International Journal of Advanced Scientific Research and Engineering Trends

ISSN: 2456-0774

Volume 10 Issue 8 (2026) | Pages: 19-42

An Overview of Various Frame Works on Learning Based Adaptive Cyber Security on Software Defined Embedded Systems

Sunil Kumar B S[1], Anil Kumar C[2], Harish S[3]

[1]Research Centre, Department of Electronics and communication Engineering, R L Jalappa Institute of Technology, Doddaballapur, affiliated to VTU belagavi, India

[1]Department of Electronics and communication Engineering, Akash College of Engineering, Devanahalli, affiliated to VTU belagavi, India

[2,3]Department of Electronics and communication Engineering, R L Jalappa Institute of Technology, Doddaballapur, affiliated to VTU belagavi, India.

[1]sunilkumar.aug25@gmail.com, [2]canilkumarc22@gmail.com, [3]harishsrinivasaiah@gmail.com

Peer Review Information

***Type**: Article*
***Received**: 11 May 2026*
***Revised**: 07 June 2026*
***Accepted**: 09 July 2026*
***Published**: 03 August 2026*

Abstract

Embedded communication networks sit at the centre of modern intelligent systems, from passenger vehicles and unmanned aerial vehicles to industrial controllers. The Controller Area Network (CAN) family, now in its third generation with CAN XL, carries most of this traffic, yet the protocol was designed for reliability rather than security and offers no native authentication or encryption. Remote exploits demonstrated on production vehicles have shown that this gap has direct safety consequences. This survey reviews the research that combines machine learning (ML) with software-defined networking concepts to protect these networks. We first summarise the evolution of embedded communication protocols and the properties of CAN XL that matter for security, then organise the known attacks into a taxonomy spanning the physical, protocol, and application layers. We examine why cryptographic schemes, rule-based intrusion detection, and physical fingerprinting fall short on their own, and then review learning-based intrusion detection in depth: classical classifiers, deep spatial-temporal models, graph neural networks, generative approaches, and federated learning. We also cover software-defined security architectures that turn detection results into dynamic policy enforcement, and the hardware questions that decide whether any of this can run on a real electronic control unit: FPGA integration, model compression, physical unclonable functions, and compliance with ISO 26262 and ISO/SAE 21434. The survey closes with open problems, including zero-day generalisation, adversarial robustness, benchmark standardisation, and explainability, and argues that the most promising direction is the tight integration of hardware-rooted authentication, lightweight ML detection, and software-defined response in a single closed loop.

Keywords: CAN XL; In-Vehicle Network; Intrusion Detection System; Machine Learning; Deep Learning; Software-Defined Security; Physical Unclonable Function; Embedded Systems; Automotive Cybersecurity.

How to Cite This Article

Kumar, S. B., Kumar, A. C., & Harish, S. (2026). An overview of various frame works on learning based adaptive cyber security on software defined embedded systems. *International Journal of Advanced Scientific Research and Engineering Trends, 10*(8), 19-42.

Introduction

Evolution of embedded and in-vehicle communication

A modern vehicle is no longer a mechanical product with a few supporting electronic modules; it is a distributed computing platform in which more than a hundred electronic control units (ECUs) exchange millions of messages per drive cycle. The Controller Area Network, standardised as ISO 11898 [9], has been the workhorse of this exchange since the late 1980s. Classical CAN offers a multi-master broadcast bus with bit-wise arbitration, a maximum signalling rate of 1 Mbps, and an 8-byte payload. CAN FD (2012) raised the payload to 64 bytes and the data-phase rate to 8 Mbps. CAN XL, specified by the CAN in Automation CiA 610 series, is the third generation: it supports payloads up to 2048 bytes, data rates up to 20 Mbps with new SIC XL transceivers, virtual network identifiers (VCID) that allow up to 256 logical networks on one physical segment, a service data unit type (SDT) field that permits tunnelling of higher-layer protocols including IP, and an optional link-layer security extension, CANsec [8], [36]. In parallel, vehicle electrical architectures are moving from domain controllers to zonal designs in which automotive Ethernet (10BASE-T1S and faster variants) and CAN XL coexist, with software-defined control of routing and policy. Figure 1 summarises this progression.

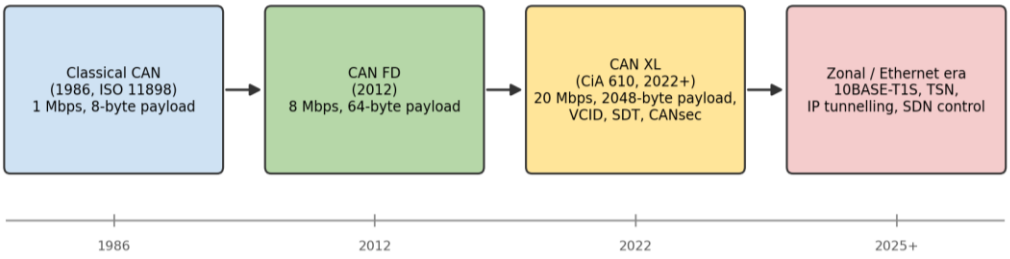

Fig. 1. *Evolution of in-vehicle communication from Classical CAN to zonal, software-defined architectures.*

Threat landscape and motivation

The security consequences of this growth became impossible to ignore after Miller and Valasek remotely compromised a production Jeep Cherokee in 2015 through its telematics unit and manipulated steering and braking over the CAN bus [1]. Earlier academic work by Koscher et al. had already shown that an attacker with bus access can control essentially every safety-critical function of a car [2], and Woo et al. demonstrated a practical wireless attack chain through a smartphone-connected diagnostic device [3]. More recent incidents, such as CAN injection thefts that exploit headlight wiring to reach the bus of a Toyota RAV4, show that the attack surface is now physical, short-range wireless, and long-range wireless at once. Vehicle-to-everything (V2X) communication, over-the-air software updates, and fleet telematics widen this surface further. Because CAN and CAN XL accept any frame with a valid identifier, a single compromised or attached node can spoof, replay, flood, or tamper with traffic that governs braking, steering, and propulsion.

Scope, contributions, and organisation

This survey covers learning-based security for embedded communication systems, with CAN XL and its software-defined integration as the anchor case. Our contributions are fourfold. First, we provide a protocol-aware background that connects the frame-level features of CAN, CAN FD, and CAN XL to the attacks they enable and the defences they permit. Second, we organise roughly forty recent works into a taxonomy of ML and deep learning intrusion detection methods, with a consolidated performance table. Third, we treat software-defined security and hardware deployment as first-class topics rather than afterthoughts, because detection accuracy means little if the model cannot run within the latency and memory budget of an ECU. Fourth, we identify open problems and sketch a reference architecture that joins hardware-rooted authentication, ML detection, and software-defined response. Section 2 gives the protocol background, Section 3 the attack taxonomy and datasets, Section 4 the limits of traditional defences, Section 5 the core review of learning-based detection, Section 6 software-defined security, Section 7 hardware and deployment, Section 8 open challenges, and Section 9 concludes.

Comparison with existing surveys

Several surveys touch parts of this space. Wu et al. [5] and Al-Jarrah et al. [6] reviewed in-vehicle intrusion detection broadly but predate CAN XL and modern transformer or graph-based models. Althunayyan et al. [4] give a thorough treatment of learning-based IDSs, including federated designs, but do not cover software-defined response or hardware roots of trust. Asaouer and Boubiche [7] focus specifically on generative AI-based IDSs. None of these consider CAN XL protocol features, PUF-based authentication, and software-defined control together. Table 1 positions the present survey against this prior work.

Table 1. *Coverage comparison with existing surveys.*

Survey	ML/DL IDS	GNN / Gen-AI	Federated	CAN XL / CANsec	SDS response	HW / PUF
Wu et al. [5], 2020	Yes	No	No	No	No	No
Al-Jarrah et al. [6], 2019	Yes	No	No	No	No	No
Althunayyan et al. [4], 2026	Yes	Partial	Yes	No	No	No
Asaouer & Boubiche [7], 2026	Partial	Gen-AI only	No	No	No	No
This survey	Yes	Yes	Yes	Yes	Yes	Yes

Background: Communication Protocols in Intelligent Embedded Systems

CAN, CAN FD, and CAN XL frame structures and security-relevant properties

Classical CAN frames carry an 11-bit (standard) or 29-bit (extended) identifier that doubles as the arbitration priority: the lower the binary value, the higher the priority. This design is elegant for real-time scheduling and disastrous for security, because any node can transmit any identifier, and receivers filter purely on that identifier with no notion of sender identity. CAN FD keeps the same trust model while enlarging the payload. CAN XL changes the frame in ways that matter for defence. The identifier is split into an 11-bit priority ID used only for arbitration and a 32-bit acceptance field used for addressing and filtering, which gives an IDS a richer and more stable addressing signal. The SDT field declares the higher-layer protocol being carried, the VCID partitions traffic into virtual networks comparable to VLANs, and the SEC bit signals extended content such as security or fragmentation headers. CANsec, modelled on MACsec (IEEE 802.1AE [12]), adds authenticated and optionally encrypted frames at layer 2 using AES-GCM; a Fraunhofer IPMS proof of concept measured about 2.7 microseconds to authenticate and encrypt a frame at 20 Mbps [36], and Wiemer and Mutter describe how the MACsec model was adapted [8]. Table 2 compares the three generations.

Table 2. *Protocol comparison across CAN generations.*

Property	Classical CAN	CAN FD	CAN XL
Max data rate	1 Mbps	8 Mbps (data phase)	20 Mbps (fast mode, PWM)
Max payload	8 bytes	64 bytes	2048 bytes
Addressing	11/29-bit identifier	11/29-bit identifier	11-bit priority ID + 32-bit acceptance field
Virtual networks	No	No	Up to 256 (VCID)
Higher-layer tunnelling	No	No	Yes (SDT, incl. IP)
Native security	None	None	Optional CANsec (AES-GCM)
Standard	ISO 11898 [9]	ISO 11898-1:2015	CiA 610 series

SOME/IP, automotive Ethernet, and gateway architectures

Above the bus layer, service-oriented middleware such as SOME/IP runs over automotive Ethernet and connects high-bandwidth domains (cameras, infotainment, ADAS compute) to the CAN-based control domains through central or zonal gateways. These gateways are natural enforcement points: they see cross-domain traffic, they have more compute than a leaf ECU, and in a software-defined architecture they can host both detection models and policy engines. They are also high-value targets, since a compromised gateway can bridge attacks from the connected domain into the safety-critical one. Surveys of in-vehicle IDS design consistently identify the gateway as the preferred deployment location for heavier models, with lightweight per-frame checks pushed to the CAN XL IP core itself [4], [5].

Why intrinsic security is absent: design trade-offs

The absence of authentication in CAN is not an oversight but a consequence of its constraints. The protocol was designed for deterministic, low-latency broadcast on microcontrollers with kilobytes of memory, over a two-wire bus shared by nodes from different vendors. Cryptographic material takes payload space that an 8-byte frame simply does not have, key management across a multi-vendor supply chain is organisationally hard, and any per-frame computation competes with control-loop deadlines measured in milliseconds. CAN XL relaxes the payload constraint and adds CANsec, but adoption will be gradual and mixed networks with legacy nodes will

persist for a decade or more. This is precisely why anomaly detection layered on top of the protocol, rather than replacement of the protocol, has become the dominant research direction.

Attack Taxonomy

Figure 2 organises the attacks reported in the literature by the layer at which they operate. The protocol-layer attacks are the ones most ML-based IDSs target, because they leave statistical traces in identifiers, payloads, and timing.

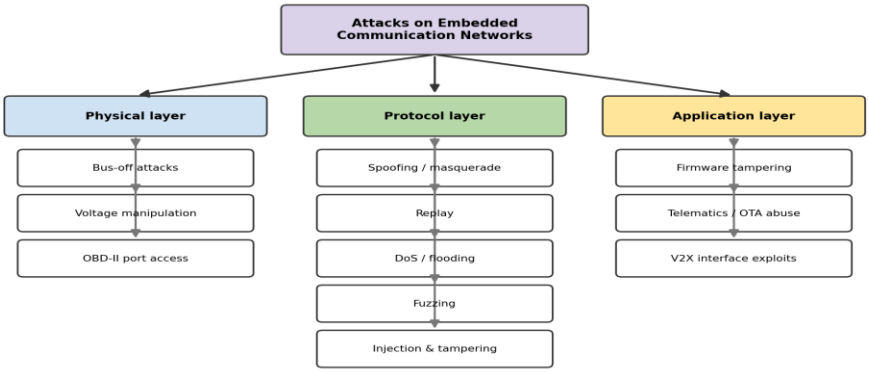

Fig. 2. *Taxonomy of attacks on embedded communication networks.*

Spoofing, replay, DoS, fuzzing, injection, and tampering

Spoofing (masquerade) attacks transmit frames with legitimate identifiers from an illegitimate source; since receivers filter only on the identifier, falsified speed or brake signals are accepted without question [2]. Replay attacks capture valid frames and retransmit them later, so every field is individually legitimate and only the timing context is wrong. Denial-of-service attacks exploit the priority arbitration itself: a node that continuously transmits the highest-priority identifier starves every other node of bus access. Fuzzing floods the bus with random identifiers and payloads, probing for exploitable receiver behaviour. Injection and tampering insert or modify frames to manipulate specific signals, for example altering a sensor reading while preserving plausible ranges. Each attack class perturbs a different subset of observable features: spoofing disturbs identifier frequency statistics, replay disturbs inter-arrival timing, DoS disturbs bus load and priority distributions, and tampering disturbs payload structure. This mapping between attack class and feature footprint is the foundation of most detection work reviewed in Section 5.

Zero-day and adaptive adversarial attacks

Signature-based systems fail by construction against attacks they have never seen. The harder problem is the adaptive adversary who knows a learning-based detector is present and shapes traffic to remain below its decision threshold, for example by replaying at frequencies inside the normal jitter band or by crafting payloads whose statistics match the training distribution. Reported detection accuracy in controlled benchmarks routinely exceeds 95%, but studies that evaluate against adaptive or previously unseen attacks report substantial drops, and adversarial perturbation of deep IDS models is a documented weakness [4]. Zero-day generalisation is therefore treated as an open problem in Section 8 rather than a solved one.

Physical-layer, protocol-layer, and application-layer threats

Physical-layer attacks include direct OBD-II access, bus-off attacks that exploit CAN error handling to silence a legitimate ECU, and voltage-level manipulation. Application-layer threats arrive through firmware update mechanisms, telematics back-ends, and V2X interfaces, and typically culminate in protocol-layer behaviour once the attacker reaches the bus. A complete defence therefore needs sensing at more than one layer: voltage or timing fingerprinting at the physical layer, statistical anomaly detection at the protocol layer, and authentication plus policy control above it. Defences confined to a single layer inherit that layer's blind spots, a point developed in Section 4.

Attack datasets and testbeds

Evaluation practice in this field leans on a small set of public datasets, summarised in Table 3. The Car-Hacking dataset (CHD) from the Hacking and Countermeasure Research Lab accompanies the GIDS work of Seo et al. [20] and contains DoS, fuzzy, gear-spoofing, and RPM-spoofing captures. The OTIDS dataset of Lee et al. was collected using remote-frame response analysis and covers fuzzy, DoS, and impersonation attacks [21]. The ROAD dataset from Oak Ridge National Laboratory was created specifically because earlier sets contained easily detectable, sometimes unrealistic injections; it provides physically verified fabrication and masquerade attacks recorded

on a dynamometer, and its accompanying guide is the most careful treatment of CAN IDS evaluation methodology to date [18]. Verma et al. note, for instance, that the vehicle in the CHD captures was stationary during attacks, which inflates the apparent separability of attack traffic [18]. No public CAN XL attack dataset exists yet; current CAN XL work, including our own, relies on CAN-generation datasets plus synthetic traffic, which is a limitation the community needs to close.

Table 3. *Public datasets used in CAN intrusion detection research.*

Dataset	Origin	Attack types	Notes
Car-Hacking (CHD)	HCRL, Korea Univ. [20]	DoS, fuzzy, gear spoof, RPM spoof	Widely used; vehicle stationary during attacks [18]
OTIDS	Lee et al. [21]	Fuzzy, DoS, impersonation	Remote-frame based collection
ROAD	ORNL, Verma et al. [18]	Fabrication, masquerade, fuzzing, accelerator	Physically verified; hardest public benchmark
Survival / others	Various	Flooding, malfunction	Smaller, vehicle-specific
CAN XL traffic	None public	—	Open gap; synthetic generation required

Traditional Security Mechanisms and Their Limitations

Cryptographic approaches and overhead analysis

Message authentication codes are the textbook answer to spoofing. AUTOSAR SecOC truncates a MAC into the payload; CANsec authenticates at layer 2 with AES-GCM [8], [36]; hardware security modules (HSMs) hold keys and accelerate the arithmetic; and dedicated crypto engines for CAN have been proposed with traceability and replay protection built in [35]. The costs are real, though. A 32-byte HMAC-SHA256 tag does not fit a classical CAN frame at all and consumes half a CAN FD frame. Key storage in non-volatile memory is a physical extraction target, key distribution across vendors remains awkward, and per-frame latency on a resource-poor ECU competes with control deadlines. Group key exchange schemes for CAN reduce the distribution problem but not the storage one [35]. Table 4 compares representative schemes; the PUF-derived approach discussed in Section 7 avoids static key storage entirely.

Table 4. *Authentication overhead of representative schemes (values as reported in the cited works).*

Scheme	Latency per frame	MAC size	Key storage	Cloning resistance
HMAC-SHA256 (software)	≈ 3.2 µs (FPGA-class)	32 bytes	NVM (static)	Low
CANsec AES-GCM [36]	≈ 2.7 µs encrypt+auth	Frame-integrated	NVM (static)	Low
HMAC + HSM	≈ 2.9 µs	32 bytes	HSM	Medium
PUF-derived HMAC (Sec. 7)	≈ 2.1 µs	16 bytes	None (dynamic)	High

Rule- and signature-based intrusion detection

Rule-based IDSs encode known attack signatures or protocol specifications. Specification-based systems such as SAIDuCANT model legitimate CAN timing and flag violations [25], and language-based approaches define grammars of acceptable message sequences. These systems are cheap, deterministic, and certifiable, which matters for ISO 26262 arguments. Their weakness is equally structural: they detect only what the rule author anticipated. Reported detection rates against novel payloads fall well below those against catalogued attacks, and rule maintenance across vehicle variants and software updates is a continuing engineering cost. In practice, rules survive as a first filter in front of learning-based stages rather than as a complete defence.

Physical fingerprinting and why it breaks under CAN FD/XL heterogeneity

Physical fingerprinting identifies the transmitting ECU from analogue characteristics. VoltageIDS showed that voltage transients distinguish transmitters well enough to catch masquerade attacks that are invisible at the frame level [24], and clock-skew methods exploit crystal oscillator differences. The trouble begins when the physical layer itself becomes heterogeneous. CAN XL mode switching changes signal amplitude between arbitration and data phases, SIC XL transceivers behave differently from classical ones, multi-vendor networks mix silicon generations, and temperature drift moves the fingerprints. Each of these erodes the stability assumption that

fingerprinting depends on. The approach remains valuable as one sensing modality among several, but it cannot anchor security for third-generation networks on its own.

Machine Learning-Based Intrusion Detection

This section is the core of the survey. Figure 3 shows the pipeline that nearly all reviewed systems share: traffic capture, pre-processing, feature extraction over identifiers, payloads, and timing, optional feature selection, a learned model, and a detection-and-response stage. The systems differ in which stage carries the intelligence.

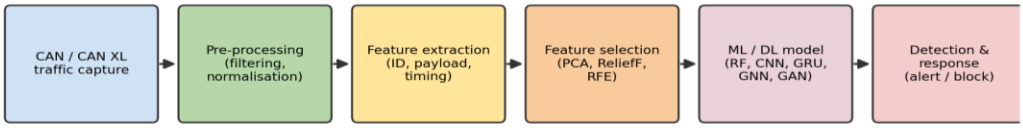

Fig. 3. *Generic pipeline of a learning-based intrusion detection system for CAN-family networks.*

Throughout the section, performance is reported with the standard metrics defined in equations (1) through (4), where TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{4}$$

Classical machine learning and feature engineering

Classical models remain competitive when paired with careful feature engineering. Random Forests and XGBoost operate on tabular vectors built from identifier frequency histograms, payload entropy and byte distributions, Hamming weights, and inter-arrival time (IAT) statistics; Isolation Forests and one-class SVMs support the normal-only training setting that real deployments often require. The LCCDE ensemble of Yang et al. combines gradient-boosted learners with per-class leader selection and reports state-of-the-art results on Internet-of-Vehicles data [37]. The strengths of this family are inference speed, small memory footprints, and interpretability through feature importances; the weakness is dependence on hand-crafted features, which an adaptive attacker can study and evade. Feature selection methods, PCA, ReliefF, and recursive feature elimination, typically cut dimensionality by 80 to 90% with negligible accuracy loss, which matters directly for embedded deployment [26].

Deep learning: CNN, recurrent, hybrid, transformer, and autoencoder models

Deep models trade interpretability for representation learning. One-dimensional CNNs treat payload bytes as sequences and learn spatial motifs; Song et al. showed early that a deep CNN over frame images detects injection attacks with high accuracy [19]. Recurrent models (LSTM, GRU, BiLSTM) capture the temporal regularity of periodic CAN traffic, which is exactly what replay and DoS attacks disturb. Hybrid spatial-temporal designs now dominate. Fu et al. propose a dual-layer LSTM-CNN that classifies at per-message granularity with latency below 3 ms and F1-scores of 96 to 98% [17], and Jo and Kim show that an aggressively pruned temporal-spatial fusion model gives up only 1 to 3% F1 while cutting model size by 30 to 40% [16]. Transformer-based systems push further on context: CAN-BiGRUBERT combines BERT-style intra-frame encoding with BiGRU inter-frame modelling and reaches 94 to 98% accuracy with strong replay detection and driving-state discrimination above 97% [13]. Autoencoder systems such as CANet learn to reconstruct normal high-dimensional traffic and flag reconstruction error, giving genuine unsupervised operation [22].

Graph neural network approaches

Graph methods model the network structure that sequence models ignore. Islam et al. built graph-based detection over CAN message relationships [23]. Du et al.'s UGL combines a GCN over the UAV's ECU topology with an LSTM over frame sequences, reporting 96 to 98% accuracy and a 10 to 15% F1 improvement over LSTM-only baselines in UAV CAN settings [14]. RAG-HIDS by Lin et al. goes further with a multi-relational graph, edges encode message type, timing, and payload similarity simultaneously, and hierarchical scoring

at both message and window level; it reports over 99.6% message-level accuracy on the Car-Hacking dataset at about 5 to 6 ms per frame [15]. The graph family is currently the accuracy frontier, and its main open question is inference cost on embedded targets.

Generative AI: GANs and VAEs

Generative models serve two distinct roles. As data augmenters, GANs synthesise realistic attack traffic to balance the severely skewed class distributions of CAN datasets; GIDS was an early demonstration of GAN-based detection on in-vehicle traffic [20]. As anomaly scorers, VAEs and GAN discriminators provide reconstruction-error or confidence-based distances from the learned normal manifold, which extends detection toward unseen attacks. The survey of Asaouer and Boubiche reports generative configurations reaching 96 to 98% F1 on known attacks and, more interestingly, 90 to 94% on unknown ones, at the price of 20 to 40% higher training complexity and memory [7]. Lightweight on-board variants of these models are an active gap.

Federated and distributed learning

Federated learning (FL) trains detectors across vehicles without centralising raw traffic, which addresses both privacy and the practical impossibility of shipping full CAN logs to the cloud. Althunayyan et al. catalogue FL-based IDS designs that hold 93 to 96% F1 while cutting uplink bandwidth by 40 to 60% relative to centralised training [4]. Zhou et al.'s adaptive segmentation approach tackles the straggler and heterogeneity problems of asynchronous FL in transportation systems [30], and Chandrasekaran et al. apply FL across decentralised network slices with a layered ecosystem design [31]. Reinforcement-learning-driven coordination in UAV-aided vehicular networks [32] suggests how mobile relays could participate in distributed defence. The recurring trade-off is communication rounds versus convergence quality, plus a new attack surface: poisoned model updates.

Consolidated performance comparison

Table 5 consolidates the reviewed detection systems. Direct numerical comparison should be read cautiously: datasets, train-test splits, and metrics differ across papers, a problem the ROAD authors document in detail [18].

Table 5. *Comparative summary of learning-based intrusion detection systems.*

Work	Model	Dataset	Reported results	Notes
Sharmin et al. [13]	BERT + BiGRU	Realistic CAN traces	94–98% acc.	Strong replay detection; driving-state aware
Du et al. (UGL) [14]	GCN + LSTM	UAV CAN	96–98% acc.	+10–15% F1 vs LSTM-only
Lin et al. (RAG-HIDS) [15]	Multi-relational GNN	Car-Hacking	>99.6% acc., F1 >99%	5–6 ms/frame
Jo & Kim [16]	Light CNN + GRU fusion	CAN benchmarks	96–98% F1	30–40% smaller model
Fu et al. [17]	Dual-layer LSTM-CNN	CAN benchmarks	>97% acc., 96–98% F1	Per-message, <3 ms
Seo et al. (GIDS) [20]	GAN	CHD	≈98% acc.	Introduced CHD dataset
Hanselmann et al. (CANet) [22]	Autoencoder + LSTM	Synthetic + real	High AUC	Unsupervised, signal-level
Islam et al. [23]	Graph-based	CHD, others	≈99% (four attacks)	Early GNN direction
Song et al. [19]	Deep CNN	CHD	>99% (known attacks)	Frame-image encoding
Yang et al. (LCCDE) [37]	Boosted ensemble	IoV data	≈99.8% F1	Per-class leader models
PUF-CNN-GRU (this group)	PUF auth + CNN-GRU + SDM	CHD, OTIDS	99.95% / 99.78% F1	Auth + detection + adaptive response

Software-Defined Security for Embedded Networks

Architecture: physical, control, and application layers

Software-defined security (SDS) lifts security functions out of fixed hardware into a programmable control layer, mirroring the SDN split between data and control planes. Figure 4 shows the standard three-layer view: a physical layer of switches, gateways, ECUs, and

programmable data planes; a control layer hosting abstracted functions such as firewalling, IDS/IPS, and trust-zone assignment; and an application layer of policy managers and analytics. The properties that make this attractive for vehicles are policy portability across hardware, automated trust-zone assignment, on-demand scaling of enforcement, and a single point of visibility across domains.

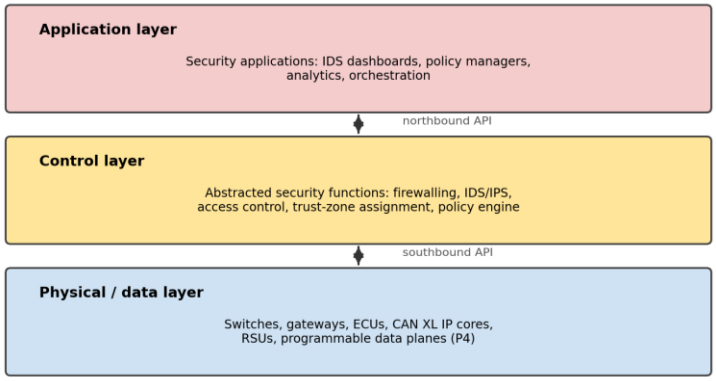

Fig. 4. Three-layer software-defined security architecture.

Dynamic policy enforcement, controller placement, and failure resilience

Centralising control creates a new dependability question: what happens when the controller fails or becomes unreachable. Dou et al. study exactly this for software-defined WANs and show that jointly optimising controller-to-switch mapping and flow paths keeps end-to-end delay growth to 10–15% under single-controller failure, against 30–40% for naive failover, while holding packet loss for critical classes under about 2% [28]. Vega et al. demonstrate the complementary data-plane direction: a P4-programmable switch feeding a lightweight ML rate controller improves flow completion time by roughly 21.7% without touching end hosts [27]. Both results transfer conceptually to vehicles, where the 'controller' may be a zonal gateway and the 'switch' a CAN XL IP core with programmable filters.

SDN-assisted vehicular networks

Marwein et al. propose a hierarchical design for heterogeneous vehicular networks: a central SDN controller performs coarse load distribution while local controllers at roadside units make latency-aware scheduling decisions. The hierarchy improves handover served ratio by 15–20%, cuts average delay by 20–30%, and reduces dropped handovers by 25–35% under high mobility [29]. For security, the same hierarchy is a natural fit: global policy and model updates flow down from the central controller, while per-zone enforcement and fast local response stay at the edge.

Closing the loop: ML detection driving software-defined response

The pieces above become a security system when detection output drives enforcement. In the framework developed by our group, the anomaly score from a CNN-GRU detector feeds a software-defined decision module that selects among Allow, Monitor, and Block through SoftMax probability estimation, applies the action directly to the CAN XL IP core filtering rules, and refines its own threshold with an exponential moving average of recent scores, as in equation (5):

$$Tht + 1 = \alpha \cdot \hat{y}t + (1 - \alpha) \cdot Tht \qquad (5)$$

where ŷ is the current anomaly score and α the adaptation rate. An ablation on the Car-Hacking dataset shows the adaptive threshold alone is worth 2.75 accuracy points, which supports the broader claim of this section: static thresholds and static rules leave measurable performance on the table in non-stationary traffic. Comparable block/monitor/allow loops appear across the SDS literature, and we expect them to become the standard interface between learned detectors and network enforcement.

Hardware and Deployment Considerations

FPGA and IP-core integration, TinyML, and model compression

A detector that cannot meet the bus deadline is not a detector. CAN XL IP cores occupy on the order of a few thousand LUTs on mid-range FPGAs and expose the frame stream with nanosecond timestamps, which makes them the right attachment point for hardware-accelerated pre-processing. On the model side, quantisation to 8-bit weights, pruning, and knowledge distillation reduce inference latency by 20–40% and memory footprint by 30–60% while keeping more than 97% of original accuracy in reviewed IDS deployments [26]. TinyML-class models under 500 KB running at ten thousand frames per second are demonstrably feasible, and the lightweight fusion results of Jo and Kim [16] show the accuracy cost of aggressive slimming is small.

Resource consumption trade-offs

Hoque et al. provide the most systematic accounting of what ML security actually costs: deep-learning IDSs can consume 30–70% more CPU cycles and two to four times the memory of signature-based detectors, edge inference spends 10–25% more energy per packet than cloud inference but saves 15–30 ms of transport latency, and, strikingly, data labelling and model tuning absorb 40–60% of total deployment effort [26]. Their conclusion applies to everything in this survey: accuracy claims are meaningful only alongside standardised energy, latency, and memory figures, which the field does not yet report consistently.

Hardware roots of trust: PUFs and key management without static storage

Physical unclonable functions derive device-unique responses from manufacturing variation, so no key ever sits in non-volatile memory waiting to be extracted. PUF circuits with reduced temperature sensitivity have been implemented on FPGA and integrated into CAN prototypes for ECU authentication, and PUF-based authentication and key agreement is a mature research area across IoT and vehicular settings [33], [34]. The practical recipe, used in our group's framework, is: generate the PUF response, stabilise it with error-correcting codes against voltage and temperature drift, derive a session key by hashing the corrected response together with the firmware hash (binding hardware identity to software integrity), and authenticate each frame with a truncated 128-bit HMAC. Measured on a Kintex-7, this runs at 2.10 µs per frame, about 34% faster than standard HMAC-SHA256, with the 16-byte tag still clearing the ISO/SAE 21434 minimum of 96 bits.

Real-time and standards compliance: ISO 26262 and ISO/SAE 21434

ISO 26262 [11] governs functional safety and imposes the ASIL-graded latency and determinism budgets that any in-line security function must respect; a detector that delays a braking frame past its deadline is itself a safety hazard. ISO/SAE 21434 [10] governs cybersecurity engineering across the vehicle lifecycle and pushes requirements upstream into risk analysis, monitoring, and incident response, which is where the logging, alerting, and adaptive-policy components of an SDS loop earn their place. Certification of learned components remains genuinely unsolved: current practice keeps the ML stage advisory or pairs it with a certifiable rule-based envelope, and explainability (Section 8.3) is the research thread most likely to change that.

Review on Existing System

This section presents a comprehensive review of recent research on intelligent intrusion detection and network security for automotive, UAV, and software-defined communication systems. It examines advanced Machine Learning, Deep Learning, Graph Neural Networks, Transformer-based models, Generative AI, and SDN-enabled architectures developed to improve cybersecurity, anomaly detection, and resource efficiency. The review highlights existing methodologies, performance achievements, limitations, and research gaps, providing a strong foundation for the proposed research framework.

Shaila Sharmin et al. [38] propose CAN-BiGRUBERT, a novel Controller Area Network (CAN)-based intrusion-detection system that models normal in-vehicle communication behavior and flags intrusions by spotting subtle anomalies in message sequences. The method combines a CAN-specific message-preprocessing pipeline with a hybrid deep-learning architecture that leverages Bidirectional Encoder Representations from Transformers (BERT) for intra-frame semantic modeling and Bidirectional Gated Recurrent Units (BiGRU) for temporal modeling of CAN traffic across windows of frames. This architecture treats the CAN bus as a sequence of tokenized frames, where each frame’s identifier (CAN ID), payload bytes, and timing features are encoded into a structured vector representation; BERT-like layers then learn contextual embeddings of these tokens to capture dependencies between fields inside a single frame, while BiGRU layers model the temporal evolution of such embeddings over sliding time windows to capture normal driving-state patterns. To detect attacks, the model computes a deviation score between the reconstructed or predicted representation and the observed CAN pattern; if this score exceeds a learned threshold, the system raises an alert, making it an anomaly-based intrusion-detection system rather than one relying solely on signature-matching.

Ying Du et al. [39] propose UGL, a comprehensive hybrid model that integrates Graph Convolutional Networks (GCN) and Long Short-Term Memory (LSTM) networks to improve intrusion detection in Unmanned Aerial Vehicle (UAV) Controller Area Network (CAN) systems. The methodology starts by modeling the UAV’s internal electronic components as a graph, where nodes represent ECUs or communication endpoints and edges encode logical or physical connectivity and message-flow patterns; the GCN layer then learns structural and spatial relationships among these nodes over the CAN topology, capturing how anomalies propagate across the network rather than treating each node in isolation. CAN traffic is preprocessed into sequences of frames (CAN IDs, payloads, and timing features), and these sequences are fed into an LSTM backbone that learns temporal dependencies across sliding time windows, thus enabling the model to detect subtle, long-lasting attack behaviors such as replay, injection, or fuzzing attacks that deviate from normal flight-phase patterns. The final UGL architecture fuses GCN-derived node embeddings with LSTM-derived temporal representations,

typically via concatenation or attention-based combination, and applies a classifier head to decide whether each time window of CAN traffic is benign or malicious.

In their experiments on UAV CAN datasets, Du et al. report detection performance around 96–98% accuracy with similarly strong precision (≈95–97%) and recall (≈94–96%), demonstrating that the GCN–LSTM hybrid outperforms baseline single-layer LSTM or standalone GCN models while maintaining acceptable computational latency for real-time UAV monitoring. The model significantly reduces false-alarm rates compared with purely feature-based or rule-driven IDS, with the combined graph-temporal representation achieving roughly a 10–15% improvement in intrusion-detection F1-score over traditional LSTM-only baselines on the same UAV-CAN setup. The novelty of UGL lies in its protocol-aware but feature-lean integration of GCN and LSTM: by exploiting both the logical topology of the UAV's CAN and the time-series nature of frame sequences, the approach achieves enhanced robustness against low-information-density CAN traffic and resource-constrained UAV environments, making it a promising solution for securing cyber-physical control channels in autonomous.

Christian Vega et al [40]. introduce a Machine Learning Controller (MLC) that uses a programmable P4-based data-plane switch to dynamically manage data rates in Science DMZ networks, which are typically used for high-throughput scientific data transfers. The method relies on passive data-plane measurements such as Round Trip Time (RTT), throughput, queuing delay, and active flow count at the campus-network edge; these telemetry signals are collected by the P4 switch and fed into a light-weight ML controller that adjusts the output rate of the Data Transfer Node (DTN) toward a user-defined target rate without modifying end-host congestion-control algorithms. The controller operates as a closed-loop rate-management system: it observes current network conditions, predicts the impact of different sending-rate decisions, and then updates the DTN rate so that bottleneck-link utilization and queuing stay within safe bounds while maximizing throughput for big-data flows.

In a testbed combining a bare-metal P4 switch, a legacy router, and emulated hosts, the authors show that this MLC-based rate controller improves Flow Completion Time (FCT) by about 21.7% on average compared with a trivial fixed-rate baseline when the DTN runs BBR2 (a modern congestion-control algorithm). The proposed scheme achieves this performance gain while keeping the impact on background campus traffic low, with only a small increase in bottleneck-link utilization and no significant disruption to non-scientific traffic. The novelty lies in tightly coupling edge-device programmability (P4) with an ML-based rate controller, enabling fine-grained, adaptive control in non-dedicated Science DMZs where DTNs share links with general campus traffic; the paper demonstrates that such a hybrid approach can effectively optimize scientific-data transfers without requiring full-dedicated infrastructure or host-stack modifications.

Muzun Althunayyan et al. [41] present a comprehensive survey of learning-based intrusion detection systems (IDSs) for in-vehicle networks, focusing on Machine Learning (ML), Deep Learning (DL), and Federated Learning (FL) approaches. The paper organizes existing research into a taxonomy that distinguishes between supervised, unsupervised, and semi-supervised learning-based IDSs and categorizes them by network type (CAN, SOME/IP, Ethernet-based in-vehicle networks) and attack type (e.g., replay, spoofing, flooding, unknown anomalies). The survey systematically reviews preprocessing techniques such as CAN-ID padding, payload encoding, time-domain feature extraction, and graph-based feature engineering, then maps how each learning paradigm is applied: classical ML models (Random Forest, SVM, XGBoost) for feature-rich, tabular representations, and DL models (Autoencoders, CNNs, LSTMs, Transformers, and GCN-based architectures) for raw or high-dimensional message sequences. The authors also cover emerging FL-based IDS designs, which aim to train detectors collaboratively across vehicles without centralizing sensitive CAN data, and discuss how these schemes balance privacy, communication overhead, and detection accuracy.

Md Muzammal Hoque et al. [42] present a systematic investigation of the resource consumption of Machine Learning (ML) in communications-network security, focusing on how ML-based security solutions impact energy, computing, memory, latency, bandwidth, and human-effort metrics. The core methodology is a comprehensive literature review combined with a proposed taxonomy that classifies ML-based security techniques by resource-consumption dimension (e.g., computation-heavy vs. memory-constrained vs. bandwidth-hungry) and by deployment scenario (edge, core networks, 5G/6G, IoT, and cloud-based security analytics). The authors analyze over 100 studies covering intrusion-detection systems (IDS), anomaly detectors, and privacy-preserving ML such as Federated Learning (FL) and Split Learning (SL), and extract per-model estimates for key resources; for example, they report that many deep-learning IDSs can consume 30–70% more CPU cycles and 2–4× more memory than traditional signature-based detectors, while FL-based network-security designs can reduce uplink bandwidth by 40–60% at the cost of 10–20% higher end-to-end latency compared with centralized training. The paper also introduces a conceptual framework to quantify the trade-off between ML-model accuracy and resource overhead, highlighting that in some 6G-oriented security studies accuracy drops by only 1–3% when lightweight models are used, but energy and memory consumption can be cut by roughly 35–50%.

Althunayyan et al., [43] presented a comprehensive survey on learning-based Intrusion Detection Systems designed for securing in-vehicle networks, particularly the Controller Area Network bus used in Connected and Autonomous Vehicles. The survey highlights that the CAN protocol lacks built-in security mechanisms such as authentication and encryption, making it vulnerable to attacks including message injection, spoofing, replay, and denial-of-service. The authors systematically review state-of-the-art IDS approaches based on Machine Learning, Deep Learning, and Federated Learning**,** classifying them according to their ability to detect known attacks, unknown attacks, and hybrid attack scenarios**.** The survey further examines commonly used benchmark datasets, feature engineering techniques, evaluation metrics, and deployment considerations for real-time automotive environments. Special emphasis is given to FL-based IDSs, which enable collaborative model training while preserving vehicle data privacy, though challenges such as communication overhead, heterogeneous data, and scalability remain. The survey also compares supervised, unsupervised, and hybrid learning methods, identifying their strengths and limitations with respect to detection accuracy, computational complexity, latency, and real-world applicability. The authors conclude that future IDSs should focus on lightweight architectures, robust zero-day attack detection, privacy-preserving federated learning, standardized evaluation methodologies, and real-time deployment to ensure secure and resilient in-vehicle communication systems for next-generation connected vehicles.

Songshi Dou et al. [44] study how controller failures affect Quality-of-Service robustness in Software-Defined Wide Area Networks and propose mechanisms to mitigate their impact on traffic forwarding and service-level guarantees. The core methodology is based on a multi-controller SD-WAN architecture where the control plane is logically centralized but physically distributed across multiple controller instances deployed at different sites; the authors analyze failure scenarios in which one or more controllers become unreachable and quantify how this degrades QoS metrics such as end-to-end delay, packet loss, and throughput for QoS-sensitive applications. Their approach builds on earlier work such as “Matchmaker”, which introduced an adaptive, heuristic-based recovery mechanism that reassigns “offline” flows to new controllers and recomputes paths under multiple controller failures; in this paper, they extend that idea to explicitly target QoS robustness by jointly optimizing controller-to-switch mappings and flow-path selection under failure conditions, while respecting controller capacity and latency constraints. The novelty lies in formulating the problem as a constrained optimization that balances controller load, link utilization, and per-path QoS bounds, rather than relying solely on simple failover or static backup mappings.

Phibadeity S. Marwein et al. [45] propose a hierarchical-controller architecture for efficient load distribution in heterogeneous vehicular networks, where vehicles connect through multiple radio access technologies (e.g., DSRC, LTE-V, 5G-NR) and edge/fog nodes support varying compute and bandwidth capacities. The methodology is built on a Software-Defined Networking (SDN)-enabled vehicular architecture that splits the control plane into two tiers: a central SDN controller (MSDNC) located in the cloud or core and multiple local Software-Defined Network Controllers (LSDNCs) deployed at Road-Side Units (RSUs) in the fog tier. The central controller maintains a global view of the network and performs coarse load-balancing decisions, while LSDNCs attached to RSUs execute fine-grained, latency-aware load-scheduling for nearby On-Board Units (OBUs), taking into account RSU capacity, OBU demand, and current radio-link conditions. The novelty lies in the integration of SDN-based controller-assisted load-balancing with RSU-fog-tier coordination: the MSDNC uses a heuristic-based load-distribution strategy to assign OBUs to available RSUs, and LSDNCs then apply a priority-aware scheduling policy that favors vehicles with limited RSU access or high-urgency requests, reducing local congestion and handover-related service disruption.

Hyunjun Jo et al. [46] propose a lightweight temporal-and-spatial fusion model for intrusion detection in automotive Controller Area Network buses, targeting the need for accurate attack detection under limited on-board ECU resources. The methodology starts from CAN-message sequences, where each message is represented in a structured way that encodes both the spatial pattern (e.g., CAN ID and payload bytes) and the temporal order of frames; the authors design a compact neural architecture that fuses these two aspects via a small-scale Convolutional Neural Network for local spatial feature extraction and a lightweight recurrent module (such as a reduced LSTM or GRU) for temporal-sequence modeling. The key novelty lies in the “lightweight” design choices: the model uses fewer convolutional filters, reduced hidden-state dimensions in the recurrent layer, and carefully constrained depth to keep parameter count and inference latency low, while still preserving the ability to capture subtle anomalies such as replay, spoofing, and fuzzing attacks. The feature-fusion mechanism aggregates CNN-extracted spatial embeddings and recurrent-derived temporal embeddings into a joint representation, which is then classified by a final fully-connected layer into benign or malicious traffic with per-message or per-frame granularity.

Guettouche Asaouer et al. [47] survey Generative AI-based Intrusion Detection Systems for intra-vehicle networks, with a focus on how Generative Adversarial Networks, Variational Autoencoders, and related generative models can improve anomaly and intrusion detection in automotive CAN-style buses. The paper’s methodology is primarily a structured review and classification of existing and emerging generative-AI-based IDS designs, organizing them along axes such as detection paradigm (supervised vs. unsupervised), use of normal-only training, and the role of generative models (data augmentation, anomaly scoring, or adversarial training). The authors argue

that generative models are particularly suited to intra-vehicle networks because they can learn complex, high-dimensional CAN-message distributions from limited labeled data and then flag traffic that lies far from the learned "normal" manifold, thereby detecting unknown or zero-day attacks without relying on signature databases. The novelty highlighted in the survey includes schemes where GANs or VAEs are used both to synthesize realistic attack traffic for training and to derive distance-based anomaly scores (e.g., reconstruction error or discriminator confidence) that drive the detection logic, often integrated with lightweight classifiers or rule modules for deployment on resource-constrained ECUs. Overall, the paper positions generative-AI-based IDSs as a promising direction for intra-vehicle security, stressing the need for lightweight, on-board-friendly variants of GANs/VAEs, standardized evaluation metrics, and better integration of generative-IDS components into automotive-specific standards such as ISO/SAE 21434.

Yu Fu et al. [48] propose a dual-layer LSTM-CNN framework for real-time and precise per-message intrusion detection in in-vehicle networks, targeting the need to detect anomalies at the granularity of individual CAN frames while satisfying low-latency constraints on embedded ECUs. The methodology uses a stacked CNN-LSTM architecture: a compact CNN layer first extracts local spatial features from each CAN message (e.g., CAN ID and payload bytes) by treating them as a 1-D sequence of symbols or bytes, and then an LSTM layer processes the sequence of CNN-encoded messages over time to capture temporal dependencies and normal communication patterns. The "dual-layer" design refers both to the CNN-for-spatial and LSTM-for-temporal separation and to the model's operation at the per-message level: instead of aggregating traffic into windows and then classifying windows, the framework produces a per-frame anomaly or class label, enabling fast reaction to attacks. The novelty emphasized in the paper is the lightweight, single-message-oriented CNN-LSTM structure, combined with careful hyperparameter tuning (layer depth, hidden-unit count, and batch-size) that keeps inference latency below a few milliseconds per frame, making it suitable for real-time deployment without relying on external cloud resources.

Hai Lin et al. [49] propose RAG-HIDS, a multi-relational graph-based hierarchical intrusion detection system for in-vehicle networks that models the CAN-bus and higher-layer communication as a dynamic multi-relational graph and performs tiered anomaly detection. The methodology starts by constructing a graph where nodes represent ECUs, message IDs, or communication endpoints, and edges encode different "relations" such as message-type, time-interval patterns, and payload-distance similarities; this multi-relational structure is then fed into a hierarchical graph-neural-network backbone that operates at both message-level and window-level granularities. The "hierarchical" aspect means that RAG-HIDS first computes local anomaly scores per CAN frame using relational graph embeddings, then aggregates these scores over sliding time windows to perform global-behavior-level detection, balancing per-message responsiveness with stable, sequence-aware judgements. The novelty of RAG-HIDS lies in this explicit use of multiple edge types (time, message type, payload similarity, etc.) within a single GNN framework, enabling the model to capture not only which nodes are active but also *how* they interact under normal and attack-induced traffic, which is particularly useful for subtle attacks such as low-rate replay or semantic-level injection.

The reviewed studies demonstrate that hybrid AI-based intrusion detection models significantly improve detection accuracy, precision, and recall while reducing false alarms across intelligent communication networks. Techniques such as CNN, LSTM, Transformers, GCN, GAN, Federated Learning, and SDN-based optimization enhance security, scalability, and real-time performance. However, challenges remain in zero-day attack detection, resource optimization, explainability, cross-dataset generalization, and deployment on resource-constrained embedded automotive systems.

Chandrasekaran et al., [50] proposed Enhancing Predictability in Decentralized Network Slices Through Federated Learning, a multi-layered federated learning ecosystem designed to improve resource prediction and management in decentralized network slicing environments for next-generation communication networks. The methodology integrates Federated Learning across multiple network layers, including edge devices, edge servers, and cloud infrastructure, enabling collaborative model training without sharing sensitive user data. The proposed architecture consists of decentralized edge nodes that locally train predictive models using network traffic and resource utilization data, while a global aggregation mechanism combines local model updates to generate an optimized global model. Technically, the framework employs distributed machine learning, hierarchical federated aggregation, edge computing, network slicing orchestration, and predictive resource allocation to improve network efficiency while preserving data privacy. The system continuously predicts traffic demands and dynamically allocates network resources to different slices, thereby minimizing congestion and improving Quality of Service (QoS).

Zhou et al., [51] proposed an Adaptive Segmentation Enhanced Asynchronous Federated Learning framework to improve learning efficiency and communication performance in sustainable intelligent transportation systems. The methodology introduces an adaptive data segmentation mechanism that partitions local datasets according to their characteristics before model training, allowing participating edge devices to train more effectively despite heterogeneous data distributions. Unlike conventional synchronous federated learning, the proposed asynchronous learning strategy enables edge devices to upload model updates independently without waiting for all participants, thereby reducing idle time and accelerating model convergence. Technically, the framework integrates adaptive data segmentation, asynchronous model aggregation, distributed optimization, edge computing, and intelligent transportation network

management to enhance learning performance while preserving user privacy since raw data remain on local devices. The adaptive segmentation mechanism minimizes the adverse effects of non-independent and identically distributed data, while asynchronous aggregation reduces communication latency and improves scalability across distributed transportation networks. Experimental evaluation demonstrates that the proposed framework achieves higher prediction accuracy, faster convergence, lower communication overhead, and improved resource utilization compared with conventional federated learning approaches. The results further show enhanced robustness under heterogeneous network conditions and dynamic traffic environments, making the proposed framework suitable for large-scale intelligent transportation applications that require efficient, privacy-preserving, and sustainable distributed learning.

Chen et al., [52] proposed a deep reinforcement learning-based trajectory planning framework to enhance routing performance in unmanned aerial vehicle-aided vehicular ad hoc networks. The methodology utilizes unmanned aerial vehicles as mobile relay nodes to support communication between vehicles in highly dynamic traffic environments. A deep reinforcement learning agent continuously learns the optimal flight trajectory by observing network conditions, vehicle mobility, and communication quality, enabling the unmanned aerial vehicles to dynamically adjust their positions for improved network connectivity. Technically, the framework integrates deep reinforcement learning, trajectory optimization, vehicular ad hoc networks, unmanned aerial vehicle-assisted communication, and dynamic routing optimization to maximize routing efficiency while minimizing communication delays. The learning model considers multiple network parameters, including link quality, transmission delay, packet delivery ratio, and vehicle movement, to determine the most suitable trajectory and routing decisions.

Li et al. [53] proposed QuanReS, a hybrid framework for resilient and secure vehicle-to-everything communications in smart cities by integrating quantum-enabled security with conventional communication technologies. The methodology combines quantum communication principles and resilient network mechanisms to address the growing cybersecurity challenges in intelligent transportation systems, such as eavesdropping, spoofing, and cyberattacks. The framework employs quantum-based key generation and secure authentication mechanisms alongside intelligent communication protocols to establish reliable and protected data exchange between connected vehicles, roadside infrastructure, pedestrians, and cloud services. Technically, the framework integrates quantum key distribution, secure authentication, resilient communication protocols, vehicle-to-everything communication, and intelligent transportation networking to enhance communication security while maintaining low latency and high reliability.The results further indicate reduced vulnerability to cyberattacks, improved communication stability, and efficient secure data transmission, making QuanReS a promising framework for future smart city transportation systems requiring robust, intelligent, and quantum-enabled secure communications.

Tang et al.,[54] proposed a resilient communication framework that integrates quantum-secured communication with software-defined networking to improve the cybersecurity and reliability of smart microgrids. The methodology combines Software-Defined Networking with Quantum Key Distribution to provide centralized network control, dynamic traffic management, and quantum-safe encryption. The architecture consists of a control plane and a data plane, where the Software-Defined Networking controller continuously monitors network conditions, detects communication failures, and reroutes traffic through alternative paths whenever faults or cyberattacks occur.. Technical validation was performed using Mininet and the Ryu controller to emulate software-defined communication networks, while network recovery and latency were evaluated under multiple link-failure scenarios. Experimental results showed that the proposed framework rapidly restored disrupted communication paths, maintained secure key distribution, minimized recovery delay, and significantly improved network availability compared with conventional communication architectures. The integration of centralized network intelligence with quantum-secure encryption demonstrates an effective solution for ensuring secure, resilient, and scalable communication in future smart microgrid infrastructures.

Janabi et al., [55] presented a comprehensive survey on Intrusion Detection Systems for Software-Defined Networking by analyzing existing security mechanisms, machine learning techniques, deep learning models, datasets, and attack detection approaches used in modern programmable networks. The methodology involved a systematic review of recent research on Software-Defined Networking security, with emphasis on vulnerabilities introduced by the separation of the control plane and data plane. The study examined various cyberattacks, including Distributed Denial of Service, Denial of Service, Probe, SQL Injection, and controller-targeted attacks, and evaluated the effectiveness of different intrusion detection approaches. Technical aspects discussed include machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine, Naïve Bayes, and K-Nearest Neighbor, along with deep learning models including Convolutional Neural Networks, Recurrent Neural Networks, Long Short-Term Memory, Autoencoders, and Gated Recurrent Units. The paper also compares widely used benchmark datasets such as NSL-KDD, CICIDS2017, CICIDS2018, UNSW-NB15, CSE-CIC-IDS2018, and InSDN for training and evaluating intrusion detection models. The survey highlights current research challenges, including real-time traffic analysis, scalability, controller overload, dataset imbalance, and high computational complexity. The authors conclude that integrating advanced artificial intelligence techniques with Software-Defined Networking can significantly

improve intrusion detection accuracy, reduce false alarms, enhance network resilience, and provide adaptive protection against evolving cyber threats, while identifying future research directions for intelligent and sustainable network security.

Mehic et al., [56] proposed a secure key management framework for Software-Defined Quantum Key Distribution networks to mitigate Denial-of-Service attacks targeting the Key Management System. The methodology focuses on preventing malicious applications from exhausting cryptographic key resources by introducing intelligent key allocation, priority-based request handling, and adaptive resource management.. The proposed mechanism was evaluated using the Quantum Key Distribution Network Simulation Model based on the NS-3 simulator with multiple legitimate and malicious applications under varying attack intensities. Simulation results demonstrated that the framework successfully prevented key exhaustion by dynamically controlling key allocation, maintained nearly constant key availability for legitimate users even during severe Denial-of-Service attacks, and improved network resilience without significantly degrading communication performance. The proposed Software-Defined Networking-based key management strategy effectively enhances the security, availability, and reliability of future quantum communication networks by resisting resource depletion attacks while maintaining continuous secure services.

Qaisar et al., [57] proposed R2Com, a reliable and resilient communication protocol for duty-cycled Software-Defined Wireless Sensor Networks to improve urban traffic monitoring in Intelligent Transportation Systems. The methodology integrates centralized Software-Defined Networking control with trust-aware routing and adaptive duty cycling to ensure reliable, energy-efficient, and low-latency communication among wireless sensor nodes. The proposed protocol was evaluated through extensive simulations and compared with existing routing protocols under different network conditions. Performance analysis considered average energy consumption, packet delivery ratio, packet success ratio, communication overhead, network lifetime, average latency, routing reliability, and throughput. Experimental results demonstrated that R2Com significantly reduced energy consumption and communication overhead while achieving higher packet delivery rates, lower latency, improved routing reliability, and longer network lifetime than conventional approaches. The study concludes that combining trust-based routing with centralized Software-Defined Networking management provides a scalable, resilient, and efficient communication framework for next-generation intelligent transportation systems and smart city traffic monitoring applications.

Chatzimilitis et al., [58] proposed a collaborative intrusion detection framework for Software-Defined Smart Grid networks that enhances cybersecurity while preserving data privacy through distributed machine learning. The methodology integrates Software-Defined Networking with collaborative learning techniques to detect cyberattacks without requiring smart devices to share their raw data. Three collaborative learning approaches were investigated: Federated Learning, Split Learning, and Split Learning with No Label Sharing. The intrusion detection models were deployed at the Software-Defined Networking application layer, where local smart meters and neighborhood area networks trained neural network models collaboratively while exchanging only model parameters or activation values. Technical evaluation focused on detecting multiple attack categories, including Denial-of-Service, Probe, Remote-to-Local, and User-to-Root attacks using the NSL-KDD dataset. The study also analyzed computational complexity, communication overhead, scalability, convergence behavior, and privacy preservation for each collaborative learning approach. Experimental results demonstrated that all three approaches achieved validation accuracy exceeding 99% after training convergence, while Split Learning consistently provided the best performance. For neighborhood area network intrusion detection, Split Learning achieved an accuracy of approximately 81.18% with an F1-score of 79.9%, outperforming Federated Learning and Split Learning with No Label Sharing. The proposed framework effectively balances detection accuracy, privacy protection, and communication efficiency, making it a scalable and resilient cybersecurity solution for future Software-Defined Smart Grid communication infrastructures.

Tricomi et al., [59] proposed a resilient fire protection framework for Software-Defined Factories to improve emergency response, fault tolerance, and operational continuity during fire incidents in industrial environments. The methodology introduces a software-defined architecture that separates control logic from physical fire protection devices, enabling centralized management and dynamic reconfiguration of emergency services. The framework integrates Internet of Things sensors, actuators, controllers, and edge computing resources into a federated architecture that continuously monitors factory conditions and automatically adapts system behavior when failures or hazardous situations occur. Technical aspects include business logic rewiring, runtime service orchestration, distributed resource sharing among neighboring factories, real-time event monitoring, and software-defined networking principles to maintain communication among emergency components. The architecture also supports collaboration between multiple industrial sites, allowing unaffected factories to temporarily provide computational resources and emergency services when a local control system becomes unavailable. The proposed framework was validated through a federated fire protection case study that analyzed different emergency scenarios involving communication failures and infrastructure disruptions. The evaluation demonstrated that the software-defined architecture significantly reduced service interruptions, improved system resilience, enabled continuous monitoring during catastrophic events, and minimized response latency through adaptive service migration and dynamic resource allocation. The results indicate that the

proposed solution provides a scalable, reliable, and flexible fire protection mechanism suitable for next-generation smart factories and industrial cyber-physical systems.

Islam et al., [60] proposed a Software-Defined Networking-based proactive routing framework for smart grids that combines Graph Neural Networks and Deep Q-Networks to improve communication resilience under cyberattacks and network failures. The methodology employs a centralized Software-Defined Networking controller that continuously collects network topology information and traffic statistics from smart grid devices. A Graph Neural Network is first used to learn the complex relationships among network nodes and links by extracting topological and traffic features from the communication graph. The extracted representations are then provided to a Deep Q-Network, which learns an optimal routing policy through reinforcement learning. Instead of reacting to failures after they occur, the framework proactively predicts network conditions and selects resilient routing paths before congestion, link failures, or attacks can significantly affect communication. Technical evaluation was performed through extensive simulations considering multiple smart grid communication scenarios, including dynamic traffic loads, node failures, and Distributed Denial-of-Service attacks. Performance metrics included packet delivery ratio, end-to-end delay, throughput, routing efficiency, packet loss, and network recovery capability. Experimental results demonstrated that the proposed intelligent routing framework consistently outperformed conventional shortest-path and Software-Defined Networking routing approaches by achieving higher packet delivery, lower latency, reduced packet loss, and faster recovery from network disruptions. The integration of Graph Neural Networks and Deep Q-Networks enabled adaptive decision-making, improved routing resilience, and enhanced communication reliability, making the framework suitable for next-generation intelligent and secure smart grid communication networks.

Janabi et al., [61] presented a comprehensive survey of Intrusion Detection Systems designed for Software-Defined Networking by reviewing recent research on network security, attack detection techniques, machine learning models, deep learning methods, and publicly available datasets. The methodology involved systematically analyzing existing intrusion detection frameworks and categorizing them based on detection techniques, deployment architectures, learning models, and performance evaluation metrics. The paper also reviews benchmark datasets such as NSL-KDD, UNSW-NB15, CICIDS2017, CICIDS2018, CSE-CIC-IDS2018, and InSDN for evaluating intrusion detection performance. The survey concludes that deep learning-based intrusion detection systems generally achieve higher detection accuracy and better adaptability than traditional methods but still face challenges related to computational complexity, dataset imbalance, scalability, real-time processing, and controller overhead. The authors identify future research directions, including lightweight artificial intelligence models, federated learning, explainable artificial intelligence, and adaptive intrusion detection for secure and resilient Software-Defined Networking environments.

Fausto et al., [62] proposed a Software-Defined Networking-based Intrusion Detection System architecture to reduce detection and response delays while improving the overall security of programmable networks. The methodology integrates an Intrusion Detection System with the centralized Software-Defined Networking controller, enabling real-time traffic monitoring, rapid attack detection, and immediate enforcement of security policies. Instead of forwarding suspicious traffic to external security appliances, the controller directly analyzes network flows and dynamically updates forwarding rules to isolate malicious traffic with minimal delay. The proposed architecture employs flow-based traffic analysis, programmable switches, and centralized decision-making to accelerate intrusion detection while maintaining efficient network operation. Experimental results demonstrated a significant reduction in overall detection and response time due to the elimination of unnecessary communication delays between network devices and external security systems. The proposed approach also maintained efficient packet forwarding, improved attack mitigation speed, and enhanced network resilience without introducing substantial computational overhead. The study concludes that integrating intrusion detection directly into the Software-Defined Networking control architecture provides faster threat response, improved security management, and better adaptability for protecting modern programmable communication networks.

Razib et al., [63] proposed a Software-Defined Networking-enabled hybrid deep learning framework for detecting cyber threats in smart environments by combining Deep Neural Networks and Long Short-Term Memory networks. The methodology integrates centralized Software-Defined Networking architecture with intelligent traffic analysis to provide real-time detection of malicious network activities. The Software-Defined Networking controller continuously gathers flow statistics from programmable switches and forwards them to the hybrid learning model for classification. The Deep Neural Network is responsible for extracting complex features from network traffic, while the Long Short-Term Memory network captures temporal dependencies and sequential traffic behavior, enabling accurate identification of evolving cyberattacks. Technical implementation includes data preprocessing, feature normalization, hybrid model training, and attack classification using benchmark intrusion detection datasets. The framework was evaluated against conventional machine learning and deep learning models using performance metrics such as accuracy, precision, recall, F1-score, false positive rate, and detection time. Experimental results demonstrated that the proposed hybrid model achieved superior detection accuracy with lower false alarm rates and faster attack identification compared with individual Deep Neural Network, Long Short-Term Memory, and traditional machine learning algorithms. The integration of Software-Defined Networking with hybrid deep learning also enabled

centralized security management, efficient traffic monitoring, and rapid mitigation of cyber threats without significantly increasing computational overhead. The study concludes that the proposed framework provides an intelligent, scalable, and resilient cybersecurity solution for protecting next-generation smart environments against sophisticated and continuously evolving network attacks.

Javeed et al., [64] proposed an intelligent intrusion detection system for smart consumer electronics networks by integrating deep learning techniques with Software-Defined Networking to provide accurate and real-time cyberattack detection. The methodology employs a centralized Software-Defined Networking controller that continuously collects network traffic information from connected smart consumer devices and forwards the traffic features to an intelligent detection engine. The proposed framework combines Deep Neural Networks and Long Short-Term Memory networks to exploit both spatial and temporal characteristics of network traffic. The Deep Neural Network automatically extracts high-level features from complex traffic patterns, while the Long Short-Term Memory network learns sequential dependencies to distinguish normal communication from malicious activities. Experimental results demonstrated that the proposed intelligent intrusion detection system achieved higher detection accuracy, lower false positive rates, and faster attack detection than conventional machine learning and individual deep learning models. The integration of Software-Defined Networking with hybrid deep learning improved centralized security management, enhanced communication reliability, and enabled scalable protection for smart consumer electronics networks against sophisticated and evolving cyber threats.

Girdhar et al., [65] proposed a Hidden Markov Model-based smart cyber switching framework to enhance cybersecurity and resilience in digital substations against sophisticated cyberattacks. The methodology integrates Hidden Markov Models with intelligent cyber switching to continuously monitor communication behavior, identify abnormal network states, and automatically initiate secure communication paths when malicious activities are detected. The framework operates within digital substations by observing network traffic patterns and estimating the probability of different system states to distinguish normal operations from cyberattacksThe proposed framework was evaluated using simulated cyberattack scenarios involving communication disruptions, false data injection, and denial-of-service attacks. Performance analysis considered attack detection accuracy, response time, communication availability, system resilience, and operational reliability. Experimental results demonstrated that the Hidden Markov Model-based smart cyber switching approach achieved high detection accuracy with rapid threat identification and automatic communication recovery while significantly reducing service disruption compared with conventional cybersecurity methods. The study concludes that combining probabilistic anomaly detection with intelligent cyber switching provides an effective and scalable solution for protecting next-generation digital substations against evolving cyber threats while ensuring secure, reliable, and resilient smart grid communication.

Rekik et al., [66] proposed a hybrid intrusion detection framework that combines Graph Neural Networks and Neural Ordinary Differential Equations to accurately detect cyberattacks in dynamic network topologies. The methodology is designed to address the limitations of conventional intrusion detection models that struggle with continuously changing network structures and traffic patterns. The proposed framework first models the communication network as a graph, where Graph Neural Networks learn the spatial relationships among network nodes, communication links, and traffic flows. The proposed model was evaluated using benchmark intrusion detection datasets under multiple attack scenarios, including Denial-of-Service, Distributed Denial-of-Service, Probe, infiltration, and other network attacks. Performance was measured using accuracy, precision, recall, F1-score, receiver operating characteristic analysis, and computational efficiency. Experimental results demonstrated that the hybrid model outperformed conventional Graph Neural Network, recurrent neural network, and transformer-based intrusion detection methods by achieving higher detection accuracy, lower false positive rates, improved adaptability to evolving network topologies, and greater robustness against sophisticated cyber threats. The study concludes that integrating Graph Neural Networks with Neural Ordinary Differential Equations provides an intelligent, scalable, and resilient intrusion detection solution for next-generation dynamic communication networks.

Kipruto et al., [67] proposed a scalable hybrid online machine learning framework for real-time intrusion detection in Electric Vehicle Charging Systems to improve cybersecurity against continuously evolving network attacks. The methodology combines online machine learning with a hybrid classification strategy that continuously learns from incoming network traffic without requiring complete model retraining. The framework processes charging station communication data in real time, allowing the intrusion detection model to adapt to changing attack patterns and network behavior while maintaining high detection performance. Technical implementation includes data preprocessing, feature extraction, incremental learning, and hybrid classification algorithms that analyze communication traffic exchanged between electric vehicles, charging stations, and backend management systems. The online learning mechanism continuously updates the model using newly arriving traffic, enabling rapid adaptation to zero-day attacks and concept drift while minimizing computational overhead. The framework was evaluated using realistic electric vehicle charging communication datasets under multiple cyberattack scenarios, including Denial-of-Service, Distributed Denial-of-Service, spoofing, replay attacks, and malicious network intrusions. Performance evaluation considered accuracy, precision, recall, F1-score, detection latency, scalability, and computational efficiency. Experimental results demonstrated that the proposed hybrid online learning framework achieved superior intrusion detection accuracy with low false positive rates and fast detection time while maintaining stable performance in large-scale charging

infrastructures. The adaptive learning capability significantly improved resilience against emerging cyber threats compared with traditional offline machine learning models. The study concludes that the proposed framework provides an efficient, scalable, and intelligent cybersecurity solution for securing future electric vehicle charging systems and smart energy networks.

Mowla et al., [68] proposed ACHILLES, a machine learning framework for developing an explainable and generalized Automotive Intrusion Detection System capable of accurately identifying cyberattacks across diverse in-vehicle communication environments. The methodology focuses on overcoming the limitations of existing intrusion detection systems, which often exhibit poor generalization and limited interpretability when applied to unseen automotive datasets. The proposed framework employs machine learning models trained on multiple automotive communication datasets to improve robustness and cross-domain performance. A key feature of ACHILLES is its explainability mechanism, which provides clear insights into the factors influencing intrusion detection decisions, thereby improving transparency and supporting cybersecurity analysis. Technical aspects include comprehensive data preprocessing, feature engineering, feature importance analysis, model training, cross-dataset validation, and explainable artificial intelligence techniques to interpret prediction outcomes. The framework was evaluated using several automotive intrusion detection datasets containing Controller Area Network traffic under multiple attack scenarios, including Denial-of-Service, spoofing, fuzzy attacks, replay attacks, and malicious message injection. Performance evaluation considered accuracy, precision, recall, F1-score, receiver operating characteristic analysis, generalization capability, and explanation quality. Experimental results demonstrated that ACHILLES consistently achieved high detection accuracy across different datasets while maintaining strong generalization performance for previously unseen attack patterns. The explainability component successfully identified the most influential communication features responsible for attack detection, enabling improved model transparency and user confidence. The study concludes that ACHILLES provides an accurate, explainable, and generalized intrusion detection framework suitable for securing next-generation connected and intelligent automotive communication systems.

Kandhro et al., [69] proposed a real-time intrusion detection framework for Internet of Things-enabled cybersecurity infrastructures to improve the detection of malicious attacks in smart and connected environments. The methodology integrates machine learning techniques with Internet of Things communication networks to continuously monitor network traffic, analyze communication patterns, and classify malicious activities in real time. The proposed framework consists of data acquisition, preprocessing, feature extraction, feature selection, machine learning-based classification, and real-time attack detection modules. Network traffic collected from Internet of Things devices is processed to remove redundant information and extract discriminative features before being supplied to the classification model.Experimental results demonstrated that the proposed framework achieved high intrusion detection accuracy with a low false positive rate while maintaining efficient real-time performance suitable for resource-constrained Internet of Things environments. The intelligent feature selection and machine learning-based classification significantly improved attack detection capability and reduced processing overhead. The study concludes that the proposed framework provides a scalable, reliable, and intelligent cybersecurity solution for protecting next-generation Internet of Things-enabled smart infrastructures against continuously evolving cyber threats.

Wang et al., [70] proposed an explainable machine learning framework for Intrusion Detection Systems that improves both attack detection accuracy and model interpretability. The methodology combines supervised machine learning with explainable artificial intelligence techniques to overcome the limitations of conventional intrusion detection models, which often operate as black boxes and provide little insight into their decision-making process. The framework consists of data preprocessing, feature selection, machine learning-based classification, and explanation generation modules. Network traffic data are first cleaned and transformed before being used to train multiple machine learning classifiers. To improve transparency, the framework employs explainability methods that identify the contribution of individual network features toward the final prediction, enabling security analysts to understand why specific traffic is classified as malicious or normal. Technical aspects include feature engineering, model optimization, local and global feature importance analysis, and comparative evaluation of different machine learning algorithms using benchmark intrusion detection datasets. Performance evaluation considered accuracy, precision, recall, F1-score, receiver operating characteristic analysis, computational efficiency, and explanation quality. Experimental results demonstrated that the proposed explainable framework achieved high intrusion detection accuracy while maintaining clear and reliable explanations for classification decisions. The feature importance analysis also reduced redundant attributes and improved model efficiency without compromising detection performance. The study concludes that integrating explainable artificial intelligence with machine learning significantly enhances the transparency, reliability, and trustworthiness of intrusion detection systems, making the framework suitable for deployment in practical cybersecurity applications where accurate decision interpretation is essential.

Cantone et al., [71] presented a comprehensive cross-dataset generalization study to evaluate the robustness of machine learning models for Network Intrusion Detection Systems across different network environments. The methodology investigates whether machine learning models trained on one intrusion detection dataset can effectively detect cyberattacks in previously unseen datasets, thereby

addressing the generalization problem commonly encountered in practical cybersecurity applications. The study involves extensive preprocessing, feature normalization, feature alignment, model training, and cross-dataset testing using multiple publicly available intrusion detection datasets. Technical aspects include the evaluation of several machine learning algorithms under both within-dataset and cross-dataset learning scenarios.The study further showed that appropriate feature selection, data normalization, and domain adaptation techniques can improve cross-dataset generalization, although challenges remain in handling heterogeneous network traffic and evolving cyber threats. The authors conclude that future intrusion detection research should prioritize developing generalized and adaptable machine learning models capable of maintaining high detection performance across diverse network environments rather than optimizing solely for benchmark datasets.

Gaspar et al., [72] proposed an explainable artificial intelligence framework for Intrusion Detection Systems by investigating the applicability of Local Interpretable Model-Agnostic Explanations and Shapley Additive Explanations for interpreting the predictions of a Multi-Layer Perceptron classifier. The methodology focuses on improving the transparency of intrusion detection models while maintaining high detection performance. The framework consists of data preprocessing, feature engineering, training a Multi-Layer Perceptron model, and applying explainability techniques to interpret both individual predictions and overall model behavior. Local Interpretable Model-Agnostic Explanations is employed to provide local explanations for specific intrusion detection decisions, whereas Shapley Additive Explanations is used to evaluate the contribution of individual network traffic features toward the model's predictions on both local and global levels. Technical evaluation was conducted using benchmark intrusion detection datasets containing normal and malicious network traffic under multiple attack scenarios Shapley Additive Explanations provided more stable and comprehensive global feature interpretations, whereas Local Interpretable Model-Agnostic Explanations offered intuitive explanations for individual predictions. The study concludes that integrating explainable artificial intelligence techniques with deep learning-based intrusion detection systems enhances model transparency, improves user trust, and supports cybersecurity experts in understanding and validating automated security decisions without sacrificing detection performance.

Gao et al., [73] proposed a security-enhanced chaotic optical communication system that strengthens secure data transmission through external temporal self-feedback hardware encryption and decryption. The methodology introduces a hardware-based encryption mechanism in which chaotic optical signals generated by semiconductor lasers are synchronized using an external temporal self-feedback structure. Unlike conventional chaotic communication systems that rely solely on optical chaos synchronization, the proposed framework incorporates an additional hardware encryption and decryption layer, making unauthorized signal recovery significantly more difficult. Technical implementation involves chaotic semiconductor lasers, external optical feedback, temporal self-feedback loops, optical synchronization, and hardware-assisted encryption and decryption circuits. The transmitter encrypts the original information using chaotic optical carriers, while the receiver accurately reconstructs the transmitted data only when the hardware configuration and synchronization parameters match those of the transmitter. The proposed communication system was evaluated through numerical simulations and experimental verification by analyzing synchronization quality, communication reliability, signal concealment, and resistance against eavesdropping attacks. Performance evaluation considered synchronization error, bit recovery accuracy, transmission stability, and communication security. Experimental results demonstrated that the proposed external temporal self-feedback mechanism significantly improved synchronization performance and enhanced resistance to unauthorized interception compared with conventional chaotic optical communication systems. The hardware-based encryption further increased the complexity of attack attempts, providing stronger protection against signal reconstruction and cryptanalysis. The study concludes that the proposed security-enhanced chaotic optical communication framework offers a reliable, high-speed, and highly secure solution for future optical communication networks requiring robust physical-layer security.

Vaasudevan et al., [74] proposed a holistic cybersecurity framework for detecting, classifying, and mitigating cyberattacks targeting the Distributed Network Protocol 3 communication protocol used in smart grid infrastructures. The methodology integrates machine learning-based intrusion detection, attack classification, and security enhancement mechanisms to provide comprehensive protection for critical smart grid communication networks. The proposed framework continuously monitors Distributed Network Protocol 3 communication traffic, preprocesses network data, extracts relevant communication features, and applies intelligent classification algorithms to distinguish normal traffic from malicious activities. After detecting an attack, the framework classifies the attack type and initiates appropriate security measures to minimize its impact on grid operations. Technical aspects include real-time traffic monitoring, feature engineering, machine learning-based attack classification, anomaly detection, protocol-aware security analysis, and automated response mechanisms. The framework was evaluated using Distributed Network Protocol 3 communication datasets under multiple cyberattack scenarios, including Denial-of-Service, replay attacks, false data injection, command injection, and reconnaissance attacks. Performance evaluation considered accuracy, precision, recall, F1-score, detection latency, classification accuracy, and system reliability. Experimental results demonstrated that the proposed framework achieved high attack detection and classification accuracy while maintaining low false alarm rates and rapid response times. The integrated security enhancement mechanisms effectively protected Distributed Network Protocol 3 communications against multiple attack types and improved the resilience and reliability of smart grid

operations. The study concludes that the proposed holistic framework provides an intelligent, scalable, and robust cybersecurity solution for safeguarding critical smart grid communication infrastructures from sophisticated and evolving cyber threats.

Sudhakara et al., [75] proposed a security enhancement framework for Autonomous Aerial Vehicle swarms by integrating Federated Learning with Shapley Additive Explanations to improve cyberattack detection while preserving data privacy. The methodology enables multiple aerial vehicles to collaboratively train a global intrusion detection model without sharing raw data, thereby protecting sensitive information and reducing communication overhead. Each aerial vehicle independently trains a local machine learning model using its own operational and network data, and only model parameters are exchanged with a central aggregation server to construct a global detection model. To improve transparency and trust in the security decisions, the framework employs Shapley Additive Explanations to identify the contribution of individual features toward attack detection and explain the reasoning behind each prediction. Technical aspects include federated model training, secure parameter aggregation, explainable artificial intelligence-based feature interpretation, distributed learning, and cyberattack classification. The framework was evaluated using realistic autonomous aerial vehicle communication datasets under multiple attack scenarios, including spoofing, denial-of-service, false data injection, and communication disruption attacks. Performance evaluation considered accuracy, precision, recall, F1-score, communication overhead, model convergence, privacy preservation, and explanation quality. Experimental results demonstrated that the proposed framework achieved high intrusion detection accuracy while significantly reducing data transmission and preserving the privacy of participating aerial vehicles. The Shapley Additive Explanations analysis successfully identified the most influential features responsible for attack detection, improving model interpretability and supporting effective security management. The study concludes that integrating Federated Learning with explainable artificial intelligence provides a scalable, privacy-preserving, and intelligent cybersecurity solution for protecting autonomous aerial vehicle swarms against evolving cyber threats.

Wang et al., [76] proposed an enhanced lightweight authentication scheme with anonymity for fog computing architectures to improve secure communication between users, fog nodes, and cloud servers while maintaining low computational overhead. The methodology enhances an existing authentication protocol by addressing its security vulnerabilities and strengthening resistance against various cyberattacks without compromising efficiency. The proposed scheme employs lightweight cryptographic operations, mutual authentication, anonymous identity management, session key establishment, and secure password verification to ensure confidential communication in distributed fog computing environments. Performance evaluation compared the proposed authentication scheme with existing lightweight authentication protocols based on computational cost, communication overhead, storage requirements, authentication delay, and security functionality. Experimental results demonstrated that the enhanced protocol achieved stronger security guarantees while maintaining low computational complexity and reduced communication overhead, making it suitable for resource-constrained fog computing devices. The study concludes that the proposed lightweight anonymous authentication framework provides a secure, efficient, and scalable solution for protecting fog computing infrastructures and supporting privacy-preserving communication in future Internet of Things and edge computing applications.

Open Challenges and Research Directions

Zero-day generalisation and adversarial robustness

Detection of catalogued attacks is close to saturated on public benchmarks; several systems in Table 5 exceed 99% F1. Detection of attacks outside the training distribution is not. Generative and reconstruction-based methods reach 90–94% on held-out attack families [7], which still means one in ten to one in twenty novel attacks passes. Adversarial training, certified robustness bounds adapted to sequence models, and ensembles that mix statistical, specification-based, and learned detectors are the visible paths forward.

Cross-dataset portability and standardised benchmarking

Models trained on one vehicle's traffic degrade on another's, and results across papers are hard to compare because splits, metrics, and attack mixes differ [4], [18]. The field needs what the ROAD authors argue for: shared benchmarks with physically verified attacks, mandatory multi-metric reporting (false-positive rate, latency, memory, energy per thousand frames), and, urgently, a public CAN XL dataset, which does not yet exist.

Explainability for safety certification

A block decision on a braking-related frame must be auditable. Attention maps, feature attributions from tree ensembles, and rule extraction from trained networks are all being explored, but none yet meets the evidentiary standard that ISO 26262 assessors expect. Explainable-by-construction hybrids, where a learned scorer ranks and a transparent rule decides, are a pragmatic near-term compromise.

Online and continual learning on ECUs

Vehicle traffic is non-stationary: software updates, new ECUs, and seasonal driving all shift the normal distribution. Adaptive thresholds such as equation (5) are the lightest form of online adaptation; continual learning without catastrophic forgetting, on-device, within TinyML budgets, is the heavier open problem, with federated aggregation [4], [30] as the natural mechanism for sharing what individual vehicles learn.

Toward integrated frameworks

The most consequential direction, in our view, is architectural rather than algorithmic: joining hardware-rooted authentication, learned anomaly detection, and software-defined response in one closed loop, so that identity, behaviour, and policy reinforce each other. Figure 5 sketches this reference architecture, instantiated in our group's PUF-CNN-GRU framework, which reaches 99.95% F1 on CHD and 99.78% on OTIDS while cutting authentication latency 34% below HMAC-SHA256. No prior system in Table 5 combines all three layers, and we consider this integration the natural template for CAN XL-era vehicle security.

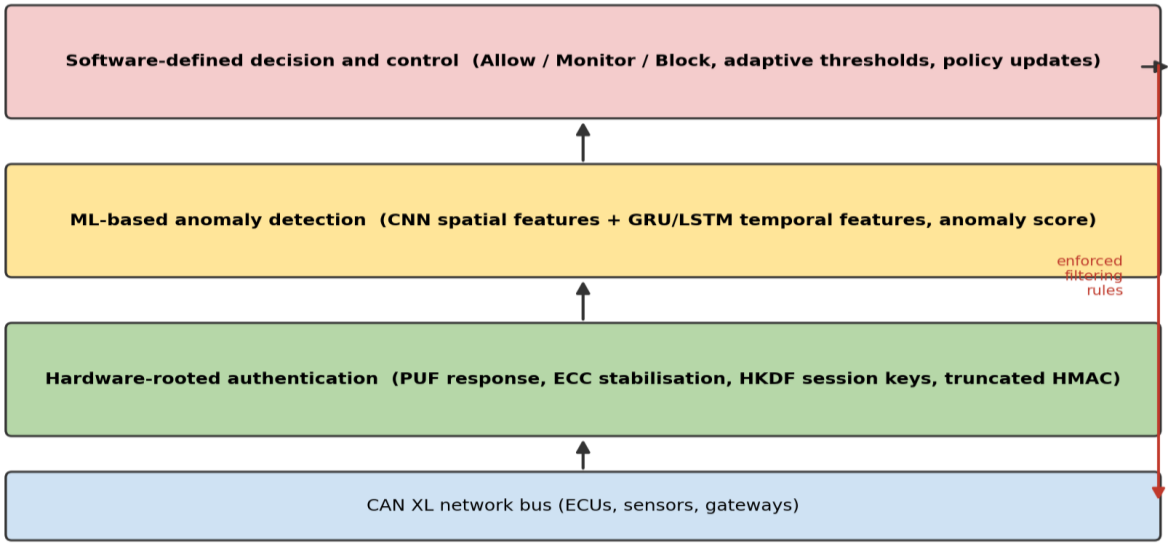

Fig. 5. *Reference architecture integrating hardware-rooted authentication, ML-based detection, and software-defined response.*

Conclusion

This survey traced the security problem of embedded communication networks from its origin in the trust model of Classical CAN, through the protocol features of CAN XL that change what defences are possible, to the learning-based detection systems, software-defined architectures, and hardware mechanisms that now define the state of the art. Three conclusions stand out. First, learning-based detection has effectively solved the catalogued-attack problem on public benchmarks but not the zero-day, adversarial, or cross-vehicle problems, and benchmark practice itself needs repair. Second, detection divorced from response and from deployment reality is of limited value: the software-defined control loop and the embedded resource budget deserve the same research attention as the model architecture. Third, the strongest systems will be layered, with hardware-derived identity beneath learned behavioural analysis beneath adaptive policy, because each layer covers the blind spots of the others. The arrival of CAN XL, with its larger frames, virtual networks, and native CANsec hooks, makes this integration more practical than it has ever been, and building and benchmarking such systems, on real CAN XL traffic, is the clear next step for the field.

References

1. C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” Black Hat USA, Las Vegas, NV, USA, 2015.
2. K. Koscher et al., “Experimental security analysis of a modern automobile,” in Proc. IEEE Symp. Security and Privacy, Oakland, CA, USA, 2010, pp. 447–462.
3. S. Woo, H. J. Jo, and D. H. Lee, “A practical wireless attack on the connected car and security protocol for in-vehicle CAN,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 993–1006, Apr. 2015.
4. M. Althunayyan, A. Javed, and O. Rana, “A survey of learning-based intrusion detection systems for in-vehicle networks,” Computer Networks, vol. 277, Art. no. 112031, 2026.

5. W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," IEEE Trans. Intell. Transp. Syst., vol. 21, no. 3, pp. 919–933, Mar. 2020.
6. O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," IEEE Access, vol. 7, pp. 21266–21289, 2019.
7. G. Asaouer and D. E. Boubiche, "Generative AI-based intrusion detection systems for intra-vehicle networks," Ad Hoc Networks, vol. 180, Art. no. 104031, 2026.
8. F. Wiemer and A. Mutter, "Beyond Ethernet: Reusing MACsec for CANsec," IACR Cryptology ePrint Archive, Rep. 2025/2224, 2025.
9. ISO 11898-1:2015, Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling, International Organization for Standardization, 2015.
10. ISO/SAE 21434:2021, Road vehicles — Cybersecurity engineering, International Organization for Standardization and SAE International, 2021.
11. ISO 26262 (series), Road vehicles — Functional safety, International Organization for Standardization, 2018.
12. IEEE Std 802.1AE-2018, IEEE Standard for Local and Metropolitan Area Networks — Media Access Control (MAC) Security, IEEE, 2018.
13. S. Sharmin, A. H. Lashkari, H. Mansor, and A. F. Abdul Kadir, "CAN-BiGRUBERT: Unveiling automotive vehicle intruders by profiling and characterizing anomalies in controller area network," Computer Networks, vol. 276, Art. no. 111963, 2026.
14. Y. Du, Y. Li, P. Cheng, Z. Han, and Y. Wang, "UGL: A comprehensive hybrid model integrating GCN and LSTM for enhanced intrusion detection in UAV controller area networks," Computer Networks, vol. 262, Art. no. 111157, 2025.
15. H. Lin, X. Yu, Z. Chen, and Y. Cao, "RAG-HIDS: A multi-relational graph-based hierarchical intrusion detection system for in-vehicle networks," Ad Hoc Networks, vol. 183, Art. no. 104108, 2026.
16. H. Jo and D. Kim, "Lightweight temporal and spatial fusion for intrusion detection in automotive controller area network," Ad Hoc Networks, vol. 187, Art. no. 104224, 2026.
17. Y. Fu, J. She, Y. Xu, Y. Xu, Z. Wang, and Y. Wu, "A dual layer LSTM-CNN framework for real time and precise per-message intrusion detection in in-vehicle networks," Ad Hoc Networks, vol. 183, Art. no. 104119, 2026.
18. M. E. Verma, R. A. Bridges, M. D. Iannacone, S. C. Hollifield, P. Moriano, S. C. Hespeler, B. Kay, and F. L. Combs, "A comprehensive guide to CAN IDS data and introduction of the ROAD dataset," PLOS ONE, vol. 19, no. 1, Art. no. e0296879, 2024.
19. H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," Vehicular Communications, vol. 21, Art. no. 100198, 2020.
20. E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," in Proc. 16th Annu. Conf. Privacy, Security and Trust (PST), Belfast, U.K., 2018, pp. 1–6.
21. Lavanya Vaishnavi D. A. and C. Anil Kumar, "Performance Enhancement of 5G MIMO Antenna Utilizing Verifiable Convolutional Neural Network Optimized With Human Evolutionary Optimization Algorithm," International Journal of Communication Systems, vol. 39, no. 4, Art. no. e70404, Jan. 2026, doi: 10.1002/dac.70404.
22. H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by offset ratio and time interval based on remote frame," in Proc. 15th Annu. Conf. Privacy, Security and Trust (PST), Calgary, AB, Canada, 2017, pp. 57–66.
23. M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data," IEEE Access, vol. 8, pp. 58194–58205, 2020.
24. R. Islam, R. U. D. Refat, S. M. Yerram, and H. Malik, "Graph-based intrusion detection system for controller area networks," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 3, pp. 1727–1736, Mar. 2022.
25. Lavanya Vaishnavi D. A. and C. Anil Kumar, "Evaluating Supervised Learning Classifier Performance for OFDM Communication in AWGN-Impacted Systems," Results in Engineering, vol. 26, Art. no. 105178, May 2025, doi: 10.1016/j.rineng.2025.105178.
26. W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "VoltageIDS: Low-level communication characteristics for automotive intrusion detection system," IEEE Trans. Inf. Forensics Security, vol. 13, no. 8, pp. 2114–2129, Aug. 2018.
27. H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "SAIDuCANT: Specification-based automotive intrusion detection using controller area network (CAN) timing," IEEE Trans. Veh. Technol., vol. 69, no. 2, pp. 1484–1494, Feb. 2020.
28. C. Anil Kumar, S. Harish, P. Ravi, M. S. V. N., B. P. Pradeep Kumar, V. Mohanavel, N. M. Alyami, S. Shanmuga Priya, and A. K. Asfaw, "Lung Cancer Prediction from Text Datasets Using Machine Learning," BioMed Research International, vol. 2022, Art. no. 6254177, Jul. 2022, doi: 10.1155/2022/6254177.

29. M. M. Hoque, I. Ahmad, J. Suomalainen, P. Dini, and M. Tahir, “On resource consumption of machine learning in communications network security,” Computer Networks, vol. 271, Art. no. 111600, 2025.
30. C. Vega, E. F. Kfoury, J. Gomez, J. E. Pezoa, M. Figueroa, and J. Crichigno, “Machine learning controller for data rate management in science DMZ networks,” Computer Networks, vol. 242, Art. no. 110237, 2024.
31. S. Dou, L. Qi, and Z. Guo, “Mitigating the impact of controller failures on QoS robustness for software-defined wide area networks,” Computer Networks, vol. 238, Art. no. 110096, 2024.
32. P. S. Marwein, S. N. Sur, and D. Kandar, “Efficient load distribution in heterogeneous vehicular networks using hierarchical controllers,” Computer Networks, vol. 254, Art. no. 110805, 2024.
33. X. Zhou, W. Liang, A. Kawai, K. Fueda, J. She, and K. I.-K. Wang, “Adaptive segmentation enhanced asynchronous federated learning for sustainable intelligent transportation systems,” IEEE Trans. Intell. Transp. Syst., vol. 25, no. 7, pp. 6658–6666, Jul. 2024.
34. G. Chandrasekaran, A. Kumar, K. Subramaniam, N. Sunil, and R. Challa, “EDgE: Enhancing predictability in decentralized network slices through federated learning — A multi layered ecosystem,” IEEE Access, vol. 12, pp. 100957–100971, 2024.
35. J. Chen et al., “Enhancing routing performance through trajectory planning with DRL in UAV-aided VANETs,” IEEE Trans. Mach. Learn. Commun. Netw., vol. 3, pp. 517–533, 2025.
36. P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, “PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey,” IEEE Internet Things J., vol. 9, no. 11, pp. 8205–8228, Jun. 2022.
37. M. N. Aman, U. Javaid, and B. Sikdar, “A privacy-preserving and scalable authentication protocol for the Internet of Vehicles,” IEEE Internet Things J., vol. 8, no. 2, pp. 1123–1139, Jan. 2021.
38. Rasheed, M. Baza, M. Badr, H. Alshahrani, and K.-K. R. Choo, “Efficient crypto engine for authenticated encryption, data traceability, and replay attack detection over CAN bus network,” IEEE Trans. Netw. Sci. Eng., vol. 11, no. 1, pp. 1008–1025, 2024.
39. Fraunhofer IPMS, “CANsec — Security for the third generation of the CAN bus,” White Paper, Dresden, Germany, 2025.
40. L. Yang, A. Shami, G. Stevens, and S. de Rusett, “LCCDE: A decision-based ensemble framework for intrusion detection in the Internet of Vehicles,” in Proc. IEEE Global Communications Conf. (GLOBECOM), Rio de Janeiro, Brazil, 2022, pp. 3545–3550.
41. Shaila Sharmin, Arash Habibi Lashkari, Hafizah Mansor, Andi Fitriah Abdul Kadir, “CAN-BiGRUBERT: Unveiling automotive vehicle intruders by profiling and characterizing anomalies in controller area network,” Computer Networks, Volume 276, 2026, 111963, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2025.111963.
42. Ying Du, Yilong Li, Pu Cheng, Zhijie Han, Yanan Wang, UGL: A comprehensive hybrid model integrating GCN and LSTM for enhanced intrusion detection in UAV controller area networks, Computer Networks, Volume 262, 2025, 11157, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2025.111157.
43. Christian Vega, Elie F. Kfoury, Jose Gomez, Jorge E. Pezoa, Miguel Figueroa, Jorge Crichigno, Machine learning controller for data rate management in science DMZ networks, Computer Networks, Volume 242, 2024, 110237, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2024.110237.
44. Muzun Althunayyan, Amir Javed, Omer Rana, A survey of learning-based intrusion detection systems for in-vehicle networks, Computer Networks, Volume 277, 2026, 112031, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2026.112031.
45. Md Muzammal Hoque, Ijaz Ahmad, Jani Suomalainen, Paolo Dini, Mohammad Tahir, On resource consumption of machine learning in communications network security, Computer Networks, Volume 271, 2025, 111600, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2025.111600.
46. Muzun Althunayyan, Amir Javed, Omer Rana, A survey of learning-based intrusion detection systems for in-vehicle networks, Computer Networks, Volume 277, 2026, 112031, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2026.112031.
47. Songshi Dou, Li Qi, Zehua Guo, Mitigating the impact of controller failures on QoS robustness for software-defined wide area networks, Computer Networks, Volume 238, 2024, 110096, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2023.110096.
48. Phibadeity S. Marwein, Samarendra Nath Sur, Debdatta Kandar, Efficient load distribution in heterogeneous vehicular networks using hierarchical controllers, Computer Networks, Volume 254, 2024, 110805, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2024.110805.
49. Hyunjun Jo, Deok-hwan Kim, Lightweight temporal and spatial fusion for intrusion detection in automotive controller area network, Ad Hoc Networks, Volume 187, 2026, 104224, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2026.104224.
50. Guettouche Asaouer, Djallel Eddine Boubiche, Generative AI-based intrusion detection systems for intra-vehicle networks, Ad Hoc Networks, Volume 180, 2026, 104031, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2025.104031.
51. Yu Fu, Junhui She, Yinan Xu, Yihu Xu, Ziyi Wang, Yujing Wu, A dual layer LSTM-CNN framework for real time and precise per-message intrusion detection in In-vehicle networks, Ad Hoc Networks, Volume 183, 2026, 104119, ISSN 1570-8705,

52. Hai Lin, Xi Yu, Zhihong Chen, Yue Cao, RAG-HIDS: A multi-relational graph-based hierarchical intrusion detection system for in-vehicle networks, Ad Hoc Networks, Volume 183, 2026, 104108, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2025.104108.
53. G. Chandrasekaran, A. Kumar, K. Subramaniam, N. Sunil and R. Challa, "EDgE: Enhancing Predictability in Decentralized Network Slices Through Federated Learning—A Multi Layered Ecosystem," in IEEE Access, vol. 12, pp. 100957-100971, 2024, doi: 10.1109/ACCESS.2024.3429631.
54. X. Zhou, W. Liang, A. Kawai, K. Fueda, J. She and K. I. -K. Wang, "Adaptive Segmentation Enhanced Asynchronous Federated Learning for Sustainable Intelligent Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 7, pp. 6658-6666, July 2024, doi: 10.1109/TITS.2024.3362058.
55. J. Chen et al., "Enhancing Routing Performance Through Trajectory Planning With DRL in UAV-Aided VANETs," in IEEE Transactions on Machine Learning in Communications and Networking, vol. 3, pp. 517-533, 2025, doi: 10.1109/TMLCN.2025.3558204.
56. S. Li, Y. Xie and M. Iqbal, "QuanReS: A Hybrid Quantum-Enabled Resilient and Secure V2X Communications Framework in Smart Cities," in IEEE Transactions on Consumer Electronics, vol. 72, no. 2, pp. 3940-3948, May 2026, doi: 10.1109/TCE.2025.3647004.
57. Z. Tang, P. Zhang and W. O. Krawec, "Enabling Resilient Quantum-Secured Microgrids Through Software-Defined Networking," in IEEE Transactions on Quantum Engineering, vol. 3, pp. 1-11, 2022, Art no. 4100811, doi: 10.1109/TQE.2022.3216530.
58. H. Janabi, T. Kanakis and M. Johnson, "Survey: Intrusion Detection System in Software-Defined Networking," in IEEE Access, vol. 12, pp. 164097-164120, 2024, doi: 10.1109/ACCESS.2024.3493384.
59. M. Mehic, S. Rass, E. Dervisevic and M. Voznak, "Tackling Denial of Service Attacks on Key Management in Software-Defined Quantum Key Distribution Networks," in IEEE Access, vol. 10, pp. 110512-110520, 2022, doi: 10.1109/ACCESS.2022.3214511.
60. M. U. F. Qaisar, W. Yuan, P. Bellavista, S. Ashraf Chaudhry, G. Han and A. Ahmed, "R2Com: Reliable and Resilient Communication in Duty-Cycled SDN-Based WSN for Urban Traffic Monitoring in Intelligent Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 11, pp. 19661-19678, Nov. 2025, doi: 10.1109/TITS.2025.3611518.
61. S. Chatzimiltis, M. Shojafar, M. B. Mashhadi and R. Tafazolli, "A Collaborative Software Defined Network-Based Smart Grid Intrusion Detection System," in IEEE Open Journal of the Communications Society, vol. 5, pp. 700-711, 2024, doi: 10.1109/OJCOMS.2024.3351088.
62. G. Tricomi, C. Scaffidi, G. Merlino, F. Longo, A. Puliafito and S. Distefano, "A Resilient Fire Protection System for Software-Defined Factories," in IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3151-3164, 15 Feb.15, 2023, doi: 10.1109/JIOT.2021.3127387.
63. M. A. Islam, R. Atat and M. Ismail, "Software-Defined Networking-Based Resilient Proactive Routing in Smart Grids Using Graph Neural Networks and Deep Q-Networks," in IEEE Access, vol. 12, pp. 111169-111186, 2024, doi: 10.1109/ACCESS.2024.3438938.
64. H. Janabi, T. Kanakis and M. Johnson, "Survey: Intrusion Detection System in Software-Defined Networking," in IEEE Access, vol. 12, pp. 164097-164120, 2024, doi: 10.1109/ACCESS.2024.3493384.
65. Fausto, G. Gaggero, F. Patrone and M. Marchese, "Reduction of the Delays Within an Intrusion Detection System (IDS) Based on Software Defined Networking (SDN)," in IEEE Access, vol. 10, pp. 109850-109862, 2022, doi: 10.1109/ACCESS.2022.3214974.
66. M. A. Razib, D. Javeed, M. T. Khan, R. Alkanhel and M. S. A. Muthanna, "Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework," in IEEE Access, vol. 10, pp. 53015-53026, 2022, doi: 10.1109/ACCESS.2022.3172304.
67. D. Javeed, M. S. Saeed, I. Ahmad, P. Kumar, A. Jolfaei and M. Tahir, "An Intelligent Intrusion Detection System for Smart Consumer Electronics Network," in IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 906-913, Nov. 2023, doi: 10.1109/TCE.2023.3277856.
68. M. Girdhar, K. Park, W. Su, J. Hong and C. -C. Liu, "Cybersecurity Enhancement in Digital Substations: Hidden Markov Model-Based Smart Cyber Switching and Threat Response," in IEEE Access, vol. 13, pp. 217022-217037, 2025, doi: 10.1109/ACCESS.2025.3648339.
69. S. Rekik and S. Mehmood, "A Hybrid Graph Neural Network and Neural ODE Model to Intrusion Detection in Dynamic Network Topologies," in IEEE Access, vol. 13, pp. 198201-198227, 2025, doi: 10.1109/ACCESS.2025.3635385.

70. J. Kipruto, B. Pranggono and R. Mani Shukla, "Scalable Hybrid Online Machine Learning for Real-Time Intrusion Detection in Electric Vehicle Charging Systems," in IEEE Access, vol. 14, pp. 12707-12716, 2026, doi: 10.1109/ACCESS.2026.3656666.
71. N. I. Mowla et al., "ACHILLES: A Machine Learning Framework for Explainable and Generalized Automotive Intrusion Detection System," in IEEE Transactions on Intelligent Transportation Systems, vol. 27, no. 7, pp. 7475-7490, July 2026, doi: 10.1109/TITS.2026.3688299.
72. A. Kandhro et al., "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," in IEEE Access, vol. 11, pp. 9136-9148, 2023, doi: 10.1109/ACCESS.2023.3238664.
73. M. Wang, K. Zheng, Y. Yang and X. Wang, "An Explainable Machine Learning Framework for Intrusion Detection Systems," in IEEE Access, vol. 8, pp. 73127-73141, 2020, doi: 10.1109/ACCESS.2020.2988359.
74. M. Cantone, C. Marrocco and A. Bria, "Machine Learning in Network Intrusion Detection: A Cross-Dataset Generalization Study," in IEEE Access, vol. 12, pp. 144489-144508, 2024, doi: 10.1109/ACCESS.2024.3472907.
75. D. Gaspar, P. Silva and C. Silva, "Explainable AI for Intrusion Detection Systems: LIME and SHAP Applicability on Multi-Layer Perceptron," in IEEE Access, vol. 12, pp. 30164-30175, 2024, doi: 10.1109/ACCESS.2024.3368377.
76. Z. Gao et al., "Security-Enhanced Chaotic Optical Communication Based on External Temporal Self-Feedback Hardware Encryption and Decryption," in IEEE Photonics Journal, vol. 14, no. 4, pp. 1-8, Aug. 2022, Art no. 7247008, doi: 10.1109/JPHOT.2022.3198527.
77. Vaasudevan et al., "A Holistic Framework for Cyber Attack Detection, Classification, and Security Enhancement of DNP3 Protocol in Smart Grids," in IEEE Access, vol. 13, pp. 200177-200195, 2025, doi: 10.1109/ACCESS.2025.3636010.
78. S. Halli Sudhakara and L. Haghnegahdar, "Security Enhancement in AAV Swarms: A Case Study Using Federated Learning and SHAP Analysis," in IEEE Open Journal of Intelligent Transportation Systems, vol. 6, pp. 335-345, 2025, doi: 10.1109/OJITS.2025.3550792.
79. Wang, H. An and Z. Chang, "Security Enhancement on a Lightweight Authentication Scheme With Anonymity Fog Computing Architecture," in IEEE Access, vol. 8, pp. 97267-97278, 2020, doi: 10.1109/ACCESS.2020.2996264.