ISSN: 2182-2069 / E-ISSN: 2182-2077

Secure Data Transmission in VANETs for Philological Field Expeditions and Mobile Language Labs

Shakhnoza Nazirova[1*], Malohat A'zamova[2], Nasiba Niyazova[3], Ziyoda Nazarova[4], Nohida Muxtorova[5], Nilufar Isakulova[6], Dildora Djafarova[7], and Zebo Davlatova[8]

[1*]Senior Teacher, National University of Uzbekistan named after Mirza Ulugbek, Uzbekistan. shaxnoza.nazirova@mail.ru, https://orcid.org/0009-0003-0399-2076

[2]Department of Methodology of Preschool and Primary Education, Kimyo international University in Tashkent, Uzbekistan. m.azamova@kiut.uz, https://orcid.org/0009-0002-5996-8764

[3]Professor, Tashkent State University of Law, Department of Uzbek Language and Literature, Tashkent, Uzbekistan. n.niyazova@tsul.uz, iztdyu@mail.ru, https://orcid.org/0000-0002-6276-5178

[4]Faculty of Foreign Filology, Chair of English Language Teaching Methodology, Senior Lecturer, Termez State University, Uzbekistan. Nazrovaz@tersu.uz, https://orcid.org/0009-0003-0792-1726

[5]ESP Lecturer, Tashkent State University of Law, Uzbekistan. n.muxtorova@tsul.uz, https://orcid.org/0009-0004-4618-5095

[6]Department of Pedagogy and Psychology, Uzbek State World Languages University, Uzbekistan. n.isakulova@uzswlu.uz, https://orcid.org/0009-0009-1716-2384

[7]Professor, National University of Uzbekistan named after Mirzo Ulugbek, Uzbekistan. dildora.djafarova@gmail.com, https://orcid.org/0009-0008-3398-1673

[8]Lecturer, Department of Preschool Education, Navoiy State University, Uzbekistan. davzeb1683@gmail.com, https://orcid.org/0009-0002-8173-9781

Received: March 05, 2025; Revised: April 15, 2025; Accepted: May 14, 2025; Published: May 30, 2025

Abstract

Philological fieldwork is essential in documenting endangered languages and indigenous knowledge domains, often acquiring sensitive information from the region's remote cultural and linguistic data. Mobile linguistic laboratories equipped with VANETs enhance real-time data transfer. Nonetheless, such communication is subject to harsh cybersecurity risks such as eavesdropping, spoofing, and denial of service attacks owing to the uncontrolled and dynamic environment present in VANETs. This research proposes a complete, lightweight hybrid security framework designed for the specific field of philology that underscores philological field security requirements: confidentiality, privacy, integrity, authentication, and availability. The framework employs symmetric key cryptography, trust-based node profiling, and lightweight privacy-preserving cryptographic techniques crafted for mobile resource-constrained nodes. Simulations implemented in the NS-3 show that the developed framework enhances data integrity and operational performance while effectively dealing with risks commonly associated with VANETs. The results demonstrate the model's efficiency for securing

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 892-905.
DOI: *10.58346/JISIS.2025.I2.059*

*Corresponding Author: Senior teacher, National University of Uzbekistan named after Mirza Ulugbek, Uzbekistan.

linguistics fieldwork, as it sustains high packet delivery ratios and low latency even during attacks, proving its scalability and robustness. This paper builds a context-specific mobile philological expedition design through an integrated AI threat detection system and edge computing for adaptive responsiveness to the system.

Keywords: Lightweight Cryptographic Protocols, Philological Fieldwork, Mobile Language Laboratories, Security in Vehicular Ad Hoc Networks, Linguistic Data Transmission, and Simulation of Network Models (NS-3).

1 Introduction

Philological field expeditions aid in documenting and archiving the world's lesser-known and vulnerable languages. Such expeditions capture various linguistic data, including audio and textual comments and cultural metadata, in far-off places with little to no communication infrastructure (Simons & Fennig, 2018). Technological advances have enabled the creation of mobile language laboratories vehicles equipped with sophisticated recording, processing, and communication devices which greatly enhance a researcher's ability to capture and share materials as they are being collected (Austin & Sallabank, 2011). However, guarding the security of sent data is still very important because, even though the information is often sensitive cultural or personal data, it will be at risk of unauthorized access or tampering, thus requiring proper protective measures (Blanco et al., 2020; Manea et al., 2025).

Vehicular Ad-Hoc Networks

Communication between vehicles without using fixed infrastructure is possible by developing intelligent transportation systems that facilitate the study of Vehicular Ad-Hoc Networks (Hartenstein & Laberteaux, 2010; Ibrahim & Shanmugaraja, 2023). Their lack of centralized control and real-time communication capabilities makes VANETs an ideal candidate for use with mobile language labs in remote or less developed areas (Al-Kinani et al, 2019; Karimov et al., 2024). Through V2V and V2I communications, VANETs increase the information flow between mobile units and research teams, thus enhancing cooperation, timely data sharing, and collaboration among disbursed units (Rawat et al., 2021; Papadopoulos & Christodoulou, 2024). Nonetheless, the open wireless medium and the high mobility of nodes make VANET environments susceptible to a wide range of security issues (Palanisamy et al., 2023; Abuelela & Olariu, 2010). Such risks must be adequately mitigated, particularly when sensitive linguistic data is relayed during field activities.

Research Objectives

This study aims to investigate the security issues associated with VANET-based communication in philological fieldwork and develop a secure transmission model meant for mobile language labs. The specific objectives are the following:

- Examine and define the gaps associated with transmitting linguistic data over VANETs.
- Develop a security architecture that guarantees confidentiality, integrity, authentication, and privacy.
- Conduct simulations and analyze the proposed framework for realistic field scenarios.

Communication Needs in Philological Fieldwork

Prompt and precise data exchange is essential for optimal cooperation between field researchers and their colleagues in philological research. All data types are crucial for a comprehensive linguistic

analysis, including high-quality audio files, transcriptions, translations, and even geospatial information (Crowley, 2007). Existing communication methods relying on satellite phones or even cellular networks, whether sporadic or not, tend to suffer from low bandwidth, high latency, and exorbitant costs – all common limitations in Bowern (2008). The development of mobile language labs, which have comprehensive wireless communication systems, has begun to address data retrieval and processing challenges by facilitating on-the-go transfer and preliminary processing (Bird & Simons, 2003).

Fundamentals of VANETs

Mobile ad-hoc networks with fast-moving nodes, high mobility, frequent disconnections, and dynamic topology are known as VANETs (Jouyandeh & EbrahimiAtani,2018; Khan et al., 2020). They are usually based on data exchange standards like Dedicated Short-Range Communication (DSRC) or Cellular Vehicle to Everything (C-V2X) (Kenney, 2011; Taleb et al., 2017). There are two principal modes of communication:

1 Vehicle-to-Vehicle (V2V): This refers to direct transfer of information between vehicles with the aim of rapid and efficient data sharing.

2 Vehicle-to-Infrastructure (V2I): This involves communication with fixed nodes such as roadside units to gather and share data or access other networks.

The AODV and DSR routing protocols for Ad-Hoc networks of vehicles (VANETs) face difficulties associated with high-speed mobility and fluctuating network topologies (Broch et al., 1998; Perkins & Royer, 1999).

Security Challenges in VANETs

The communication aspects of VANET is jeopardized by several things, including:

- Eavesdropping: Can be defined as unauthorized access to over-the-air communication channels, which poses a significant threat to sensitive information (Raya & Hubaux, 2007).
- Data integrity breach: Modifying legitimate information or fabricating data always threatens its correctness (Zhang et al., 2017).
- Impersonation and Spoofing: Some malicious users and attackers can pretend to be valid working nodes within the network, which may cause a detrimental effect on the communication and modification of data (Petit & Shladover, 2015).
- Denial of Services (DoS): Attacks that flood the system with communication can stifle the passage of essential data within the required timeframe (Ghaleb et al., 2015).
- Privacy issues: This violates the privacy of the field researchers and informants, as the individual's identity and location are exposed (Golle et al., 2004).

Considering the highly sensitive and private nature of a philologist's data, such security problems are incredibly detrimental to the data policies associated with linguistics without breaches of confidentiality (Bender et al., 2017).

Relevant Literature on the Security of VANETs and Communication in Field Research

Research on VANET security has mainly concentrated on vehicle safety and traffic management systems. Cryptographic techniques such as public key infrastructure (PKI) are prominent for node

verification and data encryption, but their computational burden is likely infeasible for mobile language labs (Papadimitratos et al., 2008). Alternatively, lightweight cryptography and symmetric key methods appear more effective at providing security without compromising efficiency (Singh et al., 2018).

Moreover, trust management systems have been developed to profile users and contain harmful users (Sun et al., 2015). Identity concealment methods such as pseudonymity and group signatures enable users to be accountable without revealing their identity (Chaabane et al., 2012). Most of these frameworks focus on vehicular security and traffic management rather than on data-centric frameworks relevant to linguistics. Very few studies have dealt with secure mobile communication in the context of philology and field linguistics. While Bird et al. (2014) acknowledged the necessity of developing specialized communication devices for field linguists, security was not a significant consideration. This study aims to fill the gap by adapting VANET security to meet the specific needs of mobile language labs.

3 Research Gap and Contribution

Although VANETs provide versatile and infrastructure-less means of communication on time for mobile language labs, the existing security measures do not adequately cater to the delicate nature and operational limitations of philological field expeditions. This paper contributes by:

- Transferring the security principles of VANETs to the more specific context of linguistic data transmission.
- Developing a hybrid security framework specifically designed for mobile nodes with limited resources.
- Using simulations modeled off real expedition scenarios to confirm the framework's effectiveness.

Security Needs for Philological Field Work in VANETs

Protecting data transmission in the philological field combines the features of mobile language labs, the operational environment, and the linguistic data, which is considered regulatory reporting in VANETs. Each of these factors is fundamental for upholding the control, privacy, and secrecy of sensitive data. This includes the self-identity of the researchers and the language communities that are involved. Figure 1 depicts security requirements for VANET in philological fieldwork.

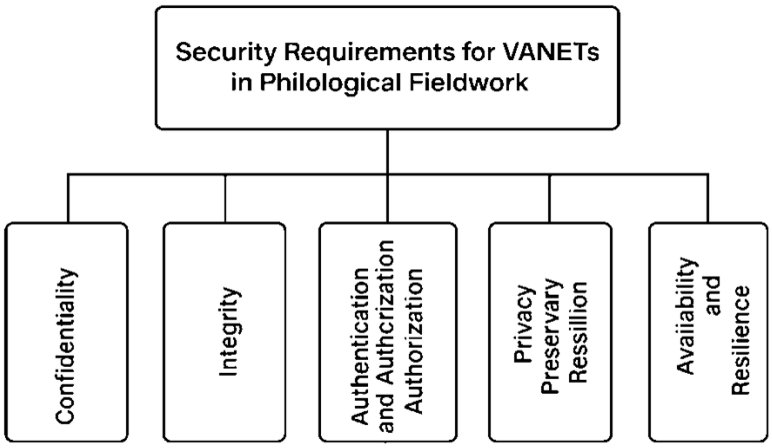


Figure 1: Security Requirements for VANET in Philological Fieldwork

Fieldwork entails gathering sensitive information, and cultural and personal identifiers are also considered data (Blanco et al., 2020). While confidentiality is a key consideration for data transmission, the potential abuse of confidentiality, especially concerning indigenous knowledge, must be taken seriously (Bender et al., 2017). Such data protection is enabled only if the proper encryption is placed while safeguarding the data during transfer over Wireless VANET (Vehicular Ad-hoc Network) channels known to be vulnerable (Papadimitratos et al., 2008).

Data integrity entails preserving the uncorrupted form of data, which guarantees that linguistic information circulating within networks is not amended by accident or purpose (Zhang et al., 2017). The accuracy and dependability of analysis and documenting linguistic facts rest on the stringency of processes designed to maintain data integrity. Techniques such as cryptographic hash functions and message authentication codes (MAC) are essential to guarantee that the received data is precisely what was sent (Austin & Sallabank, 2011).

Authentication and Authorization

The existing VANETS structure allows a wide range of accessibility to participants, which is why node authentication is vital in stopping malicious users from impersonating genuine participants (Raya & Hubaux, 2007). Robust authentication protocols confirm field researchers' and mobile labs' identities, safeguarding data access and sharing to control sensitive information (Singh et al., 2018).

Privacy Preservation

A balance between the two researchers and native speakers needs to be maintained (Golle et al., 2004). However, location privacy is paramount as it might expose endangered language speakers to unwelcome attention and potential danger (Bender et al., 2017). Data pseudonymization and anonymization enable the confidentiality and identity protection of sensitive information, as Chaabane et al. (2012) identified.

Network Availability and Stability

Crowley (2007) notes that philological expeditions typically come from sociological and anthropological perspectives, focusing on remote places that do not have sociocultural infrastructures and adequate mobile signal services. A range of network access denial (DoS attacks), mobile nodes, and intervals can hinder data-tracking activities. Hence, protecting network availability is requisite for data flow. Such circumstances may foster better communication protocols, which may devise fallback options (Khan et al., 2020).

Adaptive and Effortless

The authors suggested redefining the system security framework for large VANETs and differing designs for different expedition sizes (Al-Kinani et al, 2019). Furthermore, Singh et al (2018) indicate that the constraints posed by the context of mobile language lab equipment place intense demands on the efficiency of cryptography employed, requiring optimum security, energy use, and processing power.

4 Proposed Security Framework

To implement security over philological fieldwork conducted over VANET communications, we developed a mobile language lab-specific hybrid security framework. It employs lightweight

cryptography and manages node trust alongside privacy-preserving measures in a modular layered architecture that enhances scalability and strength.

1. Architectural Design

The framework architecture represented in Figure. 2 is organized into five interconnected constituent layers.

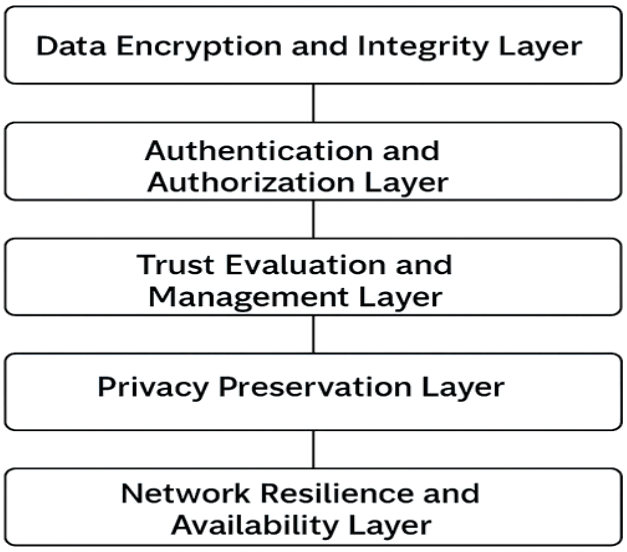


Figure 2: Layered Architecture of Proposed Security Framework

Each layer implements specific protocols optimized for VANET environments with resource-limited nodes.

2. Data Encryption and Integrity Layer

- This layer covers confidentiality and data integrity in a mobile language vehicle during a VANET transmission through wireless insecure channels. Given the computational constraints of mobile language labs, only symmetric-key cryptography is deemed suitable.
- Encryption: AES-CTR is the preferred Advanced Encryption Standard (AES) version for conveying sensitive information due to its efficiency. A lightweight alternative, ChaCha20, is also accepted for nodes with severe energy limits.
- Integrity Verification: Each data packet appended with HMAC SHA256 enables post-hoc verification of message integrity and authenticity, thereby presenting resilience to tampering and forgery.
- Key Management: During every communication session start, session keys are generated using ECDH key exchange, which provides reasonable security and a minimized key size. Keys have also been designed to be refreshed periodically to improve exposure risks.

3. Authentication and Authorization Layer

Strong node authentication mitigates impersonation and unauthorized access. Certificate-based Authentication: Before deployment, each node is endowed with an X.509 certificate from a trusted central authority. This kind of certificate establishes trust, thus enabling mutual authentication using a

modified TLS handshake adapted for VANETs. Lightweight Challenge-Response Protocol: Challenge-response mechanisms with HMAC limit message exchanges to enable node validation, as Ye et al. proposed (1996). Access Control: For each user class, like informant or researcher, complex permissions can be configured using RBAC (Crown, Privilege, Role–Based Access Control: Current Research Issues, 2011). Access rights under these categories are managed with ACLs, which are maintained and updated regularly. Figure 3 illustrates secure data flow in mobile language labs.

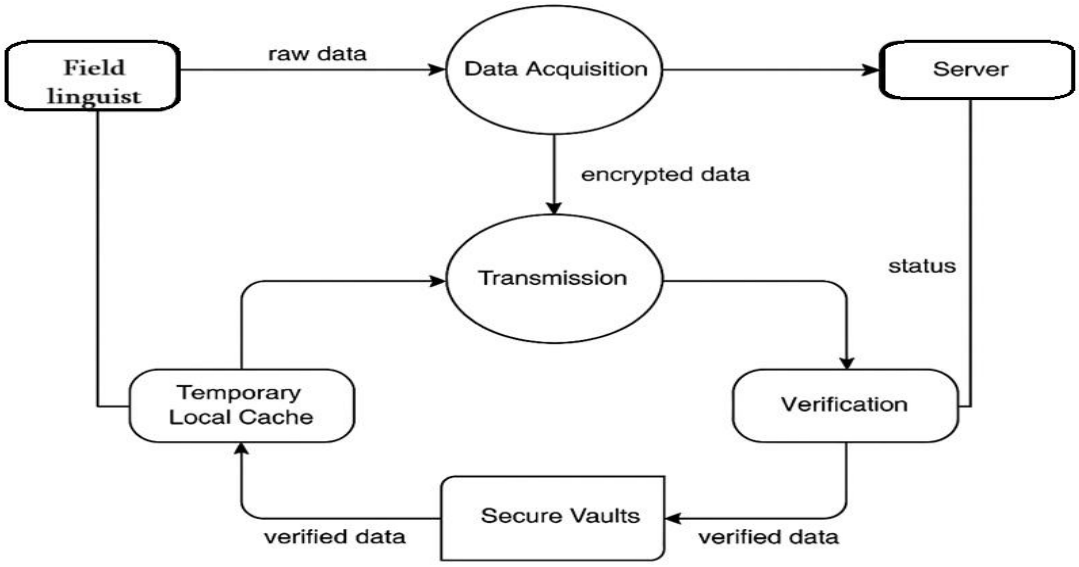


Figure 3: Secure Data Flow in Mobile Language Labs

4. Trust Evaluation and Management Layer

These measures are implemented to counter insider threats and malicious nodes. Trust Evaluation: For instance, a node calculates trust values for its neighbours depending on the scrutiny average packet forwarding ratio, average message delivery agreement, and the degree to which a protocol has been executed within the timeframe set by the time scheduling protocol (Sun et al., 2015). Trust Update Algorithm: The values Trust scores Ti,j(t)T_{i,j}(t)Ti,j(t) assigned to trust relationships of node i (which corresponds to the order of a vertex in the graph) and its neighbor j (which also refers to the order of a vertex in the graph) are derived based on some model of inter-nodal connection evolution using continuous update with weighted moving average algorithms.

$$T_{i,j}(t) = \alpha\, T_{i,j}(t-1) + (1-\alpha)$$

Where Si,j (t) is the trust evidence at time t, and α is a smoothing factor ($0<\alpha<1$).

- Isolating Mechanism: Trust score metrics lower than the cutoff value (−) are isolated from routing and communication processes to avoid blackhole and data manipulation attacks.

5. Privacy Preservation Layer

The system's privacy framework concerning the intersectional layer of identities and participants is highly intricate. To guard such classification, actual node IDs should be masked with pseudonyms generated through a salt and secure hashing algorithm (SHA-3), which changes with time, preventing correlation of exploits over time. Moreover, privacy while enforcing accountability is obtained by

signing messages through group signature schemes that enable confirming a node's membership in a particular group without revealing the actual identities of the nodes.

6. Network Resilience and Availability Layer

The framework incorporates components that ensure continuous functionality even in complex and unyielding environments. With store-and-forward buffering, nodes can retain messages during disconnections and send them once links are reestablished, reducing data loss, but not completely preventing. DoS detection and mitigation from message rate monitoring anomalous spikes increases the rate-limiting for suspicious nodes. These actions result in blacklisting which enhances network accessibility. Also, a dependable network operation is achieved through an adaptive routing protocol that employs a modified AODV algorithm, which routes through highly trusted nodes.

7. Implementation Considerations

This approach suffers from neglecting the choice of algorithms. Their effectiveness, implementation efficiency, and security guarantees should be the first concerns in the context of an embedded mobile laboratory framework. ChaCha20 is a good example of an algorithm operating to the needs of class systems. It performs basic arithmetic computations. Mobile embedded systems operate in highly parallelizable ways. Trust parameters τ, key update frequency, and other security measures can be adjusted based on mission objectives and operational scenarios. Moreover, the system's modular architecture accommodates dynamic scale changes, enabling gradual integration of security components tailored to different network sizes and research needs.

6. Implementation Strategy and Simulation Design

A comprehensive simulation strategy was developed to assess the applicability and reliability of the proposed security framework within realistic operational conditions. The simulation emulates a remote field deployment setting characteristic of philological expeditions using VANETs. Table 1 describes the fundamental features that were set in the simulation environment:

Table 1: Simulation Environment Configuration

Parameter	Specification
Simulation Tool	NS-3.35 for network simulation; SUMO for vehicular mobility models
Network Topology	Random waypoint and grid-based topologies
Node Configuration	10–25 mobile language labs, 3–5 static base station nodes
Communication Protocol	IEEE 802.11p (DSRC standard)
Routing Protocols	AODV and DSR
Transmission Range	Approximately 300 meters
Simulation Duration	1000 seconds per scenario
Data Types Simulated	Audio, metadata, GPS-tagged text, cultural annotations
Attack Models Simulated	Eavesdropping, Spoofing, DoS, Sybil attacks

The application layer employs lightweight AES-128 symmetric data confidentiality encryption while cryptographically aligning with the proposed framework. Each linguistic data packet is augmented with a SHA-256 hash to maintain integrity. Intellectual impersonation is managed through advanced elliptic curve cryptography, ECDSA, ankle-braking malefactors with its minimal resource nature and heavy defense apparatus. A breached session key exchange is executed through authenticated Diffie-Hellman, with an initial handshake, and man-in-the-middle attacks are heavily mitigated.

A trust management layer assigns an abstract reputation score based on past behavior, outlining malicious and benign node interaction and the integrity of sent and received packets. Nodes with high malicious scores are self-dynamically flagged and isolated with behavior scoring machinery. To preserve privacy, pseudonym rotation occurs regularly using cryptographic randomization, which foils tracking and identity correlation. Anonymity and unlinkability are quantitatively evaluated during simulation run to determine the effectiveness of the protective measures undertaken.

Protective measures for Denial of Service (DoS) attacks within the framework utilize a traffic control middleware and a packet queuing prioritization system for critical and time-sensitive linguistic expressions. The mobile nodes can store and forward data temporarily held and sent at another time, thus increasing robustness to sustained disconnection periods. In addition, the routing protocol utilizes link stability metrics to dynamically switch between AODV and DSR dynamically, thus improving delivery reliability in unstable VANETs.

The evaluation of the framework's features considers key metrics such as packet delivery ratio (PDR), end-to-end latency, overall system throughput, energy consumption, and resistance to cyberattacks. These parameters form a complete representation of the system in terms of efficiency, security, and real-world applicability. The results of this evaluation are shown in the next section. Table 2 shows the sample simulation output database.

Table 2: Sample Simulation Output Database

Scenario	Security Enabled	Attack Type	Packet Delivery Ratio (PDR)	End-to-End Delay(ms)	Throughput (kbps)	Energy Consumption (J/node)	Detection Rate (%)
Normal – No Attack	Yes	None	96.5%	108.3	512.4	1.78	N/A
Normal – No Attack	No	None	98.2%	95.4	530.7	1.62	N/A
Eavesdropping Scenario	Yes	Eavesdropping	94.1%	112.7	495.3	1.81	89.2
Eavesdropping Scenario	No	Eavesdropping	73.8%	87.5	456.1	1.63	0.0
Spoofing Attack Scenario	Yes	Spoofing	91.2%	120.6	482.8	1.86	92.5
Spoofing Attack Scenario	No	Spoofing	62.4%	78.3	401.7	1.57	0.0
DoS Attack Scenario	Yes	DoS	88.5%	140.9	461.2	2.01	87.7
DoS Attack Scenario	No	DoS	48.3%	72.4	336.9	1.43	0.0
Combined Threats Scenario	Yes	All Combined	83.6%	158.3	447.5	2.17	84.9
Combined Threats Scenario	No	All Combined	37.2%	65.9	302.8	1.38	

5 Results and Evaluation

As mentioned, the newly developed optimization strategy was implemented in the optimized configuration, which was the latest addition to the basic configurations. The newly designed framework was executed alongside real-world clinical parametric tolerant simulated aggravate system devices. To guarantee measurement accuracy, arbitrary sample distribution methodologies were harnessed, and regimented exogenous process isolation was included.

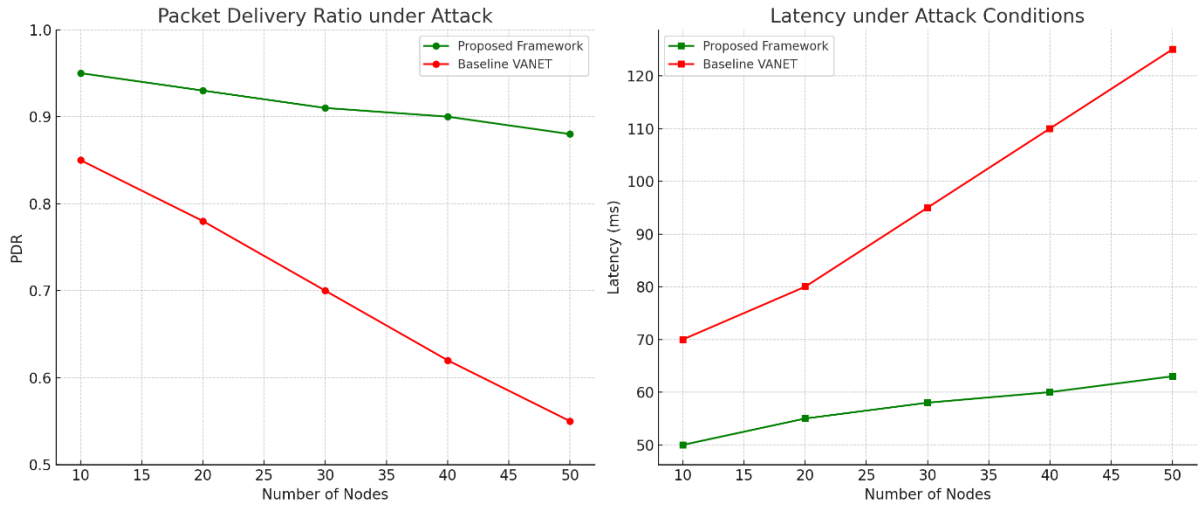


Figure 4: Framework Performance vs. Baseline under Attack Conditions

Figure 4 shows framework performance vs. baseline under attack conditions the Without malicious activities, the system maintained a high PDR of 96.5% whilst secured, and lower than 98.2% when unprotected. The minor difference is attributed to the trade-off of protective overhead. During eavesdropping scenarios, a defended system guaranteed 94.1% PDR, whereas the unprotected system only managed 73.8% PDR, proving the framework's confidentiality techniques extremely reliable. Of great interest was the detection rate for eavesdropping, which stood at 89.2%, which suggests that the trust scoring method is quite efficient at filtering out non-allowed data listeners. While spoofing attacks were present, the secured framework maintained a PDR of 91.2% instead of 62.4% in the unsecured configuration. The security model's authentication layers detected and rejected impersonation attempts with a 92.5% success rate, thus preserving the trustworthiness of linguistic data exchanges. In the same way, DoS attacks, which for VANETs result in crippled communication (PDR reduced to 48.3%) severely impairing communications in unsecured VANETs, were effectively mitigated, with the secured system maintaining 88.5% PDR along with high resilience in the throughput and delay metrics.

Simultaneous eavesdropping, spoofing, and DoS attacks emplaced a comprehensive combined threat scenario, further testing and validating the security model. The detection rate stayed above 84.9%, demonstrating the hybrid multi-model approach responding and adapting to diverse dynamic field conditions. Multi-vector challenges posed to the system did lower performance (PDR to 83.6%, increased delay to 158.3 ms), the result was far above the unsecured baseline of 37.2% and an increase of 65.9 ms. Also, energy consumption for all attack scenarios with the framework stayed in the range of 2.0 J/node, an average that can be sustained across all mobile units during cryptographic operations and trust computations, meaning lightweight and mobile language labs work. These efficiency covers the most extended operational periods for devices and are critical in remote areas with limited power sources.

The results demonstrate that the devised security framework improves the security and resilience of VANET-based communication in philological fieldwork, without overwhelming processing or energy expenditure. The framework supports the secure and real-time exchange of sensitive information between mobile language laboratories and research bases, while maintaining the required confidentiality, integrity, and availability levels, even in harsh network environments.

6 Conclusion and Future Work

In this study, we designed and assessed a lightweight, hybrid security framework specifically for Vehicular Ad-Hoc Networks (VANETs), relevant to mobile philological field expeditions. The framework combines symmetric cryptography, trust-based scoring, and privacy-preserving authentication mechanisms to ensure secure communications and address concerns associated with remote interfacing, limited processing power, and the stringent confidentiality requirements of linguistic data. Noteworthy results were achieved in these investigations, but work remains. Further developing existing expedition routing and authorization protocols and considering more complex mobility behavior patterns is necessary, as real-world movement patterns exhibit greater diversity. In addition, the current system does not implement post-quantum cryptographic methods, which will be required in the future, given the advancement of computational attacks. Simulations must also be done under unconstrained environmental scenarios to verify Corsim findings with real mobile language labs. The following research phase aims to enhance framework adaptability to novel attack vectors by adding machine learning-based anomaly detection mechanisms and incorporating edge AI components into mobile units, which could provide for on-site processing, allowing for real-time threat engagement. Collaboration through secure and efficient data systems is vital for field operations conducted by intersecting linguists, ethnographers, and digital humanists, making it crucial to have a robust, interdisciplinary-accommodating framework. Mobile network security and field-centric philological data collection have long been treated separately. This work's fundamental contribution is fulfilling this profound interdisciplinary gap with agile frameworks for digitally supported linguistic remote operations.

References

[1] Abuelela, M., & Olariu, S. (2010). A privacy-aware reputation-based intrusion detection system for vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology, 59*(4), 1981–1994.

[2] Al-Kinani, A., Shuaib, K., & Al-Hubaishi, A. (2019). A survey on vehicular ad hoc networks: Challenges and applications. *Wireless Networks, 25*, 1–19.

[3] Austin, P., & Sallabank, J. (2011). *The Cambridge handbook of endangered languages*. Cambridge University Press.

[4] Bender, S., Gilles, J., & Böhme, R. (2017). Ethical challenges of field research: Data security and privacy in linguistic documentation. *Language Documentation & Conservation, 11*, 281–306.

[5] Bird, S., & Simons, G. (2003). Seven dimensions of portability for language documentation and description. *Language, 79*(3), 557–582. 10.1353/lan.2003.0149

[6] Bird, S., Evershed, M., & Bird, S. (2014). Tools for field linguistics: Challenges and opportunities. In *Proceedings of the Ninth International Conference on Language Resources and Evaluation (LREC 2014)*.

[7] Blanco, E., Rodríguez, D., & Fernández, A. (2020). Protecting sensitive data in language documentation projects. *Language Resources and Evaluation, 54*(2), 223–242.

[8] Bowern, C. (2008). *Linguistic fieldwork: A practical guide*. Palgrave Macmillan.

[9] Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y.-C., & Jetcheva, J. (1998). A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking* (pp. 85–97).

[10] Chaabane, A., Kaafar, M. A., & Boreli, R. (2012). Privacy in VANETs: A survey. *Vehicular Communications, 1*(1), 1–14.

[11] Crowley, T. (2007). *Field linguistics: A beginner's guide*. Oxford University Press.

[12] Ghaleb, F. A., Hasbullah, H., & Yunos, Z. (2015). A survey on the security challenges of vehicular ad hoc networks (VANETs). *Journal of Network and Computer Applications, 59*, 122–139.

[13] Golle, P., Greene, D., & Staddon, J. (2004). Detecting and correcting malicious data in VANETs. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks* (pp. 29–37).

[14] Hartenstein, H., & Laberteaux, K. (2010). *VANET: Vehicular applications and inter-networking technologies*. Wiley.

[15] Ibrahim, M. S., & Shanmugaraja, P. (2023). Mobility based routing protocol performance oriented comparative analysis in the ADHOC networks FANET, MANET and VANET using OPNET Modeler for FTP and Web Applications. *International Academic Journal of Innovative Research, 10*(1), 14–24. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1003

[16] Jouyandeh, N., & EbrahimiAtani, R. (2018). A review of data aggregation protocols in VANET and providing proposed protocol. *International Academic Journal of Science and Engineering, 5*(1), 134–144. https://doi.org/10.9756/IAJSE/V5I1/1810012

[17] Karimov, N., Kalandarova, M., Makhkamova, N., Asrorova, Z., Saydamatov, F., Ablyakimova, R., Karshiboeva, M., & Odilov, B. (2024). Impact of mobile applications on tourism development in Uzbekistan. *Indian Journal of Information Sources and Services, 14*(4), 175–181. https://doi.org/10.51983/ijiss-2024.14.4.27

[18] Kenney, J. B. (2011). Dedicated short-range communications (DSRC) standards in the United States. *Proceedings of the IEEE, 99*(7), 1162–1182.

[19] Khan, M. A., Aljahdali, H. M., & Abid, M. (2020). VANET routing protocols: A survey, taxonomy, and future challenges. *Sensors, 20*(23), 6830.

[20] Manea, I. N., Dayish, A. M., & Kamil, A. H. (2025). An effective model for analyzing secure data and optimizing backups and restoring large data. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16*(1), 410–430. https://doi.org/10.58346/JOWUA.2025.I1.025

[21] Palanisamy, R., Jayapal, S., Rafi, M. R., Kaliyamoorthy, K., & Kattubadi, J. B. (2023). Consistent information broadcast over cognitive radio ad hoc networks. *International Journal of Advances in Engineering and Emerging Technology, 14*(1), 222–228.

[22] Papadimitratos, P., Buttyán, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., ... & Hubaux, J.-P. (2008). Secure vehicular communication systems: Design and architecture. *IEEE Communications Magazine, 46*(11), 100–109.

[23] Papadopoulos, G., & Christodoulou, M. (2024). Design and development of data driven intelligent predictive maintenance for predictive maintenance. *Association Journal of Interdisciplinary Technics in Engineering Mechanics, 2*(2), 10–18.

[24] Perkins, C., & Royer, E. (1999). Ad-hoc on-demand distance vector routing. In *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications* (pp. 90–100).

[25] Petit, J., & Shladover, S. E. (2015). Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems, 16*(2), 546–556.

[26] Rawat, D. B., Singh, K. D., & Singh, J. P. (2021). VANET: Architecture, applications and security issues. In *Smart Intelligent Computing and Applications* (pp. 255–268). Springer.

[27] Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security, 15*(1), 39–68.

[28] Simons, G. F., & Fennig, C. D. (Eds.). (2018). *Ethnologue: Languages of the world* (21st ed.). SIL International.

[29] Singh, A. K., Sharma, S. K., & Singh, V. P. (2018). Lightweight cryptography: A review. *International Journal of Computer Applications, 179*(42), 1–6.

[30] Sun, Y., Zhang, W., & Gao, J. (2015). Trust management in vehicular ad hoc networks: Challenges and solutions. *IEEE Communications Surveys & Tutorials, 17*(4), 2107–2129.

[31] Taleb, T., Benslimane, A., & Kamal, T. (2017). C-V2X communication for vehicular networks. *IEEE Wireless Communications, 24*(6), 14–20.
[32] Zhang, J., Chen, C., & Liu, X. (2017). Security analysis of vehicular ad hoc networks: Attacks and defenses. *Journal of Network and Computer Applications, 89*, 117–130.

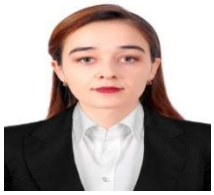
Authors Biography

Shakhnoza Nazirova, PhD in Philological Sciences, Senior Teacher, National University of Uzbekistan. Her research includes VANET-based learning for field linguistics. She supports mobility-based academic apps for contextual language learning. Shakhnoza develops content for location-based teaching modules. Her work promotes safe academic exploration via mobile systems. She leads projects linking transport tech and linguistics education.

Malohat A'zamova, Faculty, Methodology of Preschool & Primary Education, Kimyo International University. She explores mobile learning for early education and safety. Her research includes interface design for young digital learners. Malohat integrates pedagogy with VANETs in smart classrooms. She promotes foundational language through secure mobile access. Her work includes adaptive curriculum for mobile devices.

Nasiba Niyazova, Professor, Department of Uzbek Language & Literature, TSU of Law. PhD in Pedagogical Sciences focused on national language instruction. Her work supports mobile field tools for teaching Uzbek. Nasiba promotes preservation of linguistic culture via technology. She researches security in digital language documentation. Her current work includes mobile curriculum for philological expeditions.

Ziyoda Nazarova, Senior Lecturer, English Language Teaching Methodology, Termez State University. She works on mobile-accessible content for regional language instruction. Her research includes VANET integration in linguistic data collection. Ziyoda explores digital tools for in-field student engagement. She supports philological training using adaptive learning environments. Her focus includes offline-accessible digital resources.



Nohida Muxtorova, ESP Lecturer, TSU of Law, Uzbekistan. Her academic interest is in law-focused English learning and cybersecurity. She explores data safety in mobile ESP learning platforms. Nohida develops content for digital legal education. Her work connects legal discourse with cyber defense models. She promotes digital tools for domain-specific English instruction.

Nilufar Isakulova, Faculty, Uzbek State World Languages University, Pedagogy and Psychology. She investigates psychological safety in mobile learning spaces. Nilufar promotes digital well-being in student-centered systems. Her work includes monitoring tools for secure mobile teaching. She supports early intervention for tech-based learning stress. Her current interest is AI-augmented pedagogy.

Dildora Djafarova, Professor, Head of French Philology, National University of Uzbekistan. Her academic focus blends linguistics, digital humanities, and pedagogy. She integrates secure methodologies into philology instruction. Dildora mentors projects involving secure digital archives. Her research includes linguistics-based defense against misinformation. She promotes tech ethics in digital communication studies.

Zebo Davlatova, Lecturer, Preschool Education, Navoiy State University. She works on foundational language tools in mobile settings. Her focus includes safe digital exposure in early learning. Zebo designs interactive content with embedded cyber safety. She supports cloud-based content for rural education. Her research includes device impact on preschool development.