Security and integrity in 8-bit processing architectures in IoT/LPWAN networks

F. Ramírez-López[1,a], G. A. Yáñez-Casas[1,b], C. A. López-Balcázar[2,c], J. J. Hernández-Gómez[3,d], A. Gutiérrez-Aguilar[1,], A. Ruán-Aldana[1,f]
[1] Instituto Politécnico Nacional, Unidad Profesional Interdisciplinaria de Ingeniería y Tecnologías Avanzadas. Ciudad de México, 07340, México
[2] Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica Zacatenco, Sección de Estudios de Posgrado e Investigación. Ciudad de México, 07320, México.
[3] Instituto Politécnico Nacional, Centro de Desarrollo Aeroespacial. Ciudad de México, 06010, México.
Autor de Correspondencia: jjhernandezgo@ipn.mx
URL ORCID: [a][0000−0003−4832−1471] , [b][0000−0003−0167−6750], [c][0009−0001−7002−3342] , [d][0000-0002-5012-6619] , [e][0009-0008-3039-8511] , [f][0009-0005-9863-7177]

***Resumen*— El crecimiento de los sistemas de comunicación inalámbrica ha aumentado significativamente, impulsado por la creciente demanda de servicios digitales en la sociedad moderna. Las redes inalámbricas se han convertido en los sistemas más utilizados, atendiendo a una base de usuarios en rápida expansión. Dentro de este panorama, las redes inalámbricas han evolucionado y diversificado, como lo demuestran las soluciones de IoT (Internet de las Cosas) basadas en tecnologías LPWAN (Low Power Wide Area Network). Estas redes son económicas, adaptables y relativamente simples de desarrollar, lo que las hace adecuadas para una amplia gama de aplicaciones. Sin embargo, a pesar de sus ventajas y beneficios potenciales, aún existen desafíos en su diseño e implementación. Un área clave que requiere atención es el desarrollo de una estructura de encapsulación de datos adaptada a las necesidades del sistema y de la aplicación, garantizando una transmisión de datos segura, completa y eficiente, respetando siempre las limitaciones del sistema de comunicación. Este artículo presenta una estructura de protocolo de trama de datos diseñada para un sistema de monitoreo LPWAN/IoT, utilizando componentes COTS (Commercial Off-The-Shelf) para adquirir variables ambientales.**

***Palabras Clave* — Dataframe, data security, data integrity, 8-bit microcontroller, climate change, datalink communications protocol, LPWAN (Low Power Wide Area Network), sensing.**

Abstract- The growth of wireless communication systems has surged significantly, driven by the increasing demand for digital services in modern society. Wireless networks have become the most widely used systems, catering to a rapidly expanding user base. Within this landscape, wireless networks have evolved and diversified, as evidenced by IoT (Internet of Things) solutions built on LPWAN (Low Power Wide Area Network) technologies. These networks are cost-effective, adaptable, and relatively simple to develop, making them suitable for a broad range of applications. However, despite their advantages and potential benefits, challenges remain in their design and implementation. A key area requiring attention is the development of a data encapsulation structure tailored to the system's and application's needs, ensuring secure, complete, and efficient data transmission while adhering to the limitations of the communication system. This paper introduces a data framing protocol structure designed for an LPWAN/IoT monitoring system, utilizing COTS (Commercial Off-The-Shelf) components to acquire environmental variables.

INTRODUCCIÓN

The Internet of Things (IoT) has become a cornerstone in the development of modern society, enabling innovative applications across various domains [1]. A significant factor in its success is the integration with Low Power Wide Area Networks (LPWAN), which extend the reach of IoT systems and facilitate real-time data transmission [2, 3]. This integration has exponentially increased the potential applications of IoT, particularly in remote and non-urban environments where traditional wireless communication systems, such as 2G-5G or Wi-Fi, are unavailable. One of the most promising applications of LPWAN-based IoT is the monitoring of environmental variables to assess and mitigate the impacts of climate change on regional and global scales [4, 5].

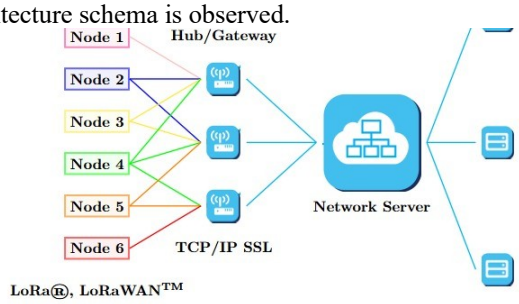
However, despite the advantages of LPWAN technologies, challenges remain in their implementation, especially when using low-power, resource-constrained devices. Current LPWAN protocols, such as LoRa/LoRaWAN, NBIoT, and Sigfox, often feature multi-layer structures that are incompatible with small-scale processing architectures, such as 8-bit microcontrollers [6]. These devices, while energy-efficient and cost-effective, struggle with the computational burden imposed by lengthy protocols, limiting their effectiveness in IoT applications [7, 8].

To address this gap, this research focuses on developing a lightweight, one-layer communication protocol tailored for IoT/LPWAN systems using 8-bit processing units. Building on the work of [7], which demonstrated the feasibility of ultra-low-power sensing nodes, this study proposes a data framing structure that is adaptable to variable data lengths and scalable to multiple sensors. Additionally, the protocol incorporates security and integrity fields optimized for small-scale architectures, ensuring efficient memory usage and processing times. The primary objective of this work is to provide a balanced solution that minimizes computational overhead while maintaining robust data transmission, enabling the deployment of IoT devices in remote and resource-constrained environments.

METHODOLOGY & DEVELOPMENT

A. Low Power Wide Area Networks and Internet of Things Applications

Wireless networks are critical to modern communication systems, but infrastructure saturation has driven the adoption of Low Power Wide Area Networks (LPWAN) [9]. LPWANs operate in two phases: ***Private Network***: Data acquisition devices and radio gateways and ***Public Network***: IP-based cloud servers for data storage. In Figure 1 the LPWAN architecture schema is observed.



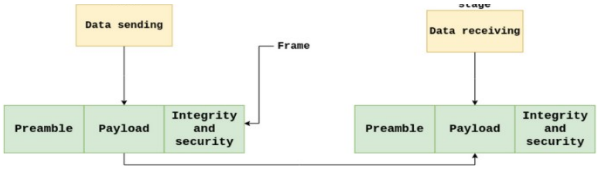
1. LPWAN Architecture [9]

IoT applications leverage LPWAN for remote data transmission, emphasizing interoperability and Edge Computing. Commonly LPWAN/IoT technologies share features like low power consumption, UDP-based protocols, and star topologies [9, 10].

B. Low Power Communication Protocols

Communication systems consist of transmission, medium, and reception stages, each with physical and logical components [10, 11]. Protocols are organized in layered stacks, with the link layer responsible for framing, error handling, and encryption.

LPWAN protocols are designed for low power and scalability, supporting short, unidirectional messages and simple security measures [12]. The layered design acknowledges the necessity of a physical layer, making subsequent layers logical, even if they rely on infrastructure. Figure 2 shows the general structure of an LPWAN protocol packet. All transmission protocols have the same structure, however in the context of LPWAN such structure has a vital importance.



2.Generic data link layer [10]

C. Eight-Bit Architectures and Serial Communication

Eight-bit architectures, like microcontrollers, have limited memory and processing power, making them ideal for low-power IoT applications [11]. Serial communication protocols are commonly used but face challenges in frame size, baud rate, and computational capacity [13]. Important technical features and common range value of a processing unit are ***Program Memory:*** *1 KB – 2 MB,* ***#Cores:*** *1 – 2,* ***Operation Frecuency:*** *4 – 64 MHz,* ***Registers length:*** *8 – 32 bits,* ***# UART Interfaces:*** *1 – 2,* ***# SPI Interfaces:*** *1 – 2 and #* I^2C ***Interface***: *1 – 2 [14].*

Serial communication is limited by the characteristics of the specific CPU. A message must be distributed in memory and must be framing before sent. Small scale architectures use a higher number of duty cycles, and since they are sent at a small frequency, they require more time to send the message *[14, 15]*.

D. Data Security and Integrity

Cyclic Redundancy Check (CRC) ensures data integrity through polynomial division, using three key variables: the dividend (data frame of size W), the divisor (polynomial G of width W), and the remainder (checksum). CRC is efficient and low-cost, making it ideal for microcontrollers and IoT devices. So, the coding process involves three stages: First chose W and polynomial G, second appending W zeros to the message M creating M', and finally divide M' by G using CRC arithmetic, with the reminder checksum.

At the receiver, the same G and W are used to verify integrity. The receiver can separate the data and checksum, recompute the checksum, and compare or compute the checksum for the entire frame, expecting a zero result for error-free data [13].

On the other hand, security is achieved using lightweight encryption techniques like Shift Cipher and Permutation Cipher, tailored for 8-bit architectures [16]. In cryptosystems, the mathematical components include plaintext (P), ciphertext (C), and keys (K), with encryption and decryption rules $\varepsilon P_i(k)$ and $\delta P_j(k)$, respectively. An ideal system has large K and C to resist brute force attacks. For 8-bit architectures, balancing security and efficiency is critical.

The Shift Cipher shifts alphabet characters by k positions. For an n-sized alphabet, $P=C=K=Z$, with $n-1$ possible shifts. For encryption: $\gamma Pi(k)=(Pi+k)\,mod n$ and decryption: $\delta Pj(k)=(Pj-k)\,mod n$ [16].

The Permutation Cipher rearranges plaintext using a permutation π. For n-sized alphabets, $P=C=Z_n$, and $K=n!$. For Encryption: $\gamma Pi(k)=\pi(x)$ and decryption: $\delta Pj(k)=\pi-1(x)$ [16].

A challenge is the lack of dynamic permutation generation, requiring pre-selected permutations and consistent keys. To optimize 8-bit systems, a hybrid of Shift and Permutation Ciphers is proposed, combining simplicity and security for resource-constrained environments like LPWAN/IoT.

1. *Base Communication System*

The proposed system is an LPWAN/IoT-based environmental monitoring system, designed for low power consumption and scalability [33]. The system consists of two main stages: the **transmission stage** and the **reception stage**. In the transmission stage, two acquisition nodes equipped with COTS sensors for meteorological variables are connected to an AVR ATMEGA328P microcontroller and a CC1101 RF transceiver. In the reception stage, a mirror circuit processes the received data and distributes it via IP networks for cloud storage and visualization.

Components: The system uses low-cost, low-power sensors and a microcontroller ATMEGA328P with 32 KB flash memory, compatible with I2C and UART protocols [66, 84, 85] (see Table 1 for more information).

Table 1.- Characteristics of the electronics components considered for the hardware of this system [17, 18, 19, 20, 21, 22, 23, 24, 25, 26] [27, 28, 29, 30, 31, 32, 33, 34, 35].

Function	Model
Processing unit component	ATMEGA328P (*microcontroller*)
Conditioning and measure components	CD4051 (*mux*), ACS712 (*analogical sensor*), LCD 1602A (*screen*).
Communication components	CC1101 (*Radio transceiver*)
Sensors node 1	BMP180 (*digital sensor*), DHT11 (*digital sensor*), Yl-83 (*analogical sensor*), ML8511 (*analogical sensor*), PH0245S (*analogical sensor*).
Sensors node 2	MQ-2, MQ-3, MQ-4, MQ-5, MQ-6, MQ-7, MQ-8, MQ-9 (*analogical sensors*)

2. Data Frame Structure and Data Convention

The proposed protocol frames data for secure and efficient transmission over wireless channels. Key considerations include: The ***Frame Fields:*** consist of several key components: the ***Preamble,*** which includes identifiers for the destination, source, sensor, and variable; the ***Data Payload***, which contains sensor readings converted from floating-point to ASCII format to reduce alphabet size; the ***Security*** field, which holds encryption keys for data protection; the ***Integrity*** field, which implements CRC-based error detection to ensure data accuracy; and the ***End Frame,*** an identifier that marks the conclusion of the frame. Together, these fields structure the frame for efficient and secure data transmission (see Table 2).

Table 2.- Protocol frame structure.

Field name	*Preamble*	*Data payload*	*Security*	*Integrity*	*End Frame*
Length (Bytes)	2	Variable	13	1	1

So, for this work the technical features considered for processing are: **Processing unit** (ATMEGA328P), ***Serial communication protocol*** (UART), ***Baud rate*** (9600 symbol per second), ***Duty cycles*** (8) and ***Operation frequency*** (433 MHZ) [18].

3. Design of CRC for the Proposed Protocol

The **Cyclic Redundancy Check (CRC)** algorithm is implemented to ensure data integrity, with specific considerations for 8-bit architectures [16]. The **Data Payload** field is the primary focus for CRC calculation, as applying the algorithm before encryption minimizes processing requirements [36]. A 4-degree polynomial of the form ($x^4+x^3+x^2+x+1$), represented as $b'11111$, is used as the **Polynomial Divisor**. This choice reduces the number of sequential divisions, with the CRC field utilizing 4 useful bits. The algorithm begins by determining the number of shifts (m_i) required for the divisor polynomial, calculated as ($m_i=n_i-5$), where (n_i) is the size of the message in bits. During the division process, the divisor is shifted left to match the length of the previous division's remainder, and any overflow bits are stored in the **Overflow Register** C. The algorithm concludes when the dividend is reduced to 1, at which point the content of the overflow register represents the CRC. If the **Data Payload** content is 0, the default CRC value is also 0 [16]. This process ensures efficient error detection while maintaining low computational overhead, making it suitable for 8-bit systems [36] .

4. Design of Cypher Technique for the Proposed Protocol

The lightweight encryption algorithm proposed for 8-bit systems combines the **Shift Cipher** and **Permutation Cipher** to achieve a balance between security and processing efficiency [16]. The **Shift Cipher** operates by shifting characters within the alphabet, while the **Permutation Cipher** rearranges characters based on predefined rules. This hybrid approach ensures a robust keyspace with minimal computational burden, which is critical for 8-bit architectures where processing resources are limited [16]. The algorithm's design leverages the strengths of both techniques: the **Shift Cipher** provides simplicity and low overhead, while the **Permutation Cipher** enhances security by introducing complexity through character rearrangements. The resulting keyspace is defined by $(\left(n_k\right)\left(k\right))$ substitutions, where (n_k) represents the number of permutations and (k) denotes the possible shifts within each permutation [16]. This combination ensures a valid and efficient keyspace, as it accounts for both the permutations and the shifts applied to a predefined ordering. By using a substitution process as the final step, the algorithm allows the same elements to be used for both encryption and decryption, further reducing processing demands [16]. This approach is particularly suited for 8-bit systems, where maintaining a low

computational workload is essential while still ensuring data security.

Results and Discussion

A. Acquisition Nodes

The transmission stage begins with two acquisition nodes, each equipped with sensors to measure environmental variables. The block diagrams for Node 1 and Node 2, shown in Figure 3, illustrate the key components of the system, including the sensors. The ATMEGA328P microcontroller plays a crucial role in ensuring low-power operation while efficiently processing sensor data. The variables measured by each sensor, along with their types and lengths, are essential for constructing the data framing protocol.

To evaluate the performance of the proposed protocol, two simulation scenarios were conducted:

Minimal Frame Transmission configuration: The smallest frame (1 byte payload) was transmitted to minimize processing burden. Processing time: 23 ms and CRC default: 0x00 (for payload = 0x00).

Full System Frame Forwarding configuration: All 35 variables from 15 sensors were transmitted in 26 frames per cycle, memory usage: 397 bytes for storage, 2985 bytes for processing, processing time: 675 ms and program memory usage: 9.16% (90.84% available for other tasks).

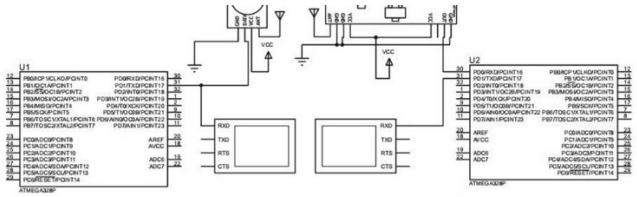
The results of these simulations are summarized in Table 3, which highlights the protocol's processing efficiency and resource utilization. Despite the limited memory and processing power of the 8-bit microcontroller, the protocol demonstrated robust performance without saturating the system's resources.

Table 3 shows data processing compilation a simulation results between small, medium and high processing unit.

Table 3.- Protocol's processing results.

Parameter	Simulation 1	Simulation 2
ATMEGA328P		
Memory [bytes]	1,427	2,985
Processing Time [ms]	23	675
AT TINy 85		
Memory [bytes]	1572	Not Available
Processing Time [ms]	43	Not available
PIC18F14Q41		
Memory [bytes]	1472	3092
Processing Time [ms]	8	14

The results demonstrate that the protocol is well-suited for the 8-bit architecture, with no saturation of microcontroller resources.



3. Circuit simulation diagram.

The protocol incorporates encryption (Shift Cipher and Permutation Cipher) and CRC-based integrity checks, tailored for low-power systems. These techniques were optimized to avoid processing overload, ensuring secure and reliable data transmission.

The proposed protocol addresses the limitations of small-scale architectures, providing a custom data framing structure for LPWAN/IoT systems. Unlike generic LPWAN protocols, this solution ensures precise and secure data handling, tailored to the specific mission and characteristics of the system.

Conclusions

This work presents a data framing structure for an LPWAN-based environmental monitoring system, optimized for low-cost **COTS components** and the **ATMEGA328P** microcontroller. The protocol ensures **efficient data handling with low power consumption**, crucial for constrained devices. It supports various sensors via **serial communication**, offering flexibility and adaptability without dependency on specific hardware. Despite its simplicity, the protocol maintains **data security and integrity**, even in low-power networks. A key advantage is **memory efficiency**—when transmitting multiple data types, memory usage remains minimal while processing time scales with variable size. However, small-scale implementations should prioritize security-critical communications, as additional datalink protocols increase memory consumption. A simulation with **eight sensing nodes** confirmed the protocol's efficiency, using only **2.985 KB of 32 KB** available in the ATMEGA328P, demonstrating its scalability for large-scale IoT/LPWAN networks.

Acknowledgements

The authors gratefully acknowledge the partial support of Secretaría de Investigación y Posgrado of Instituto Politécnico Nacional, through projects 20242752, 20240894, 20241163, 20240811 and 20241077, as well as the EDI and PIFI programs.

Ethical Disclosure

It is declared that there is no conflict of interest in the publication of this article.

REFERENCES

[1] Y. Mahmood, N. Kama, A. Azmi y S. Ya'acob, «An IoT based home automation integrated approach: Impact on society in sustainable development perspective,» *International Journal of Advanced Computer Science and Applications,* vol. 11, pp. 240-250, 2020.

[2] R. Sarath Kumar, M. Gokul Prasanth, R. Bharath Kumar, J. Abhishek y D. Ajay, «LPWAN for IoT,» de *2022 International Conference on Advanced Computing Technologies and Applications, ICACTA 2022*, 2022.

[3] S. K. Pattnaik, S. R. Samal, S. Bandopadhaya, K. Swain, S. Choudhury, J. K. Das, A. Mihovska y V. Poulkov, «Future Wireless Communication Technology towards 6G IoT: An Application-Based Analysis of IoT in Real-Time Location Monitoring of Employees Inside Underground Mines by Using BLE,» *Sensors,* vol. 22, 2022.

[4] S. El Maachi, R. Saadane, M. Wahbi, A. Chehri y A. Badaoui, «Vision of IoT, 5G and 6G Data Processing: Applications in Climate Change Mitigation,» de *2022 International Symposium on Intelligent Signal Processing and Communication Systems, ISPACS 2022*, 2022.

[5] P. Singh, D. Sammanit, R. N. Shaw y A. Ghosh, «Comprehension of Climate Change with IoT-Enabled CNN,» *Lecture Notes in Electrical Engineering,* vol. 914, pp. 385-394, 2022.

[6] G. A. Yáñez-Casas, J. J. Hernández-Gómez, J. M. Arao-Quiroz, C. Luna-García, M. Gutiérrez-Montor, I. Medina, R. de-la-Rosa-Rábago y M. A. Enciso-Aguilar, «On the capacities and applications of IoT networks: LoRaWAN, LTEM, MQTT, NBIoT and Sigfox,» *Proceedings CNIES 2021,* vol. 048, pp. 345-349, November 2021.

[7] F. Ramírez-López, G. A. Yáñez-Casas, G. E. Casillas-Aviña, J. J. Hernández-Gómez, M. F. Mata-Rivera y S. Ramírez-Espinosa, «Simulation and Implementation of an Environmental Monitoring System Based on LPWAN/IoT,» de *Telematics and Computing: 11th International Congress, WITCOM 2022, Cancún, México, November 7–11, 2022, Proceedings*, 2022.

[8] K. Chaduvula, K. Kranthi kumar, B. R. Markapudi y C. Rathna Jyothi, «Design and Implementation of IoT based flood alert monitoring system using microcontroller 8051,» *Materials Today: Proceedings,* vol. 80, pp. 2840-2844, 2023.

[9] Internet Engineering Task Force (IETF), «Low-Power Wide Area Network (LPWAN) Overview,» Dublin, 2018.

[10] A. S. Tanenbaum, Computer Networks, Prentice Hall PTR, 2003.

[11] D. S. Dawoud y P. Dawoud, Serial Communication Protocols and Standards: RS232/485, UART/USART, SPI, USB, INSTEON, Wi-Fi and WiMAX, River Publishers, 2020.

[12] International Telecommunication Union, «Technical and operational aspects of Low Power Wide Area Networks for machine-type communication and the Internet of Things in frequency ranges harmonised for SRD operation,» Ginebra, 2018.

[13] T. Schmidt y M. T. Inc., *CRC Generating and Checking,* 2021.

[14] Phillips Semiconductors, «AN10216-01 I2C Bus,» Eindhoven, 2003.

[15] M. E. Yuksel y H. Fidan, «Energy-aware system design for batteryless LPWAN devices in IoT applications,» *Ad Hoc Networks,* vol. 122, p. 102625, 2021.

[16] D. R. Stinson, Cryptography: Theory and Practice, Third Edition, CRC Press, 2005.

[17] Microchip Technology Inc.®, *AVR MCUs®,* 2021.

[18] Atmel Corp., «ATmega328P 8-bit AVR Microcontroller with 32K Bytes In-System,» California, 2015.

[19] National Semiconductor , «CD4051BM/CD4051BC Single 8-Channel AnalogMultiplexer/Demultiplexer Module,» Santa Clara, United States, 2013.

[20] Allegro MicroSystems, «Fully integrated, hall effect-based linear current sensor,» New Hampshire, United States, 2003.

[21] Hitachi, «Dot Matrix Liquid Crystal Display Controller/Driver,» Tokyo, 1998.

[22] Chipcon Products., «Low-Cost Low-Power Sub-1GHz RF Transceiver,» Texas, 2015.

[23] Bosch, «BMP180 Digital Pressure Sensor,» Gerlingen, 2013.

[24] Mouser Electronics, «DHT11 Humidity and Temperature Sensor,» Mansfield, Texas, United States, 2019.

[25] VAISALA, «Yl-83 Rain Detector,» Eindhoven, 2015.

[26] Keyestudio , «GY-ML8511 Ultraviolet Sensor Module,» Ischia, 2013.

[27] Pololu, «MQ-2 Semiconductor Sensor for Combustible Gas,» Las Vegas, United States, 2013.

[28] Pololu, «MQ-3 Semiconductor Sensor for Alcohol,» Las Vegas, United States, 2013.

[29] Pololu, «MQ-4 Semiconductor Sensor for Combustible Gas,» Las Vegas, United States, 2013.

[30] Hanwei Electronics Co., LTD, «MQ-5 Gas sensor,» Beijing, 2015.
[31] Pololu, «MQ-6 Semiconductor Sensor for Combustible Gas,» Las Vegas, United States, 2013.
[32] Pololu, «MQ-7 Semiconductor Sensor for Combustible Gas,» Las Vegas, United States, 2013.
[33] Hanwei Electronics Co., LTD, «MQ-8 Gas sensor,» Beijing, 2015.
[34] Pololu, «MQ-9 Semiconductor Sensor for Combustible Gas,» Las Vegas, United States, 2013.
[35] DFRobot, *Wind speed sensor,* 2022.
[36] MathWorks América Latina, *Comprobar la redundancia cíclica,* 2019.