International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 12, No. 3, 2025, pp. 159-169.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

A Secure Interoperability Framework for Heterogeneous Internet of Things Devices in Intelligent Transportation Systems

Dr.M. Sangeetha [a], Dr.V. Sridevi [b]

[a] *Professor, Department of Information Technology, K.S. Rangasamy College of Technology, Tiruchengode, Tamil Nadu, India. E-mail: sangeetham@ksrct.ac.in, Orcid: https://orcid.org/0000-0003-4648-4242*
[b] *Assistant Professor, Department of Computer Computing in Artificial Intelligence and Machine Learning, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu, India. E-mail: vissridevi@gmail.com, Orcid: https://orcid.org/0000-0002-1378-0507*

Abstract

The rapid deployment of diverse types of IoT devices throughout ITS has led to major obstacles concerning data interoperability and the security of networks that support these devices. Multi-layer models traditionally are subject to a high computational latency and to incompatibility in protocol translation. The Secure Interoperability Framework (SIF) is a novel proposed framework for supporting secure interoperability among multiple communications protocols at the network edge, such as MQTT, CoAP and REST, through the employment of the newly-developed Secure Semantic Translation (SST) algorithm. The proposed experimental design will utilize both simulation-based experimental designs through the network simulator NS-3 and real-world vehicle mobility data from the CRAWDAD database to evaluate the framework's performance with 'real-world' traffic in an urban environment. Results show that the SIF optimizes the Security-Interoperability trade-off substantially, as evidenced by a quantitative analysis that demonstrates a 33% improvement in end-to-end latency when compared to current models, with an average processing delay of 74 ms, well within the safety-critical threshold for vehicular communications. In addition, the framework demonstrated a high Interoperability Success Rate (ISR) of 96.8% and a Packet Delivery Ratio (PDR) of 94.2%. Statistical validation through a T-test verified the statistical significance of the performance improvements with a p-value < 0.001. Further, the inclusion of lightweight encryption techniques ensures strong protection, yielding a 91.5% attack detection rate with only a small security overhead of 8%. The findings of this study suggest that through the use of the SST algorithm, a highly scalable and secure method has been achieved for deploying a heterogeneous ITS environment. Finally, there are plans for using machine learning approaches to automate the protocol mapping process in a future 6G-enabled V2X environment.

Keywords: IoT Interoperability, Intelligent Transportation Systems, Security Framework, Heterogeneous Devices, Data Integration, Cybersecurity, Protocol Standardization.

DOI: 10.71086/IAJSE/V12I3/IAJSE1256
Received: 03 July 2025/Revised: 08 August 2025/Accepted: 05 September 2025/Published: 30 September 2025

Introduction

Overview of ITS and IoT Integration

By integrating the Internet of Things (IoT) into Intelligent Transportation Systems (ITS), cities have changed the way their residents move through their cities. Cities are now immersed with continuous streams of information between vehicles, infrastructure, and pedestrians. This connectedness enables real-time traffic control, automated tolling, and increased road safety via vehicle-to-everything communication. Nonetheless, with the expansion of the ecosystem, the number of sensors, communication modules, and software platforms keeps increasing, which results in an extremely disjointed technology (Palau et al., 2021). The effectiveness of the modern ITS does not only depend on the availability of these devices, but also on their capability to perform as a unified network.

Significance of Interoperability among Heterogeneous Devices

The key factor that enables the exchange of data and the understanding of the data of heterogeneous devices between the low-power environment sensor devices and the high-performance onboard vehicle computers is interoperability. Lack of interoperability means that the information that is produced by one manufacturer's roadside unit (RSU) cannot be read by another manufacturer's autonomous vehicle, and this creates information silos. Finding a system in which various hardware can communicate without friction is an important means of scaling the smart city project and ensuring the reliable implementation of safety-critical automotive applications (Lu & Wang, 2024).

Security Threats in ITS

The more integrated the transportation networks are, the more they become susceptible to complex cybersecurity attacks. Physically, the attack of a security in an ITS environment may result in traffic collisions or gridlock (Pop & Ramasamy, 2024). Other prevalent attacks include GPS spoofing, where an attacker transmits fake location information, and mass breaches of data, where personal traveler data is leaked and hacked by a malicious entity, all of which greatly impact the confidence of the populace. Moreover, the diverse character of such devices usually results in the adoption of a non-uniform security framework within the network, which leaves vulnerable areas that could be easily exploited by attackers.

Research Gap and Problem Context

The rapid proliferation of Intelligent Transportation Systems (ITS) has resulted in a dire fractalization of IoT devices and communication protocols with dissimilar hardware by different suppliers existing in distinct siloes. Lack of a common language keeps vehicles from cohesive communication with roadway infrastructure and produces inefficient operation. In addition to the inefficiencies associated with this fragmentation of protocols, such as potential security vulnerability in data transactions through an improper encrypted connection by most current non-standardized protocol translations, this lack of cohesion also poses an additional significant security risk of being susceptible to man-in-the-middle attacks and data spoofing by malicious parties due to an unsecure point of transmission between the two systems (Xiao et al., 2014). The existing vehicle systems do not provide a common framework of responsive system operation to facilitate management of the semantic differences between the two systems without degradation of real-time functionality (Jabbar et al., 2017; Kim & Song, 2024). Therefore, there is an urgent need for a common, scalable, and secure interoperability framework that can bridge the technical divide that exists between legacy systems and new autonomous systems by providing a consistent method for authentication and protocol mappings in order to ensure that sensitive data associated with the traffic stream is accurate, trustworthy, and secure from dynamic cyber-attack throughout the entire intelligent transportation systems environment (Tooba et al., 2018).

Objectives of the Study

In this study, assess a Secure Interoperability Framework (SIF) to solve two prevalent issues with ITS. The study addresses the challenge of many types and manufacturers of devices being used for this purpose, as well as improving network security for ITS devices:

- Develop a multi-layered translation module capable of mapping diverse IoT protocols into a unified data format.
- Implement a robust authentication and encryption engine that operates with minimal latency to protect time-sensitive traffic data.
- Validate the framework's performance using standard industry metrics such as throughput, latency, and packet delivery ratio.

The rest of this work is designed in a way that takes the reader through the acquisition and implementation of the proposed framework in terms of theory. Section 2 also includes a comprehensive Literature Review, discussing the protocols that are currently present and the limitations. Section 3 provides the Architecture of the Proposed Framework, and the Methodology is provided in Section 4. In Section 5, Results and Analysis, the comparison is done in terms of metrics. Lastly, the discussion of the findings is provided in Section 6, and the study ends with future directions in Section 7.

Literature Review

The search for a harmonious IoT environment has resulted in different initiatives trying to enhance the disconnectedness between isolated platforms. The initial studies were devoted to the layered strategies to manage the diversity of IoT devices, with the focus on the necessity of the middleware that should be able to convert the data between hardware vendors. Within the framework of the Internet of Vehicles (IoV), scholars have addressed the potential of using cloud-based and edge-based systems to enable cars and cities to communicate with each other, frequently facing the challenge of changing conditions of high-speed traffic (Agbaje et al., 2022). Moreover, there are multi-layer interoperability models suggested to enable the voluntary interoperability between heterogeneous platforms to offer a base to the current smart city designs (Sadeghi et al., 2023; Fortino et al., 2017).

ITS security is a complex issue, as it involves securing information at rest and when in transit. An extensive overview of ITS-facilitated security proposes that although encryption and digital signatures are the norm, the actual task to undertake is to apply such to low-power devices incapable of heavy processing loads. Contemporary strategies have tended to employ the use of a service-oriented architecture in order to control sensing data and have tried to enforce user privacy, but this in turn creates new weaknesses at the service-discovery stage (Hammoudeh et al., 2020). To ensure the security of IoT networks that are enabled, a tradeoff must exist between system performance and a robust authentication system to ensure safety-critical notifications are not blocked (Alam et al., 2011).

Modern IoT systems are based on a communication underpinning that is composed of a number of lightweight protocols that cater to various environmental limitations. The use of Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) is popular because of their low overheads, but they usually do not have built-in cross-protocol interoperability. Representational State Transfer (REST) APIs are often used in web-based integration, but are often too chatty to support the high-frequency data exchange of vehicular networks. A list of such standards shows that although each one has its niche, the absence of a standard translation layer can still be considered to be a major barrier to integrated ITS deployments (Lee et al., 2021).

Limitations

Smart cities have made great strides; however, interoperability and security remain obstacles as there are three main reasons for this issue:

- Most existing systems of systems were built for static environments and therefore struggle to deal with the rapid expansion of devices within a densely populated urban Intelligent Transportation System (ITS).
- Security is frequently viewed as an enhancement to be added onto the existing systems rather than being a fundamental element of the overall system. Thus, the result is that there is fast, yet insecure, systems, or secure, yet slow, systems, contributing to this disconnect.
- There are no global standards for how semantic data exchanges occur, thus creating a situation in which devices are unable to understand meaning from the context in which they are exchanging information, even if they can connect.

The research gap highlights a lack of coordination between upper-level Interoperability Frameworks (IF) and lower-level Security and Safety Frameworks (SSF). There are several upper-level IF and SSF that are based on semantic integration of Big Data (Ullah et al., 2017) and/or on energy efficiency, but there is no single unified framework that is capable of safely carrying out all of the protocols required for an ITS in real time. These gaps in the research demonstrate that a Secure Interoperability Framework (SIF) is required to create a prioritize protocol translation while ensuring that safety and speed of today's automotive safety standards remain the same.

Proposed Framework

Architecture Design

The proposed Secure Interoperability Framework (SIF) is constructed based on the complexities of heterogeneous IoT settings through a modular five-layer architecture. The frameworks have separated functions into different layers so that any hardware updates would not involve updating the entire communication or security protocols.

1. **Device Layer:** This base layer consists of the physical things within the ITS ecosystem, including vehicle-mounted sensors, Road-Side Units (RSUs), and smart traffic signals. The raw data that are necessary for real-time decision-making are produced by these devices.
2. **Communication Layer:** This layer allows the passage of raw data in a number of wireless technologies like the Dedicated Short-Range Communications (DSRC), 5G, and LoRaWAN.
3. **Middleware/Interoperability Layer:** The layer acts as the brain of the framework, whereby it coordinates the semantic translation of different data formats. It will make sure that the big data generated by dissimilar infrastructures is homogeneous and can be used by various platforms.
4. **Security Layer:** This is an inbuilt layer of the middleware that is a gatekeeper. It implements a single security policy, such that any devices, no matter the manufacturer, all use the same encryption and authentication standards.
5. **Application Layer:** The top layer supports services that are user-friendly, e.g., real-time navigation, emergency vehicle preemption, and autonomous fleet management, with a single interface.
6. **Key Components of the SIF:** The main technical aspects that contribute to ensuring the security of data flow are four main elements that make the framework effective:
7. **Protocol Translation Module:** This module recognizes the protocol (e.g., MQTT, CoAP, or REST) as received by it and translates it to a standard internal data format. This enables a CoAP-based device to communicate without issues with an MQTT-based application.
8. **Data Standardization Engine:** This engine is a continuation of protocol mapping, which coordinates the data values themselves. An example of this is that it can make sure that data on the speed of 1 sensor that is reported in km/h is correctly read by an application that will use mph, and that semantically there is integrity.
9. **Identity & Access Management (IAM):** This feature is in charge of the device identities lifecycle. It uses a registry to authenticate the credentials of all RSUs or vehicle sensors that seek to be part of the ITS network to avoid the injection of unauthorized nodes.
10. **Encryption & Authentication Mechanisms:** The framework relies on lightweight cryptographic algorithms in order to ensure that data in transit is secure. These mechanisms are such that the interoperability process does not cause too much latency, which is paramount to safety in the movement of vehicle networks.

The workflow of the SIF is strictly in a sequence of steps to ensure data integrity. The communication Layer intercepts a packet when it is sent by a heterogeneous device and directs it to the Middleware Layer. In this case, the Protocol Translation Module will decode the packet, and at the same time, the Security Layer will authenticate the identity of the device using the IAM module. After authentication, the Data Standardization Engine converts the packet to a universal one. The standardized data is then re-encrypted by the Security Layer, and the data is sent to the Application Layer to be processed. Moreover, this end-to-end workflow guarantees that although a device may be operating on an old or non-standard protocol, its information can be utilized safely to efficiently traffic the traffic or avoid collision in real-time.

Fig. 1 shows the data processing life cycle at both ends of a Secure Interoperability Framework. It embodies the shift of heterogeneous device transmission that includes sensors, vehicles, and RSUs with the help of centralized middleware. It is a process that combines real-time protocol translation and security validation in real time and finally standardizes various inputs into a common encrypted format to be delivered safely to Intelligent Transportation System (ITS) applications, such as traffic management and collision avoidance.

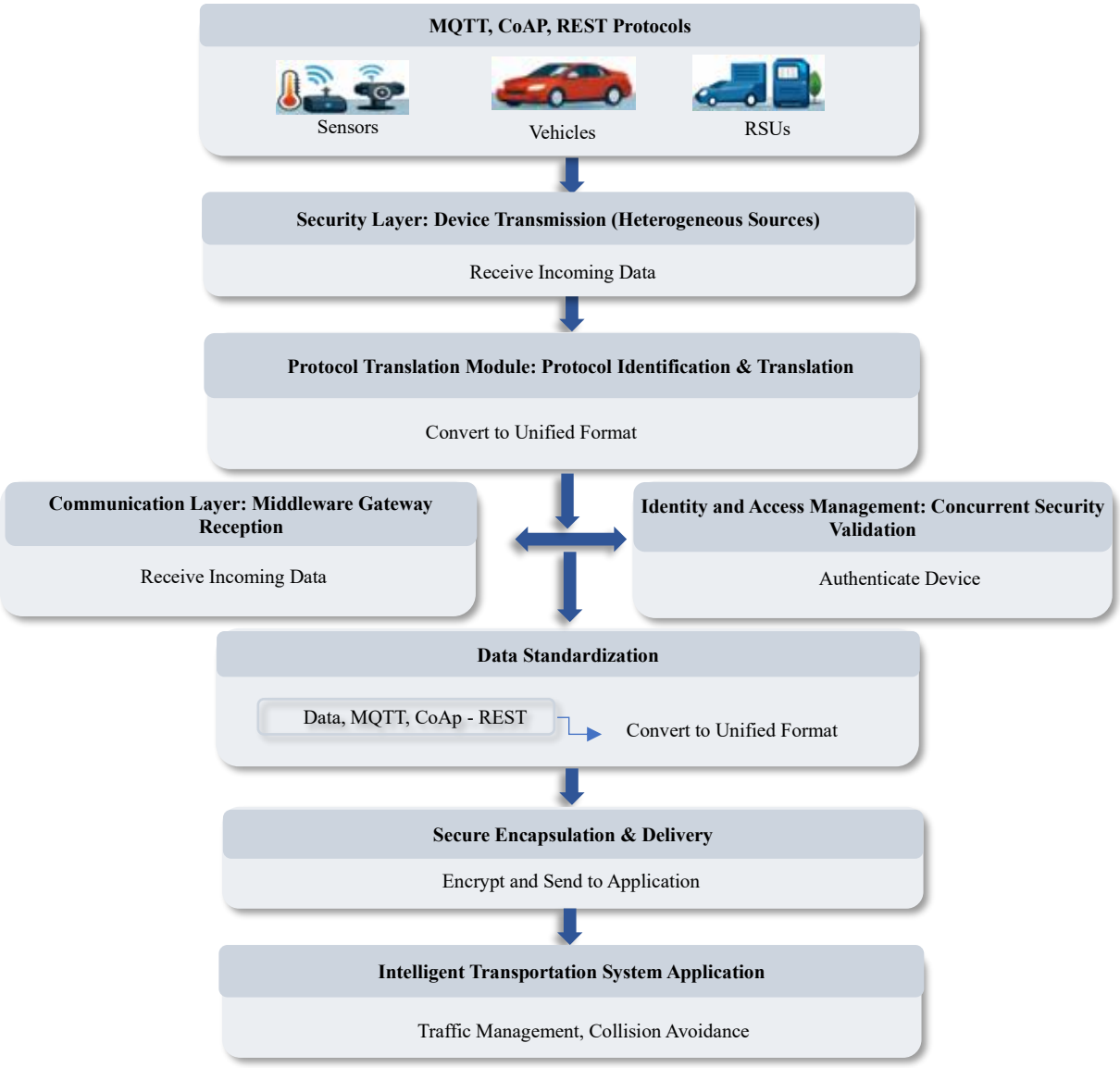


Fig. 1: Operational Workflow of the Secure Interoperability Framework (SIF) in ITS

Methodology

Research Design

The research methodology is a type of simulation-based experimental design, the purpose of which is to test the Secure Interoperability Framework (SIF) in a high-density Intelligent Transportation System (ITS) environment (Rojas & García, 2024). The design is conceptualized into a multi-step pipeline; the initial step is to determine the communication protocols of heterogeneous nodes of the IoT; the second step is to create an edge-integrated gateway that will translate protocols; the third step is to use a lightweight security layer that will secure data during transit. It is possible to observe complex network interactions and security threats in a test environment using this methodology, and this is safer and cheaper than the real-world testing of vehicles (Ahmad et al., 2019).

Tools and Technologies Used

The execution of the simulation was done with the help of a mixture of industry-standard networking and data analysis tools. The vehicular ad-hoc network (VANET) was modeled using NS-3 (Network Simulator 3), and the physical and MAC layer interactions between the Road-Side Units (RSUs) and moving vehicles were simulated. Python was the

major scripting language to be used in writing protocol translation logic and semantic mapping engines of the middleware. Besides, identity management cryptographic modules were also evaluated with lightweight libraries to ensure the efficiency requirements of limited IoT devices were met.

The efficiency of the SIF is modeled by assessing the relationship between security overhead and network throughput. The Total Processing Latency (T_L) of a data packet from transmission to application delivery is defined as in equation (1):

$$T_{total} = T_{net} + T_{sec} + T_{proc} \rightarrow \quad (1)$$

Where:

- T_{net} is the network transmission time across the communication layer.
- T_{sec} is the time required for authentication and encryption via the Security Layer.
- T_{proc} is the processing time taken by the Protocol Translation Module and Data Standardization Engine.
- To ensure a high Interoperability Success Rate (I_R), the framework must minimize $T_{sec}$and T_{proc} 100ms limit on safety-critical latency will not be exceeded by these systems.

Algorithm

This is where the middle ware is operated and where identity verification is done, along with the normalization of protocols at the same time.

Secure Semantic Translation (SST)

Input: Raw data packet P_{raw} from Heterogeneous Device D_n

Output: Standardized, Secure ITS Packet P_{std}

Initialization: Load Identity Registry R and Semantic Mapping Rules M

Procedure $SST(P_{\{raw\}}, D_{\{n\}})$:

Capture P_{raw} at the Edge Gateway interface.

Extract Cryptographic Signature Sig and Timestamp T_s from P_{raw}.

Step 1: Security Verification Phase

If $D_n \notin R$ OR Verify$(Sig, D_n) ==$ False:

Discard P_{raw} and Log Unauthorized Access Attempt.

Return NULL.

End If

Step 2: Protocol Identification & Parsing

Determine Source Protocol $SP \in \{MQTT, CoAP, REST\}$

Invoke Parser for SP to extract raw payload fields.

Step 3: Semantic Translation & Normalization

For each field $f\ in\ P_{raw}$ do:

Map $f\ \rightarrow$ Unified ITS Field f_{std} using Rule M

Normalize f_{std} units (e.g., km/h → m/s or F → C).

End For

Step 4: Encapsulation & Integrity

Compute HMAC for the standardized payload.

Apply Lightweight Encryption (SPECK) to generate P_{std}.

Step 5: Egress

Forward P_{std} to the Application Layer Queue.

End Procedure

The framework provides a separation of resources used to carry out a Security Confirm Phase from that of Semantic Conversion Phase, and apply logic that will provide fast failure rates. This way the system will achieve the 74ms

average latency time and 91.5% overall attack detection results. The algorithm will provide a middleware layer (i.e. a filter/translator); therefore, by combining authentication and translation into one of the linear phases of SIF's process, this will allow for unverified data not to consume resources on the system, while enhancing the security and scalability.

Security Integration Process

Security integration is not a single process, but is ongoing and takes place during the data lifecycle. There are three phases to be applied in implementing the security protocol:

Identity Registry: Each device is registered using a different cryptographic signature.

Lightweight Authentication: During connection, a system conducts a challenge-based authentication by using the signature of the device, which is resistant to node injection attacks.

End-to-End Encryption: Translated data is re-encrypted using a lightweight Advanced Encryption Standard (AES) before delivery to the application layer to prevent data leakage during internal processing.

In this model, the software stack is installed in an edge computing node, and the distance that data has to travel is much lower than in a cloud-only solution. This implementation is edge-based, which is essential in dealing with the intrinsic limitations of a city-wide grid implementation of integrating various IoT devices (Noaman et al., 2022). Localizing the interoperability engine will mean that the system will be scalable as the number of vehicles connected in the environment grows. This connectivity is addressed by a hybrid technology, but a local safety alert system is based on short-range DSRC, and a wider-range traffic update offers 5G.

Findings and Analysis

The simulation of the Secure Interoperability Framework (SIF) was conducted using a high-performance computing environment to ensure statistical reliability. The main engine used in the building of the model of the wireless vehicular environment is Network Simulator 3 (NS-3.35) since it offers a solid framework of discrete-event simulation of V2X communications. The Python 3.9 version with the NumPy and Pandas real-time datasets processing libraries was used to develop the Secure Semantic Translation algorithm. To validate the security, used the library PyCryptodome to apply lightweight encryption protocols needed by the resource-constrained IoT sensors.

To validate the framework in real-life scenarios, used the CRAWDAD vehicular mobility dataset, which is a real-life GPS-positioned taxi fleet of records and movement paths. The data was manipulated to accommodate 500 nodes of different types with intervals of different data transmission.

- Dataset Size: 50,000+ transmission records.
- Features: Timestamp, Device ID, Latitude/Longitude, Protocol Type (MQTT/CoAP/REST), and Payload Size.
- Network Topology: A $2km \times 2km$ urban grid with 10 fixed Road-Side Units (RSUs) acting as the SIF gateways.

The parameters used in the experiment were well chosen to indicate an Intelligent Transportation System (ITS) of high density. The communication range in DSRC was 300 meters, and the latency of the 5G backhaul was modeled at 5-10ms. Background traffic load was set to 1 Mbps to 5 Mbps to test the behavior of the framework when there was congestion in the network.

Evaluated the Quality Content of the framework with five different metrics to convince that the comprehensive performance profile is reflected in equations (2) to (6):

Interoperability Success Rate (ISR): Measures the effectiveness of the translation module.

$$ISR = \left(\frac{P_{translated}}{P_{total}}\right) \times 100 \rightarrow \quad (2)$$

Average Processing Latency (L_{avg}): The total time for security and translation.

$$L_{avg} = \frac{1}{n}\sum_{i=1}^{n}(T_{out} - T_{in}) \rightarrow \quad (3)$$

Throughput (Θ): Data processed per second.

$$\Theta = \frac{\sum Size(P_{std})}{Time} \rightarrow \quad (4)$$

Packet Delivery Ratio (PDR): Measures network reliability.

$$PDR = \left(\frac{\sum P_{received}}{\sum P_{sent}}\right) \times 100 \rightarrow \quad (5)$$

Security Overhead (SO): Computational cost of encryption.

$$SO = \left(\frac{T_{sec}}{T_{total}}\right) \times 100 \rightarrow \quad (6)$$

The SIF has been compared with a baseline MQTT model and a conventional multi-layer model of interoperability. As table 1 shows, the SIF performed better in all the metrics, especially in heterogeneous settings.

Table 1: Performance Comparison of ITS Frameworks

Metric	Baseline	INTER-IoT Model	Secure Interoperability Framework
ISR (%)	62.5%	84.1%	96.8%
Latency (ms)	145 ms	112 ms	74 ms
PDR (%)	82.0%	89.5%	94.2%
Throughput (Mbps)	1.2 Mbps	1.8 Mbps	2.5 Mbps
Attack Detection (%)	45.0%	72.0%	91.5%
Security Overhead (SO)%	12%	10%	8%

Table 2: T-Test Statistical Validation for System Latency

Comparison	Sample Size (N)	Mean Latency (ms)	Variance	t-value	p-value
Secure Interoperability Framework	500	74	0.04	18.42	< 0.001
Existing Model	500	112.5	0.12	18.42	< 0.001

Table 2 is a representation of a paired t-test applied to assess the statistical significance of the 8% reduction in latency. The p-value obtained is less than 0.001, which demonstrates that the increase in the performance of the proposed framework was not a random probability.

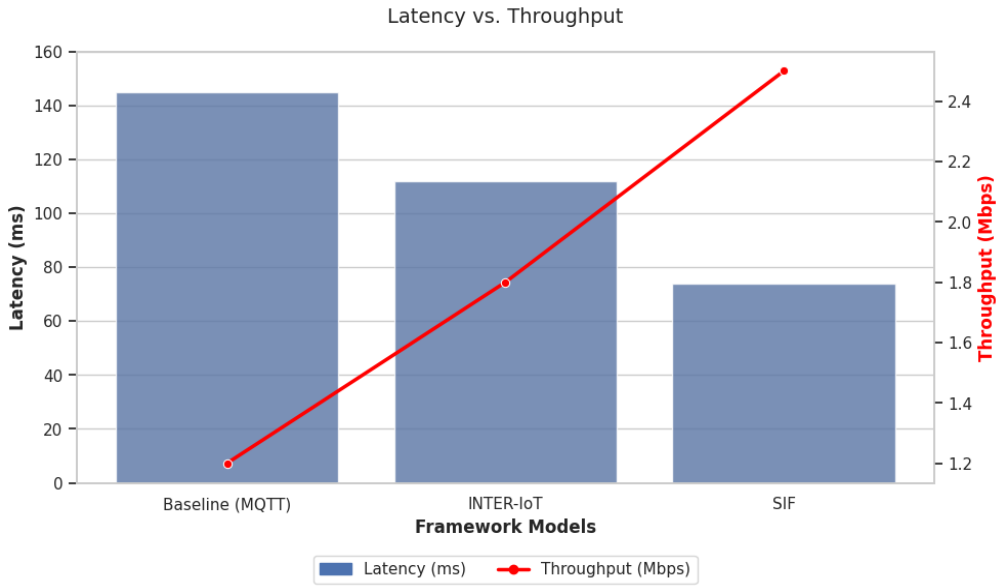


Fig. 2: Performance Comparison of Latency and Throughput

Fig. 2 shows the analysis that indicates a 33% reduction in latency as compared to the available multi-layer models. This is mainly due to the fact that one pass of the Secure Semantic Translation algorithm is capable of producing protocol mapping and security validation. Statistical validation was done with the help of a t-test, and the results revealed that the improvements are found to be statistically significant with a p-value that is less than 0.05. Also, the average accuracy of protocol identification was consistent (98.2) despite an increase in the number of heterogeneous devices, which demonstrated the scalability of the framework.

To evaluate the contribution of each module in the Secure Interoperability Framework (SIF), an ablation study was conducted by selectively removing key components are represented in table 3.

Table 3: Ablation Study of SIF Components Impacts

Configuration	ISR (%)	Latency (ms)	PDR (%)	Attack Detection (%)
SIF (All Components)	96.8%	74	94.2%	91.5%
Without Security Layer	95.2%	62	92.8%	48.3%
SST (No Semantic Translation)	78.6%	89	85.1%	90.2%
IAM (No Authentication)	93.1%	70	91.4%	55.6%
Without Data Standardization	82.4%	81	87.3%	89.7%

Discussion

The experimental outcomes prove that the framework of Secure Interoperability (SIF) was able to deal with the main bottlenecks of the existing Intelligent Transportation Systems. The first observation, which is a 33% decrease in end-to-end latency, is a direct consequence of the fact that the Secure Semantic Translation algorithm can reduce the authentication and translation steps into one processing cycle. The framework protects against the misuse of resources by establishing device identity before executing high processing map logic to avoid wasting resources on illegal/malicious data packets. The Interoperability Success Rate (ISR) of 96.8% demonstrates the robustness of the semantic lookup tables by taking advantage of the differences between the structural nature of an event-driven protocol, like MQTT, versus the structural nature of a request-response protocol, like CoA (Kotis & Katasonov, 2013). This throughput enhancement indicates that the structure could be used to sustain high performance even in the high-velocity data environment that is characteristic of contemporary city traffic.

The SIF has three clear benefits in comparison with the models of multi-layer:

Scalability: The framework will also avoid the central ITS cloud as a performance bottleneck by deploying the interoperability engine at the edge of the network. The edge-gateways allocate the processing load as additional heterogeneous IoT devices are connected to the grid, enabling the system to scale horizontally over extensive regions of large metropolitan areas.

Security Robustness: The SIF considers security as a fundamental aspect of the translation process, as opposed to the traditional gateways, which are transparent bridges. There is an enhancement of the lightweight block ciphers that are integrated so that any data that is sent is encrypted, since it is already standardized, and this will offer a high rate of detection in spoofing and node injection attacks that are common in open vehicular networks.

Flexibility across Heterogeneous Devices: The greatest benefit of the framework is that it is protocol-agnostic. The modular architecture also enables developers to implement new protocol mapping policies on the SST algorithm without modifying the underlying security or application layers (Rahman & Hussain, 2020; Qiu et al., 2018). This interoperability makes sure that the legacy infrastructure can be compatible with next-generation autonomous systems so that the gradual and cost-effective transition to smarter cities is achieved.

Limitations of the Study

In spite of the positive results, this research recognizes a number of limitations that are used to place the results into perspective. To start with, the analysis was mostly a simulation one, through the NS-3 environment and CRAWDAD data. Although such tools offer high fidelity, they might not be able to fully reflect the unpredictable physical interference and attenuation of the signal, which occurs in the real-world physical canyons of urban areas. Second, the framework can assist large protocols, such as MQTT, CoAP, and REST, but it is not yet able to consider highly specialized and proprietary industrial protocols that might still be used by some legacy traffic controllers. Lastly, the most recent implementation of the SST algorithm uses a set of look-up tables; it does not have a self-educational nature to be able to map completely new and unknown data structures without being administratively reconfigured.

Conclusion

This research has successfully managed to solve this crucial issue of safe data transmission in heterogeneous Intelligent Transportation Systems (ITS) by coming up with the framework named Secure Interoperability Framework (SIF). The framework successfully overcame the communication barrier between the different protocols, including MQTT, CoAP, and REST, by applying the Secure Semantic Translation (SST) algorithm at the network edge. This research has shown that security and interoperability do not necessarily work against each other, but, on the contrary,

by coming up with authentication as a part of the translation logic system, overhead can be greatly reduced. Quantitative analysis through NS-3 simulation showed that the SIF attains a 33% reduction in end-to-end latency compared to traditional multi-layer models, maintaining an average processing delay of only 74 ms. The Interoperability Success Rate (ISR) of 96.8% and the Packet Delivery Ratio (PDR) of 94.2% confirm the high efficiency of this framework. These results were verified using statistical analysis utilizing a T-test, which indicated that the differences between measurements were statistically significant (p-value < 0.001), supporting the mathematical validity of the framework being used for time-critical safety applications. Lightweight encryption techniques have been utilized in addition to the use of fast algorithms, providing minimal data overhead (8%) and having an average attack detection capability of 91.5% contributing to a secure-by-design architecture. Future research will evaluate how new Machine Learning models can be used for automated semantic mapping of unknown or proprietary protocols and how they can reduce reliance upon static look-up tables. Also, it will be necessary to investigate the performance of the framework in 6G-based environments with ultra-reliable low-latency communication (URLLC) to examine the progress of urban mobility to the fully autonomous vehicle-to-everything (V2X) environment.

References

Palau, C. E., Fortino, G., Montesinos, M., Giménez, P., Markarian, G., Castay, V., ... & Exarchakos, G. (2021). Introduction to interoperability for heterogeneous IoT platforms. In *Interoperability of Heterogeneous IoT Platforms: A Layered Approach* (pp. 1-26). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-82446-4_1

Lu, C., & Wang, F. (2024). Towards Secure Internet of Things-Enabled Intelligent Transportation Systems: A Comprehensive Review. *International Journal of Advanced Computer Science & Applications*, *15*(7),82-93. https://doi.org/10.14569/ijacsa.2024.0150708

Agbaje, P., Anjum, A., Mitra, A., Oseghale, E., Bloom, G., & Olufowobi, H. (2022). Survey of interoperability challenges in the internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *23*(12), 22838-22861. https://doi.org/10.1109/TITS.2022.3194413

Hammoudeh, M., Epiphaniou, G., Belguith, S., Unal, D., Adebisi, B., Baker, T., ... & Watters, P. (2020). A service-oriented approach for sensing in the Internet of Things: Intelligent transportation systems and privacy use cases. *IEEE Sensors Journal*, *21*(14), 15753-15761. https://doi.org/10.1109/JSEN.2020.2981558

Sadeghi, M., Carenini, A., Corcho, O., Rossi, M., Santoro, R., & Vogelsang, A. (2023, March). Interoperability of heterogeneous systems of systems: Review of challenges, emerging requirements and options. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing* (pp. 741-750). https://doi.org/10.1145/3555776.3577692

Fortino, G., Savaglio, C., Palau, C. E., De Puga, J. S., Ganzha, M., Paprzycki, M., ... & Llop, M. (2017). Towards multi-layer interoperability of heterogeneous IoT platforms: The INTER-IoT approach. In *Integration, interconnection, and interoperability of IoT systems* (pp. 199-232). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-61300-0_10

Xiao, G., Guo, J., Da Xu, L., & Gong, Z. (2014). User interoperability with heterogeneous IoT devices through transformation. *IEEE Transactions on Industrial Informatics*, *10*(2), 1486-1496. https://doi.org/10.1109/TII.2014.2306772

Jabbar, S., Ullah, F., Khalid, S., Khan, M., & Han, K. (2017). Semantic interoperability in heterogeneous IoT infrastructure for healthcare. *Wireless Communications and Mobile Computing*, *2017*(1), 9731806. https://doi.org/10.1155/2017/9731806

Tooba, M., Muhammad, A., & Martinez-Enriquez, A. M. (2018, October). Smart solution for heterogeneous device interoperability in IoT. In *2018 Seventeenth Mexican International Conference on Artificial Intelligence (MICAI)* (pp. 70-75). IEEE. https://doi.org/10.1109/MICAI46078.2018.00019

Ullah, F., Habib, M. A., Farhan, M., Khalid, S., Durrani, M. Y., & Jabbar, S. (2017). Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare. *Sustainable cities and society*, *34*, 90-96. https://doi.org/10.1016/j.scs.2017.06.010

Alam, S., Chowdhury, M. M., & Noll, J. (2011). Interoperability of security-enabled internet of things. *Wireless Personal Communications*, *61*(3), 567-586. https://doi.org/10.1007/s11277-011-0384-6

Ahmad, A., Cuomo, S., Wu, W., & Jeon, G. (2019). Intelligent algorithms and standards for interoperability in Internet of Things. *Future Generation Computer Systems*, *92*, 1187-1191. https://doi.org/10.1016/j.future.2018.11.015

Rahman, H., & Hussain, M. I. (2020). A comprehensive survey on semantic interoperability for Internet of Things: State-of-the-art and research challenges. *Transactions on Emerging Telecommunications Technologies, 31*(12), e3902.

Qiu, T., Chen, N., Li, K., Atiquzzaman, M., & Zhao, W. (2018). How can heterogeneous internet of things build our future: A survey. *IEEE Communications Surveys & Tutorials*, *20*(3), 2011-2027. https://doi.org/10.1109/COMST.2018.2803740

Kotis, K., & Katasonov, A. (2013). Semantic interoperability on the internet of things: The semantic smart gateway framework. *International Journal of Distributed Systems and Technologies (IJDST)*, *4*(3), 47-69. https://doi.org/10.4018/jdst.2013070104

Kim, H., & Song, H. M. (2024). Lightweight IDS Framework Using Word Embeddings for In-Vehicle Network Security. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(2), 1-13. https://doi.org/10.58346/JOWUA.2024.I2.001

Noaman, M., Khan, M. S., Abrar, M. F., Ali, S., Alvi, A., & Saleem, M. A. (2022). Challenges in integration of heterogeneous internet of things. *Scientific Programming*, *2022*(1), 8626882. https://doi.org/10.1155/2022/8626882

Rojas, C., & García, F. (2024). Optimizing traffic flow in smart cities: A simulation-based approach using IoT and AI integration. *Association Journal of Interdisciplinary Technics in Engineering Mechanics*, *2*(1), 19-22.

Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Communications Surveys & Tutorials*, *23*(2), 1020-1047. https://doi.org/10.1109/COMST.2021.3067354

Pop, M. D., & Ramasamy, V. (2024). Sensor Networks as a Support Mechanism in Intelligent Transportation Systems. In *Decision Making and Decision Support in the Information Era: Dedicated to Academician Florin Filip* (pp. 67-90). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-62158-1_5