Integration of Cryptography and Navigation Systems in Unmanned Military Mobile Robots: A Review of Current Trends and Perspectives

Makhabbat Bakyt[1], Khuralay Moldamurat[1], Assem Konyrkhanova[1], Adil Maidanov[1] and Dina Satybaldina[1]

[1]*L.N. Gumilyov Eurasian National University, Satpayev 2, Astana, 010008, Kazakhstan*

Abstract

This paper addresses the intersection of military robotics, secure data transmission, and reliable navigation systems. The navigation system is tailored for maze traversal, allowing an operator to set start and end points through Matlab functions. Navigational data, obtained from a camera situated above the terrain, is transmitted to a PC via S-video input, initiating a Matlab-based navigation algorithm.

The study emphasizes cybersecurity and precise navigation, incorporating cryptographic methods in LoRa communication devices and implementing quantum-resistant algorithms in secure robot operating systems. An image processing algorithm facilitates route planning within the maze, generating a comprehensive overview of contemporary techniques. Visual representations of the wireless robot navigation system and maze encryption algorithm are included for clarity.

Keywords

Military robotics, cryptography, navigation, cybersecurity, wireless communication, quantum-resistant algorithms

1. Introduction

With the rapid advancements in military robotics, the imperative for robust navigation systems and secure data transmission is evident, particularly amid escalating cyber threats. This article centers on the evolving landscape of unmanned military mobile robots, specifically highlighting the integration of cryptography and navigation systems.

Our proposed navigation framework relies on operator-defined waypoints within a maze, facilitated through Matlab functions. A camera situated above the robot's two-dimensional black-and-white maze captures navigational data within its field of view [1, 2]. Utilizing the S-video input of a TV card, the camera's data is transmitted to a PC, where a Matlab-based navigation algorithm initializes the XBee sending device as a serial port.

This discussion underscores the dual focus on enhancing cybersecurity and ensuring precise navigation. Cryptographic techniques are deployed in LoRa communication devices, complemented by the integration of quantum-resistant algorithms in secure robot operating systems.

A key highlight involves an image processing algorithm for maze route planning. The operator defines initial and final points, with the camera capturing a black-and-white maze image. Matlab processes this image, generating a sequence of points outlining the route [3, 4]. These coordinates are stored in a data vector, enabling the robot to traverse the predetermined path.

This article not only explores cybersecurity intricacies but also investigates methodologies for meticulous navigation. It provides a comprehensive survey of contemporary techniques and

DTESI 2023: Proceedings of the 8th International Conference on Digital Technologies in Education, Science and Industry, December 06–07, 2023, Almaty, Kazakhstan

bakyt.makhabbat@gmail.com (M. Bakyt); khuralay03@gmail.com (K. Moldamurat); erkeshank@mail.ru (A. Konyrkhanova); makeadil@mail.ru (A. Maidanov); satybaldina_dzh@enu.kz (D. Satybaldina)

0000-0002-1246-9696 (M. Bakyt); 0000-0002-3691-6948 (K. Moldamurat); 0000-0002-4923-9800 (A. Konyrkhanova); 0000-0003-2392-5164 (A. Maidanov); 0000-0003-0291-4685 (D. Satybaldina)

technologies in this domain [5, 6]. Figures 1 and 2 visually depict the wireless robot navigation system and the maze encryption algorithm implementation, respectively.

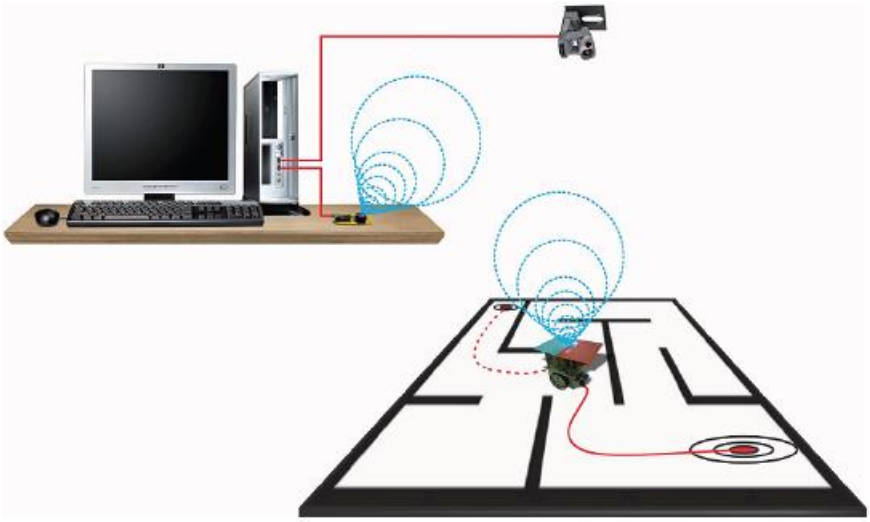

Figure 1: Implemented Wireless Robot Navigation System

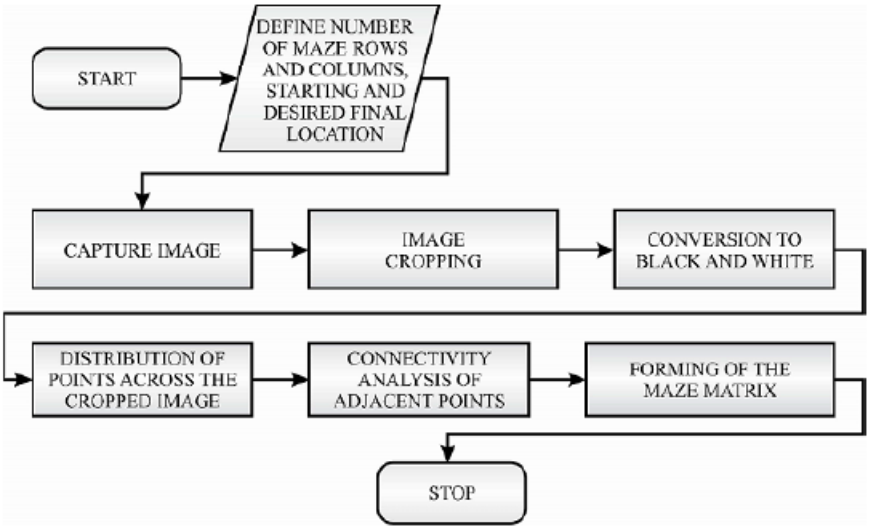

Figure 2: Maze Encryption Algorithm Flow Chart

2. Research method

The research methodology centers on a tailored hardware circuit design for effective control and supervision of wheeled robots, establishing a foundational framework. Illustrated in Figure 3, the block operation control system diagram outlines key components of a remote wheeled robot employing the SIM 908-C module [7, 8]. Two primary blocks are delineated: Block 1 for remote control and Block 2 representing the robot with wheels.

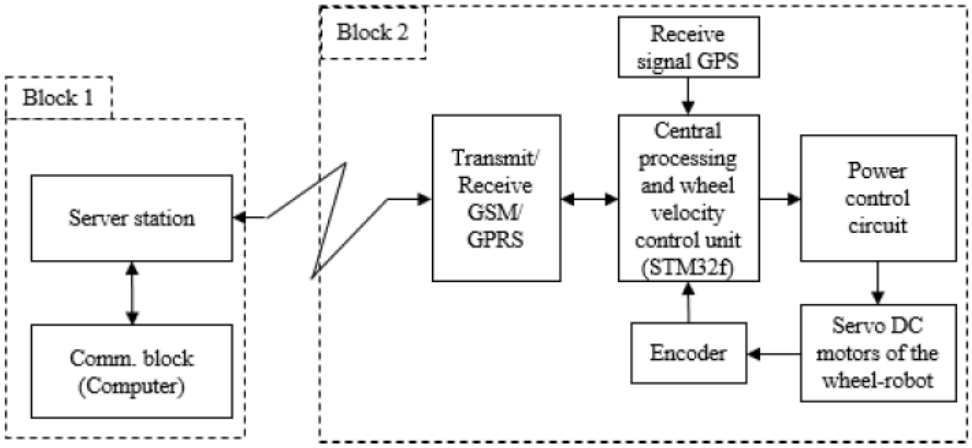

Figure 3: Block Operation Control System Block Diagram

Block 1 (Remote Control Robot) is equipped with a Tram Server for data storage and a Samsung Notebook S04VN computer running monitoring control software. Block 2 (Robot with Wheels) includes an STM32f microcontroller, a SIM908-C module for GSM/GPRS/GPS functionalities, and an R4WD chassis housing 4 servo DC motors with integrated encoders.

The principal circuit diagram elucidates the central processing and velocity control unit, communication block, SIM908-C module, and power block [9, 10]. This detailed visualization enhances comprehension of the intricate interconnections and functionalities within the system.

The wheeled-robot control algorithm, depicted in Figure 4, features a comprehensive flowchart governing hardware operations. Initiating with SIM908 module activation, initial data initialization, and signal status verification, the algorithm establishes GPRS/GPS communication with the server and seamlessly executes remote control through interface software.

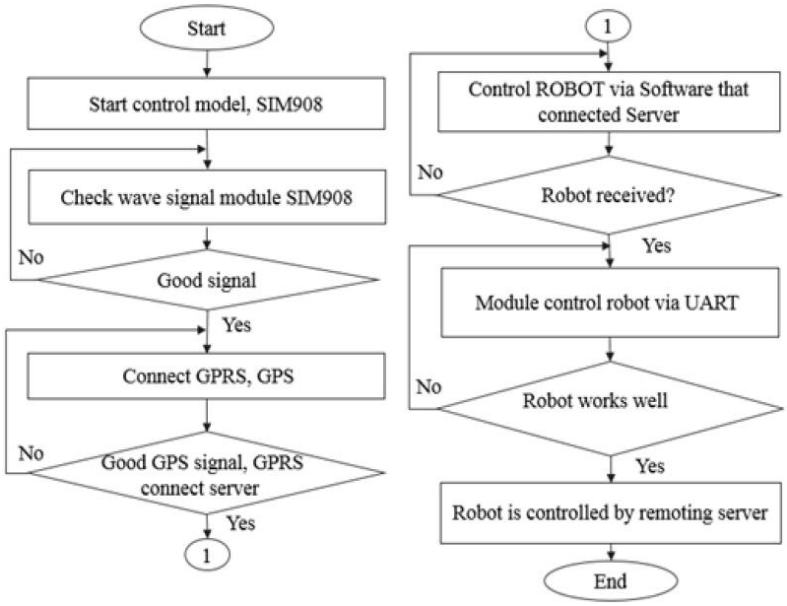

Figure 4: General Algorithm Flowchart for Wheeled-Robot Control via GSM/GPRS/GPS

This hardware circuit design serves as a pivotal component orchestrating a sophisticated system for wheeled-robot control and supervision.

In the subsequent assessment of our proposed protocol's performance, a custom C++ simulator was employed for experiments under different conditions [11, 12]. Simulations involved placing varying numbers of nodes randomly within a fixed area, simulating scenarios without mobility. Essential parameters considered were sensor transmission range, transmission rate, and observation time, with each experiment repeated multiple times for robustness.

Evaluation relied on two crucial metrics:

– Percentage of False Positives (Pfp): Identifying situations where the protocol incorrectly concludes the presence of a sensor when there isn't one.

– Percentage of False Negatives (Pfn): Identifying cases where the protocol erroneously concludes a cell lacks a sensor when it actually contains one or more sensors.

Insights from the evaluation, particularly regarding tradeoffs with only AoA information and the impact of RSS information filtering, are detailed (Figure 5). The methodology, grounded in rigorous simulation and analysis, sheds light on the protocol's efficacy across diverse scenarios [13, 14].

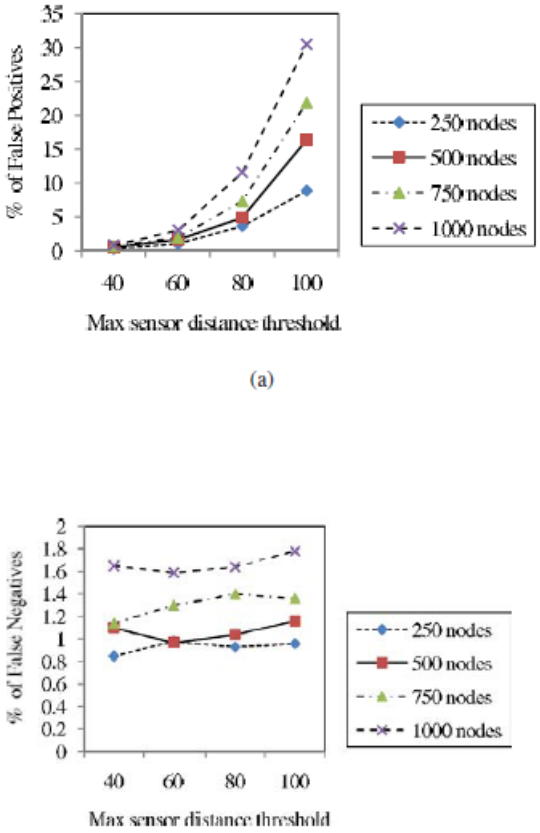

Figure 5: Impact of RSS Information Filtering on False Positives and False Negatives

The deployment methodology involves a Mobile Ad-Hoc Network (MANET) where robotic nodes form the network. This aims to strategically position nodes for communication points in communication-challenged areas [15, 16]. Wi-Fi technology with a theoretical range of 100 meters is chosen for network deployment. The proposed system integrates functionalities such as remote robot control, audio/video streaming, object tracking, and wireless network deployment.

Each network node comprises an iRobot Roomba vacuum robot connected to a Raspberry Pi. The Raspberry Pi serves as the node's core, managing commands, communications, and connections with other nodes. The network architecture configures two Wi-Fi interfaces on each Raspberry Pi, with one in reception mode and the other in Ad Hoc mode.

For a visual representation of the proposed system, refer to Figure 6 and Figure 7 in the corresponding sections.

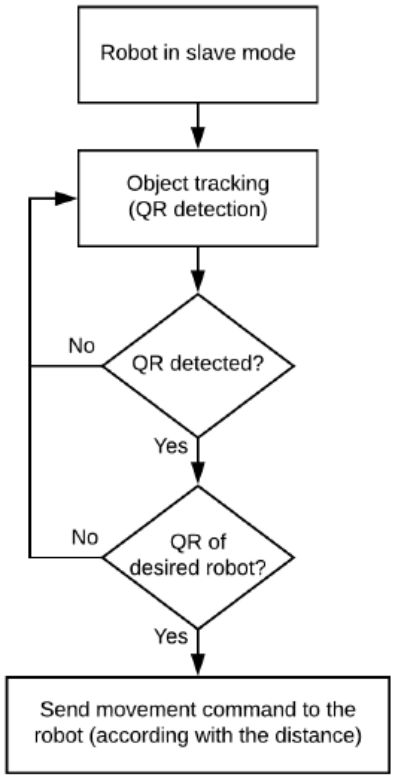

Figure 6: Network Node Configuration and Operation Diagram

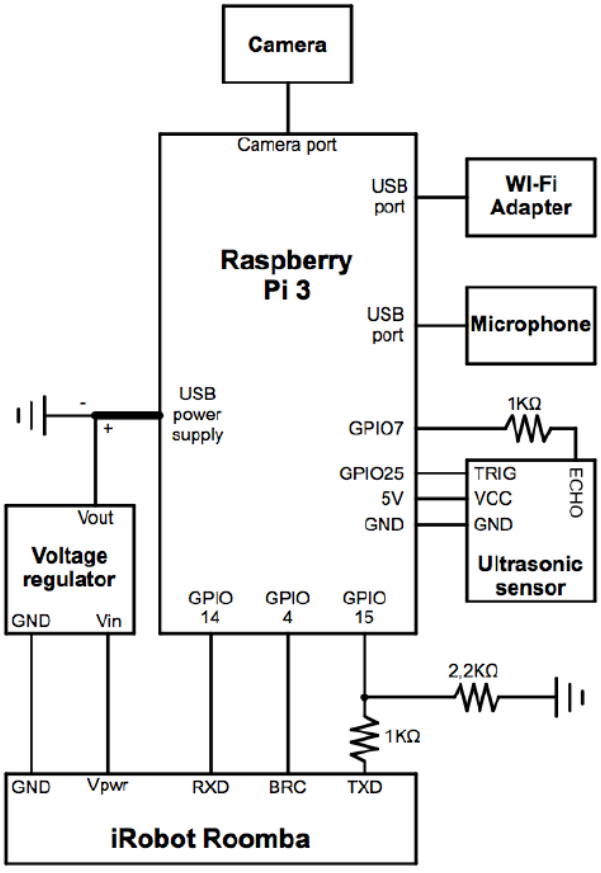

Figure 7: Node Wiring and Connection Schematic

In conclusion, this research method establishes the foundation for deploying a Robotic Ad Hoc Network (RANET) using autonomous robots as network nodes. The proposed system incorporates remote control, streaming, object tracking, and wireless network deployment functionalities [17, 18]. Figures 4 and 6 visually encapsulate key aspects of network configuration and node connections, setting the stage for a comprehensive exploration of results and findings in the following sections.

3. Results and discussion

In this section, we delve into the outcomes and discussions derived from the implementation and analysis of encryption methodologies in cutting-edge robotic systems, emphasizing the implications, challenges, and advancements in securing communication within robotic networks [19, 20]. Our exploration builds upon recent articles, such as "Message Encryption in Robot Operating System: Collateral Effects of Hardening Mobile Robots," "Post Quantum Secure Command and Control of Mobile Agents: Inserting Quantum-Resistant Encryption Schemes in the Secure Robot Operating System," and "Implementing Cryptography in LoRa Based Communication Devices for Unmanned Ground Vehicle Applications."

As autonomous technologies integrate into diverse domains, the pursuit of secure communication in robotic systems becomes paramount. Navigating through the results and discussions, we aim to unravel the intricacies of message encryption strategies and their impact on the overall performance and security of modern robotic platforms.

Application-Level Encryption and Computational Considerations

This section examines the ramifications of encrypting diverse blocks of information at the application level through an ad hoc solution. Leveraging technologies such as ROS, PyCrypto, and Python, our exploration unveils crucial scenarios that necessitate consideration before deploying arbitrary solutions to an operational robot. The computational units scrutinized in this study, termed Powerful CU (i7) and Medium CU (Atom), delineate the boundary of our research scope [21-22].

The investigation identifies AES as a superior encryption solution, demonstrating lower CPU utilization than alternative algorithms. However, it introduces a significant data overhead in the network, rendering it less suitable for multi-robot environments or applications requiring continuous interaction with consoles or external devices. Certain encryption modes, such as ECB-mode, lack semantic security and are discouraged due to inherent vulnerabilities.

Our study elucidates a correlation between message types, message rates, and the computing platform's capabilities in encrypted communications planning. Large-sized data chunks, such as image messages, impose a strain on the system, particularly affecting sensors generating high-rate data like cameras and LIDARs.

In light of the experimental findings, we propose a taxonomy for ROS communications hardening, considering the computing units and message types involved (Table 1).

Table 1
Impact of Encryption on Robot Operational Modes

CPU type	Robot system	Encryption block		
		3DES	AES	BF
Powerful CU	Navigation	⊙	✓	✓
	Perception	⊙	✓	✓
	Dialog	⊙	✓	✓
Medium CU	Navigation	▾	▾	▾
	Perception	⊙	⊙	⊙
	Dialog	⊙	⊙	⊙

✓ = No problem, ▾ = Not affordable, ⊙ = Affordable with minor adjustments.

Illustrating the significance of these considerations, we contemplate a robot like Pepper7 equipped with multiple sensors, each impacting its performance differently. Our proposed taxonomy aids in decision-making, weighing the importance of encrypting each sensor based on the final deployment scenario and the robot's computing configuration.

Further observations reveal nuanced performance differences between the two computational units when subjected to different encryption modes, particularly under CBC mode. Power consumption emerges as a crucial factor, impacting the robot's autonomy during extended operational periods.

Additionally, the study explores the impact of encryption on network communication, highlighting its overhead, especially in wireless scenarios [23-24]. The discussion categorizes robot operational modes, emphasizing the affordability of encrypting messages between nodes when Powerful CUs are available. However, Medium CUs, like those in Turtlebot models, exhibit performance issues even in basic navigation or perception modes.

Our empirical experiments and ensuing discussions pave the way for a cybersecurity characterization model, aligning encryption algorithms with message types and security requirements. This model aids researchers and developers in customizing cybersecurity approaches, considering the security level needed, robot performance requirements, autonomy, and network overhead (Figure 8).

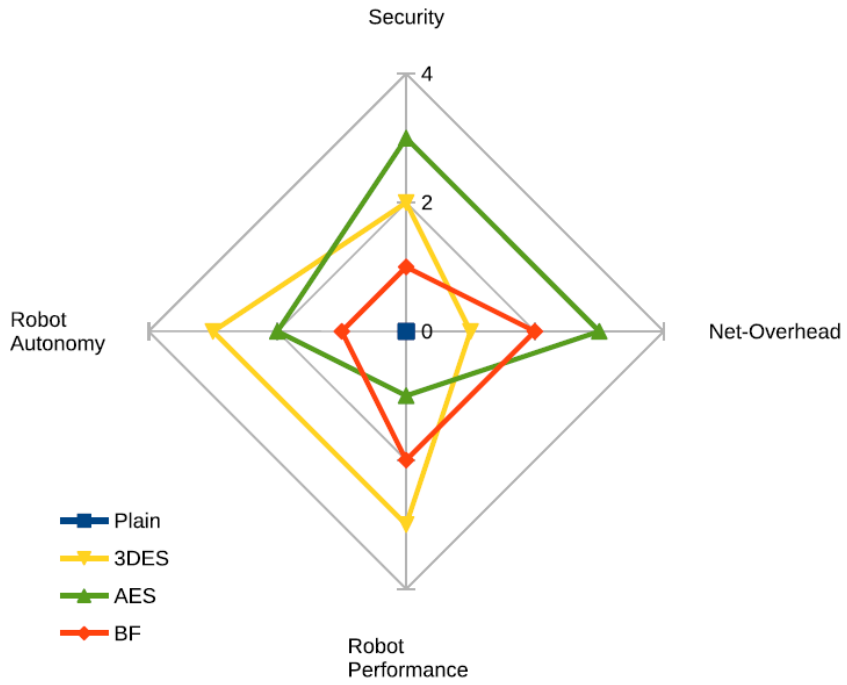

Figure 8: Cybersecurity Characterization Model for Robots

Integration of Quantum Resistant Algorithms into Secure ROS

In the continuation of this section, we delve into the integration of Quantum Resistant Algorithms into Secure ROS (B). The separation between application-level authorization and network-level authentication and encryption allows for the modification of network-level security mechanisms in Secure-ROS without altering core ROS packages [25-26].

To enhance the authentication aspect, RSA signatures in Secure-ROS are replaced with Bimodal Lattice Signature Scheme (BLISS) certificates, a modern cryptosystem designed in 2013 to resist quantum-computing attacks. BLISS operates similarly to RSA but uses lattice-based schemes for key pair creation. The implementation involves creating a self-signed Certificate Authority (CA) on the ROS ground station, generating BLISS keys with strongSwan's PKI tool, and distributing CA certificates across the network.

With quantum-resistant authentication in place, the focus shifts to securing the symmetric encryption method. Fortunately, AES is quantum secure when paired with a sufficiently large key

size (AES-256 for medium-term and AES-512 for longer term) and is compatible with strongSwan. Additionally, strongSwan supports NTRU for key exchange, a lattice-based post-quantum encryption algorithm expected to be quantum-resistant.

Security Enhancements Over Secure ROS and IPSec

Moving on to Security enhancements over Secure ROS and IPSec (C), after establishing an IPSec tunnel, Secure ROS functions seamlessly in the standard workflow. The IPSec configuration files control connections, specifying parameters such as mode of operation, authorization, encryption, and key exchange. The configuration uses a "trap all" method, securing all traffic through an IPSec tunnel, a limitation justified in the context of the robotic network's closed nature. BLISS signatures, NTRU-192 for key exchange, and AES-256 for data encryption contribute to the overall security configuration [27-28].

Demonstration Details

Moving to Demonstration details (D), a Gazebo simulation environment with a simulated mobile robot is used to showcase the security infrastructure's application to command and control of mobile agents. The ground station, mobile agent, monitoring agent, and an attacker are simulated, with security mechanisms verified at both application and network layers. Secure ROS authorization rules restrict commands, enhancing security by preventing unauthorized commands even from trusted machines.

Results and Comparison

Results and Comparison (E) provide a performance evaluation of the integrated Secure ROS and strongSwan against default IPSec in Secure ROS and a system with no security. The comparison includes BLISS signatures and NTRU key exchange, contrasting results with RSA and IKEv2 used in standard IPSec. The analysis, conducted on virtual machines, emphasizes the advantages of post-quantum schemes in terms of message frequency and connection setup time, showcasing their significant performance improvement over standard IPSec (Figure 9).

Msg Size (bytes)	Target Frequency (hz)	Actual Frequency (hz)		
		No Encryption	AES-256, SHA-512	3DES, SHA-256
706				
	5	5.000	5	4.999
	50	49.995	49.952	49.965
	500	499.806	499.101	499.589
1306				
	5	5.000	4.999	5
	50	49.994	50.001	49.992
	500	491.811	491.469	490.043
6106				
	5	4.999	5.001	5
	50	50.038	50.059	50.046
	500	160.421	141.854	129.919
12176				
	5	5.002	5.004	5.003
	50	49.993	49.909	48.891
	500	81.771	72.844	67.558
60502				
	5	5.012	5.046	5.014
	50	17.429	15.668	13.998
	500	17.185	15.634	13.643

Figure 9: Comparative Analysis of Security Schemes in ROS Communication

Secure LoRa Communication

The prototype of the control device was developed using the TTGO T-Beam LoRa ESP32 development board, known for its versatility in prototyping various LoRa-based implementations. This development board integrates an ESP32 micro-controller, a LoRa transceiver SX127x, an OLED 128 × 64 display, and a LiPo/Li-Ion battery on a compact PCB board. The base station utilized one TTGO ESP32 module, while another was mounted on the robot.

For a detailed analysis, communication between the base station and a single robot (Pioneer-P3Dx) was considered, demonstrating the effectiveness of the cryptographic protocol developed. General parameters configured for LoRa devices include spreading factor (SF), coding rate (CR), and bandwidth (BW).

Two LoRa modules, serving the base station and the robot, were assigned a frequency of 915MHz with a bandwidth of 125 KHz and a spreading factor of 10. The cryptographic protocol at the base station operates in two modes: transmitter mode (Mode-1 - BTx) and receiver mode (Mode-2 - BRx).

Operations at Secured LoRa Control Device during Mode-1 (BTx)

In Mode-1 (BTx), the LoRa control device at the base station transmits control commands to the robot. The process involves encrypting the location information (LI) using AES-128 and then applying HMAC SHA-256 to the resulting ciphertext [29]. The encrypted data, HMAC result, and a dynamically assigned device ID (DID) are concatenated to form the "Tx-Packet," representing the LoRa packet sent from the base station to the robot.

Securing Data Communicated through LoRa Device Mounted on Robot

In Mode-1 (RRx), the LoRa module on the robot acts as a receiver. The received LoRa packet, "Rx-Packet," is processed by extracting the device ID (DID), ciphertext, and HMAC result. The device ID is used as the robot ID (RID), and the ciphertext is decrypted using the AES key. The decrypted location information (LI) undergoes HMAC verification, ensuring the authenticity of the received data.

Operations at Secured LoRa Control Device during Mode-2 (BRx)

In Mode-2 (BRx), the base station operates as a receiver, receiving location information from the robot. The process involves decrypting the received ciphertext using AES-128 and verifying HMAC SHA-256. If the HMACs match, the authenticity of the data is confirmed (Figure 10).

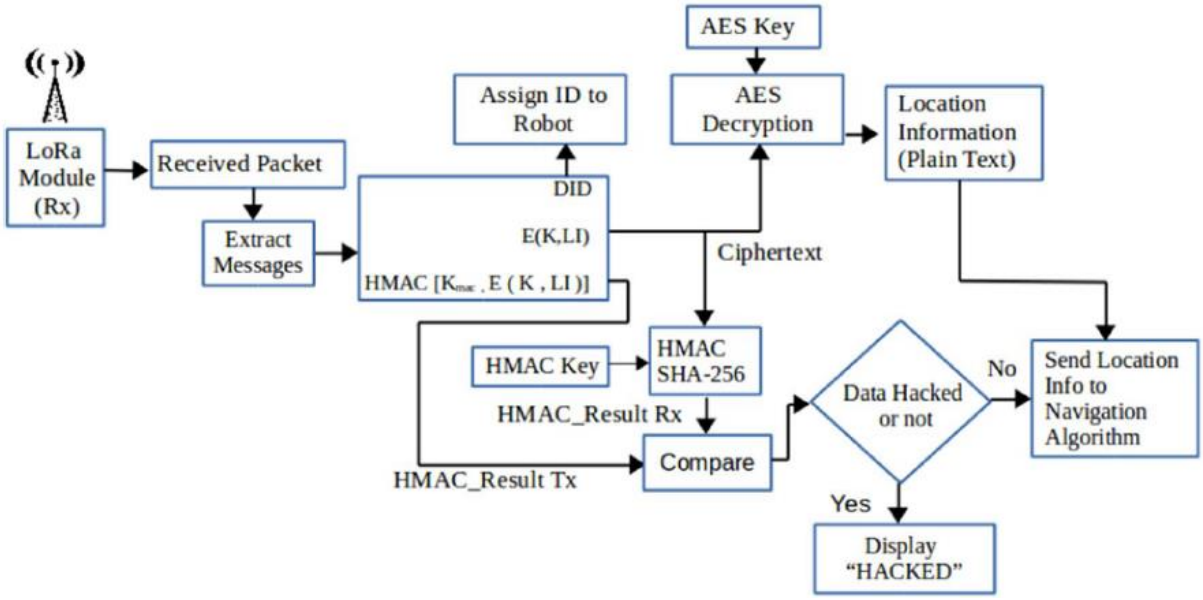

Figure 10: Secure LoRa Communication: Encrypted Traffic vs. Plain Text Transmission

This cryptographic protocol ensures secure communication between the base station and the robot, preventing unauthorized access and ensuring data integrity.

In summary, our results and discussions shed light on the intricate interdependencies between encryption choices, robotic platforms, and operational scenarios. As we navigate through the empirical findings, we unravel key insights crucial for shaping secure and efficient robotic communication frameworks.

Conclusion

In conclusion, this study has delved into crucial aspects of integrating quantum-resistant algorithms into the secure ROS (Robot Operating System) environment, employing the strongSwan IPSec VPN solution. The developed protocol ensures secure data transmission between the base station and mobile robots, with an additional focus on leveraging LoRa technology for enhanced communication.

Quantum-Resistant Authentication and Encryption

The primary research focus centered on enhancing authentication and encryption within the ROS environment. The replacement of standard RSA signatures with quantum-resistant BLISS certificates, facilitated by a self-signed Certificate Authority (CA) on the base station, establishes a higher level of authentication resistant to quantum computing attacks.

The application of AES and NTRU algorithms within the strongSwan IPSec VPN ensures cryptographic resilience at the network level. Experimental results underscore the effectiveness of quantum-resistant authentication and key exchange schemes compared to traditional methods, highlighting their potential application in future networked systems.

Security Measures in Action

The demonstration of the developed infrastructure in the Gazebo environment with a simulated mobile robot provides tangible evidence that the enhanced security measures implemented at the application and network levels effectively prevent unauthorized commands, even when an attacker gains access to a trusted host.

Performance Analysis

The performance analysis, comparing Secure ROS and strongSwan integration using quantum-resistant schemes, reveals a substantial improvement in connection setup time compared to traditional IPSec. This improvement is a testament to the efficiency and viability of quantum-resistant methods in real-world robotic applications.

Practical Implications

In summary, this study not only emphasizes the critical importance of enhancing cryptographic security in robotic systems but also provides a practical demonstration of the effectiveness of quantum-resistant methods in the field of robotics and unmanned systems. The integration of cutting-edge technologies, such as quantum-resistant algorithms and secure communication protocols, contributes to the ongoing evolution of secure and resilient robotic networks. As we progress into an era of increased reliance on autonomous systems, the insights gained from this study pave the way for the development of more secure and future-ready robotic platforms.

5. Acknowledgements

This research is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Project No. AP19677508).

6. References

[1] Manuel, M. P., & Daimi, K. (2021). Implementing cryptography in LoRa based communication devices for unmanned ground vehicle applications. SN Applied Sciences, 3(4). https://doi.org/10.1007/s42452-021-04377-y.

[2] Varma, R., Melville, C., Pinello, C., & Sahai, T. (2021, September). Post Quantum Secure Command and Control of Mobile Agents Inserting Quantum-Resistant Encryption Schemes in the Secure Robot Operating System. International Journal of Semantic Computing, 15(03), 359–379. https://doi.org/10.1142/s1793351x21400092.

[3] Rodríguez-Lera, F. J., Matellán-Olivera, V., Balsa-Comerón, J., Guerrero-Higueras, N. M., & Fernández-Llamas, C. (2018, March 2). Message Encryption in Robot Operating System: Collateral Effects of Hardening Mobile Robots. Frontiers in ICT, 5. https://doi.org/10.3389/fict.2018.00002.
[4] Yuan, J., Zhang, J., Ding, S., & Dong, X. (2017, September). Cooperative localization for disconnected sensor networks and a mobile robot in friendly environments. Information Fusion, 37, 22–36. https://doi.org/10.1016/j.inffus.2017.01.001.
[5] Roy, R., Tu, Y. P., Sheu, L. J., Chieng, W. H., Tang, L. C., & Ismail, H. (2023, March 30). Path Planning and Motion Control of Indoor Mobile Robot under Exploration-Based SLAM (e-SLAM). Sensors, 23(7), 3606. https://doi.org/10.3390/s23073606.
[6] Lin, J., & Cen, L. (2020, February 27). Design and Experiment of Remote Communication System Base on GPS/GPRS Technology. Global Journal of Science Frontier Research, 23–29. https://doi.org/10.34257/gjsfrivol20is1pg23.
[7] Honarbakhsh, S., Latif, L. B. A., Manaf, A. B. A., & Emami, B. (2014). Enhancing Security for Mobile Ad hoc Networks by Using Identity Based Cryptography. International Journal of Computer and Communication Engineering, 3(1), 41–45. https://doi.org/10.7763/ijcce.2014.v3.289.
[8] Bakyt, M., Moldamurat, Kh., Satybaldina, D.Zh., Yurkov, N.K. (2022). Modeling Information Security Threats for the Terrestrial Segment of Space Communications, CEUR Workshop ProceedingsVolume 33822022 7th International Conference on Digital Technologies in Education, Science and Industry, DTESI 2022, Almaty 20 October 2022 through 21 October 2022, Code 188290.
[9] Brimzhanova, S., Atanov, S., Moldamurat, K., Brimzhanova, K., Seitmetova, A., An intelligent testing system development based on the shingle algorithm for assessing humanities students' academic achievements, Education and Information Technologies, 2022, 27(8), pp. 10785–10807.
[10] Kyzyrkanov, A.E., Atanov, S.K., Aljawarneh, S.A.R. (2021). Formation control and coordination of swarm robotic systems, Conference Paper, ACM International Conference Proceeding Series, 2021, 3492704.
[11] Seitbattalov, Z.Y., Atanov, S.K., Moldabayeva, Z.S., (2021). An Intelligent Decision Support System for Aircraft Landing Based on the Runway Surface, Conference Paper, SIST 2021 - 2021 IEEE International Conference on Smart Information Systems and Technologies, 2021, 9466000.
[12] Adilzhan, K.K., Sabyrzhan, A.K., Timur, T.Z. (2021). The Usage of Extended Kalman Filter to Increase Navigation Accuracy of Mobile Units in Closed Spaces, Conference Paper, SIST 2021 - 2021 IEEE International Conference on Smart Information Systems and Technologies, 2021, 9465903.
[13] Jonay Suárez-Armas, Cándido Caballero-Gil, Rivero-García, A. and Pino Caballero-Gil (2018). Authentication and Encryption for a Robotic Ad Hoc Network Using Identity-Based Cryptography. arXiv (Cornell University). doi:https://doi.org/10.1109/innovate-data.2018.00018.
[14] Kemal Lutvica, Velagic, J., Kadic, N., Nedim Osmic, Gregor Dzampo and Muminovic, H. (2014). Remote path planning and motion control of mobile robot within indoor maze environment. doi:https://doi.org/10.1109/isic.2014.6967625.
[15] Sriram Chellappan, Paruchuri, V., McDonald, D.P. and Arjan Durresi (2008). Localizing sensor networks in un-friendly environments. CiteSeer X (The Pennsylvania State University). doi:https://doi.org/10.1109/milcom.2008.4753635.
[16] Hariyadi, M. A., & Fadila, J. N. (2022, November 16). Evaluation of Unmanned Aerial Vehicle (UAV) Control Range System using Lora-Based Communication System using Path Loss. Fountain of Informatics Journal, 7(2), 57–63. https://doi.org/10.21111/fij.v7i2.7571.
[17] Ma, Z., Cai, L., & Yang, M. (2022). Automatic control method of driving direction of unmanned ground vehicle based on association rules. International Journal of Vehicle Information and Communication Systems, 7(4), 350. https://doi.org/10.1504/ijvics.2022.10054141.

[18] FIRING OF UNMANNED GROUND VEHICLE USING ARDUINO. (2018, January 17). International Journal of Recent Trends in Engineering and Research, 4(1), 66–71. https://doi.org/10.23883/ijrter.2018.4011.bmel0.
[19] Zhang, J., Yue, X., Zhang, H., & Xiao, T. (2022, April 1). Optimal Unmanned Ground Vehicle—Unmanned Aerial Vehicle Formation-Maintenance Control for Air-Ground Cooperation. Applied Sciences, 12(7), 3598. https://doi.org/10.3390/app12073598.
[20] CAO, L., ZHANG, A., & GUO, F. J. (2011, June 21). Analysis system of unmanned aerial vehicle survivability based on MapX. Journal of Computer Applications, 31(5), 1443–1446. https://doi.org/10.3724/sp.j.1087.2011.01443.
[21] Duangsuwan, S., & Promwong, S. (2023, April 27). Performance Analysis of Unmanned Aerial Vehicle Assisted Wireless IoT Sensors Based on Air-to-Ground Communication Model for Smart Farming. Sensors and Materials, 35(4), 1463. https://doi.org/10.18494/sam4174
[22] Zhu, H., Liu, C., Li, M., Shang, B., & Liu, M. (2021, October). Passive detection of unmanned aerial vehicle in space-air-ground integrated networks. Physical Communication, 48, 101439. https://doi.org/10.1016/j.phycom.2021.101439.
[23] Liang, X., Chen, G., Zhao, S., & Xiu, Y. (2020, January 7). Moving target tracking method for unmanned aerial vehicle/unmanned ground vehicle heterogeneous system based on AprilTags. Measurement and Control, 53(3–4), 427–440. https://doi.org/10.1177/0020294019889074.
[24] Wu, G., Gao, X., & Wan, K. (2020, April 19). Mobility Control of Unmanned Aerial Vehicle as Communication Relay to Optimize Ground-to-Air Uplinks. Sensors, 20(8), 2332. https://doi.org/10.3390/s20082332.
[25] Rivera, Z. B., De Simone, M. C., & Guida, D. (2019, June 14). Unmanned Ground Vehicle Modelling in Gazebo/ROS-Based Environments. Machines, 7(2), 42. https://doi.org/10.3390/machines7020042.
[26] Cheng, C., Li, X., Xie, L., & Li, L. (2023, September 29). A Unmanned Aerial Vehicle (UAV)/Unmanned Ground Vehicle (UGV) Dynamic Autonomous Docking Scheme in GPS-Denied Environments. Drones, 7(10), 613.
[27] Liu, J., Anavatti, S., Garratt, M., & Abbass, H. A. (2022, June). Modified continuous Ant Colony Optimisation for multiple Unmanned Ground Vehicle path planning. Expert Systems With Applications, 196, 116605. https://doi.org/10.1016/j.eswa.2022.116605.
[28] Jiang-Yi Qin, J. Y. Q., Jiang-Yi Qin, K. W., Kai Wang, X. B. L., Xian-Bin Li, Y. J., & Yong Jiang, Y. Z. (2021, October). A Dynamic and Reconfigurable Satellite-to-ground Communication System Research Based on LoRa Technology. 電腦學刊, 32(5), 161–170. https://doi.org/10.53106/199115992021103205013.
[29] Jin, X., Li, Z., & Atzberger, C. (2020, March 13). Editorial for the Special Issue “Estimation of Crop Phenotyping Traits using Unmanned Ground Vehicle and Unmanned Aerial Vehicle Imagery.” Remote Sensing, 12(6), 940. https://doi.org/10.3390/rs12060940.