INTELLIGENT ATTACK DETECTION IN ROS BASED SYSTEMS

[1]RUDRARAJU VASANTHI, [2]P.BOBBY SOWJANYA

[1]Students, Department of MCA, B V Raju College, Bhimavaram Ap

[2]Assistant Professor, Department of MCA, B V Raju College, Bhimavaram Ap

ABSTRACT

The increasing adoption of robotic systems in domains such as healthcare, manufacturing, and autonomous vehicles has led to the widespread use of the Robot Operating System (ROS) as a flexible middleware framework. However, ROS-based systems are inherently vulnerable to various cyber-attacks due to their distributed architecture, lack of built-in security mechanisms, and open communication protocols. Attacks such as node spoofing, message tampering, denial-of-service (DoS), and unauthorized access can compromise system integrity and safety. This project proposes an intelligent attack detection system for ROS-based environments using machine learning techniques to enhance security and resilience. The proposed system monitors communication between ROS nodes by capturing network traffic and message-level data such as topics, publishers, subscribers, and message frequencies. Data preprocessing techniques including filtering, normalization, and feature extraction are applied to prepare the dataset. Machine learning algorithms such as Random Forest, Support Vector Machines (SVM), and Artificial Neural Networks (ANN) are used to classify normal and malicious activities. Additionally, anomaly detection techniques are incorporated to identify unknown or zero-day attacks that are not present in the training data. Experimental results demonstrate that the proposed system effectively detects various types of attacks with high accuracy and low false-positive rates. Ensemble models such as Random Forest show strong performance due to their ability to handle complex patterns in network behavior. The system can operate in near real-time, making it suitable for securing critical robotic applications. However, challenges such as dataset availability, real-time processing overhead, and evolving attack patterns remain. Overall, the proposed solution provides a scalable and intelligent approach to enhancing the security of ROS-based systems.

Keywords: Robot Operating System (ROS), Cybersecurity, Attack Detection, Machine Learning, Random Forest, Anomaly Detection, Intrusion Detection System (IDS), Robotics Security, Network Monitoring, Artificial Intelligence

I.INTRODUCTION

Robotic systems are increasingly being deployed in critical applications such as

healthcare, industrial automation, autonomous vehicles, and defense systems. These systems rely heavily on middleware frameworks like the Robot Operating System (ROS) to enable communication between different software components, known as nodes. ROS provides a flexible and modular architecture that allows developers to build complex robotic applications efficiently. However, its open and distributed design also introduces significant security vulnerabilities. By default, ROS lacks built-in authentication, encryption, and access control mechanisms, making it susceptible to various cyber-attacks such as node spoofing, message injection, denial-of-service (DoS), and unauthorized access.

As robotic systems become more connected and integrated with networks, the risk of cyber threats increases significantly. Traditional security mechanisms are often insufficient to detect sophisticated and evolving attacks in real-time. This has led to the adoption of intelligent security solutions based on machine learning and artificial intelligence. Machine learning algorithms can analyze communication patterns between ROS nodes, identify anomalies, and detect malicious activities. Techniques such as Random Forest, Support Vector Machines (SVM), and Artificial Neural Networks (ANN) have shown promising results in intrusion detection systems by learning complex patterns from data and distinguishing between normal and abnormal behavior.

The proposed system focuses on developing an intelligent attack detection framework for ROS-based systems using machine learning techniques. The system monitors network traffic and ROS message exchanges, extracts relevant features, and applies classification and anomaly detection models to identify potential threats. By providing real-time detection and alert mechanisms, the system enhances the security and reliability of robotic applications. This approach is particularly important for safety-critical systems where cyber-attacks can lead to severe consequences. Overall, the integration of machine learning with ROS security offers a powerful solution for protecting modern robotic systems from cyber threats.

II SURVEY OF RESEARCH

The study by M. Quigley et al. (2009) [1] introduced the Robot Operating System (ROS) as an open-source middleware for robotic applications. The methodology focuses on a distributed architecture where nodes communicate through topics and services. Results demonstrate that ROS provides flexibility and scalability for developing complex robotic systems. However, it lacks built-in security features such as authentication and encryption, making it vulnerable to cyber-attacks. This research forms the foundation for

understanding security challenges in ROS-based systems.

The work by A. Shabtai et al. (2012) [2] explored intrusion detection systems (IDS) using machine learning techniques. The methodology involves analyzing network traffic and system behavior to detect malicious activities. Results show that machine learning-based IDS can achieve high accuracy in detecting known attacks. However, detecting unknown or zero-day attacks remains a challenge. This study supports the use of machine learning for attack detection in ROS environments.

The research by S. Sicari et al. (2015) [3] discussed security and privacy issues in Internet of Things (IoT) systems. The methodology focuses on identifying vulnerabilities in distributed and connected environments. Results indicate that IoT systems are prone to attacks such as data tampering and unauthorized access. However, implementing strong security mechanisms can mitigate these risks. This research is relevant as ROS-based systems share similar characteristics with IoT systems.

The study by L. Breiman (2001) [4] introduced the Random Forest algorithm, an ensemble learning technique that improves classification accuracy. The methodology uses multiple decision trees to reduce overfitting and enhance prediction performance. Results demonstrate that Random Forest performs well in complex datasets. However, computational cost can be high. This research supports the use of Random Forest for detecting attacks in ROS systems.

The work by C. Cortes and V. Vapnik (1995) [5] introduced Support Vector Machines (SVM) for classification tasks. The methodology focuses on finding optimal decision boundaries in high-dimensional data. Results show that SVM is effective in intrusion detection applications. However, it requires careful parameter tuning. This study is relevant for classifying normal and malicious activities in ROS communication.

The research by V. Chandola et al. (2009) [6] provided a comprehensive survey on anomaly detection techniques. The methodology identifies unusual patterns in data that may indicate cyber-attacks. Results demonstrate that anomaly detection is effective in detecting unknown threats. However, it may produce false positives. This study is important for identifying zero-day attacks in ROS-based systems.

Additionally, recent advancements in cybersecurity for robotic systems have explored deep learning techniques such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) for attack detection. These models can capture complex spatial and temporal patterns in network traffic and system behavior. While they provide

higher accuracy, they also require large datasets and increased computational resources. Integrating these advanced techniques with traditional machine learning models can further enhance the effectiveness of intelligent attack detection systems in ROS environments.

III. WORKING METHODOLOGY

The proposed Intelligent Attack Detection system for Robot Operating System (ROS) begins with data collection from the communication layer of ROS-based systems. In a typical ROS environment, multiple nodes communicate through topics, services, and messages. The system captures network traffic and ROS-specific data such as message frequency, publisher-subscriber relationships, topic names, packet size, and time intervals. This raw data is collected using monitoring tools and logging mechanisms integrated within the ROS framework. In the preprocessing stage, noise and irrelevant data are removed, missing values are handled, and normalization is applied to ensure consistency across features. Feature extraction is then performed to identify key parameters that indicate normal or malicious behavior.

In the next stage, machine learning models are trained to detect cyber-attacks. Supervised learning algorithms such as Random Forest, Support Vector Machines (SVM), and Artificial Neural Networks (ANN) are used to classify system behavior as normal or malicious. The dataset is divided into training and testing sets to evaluate model performance. In addition to classification, anomaly detection techniques are applied to identify unknown or zero-day attacks that are not present in the training data. These techniques analyze deviations from normal communication patterns, such as unusual message rates or unauthorized node interactions. Ensemble methods are particularly effective in handling complex patterns and improving detection accuracy.

In the final stage, the trained model is deployed for real-time monitoring and attack detection. As the ROS system operates, incoming data is continuously analyzed, and the model predicts whether the activity is normal or malicious. If an attack is detected, the system generates alerts and logs the event for further analysis. The system can also trigger automated responses such as blocking suspicious nodes or isolating affected components. Performance metrics such as accuracy, precision, recall, and false-positive rate are used to evaluate system effectiveness. This methodology ensures a proactive and intelligent approach to securing ROS-based systems against cyber threats.

IV RESULTS EXPLANATIONS

The performance of the proposed intelligent attack detection system for Robot Operating System (ROS) is evaluated based on its ability to accurately detect malicious activities and

differentiate them from normal system behavior. Experimental results indicate that traditional rule-based security mechanisms are limited in detecting complex and evolving cyber-attacks. In contrast, machine learning-based approaches significantly improve detection accuracy by learning patterns from communication data between ROS nodes. Evaluation metrics such as accuracy, precision, recall, and F1-score demonstrate strong performance across different attack scenarios.

Among the implemented models, ensemble techniques such as Random Forest show superior performance due to their ability to handle high-dimensional data and capture nonlinear relationships between features. Support Vector Machines (SVM) also provide good classification results, particularly in distinguishing between normal and attack patterns in structured datasets. Artificial Neural Networks (ANN) further enhance detection accuracy by learning complex behavioral patterns, although they require more computational resources and training time. Comparative analysis reveals that combining classification models with anomaly detection techniques improves the system's ability to detect both known and unknown attacks.

The system was tested under various simulated attack conditions, including message spoofing, denial-of-service (DoS), and unauthorized node access. Results show that the system can detect attacks in near real-time with low false-positive rates. However, challenges such as dataset availability, real-time processing overhead, and adapting to new attack patterns remain. Despite these limitations, the system demonstrates high reliability and scalability. Overall, the results confirm that the proposed approach provides an effective and intelligent solution for enhancing the security of ROS-based robotic systems.

.

V.CONCLUSION

The proposed Intelligent Attack Detection in ROS-Based Systems presents an effective and advanced solution for enhancing the security of robotic environments. By leveraging machine learning techniques, the system successfully identifies malicious activities such as node spoofing, message tampering, and denial-of-service attacks within the Robot Operating System (ROS) framework. The integration of supervised learning models and anomaly detection techniques enables the system to detect both known and unknown threats, improving overall system reliability and safety.

Experimental results demonstrate that ensemble models such as Random Forest, along with advanced techniques like Artificial Neural Networks (ANN), achieve high accuracy and low false-positive rates in detecting cyber-attacks. The ability to monitor

real-time communication between ROS nodes and analyze behavioral patterns makes the system highly suitable for critical applications such as autonomous vehicles, healthcare robotics, and industrial automation. Additionally, the use of automated alert mechanisms and logging enhances system transparency and accountability.

In conclusion, the proposed system provides a scalable, intelligent, and robust approach to securing ROS-based systems. While challenges such as computational overhead, evolving attack patterns, and limited datasets exist, the benefits of improved security and real-time detection outweigh these limitations. Future work may focus on integrating lightweight models for edge deployment, incorporating advanced deep learning techniques, and enhancing real-time response mechanisms. Overall, this study highlights the importance of combining machine learning and cybersecurity to protect modern robotic systems from emerging threats.

REFERENCES

[1] M. Quigley et al., "ROS: An Open-Source Robot Operating System," in *Proc. IEEE Int. Conf. Robotics and Automation (ICRA) Workshop*, 2009.

[2] A. Shabtai, Y. Elovici, and L. Rokach, "A Survey of Data Leakage Detection and Prevention Solutions," *Springer*, 2012.

[3] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Comput. Netw.*, vol. 76, pp. 146–164, 2015.

[4] L. Breiman, "Random Forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001.

[5] C. Cortes and V. Vapnik, "Support-Vector Networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, 1995.

[6] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Comput. Surveys*, vol. 41, no. 3, pp. 1–58, 2009.

[7] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[8] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," *Nature*, vol. 521, pp. 436–444, May 2015.

[9] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST, 2007.

[10] W. Stallings, *Cryptography and Network Security*, 7th ed. Pearson, 2017.

[11] R. Mitchell and I. Chen, "A Survey of Intrusion Detection Techniques for Cyber-Physical Systems," *ACM Comput. Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

[12] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed. Pearson, 2010.

[13] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, 2011.

[14] M. Abadi et al., "TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems," 2015.

[15] F. Chollet, "Keras," 2015.

[16] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*. Morgan Kaufmann, 2011.

[17] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*. Springer, 2009.

[18] C. M. Bishop, *Pattern Recognition and Machine Learning*. Springer, 2006.

[19] R. Kohavi, "A Study of Cross-Validation and Bootstrap for Accuracy Estimation," in *Proc. IJCAI*, 1995, pp. 1137–1143.

[20] D. Powers, "Evaluation: From Precision, Recall and F-Measure to ROC," *J. Mach. Learn. Technol.*, 2011.