https://secvi.inet.haw-hamburg.de/

Sichere Kommunikationsnetze im Auto

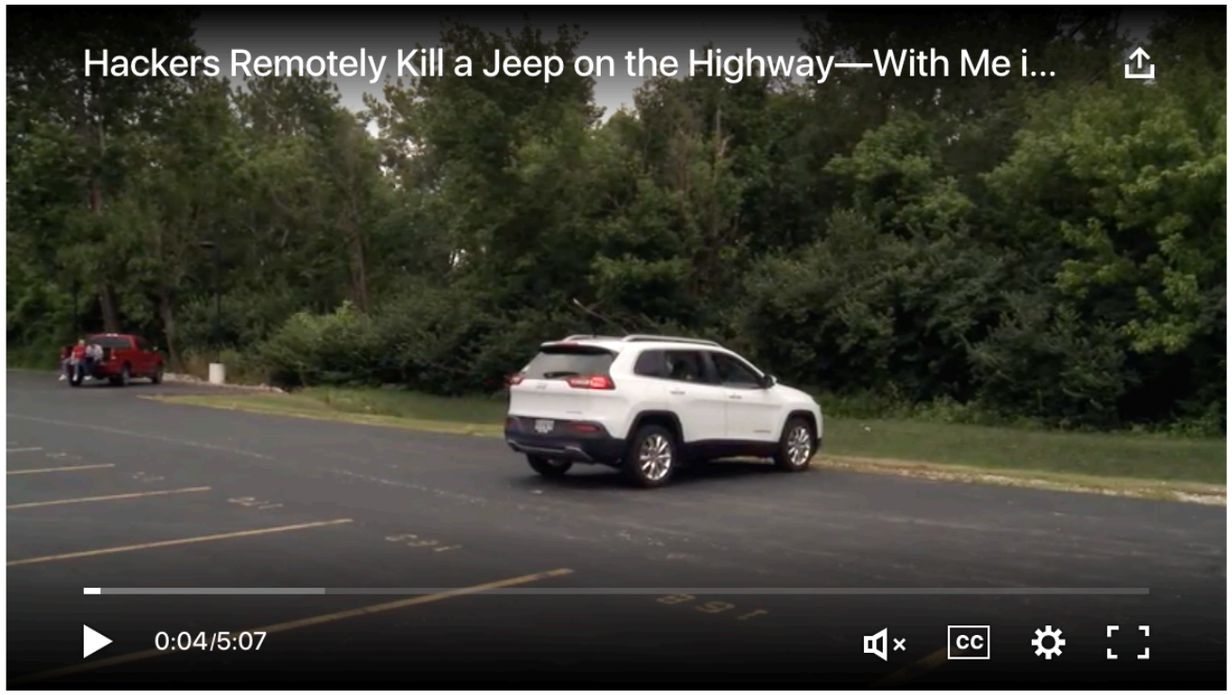
Grundseminar Vortrag von Wilhelm Schumacher, gehalten am 27.11.2018 im Rahmen des Master Informatik an der HAW Hamburg

Agenda

1. Kommunikationsnetze im Auto
2. Aktuelle Bedrohungen
3. Network Intrusion Detection
4. Software Defined Networking
5. Ausblick
6. Wichtige Konferenzen und Quellen

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

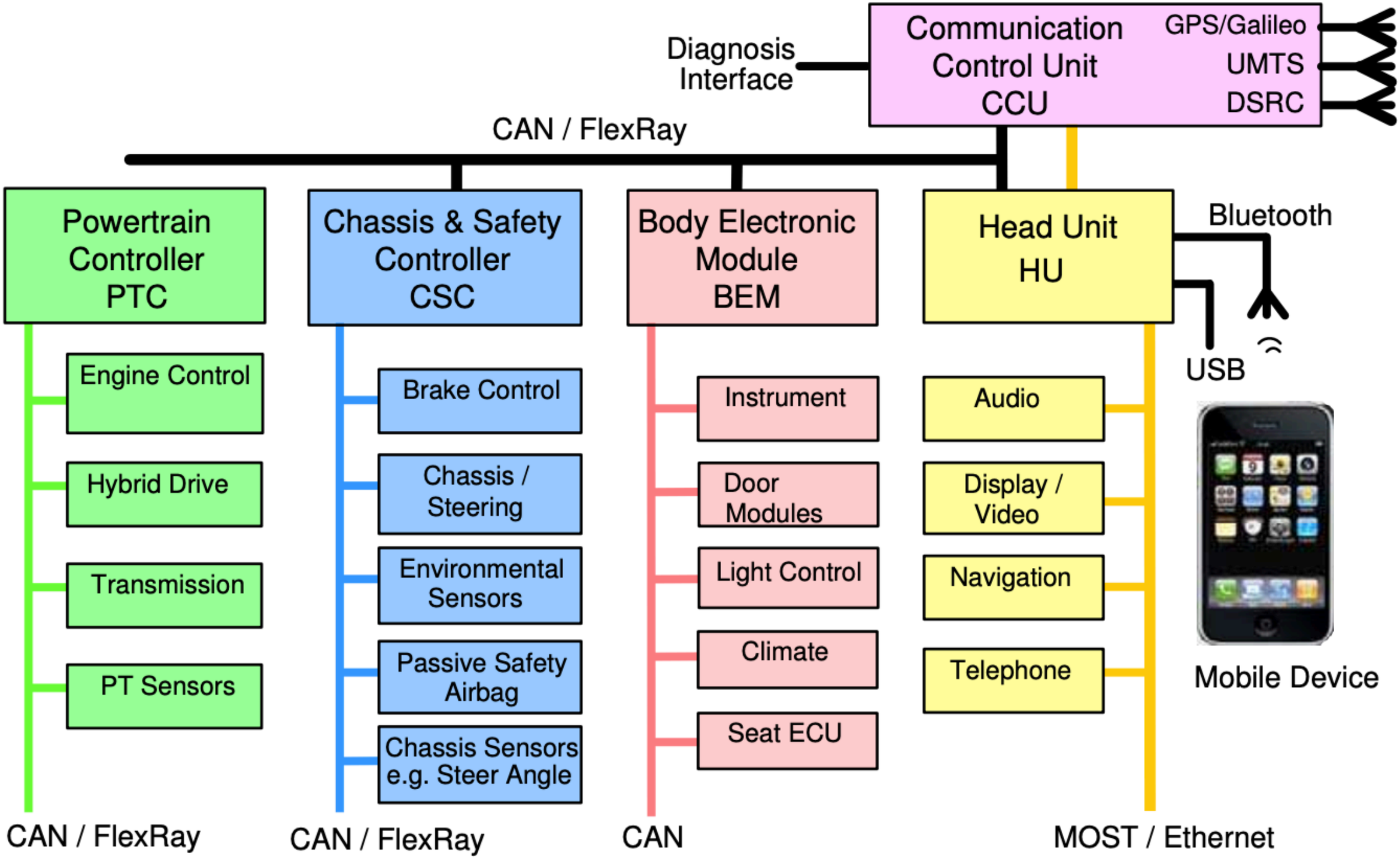
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

ANDY GREENBERG SECURITY 08.10.15 4:29 PM

A NEW WIRELESS HACK CAN UNLOCK 100 MILLION VOLKSWAGENS

ANDY GREENBERG SECURITY 08.16.17 04:55 PM

A DEEP FLAW IN YOUR CAR LETS HACKERS SHUT DOWN SAFETY FEATURES



http://www.eurecom.fr/fr/publication/3088/download/rs-publi-3088.pdf

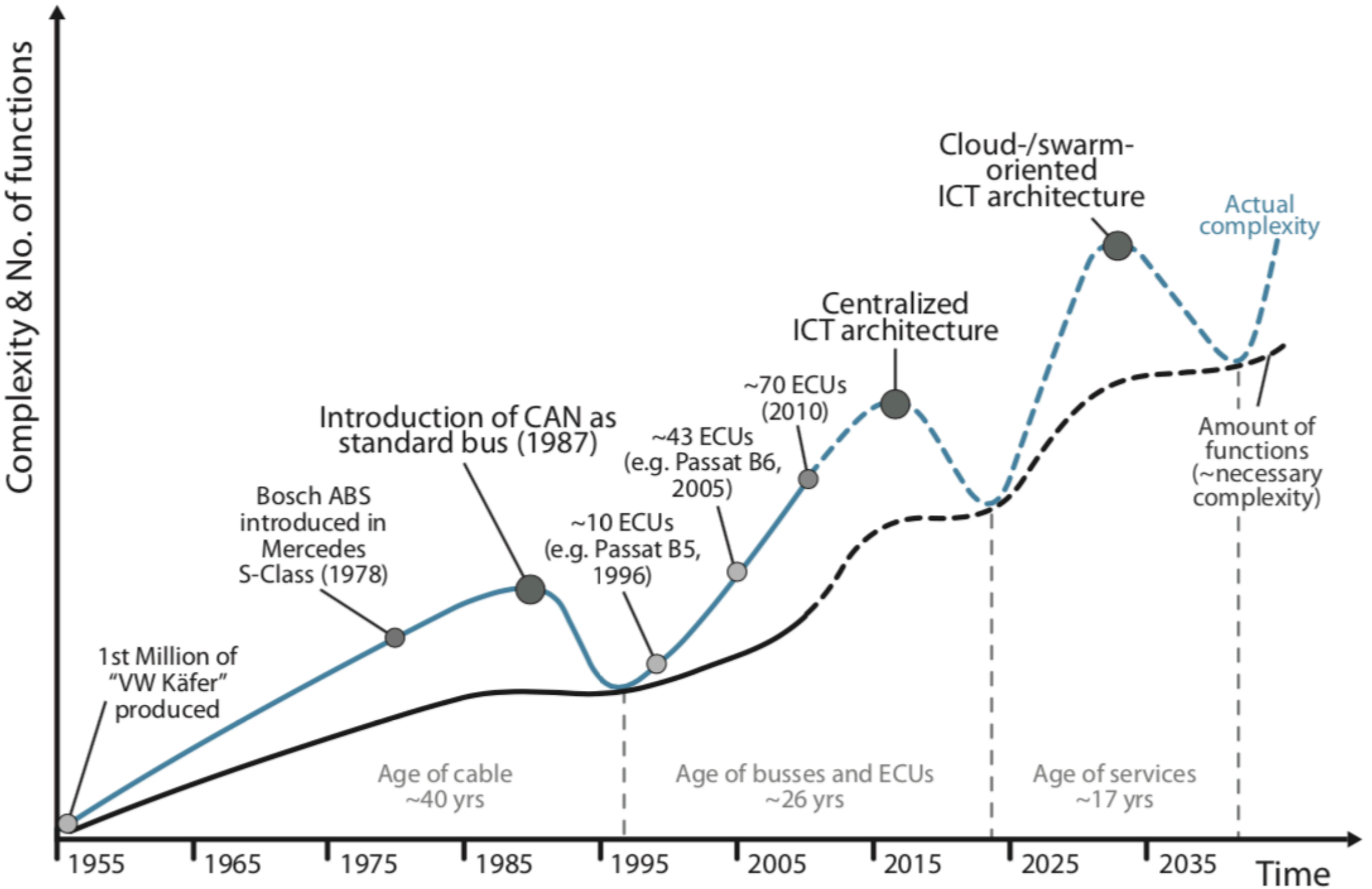


Fig. 1. Evolution of complexity in ICT architectures

Aktuelle Bedrohungen

- Kein abgeschottetes Netzwerk mehr
- **V2V** (Vehicle to Vehicle) und **V2I** (Vehicle to Infrastructure) und **V2C** (Vehicle to Cloud)
- Denkweise in **Diensten**
- Neue Sicherheitskonzepte notwendig
- Mögliche Ziele: Diebstahl, elektronisches Tuning, Sabotage, Erpressung, Sammeln privater Daten …

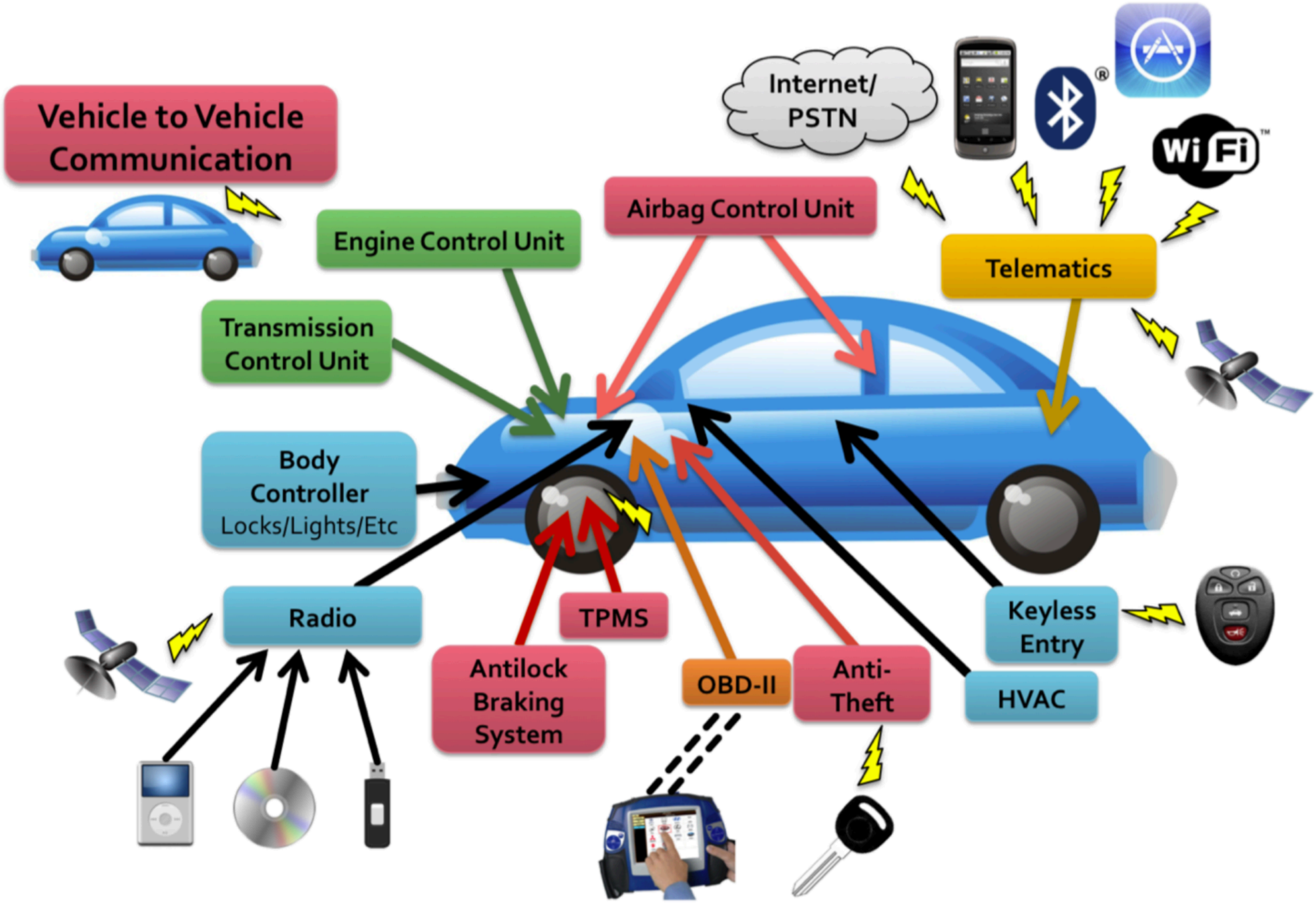


Figure 1: *Digital I/O channels appearing on a modern car.* Colors indicate rough grouping of ECUs by function.

Comprehensive Experimental Analyses of Automotive Attack Surfaces [8]

Potentielle Schwachstellen

- Unsichere Komponenten
- Keine Verschlüsselung und keine Chain of Trust
- Vermischung von Domänen in Subnetzen
- Einige ECUs erlauben updating und reflashing (mit einer ECU können möglicherweise alle anderen übernommen werden)
- Und viele weitere ….

Network Intrusion Detection

- Erkennt Attacken anhand von Mustern
- Informiert nur über Sicherheitslücken
- Angriffe können auch nach Durchbruch der Firewall noch erkannt werden
- Host-basierte Systeme vs. Netzwerk-basierte Systeme

Unterschiedliche Arten

Intrusion Detection Systems (IDS)

Misuse-based

- Sucht nach bekannten Angriffsmustern

Bekannte Angriffe werden sicher erkannt

Kein false positive

Unbekannte Angriffsarten werden nicht entdeckt

Anomaly-based

- Versucht unbekanntes, von normalen Verhalten abweichendes Verhalten, zu identifizieren

Kann möglicherweise sowohl bekannte als auch unbekannte Attacken entdecken

False positive möglich

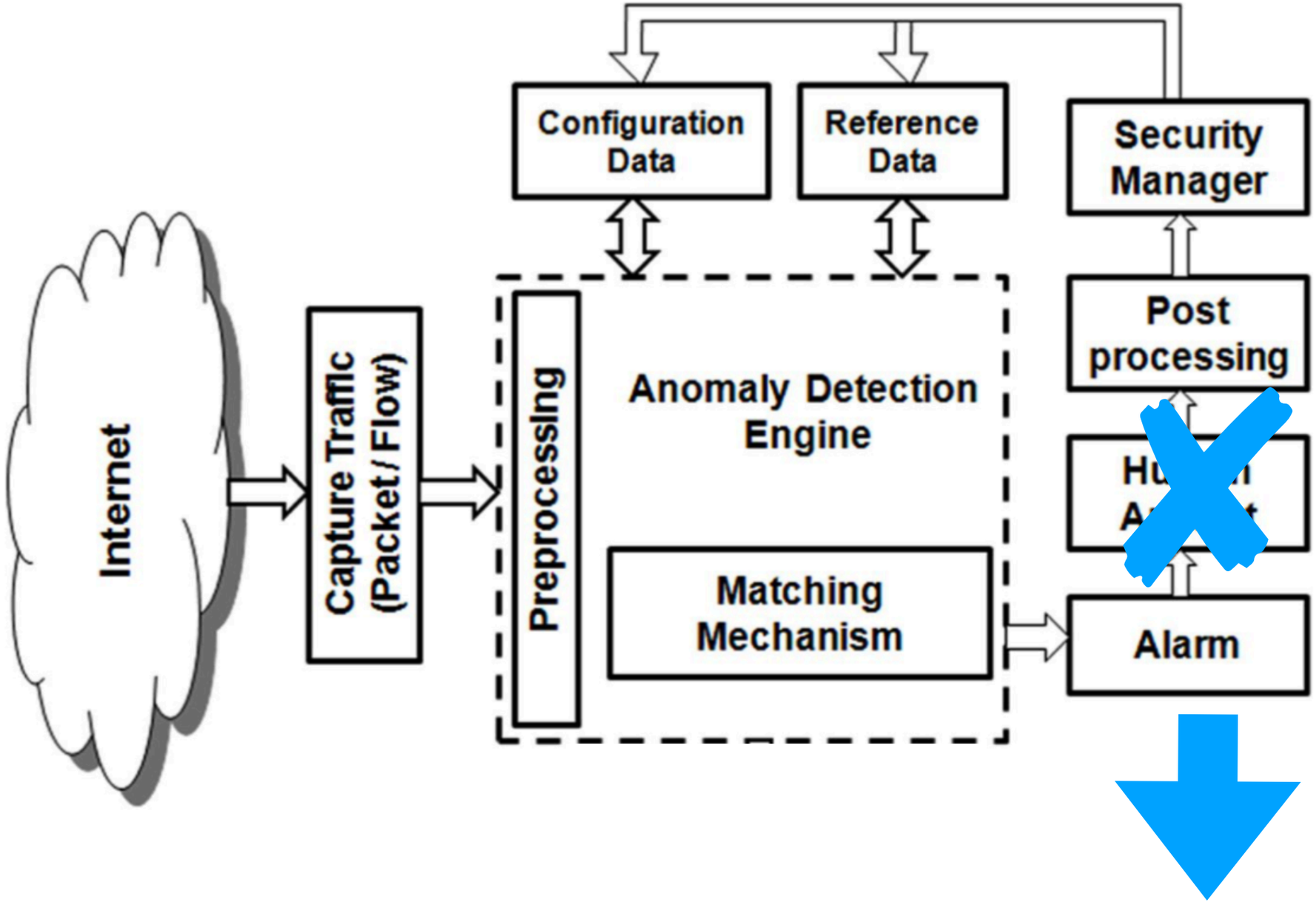


Fig. 1. A generic architecture of ANIDS

BHUYAN et al.: NETWORK ANOMALY DETECTION: METHODS, SYSTEMS AND TOOLS [5]

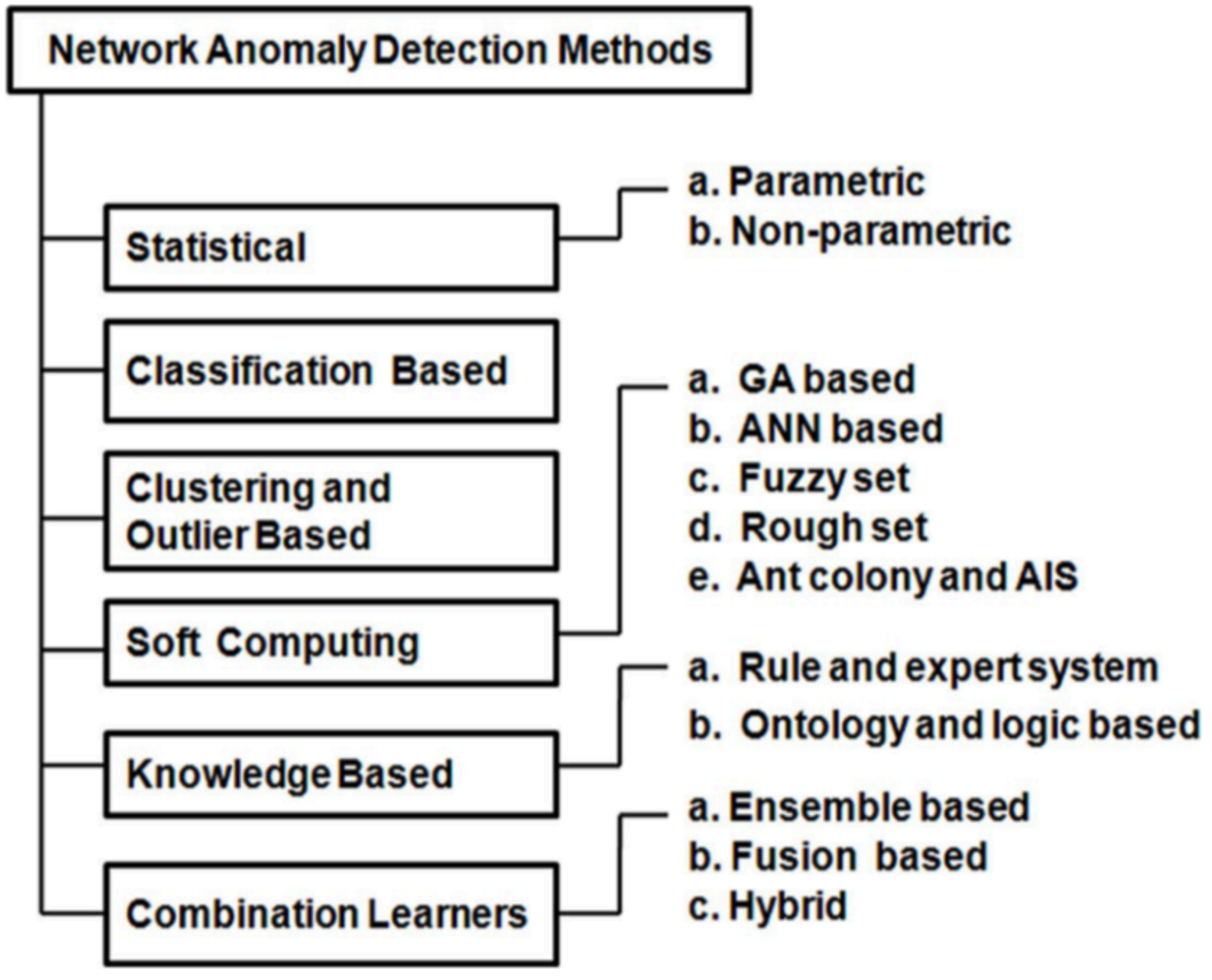
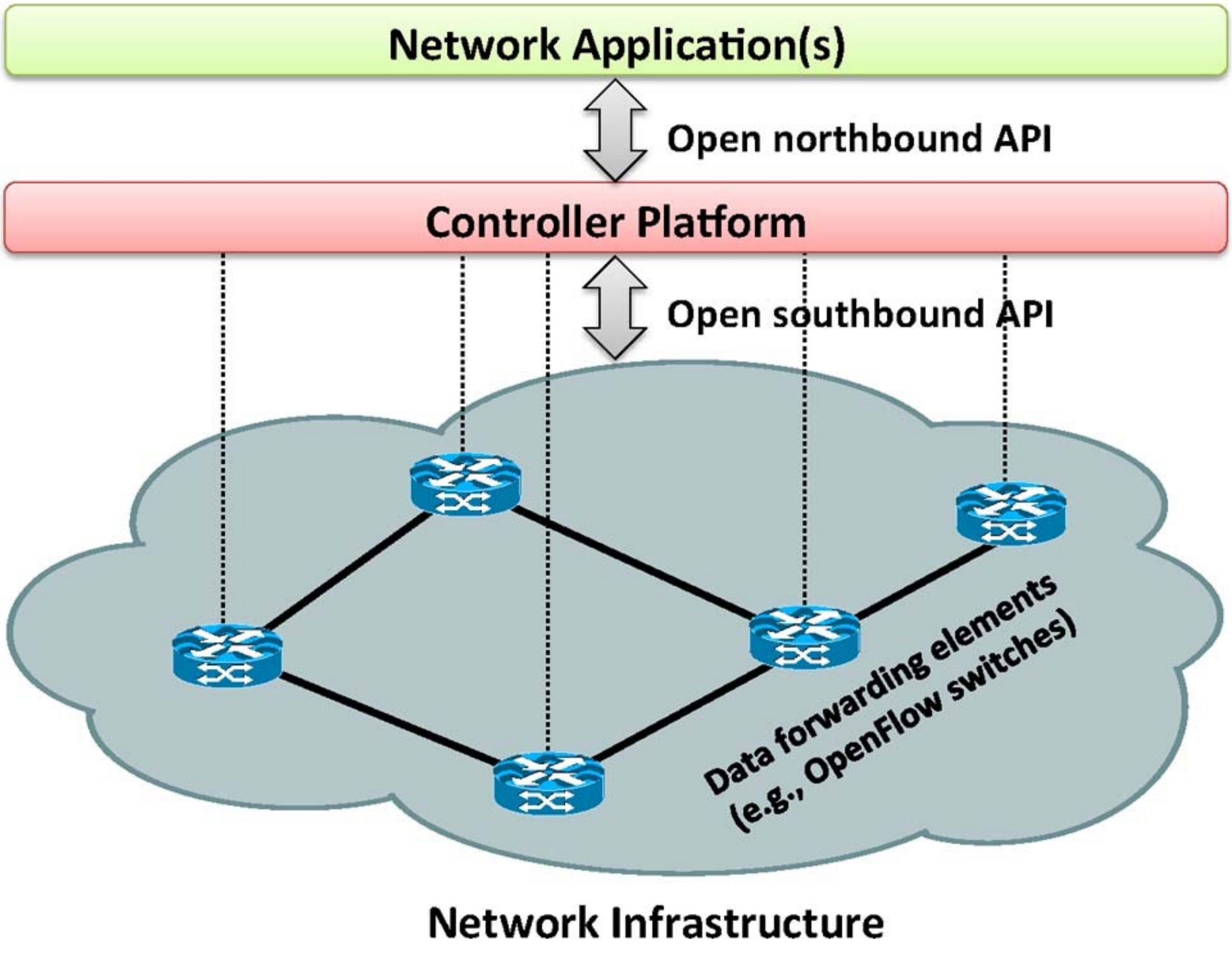


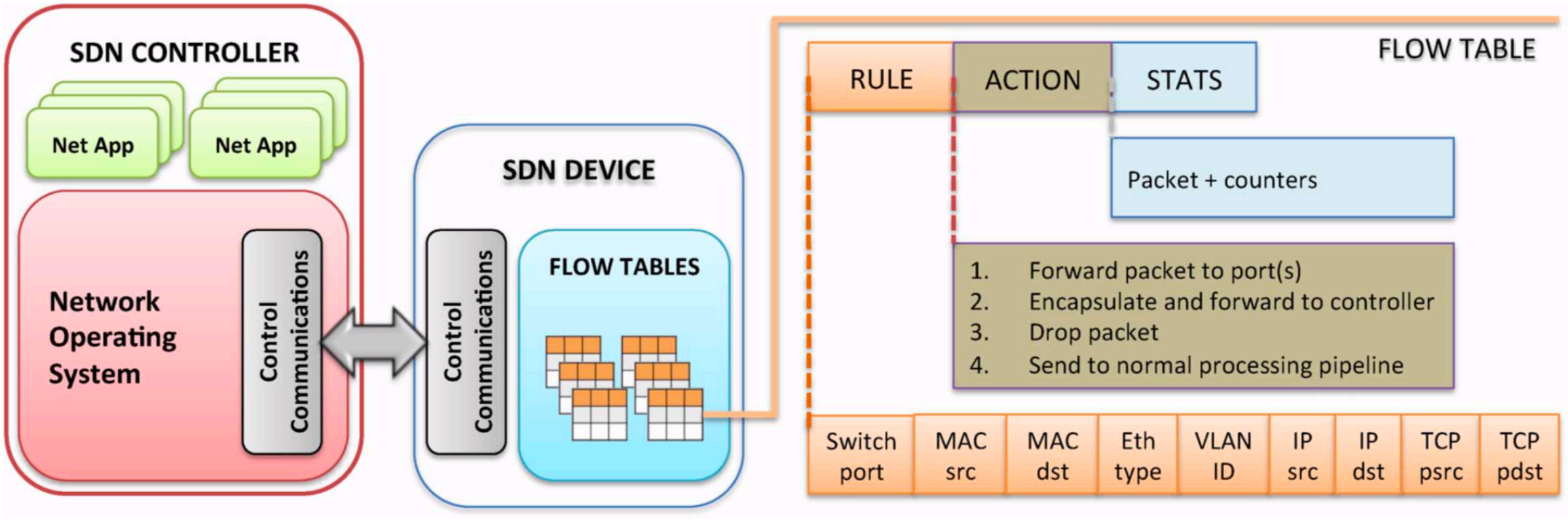
Fig. 4. Classification of network anomaly detection methods (GA-Genetic Algorithm, ANN-Artificial Neural Network, AIS-Artificial Immune System)

Software-Defined Networking

- aufkommendes Netzwerk Paradigma
- traditionelle IP Netzwerke sind komplex und schwierig zu konfigurieren
- Steuerung des Netzwerkes ist von der Datenweiterleitung in der Hardware getrennt
- Unterteilung in Data Plane und Control Plane



Kreuz et al.: Software-Defined Networking: A Comprehensive Survey [6]



Kreuz et al.: Software-Defined Networking: A Comprehensive Survey [6]

+

Kosten der Router

Zentralisierung der Architektur

Dynamische Resourcenvergabe

Filter von Paketen

Weiterleitung zu höheren Sicherheitsmechanismen

−

Single Point of Failure

Zusätzliche Netzlast

Ausblick

- Die Integration des Internets in das Auto erfordert neue Sicherheitsmechanismen

- Sicherheitsmechanismen wie **Network Intrusion Detection** oder das Netzwerkparadigma **Software Defined Network** müssen an die spezifischen Eigenschaften des Autos angepasst werden

- Ziel im Rahmen des Masters: Anpassung des Konzeptes der Network Intrusion Detection an den Kontext Auto

- Grundprojekt: Anomaly Detection, Machine Learning-Based Approaches (Classification/Statistical)

Wichtige Konferenzen

1. Automotive Security

    - Escar - The World's Leading Automotive Cyber Security Conference, November 13 to 14, 2018, Brussels

    - VDI Conference - Cyber Security for Vehicles, July 9 to 10, 2019, Düsseldorf

    - IEEE Vehicular Networking Conference (VNC) December 5–7, 2018, Taipei, Taiwan

    - Vehicular Technology Conference (VTC) Chicago

2. Automotive Security von der Industrie

    - Automotive Ethernet Kongress (Industrie) Feb 2019 in München

3. Security Konferenzen

    - Eher abschreiben als präsentieren

Quellen

- [1] https://secvi.inet.haw-hamburg.de/
- [2] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- [3] The Software Car: Building ICT Architectures for Future Electric Vehicles: - https://ieeexplore.ieee.org/document/6183198/
- [4] Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks: - https://ieeexplore.ieee.org/document/6615528/
- [5] Network Anomaly Detection: Methods, Systems and Tools: - https://ieeexplore.ieee.org/document/6524462/
- [6] Software-Defined Networking: A Comprehensive Survey: -https://ieeexplore.ieee.org/document/6994333/
- [7] Remote Exploitation of an Unaltered Passenger Vehicle: -https://ericberthomier.fr/IMG/pdf/remote_car_hacking.pdf
- [8] Comprehensive Experimental Analyses of Automotive Attack Surfaces: -http://www.autosec.org/pubs/cars-usenixsec2011.pdf

Vielen Dank für die Aufmerksamkeit