Sicheres Wireless Networking im Industrieeinsatz

Dipl.-Ing. Robert Schwebel <r.schwebel@pengutronix.de>

Pengutronix - Linux Solutions for Science and Industry

Outline

- Sound techniques
  - Cylindrical Algebraic Decomposition
  - Interval arithmetic and inner-approximation computation
- Complete techniques
  - Interval constraint solving
- Interval constraint solving and soundness
- Solving constraints with universal quantifiers
- Conclusion and perspectives

Übersicht

Pengutronix
Wireless Ethernet - Technologie
Anwendungen in der Logistik
Sicherheit
Linux und Open Source

Übersicht

Pengutronix
Wireless Ethernet - Technologie
Anwendungen in der Logistik
Sicherheit
Linux und Open Source

Pengutronix - Werbeblock

„Linux Solutions for Science and Industry“
Kleine Embedded Systeme - vollwertiges Betriebssystem
Harte Echtzeit, z.B. für Steuerungstechnik, M&R
Fernwartung, Remote-Update, Sicherheit
ARM/XScale, PowerPC, x86

Pengutronix - Werbeblock

Beratung, projektbegleitende Unterstützung
Software-Auftragsentwicklung
Projekte: Linux für Industrieanwendungen
Optimale Nutzung von Open Source

Übersicht

Pengutronix
Wireless Ethernet - Technologie
Anwendungen in der Logistik
Sicherheit
Linux und Open Source

Wireless Ethernet - Historie

Ethernet: „der“ Standard für Büro-Kommunikation
Entwickelt als ausfallsichere Technologie für das Militär (ARPANET ab 1968, TCP ab 1977)
TCP/UDP/IP Protokollfamilie

Wireless Ethernet - Historie

1982: IEEE 802.3: 10Base5 (Yellow Cable)
1986: 10Base2 (Cheapernet, Koaxialkabel)
1991: 10BaseT (Twisted Pair, 10 MBit/s, Hubs+Switche)
1995: 100BaseT (Twisted Pair, 100 MBit/s)
2000: 1000BaseT (Twistet Pair, 1000 MBit/s)

Wireless Ethernet - Standards

1999: 802.11a: bis 54 MBit/s, 5.4 GHz (lange in Deutschland verboten)
1999: 802.11b: 1 - 11 MBit/s, 2.4 GHz (gröSSte Verbreitung)
2003: 802.11g: bis 54 MBit/s, 2.4 GHz (kompatibel zu 802.11b)

Wireless Ethernet - Infrastruktur

Aufbau eines Funknetzes:
Accesspoint, Geräteanbindung mit WLAN-Karten

Wireless Ethernet - Vorteile

Keine Kabelverbindungen notwendig
Vernetzung mobiler Einheiten wird möglich (Mensch, Gabelstapler, Transportbehälter)
Einheitliche IT-Infrastruktur!
IP-Protokoll für alle Geräte, inklusive Datenquellen
Einheitliche Sicherheitsrichtlinien definierbar

Wireless Ethernet - Vorteile

Kosten: keine aufwendige Verkabelung notwendig
Standard-Komponenten einsetzbar (leichte Beschaffung)
Eine Technologie für alle Geräte (Rechner, PDAs, mobile Embedded-Einheiten)
Robuste Embedded-Plattformen nutzbar:

Übersicht

Pengutronix
Wireless Ethernet - Technologie
Anwendungen in der Logistik
Sicherheit
Linux und Open Source

Anwendungen in der Logistik

Anbindung mobiler Einheiten:
Übermittlung dezentraler Daten an IT-Infrastruktur
Weitere Anwendungen...? Diskussion!

Übersicht

Pengutronix
Wireless Ethernet - Technologie
Anwendungen in der Logistik
Sicherheit
Linux und Open Source

Sicherheit

Zwei wesentliche Probleme:
Authentifizierung - wer darf übertragen?
Datenübertragung - wie wird übertragen?

Sicherheit

Wireless LAN hat standardmäSSig Sicherheitsfunktionen (WEP - Wired Equivalent Privacy)
Authentifizierung: PaSSwort in AP, Clients
Verschlüsselung: RC4 Algorithmus
Übertragene Daten werden auf Korrektheit geprüft
WEP wurde „hinter verschlossenen Türen“ entwickelt

Sicherheit

Access-Points sind im Auslieferungszustand unverschlüsselt!
Auspacken-Einschalten Gehackt werden...
Minimum ist: WEP Mechanismus einschalten!
Aber...

WEP Probleme

Das zum Einsatz kommende Verfahren ist schwach!
Bestimmte Muster können trotz Verschlüsselung geraten werden
„Weak Packets“ - Schlüssel kann geraten werden (0.04
100 Pakete pro Sekunde - 30 Minuten im Mittel
Fazit: WEP ist keine Lösung zur Absicherung!

Sicherheit - aber wie?

Vorteil: „normale“ IT-Infrastruktur!
Technologien aus der Server-Welt können verwendet werden
VPN - Virtuelle Private Netze
Starke Verschlüsselung zwischen Teilnehmern
Starke Authentifizierung - ähnlich Homebanking

Übersicht

Pengutronix
Wireless Ethernet - Technologie
Anwendungen in der Logistik
Sicherheit
Linux und Open Source

Linux als Grundlage

Linux kommt aus der Serverwelt
Alle modernen Krypto-Technologien verfügbar
Modulares Betriebssystem
Linux läuft auf Embedded-Devices und auf Servern
Offene Technologie
Keine Lizenzkosten

Linux für Embedded-Anwendunge

Linux läuft nicht nur auf x86 Rechnern
Für mobile Geräte: ARM, PowerPC
Voraussetzung für Wireless LAN: CompactFlash, USB
Viele Prozessoren: System on Chip

Linux für Embedded-Anwendunge

PowerPC: stromsparend, leistungsfähig
x86: kostengünstig
Beispiel: SolidCard Familie
Gleiche Software auf x86 und PPC - unter Linux

Linux für Embedded-Anwendunge

ARM/XScale: besonders stromsparend!

Linux und Sicherheit

Auch auf den Embedded-Rechnern:
Standard-Technologien!
IPSec, OpenSSL, CIPE, OpenVPN, TUN/TAP, ...
Offene Entwicklung - Peer Review!
... und alles ist im Sourcecode verfügbar

Fragen? Anregungen...?