CIGRE-US National Committee
2024 Next Generation Network Paper Competition

IoT-enabled Traveling Wave Protection

D. ETINGOV[1], P. ZHANG[1,2], Y. SHAMASH[1,2]
Member ID: 920220116
Ph.D. Student, Research Project Assistant, Power Systems Engineer
1. Stony Brook University, 2. EMTEQ, LLC
Dmitrii.Etingov@StonyBrook.edu

SUMMARY

The paper presents an IoT-based Traveling Wave Protection (TWP) system for microgrids, aimed at improving real-time communication and data processing within protection systems. The system utilizes the Discrete Hilbert Transform (DHT) as a signal processing technique for time-of-arrival fault detection, chosen for its computational efficiency for low-power systems and for its suitability for dynamic microgrid environments.

The modernized IoT-based TWP system was tested across various microgrid configurations, showing high accuracy in fault detection and strong resilience against false tripping. These features are essential for maintaining stability in microgrids with Distributed Energy Resources (DERs). The system's performance was validated through Hardware-in-the-Loop (HIL) testing, where it demonstrated superior speed and reliability compared to traditional methods.

The system was built on the Nvidia Jetson Nano platform, providing a cost-effective and low-power solution that reduces power consumption compared to conventional protection systems. Practical advantages of this platform are highlighted by its favorable comparison with traditional protection systems, as well as by its ability to meet the computational demands of TWP with lower cost and reduced energy use. The system is developed to be accessible in the standalone mode with user friendly interface.

KEYWORDS

Internet of Things (IoT), Traveling Wave Protection (TWP), Microgrids, Microgrid Protection, Discrete Hilbert Transform (DHT), Fault Detection, Real-Time Data Processing, Low-Cost Smart Relays, Hardware-in-the-Loop (HIL), Renewable Energy Integration.

1. INTRODUCTION

As power system protection evolves, especially in microgrids, the Internet of Things (IoT) offers a flexible, cost-effective solution. IoT enhances real-time communication and data processing, which are critical for advanced microgrids [1, 2]. Advanced algorithms and data analytics [3] enable IoT to handle complex datasets, necessary for adaptive protection in dynamic Distributed Energy Resources (DERs) and load profiles.

While IoT integrates smart mechanisms using low-cost hardware, traditional platforms like Arduino and Raspberry Pi face challenges, such as limited support for fast, secure data communication, and accurate handling of high volumes of real-time data.

Integrating IoT with traditional relay protection in microgrids presents challenges [4], including issues like islanding, fault current variations, and false tripping during re-synchronization [5]. Grounding also poses difficulties due to the heterogeneity of the systems and the absence of zero-crossing. Previous studies [6, 7] focused on conventional methods like the differential protection [8, 9] and the overcurrent protection [10], which are more suitable for small-scale systems. DERs and varying operational modes complicate protection and automation, which aim to restore power post-fault. Travelling Wave Protection (TWP) techniques, scalable and unaffected by renewable sources, are increasingly adopted in microgrid configurations [11, 12]. However, transient detection methods, like wavelet transform, face limitations due to the transient response of capacitive voltage transformers (CVTs) and high computational demands.

Current market solutions provide directional relaying using high-frequency sampling of voltage and current, but this approach is uncommon in microgrids due to its high computational costs. In microgrids, fault-induced transient waves often reflect within the network, leading to information loss and underscoring the need for advanced strategies.

IoT platforms can enhance real-time communication and data processing in power systems, addressing gaps in speed and accuracy found in traditional systems. This approach involves implementing new algorithms to accurately interpret fault waveforms.

This paper presents an IoT-based traveling wave protection system for microgrids. The main contributions of this work are:

- A traveling wave protection scheme suitable for microgrid and distribution topology: It supports an IoT-based architecture for the time of arrival fault detection and location with composite wave impedance, and conductance, using Discrete Hilbert Transform.
- A cost-effective smart IoT prototype with functionalities of commercial relays in the designed box with a user interface accessible via screen or remotely.
- A real-time hardware-in-the-loop setup based on the advanced RTDS NovaCor chassis to validate the robustness of the proposed IoT solution with small-scale and Banshee microgrid systems: The proposed solutions work effectively when subjected to a diverse set of conditions.

2. METHODOLOGY

This section outlines the theoretical basis of our Traveling Wave Protection (TWP) method. The single-end fault location concept is based on foundational work from our lab [13] with upgraded from [14] IoT component with modified interfaces and monitoring with some additional upgrades expressed in Subsection 2.6. We introduce a novel adaptation of the Discrete Hilbert Transform (DHT) for IoT-based TW protection, chosen for its processing speed and applicability. Compared to the Wavelet Transform, DHT is more adaptable to dynamic grid topologies, offering higher computational efficiency for real-time applications.

2.1. DISCRETE HILBERT TRANSFORM FOR TIME OF ARRIVAL

The Discrete Hilbert Transform (DHT) [15] is a linear operator that generates an analytic signal from a real-valued function $f(t)$:

$$H[f(t)] = \frac{1}{\pi}\int_{-\infty}^{\infty}\frac{f(\tau)}{t-\tau}d\tau$$

This signal, $x_a(t) = x(t) + jH[x(t)]$, provides the envelope $E(t)$ and instantaneous phase $\phi(t)$:

$$E(t) = |x_a(t)| = \sqrt{x(t)^2 + H[x(t)]^2}$$

$$\phi(t) = \arg\big(x_a(t)\big) = \arctan\left(\frac{H[x(t)]}{x(t)}\right)$$

The time of arrival and the direction of the traveling wave are determined by analyzing the peaks and phases of the envelope.

2.2. PROPOSED ADDITIONAL TW-BASED PROTECTION COMPONENTS

The composite wave impedance Z_Σ and conductance S_Σ at any impedance mismatch are given by:

$$Z_\Sigma = \frac{u}{i} = \frac{1+\rho}{1-\rho}(-Z_C)$$

$$S_\Sigma = \frac{i}{u} = \frac{1-\rho}{1+\rho}\,\frac{1}{(-Z_C)}$$

where Z_C is the characteristic impedance, and ρ is the reflection coefficient. For forward faults, $\frac{Z_\Sigma}{-Z_c} \geq 1+\varepsilon_1$. For reverse faults, it remains close to 1, with $\rho = 0$.

The protection distance element isolates faults within a predefined area by calculating the apparent impedance $Z_{APP(LOOP)}$ and mapping it onto a distance-to-fault axis, *m:*

$$m = \frac{Re(V_{LOOP} \cdot S^*_{POL})}{Re(Z_R \cdot V_{LOOP} \cdot S^*_{POL})}$$

Faults are detected by identifying signals that exceed a threshold $kM(x)$, where $M(x)$ is the median value:

$$f(t) = \begin{cases} 1 & if\ x(t) > kM(x) \\ 0 & otherwise \end{cases}$$

2.3. DIRECTIONAL COMPONENT LOGIC

For directional component, the ratio $\frac{Z_\Sigma}{-Z_c}$ plays a crucial role in determining the fault directionality. The logic is defined as follows:

Forward Fault:

The ratio $\frac{Z_\Sigma}{-Z_c} \geq 1+\varepsilon_1$ indicates a forward fault condition. The value of ε_a is a small positive threshold to ensure reliable detection.

Similarly, $\frac{S_\Sigma\ (-Z_c)}{1} \geq 1+\ \varepsilon_1$ serves as a criterion for confirming a forward fault.

Reverse Fault:

In the case of reverse faults, the reflected traveling waves (TWs) are not detected at the relay point, leading to $\rho = 0$. Consequently, the $\frac{Z_\Sigma}{-Z_c}$ remains close to 1, specifically:

$$\frac{Z_\Sigma}{-Z_c} < 1+\varepsilon_2,$$

where ε_2 is a smaller threshold ensuring the detection of reverse faults. The fault detection logic involves checking if either of the above conditions is met. If so, the relay triggers a positive logic for fault occurrence. The difference in thresholds ($\varepsilon_1 > \varepsilon_2$) ensures a clear distinction between a forward fault and a reverse fault.

2.4. PHASE-TO-MODE CONVERSION FOR MULTI-PHASE SYSTEMS

In a multi-phase system, the inter-phase coupling necessitates the use of phase-to-mode conversion to apply the wave impedance relay criterion. The symmetric component transformation matrix *S* and its inverse S^{-1} are utilized

$$S = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{bmatrix},\quad S^{-1} = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix}$$

The relay's operation criterion is then extended to a three-phase system for forward faults using modulus voltage and current values where for each mode $j = 0\ (zero), \alpha\ (positive), \beta\ (negative)$ sequences the protection criterion is applied as:

$$\frac{Z_{\Sigma(j)}}{-Z_{c(j)}} \geq 1 + \varepsilon_1 \text{ or } S_{\Sigma(j)}\left(-Z_{C(j)}\right) \geq 1 + \varepsilon_1$$

On the other hand, for reverse faults:

$$\frac{Z_{\Sigma(j)}}{-Z_{c(j)}} < 1 + \varepsilon_2 \text{ or } S_{\Sigma(j)}\left(-Z_{C(j)}\right) < 1 + \varepsilon_2$$

2.5. FREQUENCY DOMAIN ANALYSIS AND REFLECTION COEFFICIENT

The reflection coefficient ρ is a critical parameter for analyzing fault-induced traveling waves. It is defined as:

$$\rho = \frac{Z_2 - Z_1}{Z_2 + Z_1}$$

where Z_2 is the impedance after the fault, and Z_1 is the impedance before the fault, and coefficient takes values between -1 and +1 and is purely real for distributed line impedances. In the frequency domain, ρ is expressed as:

$$\rho(j\omega) = \frac{Z_2(j\omega) - Z_1(j\omega)}{Z_2(j\omega) + Z_1(j\omega)}$$

This extension of the reflection coefficient into the frequency domain allows for the consideration of frequency-dependent impedance characteristics, crucial for accurate fault detection and protection in modern power systems.

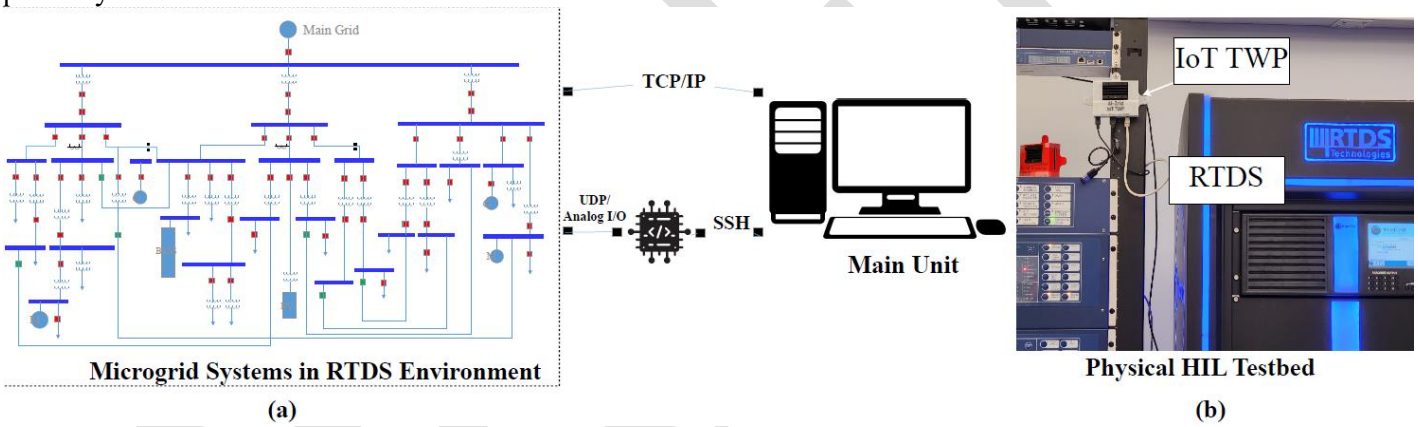


Figure 1: The IoT-Enabled Traveling Wave Microgrid Protection: (a) Schematic Overview. (b) Experimental Setup with IoT TWP v.1 mounted.

2.6. IoT COMPONENT

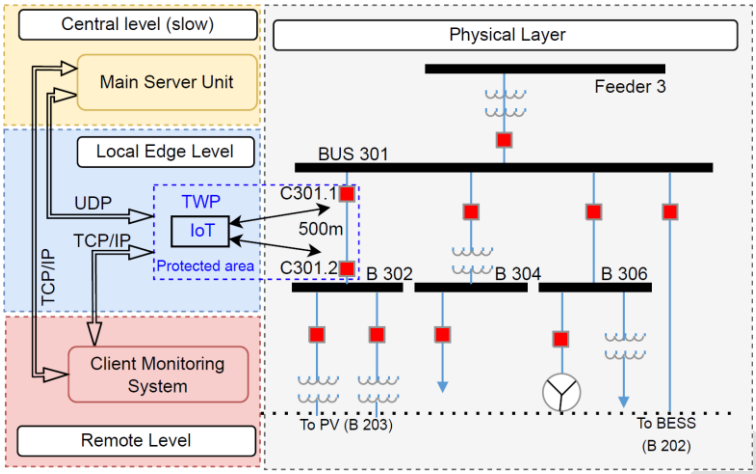
Our cost-effective, low-power traveling wave prototype is built on the Nvidia Jetson Nano 2GB hardware platform, which provides GPU processing capabilities at a cost of less than $100 per unit.

The design is intended to perform TWP functions in a distributed manner, featuring a user-friendly interface and the ability to communicate with a central unit. The TWP IoT device incorporates an integrated GPU, significantly enhancing its computational performance while maintaining a low power consumption of just 15W. Compared to traditional terminals that typically consume around 150W, this reduction in power requirement not only decreases the demand on the secondary network power but also enhances the overall system reliability. This approach has already been successfully implemented in our prototype, with the architecture illustrated in Fig. 2. The core metrics derived from the extracted TW features of an IoT setup are graphically depicted in Figures 4a, 4b, and 4c, showcasing the results obtained from processing the fault signal.

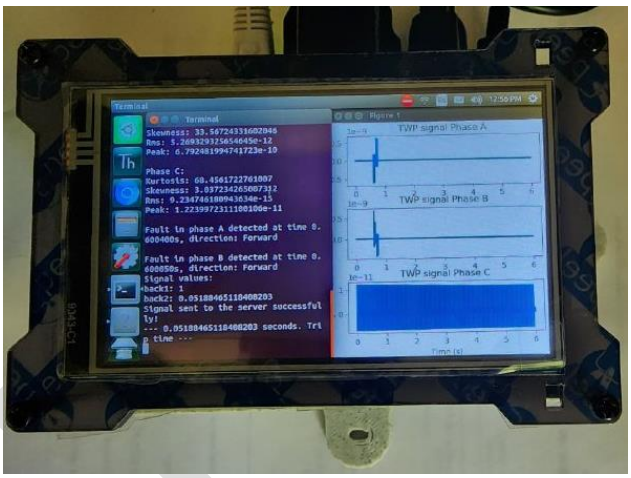
The TWP system processes a vast array of data for protection and fault location operation. The application demands reliable and real-time communication and contains a few levels:

- **Local Edge Level (Fast)**: This level ensures the execution of simple, safety-critical functions based on local information received directly from the IoT components, which are equipped with decision-making capabilities. It operates on very fast timescales to maintain system integrity, executing decisions within milliseconds, typically in less than 0.1 seconds, leveraging the current IoT hardware.

- **Central Level of the Main Unit (Slow)**: This level facilitates coordinated actions across the microgrid, providing comprehensive system monitoring for both standalone and IoT network modes. It employs complex algorithms with response times ranging from 100 milliseconds to several seconds, requiring the aggregation of data from dispersed network components to ensure synchronized and effective operation.



(a) IoT TWP architecture



(b) Developed IoT TWP v.1.2 with a standalone monitoring and control interface

Figure 2: IoT TWP architecture with the front view panel

- **Remote Level**: This level allows engineers in remote locations to observe and monitor parameters from all layers, offering an essential perspective for system oversight and performance analysis. It is designed for remote diagnostics, performance tracking, and decision-making tasks, such as predictive maintenance scheduling and protection settings optimization. These functions are driven by detailed analysis of both historical and real-time data, contributing to enhanced system reliability and operational efficiency.

Upon detecting a fault within the internal area on the local level IoT components, the system promptly dispatches two distinct command signals, labeled *back 1* and *back 2*, to the server via UDP protocol. The *back 1* signal functions as a logical trigger that can be integrated into relay logic systems for actuating circuit breakers, blinker (signal) relays, or other dispatch automatic systems as designated by a relay protection engineer. Conversely, the *back 2* signal is tasked with conveying the trip timing information. Additional parameters are stored within the IoT device, accessible off-site via a Linux-based command interface to the central level using a local network (Ethernet gate with UDP) or Internet access for monitoring and distance IoT component operation using TCP/IP, with a speed range of 256 samples per 20 ms.

To enhance the device's versatility and operational autonomy, a new version of the IoT device has been developed. This updated model features a mounted screen and an integrated cooling system, enabling it to operate in standalone mode without the need for an external device. The screen allows for direct terminal access, while SSH connections via PuTTY can be established for remote management. Additionally, the device now includes an enabled Wi-Fi module, allowing for wireless accessibility, which further simplifies deployment and monitoring in various environments.

Security is ensured through layered authorized access: monitoring engineers have Level 1 - limited access to system overview, while system engineers responsible for the operation have Level 2 access with permission to change parameters. It is important to note that for optimal performance and to ensure the safety of the prototype in the designed case, it should be placed in a covered, water-resistant environment. This protective environment should maintain a temperature range between −25°C (−13°F) and 80°C (176°F) during its Time to Peak (TTP) operation.

3. TEST AND VALIDATION

The focus is on assessing its real-time effectiveness during Hardware-in-the-Loop (HIL) testing, specifically evaluating the performance of our solution with the RTDS NovaCor element with the potential to compare traditional relay protection terminals (distance, TWP, overcurrent, and others). Given the limited availability of Traveling Wave Protection (TWP) methodologies tailored for microgrid systems, we employed the overcurrent method as a comparative basis for analyzing trip times. Communication between the IoT device and the RTDS is facilitated using the User Datagram Protocol (UDP). For remote monitoring and control functions, we utilize

a Wi-Fi module in conjunction with internet connectivity, enabling network-based SSH communication via PuTTY, assuming the IoT device is part of the network. The complete HIL setup, which is central to our study, is illustrated in Fig. 1.

Our experiments encompass both small-scale and Banshee microgrids, providing a diverse range of application scenarios to evaluate our method under various conditions. The paper provided plot results from The Banshee microgrid, which is an industrial system. It is composed of three radial feeders, handling loads ranging from 5 MW to 14 MW. It operates at voltage levels of 13.8 kV, 4.16 kV, 480 V, and 208 V. Loads within the microgrid are categorized as critical, priority, or interruptible, with contingencies managed accordingly. The microgrid is equipped with photovoltaic (PV) systems, Battery Energy Storage Systems (BESS), Combined Heat and Power (CHP) units, and diesel generators, ensuring reliable operation across a wide array of scenarios.

4. RESULTS AND DISCUSSION

The IoT-enabled Traveling Wave Protection (TWP) solution was evaluated across various microgrid configurations to assess its performance under different conditions. Signals transmitted via the IoT component were remotely monitored using the SSH protocol.

In the weak microgrid configuration, circuit breakers were maintained in the normally closed (NC) position during both islanded and grid-connected modes under normal operation.

A solid three-phase (ABC) fault was simulated outside the protection area Fig. 3a, where the TWP solution demonstrated robustness by resisting external fault tripping. Relay characteristics confirmed that the relay trajectory remained outside the trip area, ensuring that the TWP elements stayed inactive.

The response to an internal two-phase (AB) fault is illustrated in Fig. 3b. The distance element tripped earlier than the directional component, underscoring the advantage of a combined protection approach. Specific trip times are detailed in Table 1.

External faults near both the main grid source and PV 1 did not compromise the TWP performance when using the combined methods. The analysis revealed that Distributed Energy Resources (DERs) introduce more protection challenges than the main grid generator.

Island mode operations highlighted some limitations, particularly during re-synchronization, which could result in false-positive tripping. Monitoring the main grid status via IoT can aid in adjusting protection settings during islanded operations. The study also examined the detection of weaker single-phase faults. The results, depicted in Fig. 3c, demonstrated successful fault detection.

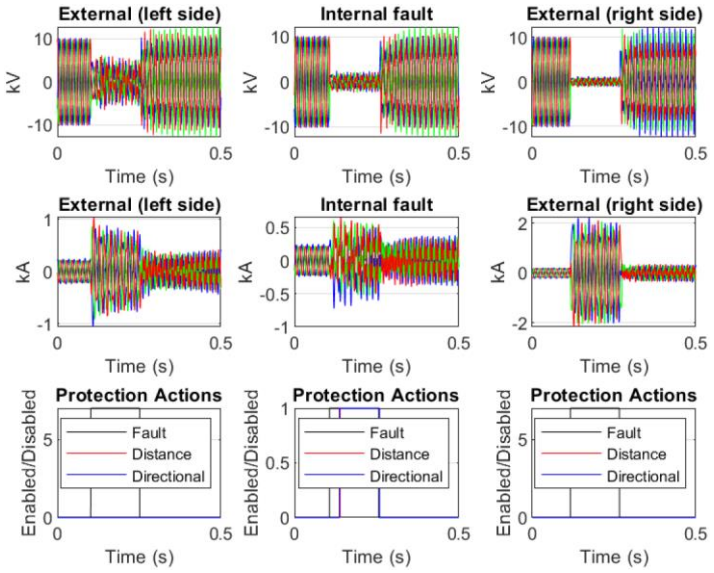
MHO impedance characteristics Fig. 5 indicated that relying solely on the distance element without the directional component could result in false-negative tripping, potentially disconnecting certain topology elements. This emphasizes the critical role of the directional component in ensuring reliable protection.

The Banshee microgrid model was tested for robustness in Fig 4. A three-phase (ABC) fault on the protected line's right side confirmed the IoT TWP solution's accuracy, with no false tripping from distance or directional elements. The extracted fault signal features show oscillations above 0.5 p.u., indicating a fault. The threshold, in per unit (p.u.), should be adjusted based on the voltage level and traveling wave window size. The complex Banshee topology introduces specific noise types—primarily related to harmonics and transients dueto the coexistence of renewable and traditional energy sources in operation.

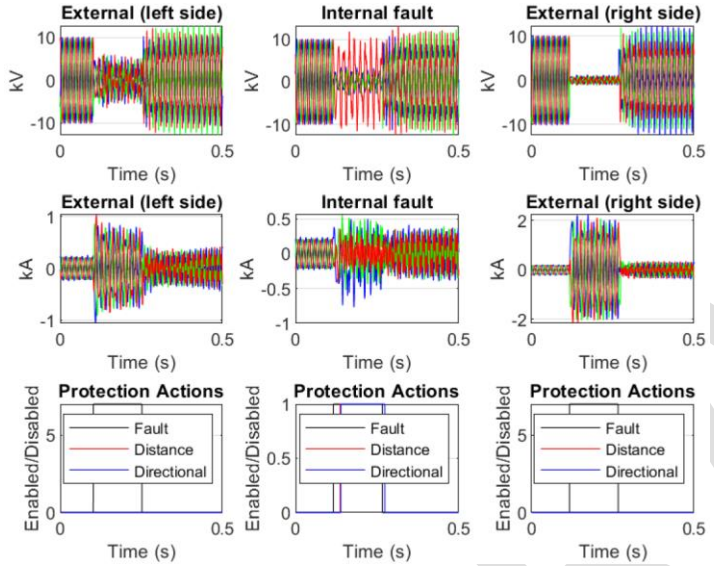
Fig. 6 highlights that the fault trajectories remained outside the MHO circle throughout the fault duration, confirming the identification of an external fault beyond the protection zone. This analysis also examined the impact of different energy sources on the system. Distributed Energy Resources (DERs) can introduce disturbances within the system, prompting the IoT component to swiftly send a trip signal. A comparative analysis demonstrated that the IoT TWP was more effective in preventing false-positive trips.

Further evaluations of two-phase (AB) and single-phase (A) faults consistently triggered reliable tripping. Fig. 6b and 6c show the IoT-enabled TWP responses. External faults, both left and right of the protection zone, revealed no tripping by the distance element, as fault characteristics remained outside the MHO circle. TW-based directional protection correctly identified reverse faults, preventing unnecessary trips.

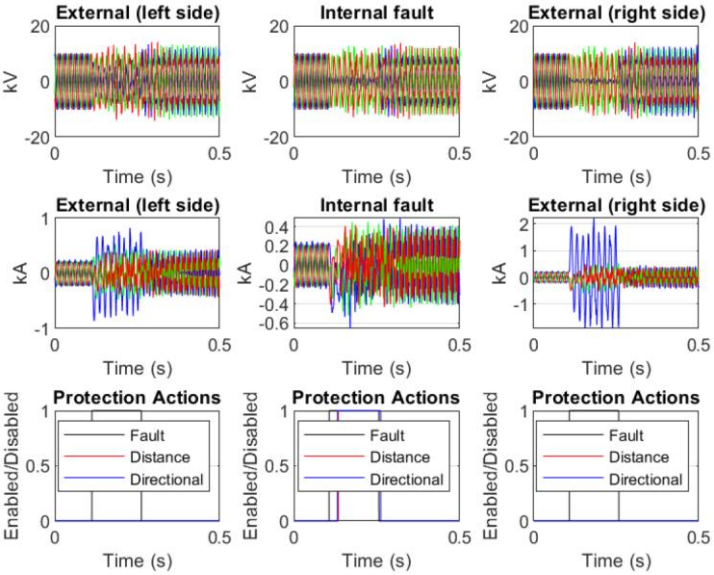
During a weak single-phase fault, the IoT TWP effectively detected the internal fault, outperforming the less sensitive and reliable RTDS TWP model in this scenario. This significant difference highlights the IoT-enabled system's superior ability in managing weak fault- conditions, showcasing the potential of IoT technology to enhance the reliability and responsiveness of microgrid protection. The study highlights IoT-based TWP solutions as crucial for enhancing microgrid resilience and efficiency, effectively addressing diverse fault conditions.



a) Three-phase fault enabled at t = 0.1 s

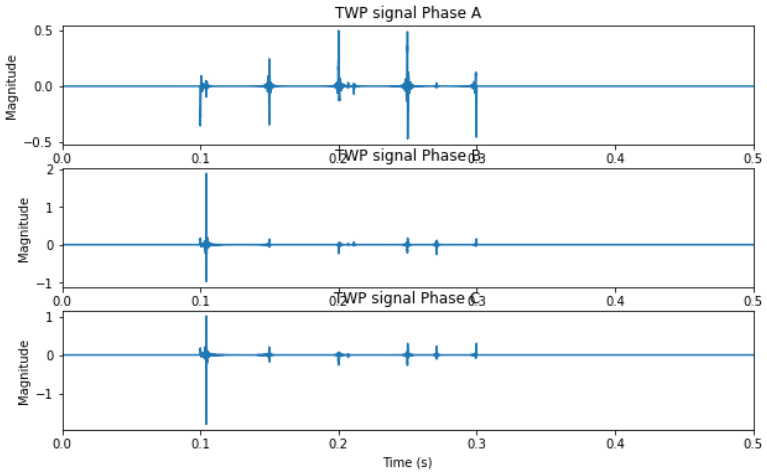


b) Two-phase fault enabled at t = 0.1 s

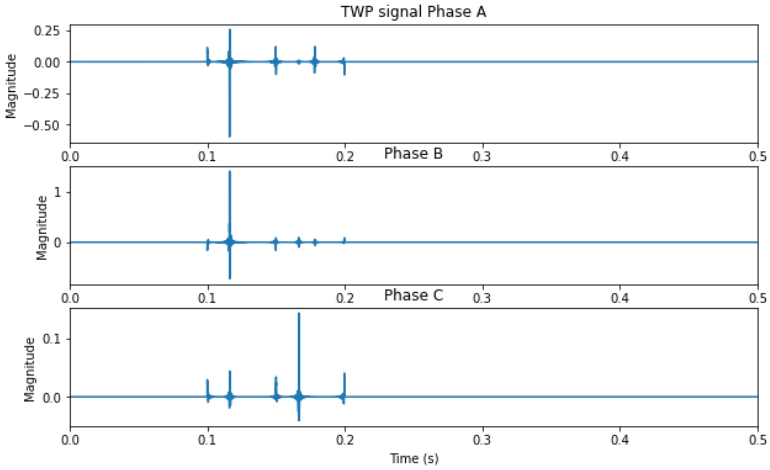


c) One-phase fault enabled at t = 0.1 s

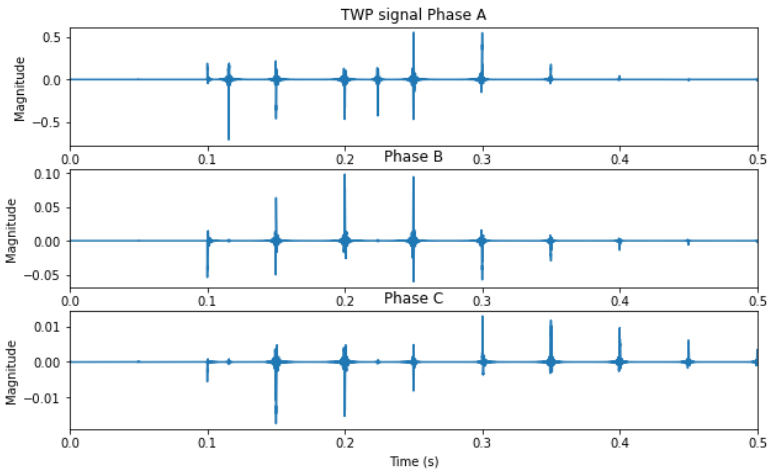
Figure 3: IoT-Enabled TWP performance in the Banshee microgrid system



a) Three-phase fault

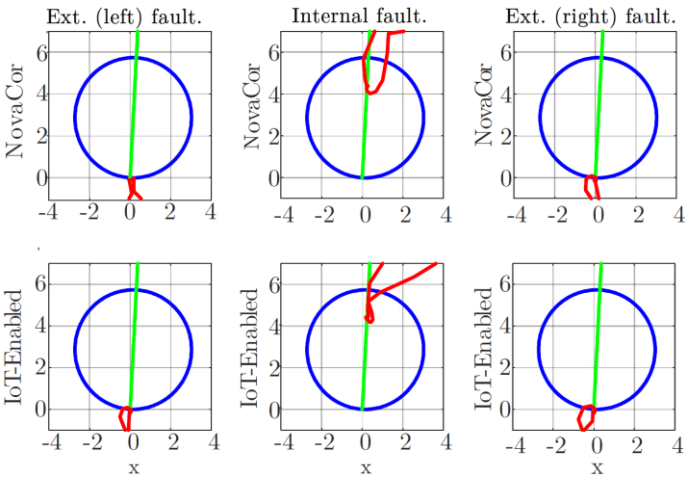


b) Two-phase fault

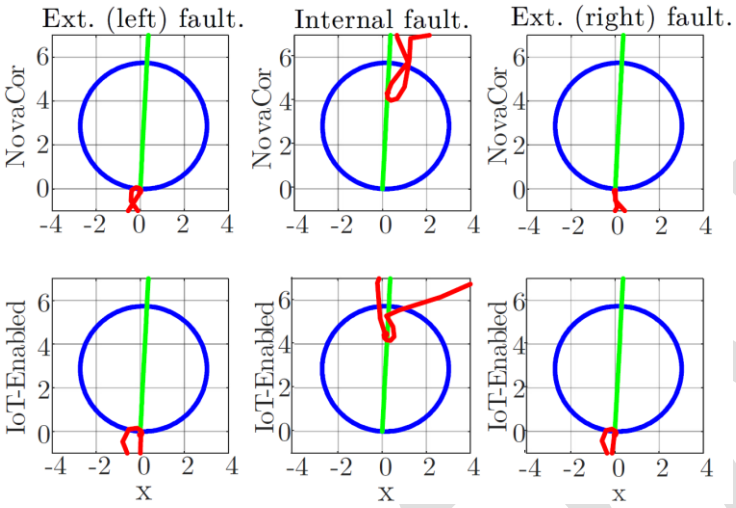


c) One-phase fault

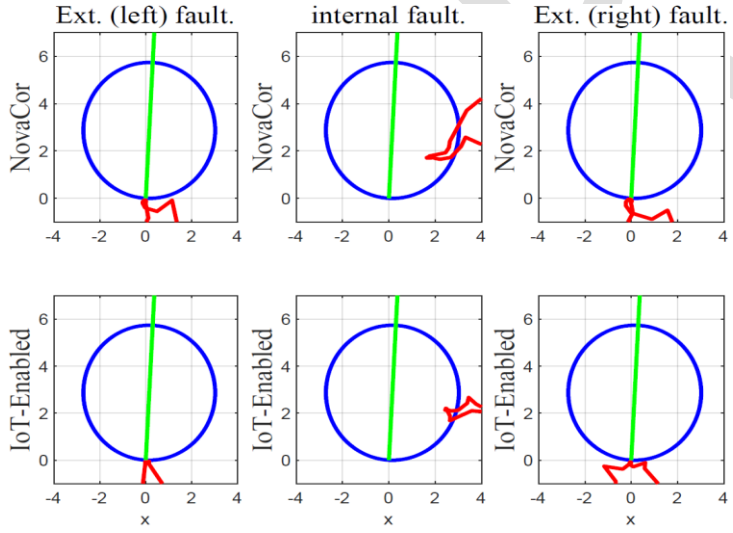
Figure 4: Processed signal from the TWP IoT hardware during fault conditions in Banshee microgrid. Note: Auto-scaling function is applied. The threshold is set for magnitudes greater than 0.5.



a) Three-phase fault

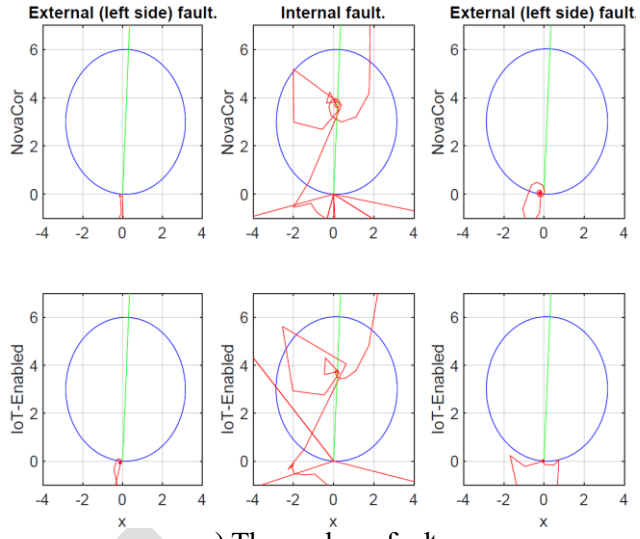


b) Two-phase fault

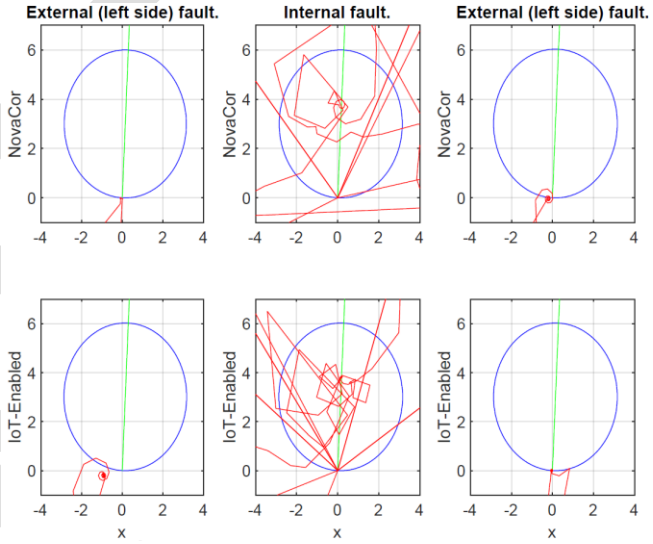


c) One-phase fault

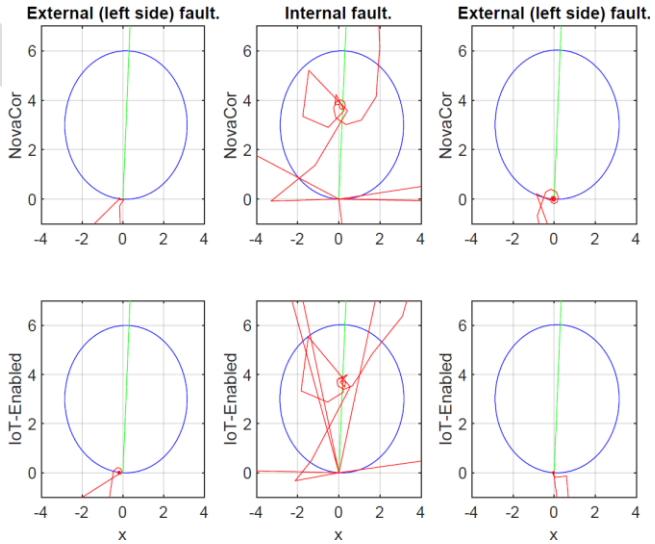
Figure 5: MHO (Z) characteristic in RTDS NovaCor protection (upper figure) compared to the received from IoT (lower figure) during faults in the small microgrid system.



a) Three-phase fault



b) Two-phase fault



c) One-phase fault

Figure 6: MHO (Z) characteristic in RTDS NovaCor protection (upper figure) compared to the received from IoT (lower figure) during faults in Banshee microgrid system.

The trip times shown in Table 1 highlight the promising potential of the proposed IoT-based Traveling Wave Protection (TWP) method. The trip times are below the threshold of 0.1 seconds for the common overcurrent protection in distribution topologies. Note: TWP is not used for distribution topologies, and standards are yet to be established due to the lack of market solutions. The distance protection terminals usually cost three times more than overcurrent solutions.

However, the better computational capacity allows for lower trip times across all fault types and system scales as outlined in Table 1. This suggests that with more advanced hardware, the trip times could be further reduced, and a more advanced hardware base with an additional sensing system for IoT might be required.

Table 1: IoT TWP trip times (*Back 2* signal) for Microgrid Systems based on Nvidia Jetson Nano 2GB capabilities.

System Scale	Fault Type	Time (s)
Small Microgrid	Three-phase (ABC) fault	0.0540
	Two-phase (AB) fault	0.0558
	One-phase (A) fault	0.0570
Banshee Microgrid	Three-phase (ABC) fault	0.058
	Two-phase (AB) fault	0.0581
	One-phase (A) fault	0.0589

Variations in trip time across different fault types and system scales highlight the challenges in microgrid protection, with time increasing as the number of faulted phases decreases. This variation is due to differing fault impedances and transient behaviours in small-scale and Banshee systems.

For internal faults in the protection zone, the Banshee system's distance element registered the fault trajectory within the MHO circle for all faulted phases. Concurrently, the TW-based directional element identified forward-oriented faults. In quantitative terms, the directional element exhibited a trip latency of milliseconds, while the distance element took slightly longer.

Results from both IoT-Enabled TWP and RTDS showed multiple frequency components in faults, suggesting the use of diverse frequencies for AI-enabled microgrid protection in future research. This might help to increase protection sensitivity in different topologies and liquidate protection blinding due to the changes in the system operation.

Table 2: Comparison of Protection Schemes for Microgrids

Metric	IoT TWP	Overcurrent*	Distance*	TWP
Trip Time (s) (3-Phase)	0.054	0.1+	0.08+	0.004
Fault Detection Accuracy	Very High	Medium	High	Very High
Directional Sensitivity	High	Low	High	Very High
Low Fault Current Handling	High	Poor	Fair	Not Applicable
False Tripping Resilience	High	Low	Medium	High
Cost-Effectiveness	Very High	High	Low	Moderate
Estimated Price	$150	$3,000+	$9,000+	$18,000+
Power Consumption (W)	15	150+	150+	100
Applicability in Microgrids	Applicable	Applicable	Moderate	Not Applicable

* Tests performed on mainstream standard commercial products.

5 CONCLUSION

This paper introduced an IoT-based Traveling Wave Protection (TWP) prototype with significant potential for implementation in low-voltage systems, particularly when integrated with renewable energy sources. The combination of IoT and TWP creates new opportunities across various grid settings, greatly enhancing the resilience of both microgrids and distribution grids.

In this study, we present a method that integrates an ensemble of developed directional and distance element schemes within an IoT framework. This integration leverages the wave impedance method alongside the Discrete Hilbert Transform to enable rapid signal processing in IoT-based applications. The result is a compact, cost-effective prototype that is well-suited for microgrids. Table 2 provides a summary comparison of different protection schemes for microgrids, highlighting key metrics such as trip time, fault detection accuracy, directional sensitivity, and cost-effectiveness.

The IoT-based TWP scheme stands out for its fast operation, high fault detection accuracy, and cost-effectiveness, making it particularly advantageous for microgrid applications. It offers significant improvements over traditional methods, including better handling of low fault currents, high resilience to false tripping, and reduced power consumption, all at a significantly lower cost. These factors position IoT TWP as a promising solution for enhancing the reliability and efficiency of microgrid protection.

Hardware-in-the-loop testing conducted with both the Real-Time Digital Simulator (RTDS) and the IoT prototype demonstrated excellent performance under both normal and fault conditions, highlighting its effectiveness compared to traditional systems. The IoT TWP approach exhibits superior accuracy over classical TWP methods, which are typically reliable only for transmission networks and less effective under single-phase faults. Moreover, the IoT TWP reduces false positives during re-synchronization with the main power grid, further emphasizing its suitability for modern grid applications.

BIBLIOGRAPHY

[1] P. Zhang, Networked microgrids. Cambridge, UK: Cambridge University Press, 2021.

[2] L. Wang, P. Zhang, Z. Tang, and Y. Qin, "Programmable crypto-control for iot networks: An application in networked microgrids," IEEE Internet of Things Journal, accepted, 2022. DOI: 10.1109/JIOT.2022.3194838.

[3] A. Mohamed, T. Lamhamdi, H. Moussaoui, and H. El Markhi, "Intelligent energy management system of a smart microgrid using multiagent systems," Archives of Electrical Engineering, vol. 69, pp. 23–38, 03 2020.

[4] A. Dagar, P. Gupta, and V. Niranjan, "Microgrid protection: A comprehensive review," Sustain. Energy Rev, vol. 149, no. 111401, 2021.

[5] H. J. Laaksonen, "Protection principles for future microgrids," IEEE Trans. Power Electron., vol. 25, no. 12, pp. 2910–2918, 2010.

[6] S. Sujeeth and O. G. Swathika, "Iot based automated protection and control of dc microgrids,"in 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 1422–1426.

[7] L. Xing, "Cascading failures in internet of things: Review and perspectives on reliability and resilience," IEEE Internet of Things Journal, vol. 8, no. 1, pp. 44–64, 2021.

[8] A. A. Eladl, M. A. Saeed, B. E. Sedhom, and J. M. Guerrero, "Iot technology-based protection scheme for mt-hvdc transmission grids with restoration algorithm using support vector machine," IEEE Access, vol. 9, pp. 86 268–86 284, 2021.

[9] D. A. Etingov and D. S. Fedosov, "Development of restraint algorithm for improvement of reliability of transformer differential protection during external short circuits," in 2019 International Ural Conference on Electrical Power Engineering (UralCon), 2019, pp. 388–393.

[10] H. Mafi, R. Yared, and L. Bentabet, "Smart residual current circuit breaker with overcurrent protection," in 2019 IEEE 2nd International Conference on Renewable Energy and Power Engineering (REPE), 2019, pp. 6–9.

[11] D. A. Etingov, P. Zhang, Z. Tang, and Y. Zhou, "AI-enabled traveling wave protection for microgrids," Electric Power Systems Research, vol. 210, p. 108078, 2022.

[12] L. Wang, Y. Qin, Z. Tang, and P. Zhang, "Software-defined microgrid control: The génesis of decoupled cyber-physical microgrids," IEEE Open Access Journal of Power and Energy, vol. 7, pp. 173–182, 2020.

[13] S. Jena and P. Zhang, "Traveling wave analysis in microgrids," in Microgrids: Theory and Practice, P. Zhang, Ed. Hoboken, New Jersey: Wiley-IEEE Press, 2024, ch. 31, pp. 761–783.

[14] D. A. Etingov, P. Zhang, Y. Shamash, "IoT-Enabled Traveling Wave Microgrid Protection," IEEE Internet of Things Journal (under review).

[15] S. Biswal, M. Biswal, and O. P. Malik, "Hilbert huang transform based online differential relay algorithm for a shunt-compensated transmission line," IEEE Transactions on Power Delivery, vol. 33, no. 6, pp. 2803–2811, 2018.