

Authentifizierung in Echtzeit-Netzwerken im Automotivkontext

Anwendungen 2

Stephan Phieler
stephan.phieler@haw-hamburg.de

Hochschule für Angewandte Wissenschaften Hamburg

9. Januar 2014



Hochschule für Angewandte Wissenschaften Hamburg

Hamburg University of Applied Sciences

1 Motivation

2 Echtzeit-Ethernet im Automobil

3 Authentifizierung

- Grundlagen
- Paper

4 Fazit & Ausblick

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielor

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung

Fazit & Ausblick

1 Motivation

2 Echtzeit-Ethernet im Automobil

3 Authentifizierung

- Grundlagen
- Paper

4 Fazit & Ausblick

- Unsichere Netzwerke
- Verteilte eingebettete Systeme
- (Echtzeit-)Ethernet
- Safety
- Automobil in schwer zu überwachender Umgebung
- Austausch/Manipulation von Hardware

- Unsichere Netzwerke
- Verteilte eingebettete Systeme
- (Echtzeit-)Ethernet
- Safety
- Automobil in schwer zu überwachender Umgebung
- Austausch/Manipulation von Hardware

- Unsichere Netzwerke
- Verteilte eingebettete Systeme
- (Echtzeit-)Ethernet
- Safety
- Automobil in schwer zu überwachender Umgebung
- Austausch/Manipulation von Hardware

- Unsichere Netzwerke
- Verteilte eingebettete Systeme
- (Echtzeit-)Ethernet
- Safety
- Automobil in schwer zu überwachender Umgebung
- Austausch/Manipulation von Hardware

- Unsichere Netzwerke
- Verteilte eingebettete Systeme
- (Echtzeit-)Ethernet
- Safety
- Automobil in schwer zu überwachender Umgebung
- Austausch/Manipulation von Hardware

- Unsichere Netzwerke
- Verteilte eingebettete Systeme
- (Echtzeit-)Ethernet
- Safety
- Automobil in schwer zu überwachender Umgebung
- Austausch/Manipulation von Hardware

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielers

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung

Fazit & Ausblick

1 Motivation

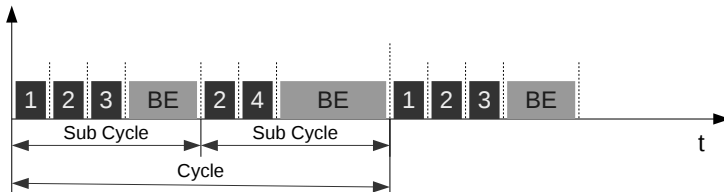
2 Echtzeit-Ethernet im Automobil

3 Authentifizierung

- Grundlagen
- Paper

4 Fazit & Ausblick

- Time Division Multiple Access
- Virtual Links
- Statisch konfiguriertes Netzwerk



(BE=Best Effort)

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielers

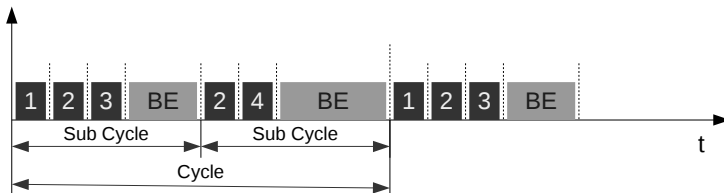
Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung

Fazit & Ausblick

- Time Division Multiple Access
- Virtual Links
- Statisch konfiguriertes Netzwerk



(BE=Best Effort)

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielers

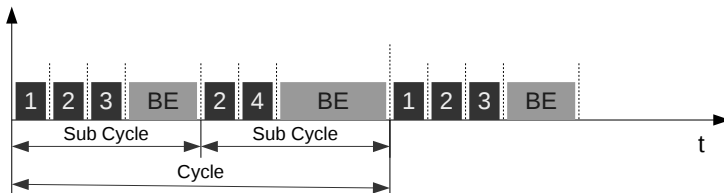
Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung

Fazit & Ausblick

- Time Division Multiple Access
- Virtual Links
- Statisch konfiguriertes Netzwerk



(BE=Best Effort)

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielers

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung

Fazit & Ausblick

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielers

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

Fazit & Ausblick

1 Motivation

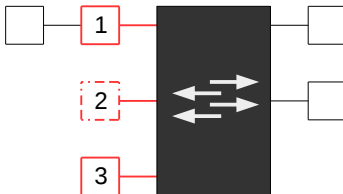
2 Echtzeit-Ethernet im Automobil

3 Authentifizierung

- Grundlagen
- Paper

4 Fazit & Ausblick

- Replay-Attacks
- Masquerade-Attacks



Verfahren:

- Symmetrisch (MAC)
- Asymmetrisch (Signature)

Wichtige Faktoren:

- Key-Infrastruktur
- Performance
- Skalierbarkeit

Verfahren:

- Symmetrisch (MAC)
- Asymmetrisch (Signature)

Wichtige Faktoren:

- Key-Infrastruktur
- Performance
- Skalierbarkeit

Verfahren:

- Symmetrisch (MAC)
- Asymmetrisch (Signature)

Wichtige Faktoren:

- Key-Infrastruktur
- Performance
- Skalierbarkeit

Verfahren:

- Symmetrisch (MAC)
- Asymmetrisch (Signature)

Wichtige Faktoren:

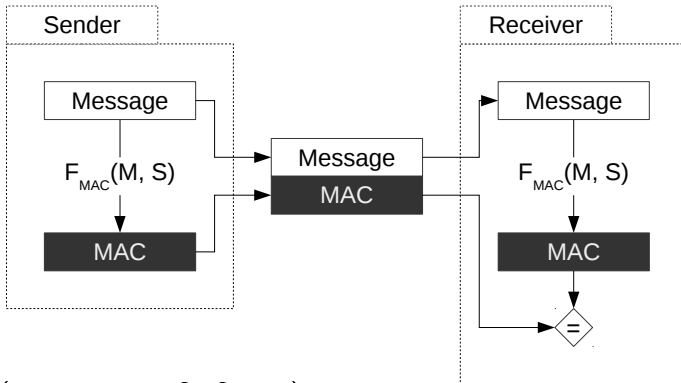
- Key-Infrastruktur
- Performance
- Skalierbarkeit

Verfahren:

- Symmetrisch (MAC)
- Asymmetrisch (Signature)

Wichtige Faktoren:

- Key-Infrastruktur
- Performance
- Skalierbarkeit



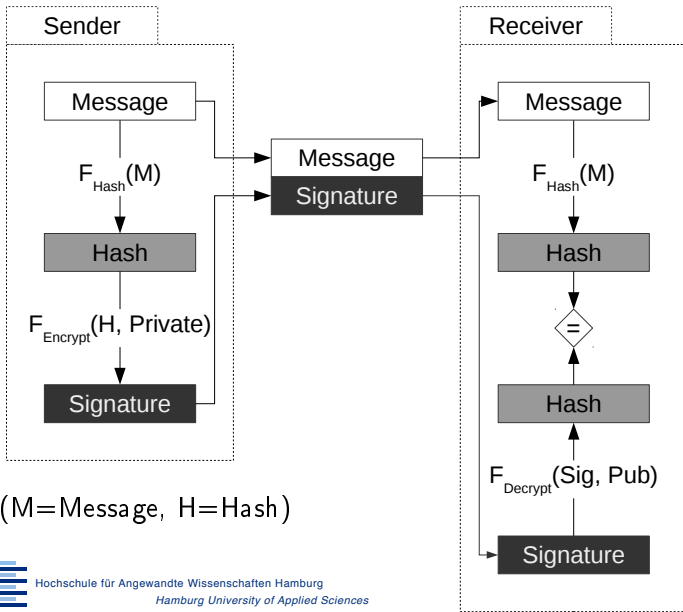
(M=Message, S=Secret)

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

Fazit & Ausblick



Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielers

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

Fazit & Ausblick

- Flexible Multicast Authentication for Time-Triggered Embedded Control Network Applications [SK09]
- Authentication in Time-Triggered Systems using Time-delayed Release of Keys [WESK11]
- Security in Integrated Vectorics: Applying Elliptic Curve Digital Signature Algorithm to a Safty-Critical Network [DOSC12]

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

Fazit & Ausblick

- Ein Schlüssel pro Empfänger (MAC)
- Unterscheidung zwischen:
 - State-changing Messages
 - Reactive control Messages



Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

Fazit & Ausblick

- Ein Schlüssel pro Empfänger (MAC)
- Unterscheidung zwischen:
 - State-changing Messages
 - Reactive control Messages



Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

Fazit & Ausblick

- Ein Schlüssel pro Empfänger (MAC)
- Unterscheidung zwischen:
 - State-changing Messages
 - Reactive control Messages



Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

Fazit & Ausblick

- Ein Schlüssel pro Empfänger (MAC)
- Unterscheidung zwischen:
 - State-changing Messages
 - Reactive control Messages



Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

Fazit & Ausblick

- Empfang von mehreren konsistenten Nachrichten
- Jede einzeln authentifiziert (valid / invalid)
- Abgelegt in history buffer
- Ausführung wenn k aus n Paketen valide

$$P_A = \sum_{i=k}^n \binom{n}{i} (2^{-b})^i (1 - 2^{-b})^{n-i} \quad (1)$$

P_A = Wahrscheinlichkeit für erfolgreichen Angriff

b = Anzahl Bits MAC

- Empfang von mehreren konsistenten Nachrichten
- Jede einzeln authentifiziert (valid / invalid)
- Abgelegt in history buffer
- Ausführung wenn k aus n Paketen valide

$$P_A = \sum_{i=k}^n \binom{n}{i} (2^{-b})^i (1 - 2^{-b})^{n-i} \quad (1)$$

P_A = Wahrscheinlichkeit für erfolgreichen Angriff

b = Anzahl Bits MAC

- Empfang von mehreren konsistenten Nachrichten
- Jede einzeln authentifiziert (valid / invalid)
- Abgelegt in history buffer
- Ausführung wenn k aus n Paketen valide

$$P_A = \sum_{i=k}^n \binom{n}{i} (2^{-b})^i (1 - 2^{-b})^{n-i} \quad (1)$$

P_A = Wahrscheinlichkeit für erfolgreichen Angriff

b = Anzahl Bits MAC

- Empfang von mehreren konsistenten Nachrichten
- Jede einzeln authentifiziert (valid / invalid)
- Abgelegt in history buffer
- Ausführung wenn k aus n Paketen valide

$$P_A = \sum_{i=k}^n \binom{n}{i} (2^{-b})^i (1 - 2^{-b})^{n-i} \quad (1)$$

P_A = Wahrscheinlichkeit für erfolgreichen Angriff

b = Anzahl Bits MAC

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielor

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

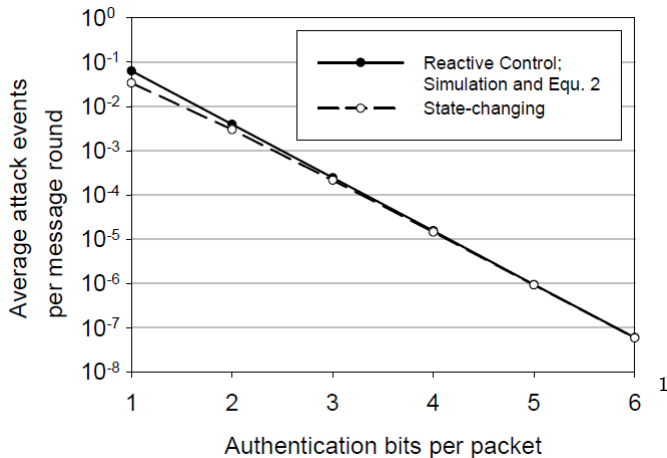
Fazit & Ausblick

- Einsatz in Regelungen
- Valide Nachricht sofort verarbeitet
- Toleranz durch Dämpfung
- Plausibilitätsprüfung unverzichtbar

- Einsatz in Regelungen
- Valide Nachricht sofort verarbeitet
- Toleranz durch Dämpfung
- Plausibilitätsprüfung unverzichtbar

- Einsatz in Regelungen
- Valide Nachricht sofort verarbeitet
- Toleranz durch Dämpfung
- Plausibilitätsprüfung unverzichtbar

- Einsatz in Regelungen
- Valide Nachricht sofort verarbeitet
- Toleranz durch Dämpfung
- Plausibilitätsprüfung unverzichtbar



¹ Bildquelle: [SK09]

- Ein Schlüssel pro Sender/Empfänger
- Tolerant ggb. Paketverlust
- Speicher für Nachrichten notwendig
- Verfahren zu Lasten der Sicherheit

- Ein Schlüssel pro Sender/Empfänger
- Tolerant ggb. Paketverlust
- Speicher für Nachrichten notwendig
- Verfahren zu Lasten der Sicherheit

- Ein Schlüssel pro Sender/Empfänger
- Tolerant ggb. Paketverlust
- Speicher für Nachrichten notwendig
- Verfahren zu Lasten der Sicherheit

- Ein Schlüssel pro Sender/Empfänger
- Tolerant ggb. Paketverlust
- Speicher für Nachrichten notwendig
- Verfahren zu Lasten der Sicherheit

Time-delayed Release of Keys

Prinzip

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielers

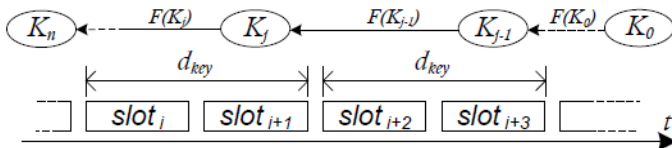
- Timed Efficient Stream Loss-tolerant Authentication
- MAC (Eine für Alle)
- Keychain
- Schlüsselverteilung über PKI

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

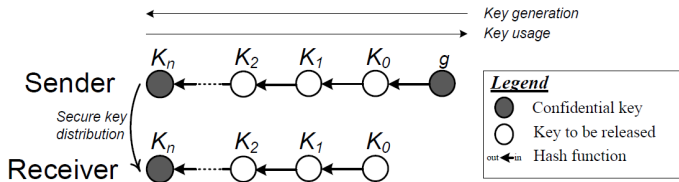
Fazit & Ausblick



2

² Bildquelle: [WESK11]

- Sichere Assoziation zwischen Schlüsseln
- Berechnung nur in einer Richtung möglich
- Keychain wird prekonfiguriert



3

³Bildquelle: [WESK11]

- Ein Schlüssel für Alle
- Kein Verlust der Sicherheit
- Tolerant ggb. Paketverlust
- Delay
- Hybrides Verfahren
- Speicher für Nachrichten/Schlüssel notwendig

- Ein Schlüssel für Alle
- Kein Verlust der Sicherheit
- Tolerant ggb. Paketverlust
- Delay
- Hybrides Verfahren
- Speicher für Nachrichten/Schlüssel notwendig

- Ein Schlüssel für Alle
- Kein Verlust der Sicherheit
- Tolerant ggb. Paketverlust
- Delay
- Hybrides Verfahren
- Speicher für Nachrichten/Schlüssel notwendig

- Ein Schlüssel für Alle
- Kein Verlust der Sicherheit
- Tolerant ggb. Paketverlust
- Delay
- Hybrides Verfahren
- Speicher für Nachrichten/Schlüssel notwendig

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung
Grundlagen
Paper

Fazit & Ausblick

- Ein Schlüssel für Alle
- Kein Verlust der Sicherheit
- Tolerant ggb. Paketverlust
- Delay
- Hybrides Verfahren
- Speicher für Nachrichten/Schlüssel notwendig

- Ein Schlüssel für Alle
- Kein Verlust der Sicherheit
- Tolerant ggb. Paketverlust
- Delay
- Hybrides Verfahren
- Speicher für Nachrichten/Schlüssel notwendig

- Seit 1985
- Asymmetrische Verschlüsselung
- Keine Kollisionen
- Daher als Einwegfunktion optimal
- Kommt mit kürzeren Schlüsseln aus
- $O(n * p)$

$$y^2 = x^3 + ax + b \quad (2)$$

- Seit 1985
- Asymmetrische Verschlüsselung
- Keine Kollisionen
- Daher als Einwegfunktion optimal
- Kommt mit kürzeren Schlüsseln aus
- $O(n * p)$

$$y^2 = x^3 + ax + b \quad (2)$$

- Seit 1985
- Asymmetrische Verschlüsselung
- Keine Kollisionen
- Daher als Einwegfunktion optimal
- Kommt mit kürzeren Schlüsseln aus
- $O(n * p)$

$$y^2 = x^3 + ax + b \quad (2)$$

- Seit 1985
- Asymmetrische Verschlüsselung
- Keine Kollisionen
- Daher als Einwegfunktion optimal
- Kommt mit kürzeren Schlüsseln aus
- $O(n * p)$

$$y^2 = x^3 + ax + b \quad (2)$$

- Seit 1985
- Asymmetrische Verschlüsselung
- Keine Kollisionen
- Daher als Einwegfunktion optimal
- Kommt mit kürzeren Schlüsseln aus
- $O(n * p)$

$$y^2 = x^3 + ax + b \quad (2)$$

- Seit 1985
- Asymmetrische Verschlüsselung
- Keine Kollisionen
- Daher als Einwegfunktion optimal
- Kommt mit kürzeren Schlüsseln aus
- $O(n * p)$

$$y^2 = x^3 + ax + b \quad (2)$$

Vergleich der Bitlängen⁴ zum Aufwand der
Schlüsselermittlung.

Symmetrisch	RSA	ECC
64	512	175
80	768	190
112	1792	210
128	2304	235

⁴Quelle: [Sel00]

- Bieten Möglichkeit für Einsatz in Echtzeit-Netzwerk
- Noch Forschungsbedarf

**Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext**

Stephan Phielers

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung

Fazit & Ausblick

1 Motivation

2 Echtzeit-Ethernet im Automobil

3 Authentifizierung

- Grundlagen
- Paper

4 Fazit & Ausblick

- Symmetrisch / Asymmetrisch
- Schlüssel kürzen
- Zeitverzögerte Schlüsselverteilung
- Elliptische Kurven

- Untersuchung von Verfahren mit elliptischen Kurven
- Implementierung in Simulationsumgebung
- Integration von Verschlüsselungshardware



Vielen Dank für die Aufmerksamkeit!

- [DOSC12] **Deshpande, A. ; Obi, O. ; Stipidis, E. ; Charchalakis, P.:**
Security in integrated vetronics: Applying elliptic curve digital signature algorithm to a safety-critical network protocol-TTP/C.
In: System Safety, incorporating the Cyber Security Conference 2012, 7th IET International Conference on, 2012, S. 1–5

- [Sel00] **Selke, G.W.:**
Kryptographie: Verfahren, Ziele, Einsatzmöglichkeiten.
 O'Reilly Vlg. GmbH & Company, 2000 (O'Reilly essentials).

Authentifizierung in
 Echtzeit-Netzwerken
 im Automotivkontext

Stephan Phielers

Motivation

Echtzeit-Ethernet im
 Automobil

Authentifizierung

Fazit & Ausblick

<http://books.google.de/books?id=yZEiAQAAMAAJ>. –
ISBN 9783897211551

- [SK09]** Szilagy, C. ; Koopman, P.:
Flexible multicast authentication for time-triggered embedded control network applications.
In: Dependable Systems Networks, 2009. DSN '09. IEEE/IFIP International Conference on, 2009, S. 165–174

- [WESK11]** Wasicek, A. ; El-Salloum, C. ; Kopetz, Hermann:
Authentication in Time-Triggered Systems Using Time-Delayed Release of Keys.

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielers

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung

Fazit & Ausblick

In: *Object/Component/Service-Oriented
Real-Time Distributed Computing
(ISORC), 2011 14th IEEE International
Symposium on, 2011. –
ISSN 1555-0885, S. 31-39*

Authentifizierung in
Echtzeit-Netzwerken
im Automotivkontext

Stephan Phielers

Motivation

Echtzeit-Ethernet im
Automobil

Authentifizierung

Fazit & Ausblick