




Please cite the Published Version

Pauu, Kulaea Taueveeve , Wu, Jun  and Bashir, Ali Kashif  (2025) TeraPRI: Homomorphic Terahertz-Empowered Joint Wireless Power and Information Transfer with Privacy-Preserving for 6G-Autonomous Vehicles. IEEE Transactions on Consumer Electronics. pp. 1-14. ISSN 1558-4127

DOI: <https://doi.org/10.1109/tce.2025.3552624>

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Version: Accepted Version

Downloaded from: <https://e-space.mmu.ac.uk/639329/>

Usage rights:  [Creative Commons: Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

Additional Information: This is an accepted manuscript of an article which first appeared in IEEE Transactions on Consumer Electronics

Enquiries:

If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

TeraPRI: Homomorphic Terahertz-Empowered Joint Wireless Power and Information Transfer with Privacy-Preserving for 6G-Autonomous Vehicles

Kulaea Taveeveve Pauu, *Graduate Student Member, IEEE*, Jun Wu, *Senior Member, IEEE*, Ali Kashif Bashir *Senior Member, IEEE*

Abstract—In sixth-generation networks, Terahertz technology enables high-speed, low-latency communication capabilities, while Mobile Edge Computing (MEC) enhances remote computation, leveraging Autonomous Vehicles capable of providing computational resources and energy support, particularly in challenging environments where conventional terrestrial infrastructure is absent. However, challenges remain, particularly with the limited energy of end-user nodes and the constrained data capabilities of MEC nodes in THz networks, which require substantial energy to transmit large volumes of data. Efficient coordination of energy supply and information transfer is essential. Additionally, such networks can face signal interference and leakage of privacy-sensitive information, complicating data security and reliable communication. To address these challenges, we propose TeraPRI, a novel framework for homomorphic THz-empowered joint wireless power and information transfer with privacy preservation for 6G Autonomous Vehicles. First, we introduce a dual-mode adaptive resource allocation method that alternates between "harvest-and-then-transmit-mode" (HaT-mode) and "transmit-and-then-harvest-mode" (TaH-mode) based on end-user node demands. Second, we design a selective CKKS homomorphic encryption technique with lightweight thresholding for frequency allocation, enabling the MEC to securely assign unique THz sub-channels to end-user nodes in the low-THz band (0.1–1.0 THz) while enhancing communication security through randomized frequency hopping. Extensive simulations show that TeraPRI significantly improves power transfer, information transfer rates, and privacy over existing methods.

Index Terms—6G networks, terahertz technology, mobile edge computing, wireless power and information transfer, autonomous vehicles, privacy-preserving

I. INTRODUCTION

IN recent years, the rise in new age Internet-of-Things (IoT) consumer electronics, such as wearable gadgets, monitoring sensors, wireless terminals, smart devices, etc. [1]–[4], referred to as end-user nodes, has marked the beginning of a new era of transformation for the IoT. By 2030, it is estimated that nearly 500 billion IoT devices will be in operation, playing a vital role in wireless data collection for various data-intensive applications, including weather monitoring, road

monitoring for public safety, and emergency detection in different scenarios [5]. These end-user nodes will be connected intelligently in a massive network to collect and share data on locations, tracking, delivery routes, etc. [5], [6]. They will amass significant amounts of data from multiple sources, which are then transmitted for processing. Since these end-user nodes gather large volumes of data and rely on limited battery power, they often deplete their energy quickly [7], limiting their ability to upload data efficiently. Additionally, in such a network, the data upload process can increase network traffic and lead to prolonged propagation delays [8]. Therefore, addressing the energy needs of these battery-constrained end-user nodes and efficiently managing data uploads is crucial to maintaining the high-speed data transmission and low latency required in massive IoT networks.

In 6G networks, the THz spectrum which operates within the frequency range of 0.1 to 10 THz [9], offers a vast array of resources that can address the requirements of high-speed data transmission and low-latency communication capabilities. The abundance of available bandwidth within the THz spectrum enables the efficient handling of large volumes of data, ensuring that end-user nodes receive timely and responsive services [10]–[12]. However, THz signals are highly sensitive to environmental factors such as atmospheric absorption and signal attenuation, making traditional edge computing unsuitable as it restricts wireless communication ranges and increases vulnerability to damage, thereby making it challenging to deliver services to end-user nodes, especially in remote areas or regions affected by natural disasters [13]–[15]. Meanwhile, MEC leveraging 6G-autonomous vehicles (AVs) encompasses a range of platforms capable of independent operation, including ground-based systems such as self-driving cars and aerial platforms like unmanned aerial vehicles (UAVs) [16]–[18]. This paper takes UAVs as an example of AVs, highlighting their role in enabling efficient short-range wireless connections by bringing computation and transmission services closer to end-user nodes at the network's edge [19]–[21]. UAVs provide unique advantages such as rapid deployment, wide-area coverage, and accessibility in remote or disaster-affected regions, making them a suitable MEC platform for this work. This approach also enhances THz capabilities by establishing short-distance line-of-sight (LoS) links [22]–[24]. The proximity of the MEC nodes to end-user nodes facilitates efficient task distribution, reduces latency, and improves the speed of data transmission and response times

This work was supported in part by the JSPS KAKENHI under Grants 23K11072, and in part by the Japan International Cooperation Agency (JICA) Long-term Scholarship under the SDGs Global Leadership Program. (*Corresponding author: Jun Wu.*)

Kulaea Taveeveve Pauu and Jun Wu are with the Graduate School of Information, Production and Systems, Waseda University, Japan. (email: junwu@aoni.waseda.jp).

Ali Kashif Bashir is with the Department of Computing and Mathematics, Manchester Metropolitan University, UK. (e-mail: dr.alikashif.b@ieee.org).

[25], [26]. The integration of MEC with THz spectrum in 6G networks offers significant potential for achieving high-speed, low-latency communication. By positioning computation closer to end-user nodes, MEC nodes can improve the efficiency of THz transmissions. Despite its potential, this integration faces challenges:

First, end-user nodes encounter limited energy resources, as transmitting large volumes of data in the THz spectrum requires considerably higher power. MEC nodes have limited data handling capabilities, which further reduces their efficiency in managing and transmitting large volumes of data. Therefore, to efficiently manage these demands, effective coordination of wireless power transfer and information transfer is essential to address the energy limitations of end-user nodes and the constrained capabilities of MEC nodes. While significant progress has been made, existing studies—ranging from RF-based solutions to advanced THz spectrum methods—exhibit key limitations in the the coordination of wireless power and information transfer [27]–[31]. For instance, Ju *et al.* [27] proposed a wireless-powered communication network (WPCN) operating in the RF spectrum. Their work introduced a harvest-then-transmit protocol, where users first harvest energy during the downlink (DL) phase and then transmit information in the uplink (UL) using time-division multiple access (TDMA). While foundational, this approach is static and does not adapt to real-time energy demands, limiting its efficiency. To leverage the potential of the THz spectrum, recent works have explored joint power and information transfer methods. Rong *et al.* [28] proposed a SWIPT scheme for nanonetworks operating in the THz band. Their work used an amplify-and-forward (AF) relaying mechanism, where the relay node harvested energy from the received signal and forwarded information to the destination. However, this approach lacks dynamic adaptability to real-time user energy states. Hanif *et al.* [29] introduced Simultaneous Terahertz Imaging with Information and Power Transfer (STIIPT), integrating energy transfer, data communication, and radar imaging. While leveraging advancements in THz semiconductor technologies and antenna design, their system does not address dynamic resource allocation at the individual node level. Pan *et al.* [30] developed a reconfigurable intelligent surface (RIS)-aided STIIPT system to optimize power transfer and data rates for energy users (EUs) and information users (IUs). Although effective in improving system-wide performance, their approach lacks adaptability to individual user conditions, focusing instead on global optimization. Jeong *et al.* [31] investigated a UAV-enabled SWIPT system, where UAVs optimize power allocation, power-splitting ratios, and flight trajectories to deliver energy and information to multiple nodes. However, the reliance on fixed power-splitting ratios limits the system’s ability to adapt to varying energy demands of individual users.

Second, coordinating wireless power and information transfer often leads to signal interference and privacy-sensitive information leakage [32], complicating efforts to ensure data security and reliable communication channels. Several existing studies have addressed this challenge [33]–[38]. For instance, Lai *et al.* [33] proposed a method to enhance security in an MEC network against eavesdroppers. The method mini-

mizes the secrecy outage probability (SOP) while balancing latency and energy constraints. Azari *et al.* [34] proposed privacy-preserving aggregation for secure THz communication in emergency scenarios. Alali *et al.* [35] optimized UAV-ground communication security in sub-Terahertz bands using cooperative UAV jamming and multiple-input-multiple-output (MIMO) techniques. Zhou *et al.* [36] proposed a secure MEC system using UAVs to offload computing tasks from ground users. It addresses security challenges posed by multiple eavesdropping UAVs by implementing jamming signals and optimizing system parameters for secrecy capacity, latency, and power constraints. Jin *et al.* [37] proposed a novel physical-layer assisted secure offloading scheme for MEC to address privacy risks. It involves edge servers broadcasting jamming signals and utilizing full-duplex communication to suppress eavesdropping and self-interference. Singh *et al.* [38] emphasized robust encryption for THz communications, highlighting privacy vulnerabilities.

The aforementioned studies on both challenges have primarily focused on either coordinating wireless power and information transfer or addressing privacy preservation separately. To the best of the authors’ knowledge, at the time of writing, this paper is the first to provide a unified solution addressing both challenges. We emphasize the need for a framework that:

- Integrates wireless power transfer to extend the operational lifetime of end-user nodes and information transfer to offload collected monitoring data from end-user nodes to MEC nodes for efficient processing; and
- Ensures the privacy preservation of transmitted information while mitigating signal interference.

In this context, we propose TeraPRI, a novel framework for homomorphic THz-empowered joint wireless power and information transfer with privacy preservation, specifically designed for 6G networks where AVs serve as MEC nodes. TeraPRI enables MEC nodes to efficiently coordinate energy and data transfer, managing the high energy and data transmission demands of end-user nodes. It also addresses signal interference and privacy leakage, ensuring secure and reliable communication. The main contributions of this study can be summarized as follows:

- 1) We propose TeraPRI, a novel framework for homomorphic THz-empowered joint wireless power and information transfer with privacy preservation tailored for 6G-Autonomous Vehicles serving as MEC nodes. TeraPRI efficiently integrates energy harvesting and secure information transmission while addressing the dual challenges of energy constraints and privacy-sensitive communication.
- 2) Within the TeraPRI framework, we develop a dual-mode adaptive resource allocation method to dynamically allocate the received power in the signal for joint wireless power and information transfer. This method adapts between two modes based on real-time energy demands of the end-user nodes:
 - harvest-and-then-transmit-mode (HaT-mode): Prioritizes energy harvesting when the node’s battery level is below a predefined threshold.

- transmit-and-then-harvest-mode (TaH-mode): Allocates power for information transmission when sufficient energy is available.
- 3) We design a selective CKKS homomorphic encryption technique with lightweight thresholding for frequency allocation, enabling the MEC to securely assign unique THz sub-channels to end-user nodes in the low-THz band (0.1–1.0 THz) [39]–[41], while enhancing communication security through randomized frequency hopping.

The remaining sections of this paper are organized as follows: Section II introduces the TeraPRI Network Model, followed by Section III presenting the proposed framework solution of TeraPRI, Section IV focuses on the performance analysis of the simulation experiments, while Section V concludes the work and outlines potential future research.

II. TERAPRI NETWORK MODEL

In this section, we introduce the network model of TeraPRI illustrated in Fig. 1.

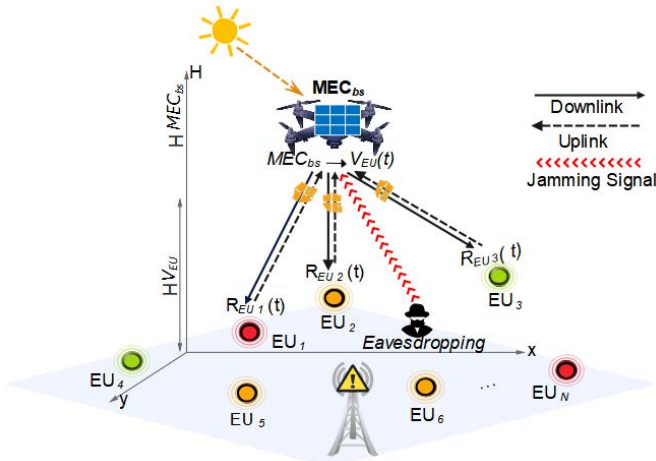


Fig. 1: Illustration of the TeraPRI network model, highlighting wireless power transfer in the downlink, wireless information transfer in the uplink, and potential jamming signals from eavesdroppers.

This paper focuses specifically on the time window during which the MEC is within communication range of the end-user nodes. We consider a set of N end-user nodes, denoted as $V_{EU} = \{EU_i \mid i \in [1 : N]\}$, which can be movable, such as those found on wearable nodes, body sensors etc. The altitude of the end-user nodes is maintained at a minimum altitude $H_{V_{EU}} \geq 0$. These nodes could potentially be situated beyond the network coverage area, and the conventional edge server may experience disruptions due to various factors, such as unforeseen disasters. Because of these possibilities, we consider MEC servers, denoted as MEC_{bs} , such as AVs, including UAVs, that are equipped with power transmitters and computation capabilities. The MEC_{bs} is capable of providing charging services to the V_{EU} , and each EU_i is equipped with a limited rechargeable battery capable of harvesting energy, as well as a THz modulator for backscatter communication.

We assume that MEC_{bs} relies on a stable solar power system for uninterrupted operation and maintains a minimum altitude $H_{MEC_{bs}} > 0$. Each EU_i in V_{EU} relies solely on received THz signals transmitted by MEC_{bs} for energy supply. The EU_i stores this energy and utilizes it to power its operational circuits. Both MEC_{bs} and V_{EU} are assumed to be equipped with GPS sensors to determine the location and a single antenna to facilitate communication.

The TeraPRI network model operates in two phases: downlink and uplink. During the downlink phase, the MEC_{bs} transmits energy to the end user nodes V_{EU} for energy harvesting. Each node $EU_i \in V_{EU}$ uses this energy to recharge its battery if its battery level is below a predefined threshold. Once the battery level of EU_i exceeds the predefined threshold, it transitions to the uplink phase, using the received signal to backscatter the modulated information back to MEC_{bs} . This decision-based mechanism ensures efficient energy use and seamless transitions between energy harvesting and information transmission. Synchronization between backscatter modulation and MEC_{bs} is achieved dynamically without explicit time-slot allocation. Each end-user node EU_i autonomously decides whether to reflect information or harvest energy based on its battery level. During the uplink phase, the MEC_{bs} detects the reflected modulated signals from active nodes $EU_i \in V_{EU}$ and processes the data accordingly. The short-range and narrow-beam characteristics of THz signals allow the MEC_{bs} to focus on individual nodes, reducing interference and ensuring reliable data reception. This configuration supports low-power, energy-efficient communication, leveraging the unique capabilities of THz frequencies and backscatter modulation to enable robust and sustainable applications.

A. THz Signal Generation and Transmission by MEC_{bs}

We assume the MEC_{bs} is equipped with a THz source capable of modulating a THz signal waveform. The signal transmitted from MEC_{bs} to a EU_i in V_{EU} at time t is a modulated carrier wave with amplitude and frequency modulation that does not carry any information. The signal is represented as a sum over k from 0 to $L - 1$, covering all chips in the signal:

$$S_{MEC_{bs}}(t) = \sum_{k=0}^{L-1} \left[A_k \times \sin(2\pi(f_{c,k} + F_{h,k})t) \times \sqrt{p_k} \times S_k(t - (k \times T_k)) \right], \quad (1)$$

where L is the total number of bits, k is an integer that represents the index of the chip in the sequence, A_k is the amplitude, $f_{c,k}$ is the carrier frequency, $F_{h,k}$ is the frequency offset in the hopping sequence, $\sqrt{p_k}$ is the amplitude scaling factor for the k -th chip, based on the power p_k in the transmitted signal, and $S_k(t - (k \times T_k))$ is the frequency modulation function. The term $t - (k \times T_k)$ shifts the function by $k \times T_k$, where T_k is the chip duration. This means that $k \times T_k$ delays the k -th chip by k times the duration of one chip.

The power of the k -th bit of the transmitted signal is given by:

$$p_k = \int_{t_k}^{t_{k+1}} |S_{\text{MEC}_{b_s}}(t)|^2 dt, \quad (2)$$

The average power for each k -th bit over its duration T_k is:

$$p_{\text{avg},k} = \frac{1}{T_k} \int_{t_k}^{t_{k+1}} |S_{\text{MEC}_{b_s}}(t)|^2 dt, \quad (3)$$

The average power for the entire signal over its total duration T_{tot} is:

$$p_{\text{avg}} = \frac{1}{T_{\text{tot}}} \int_{t_{\text{start}}}^{t_{\text{end}}} |S_{\text{MEC}_{b_s}}(t)|^2 dt, \quad (4)$$

The peak power is the maximum power among all bits:

$$p_{\text{pk}} = \max(p_k), \quad k \in [0, L-1]. \quad (5)$$

B. Propagation of the THz Signal

Following the THz signal generation and transmission from MEC_{b_s} , it propagates through the environment to the intended EU_i . Assuming a direct LoS path with minimal NLoS deviations, the time-varying channel response between MEC_{b_s} and EU_i is expressed as:

$$h_{S_{\text{MEC}_{b_s}}}(t) = \sqrt{\frac{G_{\text{tx}}G_{\text{rx}}\lambda^2}{4\pi(d_t)^2}} \times \exp\left(-j\frac{2\pi}{\lambda}d_t\right) + \Delta h(t), \quad (6)$$

Here, $-j$ denotes the imaginary unit ($\sqrt{-1}$), indicating phase shift. The term $\sqrt{\frac{G_{\text{tx}}G_{\text{rx}}\lambda^2}{4\pi(d_t)^2}}$ represents free-space path loss, accounting for antenna gains G_{tx} and G_{rx} , wavelength λ , and distance d_t . The phase shift $\exp\left(-j\frac{2\pi}{\lambda}d_t\right)$ includes amplitude and phase information. $\Delta h(t)$ represents time-varying channel fluctuations. The distance d_t is the Euclidean distance as defined in [7].

Molecular absorption loss occurs when the THz signal is attenuated due to interactions with molecules in the atmosphere. This phenomenon is quantified by Beer-Lambert Law and is expressed as:

$$L_{\text{mab}} = \exp\left(-\frac{1}{2} \sum_m \left(\frac{p_{\text{sys}}}{p_{\text{ref}}}\right) \cdot \left(\frac{P_{\text{temp}}}{T_s}\right) \cdot Q_m \cdot \delta_m(f_c) \cdot d_t\right), \quad (7)$$

where $\sum_m \left(\frac{p_{\text{sys}}}{p_{\text{ref}}}\right) \cdot \left(\frac{P_{\text{temp}}}{T_s}\right) \cdot Q_m \cdot \delta_m(f_c)$ represents the medium's absorption coefficient. Here, p_{sys} is the system pressure, $p_{\text{ref}} = 1$ atm is the reference pressure, $P_{\text{temp}} = 273.15$ K is the standard temperature, T_s denotes the system temperature measured in Kelvin (K), Q_m is the molecule density of gas m , and δ_m is the absorption cross-section of gas m [29]. Details of the derivation are in [42], and parameters are from HITRAN [43]. Besides molecular absorption loss, the transmitted THz signal in equation (1) encounters thermal noise and water vapor absorption noise in the channel [44], modeled as Gaussian distributions via the Central Limit Theorem [45], [46].

The instantaneous additive channel noise at time t is expressed as:

$$n_{\text{EU}_i}(t) \sim \mathcal{N}\left(0, k_B T_s B F_n + \frac{2k_B T_s L_{\text{mab}}(f_c)}{B}\right), \quad (8)$$

where $\sim \mathcal{N}$ indicates that $n_{\text{EU}_i}(t)$ follows a Gaussian distribution with a mean of 0. The term $k_B T_s B F_n$ represents the power spectral density of thermal noise, while $\frac{2k_B T_s L_{\text{mab}}(f_c)}{B}$ accounts for the molecular absorption noise component. Here, k_B is the Boltzmann constant (1.38×10^{-23} J/K), T_s is the system temperature, B is the bandwidth of the communication channel, and F_n is the receiver noise figure. The thermal noise originates from Johnson-Nyquist noise, while molecular absorption noise results from THz signal attenuation due to atmospheric interactions.

The noise power for a given frequency f_c at a distance can be expressed as [42]:

$$\sigma_{n,\text{EU}_i}^2 = \int_{f_c - \frac{B}{2}}^{f_c + \frac{B}{2}} (k_B \cdot T_s) \cdot \eta(f_c, t)^2 df, \quad (9)$$

The system's noise temperature is primarily influenced by the molecular absorption noise temperature, as derived from (8), and this influence is particularly significant in environments where other electronic noise sources are minimal. Therefore, in scenarios where the receiver lacks specific elements such as amplifiers and frequency converters, the molecular absorption noise temperature is the key factor shaping the noise temperature of the system, and it is expressed as:

$$T_{\text{abs}}(f_c, d) = \frac{2k_B T_s L_{\text{mab}}(f_c)}{B}, \quad (10)$$

Here, $L_{\text{mab}}(f_c)$ is the molecular absorption coefficient at carrier frequency f_c . The molecular absorption noise temperature represents the additional noise from THz signal absorption by water vapor and other atmospheric molecules. The channel power gain follows a free-space path loss model given by:

$$|h_{S_{\text{MEC}_{b_s}}}(t)|^2 = \frac{G_{\text{tx}}G_{\text{rx}}\lambda^2}{(4\pi d_t)^{\varrho}}, \quad (11)$$

where d_t represents the Euclidean distance (in meters) between MEC_{b_s} and EU_i at time t , $\frac{1}{16\pi^2}G_{\text{tx}}G_{\text{rx}}$ represents a reference channel gain at a 1m distance, and ϱ is the path loss exponent. Thus, the total path loss is:

$$L_{\text{tot}} = \frac{(4\pi d_t)^{\varrho}}{G_{\text{tx}}G_{\text{rx}}\lambda^2} \times L_{\text{mab}}. \quad (12)$$

C. Reception of the THz Signal at EU_i

After being transmitted from MEC_{b_s} , the THz signal reaches EU_i . The received signal at this node is influenced by the MEC_{b_s} transmitter antenna gain G_{tx} , the time-varying channel response $h_{S_{\text{MEC}_{b_s}}}(t)$, the total path loss L_{tot} , and the EU_i antenna gain G_{rx} :

$$R_{\text{EU}_i}(t) = \sqrt{G_{\text{tx}}G_{\text{rx}}} \cdot \frac{h_{S_{\text{MEC}_{b_s}}}(t)}{\sqrt{L_{\text{tot}}}} \cdot S_{\text{MEC}_{b_s}}(t) + n_{\text{EU}_i}(t), \quad (13)$$

where $S_{\text{MEC}_{b_s}}(t)$ is the transmitted signal from equation (1), and $n_{\text{EU}_i}(t)$ represents the instantaneous additive noise received by EU_i , modeled as a zero-mean Gaussian distribution incorporating both thermal and molecular absorption noise.

The received signal's reliability is evaluated based on the signal-to-noise ratio (SNR), which is defined as the ratio of the received signal power to the noise power at time t :

$$\text{SNR}_{\text{down}}(t) = \frac{p_{\text{rx}} \cdot |h_{S_{\text{MEC}_{b_s}}}(t)|^2}{L_{\text{tot}} \cdot \sigma_{n,\text{EU}_i}^2}, \quad (14)$$

where $p_{rx} = p_k \cdot G_{tx} \cdot G_{rx}$ represents the received usable power at EU_i , with p_k being the power of the k -th bit of the transmitted signal from equation (1), while σ_{n,EU_i}^2 represents the noise power at EU_i .

D. Reflection of THz Signal to the MEC_{bs}

In this step, the EU_i does not generate a new signal; instead, it modulates the received THz signal from MEC_{bs} in equation (1) with its own information and reflects it to the MEC_{bs} . The reflected signal received at the MEC_{bs} is given by:

$$R_{MEC_{bs}}(t) = \sqrt{G_{rx}} \cdot h_{SMEC_{bs}}(t) \cdot \Gamma_{mod}(t) \cdot R_{EU_i}(t) + n_{MEC_{bs}}(t), \quad (15)$$

where $\Gamma_{mod}(t)$ is the modulation coefficient applied by EU_i to encode the information, and $n_{MEC_{bs}}(t)$ is the additive noise at MEC_{bs} .

The SNR for backscatter communication, which is influenced by two-way path loss and the efficiency of the modulation process, is given by:

$$SNR_{up}(t) = \frac{(\Gamma_{mod}(t))^2 \cdot p_{rx} \cdot |h_{SMEC_{bs}}(t)|^2}{L_{tot}^2 \cdot \sigma_{n,MEC_{bs}}^2}, \quad (16)$$

where $p_{rx} = p_k \cdot G_{tx} \cdot G_{rx}$ denotes the received power at EU_i , and $\sigma_{n,MEC_{bs}}^2$ represents the noise power at MEC_{bs} . Since backscatter involves two-way propagation, the total path loss is squared L_{tot}^2 to account for both the downlink and uplink attenuation.

III. THE PROPOSED TERAPRI FRAMEWORK

This section provides the detail solution of our proposed TeraPRI framework, designed to efficiently coordinate power and information transfer while ensuring privacy and communication reliability. The workflow is illustrated in Fig. 2.

A. Adaptive Resource Allocation for THz-Empowered Joint Wireless Power and Information Transfer

We design an adaptive resource allocation method for joint wireless power and information transfer within a proposed low-THz frequency range (0.1 – 1.0THz). This method dynamically switches between HaT-mode and TaH-mode based on the demands from EU_i , allocating the power resources received by EU_i from the signal $R_{EU_i}(t)$ in equation (13) for either energy harvesting or information transmission. The resource allocation is managed through a condition-based approach:

$$R_{alloc} = \begin{cases} B_{rec}, & \text{if } \rho_t^{in} \leq \rho_{thres}, \\ I_{tran}, & \text{else if } \rho_t^{in} \geq \rho_{thres}, \end{cases} \quad (17)$$

Here, the logic behind R_{alloc} is as follows: if the initial battery level ρ_t^{in} of EU_i upon receiving the signal R_{EU_i} at time t is less than or equal to a predefined threshold ρ_t^{in} , all the received power will be allocated towards recharging of EU_i . However, if the initial battery level ρ_t^{in} is above the predefined threshold ρ_{thres} , the received power is then allocated towards transmitting information from EU_i to MEC_{bs} .

In the scenario where $\rho_t^{in} \leq \rho_{thres}$, the HaT-mode is activated, allocating all of R_{alloc} for the battery recharging

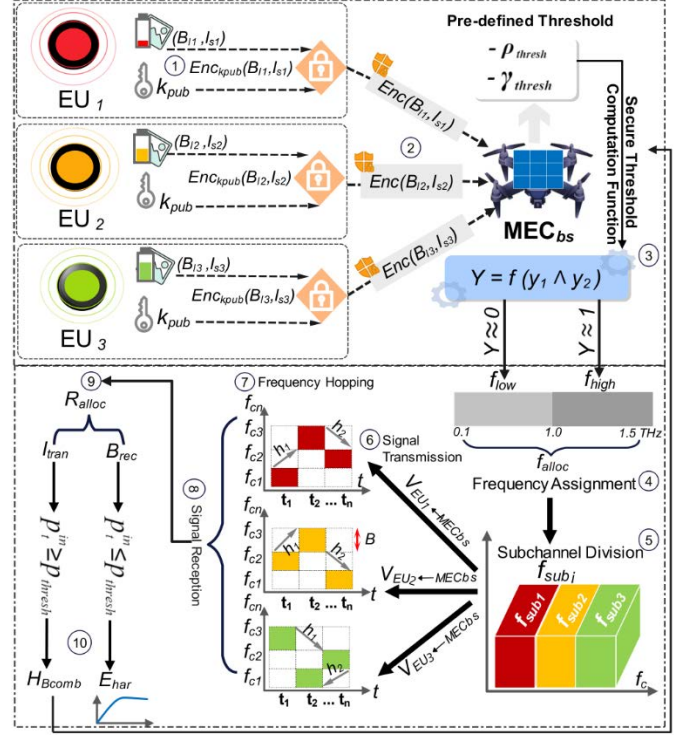


Fig. 2: Our proposed TeraPRI framework workflow.

B_{rec} . All energy-related quantities in this work are measured in joules (J). The amount of energy harvested at each node EU_i during the h -th hop at time t is given by:

$$E_{har,EU_i,h,t} = \eta_{EU_i} \cdot p_h \cdot |h_{SMEC_{bs}}(t)|^2 \cdot \psi_h, \quad (18)$$

where, $\eta_{EU_i} \in (0, 1)$ is the conversion efficiency of the energy harvested at EU_i , and ψ_h is the duration of the frequency hop.

The energy consumed by EU_i at time t , denoted as $E_{EU_i}(t)$, should not exceed the total energy harvested during that time, which is given by:

$$E_{EU_i}(t) \leq \sum_{h=1}^H E_{har,EU_i,h,t}, \quad (19)$$

where H denotes the total number of frequency hops.

The update battery level of EU_i at time $t + 1$ is:

$$\rho_{EU_i}(t + 1) = \rho_{EU_i}(t) + \sum_{h=1}^H E_{har,EU_i,h,t} - E_{EU_i}(t), \quad (20)$$

The computational complexity of Algorithm 1 is derived based on its iterative structure and the key operations performed during the HaT-mode and TaH-mode. The algorithm processes N end-user nodes iterating through each node EU_i to dynamically determine the appropriate resource allocation method. Feedback information in TaH mode is processed through concatenation, hashing (SHA-256), and encoding operations. These operations are proportional to the length of the feedback information processed, denoted L . Thus, the computational complexity of Algorithm 1 can be formally derived as:

$$T(N, L) = \sum_{i=1}^N (T_{cons} + T_{mode}(L)), \quad (21)$$

Algorithm 1 Adaptive Resource Allocation for THz-Empowered Joint Wireless Power and Information Transfer

Input: R_{EU_i} , ρ_t^{in} , ρ_{thresh} , η_{EU_i} , ψ_h , t .

Output: $I_{\text{tranEU}_i}(t)$ from EU_i to MEC_{bs} at t via backscatter.

```

1: Initialization: Set initial battery level  $\rho_t^{\text{in}}$ 
2: for each  $EU_i$  in  $V_{EU_c}$  do
3:   Determine resource allocation method  $R_{\text{alloc}}$ 
4:   if  $\rho_t^{\text{in}} \leq \rho_{\text{thresh}}$  then
5:     HaT-mode Activated:
6:     Harvest energy  $\sum_{h=1}^H E_{\text{har,EU}_i,h,t}$ 
7:     Update battery level  $\rho_{EU_i}(t+1)$ 
8:     Stop recharging if  $\rho_{EU_i}(t+1) \geq \rho_{\text{thresh}}$ 
9:   else
10:    TaH-mode Activated:
11:    Encode  $ID_{EU_i}$ ,  $m_d$ ,  $T_{\text{stp}}$ ,  $R_{\text{loc}}$  with UTF-8 and  $B_{\text{Inf}}$ 
12:    Convert  $m_d$  to binary  $B_q$  and map to  $m_{d_j}$  via  $G_q$ 
13:    Concatenate feedback information  $B_{\text{comb}}$ 
14:    Pad  $B_{\text{comb}}$  to a multiple of 512 bits before hashing
15:    Apply SHA-256 hash to obtain  $H_{B_{\text{comb}}}$ 
16:    Modulate  $H_{B_{\text{comb}}}$  into the signal using  $M_{\text{pro}}(t)$ 
17:    Transmit  $I_{\text{tranEU}_i}(t)$  while  $\rho_t^{\text{in}} > \rho_{\text{thresh}}$ 
18:    Stop transmission when  $\rho_t^{\text{in}} \leq \rho_{\text{thresh}}$ 
19:   end if
20: end for

```

where N is the number of end-user nodes (V_{EU}), L is the length of the processed feedback information, T_{cons} represents the constant time required to evaluate the condition $\rho_t^{\text{in}} \leq \rho_{\text{thresh}}$, and $T_{\text{mode}}(L)$ represents the time complexity of mode-specific operations (HaT-mode or TaH-mode).

For each EU_i in HaT-mode ($\rho_t^{\text{in}} \leq \rho_{\text{thresh}}$), the algorithm performs energy harvesting operations. These involve state updates that are independent of L , contributing a constant complexity:

$$T_{\text{mode}}^{\text{HaT}}(L) = O(1). \quad (22)$$

In TaH-mode ($\rho_t^{\text{in}} > \rho_{\text{thresh}}$), the algorithm processes feedback information via concatenation, hashing (SHA-256), and encoding. These operations are proportional to L , resulting in:

$$T_{\text{mode}}^{\text{TaH}}(L) = O(L). \quad (23)$$

The total computational complexity becomes:

$$T(N, L) = \sum_{i=1}^N (O(1) + O(L)) = O(N \cdot L), \quad (24)$$

where (N) is the number of end-user nodes, and (L) is the size of the processed feedback information. The total computational complexity ensures that Algorithm 1 scales linearly with both the number of end-user nodes and the size of the processed data, making it efficient for large-scale deployments.

In the scenario where $\rho_t^{\text{in}} \geq \rho_{\text{thresh}}$, the TaH-mode is activated, allocating all R_{alloc} to the information transmission I_{tran} . The transmitted information is referred to as "*feedback information*", and it includes the EU_i identifier ID_{EU_i} , collected data m_d , timestamp T_{stp} , and current location R_{loc} .

The encoding process for ID_{EU_i} , T_{stp} , and R_{loc} involves converting these elements into UTF-8 binary representations. Let C_n denote the UTF-8 binary representation of each component, where:

$$C_n = \text{UTF-8}(U_n). \quad (25)$$

The combined binary representation B_{Inf} is calculated by summing the UTF-8 values multiplied by their positional weights:

$$B_{\text{Inf}} = \sum (C_n \cdot 2^{(k_j-1)}). \quad (26)$$

For binary values B_j with fewer than 7 bits ($\text{len}(B_j) < 7$), they are left-shifted to 8 bits:

$$E_{\text{short},j} = B_j \times 2^{(8-\text{len}(B_j))}. \quad (27)$$

For binary values B_j with 7 bits or more ($\text{len}(B_j) \geq 7$), 1s are prefixed, followed by 0s to complete each byte:

$$E_{\text{long},j} = 2^{(7 \times b_j)} + B_j \times 2^{(8 \times (b_j-1))}. \quad (28)$$

The number of bytes required is given by:

$$b_j = \lceil (\text{len}(B_j) - 1) / 7 \rceil, \quad (29)$$

where B_j is the UTF-8 binary value, and $\text{len}(B_j)$ is its length.

The encoding process for m_d depends on the number of bits S_{bits} , which is determined by the total number of items M using $S_{\text{bits}} = \lceil \log_2(M) \rceil$. The binary representation of each item is generated using Gray code [47], ensuring that consecutive values differ by only one bit. For each integer B_q in the range 0 to $2^{S_{\text{bits}}} - 1$, Gray code G_q is computed as:

$$B_q \in \{0, 1\}^{S_{\text{bits}}}, \quad (30)$$

$$G_q = [B_q[0] \oplus B_q[1] \oplus \dots \oplus B_q[S_{\text{bits}} - 1]].$$

This method XORs adjacent bits in the binary representation to produce G_q . Each monitoring data item m_{d_j} is assigned a unique Gray code denoted as G_{q_j} using the mapping function G_{map} , expressed as:

$$G_{\text{map}}(m_{d_j}) = G_{q_j}, \quad \text{for } j \in \{1, 2, \dots, M\}, \quad (31)$$

where G_{q_j} is the Gray code corresponding to m_{d_j} .

After encoding ID_{EU_i} , R_{loc} , m_d , and T_{stp} , the combined binary representation of the feedback information is denoted as B_{comb} . This representation is obtained by concatenating the individual encoded components in a specific order, as described in equation (38), where $\|$ indicates the concatenation operation. To ensure the integrity of B_{comb} , we apply a SHA-256 hash function, as previously implemented in our work [13]. Since B_{comb} can vary in length, we pad it to a multiple of 512 bits by appending a '1' bit followed by '0' bits until the length is $448 \bmod 512$. Finally, we append the length of B_{comb} as a 64-bit binary representation. The padded binary string is given by:

$$B_{\text{pad}} = B_{\text{comb}} \| 1 \| \underbrace{0^k}_{\text{appended '0' bits}} \| L_{B_{\text{comb}}}, \quad (32)$$

where $L_{B_{\text{comb}}}$ represents the 64-bit length of B_{comb} .

For further processing, the binary string B_{pad} is divided into 64 segments, each consisting of 32 bits. These segments are

denoted as D_i , where i ranges from 1 to 64. Each D_i represents a 32-bit word extracted from B_{pad} . This decomposition is expressed as:

$$D_{B_{\text{pad}}} = \underbrace{D_1}_{32\text{-bit word}} \parallel \underbrace{D_2}_{32\text{-bit word}} \parallel \dots \parallel \underbrace{D_{64}}_{32\text{-bit word}}, \quad (33)$$

where \parallel indicates the concatenation of the 32-bit words D_i .

To compute each D_i word, we use functions F_1 and F_0 , which perform bitwise operations and iterate over 64 rounds. The computation is expressed as:

$$D_i = \underbrace{F_1(D_{i-2})}_{\text{bitwise operations}} + D_{i-7} + F_0(D_{i-15}) + D_{i-16},$$

e.g., $(\text{RotR}(D_{i-2}, 2) \oplus \text{RotR}(D_{i-2}, 13) \oplus \text{RotR}(D_{i-2}, 22)).$ (34)

After processing all blocks of B_{comb} , we concatenate the updated hash values to obtain a final hash value denoted as $H_{B_{\text{comb}}}$. This $H_{B_{\text{comb}}}$ serves as a unique checksum to ensure the integrity and authenticity of B_{comb} . Next, $H_{B_{\text{comb}}}$ is modulated into the received signal using backscatter modulation, as described in equation (13). In this process, the carrier frequency at the time of reception carries the feedback information back to the MEC_{bs}. The modulation process is given by:

$$M_{\text{pro}}(t) = \sum_{q=0}^{S-1} (A \cdot \sin(2\pi(f_{c,\text{rec}t} + F_{ht})t) \cdot H_{B_{\text{comb},q}}), \quad (35)$$

where S represents the total number of bits in the feedback information $H_{B_{\text{comb}}}$, A is the amplitude of the modulated signal, $f_{c,\text{received}t}$ is the received carrier frequency at time t , $F_h(t)$ adjusts the carrier frequency at time (t) based on a random frequency hopping pattern, and $H_{B_{\text{comb},q}}$ is the q -th bit of the binary sequence $H_{B_{\text{comb}}}$ being modulated.

The transmitted feedback information is given by:

$$I_{\text{tranEU}_i}(t) = (\Gamma_i \cdot s_{\text{MEC}_{bs}}(t) \cdot M_{\text{pro}}(t)) + n_{\text{EU}_i}(t), \quad (36)$$

where Γ_i is the reflection coefficient representing the reflected signal power, $s_{\text{MEC}_{bs}}(t)$ is the strength of the signal at MEC_{bs}.

The achievable information rate during the h -th hop is:

$$\text{AIR}_{i,h} = \tau \cdot B \cdot \log_2 \left(1 + \frac{|\Gamma_i \cdot h s_{\text{MEC}_{bs}}(t)|^2 \cdot p_{\text{TX}}}{\sigma_{n,\text{MEC}_{bs}}^2} \right), \quad (37)$$

where τ is the transmission time constant, Γ_i is the reflection coefficient for EU_i .

B. Selective Privacy-Preserving Frequency Allocation with Enhanced Security

For clarity, this work focuses on the time window during which an EU_i is within the communication range R_{comm} of the MEC_{bs} and actively connected for direct communication. During this time window, a selective CKKS homomorphic encryption technique with lightweight thresholding enables the MEC to securely allocate unique THz sub-channels to end-user nodes while enhancing communication security through randomized frequency hopping.

Algorithm 2 Selective Privacy-Preserving Frequency Allocation with Enhanced Security

Input: $V_{\text{EU}}, R_{\text{comm}}, B_l, I_s, k_{\text{pub}}, k_{\text{pri}}, \rho_{\text{thresh}}, I_{\text{thresh}}, N, q, \Delta, \epsilon_1, \epsilon_2, t$

Output: Sub-channel frequency range assignment f_{sub_i} for each EU_i in V_{EU_c}

- 1: **Initialization:**
- 2: Identify $V_{\text{EU}_c}(t) = \{\text{EU}_i \mid i \in [1 : N], d_i(t) \leq R_{\text{comm}}\}$;
- 3: Generate $(k_{\text{pub}}, k_{\text{pri}}) = \mathcal{K}_{\text{gen}}(N, q, \Delta)$
- 4: **for** each EU_i in V_{EU_c} at t **do**
- 5: Extract battery level B_{l_i} and collected data size I_{s_i}
- 6: Encrypt $\text{Enc}(B_{l_i})$ and $\text{Enc}(I_{s_i})$
- 7: Transmit $\text{Enc}(\text{ID}_{\text{EU}_i}, k_{\text{pub}}, B_{l_i}, I_{s_i})$ to MEC_{bs}
- 8: **for** each received $\text{Enc}(\text{ID}_{\text{EU}_i}, k_{\text{pub}}, B_{l_i}, I_{s_i})$ **do**
- 9: Compute $Y_1 = \frac{1}{2} \left(1 + \tanh \left(\frac{\Delta(\text{Enc}[B_{l_i}] - \rho_{\text{thresh}})}{\epsilon_1} \right) \right)$
- 10: Compute $Y_2 = \frac{1}{2} \left(1 + \tanh \left(\frac{\Delta(\text{Enc}[I_{s_i}] - I_{\text{thresh}})}{\epsilon_2} \right) \right)$
- 11: Compute $Y = (Y_1)_{\text{thresh}} \wedge (Y_2)_{\text{thresh}}$
- 12: **if** $Y \leq 0.5$ **then** ▷ Values close to 0 $Y \approx 0$
- 13: Assign low-frequency band $f_{\text{alloc}} = f_{\text{alloc}_{\text{low}}}$
- 14: **else** ▷ Values close to 1 $Y \approx 1$
- 15: Assign high-frequency band $f_{\text{alloc}} = f_{\text{alloc}_{\text{high}}}$
- 16: **end if**
- 17: Compute sub-channel frequency f_{sub_i} for each EU_i
- 18: Compute dynamically adjusted frequency:

$$f_{c_i} = f_{\text{sub}_i} + (h - 1) \cdot \Delta f_h + R_h \cdot T_{\text{hop}}$$
- 19: Use f_{c_i} during signal transmission.
- 20: **end for**
- 21: **end for**

Let the set of end-user nodes within R_{comm} be defined as:

$$V_{\text{EU}_c}(t) = \{\text{EU}_i \mid i \in [1 : N], d_i(t) \leq R_{\text{comm}}\}. \quad (39)$$

To ensure secure communication and data privacy, we employ CKKS homomorphic encryption [48] to protect the sensitive data during communication with the MEC_{bs}. The process starts with key generation, where each EU_i in V_{EU_c} generates a pair of public k_{pub} and private k_{pri} keys:

$$(k_{\text{pub}}, k_{\text{pri}}) = \mathcal{K}_{\text{gen}}(N, q, \Delta), \quad (40)$$

where N is the polynomial degree, q is the ciphertext modulus size, and Δ is the scaling factor.

Once generated, the public key k_{pub} is used by EU_i to encrypt its battery level B_l and collected data size I_s :

$$\text{Enc}(B_{l_i}) = \text{Enc}_{k_{\text{pub}}}(B_{l_i}), \quad \text{Enc}(I_{s_i}) = \text{Enc}_{k_{\text{pub}}}(I_{s_i}), \quad (41)$$

where $\text{Enc}(B_{l_i})$ and $\text{Enc}(I_{s_i})$ denote the encrypted battery level and the size of the collected monitoring data, respectively. The encrypted data is sent to the MEC_{bs}:

$$\text{Enc}(\text{ID}_{\text{EU}_i}, k_{\text{pub}}, B_{l_i}, I_{s_i}) \rightarrow \text{MEC}_{bs}, \quad (42)$$

where ID_{EU_i} ensures accurate data association by the MEC_{bs}. For simplicity, we assume that this process occurs over a separate frequency band, the details of which are beyond the scope of this work.

$$B_{\text{comb}} = \left(\sum_{j=1}^n \text{UTF-8}(U_{\text{ID}_{\text{EU}_i, j}}) \cdot 2^{(q_{\text{DEU}_i, j} - 1)} \right) \parallel \left(\sum_{j=1}^n \text{UTF-8}(U_{R_{\text{loc}_j}}) \cdot 2^{(q_{\text{loc}_j} - 1)} \right) \parallel G_{\text{map}}(m_{d_j}) \parallel \left(\sum_{j=1}^n \text{UTF-8}(U_{\text{tstp}_j}) \cdot 2^{(q_{\text{tstp}_j} - 1)} \right), \quad (38)$$

Upon receiving $\text{Enc}(\text{ID}_{\text{EU}_i}, k_{\text{pub}}, B_{l_i}, I_{s_i})$, the MEC_{bs} uses the public key k_{pub} to perform secure threshold computations on the encrypted data, comparing $\text{Enc}(B_{l_i})$ and $\text{Enc}(I_{s_i})$ against the thresholds ρ_{thresh} and γ_{thresh} , respectively, without decryption. The computations are defined as follows:

$$Y_1 = \frac{1}{2} \left(1 + \tanh \left(\frac{\Delta(\text{Enc}(B_{l_i}) - \rho_{\text{thresh}})}{\epsilon_1} \right) \right), \quad (43)$$

$$Y_2 = \frac{1}{2} \left(1 + \tanh \left(\frac{\Delta(\text{Enc}(I_{s_i}) - \gamma_{\text{thresh}})}{\epsilon_2} \right) \right),$$

where

$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}, \quad (44)$$

is the function normalizes its input to a range between -1 and 1 . The parameter Δ controls the sensitivity of the comparison, and ϵ_1 and ϵ_2 indicate the acceptable range around 1, allowing for a margin of error. The value Y_1 assesses the encrypted battery level against ρ_{thresh} , and Y_2 evaluates the encrypted data size against γ_{thresh} .

To determine the result of the secure threshold computation, we first apply a threshold function to the computed values Y_1 and Y_2 :

$$(Y_i)_{\text{thresh}} = \begin{cases} 1, & \text{if } Y_i \geq 0.5, \\ 0, & \text{otherwise.} \end{cases} \quad (45)$$

In this process, $(Y_i)_{\text{thresh}}$ converts Y_i into a binary value. The final decision Y is then determined as:

$$Y = (Y_1)_{\text{thresh}} \wedge (Y_2)_{\text{thresh}}. \quad (46)$$

Consequently, Y is 1 only if both Y_1 and Y_2 are greater than or equal to 0.5. If either value is close to or below 0.5, Y is 0. This ensures that both conditions must be satisfied for making the frequency allocation decision.

The frequency sub-channels f_{alloc} are allocated as follows:

$$f_{\text{alloc}} = \begin{cases} f_{\text{alloc}_{\text{high}}}, & \text{if } Y \approx 1, \\ f_{\text{alloc}_{\text{low}}}, & \text{if } Y \approx 0, \end{cases} \quad (47)$$

where

$$f_{\text{alloc}_{\text{high}}} = f_{\text{mid}} + \frac{f_{\text{max}} - f_{\text{mid}}}{2}, \quad (48)$$

$$f_{\text{alloc}_{\text{low}}} = f_{\text{mid}} - \frac{f_{\text{mid}} - f_{\text{min}}}{2}, \quad (49)$$

The values $f_{\text{alloc}_{\text{high}}}$ and $f_{\text{alloc}_{\text{low}}}$ represent the allocated high and low frequency sub-bands, respectively. The THz frequency band used in this work ranges from 0.1 THz to 1.0 THz. Based on the result of Y , if $Y \approx 1$, the allocated frequency falls within the upper range of 1.0 to 1.0 THz. Conversely, if $Y \approx 0$, the allocated frequency lies within the lower range of 0.1 to 1.0 THz.

Following the strategic assignment of f_{alloc} based on (47), subchannels are divided to enable efficient, interference-free communication:

$$f_{\text{sub}_i} = \begin{cases} f_{\text{alloc}_{\text{high}}} + i \cdot \frac{(f_{\text{alloc}_{\text{high}}} - f_{\text{alloc}_{\text{low}}})}{V_{\text{EU}_c}(t)}, & \text{if } Y \approx 1, \\ f_{\text{alloc}_{\text{low}}} + i \cdot \frac{(f_{\text{alloc}_{\text{high}}} - f_{\text{alloc}_{\text{low}}})}{V_{\text{EU}_c}(t)}, & \text{if } Y \approx 0. \end{cases} \quad (50)$$

After determining the subchannel frequency range, the MEC_{bs} transmits the signal to EU_i at time t , as described in equation (1). Within the transmitted signal, the frequency of each assigned subchannel varies across consecutive hops, introducing randomness and enhancing privacy. This frequency hopping mechanism enhances privacy by dynamically adjusting the carrier frequency f_c in each hop cycle, as defined by:

$$f_{c_i} = f_{\text{sub}_i} + (h - 1) \cdot \Delta f_h + R_h \cdot T_{\text{hop}}, \quad (51)$$

where f_{sub_i} is the allocated frequency for the i -th node, $(h - 1) \cdot \Delta f_h$ represents the hop index, R_h introduces randomness, and T_{hop} is the hopping duration.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of our proposed TeraPRI framework across various metrics and parameters. For comparison, we consider two benchmark schemes, where we only extract their power allocation method and implement it within our TeraPRI framework to compare performance under the same system setup:

- **Scheme in [31]:** Originally developed for the RF spectrum, this scheme employs a power-splitting method, where the received signal power is divided into two portions: $\tilde{y}_i(t) = \sqrt{\rho_i} y_i(t)$ for energy harvesting and $\tilde{y}_i(t) = \sqrt{1 - \rho_i} y_i(t)$ for information decoding, with a constant power ratio $\rho_i : 1 - \rho_i$ ($\rho_i \in (0, 1)$). In this work, we adapt the power-splitting methodology within the THz-based TeraPRI framework. Specifically, $\tilde{y}_i(t) = \sqrt{1 - \rho_i} y_i(t)$ is repurposed to transmit feedback information during the uplink phase.
- **Scheme in [27]:** This scheme implements a harvest-and-then-transmit approach based on TDMA, where end-users first harvest energy during a portion of the time frame $\tau_0 T$ in the downlink and then transmit information during the uplink in the remaining time.

A. Simulation Setup

The simulations were conducted on a Windows 11 system with an Intel Core i7-11800H CPU (2.30 GHz), 64 GB RAM, and a 64-bit OS. The simulation framework was implemented in Python 3.9.12, utilizing libraries for THz channel modeling, signal processing, and CKKS encryption operations. All distance-related units are in meters, and angles are in degrees. In all simulations, we assume a direct line-of-sight path with minimal non-line-of-sight deviations between the MEC_{bs} and EU_i . Additionally, all plotted values are averages.

1) *CKKS Encryption*: We use a polynomial modulus degree $N_{\text{poly}} = 16384$, which supports complex computations and large datasets. The coefficient moduli q_0, q_1, q_2, q_3 are each set to 2^{60} to maintain precision and control noise growth during homomorphic operations. The global scale $\Delta_{\text{CKKS}} = 2^{40}$ determines the resolution of the encrypted data. The cumulative coefficient modulus q ranges from 2^{240} to 2^{300} , allowing flexibility in the number of operations before decryption is required. The security level exceeds 128 bits, providing strong cryptographic protection.

TABLE I: Simulation Scenario and Parameters

Parameter Description	Initial Values
Minimum altitude of $H_{\text{MEC}_{bs}}$	10m
Communication range R_{comm}	10m
Battery capacity of EU_i	LiPo 15.2V/3.0Ah
ρ_t^{in} initial battery level	20% to 60%
ρ_{thresh} battery level threshold	40%
Energy harvesting efficiency (η)	0.2, $\forall i \in [1 : N]$
THz frequency band used	0.1 to 1.0 THz
Frequency hops	10 h
Selective allocated bandwidth (B)	9.0×10^{11} Hz
G_t antennas and G_r antennas	40dB and 32dB
Transmit power (p_k) of MEC_{bs}	20dBm = 100mW
Reference channel gain at 1m	≈ -115.81 dB
Path loss exponent (ρ)	2.5
Molecular absorption coefficients	Generated according to [43]
Time (t)	10^{12} ps = 1s

B. Power Transfer Performance:

The power transfer performance during the downlink phase is evaluated in terms of energy harvesting (Wh) and battery levels (%). For clarity, our simulation results use watt-hours (Wh), where 1 Wh = 3600 J.

First, we evaluate the impact of varying the number of frequency hops h ranging from 10 to 50 with $EU_i = 5$, $\text{MEC}_{bs} = 1$, while other parameters remain unchanged. We can observe in Fig. 3(a) and 3(b), as the number of hops increases, all results across all schemes improves. However, our proposed scheme outperforms those in [31] and [27] as it allocates all received signal power R_{EU_i} to energy harvesting when the battery level is below ρ_{thresh} . This dynamic approach allows our scheme to harvest energy ranging from 15.42Wh to 38.43Wh while maintaining battery levels between 49.59% and 72.77%, ensuring prolonged operation and improved power sustainability.

Second, we evaluate the impact of varying the distance between the MEC_{bs} and EU_i from 10m to 90m, with $EU_i = 5$, $\text{MEC}_{bs} = 1$, and the number of frequency hops fixed at 50, while other parameters remain unchanged. We can observe in Fig. 4(a) and Fig. 4(b) that as the distance increases, both the harvested energy and battery levels decrease for all schemes. This reduction is attributed to the sensitivity of THz signals to molecular absorption loss and free-space path loss. As modeled in equation (11), the channel power gain

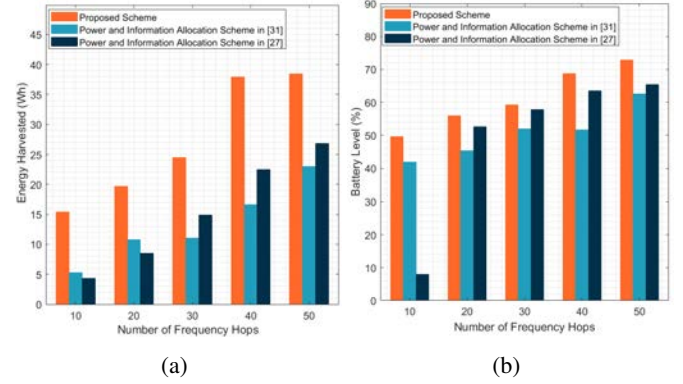


Fig. 3: The impact of varying the number of frequency hops on (a) energy harvested, and (b) battery level.

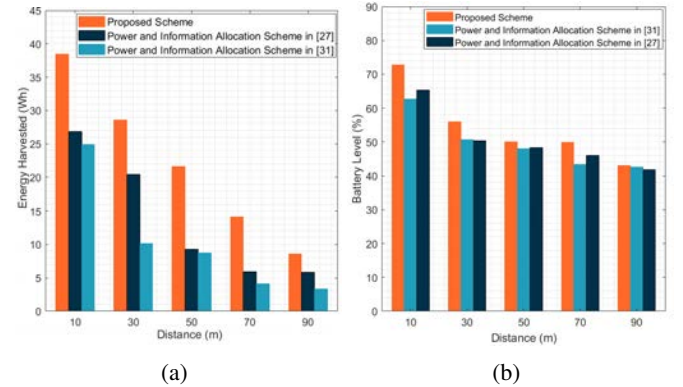


Fig. 4: The impact of varying distances on (a) energy harvested, and (b) battery level.

follows an inverse relationship with distance. This formulation demonstrates that as d_t increases, the received signal power decreases significantly due to increasing THz path loss, leading to lower harvested energy at the end-user nodes. Despite this, our proposed scheme outperforms [27] and [31] at 90 m, achieving 8.56 Wh of harvested energy with a battery level of 43.10%. In comparison, [27] achieves 5.85 Wh with 41.83%, while [31] achieves 3.33 Wh with a slightly higher battery level of 42.54%. The variations stem from differences in initial battery levels ρ_t^{in} , and energy allocation strategies.

Third, we evaluate the impact of varying the number of SNR for the downlink phase, again with $EU_i = 5$, $\text{MEC}_{bs} = 1$, the number of frequency hops fixed at 50, while keeping other parameters unchanged. As shown in Fig. 5(a) and Fig. 5(b), our proposed scheme outperforms existing schemes as the SNR increases from 6 dB to 18 dB, with harvested energy ranging from 13.65 Wh to 31.09 Wh and battery levels maintained between 50.85% and 65.57%. This performance improvement is attributed to the relationship between the received power (13) and SNR (14). As SNR_{down} increases, the received power p_{rx} improves, leading to higher energy harvesting efficiency. In comparison, [27] achieves 10.48 Wh to 27.47 Wh with battery levels from 48.37% to 55.22%, and [31] achieves 7.87 Wh to 22.57 Wh, with a slightly higher battery level ranging from 44.07% to 57.24%.

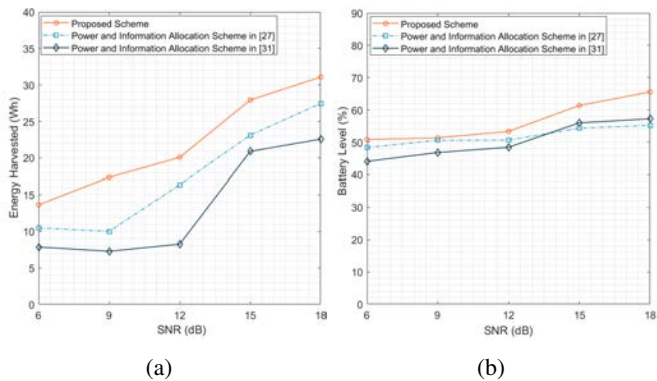


Fig. 5: The impact of varying SNR_{down} levels on (a) energy harvested, and (b) battery level.

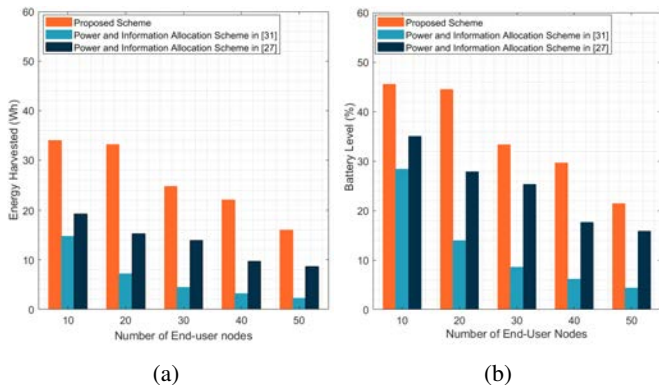


Fig. 6: The impact of varying the number of end-user nodes on (a) energy harvested, and (b) battery level.

Fourth, we evaluate the impact of varying the number of end-user nodes from 10 to 50, with $MEC_{bs} = 1$ and $h = 50$, while keeping other parameters unchanged. As shown in Fig. 6, increasing the number of nodes reduces harvested energy and battery levels due to the limited power budget being focused on fewer nodes at a time, based on the THz beamwidth. For instance, in the proposed scheme, harvested energy decreases from 33.96 Wh (10 nodes) down to 15.99 Wh (50 nodes), while battery levels drop from 45.57% down to 21.47%. Similarly, the schemes in [31] and [27] show a greater drop, achieving only 2.29 Wh and 8.68 Wh, and 4.39% and 15.8%, respectively, at 50 nodes. Our proposed scheme outperforms existing methods by adaptively allocating frequency and power, improving energy harvesting and battery performance in high-density networks.

C. Information Transfer Performance

The performance of information transfer during the uplink phase is assessed in terms of achievable information rate (AIR) in bps, where values in the terabits per second (Tbps) range, and information transmission success rate (ITSR) (%).

First, we evaluate the impact of varying the number of frequency hops from 10 to 50 with $EU_i = 5$, $MEC_{bs} = 1$, feedback information size ranging from 100 KB to 1000 KB, while keeping other parameters unchanged. We can observe in Fig. 7(a) that as the number of frequency hops reaches 50, our

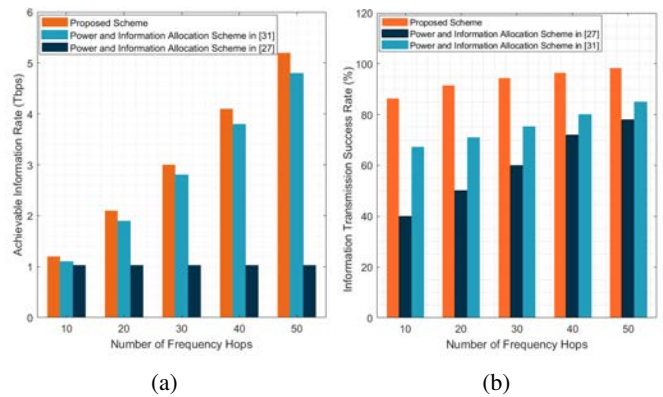


Fig. 7: The impact of varying the number of frequency hops on (a) the achievable information rate, and (b) the information transmission success rate.

proposed scheme achieves an information rate of 6.5×10^{12} bps, compared to 5.9×10^{12} bps for [31], and a constant rate of 1.03×10^{12} bps for [27]. In Fig. 7(b), our scheme achieves the highest success rate reaching 98.5% at 50 hops, due to its adaptive mechanism. While [31] has a slightly higher AIR than [27], its success rate fluctuates between 67.2% and 85.0%, whereas [27] improves from 40.0% to 78.0%.

Second, in Fig. 8(a) and Fig. 8(b), we evaluate the impact of varying the distance between EU_i and MEC_{bs} from 10m to 90m, with $EU_i = 5$, $MEC_{bs} = 1$, information sizes ranging from 100KB to 1000KB, number of frequency hops set to 50, and other parameters remain unchanged. In Fig. 8(a), channel capacity decreases with distance due to THz signal attenuation from path loss and molecular absorption, as modeled in equation (11). As d_t increases, the denominator grows, sharply reducing received signal power and negatively impacting AIR and ITSR. Despite severe THz attenuation, our proposed scheme still achieves an AIR of 1.8×10^{12} bps and a success rate of 64.86% at 90m, surpassing [31] with an AIR of 9.5×10^{11} bps and a success rate of 42.54%, and [27] with an AIR of 4.7×10^{11} bps and a success rate of 41.83%. This superior performance is due to its adaptive frequency and power allocation, which dynamically mitigates path loss and enhances reliability over long distances.

Third, we evaluate the impact of varying the number of SNR levels for the uplink phase, with $EU_i = 5$, $MEC_{bs} = 1$, and the number of frequency hops fixed at 50, while keeping other parameters unchanged. We can observe in Fig. 9(a) that as SNR_{up} increases, [31] achieves the highest AIR of 1.08×10^{12} bps at 18 dB due to static power allocation, while our proposed scheme reaches 1.05×10^{12} bps, and [27] achieves 0.55×10^{12} bps. However, in Fig. 9(b), our proposed scheme maintains the highest success rate 96.64% to 98.33% by dynamically adjusting power and frequency. In contrast, [31] suffers from lower adaptability 41.61% to 81.99%, and [27] improves 42.43% to 85.21% but remains limited by its harvest-then-transmit strategy.

Fourth, we evaluate the impact of increasing the number of end-user nodes from 10 to 50, with $MEC_{bs} = 1$, $h = 50$, and feedback sizes ranging from 100 KB to 1000 KB, while keep-

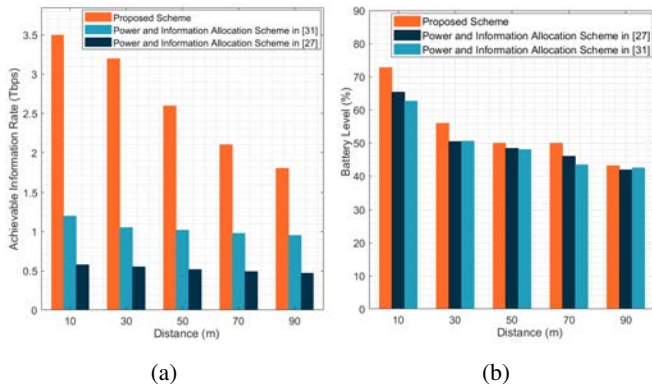


Fig. 8: The impact of varying distances on (a) the achievable information rate, and (b) the information transmission success rate.

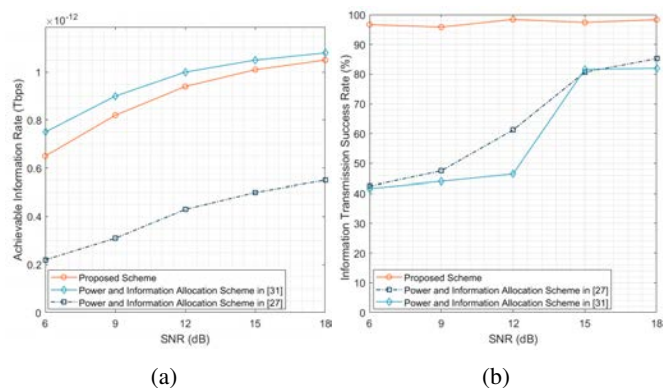


Fig. 9: The impact of varying SNR_{up} levels on (a) the achievable information rate, and (b) the information transmission success rate.

ing other parameters unchanged. As shown in Fig. 10, increasing the number of end-user nodes reduces both the achievable information rate and information transmission success rate due to limited power distribution and THz beamwidth constraints. Despite this, our proposed scheme maintains higher AIR, decreasing slightly from 1.423×10^{12} bps to 1.405×10^{12} bps, while ITSR drops marginally from 95.35% to 92.48%, thanks to its adaptive frequency and power allocation. In contrast, [31] sees minimal AIR reduction from 1.016×10^{12} bps down to 1.003×10^{12} bps, but experiences a steep ITSR decline from 34.76% down to 11.47%, due to its static power allocation, limiting efficiency in dense networks. Similarly, [27] maintains a nearly constant AIR, decreasing slightly from 1.017×10^{12} bps down to 1.003×10^{12} bps, while its ITSR drops from 40.93% to 32.12%, this is due to limited transmission time per end-user node EU_i .

D. TeraPRI Privacy and Security Analysis

In our TeraPRI framework, we employ CKKS homomorphic encryption [48] in Algorithm 2 to securely process and compute data. This technique enables the MEC_{b_s} to perform computations directly on encrypted data without requiring

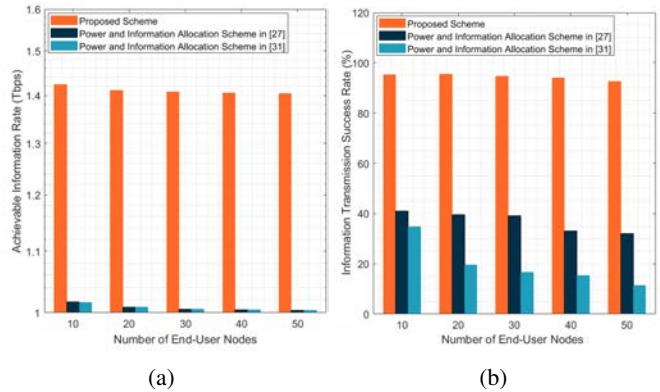


Fig. 10: The impact of varying the number of end-user nodes on (a) the achievable information rate, and (b) the information transmission success rate.

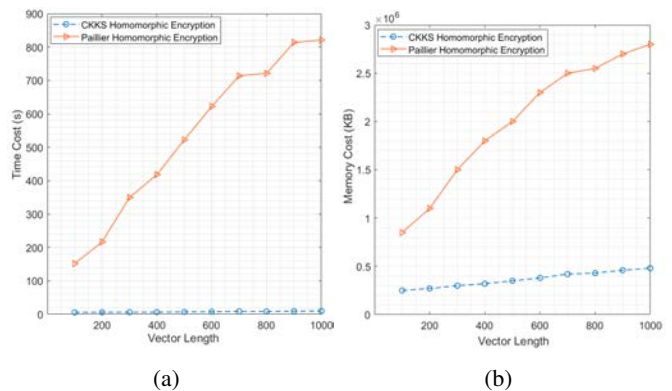


Fig. 11: Homomorphic encryption performance in terms of (a) time consumption, and (b) memory usage.

decryption, thereby preserving the confidentiality of sensitive information from the end-user nodes in $V_{EU_c}(t)$.

In Fig. 11, we compare the performance of the CKKS and Paillier homomorphic encryption schemes within the TeraPRI framework. The results demonstrate that CKKS outperforms Paillier in both time consumption and memory usage. As the vector length increases, the time cost of Paillier rises significantly, reaching up to 800 s for a vector length of 1000, while CKKS remains much more efficient, peaking at less than 20 s. Similarly, in Fig. 11(b), CKKS exhibits superior memory efficiency, requiring only 480 KB for a vector length of 1000, compared to 2.8 MB for Paillier. These results highlight CKKS's superior computational efficiency, making it a better fit for the complex operations required in the TeraPRI framework while ensuring scalability and security without incurring excessive computational overhead.

Theorem: The CKKS homomorphic encryption in our TeraPRI framework robustly safeguards the privacy of the encrypted battery level (B_l) and collected data size (I_s) during encryption, transmission, and computation.

Proof 1: Let B_l be the battery level and I_s the data size. Keys k_{pub} and k_{pri} are generated with parameters N , q , and Δ . The k_{pub} is for encryption and operations, while k_{pri} is for decryption. TeraPRI shares k_{pub} with MEC_{b_s} and keeps

k_{pri} secure on each EU_i . This ensures MEC_{bs} cannot access original data without the private key. The encryption function Enc encrypts B_l and I_s using k_{pub} , producing ciphertexts $\text{Enc}_{k_{\text{pub}}}(B_l)$ and $\text{Enc}_{k_{\text{pub}}}(I_s)$.

$$\begin{aligned} \text{Enc}_{k_{\text{pub}}}(B_l) &= \text{Enc}(B_l, k_{\text{pub}}, N, q, \Delta), \\ \text{Enc}_{k_{\text{pub}}}(I_s) &= \text{Enc}(I_s, k_{\text{pub}}, N, q, \Delta), \end{aligned} \quad (52)$$

The encryption process introduces variability to the encrypted data, making pattern detection difficult even with the same private key k_{pri} . This variability preserves the original data's privacy. The encryption process is secure due to the following properties:

- Given $E(B_l, k_{\text{pub}}, N, q, \Delta)$ and $\text{Enc}(I_s, k_{\text{pub}}, N, q, \Delta)$, it is computationally infeasible to determine B_l without k_{pri} ;
- Only k_{pub} is shared, with k_{pri} securely stored on each EU_i node;
- The encryption process obscures patterns in the encrypted data, even with k_{pri} .

During transmission, EU_i send $\text{Enc}_{k_{\text{pub}}}(B_l)$ and $\text{Enc}_{k_{\text{pub}}}(I_s)$ to MEC_{bs} . This ensures B_l and I_s remain confidential and indistinguishable from random data without k_{pri} . The MEC_{bs} then performs secure threshold computations on the encrypted data.

Proof 2: Let $\delta' > 0$ be a small positive number such that $\tanh(x)$ is approximately linear within the interval $(-\delta', \delta')$. This means that for x in this interval, $\tanh(x)$ can be approximated by x . Thus, we have:

$$\tanh(x) \approx x \text{ for } |x| < \delta'. \quad (53)$$

The hyperbolic tangent function $\tanh(x)$ ensures the actual values of B_l and I_s are not revealed during computation. When $|\Delta(\text{Enc}[B_{l_i}] - \rho_{\text{thresh}})| < \delta'$ and $|\Delta(\text{Enc}[I_{s_i}] - \gamma_{\text{thresh}})| < \delta'$, we use the linear approximation of $\tanh(x)$ within this interval:

$$\begin{aligned} Y_1 &\approx \frac{1}{2} \left(1 + \frac{\Delta(\text{Enc}[B_{l_i}] - \rho_{\text{thresh}})}{\epsilon_1} \right), \\ Y_2 &\approx \frac{1}{2} \left(1 + \frac{\Delta(\text{Enc}[I_{s_i}] - \gamma_{\text{thresh}})}{\epsilon_2} \right), \end{aligned} \quad (54)$$

The computations Y_1 and Y_2 involve two checks combined using a logical AND operation to produce the final binary output Y :

$$Y = (Y_1 \geq 0.5) \wedge (Y_2 \geq 0.5), \quad (55)$$

which can be written as:

$$Y = \begin{cases} 1 & \text{if } Y_1 \geq 0.5 \text{ and } Y_2 \geq 0.5, \\ 0 & \text{otherwise.} \end{cases} \quad (56)$$

Since δ' is small, the linear approximations are valid when $\Delta(\text{Enc}[B_{l_i}] - \rho_{\text{thresh}})$ and $\Delta(\text{Enc}[I_{s_i}] - \gamma_{\text{thresh}})$ are close to 0. Consequently, Y_1 and Y_2 are close to 1 when the encrypted values are within their respective thresholds. Thus, the logical AND operation ensures that Y is 1 only if both $Y_1 \geq 0.5$ and $Y_2 \geq 0.5$. This implies that the final output Y will be 1 if the conditions are met, thus preserving the privacy of B_{l_i} and I_{s_i} by ensuring that only whether the values fall within the thresholds is revealed, not the actual values.

The privacy of TeraPRI is enhanced beyond CKKS homomorphic encryption by incorporating randomized frequency hopping into Algorithm 2. This technique rapidly shifts frequencies, making the communication channel harder to intercept and strengthening protection against threats such as jamming attacks. In Fig. 12, we observe that interference

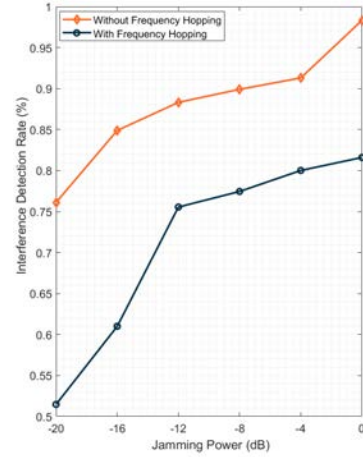


Fig. 12: Impact of varying jamming power on the interference detection rate.

detection rates increase with higher jamming power in both secure and non-secure scenarios. Despite the increase in the interference detection rate from 0.51 at -20 dB to 0.81 at 0 dB in secure scenarios, it still outperforms the non-secure scenario, where the interference detection rate ranges from 0.76 at -20 dB to 0.98 at 0 dB. As shown in Fig. 13, the latency

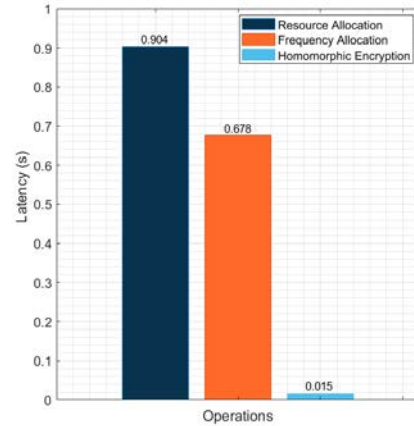


Fig. 13: Latency of various operations in the TeraPRI framework.

introduced by different operations in the TeraPRI framework is analyzed. The results indicate that while switching modes and performing encryption during resource allocation, as described in Algorithm 1, introduce some latency, their impact on overall system performance is minimal. Specifically, the latency for resource allocation, including mode switching, is 0.904 s. In comparison, frequency allocation incurs a latency of 0.678 s, while homomorphic encryption contributes a much lower latency of 0.015 s. These results demonstrate that although

encryption and mode switching slightly increase latency during resource allocation, the overall impact on task completion is negligible, and the security benefits of encryption outweigh the minor performance trade-off.

V. CONCLUSION

In conclusion, this paper introduced TeraPRI, a novel framework for homomorphic THz-empowered joint wireless power and information transfer with privacy preservation for 6G-autonomous vehicles. TeraPRI implemented a dual-mode adaptive resource allocation approach to coordinate the joint wireless power and information transfer, dynamically switching between HaT-mode and TaH-mode to meet end-user demands. Additionally, a selective CKKS homomorphic encryption technique with lightweight thresholding was designed to enable the MEC to securely allocate THz sub-channels while enhancing security through randomized frequency hopping. Performance evaluation shows that TeraPRI enhances wireless power transfer and information transmission, outperforming benchmarks in energy efficiency, success rates, and interference robustness. Its adaptive mechanisms ensure reliable operation across extended distances and multiple frequency hops, validating its effectiveness in the THz spectrum. This study primarily focused on line-of-sight communication to evaluate TeraPRI's performance. Future work will address non-line-of-sight (NLoS) challenges using Intelligent Reflecting Surfaces (IRS) to create virtual LoS paths, enhancing efficiency and reliability. Furthermore, AI-driven techniques will be explored for dynamic channel prediction, frequency optimization, and resource allocation to improve real-time adaptability, ensure fair resource distribution, and optimize THz spectrum utilization for end-user nodes at varying distances.

ACKNOWLEDGMENTS

This work was supported in part by the JSPS KAKENHI under Grants 23K11072, and in part by the Japan International Cooperation Agency (JICA) Long-term Scholarship under the SDGs Global Leadership Program.

REFERENCES

- [1] G. Chen, J. Wu, W. Yang, A. K. Bashir, G. Li, and M. Hammoudeh, "Leveraging graph convolutional-LSTM for energy-efficient caching in blockchain-based green IoT," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1154–1164, 2021.
- [2] E. L. C. Macedo, F. C. Delicato, L. F. M. de Moraes, and G. Fortino, "Assigning trust to devices in the context of consumer IoT applications," *IEEE Consumer Electronics Magazine*, vol. 13, no. 1, pp. 12–21, 2024.
- [3] C. K. Wu, C.-T. Cheng, Y. Uwate, G. Chen, S. Mumtaz, and K. F. Tsang, "State-of-the-art and research opportunities for next-generation consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 937–948, 2023.
- [4] S. S. Tripathy, S. Bebortta, M. I. u. Haque, Y. Zhu, and T. R. Gadekallu, "Toward multi-modal deep learning-assisted task offloading for consumer electronic devices over an IoT-fog architecture," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1656–1663, 2024.
- [5] A. Taneja and S. Rani, "A novel energy conservation scheme for IoT-based wireless networks: A use case of E-commerce systems for consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1648–1655, 2024.
- [6] C. Gao, T.-H. Lin, N. Li, D. Jin, and Y. Li, "Cross-platform item recommendation for online social E-commerce," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 2, pp. 1351–1364, 2023.
- [7] K. T. Pauu, H. Xu, and B. Wang, "A novel UAV charging scheme for minimizing coverage breach in rechargeable sensor networks," in *Green, Pervasive, and Cloud Computing: 15th International Conference, GPC 2020, Xi'an, China, November 13–15, 2020, Proceedings 15*, 2020, pp. 347–361.
- [8] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE communications surveys & tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.
- [9] A. Shafie, N. Yang, C. Han, J. M. Jornet, M. Juntti, and T. Kürner, "Terahertz communications for 6G and beyond wireless networks: Challenges, key advancements, and opportunities," *IEEE Network*, vol. 37, no. 3, pp. 162–169, 2022.
- [10] O. A. Amodu, S. A. Busari, and M. Othman, "Physical layer aspects of terahertz-enabled UAV communications: Challenges and opportunities," *Vehicular Communications*, vol. 38, p. 100540, 2022.
- [11] I. F. Akyildiz, C. Han, Z. Hu, S. Nie, and J. M. Jornet, "Terahertz band communication: An old problem revisited and research directions for the next decade," *IEEE Transactions on Communications*, vol. 70, no. 6, pp. 4250–4285, 2022.
- [12] C. Chaccour, M. N. Soorki, W. Saad, M. Bennis, P. Popovski, and M. Debbah, "Seven defining features of terahertz (THz) wireless systems: A fellowship of communication and sensing," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 967–993, 2022.
- [13] K. T. Pauu, J. Wu, Y. Fan, Q. Pan, and M.-V. Maka, "Differential privacy and blockchain-empowered decentralized graph federated learning-enabled UAVs for disaster response," *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 20930–20947, 2024.
- [14] K. T. Pauu, Q. Pan, J. Wu, A. K. Bashir, M. Omar *et al.*, "Irs-aided federated learning with dynamic differential privacy for UAVs in emergency response," *IEEE Internet of Things Magazine*, vol. 7, no. 4, pp. 108–115, 2024.
- [15] F. Zhou, R. Q. Hu, Z. Li, and Y. Wang, "Mobile edge computing in unmanned aerial vehicle networks," *IEEE Wireless Communications*, vol. 27, no. 1, pp. 140–146, 2020.
- [16] Y. Luo, Y. Wang, Y. Lei, C. Wang, D. Zhang, and W. Ding, "Decentralized user allocation and dynamic service for multi-UAV-enabled MEC system," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 1306–1321, 2024.
- [17] Y. K. Tun, K. T. Kim, L. Zou, Z. Han, G. Dán, and C. S. Hong, "Collaborative computing services at ground, air, and space: An optimization approach," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 1491–1496, 2024.
- [18] D. S. Lakew, A.-T. Tran, N.-N. Dao, and S. Cho, "Intelligent Self-Optimization for Task offloading in LEO-MEC-Assisted Energy-Harvesting-UAV Systems," *IEEE Transactions on Network Science and Engineering*, pp. 1–14, 2024.
- [19] Y. M. Park, S. S. Hassan, Y. K. Tun, Z. Han, and C. S. Hong, "Joint trajectory and resource optimization of MEC-Assisted UAVs in sub-thz networks: A resources-based multi-agent proximal policy optimization drl with attention mechanism," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 2, pp. 2003–2016, 2024.
- [20] L. Xu, M. Chen, M. Chen, Z. Yang, C. Chaccour, W. Saad, and C. S. Hong, "Joint location, bandwidth and power optimization for THz-enabled UAV communications," *IEEE Communications Letters*, vol. 25, no. 6, pp. 1984–1988, 2021.
- [21] J. Liu, X. Zhao, P. Qin, S. Geng, Z. Chen, and H. Zhou, "Learning-based multi-UAV assisted data acquisition and computation for information freshness in wpt enabled space-air-ground plot," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 1, pp. 48–63, 2024.
- [22] Q. Zhang, Y. Luo, H. Jiang, and K. Zhang, "Aerial edge computing: A survey," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14357–14374, 2023.
- [23] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—A key technology towards 5G," *ETSI white paper*, vol. 11, no. 11, pp. 1–16, 2015.
- [24] A. Samanta and J. Tang, "Dyme: Dynamic microservice scheduling in edge computing enabled IoT," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6164–6174, 2020.
- [25] F. Zhou, Y. Wu, H. Sun, and Z. Chu, "UAV-enabled mobile edge computing: Offloading optimization and trajectory design," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.
- [26] Y. K. Tun, G. Dán, Y. M. Park, and C. S. Hong, "Joint UAV deployment and resource allocation in thz-assisted MEC-enabled integrated space-air-ground networks," *arXiv preprint arXiv:2401.11419*, 2024.

- [27] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 1, pp. 418–428, 2014.
- [28] Z. Rong, M. S. Leeson, M. D. Higgins, and Y. Lu, "Simultaneous wireless information and power transfer for AF relaying nanonetworks in the terahertz band," *Nano communication networks*, vol. 14, pp. 1–8, 2017.
- [29] A. Hanif and M. Doroslovački, "Simultaneous terahertz imaging with information and power transfer (STIIPT)," *IEEE Journal of Selected Topics in Signal Processing*, vol. 17, no. 4, pp. 806–818, 2023.
- [30] Y. Pan, K. Wang, C. Pan, H. Zhu, and J. Wang, "Self-sustainable reconfigurable intelligent surface aided simultaneous terahertz information and power transfer (STIPT)," *IEEE Transactions on Wireless Communications*, vol. 21, no. 7, pp. 5420–5434, 2022.
- [31] C. Jeong and S. H. Chae, "Simultaneous wireless information and power transfer for multiuser UAV-enabled IoT networks," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8044–8055, 2021.
- [32] Q. Pan, J. Wu, A. K. Bashir, J. Li, W. Yang, and Y. D. Al-Otaibi, "Joint protection of energy security and information privacy for energy harvesting: An incentive federated learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3473–3483, 2022.
- [33] X. Lai, L. Fan, X. Lei, Y. Deng, G. K. Karagiannidis, and A. Nalanthan, "Secure mobile edge computing networks in the presence of multiple eavesdroppers," *IEEE Transactions on Communications*, vol. 70, no. 1, pp. 500–513, 2022.
- [34] M. M. Azari, S. Solanki, S. Chatzinotas, and M. Bennis, "THz-empowered UAVs in 6G: Opportunities, challenges, and trade-offs," *IEEE Communications Magazine*, vol. 60, no. 5, pp. 24–30, 2022.
- [35] A. Alali, D. B. Rawat, and C. Liu, "Trajectory and power optimization in sub-THz band for UAV communications," in *ICC 2022-IEEE International Conference on Communications*, 2022, pp. 1–6.
- [36] Y. Zhou, C. Pan, P. L. Yeoh, K. Wang, M. Elkashlan, B. Vucetic, and Y. Li, "Secure communications for UAV-enabled mobile edge computing systems," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 376–388, 2020.
- [37] X. He, R. Jin, and H. Dai, "Physical-layer assisted secure offloading in mobile-edge computing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 4054–4066, 2020.
- [38] R. Singh and D. Sicker, "THz communications-a boon and/or bane for security, privacy, and national security," in *TPRC48: The 48th Research Conference on Communication, Information and Internet Policy*, 2020.
- [39] D. Srinivasan, M. Premkumar, S. D. Nivethika, P. Dhilipkumar, S. Parameswari, and M. K. Chowdary, "A review on wideband high-gain low-THz antennas for wireless applications," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2024, pp. 1644–1648.
- [40] J. M. Eckhardt, C. E. Reinhardt, T. Doeker, E. A. Jorswieck, and T. Kürner, "Capacity analysis for time-variant MIMO channel measurements at low THz frequencies," in *2023 17th European Conference on Antennas and Propagation (EuCAP)*, 2023, pp. 1–5.
- [41] R. Du, F. Norouzian, E. Marchetti, B. Willetts, M. Gashinova, and M. Cherniakov, "Characterisation of attenuation by sand in low-THz band," in *2017 IEEE Radar Conference (RadarConf)*, 2017, pp. 0294–0297.
- [42] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3211–3221, 2011.
- [43] I. E. Gordon, L. S. Rothman, R. Hargreaves, R. Hashemi, E. V. Karlovets, F. Skinner, E. K. Conway, C. Hill, R. V. Kochanov, Y. Tan *et al.*, "The HITRAN2020 molecular spectroscopic database," *Journal of quantitative spectroscopy and radiative transfer*, vol. 277, p. 107949, 2022.
- [44] P. Sen and J. M. Jornet, "Experimental demonstration of ultra-broadband wireless communications at true terahertz frequencies," in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2019, pp. 1–5.
- [45] A. Papoulis and S. Unnikrishna Pillai, *Probability, random variables and stochastic processes*, 2002.
- [46] J. M. Jornet and I. F. Akyildiz, "Femtosecond-long pulse-based modulation for terahertz band communication in nanonetworks," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1742–1754, 2014.
- [47] R. W. Doran, "The gray code," *Citeseer, Tech. Rep.*, 2007.
- [48] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *Advances in Cryptology-ASIACRYPT 2017: 23rd International Conference on the Theory and*
- Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I 23, 2017*, pp. 409–437.