This article has been accepted for publication in IEEE Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MWC.2025.3600024

Autonomous Networked Wireless Power Transfer for the Internet of Batteryless Things: Future Vision and Research Opportunities

Ye Liu, Mikael Gidlund, Honggang Wang, and Gerhard Petrus Hancke

***Abstract*—The 6G massive Internet of Things envisions trillions of interconnected devices, set to revolutionize society by creating a more efficient and convenient ecosystem. However, this rapid expansion presents significant sustainability challenges, particularly in achieving alignment with the United Nations Sustainable Development Goals. A pressing concern is the "trillion-battery problem," where the need for frequent battery replacements poses environmental risks and disrupts data continuity. Zero-energy device technology is seen as a potential solution, yet it remains in its early stages, facing obstacles such as complex wireless power transfer behaviors, efficient charge scheduling, and vulnerability to malicious energy attacks. This article reviews the state-of-the-art in these areas, identifying existing knowledge gaps. A bibliometric analysis is conducted to reveal key research trends and developments. Building on these insights, we propose a versatile paradigm for autonomous networked wireless power transfer (AutoNetWPT), outlining research opportunities to address the challenges identified. This work is critical in shaping a sustainable, secure, and interconnected future for 6G zero-energy massive Internet of Batteryless Things.**

I. Introduction

THE advent of 6G technology marks a transformative era in connectivity, vastly expanding the Internet of Things (IoT) ecosystem. In this future landscape, trillions of interconnected devices will perform a wide array of sensing and communication tasks across sectors such as healthcare, agriculture, industrial automation, and smart cities. The capabilities of 6G IoT will enable real-time data collection, analysis, and intelligent decision-making, fundamentally changing how we live and work. According to Gartner Research's 2024 forecast, the IoT market is projected to reach $991 billion by 2028, underscoring its enormous potential for growth.

However, the proliferation of 6G IoT presents both opportunities and significant challenges, especially in the context of meeting the United Nations (UN) Sustainable Development Goals (SDGs) [1]. One of the most pressing challenges is the "trillion-battery problem," which introduces several critical obstacles: (i) frequent manual battery replacements; (ii) disruptions in mission-critical data due to battery depletion; (iii) reduced sensing frequency to conserve power, leading to incomplete or outdated data; (iv) limitations imposed by battery size; and (v) environmental and safety hazards associated with battery disposal. These issues directly affect SDG 7 (Affordable and Clean Energy) and SDG 9 (Industry, Innovation, and Infrastructure).

Ye Liu (corresponding author) is with Nanjing Agricultural University and Mid Sweden University; Mikael Gidlund is with Mid Sweden University; Honggang Wang is with Yeshiva University; Gerhard Petrus Hancke is with the City University of Hong Kong.

Addressing these battery-related challenges is essential for the successful deployment of 6G massive IoT [2]. Emerging zero-energy devices are garnering significant interest from both academia and industry [3]. These devices operate without batteries or manual charging by harvesting energy from the environment via green wireless power transfer (WPT) or ambient energy harvesting [4]. Future zero-energy devices, potentially as small as a grain of rice, will play a pivotal role in enhancing the sustainability of 6G IoT by reducing dependency on conventional batteries and mitigating electronic waste. The integration of zero-energy devices into 6G massive IoT offers substantial benefits, including improved energy efficiency, reduced operational costs, and enhanced applications. This innovation promotes sustainability by minimizing electronic waste and fostering environmentally responsible production, contributing to a more equitable and resilient global future.

To fully realize the potential of zero-energy devices, several challenges must be addressed. First, understanding the complex dynamics of WPT in three-dimensional environments is crucial, as it involves managing interactions between distributed power transmitters and ultra-dense networks of zero-energy IoT devices. Second, the scheduling of wireless power transmitters must be optimized to dynamically manage power distribution, adapting in real-time to fluctuating application requirements, device mobility, and variable wireless power conditions. Third, the threat of malicious energy attacks poses a significant security concern. As IoT devices become reliant on harvested energy, they are vulnerable to energy attacks, where adversaries may drain or overload energy resources, leading to system failures. Unlike data communication, wireless energy transmission cannot be encrypted or authenticated, making it an attractive target for malicious actors. Moreover, zero-energy devices' limited energy and computational capacity complicates the development of robust security mechanisms.

This article overcomes these challenges for the zero-energy Internet of Batteryless Things (IoBT) by providing the following specific contributions:

- We conducted an extensive bibliometric analysis of WPT research for the zero-energy IoBT from 2015 to 2024, shedding light on key trends and highlighting the field's evolutionary trajectory. This analysis identifies major research themes and emerging opportunities within the IoBT landscape.

- Building on insights from our bibliometric analysis, we introduce AutoNetWPT (Autonomous Networked Wireless Power Transfer), a flexible and autonomous system designed to manage wireless power distribution securely and efficiently. Tailored for the 6G zero-energy IoBT, AutoNetWPT offers advanced features for adaptive power management and enhanced security in energy transfer.
- We conducted extensive experimental studies on distributed charging networks with concurrent power transmission and reception, uncovering the complex power dynamics that characterize these systems. Additionally, we examined malicious energy attacks targeting power transmitters and zero-energy devices, revealing insights into vulnerabilities and suggesting defense strategies for more secure energy transmission.

The remainder of this article is structured as follows. First, we review the current state-of-the-art and extend the discussion beyond existing challenges. Next, we introduce our vision of an autonomous networked wireless power transfer system, supported by bibliometric analysis. We then identify key research opportunities to bridge existing gaps. Finally, we provide concluding remarks.

II. State-of-the-Art and Beyond

Zero-energy devices powered by green WPT are rapidly gaining traction as a cornerstone technology for sustainable 6G massive IoT [5]. This area, while attracting substantial interest from academia and industry, is still in its nascent stages, necessitating further research and innovation. This section reviews the current state-of-the-art, addressing knowledge gaps associated with the challenges previously outlined.

A. Theoretical Modeling and Experimental Studies

Numerous studies have used circuit and microwave theories to model WPT system behavior [6], with some incorporating computational intelligence to enhance modeling accuracy and system optimization [7]. Experimental efforts, including our prior work [8], have evaluated the effects of environmental factors on WPT performance. However, much of the research to date is limited to two-dimensional deployments with simplifying assumptions, such as perfect time synchronization, omnidirectional antennas, and sparse IoT device distribution. Our recent study has critically examined these assumptions, highlighting their limitations in real-world applications [9].

With future 6G IoT networks expected to function in three-dimensional spaces containing distributed power transmitters and dense arrays of batteryless devices, a comprehensive understanding of WPT behavior in 3D environments is essential. This will require a rigorous investigation through detailed theoretical models, experimental validation, and simulations to develop more effective scheduling strategies and secure energy transmission mechanisms.

B. Charge Scheduling of Wireless Energy Transmitters

Current charge scheduling architectures in WPT involve either centralized antenna array systems or distributed charging networks. Centralized systems leverage beamforming techniques to focus energy by manipulating signal phases and amplitudes, with some closed-loop approaches using backscatter for efficient power distribution [10]. Recent advancements include joint beam scheduling and power allocation strategies designed to maximize energy harvesting across zero-energy devices [11]. Distributed charging networks use stationary and mobile charging approaches [12]. Stationary charging optimizes transmitter deployment and scheduling to enhance efficiency while maintaining electromagnetic safety, whereas mobile charging focuses on minimizing resource use and delays, thereby maximizing network coverage and lifespan.

Anticipated 6G IoT networks will likely operate in hybrid environments, requiring a coordinated, distributed WPT network capable of managing multiple power sources to charge numerous IoT devices on demand. This network must dynamically adapt to changes in application requirements, network topology, and power availability. However, research into self-adaptive scheduling for networked WPT within 6G zero-energy environments remains limited. Thus, developing advanced algorithms and protocols for efficient collaboration among wireless power transmitters will be crucial to achieving optimal power distribution.

C. Malicious Energy Attacks and Defense Strategies

While securing wireless data communication has been a primary research focus, WPT system security has received comparatively little attention. Malicious energy attacks, often leveraging reinforcement learning, have emerged as a critical threat, allowing attackers to manipulate routing paths and selectively target energy-harvesting devices at the network layer [13]. Additionally, newer attack types have been identified that can lead to denial of service, livelock, and starvation scenarios in WPT systems [14]. For instance, livelock can trap a device in repetitive operations without progress, while starvation prevents task execution due to incomplete charging in multi-capacitor architectures.

Advances in deep learning techniques offer promising avenues for detecting such malicious energy attacks [15]. However, research specifically focused on countering energy attacks targeting zero-energy devices is limited, and robust defense mechanisms remain scarce. Addressing these security challenges is crucial to ensure the safe and reliable operation of the 6G zero-energy Internet of Batteryless Things. Moreover, the absence of specific ITU/IEC/ISO/SAE standards for energy attacks in WPT highlights the urgent need for standardized cybersecurity protocols and further research to safeguard against these emerging threats.

III. Future Vision of Autonomous Networked Wireless Power Transfer

This section presents insights from a bibliometric analysis on the scientific evolution of wireless power transfer for the zero-energy Internet of Batteryless Things over the past decade. Building on these findings, we propose a versatile wireless powering infrastructure for the 6G era.

This article has been accepted for publication in IEEE Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MWC.2025.3600024

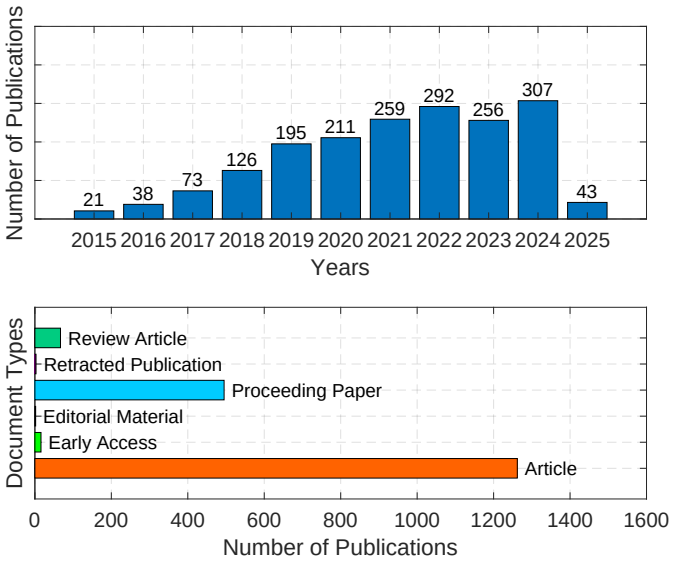
A. Bibliometric Analysis

1) Methodology: This study employed two research methods: statistical analysis and bibliometric visualization. Statistical analysis was used to examine publication trends including temporal patterns and disciplinary distribution. Bibliometric visualization, supported by the CiteSpace software, enabled the visual analysis of geographical distribution, keyword clusters, and research timelines, offering deeper insights into the field's focus areas and developmental trajectory.

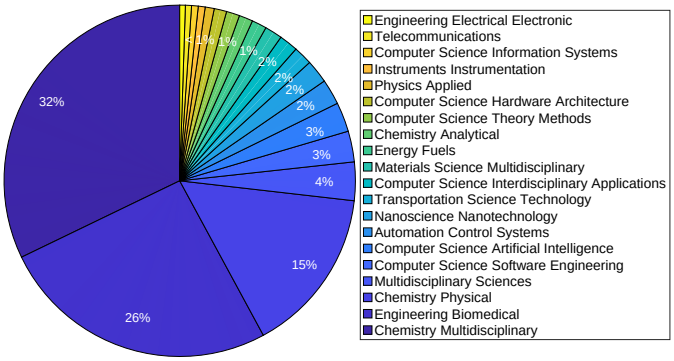
2) Data Source: The data for this analysis were sourced from the Web of Science Core Collection, covering a comprehensive range of scholarly outputs published between January 1, 2015, and March 31, 2025. To capture the breadth of relevant research, the citation index was set to "All." Search queries combined the keyword "Wireless Power Transfer" with terms such as "6G," "Zero-Energy," "Internet of Batteryless Things," "Battery-Free," and a broader term "Internet of Things." After eliminating duplicate records, the final dataset comprised 1,821 publications. This dataset serves as a robust foundation for analyzing research output, trends, and thematic developments in WPT as it relates to IoT technologies.

3) Results: As shown in Fig. 1a, the analysis indicates a clear upward trend in the number of WPT-related publications each year, reflecting the growing interest and research activity in this domain. While 2025 shows a decline in publications, this is attributable to incomplete data collection, with records extending only until March 2025. These publications span 72 disciplinary categories with the top 20 fields shown in Fig. 1b. The geographical distribution of the research in Fig. 1c further underscores the global significance of this field, with contributions from 88 countries and regions. This widespread participation highlights the international collaborative efforts in advancing WPT technologies, especially in the context of their applications for 6G zero-energy IoBT.

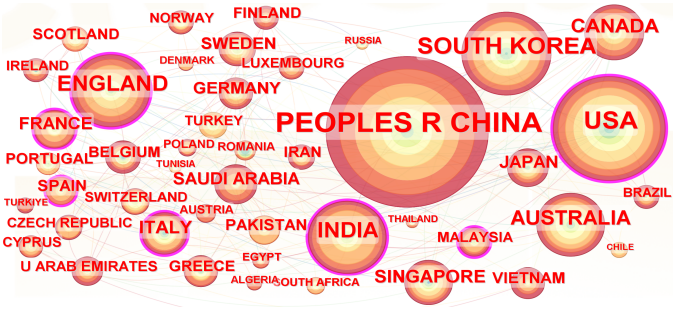
4) Research Evolution Trends: By employing keyword co-occurrence analysis, clustering, and timeline visualization using CiteSpace, we identified key trends shaping the field. The timeline of co-occurring keywords in Fig. 2 illustrates the chronological progression of research, revealing the development of various themes and advancements over the past decade. This period witnessed a broadening focus from foundational IoT energy management topics to sophisticated integrations with artificial intelligence and adaptive technologies. Notably, energy harvesting has been a key area of advancement, progressing from sensor networks to next-generation applications like cooperative NOMA. Mobile Edge Computing (MEC) has similarly gained traction, moving from architectural improvements to the incorporation of localization and advanced electronics for enhanced scalability. The integration of Intelligent Reflecting Surfaces (IRS) emerged as a pivotal trend, enhancing both signal processing and energy efficiency in WPT. Additionally, research into UAV-assisted SWIPT (Simultaneous Wireless Information and Power Transfer) has accelerated, with significant strides made toward UAV trajectory optimization and applications within smart cities and mobile edge networks.



(a) The trend of publications



(b) Discipline distribution



(c) Geographical distribution

Fig. 1. Statistical analysis and bibliometric visualization results on wireless power transfer for the Internet of Things from 2015 to 2025.

B. Autonomous Networked Wireless Power Transfer

Building on the identified trends, we propose an innovative paradigm called Autonomous Networked Wireless Power Transfer (AutoNetWPT) as shown in Fig. 3. This concept is designed to address the demands of the 6G era, providing a robust, adaptable wireless powering infrastructure for the zero-energy Internet of Batteryless Things. AutoNetWPT envisions a fully autonomous, self-regulating network that dynamically optimizes energy transfer to meet the needs of connected devices in real time. This section explores the core components of this vision and the transformative potential they offer.

This article has been accepted for publication in IEEE Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MWC.2025.3600024

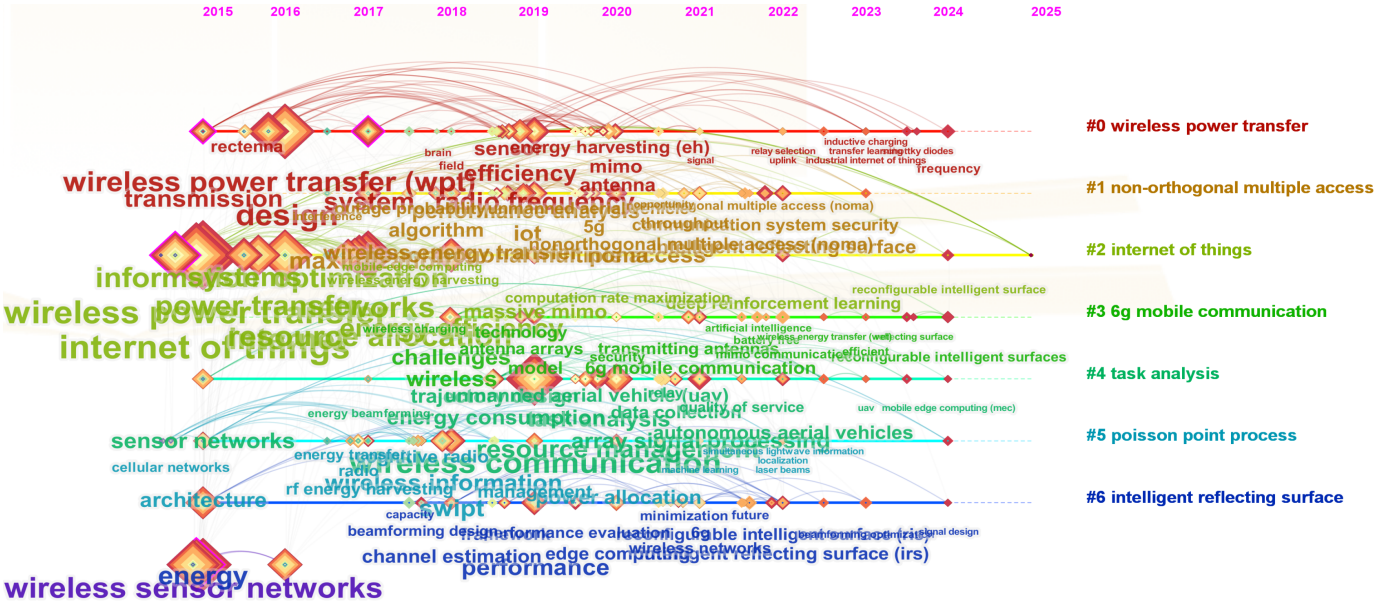


Fig. 2. Timeline of research progression and key developments in wireless power transfer for the Internet of Things from 2015 to 2025.

1) Distributed Charging Networks: At the heart of AutoNetWPT is the notion of distributed charging networks. These networks consist of multiple decentralized wireless power transmitters that collaborate to deliver energy where it is needed most. This distributed architecture enhances both coverage and efficiency, particularly in dense IoT environments, where device energy needs can vary widely and dynamically. By intelligently allocating power across different regions and devices, the system ensures that energy delivery is seamless and efficient, reducing wastage and maximizing the operational lifespan of devices. This capability is especially crucial for batteryless devices, which rely entirely on external power sources for their operation. The flexibility and adaptability of distributed charging networks allow them to meet the varying energy demands of these devices, ensuring uninterrupted operation even in scenarios with high power consumption.

2) Green Energy Integration: Sustainability is a key driver of future wireless power transfer systems. AutoNetWPT incorporates renewable energy sources, such as solar, wind, and hydropower, into its infrastructure to create an environmentally friendly and sustainable network. By leveraging these green energy sources, AutoNetWPT not only minimizes the carbon footprint associated with wireless powering but also supports global sustainability goals. This approach ensures that the growing demand for IoT devices and connected systems does not come at the cost of environmental degradation. Furthermore, renewable energy sources can be distributed across the network to ensure stable power availability. These green energy hubs can act as both energy providers and backup power sources, contributing to the overall resilience of the system. In the long run, this integration helps mitigate concerns around pollution and resource depletion, making AutoNetWPT a viable solution for a sustainable IoBT ecosystem.

3) Mobile Edge Computing: Another critical component of AutoNetWPT is MEC. It brings computational power closer

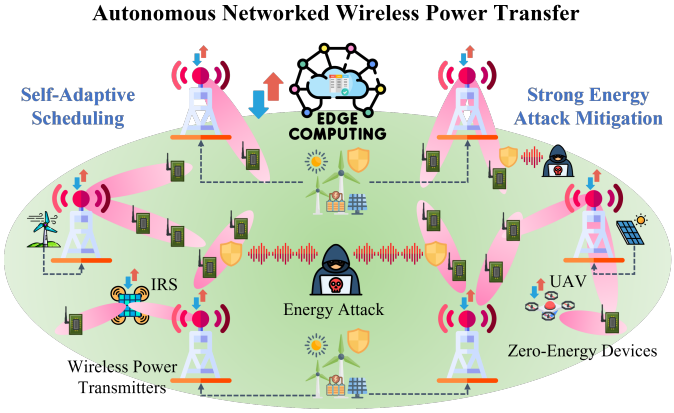


Fig. 3. Vision of autonomous networked wireless power transfer for 6G zero-energy Internet of Batteryless Things.

to the edge of the network, allowing data processing to happen near the source of data generation. In the context of AutoNetWPT, MEC plays a crucial role in optimizing energy distribution, as it enables real-time analysis of device power needs and network conditions. This allows the network to adapt energy delivery dynamically, ensuring that devices receive the precise amount of power they require without unnecessary delays or losses. By reducing latency and minimizing the need for centralized cloud processing, MEC enhances the overall efficiency of the network. Additionally, the proximity of computation to power distribution points reduces the energy required for data transmission, further improving the network's sustainability. This is particularly relevant for applications requiring real-time decision-making, such as autonomous systems and smart cities.

4) Intelligent Reflecting Surfaces: The inclusion of IRS is a groundbreaking feature in AutoNetWPT. IRS technology manipulates electromagnetic waves to steer energy precisely

toward the devices that need it. By intelligently directing power beams, IRS significantly improves the efficiency and accuracy of wireless power transfer, especially in complex environments with many obstacles or signal interference. This ability to adaptively reconfigure the propagation environment ensures that power reaches even hard-to-reach devices, reducing energy loss and improving overall system reliability. In addition to improving energy transfer, IRS also enhances the security of the system. By controlling the directionality of power beams, the system can prevent energy leakage and minimize the risk of interference or unauthorized energy use. This technology enables a more robust, interference-free energy distribution network that can meet the demands of diverse and dynamic IoT deployments.

5) UAV-Assisted SWIPT: Unmanned aerial vehicles are an essential enabler of the AutoNetWPT ecosystem, particularly in remote or hard-to-access locations. By integrating UAVs with SWIPT technology, AutoNetWPT extends its coverage and flexibility. UAVs can deliver power to mobile devices in areas without access to fixed power sources, making them ideal for applications such as disaster recovery, environmental monitoring, and smart agriculture. With UAV-assisted SWIPT, power delivery becomes highly flexible and adaptable. UAVs can dynamically adjust their flight paths and power transmission parameters based on real-time network conditions, ensuring optimal energy delivery to devices in motion or located in geographically challenging environments. This capability significantly enhances the scalability of the system, enabling energy transfer to areas that would otherwise be unreachable.

6) Self-Adaptive Scheduling and Energy Security: One of the key innovations in AutoNetWPT is its ability to perform self-adaptive scheduling. This feature allows the network to autonomously coordinate the activities of its wireless power transmitters, ensuring that power is delivered exactly when and where it is needed. By continuously monitoring network conditions and device power levels, the system can optimize charging schedules in real time. This self-adaptive capability ensures efficient energy use, reduces downtime for devices, and improves overall system performance. In addition to adaptive scheduling, AutoNetWPT incorporates strong energy security measures. As the networked WPT system becomes more autonomous and widespread, the threat of malicious energy attacks grows. To counter this, AutoNetWPT integrates robust defense mechanisms to detect and mitigate such threats. These security measures include real-time monitoring of energy flows, anomaly detection algorithms, and automated responses to prevent energy hijacking or disruption. By safeguarding the energy transfer process, AutoNetWPT ensures the integrity and reliability of the IoBT ecosystem.

7) Envisioning the Future of Wireless Power Transfer: AutoNetWPT aligns with the current trajectory of WPT research while also anticipating the future needs of a sustainable, energy-efficient 6G IoT ecosystem. Its integration of distributed charging networks, green energy, MEC, IRS, UAV-assisted SWIPT, and self-adaptive scheduling offers a comprehensive solution to the challenges facing next-generation WPT systems. By facilitating zero-energy operations and enabling continuous connectivity for batteryless devices, AutoNetWPT paves the way for a future where the IoBT thrives on intelligent, sustainable, and secure energy solutions.

TABLE I
A SUMMARY OF EXPERIMENT DEVICES AND KEY PARAMETERS.

Device	Model	Frequency	Gain	Radiation Pattern
Transmitter 1	TX91501B	915 MHz	8 dBi	H: 60° V: 60°
Transmitter 2	TX91503	915 MHz	6 dBi	H: 70° V: 130°
Rx Antenna 1	PA-915-01	915 MHz	6.1 dBi	H: 122° V: 68°
Rx Antenna 2	DA-915-01	915 MHz	1 dBi	Omni-directional
Sensor Board	P2110-EVB	915 MHz	-	-

IV. RESEARCH OPPORTUNITIES

In this section, we explore the future research directions within the AutoNetWPT paradigm by addressing the three key challenges discussed in Section II. The key experimental devices and their parameters are summarized in Table I.

A. WPT in Three-Dimensional (3D) Complex Environments

A significant research challenge lies in understanding and optimizing WPT performance in complex 3D environments. Unlike two-dimensional scenarios, 3D WPT systems must contend with additional spatial variables and dynamic factors that influence energy delivery efficiency. For instance, spatial misalignment between transmitters and receivers can drastically reduce received power due to the directionality of radiative energy beams. The presence of obstacles, reflections, and multipath fading further complicates power propagation, especially in indoor or urban settings. Moreover, the mobility of devices, such as UAVs or wearable IoT nodes, introduces time-varying spatial relationships that require real-time power adjustment and beam steering.

In addition, non-uniform energy field distribution across 3D space poses additional challenges in ensuring fair and efficient energy coverage, necessitating intelligent scheduling and coordination mechanisms. Finally, interference and electromagnetic coupling between multiple transmitters or overlapping charging zones can degrade system performance, calling for advanced control strategies and interference mitigation techniques. Addressing these challenges is crucial for building scalable and reliable WPT infrastructures to support IoBT.

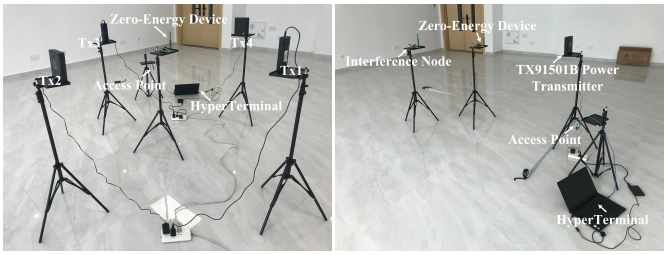
B. Modeling the Behaviors of Distributed Charging Networks

A comprehensive understanding of distributed WPT is essential for developing efficient scheduling and security mechanisms within the AutoNetWPT framework. To achieve this, detailed modeling, theoretical analysis, simulations, and experimental validation are needed. These approaches will shed light on the dynamic interactions that occur within three-dimensional spaces where distributed power transmitters and ultra-dense zero-energy IoT devices coexist. Advanced modeling should simulate both spatial and temporal energy distribution dynamics, accounting for critical factors such as transmitter placement, antenna directionality, concurrent power transfer, and fluctuating device densities. The foundation for these

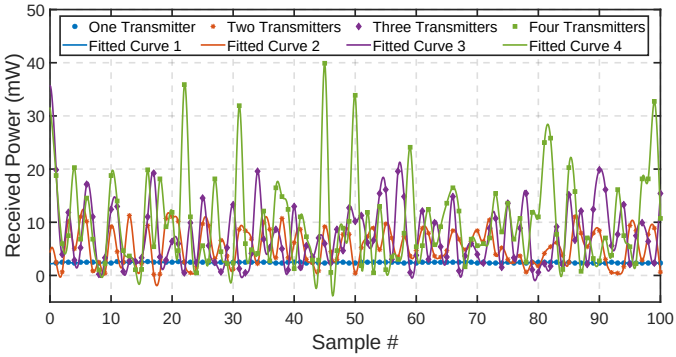
This article has been accepted for publication in IEEE Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MWC.2025.3600024

models will draw on antenna theory, wave interference theory, and radio wave propagation principles. Key assumptions about realistic antenna behavior and dense device distributions must be iteratively refined through experimental data. Challenges such as interference between transmitters, dynamic changes in device locations, and varying energy harvesting efficiencies must be rigorously addressed through theoretical analysis and high-fidelity simulations. Experimental validations will play a pivotal role in ensuring that the models accurately reflect real-world behavior, providing a solid basis for optimizing power distribution across distributed charging networks.

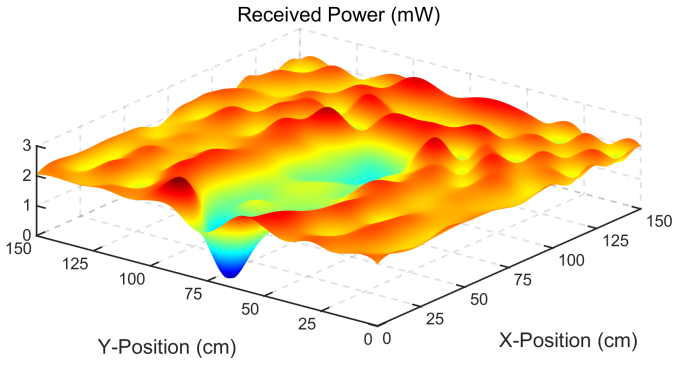
Preliminary experimental scenarios and results are depicted in Fig. 4. In the concurrent transmitting scenario (Fig. 4a and 4c), phase alignment among transmitters plays a critical role in determining charging performance. When the transmitters are synchronized in phase, the received power increases proportionally to the square of the combined electric field amplitude, yielding power gains of approximately 4×, 9×, and 16× for setups with two, three, and four transmitters, respectively, compared to a single-transmitter baseline. In contrast, out-of-phase transmissions can result in destructive interference, leading to significant power degradation, in extreme cases, reducing the received power to nearly 0 mW. In the concurrent receiving case (Fig. 4b and 4d), introducing a neighboring IoT device along the main charging path led to significant signal degradation, with the received power dropping to 0 mW in the worst case due to signal absorption and blockage. In other positions, the interfering node caused alternating constructive and destructive interference, producing power fluctuations which consist with wave interference theory and Fresnel zone effects. The observed maximum value increased from 1.57 mW to 2.88 mW, reflecting a 83% improvement due to constructive interference.



(a) Concurrent transmitting (b) Concurrent receiving



(c) Results of concurrent transmitting



(d) Results of concurrent receiving

Fig. 4. Experimental study of distributed charging networks. (a) Multiple wireless power transmitters charge a zero-energy device simultaneously. Transmitters Tx1 and Tx3 are Powercast TX91503 PowerSpot RF wireless power transmitters, while Tx2 and Tx4 are Powercast TX91501B-3W RF wireless power transmitters. The zero-energy device is equipped with a dipole antenna and a Powercast P2110-EVB evaluation board. A WSN-AP-01 access point is connected to a laptop to display the received signal strength indicator (RSSI) using HyperTerminal-5. (b) Two zero-energy devices are charged concurrently. One device is stationary at coordinates (100, 75) cm, while the other, acting as an interference node, is gradually repositioned both vertically and horizontally from (0, 0) to (150, 150) cm. Each device consists of a dipole antenna, a Powercast P2110-EVB evaluation board, and a WSN-EVAL-01 wireless sensor board. The power transmitter used in this setup is the TX91501B. (c) and (d) are measurement results in the experimental scenarios.

C. Self-Adaptive Wireless Powering Scheduling

Developing dynamic algorithms and protocols that enable power transmitters to collaborate efficiently is crucial for optimizing on-demand power distribution within the AutoNetWPT system. Insights from WPT modeling, combined with communication and optimization theories, form a robust foundation for achieving this goal. Communication theory, in particular, plays a pivotal role in networked WPT in the following ways:

1) Signal Encoding and Modulation: It helps design efficient encoding and modulation schemes to maximize power transfer efficiency while minimizing interference.

2) Channel Estimation and Equalization: Accurate modeling and understanding of the wireless channel are essential. Communication theory offers methods for estimating and equalizing channels, which improves power transfer accuracy and reliability in dynamic environments.

3) Interference Management: Strategies derived from communication theory are useful in managing and mitigating interference among multiple WPT systems.

4) Network Protocols and Optimization: Communication protocols, rooted in network theory, can coordinate power transfer among multiple nodes, optimizing system performance and energy distribution. These protocols can handle tasks such as scheduling and load balancing.

5) Error Correction and Reliability: Techniques like error correction codes enhance power transfer reliability by correcting any errors in transmitted power signals, ensuring stable and efficient energy delivery.

6) Resource Allocation: Communication theory provides tools for resource allocation, ensuring optimal distribution of power resources among devices in a networked WPT, thereby maximizing overall system performance.

Optimization theory, in turn, guides the formulation of

objective functions and constraints, such as minimizing power consumption and addressing bandwidth limitations. Emerging technologies like edge computing and intelligent reflecting surfaces can further improve adaptability and efficiency. Real-time data collected through edge computing facilitates rapid decision-making, while IRS can manage signal paths and mitigate interference in dynamic environments. Extensive simulations and experimental evaluations will be essential to fine-tune the integration and effectiveness of these technologies.

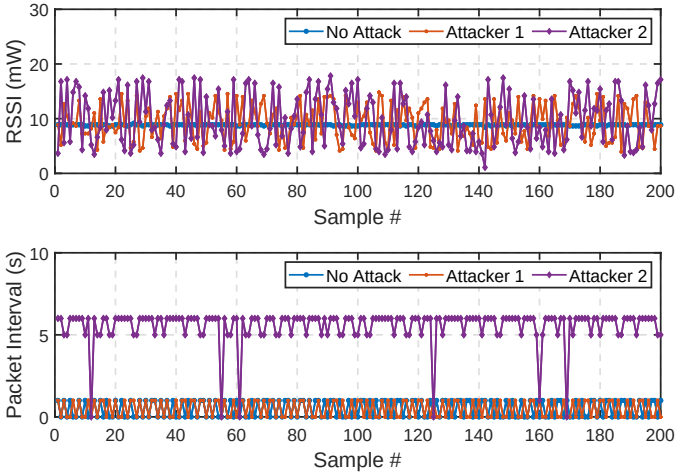
D. Strong Energy Attack Mitigation

Malicious energy attacks pose a significant threat to the stability of AutoNetWPT systems. Fig. 5a illustrates the experimental scenarios involving malicious energy attacks. Although the power transmitter remains robust against Brazilian lucky wood, as indicated by the green status LED, placing a patch antenna in close proximity as an obstruction can quickly halt power transmission, as indicated by the blinking red LED. Furthermore, a malicious energy attacker can target either the power transmitter (Attacker 1) or the zero-energy device (Attacker 2). The results related to the received power (Received Signal Strength Indicator, RSSI) and the time differential between received packets are displayed in Fig. 5b. It can be observed that Attacker 1 significantly affects the instantaneous received power without being detected through packet intervals. In addition to impacting RSSI, Attacker 2 can cause the zero-energy device to enter a sub-active state, increasing the packet interval from 1 second to 5 or 6 seconds. Additionally, we monitored the zero-energy device's status by measuring its storage capacitor voltage (yellow line), DC output voltage (green line), and shutdown signal (blue line), as shown in Fig. 5c. These results demonstrate that Attacker 2 can maliciously discharge the storage capacitor, leading to instability in the zero-energy device.

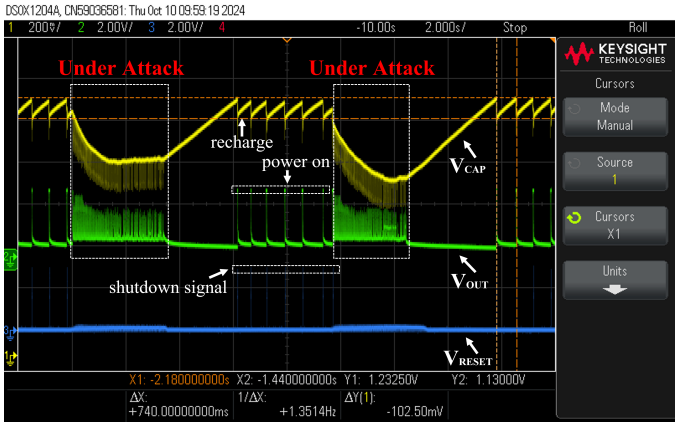
To mitigate the risks posed by malicious energy attacks, it is essential to develop robust detection and defense mechanisms tailored to the energy and computational constraints of zero-energy IoT devices. One promising approach is energy fingerprinting, which involves profiling normal energy harvesting and consumption patterns to detect anomalies and malicious activities. However, the practical feasibility of implementing energy fingerprinting on resource-constrained devices requires careful consideration of computational overhead, as the added processing burden could negatively impact system performance. In addition, there are challenges in terms of real-time processing and the need for data storage, which could strain the limited resources of IoT devices. Therefore, it is crucial to evaluate the trade-offs between security effectiveness and resource consumption, ensuring that defense mechanisms like energy fingerprinting do not undermine the core functionality of the devices. Future work should focus on developing lightweight algorithms that can balance these trade-offs, supported by comprehensive simulations and real-world testing to better understand the challenges and limitations of such systems in practical environments.

Techniques such as channel hopping, commonly employed in reliable wireless communication, can be adapted to wireless power transfer. By frequently changing operating frequencies, the system can avoid malicious interference. Furthermore, technologies like IRS and concurrent energy transmission, leveraging both destructive and constructive interference, could be explored to actively defend against energy attacks. By using IRS to control the propagation environment, the system can prevent attackers from exploiting predictable signal paths, while constructive interference could enhance the robustness of power delivery. Comprehensive simulations and real-world testing will be necessary to refine these defenses and ensure their effectiveness against evolving attack strategies.

(a) Experimental scenarios of malicious energy attacks



(b) Results of received signal strength indicator (RSSI) and packet intervals



(c) Voltage status observed by a Keysight DSOX1204A oscilloscope

Fig. 5. Experimental study of malicious energy attacks. The zero-energy device is equipped with a patch antenna, a Powercast P2110-EVB evaluation board, and a WSN-EVAL-01 wireless sensor board. Three Powercast TX91501B units are employed, with one serving as the primary power transmitter and the other two as attackers.

V. Conclusion

This article has provided a thorough exploration of WPT within the emerging 6G zero-energy massive Internet of Batteryless Things. We began by reviewing the current state of WPT technology, addressing theoretical modeling, experimental studies, wireless energy transmitter charge scheduling, and the challenges posed by malicious energy attacks, alongside strategies for their mitigation. Key limitations and research gaps were identified in these areas. To complement this, a bibliometric analysis was conducted, offering insights into publication trends, disciplinary and geographical distributions, and the development of key research clusters. Building on this foundation, we introduced the AutoNetWPT paradigm, which integrates advancements such as distributed charging networks, green energy solutions, mobile edge computing, intelligent reflecting surfaces, and UAV-assisted simultaneous wireless information and power transfer. Finally, we outlined future research directions with experimental insights.

Acknowledgment

The authors would like to express their sincere gratitude to anonymous reviewers, Prof. Sarder Abedin Fakhrul, Prof. Aamir Mahmood, and Katrin Lindbäck of Mid Sweden University for their valuable suggestions. The work by Ye Liu is supported by the Marie Skłodowska-Curie Actions (MSCA) Postdoctoral Fellowship under Grant No. 101201988.

References

[1] M. Matinmikko-Blue, S. Yrjölä, P. Ahokangas, K. Ojutkangas, and E. Rossi, "6G and the UN SDGs: Where is the Connection?" *Wireless Personal Communications*, vol. 121, pp. 1339–1360, 2021.

[2] S. Ahmed, B. Islam, K. S. Yildirim, M. Zimmerling, P. Pawełczak, M. H. Alizai, B. Lucia, L. Mottola, J. Sorber, and J. Hester, "The Internet of Batteryless Things," *Communications of the ACM*, vol. 67, no. 3, p. 64–73, feb 2024.

[3] S. Naser, L. Bariah, S. Muhaidat, and E. Basar, "Zero-Energy Devices Empowered 6G Networks: Opportunities, Key Technologies, and Challenges," *IEEE Internet of Things Magazine*, vol. 6, no. 3, pp. 44–50, 2023.

[4] Y. Liu, D. Li, B. Du, L. Shu, and G. Han, "Rethinking Sustainable Sensing in Agricultural Internet of Things: From Power Supply Perspective," *IEEE Wireless Communications*, vol. 29, no. 4, pp. 102–109, 2022.

[5] O. L. A. López, H. Alves, R. D. Souza, S. Montejo-Sánchez, E. M. G. Fernández, and M. Latva-Aho, "Massive Wireless Energy Transfer: Enabling Sustainable IoT Toward 6G Era," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8816–8835, 2021.

[6] B. Clerckx, R. Zhang, R. Schober, D. W. K. Ng, D. I. Kim, and H. V. Poor, "Fundamentals of Wireless Information and Power Transfer: From RF Energy Harvester Models to Signal and System Designs," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 4–33, 2019.

[7] D. Sarkar, T. Khan, F. A. Talukdar, and S. R. Rengarajan, "Computational Intelligence for Modeling and Optimization of RFEH and WPT Systems: A Comprehensive Survey," *IEEE Microwave Magazine*, vol. 24, no. 9, pp. 46–60, 2023.

[8] Y. Liu, D. Li, H. Dai, C. Li, and R. Zhang, "Understanding the Impact of Environmental Conditions on Zero-Power Internet of Things: An Experimental Evaluation," *IEEE Wireless Communications*, vol. 30, no. 6, pp. 152–159, 2023.

[9] Y. Liu, D. Li, H. Dai, X. Ma, and C. A. Boano, "Understanding Concurrent Radiative Wireless Power Transfer in the IoT: Out of Myth, into Reality," *IEEE Wireless Communications*, vol. 31, no. 3, pp. 398–405, 2024.

[10] Y. Tanaka, H. Hamase, K. Kanai, R. Hasaba, H. Sato, Y. Koyanagi, T. Ikeda, H. Tani, M. Gokan, S. Kajiwara, and N. Shinohara, "Simulation and Implementation of Distributed Microwave Wireless Power Transfer System," *IEEE Transactions on Microwave Theory and Techniques*, vol. 71, no. 1, pp. 102–111, 2023.

[11] Y. Zhang and C. You, "SWIPT in Mixed Near- and Far-Field Channels: Joint Beam Scheduling and Power Allocation," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 6, pp. 1583–1597, 2024.

[12] Z. Cai, Q. Chen, T. Shi, T. Zhu, K. Chen, and Y. Li, "Battery-Free Wireless Sensor Networks: A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 5543–5570, 2023.

[13] L. Li, Y. Luo, J. Yang, and L. Pu, "Reinforcement Learning Enabled Intelligent Energy Attack in Green IoT Networks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 644–658, 2022.

[14] L. Mottola, A. Hameed, and T. Voigt, "Energy Attacks in the Batteryless Internet of Things: Directions for the Future," in *Proceedings of the 17th European Workshop on Systems Security*, ser. EuroSec '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 29–36.

[15] X. Zhang, L. Li, L. Pu, J. Yang, Z. Wang, R. Fu, and Z. Jiang, "Deep Learning-based Malicious Energy Attack Detection in Sustainable IoT Network," in *2024 International Conference on Computing, Networking and Communications (ICNC)*, 2024, pp. 417–422.

Ye Liu (yeliu@njau.edu.cn) received the M.S. and Ph.D. degrees in electronic science and engineering from Southeast University, Nanjing, China, in 2013 and 2018, respectively.,He was a Visiting Scholar with Montana State University, Bozeman, MT, USA, from 2014 to 2015. He was a visiting Ph.D. student with the Networked Embedded Systems Group, RISE Swedish Institute of Computer Science, Kista, Sweden, from 2017 to 2018. He was a Macau Young Scholar with the Macau University of Science and Technology, Macau, SAR, China, from 2022 to 2024. He is currently an Associate Research Professor with Nanjing Agricultural University, China.

Mikael Gidlund (mikael.gidlund@miun.se) received the Licentiate degree from KTH, Stockholm, in 2004, and the Ph.D. in electrical engineering from Mid Sweden University in 2005. He held research and leadership roles at Acreo AB, Nera Networks AS, and ABB Corporate Research between 2006 and 2015. Since 2015, he has been a Professor of Computer Engineering at Mid Sweden University. He holds over 20 patents in wireless communication. His research interests include wireless communication, sensor networks, MAC protocols, and security.

Honggang Wang (honggang.wang@yu.edu) is the founding Chair and Professor of the Department of Graduate Computer Science and Engineering, Katz School of Science and Health, Yeshiva University in New York City. He is an alumnus of NAE Frontiers of Engineering program. He is an IEEE distinguished lecturer and a Fellow of IEEE and AAIA. He has served as the Editor in Chief (EiC) for IEEE Internet of Things Journal during 2020–2022. He was the past Chair (2018–2020) of IEEE Multimedia Communications Technical Committee and the past IEEE eHealth Technical Committee Chair (2020–2021).

Gerhard Petrus Hancke (gp.hancke@cityu.edu.hk) Received B.Eng. and M.Eng. degrees in computer engineering from the University of Pretoria, South Africa, in 2002 and 2003, respectively, and the Ph.D. degree in computer science from the University of Cambridge, U.K., in 2009. He is currently a Professor with the City University of Hong Kong, Hong Kong. His research interests include system security, reliable communication, and distributed sensing for the industrial Internet of Things. He is a Member of Industrial Electronics Society and a Fellow of IEEE.