International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Defense utility robot

[1]Lachi Hari Krishna,[2]Inguva Venkata Naga Manikanta Sai Raman, [3]Kosuri Vishnu Vardhan, [4]Keerthi Prem Kumar,[5]Y. John Varakumar

[1,2,3,4]U. G Student, Dept ELECTRONICS AND COMMUNICATION ENGINEERING, St. Ann's College of Engineering and Technology, (Autonomous)Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

[5]Associate Professor, Dept ELECTRONICS AND COMMUNICATION ENGINEERING, St. Ann's College of Engineering and Technology (Autonomous), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

Abstract: Military operations often involve dangerous tasks such as surveillance, border monitoring, and intruder detection, which can put soldiers' lives at risk. To overcome these challenges, a wireless military defense robot is proposed to perform surveillance and monitoring activities in hazardous environments. The system utilizes NodeMCU, Wi-Fi communication, sensors, and mobile technologies to provide both automatic and manual control. It incorporates ultrasonic, PIR, infrared, flame, and gas sensors for threat detection and monitoring. The robot also uses Skype video calling for real-time surveillance, reducing the need for expensive camera systems. The proposed solution offers a cost-effective, energy-efficient, and reliable approach for military and defense applications.

KEYWORDS- Defense Robot, Wireless Communication, NodeMCU, Wi-Fi Technology, Surveillance System, Military Application, Ultrasonic Sensor, PIR Sensor, Skype Video Calling, IoT.

INTRODUCTION

Recent advancements in robotics and wireless communication technologies have significantly improved the efficiency of surveillance and monitoring systems. In military and defense sectors, soldiers often face life-threatening situations while performing border surveillance and reconnaissance operations. To reduce human risk and improve operational effectiveness, defense robots are increasingly being deployed in hazardous environments. These robots can perform surveillance, monitor enemy activities, and transmit real-time information to authorized personnel. Various communication technologies such as

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

ZigBee, RFID, Bluetooth, and Wi-Fi have been used in robotic systems for remote control and monitoring. The proposed wireless military defense robot uses NodeMCU with Wi-Fi communication and multiple sensors to provide both automatic and manual operation modes. The system enhances surveillance capabilities while reducing operational costs and power consumption.

RELATED WORK

Numerous defense robots have been developed using communication technologies such as ZigBee, Bluetooth, RFID, and Wi-Fi. Existing systems focus on surveillance, intruder detection, remote monitoring, and battlefield reconnaissance. Most systems utilize cameras, wireless communication modules, and sensors to provide live monitoring and control capabilities. While these robots have improved military operations, many suffer from limited communication range, high implementation costs, increased power consumption, and dependence on expensive surveillance equipment. Recent research has therefore focused on integrating cost-effective communication technologies and intelligent control systems to improve surveillance efficiency while minimizing operational complexity.

LITERATURE SURVEY

Several researchers have developed robotic systems for military surveillance and defense applications. Joshi and Tondarkar proposed a surveillance robot using Raspberry Pi and IoT technologies for monitoring border areas. Their system provided live video streaming and supported both automatic and manual operation through web-based control. Bhatnagar and Gola introduced a rough terrain defense robot that incorporated infrared, PIR, ultrasonic sensors, Bluetooth, and Wi-Fi technologies for multipurpose military applications. Another study by Tarunpreet Kaur presented a wireless multifunctional robot based on 3G technology that enabled unlimited communication range, autonomous navigation, and live video transmission for surveillance in remote locations. Premkumar Manoharan developed an intelligent unmanned robot using ZigBee wireless sensor networks to detect intruders and automatically perform defense operations while reducing human intervention. Furthermore, Saliyah Kahar discussed the utilization of mobile technologies such as Bluetooth, Wi-Fi, and 3G for robot control, highlighting their communication performance and applicability in robotic systems. Although

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

these systems improved military surveillance and monitoring, they faced limitations related to communication range, battery consumption, and deployment costs, creating the need for a more efficient and economical solution.

EXISTING METHOD

The existing military surveillance robots utilize technologies such as ZigBee, Bluetooth, RFID, and 3G communication for monitoring and control. These systems generally employ cameras, wireless sensors, and microcontrollers to perform surveillance and intruder detection tasks. Some robots provide autonomous navigation, while others require manual control through mobile devices or computers. Although effective for surveillance, these systems often rely on expensive camera equipment and continuously active monitoring, leading to higher power consumption and increased operational costs. Additionally, communication range limitations in ZigBee and Bluetooth-based systems restrict their effectiveness in large-scale military environments.

PROPOSED METHOD

The proposed wireless military defense robot utilizes a NodeMCU controller integrated with Wi-Fi technology to provide efficient communication and control. The robot operates in both automatic and manual modes, allowing flexibility in surveillance operations. Various sensors, including ultrasonic, PIR, infrared, flame, and gas sensors, continuously monitor the environment and detect potential threats. Whenever abnormal activity is detected, alert messages are transmitted to a web server for immediate response. Instead of using expensive surveillance cameras, the system employs Skype video calling through a smartphone mounted on the robot to provide real-time video streaming. This approach significantly reduces system cost while maintaining effective monitoring capabilities. The proposed design also conserves battery power by activating surveillance functions only when required, making the system more efficient and suitable for military applications.

SYSTEM ARCHITECTURE

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

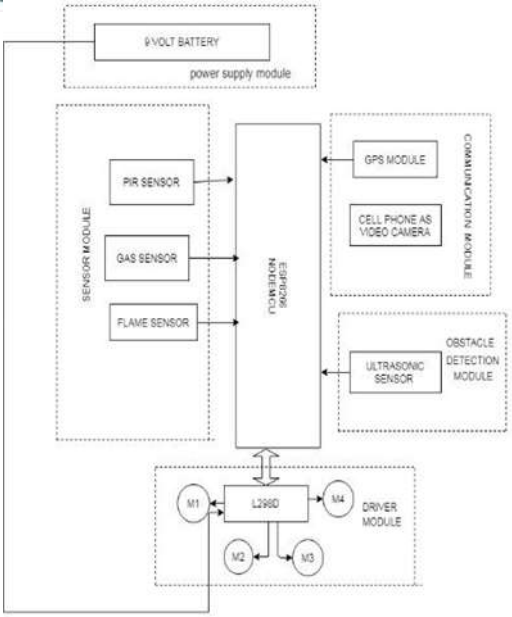

Fig.1 System Architecture

MODULE DESCRIPTION

NodeMCU Controller Module: The NodeMCU acts as the main controller of the defense robot and manages the overall system operation. It receives input from various sensors, processes the collected data, and controls robot movement and communication functions. The built-in Wi-Fi capability enables seamless connectivity with remote monitoring systems. This module serves as the central intelligence unit of the robot.

Wi-Fi Communication Module: The Wi-Fi module enables wireless communication between the defense robot and authorized users. It allows remote monitoring, control, and transmission of sensor data through internet connectivity. This module ensures real-time communication without requiring physical connections. It enhances operational flexibility in military surveillance applications.

Ultrasonic Sensor Module: The ultrasonic sensor is used to detect obstacles and measure the distance between the robot and surrounding objects. It helps the robot navigate safely by avoiding collisions during movement. The sensor continuously emits ultrasonic waves and calculates distance based on the reflected signals. This module supports autonomous navigation and path planning.

PIR Sensor Module: The Passive Infrared (PIR) sensor detects human presence by sensing changes in infrared radiation emitted by living beings. It plays an important role in identifying intruders and unauthorized movement in surveillance areas. Once motion is detected, the sensor triggers an alert for immediate action. This improves the robot's security monitoring capability.

Infrared Sensor Module: The infrared sensor is responsible for detecting nearby objects and environmental changes. It assists the robot in obstacle avoidance and improves navigation accuracy. The sensor continuously monitors the surroundings

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

and provides input to the controller for decision-making. This module enhances the overall efficiency of the surveillance system.

Flame Sensor Module: The flame sensor detects the presence of fire and abnormal heat sources in the monitored environment. When fire is detected, the sensor immediately sends a signal to the controller, which generates an alert notification. This helps prevent accidents and enables rapid emergency response. The module improves safety in military and hazardous environments.

Gas Sensor Module: The gas sensor monitors the surrounding atmosphere for the presence of harmful or toxic gases. It continuously measures gas concentration levels and alerts the system when dangerous conditions are detected. This feature helps protect military personnel from hazardous environmental conditions. The module enhances environmental safety and threat detection.

Surveillance Module: The surveillance module utilizes a smartphone mounted on the robot along with Skype video calling technology for live video streaming. It allows authorized users to remotely monitor the robot's surroundings in real time. This approach eliminates the need for expensive surveillance cameras while maintaining effective monitoring capabilities. The module provides continuous visual feedback during military operations.

Alert Notification Module: The alert notification module is responsible for informing authorized personnel whenever any threat, intrusion, fire, gas leakage, or abnormal activity is detected. Alerts are transmitted through the web server and communication network for immediate response. The module ensures timely notification and improves situational awareness. This helps enhance the overall effectiveness of the defense system.

RESULTS AND DISCUSSION

The proposed Wireless Military Defense Robot was successfully designed to perform surveillance, obstacle detection, intruder monitoring, and environmental sensing in military and border security applications. The integration of NodeMCU with Wi-Fi communication enabled efficient remote control and real-time data transmission. Sensors such as PIR, ultrasonic, flame, and gas sensors accurately detected human movement, obstacles, fire, and harmful gases, improving the robot's situational awareness. Furthermore, the use of Skype

video calling through a smartphone provided reliable live video streaming at a significantly lower cost than conventional surveillance cameras. The experimental analysis demonstrates that the proposed system offers enhanced monitoring capabilities, reduced power consumption, improved battery efficiency, and cost-effective operation, making it suitable for defense and surveillance environments.

CONCLSUION AND FUTURE SCOPE

The proposed wireless military defense robot offers an effective solution for military surveillance and border security by integrating wireless communication, environmental sensing, and real-time monitoring technologies. The system reduces human risk, minimizes operational costs, and improves surveillance efficiency through intelligent automation. Future enhancements may include artificial intelligence-based target recognition, autonomous path planning, advanced night-vision systems, and drone integration for extended surveillance coverage. These improvements can further enhance the reliability and effectiveness of defense robotic systems.

REFERENCES

1. S. A. Joshi and A. Tondarkar, "Surveillance Robot for Military Application," *International Journal of Engineering and Computer Science (IJECS)*, vol. 7, no. 5, 2018.
2. S. Bhatnagar and S. K. Gola, "A Review on Rough Terrain and Defense Robot," *International Journal of Scientific Research and Management (IJSRM)*, vol. 4, no. 10, 2016.
3. D. Kumar and T. Kaur, "Wireless Multifunctional Robot for Military Applications," *IEEE International Conference on Recent Advances in Engineering and Computational Sciences (RAECS)*, 2015.
4. P. Manoharan, "Unmanned Multifunctional Robot Using ZigBee Adopter Network for Defense Application," *International Journal of Engineering Research and Applications*, ISSN: 2278-1323.
5. S. Kahar and R. Souilman, "Utilization of Mobile Technology for Mobile Robot Controller," *IEEE Conference on Open Systems (ICOS)*, 2011.
6. Hargovind, "NodeMCU-Based IoT Project: Connecting MQ2 Sensor," *Hackster.io*, Available Online.
7. "Interfacing GSM and GPS Module Using Arduino: A Step-by-Step Guide for Tracking," *Steemit Technical Tutorials*, Available Online.
8. "Flame Detection Alert System Using NodeMCU," *Boodskap Community Resources*, Available Online.

9. Dhana Lakshmi et al., "Surveillance Robot System for Security Applications," *International Journal of Advanced Engineering and Green Technology (IJAEGT)*, 2014.
10. "Radio Frequency Controlled Surveillance Robot," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)*, 2015.
11. Divakar K., "IEEE Conference Paper on Military Surveillance Robotics," *SlideShare Technical Publication*, Available Online.
12. "Bluetooth Technology Based Wireless War Field Robot with Night Vision Camera," *International Journal of Engineering Development and Research (IJEDR)*, 2017.
13. "Multifunctional Robot Using ZigBee," *International Journal of Technical Research and Engineering (IJTRE)*, 2016.
14. "Surveillance Robot for Defense Environment," *International Journal of Research and Analytical Reviews (IJRAR)*, 2018.
15. "Wireless Controlled Surveillance Robot," *International Journal of Advanced Research in Computer Science and Management Studies (IJARCSMS)*, vol. 2, no. 2, 2014.
16. Babburi, S. Lightweight Distributed Provenance Framework for Edge and IoT Data Systems.
17. Gaddam, S. From Fixed Specifications to Self-Adapting Systems: A Machine Learning Perspective on Software Engineering.
18. Immadi, S. K. (2025). Optimizing ERP for Human Capital Management. Applied Research for Growth, Innovation and Sustainable Impact, 377–384. https://doi.org/10.1201/9781003684657-63
19. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
20. Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.
21. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
22. Viswanathan, V. Generative AI for Smarter Workforce Planning and Enterprise Resource Decisions.
23. Gajula, S. (2026, March). Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
24. Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.

25. P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. Eudoxus Press Journal.
26. Srikanth Kavuri. (2025). AI-DRIVEN TEST AUTOMATION FRAMEWORKS: ENHANCING EFFICIENCY AND ACCURACY IN SOFTWARE QUALITY ASSURANCE. International Journal of Applied Mathematics, 38(10s), 699–710. https://doi.org/10.12732/ijam.v38i10s.990
27. Gummadi, V. P. K., Chilamkurthi, L. S., & Kavuri, S. (2026). Service Level Objective (SLO) Observability with Splunk and Dynatrace in Microservices. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–4. https://doi.org/10.1109/icaiset66439.2026.11541542
28. Shashank, A. (2025). AI-Enhanced ETL Processes: Leveraging Artificial Intelligence for Optimized Data Integration Systems. Journal Of Multidisciplinary, 5(8), 219-225.
29. Kandula, S. T. R., Susarla, R. S., & Boyapati, P. K. (2025, July). Enhanced Cyber Security Using Global Local Artificial Neural Network Based Intrusion Detection in Big Data Environment. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 426-431). IEEE.
30. Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219