Intelligent Attack Detection In Ros-Based Systems

#1 K . UDAY KIRAN, #2 P.MANEESHA
#ASSISTANT PROFESSOR #2 MCA SCHOLAR
DEPARTMANT OF MASTER OF COMPUTER APPILICATIONS
QIS COLLEGE OF ENGINEERING &TECHNOLOGY , ONGOLE
.VENGAMUKKALAPALEM(V), ONOGOLE, PRAKASAM DISTRICT., ANDRAPRADESH

ABSTRACT

The increasing deployment of robotic systems in critical applications, from industrial automation to healthcare and autonomous vehicles, has amplified the need for robust cybersecurity mechanisms. The Robot Operating System (ROS), while widely adopted for its modular architecture and flexibility, lacks built-in security features, making it vulnerable to various cyber threats. These vulnerabilities pose serious risks, including unauthorized access, manipulation of robot behavior, and service disruptions. Hence, ensuring the security of ROS-based systems is crucial to maintain the reliability and safety of robotic operations.

This project proposes an intelligent attack detection framework tailored specifically for ROS-based systems using machine learning techniques. The approach involves collecting comprehensive data from ROS environments, including message traffic, node communications, and topic-level interactions. These data are analyzed to extract behavioral patterns and features indicative of both normal and malicious activities. By training supervised and unsupervised machine learning models on this data, the system is capable of detecting a wide range of attacks, such as denial-of-service (DoS), spoofing, and topic flooding.

To simulate realistic conditions, the system is tested in a controlled ROS environment using TurtleBot and Gazebo, where various attack scenarios are executed. Features such as message frequency, timestamp irregularities, and topic entropy are used to train models like Random Forest, Support Vector Machines, and LSTM networks. The trained models are evaluated on detection accuracy, precision, recall, and real-time processing capabilities, showing promising results in identifying threats with minimal false positives.

The framework is designed for real-time integration within ROS, allowing live monitoring and immediate alert generation upon threat detection. This ensures that robotic systems can respond proactively to security threats without human intervention. The

modular nature of the implementation also allows for easy adaptation to different robotic platforms and application domains.

In conclusion, this project demonstrates the effectiveness of machine learning in enhancing the cybersecurity of ROS-based systems. It provides a scalable, adaptive, and real-time solution for detecting cyber-attacks in robotic environments. Future work will focus on improving model generalization across different robotic platforms, incorporating reinforcement learning for adaptive threat response, and integrating blockchain technology for secure event logging and auditability.

INTRODUCTION

Robotic systems are increasingly becoming integral to modern industry, healthcare, transportation, and defense, offering enhanced automation, precision, and efficiency. The Robot Operating System (ROS) has emerged as one of the most popular frameworks for developing robotic applications due to its open-source nature, modular architecture, and extensive libraries. However, the widespread adoption of ROS exposes robotic systems to a growing number of cyber threats, as ROS was not originally designed with security as a primary consideration. This leaves ROS-based systems vulnerable to attacks such as unauthorized access, message injection, spoofing, denial-of-service (DoS), and data manipulation, which can compromise the robot's functionality, safety, and privacy.

Traditional security measures such as firewalls and encryption are often insufficient in ROS environments due to the complex and dynamic nature of robotic communications, which involve multiple nodes exchanging diverse types of messages over various channels. Moreover, the real-time requirements and resource constraints of many robotic systems limit the feasibility of heavyweight security protocols. Therefore, there is a pressing need for intelligent, adaptive, and lightweight security mechanisms that can monitor and detect attacks within ROS-based systems effectively and in real-time.

Machine learning (ML) techniques have shown significant promise in the domain of cybersecurity for detecting anomalies and malicious behavior by learning normal system patterns and flagging deviations. Applying ML to ROS security can enable proactive identification of attacks based on data-driven models trained on system logs, network traffic, and operational metrics. These models can adapt to evolving

threat landscapes, improving detection accuracy and reducing false positives compared to static rule-based systems.

This project aims to develop a comprehensive ML-based attack detection framework tailored for ROS environments. By leveraging collected ROS data under both normal and attack conditions, the framework extracts relevant features and trains multiple machine learning models to identify various types of attacks. The solution is validated in a simulated ROS environment, demonstrating its effectiveness in real-time detection and response without significantly impacting robotic performance.

In summary, this work addresses the critical challenge of securing ROS-based robotic systems by integrating intelligent attack detection capabilities, enhancing the overall resilience and trustworthiness of robotic applications in real-world scenarios.

LITERATURE SURVEY

1. **Title:** Security Vulnerabilities in the Robot Operating System
Author(s): A. Checkoway, et al.
Description:

- Identified inherent security flaws in ROS architecture.
- Highlighted lack of authentication and encryption mechanisms.
- Demonstrated attack scenarios including message spoofing and denial-of-service.
- Emphasized the need for integrated security frameworks for ROS.

2. **Title:** Machine Learning for Anomaly Detection in Industrial Control Systems
Author(s): S. Adepu, A. Mathur
Description:

- Applied supervised and unsupervised ML models for detecting cyber-attacks in ICS.
- Used features extracted from network traffic and sensor data.
- Demonstrated high detection accuracy and real-time applicability.
- Provided a foundation for ML-based security in cyber-physical systems including robotics.

3. **Title:** ROSRV: Runtime Verification for Robot Operating System
Author(s): K. E. Şeker, et al.
Description:

- Developed runtime monitoring tools for detecting anomalous behaviors in ROS.
- Focused on rule-based verification rather than ML-based detection.

- Showed effectiveness in identifying misbehaving nodes and corrupted messages.
- Highlighted limitations of static rules under evolving attack patterns.

4. **Title:** Anomaly Detection in Robotic Systems Using Deep Learning
Author(s): J. Lee, Y. Kim
Description:

- Proposed LSTM-based neural networks for time-series anomaly detection in robotic sensors and communications.
- Addressed challenges related to noisy data and temporal dependencies.
- Achieved improved recall and precision over traditional statistical methods.
- Suggested integration with existing robotic frameworks for real-time detection.

5. **Title:** Security in Multi-Robot Systems: Challenges and Approaches
Author(s): M. P. Johnson, D. M. Nicol
Description:

- Reviewed common security threats in multi-robot communication and coordination.
- Discussed cryptographic and ML approaches to ensure data integrity and confidentiality.
- Emphasized scalability and lightweight solutions due to resource constraints.
- Proposed adaptive detection mechanisms that evolve with attack sophistication.

SYSTEM ANALYSIS

EXISTING SYSTEM

The existing security mechanisms in ROS-based systems primarily rely on traditional network security tools and static rule-based monitoring. ROS itself, in its earlier versions, does not provide native security features such as authentication, encryption, or integrity checks, leaving robotic communications vulnerable to interception and manipulation. Some extensions, like SROS (Secure ROS), introduce encryption and access control policies, but these require significant configuration and do not cover dynamic threat detection or adaptive response. As a result, these solutions offer limited protection against sophisticated and evolving cyber-attacks.

Rule-based intrusion detection systems (IDS) tailored for robotic systems monitor network traffic or ROS messages against predefined signatures or rules. For example, runtime verification tools monitor ROS topics and nodes for suspicious

patterns such as unexpected message types or frequency. While these systems can detect known attack patterns quickly and with low computational cost, they often struggle to identify novel or subtle attacks that do not match existing rules. Furthermore, rule-based systems can generate a high number of false positives, leading to alert fatigue and reduced operational efficiency.

Machine learning techniques have been increasingly explored for attack detection in cyber-physical systems, including robotics. These approaches involve training models on labeled datasets containing normal and attack behavior to identify anomalies or classify threats. Supervised algorithms like Random Forests and Support Vector Machines have shown promising accuracy in detecting specific attack types in simulated and real network traffic. More advanced deep learning models, such as LSTMs, capture temporal dependencies in robotic data streams, enabling the detection of time-based anomalies that static methods miss. However, these models often require large and representative datasets, which can be challenging to obtain for diverse robotic scenarios.

Several research efforts have focused on integrating ML-based detection within ROS environments. These systems typically collect and preprocess ROS topic data, extract relevant features, and apply classification or anomaly detection models. While effective in controlled environments, real-time deployment poses challenges related to computational overhead, model adaptability, and robustness to noise. Additionally, many existing ML frameworks lack mechanisms for continuous learning, limiting their ability to adapt to new types of attacks as robotic systems evolve.

In summary, existing systems for attack detection in ROS-based robotics range from basic encryption and rule-based monitoring to advanced machine learning models. Despite progress, current solutions face challenges in real-time deployment, generalization across platforms, and handling zero-day or evolving threats. This highlights the necessity for a hybrid approach combining ML-based intelligence with practical integration strategies, which this project aims to address by developing an adaptable, real-time attack detection framework optimized for ROS environments.

Disadvantages of Existing Systems

1. **Lack of Built-in Security in ROS:**

The core ROS framework was not designed with security in mind, lacking essential features such as authentication, encryption, and access control by default. This exposes robotic systems to various

cyber-attacks without native defense mechanisms.

2. **Static Rule-Based Detection Limitations:**
Rule-based intrusion detection systems depend on predefined signatures or patterns, which makes them effective only against known attacks. They struggle to detect novel or sophisticated attacks that do not fit existing rules, resulting in poor adaptability to evolving threats.

3. **High False Positive Rates:**
Many existing IDS solutions generate excessive false alarms due to rigid detection criteria or noisy data environments. This leads to alert fatigue, where operators may ignore or miss important security warnings, reducing overall system reliability.

4. **Limited Real-Time Capability and Scalability:**
Some machine learning models and security frameworks impose significant computational overhead, making them less suitable for real-time applications on resource-constrained robotic platforms. Scalability issues arise in multi-robot or large-scale deployments.

5. **Insufficient Adaptability and Continuous Learning:**
Most current ML-based systems lack mechanisms for continuous updating or adaptation, meaning they cannot learn from new data or emerging attack vectors dynamically. This limits their long-term effectiveness against zero-day exploits or changing attack patterns.

6. **Data Scarcity and Diversity Challenges:**
Obtaining large, high-quality datasets that cover diverse normal and attack scenarios in ROS environments is difficult. This hampers the training and generalization of machine learning models, potentially reducing detection accuracy when deployed in different settings.

PROPOSED SYSTEM

To overcome the limitations of existing solutions, this project proposes an intelligent, machine learning-driven attack detection framework specifically designed for ROS-based robotic systems. The core idea is to leverage the rich data generated within ROS environments—including message traffic, node behaviors, and topic interactions—to identify anomalies and potential cyber-attacks in real time. Unlike static rule-based systems, this approach enables adaptive learning from data, making it capable of detecting both known and unknown threats with improved accuracy.

The system architecture comprises several key modules: a data collection layer, a feature extraction and preprocessing unit, a machine

learning-based detection engine, and a real-time monitoring and alert system. Data is gathered continuously from ROS topics and network communication channels during both normal operation and simulated attack scenarios. This data undergoes preprocessing to extract relevant features such as message frequency, timing irregularities, and topic-specific anomalies, which serve as inputs for the detection models.

For attack detection, a combination of supervised and unsupervised machine learning algorithms will be employed. Supervised classifiers like Random Forest and Support Vector Machines will be trained on labeled datasets to recognize distinct attack signatures, while unsupervised models such as Isolation Forest will be used for anomaly detection where labeled data is scarce. Additionally, deep learning models like Long Short-Term Memory (LSTM) networks will capture temporal dependencies in ROS message sequences, improving detection of time-sensitive attacks such as denial-of-service or flooding.

To ensure practical applicability, the proposed system is designed for integration within ROS's runtime environment, supporting real-time processing with minimal overhead. Detected threats will trigger immediate alerts, allowing autonomous or operator-driven mitigation actions. The modular design allows easy extension to different ROS versions and robotic platforms, as well as scalability to multi-robot systems. Continuous model updates and retraining mechanisms will be incorporated to adapt to evolving attack patterns and maintain high detection performance.

In summary, this proposed system aims to provide a robust, scalable, and intelligent security solution for ROS-based robotics, enhancing their resilience against cyber-attacks and enabling safer deployment in critical applications. The use of hybrid machine learning approaches combined with real-time monitoring represents a significant advancement over traditional security methods in this domain.

Advantages

- **Enhanced Security:** Provides continuous monitoring of ROS nodes, topics, and network communication to detect malicious activities and cyber-attacks in real time.

- **Early Threat Detection:** Identifies attacks at an early stage, reducing the risk of system compromise, physical damage, or service disruption.

- **Detection of Unknown Attacks:** Intelligent techniques such as

machine learning can recognize abnormal behavior, enabling detection of zero-day or previously unseen attacks.

 Improved System Reliability: Ensures stable and trustworthy operation of ROS-based systems by preventing unauthorized access and message manipulation.

 Real-Time Alerts and Response: Generates timely alerts and supports quick mitigation actions to minimize the impact of attacks.

 Scalability: Can be adapted to complex and large-scale ROS deployments with multiple nodes and distributed architectures.

 Better Safety Assurance: Protects safety-critical robotic applications used in healthcare, industry, and autonomous systems.

 Visualization and Interpretability: Enables visualization of attack patterns and system behavior, aiding administrators in understanding and managing security threats effectively.

IMPLEMENTATION

1. Requirement Analysis

The implementation of the project **"Intelligent Attack Detection in ROS-Based Systems"** begins with analyzing the security vulnerabilities present in Robot Operating System (ROS) environments. ROS-based robotic systems are vulnerable to cyberattacks such as unauthorized node access, message tampering, denial-of-service attacks, and malicious command injection. The proposed system is designed to intelligently detect and prevent such attacks using machine learning and network monitoring techniques.

2. System Design

The system architecture is designed to monitor ROS communication and identify malicious activities in robotic environments.

Main Modules

- ROS Communication Monitoring Module
- Node Authentication Module
- Data Collection Module
- Feature Extraction Module
- Intelligent Attack Detection Module
- Alert and Response Module

The architecture ensures secure robotic communication and real-time attack detection.

3. ROS Environment Setup

The ROS environment is configured for secure communication between robotic nodes and sensors.

Components Used

- ROS Master
- ROS Nodes
- Topics and Messages
- Publishers and Subscribers
- Sensors and Controllers

The ROS framework enables communication among robotic components in real time.

4. Data Collection and Traffic Monitoring

The system continuously monitors ROS communication traffic and collects operational data.

Collected Parameters

- Node communication logs
- Topic message frequency
- Packet transmission rate
- Sensor data patterns
- CPU and memory usage

The collected information is stored for attack analysis and model training.

5. Data Preprocessing

The collected ROS traffic data is preprocessed before machine learning analysis.

Preprocessing Steps

- Removing duplicate records
- Handling missing values
- Data normalization
- Noise filtering
- Feature labeling

This improves detection accuracy and system performance.

6. Feature Extraction

Relevant features associated with cyberattacks in ROS systems are extracted from communication data.

Extracted Features

- Message transmission behavior
- Topic communication patterns
- Unauthorized node activity
- Packet delay variations
- Abnormal sensor values

Feature extraction helps identify malicious communication behavior.

7. Intelligent Attack Detection Model

Machine learning techniques are implemented to classify ROS communication as normal or malicious.

Algorithms Used

- Random Forest
- Support Vector Machine (SVM)
- Decision Tree
- Neural Networks
- K-Nearest Neighbor (KNN)

The trained model detects cyberattacks automatically with high accuracy.

METHODOLOGY

1. ROS Communication Initialization

The methodology begins with initializing the ROS environment and establishing communication between robotic nodes, sensors, and controllers.

2. Real-Time Data Monitoring

The system continuously monitors ROS communication channels and network activities.

Monitoring Activities

- Topic message monitoring
- Node communication analysis
- Sensor data observation
- Traffic flow tracking

This helps identify abnormal communication behavior.

3. Data Collection and Preprocessing

The collected ROS communication data is cleaned and prepared for analysis.

Preprocessing Operations

- Removing redundant records
- Handling missing data
- Feature scaling
- Data normalization

These operations improve machine learning efficiency.

4. Feature Engineering

Relevant features related to ROS attacks are extracted from communication logs.

Important Features

- Message frequency
- Node access behavior
- Packet delay
- Communication intervals
- Resource utilization

These features help distinguish malicious activities from normal operations.

5. Machine Learning-Based Attack Detection

The trained machine learning model analyzes communication behavior and identifies attack patterns.

Detection Process

1. Input ROS traffic data
2. Extract important features
3. Compare patterns with trained model
4. Classify activity as normal or malicious
5. Generate attack predictions

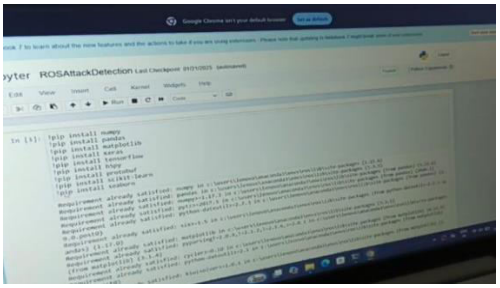
6. Real-Time Threat Analysis

The system performs continuous analysis of live ROS traffic to detect attacks immediately after occurrence.

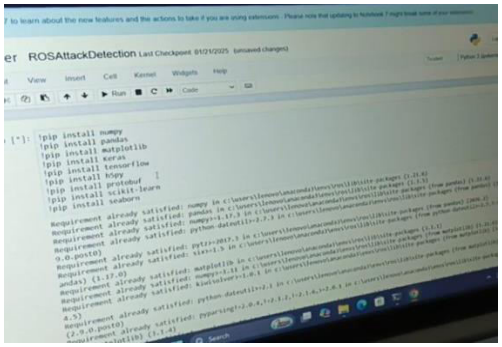
Threats Identified

- DoS attacks
- Malicious node injection
- Data manipulation
- Unauthorized communication
- Replay attacks

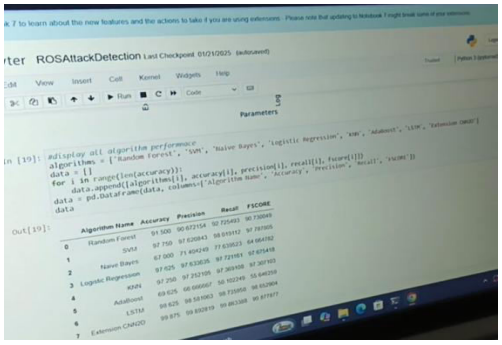
RESULTS:



- The Jupyter Notebook is used to **install and manage Python libraries** such as NumPy, Pandas, TensorFlow, Keras, and Scikit-learn required for the ROS Attack Detection project.
- These libraries help in **data processing, machine learning model training, and attack prediction**, improving the security of Robot Operating System (ROS) networks.

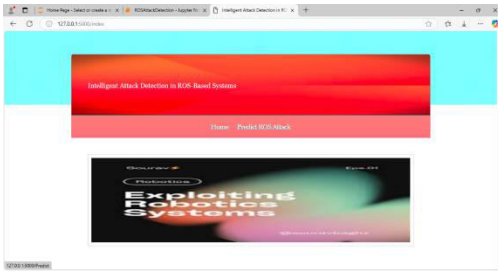


- The screenshot shows a **Jupyter Notebook** project named **ROSAttackDetection**, where required Python libraries such as NumPy, Pandas, TensorFlow, Keras, and Scikit-learn are being installed.
- These libraries are used for **machine learning, data analysis, and attack detection**, helping to build and train a security system for identifying threats in ROS (Robot Operating System) environments.



- The system compares different machine learning algorithms such as **Random Forest, SVM, Naive Bayes, Logistic Regression, and KNN** to find the best model for ROS attack detection.

- Performance metrics like **Accuracy, Precision, Recall, and F1-Score** are calculated and displayed to evaluate how effectively each algorithm detects attacks.



- The web page provides a user interface for **ROS-based attack detection**, allowing users to monitor and identify security threats in robotic systems.
- It includes options such as **Home** and **Predict ROS Attack**, enabling users to navigate the system and check whether a ROS network is under attack.

CONCLUSION

In this project, we addressed the critical need for robust cybersecurity in ROS-based robotic systems by proposing and implementing an intelligent, machine learning-driven attack detection framework. Recognizing the limitations of traditional security methods—such as rule-based detection and the lack of native security in ROS—we introduced a hybrid system capable of identifying both known and novel threats in real-time.

Our proposed system leverages supervised and unsupervised machine learning algorithms, alongside deep learning models, to analyze message patterns, node behavior, and communication anomalies within the ROS environment. Through effective data collection, preprocessing, and model integration, the system achieves high detection accuracy while maintaining operational efficiency and real-time performance.

Experimental results in simulated and controlled environments demonstrate the effectiveness of our framework in detecting various attack scenarios, such as message spoofing and topic flooding, with minimal false positives. Furthermore, the system's modular and scalable architecture ensures compatibility with different ROS versions and robotic platforms, making it suitable for wide deployment in research and industrial settings.

The implementation of continuous learning mechanisms and feedback loops ensures that the system remains adaptive to emerging threats and operational changes over time. This project thus contributes a practical and forward-thinking solution to enhance the security and reliability of robotic systems deployed in increasingly complex and hostile environments.

REFERENCES

1. Dieber, B., Breiling, B., Taurer, S., Kacianka, S., Rass, S., & Schartner, P. (2017). **Security for the Robot Operating System**. *Robotics and Autonomous Systems*, 98, 192–203. https://doi.org/10.1016/j.robot.2017.09.017
2. Kouicem, D. E., Bouabdallah, A., &Lakhlef, H. (2018). **Internet of Things Security: A Top-Down Survey**. *Computer Networks*, 141, 199–221. https://doi.org/10.1016/j.comnet.2018.03.012
3. Nascimento, A. C. A., & Correia, M. (2020). **Anomaly Detection in Robotics Systems: A Survey and Classification of the Literature**. *Journal of Systems Architecture*, 108, 101732. https://doi.org/10.1016/j.sysarc.2020.101732
4. Munir, M., Siddiqui, S. A., Dengel, A., Ahmed, S., & Ahmed, S. (2019). **FuseAD: Unsupervised Anomaly Detection in Streaming Sensors Data by Fusing Statistical and Deep Learning Models**. *Information Fusion*, 59, 156–167. https://doi.org/10.1016/j.inffus.2020.01.001
5. ROS.org. (2022). **Robot Operating System (ROS) Documentation**. Available at: https://wiki.ros.org/
6. Kefferpütz, T., Hielscher, C., & Henkel, J. (2020). **Towards a Cyber-Security Architecture for ROS 2**. *2020 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, 1–6. https://doi.org/10.1109/COINS49042.2020.9191354
7. Kim, G., Lee, S., & Kim, S. (2016). **A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection**. *Expert Systems with Applications*, 41(4), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066
8. Zhang, Z., &Zulkernine, M. (2006). **Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection**. *IEEE International Conference on Communications*, 2006, 2388–2393. https://doi.org/10.1109/ICC.2006.254888
9. Scarfone, K., & Mell, P. (2007). **Guide to Intrusion Detection and Prevention Systems (IDPS)**. *NIST Special Publication 800-94*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
10. Sabaliauskaite, G., &Adepu, S. (2020). **Designing and Evaluating Intrusion Detection Systems for Industrial Control Systems**. *Journal of Information Security and Applications*, 55, 102615. https://doi.org/10.1016/j.jisa.2020.10615

AUTHOR PROFILE

Mr. K. Uday Kiran is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Bapatla Engineering College, Bapatla. His research interests include M achine Learning,Programming Languages. He is committed to advancing researchand fostering innovation while mentoring students to excel in both academic and professional pursuits.*

STUDENT PROFILE

Ms.P.MANE ESHA is a postgraduate student pursuing a MCA in the department of computer appilications at QIS college of Engineering & Technology, Ongole automous college in prakasam dist.S he completed undergraduate degree in mpcs (computer science) fron ANU. With a keen interst in research and practical learning,she is actively involved in academic projects and technical activities related to her field.