

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf. Klaus Plößl



Vorschlag für eine Sicherheitsinfrastruktur für Vehicular Ad Hoc Networks

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


Automotive – Safety & Security 2006
12.10.2006

1

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf. Klaus Plößl

Gliederung

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



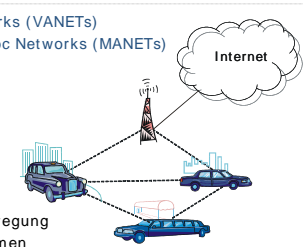
2

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf. Klaus Plößl

Automobiles Ad-hoc-Netz

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

- Hauptunterschied
 - 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)

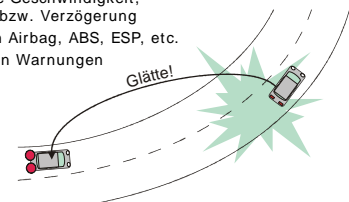


3

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf. Klaus Plößl

Automobiles Ad-hoc-Netz

- Hauptziel
 - Erhöhung der Verkehrssicherheit
- Zielerreichung
 - Fahrzeuge agieren als Sensoren
 - Austausch von Telematikdaten, wie
 - Position, aktuelle Geschwindigkeit, Beschleunigung bzw. Verzögerung
 - Sensordaten von Airbag, ABS, ESP, etc.
 - Ggf. Aussendung von Warnungen
- Bsp. für Warnungen
 - Unfallwarnung
 - Stauwarnung
 - Wetterwarnung
 - ...



4

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf. Klaus Plößl

Anwendungskategorien

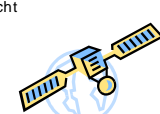
- Telematiknachrichten und Warnungen (A1)
 - Geocast
 - Bsp. Warnung bei Vollbremsung, Auslösen eines Airbags, erkanntem Stau, ...
- Alarmsignale und Anordnungen (A2)
 - Geocast und Unicast
 - Bsp. Feuerwehr, Polizei, Geschwindigkeitsbegrenzung, Kreuzungsassistent, ...
- Komfort-Dienste (A3)
 - Meist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

5

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf. Klaus Plößl

Begriff „Sicherheitsinfrastruktur“ und Annahmen

- Sicherheitsinfrastruktur
 - Schafft Vertrauensbasis
 - Ermöglicht den Einsatz von Kryptographie
 - Umfasst alle technischen und organisatorischen Maßnahmen und Einrichtungen zum Erreichen der Schutzziele
- Annahmen
 - Daten innerhalb des Fahrzeugs sind korrekt
 - Einbindung korrekter Zeit- und Ortsangaben in die Nachrichten wird durch andere Infrastruktur ermöglicht



6

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf.
Klausur P10&I

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)

7

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf.
Klausur P10&I

Anforderungen

- **Mehrseitige Sicherheit**
 - Erstellung von Bewegungs- und Dienstnutzungsprofilen erschweren (D1)
 - Automatisierte Überwachung und Strafverfolgung verhindern (D2)
 - Sender- und Empfängeridentität schützen (D3)
- **Wirtschaftlichkeit und Akzeptanz**
 - Niedrige Kosten für Fahrzeughard- und Software (W1)
 - Wenig Aufwand bei der Registrierung (W2)
 - Betrieb möglichst kostengünstig (W3)
 - Akzeptanz der Teilnehmer (W4)

8

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf.
Klausur P10&I

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

9

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf.
Klausur P10&I

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

10

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf.
Klausur P10&I

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

11

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf.
Klausur P10&I

Grundsätzliche Überlegungen: Identität

- **Fazit**
 - 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

12

Sicherheitsinfrastruktur für VANETs

Dipl.-Wirtsch.-Inf. Klausur P106I

Grundsätzliche Überlegungen: Authentifizierung

- Symmetrische oder asymmetrische Kryptographie
- Vorverteilung des benötigten kryptographischen Materials relativ problemlos
- 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

13

Sicherheitsinfrastruktur für VANETs

Dipl.-Wirtsch.-Inf. Klausur P106I

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
 - Wechselnde Pseudonyme
 - Integritätssicherung nicht verkehrssicherheitskritischer Nachrichten (A3 und teilweise A1)
 - Verschlüsselung
 - Benötigt manipulationssichere Hardware
 - Einteilung in geographische Cluster mit zuständiger TTP

14

Sicherheitsinfrastruktur für VANETs

Dipl.-Wirtsch.-Inf. Klausur P106I

Vorschlag für eine Sicherheitsinfrastruktur

- Initialisierung
 - Erst beim Eigentümer wird Identität festgelegt
 - Anforderung V1: wechsellieferfähige Schlüssel
 - Eigentümer ist für PKI verantwortlich
 - Automobilhersteller:
 - TPM-Einbau
 - ZERT_{Werkst} in TPM
 - Pre-Shared-Key in TPM
 - und auf SmartCard Einspielen
 - Eigentümer des Fahrzeugs A:
 - Erzeugung SK_{TPMA} und PK_{TPMA}
 - Physische Deaktivierung der SK_{TPMA} und PK_{TPMA}-Erzeugungsfunktion
 - Erzeugung SK_{SCA} und PK_{SCA} und Transfer dieser auf SmartCard
 - Prüfung und ggf. Einspielen der ZERT_{Werkst}
 - Nach Zulassung:
 - Einspielen ZERT_{TPMA}
 - Anforderung W2, W3, W4
 - Zulassungsstelle:
 - Auslesen des vorgelegten ZERT_{Werkst}
 - Prüfung der Halterdaten
 - Verifizierung der physischen Deaktivierung der Schlüsselerzeugung im TPM
 - Weiterleitung der Daten an KBA
 - Kraftfahrt-Bundesamt:
 - Ausstellung ZERT_{TPMA}
 - Anforderung W2, W3, W4
 - Anforderung W2, W3, W4
 - Anforderung W2, W3, W4

15

Sicherheitsinfrastruktur für VANETs

Dipl.-Wirtsch.-Inf. Klausur P106I

Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
 - Asymmetrischer Teil
 - Asymmetrisch gesicherte Nachricht

Daten mit Adressinformationen	Digitale Signatur	ZERT _{Sender}
-------------------------------	-------------------	------------------------

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

16

Sicherheitsinfrastruktur für VANETs

Dipl.-Wirtsch.-Inf. Klausur P106I

Vorschlag für eine Sicherheitsinfrastruktur

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

17

Sicherheitsinfrastruktur für VANETs

Dipl.-Wirtsch.-Inf. Klausur P106I

Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
 - Symmetrischer Teil
 - Symmetrisch gesicherte Nachricht

Daten mit Adressinformationen	PA	HMAC mit k_{MACPA}	HMAC mit k_{MACALL}
-------------------------------	----	----------------------	-----------------------

verschlüsselt mit k_c

- k_c und k_{MACALL}
 - Für alle Teilnehmer im bestimmten geographischen Gebiet gleich
 - Periodischer Wechsel
- PA und k_{MACPA}
 - Mindestens ein Paar pro TTP
 - Periodischer Wechsel
- Nachrichtenbearbeitung und -speicherung komplett in manipulationssicherer Hardware
- Für Komfort-Dienste anwendungsspezifische Verschlüsselung möglich

18

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf.
Klaus Ploessl

Vorschlag für eine Sicherheitsinfrastruktur

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

V3 durch übliche Mittel der Rechner- und Netzwerksicherheit

1) Gegenseitige Authentifizierung mit TTP über GSM ($ZERT_{PM_A}$, $ZERT_{TP}$)

2) Nach gegenseitiger Authentifizierung PA , k , $kMAC_{A12}$, $kMAC_m$ und weitere Infos an A (verschlüsselt)

3) Gegenseitige Authentifizierung mit TTP über das VANET ($ZERT_{PM_B}$, $ZERT_{TP}$)

4) Nach gegenseitiger Authentifizierung PB , k , $kMAC_{B12}$, $kMAC_m$ und weitere Infos an B (verschlüsselt)

Teilnehmer A Teilnehmer B Teilnehmer C (vermittelt Anmeldepakete zwischen B und TTP) Zuständige TTP

Anforderung V2 und V3

19

Sicherheitsinfrastruktur für VANETs Dipl.-Wirtsch.-Inf.
Klaus Ploessl

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
 - Spezifizierung der Bedingungen zur Herausgabe der Zuordnung Identität ↔ Pseudonym
- Kontakt:
 - Klaus.Ploessl@wiwi.uni-regensburg.de

20