scientific reports

Check for updates

OPEN

A novel 6G-oriented secure bidirectional key exchange scheme based on graphene-assisted terahertz physical layer

Yashar Salami[1,2]✉, Yaser Pourshadlou[3], Mohammad Bagher Karimi[4] & Nooshin Allahbakhshi[5]

This paper proposes a graphene-assisted bidirectional key exchange protocol that integrates terahertz (THz) physical-layer modulation with the Diffie–Hellman (DH) cryptographic framework, addressing a critical gap in secure session establishment over open wireless channels. While prior graphene-based antennas, metasurfaces, and sensing platforms have primarily focused on enhancing electromagnetic performance, secure bidirectional key exchange at the physical layer has remained largely unexplored. The proposed architecture employs a dual-layer graphene metasurface operating at 1 THz, where tunable surface conductivity enables binary phase-shift keying (BPSK) modulation for concurrent transmission. Authenticated public parameters, identity bindings, and freshness values are embedded within the THz waveform, and a shared secret is derived through DH computation. Simulation results over an SNR range of 0–30 dB demonstrate reliable demodulation under AWGN, coherent current density distributions across graphene layers, and consistent key agreement between communicating parties. The bit error rate (BER) decreases sharply between 5 and 10 dB, reaches the 10^{-3} regime at 10 dB, and converges to zero within simulation resolution for SNR values of 15 dB and above, indicating reliable parameter recovery under practical noise conditions. An informal security analysis conducted under the Dolev–Yao adversarial model, together with a comparative assessment of the defined security requirements, indicates that the proposed scheme demonstrates resistance against both passive and active attacks. Furthermore, the comparative evaluation suggests that the proposed framework more comprehensively satisfies the considered security requirements relative to existing schemes. These findings establish the feasibility of graphene-assisted secure key exchange and provide a structured foundation for secure deployment of graphene-enabled terahertz communication systems, particularly within emerging 6G network architectures, as well as in IoT and biomedical applications.

Keywords Graphene, Key exchange, Secure, 6G

Graphene, a single-atom–thick sheet of carbon arranged in a hexagonal lattice, is the first truly two-dimensional material[1]. Isolated from graphite in 2004 by Geim and Novoselov through mechanical exfoliation[2,3]—a discovery that earned the 2010 Nobel Prize in Physics—it transformed our understanding of nanoscale materials and opened pathways in electronics, medicine, and energy[4]. With its atomic thickness, ultrafast electron mobility, and remarkable mechanical flexibility, graphene remains one of the most significant materials for both fundamental research and advanced applications[5].

Graphene exhibits exceptional properties, including ultrahigh electrical conductivity with massless Dirac fermions[6,6], thermal conductivity up to 5000 W m^{-1} K^{-1}, a Young's modulus near 1 TPa, and optical transparency of ~ 98% [8,]9]. These attributes make it a multifunctional material for next-generation electronics, energy systems,

[1]Department of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran. [2]Faculty of Computer and Information Technologies, Cappadocia University, Nevsehir, Turkey. [3]Department of Electrical and Electronics Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran. [4]Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran. [5]Department of Computer and Information Technology Engineering, Khoy Branch, Islamic Azad University, Khoy, Iran. ✉email: yashar.salami@kapadokya.edu.tr

biosensors, and biomedical devices, while its ability to retain such performance at nano- and microscale dimensions continues to drive innovative applications [10].

Commercializing graphene requires overcoming production challenges, and several synthesis methods have been developed[11]. Mechanical exfoliation produces the highest-quality graphene but is limited to laboratory use due to poor scalability[12]. For industrial-scale fabrication, chemical vapor deposition (CVD) and reduction of graphene oxide are the most common approaches: CVD enables uniform, wafer-scale films for advanced electronics[13], while graphene oxide reduction offers a simpler and cheaper route, though with reduced performance[14]. Current research focuses on refining these methods to improve quality, scalability, and cost-efficiency, thereby accelerating graphene's widespread adoption[15]. Beyond materials engineering, graphene is increasingly explored for secure communication in emerging domains such as 6G networks, the Internet of Things (IoT), and biomedical systems[16–18]. Its high conductivity, tunable Fermi level, and ultrafast signal modulation make it uniquely suited for THz physical-layer devices. However, a significant research gap persists: the absence of secure bidirectional key exchange protocols at the physical layer. Without such mechanisms, graphene-based systems—including THz antennas, biosensors, and smart-grid devices—remain vulnerable to interception and tampering, especially in sensitive contexts like remote healthcare, critical infrastructure, and quantum communication. This paper addresses this gap by proposing a novel bidirectional secure key exchange protocol that integrates graphene-enabled THz physical-layer modulation with the DH algorithm, ensuring robust, noise-resilient, and secure data transmission.

Motivation

Graphene has demonstrated remarkable potential across diverse domains, including THz antennas, wearable sensors, energy harvesting systems, and biomedical devices, owing to its superior electrical conductivity, mechanical strength, and tunable properties. These advances highlight graphene as a foundational material for next-generation technologies such as 6G, IoT, and secure biomedical communications. However, as emphasized in the related work and research gap analysis, a critical limitation persists: the absence of a secure bidirectional key exchange mechanism at the physical layer. Without such protocols, graphene-enabled communication systems remain exposed to interception, tampering, and unauthorized access, particularly in sensitive applications. This unresolved challenge forms the core motivation of this study, driving the need to design a graphene-based framework that ensures secure, noise-resilient, and efficient key exchange.

Contribution

The main contributions of this paper can be summarized as follows:

- Integrated Physical-Layer Modulation and Cryptographic Key Exchange:
- We introduce a bidirectional session establishment framework that integrates graphene-based THz physical-layer modulation with the DH scheme. This dual-layer architecture unifies electromagnetic signal modeling and cryptographic key exchange within a coherent transmission framework, enabling authenticated session establishment over a THz channel.
- Graphene-Assisted Concurrent Transmission Architecture:
- By exploiting the tunable surface conductivity of dual-layer graphene metasurfaces, the proposed protocol enables concurrent two-way transmission of authenticated DH parameters using BPSK modulation under the assumption of ideal isolation. This material-assisted design extends prior graphene-enabled communication studies beyond purely electromagnetic optimisation toward the realisation of integrated secure protocols.
- Explicit Delineation Between Cryptographic Security and Physical-Layer Robustness:
- While the confidentiality of the established session key remains grounded in the computational hardness of the discrete logarithm problem underlying DH, the physical layer is positioned as a transmission and robustness component that supports reliable authenticated parameter exchange under THz propagation conditions, rather than as an independent secrecy mechanism.
- Informal Security Analysis and Threat-Model Evaluation:A formally defined Network Model and Threat Model under the Dolev–Yao adversarial framework are incorporated. An expanded Informal Security Analysis evaluates confidentiality, integrity, freshness, and key agreement properties within the explicitly defined adversarial assumptions.
- Structured Security Requirements Assessment:A comparative evaluation against predefined security requirements is conducted to assess the proposed framework's compliance with existing approaches. The analysis clarifies the scope and boundaries of the security guarantees provided.
- Comprehensive Simulation and Transmission Performance Validation:MATLAB-based simulations are conducted to evaluate modulation/demodulation behaviour, current–density distributions across graphene layers, reconstructed parameter consistency, and bit error rate (BER) under AWGN conditions. The results demonstrate reliable parameter recovery and stable key agreement across the evaluated SNR range (0–30 dB), with BER entering the 10^{-3} regime at 10 dB and approaching zero within simulation resolution for SNR values of 15 dB and above.

Paper organization

The remainder of this paper is organized as follows: Sect. 2 reviews related work on graphene-enabled antennas, metasurfaces, and sensors, and identifies the research gap in secure bidirectional key exchange at the physical layer. Section 3 provides the Network Model, assumptions, Threat Model, and Problem Statement. Section 4 presents the proposed bidirectional key exchange protocol that integrates graphene-based THz physical-layer modulation with the DH framework. The system model, symbols, and protocol phases are described in detail. Section 5 discusses the simulation setup, assumptions, and parameters, followed by experimental results and

performance evaluation. Key aspects, such as modulation/demodulation under noise, current density stability, reconstructed keys, and BER analysis, are examined and highlight the study's limitations. Section 6 concludes the paper by summarising the contributions and the potential of the proposed protocol for deployment in secure communication scenarios such as IoT, biomedical systems, and smart grids.

Related work

This section presents the related work and highlights the existing research gap.

Bouzid et al. (2024) This work presents a 300 GHz rectangular graphene–LCP microstrip patch antenna array enhanced by photonic band-gap substrates for ultra-broadband THz applications. However, it does not propose any secure two-way key exchange protocol or establish an encrypted communication channel between transmitter and receiver[19]. Kong et al. (2024) This review analyzes flexible wearable graphene sensors, detailing their sensing mechanisms, material properties, and fabrication challenges. It overlooks any design or implementation of a bidirectional key exchange or security framework for encrypted data transmission[20]. Babu et al. (2024) The authors design a polarization-insensitive bifunctional graphene–graphite THz metasurface absorber for sensing and electromagnetic shielding with high bandwidth and sensitivity. No mechanism for secure key exchange or encrypted channel establishment over the metasurface is considered[21]. Shen et al. (2024) A graphene textile composite sensor–based wearable knee rehabilitation system is implemented and validated using an improved XGBoost algorithm for angle estimation. The study does not incorporate any secure two-way key exchange or encrypted link between the wearable device and backend[22]. Dhadwal et al. (2025) A dual-band 5G graphene–RT-duroid microstrip patch antenna with complementary metamaterial resonators is optimized for gain and bandwidth. There is no discussion of secure key exchange or mutual authentication over the wireless link[23]. Lazaro et al. (2025) Non-cloneable chipless RFID tags using laser-induced graphene on cork are proposed to prevent product counterfeiting via unique spectral signatures. The paper does not address secure key negotiation or encrypted communication between the RFID tag and reader[24]. Rai et al. (2025) A compact, machine-learning-tuned hexagonal graphene THz antenna supports three frequency bands with high impedance bandwidth. No secure key exchange protocol or physical-layer security mechanism is implemented for data encryption[25]. Althuwayb et al. (2024) A 2×2 spiral-shaped graphene-assisted terahertz MIMO antenna is developed for high-gain biomedical and WBAN communications. The design omits any two-way key exchange or secure channel establishment for protecting medical data[26]. Shukla et al. (2025) An aluminum–$BiFeO_3$ plasmonic device enhanced with graphene and other 2D materials is analyzed for near-infrared sensing via transfer-matrix modeling. The study does not propose a cryptographic key exchange or secure data link for the sensed signals[27]. Narayanan et al. (2024) A hybrid energy-harvesting framework integrates multiple sources with a graphene-based supercapacitor for 6G and smart-grid networks. No protocol for secure key exchange or encrypted communication between system components is introduced[28]. Singh et al. (2025) A graphene-based nano-antenna for THz wireless communications is designed on GaAs substrate to achieve high gain and broad bandwidth. There is no consideration of physical-layer key exchange or channel encryption to secure the transmitted data[29]. Oh et al. (2024) A coplanar waveguide using a graphene–silver nanowire/PET composite is fabricated, showing low RF loss and high bending stability for X-band wearables. The work lacks any mechanism for secure key exchange or two-party authentication over the flexible link[30]. Singh et al. (2024) Dual-substrate graphene patch antennas optimized via genetic algorithms are compared for THz spectroscopy and 6G applications. No secure key negotiation or encrypted channel is provided in the antenna design methodology[31]. García-Pineda et al. (2024) A PRISMA-based literature review charts research trajectories of graphene antennas in wireless communications, highlighting trends and performance metrics. Despite comprehensive coverage, no secure two-way key exchange protocols or encryption frameworks are surveyed[32]. Jarchi et al. (2024) A series graphene transmission-line amplitude modulator for low-THz band is designed and analyzed via ABCD-matrix and full-wave simulations. The modulator design does not incorporate any key exchange or means to establish a secure transmission channel[33]. Cali et al. (2024) An experimental platform implements molecule-shift keying using graphene quantum dots for enhanced molecular communication. No cryptographic key exchange or encrypted link between transmitter and fluorescence-based receiver is implemented[34].Ren et al. (2025) A graphene quantum-capacitor PUF generates unique RF fingerprints for anti-counterfeiting labels via near-field interrogation. The PUF outputs are digitized into keys, but no two-way key exchange protocol or secure wireless channel is developed[35]. Khani et al. (2024) An ultrathin metamaterial with patterned graphene rings and ribbons is proposed for multiband THz wave coupling. The coupling analysis omits any secure key exchange or encryption scheme for the transmitted waves[36]. Xuan et al. (2024) A flexible 920 MHz graphene antenna sensor monitors humidity wirelessly, achieving high sensitivity and 100 m range for IoT. The system does not include any protocol for key exchange or secure channel encryption between sensor and receiver[37]. Asaad et al. (2024) A compact 2×2 graphene-based THz MIMO antenna is evaluated for 6G, demonstrating low ECC and high efficiency. The paper does not propose any secure key exchange mechanism or encrypted data link for the MIMO channels[38]. Chude-Okonkwo et al. (2024) A CRISPR-enabled graphene FET bio-cyber interface model is formulated via differential equations for in vivo monitoring. No cryptographic key exchange or secure data channel is considered in the bio-cyber communication framework[39].Sakai et al. (2024) A deformable 3D graphene electrode array ("brain-on-a-chip") records spatiotemporal neuronal signals to study network dynamics. There is no mechanism for secure key exchange or encryption of the neural data transmitted off-chip[40]. Srivastava et al. (2024) A high-gain circularly polarized dielectric resonator antenna using silicon/graphene materials is designed for 6G IoT and biosensing. The design does not address secure key exchange or encrypted channel creation for sensitive biosensing transmissions[41]. Upender et al. (2024) Ultrathin VO_2–graphene films are introduced for wideband switchable THz absorption with tunable performance up to 8.75 THz. No secure key exchange protocol or encrypted communication channel is integrated into the absorber application[42]. Farzin et al. (2024) develop a graphene-enabled polarization modulation metasurface supporting multi-channel THz encryption via DRPE-

based wave encoding. Although the approach enhances waveform-level confidentiality through polarization manipulation, it does not incorporate a secure bidirectional key agreement protocol or mutual session establishment mechanism. As a result, physical-layer encryption is achieved without integrating cryptographic key negotiation between transmitter and receiver[43].De Feo et al. develop a practical post-quantum isogeny-based key exchange with formal security guarantees. However, no physical-layer integration or THz communication framework is considered[44]. Xiao et al. (2025) develop a space–time coding metasurface platform for secure wireless BCI communication using harmonic-encrypted beams. Although the system enhances physical-layer confidentiality, it does not implement cryptographic key exchange or authenticated session establishment between parties[45]. Ning et al. (2025) develop a programmable nonlinear diffractive neural network with fast ReLU activation using metasurfaces. While the system advances wave-based computation and real-time processing, it does not incorporate secure key exchange or physical-layer communication security mechanisms[46].Xiao et al. (2025) develop a mechanically programmable diffractive neural network using Pancharatnam–Berry phase metasurfaces for energy-efficient wave-based computation. Although the architecture advances reconfigurable optical processing, it does not address secure key exchange or physical-layer communication security[47].Yao et al. (2026) develop a nonlocal meta-lens for intensity-asymmetric wavefront shaping and directional nonlinear focusing. While advancing nonreciprocal photonic control, the work does not address secure key exchange or encrypted communication at the physical layer[48]. Zhang et al. (2026) explore non-local bound states in the continuum for high-precision nanoscale alignment in semiconductor systems. While advancing photonic resonance engineering, the work does not incorporate secure key exchange or physical-layer communication security architectures[49]. As highlighted in Table 1, existing research on graphene-enabled technologies has largely concentrated on improving electromagnetic performance in antennas, metasurfaces, sensors, and absorbers, while neglecting the design of secure key exchange mechanisms at the physical layer. The absence of secure bidirectional key exchange exposes graphene-based communication devices to interception, tampering, and unauthorized access, especially in critical domains such as remote medical monitoring, smart grids, and quantum communication. This unresolved challenge in physical-layer security has become a key barrier that prevents the widespread adoption and expansion of graphene-based systems in real-world environments. To overcome this limitation, this paper proposes a novel bidirectional secure key exchange protocol that integrates graphene-based terahertz physical-layer modulation with the DH key exchange, ensuring robust, noise-resilient, and secure data transmission.

Research gap

This research gap, particularly in the domain of physical-layer security, poses a critical barrier to the reliable expansion and deployment of graphene-enabled technologies. Without secure key-exchange protocols, data transmitted through graphene-based devices—such as THz antennas or biosensors—remains vulnerable to interception, tampering, or unauthorized access. This vulnerability is especially pronounced in sensitive use cases like remote medical monitoring, smart grids, and quantum communication, all of which demand strong protection and secure bidirectional key exchange. The lack of attention to this vital aspect has thus limited the adoption of graphene technologies in real-world environments and hindered the full realization of their potential for secure and efficient communication. This paper proposes a novel bidirectional secure key exchange protocol that integrates graphene-based terahertz physical-layer modulation with the DH key exchange, thereby enabling robust, noise-resilient, and secure data transmission.

Network model

This section presents the network model, underlying assumptions, threat model, and problem statement.

The network architecture is structured as a three-tier hierarchical framework comprising the Cloud, Fog, and End layers. At the top tier, the Cloud operates as the central authority and global coordination entity. Equipped with substantial computational resources and scalable infrastructure, it defines system-wide security policies, manages long-term credentials, and orchestrates interactions across subordinate layers. Owing to its centralised governance and superior processing capacity, the Cloud serves as the principal trust anchor of the architecture. The intermediate Fog layer is geographically distributed and positioned closer to end users to reduce latency and support localised processing. Although less resource-intensive than the Cloud, Fog nodes perform authentication and security verification while maintaining mutually authenticated trust relationships with the Cloud. Communication between these layers is assumed to be secure and integrity-protected. To reinforce distributed trust, the Fog layer integrates with a blockchain infrastructure that records security events, manages credential lifecycles, and registers temporary keys, thereby enhancing transparency and tamper resistance. At the lowest tier, the End layer comprises RSUs, access points, and user devices communicating over an open wireless medium. In contrast to the upper tiers, this domain operates without pre-established trust relationships. Entities do not share prior credentials or mutual authentication, and wireless transmissions are inherently exposed to adversarial actions, including eavesdropping, replay, modification, and man-in-the-middle attacks. Accordingly, secure key exchange must be established before any data transmission can be trusted. In this context, developing a graphene-assisted terahertz physical-layer key-exchange mechanism represents a central challenge for the End layer. Figure 1 illustrates the overall network model.

Assumptions

The network model assumptions are defined as follows:

- Cloud–Fog communication is assumed to operate over secure, mutually authenticated links, ensuring the confidentiality and integrity of exchanged control and management messages.

No	Focus of work	Limitation
Bouzid et al.	300 GHz graphene–LCP antenna array with photonic band-gap substrates for THz applications	No mechanism for secure bidirectional key exchange; transmitted data remains vulnerable to interception
Kong et al.	Review of wearable graphene sensors, material properties, and fabrication challenges	Lacks any physical-layer security or key-exchange framework; unsuitable for secure biomedical IoT use
Babu et al.	Graphene–graphite THz metasurface absorber for sensing and shielding	Focuses only on EM performance; no secure channel establishment to prevent tampering or unauthorized access
Shen et al.	Wearable graphene textile sensor for knee rehabilitation	Omits bidirectional secure key exchange; sensitive medical data exposed to interception risks
Dhadwal et al.	Dual-band 5G graphene–RT-duroid patch antenna with metamaterials	No physical-layer security or mutual authentication; limits deployment in secure 5G/6G networks
Lazaro et al.	Non-cloneable chipless RFID tags using laser-induced graphene	Provides uniqueness but no secure data exchange; RFID data remains accessible to attackers
Rai et al.	ML-tuned graphene THz antenna supporting multiband operations	High bandwidth achieved but no secure key negotiation; unsuitable for sensitive IoT/6G communications
Althuwayb et al.	2 × 2 graphene-assisted THz MIMO antenna for biomedical/WBAN	Omits secure key exchange; critical risk for medical data confidentiality
Shukla et al.	Graphene-enhanced plasmonic device for near-IR sensing	No secure key exchange; sensed signals remain unprotected against tampering
Narayanan et al.	Energy-harvesting framework with graphene supercapacitor for 6G/smart grids	Secure key exchange not considered; vulnerable to unauthorized access in smart-grid integration
Singh et al.	Graphene nano-antenna for THz wireless on GaAs	No physical-layer key exchange; transmitted THz signals unprotected
Oh et al.	Graphene–silver nanowire CPW for flexible wearables	Secure two-way authentication missing; unsuitable for secure wearable communication
Singh et al.	Dual-substrate graphene patch antennas optimized via GA	No secure key-exchange protocol; limited use in secure spectroscopy/6G
García-Pineda et al.	PRISMA-based review of graphene antennas in wireless communications	Omits secure, bidirectional key exchange protocols from the survey
Jarchi et al.	Graphene transmission-line amplitude modulator	No secure transmission or key agreement; leaves modulation open to interception
Cali et al.	Molecular communication using graphene quantum dots	No secure key exchange; the transmitter–receiver link is exposed to unauthorised access
Ren et al.	Graphene quantum-capacitor PUF for anti-counterfeiting	Generates unique fingerprints but lacks two-way key exchange
Khani et al.	Ultrathin graphene metamaterial for multiband THz coupling	No secure key exchange; data transmission vulnerable to eavesdropping
Xuan et al.	Flexible graphene antenna sensor for humidity/IoT	No secure channel or key-exchange protocol; unsuitable for protecting IoT data
Asaad et al.	Compact 2 × 2 graphene-based THz MIMO antenna for 6G	No secure key exchange; weakens applicability in 6G security-sensitive scenarios
Chude-Okonkwo et al	CRISPR-enabled graphene FET bio-cyber interface	Bio-cyber signals transmitted without secure key exchange; vulnerable in monitoring
Sakai et al.	3D graphene electrode array for neuronal signal recording	No secure key exchange; neural data unprotected during transmission
Srivastava et al.	Graphene–silicon circularly polarized dielectric resonator antenna for 6G IoT/biosensing	Secure data exchange not addressed; biosensing transmissions vulnerable
Upender et al.	VO_2–graphene films for wideband switchable THz absorption	Omits secure key-exchange mechanism; THz absorber system exposed to attacks
Farzin et al.	Graphene polarization-modulation metasurface for multi-channel THz encryption	No secure bidirectional key exchange or session-based key negotiation mechanism
De Feo et al.	Practical post-quantum isogeny-based key exchange with formal session-key and IND-CPA security guarantees	Does not address physical-layer implementation, waveform-based modulation, or integration with graphene-enabled THz communication systems
Xiao et al.	Secure wireless BCI using space–time coding metasurface and harmonic beam encryption	No cryptographic key exchange or session-oriented key establishment mechanism
Ning et al.	Programmable nonlinear diffractive neural network with metasurface-based ReLU activation	No secure key exchange or encrypted communication framework considered
Xiao et al.	PB-phase mechanically programmable diffractive neural network	No secure key exchange or physical-layer communication security framework
Yao et al.	Nonlocal meta-lens for asymmetric wavefront shaping	No secure key exchange or encrypted communication framework considered
Zhang et al.	Non-local BIC-based nanoscale alignment for semiconductor manufacturing	Does not incorporate cryptographic key exchange or secure communication protocols

Table 1. Summary of related work.

- Inter-Fog communication, when required, is protected at the infrastructure level using authenticated, integrity-preserving mechanisms.
- End-layer communication occurs over an open wireless medium and is considered inherently insecure, with no prior guarantees of confidentiality or integrity.
- Under the Dolev–Yao adversarial model, an attacker is assumed to have full control over End-layer channels, including the ability to intercept, replay, inject, modify, or suppress messages.
- The graphene-assisted terahertz key exchange link is part of this adversarial wireless domain and must therefore be designed to resist both active and passive channel manipulation.
- It is assumed that all devices in the End layer maintain loosely synchronised clocks, enabling the use of timestamps and bounded delay constraints to detect and discard stale or replayed messages.

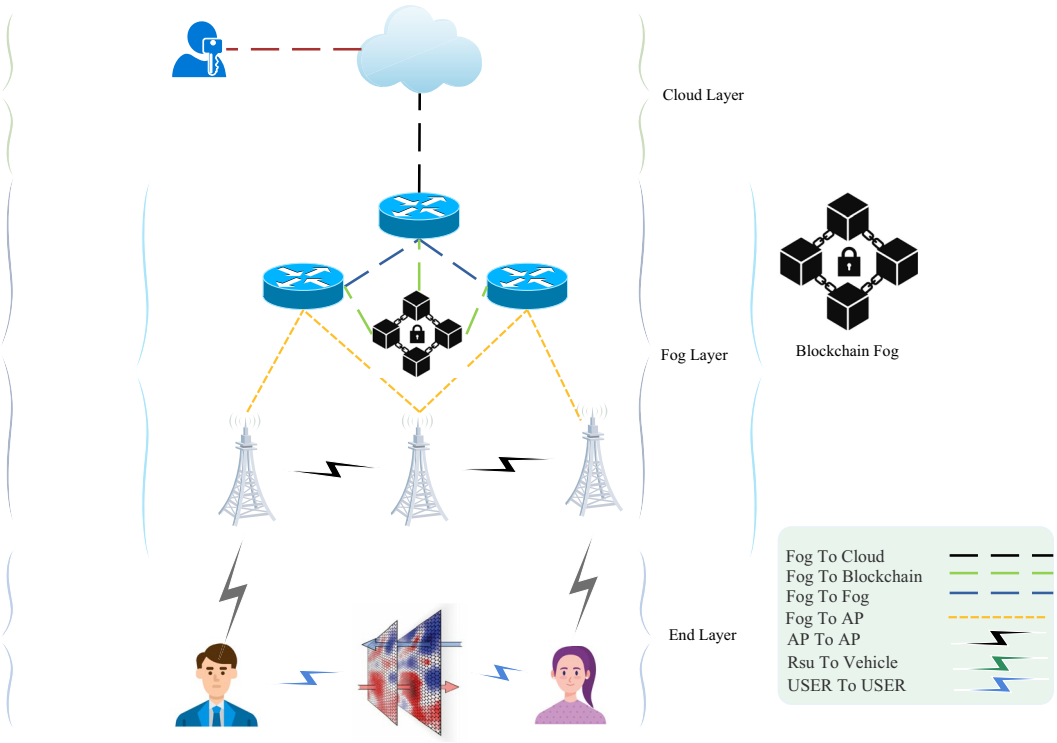

Fig. 1. Network model.

Model thread

Under the defined communication assumptions, the End layer is modelled as a fully adversarial wireless domain consistent with the Dolev–Yao (D–Y) framework.

In this layer, the attacker is assumed to have complete control over the THz communication channel. Specifically, the adversary can:

- Intercept all transmitted messages between End-layer entities;
- Replay previously captured transmissions.
- Modify, delay, or suppress legitimate communications;
- Perform man-in-the-middle (MITM) attacks during the key exchange phase.

The attacker is computationally bounded and cannot break the underlying hardness assumptions of the key exchange mechanism. However, no restrictions are imposed on its control of the wireless medium. Consequently, any message exchanged within the End layer—including those involved in the graphene-assisted terahertz key establishment process—is exposed to active and passive adversarial manipulation. Under this model, the central security objective is to enable two previously untrusted entities to establish a shared session key despite the adversary's full channel control. The key exchange protocol must therefore ensure resistance against replay, message injection, modification, and MITM attacks while guaranteeing freshness and agreement of the derived key.

Problem statement

In the proposed network model, a three-tier architecture, the End layer constitutes a zero-trust wireless domain where communicating entities share neither prior credentials nor established trust relationships. Unlike the Cloud and Fog tiers, which operate over authenticated and protected infrastructure links, the End layer relies on an open THz communication medium that offers no inherent guarantees of confidentiality, integrity, or authenticity. Under the Dolev–Yao adversarial model, the wireless channel is assumed to be fully controlled by an active attacker capable of intercepting, replaying, injecting, modifying, or suppressing protocol messages. In such an environment, the absence of an intrinsic secure key-exchange mechanism becomes a structural vulnerability: any attempt to initiate communication is exposed during the key establishment phase, where trust must be created from scratch. This vulnerability is amplified in safety–critical and mission-sensitive applications—including remote medical monitoring, smart energy infrastructures, and quantum-integrated communication systems—where secure and reliable bidirectional key establishment is a foundational requirement for system-level trust. The central problem addressed in this work is therefore the design of a graphene-assisted physical-layer key exchange mechanism that enables two previously untrusted entities to derive a shared session key over a fully adversarial THz wireless channel. Resolving this challenge is essential to elevate the End layer from an

inherently insecure broadcast environment to a communication domain capable of supporting trustworthy and resilient operation.

Proposed scheme

In this section, we propose a novel protocol that integrates the physical-layer modulation capabilities of graphene metasurfaces with the DH cryptographic framework. Operating at a THz frequency of 1 THz, the protocol leverages graphene's exceptional electrical conductivity and tunable Fermi level to enable secure, low-latency key exchange between two parties, Alice and Bob. The method is structured into five phases, ensuring both physical robustness and cryptographic security, making it suitable for applications in 6G networks, IoT, and biomedical communications. The integration of physical-layer modulation with DH also provides an additional entropy source, which significantly complicates eavesdropping attempts.

Symbol

Table 2 shows the symbols used in the proposed scheme.

Proposed phase

Phase 1: System Initialization.

In the initialization stage, Alice and Bob define a common set of physical and cryptographic parameters governing both the electromagnetic and security layers of the system.

At the physical layer, the architecture consists of a dual-layer graphene configuration separated by a quartz dielectric gap of thickness $\mathrm{d_{gap}} = 300\,nm$ and relative permittivity $\varepsilon_{\mathrm{r}} = 3.75$. The total thickness of the graphene–dielectric stack is $\mathrm{d_{total}} = 1\,\mu m$.

The carrier frequency is fixed at 1 THz. The corresponding wavelength is determined by the fundamental electromagnetic relation

$$\lambda = \frac{\mathrm{c}}{\mathrm{f}}, \tag{1}$$

where c denotes the speed of light in free space. As defined in Eq. (1), the wavelength at the selected operating frequency becomes $\lambda = 3 \times 10^{-4}\,m$.

The graphene electronic parameters are specified by a Fermi level $\mathrm{E_f} = 0.5\,eV$, relaxation time $\tau = 1\,ps$, and operating temperature $\mathrm{T} = 300\,K$, ensuring compatibility with terahertz transport conditions.

- Graphene Surface Conductivity Model

The complex surface conductivity of graphene is described using the intraband contribution of the Kubo formalism, which dominates in the terahertz regime. The conductivity is expressed as

$$\sigma(\omega) = \frac{2\mathrm{i}e^2\mathrm{k_B T}}{\pi\hbar^2\left(\omega + \frac{\mathrm{i}}{\tau}\right)} \ln\left(2\cosh\left(\frac{\mathrm{E_f}}{2\mathrm{k_B T}}\right)\right), \tag{2}$$

as shown in Eq. (2), where the dependence on temperature, relaxation time, carrier frequency, and Fermi level is explicitly observed.

The resulting complex conductivity is decomposed into its real and imaginary components,

$$\sigma(\omega) = \sigma_{real} + \mathrm{i}\,\sigma_{imag}, \tag{3}$$

as formulated in Eq. (3). Based on this decomposition, an effective conductivity magnitude is defined as

$$\sigma_{eff} = \sqrt{\sigma_{real}^2 + \sigma_{imag}^2}, \tag{4}$$

where Eq. (4) provides the effective surface conductivity employed in the numerical implementation of the current–density and modulation stages.

Wave propagation representation

Wave propagation through the graphene–dielectric structure is captured using a reduced transfer-matrix formulation. The free-space propagation constant is defined as

$$\mathrm{k} = \frac{2\pi}{\lambda}, \tag{5}$$

as given in Eq. (5), while the propagation constant within the dielectric gap becomes

$$\mathrm{k_{gap}} = \frac{2\pi\sqrt{\varepsilon_{\mathrm{r}}}}{\lambda}. \tag{6}$$

Using the propagation constants defined in Eqs. (5) and (6), the cumulative phase transformation across the layered structure is represented by

$$\mathrm{T_{total}} = \mathrm{T_{free}}\mathrm{T_{gap}}, \tag{7}$$

Symbol	Definition	Unit
c	Speed of light in free space	m/s
	Carrier frequency	Hz
$\lambda = \frac{c}{f}$	Wavelength	m
$\omega = 2\pi f$	Angular frequency	rad/s
ε_r	Relative permittivity of dielectric	–
d_gap	Dielectric gap thickness	m
d_total	Total graphene–dielectric thickness	m
E_f	Graphene Fermi level	eV
tau	Carrier relaxation time	s
T	Operating temperature	K
e	Elementary charge	C
$\hbar$	Reduced Planck constant	J · s
k_B	Boltzmann constant	J/K
$\sigma(\omega)$	Complex graphene surface conductivity	S
σ_real	Real part of conductivity	S
σ_imag	Imaginary part of conductivity	S
$\sigma_{eff} = \text{sqrt}(\sigma\_\text{real}^2 + \sigma\_\text{imag}^2)$	Effective conductivity magnitude	S
$k = \frac{2\pi}{\lambda}$	Free-space propagation constant	rad/m
k_gap	Propagation constant in dielectric gap	rad/m
T_free	Free-space transfer matrix	–
T_gap	Dielectric transfer matrix	–
T_total	Overall transfer matrix	–
E_inc(x)	Incident electric field	V/m
E_ref1	Reflected field (graphene layer 1)	V/m
E_ref2	Reflected field (graphene layer 2)	V/m
J_s	Surface current density	A/m
p	Prime modulus in DH	–
g	Generator of cyclic group Z_p*	–
a, binZ_p*	Private exponents of Alice and Bob	–
$A = g^a \text{mod} p$	Alice's public key	–
$B = g^b \text{mod} p$	Bob's public key	–
$K = g^{(ab)} \text{mod} p$	Shared secret key	–
ID_A, ID_B	Identity sequences	bit
T_A, T_B	Timestamp values	bit
H_A = H(A||ID_A||T_A)	Alice's authentication hash	bit
H_B = H(B||ID_B||T_B||A)	Bob's authentication hash	bit
Payload_A	{A, ID_A, T_A, H_A}	bit
Payload_B	{B, ID_B, T_B, H_B}	bit
A_bits, B_bits	Binary representations of public keys	bit
bin{0,1}	Binary bit	–
2b − 1	BPSK mapping rule	–
mod_A, mod_B	BPSK-modulated THz signals	–
m_tilde_A, m_tilde_B	Received noisy signals	–
b_hat	Detected bit after threshold decision	–
SNR	Signal-to-noise ratio	dB
BER	Bit error rate	–
AWGN	Additive white Gaussian noise	–

Table 2. Symbol proposed scheme.

where Eq. (7) governs the overall field evolution across the substrate and dielectric regions.

Phase 2: Private Key Selection and Key Stream Formation

In this phase, each party prepares its cryptographic parameters in bit-level form for subsequent transmission and physical-layer embedding. Alice generates a 256-bit binary sequence, denoted as A, representing her public DH parameter in bit form. Similarly, Bob generates a 256-bit binary sequence B. These bit sequences are randomly generated in the implementation and serve as the public cryptographic parameters exchanged during the protocol execution.

In addition to the public parameters, each party generates:

- A 32-bit identity sequence ($\mathrm{ID_A}$, $\mathrm{ID_B}$),
- A 64-bit timestamp ($\mathrm{T_A}$, $\mathrm{T_B}$) to provide freshness.

To bind identity and temporal information to the public parameters, Alice computes a hash value

$$\mathrm{H_A} = \mathrm{H}(\mathrm{A} \parallel \mathrm{ID_A} \parallel \mathrm{T_A}), \tag{8}$$

where $\parallel$ denotes bitwise concatenation. Similarly, Bob computes

$$\mathrm{H_B} = \mathrm{H}(\mathrm{B} \parallel \mathrm{ID_B} \parallel \mathrm{T_B} \parallel \mathrm{A}), \tag{9}$$

thereby explicitly binding his response to Alice's public parameter and preventing message substitution across sessions.

The complete transmitted payloads are therefore constructed as

$$Payload_{\mathrm{A}} = \{\mathrm{A}, \mathrm{ID_A}, \mathrm{T_A}, \mathrm{H_A}\}, \tag{10}$$

$$Payload_{\mathrm{B}} = \{\mathrm{B}, \mathrm{ID_B}, \mathrm{T_B}, \mathrm{H_B}\}. \tag{11}$$

As expressed in Eqs. (10) and (11), each transmitted structure integrates public cryptographic parameters, identity information, timestamp-based freshness, and hash-based integrity protection within a single bitstream.

Beyond their cryptographic role, the resulting payload bit sequences are directly mapped onto the physical layer and used as modulation streams for the graphene-assisted terahertz transmission. In this way, the cryptographic content is physically embedded into the THz waveform, tightly coupling logical key exchange with electromagnetic signal propagation.

This unified design ensures that security enforcement occurs simultaneously at both the cryptographic and physical layers, eliminating any separation between key establishment and physical transmission.

Phase 3: Public Key Computation and Physical Encoding.

In the theoretical formulation of the proposed scheme, Alice and Bob each select a private secret integer within the multiplicative group modulo p. Let

$$\mathrm{a} \in \mathbb{Z}_{\mathrm{p}}^{*}, \mathrm{b} \in \mathbb{Z}_{\mathrm{p}}^{*} \tag{12}$$

denote the private exponents chosen independently by Alice and Bob, respectively.

Using the agreed public parameters p and generator g, the corresponding public keys are computed according to the classical DH construction:

$$\mathrm{A} = \mathrm{g}^{\mathrm{a}} \mathrm{mod p}, \tag{13}$$

$$\mathrm{B} = \mathrm{g}^{\mathrm{b}} \mathrm{mod p}. \tag{14}$$

Upon exchanging A and B, both parties derive the shared session key as

$$\mathrm{K} = \mathrm{B}^{\mathrm{a}} \mathrm{mod p} = \mathrm{A}^{\mathrm{b}} \mathrm{mod p} = \mathrm{g}^{\mathrm{ab}} \mathrm{mod p}. \tag{15}$$

Equation (15) guarantees key agreement due to the commutativity of exponentiation in the cyclic group modulo p.

- Bit-Level Representation for Physical Embedding

For physical-layer transmission, the public parameters A and B are represented in binary form. Let

$$\mathrm{A} \rightarrow \mathbf{A}_{\mathrm{bits}}, \mathrm{B} \rightarrow \mathbf{B}_{\mathrm{bits}}, \tag{16}$$

where the resulting sequences are 256-bit binary vectors in the implemented model.

These bit-level representations form part of the authenticated payload structures previously defined in Eqs. (10)–(11). Thus, while Eqs. (13)–(15) describe the cryptographic foundation of the protocol, Eq. (16) bridges the mathematical public keys with their physical-layer encoding.

Transfer-matrix-based field formation

The incident electric field is modeled as

$$E_{inc}(x) = e^{ikx}, \tag{17}$$

where the propagation constant k is defined in Eq. (5).

Wave evolution through the layered graphene–dielectric structure is governed by

$$T_{total} = T_{free} T_{gap}, \tag{18}$$

as introduced in Eq. (7).

The reflected field components associated with the two graphene layers are given by

$$E_{ref1} = E_{inc} \cdot T_{total}(1,1), \tag{19}$$

$$E_{ref2} = E_{inc} \cdot T_{total}(2,2). \tag{20}$$

- BPSK-Based Physical Encoding

To embed the cryptographic data into the terahertz waveform, the binary payload sequences are mapped using BPSK. Each bit $b \in \{0,1\}$ is transformed as

$$b \mapsto (2b - 1), \tag{21}$$

producing symbols in $\{-1, +1\}$.

The modulated signals are therefore expressed as

$$mod_A = \Re\{E_{ref1}\} \cdot (2\, Payload_A - 1), \tag{22}$$

$$mod_B = \Re\{E_{ref2}\} \cdot (2\, Payload_B - 1). \tag{23}$$

Thus, while Eqs. (13)–(15) establish the cryptographic correctness of the shared secret, Eqs. (22)–(23) physically embed the corresponding public parameters and authentication tags into the graphene-assisted terahertz channel.

This formulation preserves the mathematical integrity of DH while simultaneously coupling it to electromagnetic signal formation at the physical layer.

Phase 4: Bidirectional Transmission through Graphene Metasurface.

The modulated terahertz waveforms defined in Eqs. (22)–(23) are transmitted simultaneously in a bidirectional manner through a wireless channel impaired by AWGN. To evaluate robustness under realistic propagation conditions, the signal-to-noise ratio (SNR) is varied from 0 to 30 dB.

The electromagnetic interaction within the graphene layers induces a surface current density expressed as

$$J_s = \sigma_{eff}\, \Re\{E_{ref}\}, \tag{24}$$

where the effective conductivity σ_{eff} is defined in Eq. (4) from the real and imaginary components of the Kubo conductivity, as previously introduced. As described by Eq. (24), the induced surface current scales directly with the effective conductivity, thereby governing the strength and stability of the encoded THz signal.

During transmission, Alice's waveform carries her public parameter $\mathbf{A}$ embedded within $Payload_{\mathbf{A}}$, while Bob's waveform carries his public parameter $\mathbf{B}$ embedded within $Payload_{\mathbf{B}}$. Because both signals propagate concurrently through the graphene-assisted channel, the exchange is inherently bidirectional.

Phase 5: Reception, Demodulation, and Shared Secret Derivation.

At the receiver side, the incoming terahertz signals are corrupted by additive white Gaussian noise, yielding the received waveforms $\widetilde{m}_A$ and $\widetilde{m}_B$, corresponding to Alice's and Bob's transmissions, respectively.

Binary recovery is performed using zero-threshold detection. The decision rule is defined as

$$\widehat{b} = \begin{cases} 1, & \widetilde{m} > 0, \\ 0, & \widetilde{m} \le 0, \end{cases} \tag{25}$$

which corresponds to the implemented condition $demod = (noisy > 0)$.

According to Eq. (25), Alice extracts Bob's public parameter B from $\widetilde{m}_B$, while Bob extracts Alice's public parameter A from $\widetilde{m}_A$.

Once the public parameters are successfully recovered, the shared secret key is computed following the classical DH relation

$$K = B^a \bmod p = A^b \bmod p, \tag{26}$$

which is consistent with the theoretical construction introduced earlier. The equality in Eq. (26) follows from the commutative property of modular exponentiation in cyclic groups, ensuring that both parties derive an identical session key. Beyond cryptographic correctness, the embedding of public parameters within the graphene-assisted terahertz waveform establishes a structural alignment between logical key exchange and physical-layer transmission. It is important to clarify that the confidentiality of the session key remains grounded in the computational hardness of the DH problem. The physical layer in this framework serves as a controlled transmission mechanism that supports authenticated parameter exchange under defined channel conditions,

without introducing additional cryptographic entropy or altering the mathematical security foundation of DH. This integration primarily enhances transmission coherence and implementation-level robustness rather than modifying the underlying security assumptions. Figure 2 illustrates the overall architecture of the proposed graphene-assisted secure key exchange scheme.

Performance evaluation

This section presents the simulation settings and underlying assumptions, followed by the obtained results, informal security analysis, security requirements, and a discussion of the experimental limitations.

Simulation setup and assumptions

Simulation Setup and Assumptions as follows:

- Channel Model: The communication channel is represented by an AWGN model, which captures the random thermal noise affecting transmitted signals. More complex phenomena, such as multipath fading, interference, and non-linear distortions, are excluded to maintain analytical tractability.
- Material Properties: Graphene conductivity is computed using the Kubo formalism, under the assumption of ideal and uniform graphene layers. The dielectric substrate is modeled as quartz with a relative permittivity of $\varepsilon_r = 3.75$. The overall structure is defined with a total thickness of 1 μm, including a dielectric gap of 300 nm between the two graphene layers. A constant temperature of 300 K (room temperature) is assumed to ensure stable operating conditions.
- System Parameters: The simulations are performed at a carrier frequency of 1 THz, corresponding to a wavelength of 3×10^{-4} m. The graphene Fermi level is set to 0.5 eV, the relaxation time to $\tau = 1$ ps, and the free-space impedance is considered as $Z_0 = 377\ \Omega$. These values are consistent with established physical parameters for terahertz graphene-based systems.
- Key Exchange Modeling: The key exchange process follows a DH-inspired framework integrated into the physical layer. Both Alice and Bob generate independent 256-bit public parameter sequences. Each transmission frame further includes a 32-bit identity field, a 64-bit timestamp field, and a 256-bit integrity field, resulting in a total payload length of 608 bits. These bitstreams simultaneously serve as cryptographic parameters and as modulation inputs for graphene-based terahertz signal encoding.
- Noise and SNR Conditions: To evaluate robustness, the signal-to-noise ratio (SNR) is varied between 0 and 30 dB. The bit error rate (BER) is measured as the main performance indicator, reflecting the reliability of key exchange under different noise levels.

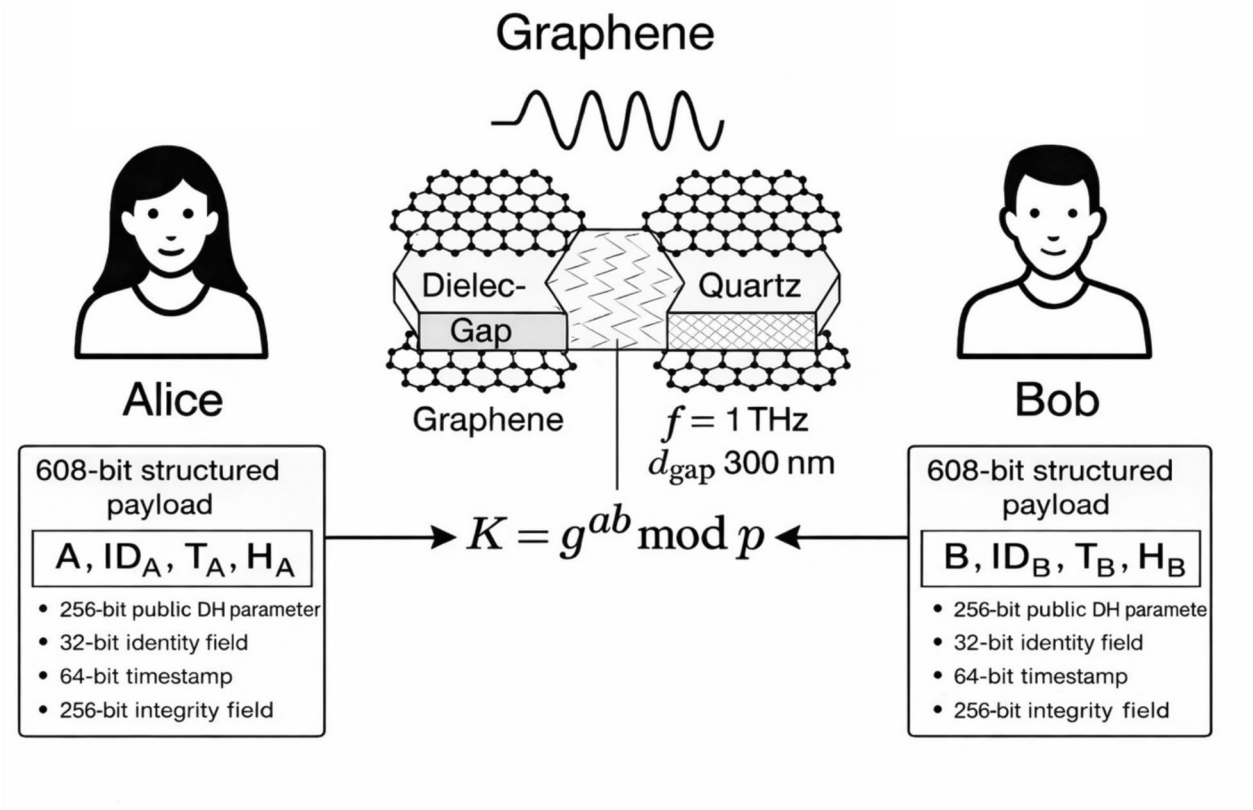

Fig. 2. Proposed graphene-based secure key exchange.

The analysis assumes ideal conditions: fabrication imperfections, thermal fluctuations, and material non-uniformities are not considered. Moreover, graphene layers are assumed to maintain stable conductivity without degradation, allowing the study to focus on the fundamental feasibility of the protocol.

Simulation parameter

Table 3 shows the Simulation parameters.

Simulation result

The experimental results demonstrate that the proposed graphene-based bidirectional key exchange protocol achieves both physical robustness and secure performance under noisy terahertz channel conditions. Each transmitted frame consists of 608 bits, including a 256-bit DH public parameter, a 32-bit identity field, a 64-bit timestamp field, and a 256-bit integrity field. Performance evaluation is conducted over the complete 608-bit payload, while waveform figures display only a representative 200-bit segment for visual clarity.By analyzing the modulation, demodulation, current density distribution, key reconstruction, and BER behavior, the findings confirm that the system maintains high accuracy and stability across varying SNR levels. The detailed results are presented in Figs. 3, 4, 5, 6, and 7.

Figure 3 presents the end-to-end transmission dynamics of the proposed graphene-assisted terahertz link, illustrating only the first 200 bits of the payload sequence. Although the complete transmitted frame comprises 608 bits, displaying the full sequence would compromise visual resolution and obscure temporal transitions; therefore, a representative 200-bit segment is shown for clarity.

The red trace depicts Alice's bipolar modulation, where binary states are encoded as discrete amplitude levels of + 1 and − 1. The blue dashed curve represents the signal observed at Bob under additive white Gaussian noise at 20 dB SNR. As evident, the received waveform exhibits stochastic amplitude perturbations; however, these fluctuations remain tightly clustered around the nominal logical levels, preserving a distinct separation between the two signal states.

The dotted black trace shows the demodulated sequence obtained via zero-threshold hard decision detection. Notably, the reconstructed bits align almost perfectly with the transmitted waveform across the entire interval, with no visible burst errors or systematic drift. The decision boundary at zero remains well isolated from noise

Parameter	Symbol	Value	Unit	Description
Speed of light	C	3.0 × 10^8	m/s	Propagation speed in free space
Carrier frequency	F	1.0 × 10^12	Hz	THz operating frequency
Wavelength	λ = c/f	3.0 × 10^-4	m	Wavelength at 1 THz
Vacuum permittivity	ε_0	8.854 × 10^-12	F/m	Free-space permittivity
Vacuum permeability	μ_0	4π × 10^-7	H/m	Free-space permeability
Free-space impedance	$Z_0 = \sqrt{(\mu_0/\varepsilon_0)}$	≈376.73	Ω	Free-space characteristic impedance
Relative permittivity	ε_r	3.75	-	Dielectric constant
Total thickness	d_{total}	1.0 × 10^-6	m	Total structure thickness
Dielectric gap thickness	d_{gap}	300 × 10^-9	m	Gap between graphene layers
Substrate thickness	d_{sub}	700 × 10^-9	m	d_total—d_gap
Elementary charge	E	1.6 × 10^-19	C	Used in Kubo model
Reduced Planck constant	ħ	1.05 × 10^-34	J·s	Used in Kubo model
Boltzmann constant	k_B	1.38 × 10^-23	J/K	Used in Kubo model
Temperature	T	300	K	Operating temperature
Relaxation time	T	1.0 × 10^-12	s	Electron relaxation time
Fermi level (input)	E_F	0.5	eV	Graphene Fermi energy
Fermi level (used)	$E_F = 0.5e$	8.0 × 10^-20	J	Converted to Joules in code
Effective conductivity	σ_eff	$\sqrt{(\sigma\_real^2 + \sigma\_imag^2)}$	-	Magnitude of Kubo conductivity
Free-space wavenumber	$g = 2\pi/\lambda$	Computed	rad/m	Used in EM simulation
Dielectric wavenumber	$k_{gap} = 2\pi\sqrt{\varepsilon_r}/\lambda$	Computed	rad/m	Used in gap propagation
DH field length	DH_{LEN}	256	bit	DH bits
ID field length	ID_{LEN}	32	bit	Identity bits
Timestamp length	TS_{LEN}	64	bit	Timestamp bits
Hash length	H_{LEN}	256	bit	Hash bits
Payload length	$L_{payload}$	608	bit	Total payload length
SNR sweep	SNRs	0:5:30	dB	BER evaluation range
Fixed SNR	SNR_{fixed}	20	dB	Example BER computation
Noise model	-	AWGN (measured)	-	Additive white Gaussian noise
Demodulation rule	-	Threshold at 0	-	Hard decision detection

Table 3. Simulation parameters.

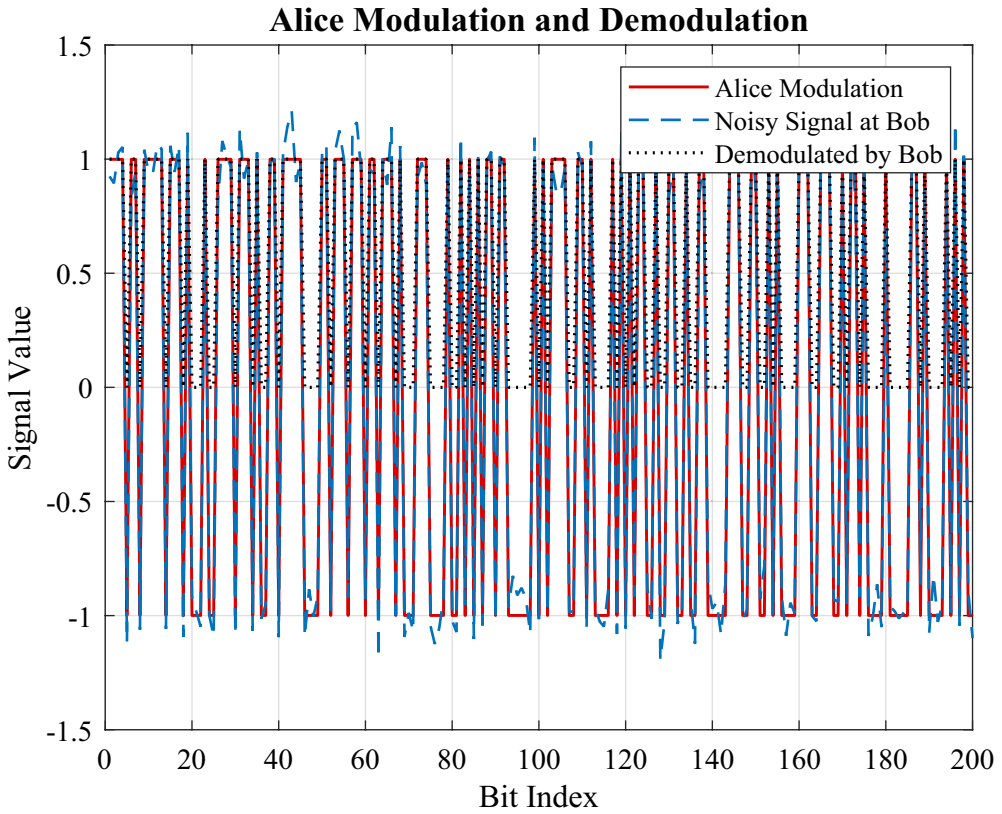

Fig. 3. Modulation at Alice, noisy signal at Bob, and recovered bit sequence.

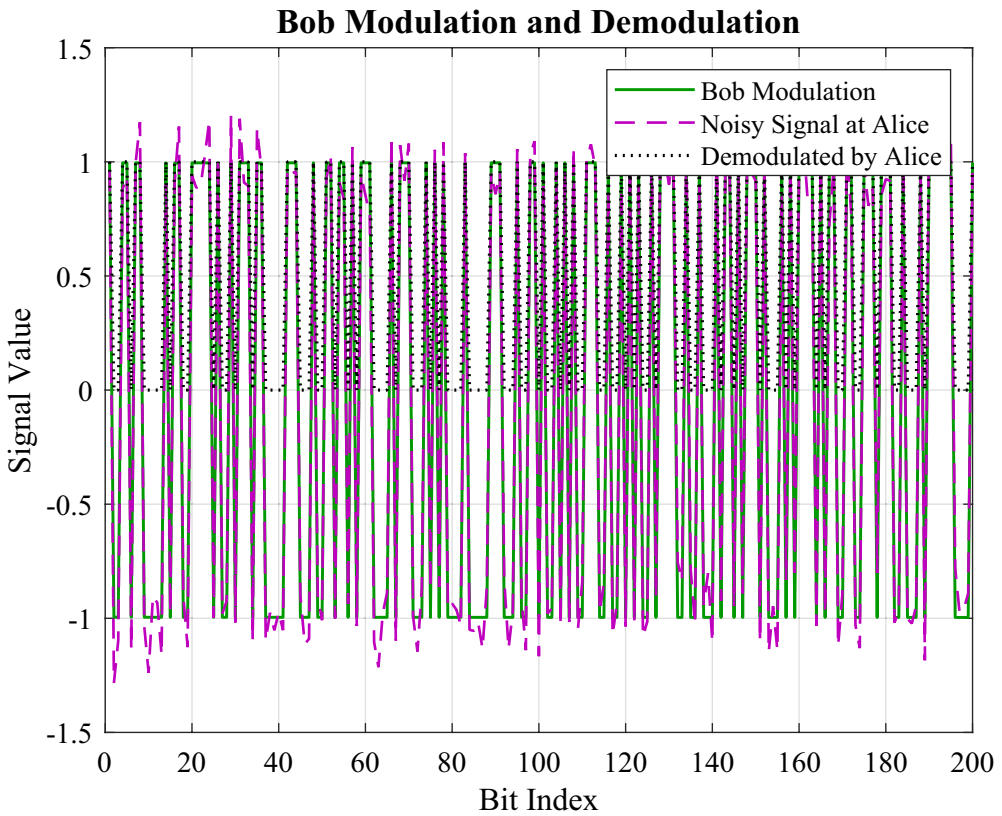

Fig. 4. Modulation at Bob, noisy signal at Alice, and recovered bit sequence.

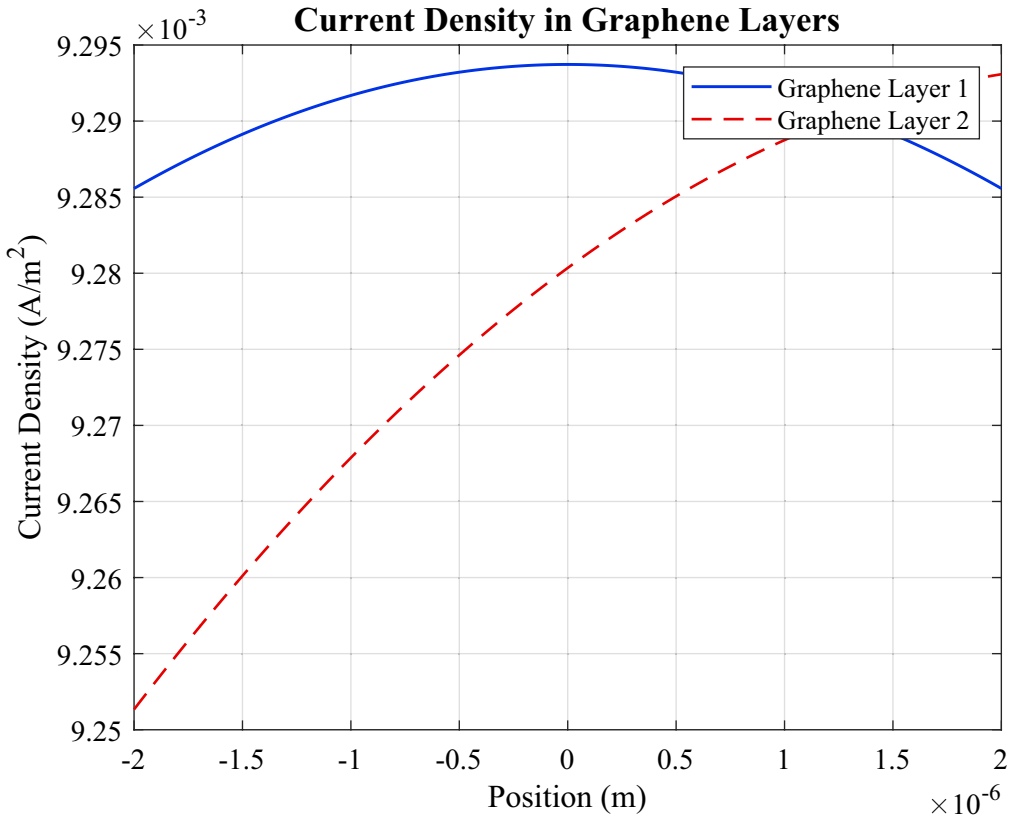

Fig. 5. Spatial variation of current density in the dual-layer graphene structure.

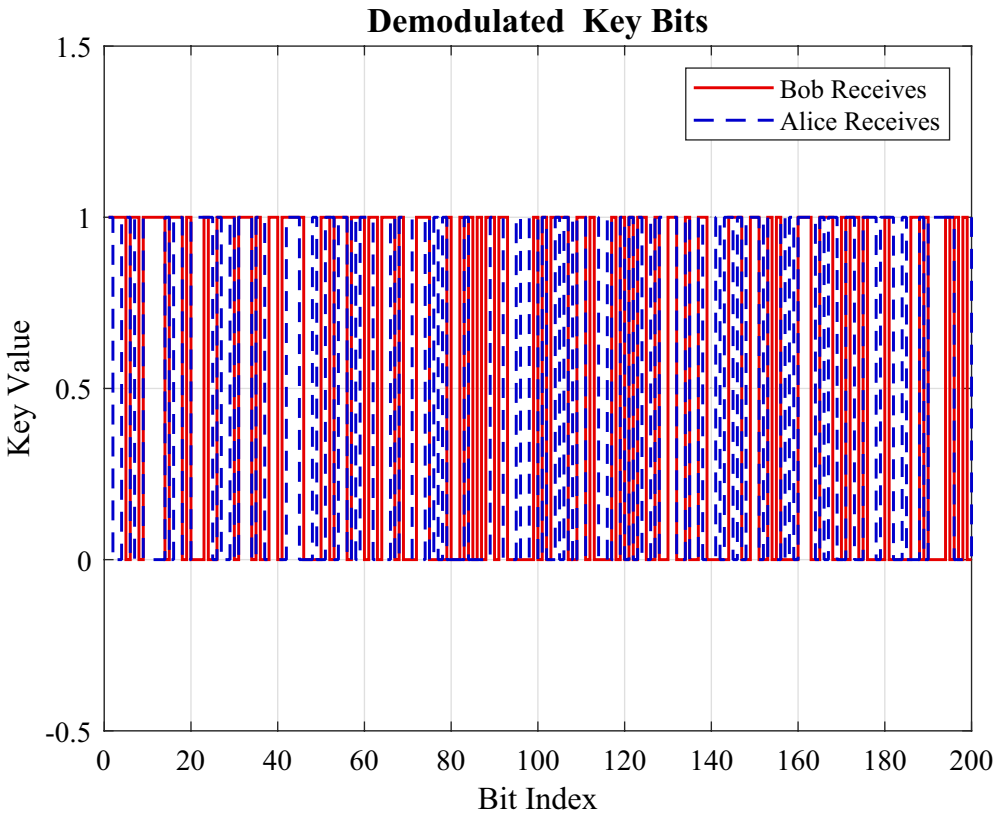

Fig. 6. Final demodulated key sequences independently reconstructed by Alice and Bob.

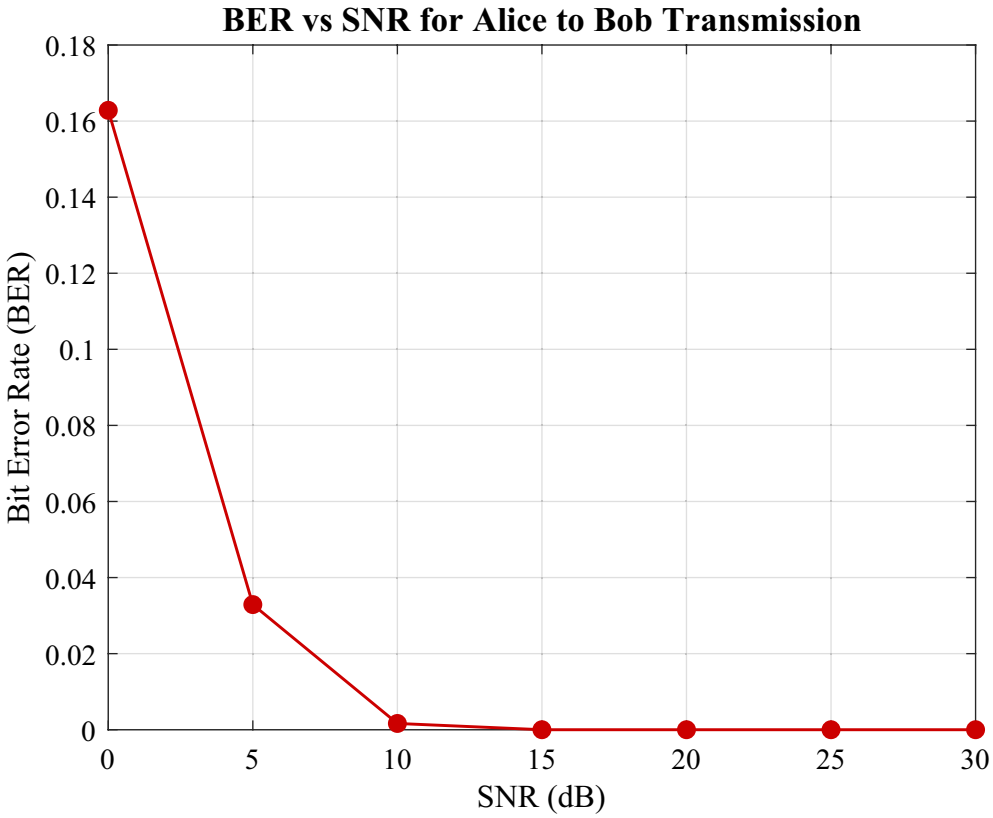

Fig. 7. BER performance versus SNR.

excursions, indicating that the amplitude margin is sufficiently large to prevent erroneous crossings at the considered SNR.

From a physical-layer security perspective, the figure demonstrates that the graphene-enabled THz channel maintains signal distinguishability despite moderate stochastic impairment. The preserved amplitude separation directly ensures reliable bit discrimination, thereby supporting stable and secure key exchange over the wireless THz medium. The observed robustness confirms that the proposed architecture achieves high detection fidelity without sacrificing structural simplicity.

Figure 4 illustrates the forward transmission from Bob to Alice, showing Bob's bipolar modulation (green), the noisy waveform observed at Alice (magenta dashed), and the corresponding demodulated output (black dotted). The transmitted signal alternates between + 1 and − 1, representing binary logical states across rapid transitions along the bit index.

After propagation through the graphene-assisted terahertz channel, the received waveform exhibits stochastic amplitude fluctuations around the nominal ± 1 levels due to additive noise. Importantly, these perturbations remain bounded and do not approach the zero decision boundary in a sustained manner. The separation between logical states in signal space is therefore preserved throughout the transmission interval.

The demodulated sequence maintains near-perfect temporal alignment with the transmitted waveform, with no visible burst errors, systematic drift, or degradation in logical discrimination—even in regions with dense state transitions. The zero-threshold detector consequently preserves stable decision behavior under moderate channel impairment.

From a physical-layer standpoint, the figure confirms that the graphene-enabled THz structure maintains amplitude margin and signal distinguishability under realistic noise conditions. The sustained separation in signal space directly ensures reliable bit recovery, thereby supporting robust and secure bidirectional key exchange over the wireless terahertz medium.

Figure 5 illustrates the spatial distribution of current density across the two graphene sheets in the graphene–dielectric multilayer structure at terahertz frequency. The current magnitude in both layers remains on the order of 10^{-3} A/m^2, indicating stable electromagnetic excitation under the selected operating conditions.

Graphene Layer 1 (solid blue) exhibits a smooth, weakly curved profile with a shallow maximum near the central region, reflecting symmetric field confinement and coherent carrier dynamics across the structure. In contrast, Graphene Layer 2 (dashed red) shows a gradual spatial increase along the propagation axis, forming a gently varying monotonic profile without abrupt transitions or localized peaks.

Although the two distributions are not identical, their magnitudes remain closely aligned throughout the spatial domain, with only minor deviation between layers. The absence of sharp gradients or current

concentration points suggests that the dielectric gap effectively moderates interlayer coupling while preserving electromagnetic stability.

From a physical-layer standpoint, the smooth and well-regulated current profiles indicate synchronized electromagnetic behavior across the multilayer configuration. Such spatial coherence minimizes scattering-induced disturbances and maintains consistent modulation capability, thereby supporting stable terahertz signal encoding within the proposed secure communication architecture.

Figure 6 presents the final reconstructed key sequences independently obtained by Alice and Bob following bidirectional transmission and demodulation. The bitwise representations are plotted over the transmission interval to enable direct visual comparison of key consistency.

An almost complete overlap between the two reconstructed sequences is observed, with virtually all bits exhibiting exact correspondence. The alignment remains stable even across regions of dense transitions, indicating precise temporal synchronization and consistent threshold-based detection at both endpoints. No visible burst-error patterns, extended mismatch regions, or systematic divergence are apparent.

From a physical-layer perspective, the near-perfect agreement confirms that the graphene-assisted terahertz link preserves logical integrity during concurrent protocol-level transmission. The modulation, propagation, and detection processes collectively maintain signal distinguishability and decision stability, thereby enabling reliable symmetric key establishment under the considered channel assumptions.

Figure 7 depicts the bit error rate (BER) as a function of signal-to-noise ratio (SNR), quantitatively characterizing the reliability of the proposed graphene-assisted terahertz link.

At 0 dB SNR, the BER is approximately 1.6×10^{-1}, indicating substantial symbol distortion under severe noise conditions. Increasing the SNR to 5 dB yields a sharp reduction in error probability to about 3×10^{-2}, reflecting improved signal-space separation and more reliable threshold discrimination. A pronounced transition occurs between 5 and 10 dB, where the BER rapidly collapses toward zero within the resolution of the evaluated bit sequence.

For SNR values of 15 dB and above, no detectable bit errors are observed across the simulated transmission window. Importantly, the high-SNR regime exhibits no evidence of an error floor, suggesting the absence of residual structural distortions or systematic decision bias.

The steep monotonic decay of the BER curve confirms that the graphene-assisted multilayer configuration effectively preserves signal distinguishability as noise power diminishes. This rapid convergence to near error-free operation demonstrates robust physical-layer performance within practical SNR ranges relevant to terahertz wireless systems.

Informal security analysis

Under the Dolev–Yao adversarial model, the End layer is assumed to operate over a fully compromised THz wireless channel. The attacker has complete control over the communication medium and may attempt the following attacks: Eavesdropping, Replay Attack, Message Modification and Injection, Man-in-the-Middle (MITM) Attack, and Suppression and Delay Attacks. The resistance of the proposed graphene-assisted key exchange protocol against each of these threats is analyzed below.

Eavesdropping: An adversary may intercept all public parameters exchanged during the DH procedure. However, the shared session key is derived from independently chosen private values, and its security relies on the computational hardness of the discrete logarithm problem. Thus, observing public parameters alone does not enable recovery of the private secrets or the session key under standard cryptographic assumptions. In the proposed framework, public parameters are additionally embedded within a graphene-assisted terahertz waveform. The physical layer does not replace cryptographic security but increases the complexity of implementation-level interception. While cryptographic security does not depend on physical-layer secrecy, this integration increases the complexity of practical interception, thereby preserving session key confidentiality against passive attacks.

Replay Attack: Replay resistance is ensured through timestamp-based freshness validation. Each transmitted message associates the exchanged public parameter with the sender's identity and current temporal information. Any replayed transmission will contain outdated timing data and will therefore fail verification at the receiver. Since session key establishment occurs only after successful identity and freshness checks, replayed messages cannot result in a valid key. The protocol thus guarantees session key freshness.

Message Modification and Injection: Integrity of transmitted data is protected through hash-based authentication. Any modification of A, B, identity fields, or timestamps changes the hash output and is detected before key derivation. Similarly, injection of forged parameters requires generation of a valid authentication hash consistent with the altered payload. Under standard assumptions of hash collision resistance and preimage resistance, such forgery is computationally infeasible. Therefore, the protocol ensures strong protection against unauthorized modification or injection of public parameters.

Man-in-the-Middle (MITM) Attack: Classical DH is vulnerable to MITM attacks when public parameters are not authenticated. In the proposed scheme, authentication is enforced through cross-binding of public parameters within the hash computation. Bob's authentication value explicitly incorporates Alice's public parameter, and vice versa. This interdependence prevents independent substitution of public values. An adversary attempting a MITM attack must simultaneously generate consistent authentication hashes and maintain coherent physical-layer modulation. Failure in either dimension leads to verification rejection. Consequently, the protocol achieves authenticated key agreement and resists classical MITM substitution attacks under the Dolev–Yao model.

Suppression and Delay Attacks: Message suppression or intentional delay may disrupt communication but does not compromise secrecy or key integrity. The protocol follows a fail-safe design: if authentication or freshness verification fails, no session key is derived. Timestamp validation prevents delayed transmissions from

Security requirements	[44]	[43]	Poposed Scheme
$F1$	NO	NO	Yes
$F2$	NO	NO	Yes
$F3$	NO	NO	Yes
$F4$	NO	NO	Yes
$F5$	NO	NO	Yes
$F6$	Yes	Yes	Yes

Table 4. Security requirements F1: Eavesdropping, F2: Replay Attack; F3: Message Modification and Injection; F4: Man-in-the-Middle (MITM) Attack; F5: Suppression and Delay Attacks; F6:Graphene based.

being accepted as valid session messages. Thus, availability may be affected, but confidentiality and agreement properties remain intact.

The results of the Informal Security Analysis indicate that the proposed scheme is resistant to the defined attacks under the stated adversarial model. Within the Dolev–Yao framework, the scheme preserves session key confidentiality, integrity, freshness, and key agreement properties against the considered threat scenarios.

Security requirements

Table 4 presents the security requirements considered for comparative evaluation. As shown, prior schemes [43,44] do not demonstrate resistance against several fundamental passive and active adversarial models, including eavesdropping (F1), replay attacks (F2), message modification and injection (F3), man-in-the-middle (MITM) attacks (F4), and suppression or delay attacks (F5).By contrast, the proposed scheme is architecturally designed to mitigate these threats through the combined application of robust key-exchange mechanisms and graphene-assisted physical-layer modulation. In addition, while graphene-based capability (F6) is only partially addressed in related work, it constitutes an intrinsic structural component of the proposed framework. Collectively, the comparative analysis indicates that the proposed scheme fulfills all defined security requirements under the assumed adversarial mode.

Discussion

The presented results indicate that secure session key establishment over a graphene-assisted terahertz link can remain both physically stable and cryptographically reliable under the evaluated AWGN conditions. The preserved separation between bipolar logical states enables deterministic threshold-based demodulation, which is essential for the correctness of DH key derivation. The electromagnetic consistency of the dual-layer graphene configuration and the spatial coherence of current density distributions further demonstrate that embedding cryptographic payloads does not destabilize carrier dynamics. This material-level robustness supports reliable parameter transmission within the key exchange process. At the protocol level, the near-identical reconstruction of key sequences at both endpoints confirms that channel perturbations do not propagate into systematic key mismatch, a requirement that is fundamental for DH agreement. The BER behavior exhibits a rapid monotonic decline with increasing SNR, approaching near error-free performance at moderate-to-high SNR levels without observable error floors. Under these conditions, the probability of key disagreement becomes negligible within the evaluated regime.

Even a single bit inconsistency in the recovered public parameters would result in a completely different session key and therefore cause key agreement failure. Accordingly, reliable key establishment depends on sufficiently low physical-layer error probability. Under practical operating conditions, the observed transmission behaviour indicates that the likelihood of such inconsistencies becomes negligible. In the event of a mismatch, the protocol employs a fail-safe design in which key derivation is aborted, and practical implementations may incorporate retransmission or explicit key-confirmation mechanisms to ensure robustness.

Importantly, the contribution of this work lies not merely in demonstrating waveform robustness, but in establishing that graphene-assisted terahertz transmission can reliably support cryptographic key exchange at the physical layer. While prior graphene research has primarily focused on electromagnetic optimisation, secure bidirectional key establishment has remained outside the scope of material-driven architectures. By integrating DH exchange directly into graphene-modulated transmission, the proposed framework unifies material controllability with secure session establishment. Collectively, these findings suggest that graphene-based terahertz platforms may serve as promising substrates for secure key exchange in emerging 6G and IoT environments, where establishing confidentiality-preserving sessions over open wireless channels is essential.

To further bridge the gap between the present simulation-oriented framework and prospective real-world deployment, a conceptual system-level implementation pathway can be considered. In a practical proof-of-concept architecture, the proposed scheme could be realised by integrating a graphene-based reconfigurable metasurface with a terahertz transceiver front-end, in which electrically tunable surface conductivity enables dynamic, programmable modulation of the transmitted waveform. Within such a configuration, the cryptographic payload—including Diffie–Hellman public parameters and associated protocol fields—can be directly encoded onto the THz carrier via bias-controlled modulation of the graphene layers. At the receiver side, a corresponding THz detection and demodulation module, coupled with digital signal processing units, would facilitate accurate reconstruction of the transmitted symbols and subsequent key derivation. In light of recent advances in programmable metasurfaces and real-time THz communication systems, such system-

level integration appears increasingly feasible within emerging 6G communication paradigms. Nevertheless, it is emphasised that this perspective remains a conceptual extension of the present work, and hardware-level realisation and experimental validation are reserved for future investigations.

Limitation

A limitation of the present study lies in the use of an AWGN abstraction for performance evaluation. Although the fundamental propagation relation has been introduced earlier (see Eq. 1) and the relevant physical parameters are summarised in Table 3, a complete THz link-budget analysis was not conducted. The SNR threshold identified for reliable parameter recovery can, in principle, be related to an indicative operating range using the previously defined propagation framework. However, a comprehensive deployment-level assessment incorporating transmit power, antenna gain, molecular absorption, and hardware constraints remains beyond the scope of this study and is left for future investigation.

A further limitation concerns the scope of the proposed integration between graphene-assisted terahertz modulation and cryptographic key exchange. The present study does not claim to introduce additional cryptographic entropy beyond the standard DH security assumptions. Rather than proposing a new cryptographic primitive, the work focuses on the architectural integration of parameter generation, authenticated exchange, and physical-layer signalling within a unified framework. Consequently, the security guarantees remain fundamentally dependent on the established hardness assumptions of the DH mechanism. Moreover, while the framework demonstrates the feasibility of embedding structured key exchange into graphene-modulated THz transmission, it does not provide a comprehensive system-level validation across diverse deployment environments. In addition, due to practical constraints, the proposed framework has not been implemented or validated at the hardware level, and no experimental prototype has been developed. Therefore, the current results should be interpreted as a feasibility-oriented study at the modelling, protocol, and simulation levels rather than a complete hardware realisation. The broader generalisation of this architectural approach to heterogeneous channel models, large-scale networks, or fully integrated hardware implementations remains subject to future investigation.

Conclusion

This study presents a graphene-assisted bidirectional key exchange protocol that integrates terahertz (THz) physical-layer modulation with the Diffie–Hellman (DH) cryptographic framework to address a critical challenge in secure session establishment over open wireless channels. The proposed architecture enables concurrent bidirectional transmission at the protocol level under the assumed channel conditions, while preserving reliable key agreement in the presence of noise. Simulation results demonstrate stable signal recovery, coherent current–density distributions across graphene layers, and consistent key reconstruction between communicating entities. The BER analysis reveals a pronounced performance transition between 5 and 10 dB, followed by convergence toward near-error-free operation at SNR values of 15 dB and above, confirming robust key establishment within the evaluated noise range. These results indicate that graphene-enabled THz modulation can effectively support secure session establishment in practical wireless environments. An informal security assessment under the Dolev–Yao adversarial model, together with a comparative evaluation of defined security requirements, suggests that the proposed scheme is resilient to both passive and active adversarial behaviours within the considered threat framework. Overall, the findings substantiate the feasibility of integrating graphene-based physical-layer modulation with cryptographic protocols, positioning the proposed framework as a promising security enabler for emerging 6G THz networks, as well as IoT and biomedical communication systems. Despite these contributions, the present work is subject to several limitations, including its reliance on idealised material assumptions and AWGN-based channel modelling. Real-world factors—such as multipath propagation, hardware impairments, and fabrication tolerances—remain to be systematically investigated. In addition, the experimental realization and hardware-level validation of the proposed framework are designated as future work, where practical implementation on programmable graphene-based terahertz platforms will be pursued.

Data availability

The data used to support this novel scheme are included within the article.

Received: 16 September 2025; Accepted: 25 April 2026
Published online: 18 May 2026

References

1. Xu, M., Liang, T., Shi, M. & Chen, H. Graphene-like two-dimensional materials. *Chem. Rev.* **113**(5), 3766–3798 (2013).
2. Geim, A. K. & Novoselov, K. S. The rise of graphene. *Nat. Mater.* **6**(3), 183–191 (2007).
3. Novoselov, K. S. et al. Two-dimensional atomic crystals. *Proc. Natl. Acad. Sci. U. S. A.* **102**(30), 10451–10453 (2005).
4. Dhinakaran, V., Lavanya, M., Vigneswari, K., Ravichandran, M. & Vijayakumar, M. D. Review on exploration of graphene in diverse applications and its future horizon. *Mater. Today Proc.* **27**, 824–828 (2020).
5. Youvan, D. C. Integrating buckminsterfullerene and graphene: hybrid carbon nanostructures for advanced nanotechnology applications (2024).
6. Qadoos, A. et al. Bandgap engineering in graphene oxide (GO) via integrating DFT calculations with atmospheric-pressure microplasma (AMP) treatment for optoelectronic applications. *Hybrid Adv.* **8**, 100353 (2025).
7. Feraco, G. Transition metal dichalcogenides and graphene: band structure investigation and molecular functionalization (2025).
8. Yuan, W. et al. Latest advances in the scalable synthesis of graphene and its versatile applications in energy, electronics, composites, biomedical, and environmental technologies. *2D Mater.* https://doi.org/10.1088/2053-1583/adff93 (2025).
9. Sundar, S. & Nitin, S. Emerging trends of graphene-based nanomaterials as digital materials for data generation in Industry 4.0. *Advancements in Intelligent Process Automation*, 325–358 (2025).

10. Shahzad, T. et al. A review on cutting-edge three-dimensional graphene-based composite materials: Redefining wastewater remediation for a cleaner and sustainable world. *J. Compos. Sci.* **9**(1), 18 (2025).
11. Ganguly, S. & Sengupta, J. Graphene-based nanotechnology in the internet of things: A mini review. *Discov. Nano* **19**(1), 110 (2024).
12. Ramezani, M. J. & Rahmani, O. A review of recent progress in the graphene syntheses and its applications. *Mech. Adv. Mater. Struct.* https://doi.org/10.1080/15376494.2024.2420911 (2024).
13. Yang, Y. et al. Fluid-dynamics-rectified chemical vapor deposition (CVD) preparing graphene-skinned glass fiber fabric and its application in natural energy harvest. *J. Am. Chem. Soc.* **146**(36), 25035–25046 (2024).
14. Tarcan, R. et al. Reduced graphene oxide today. *J. Mater. Chem. C Mater.* **8**(4), 1198–1224 (2020).
15. Deng, B., Liu, Z. & Peng, H. Toward mass production of CVD graphene films. *Adv. Mater.* **31**(9), 1800996 (2019).
16. Salami, Y. "SOBT-UF: Secure offloading in blockchain infrastructure for intelligent transportation systems using 5G-enabled UAVs within a fog-edge computing federation. In *2024 19th Iranian Conference on Intelligent Systems (ICIS)*, IEEE, 217–222 (2024).
17. Salami, Y. & Khajehvand, V. SMAK-IOV: Secure mutual authentication scheme and key exchange protocol in fog based IoV. *J. Comput. Robot.* **13**(1), 11–20 (2020).
18. Salami, Y. SOBV-FEF: Secure lightweight data offloading base in blockchain technology for internet of vehicles enabled handover UAVs within a Fog-Edge federation. *Sci. Rep.* https://doi.org/10.1038/s41598-025-31114-x (2025).
19. Bouzid, H. A., Belkheir, M., Mokaddem, A., Rouissat, M. & Ziani, D. Enhancing the performance of graphene and LCP 1x2 rectangular microstrip antenna arrays for terahertz applications using photonic band gap structures. *Comput. Electr. Eng.* https://doi.org/10.1016/j.compeleceng.2024.109858 (2024).
20. Kong, M. et al. Graphene-based flexible wearable sensors: Mechanisms, challenges, and future directions. *Int. J. Adv. Manuf. Technol.* **131**(5–6), 3205–3237. https://doi.org/10.1007/s00170-023-12007-7 (2024).
21. Babu, R., Agrahari, R., Jain, P. K. & Mahto, M. Bifunctional graphene-graphite-based THz wave metasurface absorber for sensing and electromagnetic shielding. *IEEE Trans. Circuits Syst. I Regul. Pap.* **71**(11), 5339–5348. https://doi.org/10.1109/TCSI.2024.3397691 (2024).
22. Shen, C. et al. A wearable knee rehabilitation system based on graphene textile composite sensor: Implementation and validation. *Eng. Appl. Artif. Intell.* https://doi.org/10.1016/j.engappai.2024.108954 (2024).
23. Dhadwal, D., Sahni, P., Mittal, V., Agarwal, N. & Mittal, R. Graphene and RT-duroid based microstrip patch antenna with complementary SSTR metamaterial for dual band 5G communication. *Expert Syst. Appl.* https://doi.org/10.1016/j.eswa.2025.127231 (2025).
24. Lazaro, A., Cujilema, M. R., Villarino, R., Lazaro, M. & Girbau, D. Anti-counterfeiting near-field chipless RIFD tags based on laser-induced graphene on cork. *IEEE J. Radio Freq. Identif.* **9**, 295–307. https://doi.org/10.1109/JRFID.2025.3573941 (2025).
25. Rai, J., Patel, U., Tiwari, P., Ranjan, P. & Chowdhury, R. Machine learning enabled compact frequency-tunable triple-band hexagonal-shaped graphene antenna for THz communication. *Int. J. Commun. Syst.* https://doi.org/10.1002/dac.6044 (2025).
26. Althuwayb, A. A. et al. Broadband, high gain 2 × 2 spiral shaped resonator based and graphene assisted terahertz MIMO antenna for biomedical and WBAN communication. *Wirel. Netw.* **30**(1), 495–515. https://doi.org/10.1007/s11276-023-03494-3 (2024).
27. Shukla, S., Raghunath, P., Mehta, S. & Arora, P. Design and comparative analysis of aluminum-$BiFeO_3$-based plasmonic device in the near-infrared region. *Microsyst. Technol.* **31**(5), 1113–1120. https://doi.org/10.1007/s00542-024-05672-5 (2025).
28. Narayanan, V. & Govindasamy, A. A hybrid energy harvesting framework and graphene-based supercapacitor for 6G and smart grid networks. *Int. J. Commun. Syst.* https://doi.org/10.1002/dac.5654 (2024).
29. Singh, R. K., Mamta, K. & Kumar, D. Graphene based nano-antenna for wireless communication systems at terahertz band. *Bull. Electr. Eng. Inform.* **14**(2), 1045–1053. https://doi.org/10.11591/eei.v14i2.8727 (2025).
30. Oh, H.-S., Jeong, S., Yun, Y. & Jeong, S. Y. Development of transmission line employing graphene-silver nanowire/PET structure for application in flexible and wearable devices in X-Band wireless communication systems. *J. Electromagn. Eng. Sci.* **24**(1), 1–8. https://doi.org/10.26866/jees.2024.1.r.198 (2024).
31. Singh, G., Sandha, K. S. & Kansal, A. Impact of sole layer duple substrates on GA-based optimised graphene antennas for THz applications. *Nano Commun. Netw.* https://doi.org/10.1016/j.nancom.2024.100508 (2024).
32. García-Pineda, V., Zapata-Ochoa, E. A., Arias, A. V., Molina, O. D. O. & Giraldo, F. E. L. Research trends in wireless communications using graphene: Research trajectories in antenna applications. *Indones. J. Sci. Technol.* **9**(3), 847–884. https://doi.org/10.17509/ijost.v9i3.75239 (2024).
33. Jarchi, S. Amplitude modulator design using series graphene transmission lines in terahertz frequency band. *IEEE Trans. Nanotechnol.* **23**, 323–328. https://doi.org/10.1109/TNANO.2024.3385507 (2024).
34. Cali, F. et al. Experimental implementation of molecule shift keying for enhanced molecular communication. *IEEE Trans. Mol. Biol. Multiscale Commun.* **10**(1), 175–184. https://doi.org/10.1109/TMBMC.2024.3368759 (2024).
35. Ren, Y., Sun, C.-H., Liu, C.-H., Wu, C.-T.M. & Chen, P.-Y. Wireless anti-counterfeiting labels using RF oscillators with graphene quantum capacitors. *IEEE J. Radio Freq. Identif.* **9**, 38–45. https://doi.org/10.1109/JRFID.2025.3529343 (2025).
36. Khani, A. A. M., Salmanpour, A., Soldoozy, A. & Zandi, E. An ultra-thin meta-material including graphene patterns: Coupling application. *Memories (Mater. Dev. Circuits Syst.)* https://doi.org/10.1016/j.memori.2024.100103 (2024).
37. Xuan, X. et al. Flexible antenna sensor based on vertical graphene for wireless humidity monitoring and IoT applications. *IEEE Internet Things J.* **11**(10), 18099–18110. https://doi.org/10.1109/JIOT.2024.3361009 (2024).
38. Asaad, N. S., Saleh, A. M. & Alzubaidy, M. A. Analyzing performance of THz band graphene-based MIMO antenna for 6G applications. *J. Telecommun. Inf. Technol.* **3**, 23–29. https://doi.org/10.26636/jtit.2024.3.1518 (2024).
39. Chude-Okonkwo, U. A. K. & Vasilakos, A. V. CRISPR-enabled graphene-based bio-cyber interface model for in vivo monitoring of non-invasive therapeutic processes. *IEEE Trans. Nanobiosci.* **23**(2), 300–309. https://doi.org/10.1109/TNB.2023.3348201 (2024).
40. Sakai, K., Teshima, T. F. & Goto, T. Brain-on-a-chip model using deformable graphene-based electrode array. *NTT Tech. Rev.* **22**(5), 31–38. https://doi.org/10.53829/ntr202405fa3 (2024).
41. Srivastava, S., Gupta, S., Sachan, V. K., Saxena, G. & Srikant, S. S. High gain circularly polarized graphene inspired dielectric resonator antenna for 6G IOT THz optical communication and optical refractive index biosensing applications. *Eng. Sci. Technol. Int. J.* https://doi.org/10.1016/j.jestch.2023.101603 (2024).
42. Upender, P., Vardhini, P. A. H., Kumba, K., Bharathi, S. P. & Kumar, A. VO2-graphene ultrathin films: Enabling wideband switchable and tunable THz absorption. *IEEE Access* **12**, 74432–74443. https://doi.org/10.1109/ACCESS.2024.3404480 (2024).
43. Farzin, P., Hajiahmadi, M. J. & Soleimani, M. Multi-channel polarization manipulation based on graphene for encryption communication. *Sci. Rep.* https://doi.org/10.1038/s41598-024-61323-9 (2024).
44. J., De Feo Luca S. B. & Kieffer. Towards practical key exchange from ordinary isogeny graphs. In *Advances in Cryptology – ASIACRYPT 2018*, S. Peyrin Thomas and Galbraith, Ed., Cham: Springer International Publishing, 2018;365–394.
45. Xiao, Q. et al. Secure wireless communication of brain–computer interface and mind control of smart devices enabled by space-time-coding metasurface. *Nat. Commun.* **16**(1), 7914 (2025).
46. Ning, Y. M. et al. Multilayer nonlinear diffraction neural networks with programmable and fast ReLU activation function. *Nat. Commun.* **16**(1), 10332 (2025).
47. Ning, Y. M. et al. Mechanically programmable diffractive neural networks based on Pancharatnam-Berry Phase. *Adv. Funct. Mater.* **36**(9), e12689 (2026).
48. Yao, J. et al. Intensity-asymmetric wavefront shaping in nonlocal meta-lens. *Nat. Commun.* https://doi.org/10.1038/s41467-026-68638-3 (2026).

49. Zhang, J. C., Tsai, D. P. & Pang, S. W. Non-local bound states in the continuum for nanoscale alignment. *Nat. Photonics*. 1–5 (2026).

Author contributions

Y.S. conceived the main idea, designed the protocol framework, and supervised the project. Y.P. performed the simulations and data analysis. M.B.K. contributed to the theoretical modelling and validation of the proposed scheme. N.A. reviewed the related work and prepared the initial draft of the manuscript. Y.S. and Y.P. wrote the main manuscript text, and M.B.K. and N.A. contributed to protocol and revisions and figure preparation. All authors reviewed and approved the final manuscript.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Y.S.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.