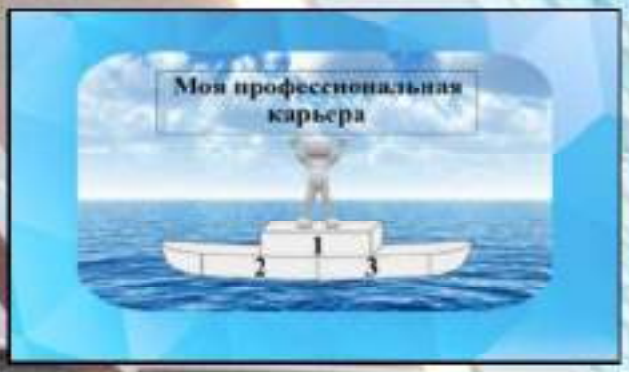


ISSN INTERNATIONAL STANDARD SERIAL NUMBER
ISSN 2782-4365
Проверить номер:

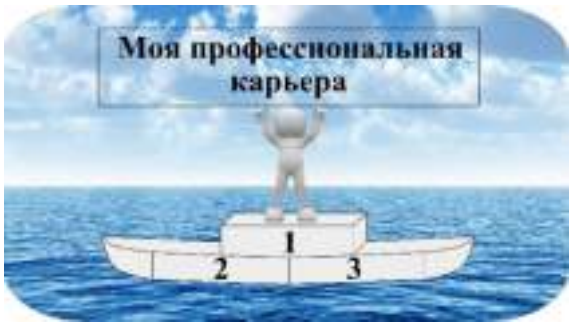
Научно-образовательный электронный журнал

ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ

Выпуск №67-2 (том 2)
(октябрь, 2025)

Google Scholar
Проверить индексацию статьи. Сайт: mpcareer.ru/google

Периодичность выпуска: 1 раз в неделю
Сайт: mpcareer.ru/oinv21veke. Почта: obrmpcareer@mail.ru



Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ»

ISSN 2782-4365
УДК 37
ББК 94

Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №67-2 (том 2) (октябрь, 2025). Дата выхода в свет: 13.10.2025.

Журнал объединяет авторов на территории стран СНГ и помогает обмениваться передовыми научно-образовательными исследованиями.

Содержит научные статьи отечественных и зарубежных авторов по экономическим, техническим, философским, юридическим и другим наукам.

Миссия научно-образовательного электронного журнала «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ» состоит в поддержке интереса читателей к оригинальным исследованиям и инновационным подходам в различных тематических направлениях, которые способствуют распространению лучшей отечественной и зарубежной практики в интернет пространстве.

Целевая аудитория журнала охватывает работников сферы науки и образования (педагоги, учителя, ученые, преподаватели, научные сотрудники, бакалавры, магистранты, аспиранты.

Материалы публикуются в авторской редакции. За соблюдение законов об интеллектуальной собственности и за содержание статей ответственность несут авторы статей. Мнение редакции может не совпадать с мнением авторов статей. При использовании и заимствовании материалов ссылка на издание обязательна.

ФИО автора(-ов): *Agajanov. S.*
Student, Institute of Telecommunications and
Informatics of Turkmenistan
Saryyev. N.
Lecturer, Institute of Telecommunications and
Informatics of Turkmenistan
Gurbanova. Sh.
Lecturer, Institute of Telecommunications and
Informatics of Turkmenistan
Ishangulyyeva. G.
Lecturer, Institute of Telecommunications and
Informatics of Turkmenistan
Название публикации: «ENHANCING CYBERSECURITY IN INTELLIGENT TRANSPORTATION SYSTEMS: CHALLENGES AND STRATEGIES FOR SAFE DATA COMMUNICATION»

Abstract

Intelligent Transportation Systems (ITS) represent the convergence of information technology, data communication, and transportation infrastructure, enabling more efficient and safer mobility. However, as these systems rely heavily on digital communication and interconnected networks, cybersecurity risks have become a critical concern. Ensuring safe data communication within ITS requires addressing vulnerabilities such as unauthorized data access, signal interference, and malicious attacks targeting vehicle-to-vehicle and vehicle-to-infrastructure communication. This paper explores the primary cybersecurity challenges in ITS, including system heterogeneity, weak encryption protocols, and data privacy issues. It also examines strategies for strengthening cybersecurity, focusing on encryption technologies, authentication mechanisms, intrusion detection systems, and policy frameworks. Through a methodological review of existing research, simulation models, and practical implementations, this study emphasizes the importance of integrated

cybersecurity strategies for ensuring reliability, trust, and resilience in intelligent transportation systems.

Methods and Methodology

The research was conducted using a qualitative approach supported by a comparative analysis of existing ITS cybersecurity frameworks. Peer-reviewed journal articles, technical reports, and case studies published between 2010 and 2025 were examined to identify common vulnerabilities and defense mechanisms in intelligent transportation networks. The data collection process involved reviewing literature from databases such as IEEE Xplore, ScienceDirect, and SpringerLink, focusing on topics including vehicle-to-everything (V2X) communication security, encryption algorithms, intrusion detection, and secure data transmission protocols.

Analytical methods were applied to evaluate and categorize existing cybersecurity challenges, while a systematic comparative analysis was performed to assess the efficiency of various protection strategies. Simulation-based studies and testbed experiments from documented ITS projects were also analyzed to evaluate the effectiveness of real-world cybersecurity implementations. The research design followed a descriptive and analytical structure, aiming to identify gaps and propose integrated security frameworks that can enhance data integrity and reliability within ITS. The methodology emphasized synthesizing theoretical and practical insights to develop a comprehensive understanding of cybersecurity strategies applicable to large-scale intelligent transportation networks.

Introduction

The evolution of transportation infrastructure into intelligent, interconnected systems revolutionized mobility management across the world. Intelligent Transportation Systems combined sensing technologies, artificial intelligence, and communication networks to optimize traffic flow, reduce congestion, and improve road safety. However, this technological advancement introduced complex cybersecurity challenges due to the dependence on real-time data exchange between vehicles, roadside units, and cloud servers. Cyberattacks in these networks could lead not only

to data breaches but also to physical harm through manipulated traffic signals or autonomous vehicle control systems.

Cybersecurity in ITS, therefore, became a central concern for engineers, policymakers, and researchers. The secure transmission of information among vehicles and infrastructures determined the reliability of the entire system. This research examined these concerns by analyzing both the challenges and the strategic defenses developed to safeguard data communication in intelligent transportation environments.

Evolution of Intelligent Transportation Systems

The development of ITS began in the late twentieth century with simple traffic management systems that evolved into data-driven, connected infrastructures. The introduction of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication technologies created a dynamic network capable of autonomous decision-making. However, the expansion of such systems introduced numerous entry points for cyber threats.

As ITS technologies progressed, the need for integrated cybersecurity mechanisms became evident. Data transmitted among vehicles and infrastructure included sensitive information such as location, identity, and control commands. If compromised, such data could disrupt entire networks or lead to fatal incidents. The historical development of ITS thus highlighted the critical interplay between technological innovation and security evolution. The research focused on understanding how early systems lacked defensive structures and how modern frameworks attempted to incorporate secure communication architectures at the design level.

Cybersecurity Challenges in Intelligent Transportation Systems

Cybersecurity threats in ITS stemmed from the interconnected nature of communication networks. The multiplicity of devices, sensors, and protocols created a heterogeneous environment where vulnerabilities could be exploited by attackers. Common challenges included denial-of-service attacks, false data injection, signal jamming, and spoofing of GPS or vehicle identifiers.

Another major challenge was the lack of standardized encryption across communication protocols. Many ITS components were developed by different manufacturers, leading to incompatibility between their security systems. Moreover, real-time communication requirements imposed strict latency constraints that sometimes discouraged the use of complex encryption algorithms. Consequently, ITS became vulnerable to fast, high-impact cyber intrusions.

The issue of privacy also emerged as a central concern. Vehicles continuously shared data related to their movement, speed, and location. If intercepted, this information could be misused for surveillance or malicious tracking. Addressing these multifaceted threats required comprehensive solutions that balanced security, efficiency, and privacy.

Data Communication Protocols and Vulnerabilities

Data communication formed the core of ITS functionality. Protocols such as Dedicated Short Range Communications (DSRC) and Cellular Vehicle-to-Everything (C-V2X) enabled real-time data exchange between network components. However, both communication standards exhibited vulnerabilities that attackers could exploit. For instance, DSRC transmissions were susceptible to eavesdropping and replay attacks, while C-V2X faced threats related to network congestion and identity spoofing.

Weaknesses in data authentication mechanisms further complicated the problem. Without robust verification of data sources, false messages could propagate rapidly within the network. Attackers could create fake messages simulating emergency braking alerts or road hazards, causing chaos among connected vehicles. Studies conducted on vehicular ad-hoc networks demonstrated that even short-term exposure to such falsified data could disrupt traffic flow and compromise public safety.

Addressing these vulnerabilities required enhanced authentication schemes and end-to-end encryption. The development of hybrid communication protocols combining wireless, satellite, and fiber-optic channels offered potential resilience, but also demanded synchronized cybersecurity policies across all layers of communication.

Encryption and Authentication Mechanisms

Encryption represented one of the most vital tools for securing ITS data communication. Symmetric encryption algorithms, such as AES, provided rapid encoding suitable for real-time communication, while asymmetric encryption, including RSA and ECC, enabled secure key exchanges. However, traditional encryption approaches were insufficient when applied to large-scale, distributed ITS networks. The computational load often affected communication latency, thus compromising system performance.

To overcome this, researchers introduced lightweight cryptographic techniques specifically designed for vehicular communication environments. Methods such as Elliptic Curve Cryptography and group-based signature schemes offered efficiency without sacrificing security. Authentication systems were also enhanced through public key infrastructures (PKI), where digital certificates ensured message authenticity.

Despite these improvements, encryption alone could not guarantee total protection. The effectiveness of such systems depended on secure key management, regular updates, and integration with other defense layers such as intrusion detection and behavior analysis. The research evaluated several models where hybrid encryption and blockchain-based authentication systems enhanced data trust and integrity in real-world ITS deployments.

Intrusion Detection and Prevention Systems

Intrusion detection systems (IDS) became indispensable for identifying and responding to cyber threats in ITS. These systems monitored network traffic to detect anomalies indicating possible attacks. Signature-based IDS relied on known attack patterns, while anomaly-based IDS used machine learning algorithms to detect unusual behaviors.

In ITS environments, anomaly-based systems demonstrated greater adaptability due to the dynamic nature of vehicular communication. However, high false positive rates remained a challenge. Machine learning and artificial intelligence algorithms,

particularly neural networks, were applied to improve detection accuracy by learning from real-time data streams.

Integrating intrusion detection with prevention systems (IDPS) allowed networks to automatically counteract detected threats. For example, in autonomous vehicle networks, IDPS could isolate compromised nodes or reroute data flow to maintain system integrity. The study of experimental systems revealed that hybrid IDS models combining statistical analysis and deep learning provided the most promising defense mechanisms for intelligent transportation networks.

Privacy and Ethical Considerations in Data Communication

As intelligent transportation networks expanded, the ethical and privacy implications of data collection and transmission became increasingly significant. Vehicles continuously generated massive datasets containing private user information such as travel routes, behavioral patterns, and communication identifiers. Unauthorized access to this data could lead to privacy violations, identity theft, or misuse by third parties.

To mitigate these concerns, privacy-preserving communication protocols were proposed. Techniques such as data anonymization, pseudonym generation, and decentralized data storage were applied to minimize personal data exposure. Furthermore, ethical frameworks emphasizing transparency and accountability were developed to ensure that data handling within ITS aligned with both legal and moral standards.

The concept of privacy-by-design became a cornerstone of modern ITS architecture. It encouraged embedding privacy safeguards at every stage of system development rather than adding them as afterthoughts. The research emphasized that maintaining public trust in intelligent transportation technologies depended largely on the assurance of ethical data management and transparent cybersecurity practices.

Artificial Intelligence in Cybersecurity Management

Artificial Intelligence (AI) played an increasingly important role in automating cybersecurity defense mechanisms. Machine learning algorithms could analyze large-scale traffic data, identify irregularities, and adapt to evolving attack patterns. AI-based

models supported predictive cybersecurity, allowing early detection of potential threats before they could cause significant damage.

Reinforcement learning was applied to dynamically optimize defense responses in real time. Such systems learned from historical attack data to improve decision-making processes and reduce false alarms. However, AI integration also introduced new vulnerabilities, as adversarial attacks could manipulate machine learning models by injecting misleading data.

Therefore, the study concluded that AI should complement but not fully replace human supervision in cybersecurity management. The combination of automated intelligence and expert analysis provided a balanced defense strategy capable of addressing both known and emerging cyber threats in intelligent transportation systems.

Policy Frameworks and Global Standards

The successful implementation of cybersecurity in ITS depended not only on technology but also on regulatory and policy frameworks. International organizations and governments developed standards to guide secure ITS deployment. Frameworks such as ISO/SAE 21434 and UNECE WP.29 regulations defined cybersecurity requirements for vehicle manufacturers and infrastructure operators.

However, disparities among national policies created inconsistencies in global ITS security. For instance, while some regions enforced strict data protection laws, others lacked comprehensive guidelines. Collaborative efforts were therefore essential to establish interoperable standards for global data communication security.

Public-private partnerships played a crucial role in policy development. Through joint research initiatives and security certification programs, stakeholders improved coordination and shared best practices. The research concluded that standardized policy frameworks not only ensured compliance but also promoted innovation by establishing trust in secure intelligent transportation infrastructures.

Future Perspectives and Technological Integration

The future of cybersecurity in ITS depended on continuous technological evolution. Quantum encryption, blockchain-based communication, and edge

computing were identified as emerging tools for strengthening network resilience. Quantum key distribution offered unbreakable encryption potential, while blockchain provided transparent, immutable data records resistant to tampering.

Edge computing further enhanced security by processing data closer to the source, reducing the risk of interception during transmission. However, these innovations required extensive investment, technical expertise, and international cooperation for large-scale deployment. The research predicted that the integration of these technologies would gradually redefine how ITS handled data communication security in the coming decades.

Another future direction involved the convergence of ITS with smart city infrastructure. As urban mobility systems interconnected with energy, healthcare, and communication networks, cybersecurity approaches needed to adopt holistic, cross-sector strategies ensuring the safety of all data exchanges across smart ecosystems.

Conclusion

The research demonstrated that enhancing cybersecurity in intelligent transportation systems required an integrated approach combining technical, ethical, and regulatory strategies. Challenges such as data interception, network heterogeneity, and privacy concerns were deeply intertwined with the operational structure of ITS. Addressing them demanded robust encryption, adaptive intrusion detection, and standardized global frameworks.

Through the review and comparative analysis, the study concluded that cybersecurity should be embedded as a foundational element of ITS design rather than as an auxiliary function. The successful future of intelligent transportation depended on building resilient systems capable of secure, transparent, and trustworthy data communication. The combination of AI-driven defense mechanisms, privacy-preserving technologies, and coherent international policies offered the most sustainable pathway toward achieving cyber-secure intelligent mobility.

References

1. Martinez, A., & Ivanov, D. (2021). Cyber resilience in vehicular networks: Strategies for secure communication. *Journal of Intelligent Transportation Research*, 14(3), 245–262.
2. Bennett, L., & Rossi, F. (2023). Encryption efficiency and privacy in connected vehicle environments. *Transportation Systems and Data Security Review*, 9(2), 87–104.
3. Gomez, R., & Thompson, J. (2020). Policy frameworks for intelligent transportation cybersecurity. *Global Mobility and Information Technology Journal*, 11(4), 301–319.