Table 4: Differences from existing location taxonomy.

Work	Count	Location taxonomy
Ours	**3** (8)	**Outside-vehicle** (Cloud platform, APP, Charging pile), **In-vehicle** (IVI, ECU, T-Box, Radio), **Network**
Pekaric et al.[5]	**3** (20)	**Physical Access** (On-board diagnostic port (OBD), ECUs, On-board computers, Modules, Media systems, Navigation system, dashboard), **Close Proximity** (Bluetooth, Key/ignition, Sensors, Tire pressure monitoring system (TPMS), Dedicated short range communication, Wi-Fi, WAVE, Voice controllable, Speech recognition system), **Remote Access** (GPS, Radio, Cellular or mobile network, Internet)
Pham et al.[8]	8	OBD, ECUs, CAN, LIDAR, Radar, GPS, Cameras, Communication mechanism
Sommer et al.[9]	**2** (28)	**Remote** (WLAN, Bluetooth, Cellular, GPS, digital video broadcasting-terrestrial (DVB-T)/digital video broadcasting-terrestrial, 2nd generation (DVB-T2), digital audio broadcasting (DAB), Radio, Tire pressure monitoring system (TPMS), Radio frequency identification (RFID), Infrared), **Internal** (USB, Auxiliary, CD, DVD, ECU, Component, OBD, CAN, CAN FD, LIN, media oriented system transport (MOST), desktop-bus (D-Bus), FlexRay, Ethernet, Camera, LiDAR, radio detection and ranging (Radar), Software)
Thing et al.[20]	7	ECUs, Sensors, GPS, Intra-vehicular links, V2V communication links, V2I communication links, V2IoT communication links
Sun et al.[21]	14	GPS, Lidar, Camera, Radar, CAN and SAE J1939 busses, Integrated business services, Machine learning systems, Password and key, Communicated data, ECUs, TPMS, Bluetooth, Key fob and keyless entry, Vehicle to everything network
Limbasiya et al.[22]	**6** (13)	**Wireless Interfaces** (DSRC, Wifi, LTE, Bluetooth), **Physical Ports** (USB, OBD-II), **Keyless Entry Systems** (Remote Key), **In-vehicle Network** (ECUs, CAN buses), **Infotainment system** (Firmware-over-the-air Update), **Perception Sensors** (Radar, LiDAR, Cameras)
Gupta et al.[23]	**3** (23)	**CLOUD** (AI-based data analysis, Device management, Microservices management, Data management, Network management), **FOG** (Software defined networking (SDN)/Time sensitive networking (TSN), Heterogeneous computing platform, Time series database, AI-based data analysis, Power management), **EDGE** (Powertrain controller, Chassis safety controller, Body electronic controller, Infotainment system, Navigation system, Internal control bus, Artificial intelligence, Onboard computer systems, Onboard diagnostics systems, Data analysis and management, Network systems, Sensors, Power management)
Niroumand et al.[24]	**2** (7)	**Automotive Control System** (ECU, CAN), **Automotive Driving System** (OBD, RADAR, Vision, LiDAR, GPS)
Bouchelaghem et al.[25]	**3** (9)	**Vehicle** (Sensors, In-vehicle network, Vehicular communications), **Environment** (Road signs, Traffic lights, Charging stations, Neighbor vehicles), **Software and mobile applications** (Firmware updates, Internet-connected features)
Luo et al.[26]	**2** (19)	**Penetration Testing** (GNSS, keyless entry, Cellular, Wifi, Bluetooth, IVI, Mobile app, Sensors, ECU, In-vehicle network, Debug interfaces, OBD), **Fuzzing** (Automotive system, SOME/IP, ECU Firmware, UDS, CAN FD, CAN, Bluetooth)
Gao et al. [16]	**3** (23)	**V2X** (Smart Phone, Passive Keyless Entry, Remote Link Type App, OTA, Bluetooth, Remote Key, DSRC-based Receiver), **In-Vehicle Systems** (USB, OBD-II, CD Player, TPMS, Charger, Airbag ECU, ADAS System ECU, Lighting System ECU (Interior & Exterior), Steering & Braking ECU, Vehicle Access System ECU, Engine & Transmission ECU), **Sensors** (Camera, GNSS/IMU, Ultrasonic Sensor, Millimeter-wave Radar, LiDAR)
Tang et al. [12]	5	Sensing, Perception, Planning, Control, End-to-end
Garcia et al. [17]	**14** (19)	**Perception** (Object Detection, Object Tracking, Data Fusion), **Localization** (Multi-Sensor Fusion, Lidar Locator), **Trajectory Prediction**, **Map**, **Planning**, **Control**, **Sensor Calibration**, **Drivers**, **CAN Bus** (Actuation, Communication, Monitor), **Robotics-MW**, **Utilities and Tools**, **Docker**, **Documentation and Others**

Table 5: Differences from existing type taxonomy.

Work	Count	Type taxonomy
Ours	**9** (31)	**Authorization** (Unauthorized accessing, Weak password, Privilege escalation, Identity spoofing), **Information leakage**, **Injection** (SQL injection, Command injection), **OS** (Kernel, Arbitrary software installation, USB, Debug interface exposure, Upgrade forgery), **DoS**, **File operation** (File accessing, File download, File tampering, File upload, File traversal, File delete), **Interception** (Relay, Replay, Man-in-the-middle, GPS spoofing, Traffic hijacking, DNS hijacking), **Web-specific** (XSS, Deserialization, Phishing, XXE), **Memory** (Buffer overflow, Integer overflow)
Pekaric et al.[5]	**21** (48)	**Content spoofing** (Message tampering, Audio attack, Replay, GPS spoofing, GPS time spoofing, Camera/Radar/LiDAR spoofing), **Identity spoofing** (Sybil attack, Falsified entities attack, Node impersonation, Repudiation attack, Key/Certificate replication), **Manipulation of human behavior** (Illusion attack), **Flooding** (Flooding attack, Routing table overflow), **Sustained client engagement** (Bus-off attack, Spamming attack), **Protocol manipulation** (TCP ACK storm), **Software integrity attack** (ECU tampering, Rogue software update, Map database poisoning), **Infrastructure manipulation** (Traffic control attack, Routing request modification, Routing cache poisoning, Black hole attack, Gray hole attack, Wormhole attack, Byzantine attack, Rushing attack), **Obstruction** (Channel interference attack, GPS jamming, Camera/Radar/LiDAR jamming, Radio signal jamming, Key fob jamming), **Traffic injection** (Message injection attack, Message fabrication attack), **Local code execution** (Malware attack), **Code inclusion** (Remote code execution), **Exploiting trust in client** (Man-in-the-middle attack), **Privilege abuse** (Man-at-the-end attack), **Exploitation of trusted credentials** (Session hijacking), **Interception** (Eavesdropping), **Reverse engineering** (Side-channel attack), **Footprinting** (ID disclosure attack, Location tracking attack, Trajectory tracking attack), **Packet fuzzing**, **Password/Key attack**, **Timing attack**
Pham et al.[8]	**3** (12)	**Interrupting operations** (LiDAR Jamming, Radar Jamming, GPS Jamming, Camera Blinding, Network Denial of Service) , **Gaining Control over CAVs** (LiDAR Spoofing, Radar Spoofing, GPS Spoofing, Adversarial Images), **Stealing information** (CAN, ECU, LiDAR)
Sommer et al.[9]	**6** (26)	**Spoofing** (Brute force, Man-in-the-middle, Hijacking, Replay), **Tampering** (XSS, SQL injection, Firmware modification, Virus, Worm, Fuzzing, Adversarial attack), **Repudiation** (Repudiation attack, Stealth attack), **Information disclosure** (Eavesdropping, Trojan, Spyware, Reverse engineering, Cryptoanalysis, Portscanning, Side-channel-attack, Fingerprinting), **Denial of service** (Distributed DoS, Jamming), **Elevation of privilege** (Buffer overflow, Rootkit, Backdoor)
Thing et al.[20]	**2** (8)	**Physical Access** (Side-channel, Code modification, Code injection, Packet sniffing, Packet fuzzing, In-vehicle spoofing), **Remote Access** (External signal spoofing, Jamming)
Sun et al.[21]	**3** (17)	**In-vehicle network attacks** (Remote sensor attacks, GPS spoofing, Location trailing, Close proximity vulnerabilities, CAN and SAE J1939 buses vulnerabilities, ECUs software flashing, Integrated business services attacks), **Vehicle to everything network attacks** (DoS, Impersonation, Replay, Routing attacks, Data falsification, Eavesdropping, Password and key attacks), **Other attacks** (Infrastructure attacks, Slight attacks, Attacks on machine learning systems)
Limbasiya et al.[22]	10	Impersonation, DoS, Sybil, Modification, Replay, Injection, Side-channel, Fuzzing, Bus-off, Remote sensor
Gupta et al.[23]	**3** (19)	**SOFTWARE** (Fake node or sybil attack, Replay, AI/ML attack, Social engineering attack, System's availability, Denial of Sleep, Malicious code, Injection), **NETWORK** (Man-in-The-Middle, Eavesdropping or sniffing, DoS, Routing attack, Gray hole, Black hole, Wormhole), **HARDWARE** (Node-capture, Side-channel attack, Timing attack, Cryptanalysis attack)
Niroumand et al.[24]	8	False Data Injection, Time Delay Switch, Denial of Service, Communication Jamming, Man in the Middle, Vehicular Ad-hoc Networks, Infotainment, Machine Learning based Attacks
Bouchelaghem et al.[25]	6	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privileges
Luo et al.[26]	17	DoS, Channel attack, Privilege escalation, Heap overflow attack, Jamming, Blinding attack, Malicious app installation, Wireless attack, Replay attack, Spoofing, Data extraction/modification, Diagnostic attack, Injection attack, Tampering, Unauthorized access, Reverse engineering, Sniffing/Eavesdropping
Gao et al. [16]	**4** (19)	**Authenticity/Identification** (Sybil, Key or Certificate Replication, GNSS Spoofing, Timing), **Availability** (DoS, DDoS, Spamming, Flooding, Wormhole, Blackhole, Malware, Jamming, Broadcast Tampering), **Data Integrity** (Masquerading, Replay, Illusion, Message Alteration), **Confidentiality** (Traffic Analysis, Eavesdropping)
Tang et al. [12]	**9** (10)	**Physical testing**, **Deliberate attack** (Jamming attack, Spoofing attack), **Optimization-based attack**, **GAN-based attack**, **Trojan attack**, **Search-based testing**, **Fault injection**, **Sampling**, **Falsification**
Garcia et al. [17]	13	Incorrect algorithm implementation, Incorrect numerical computation, Incorrect assignment, Missing condition checks, Data, Misuse of an external interface, Misuse of an internal interface, Incorrect condition logic, Concurrency, Memory, Invalid Documentation, Incorrect configuration, Other