Anonymisierung von MAC Adressen

Max Riegel

2014-11-23

Ankündigung

- **Anonymisierung von MAC Adressen**

Die MAC Adresse ist beim WLAN eine fest zugeordnete Endgerätekennung, die von WLAN Betreibern häufig dazu ausgenutzt wird, ein Bewegungsprofil des Endgeräts und damit auch des Benutzers zu erstellen. Der Vortrag stellt die aktuelle Diskussion zur dynamischen Vergabe von MAC Adressen an Endgeräte vor. Damit können Geräte und Benutzer nicht mehr anhand der MAC Adresse verfolgt werden.

Inhaltsübersicht

- **Das Problem**
  - Daten zur Laufkundschaft
  - Gefährdung der Privatsphäre
  - Erkennbarkeit von WLAN Geräten
- **MAC Adressen**
  - Format und Registrierung
- **Lösungsansätze**
  - Zuweisung von zufälligen MAC Adressen
  - Notwendige Mechanismen
- **Standardisierungsbemühungen**
  - IEEE P802c
  - Pilotversuche
- **Ausblick und Diskussion**

Anonymisierung von MAC Adressen

DAS PROBLEM

WLAN ist Teil unseres täglichen Lebens

- **Die mobilen WLAN Geräte sind ein Teil von uns**
- **WLAN wird im öffentlichen Bereich eingesetzt**
- **Mobile WLAN Geräte sind immer und überall aktiv**
- **Über unsere mobilen WLAN Geräte sind wir immer und überall erkennbar**

Wissen ist Macht (…und Geld)

- **Der Wert von Google, Twitter, Facebook, … beruht auf dem Wissen um Menschen**
  - …was sie tun, mit wem sie kommunizieren, was sie denken, wofür sie ihr Geld ausgeben
  - Leider ist die räumliche Zuordnung im Internet etwas schwierig
- **Das Bewegungsprofil von Menschen hat einen besonderen Wert**
  - Der größte Umsatz wird immer noch lokal in Geschäften, Restaurants, Veranstaltungen gemacht
  - Alle sind bereit, Geld für genauere Informationen über ihre Kunden auszugeben
  - … um so mehr, je anonymer die Kunden sind (‘Laufkundschaft’)
- **Betreiber von öffentlichem WLAN haben begonnen, systematisch mobile WLAN Geräte zu verfolgen**
  - Auswertung von Kommunikationsdaten zur Erstellung von möglichst individuellen Profilen.

Gefährdungspotentiale der Privatsphäre

Gefährdungspotentiale

- Überwachung
  - Beobachtung und Verfolgung der persönlichen Kommunikation
  - Gezielte Ausspähung
    - Maßnahmen ermitteln nur die Kommunikationsdaten einer Einzelperson
  - Massenhafte Überwachung
    - Alle Kommunikation wird aufgezeichnet und ausgewertet
- Ausspähung von persönlichen Daten
  - Unberechtigter Zugriff auf persönliche Daten die in Systemen abgelegt sind
- Beeinträchtigung der persönlichen Kommunikation
  - Belästigung durch Spam oder Verhinderung durch mutwillige Eingriffe
- Verfälschung von persönlicher Kommunikation
  - Fehlzuordnung von Kommunikationsdaten durch Manipulation von Informationselementen

Angriffspunkte der Privatsphäre

Aspekte

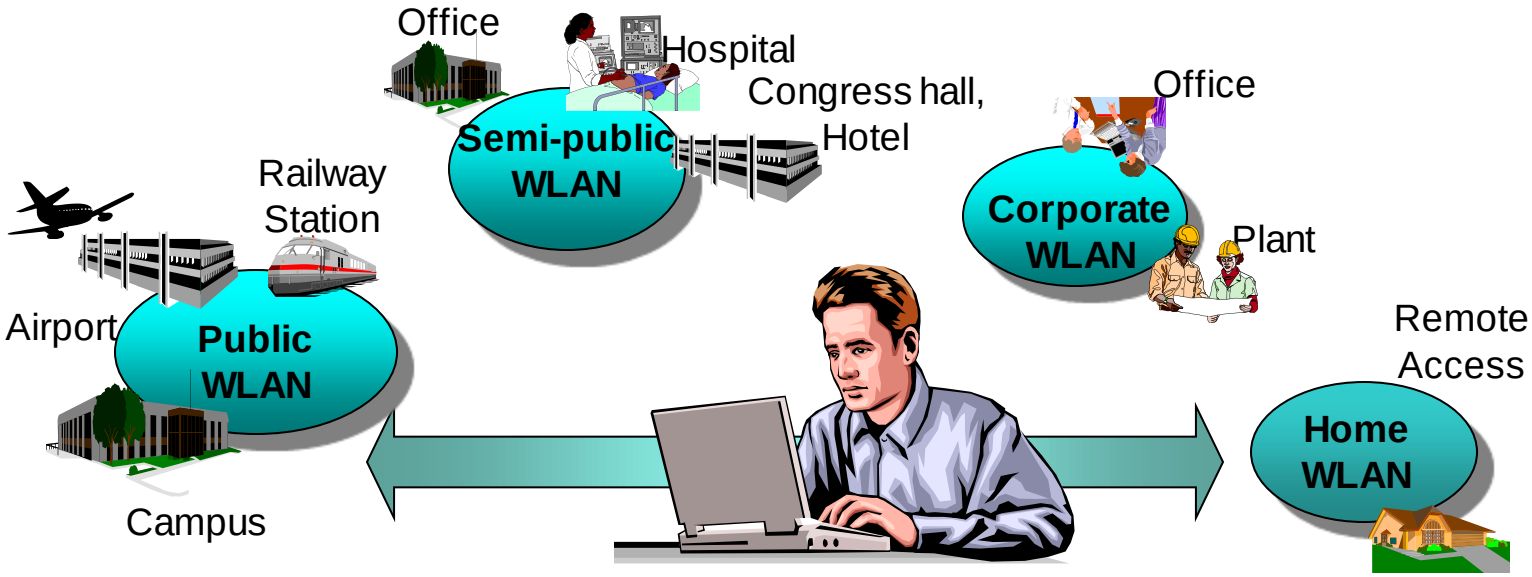
- Korrelation
  - Zusammenfügen und Verbinden von verschiedenen Informationen zur Gewinnung von Mustern
- Identifizierung
  - Zuweisen von Informationen zu einer einzelnen Person/Einheit
- Zweit-/Wiederverwertung
  - Gebrauch von Informationen zu anderen Zwecken als ursprünglich vorgesehen
- Offenlegung/Veröffentlichung
  - Private (vertrauliche) Information anderen zugänglich machen
- Übergehen/Ausschluss
  - Personen werden nicht über die Existenz und Verarbeitung persönlicher Daten in Kenntnis gesetzt

Referenzen zur Privatsphäre im Internet

- **RFC 6973 - Privacy Considerations for Internet Protocols**
  - http://tools.ietf.org/html/rfc6973
- **Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement**
  - http://tools.ietf.org/html/draft-iab-privsec-confidentiality-threat-00
- **RFC 7258 - Pervasive Monitoring is an Attack**
  - http://tools.ietf.org/html/rfc7258

Identifizierung von Geräten im WLAN

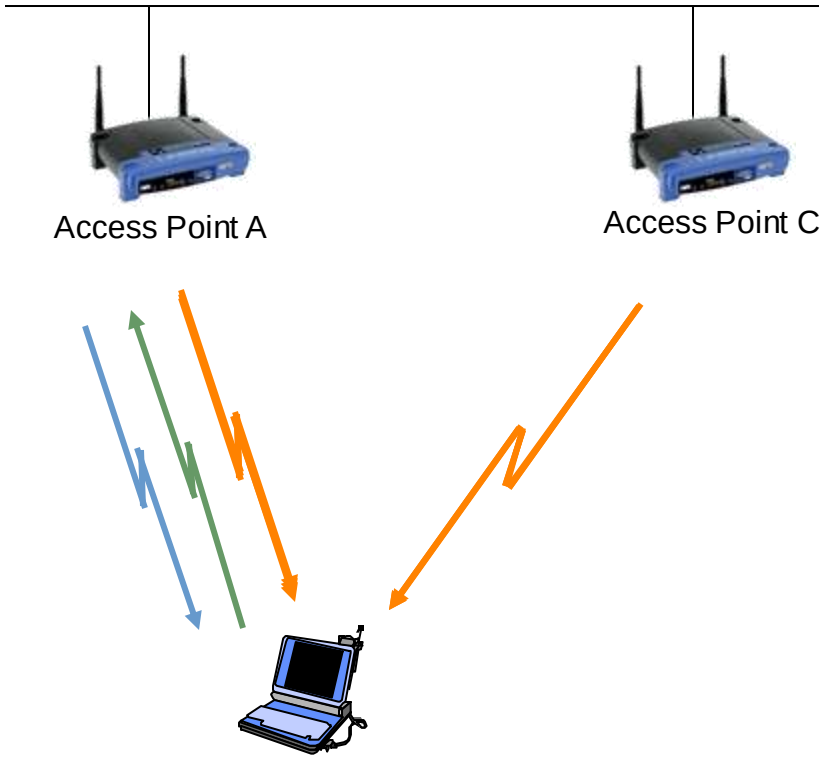
- **Alle Geräte im WLAN haben eine eindeutige Kennzeichnug.**
- **Diese Kennzeichnung wird bereits sichtbar, noch bevor das Gerät in das WLAN eingebucht ist.**



- **Durch die WPA2-PSK/WPA2-Enterprise Verschlüsselung können zumindest die übertragenen Daten nicht mitgelesen werden.**
- **Technisch bedingt sind die Absenderadresse und die Empfängeradresse immer offen lesbar.**

Einbuchen ins WLAN, Variante 1: *Passive Scanning*

- **Initiale Verbindungsaufnahme zu einem Access Point**
  - Reassociation erfolgt nach ähnlicher Prozedur



Schritte zur Verbindung:

APs schickt *Beacons*.

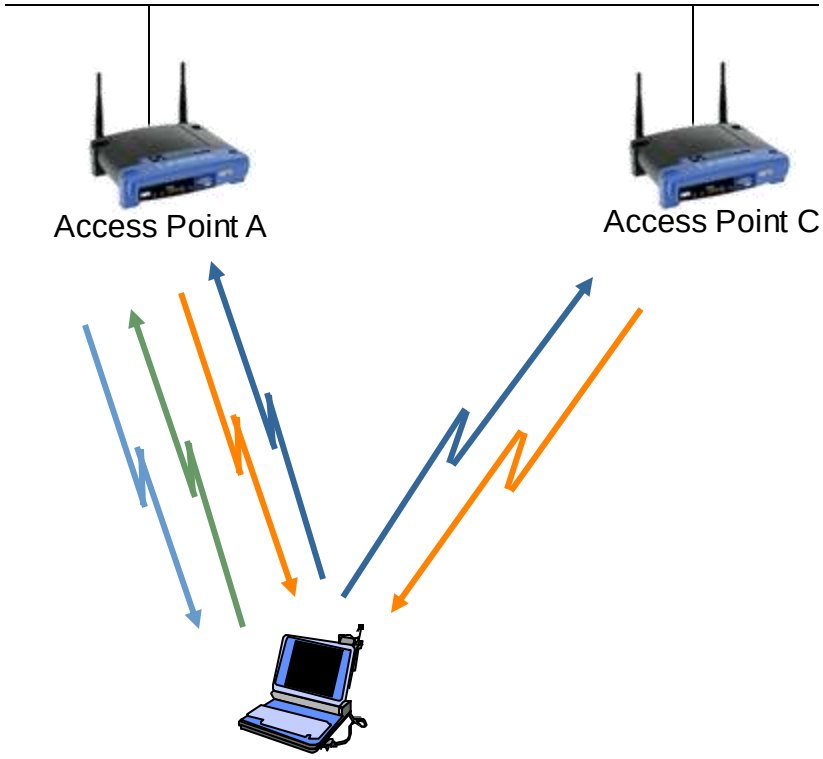
Station wählt besten AP aus.

Station schickt Association Request zum gewählten AP.

AP antwortet mit Association Response.

Einbuchen ins WLAN, Variante 2: Active scanning

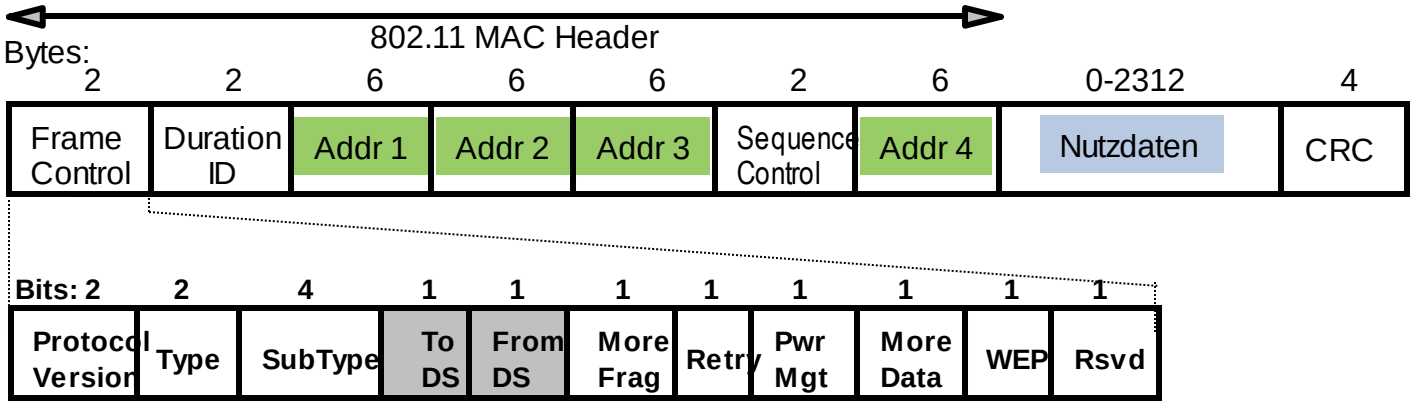
- **Wenn es schnell gehen soll oder die passende SSID nicht sichtbar ist, wird aktiv nach dem passenden WLAN gesucht:**



Schritte zur Verbindung:

- Station schickt *Probe Req*.
- APs antworten mit *Probe Resp*.
- Station wählt besten AP aus.
- Station schickt *Association Request* zum gewählten AP.
- AP antwortet mit *Association Response*.

IEEE802.11 Übertragungsrahmen



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

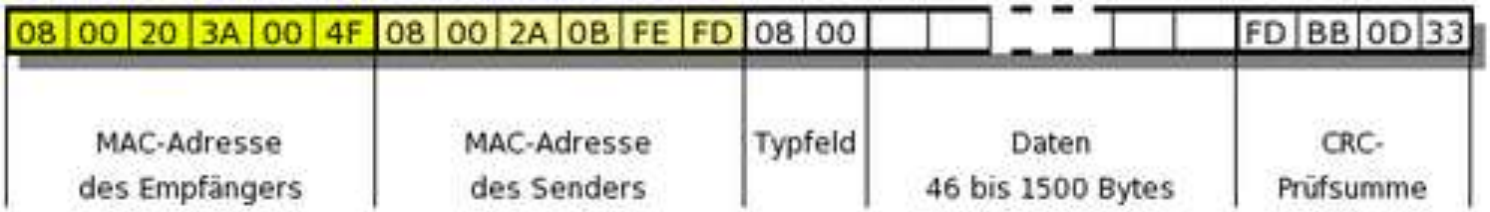
- **Addr 1 = Empfängeradresse**
- **Addr 2 = Senderadresse**
  - Gibt den Absender der Funkstrecke an.
- **Addr 3 = Abhänging von To und From DS Bits.**
- **Addr 4 = Wird zur Angabe der ursprünglichen Absenderadresse benutzt**

Anonymisierung von MAC Adressen

MAC ADRESSEN

Definition und Verwendung

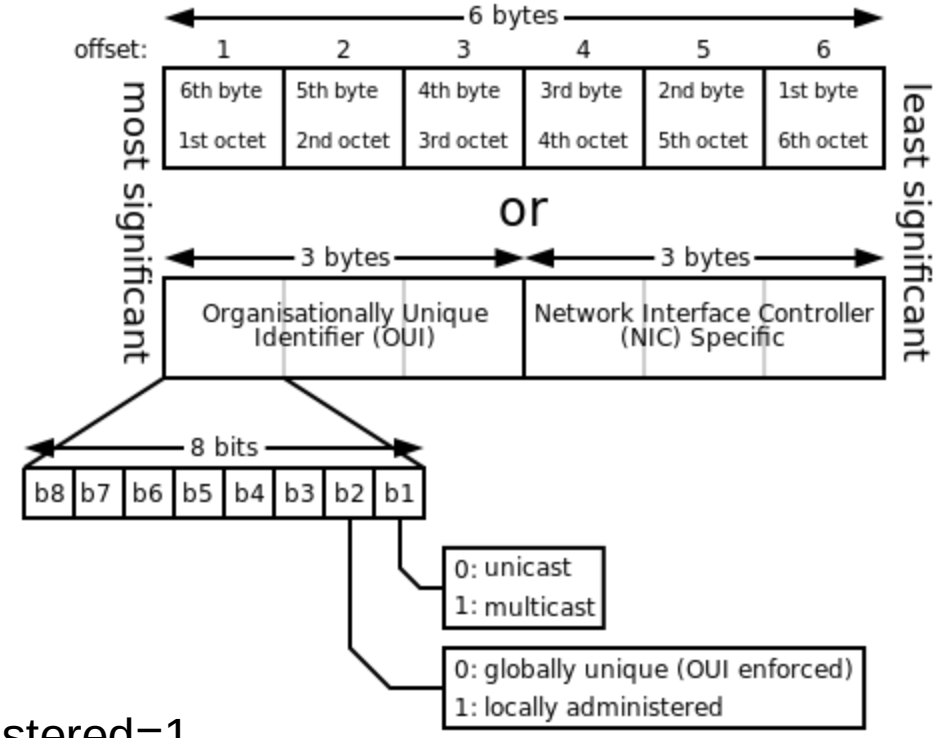
- **Spezifiziert in IEEE Std 802-2014**
- **MAC Adresse ist eine 48-Bit Nummer**
  - Extended MAC Adresse ist eine 64-Bit Nummer
- **MAC = Media Access Control**
  - Funktionalität der Schicht 2 des ISO-OSI 7 Schichten Modells
- **Identifiziert Schicht-2 Endpunkte von Datenübertragung**
- **Beispielhafte Schreibweisen:**
  - 10-0B-A9-62-B9-E8
  - 10:0b:a9:62:b9:e8
  - 100b.a962.b9e8
- **Verwendung:**
  - z.B.: Ethernet Übertragungsrahmen



Struktur von MAC Adressen

- **Der Aufbau der MAC Adresse**
  - 2 Teile
    - Organisationally Unique Identifier
    - Network Interface Controller
- **OUI wird von IEEE vergeben**
  - 3 verschiedene Formate
    - MA-L: 24bit = OUI
    - MA-M: 28bit
    - MA-S: 36bit
- **Spezielle Bits im ersten Oktett**
  - Bit 1: unicast=0 / multicast=1
  - Bit 2: globally unique=0 / locally administered=1
- **Beispiele für OUIs:**

00-50-8B-xx-xx-xx	Compaq
00-07-E9-xx-xx-xx	Intel
00-60-2F-xx-xx-xx	Cisco
00-15-F2-xx-xx-xx	Asus



Anonymisierung von MAC Adressen

LÖSUNGSANSÄTZE

Zufällige MAC Adressen

- **Die Vergabe von ‘zufälligen’ MAC Adressen an WLAN Geräte verhindert eine Erkennung anhand der MAC Adresse**

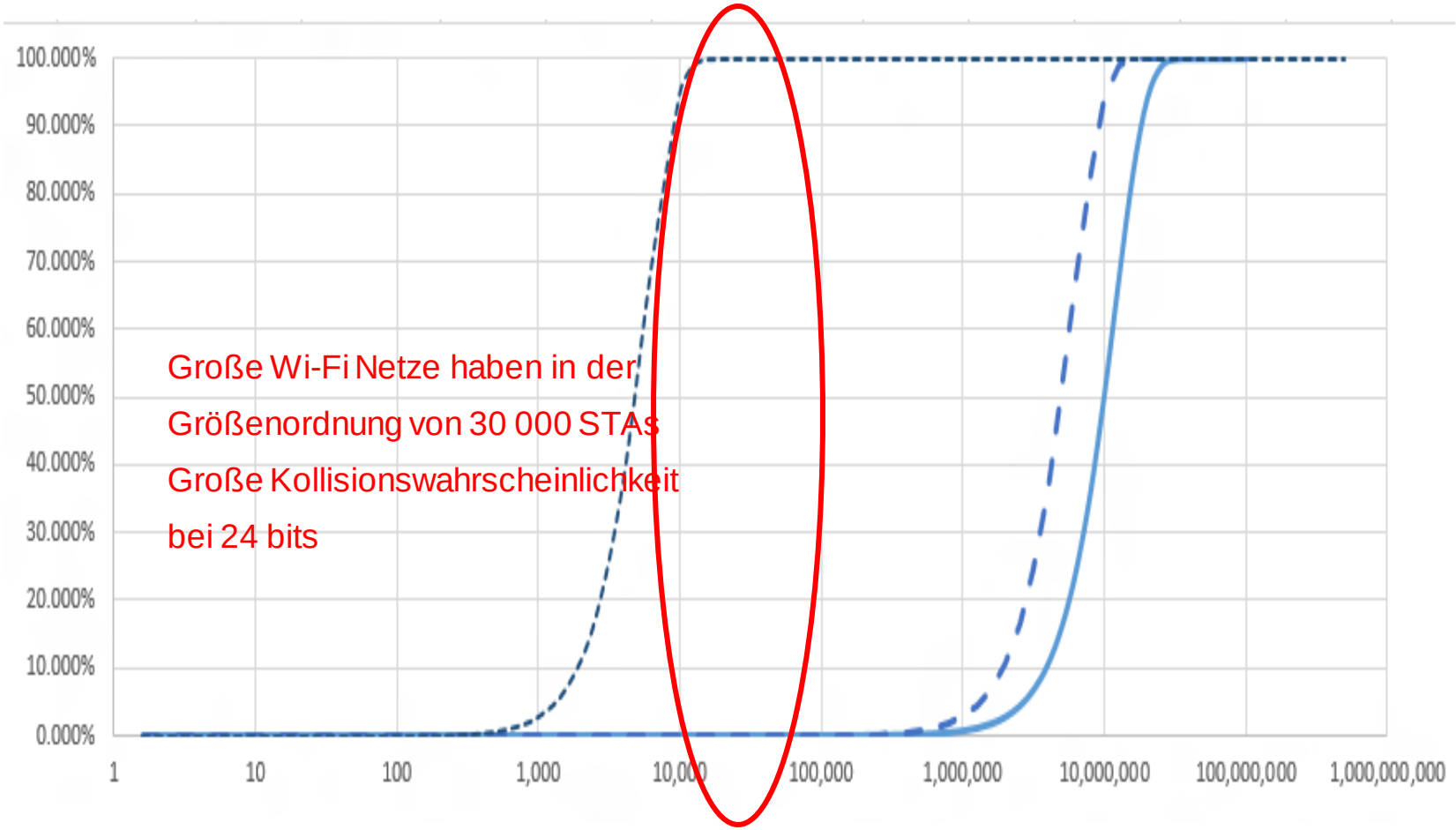
- **MAC Adressen müssen nur während einer WLAN Session konstant sein, dürfen sich aber von Session zu Session durchaus ändern.**

- **In Probe Requests können immer zufällige MAC Adressen verwendet werden.**
  - STA muss nur Antworten auf diese MAC Adresse empfangen können.
  - Verwendete MAC Adresse hat keine Auswirkung auf die Funktion des WLAN Aps

- **Problem:**
  Wie verhindert man Kollisionen von MAC Adressen
  - Auch ‘zufällige’ MAC Adressen müssen eindeutig sein.

Wahrscheinlichkeit von Kollisionen

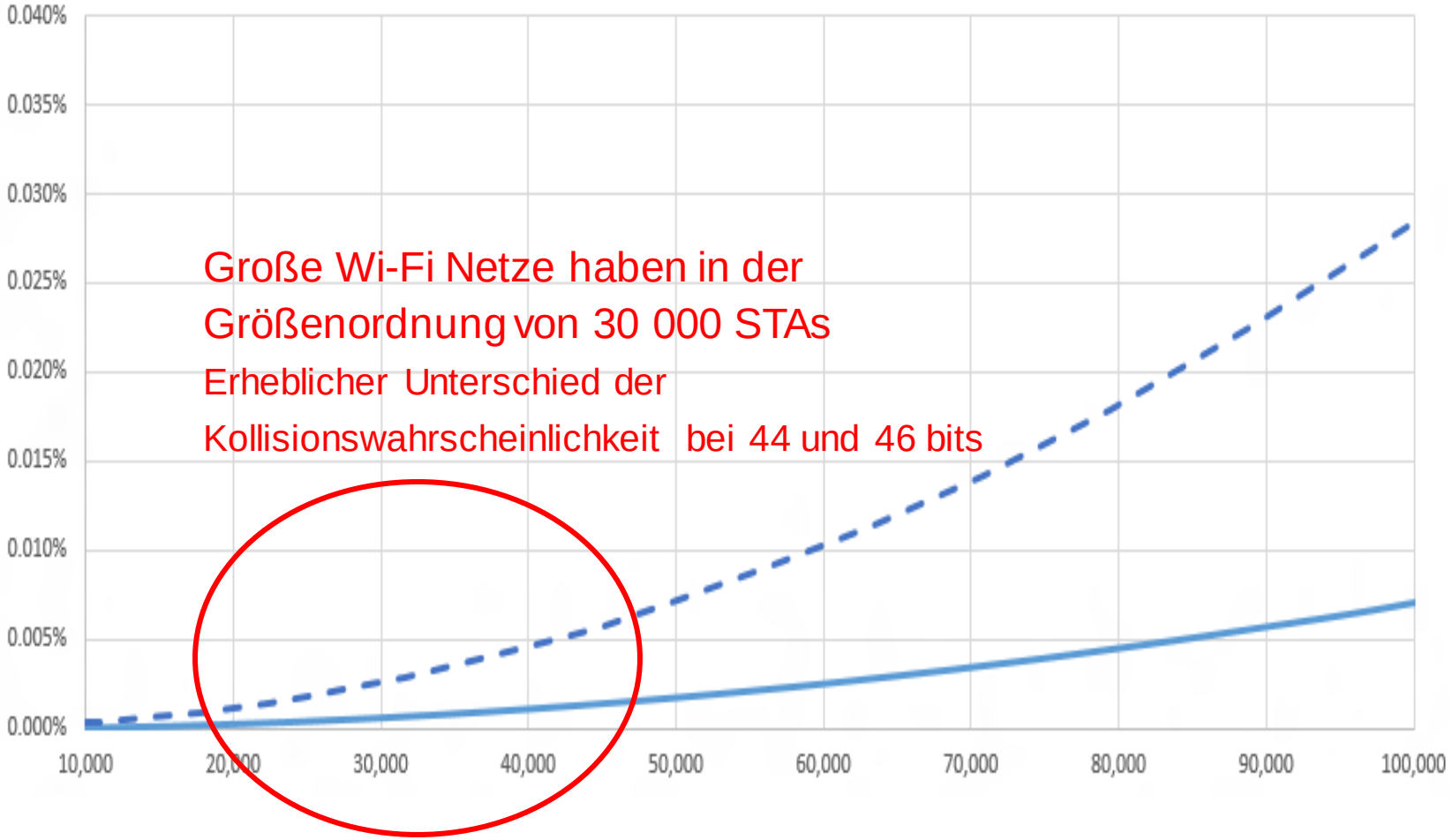
Kollisionswahrscheinlichkeit in Abhängigkeit der Netzwerkgröße, für 24, 44 and 46 Bit Zufallslänge



Source: Christian Huitema http://grouper.ieee.org/groups/802/PrivRecsg/email/msg00102.html

Kollisionswahrscheinlichkeit – Detail

Vergrößerung der Wahrscheinlichkeit bei 10,000 bis 100,000 Teilnehmern



Source: Christian Huitema http://grouper.ieee.org/groups/802/PrivRecsg/email/msg00102.html

‘Zufällige’ MAC Adressen

- **Keine Garantie gegen Kollisionen**
- **Vorschläge, Kollisonen durch kryptographische Methoden zu vermeiden, bringen nicht viel**
  - 48 bit Schlüssellänge können leicht geknackt werden
- **Protokolle zur Vermeidung von Kollisionen können leicht für ‘Denial of Service’ Angriffe ausgenutzt werden**
  - z.B. Duplicate Address Detection bei IPv6
- **Am besten wäre es, die Wahrscheinlichkeit so klein zu machen, dass kein Protokoll zur Vermeidung von Kollisionen notwendig ist.**
  - D.h. 46 bit Adressraum

Anonymisierung von MAC Adressen

STANDARDISIERUNG

IEEE P802c Projektvorschlag

- **Die Standarderweiterung soll für lokal zugewiesene MAC Adressen eine Struktur einführen.**
- **Der Vorschlag ist, den lokal zugewiesenen Adressbereich mittels Verwendung von Company IDs in Unterbereiche von 24bit aufzuteilen**
  - Company IDs werden ähnlich OUIs von der IEEE vergeben
- **Eine Unteraufteilung des lokal verwalteten MAC Adressbereichs erleichtert die Verwaltung von MAC Adressen in Data Centers**
  - VMs (Virtual Machines) benötigen eine eindeutige MAC Adresse, haben aber keine Hardware NICs
- **Der Konflikt zwischen möglichst großem Adressraum zur Vermeidung von Kollisionen und der Unteraufteilung zur Erleichterung der Verwaltung in Data Centers ist noch nicht gelöst.**

Feldversuche zur Anonymisierung

- **Sammlung von Tests von MAC Randomization Tools**
  - Target platform (OS, driver, …)
  - Type of MAC generated by the tool
  - Notes and usage instructions
  - http://oruga.it.uc3m.es/802-privacy/index.php/Main_Page

- **Während der IETF-91 in Honululo, HI wurde ein großer Test mit dynamisch gewählten MAC Adressen durchgeführt.**
  - Es traten keine Probleme mit dynamischen MAC Adressen auf
  - Sorgfältige Vorbereitung
    - Z.B. Verringerung der DHCP Lease Time zur Vermeidung von Adressengpässen
  - https://www.ietf.org/registration/MeetingWiki/wiki/91privacy

Zusammenfassung

- **Das Problem statischer MAC Adressen für den Schutz der Privatsphäre wurde erkannt.**
- **Dynamisch gewählte MAC Adressen können das Problem verringern.**
- **Erste Implementierungen sind vorhanden.**
  - Eine Anzahl von Tools für nahezu alle Betriebssysteme
  - Apple verwendet in iPhone6/iOS8 dynamische MAC Adressen für Probe Requests.
- **Experten empfehlen einen möglichst großen Adressraum zur Vermeidung von Adresskollisionen zu verwenden.**
  - 46 bit Adressraum wünschenswert
- **Die IEEE 802 ist sich noch nicht klar, wie sie konträre Anforderungen bzgl. Strukturierung des lokal administrierten MAC Adressraums unter einen Hut bringt.**

Vielen Dank für die Aufmerksamkeit

FRAGEN?, KOMMENTARE!