# Eine mögliche Sicherheitsinfrastruktur für Vehicular Ad Hoc Networks

Dipl.-Wirtsch.-Inf. Klaus Plößl
Lehrstuhl Management der Informationssicherheit

Wissenschaftlicher Vortrag nach §12 der Promotionsordnung der Universität Regensburg
20.11.2006





## Gliederung

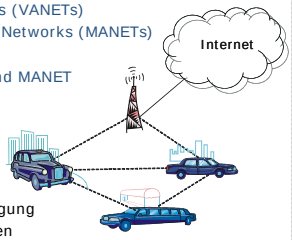
- Begriffe und Annahmen
- Anforderungen an eine Sicherheitsinfrastruktur
- Grundsätzliche Überlegungen
- Vorschlag für eine Sicherheitsinfrastruktur
- Fazit





## Automobiles Ad-hoc-Netz

- Engl. Vehicular Ad Hoc Networks (VANETs)
- Untergruppe der Mobile Ad Hoc Networks (MANETs)




- Hauptunterschied zw. VANET und MANET
  - Router = Automobil
- Besonderheiten
  - Hohe Geschwindigkeiten
  - Hohe Skalierbarkeit nötig
  - Relativ vorhersehbare Bewegung
  - U. U. hohes Datenaufkommen
- Betrachtung von
  - Vehicle-to-vehicle communications (V2V)
  - Vehicle-to-roadside communications (V2R)





## Anwendungskategorien

- Telematiknachrichten und Warnungen (A1)
  - Bsp.: Warnung bei Vollbremsung, Auslösen eines Airbags, erkanntem Stau, ...
  - Geocast
- Alarmsignale und Anordnungen (A2)
  - Bsp.: Feuerwehr, Polizei, Geschwindigkeitsbegrenzung, Kreuzungsassistent, ...
  - Geocast und Unicast
- Komfort-Dienste (A3)
  - Meist nicht kritisch für Verkehrssicherheit
  - Bsp.: Breitbandiger Internet-Zugang, Location Based Services, Fernwartung des Fahrzeugs, ...
  - Meist Unicast





## Angreifermodell und Annahmen

- Angreifermodell
  - Rollen: Fahrzeugführer, -halter, Werkstattpersonal, Außenstehende, Dienst-, Netzbetreiber, Konkurrenten, Exekutive
  - Verhalten: aktiv und passiv
  - Verbreitung: gering bis hoch
  - Kompetenzen und Ressourcen: gering bis hoch
  - Besonderheiten:
    - Drahtlose Kommunikation kann leicht abgehört werden
    - Physischer Zugriff kann oft nicht verhindert werden
- Annahmen
  - Daten innerhalb des Fahrzeugs sind korrekt
  - Einbindung korrekter Zeit- und Ortsangaben in die Nachrichten wird durch andere Infrastruktur ermöglicht





## Anforderungen

- Integrität
  - Veränderung von Nachrichten bei der Übertragung im VANET verhindern bzw. erkennbar machen (I1)
  - Eindeutige Senderauthentifizierung für A2 (I2a)
  - Nachträgliche Zurechenbarkeit für A1 und A3 (I2b)
- Vertraulichkeit
  - Verschiedene Vertraulichkeitsstufen (V1)
  - Vertraulichkeit administrativer Nachrichten (V2)
  - Schutz der Sicherheitsinfrastruktur (V3)
- Performance und Verfügbarkeit
  - Effizienz bei Rechenkapazität und Bandbreite (P1)

## Anforderungen

- Mehrseitige Sicherheit
  - Erstellung von Bewegungs- und Dienstnutzungsprofilen erschweren (D1)
  - Automatisierte Überwachung und Strafverfolgung verhindern (D2)
- Wirtschaftlichkeit und Akzeptanz
  - Niedrige Kosten für Fahrzeughard- und -software (W1)
  - Wenig Aufwand bei der Registrierung (W2)
  - Betrieb möglichst kostengünstig (W3)
  - Akzeptanz der Teilnehmer (W4)
- Sicherheitsinfrastruktur
  - Schafft Vertrauensbasis
  - Ermöglicht den Einsatz von Kryptographie
  - Umfasst alle technischen und organisatorischen Maßnahmen und Einrichtungen zum Erreichen der Schutzziele





## Grundsätzliche Überlegungen: Identität

- Zielkonflikt
  - Zurechenbarkeit vs. Privatsphäre
- Lösungsmöglichkeiten
  - System, in dem Missbrauch nicht möglich ist
  - Vertrauenswürdige Dritte, die Pseudonymität ermöglichen
- Pseudonymität benötigt eine „Basisidentität“
  - Fahrzeugbezogen
  - Personenbezogen
  - Fahrzeug- und personenbezogen





## Grundsätzliche Überlegungen: Identität

- Fahrzeugbezogene Identität
  - Motivation
    - Viele fahrzeugbezogene, oft automatisch versendete Daten
    - Fahrer unter Umständen nicht für eventuelle Falschmeldungen verantwortlich
  - VANET-Identität aus Identitätsmerkmalen des Fahrzeugs
  - Entspricht in digitaler Form der gegenwärtigen Situation
  - Speicherung
    - In manipulationssicherer Hardware im Fahrzeug





## Grundsätzliche Überlegungen: Identität

- Personenbezogene Identität
  - Motivation
    - Alle Nachrichten hängen von der Fahrweise und dem Zustand des Fahrzeugs ab
  - Erleichtert die Rekonstruktion von Unfall- und Fahrerflucht-Situationen
  - Aktuelle Gesetzgebung macht allerdings grundsätzlich den Fahrzeughalter verantwortlich
  - Sinnvoll für Personen mit erhöhten Privilegien
  - Speicherung
    - Fahrzeug und Fahrzeugschlüssel nicht geeignet
    - Elektronischer Führerschein





## Grundsätzliche Überlegungen: Identität

- Gemischte Identität
  - Motivation
    - Nachrichten sind sowohl dem Fahrzeug als auch dem Fahrer zurechenbar
  - Einsatz erhöhter Privilegien besser kontrollierbar
  - Unter Umständen genauere Bewegungsprofile möglich
  - Mehrkosten für zwei Identitäten
  - Speicherung
    - Fahrzeug und elektronischer Führerschein





## Grundsätzliche Überlegungen: Identität

- Ergebnis
  - Pseudonyme Nutzung sollte ermöglicht werden
  - Fahrzeugbezogene Identität angemessen
  - Zusätzliche personenbezogene Identität
    - Für Personengruppen mit erhöhten Privilegien
    - In bestimmten Situationen auch für „normalen“ Fahrer sinnvoll
      - Nachträgliche Identifizierung ausreichend
      - Sollte nicht zwangsweise zur VANET-Identität gehören

## Grundsätzliche Überlegungen: Authentifizierung

- Kombinierte Authentifizierung und Integritätssicherung für jede Nachricht wünschenswert
- Symmetrische oder asymmetrische Kryptographie

- Symmetrische Kryptographie
  - Beide Kommunikationspartner kennen den Schlüssel
  - Verlust der Nichtabstreitbarkeit
  - Nur mit Hilfe einer Trusted Third Party (TTP) realisierbar

- Asymmetrische Kryptographie
  - Public Key Infrastruktur (PKI) nötig
  - Digitale Signatur und Zertifikate vergrößern die Nachricht
  - Nicht so performant wie symmetrische Kryptographie
  - Zertifikatsrückrufe müssen behandelt werden





## Existierende Ansätze

- Viele unterschiedliche Ausprägungen
  - Mit und ohne Basisstationen
  - Mit und ohne zentraler TTP
  - Basierend auf
    - Klassischer zentralisierter PKI
    - Verteilter PKI
    - Identitätsbasierter Kryptographie
    - Symmetrischer Kryptographie
  - Eindeutige Identität bis Anonymität

- Einschränkungen
  - Wenige Ansätze explizit für VANETs
  - Kein Ansatz erfüllt bisher alle Anforderungen





## Vorschlag für eine Sicherheitsinfrastruktur

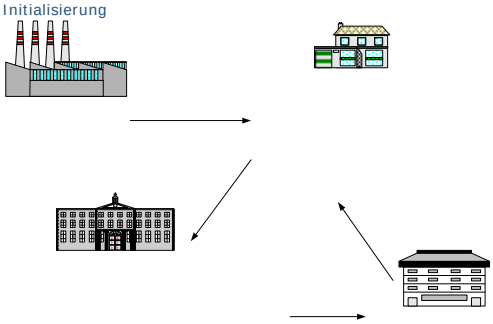
- Überblick
  - Asymmetrischer Teil mit PKI
    - Fahrzeugbezogene Identität
    - Erhöhte Privilegien durch Attribut-Zertifikate
    - Integritätssicherung verkehrssicherheitskritischer Nachrichten (A2 und teilweise A1)
    - Basis-Authentifizierung
    - Sicherung der Schlüsselverteilung des symmetrischen Teils
  - Symmetrischer Teil
    - Integritätssicherung nicht verkehrssicherheitskritischer Nachrichten (A3 und teilweise A1)
    - Verschlüsselung
    - Wechselnde Pseudonyme
    - Benötigt manipulationssichere Hardware
    - Einteilung in geographische Cluster mit zuständiger TTP





## Vorschlag für eine Sicherheitsinfrastruktur

- Initialisierung







## Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
  - Asymmetrischer Teil
    - Asymmetrisch gesicherte Nachricht

| Daten mit Adressinformationen | Digitale Signatur | $ZERT_{Sender}$ |
|---|---|---|

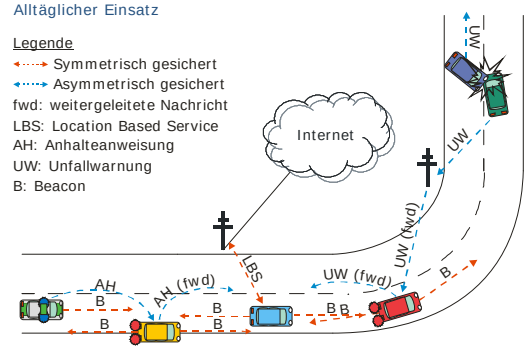
    - Nach dem Initialisierungsprozess einsetzbar
    - Gesicherte Nachrichten
      - Verkehrssicherheitskritische Meldungen
      - Alarmsignale
      - Anweisungen
    - Rückruflisten
      - Für Warnungen nicht kritisch
      - Für Alarmsignale und Anweisungen
        - » Kurzzeit-Attributzertifikate





## Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz



## Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
  - Symmetrischer Teil
    - Gesicherte Nachrichten
      - Nicht verkehrssicherheitskritische Meldungen
      - Nachrichten der Komfort-Dienste
    - Setzt gelegentlichen Kontakt mit zuständiger TTP voraus
      - Verteilung von Pseudonymen
        - » Nur TTP speichert Zuordnung der Pseudonyme zu (fahrzeugbezogenen) Identitäten
        - » Unabhängige Datenschutzorganisationen als TTPs
      - Verteilung symmetrischer Schlüssel für
        - » Nachrichtenverschlüsselung
        - » Nachrichtenauthentifizierung
    - Performanter als asymmetrischer Teil
    - Ausschluss von Störern leicht möglich





## Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
  - Symmetrischer Teil
    - Symmetrisch gesicherte Nachricht

| Daten mit Adressinformationen | $PA$ | HMAC mit $k_{MAC_{PA}}$ | HMAC mit $k_{MAC_{ALL}}$ |
|---|---|---|---|
| verschlüsselt mit $k_c$ | | | |

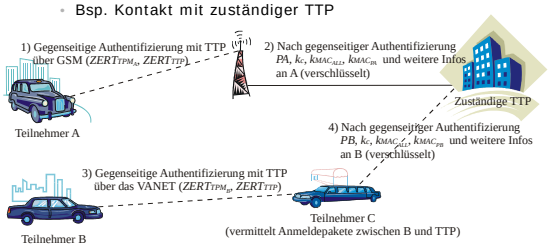
    - $k_c$ und $k_{MAC_{ALL}}$
      - Für alle Teilnehmer in einem bestimmten geographischen Gebiet gleich
      - Periodischer Wechsel
    - $PA$ und $k_{MAC_{PA}}$
      - Mindestens ein Paar pro Teilnehmer
      - Periodischer Wechsel
    - Nachrichtenbearbeitung und Schlüsselspeicherung komplett in manipulationssicherer Hardware
    - Für Komfort-Dienste anwendungsspezifische Verschlüsselung möglich





## Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
  - Symmetrischer Teil
    - Bsp. Kontakt mit zuständiger TTP








## Vorschlag für eine Sicherheitsinfrastruktur

- Performancebetrachtung
  - Annahmen
    - Nachrichtenlänge: ca. 300 Byte
    - RSA mit SHA-256 (Schlüssellänge 2048 Bit)
    - HMAC SHA-256 (Schlüssellänge 192 Bit)
    - AES (Schlüssellänge 192 Bit)
    - Pseudonym 48 Bit
  - Testumgebung
    - JRE 1.5.0_06
    - Mobile AMD Athlon4 2400+
    - 768 MB RAM
    - Windows XP Sp2





## Vorschlag für eine Sicherheitsinfrastruktur

- Performancebetrachtung
  - Overhead
    - Pro Nachricht
      - Asymmetrisch
        - » Digitale Signatur + Zertifikat
        - » 2048 Bit + (2048 Bit + 2048 Bit) = 768 Byte
        - » Gesamt 1068 Byte ⇒ 72% Overhead
      - Symmetrisch
        - » PA + 2 * HMAC
        - » 48 Bit + 2 * 256 Bit = 70 Byte
        - » Gesamt 370 Byte ⇒ 19% Overhead
    - Für Schlüsselaustausch
      - Vernachlässigbar, da TTP nur selten kontaktiert werden muss und Nachrichten klein sind
    - Für Zertifikatsrückrufliste
      - Nicht benötigt





## Vorschlag für eine Sicherheitsinfrastruktur

- Performancebetrachtung
  - Berechnungszeit
    - Signaturgenerierung
      - Asymmetrisch: 98 ms
      - Symmetrisch: 2 * 0,035 ms = 0,07 ms
    - Signaturprüfung
      - Asymmetrisch: 2,9 ms
      - Symmetrisch: 0,035 ms
    - Verschlüsselung (symmetrisch, 370 Byte): 0,029 ms
    - Entschlüsselung: 0,031 ms
  - Gesamtverzögerung
    - Asymmetrisch: 100,9 ms
    - Symmetrisch: 0,165 ms
    - Mensch: ca. 1000 ms

## Fazit und Ausblick

- Fazit
  - Integrität und Authentizität aller Nachrichten wird gewährleistet
  - Keine gravierenden Performance-Einbußen oder Verletzungen der Privatsphäre
  - Gezielte Vergabe erhöhter Privilegien
  - ⇒ Kombination asymmetrischer und symmetrischer Kryptographie erfüllt Anforderungen besser als bisherige getrennte Ansätze
- Ausblick
  - Untersuchungen in Bezug auf den Zeitraum der Schlüsselgültigkeit und der geographischen Verteilung der TTPs
  - Weitere Untersuchung geeigneter Algorithmen
  - Spezifizierung der Bedingungen zur Herausgabe der Zuordnung Identität ↔ Pseudonym
- Kontakt:
  - Klaus.Ploessl@wiwi.uni-regensburg.de