International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Smart Network Interconnect for Chiplet - based Vehicular System's Security

Avani Dave[1], Krunal Dave[1]

[1]Email: *daveavani[at]gmail.com*

[2] Email: *krunaldave10[at]gmail.com*

Abstract: ***With technological advancements, semiconductors have become critical components for modern - day automotive systems. They are extensively used in various applications such as vehicular - safety, efficiency, connectivity, infotainment, and autonomous driving. The automotive industry is experiencing a surge in demand for high - performance computing, power, and area - efficient systems. With physical, economic, technological, and design challenges, Moore's Law is reaching its practical limits. Also, supply chain issues during the COVID - 19 pandemic have forced the automotive industry to search for alternative scalable design architecture such as chiplets, 3D stacking, and quantum computing. Network - on - Chip (NOC) seems to help speed standardized interface integration and reduce complexity for chiplet connections. However, it opens security concerns as NOC becomes a single and critical point for interconnect. To this end, this work comprehensively surveys attack - resilient, secure NOC systems and proposes a new smart NOC - based access control and monitoring interconnect. This approach helps enhance security and prevents unauthorized access to a network of chiplets. The simulation results of smart NOC indicate minor latency and area impacts. However, it is negligible compared to the level of attack resilience, configurability, modularity, and security it offers.***

Keywords: Automotive chiplet architecture, next - generation vehicular systems, Autonomous driving, fusion sensors, ADAS, Infotainment, gem5, chiplet, Mcpat, vehicle to everything

1. Introduction

The exemplar shift in the automotive industry is driven by advancements in Machine Learning (ML), Artificial Intelligence (AI), and semiconductor technology. Modern vehicles are no longer mere mechanical constructs; they have evolved into complex cyber - physical systems equipped with advanced electronics, sensors, and computational capabilities. This transformation is ushering in a new era of intelligent and connected vehicles, where the traditional boundaries between hardware and software are increasingly blurred. Industrial researchers have projected the semiconductor industry growth up to 1 Trillion, and 70% of it will come from automotive, computing, data storage, and wireless industries [1].

Fig.1 highlights the Society of Automotive Engineers (SAE) recommended self - driving evaluation timeline and its impact on electronics systems cost as % total car cost of the electronics devices. The automotive industry has projected ~30 to 35% growth in semiconductor utilization by 2030 [2, 3] with the arrival of fully automatic self - driving cars (levels 4 & 5), vehicle of everything (V2X) [4, 5], and software - defined vehicles [6]. Furthermore, the semiconductor industry has faced the significant impact of the global COVID - 19 pandemic due to the shutdown of production, supply chain disruption, and bottlenecks [7, 8]. The automotive industry was also affected badly by car production, chip shortages, increased prices, lack of inventories, and long waiting, making customers choose pre - owned alternatives [9, 10].

This dynamic shift in the automotive industry has increased the demand for semiconductor devices with high computing, high performance, multiple sensors, storage, AI, and ML accelerators. One emerging chiplet - based architecture is gaining popularity in automotive semiconductor manufacturers due to its ability of modularity, scalability, ease of configuration, and cost - effectiveness [11]. The network's security on a chip has emerged as the biggest and most popular attack vector for exploiting its vulnerability and compromising chiplet - based architecture's security [12].

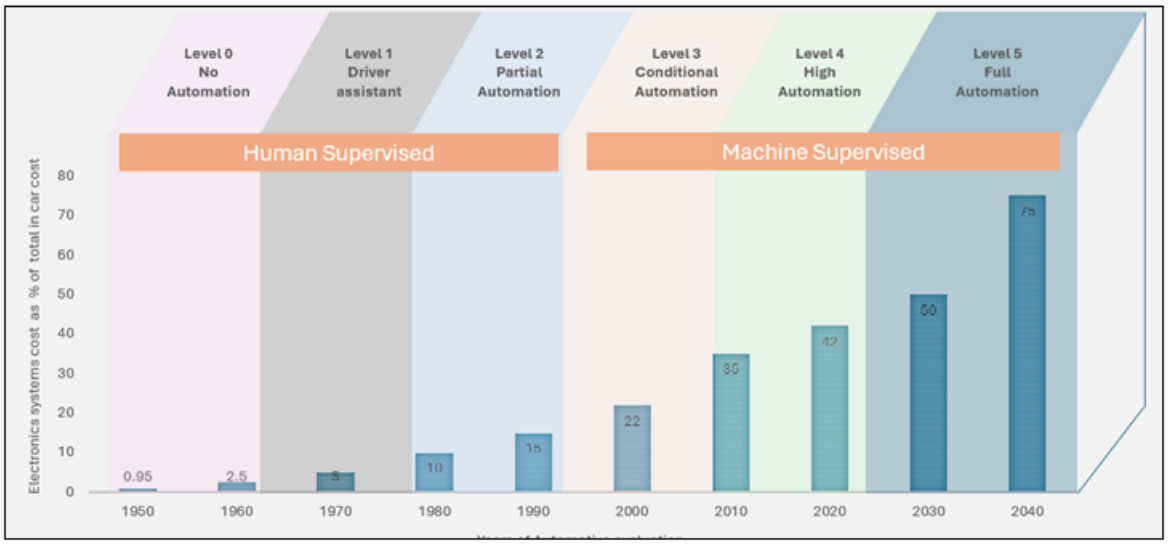

Figure 1: Highlights the evaluation of SAE levels and electronics systems cost as % total car cost.

To this end, this work presents the novel smart network on ship interconnects for chiplet - based vehicular system security. The work starts with an overview of the state - of - the - art chiplet - based automotive systems and their attack vectors. It then discussed the challenges of smart networks on chip security and trade - off choices. Then it presents the novel attack resilient and access control aware smart network on chip interconnect. The proposed smart NOC - based chiptel architecture's performance evaluation results show high efficiency and hardware - based attack detection and avoidance systems. Additionally, the smart NOC - based chiplet architecture design increases the latency marginally and offers fast prototyping, attack resilient and robust design.

2. Related work

Fig 2 depicts the high - level semiconductor/electronics utilization in modern - day vehicular systems. This work has classified vehicular ECUs, sensors, and electronics networks into four broad categories for literature review.

a) Distributed Monolithic systems.

Automotive systems have extensively used electronic control units (ECU) for specific task handling, such as powertrain management [13], advanced driver assistance systems (ADAS) [14], infotainment [15], and motion and environment perception sensors [16]. Vehicular communication has evolved significantly in recent years with the introduction and integration of Dedicated short - range communication (DSRC), Wifi, Bluetooth, 3G, Long Term Evolution (LTE) technologies, radio, and satellite communications [19]. This hybrid communication provides significant advantages for efficient, seamless, low latency, and high throughput data and information transfer [20]. However, this approach has led to complex systems design, interconnect/wiring management, and weight, resulting in increased communication latency.

b) Central controller/Hub - based systems

To address the issues of a distributed ECUs - based monolithic approach, the automotive industry has adopted a centralized controller - based architecture system design. The centralized controller - based approach has a central high - performance compute and connection unit that coordinates and manages the communication between different ECUs. This approach reduces the networking/ wiring complexity, improves data processing, and offers over - the - air firmware software updates [13]. It is a resource - efficient system design since it consolidates the functionality usage to the central hub [12]. However, it makes the central hub a single point of failure and increases security vulnerability risk.

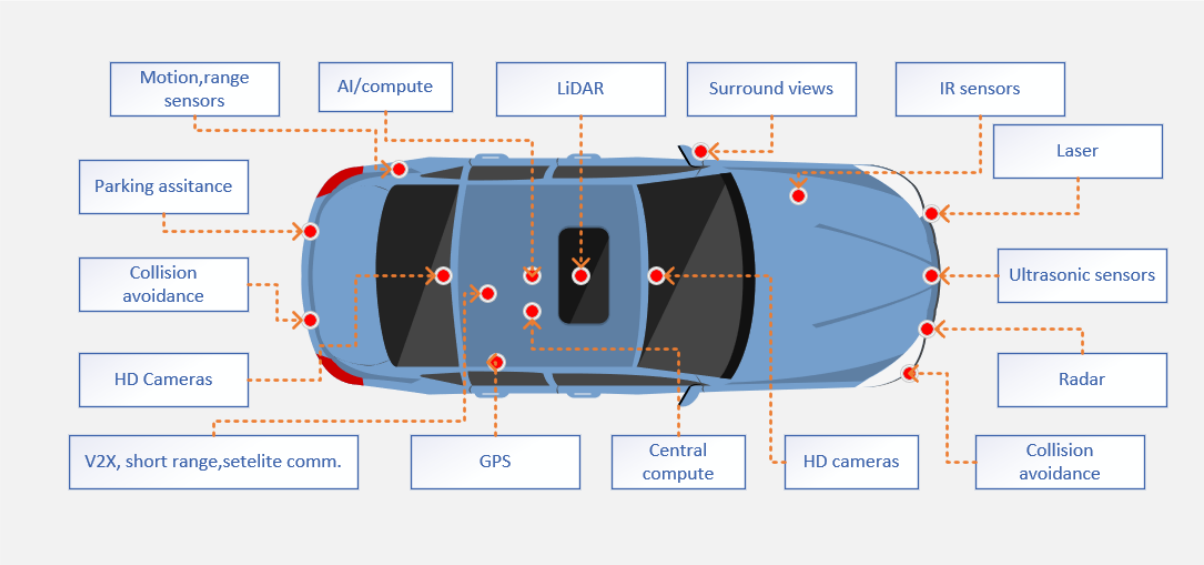

Figure 2: Depicts the electronics utilization in modern - day vehicular systems.

c) Zone - based systems.

Zone - based architecture design for automotive ECUs is the most recent approach. The zones are defined based on the physical placement and usage of the ECUs and sensors within the vehicles; e. g., four controllers will be placed on each side of the vehicle to handle multiple ECUs and transactions within that region. It aims to achieve the balance between monolithic and central controller - based systems design by offering a more scalable, modular design that can handle growing expansion demands with less complex system design [17, 18].

d) Chiplet - based systems.

The chipset - based system design approach is not new for the commercial PC market to achieve high yield and energy - efficient systems design. Recently, the automotive industry has also started shifting toward a chiplet and zone - based design approach for supporting high - performance and low - cost systems. The automotive chiplet based architecture and usage is covered by [25] researchers and industry. The study of new networks on chip - based attacks is covered by [11, 12, 25]

In summary, with changing demand and increased complex usage of semiconductors/electronics in vehicular systems, the industry has adopted different changes in system architecture. Few recent studies have also highlighted the utilization and challenges of Chiplet - based architecture for vehicular systems [11, 12, 21]. However, with the introduction of ML and AI - based accelerators, high - performance compute usages and the increased need for connectivity have become a challenging market for automotive semiconductor/systems vendors to keep up with.

To this end, this work presents a novel zone - based chiplet architecture for next - generation vehicular systems. This approach provides optimum resource utilization with adequate communication requirements. Compared to a monolithic vehicular electronics system on simulation design, it reduces the hardware software resource requirements, area, power, and performance footprints. This work paves the way for next - generation chiplet - based system design researchers to explore the use of case - specific zoning, systems selection, and Chiplet and interconnect options.

3. Smart Network Interconnect for CHIPLET BASED system's security

Fig 3 shows a proposed smart NOC interconnect - based chiplet architecture for vehicular systems. This work has identified six different chiplet zones based on internal and external communication, performance, and security requirements.

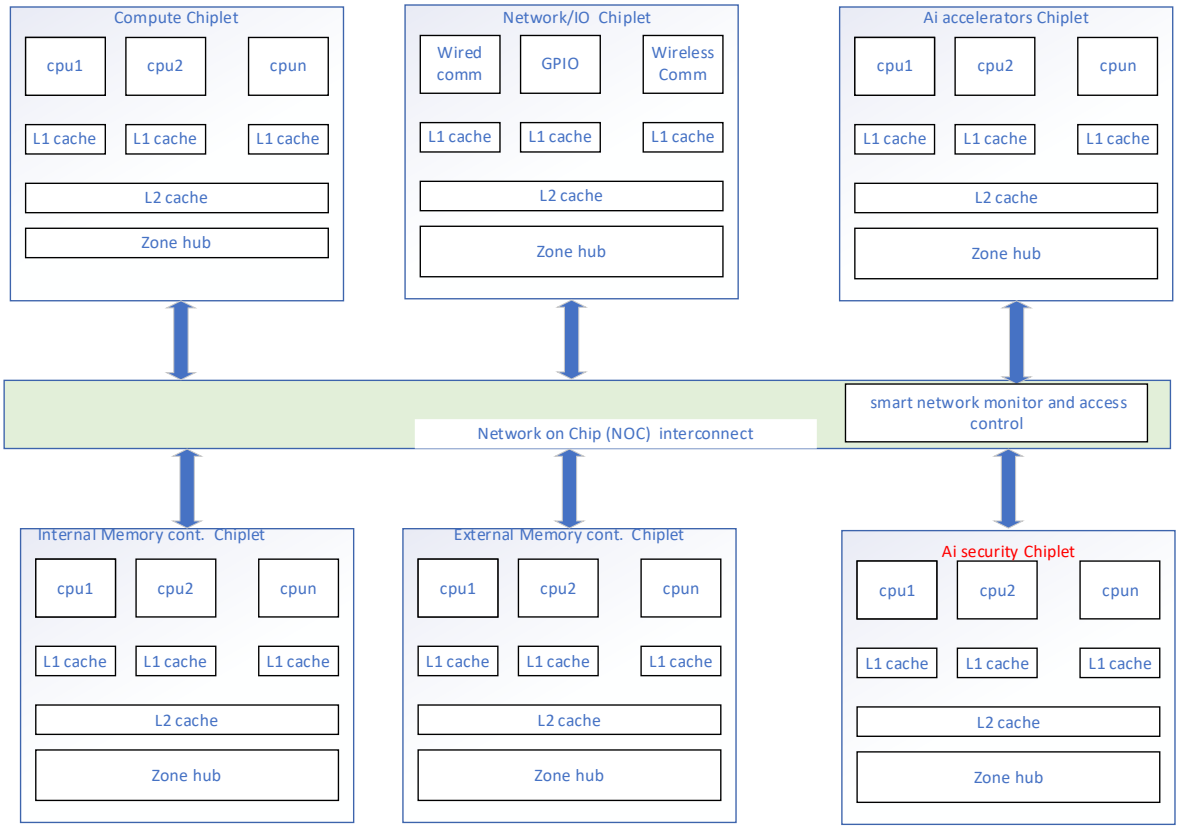

Figure 3: Zone - based monolithic system.

The compute chiplet is mainly responsible for different automotive sensors' data collection and processing. Each CPU in the compute die is directly responsible for dedicated sensor data reading and post - processing such as cameras, Lidar, Radar, Ultrasonic range detectors, and parking assistance sensors. The network/IO chiplet is responsible for wired and wireless external connections such as NIC, WiFi, JTAG, Bluetooth interconnect, etc.

AI accelerator chiplet provides computing cores for offloading AI and ML code execution for the next generation. Applications. Internal and External Memory controller chiplets are provided to route and filter the respective memory access requests. These chiplets control and process the DMA, flash, and external memory access.

In Addition, the AI security chiplet is added for incorporating internal monitoring and security code execution. For the smart network - on - chip design. Based on the use cases, different permutations and combination of inter- chiplet code and data transferred are allowed. The NOC has manufacturer and authorized user configurable.

Smart network monitor and access control system. During the system initialization vendor verified ROM code programs the initial access controls. After that, it cannot be updated. The user interface level access is provided for a user to configure less secure ring access for inter chiplet access control. The Monitor agent runs on ai security. chiplet to monitor the access and trigger an alarm by setting a hardware bit in the control register to indicate an attack. It further rejects the unauthorized access request from routing to the destination.

4. Implementation & Evaluation

The system design was simulated using gem5 [22], and power, area, and timing results evaluations were performed using McPat [23]. The network modeling was done by integrating Garnet with gem5 and updating its security stack to add access control and monitoring policies. Additional data memory was provided for user access so that the user could update the chiplet - based access controls during the runtime.

The simulation results indicate the latency of smart NOC - based zone - based architecture is increased by ~7% compared to only zone - based chiplet architecture. However, the area and power saving are significant with chiplet - based system design. Furthermore, a chiplet - based zoning system isolates and limits potential attack surfaces. The standard NOC interconnect provides flexibility and a fast communication channel, reducing the interconnection complexity.

Config	Cost	Throughput	Latency
Chiplet based system	129.534	1.95E+07	30.341
Smart NOC + Chiplet based system	145.02	1.85E+04	34.639

Cost is calculated by following equations 1 and 2.
cost=costforeachDie/Yieldforassembly (1)

Yieldforassembly=0.999Numdie∗0.999999Numg (2)

Numdie is the number of dies made from a 300 mm wafer and Numg is the number of gates on 7nm.

The simulation results indicate monolithic system cost is ~3 times higher than that of chiplet - based architecture.

5. Challenges and considerations

One of the key challenges in adopting the smart NOC - based chiplet architecture is the transitioning and training for resources in adopting the changes. It also requires the system architect and designer to carefully quorate and configure low - level access policies during the system initialization. The system also requires the trusted agent to update the access policies during runtime. The scope can be extended to include AI based security attack detection framework to run on ai security chiplet. This increases the overall attack resiliency of the system with marginal impact on latency requirement. Smart NOC - based systems need to be standardized for easy integration.

6. Conclusions

The automotive industry is facing increased demands for vehicular features and functions that, intern require high - performance compute engines and complex networking. To support current rapid market demands, chip makers are gearing towards combining readily available multiple application - specific hardware - software stacks. This hybrid environment puts more pressure on design to adopt different hardware integration, scalable, area power efficient design development and opens multiple security concerns. Chiplet - based architecture has proven to solve multiple supply chain issues and achieve high - performance and energy - efficient designs. The standardized NOC - based approach helps streamline interconnection issues with chiplet - based architecture. This work provides a state - of - the - art study of security issues with chiplet - based architecture. It provides smart NOC - based Chiplet architecture to monitor and access control the inter chiplet transactions.

References

[1] Gottscho, R A., Levine, E V., Liu, T K., McIntyre, P C., Mitra, S., Murmann, B., Rabaey, J M., Salahuddin, S., Shih, W C., & Wong, H P. (2022, January 1). Innovating at Speed and at Scale: A Next Generation Infrastructure for Accelerating Semiconductor Technologies. Cornell University. https: //doi. org/10.48550/arxiv.2204.02216

[2] Tsarchopoulos, P. (2006, May 3). Current and future research directions in embedded systems. https: //doi. org/10.1145/1128022.1128024

[3] The future of automotive compute: https: //media - publications. bcg. com/The - Future - of - Automotive - Compute. pdf

[4] Špitálová, Z. (2023). Vehicle - to - Everything Communication. *Communications - Scientific Letters of the University of Zilina*, *25* (1), C24 - 35. doi: 10.26552/com. C.2023.017

[5] Zhou, H., Xu, W., Chen, J., & Wang, W. (2020). Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities. *Proceedings of the IEEE*, 108, 308 - 323. https: //doi. org/10.1109/JPROC.2019.2961937.

[6] Kato, S., Takeuchi, E., Ishiguro, Y., Ninomiya, Y., Takeda, K., & Hamada, T. (2015). An Open Approach to Autonomous Vehicles. *IEEE Micro*, 35, 60 - 68. https: //doi. org/10.1109/MM.2015.133.

[7] Krolikowski, P., & Naggert, K. (2021). Semiconductor Shortages and Vehicle Production and Prices. *Economic Commentary (Federal Reserve Bank of Cleveland)*. https: //doi. org/10.26509/FRBC - EC - 202117.

[8] Ngo, C N., & Dang, H. (2022, July 26). Covid-19 in America: Global supply chain reconsidered. Wiley - Blackwell, 46 (1), 256 - 275. https: //doi. org/10.1111/twec.13317

[9] Putro, A S H., & Santoso, A S. (2023, June 18). Supply Chain and Digital Transformation of the Tire Manufacturing Company during the COVID - 19 Pandemic: A Case Study of PT. X. https: //doi. org/10.32388/9op4jk.2

[10] Zhan, J., & Lu, S. (2021, January 1). Influence of COVID - 19 Epidemic on China and Global Supply Chain and Policy Suggestions. Scientific Research Publishing, 09 (05), 2497 - 2512. https: //doi. org/10.4236/ojbm.2021.95136

[11] Kukkala, V K., Thiruloga, S V., & Pasricha, S. (2022, November 1). Roadmap for Cybersecurity in Autonomous Vehicles. Institute of Electrical and Electronics Engineers, 11 (6), 13 - 23. https: //doi. org/10.1109/mce.2022.3154346

[12] Jo, H J., & Choi, W. (2022, July 1). A Survey of Attacks on Controller Area Networks and Corresponding Countermeasures. Institute of Electrical and Electronics Engineers, 23 (7), 6123 - 6141. https: //doi. org/10.1109/tits.2021.3078740

[13] Ayres, N., Deka, L., & Paluszczyszyn, D. (2021, March 20). Continuous Automotive Software Updates through Container Image Layers. Multidisciplinary Digital Publishing Institute, 10 (6), 739 - 739. https: //doi. org/10.3390/electronics10060739

[14] Fleming, B. (2012, December 1). New Automotive Electronics Technologies [Automotive Electronics]. Institute of Electrical and Electronics Engineers, 7 (4), 4 - 12. https: //doi. org/10.1109/mvt.2012.2218144

[15] Kook, J. (2021, February 28). The Design, Implementation, and Demonstration of the Architecture, Service Framework, and Applications for a Connected Car. Korea Society of Internet Information, 15 (2). https: //doi. org/10.3837/tiis.2021.02.014

[16] Liang, L., Hao, Y., & Li, G Y. (2019, February 1). Toward Intelligent Vehicular Networks: A Machine Learning Framework. Institute of Electrical and Electronics Engineers, 6 (1), 124 - 135. https: //doi. org/10.1109/jiot.2018.2872122

[17] Dominguez, X., Mantilla-Perez, P., & Arboleyá, P. (2020, March 1). Toward Smart Vehicular dc Networks in the Automotive Industry: Process, computational tools, and trends in the design and simulation of vehicle electrical distribution systems. IEEE Power & Energy Society, 8 (1), 61 - 68. https: //doi. org/10.1109/mele.2019.2962890

[18] Emadi, A., & Ehsani, M. (2002, November 13). Multi - converter power electronic systems: definition and applications. https: //doi. org/10.1109/pesc.2001.954287
[19] Maalej, Y., & Balti, E. (2022, January 1). Integration of Vehicular Clouds and Autonomous Driving: Survey and Future Perspectives. Cornell University. https: //doi. org/10.48550/arxiv.2201.02893
[20] Higuchi, T., & Altintas, O. (2017, October 1). Leveraging cloud intelligence for hybrid vehicular communications. https: //doi. org/10.1109/itsc.2017.8317909
[21] Ferràs - Hernández, X., Tarrats - Pons, E., & Serrat, N A. (2017, November 1). Disruption in the automotive industry: A Cambrian moment. Elsevier BV, 60 (6), 855 - 863. https: //doi. org/10.1016/j. bushor.2017.07.011
[22] Nathan Binkert, Bradford Beckmann, Gabriel Black, Steven K. Reinhardt, Ali Saidi, Arkaprava Basu, Joel Hestness, Derek R. Hower, Tushar Krishna, Somayeh Sardashti, Rathijit Sen, Korey Sewell, Muhammad Shoaib, Nilay Vaish, Mark D. Hill, and David A. Wood.2011. The gem5 simulator. SIGARCH Comput. Archit. News 39, 2 (May 2011), 1–7. https: //doi. org/10.1145/2024716.2024718
[23] S. Li, J. H. Ahn, R. D. Strong, J. B. Brockman, D. M. Tullsen and N. P. Jouppi, "McPAT: An integrated power, area, and timing modeling framework for multicore and manycore architectures, " *2009 42nd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, New York, NY, USA, 2009, pp.469 - 480. keywords: {Timing; Multicore processing; Semiconductor device modeling; Predictive models; Costs; Out of order; Electronic design automation and methodology; Integrated circuit interconnections; Space exploration; Microarchitecture; Performance; Verification}
[24] Jeong, J., Shen, Y., Oh, T H., Céspedes, S., Benamar, N., Wetterwald, M., & Härri, J. (2021, June 1). A comprehensive survey on vehicular networks for smart roads: A focus on IP - based approaches. Elsevier BV, 29, 100334 - 100334.
[25] Dibaei, M., Zheng, X., Jiang, K., Maric, S., Abbas, R., Liu, S., Zhang, Y., Deng, Y., Wen, S., Zhang, J., Xiang, Y., & Yu, S. (2019, January 1). An Overview of Attacks and Defences on Intelligent Connected Vehicles. Cornell University. https: //doi. org/10.48550/arxiv.1907.07455