Autonomous Network Reconstruction Using LPWA for Disaster Prevention

Kou Nakakubo[1(✉)], Kazuaki Tanaka[1], and R. Krishnamoorthy[2]

[1] Kyushu Institute of Technology, Fukuoka, Japan
nakakubo.ko922@mail.kyutech.jp, kazuaki@ics.kyutech.ac.jp
[2] Chennai Institute of Technology, Chennai, India
krishnamoorthyr@citchennai.net

Abstract. In recent years, the use of IoT networks for environmental data collection by local governments has been increasing. However, these networks face a critical issue: when relay points are lost due to disasters, most communications are disrupted. In this study, we propose a system that utilizes Low Power Wide Area (LPWA) communication technology to autonomously reconstruct communication networks. The proposed system employs a tree-structured LPWA network that dynamically reconfigures itself in the event of a failure. Specifically, each node assesses the health of its upstream node based on relayed uplink packet information and dynamically selects an optimal alternative route. We evaluate the effectiveness of our method through field experiments, confirming that network prevention can be appropriately performed even in the presence of node failures.

Keywords: LPWA · Disaster Prevention · Autonomous Network Reconstruction

1 Introduction

1.1 Background

In recent years, local governments and public institutions have increasingly adopted IoT devices for environmental data collection [1]. In particular, Low Power Wide Area (LPWA) technology has played a crucial role in environmental monitoring and smart city projects due to its ability to cover wide areas while maintaining low power consumption. In practice, LPWA has been actively utilized in atmospheric and water quality monitoring by the Ministry of the Environment and in smart city initiatives promoted by the Ministry of Economy, Trade, and Industry. However, conventional LPWA networks face a significant challenge: if a relay node fails, the entire network communication is disrupted. This issue becomes particularly severe in disaster scenarios, where multiple nodes may fail simultaneously, making network prevention difficult.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2026
O. Gervasi et al. (Eds.): ICCSA 2025 Workshops, LNCS 15890, pp. 235–246, 2026.
https://doi.org/10.1007/978-3-031-97606-3_16

1.2 Existing Technologies and Challenges

In conventional LPWA networks, when a failure occurs, relay points must be manually reconfigured, which requires time and hinders immediate communication prevention [2]. Various solutions, such as mesh networks and communication reconstruction using drones, have been proposed. However, these solutions pose challenges in terms of cost and power consumption, making them difficult to implement in practical scenarios. Additionally, traditional LPWA networks risk losing data from leaf nodes when intermediate relay nodes fail, leading to disruptions in information transmission during disasters. Thus, there is a need for a communication method that enables autonomous network reconstruction while ensuring reliable data transmission from leaf nodes.

1.3 Objective of This Study

To address this issue, this study proposes an autonomous network reconfiguration method for communication continuity in the event of a failure [5]. In this method, nodes monitor uplink communication and assess the health status of their upstream nodes. If a failure is detected, nodes autonomously select the optimal relay node and retransmit the lost packets. By doing so, this method ensures that data from leaf nodes reaches the root node, thereby enhancing communication continuity in disaster scenarios. The effectiveness of this method is evaluated through real-world experiments.

2 LPWA Technology and Characteristics

2.1 Overview of LPWA Technology

Low Power Wide Area (LPWA) is a wireless communication technology designed for the Internet of Things (IoT) that enables long-range communication with low power consumption. Unlike conventional Wi-Fi or cellular networks (LTE, 5G), LPWA provides a balance between extended coverage and energy efficiency (Fig. 1).

However, LPWA has certain limitations, such as low data transmission speed and long communication intervals. Therefore, an appropriate routing control protocol is required depending on the use case. Table 1 compares the characteristics of LPWA (LoRa) with cellular communication (4G/5G).

Table 1. Limitations of LPWA

	LPWA (LoRa)	4G/5G (Cellular Network)
Data Rate	0.016 Mbps	290 Mbps
Communication Interval	≤4400 ms	≤1 ms

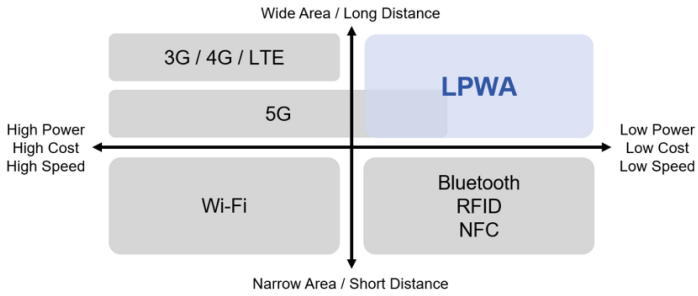

Fig. 1. Comparison of Communication Characteristics: Wi-Fi, LTE, and LPWA.

2.2 Major LPWA Standards Overview

LPWA includes multiple communication standards, and an appropriate standard must be selected depending on the application. Table 2 summarizes the characteristics of major LPWA standards.

Table 2. Major LPWA Standards and their Characteristics

LoRa	Promoted by the LoRa Alliance and freely available for private use. Only the modulation method is specified.
LoRaWAN	Communication network based on the LoRa system, which requires the use of LoRa Alliance-certified equipment.
NB-IoT	Using the mobile carrier band. Available only in the carrier's service area.
Sigfox	Ultra-narrowband network managed globally by UnaBiz. Available in multiple countries via international roaming.
LTE-M	LTE for machine-type communication. Same area as LTE service. Relatively high speed communication.

2.3 LPWA Module Used in This Study

This study adopts LoRa due to its license-free nature and low power consumption [4], making it suitable for remote sensing applications with energy constraints.

For implementation, we used the ES920LR3 module, which supports LoRa modulation and is optimized for ultra-low power operation. This module integrates a Cortex-M4 MCU and RF transceiver, enabling compact, power-efficient, and autonomous deployments in the field.

Although power consumption was not the primary focus of evaluation in this study, the adoption of this module ensures practical feasibility for long-term operation in remote or disaster-prone areas without the need for frequent maintenance [3] (Fig. 2).

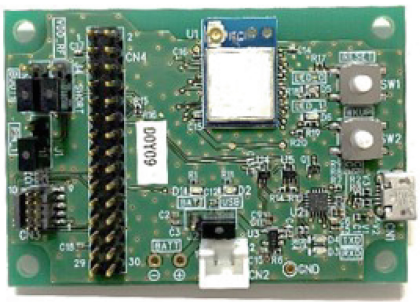

Fig. 2. ES920LR3 module and its development board.

3 System Design

3.1 Structure of the Tree-Based LPWA Network

The proposed communication network adopts a tree topology consisting of a root node (HQ; Head Quarter named in this study) and multiple relay nodes and leaf nodes. Each node selects a single optimal parent node based on RSSI (Received Signal Strength Indicator) and node depth information to construct the tree structure, ensuring that data flows along a unique path to the HQ. As shown in Fig. 3, the structure comprises HQ, relay nodes, and leaf nodes.

In this configuration, data originating from leaf nodes is sequentially forwarded through one or more relay nodes until it reaches the HQ node. Because each node communicates only with its selected parent, this hierarchical transmission model simplifies routing and eliminates redundant transmissions, making it highly suitable for power-constrained LPWA environments.

3.2 Dynamic Path Selection Method

Each node constantly monitors packets transmitted by upper-layer nodes (closer to the HQ) and extracts RSSI, depth, and node ID information. Using this information, the node determines the optimal communication path and maintains multiple alternative routes to enable rapid switching in case of a failure. By maintaining a table of multiple uplink routes, the system ensures rapid path switching when a failure occurs.

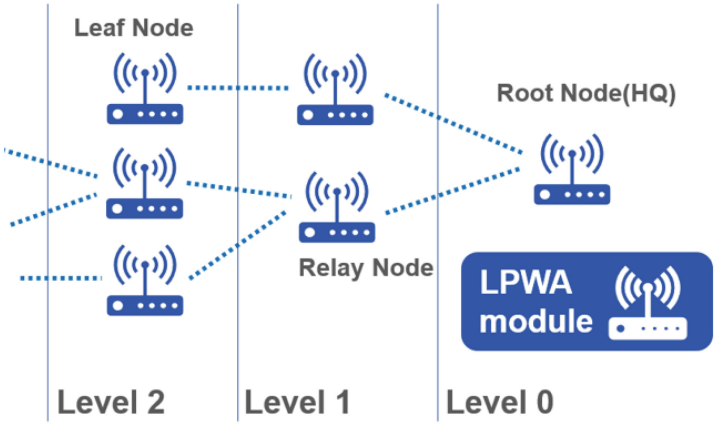

Fig. 3. Structure of the Tree-Based LPWA Network.

To enhance the responsiveness of the system to environmental changes such as signal obstruction or interference, the routing table is not based on historically maximum RSSI values but is instead dynamically updated with the latest observed RSSI readings for each uplink candidate. This design avoids overfitting to outdated or temporary signal conditions and ensures that the selected route reflects the most current network status.

Algorithm 1. Candidate Table Maintenance Algorithm

Input: Received packet from node i with RSSI $rssi_i$ and level $level_i$
Data: Candidate table $T = \{(ID_j, RSSI_j, Level_j)\}$
for all entry $(ID_j, RSSI_j, Level_j)$ in T **do**
    if $ID_j = i$ **then**
        $RSSI_j \leftarrow rssi_i$
        $Level_j \leftarrow level_i$
        return
    end if
end for
Insert new entry $(i, rssi_i, level_i)$ into T

To avoid unnecessary structural disruptions in the overall tree topology, each node prioritizes candidate uplink nodes from the layer directly above its own (i.e., level $n-1$). This hierarchical constraint minimizes the likelihood of triggering cascading reconfigurations across subordinate nodes, which would otherwise be required to update their own uplink paths in response to their parent node's level change.

Algorithm 2. Parent Node Selection Algorithm (Hierarchical Fallback)

Input: Candidate table $T = \{(ID_j, RSSI_j, Level_j)\}$, current node level L
Output: Selected parent node ID (or `null` if not found)
for $d = 1$ to $L - 1$ **do**
  $C \leftarrow \{(ID_j, RSSI_j) \in T \mid Level_j = L - d\}$
  if C is not empty **then**
    Sort C by descending $RSSI_j$
    return ID of the first element in C
  end if
end for
return `null` ▷ No valid parent found

3.3 Node Health Check and Retransmission Mechanism

The proposed system enables nodes to assess the health of their parent nodes based on the relayed uplink packet information, ensuring network stability. Additionally, after switching the uplink destination, failed transmission data is retransmitted. The selection of the new uplink destination in this process follows the routing policy described in Sect. 3.2, which is based on the most recent RSSI values and hierarchical level constraints. The operational algorithm is as follows:

1. The leaf node (n+2 layer) sends an uplink packet to the relay node (n+1 layer).
2. The sent packet is recorded, and **a timer is started**.
3. The relay node (n+1 layer) receives the packet and forwards it to the root node (HQ, n layer).
4. Determine the status of the relay node
   - **If the relay node is operational (Relay Success)**:
     Within the set time, the leaf node receives the forwarded packet sent by the relay node to the root node. If the received packet matches the recorded packet, the record is deleted, and the relay node is deemed functional. This normal relaying process is illustrated in Fig. 4.
   - **If the relay node is down (Relay Failure)**:
     If the leaf node does not receive the forwarded packet within the set time, it detects a failure in the relay node and selects a new uplink destination. Using the stored information in the table, it attempts to reconnect to a new uplink node. Once a new uplink destination is established, the recorded packet is retransmitted. The reconfiguration and retransmission flow is illustrated in Fig. 5.

4 Experiments and Evaluation

4.1 Experimental Setup

The experimental network consists of one root node (ID:00), three relay nodes (ID:01, ID:02, ID:03) at Level 1, two intermediate nodes (ID:04, ID:05) at Level 2, and one leaf node (ID:06) at Level 3, as illustrated in Fig. 6.

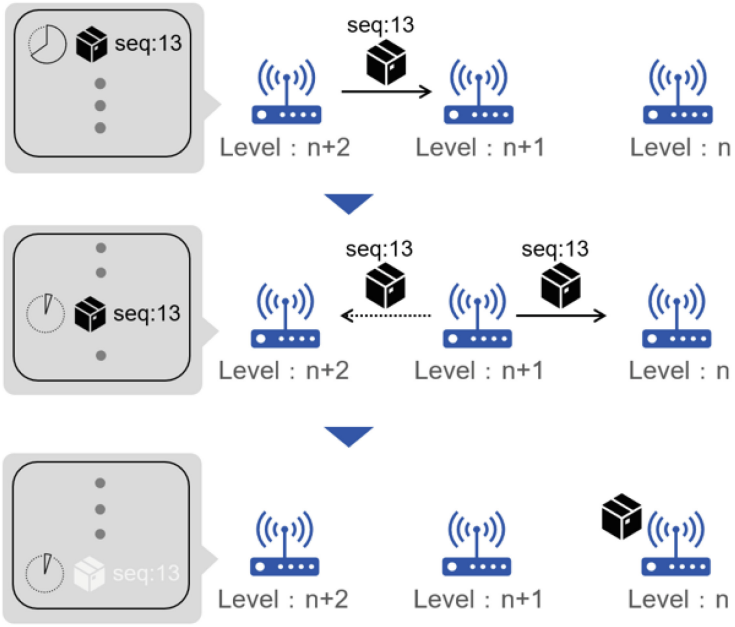

Fig. 4. Normal Relaying Process.

Initially, each node was manually configured to connect with a designated parent node based on deployment location and predefined ID mapping. This initial setup allowed control over the network's logical topology, ensuring that nodes began with the intended hierarchical structure. The experiment later evaluates the system's capability to autonomously reconfigure paths upon node failure, according to the routing policy discussed in Sect. 3.2.

4.2 Failure Scenario and Reconfiguration Test

To evaluate the fault tolerance of the system, we simulated a failure of relay node ID:03.

Node ID:05 was pre-configured with multiple uplink candidates and, upon detecting the failure, was expected to autonomously select a new uplink using its stored RSSI and level information.

Table 3 lists the actual uplink candidate entries stored by node ID:05 before the failure of ID:03. As shown, node ID:02 had the strongest RSSI among nodes at Level 1.

The network configuration during the failure scenario is depicted in Fig. 7.

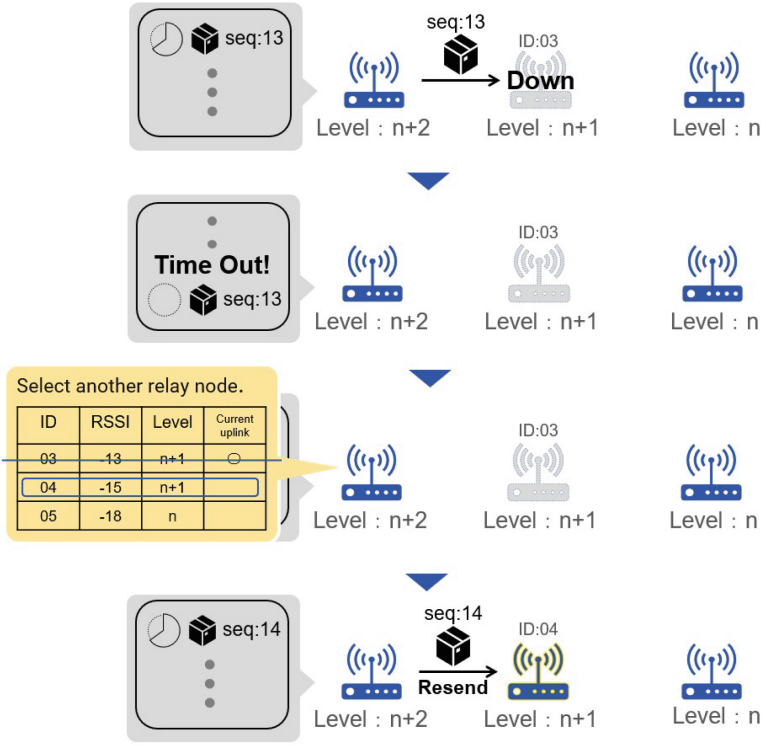

Fig. 5. Retransmission Process.

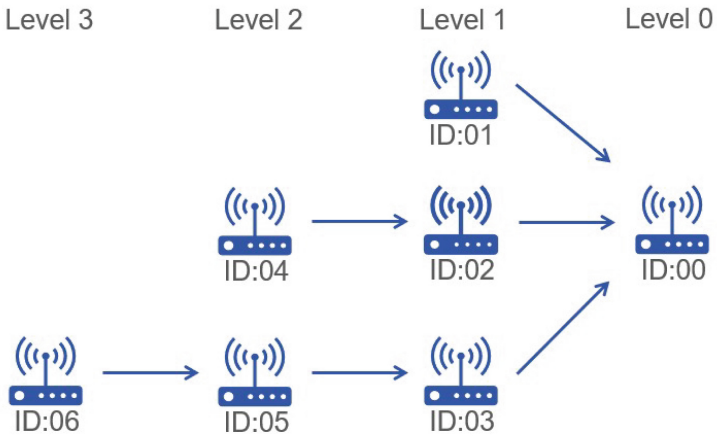

Fig. 6. Initial uplink paths of each node.

Table 3. Stored Uplink Candidates in Node ID:05 (Before Failure)

ID	RSSI	Level
01	–23	1
02	–20	1
03	–18	1
04	–19	2
06	–18	3

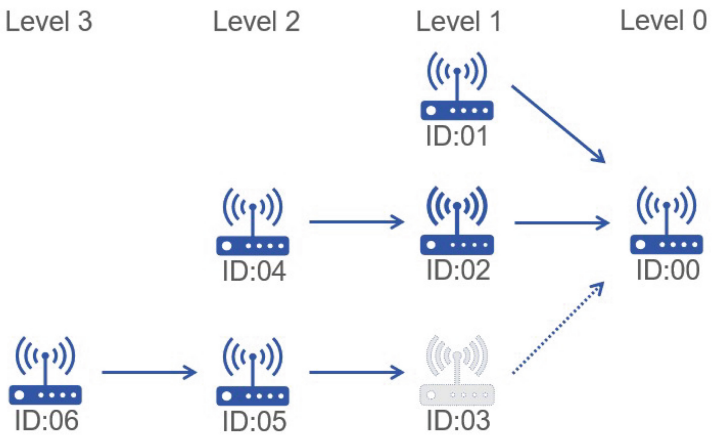

Fig. 7. Network Configuration During Failure.

4.3 Results and Recovery Performance

After ID:03 failed, node ID:05 autonomously selected ID:02 as the new uplink node. This selection was based on the highest RSSI and level consistency with the hierarchical constraint defined in the routing policy. Subsequently, the packet from ID:06 was successfully routed through ID:05 and ID:02 to the HQ (ID:00).

These results demonstrate that the proposed system can autonomously reconfigure the network in response to node failure and maintain uninterrupted data delivery. Figure 8 illustrates the reconfigured network topology.

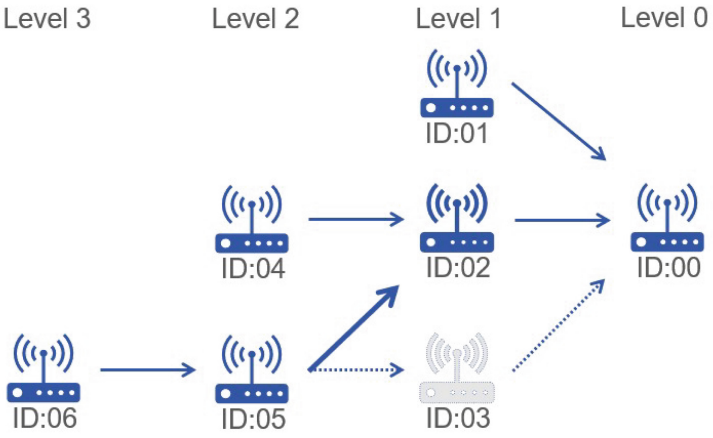

Fig. 8. Network Topology After Reconfiguration.

5 Discussion

This section outlines how the proposed system operates under real-world disaster scenarios, focusing on the failure conditions and the autonomous recovery process executed at each node.

5.1 Expected Failure Conditions

The system is designed to address the following common failure cases:

- A relay node becomes unreachable due to physical damage (e.g., landslides, flooding, or power outages).
- Temporary signal loss or obstruction causes upstream acknowledgment packets (ACKs) to be undelivered within the timeout period.

In such situations, each node autonomously executes a predefined recovery sequence to restore communication and continue data delivery.

5.2 Autonomous Recovery Steps

1. **Failure Detection:** The node monitors the return of acknowledgment packets. If no ACK is received within the specified timeout period, the uplink is considered failed.
2. **Candidate Lookup:** The node refers to its locally maintained table of candidate uplink nodes, which includes each candidate's RSSI and hierarchical level.
3. **Prioritized Selection:** Among candidates at the upper layer (i.e., level $n-1$), the node selects the one with the strongest RSSI as the new parent.

4. **Uplink Reconfiguration:** The node reconfigures its uplink path to the newly selected parent node.
5. **Data Retransmission and Confirmation:** Buffered data is retransmitted through the new uplink. Upon receiving an acknowledgment, the node deletes the corresponding buffered packet.

This fully distributed and lightweight recovery mechanism allows the network to self-heal without any centralized coordination or manual intervention, thereby preserving communication continuity even under partial infrastructure failures (Fig. 9).

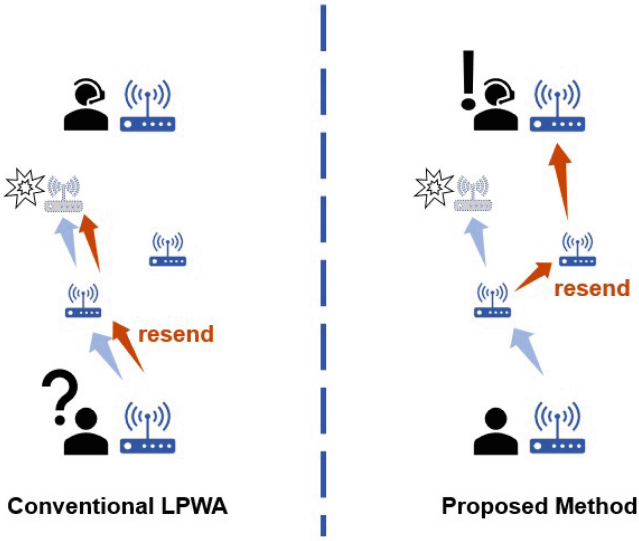

Fig. 9. Comparison between Conventional LPWA and Proposed Method in failure scenarios.

5.3 Practical Scenario: Disaster-Affected Regions

A typical real-world application is in disaster-stricken evacuation shelters equipped with LPWA-enabled sensors. These sensors transmit emergency alerts or environmental data to the municipal headquarters (HQ), which acts as the root node. Even if intermediate relay nodes become inoperable, the shelter (leaf node) can autonomously reconfigure its path and continue transmitting critical information—such as survivor counts or hazard warnings—without confirming delivery status or relying on external support.

6 Conclusion

In this study, we proposed an autonomous communication network reconstruction method using LPWA to restore communication infrastructure in disaster scenarios. The proposed method enables each node to dynamically assess the health status of its upper-layer node and select an alternative relay node when a failure occurs, ensuring network continuity.

The experimental results demonstrated that even in the event of a node failure, end nodes could autonomously select an appropriate relay node and successfully transmit data to the root node. Specifically, when a relay node became inoperable, an alternative uplink path was dynamically selected, ensuring successful data delivery from the end node to the root node. These findings confirm the effectiveness of the proposed method in maintaining network integrity under failure conditions.

For future work, evaluations in larger-scale network environments and verification of interoperability with different LPWA technologies are necessary. Additionally, optimizing the dynamic path selection algorithm could further enhance the speed and stability of network reconstruction, contributing to the realization of a more resilient LPWA-based communication network.

References

1. Ministry of Internal Affairs and Communications: Latest Trends in Wireless Communication Technologies for the IoT Era (2023). https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000114.html
2. Tanaka, K., Maeda, H., Yamashita, K., Liu, Y., Hazarika, H.: Implementation and proof experiment of communication network for disaster prevention using LPWA. In: Gervasi, O. et al. (eds.) ICCSA 2022 Workshops, LNCS, vol. 13379, pp. 42–55. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-10545-6_4
3. EASEL Co., Ltd.: ES920LR3 Product Overview. https://www.easel5.com/products/es920lr3/
4. Noreen, U., Bounceur, A., Clavier, L.: A study of LoRa low power and wide area network technology. In: 2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), pp. 1–6. IEEE (2017). https://doi.org/10.1109/ATSIP.2017.8075570
5. Kinoshita, S., Tanaka, K.: Tree topology communication network construction of LPWA. In: Proceedings of the 11th International Symposium on Applied Engineering and Sciences (SAES2023), pp. 305–306 (2023)