt: NEC Europe Ltd. Mobile Internet Group
© Dirk Westhoff (dirk.westhoff@ccrle.nec.de)

Problem, Bedarf und Partizipationsmodell

Kooperationsverfahren…

- Fragwürdig ob Kooperationsverfahren tatsächlich vorteilhaft für die Gemeinschaft sind
- Bedarf an rationaler Abschätzung durch statistische Evaluierung

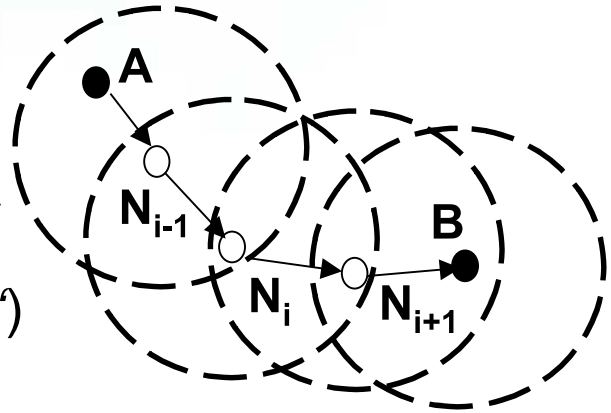
Einfaches Partizipationsmodell…

- Pro Übertragung entscheiden Knoten Daten weiterzuleiten oder fallen zu lassen
- Verhältnis Weiterleiten zu Verwerfen ist gleichverteilt über alle Knoten.

insbesondere: ‚*Gray hole attack*' (Knoten partizipieren in ‚route discovery' Phase verwerfen aber Pakete in der ‚forwarding' Phase

Auswirkung einer Partizipationserhöhung (1)…

Ereignisse und Wahrscheinlichkeiten…



- $Pr(E^i_p) = e$, und $e \in [0,1]$
- $E^i_{p,p'}$: Knoten N_i leitet in Gegenwart von p und p' weiter
- E^i_p: Knoten N_i leitet in Gegenwart von p weiter (nicht p')
- $Pr(E^i_{p,p'}) = e+\Delta e$, und $\Delta e \in [0,1-e]$

Ankunftswahrscheinlickeit…

Einfluss von p' auf die am Zielknoten empfangenen Pakete:

- $Pr(.)$ in **Abwesenheit** von p': $Pr\,(E^1_p \wedge,\ldots,\wedge E^n_p) = e^n$ mit $lim\ e^n=0$
- $Pr(.)$ in **Gegenwart** von p': $Pr\,(E^1_{p,p'} \wedge,\ldots,\wedge E^n_{p,p'}) = (e+\Delta e)^n$ mit $lim(e+\Delta e)^n=0$

Beobachtung (1)…

gleich welches $\Delta e \in [0,1-e]$ p' verursacht hat ($e+\Delta e=1$ praktisch irrelevant)

$\Rightarrow$ absolute Einfluss von p' ist vernachlässigbar für ‚grosses' n

Auswirkung einer Partizipationserhöhung (2)…

Einfluss bei begrenzter Zahl von Zwischenknoten…

- *T:*= minimale Ende-zu-Ende Verfügbarkeit des Netzwerks

$$e^n = T \Rightarrow n = \ln T / \ln \quad \text{resp.} \quad (e+\Delta e)^n = T \Rightarrow n = \ln T / \ln(e+\Delta e)$$

- *absolute* (Δn_a) und *relative* (Δn_r) Erhöhung der Erreichbarkeit:

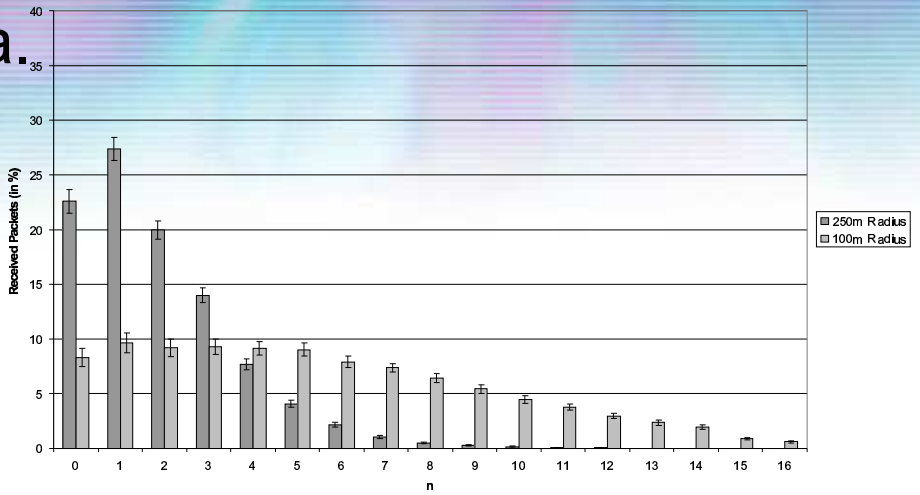
$$\Delta n_a = \frac{\ln T}{\ln(e+\Delta e)} - \frac{\ln T}{\ln e} \qquad \Delta n_r = \frac{\frac{\ln T}{\ln(e+\Delta e)} - \frac{\ln T}{\ln(e)}}{\frac{\ln T}{\ln e}}$$

Beobachtung (2)…

- der relative und absolute Einfluss von Δe auf die allgemeine Erreichbarkeit ist
  - *unterproportional* für kleines Δe
  - *überproportional* für grosses Δe
  - *mit 'geeignetem' e, kann auch ein kleines Δe sich überproportional auf die Erreichbarkeit auswirken*

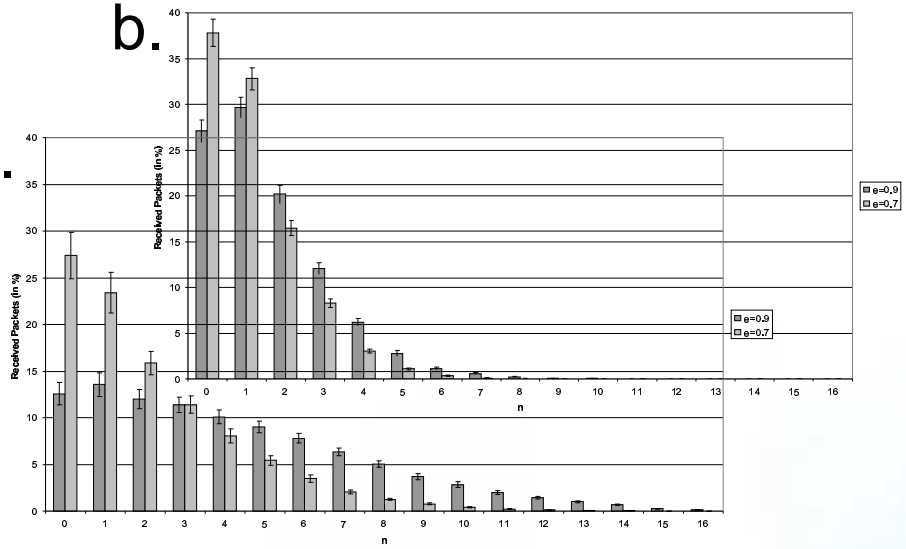
Simulation…

a.



b.

c.



Keine egoistischen Knoten

- durchschnitt. Pfadlänge (fig. a):
  - nicht mehr als max. 6 Hops (250m Radius)
  - bis zu 16 Hops (100m Radius)

Egoistische Knoten mit/ohne Kooperation

- T=0.6, e=0.7, und $\Delta e = 0.0$ oder $\Delta e = 0.2$:
  - 250m Radius (fig. b)
    ohne *p'* : 49.7% Verkehr erreicht Ziel
    mit *p'* : 91.3 % Verkehr erreicht Ziel
  - 100m Radius (fig. c)
    ohne *p'* : 17.5% Verkehr erreicht Ziel
    mit *p'* : 44.7% Verkehr erreicht Ziel

Bestätigung der 2. Beobachtung

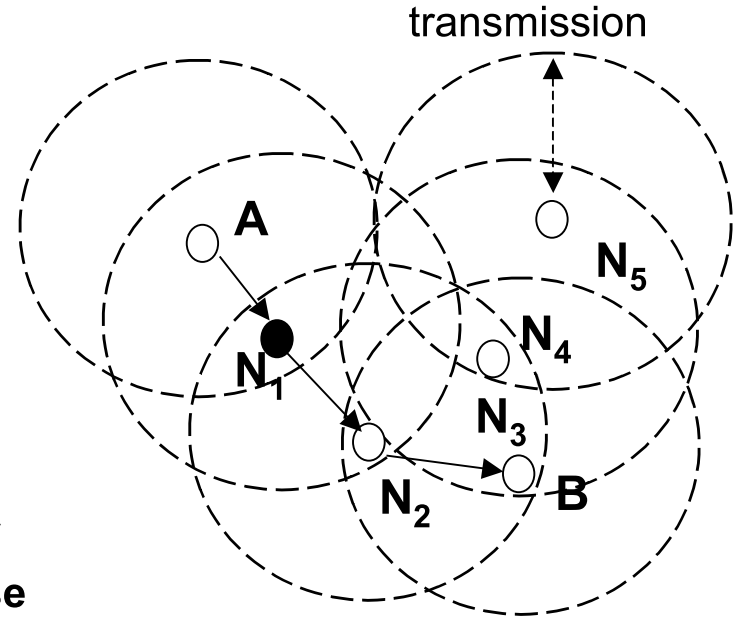
- auch kleines $\Delta e (= 0.2)$ kann die Erreichbarkeit drastisch erhöhen, wenn das e(=0.7) geeignet ist

Uni Bonn
ISCHE FRIEDRICH-WILHELMS-UNIVERSITÄT
Kontakt: NEC Europe Ltd. Mobile Internet Group
© Dirk Westhoff (dirk.westhoff@ccrle.nec.de)

Detektionsbasierter Ansatz...

Route Schutz:

- Gleichwichtig wie Datenschutz (Knoten agieren als Router)
- Bei DSR können Knoten Routeinformationen manipulieren
- Manipulationsmöglichkeiten in
  - **Route Request Phase**,
  - **Route Reply Phase**, or
  - **Data Forwarding Phase**
- Angriffsarten
  - **Aktiv destruktiv**,
  - **Aktiv 'sinnvoll'**, oder
  - **Passiv 'egoistisch'** (Verwerfen von Paketen)



$S(N_2)=\{N_1,N_2,N_3,N_4\}$
$S^*(N_2)=\{N_1,N_2,N_3,N_4\}\backslash N_2$

Bedarf: Angst-basiertes Bewusstsein bösartiger Knoten
=> Aktionen werden beobachtet und 'schwach'-abstreitbar bewertet

Detektionsbasierter Ansatz...

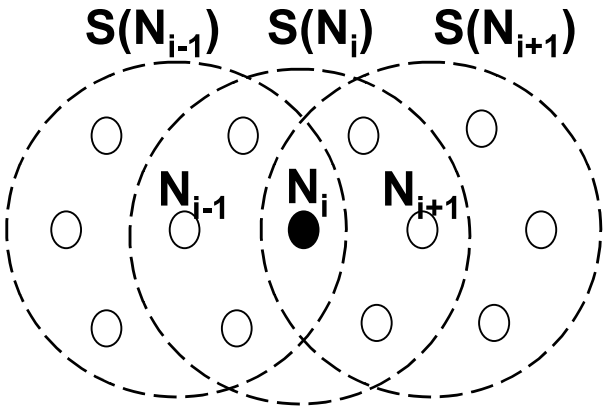
Route Schutz:

1. A -> N_1 wobei N_1 aus S*(A):
   RREQ:= [A:B] || h(A:B,r)
2. N_{i-1} -> N_i wobei N_i aus S*(N_{i-1}):
   RREQ:= [A:B] || N_1 ,…,N_{i-1} || h(N_{i-1},h(…h(A:B,r)…)
3. N_n -> B wobei B aus S*(N_n):
   B berechnet Hash und vergleicht mit empfangenen

Ergebnisse:

- B hat Garantie dass kein N_i vorherige Einträge N'_1,…,N'_{i-1} aus RREQ manipuliert hat
- B kann Angriff erkennen; er kann jedoch nicht den Angreifer erkennen
  => Zwischenknoten sollten beobachten

Detektionsbasierter Ansatz...



Sets $S(N_{i-1})$, $S(N_i)$, and $S(N_{i+1})$

Angriffe in der Anfragephase:

- **Präfix Angriff:**
  $RREQ=[A:B]||N_1,\ldots,N_{i-1},N'_i,\ldots,N'_j,N_i||\ h(N_i,h(\ldots h(A:B,r)\ldots),$
- **Präfix Angriff mit falschem Hash:**
  $RREQ= [A:B]||N'_i,\ldots N'_j N_i||h(N_i,h(\ldots h(A:B,r)\ldots),$
- **Suffix attack:**
  $RREQ= [A:B]||N_1,\ldots,N_{i-1},N'_i,\ldots,N'_j||h(N'_j,\ h(\ldots h(A:B,r)\ldots)$ oder
  $RREQ= [A:B]||N_1,\ldots,N_{i-1},N_i,N'_i,\ldots,N'_j\ ||\ h(N'_j,h(\ldots h(A:B,r)\ldots)$

wobei (j>=0).

Angriffe in der Anfragephase: Aufdeckung

Präfix Angriff, Suffix Angriff und Angreifer sind erkennbar von

- **$INT = S(N_{i-1}) \cap S^*(N_i)$** : Präfix und Suffix Angriff -> 1) unicast SECM nach A
- **$REST = S^*(N_i) - [S(N_{i-1}) \cap S^*(N_i)]$** : nur Suffix Angriff -> 2) keine Pfad nach A und B

1) Stabil und 2) hoch bei Gleichverteilung von Knoten (zumindest Knoten aus INT informieren A).

Detektionsbasierter Ansatz...

Inferenz Mechanismus

- Mehrheitswahl, 'schwach'-abstreitbar, defensiv, gleiche Prioritaet in Raum-Zeit Kontext,
- funktioniert nur bei >3 empfangenen Anklagen

Route Response and Route Maintenance

- RREP ist statisch => Marti et al.
- N_i sendet bösartig LBR nach A
- N_{i+1} erkennt Angriff mit Empfang von LBR
- $S^*(N_i) \cap S(N_{i+1})$ senden SECM wenn sie $A(N_i)$ von N_{i+1} empfangen nachdem sie LBR von N_i empfangen

$S^*(N_i) \cap S(N_{i+1})$:

I_D: If SECMs indicate LBR attack
Case I_{D1}: A t least n (=3) messages contain $A(N_i)$ **then** $C(N_i)$,
Else: no culprit detectable

Route Request

INT and REST:

I_A: If SECMs indicate suffix attack, **then**
CaseI_{A1}: At least n (=4) claims contain $A(N_i)$ & all of them contain same original RREQ, **then** $C(N_i)$,
CaseI_{A2}: If only a single node N accuses N_i, **then** C(N)
Else: no culprit detectable

INT and REST:

I_B: If SECMs indicate prefix attack or prefix attack with incorrect hash, **then**
CaseI_{B1}: At least n (=3) claims contain $A(N_i)$ & all of them contain same original RREQ, **then** $C(N_i)$,
Else: no culprit detectable

N_{i-1}:

I_C: If SECMs indicate drop attack
CaseI_{C1}: At least n (=3) claims contain $A(N_i)$ & all of them contain same original RREQ **then** $C(N_i)$,
CaseI_{C2}: Only N_{i-1} sends A (N_i) and at least n (=2) other nodes sends $A(N_{i-1})$ & all of them contain same original RREQ, **then** $C(N_{i-1})$,
Else: no culprit detectable

Motivationsbasierter Ansatz...

Was veranlasst Knoten an der Ad-Hoc Gemeinschaft zu partizipieren?

- keine Routeinformation zu manipulieren,
- keine Pakete zu verwerfen,
- nicht die Identität zu wechseln, oder
- vor Angriffen die keinerlei Gewinn bringen?

Ad-hoc Netzwerk mit Zugang zum Festnetz…

Ist es für den ISP möglich ein 'win-win' Geschäftsmodell zu propagieren, das

- Teilnehmer motiviert ein Ad-hoc Netzwerk zu formen,
- Ad hoc Knoten kommunizieren nicht via Access Point (AP), oder
- in mehrfach Hop Weise via AP falls Zielknoten im Festnetz sitzt,

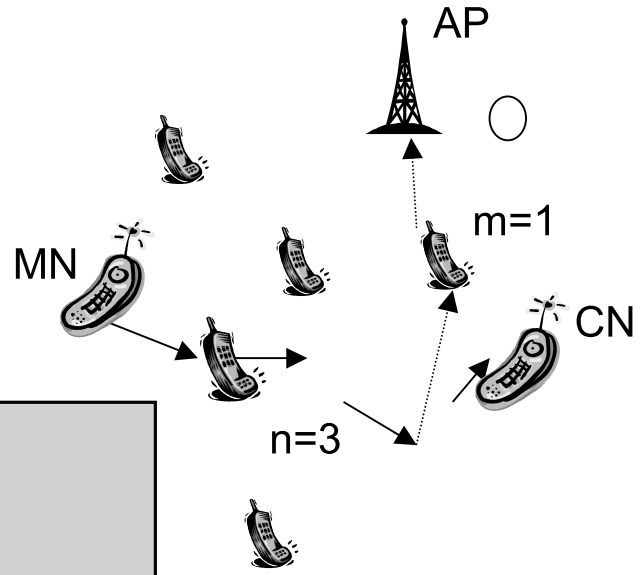
ohne dass

- ISP als Verlierer hervorgeht,

Geschäftsmodell...

Motivation

- **Teilnehmer bewegen** ein Ad Hoc Netzwerk zu formen
- gleichzeitig **verdient ISP**
- **Knoten verdienen** fürs Weiterleiten
- **Integrierte Abrechnung** beim ISP



Bei Preis pro Einheit für **Senden** oder **Empfangen** (p^+),
und negativen Preis (Belohnung) pro Einheit fürs **Weiterleiten** (p^-),
ist das GM für ISP vorteilhaft, wenn

$$|2p^+| > |(n+m)p^-| \quad \text{(dezentral)}$$
$$|p^+| > |mp^-| \quad \text{(zentral)}.$$

- **volumenbasierte Gebühren**.

Secure Charging Protocol (1)...

SCP's Phasen:

Registrations Phase:
- Initiale Authentikation von MN

Forwarding Phase:
- Kommunikation zwischen MN und CN

Charging Phase:
- Kommunikation zwischen N_n und AP (zeitversetzt)

h()	un-keyed hash function
$h_X()$	keyed hash function with symmetric key from X and AP
(e_X, p_X)	public/private key pair of X
k_X	secret key between X and AP
$<e_X,X>_Y$	identity certificate issued for X by Y
$Sig_X(m)$	digital signature of message m from X with private key p_X

Kryptograpische Primitive

Secure Charging Protocol (2)...

Registration Phase:

1. **AAA Architektur:**
   - Authentikation beim ISP,
   - Verifikation des Heimatdomains,
   - Authorisationsinformationen zu MN

$\overline{\text{AAAH -> AP and MN}}$ (SA1,SA2,SA3):
$(e_{CA}, e_{MN}, p_{MN}, k_{MN}, p^{+}, p^{-})$
$<e_{MN},MN>_{CA}$

Forwarding Phase:

- Kommunikation zwischen MN und CN

Charging Phase:

- Kommunikation zwischen N_n und AP (zeitversetzt)
  Informationen zu
  - involvierten Zwischenknoten
  - Datenmenge

Secure Charging Protocol (3)...

Forwarding Phase:

2. Am Startknoten MN:

- Finde Route: On demand Source Routing Protocol
  => MN, N_1, N_2,…, N_n, CN

3. MN's ordentliche Registration:

MN sendet (zusammen mit Daten):

- Dig. Sig.: von MN mit MN, N_1, N_2,…, N_n, CN,
- Initiale hash Kette: 'keyed hash' über MN,CN
- Identitätszertifikat von MN (Registrationsnachweis)

$$[MN,CN],N_1,\ldots N_n,\ Sig_{MN}(h(N_1,\ldots,N_n)t),\ h_{MN}(MN,CN),<e_{MN},MN>_{CA}$$

4. An jedem Zwischenknoten:

- N_i prüft Signatur von MN
- 'keyed hash' für Nachfolger

5. Am letzten Zwischenknoten:

- wie alle anderen Zwischenknoten
- Dienstbestätigung: N_n prüft Schritt-für-Schritt Bestätigungen von CN

$$[MN,CN],N_1,\ldots N_n,\ Sig_{MN}(h(N_1,\ldots,N_n)t)\ h_{Ni}(\ldots(h_{N1}(h_{MN}(MN,CN))\ldots),<e_{MN},MN>_{CA}$$

6. Am Zielknoten CN:

- Bestätigung der Diensbereitstellung:
  CN signiert Betrag der von N_n erhaltenen Datenmenge

$$Sig_{CN}(no\_of\_data\_amount)t),<e_{CN},CN>_{CA}$$

Secure Charging Protocol (4)...

Charging Phase: **7.**

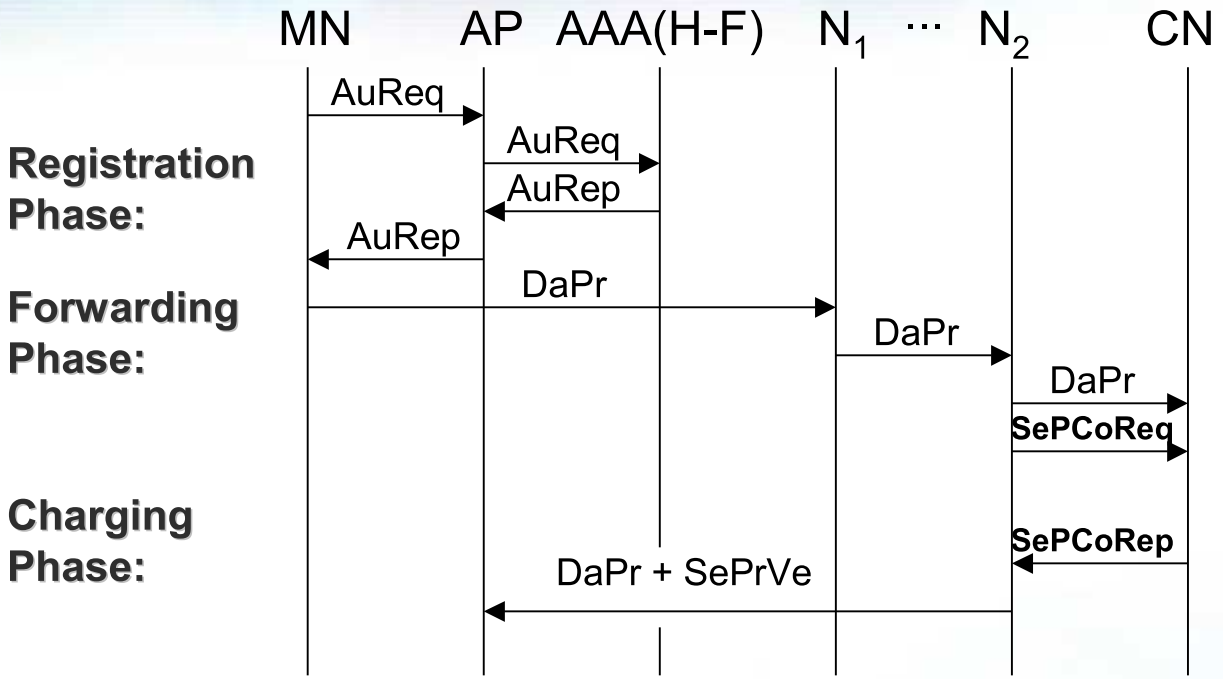
Am Zugangspunk AP

AP verifiziert Partizipation einzelner Knoten:

- hash chain Verifikation -> Belohnung für Zwischenknoten und Gebühren für Quelle und Ziel
- Signaturverifikation der Datenmenge -> Faktor
- $N_1,\ldots,N_n$ müssen explizit gesendet werden da die augenblicklichen Zwischenknoten $N_1,\ldots,N_m$ sind
- Signaldaten von N_n nach AP werden in gleicher Weise behandelt (AP und N_n nicht belastet)

$$[MN,CN],N1,\ldots Nn,Sig_{MN}(h(N1,\ldots,Nn)t)\ h_{Ni}(\ldots(h_{N1}(h_{MN}(MN,CN))\ldots),<e_{MN},MN>_C\ Sig_{MN}(No\_of\_data\_unit)_A$$

SCP Protokollspezifikation...



SCP Kontrollfluss

AuReq: type x001

type [3b]	MNcred.[16B]

AuRep: type x002

type [3b]	CAKey [64B]
Mnkeys [128B]	
sharedkey MN-AP [16B]	
current price [1B]	

DaPr: type x003, x006

type [3b]	Cert.flag [1b]
Hash chain [8B]	
Signature [64B]	
Certificate [500B]	

SePCoReq: type x004

type [3b]	Cert.flag [1b]
DataUnits [7b]	

SePCoRep: type x005

type [3b]	Cert.flag [1b]
Signature [64B]	
Certificate [500B]	

SePrVe: type x006

type [3b]	Signature [64B]
Hash chain [8B]	
Signature [64B]	
hops[1B]	Ad1-n [n*64B]

b:=Bit

B:=Byte

Paketformate

Angriffe ...

- DoS nicht Gegenstand (kein geldwerter Gewinn)
- MN und CN können Dienstnutzung nicht leugnen
- Aber: MN muss CN vertrauen
  (kann unnötig Daten bestätigen, unwahrscheinlich)
- Zwischenknoten können Gewinn steigern durch
  - Senden zusätzlichen Verkehrs
  - mehrfach involviert sein

  Erster Angriff bedarf allgemeiner Datenintegrität (Ende-zu-Ende Auth.)

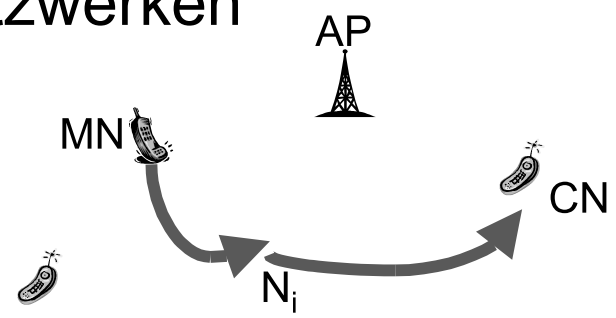
  zweiter Angriff resultiert oftmals in sub-optimaler Route
- konspirierende Angriffe brechen das Protokoll !!!

Pros/Cons asymmetrischer Authentisierung…

- **Pros:**
  - *Nicht-Abstreitbarkeit*: ‘Dienst der eine Entität davon abhält erteilte Bestätigungen oder Aktionen abzustreiten [Menezes]
  - *Skalierbarkeit*: *N* Schlüssel-Paare anstatt of *N(N-1)/2* Schlüssel für symmetrische MAC-basierte Verfahren
- **Cons:**
  - *Berechnungskosten*: Faktor 10^2 – 10^3 mehr Berechnungskosten gegenüber symmetrischen MACs
  - *Sicherheitsinfrastruktur* erforderlich (PKI, Schwellenwert Kryptographie, PGP-artige Ansätze)

Motivation für eine Analyse…

- ‘Neue’ Sicherheitsprotokolle in Ad Hoc Netzwerken
  - sicheres Routing
  - Fairness and Kooperation
  - Abrechnung etc.

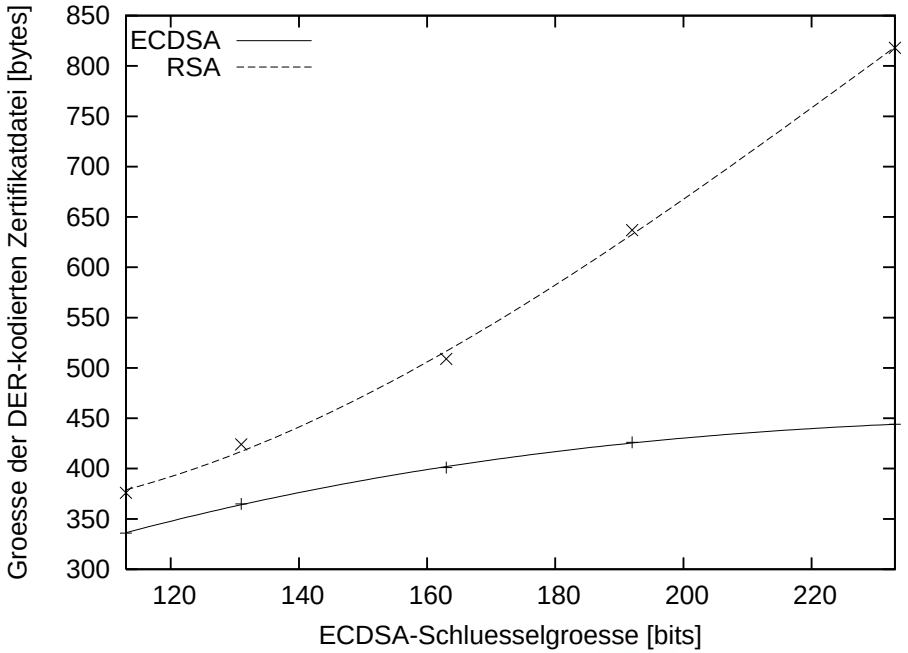


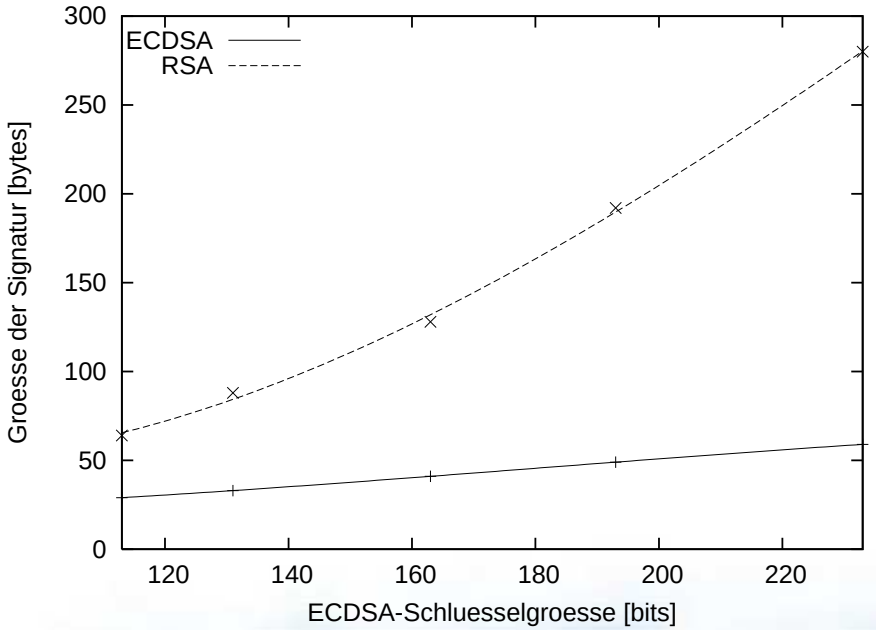
- Eigenschaften:
  - Mehr als zwei Teilnehmer explizit involviert
  - erforderliches Sicherheitsniveau and Sicherheitsdauerhaftigkeit eher gering
  - Teilnehmerrollen variabel

⇨ **Beispiele: *Sprite [Infocom03], SCP [Elsevier03]***
... zur geldwerten Abrechnung in Ad Hoc Netzwerken

Vergleich RSA vs. ECDSA (1):

(Datenvolumen)





⇨ECDSA entscheidend vorteilhaft bei hohem Sicherheitsniveau

⇨benötigte Bandbreite und Speicherplatz geringer

Vergleich RSA vs. ECDSA (2):

(Ausführungszeit)

Level of Security	Sign [ms]		Verify [ms]	
	RSA	ECDSA	RSA	ECDSA
512 bit	13.7	2.8	1.3	7.5
704 bit	32.4	3.8	2.5	11.5
1024 bit	78.0	5.7	4.3	17.9
1536 bit	251.9	7.6	9.7	26.0
2240 bit	731.8	10.1	20.4	37.3

Zielplattform

- **StrongARM CPU (Intel SA-1110) @ 206 MHz**
- **16 MB Flash-ROM**
- **64 MB RAM**
  - **32 MB for processes**
  - **32 MB for file storage**
- **Embedix Linux 2.4 OS**
- **WLAN Network Adapter**

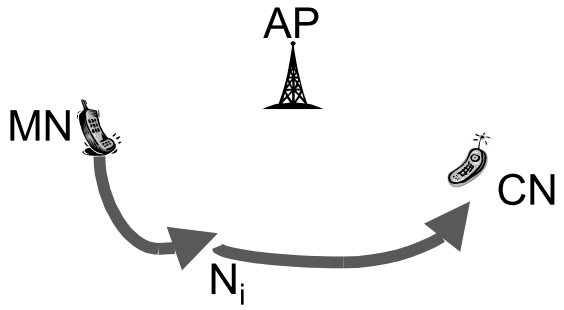
⇨**ECDSA ist schneller für SIGN**

⇨**RSA ist schneller für VERIFY**

Beispiele: SCP und Sprite…

SCP und Sprite:

- *MN* **signiert** jedes Paket
- N_1 bis N_n **verifizieren** jedes Paket



nur SCP:

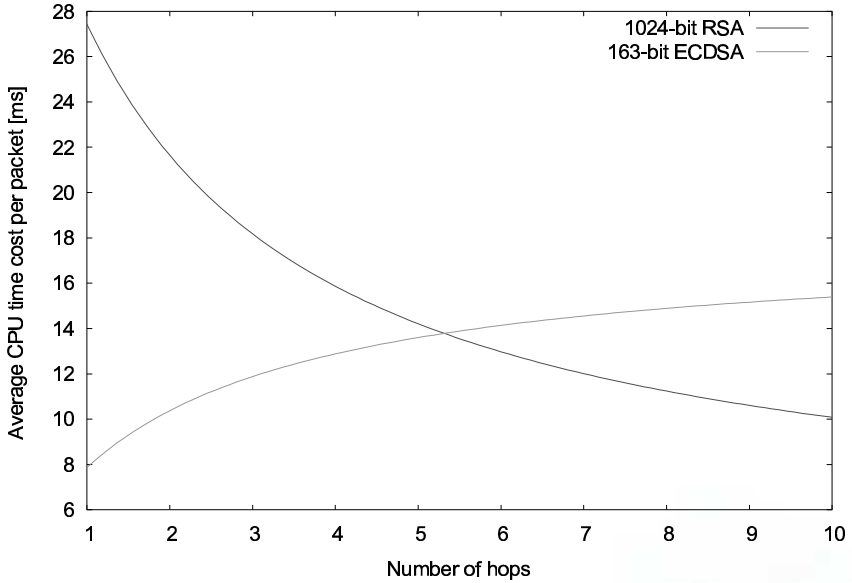
- *CN* **signiert** die empfangene Datenmenge
- N_n **verifiziert** Signaturen

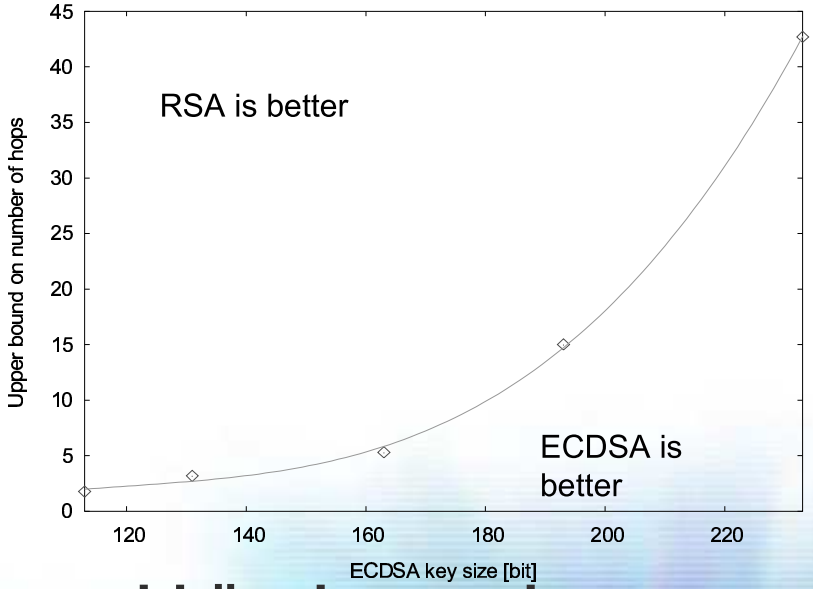
Vergleich RSA vs. ECDSA (3):
(CPU Kosten pro Knoten)

$$t(X)_{CPU} = P(X=S)t_g + \sum^{n}_{i=1} P(X=N_i)t_v + P(X=D)t_v$$

$$P(X=S)=P(X=N_i)=P(X=D)=1/(n+2)$$

- S,N,D:=Quelle, Ziel, Zwischenknoten
- n:= Anzahl Hops
- t_g t_v :=Zeiten Sig. Gen., Sig. Verifikation
- P := Wahrscheinlichkeit



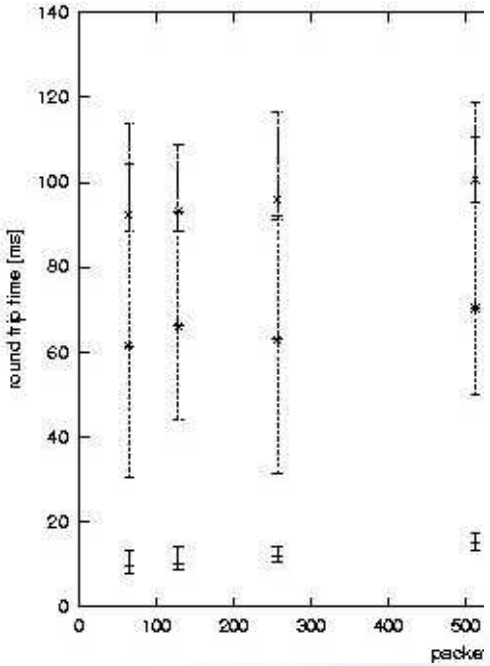


⇨Optimales Signaturverfahren abhängig von der Anzahl involvierter Knoten

⇨ECDSA besser für höheres Sicherheitsniveau

SCP Demonstrator:

Szenario:



- **4 PDAs (Abstand 50cm bis 10m)**
- **zwei Sitzungen, jede mit 50 Paketen unterschiedlicher Grösse**
- **‘round trip times’ und ‘jitter’ in Abwesenheit bzw. in Gegenwart von SCP (mit l=1 und l=2)**

⇨**bei moderater Knotenanzahl ist SCP kompatibel zu den verschiedensten Verkehrstypen…**

Sicherheitsniveau und Dauerhaftigkeit:

(geschätztes Jahr bis zu dem S-Niveau ausreicht)

Year	RSA key size	ECDSA key size
1999	512	113
2006	704	131
2015	1024	163
2026	1536	193
2039	2240	233

- **Internet Zugang im Supermarkt, Flughafen oder Bahnstation**
- **Teilnehmer bleibt nicht länger als 24 Stunden**
- **Geldwert weniger als 250€ pro Knoten**
- **Verteiltes Netzwerk von 300 Computern braucht 3.7 Monate um eine 512-bit RSA ‚Challenge Number' zu faktorisieren**
- **163-bit ECDSA ausreichend für Protokolle wie SCP oder Sprite die frühstens für 2008-2010 erwartet werden.**

⇨ **Kryptosystem braucht nur kurzzeitige Sicherheit zu bieten (24 h)**

⇨ **Angreifer wird nur Hardware mit moderaten Kosten verwenden**

Empfehlungen (1):

Skalierbarkeit der Sicherheitsrelationen (Anzahl Schlüssel)

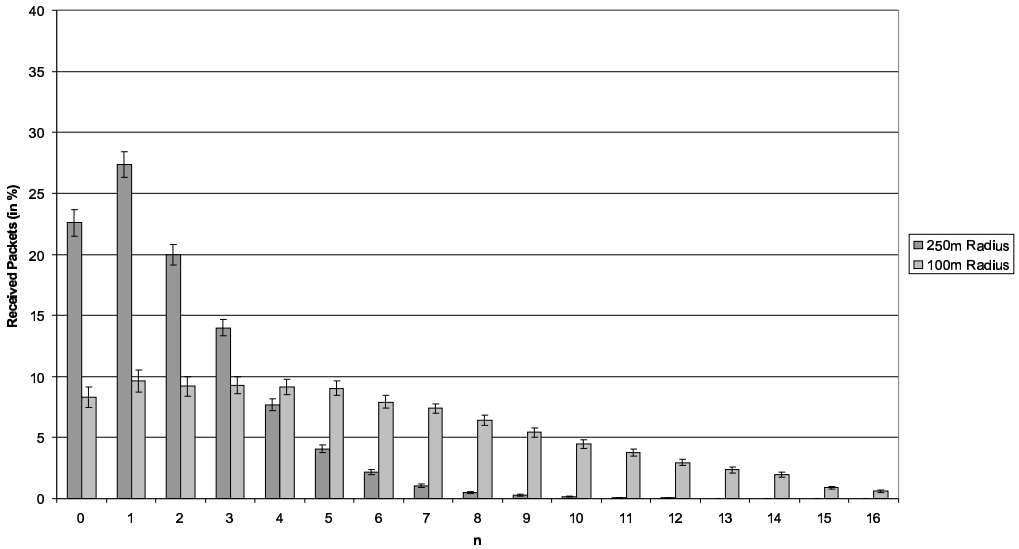
- ***unilateral*** **Auth. von *x* Urhebern geg. *y* Verifizierern (*x*→*y* bzw. *y*←*x*), *x,y*∈{*1,…,N*}**
- ***bilateral*** **Auth. von *x* Urherbern geg. *y* Verifizierern und umgekehrt (*x*↔*y*)**

	1→N	1←N	1↔N	N→N	N↔N	M→N	M←N	M↔N
Sig.	1	N-1	N-1	N	N	M	N	N
MAC	N-1	N-1	N-1	N(N-1)/2	N(N-1)/2	$\sum^{M}_{i=1}$ N-i,	$\sum^{M}_{i=1}$ N-i,	$\sum^{M}_{i=1}$ N-i

⇨Für N=100, und N→N oder N↔N 100 öffentliche/private Schlüsselpaare versus 4950 symmetrische Schlüssel
⇨Für eine Reihe von Sicherheitsbeziehungen skalieren dig.Sig. besser als MACs

Empfehlungen (2):

Topologie des Netzwerks **(Ausführungszeiten)**



Simulator:

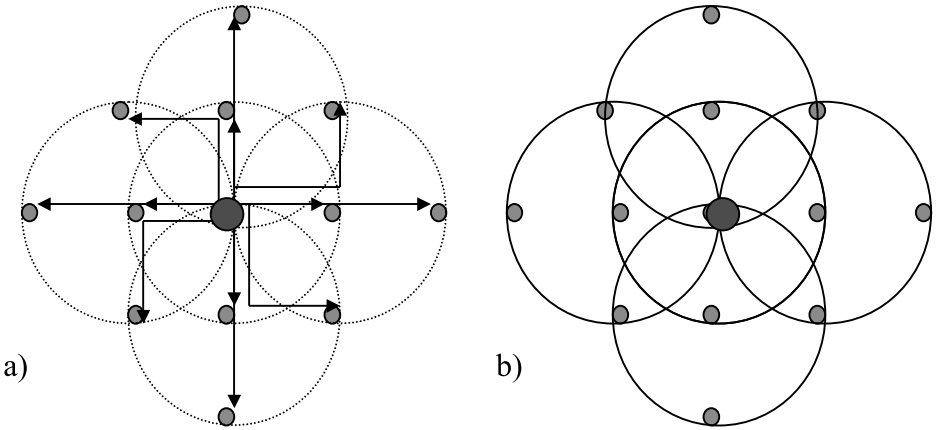
- **NS2**
- **N=100**
- **1000m x 1000m**
- **AODV**
- **random-waypoint 1-2m/2**
- **etc.**

⇨R=*250m*: mehr als 90% des Netzwerkverkehrs wird über weniger als fünf Zwischenknoten geleitet => ECDSA

⇨R=*100m*: nur ca. 41.5% des Netzwerverkehrs wird über weniger als fünf Zwischenknoten geleitet => RSA

Empfehlungen (3):

- *Teilnehmer Dynamik* **(Datenvolumen)**



a) Unicast N symmetrischer Schlüsselübereinkunftsinformation
b) Broadcast eines Zertifikats zu N Knoten in einer Topologie mit C=4 und l=2.

N	4	12	24	40	60	84	122	144
l	1	2	3	4	5	6	7	8
$\#_b$	1	5	9	17	25	37	47	62

- ● := **Neueinsteiger**
- **N :=** $=\sum_{i=1}^{l} i \cdot C$ **Anzahl Knoten**
- **C:= Konnektivität**
- **l := längster Pfad**
- **statisch und gleichverteilt auf quadratischem Areal**

⇨ $\mathbf{Cost_{MAC}=\sum_{i=1}^{l} 2i^2 \cdot C|d|}$ |d| := Grösse Schlüsselinformationen

⇨ $\mathbf{Cost_{Sig}= \#_b \cdot |c|}$ |c| :=Zertifikatsgrösse

⇨ **163-bit ECDSA S-Niveau: N>40 ECDSA Sig. besser als MAC**
N>84 RSA Sig. besser als MAC

Zusammenfassung:

	RSA	ECDSA
Netzwerk Topologie	mittlere bis grosse Routelängen	kleine Routelängen
Teilnehmerfluktuation	keine bis gering	keine bis hoch
mehrheitliche Operation	Signatur Verifikation	Signatur Generierung
gefordertes Sicherheitsniveau	schwach	schwach bis hoch
Verkehrsart	asynchron, zeitflexibel	auch synchron und echtzeitkonform

⇨In Ad Hoc Netzwerken ist ECDSA nicht zwingend beste Wahl

(im Gegensatz zu 'einfachen drahtlosen Hop)

⇨Aber: ECDSA flexibler

⇨In bestimmten Szenarien ist RSA die bessere Wahl

Kontakt: NEC Europe Ltd. Mobile Internet Group
© Dirk Westhoff (dirk.westhoff@ccrle.nec.de)

Agenda…

- Paketurheberverifikation am Zugangsrouter
- Kooperation in Ad Hoc Netzwerken
  - Wert
  - Detektion vs. Motivation
  - Charging Unterstützung
  - Empfehlungen

Sensor Netzwerke

- ‘Zero-Common Knowledge’ Authentikation

Einteilung

- Einleitung
- ‘Zero Common-Knowledge’ (ZCK) Authentikations Verfahren
- ‘Key-Chain’ Verfahren
- Komplexitäts Vergleich
- Zusammenfassung

Einleitung

- (Ad-hoc und) Sensor Netzwerke haben grosse Sicherheitslücken
  - drahtloses Medium
  - keine Infrastruktur
  - Geräte sind extrem resourcenbeschränkt

- Beobachtung
  - Authentisierung unbekannter Entitäten nicht möglich
  - schwächere Authentikationsformen reichen möglichlicherweise aus

Beispiel

- Zwei Fremde begegnen sich…
- keinerlei Infrastruktur, kein Reisepass
- Etablieren Schritt für Schritt eine Vertrauensbeziehung aufgrund persönlicher Erfahrung
- Beide möchten sich zumindest wiederkennen können…
- $\Rightarrow$ denkbar in P2P Netzwerken

Definition, Voraussetzungen und Ziele

Definition:

- *ZCK authentication*: A kann B ohne gemeinsames Vorwissen B ‘authentizieren’ wenn A die Entität B ‘wieder’erkennen kann.

Voraussetzung:

- *Pure network*: Weder ein zentraler Dienst noch eine fixe Infrastruktur existieren
- *Beschränkte Geräte*: keine weiteren Annahmen wie ‘manipulationssicher’ oder ‘eindeutige ID’

Ziel:

- ZCK Authentisierung in rein drahtlosen Netzwerk mit schwachen Geräten
- Anwendungen: Routing Protokolle, Kooperation, P2P

ZCK Authentisierungsverfahren

	Alice		Bob
1:		PK ←	wahlfrei *SK*
2:	wahlfrei *r*	*r* →	
3:		$(r)_{SK}$ ←	berechne $(r)_{SK}$
4:	$((r)_{SK})_{PK} = r$? Wenn 'ja', *akzeptiere*, andernfalls *verwerfe*		

- **Auch zur Authentisierung von Nachrichten denkbar (ersetze2-4):**

2':		$(m)_{SK}$ ←	$(m)_{SK}$
3':	$((m)_{SK})_{PK} = m$? Wenn 'ja', *akzeptiere*, andernfalls *verwerfe*		

Realisierung

- Symmetrisches Verfahren (MAC)
  - sehr effizient
  - verlangt geographische Nähe fuer Schlüsselaustausch, bzw. vertrauenswürdige Instanz
- Assymmetrische Verfahren (dig. Signatur)
  - sehr flexibel und funktional
  - Aber: leistungsstarke Geräte (PDA,Handy)
- 'Key-chain' Verfahren
  - Fast so effizient wie symmetrisches Verfahren
  - Bietet ZCK (Nachrichten) Authentisierung

‘Key-Chain’ Verfahren: Idee

- Nutze 2 ‘key-chains’ (eine Bob, eine Alice)
  $k_n \leftarrow k_{n-1} \leftarrow \ldots \leftarrow k_0$ mit $h(k_i) = k_{i+1}$
- privat k_0, öffentlich k_n
- Alice und Bob tauschen das letzte Element k_n einer Schlüsselkette
- Zur A*uthentisierung:*
  Alice und Bob zeigen Wissen über vorherige Elemente der Kette
- Zur *Nachrichten Authentisierung*:
  Alice nutzt MAC mit k_{i+1} und beweist Wissen über k_i

Key-Chain Verfahren

	Alice		Bob
1:	public key x_n^A	→	stores $(x_n^A, n', 1)$
2:	stores $(x_n,^B, n, 1)$	←	public key $x_n,^B$
Wiederhole für jede Authentikation:			
3:	A stores (x_i^B, j, u)		B stores (x_j^A, i, v)
4:	(+) MAC(m, x_{j-u-1}^A)	→	
5:	(+)	←	MAC(m, x_{i-v}^B)
6:	open x_{j-1}^A	→	check if h$(x_{j-1}^A) = x_j^A$
7:	for k=1 to $k' \leftarrow \max\{u, v\}$ repeat		
7.1:	check if h$(x_{i-k}^B) = x_{i-k+1}^B$	←	open x_{i-k}^B
7.2:	open x_{j-k-1}^A	→	check if h$(x_{j-k-1}^A) = x_{j-k}^A$
7.3:	If *failure*,		
	store $(x_i^B, j, \max\{u, k+1\})$		store $(x_j^A, i, \max\{v, k+1\})$
8:	store $(x_{i-k},^B, j-k'-1, 1)$		store $(x_{j-k'-1}^A, i-k', 1)$

Bemerkungen

- Oeffentlicher Schlüssel ist beim ersten Kontakt gebunden an einen Dienst (nicht Gerät)
- A muss *B*'s öffentlichen Schlüssel speichern, der dann verknüpft ist mit vorherigen Erfahrungen
- Man-in-the-middle Angriff möglich aber bedeutungslos
  - Alice etabliert Vertrauensbeziehung zum Dienstanbieter
  - Bedeutungslos ob es Bob ist oder man-in-the-middle solange Alice mit dem Dienst zufrieden ist
  - Man-in-the-middle nach Schlüsselautausch nicht mehr möglich
- Protokoll kann leicht zu beidseitiger Authentisierung erweitert werden

Komplexität

	Key-Chain	Public-Key	Sym. Key
Public-key size (bytes)	24	‡	10†
Exchanged messages	3	2	2
Exchanged bytes	30	‡	20
Computational effort	0	2 PK Op.	0
ZCK authentication	x	x	x
Message authentication	x	x	x
ZCK non-repudiation	-	x	-
Key-exchange	-	x	-
Signature	-	x	-
Mutual authentication	x	o	o

‡ depends on the used public-key scheme
† size of the shared key

'x' : provided
'-' : not provided
'o': with modifications (at higher cost)

Kontakt: NEC Europe Ltd. Mobile Internet Group
© Dirk Westhoff (dirk.westhoff@ccrle.nec.de)

Zusammenfassung

- Vorgeschlagene Basisauthentisierung in ‘pervasive networks’
- Drei Realisierungen:
  - Public-key Verfahren: am flexibelsten und funktional aber zu rechenaufwändig
  - Symmetric-key Verfahren: am effizientesten, aber bedarf entweder geograpische Nähe oder gemeinsamer Vertrauensauthorität
  - Key-chain scheme: fast so effizient wie symmetrisches Verfahren ohne dessen Nachteile

Demnächst…

BMB+F Projekt **SicAri*** (ab 1.Oktober 2003)

- Implementierung ZCK-Authentisierung für Mica Nodes unter TinyOS
- Poset Analyse…
- Simulation bzgl. Skalierbarkeit und ‘Bits-Per-Joule’ Bedarf

http://www.cs.berkeley.edu/~jhill/tos/

…

*EineSicherheitsarchitektur und deren Werkzeuge zur ubiqitären Internetnutzung

Einige Arbeiten...

B. Lamparter, C. Paar, A. Weimerskirch, D. Westhoff, *On Digital Signatures in Ad Hoc Networks*, eingereicht zu IEEE Journal on Selected Areas in Communications, 'Wireless Ad Hoc Networks', 4th Quarter 2004.

A. Weimerskirch, D. Westhoff, Identity Certified Zero-Common Knowledge Authentication, ACM Workshop on Security of Ad Hoc and Sensor Networks in conjunction with the Tenth ACM Conference on Computer and Communications Security, ACM SASN'03, Oktober 2003.

A. Weimerskirch, D. Westhoff, *Zero-Common Knowledge Authentication for Pervasive Networks*, Selected Areas in Cryptography, SAC'03, Springer-Verlag LNCS 28??, August 2003, Ottawa, Ontario, CA.

B. Lamparter, K. Paul, D. Westhoff, *Charging Support for Ad Hoc Stub Networks*, Elsevier Journal of Computer Communication, Special Issue on 'Internet Pricing and Charging: Algorithms, Technology and Applications', Elsevier Science, Vol. 26, Issue 13, August 2003.

B. Lamparter, M. Plaggemeier, D. Westhoff, *About the impact of Co-operation Approaches for Ad Hoc Networks*, Extended abstract, ACM MobiHoc'03: The Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing, Annapolis, Maryland, USA, June 2003.

B. Lamparter, D. Westhoff, *A Low-Cost Packet Originator verification for Metering Access-Routers*, Third International Workshop on Internet Charging and QoS Technology (ICQT'03), Springer-Verlag LNCS 2816, September 2003, Munich, Germany.

K. Paul, D. Westhoff: *Context Aware Detection of Selfish Node in DSR based Ad-hoc Network*, IEEE GLOBECOM 2002, Taipei, Taiwan, Nov. 2002.

B. Lamparter, I. Riedel, D. Westhoff, *Anmerkungen zur Nuztung digitaler Signaturen in Ad Hoc Netzwerken*, Praxis der Informationsverarbeitung und Kommunikation, Themenheft: Mobile Ad Hoc Netzwerke, Dezember 2003.

Vielen Dank…