Soil-Assisted Trust Establishment For Underground Wireless Networks

Ebuka P. Oguchi *Member, IEEE*, Nirnimesh Ghose *Senior Member, IEEE*, Mehmet C. Vuran *Member, IEEE*

***Abstract*—In the agricultural Internet of Things (Ag-IoT) infrastructures, ensuring the sensitive agricultural information protection and its timely delivery is crucial. Trust is critical to facilitate secure communication between nodes, even in large-scale farming operations. This paper addresses the challenge of establishing trust without prior secrets in commercial off-the-shelf (COTS) underground nodes, leveraging an aboveground gateway and an underground trusted node. The proposed approach involves authentication and secret key establishment based on the hard-to-forge underground wireless signal propagation laws. By utilizing soil-assisted trust establishment, the underground wireless network is deployed in a sector network configuration, with a single trusted node and multiple legitimate nodes in each sector, effectively covering a large farm area. Importantly, this trust establishment mechanism is resilient against active signal injection attacks, ensuring integrity and security. The security level achieved by the soil-assisted trust establishment approach for underground wireless networks is comparable to the NP-hard problem of underdefined systems of multivariate equations. To validate the effectiveness of this approach, several experiments were conducted using data collected from an underground wireless testbed. These experiments provide practical evidence of the system's performance and security in real-world scenarios.**

***Index Terms*—Ag-IoT, secure bootstrapping, underground wireless, secret-free, message integrity, authentication.**

I. Introduction

THE growing adoption of the agricultural Internet of Things (Ag-IoT) transforms farming by enabling wireless networks that enhance agricultural productivity and optimize resource utilization. Ag-IoT sensors provide real-time data on crop, soil, and weather conditions, such as moisture, precipitation, temperature, and leaf quality [1], [2], enabling partial automation, including sensor-controlled irrigation systems. However, ensuring data integrity is critical, as erroneous data can lead to significant financial losses due to yield reductions or excessive resource usage [3], [4]. This challenge is amplified by the large number of Ag-IoT sensors with limited computational power, and the sensitive nature of the data they collect within smart farming ecosystems.

Recently, buried sensors with wireless communication capabilities through soil have been utilized in commercial Ag-IoT products [5], [6]. These solutions provide sensing systems protection from natural elements and agricultural machinery to observe and provide soil information while reducing operation costs. In these architectures, secure communication is critical to protect sensitive soil information exchanged between buried sensors and the gateway. The stochastic nature of soil parameters, influenced by factors such as moisture, porosity, soil type, and permittivity, must be considered in security designs. Prior work on soil-assisted underground networks used the physical propagation characteristics of the soil to enable secure communication between underground and aboveground nodes [7]. Building on these foundations, this paper expands the approach by creating a scalable, secret-free trust establishment protocol that is robust to emulation attacks from the gateway to legitimate nodes and can cover an entire farm.

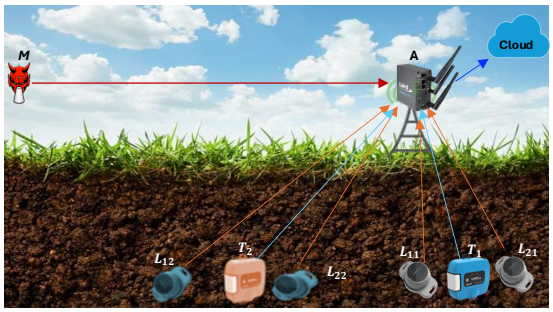


Fig. 1. Several underground nodes $\mathbf{L}_i$ securely bootstrap with the gateway A assisted by the trusted node T_i in presence of an adversary M.

Recent incidents highlight the vulnerability of Ag-IoT infrastructure to physical and online attacks, including spoofing, malicious injections, WiFi jamming, and man-in-the-middle attacks, which have led to operational disruptions and financial losses [4], [3]. In Ag-IoT systems, generally, a gateway-centric model facilitates data collection, remote control, and progression through key stages such as collection, storage, utilization, sharing, and destruction. To secure communication, gateways and end nodes must establish mutual trust through two steps: mutual authentication by verifying device legitimacy, and shared secret establishment. This enables secure communication and supports cryptographic operations for confidentiality and integrity.

Lightweight bootstrapping methods like Activation by Personalization (ABP) and Over-the-Air Activation (OTAA) are widely used. OTAA is preferred for its zero-interaction setup, while ABP requires physical authentication by the user [8]. However, both are vulnerable to attacks such as secret compromise, jamming, replay, and wormholes due to limited computational resources, weak authentication mechanisms, and scala-

Ebuka P. Oguchi is with the Department of Computer and Information Sciences, Spelman College (e-mail: ebukaoguchi@spelman.edu). Nirnimesh Ghose, and Mehmet C. Vuran are with the School of Computing, University of Nebraska–Lincoln (e-mail: {nghose, mcv}@unl.edu).

Manuscript received January XX, 20XX; revised May XX, 20XX and July XX, 20XX.

bility challenges [9]. Addressing these vulnerabilities is critical to improving bootstrapping mechanisms while maintaining a lightweight design for resource-constrained IoT environments. Moreover, conventional approaches face major challenges in terms of scalability, usability, and interoperability. Underground wireless devices typically lack interfaces for entering or modifying passwords. Even when passwords are preconfigured in advance, manufacturers often use default credentials, which are prone to leakage. In fact, the largest recorded DDoS attack exploited such default passwords preloaded onto IP cameras, digital video recorders, and similar devices to create the Mirai botnet, which targeted critical DNS infrastructure. Furthermore, public key cryptography–based solutions are difficult to deploy widely across heterogeneous manufacturers, further limiting their adoption. To address the abovementioned problem, in-band solutions leverage hard-to-forge physical layer properties over the air [10], [11]. However, these properties are not directly applicable to the wireless underground communication model.

Prior research highlights significant differences between wireless over-the-air (OTA) and underground channel models [12], [13], [14], [15]. Two key in-band properties can be utilized in an *underground network, absent in OTA communication*. First, attacks based on channel prediction are infeasible since the adversary *cannot directly observe or measure the underground channel characteristics without knowing the buried nodes' location.* Additionally, a remote attacker does not have physical access to the farm nodes. Second, the *wireless channel characteristics*, such as signal propagation and interference, *differ significantly between the interior and exterior of the field* due to varying soil conditions caused by seeding, irrigation, and fertigation. Inside the field, wireless channels exhibit temporal and spatial stability [14], [16]. This stability simplifies the design and operation of communication within the farm area, as regions with different agricultural practices exhibit distinct channel characteristics.

To address the issue of secure bootstrapping for underground wireless communication, in this paper, we present STUN: **S**oil assisted **T**rust-establishment for **U**nderground wireless **N**etworks[1]. This work leverages the hard-to-forge wireless underground physical layer properties to develop secret-free secure bootstrapping for underground nodes. We follow a gateway model, where legitimate underground nodes securely bootstrap into the network controlled by the gateway. The gateway wirelessly collects data from the network of underground nodes and either processes it locally or forwards it to the cloud for further analysis and storage. This model supports a wide range of Ag-IoT applications, including field monitoring and irrigation automation. Additionally, we develop an in-band secret-free authentication and message integrity verification technique that can be integrated with existing trust-establishment methods, such as OTAA to improve security in underground IoT deployments.

Main Contributions: We make the following salient contributions:

- We develop the STUN protocol, which prevents rogue device access by using a hard-to-forge underground wireless channel model, and integrate it with the Diffie-Hellman key agreement for secure in-band pairing. We present it to support multiple trusted and legitimate nodes with a single gateway, deploying the system in a hexagonal sector pattern for full farmland coverage. Theoretical and experimental analyses optimize node placement.
- We design security measures for both uplink and downlink communication, showing that STUN resists attacks like signal injection and overshadowing from external adversaries. Our analysis proves STUN's security is comparable to the NP-hard problem of underdefined systems of multivariate equations [17] against advanced active adversaries with transmission power control and colluding nodes.
- We conduct experimental evaluations to measure signal strength at underground nodes and the gateway, identifying optimal distances for reliable and secure communication across different environments and soil conditions. We assess system performance, authentication, and message integrity using data from an underground wireless testbed. Adversarial experiments evaluate signal injection feasibility and validate the security of STUN against colluding attackers, supporting our theoretical findings.

Paper Organization: The remainder of the paper is organized as follows: The related works are discussed in Section II. The model and preliminaries are presented in Section III. The Secret-Free Trust-Establishment protocol for Underground Wireless Networks is described in Section IV. The security analyses of STUN are discussed in Section V. The experimental evaluations of STUN are shown in Section VI. The paper is concluded in Section VII.

II. Related Work

In this section, we first provide an overview of wireless underground sensor networks for agricultural IoT systems. We then review the state-of-the-art in the security of agricultural IoT infrastructures, followed by a discussion of existing secure bootstrapping mechanisms for wireless systems. In Table I, we provide a comparison of STUN with the state-of-the-art in agricultural IoT security and secure bootstrapping.

A. Wireless Underground Sensor Networks

Wireless underground sensor networks (WUSNs) have emerged as a promising technology with a wide range of applications, particularly in precision agriculture and environmental monitoring [42], [43], [44], [45], [46], [47], [48], [49], [50]. Comprehensive overviews of WUSNs and the associated Internet of Underground Things are provided in [42] and [43], [44], respectively, with application areas and research challenges. To support these applications, various communication paradigms have been explored, such as magnetic induction (MI) communication [45], [46] and electromagnetic (EM) based communication [47], [48], including backscatter communication [49], and low-power wide-area networks (LPWAN)[50], [51]. Furthermore, WUSN architectures are overwhelmingly

[1]An earlier version of this work appeared in [7].

TABLE I
COMPARISON OF STATE-OF-THE-ART SECURITY WITH STUN (OUR APPROACH) (✗: NOT MET, ✓*: MET PARTIALLY WITH SIGNIFICANT USER INTERACTION, ✓: MET)

Method	Underground Compatibility	Passive Attacker	MitM Attacks	Advanced MitM Attacks
Security of Ag. IoT Network				
Homomorphic encryption – location obfuscation [18], [19], [20]	✓	✓	✗	✗
Zero-trust security architecture [21]	✓	✓	✓	✗
Machine and deep learning based data security [22], [23]	✓	✓	✗	✗
Blockchain-based secure data management [24], [25], [26]	✓	✓	✗	✗
Secure Bootstrapping				
Password typing [27]	✓*	✓	✗	✗
Secret preloading [28], QR codes [29]	✓*	✓	✓	✗
Public key infrastructure [30]	✓*	✓	✓	✓
Out-of-band channels [31], [32], [33], [34], [35], [36]	✗	✓	✓	✗
In-band, special hardware [37], [38], [39]	✗	✓	✓	✗
In-band, special modulation [40], [41]	✗	✓	✓	✓
STUN (Our Approach)	✓	✓	✓	✓

based on a star topology with a gateway on the premises [43], while other architectures, such as UG to satellite [50] and UG to unmanned aerial vehicles (UAV) [52], [53], have been explored recently.

Salient use cases of WUSNs include soil property monitoring [54], [52], [55], [56], soil toxicity detection, infrastructure health monitoring [57], border surveillance [58], and security applications. In precision agriculture, underground sensors are widely deployed to measure critical parameters such as soil moisture, temperature, pH, nutrient levels, and salinity, enabling informed decisions regarding irrigation, fertilization, and other farming practices. Depending on deployment needs, sensors may operate entirely underground [58], with communication occurring either underground-to-underground [45], [46], [49] or underground-to-over-the-air [59], [15], [60], [61].

Underground channel modeling [62], [59], [15], [60], [61] has advanced in recent years. These models reveal that signal propagation is heavily influenced by soil dielectric properties, volumetric water content, and transmission frequency, all of which govern attenuation characteristics and communication range [61]. In underground-to-over-the-air communication, signals undergo a transition from a dense soil medium to a less dense air medium. This transition introduces unique challenges, including refraction, reflection losses, and significant signal distortion at the soil–air interface. Moreover, buried antennas are affected by the soil medium because the permittivity of the soil changes the antenna's resonant frequency [15], requiring antennas to be designed for a specific soil type [63]. Environmental variables such as soil texture, compaction, and moisture content further exacerbate these effects, often requiring adaptive modulation and transmission schemes.

In this work, we specifically focus on securing underground-to-over-the-air communication for the WUSNs by developing a protocol that ensures both authentication and data integrity verification. This type of communication is the most common connectivity approach for WUSNs, as observed in commercial products [64]. Using existing channel models and accounting for environmental variability, the proposed framework enhances the resilience of underground wireless communications, ensuring that data transmitted from underground nodes remains trustworthy and robust under real-world conditions.

B. Security of Agricultural Internet-of-Things Network

Security and privacy solutions for agricultural IoT remain in a nascent stage of development. Recent advances in this domain, such as those proposed by Yan *et al.* [18], [19], [20], introduce innovative techniques to estimate internode distances without revealing the precise locations of the underground nodes. These methods leverage homomorphic cryptosystems to ensure location confidentiality while enabling efficient distance computations. However, while such approaches address the confidentiality aspect, they do not sufficiently meet the integrity and authentication requirements essential for secure underground-to-over-the-air communication.

Ensuring that transmitted data remains unaltered during propagation and reception, and verifying the legitimacy of the communicating devices, are critical for the secure operation of underground networks. To this end, recent works have explored the adoption of zero-trust security architectures [21], which have inspired our efforts to design a signal-based authentication and integrity verification mechanism at the physical (PHY) layer.

In parallel, researchers have proposed application layer security enhancements based on machine learning and deep learning based data security [22], [23] as well as blockchain-based frameworks [24], [25], [26]. While these solutions demonstrate promise, they are predominantly tailored to specific use cases and often lack the generality required for widespread adoption across heterogeneous underground wireless.

Recent AI-driven security frameworks for encrypted network traffic provide useful cross-domain insights for underground wireless security. In particular, work by Ali *et al.* on DNS over HTTPS (DoH) threat detection demonstrates advanced architectural principles; including adaptive anomaly detection, decentralized trust verification, adversarial robustness, privacy-preserving inference, and explainable AI that, while not directly applicable to underground wireless systems due to distinct propagation and resource constraints, offer valuable inspiration for future trust establishment and security design in such

environments [65], [66], [67]. In contrast, we present STUN, a PHY-layer framework that ensures both the authenticity and integrity of transmitted information in an application-agnostic manner, thereby offering a more scalable and robust security foundation for underground wireless communication networks.

C. Secure Bootstrapping for Wireless Network

The key agreement between an underground and above-ground node can be based on the Diffie-Hellman key agreement protocol [68]. However, key exchange through a public channel can be vulnerable to man-in-the-middle attacks. To secure this key exchange, there are two primary approaches: out-of-band (OOB) [69], [70] and in-band [71], [72], [73], [74] communication. Several works have been conducted on secret-free bootstrapping wireless end nodes, including studies, which can be categorized as either out-of-band (OOB) [31], [32], [33], [34], [35], [36] or in-band [40], [75], [41], [76].

1) Out-of-Band Solutions: For OOB techniques, such as the one described in Liang *et al.* [31], the authors utilize a brightness channel to enhance security for wearables. Berg *et al.* [32] investigate the impact of visual stimuli on the performance of security-critical tasks, such as pairing two Bluetooth devices in the presence of unexpected visual stimuli. Another OOB pairing solution utilizes locally generated ambient sound [77], where the propagation delay of ambient sound signals is used to generate unique keys for key agreement. Whereas, [78], [79] proposes employing the unique IDs of IoT devices for identity-based encryption. Han *et al.* [33] propose a context-based pairing mechanism that leverages time as a common factor for different sensor types by utilizing their fingerprints. Gao *et al.* [34] utilized voiceprints extracted from sound transmission from the throat to the ear canal to establish a secure authentication scheme for earphones. In contrast, Chen *et al.* [35] utilize distinctions in chest motions during a speech to develop a secure multi-factor authentication system. One common aspect of these OOB techniques is the requirement for external hardware, which can increase costs and the need for an external communication channel, leading to higher computational costs during implementation. The challenges associated with implementing OOB techniques in underground networks are further compounded by the absence of OOB channels such as visual, audio, and user interaction. The burial of sensors underground renders OOB techniques unnecessary and challenging to implement.

2) In-Band Solutions: For in-band solutions, such as the study conducted by Pan *et al.* [40], the authors examined optimal signal cancellation attacker behavior over a wireless channel in an in-band setting. Ghose *et al.* [41] employ a helper device that had already established trust with one of the devices, enabling the devices to pair with each other without prior association to protect against signal cancellation attacks. However, several challenges are associated with in-band solutions. These include scalability, interference, bandwidth limitations, signal degradation, compatibility, and security concerns. Additionally, implementing in-band solutions like those proposed in Pan *et al.* [40]. Furthermore, in-band solutions that utilize hard-to-forge PHY-layer randomness are designed explicitly for wireless channels OTA, as seen in works like Zhang *et al.* [75] and Ghose *et al.* [41]. Another set of in-band pairing without pre-shared secrets include proximity [37], [38], [39], where differences in RSS are used to detect the proximity of IoT devices for authentication; location differences [80], [81], which utilize multiple antennas on a receiver near a sender for ad hoc pairing and authentication using location information.

These solutions do not apply to underground communication scenarios as they are developed for over-the-air communication. This motivated us to create an in-band bootstrapping approach for underground wireless nodes leveraging the unique and hard-to-forge PHY-layer properties specific to underground environments. We leverage the variations in path loss between different mediums to ensure the security of the communication channel, known only to legitimate devices. The adversary would need help guessing the pathloss at the transmitter and receiver ends, making this PHY-layer property challenging to forge. The security of our protocol relies on this principle, utilizing the hard-to-forge PHY-layer property of pathloss variations. We propose STUN to provide security for underground wireless networks. Our approach ensures confidentiality and incorporates mechanisms for data integrity and device authentication in underground-to-OTA communication. By implementing this security paradigm, we take a significant step towards safeguarding underground wireless networks. Furthermore, we explore the scalability of this security solution, demonstrating its potential to cover entire farmland areas.

III. Model and Preliminaries

In this section, we first define STUN's system and adversarial models, followed by the preliminaries of underground wireless channels. We begin by presenting Table II, which summarizes the frequently used notations in this paper.

TABLE II
Table of Notations

Notation	Description
A	Gateway
$\mathbf{T}$	Set of trusted nodes, $\mathbf{T} = \{T_i : i \in \mathcal{I}\}$
$\mathcal{I}$	Index set of trusted nodes
$\mathbf{L}_i$	Set of legitimate nodes, $\mathbf{L}_i = \{L_{ij} : j \in \mathcal{J}_i\}$
$\mathcal{J}_i$	Index set of legitimate nodes for each trusted node T_i
M	Adversary
d^u_{xy}	Underground path length between x and y
d^u_x	Underground depth of node x
d^a_{xy}	Aboveground path length between x and y
α^u_x	Underground attenuation constant at node x
β^u_x	Underground phase shift constant at x
η	OTA attenuation constant
ϵ^a_x	OTA permittivity constant
ϵ^u_x	Underground permittivity constant
μ_x	Relative permeability
P^{tx}_x	Transmit power of node x
P^{rx}_{xy}	Received power at node x from y
G_x	Antenna gain of the node x
PL^u	Underground pathloss
PL^a	Over-the-air pathloss
PL^ρ	Refraction loss
m_x	Message transmitted by node x
τ	Threshold for detection of adversarial node among T_i and L_{ij}
τ^i_x	Threshold for identifying outlier received signal strength (RSS) for T_i
d^u_{max}	Maximum sector size

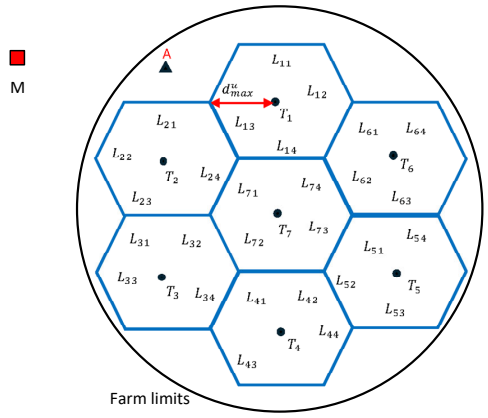


Fig. 2. Several underground Trusted nodes $T_i \in \mathbf{T}$ with the over-the-air gateway A deployed in the field in a hexagonal sector pattern in presence of an active adversary M outside the farm limits.

A. System Model

As shown in Fig. 2, the system model consists of four types of nodes: (1) Gateway, A, (2) Trusted nodes, $\mathbf{T} = \{T_i : i \in \mathcal{I}\}$, where $\mathcal{I}$ is the index set of trusted nodes, and (3) Sets of legitimate nodes, $\mathbf{L}_i = \{L_{ij} : j \in \mathcal{J}_i\}$, where $\mathcal{J}_i$ is the index set of legitimate nodes for each trusted node T_i, and (4) an active adversary, M.

Gateway (A)**:** The aboveground gateway coordinates, captures, and authenticates the data transmitted by the deployed nodes. Functioning as a tower, it receives messages from the underground legitimate and trusted nodes. The gateway is responsible for authenticating the data received from these legitimate nodes. Moreover, the gateway is located within the farm under the user's control.

Trusted Nodes $(\mathbf{T})$**:** The trusted nodes $\{T_1, T_2, \ldots, T_{|\mathcal{I}|}\}$ have high battery and computation power, enabling them to perform cryptographic functions efficiently. These nodes, deployed underground, collectively cover the entire farm in a sector-based deployment with a maximum sector size d^u_{max}, as shown in Fig. 2. A trusted channel between T_i and A is established using a shared secret K_{AT_i}, and transmissions are secured with authenticated encryption AE$(\cdot)$ [82]. This can be implemented as encrypt-then-MAC for symmetric cryptography or as a sign/encrypt/sign scheme for public key cryptography. The protocol, designed for a single T_i, can scale to multiple $\mathbf{T}$ nodes to ensure complete farm coverage.

Legitimate Nodes $(\mathbf{L}_i)$**:** The nodes $\{L_{i1}, L_{i2}, \ldots, L_{i|\mathcal{J}_i|}\}$ are deployed underground within the user's control and are within the communication range of at least one trusted node. These legitimate nodes collect and transmit data directly to A through a wireless channel. The deployment of the legitimate nodes is randomized, subject to application requirements, covering the entire farm area as depicted in Fig. 2.

B. Threat Model

We consider an active adversary (M), controlling one or more colluding devices. We assume that M ***operates outside the trusted farm's perimeter***, such as on adjacent roads, without entering the fields[2]. A remote adversary can compromise any infrastructure within the communication range of the farm to realize its goal. The adversary aims to either pair with A as a legitimate device L_{ij} or spoof a rogue gateway to pair with L_{ij}. As the secure bootstrapping session is initialized by a user, M attempts to realize this goal by launching a Man-in-the-Middle (MitM) attack during the pairing session. The MitM attack is performed by the adversary employing signal injection attacks, including overshadowing attacks, which require only 6dB stronger signal for LPWAN technologies [8]. While M knows the communication protocol, they lack physical access to the nodes and cannot perform jamming or physically block signals (e.g., via a Faraday cage). There are two types of attackers with advanced capabilities considered in this scenario.

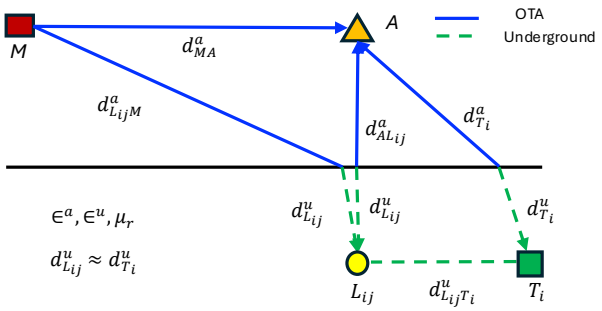


Fig. 3. M attempting to highjack the bootstrap session of L_{ij} with A.

Type 1 Adversary: This adversary attempts to inject its signal simultaneously at both A and T_i.

Type 2 Adversary: Type 2 adversary can deploy colluding aboveground and underground wireless nodes controlled by a single adversary in addition to the capabilities of Type 1 M. By leveraging these additional nodes, the Type 2 adversary can achieve the required received signal strength (RSS) at both A and T_i.

C. Preliminaries: Underground-to-Air Wireless Channel Model

We present the underground-to-OTA channel model, essential for the security protocol due to the channel's inherent unpredictability [13]. This study focuses on underground nodes communicating with an aboveground gateway. In underground communication, soil properties such as soil composition and soil moisture lead to a higher permittivity than in air, which in turn increases the attenuation for propagation of electromagnetic waves [16]. Moreover, variations in soil moisture alter the resonance characteristics of underground antennas, leading to additional loss. Furthermore, the soil-air interface, through which the waves propagate, causes reflection and refraction, impacting the received signal.

Consider a gateway, A, located aboveground, receiving wireless signal from an underground node L_{ij}, as illustrated in Fig. 3. The wireless signal travels a path length of $d_{AL_{ij}} = d^a_{AL_{ij}} + d^u_{L_{ij}}$, where $d^a_{AL_{ij}}$ represents the distance from the point where the signal crosses the soil-air border to node A, and $d^u_{L_{ij}}$ represents the vertical distance between the underground

[2]Trespassing is assumed to be deterred by law enforcement.

node and the soil-air interface. The underground path $d^u_{L_{ij}}$ is approximately equal to the depth of the underground node $d^u_{L_{ij}}$ since the dominant signal takes the shortest path to exit the underground environment [13]. The deployment depth of all the underground nodes and trusted node remains consistent, ensuring uniform signal propagation characteristics. At the soil-air border, the signal undergoes refraction due to the changes in the propagation medium. The power received by L_{ij} in dB can be expressed as [13]:

$$P^{rx}_{L_{ij}A} = P^{tx}_A + G_A + G_{L_{ij}} - PL^u - PL^a - PL^\rho, \quad (1)$$

where P^{tx}_A is the transmit power of the gateway (A), G_x is the antenna gain of the transceiver x, and PL^u, PL^a, PL^ρ are the losses due to underground and OTA paths, and refraction at the ground level, respectively in dB.

The path loss of the OTA wireless channel is given by [13]:

$$PL^a = C_a + 10\eta \log(d^a_{AL_{ij}}) + 20\log(f), \quad (2)$$

where $d^a_{AL_{ij}}$ is the distance between the point where the wireless channel transitions from underground to air and node A, η is the attenuation factor, f is the center frequency, and $C_a = -147.6$.

The path loss attributed to the underground channel is given by [13]:

$$PL^u = C_u + 20\log(d^u_{L_{ij}}) + 20\log(\beta^u_{L_{ij}}) + \rho_u \alpha^u_{L_{ij}} d^u_{L_{ij}}, \quad (3)$$

where $d^u_{L_{ij}}$ represents the depth of the underground node L_{ij}, α^u_x and β^u_x denote the attenuation and phase-shifting constants of the soil, and $C_u = 6.4, \rho_u = 8.69$, respectively.

Lastly, the path loss caused by refraction can be calculated separately for air-to-underground as follows:

$$PL_{\rho,a-u} = 20\log((r+1)/4),$$

where $r = \sqrt{(\sqrt{(\epsilon^a)^2 + (\epsilon^u)^2} + \epsilon^a)/2}$ represents the refractive index of the soil [13]. Alternatively, for the underground-to-air link, the signal propagates perpendicularly without refraction, resulting in $PL_{\rho,u-a} = 1$ [13].

IV. STUN:Secret-Free Trust-Establishment for Underground Wireless Networks

We introduce STUN, a trust establishment protocol for underground wireless networks that leverages the unique physical propagation properties of soil for secure in-band communication. STUN incorporates a unique PHY-layer trust verification primitive to authenticate the legitimacy of the underground nodes, $\mathbf{L}_i$, and ensure the integrity of their transmissions. In practice, the gateway A is not explicitly authenticated. Instead, its integrity is ensured through secure firmware installation and enrollment. In contrast, within STUN we explicitly authenticate A using the mechanism described in Section IV-A2.

A. STUN: The Protocol

The central concept involves A coordinating the key establishment process with each $\mathbf{L}_i$ in their respective sectors using a time division approach[3]. First, A creates a transmission schedule for T_i and broadcasts this schedule to all trusted nodes $\mathbf{T}$. Subsequently, each T_i sends a message to coordinate all legitimate nodes $\mathbf{L}_i$ within its communication range.

Once the legitimate nodes, $\mathbf{L}_i$, receive the coordination message from T_i, they transmit their key primitives in a time division manner. These key primitives are then verified by the trusted node and the gateway to ensure their authenticity and integrity. *Without loss of generality, we present STUN with the Diffie-Hellman key exchange protocol [68], which can be interchanged with any other key exchange protocol with desired security properties.* ***STUN is a message authentication and integrity verification technique for the key primitive exchange to strengthen any underlying key exchange.*** We present the protocol for both uplink and downlink communications.

1) Securing Uplink ($\mathbf{L}_i$-to-A) communication: The trust establishment protocol consists of the following steps:

1) **Initialization:** The protocol begins with A transmitting a synchronization message to $\mathbf{L}_i$ and $\mathbf{T}$. Next, A schedules all participating trusted nodes $ID_{T_1}, \ldots, ID_{T_{|\mathcal{I}|}}$. The gateway sends an initialization message to T_i as $\text{AE}_{K_{AT_i}}(\text{INIT}||\eta)$, where η is a nonce. $\text{AE}_{K_{AT_i}}$ ensures the confidentiality and integrity of the message using a shared key K, allowing only T_i to decrypt and verify it. All entities agree on Diffie-Hellman (DH) public parameters: $\mathbb{G}, q, g$.
2) **Initialization of a sector:** The trusted node, T_i, broadcasts a Ready-to-Authenticate (RTA) message to all the underground nodes in the vicinity, $\mathbf{L}_i$.
3) **Primitive transmission from $\mathbf{L}_i$:** Each legitimate node, $L_{ij} \in \mathbf{L}_i$, picks a secret value, $X_{ij} \in_U \mathbb{Z}_q$, computes the public value, $z_{ij} \leftarrow g^{X_{ij}}$, and transmits its message, $m_{ij} \leftarrow \{ID_{ij}, z_{ij}\}$.
4) **Verification at T_i:** T_i synchronizes with the preamble and receives all the messages, $m'_{ij}\ \forall\ j = 1, \ldots, |\mathcal{J}_i|$, and records the corresponding received signal strength (RSS), $\mathbf{r}^{T_i}_j = \{r^{T_i}_j(1), r^{T_i}_j(2), \ldots, r^{T_i}_j(\ell)\}$. Finally, T_i performs the following verification if
$$\tau^{T_i}_{low} \le \mathbf{r}^{T_i}_j(\kappa) \le \tau^{T_i}_{high};\ \ \forall\ j = 1, \ldots |\mathcal{J}_i|;\ \kappa = 1 \ldots \ell.$$
After successful verification, the trusted node relays $m_i := \text{AE}_{K_{AT_i}}(m'_{i1}||ID_{i1}, \ldots, m'_{ij}||ID_{ij}, \ \ldots, m'_{i|\mathcal{J}_i|}||ID_{i|\mathcal{J}_i|})$ to A after $L_{i|\mathcal{J}_i|}$'s transmission in a time division fashion.
5) **Reception at A:** The gateway, A, records RSS samples, $\mathbf{r}_{ij} = \{r_{ij}(1), r_{ij}(2), \ldots, r_{ij}(\ell)\}$, while receiving m''_{ij}. Further, A records the RSS samples, $\mathbf{r}_{T_i} = \{r_i(1), r_i(2), \ldots, r_i(\ell')\}$, while receiving m'_i.
6) **Verification at A:** The gateway decrypts m'_i to obtain $m'_{ij}||ID_{ij}\ \forall\ j = 1, \ldots, |\mathcal{J}_i|$ and verifies its integrity using the corresponding verification function. A rejects all

[3]In this work, we assume a time-division approach, whereas any medium access control approach could be adopted without loss of generality.

received messages if verification fails. Further, A verifies $m'_{ij} \stackrel{?}{=} m''_{ij}\ \forall\ j = 1, \ldots, |\mathcal{J}_i|$; and rejects if the verification fails. Finally, A computes:

$$\Gamma_{ij} = \{\gamma_{ij}(1), \gamma_{ij}(2), \ldots, \gamma_{ij}\ell\}, \quad \gamma_{ij}(\kappa) = \frac{r_i(\kappa)}{r_{ij}(\kappa)}$$

$\forall\ j = 1, \ldots, |\mathcal{J}_i|$. The gateway accepts m''_{ij} if $\tau_{low} \leq \gamma_{ij}(\kappa) \leq \tau_{high};\ \ \forall\ \kappa = 1 \ldots \ell,\ j = 1, \ldots, |\mathcal{J}_i|$.

7) **Primitive transmission from A:** Following successful verification, A picks a secret value, $X_A \in_U \mathbb{Z}_q$, computes the public value, $z_A \leftarrow g^{X_A}$, and transmits as $m_A \leftarrow \{ID_A, z_A\}$.
8) **Key establishment:** After reception of the message, $\mathbf{L}_j$ computes the pairwise keys as $K_{Aij} \leftarrow (z_A)^{X_{ij}}$ and A computes as $K_{Aij} \leftarrow (z_{ij})^{X_A}$. Immediately following the key agreement, L_{ij} and A engage in a key confirmation phase, initiated by L_{ij}. This can be done by executing a two-way challenge-response protocol [83].
9) **Repeat for all sectors:** All the above steps are repeated for $i = 1, \ldots, |\mathcal{I}|$. If any of the steps fail for a legitimate node, L_{ij}, is detected at any of the entities, and the steps are repeated for the node. Otherwise, the gateway, A, notifies the user of the successful completion of the trust establishment.

If trust establishment steps like key confirmation fail, it may indicate adversarial activity or communication issues. The affected node can notify a trusted node to retry the process, maintaining protocol integrity. Persistent failures may require human intervention to address potential security breaches.

2) Securing Downlink (A-to-$\mathbf{L}_i$) communication: In the protocol outlined in Section IV-A1, underground nodes (L_{ij}) do not explicitly verify the authenticity of gateway messages (m_A) during the key confirmation process. An adversary (M) impersonating the gateway would disrupt the session with the legitimate gateway (A), triggering protocol failure and user notification. Trusted nodes (T_i) are employed to enable explicit message verification. After A validates messages from L_{ij} nodes, it sends an authenticated and encrypted version (m'_A) to T_i using a shared key (K_{AT_i}). Simultaneously, A broadcasts the plaintext message (m_A) to all L_{ij} nodes and their respective T_i nodes. Each T_i verifies the authenticity of m_A by comparing it with m'_A. Depending on the result, T_i broadcasts a success or failure message. While adversaries could exploit this to perform a DoS attack, such scenarios are outside the scope of this work.

3) Size of T_i's Sector: The size of the sector for T_i is determined by the maximum possible distance, denoted as d^u_{max}, between the trusted node, T_i, and the legitimate nodes, $\mathbf{L}_i$. We employ the underground path loss model given by (3) to calculate this distance. Considering the assumption that the legitimate nodes, $\mathbf{L}_i$, have lower capabilities and transmit at lower power compared to T_i, this determines the communication range of the sector. The size of T_i's sector can be calculated using (3), yielding the following expression:

$$d^u_{max} = \frac{20W\left(\alpha^u_x \rho_u e^X K\right)}{\alpha^u_x \rho_u \log(10)}, \tag{4}$$

where $K = \log(10)/20$ is a constant multiplier, and $X = [\log(10^{-C_u}) + PL^u \log(10) - 20\log(\beta^u_x)]/20$ is an intermediate variable that encapsulates the logarithmic and path loss dependencies. Each T_i broadcasts the RTA message in Step 2. This message is received by every L_{ij} in range. In the case that one L_{ij} receives messages from multiple T_is, it selects the T_i with the higher-power signal.

B. Selection of Thresholds

Now, we first theoretically describe selecting the thresholds utilized in Steps 3 and 5 of STUN:

1) Thresholds for T_i: The detection thresholds at trusted nodes (T_i) for identifying outlier RSS values are determined using the Median Absolute Deviation (MAD) method, a robust measure less sensitive to outliers compared to standard deviation [84]. The thresholds are defined as:

$$\tau^{T_i}_{low} = \widetilde{\mathbf{r}^{T_i}_j} - \zeta * \nu, \quad \tau^{T_i}_{high} = \widetilde{\mathbf{r}^{T_i}_j} + \zeta * \nu, \tag{5}$$

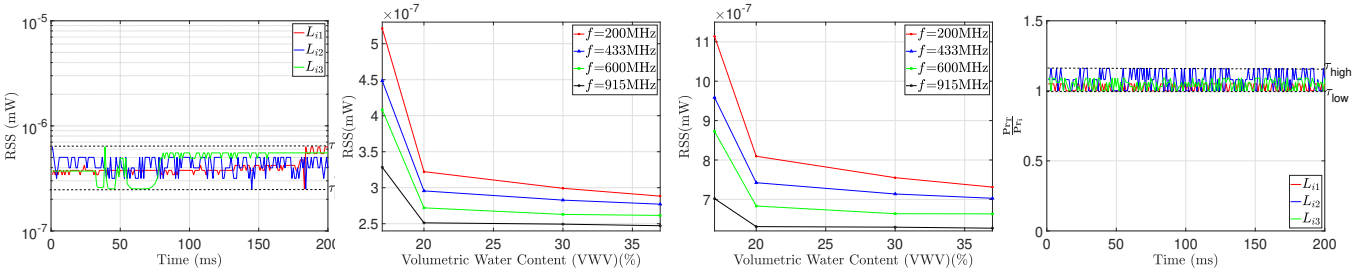
where $\widetilde{\mathbf{r}^{T_i}_j}$ is the median of all the RSS samples, ζ controls the strictness of the outlier rule, and ν is MAD

$$\nu = b \cdot |\widetilde{\mathbf{r}^{T_i}_j - \mathbf{r}^{T_i}_j}|, \tag{6}$$

where $\tilde{\cdot}$ is the median of all the samples over all the nodes, and $b = 1/Q(0.75) = 1.4826$. Empirical results [51] in Fig. 4(a) illustrate that the RSS received at T_i from three underground nodes. We observe that the RSS is relatively stable over time and that the $\tau^{T_i}_{low} = 2.512 \times 10^{-7}$mW and $\tau^{T_i}_{high} = 6.309 \times 10^{-7}$mW, due to high path loss of the underground communication.

For calculating the received signal strength (RSS), we kept an underground depth of $d^u_{L_{ij}}$, and $d^u_{T_i}$ fixed at 0.2m, and the distance between the underground nodes and the trusted device was kept constant at $d^u_{L_{ij}T_i} = 1.0$m. The outdoor testbed contains 13.09cm of silty clay loam soil with varying volumetric water content (VWC) ranging from 17% (dry) to 37% (wet). From Fig. 4(b) and (c), we observe that when the volumetric water content (VWC) of the soil increases, the received power goes down. As we know, when the VWC increases, the dielectric constant of the soil also increases. Hence, we need to calibrate the trusted node thresholds based on the VWC of the soil or the dielectric constant (which can change due to changes in salinity, fertilizer, etc.).

Recalibration of threshold. The calibration at the start of each STUN protocol is performed based on the received signal strength (RSS) from a legitimate node. The detection thresholds at trusted nodes (T_i) for identifying outlier RSS values are determined using the Median Absolute Deviation (MAD) method, a robust measure less sensitive to outliers compared to standard deviation [84]. Any attack during the recalibration process is handled by the Median Absolute Deviation (MAD) method [84]. Any overshadowing attack can be detected as the signal will be an outlier for the MAD method. The recalibration process is required before each bootstrapping and the threshold remains stable during the bootstrapping.



(a) (b) (c) (d)

Fig. 4. (a) Power received at the trusted node from three $\mathbf{L}_i$, power received at the trusted node from $\mathbf{L}_i$ at depth of 0.2m against volumetric content of water (VWC) (%) of soil for varying center frequency (b) for $d^u_{L_{ij}T_i} = 2.1$m, (dc) $d^u_{L_{ij}T_i} = 1.0$m, and (d) RSS ratio at A of power received from T_i to power received from $\mathbf{L}_i$.

2) Thresholds for A: To calculate the threshold for the gateway, the power received from the trusted node, T_i, is divided by the power received from the legitimate node, $\mathbf{L}_i$. The threshold can be expressed as:

$$\tau = 20\log(d^u_{T_i}) - 20\log(d^u_{L_{ij}}) + 20\log(\beta^u_{T_i}) - 20\log(\beta^u_{L_{ij}}) + \rho_u\alpha^u_{T_i}d^u_{T_i} - \rho_u\alpha^u_{L_{ij}}d^u_{L_{ij}}\ , \tag{7}$$

where $d^u_{T_i}$ is the underground depth of the trusted node, $d^u_{L_{ij}}$ is the underground depth of L_{ij}, and α^u_x and β^u_x are the parameters due to soil characteristics. The aboveground distance to the gateway A cancels out due to the proximity of the underground node. Since variations in the OTA path loss may affect the accuracy of this calculation, an adjustment factor δ_{low} and δ_{high} are introduced. Two thresholds are then defined as:

$$\tau_{low} = \tau - \delta_{low},\quad \tau_{high} = \tau + \delta_{high}. \tag{8}$$

Empirical results in (Fig. 4(d)), illustrate that the RSS ratio between signals from T_i and $\mathbf{L}_i$ remains close to 1 over time. The calculated thresholds $\tau_{low} = 0.9$ and $\tau_{high} = 1.160$, indicate less than 10% error due to underground fading. This confirms the protocol's effectiveness in mitigating the impact of underground channel variability on OTA communication.

V. Security Analysis of STUN

We analyze the security of STUN against the adversary defined in Section III-B. In an attempt to pair with the gateway A, the adversary can compute $z_M := g^{X_M} \mod p$ where X_M is uniformly chosen from the set $\mathbb{Z}_q$. Then compiling and injecting a message $m_M := \{ID_M, z_M\}$ to the gateway A. However, for A to accept the message, the adversary must pass the verification of Steps 4 and 6 at T_i and A, respectively, in STUN's verification. We will first analyze a Type 1 adversary followed by a Type 2 adversary.

A. Type 1 Adversary

A Type 1 M is a remote aboveground entity outside the farm, injecting m_M into A and T_i with power P^{tx}_M as shown in Fig. 3. M has to compute the power P^{tx}_M to defeat Step 4 and Step 6 simultaneously. In the next proposition, we evaluate the adversary's capability to compute the transmit power P^{tx}_M. It should be noted here that M does not have a visual channel to T_i and $\mathbf{L}_i$ to know their actual locations underground. We present the proof for single and multiple $\mathbf{T}$.

Proposition 1. *A Type 1 aboveground adversary M simultaneously injecting messages at T_i, as well as A can be detected with certainty if the distance between M and A does not satisfy*

$$\begin{aligned}10\eta\log(d^a_{MA}) = {} & C_a + C_u + PL_{\rho,a-u} + \rho_u\alpha^u_{L_{ij}}d^u_{L_{ij}T_i} \\ & + \eta 10\log(d^a_{AT_i}) + \eta 10\log(d^a_{MT_i}) \\ & + 20\log(\beta^u_{T_i}) - 20\log(\beta^u_{L_{ij}}) \\ & + 40\log(d^u_{T_i}) - 20\log(d^u_{L_{ij}T_i}) + 20\log(f),\end{aligned}$$

where d^a_{xy} is the aboveground distance between x and y, d^u_{xy} is the underground distance between x and y, d^u_x is the underground depth of x, α^u_x and β^u_x are the underground attenuation constant and phase shifting constants for transmission from x, respectively, η is the OTA attenuation constant, and $\delta = \delta^a \pm \delta^u$, where δ^a is the relaxation introduced by the outlier evaluation technique and δ^u is the relaxation introduced due to the threshold selection.

Proof. A Type 1 adversary M injecting its message from an aboveground location will need to pass the verification of Steps 4 and 6 for A to accept and bootstrap M. We evaluate the strategy of M to compute the transmit power independently for steps 4 and 6, and then we evaluate the effect of one step on the other. Using (1), (2), (3), and Step 4, the transmit power required by M for passing the verification in Step 4. The power received at T_i from L_{ij} is given by for $C_u = 6.4$ and antenna gains G_X

$$\begin{aligned}P^{rx}_{T_iL_{ij}} = {} & P^{tx}_{L_{ij}} + G_{L_{ij}} + G_{T_i} - C_u \\ & - 20\log(d^u_{L_{ij}T_i}) - 20\log(\beta^u_{L_{ij}}) \\ & - \rho_u\alpha^u_{L_{ij}}d^u_{L_{ij}T_i}.\end{aligned} \tag{9}$$

Moreover, the power received from M at T_i is given by for $C_a = -147.6$

$$\begin{aligned}P^{rx}_{T_iM} = {} & P^{tx}_M + G_M + G_{T_i} - C_a - C_u - 10\eta\log(d^a_{MT_i}) - 20\log(f) \\ & - 20\log(d^u_{MT_i}) - 20\log(\beta^u_{T_i}) - \rho_u\alpha^u_{T_i}d^u_{MT_i} - PL_{\rho,a-u}.\end{aligned} \tag{10}$$

In Step 4, T_i accepts M's signal if (9) and (10) are satisfied with some relaxation, which gives M's transmit power as

$$\begin{aligned}P^{tx}_M = {} & P^{tx}_{L_{ij}} + G_{L_{ij}} - G_M + C_a - 20\log(d^u_{L_{ij}T_i}) \\ & + 20\log(d^u_{MT_i}) - 20\log(\beta^u_{L_{ij}}) + 20\log(\beta^u_{T_i}) \\ & + \rho_u\alpha^u_{L_{ij}}d^u_{L_{ij}T_i} - \rho_u\alpha^u_{T_i}d^u_{MT_i} + 10\eta\log(d^a_{MT_i}) \\ & + 20\log(f) + PL_{\rho,a-u} \pm \delta^a,\end{aligned} \tag{11}$$

where d^a_{xy} is the aboveground distance between x and y, d^u_{xy} is the underground distance between x and y, α^u_x and β^u_x the underground attenuation constants and phase shifting constants for x, respectively, η is the OTA attenuation constant, and δ^a is the relaxation for the outlier evaluation technique.

Now, for evaluating the capability of Type 1 M in defeating Step 6, we compute the power received by A:

$$P^{rx}_{AM} = P^{tx}_M + G_M + G_A - C_a - 10\eta\log(d^a_{MA}) - 20\log(f). \quad (12)$$

Then the power received by the gateway from T_i is:

$$P^{rx}_{AT_i} = P^{tx}_{T_i} + G_A + G_i - C_a - C_u - 10\eta\log(d^a_{AT_i}) - 20\log(f) - 20\log(d^u_{T_i}) - 20\log(\beta^u_{T_i}) - \rho_u\alpha^u_{T_i}d^u_{T_i}. \quad (13)$$

Equating (13) and (12) and equating to the threshold (7), we compute the transmission power to pass Step 6 as:

$$P^{tx}_M = P^{tx}_{T_i} - G_M + G_{T_i} - C_u - 10\eta\log(d^a_{AT_i}) + 10\eta\log(d^a_{MA}) - 20\log(d^u_{T_i}) - 20\log(\beta^u_{T_i}) - \rho_u\alpha^u_{T_i}d^u_{T_i} \pm \delta^u, \quad (14)$$

where δ^u is the relaxation introduced due to the threshold selection. Now, for the adversary to pass both the verification simultaneously, the transmit power in (11) should equate to the transmit power in (14). Equating (11) and (14) and approximating $d^u_{MT_i} \approx d^u_{AT_i} \approx d^u_{T_i}$ to depth of the node, we compute the distance between the adversary and the gateway as:

$$10\eta\log(d^a_{MA}) = C_a + C_u + PL_{\rho,a-u} + \rho_u\alpha^u_{L_{ij}}d^u_{L_{ij}T_i} + \eta 10\log(d^a_{AT_i}) + \eta 10\log(d^a_{MT_i}) + 20\log(\beta^u_{T_i}) - 20\log(\beta^u_{L_{ij}}) + 40\log(d^u_{T_i}) - 20\log(d^u_{L_{ij}T_i}) + 20\log(f), \quad (15)$$

where $\delta = \delta^a \pm \delta^u$, and assuming $P^{tx}_{L_{ij}} + G_{L_{ij}} - P^{tx}_{T_i} - G_i = 0$, or the power transmitted by the legitimate and trusted node is the same, and the antenna gains are the same. Therefore, a Type 1 adversary at d^a_{MA} of the gateway can defeat STUN by transmitting from an aboveground location. □

When several trusted nodes are installed on the farm and transmit information to a single A, numerous legitimate nodes are also deployed in a single/multiple node(s)-to-single trusted node arrangement in each sector to cover the entire farm. Each trusted node is connected to at least one legitimate node, and all the nodes are transmitting their signal to A, where $L_{ij} \in \mathbf{L}_i$ and $T_i \in \mathbf{T}$. We provide empirical results to visualize this distance in Section VI-C1. Our experimental results show that ***an adversary would require an infeasibly high transmission power of*** $\approx 10^6$***W, and the adversary needs to be positioned at a very far distance reaching about*** ≈ 5***Km range to execute this attack, making such an attack impractical.***

1) Security Against a Rogue Gateway: An aboveground Type 1 M attempts to inject m_M at one or more legitimate nodes (L_{ij}), emulating a rogue A. The adversary, typically located outside the farm's perimeter, is assumed to be closer to the legitimate node than the trusted node, resulting in lower attenuation to L_{ij}. The adversary's message (m_M) is simultaneously received by both L_{ij} and the corresponding trusted node (T_i) in the same underground environment. For m_M to be reliably received at T_i, the signal-to-noise ratio (SNR) at T_i must equal the SNR at L_{ij}. To analyze this, the power received by the trusted node ($P^{rx}_{T_iM}$) and the legitimate node ($P^{rx}_{L_{ij}M}$) from the adversary is evaluated. The conditions under which $P^{rx}_{T_iM}$ is greater than or equal to $P^{rx}_{L_{ij}M}$ are derived, considering the adversary's transmission power (P^{tx}_M) and its relative proximity to L_{ij} compared to T_i.

Proposition 2. *An aboveground Type 1 M attempting to pair with any underground node L_{ij} as a rogue gateway can be detected with certainty when located at a distance given by:*

$$10\eta\log(d^a_{MT_i}) - 20\log(d^u_{T_i}) - 20\log(\beta^u_{T_i}) - \rho_u\alpha^u_{T_i}d^u_{T_i} \geq 10\eta\log(d^a_{L_{ij}M}) - 20\log(d^u_{L_{ij}}) - 20\log(\beta^u_{L_{ij}}) - \rho_u\alpha^u_{L_{ij}}d^u_{L_{ij}},$$

where d^a_{xy} is the aboveground distance between x and y, and d^u_x is the underground depth of x. $\beta^u_{L_{ij}}$ and $\alpha^u_{L_{ij}}$ are the attenuation and phase-shifting constants, for each node L_{ij}, respectively.

Proof. In an attempt to force a legitimate node L_{ij} with itself, the adversary M injects their message m_M with transmit power P^{tx}_M to over overshadow A's message m_A. For evading detection, m_M should be received at L_{ij} and simultaneously not received at the corresponding T_i. We consider the best case for the adversary where the legitimate node is closer to the adversary than the trusted node, as shown in Fig. 3, such that the attenuation from the adversary to the legitimate node is lower than the trusted node.

We compute the power received by L_{ij} from M given by

$$P^{rx}_{L_{ij}M} = P^{tx}_M + G_M + G_{L_{ij}} - C_a - C_u - 10\eta\log(d^a_{L_{ij}M}) - 20\log(f) - 20\log(d^u_{L_{ij}M}) - 20\log(\beta^u_{L_{ij}}) - \rho_u\alpha^u_{L_{ij}}d^u_{L_{ij}M} - PL_{\rho,a-u}, \quad (16)$$

where P^{tx}_M is the transmit power by M, G_x is the antenna gains of the transceivers, $PL_{\rho,a-u}$ is the air-to-underground path loss, d^a_{xy} is the above ground distance between x and y, d^u_{xy} is the underground distance between x and y, f is the center frequency, α^u_x, β^u_x are the underground attenuation and phase shift constant from x.

Next, we compute the power simultaneously received by the corresponding trusted node T_i from M, given by

$$P^{rx}_{T_iM} = P^{tx}_M + G_M + G_{T_i} - C_a - C_u - 10\eta\log(d^a_{MT_i}) - 20\log(f) - 20\log(d^u_{MT_i}) - 20\log(\beta^u_{T_i}) - \rho_u\alpha^u_{T_i}d^u_{MT_i} - PL_{\rho,a-u}, \quad (17)$$

where P_M^{tx} is the transmit power by M, G_x is the antenna gains of the transceivers, $PL_{\rho,a-u}$ is the air-to-underground path loss, d_{xy}^a is the above ground distance between x and y, d_{xy}^u is the underground distance between x and y, f is the center frequency, α_x^u, β_x^u are the underground attenuation and phase shift constant from x.

For the Type 1 adversary to be detected, the message m_M should be received simultaneously at T_i and L_{ij}, as the detection is performed at T_i. This happens with certainty if the received power received $P_{T_iM}^{rx} \geq P_{L_{ij}M}^{rx}$, or T_i receives higher power than L_{ij}. This is under the assumption both T_i and L_{ij} are in similar underground environment such as SNR at T_i is greater than or equal to that of L_{ij}. Now from (17) and (16); $P_{MT_i}^{rx} \geq P_{L_{ij}M}^{rx}$ gives:

$$\begin{aligned} &P_M^{tx} + G_M + G_{T_i} - C_a - C_u - 10\eta \log(d_{MT_i}^a) - 20\log(f) \\ &- 20\log(d_{MT_i}^u) - 20\log(\beta_{T_i}^u) - \rho_u \alpha_{T_i}^u d_{MT_i}^u - PL_{\rho,a-u} \\ &\geq P_M^{tx} + G_M + G_{L_{ij}} - C_a - C_u - 10\eta \log(d_{L_{ij}M}^a) \\ &- 20\log(f) - 20\log(d_{L_{ij}M}^u) - 20\log(\beta_{L_{ij}}^u) \\ &- \rho_u \alpha_{L_{ij}}^u d_{L_{ij}M}^u - PL_{\rho,a-u}. \end{aligned} \tag{18}$$

Now we can simplify the numerator if we assume $G_{T_i} = G_{L_{ij}}$, this is a valid assumption with the most underground sensors equipped with similar wireless modules. Under the assumption that T_i and L_{ij} are in similar underground environments, they will experience similar OTA-to-underground pathloss. Hence we can simplify $PL_{\rho,a-u}$ and approximating $d_{Mx}^u \approx d_{Ax}^u \approx \log(d_x^u)$ to depth of the node x which gives:

$$\begin{aligned} 10\eta \log(d_{MT_i}^a) - 20\log(d_{T_i}^u) - 20\log(\beta_{T_i}^u) - \rho_u \alpha_{T_i}^u d_{T_i}^u \\ \geq 10\eta \log(d_{L_{ij}M}^a) - 20\log(d_{L_{ij}}^u) \\ - 20\log(\beta_{L_{ij}}^u) - \rho_u \alpha_{L_{ij}}^u d_{L_{ij}}^u, \end{aligned} \tag{19}$$

where d_{xy}^a is the above ground distance between x and y, d_{xy}^u is the underground distance between x and y, $\beta_{L_{ij}}^u$ and $\alpha_{L_{ij}}^u$ are the attenuation and phase-shifting constants, for each node $L_{ij} \in \mathbf{L}_i$, respectively. □

The inequality in Proposition 2 can be simplified using numerical methods like the Newton-Raphson approximation [85]. In Fig. 5, we approximate the distances between the adversary (M), the legitimate node (L_{ij}), and the trusted node (T_i), assuming $d_{MT_i}^u = d_{L_{ij}M}^u + d_{L_{ij}T_i}^u$. Solving for these distances requires optimization techniques, where convergence depends on factors like the initial guess (x_0), tolerance (tol), and the number of iterations (N_{max}). Precision in setting tolerance and monitoring convergence is critical to balance computational cost and accuracy, as improper settings may prevent convergence or lead to suboptimal results.

Figures 5(a) and (b) illustrate that small changes in $d_{L_{ij}T_i}^u$ ***significantly affect the underground distance between*** M ***and*** L_{ij}, making it difficult for M, which lacks precise knowledge of T_i's location, to target legitimate nodes without being detected. Similarly, Figures 5(c) and (d) show that even slight variations in legitimate underground distances ***require the adversary to transmit at very high power levels to compensate for attenuation***. For instance, to avoid detection, M must be located approximately 1 km away and transmit at an infeasible power of about 10^{47} W. This supports the hypothesis that an adversary outside the farm's limits emulating a rogue gateway will be detected with certainty.

B. Type 2 Adversary

A Type 2 M is a remote aboveground adversary colluding with an underground adversarial node outside the farm injecting m_M transmitting at aboveground power P_M^{tx}, and underground P_M^{tx} to A and T_i, respectively as shown in Fig. 6. M with a visual channel to A may be able to predict the channels for computing the aboveground power P_M^{tx} to defeat Step 6. In the next proposition, we evaluate the adversary's capability to compute the transmit underground power P_M^{tx} for defeating Step 4. It should be noted here that M does not have a visual channel to T_i and $\mathbf{L}_i$. We present the proof for single then generalizing for multiple $\mathbf{T}$.

Proposition 3. *STUN can detect a Type 2 aboveground and underground colluding adversary M injecting message at T_i and A with certainty if at least four legitimate nodes participate in STUN bootstrapping for every trusted node.*

Proof. The colluding Type 2 adversary's underground node in an attempt to defeat Step 4 of STUN must overshadow all the transmissions from the legitimate nodes $\mathbf{L}_i$ in that sector. This is because if the adversary allows any one of the transmissions from $\mathbf{L}_i$ to reach T_i, it will be the outlier and cause STUN to fail. Moreover, without a visual channel to the legitimate nodes and not knowing the location of the target legitimate node. M cannot just target one legitimate node. The adversary has to compute the transmit power to overshadow all the legitimate nodes $\mathbf{L}_i$ in a sector. Thus, according to MAD, it can pass the thresholds set at T_i. The underground node of the colluding Type 2 adversary has to transmit at least an underground power P_M^{tx} for each of $\mathbf{L}_i$ such that its power is within the acceptable range of the other legitimate underground nodes $\mathbf{L}_i$. Further, the adversary cannot just transmit a very high power as that will be detected by other trusted nodes. As the detection in Step 4 is performed by detecting the outlier, the transmit power has to satisfy (11).

Therefore, the adversary has to compute its transmit power according to the equation system S to overshadow all the underground nodes in a sector:

$$(S) \begin{cases} P_M^{tx} = P_{L_{i1}}^{tx} + G_{L_{i1}} - G_M + 20\log(d_{MT_i}^u) - 20\log(d_{L_{i1}T_i}^u) \\ \quad +20\log(\beta_M^u) - 20\log(\beta_{L_{i1}}^u) + \rho_u \alpha_M^u d_{MT_i}^u - \rho_u \alpha_{L_{i1}}^u d_{L_{i1}T_i}^u, \\ \vdots \\ P_M^{tx} = P_{L_{i|\mathcal{J}_i|}}^{tx} + G_{L_{i|\mathcal{J}_i|}} - G_M + 20\log(d_{MT_i}^u) \\ \quad -20\log(d_{L_{i|\mathcal{J}_i|}T_i}^u) + 20\log(\beta_M^u) - 20\log(\beta_{L_{i|\mathcal{J}_i|}}^u) \\ \quad +\rho_u \alpha_M^u d_{MT_i}^u - \rho_u \alpha_{L_{i|\mathcal{J}_i|}}^u d_{L_{i|\mathcal{J}_i|T_i}}^u. \end{cases} \tag{20}$$

The equation system S is an underdefined multivariate quadratic equation system. It is well known that the solution of such an equation system is NP-hard [17]. Moreover, even for small values of some equations (e), the best-known algorithms

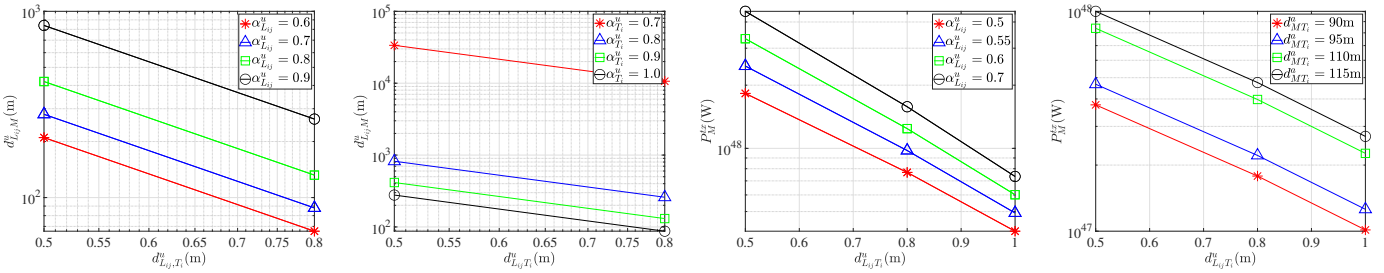


Fig. 5. The distance of Type 1 M from the legitimate nodes against the distance of the legitimate nodes from the trusted nodes while varying, (a) the attenuation of the legitimate nodes, (b) attenuation of the trusted node. Plots of the power transmitted from the Type 1 M to the legitimate node against the legitimate underground distances while varying, (c) the attenuation $\alpha^u_{T_i}$, and (d) aboveground M distance from T_i.

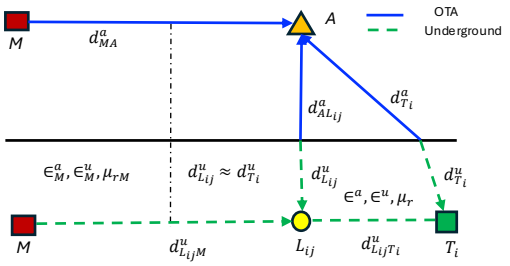


Fig. 6. A Type 2 M attempting to inject m_M to hijack the bootstrap session of L_{ij} with A with T_i performing simultaneous STUN verification.

perform an exhaustive search [17]. Therefore, this type of system is known as an Unbalanced Oil and Vinegar (UOV) signature scheme (NP-hard problem of underdefined systems of multivariate equations). The security of UOV systems is proved for $3e \leq v \leq {}^{e(e+2)}/_{2}$ [17]. Where the system has e equations and v unknowns. Out of the total number of variables, e is known as the "oil" unknowns, and $(v-e)$ is called the "vinegar" unknowns. For our equation system S, we have seven variables in S which are known to underground transmit power of the legitimate node $(P^{tx}_{L_{ij}})$, gain of antenna (G_x), operating frequency (f), and the relaxation introduced by the outlier evaluation technique (δ^a). Further, there are six variables in S which are unknown transmit power of the underground adversary (P^{tx}_M), distance from the adversary to the trusted node $(d^a_{MT_i})$, soil parameters (permittivity constants (ϵ^a, ϵ^u), relative permeability (μ_r)) as these control the variables $(\alpha^u_{L_{ij}}$, α^u_M, $\beta^u_{L_{ij}}$ and $\beta^u_M)$, and distance between the legitimate node and trusted node $d^u_{L_{ij}T_i}$. Hence, S has $n+5$ number variables for n number of equations, where n is the number of legitimate node in our setup. Therefore, to satisfy the conditions for the UOV public cryptosystem, the minimum number of legitimate nodes required per trusted node is four. □

Hence, a Type 2 adversary cannot pass Step 4 with certainty. In addition, it is essential to note that in practice, the underground-to-underground wireless channel (e.g., M-T_i) has a limited communication range (i.e., less than 10m [61]). Consequently, in typical deployment conditions, ***any adversary positioned outside the farm limits and attempting to pass Step 4 would be beyond the communication range of*** T_i. Therefore, Type 2 attacks are practically rare and otherwise detectable, as per Proposition 3. This is even more challenging if the adversary wants to defeat multiple sectors because each sector contains at least four legitimate nodes per trusted node.

1) Security Against a Rogue Gateway : A colluding Type 2 adversary at a distance aboveground and underground outside the farm's perimeter injects its signal at the legitimate nodes $\mathbf{L}_i$ to emulate a rogue A's signal, as shown in Fig. 6. Without access to the secure channel between A-to-T_i, the adversary has to inject the signal such that it cannot be detected by corresponding T_i. Now we evaluate whether a Type 2 adversary can transmit underground power P^{tx}_M such that it is only received at $\mathbf{L}_i$, and not at the corresponding T_i.

Proposition 4. *An aboveground and underground Type 2 colluding adversary M attempting to pair with underground nodes $\mathbf{L}_i$ as a rogue gateway can be detected with certainty when located at a distance*

$$20\log(d^u_{L_{ij}M}) + 20\log(\beta^u_{L_{ij}}) + \rho_u \alpha^u_{L_{ij}} d^u_{L_{ij}M} \geq 20\log(d^u_{L_{ij}T_i}) + 20\log(\beta^u_{T_i}) + \rho_u \alpha^u_{T_i} d^u_{L_{ij}T_i},$$

where d^u_{xy} is the underground distance between entities x and y,, and β^u_x and α^u_x are the attenuation and phase-shifting constants, respectively.

Proof. The underground node of the colluding Type 2 adversary has to transmit at an underground power P^{tx}_M to the legitimate nodes and must be at a distance that is less than the distance of the legitimate nodes L_{ij} and the trusted node T_i.

The adversary transmit power is provided by:

$$\begin{aligned} P^{tx}_M = {} & P^{tx}_{T_i} + G_{T_i} - G_M + 20\log(d^u_{L_{ij}M}) + 20\log(\beta^u_{L_{ij}}) \\ & - 20\log(d^u_{L_{ij}T_i}) - 20\log(\beta^u_{T_i}) + \rho_u \alpha^u_{L_{ij}} d^u_{L_{ij}M} \\ & - \rho_u \alpha^u_{T_i} d^u_{L_{ij}T_i}. \end{aligned} \tag{21}$$

Next, we compute the received power at L_{ij} from T_i, which is given by

$$\begin{aligned} P^{rx}_{L_{ij}T_i} = {} & P^{tx}_{T_i} + G_{L_{ij}} + G_{T_i} - (C_u + 20\log(d^u_{L_{ij}T_i}) \\ & + 20\log(\beta^u_{T_i}) + \rho_u \alpha^u_{T_i} d^u_{L_{ij}T_i}). \end{aligned} \tag{22}$$

The transmit power and the distance have to satisfy (21), and (22). In the best case, the adversary with the full knowledge of all the legitimate nodes can only be successful when transmitting in a location less than the distance between T_i and

L_{ij}. Otherwise, the transmission will be overhead by T_i, and a failure message will be broadcast to other nodes. Note that the adversary does not know the exact location of T_i.

Accordingly, we compute the received power at L_{ij} from M, which is given by

$$P^{rx}_{L_{ij}M} = P^{tx}_{M} + G_M + G_{L_{ij}} - C_u - 20\log(d^u_{L_{ij}M}) - 20\log(\beta^u_{L_{ij}}) - \rho_u \alpha^u_{L_{ij}} d^u_{L_{ij}M}. \quad (23)$$

Since the underground power received $P^{rx}_{L_{ij}T_i} \geq P^{rx}_{L_{ij}M}$,

$$P^{tx}_{T_i} + G_{L_{ij}} + G_{T_i} - C_u - 20\log(d^u_{L_{ij}T_i}) - 20\log(\beta^u_{T_i}) - \rho_u \alpha^u_{T_i} d^u_{L_{ij}T_i} \geq P^{tx}_{M} + G_M + G_{L_{ij}} - C_u - 20\log(d^u_{ML_{ij}}) - 20\log(\beta^u_{L_{ij}}) - \rho_u \alpha^u_{L_{ij}} d^u_{ML_{ij}}. \quad (24)$$

From (24), with the assumption that the adversary has near perfect estimates of the transmits power and gains, which means that $P^{tx}_{T_i} + G_{T_i} - P^{tx}_{M} - G_M \approx \xi$, therefore it must be at a distance given by

$$20\log(d^u_{L_{ij}M}) + 20\log(\beta^u_{L_{ij}}) + \rho_u \alpha^u_{L_{ij}} d^u_{L_{ij}M} \geq 20\log(d^u_{L_{ij}T_i}) + 20\log(\beta^u_{T_i}) + \rho_u \alpha^u_{T_i} d^u_{L_{ij}T_i}, \quad (25)$$

where d^u_{xy} is the underground distance between x and y, β^u_x and α^u_x are the attenuation and phase-shifting constants, respectively. □

The inequality in Proposition 4 can be simplified using the Newton-Raphson approximation [85], as illustrated in Fig. 7. Achieving convergence requires careful selection of parameters like tolerance (tol), maximum iterations (N_{max}), and the initial guess (x_0). For example, using $tol = 10^{-6}$, $N_{max} = 1000$, and $x_0 = 1$ fails to converge, even with known parameters like $\alpha^u_{L_{ij}}, \alpha^u_{T_i}, \beta^u_{L_{ij}}, \beta^u_{T_i}$, and $d^u_{L_{ij}T_i}$. While higher values can expedite convergence, they risk reducing accuracy. Thus, achieving convergence often involves iterative optimization of these values. Therefore, an adversary must know the trusted node's location to perform this attack.

From Fig. 7(a)-(d), even with legitimate and trusted nodes separated by [0.5–2]m and varying attenuation and phase shift constants, the adversary must transmit enormous power from a farther distance. ***To evade detection, a Type 2 adversary must transmit approximately*** 10^6 ***W from*** ≈ 0.5 ***km away, which is impractical.*** These findings confirm that a Type 2 adversary can only emulate a rogue gateway with precise knowledge of underground node locations.

C. Security Against a Compromised Trusted Node

While compromise of T_i could occur via traffic analysis or physical access, such risks can be mitigated through ephemeral session keys, secure key storage, and operational safeguards, and are orthogonal to the initial bootstrapping focus of this work [86]. If K_{AT_i} is nonetheless exposed, an adversary may inject forged messages during the active bootstrapping phase by transmitting at significantly higher power to satisfy the RSS ratio constraints $(\tau_{\text{low}}, \tau_{\text{high}})$. However, this anomalous power increase can be detected at A as a sector-localized RSS deviation (e.g., $\geq$ 6dB), enabling alarm generation and manual rekeying of the affected sector. A physical displacement of trusted node (T_i) can be detected at the gateway due to change in RSS of the received signal on the authenticated and encrypted channel between them. Thus, it can be detected and rectified.

D. Security Against Advanced Attacks

STUN considers several attack classes during bootstrapping: (1) A *shallow-probes attack* during Step 1, where an adversary may replay the unencrypted synchronization message from A but cannot forge the authenticated initialization message $\text{AE}_{K_{AT_i}}(\text{INIT}|\eta)$ sent to trusted nodes T_i, thus preventing unauthorized participation; (2) A *reflector/high-power (wormhole or replay-based) attack*, where messages from T_i are injected across sectors or sessions, leading to mismatches detected in Step 6 and resulting in a denial-of-service that is orthogonal to the protocol's security goals; and (3) Reactive mobile injector attacks, in which an adversary injects signals in real time using SDRs or mobile hardware, which STUN is explicitly designed to detect and mitigate through verification at T_i (Step 4) or at the gateway A (Step 6), while also preventing masquerading as A via authenticated downlink detection at T_i.

VI. Performance Evaluations

We evaluate STUN using experimental data from our wireless underground outdoor experiments in [51], [87], [88], [13]. First, we describe the experimental configuration and evaluate STUN's correctness and robustness.

A. Setup

Underground Testbed: We use data from outdoor experiments in [51], [87], [88], [13] under varying conditions of distances. In these outdoor experiments, a 433MHz dipole antenna and an underground wideband planar antenna [63] are utilized. Wideband planar antennas have been experimentally shown to be more suitable for underground communication, enhancing the communication range and increasing the channel link budget [63]. Additionally, a dipole antenna was employed for underground transmission when the aboveground node distance was fixed. We kept an underground depth of $d^u_{L_{ij}}$, and $d^u_{T_i}$ fixed at 0.2m, with a maximum distance of $d^a_{AT_i} = 115$m. The distance between the underground nodes and the trusted device was kept constant at $d^u_{L_{ij}T_i} = 2.1$m.

The aboveground height was kept at 1.78m and the aboveground distances of the gateway $d^a_{AT_i}$ were varied at different intervals of [30, 60, 80, and 110m]. The outdoor testbed contains 13.09cm of silt clay loam soil with varying volumetric water content (VWC) ranging from 17% to 37% dry and wet. The VWC of the soil was kept at 37% for the most part. The transmit power ranges between [0.0032W - 0.2W] with a gain of 0.02W with a dipole antenna for the underground nodes. $d^a_{AT_i}$ was shown in [51] to cover a distance as far as 115m when a long-range device is used and move up to 200m [89]. The $PL_{\rho,a-u}$ was observed to be 4.2063×10^{-9}W, equivalent to -53dBm.

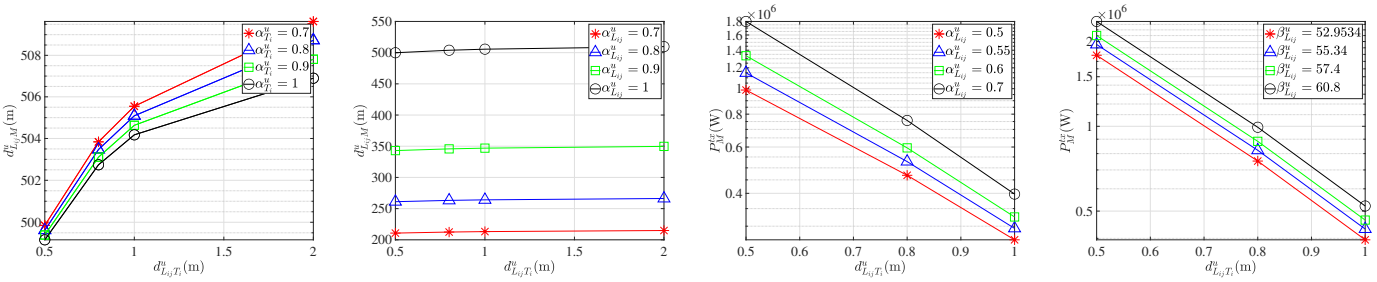


Fig. 7. Type 2 M distances against the legitimate distance while varying (a) the legitimate node attenuation, and (b) the trusted node attenuation to determine the distance of the adversary from the legitimate nodes. The power transmitted by the underground adversary to the legitimate nodes against the legitimate underground distance while varying (c) the attenuation $\alpha^u_{L_{ij}}$, and (d) the phase shift constant to determine the power of M from $\mathbf{L}_i$.

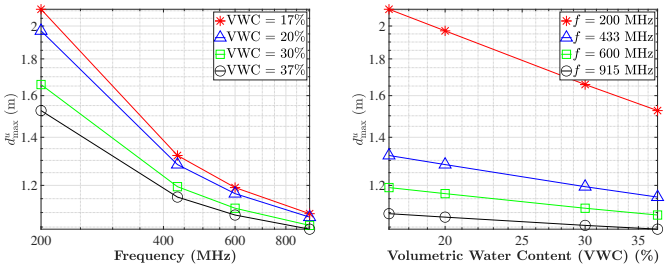


Fig. 8. The maximum size of T_i's sector against (a) the frequency while varying volumetric water content of soil, and (b) the volumetric water content while varying the frequency to determine the placement of the legitimate nodes.

B. Correctness Evaluations

We evaluate the maximum range of a trusted node, T_i, to assess the area of the sector for placement of legitimate nodes, $\mathbf{L}_i$. We use the information from the underground path loss to estimate the sector size of T_i in (4), giving us the maximum separation between the trusted node and the legitimate nodes underground within each sector.

***Exp1.Authorized sector size variation for volumetric water content*:** We show in Fig. 8(a) the maximum sector size of a trusted node against the frequency for various volumetric water content. We can deduce that the maximum separation in each sector is approximately 2.1m.

***Exp2.Authorized sector size variation for soil moisture level*:** Similarly, we show in Fig. 8(b) the maximum sector size against the soil moisture content for various center frequencies. We observe that the underground separation decreases as the water content in the soil increases.

***Experiment outcome*:** The maximum range of T_i depends on the operational frequency since lower frequency antennas can cover more distances. When placing nodes underground, the separation of the nodes should be within 2.1m, and the soil moisture content influences the maximum range between the legitimate node and the trusted node.

C. Robustness Evaluation

In this section, we evaluate the robustness of STUN against Type 1 and Type 2 adversaries.

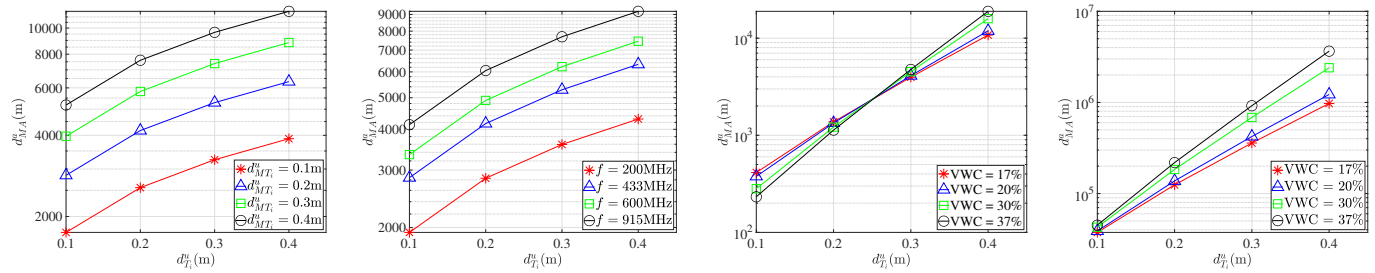
1) Type 1 Adversary: To evaluate the capabilities of an adversary, we emulate the adversarial data utilizing experimentally obtained wireless channel parameters, precisely measuring the effective soil permittivity and relative permeability of the soil from the experimental setup described in Section VI. The underground wireless channel is relatively stable and mostly deterministic compared to the OTA wireless channel [88].

***Exp3.Type 1 Adversary distance to defeat STUN*:** In Fig. 9(a), we illustrate how the gateway-to-adversary distance changes with the underground depth of the trusted node ($d^u_{T_i}$), considering various underground adversary distances ($d^u_{MT_i}$). Similarly, in Fig. 9(b), we vary the center frequencies and analyze the impact on the adversary distance. Our results show that M must position itself between 2000m and 10000m from the gateway to achieve an equivalent path loss in underground-to-OTA while located aboveground. In Fig. 12(c), (d), we demonstrate how aboveground gateway-to-adversary distance changes with underground depth ($d^u_{T_i}$), while varying the volumetric water content (VWC). We observe that in Fig. 9(c) and (d), while we keep the $d^u_{MT_i}$ at 0.2m and 0.4m. We observe that water content alters the adversary's position, shifting the distance from the underground node to soil the surface.

***Exp4.Type 1 Adversary transmit power to defeat STUN*:** In Fig. 10(a) and (b), we examine how successful an aboveground adversary can be in passing the verification at the gateway. We observed that the transmitter power is above the threshold at the gateway for various underground ($d^u_{T_i}$) and aboveground ($d^a_{AT_i}$) distances. Even when the adversary operates with the experimentally measured acceptable distance, our results reveal that the required power remains more than the threshold needed to pass Step 6. The adversary must transmit at a precise power level, maintaining an RSS ratio between 1 and 1.5. Adversary can compute the needed power for the gateway due to positional knowledge of the gateway aboveground but needs to do the same for the trusted node underground whose location is unknown.

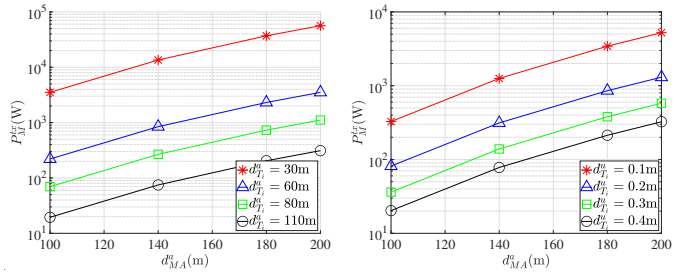
Similarly, in Fig. 11(a), and (b), we show that the power transmitted from aboveground Type 1 adversary attempting to pass Step 4 verification, even when the adversary distance ($d^a_{MT_i}$) from the trusted node is within the communication range. Our results show that the adversary transmit power to the trusted node is very high while changing the underground depth, and center frequency.

***Experiment outcome*:** Our findings indicate that the adversary needs to transmit a precise power to maintain an RSS



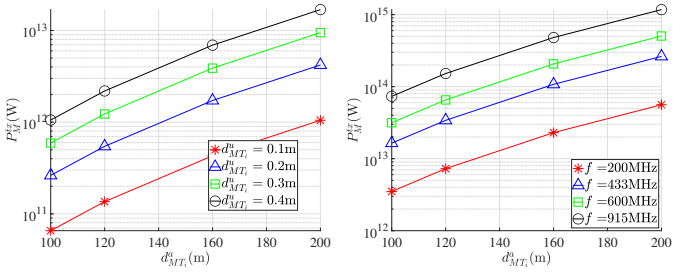
(a) (b) (c) (d)

Fig. 9. The distance between a Type 1 M from A against (a) the underground depth of T_i, and (b) the underground depth of T_i. (c) The distance between a Type 1 M from A against the underground depth of T_i at different volumetric water content for $d^u_{MT_i} = 0.2$m, (d) the distance between a Type 1 M from A against the aboveground distance of A at different volumetric water content for $d^u_{MT_i} = 0.4$m.



(a) (b)

Fig. 10. The required power transmitted by the Type 1 M to defeat Step 6 of STUN against the distance between M and A (a) for various aboveground distance of A from T_i, and (b) for various depth of T_i.



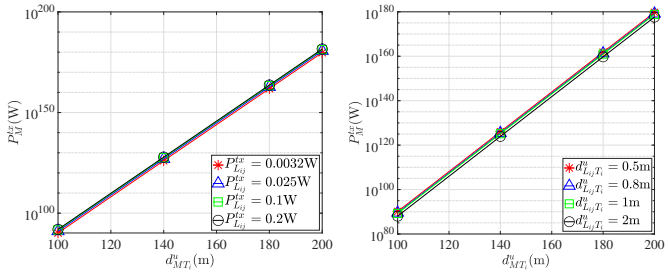
(a) (b)

Fig. 11. The required power transmitted by the Type 1 M to defeat Step 4 of STUN against the distance between M and A (a) for various aboveground distance of A from T_i, (b) for various depth of T_i, and (c) for different volumetric water content

threshold between 2.512×10^{-7}mW and 6.309×10^{-7}mW for verification at the trusted node. The likelihood of a successful attack is low, given that the adversary typically lacks exact positional knowledge of the trusted nodes and does not possess physical access to the farm. Our results attest to our theoretical findings that the adversary must operate at considerably far distances. M cannot reduce the transmit power rather than increase the distance, as this will cause the adversary to fail Step 4 due to high attenuation for OTA-to-underground transmissions.

2) Type 2 Adversary: In our evaluation, we assess the transmission power of an underground adversary to the trusted nodes as the distance between them increases.

***Exp5.Type 2 adversary transmit power to defeat STUN*:** The legitimate nodes maintain a consistent transmit power of [0.0032W, 0.025W, 0.1W, 0.2W], while the distance between the legitimate and trusted nodes remains at [0.5m, 0.8m, 1m, 2m]. The adversary succeeds if the received power of the



(a) (b)

Fig. 12. The required power transmitted by the Type 2 M against the distance between M and T_i (j) for various power transmitted by the legitimate node, and (k) for various distance between L_{ij} and T_i.

trusted node is between $\tau^{T_i}_{low} = 2.512 \times 10^{-7}$mW and $\tau^{T_i}_{high} = 6.309 \times 10^{-7}$mW as obtained in Section IV-B. We emulate the adversary's path loss according to (3) with the soil parameters obtained from the testbed. We ran the experiment 10,000 times. Fig. 12(a) and (b) depict the underground power transmitted by the Type 2 adversary (P^{tx}_M) against the underground distance between the adversary and the trusted node ($d^u_{MT_i}$), with variations in the power transmitted by the legitimate nodes ($P^{tx}_{L_{ij}}$) and the underground distance between the trusted node and the legitimate node ($d^u_{L_{ij}T_i}$).

***Experiment outcome*:** Our observations reveal that the adversary's power is sufficient to cause damage to the sensors. Furthermore, as the adversary's underground distance from the farm's perimeter increases, it becomes increasingly challenging to counter step 4 due to changes in soil conditions securely.

D. Bootstrapping Overhead and Scalability

Since STUN is a one-time bootstrapping protocol, its scalability is dominated by onboarding overhead rather than continuous monitoring costs. Under the time-division design, the message and verification complexity scales linearly with the number of legitimate nodes $|L_{ij}|$ in a sector, yielding a bootstrapping latency

$$t_{\text{boot}} = t_{\text{init}} + |L_{ij}|t_{\text{slot}} + t_{\text{relay}} + t_{\text{verify}},$$

where t_{init} denotes initialization overhead, t_{slot} is the time allocated per L_{ij} transmission in the time-division schedule, t_{relay} is T_i forwarding delay, and t_{verify} captures the verification overhead at T_i and G. This cost is incurred only during secure onboarding, after which established keys enable protected

routine operation without repeated trust establishment. While future decentralized or federated monitoring may be layered atop STUN to enhance scalability and privacy during normal operation, such mechanisms operate at a different layer and are beyond the scope of the present bootstrapping design [90]. Assuming an initialization message of 100kb, $|L_{ij}| = 10$, ECC-based key primitives of size 512kb [91], a trusted-node message length of approximately 6000kb, and negligible processing delay relative to transmission time, the resulting bootstrapping latency is estimated to be about 225s per sector over a 50kbps LoRaWAN communication link [8].

E. Reproducibility

We have released a public GitHub repository with the MATLAB scripts used for analytical evaluations in the paper, including path-loss modeling, incident-angle analysis, sector-size estimation, and adversarial-feasibility analysis, available at https://go.unl.edu/stun, to support reproducibility and further research.

VII. Conclusion

We address the problem of a secret-free secure bootstrapping for COTS underground nodes with an aboveground gateway. We propose STUN, which uses hard-to-forge underground wireless propagation laws to achieve node authentication and secret establishment in-band with the help of a trusted underground node. We demonstrate that STUN resists active signal injection attacks and scales well as the number of underground nodes increases. In addition, We theoretically prove that STUN has a security equivalent to the NP-hard problem of underdefined systems of multivariate equations (UOV scheme) in public cryptography. We also validate our theoretical results with outdoor underground wireless testbed experiments. We evaluate the placements of the trusted nodes to cover an agricultural farm in a hexagonal sector format. To optimize the required number of trusted nodes, we investigated the distance of the trusted nodes from the farm boundary and the distance between each other. Finally, we developed security for the downlink communication and multiple trusted and legitimate nodes.

Acknowledgments

We thank the anonymous reviewers for their insightful comments. This research was supported in part by the NSF under grants ECCS-2030272, CNS-1619285, CNS-2331191. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the NSF.

References

[1] D. Wohwe Sambo and A. Förster, "Wireless underground sensor networks: A comprehensive survey and tutorial," *ACM Computing Surveys*, vol. 56, no. 4, pp. 1–44, 2023.

[2] A. Pal, H. Guo, S. Yang, M. A. Akkas, and X. Zhang, "Taking wireless underground: A comprehensive summary," *ACM Transactions on Sensor Networks*, vol. 20, no. 1, pp. 1–44, 2023.

[3] B. A. News. (2024) Cyberattacks a growing concern for ag industry. [Online]. Available: https://www.brownfieldagnews.com/news/cyberattacks-a-growing-concern-for-ag-industry/

[4] Wisdiam. (2024) Recent cyber attacks on the food and agriculture sector. [Online]. Available: https://wisdiam.com/publications/recent-cyber-attacks-food-agriculture-sector/

[5] GroGuru. (2025) Groguru wireless underground system (wugs). [Online]. Available: https://www.groguru.com/products/

[6] S. Scout. (2025) Wireless soil moisture sensor for precision agriculture. [Online]. Available: https://soilscout.com/solution/wireless-soil-moisture-sensor

[7] E. Oguchi, N. Ghose, and M. C. Vuran, "STUN: Secret-Free Trust-Establishment For Underground Wireless Networks," in *Proc. of IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2022, pp. 1–6.

[8] SEMTECH, "What are LoRa® and LoRaWAN®?" *URL https://lora-developers.semtech.com/library/tech-papers-and-guides/lora-and-lorawan/*, 2020.

[9] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of LoRa," in *Proc. of IEEE International Conference on Cybernetics (CYBCONF)*. IEEE, 2017, pp. 1–6.

[10] X. Xue, S. Yu, and M. Song, "Secure Device Trust Bootstrapping Against Collaborative Signal Modification Attacks," in *Proc. of IEEE INFOCOM 2023-IEEE Conference on Computer Communications*. IEEE, 2023, pp. 1–10.

[11] Z. Xu, J. Li, Y. Pan, M. Li, and L. Lazos, "Harvesting physical-layer randomness in millimeter wave bands," *IEEE Transactions on Mobile Computing*, 2024.

[12] X. Dong and M. C. Vuran, "Spatio-temporal soil moisture measurement with wireless underground sensor networks," in *Proc. of IFIP Med-Hoc-Net*. IEEE, 2010, pp. 1–8.

[13] X. Dong, M. C. Vuran, and S. Irmak, "Autonomous precision agriculture through integration of wireless underground sensor networks with center pivot irrigation systems," *Ad Hoc Networks*, vol. 11, no. 7, pp. 1975–1987, 2013.

[14] X. Dong and M. C. Vuran, "Environment aware connectivity for wireless underground sensor networks," in *Proc. of IEEE INFOCOM*. IEEE, 2013, pp. 674–682.

[15] A. Salam and M. C. Vuran, "EM-based wireless underground sensor networks," in *Proc. of Underground sensing*. Elsevier, 2018, pp. 247–285.

[16] X. Dong and M. C. Vuran, "A channel model for wireless underground sensor networks using lateral waves," in *Proc. of IEEE Global Telecommunications Conference-GLOBECOM*. IEEE, 2011, pp. 1–6.

[17] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in *Proc. of EUROCRYPT*. Springer, 1999, pp. 206–222.

[18] Q. Yan, H. Yang, M. C. Vuran, and S. Irmak, "SPRIDE: Scalable and private continual geo-distance evaluation for precision agriculture," in *Proc. of IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2017, pp. 1–9.

[19] Q. Yan, J. Lou, M. C. Vuran, and S. Irmak, "Scalable Privacy-preserving Geo-distance Evaluation for Precision Agriculture IoT Systems," *ACM Transactions on Sensor Networks (TOSN)*, vol. 17, no. 4, pp. 1–30, 2021.

[20] A. Naseer, M. Shmoon, T. Shakeel, S. U. Rehman, A. Ahmad, and V. Gruhn, "A systematic literature review of the iot in agriculture—global adoption, innovations, security, and privacy challenges," *IEEE Access*, vol. 12, pp. 60 986–61 021, 2024.

[21] L. Carvalho, T. Adão, R. Morais, A. R. Costa, and E. Peres, "Conventional and zero trust security measures for precision agriculture devices: the mysense's vineinspector case-study," *Procedia Computer Science*, vol. 256, pp. 246–254, 2025.

[22] S. A. Ansari, S. Ali, M. Luqman, and S. Ahmad, "Deep learning enabled secure iot module for smart agriculture in diverse environmental conditions," in *Proc. of IEEE International Conference on Communication Systems and Network Technologies (CSNT)*. IEEE, 2025, pp. 94–99.

[23] S. Halder, M. R. Islam, Q. Mamun, A. Mahboubi, P. Walsh, and M. Z. Islam, "A comprehensive survey on AI-enabled secure social industrial internet of things in the Agri-food supply chain," *Smart Agricultural Technology*, p. 100902, 2025.

[24] J. B. Awotunde, A. E. Adeniyi, P. B. Falola, and T. C. Adeniran, "A blockchain-enabled framework to enhance cybersecurity challenges in smart agriculture," *Blockchain and Digital Twin Applications in Smart Agriculture*, pp. 69–91, 2025.

[25] R. K. Munaganuri, N. R. Yamarthi, and S. C. Bolem, "Design of an improved graph-based model integrating lstm, lorawan, and blockchain for smart agriculture," *PeerJ Computer Science*, vol. 11, p. e2896, 2025.

[26] C. N. Kasimatis, D. Apostolou, A. Efthimiadou, and G. Mentzas, "Agricultural product traceability using blockchain-based digital product passports," in *Proc. of International Conference on Information, Intelligence, Systems & Applications (IISA)*. IEEE, 2024, pp. 1–8.

[27] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 63–75, 2010.

[28] Y.-H. Lin, A. Studer, Y.-H. Chen, H.-C. Hsiao, L.-H. Kuo, J. M. McCune, K.-H. Wang, M. Krohn, A. Perrig, B.-Y. Yang *et al.*, "Spate: small-group pki-less authenticated trust establishment," *IEEE Transactions on Mobile Computing*, vol. 9, no. 12, pp. 1666–1681, 2010.

[29] K.-C. Liao and W.-H. Lee, "A novel user authentication scheme based on qr-code," *Journal of networks*, vol. 5, no. 8, p. 937, 2010.

[30] J. Y. Hwang, S. Eom, K.-Y. Chang, P. J. Lee, and D. Nyang, "Anonymity-based authenticated key agreement with full binding property," *IEEE Journal of Communications and Networks*, vol. 18, no. 2, pp. 190–200, 2016.

[31] X. Liang, R. Peterson, and D. Kotz, "Securely connecting wearables to ambient displays with user intent," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 4, pp. 676–690, 2018.

[32] B. Berg, T. Kaczmarek, A. Kobsa, and G. Tsudik, "Lights, Camera, Action! Exploring Effects of Visual Distractions on Completion of Security Tasks," in *Proc. of International Conference on Applied Cryptography and Network Security*. Springer, 2017, pp. 124–144.

[33] J. Han, A. J. Chung, M. K. Sinha, M. Harishankar, S. Pan, H. Y. Noh, P. Zhang, and P. Tague, "Do you feel what i hear? Enabling autonomous IoT device pairing using different sensor types," in *Proc. of IEEE Symposium on Security and Privacy*. IEEE, 2018, pp. 836–852.

[34] Y. Gao, Y. Jin, J. Chauhan, S. Choi, J. Li, and Z. Jin, "Voice in ear: Spoofing-resistant and passphrase-independent body sound authentication," *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, no. 1, pp. 1–25, 2021.

[35] Y. Chen, M. Xue, J. Zhang, Q. Guan, Z. Wang, Q. Zhang, and W. Wang, "Chestlive: Fortifying voice-based authentication with chest motion biometric on smart devices," *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, no. 4, pp. 1–25, 2021.

[36] H. Farrukh, M. O. Ozmen, F. K. Ors, and Z. B. Celik, "One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2022, pp. 1693–1709.

[37] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, "Proximity based IoT device authentication," in *Proc. of IEEE INFOCOM 2017*. IEEE, 2017, pp. 1–9.

[38] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proc. of the 9th international conference on Mobile systems, applications, and services*, 2011, pp. 211–224.

[39] X. Xiao, F. Guo, and A. Hecker, "A lightweight cross-domain proximity-based authentication method for iot based on iota," in *Proc. of IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2020, pp. 1–6.

[40] Y. Pan, Y. Hou, M. Li, R. M. Gerdes, K. Zeng, M. A. Towfiq, and B. A. Cetiner, "Message Integrity Protection over Wireless Channel: Countering Signal Cancellation via Channel Randomization," *IEEE Transactions on Dependable and Secure Computing*, 2017.

[41] N. Ghose, L. Lazos, and M. Li, "In-band Secret-Free Pairing for COTS Wireless Devices," *IEEE Transactions on Mobile Computing*, 2020.

[42] I. F. Akyildiz and E. P. Stuntebeck, "Wireless underground sensor networks: Research challenges," *Ad Hoc Networks*, vol. 4, no. 6, pp. 669–686, 2006.

[43] M. C. Vuran, A. Salam, R. Wong, and S. Irmak, "Internet of underground things in precision agriculture: Architecture and technology aspects," *Ad Hoc Networks*, vol. 81, pp. 160–173, 2018.

[44] N. Saeed, M.-S. Alouini, and T. Y. Al-Naffouri, "Toward the internet of underground things: A systematic survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3443–3466, 2019.

[45] Z. Sun and I. F. Akyildiz, "Magnetic induction communications for wireless underground sensor networks," *IEEE transactions on antennas and propagation*, vol. 58, no. 7, pp. 2426–2435, 2010.

[46] J. Wang, W. Cheng, W. Zhang, and H. Zhang, "Backscatter based bidirectional full-duplex magnetic induction communications," *IEEE Transactions on Communications*, vol. 71, no. 11, pp. 6258–6271, 2023.

[47] A. Salam and M. C. Vuran, "Impacts of soil type and moisture on the capacity of multi-carrier modulation in internet of underground things," in *Proc. of 25th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2016, pp. 1–9.

[48] Z. Sun, I. F. Akyildiz, and G. P. Hancke, "Dynamic connectivity in wireless underground sensor networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 12, pp. 4334–4344, 2011.

[49] G. Liu, H. Zhang, S. Deng, and T. Jiang, "Conductor-aware wireless underground sensor networks based on magnetic induction: Research challenges," *IEEE Network*, vol. 38, no. 6, pp. 259–266, 2024.

[50] K. Lin, M. A. Ullah, H. Alves, K. Mikhaylov, and T. Hao, "Subterranean mMTC in Remote Areas: Underground-to-Satellite Connectivity Approach," *IEEE Communications Magazine*, 2022.

[51] B. Zhou, V. S. S. L. Karanam, and M. C. Vuran, "Impacts of soil and antenna characteristics on LoRa in Internet of Underground Things," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2021, pp. 1–6.

[52] Y. Luo and L. Pu, "UAV Remotely-Powered Underground IoT for Soil Monitoring," *IEEE Transactions on Industrial Informatics*, 2023.

[53] S. M. Hashir, M. C. Vuran, and J. Camp, "ECHO: Empirical characterization and height optimization of UAV-to-underground channels," in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2023, pp. 1–7.

[54] K. Lin, O. L. A. López, H. Alves, and T. Hao, "On CSI-Free Multi-Antenna Schemes for Massive Wireless-Powered Underground Sensor Networks," *IEEE Internet of Things Journal*, 2023.

[55] B. Kashyap and R. Kumar, "Sensing methodologies in agriculture for soil moisture and nutrient monitoring," *IEEE Access*, vol. 9, pp. 14 095–14 121, 2021.

[56] G. Zhao, K. Lin, D. Chapman, N. Metje, and T. Hao, "Optimizing energy efficiency of lorawan-based wireless underground sensor networks: A multi-agent reinforcement learning approach," *Internet of Things*, vol. 22, p. 100776, 2023.

[57] Z. Sun and I. F. Akyildiz, "Channel modeling and analysis for wireless networks in underground mines and road tunnels," *IEEE Transactions on communications*, vol. 58, no. 6, pp. 1758–1768, 2010.

[58] I. F. Akyildiz, Z. Sun, and M. C. Vuran, "Signal propagation techniques for wireless underground communication networks," *Physical Communication*, vol. 2, no. 3, pp. 167–183, 2009.

[59] A. Salam, M. C. Vuran, and S. Irmak, "Towards internet of underground things in smart lighting: A statistical model of wireless underground channel," in *Proc. of IEEE 14th International Conference on Networking, Sensing and Control (ICNSC)*. IEEE, 2017, pp. 574–579.

[60] A. Salam, M. C. Vuran, X. Dong, C. Argyropoulos, and S. Irmak, "A theoretical model of underground dipole antennas for communications in internet of underground things," *IEEE Transactions on Antennas and Propagation*, vol. 67, no. 6, pp. 3996–4009, 2019.

[61] A. Salam, M. C. Vuran, and S. Irmak, "A statistical impulse response model based on empirical characterization of wireless underground channels," *IEEE Transactions on Wireless Communications*, vol. 19, no. 9, pp. 5966–5981, 2020.

[62] H. M. Jawad, A. M. Jawad, R. Nordin, S. K. Gharghan, N. F. Abdullah, M. Ismail, and M. J. Abu-AlShaeer, "Accurate empirical path-loss model based on particle swarm optimization for wireless sensor networks in smart agriculture," *IEEE Sensors Journal*, vol. 20, no. 1, pp. 552–561, 2019.

[63] M. C. Vuran, X. Dong, and D. Anthony, "Antenna for wireless underground communication," U.S. Grant US 9 532 118, Dec. 27, 2016.

[64] "GroGru products," https://www.groguru.com/products/.

[65] B. Ali and G. Chen, "Neuromorphic quantum adversarial learning (NQAL): a bio-inspired paradigm for DNS over HTTPS threat detection," *EURASIP Journal on Information Security*, vol. 2025, no. 1, p. 35, 2025.

[66] ——, "Next-generation AI for advanced threat detection and security enhancement in DNS over HTTPS," *Journal of Network and Computer Applications*, vol. 244, p. 104326, 2025.

[67] ——, "Proactive and privacy-preserving defense for DNS over HTTPS via federated AI attestation (PAFA-DoH)," *Neural Networks*, vol. 196, p. 108343, 2026.

[68] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[69] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human-verifiable authentication," in *Proc. of IEEE Symposium on Security and Privacy (S&P'05)*. IEEE, 2005, pp. 110–124.

[70] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks." in *Proc. of NDSS*. Citeseer, 2002.

[71] G. Li, H. Luo, J. Yu, A. Hu, and J. Wang, "Information-Theoretic Secure Key Sharing for Wide-Area Mobile Applications," *IEEE Wireless Communications*, 2023.

[72] C. Jacomme, E. Klein, S. Kremer, and M. Racouchot, "A comprehensive, formal and automated analysis of the EDHOC protocol," in *Proc. of USENIX Security'23-32nd USENIX Security Symposium*, 2023.

[73] Q. Yang, K. Cui, and Y. Zheng, "VoShield: Voice Liveness Detection with Sound Field Dynamics," in *Proc. of IEEE INFOCOM*, 2023.

[74] S. Zhang, P. K. Sangdeh, H. Pirayesh, H. Zeng, Q. Yan, and K. Zeng, "AuthIoT: A Transferable Wireless Authentication Scheme for IoT Devices Without Input Interface," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 23 072–23 085, 2022.

[75] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, "Proximity Based IoT Device Authentication," in *Proc. of INFOCOM*, 2017.

[76] H. Ye, Q. Zeng, J. Liu, X. Du, and W. Wang, "Easy peasy: A New Handy Method for Pairing Multiple COTS IoT Devices," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[77] M. Jin, X. Wang, and C. Zhou, "Key Agreement on IoT Devices With Echo Profiling," *IEEE/ACM Transactions on Networking*, 2023.

[78] B. B. Gupta, A. Gaurav, K. T. Chui, and C.-H. Hsu, "Identity-based authentication technique for iot devices," in *Proc. of IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2022, pp. 1–4.

[79] S. Roy, D. Das, A. Mondal, M. H. Mahalat, B. Sen, and B. Sikdar, "PLAKE: PUF based secure Lightweight Authentication and Key Exchange Protocol for IoT," *IEEE Internet of Things Journal*, 2022.

[80] L. Cai, K. Zeng, H. Chen, and P. Mohapatra, "Good Neighbor: Ad hoc Pairing of Nearby Wireless Devices by Multiple Antennas." in *Proc. of NDSS*, 2011.

[81] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for IoT with location information," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3335–3351, 2018.

[82] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2000, pp. 531–545.

[83] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password-authenticated key exchange using Diffie-Hellman," in *Proc. of Eurocrypt*, 2000, pp. 156–171.

[84] C. Leys, C. Ley, O. Klein, P. Bernard, and L. Licata, "Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median," *Journal of experimental social psychology*, vol. 49, no. 4, pp. 764–766, 2013.

[85] T. J. Ypma, "Historical development of the Newton–Raphson method," *SIAM review*, vol. 37, no. 4, pp. 531–551, 1995.

[86] M. A. Kiran, M. Thaile, A. Anitha, R. B. Pittala, A. Sanjana, L. P. Byrapuneni, B. K. Kumar, D. Neha, and P. Nagamani, "Compromise node detection using linear regression model in wireless sensor networks," in *Proc. of International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)*. IEEE, 2025, pp. 1–5.

[87] A. R. Silva and M. C. Vuran, "Empirical evaluation of wireless underground-to-underground communication in wireless underground sensor networks," in *Proc. of International Conference on Distributed Computing in Sensor Systems*. Springer, 2009, pp. 231–244.

[88] ——, "Development of a testbed for wireless underground sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, pp. 1–14, 2010.

[89] X.-f. Wan, Y. Yang, J. Cui, and M. S. Sardar, "Lora propagation testing in soil for wireless underground sensor networks," in *Proc. of Sixth Asia-Pacific Conference on Antennas and Propagation (APCAP)*. IEEE, 2017, pp. 1–3.

[90] B. Ali, "On the fog's frontline: a federated machine learning approach for industrial network threat detection and intrusion prevention," *Journal of Cybersecurity*, vol. 11, no. 1, p. tyaf041, 2025.

[91] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, codes and cryptography*, vol. 19, no. 2, pp. 173–193, 2000.

Ebuka Philip Oguchi (Member, IEEE) received the B.Eng. degree in electronic and computer engineering from Nnamdi Azikiwe University, Awka, Nigeria, in 2016, the M.S. degree in computer applied technology from Changchun University of Science and Technology, Changchun, China, in 2020, and the Ph.D. degree in computer science from the University of Nebraska–Lincoln, Lincoln, NE, USA, in 2025. He is currently an Assistant Professor with the Department of Computer and Information Sciences, Spelman College, Atlanta, GA, USA. His research interests include cybersecurity, wireless network security, authentication and message integrity verification, machine learning for security, underground wireless communications, vehicular networks, and molecular and nano-communication systems. Dr. Oguchi has served as a reviewer for several international conferences and IEEE journals in wireless communications and cybersecurity.

Nirnimesh Ghose (Senior Member, IEEE) received his Ph.D. in the Electrical and Computer Engineering from the University of Arizona, Tucson in 2019. He is an Associate Professor of computing at the University of Nebraska-Lincoln. He received his MS degree in Electrical and Computer Engineering from the Illinois Institute of Technology, Chicago in 2012, and his B.Tech. degree in Electronics and Communication Engineering from the Uttar Pradesh Technical University (now Dr. A.P.J. Abdul Kalam Technical University), Lucknow, India in 2010. His research focuses on network security and privacy with applications to emerging wireless networks, cyber-physical systems, the Internet of Things, aviation and transportation networks, and the interaction between cybersecurity and social networks. He has authored papers in flagship security conferences and journals like IEEE Security and Privacy, IEEE INFOCOM, USENIX Security, and IEEE Transactions on Mobile Communications. He has served as a web chair for IEEE CNS 2018 and as a reviewer for numerous conferences and journals.

Mehmet Can Vuran (Member, IEEE) received the B.S. degree in electrical and electronics engineering from Bilkent University, Türkiye, in 2002, and the M.S. and Ph.D. degrees in electrical and computer engineering from Georgia Institute of Technology, in 2004 and 2007, respectively. Currently, he is the Dale M. Jensen Professor of computing with the University of Nebraska-Lincoln. He received an NSF CAREER (2010) for "Bringing Wireless Sensor Networks Underground" and was recognized as a Highly Cited Researcher in Computer Science three years in a row by Thomson Reuters, ranking in the top 1% researchers for most cited documents in the field. He is a National Strategic Research Institute Fellow and a Daugherty Water for Food Global Institute Fellow. He is the co-author of Wireless Sensor Networks. His research interests include the Internet of Things, wireless underground sensing and communications, mmWave and THz sensing and communications in challenging environments, dynamic spectrum access, connected autonomous systems, and cyber-physical networking. He has served as the TPC Co-Chair for IEEE INFOCOM 2020 and on the Editorial Boards of IEEE Transaction on Wireless Communication, IEEE Transaction on Mobile Computing, and IEEE Communications Surveys and Tutorials Journal.