Intent-Based Management for In-Network Computing Functions in Cooperative Intelligent Transportation Systems

Byoungman (Robert) An and Seonghyun (Alex) Jang
Mobility Platform Research Center
Korea Electronics Technology Institute
Seongnam, Republic of Korea
Email: {bman, jang.sh}@keti.re.kr

Jaehoon (Paul) Jeong
Department of Computer Science & Engineering
Sungkyunkwan University
Suwon, Republic of Korea
Email: pauljeong@skku.edu

2025 IEEE 11th International Conference on Network Softwarization (NetSoft) | 979-8-3315-4345-7/25/$31.00 ©2025 IEEE | DOI: 10.1109/NETSOFT64993.2025.11080550

***Abstract*—This paper proposes an intent-based management framework for orchestrating In-Network Computing Functions (ICFs) in Cooperative Intelligent Transportation Systems (C-ITS). Software-Defined Vehicles (SDVs) are emerging as key enablers of autonomous driving in C-ITS. SDVs leverage cloud-native platforms (e.g., Kubernetes) with their own in-vehicle networks and Vehicle-to-Everything (V2X) communication device. The proposed framework enables high-level intent-driven configuration of networking, security, and application services across SDVs, infrastructure nodes, and Mobile Network Operators (MNOs). A prototype implementation of the ICF framework demonstrates the feasibility of its architecture. This paper discusses several design challenges to guide future research in scalable, intent-based orchestration for SDV ecosystems.**

***Index Terms*—C-ITS, Intent-Based Management, In-Network Computing Function, V2X, Connected Vehicle.**

I. Introduction

Modern network environments have evolved beyond static configurations, moving toward fully automated, intent-driven operations. This shift, termed intent-based networking (IBN) [1], arises from the growing need to manage complex, large-scale, and dynamic infrastructures while maintaining efficiency, security, and agility [2]. Rather than specifying explicit operational procedures, IBN allows administrators to declare high-level goals, leaving the system to interpret and execute the necessary actions. Intent-based networks are governed by intent-based systems (IBS) [1], which streamline management through abstraction and policy-driven automation. Emerging technologies like artificial intelligence (AI), machine learning (ML), and software-defined networking (SDN) underpin these systems, enabling rapid service provisioning, adaptive policy enforcement [3], and compliance management [4], while minimizing manual intervention.

With the rapid advancement of computer, sensor, and wireless communication technologies, the concept of intelligent vehicles has evolved from standalone systems to cooperative vehicle–infrastructure systems. This evolution has led to the emergence of Intelligent Transportation Systems (ITS) as a critical solution for future mobility. The Internet of Vehicles (IoV) leverages a combination of advanced technologies such as communication, control, and computing to enhance road utilization in urban environments, improve traffic efficiency, reduce accidents and energy consumption, and support sustainable transportation development [5]–[8]. A typical architecture of an Intelligent Vehicle-Infrastructure Cooperative System (IVICS) consists of two core components: the Road-Side Unit (RSU) and the On-Board Unit (OBU), as illustrated in Fig. 1. Through V2X communication, vehicles can exchange data with the surrounding environment, enabling them to obtain a more accurate situational awareness that enhances traffic safety and efficiency. For instance, sensors installed on RSUs can detect approaching objects such as pedestrians and other vehicles and estimate their speed and distance. Based on this data, RSUs can dynamically adjust traffic signal phase information to optimize road traffic flows. Similarly, intelligent parking systems can analyze available parking space around a vehicle using surrounding environmental data. In recent years, V2X has attracted increasing research interest, focusing on topics such as standardization, scenario-based algorithm designs, opportunities, and challenges in deploying V2X technologies [9], [10]. For example, the work in [11] presents a Vehicle-to-Pedestrian (V2P) system

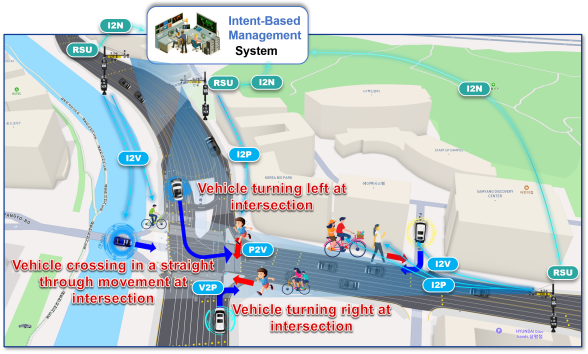

Fig. 1. Intent-Based Management System in C-ITS Environment

979-8-3315-4345-7/25/$31.00 ©2025 IEEE

Authorized licensed use limited to: Sungkyunkwan University. Downloaded on September 06,2025 at 23:30:12 UTC from IEEE Xplore. Restrictions apply.

framework that incorporates detection, tracking, trajectory prediction, and behavioral modeling of Vulnerable Road Users (VRUs), while addressing several key challenges in integrating V2X with VRU systems.

In the context of Intent-Based Management for In-Network Computing Functions (ICF) for Cooperative Intelligent Transportation Systems (C-ITS), it is essential to design and investigate an IBS tailored for Software-Defined Vehicles (SDVs) and intelligent robots, considering both in vehicle IP networks and external C-ITS integrated V2X communication environments. Modern SDVs are equipped with a variety of automotive applications, such as Advanced Driver Assistance Systems (ADAS), Automatic Emergency Braking (AEB), Forward Collision Warning (FCW), and Lane Keeping Assist (LKA). Data communications among these in-vehicle applications are increasingly handled through Virtual Network Functions (VNFs). At the same time, real-time interaction with external C-ITS networks, including Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, plays a critical role in enhancing situational awareness, safety, and efficiency on the road.

In this paper, we propose a framework and interface for IBN management within C-ITS. The proposed framework automates the configuration and monitoring of network and security policies across various entities infrastructure cloud, road-side infrastructure, Mobile Network Operators (MNOs), VRUs, and SDVs by leveraging their respective mobile and network connectivity.

The organization of this paper is as follows. Section II reviews prior research on IBN-based systems. Section III describes the overall architecture and core design principles of the proposed IBN framework for C-ITS. Section IV presents a preliminary implementation and system behavior. Finally, Section V concludes the paper along with future work.

II. Related Work

In this section, we review prior work related to IBN systems. We begin by outlining the technological evolution and motivations behind IBN. We then discuss the industrial initiatives and standardization efforts related to SDVs and V2X communications.

One of the primary motivations for adopting IBN is the increasing complexity of modern networks, which comprise a vast number of interconnected devices, services, and protocols [2]. Manually managing such complexity is no longer practical, thus necessitating automated and intent-driven approaches. In addition, modern networks must operate at massive scale, often spanning wide geographical regions and supporting millions of users, which makes scalability a crucial concern. IBN offers efficient management capabilities suited to such large-scale environments.

From an operational perspective, IBN reduces the reliance on human intervention, improving efficiency by enabling faster and more accurate execution of

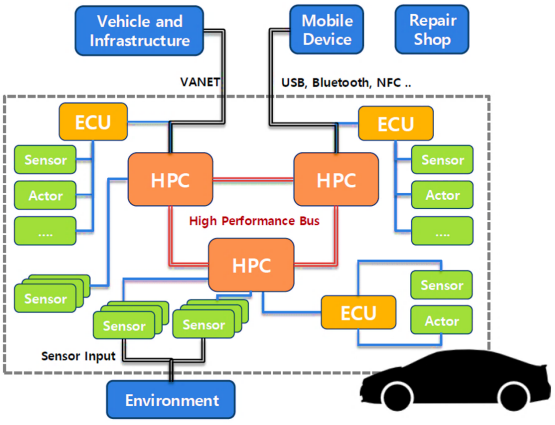

Fig. 2. Modern Automotive SDV Systems

network tasks. Moreover, networks are inherently dynamic, that is, frequently undergoing changes due to varying user demands, traffic patterns, mobility, and evolving security threats [12]. IBN facilitates adaptability to these changes in real time.

The development of IBN has been further accelerated by the integration of emerging technologies such as AI, ML, and SDN, which enhance automation and network intelligence [13], [14]. As the demand for new services and applications continues to grow, IBN plays a key role in enabling rapid and reliable service provisioning.

In the SDV field, a great number of initiatives have been proposed in the industry. The AUTomotive Open System ARchitecture (AUTOSAR) [15] organization has been extending its architecture design to integrate SDVs with cloud/edge services. The Scalable Open Architecture For Embedded Edge (SOAFEE) [16] aims at bringing the cloud-native development paradigm to the highly diverse, heterogeneous compute platforms for the next generation of automotive and safety critical systems. Eclipse SDV working group [17] facilitates open-source development of automotive software, including software stacks and associated tooling for the core functionality of SDVs. The Connected Vehicle Systems Alliance (COVESA) [18] focuses on connected vehicles and their related technologies to unlock the full potential of connected vehicles for SDVs. Particularly, they design the vehicle signal specification to unify vehicle data models. Fig. 2 shows a typical SDV platform that integrates both classical and software-oriented architectures. A vehicle's Electrical/Electronic (E/E) hardware devices, e.g., ECUs, sensors, and actuators, are grouped for the vehicle's High Performance Computing (HPC), which can maximally explore the potential of the data generated from those hardware devices.

In recent years, the 5G Automotive Association (5GAA) has proposed detailed specifications for a wide range of V2X use cases, including several innovative and original scenarios across different categories [19]. On the standards front, the radio access

Authorized licensed use limited to: Sungkyunkwan University. Downloaded on September 06,2025 at 23:30:12 UTC from IEEE Xplore. Restrictions apply.

layer is governed by the Third Generation Partnership Project (3GPP), which is progressing toward Release 18, expected to be finalized by the end of 2023 with further enhancements for V2X [20]. Higher-layer protocols and profiles are being standardized by regional bodies such as ETSI, SAE International, NTCAS, C-SAE, and ARIB, among others. These efforts aim to support advanced use cases such as group start and cooperative driving scenarios.

The International Organization for Standardization (ISO) is also driving standardization for services like Automated Valet Parking (AVP) in Europe and globally. To enable advanced cooperative driving and connected assistance services, enabling technologies such as positioning accuracy, power efficiency, and multi-access edge computing (MEC) are being continuously improved through global standardization efforts. The most recent roadmap reflects the increasing complexity of software-defined functions and emphasizes the need for ecosystem-wide collaboration.

In addition, network-based approaches are being explored to improve safety awareness for VRUs. Emerging use cases such as group start and cooperative maneuvers for highly automated driving will require further time and development before widespread deployment [19], [20].

III. Intent-Based Management Architecture for Cooperative Intelligent Transportation Systems

Based on the IBN life cycle model described in [1], Fig. 3 illustrates the intent-based networking process tailored for C-ITS management. The life cycle is organized into three conceptual domains: the user space, the IBS space, and the network operations and applications space. Each domain is further divided into two functional phases: fulfillment and assurance. The fulfillment phase comprises a sequential pipeline of operations, including intent input, translation and refinement, learning, planning, installation, and configuration or provisioning. This process drives the delivery of Service Functions (SFs), such as Network Functions (NFs) and Application Functions (AFs) deployed across SDVs and infrastructure nodes in C-ITS environments. The assurance phase focuses on monitoring the outcomes of the fulfillment process to validate intent realization and evaluate the behavior of the resulting NFs and AFs. In this section, we introduce our proposed Intent-Based System (IBS) architecture for C-ITS, which encompasses both NFs and AFs across heterogeneous networked components within the C-ITS ecosystem.

A. IBS for In-Network Computing Functions in C-ITS

In-network computing has recently emerged as a compelling research area due to advances in data plane programmability, which have opened up new opportunities for application developers and network operators to optimize performance. [21] A wide range of ICFs

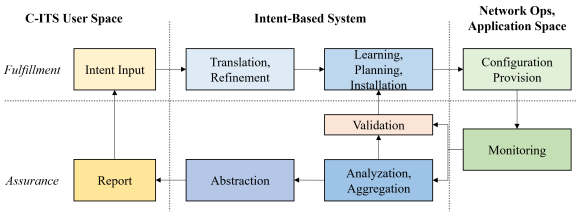

Fig. 3. The Life Cycle of IBS for C-ITS Management

have demonstrated their effectiveness in domains such as machine learning, real-time analytics, and large-scale distributed systems. In particular, in-network aggregation techniques have accelerated collective communication primitives such as Allreduce and Broadcast which are essential for distributed training of machine learning models. These advancements have contributed to the gradual commercialization of in-network computing technologies and have led to broader use case exploration in recent studies [22]–[24]. Despite these promising developments, one of the key challenges remains the absence of a unified and standardized framework for registering, configuring, managing, and monitoring ICFs. While frameworks such as I2NSF provide a foundation for orchestrating Network Security Functions (NSFs), they are not sufficient to accommodate the unique requirements of ICFs [25]. Unlike traditional NSFs, ICFs often require tight coordination between programmable network devices and endpoint computing components to collaboratively enhance application performance. To address this gap, we propose an IBS architecture that incorporates ICFs as dynamic service functions within the data plane. In our design, intents related to performance critical C-ITS applications such as low-latency V2V communication or distributed sensor data aggregation are translated through the fulfillment process into executable policies that activate and configure specific ICFs deployed on programmable infrastructure. Furthermore, the assurance process within the IBS continuously monitors the behavior and performance of the ICFs, validating whether the deployed functions are meeting the user's original service intent. This tight integration between IBS and ICFs enables an adaptive, intelligent, and secure orchestration of in-network computing within C-ITS environments. It also supports efficient service delivery, improved traffic control, and enhanced cybersecurity across SDVs, RSUs, and MNOs operating within highly dynamic and interconnected transportation systems.

Fig. 4 illustrates a framework for Interface to In-Network Computing Functions (I2ICF) in C-ITS. This architecture integrates the components of the I2ICF framework to support coordination across C-ITS and MNO networks, and includes several core elements and their associated interfaces for intent processing, policy enforcement, and service orchestration.

- **Central Cloud**: The central control layer of the C-ITS ecosystem. It manages integrated infor-

Authorized licensed use limited to: Sungkyunkwan University. Downloaded on September 06,2025 at 23:30:12 UTC from IEEE Xplore. Restrictions apply.

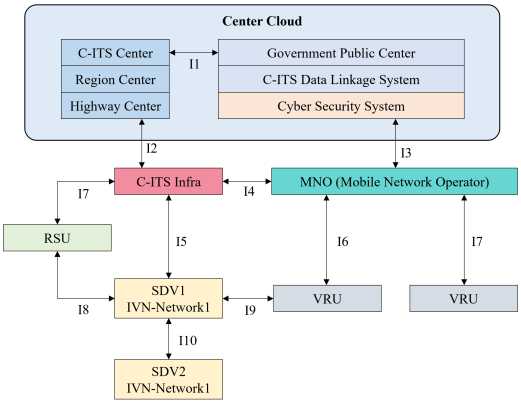

Fig. 4. I2ICF Framework and Interfaces

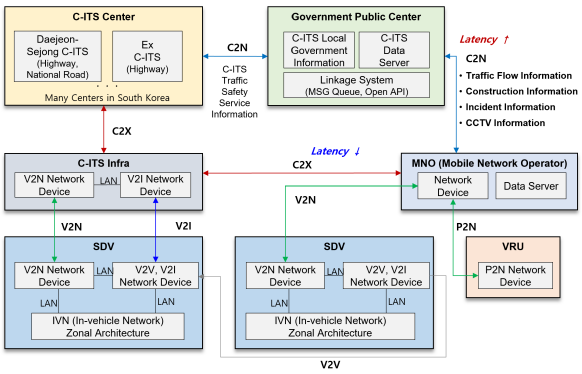

Fig. 5. A Use Case of I2ICF in C-ITS

mation from national and regional centers, coordinates data exchange between the government-operated Public Center and end users, and provides centralized cybersecurity services.

- **C-ITS Center**: A general term encompassing both Region and Highway Centers. It functions as the core control hub for C-ITS operations, enabling data-driven traffic management and communication across urban and highway systems.
- **Region Center**: A local traffic management unit connected to RSUs, responsible for collecting and exchanging data with the Central Cloud. It ensures regional infrastructure operates in sync with national-level traffic systems.
- **Highway Center**: Similar to the Region Center but optimized for highway environments. It handles high traffic volumes and dense RSU deployments, supporting real-time communication and control for autonomous vehicles on highways.
- **Government Public Center**: A government-managed system responsible for distributing trusted infrastructure data. It ensures data integrity and reliability for public use, addressing challenges that arise from privatized traffic data sources.
- **C-ITS Data Linkage System**: A platform that connects C-ITS infrastructure data to external users through APIs and data interfaces. It enables integration of real-time traffic information into third-party services and applications.
- **Cyber Security System**: This system secures communications between SDVs, VRUs, RSUs, MNOs, and infrastructure components. It implements encryption using public-private key pairs and ensures the integrity and confidentiality of data in transit.
- **C-ITS Infrastructure**: A field-deployed system collecting real-time data, such as traffic signals, environmental conditions, and VRU activity. Its capabilities depend on roadside hardware configurations and enable V2X data exchange.
- **RSU (Road-Side Unit)**: A communication gateway between SDVs and C-ITS infrastructure. RSUs enable V2V and V2I interactions, delivering critical information like road conditions and safety alerts to vehicles in real time.
- **SDV1 and SDV2**: Example vehicles in the architecture diagram. Each SDV includes dual interfaces: an external communication interface for V2X (V2V, V2I, V2N), and an In-Vehicle Network (IVN) interface for managing in-vehicle components.
- **IVN-Network1 and IVN-Network2**: Sample internal networks within SDVs. Based on a zonal architecture, these IVNs optimize data flow between sensors, controllers, and actuators for real-time autonomous driving support.
- **VRU (Vulnerable Road User)**: Pedestrians, cyclists, and motorcyclists who can interact with SDVs or MNOs. Through direct or indirect communication, they exchange safety-critical data to enhance their visibility and protection in the traffic system.
- **MNO (Mobile Network Operator)**: Telecom operators that provide infrastructure for cellular connectivity. MNOs support low-latency, high-reliability V2X communication and collaborate with C-ITS entities to deliver secure, efficient mobility services.

For instance, when a vehicle submits a low-latency intent for V2V communication, the IBS translates it into policies that activate aggregation-based ICFs on RSUs, and monitors feedback to ensure QoS targets are met.

B. IBS Use Cases in C-ITS

This section presents representative use cases of the I2ICF framework in the context of C-ITS and MNO integration. These scenarios highlight how emerging technologies such as SDVs, End-to-End (E2E) communication, and edge computing can benefit from the architecture to enhance safety, responsiveness, and cybersecurity in intelligent transportation environments as shown in Fig. 5.

One primary use case involves real-time data processing for SDVs. Through interfaces such as I5 (between the C-ITS infrastructure and SDVs) and I8 (for V2V communication via RSUs), the I2ICF framework

Authorized licensed use limited to: Sungkyunkwan University. Downloaded on September 06,2025 at 23:30:12 UTC from IEEE Xplore. Restrictions apply.

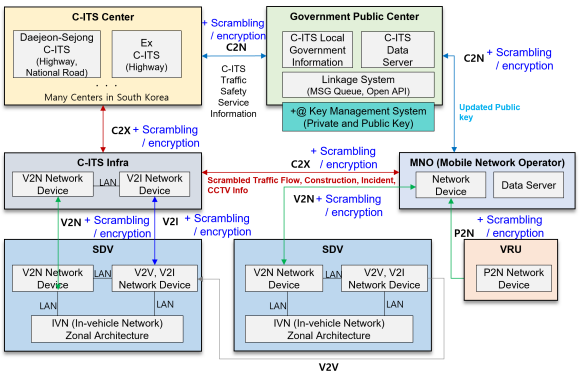

Fig. 6. A Use Case of I2ICF for C-ITS with Security Consideration

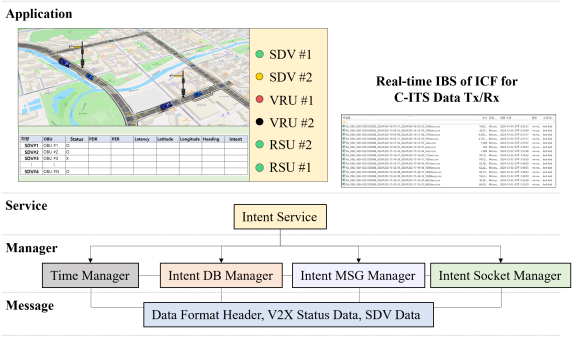

Fig. 7. Implementation of Real-time IBS for ICFs in C-ITS

facilitates timely delivery of traffic signal information, road conditions, and hazard alerts to SDVs. Offloading specific processing tasks to RSUs reduces the computational load on vehicles, allowing faster responses to time-sensitive scenarios like emergency braking or lane changes.

Another critical use case is E2E communication for cooperative driving. By integrating MNO networks with the C-ITS infrastructure through interfaces like I4 (C-ITS Infra ↔ MNO) and I6 (MNO ↔ VRU/SDV), the framework enables reliable and low-latency communication between vehicles and infrastructure. This capability is essential for coordinated maneuvers such as merging, platooning, or intersection crossing, where real-time data sharing among multiple vehicles is crucial.

Cybersecurity is also a fundamental requirement for C-ITS and MNO cooperation. The I2ICF framework incorporates a Cyber Security System operating through interfaces such as I3 (Government Public Center ↔ MNO) and I10 (intra-vehicle communication). It supports end-to-end encryption and secure key management, including OTA-based private key updates. In the event of a security breach, the system can execute a global rekeying procedure to maintain the integrity and confidentiality of the network.

In high-density traffic scenarios, such as urban intersections or congested highways, dynamic resource allocation becomes essential. Interfaces like I7 (RSU ↔ C-ITS Infra) and I9 (SDV ↔ VRU) enable the I2ICF framework to prioritize bandwidth and processing power for emergency vehicles or time-critical messages, thereby minimizing latency and avoiding congestion in the communication infrastructure.

Lastly, the framework supports edge computing for latency-sensitive applications. Interfaces such as I1 (C-ITS Center ↔ Government Public Center) and I8 (SDV ↔ SDV via RSU) allow offloading of tasks like object detection and trajectory prediction to edge nodes, such as RSUs or Programmable Network Devices (PNDs). This reduces dependency on centralized cloud services and significantly improves response times for autonomous driving operations.

Collectively, these use cases demonstrate the I2ICF framework's ability to enhance communication performance, ensure security, and enable adaptive service orchestration across connected and autonomous transportation systems.

C. Security Considerations of IBS in C-ITS

The I2ICF framework provides substantial benefits for C-ITS and MNO-based network environments by enabling integrated communication across heterogeneous entities such as vehicles, infrastructure devices, cloud systems, and VRUs. However, this high degree of interconnectivity also introduces significant security challenges due to the wide exposure of data and control functionalities during network configuration and operation as shown in Fig. 6.

To mitigate potential risks and ensure system-wide security, several key measures should be considered. First, application development and deployment should be managed by the same trusted entities such as cloud service providers or mobile network operators that maintain ownership of the underlying network and computing infrastructure. This alignment helps minimize third-party risks and ensures accountability.

Second, devices deployed within cloud and central management systems should be assigned predefined security zones to facilitate logical traffic separation. This prevents unintended interactions between services and limits the propagation of malicious traffic.

Third, encryption keys for all components must be centrally administered by the cloud management system. To respond swiftly to key compromise incidents, the framework should support Over-The-Air (OTA) key update mechanisms to replace exposed keys in a timely manner.

Finally, in the event of a critical breach particularly one that compromises keys within the centralized controller a full system reset and reinitialization process must be triggered. This process involves generating and securely distributing new encryption keys to all participating components, thereby restoring trust and preserving data confidentiality throughout the network.

IV. Implementation

We implemented a preliminary IBN testbed for SDV management to show a Proof of Concept (PoC). This PoC uses an open-source cellular network framework to connect SDVs. As shown in Fig. 7, the Autonomous

Authorized licensed use limited to: Sungkyunkwan University. Downloaded on September 06,2025 at 23:30:12 UTC from IEEE Xplore. Restrictions apply.

Telecommunication Hyper Enhanced Network Architecture (ATHENA) is implemented as the core framework for managing V2X communication technologies and the diverse C-ITS services operating on top of them within the South Korean V2X testbed [26]. Our ATHENA has not accommodated the I2ICF framework and interfaces, but we will enhance the ATHENA with the data models of the I2ICF interfaces as a next step.

V. Conclusion

This paper presented an intent-based management framework and a representative use case for the In-Network Computing Functions (called ICFs) in C-ITS. The proposed framework facilitates the agile orchestration of virtualized network functions and applications, enabling dynamic reconfiguration of network resources and flexible updates for various devices within C-ITS environments. A preliminary implementation of the framework was introduced to demonstrate its feasibility, and several technical challenges and future research directions were discussed. Compared to ETSI MEC and conventional orchestration systems, the proposed framework uniquely supports fine-grained, intent-driven coordination of ICFs across SDVs and RSUs. As future work, we will further develop and implement the essential system components and interfaces required to realize the proposed framework in real-world C-ITS deployments. In addition, we will explore intent-based security mechanisms to enhance the reliability and trustworthiness of the proposed architecture.

Acknowledgment

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (No. 2022-0-00199 and No. RS-2024-00398199). Note that Jaehoon (Paul) Jeong is the corresponding author.

References

[1] A. Clemm, L. Ciavaglia, L. Z. Granville, and J. Tantsura, "Intent-Based Networking - Concepts and Definitions," RFC 9315, Oct. 2022. [Online]. Available: https://www.rfc-editor.org/info/rfc9315

[2] A. Leivadeas and M. Falkner, "A Survey on Intent-Based Networking," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 625–655, 2023.

[3] J. Kim, E. Kim, J. Yang, J. Jeong, H. Kim, S. Hyun, H. Yang, J. Oh, Y. Kim, S. Hares, and L. Dunbar, "IBCS: Intent-Based Cloud Services for Security Applications," *IEEE Communications Magazine*, vol. 58, no. 4, pp. 45–51, Apr. 2020.

[4] P. Lingga, J. Jeong, J. Yang, and J. Kim, "SPT: Security Policy Translator for Network Security Functions in Cloud-Based Security Services," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 6, pp. 5156–5169, Nov. 2024.

[5] L. Hu, J. Ou, J. Huang, Y. M. Chen, and D. P. Cao, "A Review of Research on Traffic Conflicts Based on Intelligent Vehicles," *IEEE Access*, vol. 8, pp. 24 471–24 483, 2020.

[6] J. P. Zhang, F. Y. Wang, K. F. Wang, W. H. Lin, X. Xu, and C. Chen, "Data-Driven Intelligent Transportation Systems: A Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1624–1639, 2011.

[7] S. E. Shladover, "Connected and Automated Vehicle Systems: Introduction and Overview," *Journal of Intelligent Transportation Systems*, vol. 22, no. 3, pp. 190–200, 2018.

[8] L. Zhu, F. R. Yu, Y. G. Wang, B. Ning, and T. Tang, "Big Data Analytics in Intelligent Transportation Systems: A Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 1, pp. 383–398, 2019.

[9] K. Kiela, V. Barzdenas, M. Jurgo, V. Macaitis, J. Rafanavicius, and A. Vasjanov, "Review of V2X-IoT Standards and Frameworks for ITS Applications," *Applied Sciences*, vol. 10, no. 12, 2020.

[10] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 308–323, 2020.

[11] P. Sewalkar and J. Seitz, "Vehicle-to-Pedestrian Communication for Vulnerable Road Users: Survey, Design Considerations, and Challenges," *Sensors*, vol. 19, no. 2, 2019.

[12] M. Avgeris, A. Leivadeas, N. Athanasopoulos, I. Lambadaris, and M. Falkner, "Model Predictive Control for Automated Network Assurance in Intent-Based Networking enabled Service Function Chains," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 2023, pp. 1–7.

[13] J. J. D. Rivera, M. M. S. Sarwar, S. Alam, T. A. Khan, M. Afaq, and W.-C. Song, "An Intent-Based Networking mechanism: A study case for efficient path selection using Graph Neural Networks," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 2023, pp. 1–6.

[14] Collet, Alan and Banchs, Albert and Fiore, Marco, "LossLeaP: Learning to Predict for Intent-Based Networking," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, 2022, pp. 2138–2147.

[15] AUTomotive Open System ARchitecture (AUTOSAR) Adaptive Platform. [Online]. Available: https://www.autosar.org/standards/adaptive-platform

[16] Scalable Open Architecture for Embedded Edge (SOAFEE). [Online]. Available: https://www.soafee.io/

[17] E. S. D. V. W. Group. (2024) Eclipse sdv working group charter. Accessed: 2024-07-05. [Online]. Available: https://www.eclipse.org/org/workinggroups/sdv-charter.php

[18] The Connected Vehicle Systems Alliance (COVESA). [Online]. Available: https://covesa.global/

[19] 5GAA, "A Visionary Roadmap for Advanced Driving Use Cases, Connectivity Technologies, and Radio Spectrum Needs," Online Article, Nov. 2022, available via CrossRef.

[20] Qualcomm Research, "3GPP Rel. 17: To Bring New System Capabilities and Expand 5G to New Devices, Applications, and Deployment. Completing the First Phase of the 5G Evolution," Online Article, Mar. 2022, available via CrossRef.

[21] B. An, J. P. Jeong, and S. A. Jang, "Interface to In-Network Computing Functions for Cooperative Intelligent Transportation Systems," Internet-Draft, draft-ahn-opsawg-i2icf-cits-00, Mar. 2025, Work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ahn-opsawg-i2icf-cits/

[22] I. Kunze, K. Wehrle, D. Trossen, M. Montpetit, X. de Foy, D. Griffin, and M. Rio, "Use Cases for In-Network Computing," Internet-Draft, draft-irtf-coinrg-use-cases-07, Dec. 2024, Work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-irtf-coinrg-use-cases-07

[23] J. P. Jeong, Y. Shen, Y. Ahn, Y. Kim, E. P. D. Jr., and K. Yao, "Interface to In-Network Computing Functions (I2ICF): Problem Statement," Internet-Draft, draft-jeong-opsawg-i2icf-problem-statement-00, Mar. 2025, Work in Progress. [Online]. Available: https://datatracker.ietf.org/api/v1/doc/document/draft-jeong-opsawg-i2icf-problem-statement/

[24] K. Yao, X. Shiping, Y. Li, H. Huang, and D. Kutscher, "Collective Communication Optimization: Problem Statement and Use cases," Internet-Draft, draft-yao-tsvwg-cco-problem-statement-and-usecases-00, Oct. 2023, Work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-yao-tsvwg-cco-problem-statement-and-usecases-00

[25] D. Lopez, E. Lopez, L. Dunbar, J. Strassner, and R. Kumar, "Framework for Interface to Network Security Functions," RFC 8329, Feb. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8329

[26] ATHENA Framework, "ATHENA Framework Github," https://github.com/KETI-A/athena, 2024, accessed: 2025-04-02.

Authorized licensed use limited to: Sungkyunkwan University. Downloaded on September 06,2025 at 23:30:12 UTC from IEEE Xplore. Restrictions apply.