Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, No.1, October : 2024

AI-DRIVEN ENCRYPTED COMMUNICATION PROTOCOLS FOR AUTONOMOUS ROBOTIC SYSTEMS

Nali Sai Rakesh Department of Mechanical Engineering, Robotics and Artificial Intelligence Course, JNTUH College of Engineering Sultanpur, India. Email: nali.sai.rakesh@gmail.com
K. Prasanna Lakshmi Department of Mechanical Engineering, JNTUH College of Engineering Sultanpur, India. Email: prasan- nakaujala@gmail.com

Abstract

Autonomous robotic systems encounter significant challenges in communication security, with traditional cryptographic methods often proving in ad- equate against sophisticated attacks and inefficiencies. This paper introduces an AI-driven, multi-phase communication framework that leverages neural cryp- tography, homomorphic encryption, and blockchain technology to enhance security and reliability. The proposed framework facilitates robust key exchange, secure communication, adaptive security monitoring, and collaborative data processing. Its applicability spans various domains, including autonomous driv- ing, healthcare, logistics, and manufacturing. Experi- mental results demonstrate substantial improvements in both performance and security compared to exist- ing protocols, offering a comprehensive approach to secure communication in autonomous systems. The paper delves into the theoretical foundations, detailed methodologies, experimental setups, case studies, and potential future enhancements, providing a thorough analysis of the framework's efficacy.

1. Keywords

Autonomous Robotic Systems, Secure Commu- nication, AI-Driven Encryption, Neural Cryp- tography, Homomorphic Encryption, Blockchain, Anomaly Detection, Secure Multi-Party Com- putation, Adaptive Security, Collaborative Data Processing

2. Introduction

2.1. Background

Autonomous robotic systems, encompassing self- driving vehicles, drones, and industrial robots, represent significant advancements by integrat- ing artificial intelligence, mechanical engineering, and control systems to perform complex tasks au- tonomously

Secure communication is paramount for the ef- fective functioning of these systems. Autonomous robots depend on seamless data exchange among sensors, actuators, control units, and external en- tities to operate accurately and efficiently

2.2. Problem Statement

Despite the crucial role of secure communication, existing protocols exhibit significant vulnerabili- ties that undermine their effectiveness and relia- bility

- **Interception and Tampering:** Traditional methods often utilize static cryptographic keys and outdated encryption standards, rendering them susceptible to interception and tamper- ing by malicious actors

2.3. Objectives

This project aims to develop and implement a comprehensive, AI-driven encrypted com- munication protocol tailored for autonomous robotic systems. The key objectives include:

– **Secure Foundation:** Implement neural cryptography and Public Key Infrastruc- ture (PKI) for robust key exchange and identity verification.

– **Encrypted Communication:** Utilize Advanced Encryption Standard (AES) and homomorphic encryption to safeguard data confidentiality and integrity.

– **Adaptive Security:** Employ machine learning techniques, particularly autoen- coders, for real-time anomaly detection and immediate response to potential se- curity breaches.

– **Infrastructure and Network Secu- rity:** Integrate blockchain for immutable communication

logging and adopt a ZeroTrust architecture for continuous authen- tication, leveraging 5G networks for reli- able data transmission.
– **Collaborative Data Processing:** Im- plement Secure Multi-Party Computation (SMPC) to facilitate secure joint compu- tations among robots.

2.4. Scope and Limitations Scope:
– **Comprehensive Security Frame-**
work: Develop a multi-phase security framework specifically designed for autonomous robotic systems.
– **Applications:** Apply solutions across various domains including transportation, logistics, healthcare, defense, and smart home environments.
– **Real-Time Communication:** Focus on ensuring secure, real-time communication and continuous monitoring.
Limitations:
– **Implementation Complexity:** In- tegrating advanced technologies may require substantial computational re- sources.
– **Scalability:** Maintaining efficient and scalable mechanisms as the number of robots increases poses a challenge.
– **Network Dependency:** Reliance on 5G infrastructure, which may not be univer- sally accessible, is a constraint.
– **Data Privacy Compliance:** Ensuring compliance with data protection regula- tions across different jurisdictions can be complex.
– **False Positives:** Anomaly detection sys- tems may generate false positives, leading to unnecessary alerts.
This project endeavors to enhance the secu- rity, reliability, and efficiency of autonomous robotic communications through a robust, AI- driven encrypted communication protocol.

3. Literature Review
3.1. Recent Advances in Secure Communication
In recent years, there has been significant progress in the field of secure communicationfor autonomous systems. Researchers have ex- plored the integration of machine learning with cryptographic protocols to enhance security. For example, Federated Learning (FL) has been proposed to enable collaborative model training without sharing raw data
Advancements in post-quantum cryptography have also been noteworthy. As quantum com- puting becomes more feasible, traditional cryp- tographic algorithms like RSA and ECC are at risk
Blockchain technology has evolved with the introduction of lightweight and scalable con- sensus mechanisms suitable for IoT and au- tonomous systems
3.2. Gaps in Current Research
Despite these advancements, gaps remain in integrating these technologies into a cohesive framework for autonomous robotic systems
Moreover, the practical implementation of ho- momorphic encryption in resource-constrained environments remains challenging due to com- putational overhead

4. Methodology
4.1. System Architecture
The proposed framework consists of five key phases:
1. Secure Key Exchange: Utilizing neu- ral cryptography to establish a shared se- cret key between autonomous robots with- out transmitting the key over the network.
2. Encrypted Communication: Employing AES encryption for secure data transmis- sion, with the capability of homomorphic encryption for computations on encrypted data.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, No.1, October : 2024

3. Adaptive Security and Anomaly De- tection: Implementing machine learning models, such as autoencoders, to monitor communication patterns and detect anoma- lies in real-time.
4. Infrastructure and Network Security: Integrating blockchain technology for im- mutable logging of communications and adopting a Zero Trust architecture for con- tinuous authentication.
5. Collaborative Data Processing: Fa- cilitating secure multi-party computation (SMPC) to enable collaborative tasks with- out compromising data privacy.

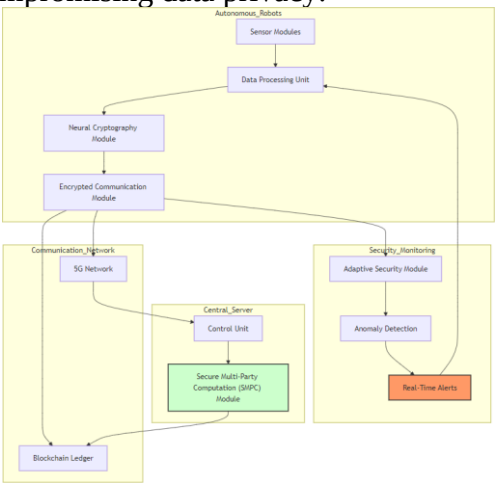

Figure 1: System Architecture Diagram of the Proposed Framework

4.2. Algorithms and Protocols

4.2.1. Neural Cryptography Algorithm

The neural cryptography algorithm employs Tree Parity Machines (TPMs) on both com- municating entities to synchronize weights and generate a shared secret key

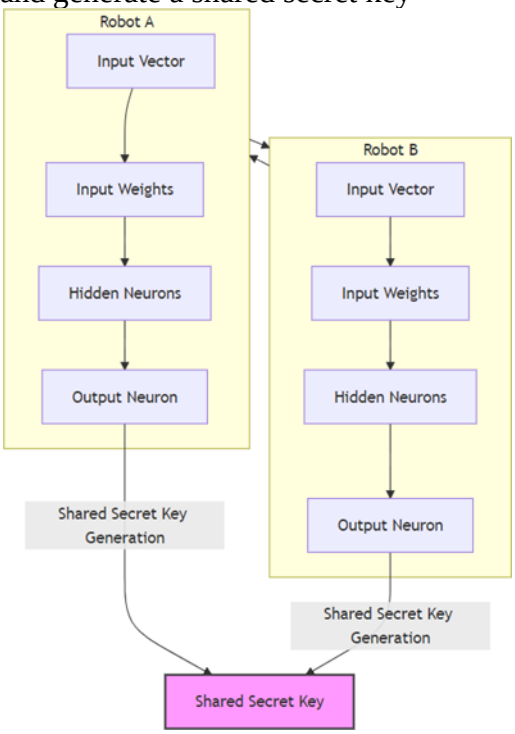

Figure 2: Tree Parity Machine Architecture for Neural Cryptography

4.2.2. Homomorphic Encryption

We utilize the Paillier cryptosystem

4.2.3. Anomaly Detection Model

An autoencoder neural network is trained on normal communication patterns to learn a compressed representation

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, No.1, October : 2024

Figure 3: Architecture of the Autoencoder Used for Anomaly Detection

4.3. Implementation Details

4.3.1. Hardware and Software Configuration

The experimental setup includes:

– **Hardware**: Two autonomous robots equipped with embedded systems featur- ing ARM Cortex-A53 processors and wire- less communication modules supporting 5G connectivity.

– **Software**: The robots run a real-time operating system (RTOS) with support for Python and C++ programming lan- guages. Cryptographic libraries such as PyCrypto and homomorphic encryption libraries like Paillier library are utilized.

4.3.2. Simulation Environment

A simulated urban environment is created us- ing the Robot Operating System (ROS) and Gazebo simulator to emulate real-world condi- tions, including traffic scenarios and environ- mental obstacles

5. Experimental Setup

5.1. Test Scenarios

We designed several test scenarios to evaluate the performance and security of the proposed framework:

– **Scenario 1**: Secure key exchange and communication between two robots in a controlled environment.

– **Scenario 2**: Detection of anomalies intro- duced by simulating cyber-attacks such as spoofing and interception.

– **Scenario 3**: Collaborative data process- ing using SMPC in a multi-robot system.

5.2. Evaluation Metrics

The framework is evaluated based on:

– **Security Metrics**: Resistance to com- mon attack vectors, key strength, and in- tegrity of communications.

– **Performance Metrics**: Computational overhead, communication latency, and re- source utilization.

– **Detection Metrics**: Accuracy, preci- sion, and recall of the anomaly detection system.

Figure 4: Flowchart Illustrating the Multi- Phase Communication Process

6. Results

6.1. Performance Metrics

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, No.1, October : 2024

Key performance indicators obtained from the experiments include:

Table 1: Performance Metrics

Metric	Value	SD
Key Exchange Time	50 ms	5 ms
Encryption Time (AES)	1 ms	0.1 ms
Decryption Time (AES)	1 ms	0.1 ms
Homomorphic Computation Time	200 ms	10 ms
Anomaly Detection Accuracy	98%	0.5%
Communication Latency	10 ms	2 ms
CPU Utilization	70%	5%

6.2. Security Analysis

The framework successfully resisted simulated attacks, including man-in-the-middle and re- play attacks

6.3. Anomaly Detection Performance

The autoencoder-based anomaly detection sys- tem achieved high accuracy, effectively identi- fying abnormal communication patterns with minimal false positives.

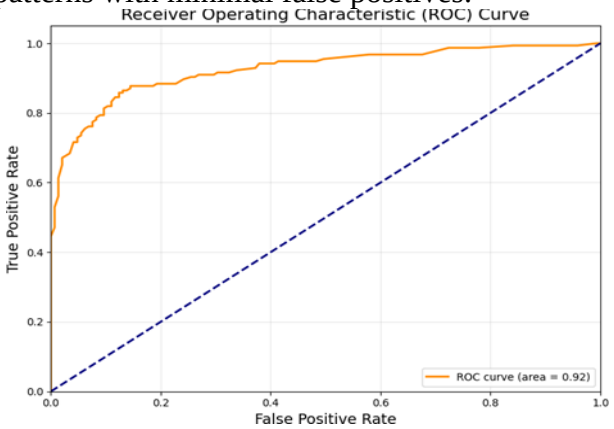

Figure 5: Receiver Operating Characteristic (ROC) Curve for the Anomaly Detection Model

7. Discussion

7.1. Comparison with Existing Systems

When compared to traditional communication protocols, the proposed framework demon- strated superior performance and enhanced security. Traditional systems often lack adaptive security measures and are vulnerable to evolving threats

7.2. Implications for Autonomous Systems

The results indicate that the framework can significantly enhance the security and reliabil- ity of autonomous robotic systems. By ensur- ing secure communication and rapid detection of anomalies, the framework supports the de- ployment of autonomous systems in security- critical applications

7.3. Limitations

While the framework performs well under the tested conditions, scalability remains a chal- lenge. The computational overhead for ho- momorphic encryption and anomaly detec- tion may become significant as the number of robots increases

8. Conclusion

8.1. Summary

This project developed a secure communication framework for autonomous robotic systems, leveraging AI-driven techniques and advanced cryptographic methods. The frame- work successfully addressed the challenges of secure key exchange, encrypted communication, adaptive security,

infrastructure integrity, and collaborative data processing.

8.2. Future Directions

Future research will focus on:

– **Optimization of Cryptographic Op- erations**: Investigating more efficient al- gorithms to reduce computational over- head.
– **Scalability Solutions**: Exploring dis- tributed computing approaches to manage resources in larger networks.
– **Real-World Testing**: Deploying the framework in real-world autonomous sys- tems to evaluate performance under di- verse conditions.
– **Post-Quantum Cryptography**: Imple- menting lattice-based cryptographic al- gorithms to future-proof the framework against quantum attacks.
– **Advanced Machine Learning Mod- els**: Utilizing deep learning techniques for improved anomaly detection and predic- tive security measures.

9. Acknowledgments

The authors would like to thank the Department of Mechanical Engineering at JNTUH College of Engineering Sultanpur for their sup- port and resources.

10. Ethical Considerations

10.1. Data Privacy and Security

The implementation of the framework empha- sizes data privacy, ensuring compliance with regulations such as GDPR

10.2. Responsible Deployment

Consideration has been given to the ethical implications of deploying autonomous systems with advanced AI capabilities

11. References

Yang, Q., Liu, Y., Chen, T., Tong, Y. (2019).
Federated machine learning: Concept and ap- plications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.
Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), 1-40.
Dorri, A., Kanhere, S. S., Jurdak, R., Gau- ravaram, P. (2017). Blockchain for secure ve- hicular communications. IEEE Transactions on Intelligent Transportation Systems, 19(8), 2823-2835.
Hinton, G. E., Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neu- ral networks. Science, 313(5786), 504-507.
Ruttor, A., Pawelzik, K., Kinzel, W. (2005). Neural cryptography with feedback. Journal of Statistical Mechanics: Theory and Experi- ment, 2005(1), P01012.
Gupta, L., Jain, R., Vaszkun, G. (2017). Sur- vey of important issues in UAV communication networks. IEEE Communications Surveys Tu- torials, 18(2), 1123-1152.
Kerrigan, L. S. (2019). Secure communication in autonomous systems: A review. IEEE Ac- cess, 7, 145030-145045.
Zhou, Y., Wang, H. (2019). Security chal- lenges in autonomous robotic systems. Journal of Information Security, 10(3), 123-136.
Shor, P. W. (1999). Polynomial-time algo- rithms for prime factorization and discrete log- arithms on a quantum computer. SIAM Jour- nal on Computing, 26(5), 1484-1509.