Security with Software-Defined Networking in Automotive Networks

Mehmet Cakir

Dept. Computer Science, Hamburg University of Applied Sciences

mehmet.cakir@haw-hamburg.de

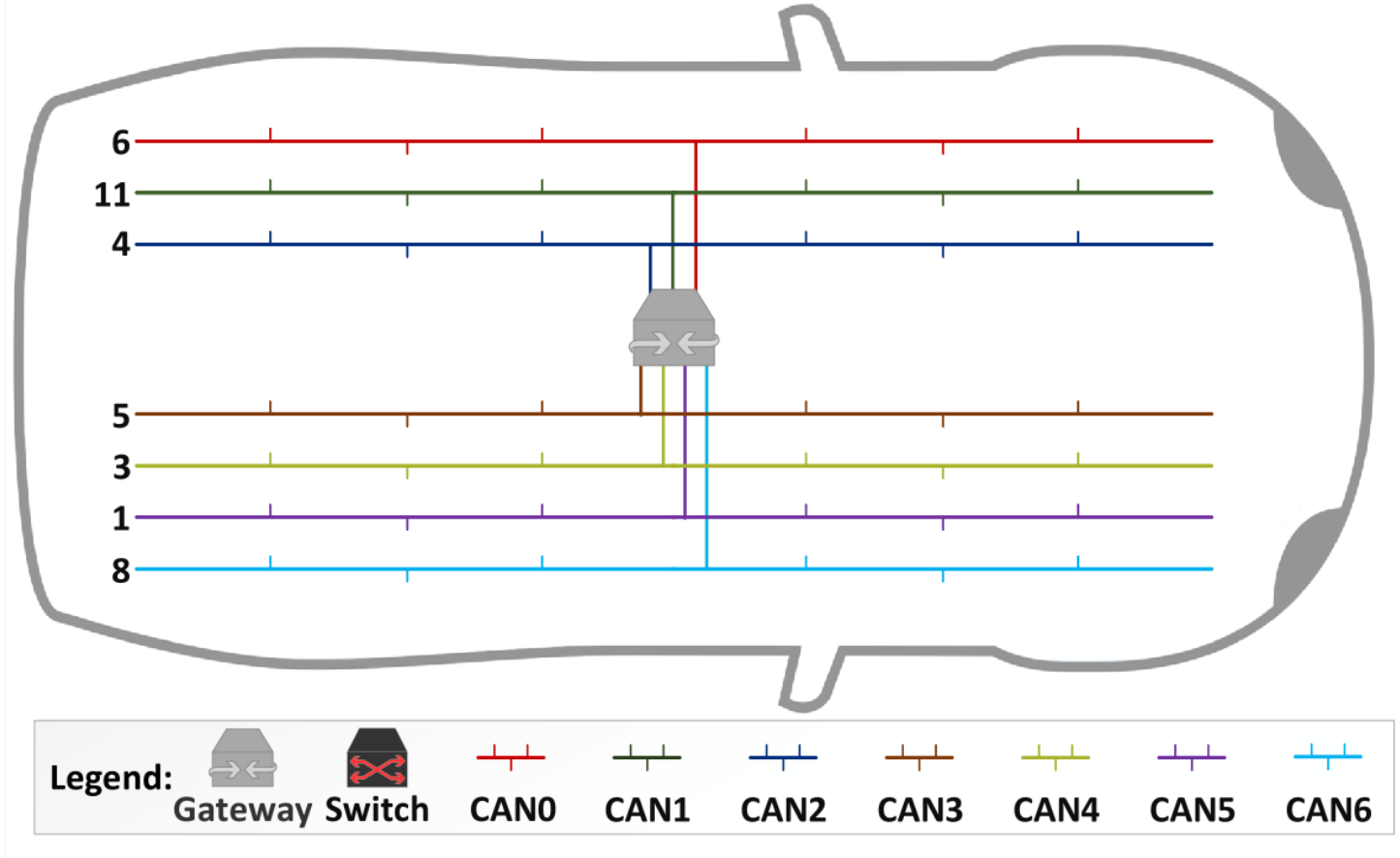
Outline

- Introduction to Automotive Networks
- State-of-the-Art Automotive Networks
- Security Standards and Guidelines
- Security Concepts
- Software-Defined-Networking (SDN)
- SDN Security Concepts in LANs
- SDN Concepts in Cars
- Conclusion & Outlook

Introduction to Automotive Networks

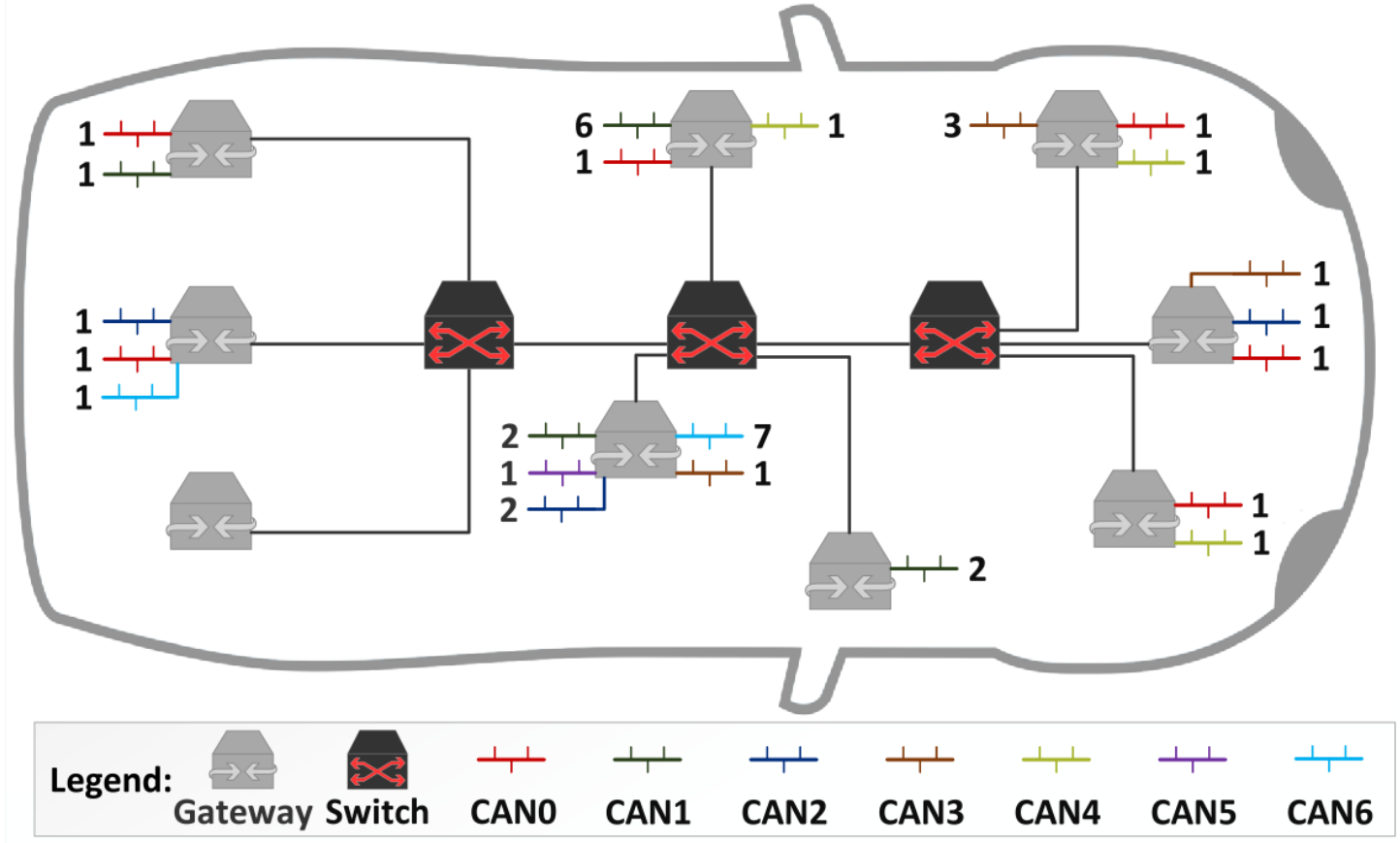
- Vehicle-to-Everything (V2X) requires security
- Ethernet is increasingly being used in automotive networks
- IEEE Time-Sensitive Networking (TSN) enables real-time in Ethernet
- Software-Defined Networking controls flows

State-of-the-Art Automotive Networks



Source: M. Cakir, T. Häckel, S. Reider, P. Meyer, F. Korf, and T. C. Schmidt, "A QoS Aware Approach to Service-Oriented Communication in Future Automotive Networks," in 2019 IEEE Vehicular Networking Conference (VNC). Piscataway, NJ, USA: IEEE Press, Dec. 2019.

State-of-the-Art Automotive Networks



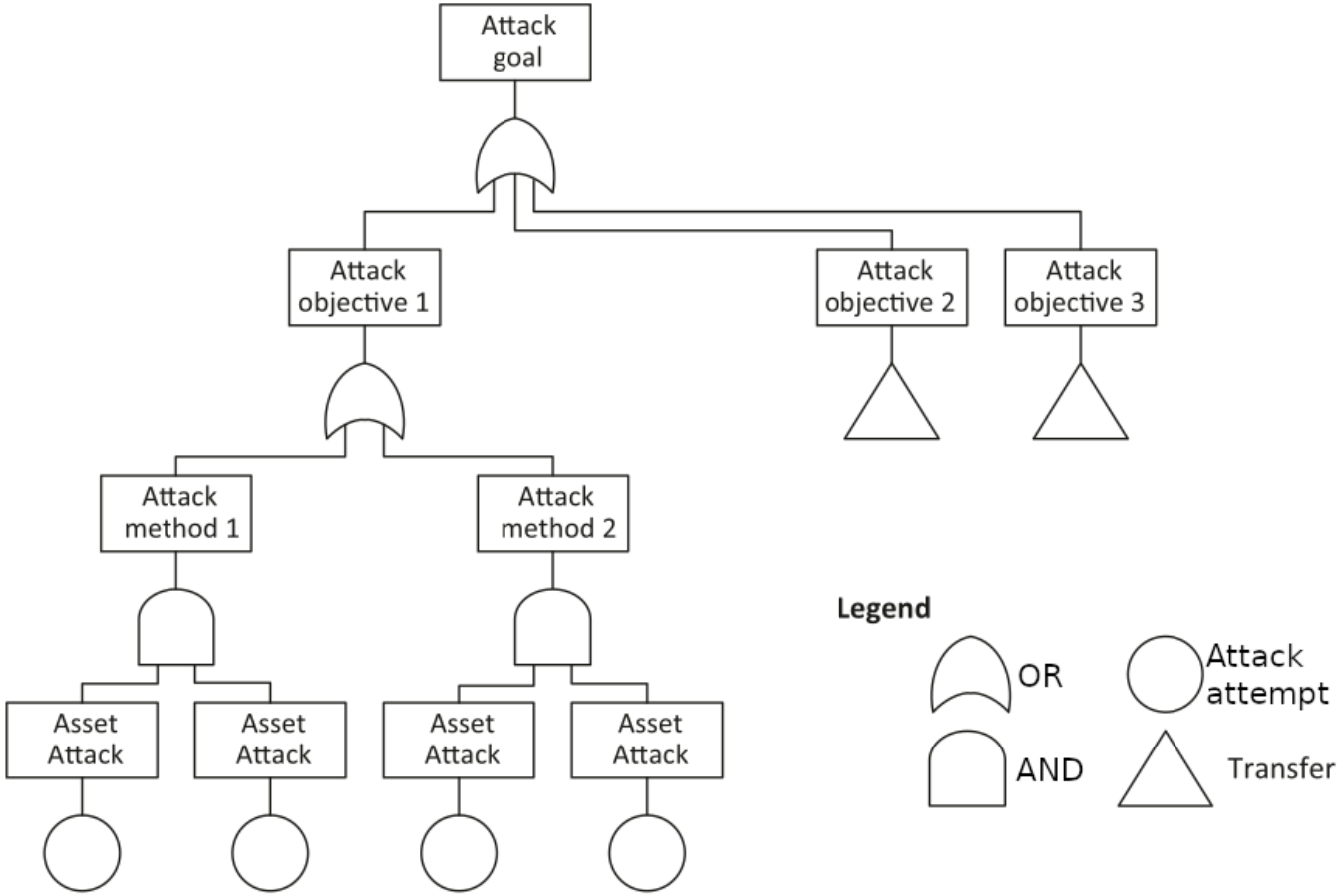
Source: M. Cakir, T. Häckel, S. Reider, P. Meyer, F. Korf, and T. C. Schmidt, "A QoS Aware Approach to Service-Oriented Communication in Future Automotive Networks," in 2019 IEEE Vehicular Networking Conference (VNC). Piscataway, NJ, USA: IEEE Press, Dec. 2019.

Security Standards and Guidelines

- ISO 26262 (safety) and SAE J3061 (security)
- Risk identification
- Risk assessment
- Goals
- Concept
- Functional requirements
- ISO/SAE 21434

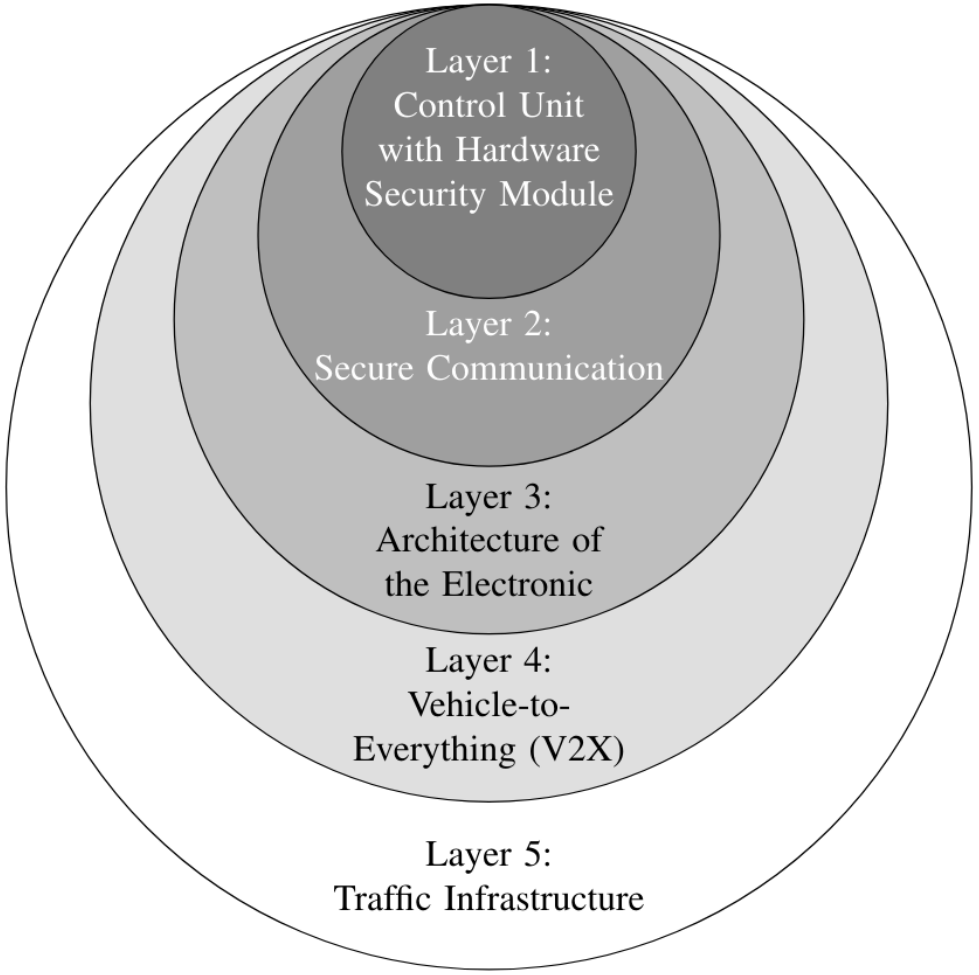
Source: L. Schnieder and R. S. Hosse, “Entwurf angriffssicherer Systeme,” in Leitfaden Automotive Cybersecurity Engineering. Springer Fachmedien Wiesbaden, 2018, pp. 13–24.

Security Standards and Guidelines



Source: L. Schnieder and R. S. Hosse, “Entwurf angriffssicherer Systeme,” in Leitfaden Automotive Cybersecurity Engineering. Springer Fachmedien Wiesbaden, 2018, pp. 13–24.

Security Standards and Guidelines

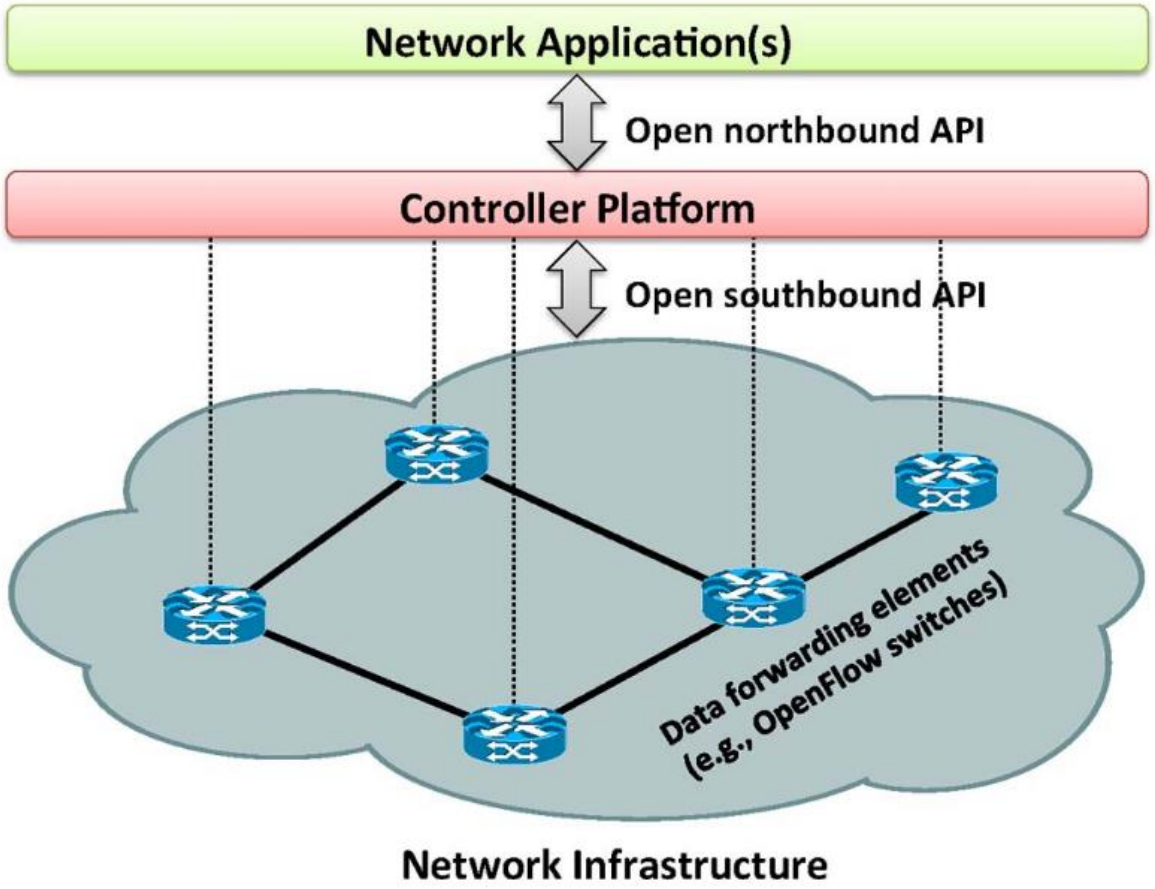


Source: L. Schnieder and R. S. Hosse, “Entwurf angriffssicherer Systeme,” in Leitfaden Automotive Cybersecurity Engineering. Springer Fachmedien Wiesbaden, 2018, pp. 13–24.

Security Concepts

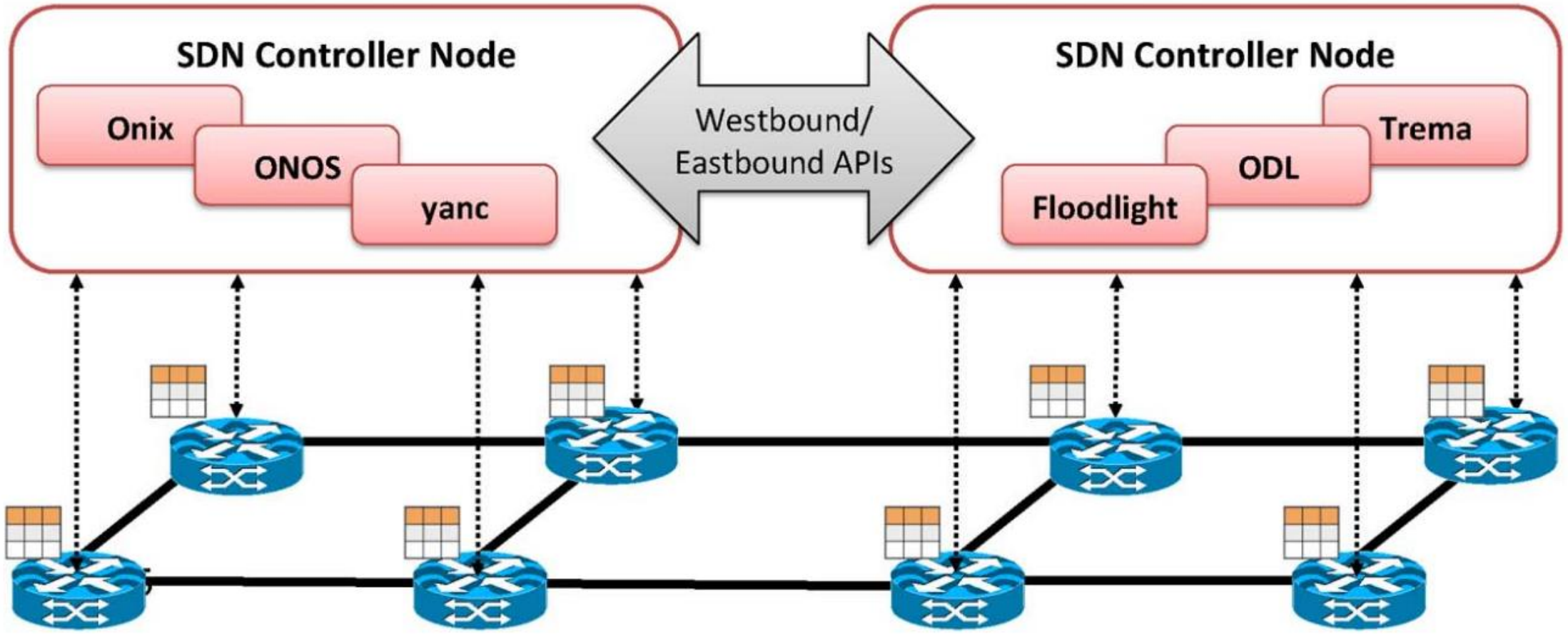
- Isolate domains physically and logically [1]
- Message Authentication Codes (MACs) [2]
- Cloud computing security and adaptive security [3]
- Automotive firewalls with filtering uncommon content [4]
- Intrusion Detection System coordinating other system units [5]
- VLAN Segmentation isolate traffic logically [6]
- TLS, DTLS and IPsec [7]

Software-Defined Networking (SDN)



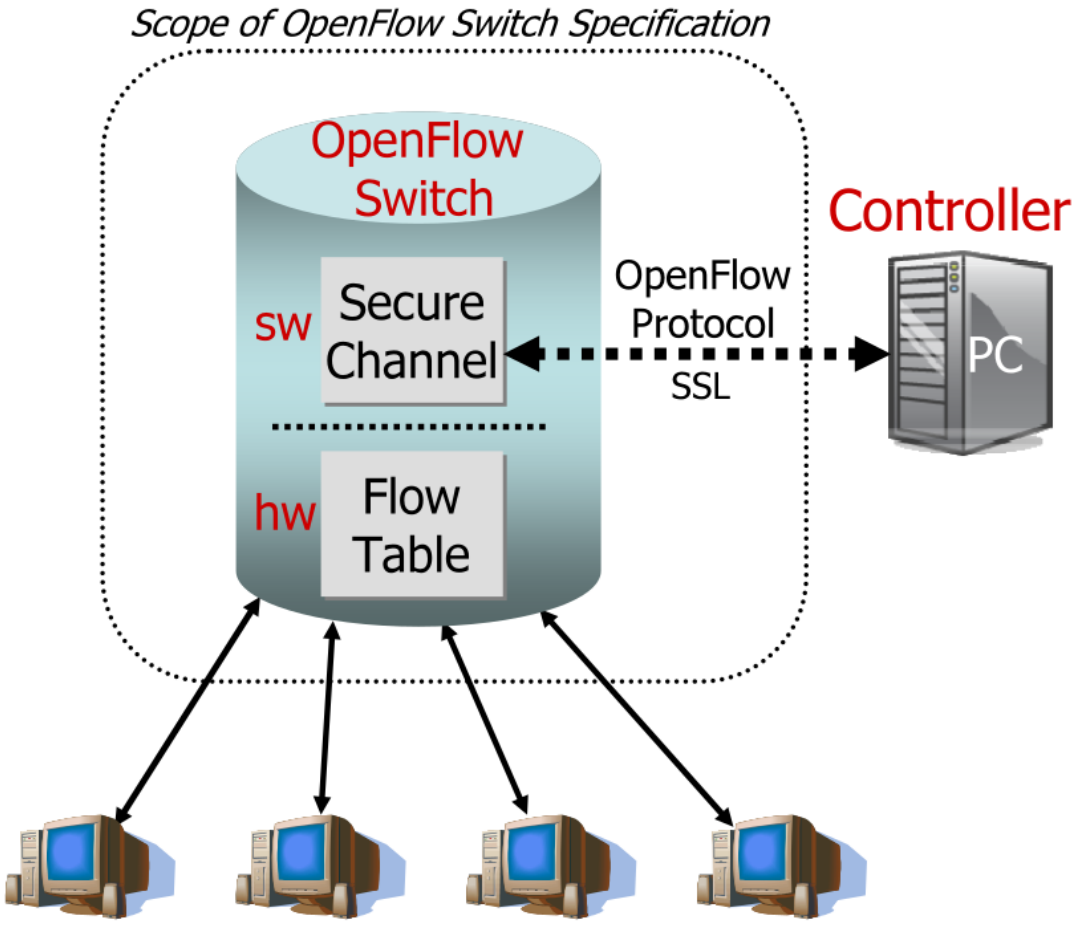
Source: D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.

Software-Defined Networking (SDN)



Source: D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.

Software-Defined Networking (SDN)



Source: N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008.

SDN Security Concepts in LANs

- Security in control plane with additional security devices [8]
- Detection of IP and MAC spoofing attacks in the SDN controller [9]
- TLS extension by defining a timestamp [10]
- DDoS prevention by blocking or redirecting with flow rules [11]
- Security approach on all layers [12]

SDN Concepts in Cars

- Time-Sensitive Software-Defined Networking (TSSDN) [13]
- Network Anomaly Detection System (NADS) using SDN and TSN [14]
- Redundant links and rate limiting (data plane) [15]
- Access control lists to regulate access of applications [15]
- TSN re-configuration with a hybrid solution [15]
- Signed manifests for device and application authentication [15]
- Ensure safety critical traffic or even stop the car [15]

Conclusion & Outlook

- Beginning overview about the current state of automotive networks
- Security and Software-Defined Networking (SDN) concepts
- Real-time requirements can be met with (TSSDN)
- SDN opens up new attack surfaces like the centralized control plane
- Flow rules can isolate traffic
- Network Anomaly Detection has a promising hit rate

- Further research, simulation and evaluation

References

[1] H. Ju, B. Jeon, D. Kim, B. Jung, and K. Jung, “Security Considerations for In-Vehicle Secure Communication,” in 2019 International Conference on Information and Communication Technology Convergence(ICTC), 2019, pp. 1404–1406.

[2] Q. Hu and F. Luo, “Review of Secure Communication Approaches for In-Vehicle Network,” vol. 19, no. 5, pp. 879–894, Sep.

[3] V. L. L. Thing and J. Wu, “Autonomous Vehicle Security: A Taxonomy of Attacks and Defences,” in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing(CPSCom) and IEEE Smart Data (SmartData), Dec 2016, pp. 164–170.

[4] Q. Hu and F. Luo, “Review of Secure Communication Approaches for In-Vehicle Network,” vol. 19, no. 5, pp. 879–894, Sep.

[5] H. Kwon, S. Lee, J. Choi, and B. Chung, “Mitigation Mechanism against In-Vehicle Network Intrusion by Reconfiguring ECU and Disabling Attack Packet,” in 2018 International Conference on Information Technology (InCIT), 2018, pp. 1–5.

References

[6] C. Lin and H. Yu, “Invited: Cooperation or Competition? Coexistence of Safety and Security in Next-Generation Ethernet-based Automotive Networks,” in 2016 53nd ACM/EDAC/IEEE Design Automation Conference(DAC), 2016, pp. 1–6.

[7] J. Lastinec and L. Hudec, “Comparative Analysis of TCP/IP Security Protocols for Use in Vehicle Communication,” in 2016 17th International Carpathian Control Conference (ICCC), 2016, pp. 429–433.

[8] X. Xu and L. Hu, “A Software Defined Security Scheme Based on SDN Environment,” in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017, pp.504–512.

[9] M. Al-Zewairi, D. Suleiman, and S. Almajali, “An Experimental Software Defined Security Controller for Software Defined Network,” in 2017 Fourth International Conference on Software Defined Systems (SDS), 2017, pp. 32–36.

[10] S. Midha and K. Triptahi, “Extended TLS Security and Defensive Algorithm in OpenFlow SDN,” in 2019 9th International Conference on Cloud Computing, Data Science Engineering (Confluence), 2019, pp. 141–146.

References

[11] S. Krishnan and J. J. E. Oliver, “Mitigating DDoS Attacks in Software Defined Networks,” in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 960–963.

[12] Y. Liu, B. Zhao, P. Zhao, P. Fan, and H. Liu, “A Survey: Typical Security Issues of Software-Defined Networking,” China Communications, vol. 16, no. 7, pp. 13–31, 2019.

[13] T. Häckel, P. Meyer, F. Korf, and T. C. Schmidt, “Software-Defined Networks Supporting Time-Sensitive In-Vehicular Communication,” in 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). Piscataway, NJ, USA: IEEE Press, Apr. 2019, pp. 1–5.

[14] P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, “Network Anomaly Detection in Cars based on Time-Sensitive Ingress Control,” in 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall). Piscataway, NJ, USA: IEEE Press, Nov. 2020.

[15] M. Haeberle, F. Heimgaertner, H. Loehr, N. Nayak, D. Grewe, S. Schildt, and M. Menth, “Softwarization of Automotive E/E Architectures: A Software-Defined Networking Approach,” in 2020 IEEE Vehicular Networking Conference (VNC), 2020, pp. 1–8.