STUN: Secret-Free Trust-Establishment For Underground Wireless Networks

Ebuka Oguchi
School of Computing
University of Nebraska–Lincoln
eoguchi2@huskers.unl.edu

Nirnimesh Ghose
School of Computing
University of Nebraska–Lincoln
nghose@unl.edu

Mehmet C. Vuran
School of Computing
University of Nebraska–Lincoln
mcv@unl.edu

***Abstract*—Emerging agricultural internet-of-things (Ag-IoT) is increasing the efficiency of farming. The data collected by the wireless-enabled Ag-IoT infrastructure is highly sensitive as corrupting the data can cause significant damages to farm production and the livelihood of growers. The trust of the data can be established by initial secure bootstrapping of the wireless underground end nodes. This paper tackles the problem of scalable and secret-free trust-establishment for commercial off-the-shelf (COTS) underground nodes with an aboveground gateway applicable to heterogeneous end nodes. Secure bootstrapping requires authentication and secret establishment, which are achieved in-band, aided by a trusted underground node by exploiting the unique and hard-to-forge underground wireless signal propagation laws. The secret-free trust-establishment for underground wireless networks (STUN) protocol is resistant to active signal injection attacks and is scalable with an increasing number of underground nodes. Further, it is theoretically proven that STUN has security equivalent to the unbalanced oil and vinegar scheme in public cryptography. STUN is validated based on experimental data from an underground wireless testbed.**

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

I. Introduction

The emerging agricultural Internet-of-things (Ag-IoTs) provide a wireless-enabled smart-farming ecosystem to increase the quality and quantity of the agricultural yield with efficient use of human labor and natural resources. Ag-IoT sensors in the field can provide real-time information about plants and the soil, including soil moisture, precipitation, temperature, leaf quality, and crop health [1], [2]. Accordingly, crop production can be semi-automated, where the sensor-controlled irrigation systems can maintain an optimum soil moisture content. However, all the data collected by the sensors are highly sensitive as it relates to farmers' livelihoods. In a sensor-controlled irrigation system, injection of corrupt data can cause yield loss or excessive water consumption, causing millions of dollars in losses. Thus, trust verification is needed for the data flowing through the smart farming infrastructure. The problem of trust-verification of the data is exacerbated by the high number of Ag-IoT sensors from varied vendors with low computation and limited power available, which collect the sensitive data flowing in the smart farming infrastructure.

Many commercially available devices adopt a gateway model in the Ag-IoT infrastructure where the gateway connects to the end nodes for data collection and remote actuation. The gateway and end-nodes should bootstrap trust before communicating securely to secure the collected data. Initial trust bootstrapping has two steps mutual authentication and establishing a shared secret. In the first step, verification of the devices' identities (or legitimacy) occurs, whereas a secure channel is established in the second step. There are existing lightweight solutions for bootstrapping for Ag-IoT, such as Activation by Personalization (ABP) and Over-the-Air Activation (OTAA) (preferred due to zero-interaction) [3]. The existing bootstrapping methods are prone to compromise of secrets, jamming attacks, replay attacks, and wormhole attacks due to the minimal capabilities of the end nodes, lack of authentication, or difficulty implementing mutual authentication for a huge number of devices. Nonetheless, existing solutions are prone to several challenges such as scalability, the absence of interfaces, interoperability, and usability. Manufacturers circumvent the problem by pre-loading default keys that can be leaked easily, which was the cause of the Mirai Botnet DDoS attack on DNS infrastructure.

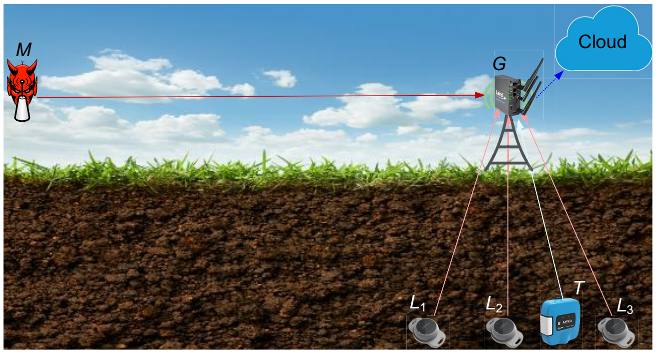


Fig. 1. Several underground nodes $\mathbf{L}$ securely bootstrap with the gateway G assisted by the trusted node T in the presence of an adversary M.

This has motivated researchers to propose secret-free bootstrapping, classified as out-of-band (OOB) verification using visual or audio channels [4], and in-band verification utilizing the wireless interface [5], [6]. The OOB channels are absent for the underground wireless networks. A class of in-band verification relies on techniques such as Manchester coded ON/OFF keying for curtailing overshadowing or signal injection attacks that require updating the transmitter's firmware [5]. This limits the implementation of heterogeneous underground nodes from different vendors. Another class of in-band verification is based on hard-to-forge wireless properties [6]. These cannot be implemented for underground nodes due to distinction in Over-The-Air (OTA) and underground wireless channels [7], [8].

To tackle the problem of secure bootstrapping for underground wireless communication, in this paper we propose STUN: **S**ecret-free **T**rust-establishment for **U**nderground wireless **N**etworks. To the best of our knowledge, this is the first work to develop secret-free secure bootstrapping for underground nodes, exploiting the hard-to-forge underground wireless physical layer properties. A legitimate node L_i executes an initial trust establishment session with the gateway G, as shown in Fig. 1. The adversary M executes an active attack over the public wireless channel to establish a common secret with the gateway. In STUN, active attacks can be detected by correlating received signal strength (RSS) variations recorded at G from L_i and a co-located underground trusted node T. STUN is developed to increase the attack complexity such that an adversary cannot inject malicious data while driving next to the farm but is forced to trespass. Such an adversary is generally physically detected and removed.

- We develop STUN protocol, which detects and prevents rogue devices from joining the gateway using a novel PHY-layer primitive based on the hard-to-forge underground wireless channel model and integrate with Diffie-Hellman (DH) key agreement to develop an in-band pairing protocol that allows a legitimate end-node to establish a pairwise key with the gateway.
- We analyze the security of STUN and theoretically show the security is comparable to an unbalanced oil and vinegar public cryptography scheme [9] against an active adversary with advanced abilities (transmission power control and colluding adversarial nodes).
- We undertake extensive empirical evaluations for ascertaining the definite traits for authentication and message integrity verification. We also analyzed the security of STUN utilizing the data captured from an underground wireless testbed.

II. Model and Preliminaries

A. System Model

Gateway (G)**:** The aboveground gateway coordinates the deployed nodes and captures and authenticates the data transmitted by the nodes.

Legitimate Nodes $(\mathbf{L})$**:** $\{L_1, L_2, \ldots, L_n\}$ are deployed underground throughout the farm under the user's control.

Trusted Node (T)**:** The trusted node with higher battery and computation powers to handle cryptographic functions has an existing trust with G, and is deployed underground at the same depth of $\mathbf{L}$ in the farm under the user's control. There are multiple Ts available covering the whole area of the farm. For this work, we develop the protocol for a single T, which can be scaled to multiple Ts. T's transmissions to G are secured using an authenticated encryption function AE$(\cdot)$ utilizing the shared secret K_{GT} [10]. This will guarantee the source's authenticity, message integrity, and confidentiality.

B. Threat Model

Here an active adversary (M) controls one or more colluding adversarial devices. The adversary is outside the perimeter of the trusted farm. This is relevant as the adversary can drive on the roads next to the farm but cannot trespass the fields. M's objective is to spoof messages in an attempt to bootstrap at G posing as a rogue node. In an attempt to undertake its objective, M launches a signal injection attack to inject rogue messages to G at any time, as this does not require any user authentication. The signal injection can also be performed as an overshadowing attack when $\mathbf{L}$ is transmitting [11]. As only 6dB higher power signal is required to perform the overshadowing attack for LPWAN technologies [3]. We assume that M knows the protocol implemented by the legitimate entities. However, the adversary cannot physically access any of the wireless nodes. Also, we do not consider a denial-of-service (DoS) attacker who can perform jamming. M cannot physically block any signal (e.g., using a Faraday cage) around legitimate wireless nodes. We consider two types of attackers with progressive capabilities.

Type 1 adversary attempts to inject its signal simultaneously at G, and T.

Type 2 adversary can additionally deploy colluding aboveground and underground wireless nodes to achieve the required received signal strength at G, and T.

C. Underground-to-Air Wireless Channel Model

We introduce the basic underground-to-air channel model, as the security protocol developed in this paper relies on the unpredictability of the model [8]. The wireless channel is evaluated for effects of underground and Over-The-Air (OTA) wireless communications. It has been shown by Dong *et al.* [12] that the electromagnetic wave propagation in soil experiences higher attenuation as compared to OTA communications. Higher soil permittivity compared to air permittivity, along with soil moisture, increases signal attenuation. This also causes refraction and reflection at the border of soil and air.

Consider an aboveground node G receiving a wireless signal from an underground node L_i, as shown in Fig. 1. The wireless signal from node G to node L_i has a path-length of $d_{Gi} = d'_{Gi} + d''_{Gi}$. Where d'_{Gi} is the distance between where the signal crosses the soil-air border to G and d''_{Gi} is vertically upwards towards the soil-air medium and the readers should note here that the underground path d''_{Gi} is approximately the same as the depth of the underground node because the signal takes the shortest path to escape the underground [8]. The power received by L_i is given by [8]

$$Pr_i = \frac{Pt_G \times G_G \times G_i}{PL_{ug} \times PL_{ag} \times PL_R}, \quad (1)$$

where Pt_G is the transmit power of G, G_x is the antenna gain of the transceiver x, and PL_{ug}, PL_{ag}, PL_R are pathloss for underground, OTA and refraction at the ground level,

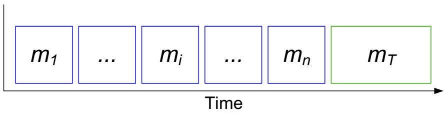


Fig. 2. Messages from $\mathbf{L}$ and T in a time-division fashion to G.

respectively. Now we will discuss the respective pathloss, starting with the OTA wireless channel [8]

$$PL_{ag} = \frac{(d'_{Gi})^{\eta} \times f^2}{10^{14.76}}, \tag{2}$$

where d'_{Gi} is the distance between the point where the wireless channel crosses from underground-to-air to the node G, η is the attenuation factor, and f is the center frequency. Second, the pathloss due to the underground channel [8]

$$PL_{ug} = 10^{(0.64+0.869\alpha d''_{Gi})} \times (d''_{Gi} \times \beta)^2, \tag{3}$$

where d''_{Gi} is the depth of underground node L_i, α and β are the attenuation and phase shifting constants. Finally, the pathloss due to refraction can be evaluated as either for air-to-underground as $PL_{R_{AG-UG}} = ({}^{r+1}/{}_{4})^2$, where $r = \sqrt{{}^{\sqrt{\epsilon'^2+\epsilon''^2}+\epsilon'}/{}_{2}}$ is the refractive index of the soil [8]. Or for the underground-air link, the signal propagates perpendicularly without refraction, and hence, $PL_{R_{UG-AG}} = 1$ [8].

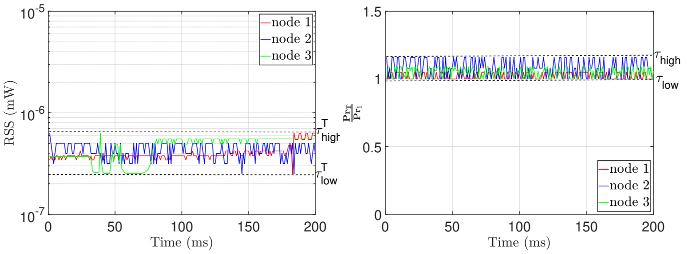
III. Secret-Free Trust-Establishment For Underground Wireless Networks

We present STUN, an in-band and secret-free trust establishment protocol for an underground wireless network. STUN uses a novel PHY-layer trust-verification primitive that verifies the authenticity of the legitimate underground nodes $\mathbf{L}$, and the message integrity of the transmissions from $\mathbf{L}$.

A. Trust Establishment Protocol

The basic idea behind the trust verifier is to utilize the similarities between the $\mathbf{L}$-to-G and T-to-G channels, specifically the underground-to-air pathloss. Here, we will be exploiting two factors of the underground-to-air wireless channels coherence time of hours and spatial correlation of 10s of meters [7]. Note here that $\mathbf{L}$ and G do not have a prior security association. Consider $L_i \in \mathbf{L}$ transmit its key primitive m_i to G, for all $i = 1, \ldots, n$. G and T record the RSS while receiving m_i. T synchronizes with the transmission using any known technique such as synchronization with preamble [13]. Then T relays all the received messages to G in an authenticated encryption as m_T in a time-division fashion after the transmission from L_n, as shown in Fig. 2. G records the RSS for m'_i, and also for m'_T. Next, the gateway computes the ratio between the RSS received from L_i and T. G uses the similarity of the underground pathloss of the channels from L_i and T to authenticate L_i and verify the integrity of m_i. The trust-establishment is performed by following steps:

1) **Initialization:** The protocol is initiated when G transmits a synchronization message which is received by $\mathbf{L}$ and T. All the entities are assumed to have agreed on DH public parameters $\mathbb{G}, q, g$.



(a) (b)

Fig. 3. (a) Power received at the trusted node from three $\mathbf{L}$, and (b) RSS ratio at G of power received from T to power received from $\mathbf{L}$, with thresholds.

2) **Primitive transmission from L:** All the legitimate nodes $L_i \in \mathbf{L}$ picks a secret value $X_i \in_U \mathbb{Z}_q$, computes the public value $z_i \leftarrow g^{X_i}$, and transmits their messages $m_i \leftarrow \{ID_i, z_i\}$.
3) **Verification at T:** The trusted node T synchronizes with the preamble and receives all the messages $m'_i \ \forall\ i = 1, \ldots, n$; and records corresponding the RSS $\mathbf{Pr}_{Ti} = \{Pr_{Ti}(1), Pr_{Ti}(2), \ldots, Pr_{Ti}(\ell)\}$. Finally, T performs the following verification if

$$\tau^T_{low} \leq \mathbf{Pr}_{Ti}(k) \leq \tau^T_{high}; \quad \forall\ i = 1, \ldots n; \ \ k = 1 \ldots \ell.$$

After successful verification, the trusted node relays $m_T := \mathrm{AE}_{K_{GT}}(m'_1||ID_1, \ldots, m'_i||ID_i, \ldots, m'_n||ID_n)$ to G after $L'_n s$ transmission in a time division fashion.
4) **Reception at G:** The gateway G records RSS samples $\mathbf{Pr}_i = \{Pr_i(1), Pr_i(2), \ldots, Pr_i(\ell)\}$ while receiving m''_i. Further, G records the RSS samples $\mathbf{Pr}_T = \{Pr_T(1), Pr_T(2), \ldots, Pr_T(\ell')\}$ while receiving m'_T.
5) **Verification at G:** The gateway decrypts m'_T to obtain $m'_i||ID_i \ \forall\ i = 1, \ldots, n$ and verifies its integrity using the corresponding verification function. G rejects all received messages, if verification fails. Further, G verifies $m'_i \overset{?}{=} m''_i \ \forall\ i = 1, \ldots, n$; and rejects if the verification fails. Finally, G computes:

$$\Gamma = \{\gamma(1), \gamma(2), \ldots, \gamma_{\ell}\}, \gamma(k) = \frac{Pr_i(k)}{Pr_T(k)} \ \forall\ i = 1, \ldots, n.$$

The gateway accepts m''_i if $\tau_{low} \leq \gamma(k) \leq \tau_{high}; \quad \forall\ k = 1 \ldots \ell$, for all $i = 1, \ldots, n$.
6) **Primitive transmission from G:** Following successful verification G picks a secret value $X_G \in_U \mathbb{Z}_q$, computes the public value $z_G \leftarrow g^{X_i}$, and transmits as $m_G \leftarrow \{ID_G, z_G\}$.
7) **Key Establishment:** After reception of the message $\mathbf{L}$ computed the pairwise keys as $K_{Gi} \leftarrow (z_G)^{X_i}$ and G computes as $K_{Gi} \leftarrow (z_i)^{X_G}$.

Please note that the above protocol secures the $\mathbf{L}$-to-G communications. G-to-$\mathbf{L}$ communication is not secured and the nodes may establish trust with rogue G. Such a case can be observed by missing sensor data by a user and rectified.

B. Selection of Thresholds

Now, we first theoretically describe selecting the thresholds utilized in Steps 3 and 5 of STUN, followed by experimental results utilizing the following setup:

Setup: The data was captured previously on our underground testbed [8], [14], [15]. Specifically we utilized a 433 MHz Mica2 underground testbed in sandy and clay soil with a volumetric water level of 30%. The testbed utilized an antenna that can work with 30-69 cm wavelength, specifically G utilized a Full-Wave dipole antenna, whereas $\mathbf{L}$ and T utilized Single Ended Elliptical Antennas with up to 10dB gains. The distances were set as $d''_{GT} = 0.35$m, $d''_{Gi} = 0.40$m, $d'_{GT} = 7.8$m, $d'_{Gi} \approx 7.0$m, $d''_{Ti} \approx 2-5$m. A TinyOS application to implement message transmissions between the nodes. For all the experiments, we utilized 10dBm or 10mW transmission powers with 37 bytes packet size and 100 ms inter-packet time.

1) Thresholds τ^T for T: The objective of the threshold at T is to detect any outlier RSS values, as the pathloss from the co-located legitimate nodes are similar. Therefore, we utilize the median absolute deviation methodology [16]. The thresholds for detection at T are:

$$\begin{aligned} \tau^T_{low} &= \widetilde{\mathbf{Pr}_{Ti}} - \zeta * \nu \\ \tau^T_{high} &= \widetilde{\mathbf{Pr}_{Ti}} + \zeta * \nu, \end{aligned} \tag{4}$$

where $\widetilde{\mathbf{Pr}_{Ti}}$ is the median of all the RSS samples for all the nodes n, ζ is the parameter controlling the strictness of the outlier rule, and ν is the median absolute deviation

$$\nu = b \cdot \widetilde{|\mathbf{Pr}_{Ti} - \widetilde{\mathbf{Pr}_{Ti}}|}, \tag{5}$$

where $\tilde{\cdot}$ is the median of all the samples over all the nodes, and b is $1/Q(0.75) = 1.4826$. From our empirical experiments in Fig. 3(a), we show the plot between the RSS received at T from three underground nodes. We can observe that the RSS is constant over time. We also observe the $\tau^T_{low} = 2.512 \times 10^{-7}$mW and $\tau^T_{high} = 6.309 \times 10^{-7}$mW, due to high pathloss of the underground communication.

2) Thresholds τ for G: The objective of the threshold at the gateway is to determine the adversarial node from co-located nodes to the trusted nodes. Therefore, the threshold depends on the depth and soil characteristics of the underground nodes. The threshold is computed by taking the ratio of power received from the T and $\mathbf{L}$, which is given by

$$\tau = 10^{0.89(\alpha_T d''_{GT} - \alpha_i d''_{Gi})} \left(\frac{\beta_T d''_{GT}}{\beta_i d''_{Gi}} \right)^2, \tag{6}$$

where d''_{GT} is the underground depth of the trusted node, d''_{Gi} is the underground depth of the legitimate node L_i, and α_X and β_X are the parameters due to soil characteristics. Here, we assume that the OTA channel from both T and L_i is the same due to the same distance of G from the ground level. However, this is not true in practice due to other factors affecting the pathloss on the OTA portion of the wireless channel. Hence, we introduce a variable δ, thus two thresholds are given by

$$\begin{aligned} \tau^T_{low} &= \tau - \delta \\ \tau^T_{high} &= \tau + \delta. \end{aligned} \tag{7}$$

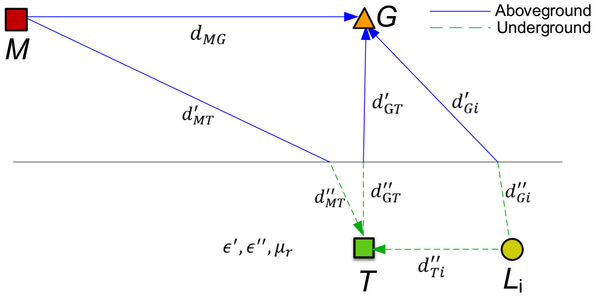


Fig. 4. A type 1 adversary M attempting to inject m_M and bootstrap with G with T performing simultaneous STUN verification.

We show the ratio of RSS in Fig. 3(b) of the signal received from T and $\mathbf{L}$ over time. We observe the ratio is close to 1. We also observe $\tau_{low} = 0.9$ and $\tau_{high} = 1.160$. Thus, the error is less than 10% is introduced by the underground fading channel due to communication over the air.

IV. Theoretical And Experimental Evaluation

We analyze the security of STUN against an adversary we have defined in Section II-B. In an attempt to pair with the gateway G 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 G. However, for G to accept the message, the adversary must pass the verification of Steps 3 and 5 at T and G, respectively, in STUN's verification.

A. Type 1 Adversary

M is a remote aboveground adversary outside the farm injecting m_M at power Pt_M, as shown in Fig 4, simultaneously received at underground T and aboveground G.

We evaluate the strategy of M to compute the transmit power for steps 3 and 5 independently and then evaluate effect of one step on the other. Using (1), (2), (3), and Step 3, the transmit power required by M for passing the verification in Step 3. The power received at T from L_i is given by

$$Pr_{Ti} = \frac{Pt_i G_i G_T}{10^{0.64+0.869\alpha_i d''_{Ti}} (d''_{Ti}\beta_i)^2}. \tag{8}$$

Further, the power received from M at T is given by

$$Pr_{TM} = \frac{Pt_M G_M G_T 10^{14.76}}{PL_{R_{AG-UG}} (d'_{MT})^{\eta} f^2 10^{0.64+0.869\alpha_T d''_{MT}} (d''_{MT}\beta_T)^2}. \tag{9}$$

In Step 3, T accepts M's signal if (8) and (9) are satisfied with some relaxation, which gives M's transmit power as

$$Pt_M = \frac{Pt_i G_i}{G_M} \frac{f^2 (d'_{MT})^{\eta} PL_{R_{AG-UG}}}{10^{14.76+0.869(\alpha_i d''_{Ti} - \alpha_T d''_{MT})}} \left(\frac{d''_{MT}\beta_T}{d''_{Ti}\beta_i} \right)^2 \pm \delta', \tag{10}$$

where d'_{XY} is the OTA distance between X and Y, d''_{XY} is the underground distance between X and Y, α_X and β_X the underground attenuation constant and phase shifting constants for X, respectively, η is the OTA attenuation constant, and δ' is the relaxation for the outlier evaluation technique.

Now for evaluating the capability of the type 1 M in defeating Step 5, we compute the power received by G

$$Pr_{GM} = \frac{Pt_M G_M G_G 10^{14.76}}{(d_{MG})^{\eta} f^2}. \tag{11}$$

Then the power received by the gateway from T

$$Pr_{GT} = \frac{Pt_T G_G G_T 10^{14.76}}{(d'_{GT})^{\eta} f^2 10^{0.64+0.869\alpha_T d''_{GT}} (d''_{GT}\beta_T)^2}. \tag{12}$$

Taking the ratio of (12) to (11) and equating to the threshold (6), we compute the transmission power to pass Step 5

$$Pt_M = \frac{Pt_T G_T}{G_M} \left(\frac{d_{MG}}{d'_{GT}}\right)^{\eta} \frac{1}{(d''_{GT}\beta_T)^2 10^{0.64+0.869\alpha_T d''_{GT}}} \pm \delta'', \tag{13}$$

where δ'' is the relaxation introduced due to the threshold selection. Now, for the adversary to pass both the verification simultaneously, the transmit power in (10) should equate to the transmit power in (13). Equating (10) and (13), we compute the distance between the adversary and the gateway as

$$d_{MG} = \left[\left(\frac{d''_{MT} d''_{GT} \beta_T^2}{d''_{Ti}\beta_i} \right)^2 \left(\frac{f^2 (d'_{MT} d'_{GT})^{\eta} PL_{R_{AG-UG}}}{10^{14.07+0.89(\alpha_i d''_{Ti} - \alpha_T (d''_{MT} + d''_{GT}))}} \right) \pm \delta \right]^{1/\eta} \tag{14}$$

where $\delta = \delta' \pm \delta''$, and assuming $Pt_i G_i / Pt_T G_T = 1$, or the power transmitted by legitimate and trusted node is the same and the antenna gains are the same. Therefore, a type 1 adversary at d_{MG} of the gateway can defeat STUN by transmitting from an aboveground location.

Experimental Evaluation: For evaluating the capabilities of an adversary, we emulate the adversarial data utilizing experimentally obtained wireless channel parameter specifically measured effective soil permittivity and relative permeability of the soil from the experimental setup described in Section III-B. In Fig 6(a), we plotted distance between a type 1 adversary from the gateway against distance between T and G for various center frequencies. We observe that the type 1 M has to be placed extremely far from G because M has to achieve same pathloss for underground-to-air while being aboveground. Also, M cannot reduce the transmit power rather than increasing the distance, as this will cause the adversary to fail Step 3 due to high attenuation for air-to-underground transmissions. Further, in Fig 6(b), shows the required transmission power for the type 1 adversary to defeat Step 3 of STUN for various center frequencies. We observe that the type 1 M has to transmit at extremely high powers when the legitimate nodes transmit at 3W. This is because the adversary has to have a communication range to G and underground T, simultaneously from the extremely far distance.

B. Type 2 Adversary

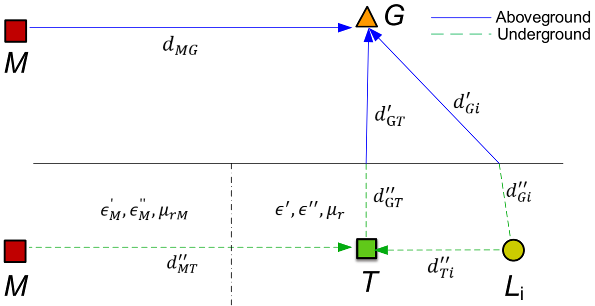


Fig. 5. A type 2 M attempting to inject m_M and bootstrap with G with T performing simultaneous STUN verification.

M is a remote aboveground adversary and a colluding underground adversarial node outside the farm injecting m_M transmitting at power Pt'_M, and Pt''_M to G and T, respectively as shown in Fig 5. M with a visual channel to G may be able to compute the power Pt'_M to defeat Step 5 according to (13).

To defeat Step 3, the transmit power has to satisfy (10). The best case for an adversary without knowing the location of the legitimate nodes cannot target just one legitimate node for defeating STUN with certainty. As the targeted node can be on the threshold of detection. Therefore, the adversary has to compute its transmit power according to the equation system S for all the underground nodes:

$$(S) \begin{cases} Pt''_M = \frac{Pt_1 G_1}{G_M} \left(\frac{d''_{MT}\beta_M}{d''_{T1}\beta_1}\right)^2 10^{0.89(\alpha_M d''_{MT} - \alpha_1 d''_{T1})} \pm \delta', \\ \vdots \\ Pt''_M = \frac{Pt_n G_n}{G_M} \left(\frac{d''_{MT}\beta_M}{d''_{Tn}\beta_n}\right)^2 10^{0.89(\alpha_M d''_{MT} - \alpha_n d''_{Tn})} \pm \delta'. \end{cases} \tag{15}$$

The equation system S is an underdefined multivariate quadratic equation system. It is well known that solution of such an equation system is NP-hard [9]. Moreover, even for small values of some equations (e) the best-known algorithms perform an exhaustive search [9]. Therefore, this type of systems are known as Unbalanced Oil and Vinegar (UOV) signature scheme. The security of UoV systems are proved for $3e \leq v \leq e(e+2)/2$ [9]. Where the system has e equations and v unknowns. Out of total number of variables e are known as the "oil" unknowns, and $(v - e)$ are called the "vinegar" unknowns. For our equation system S, we have seven variables in S which are known transmit power of the legitimate node (Pt_i), gain of antenna (G_X), operating frequency (f), and the relaxation introduced by the outlier evaluation technique (δ'). Further, there are six variables in S which are unknown transmit power of the underground adversary (Pt''_M), distance from the adversary to the trusted node (d'_{MT}), soil parameters (permitivity constants (ϵ', ϵ''), relative permeability μ_r)) as these control the variables (α_i, α_M, β_i and β_M), and distance between the legitimate node and trusted node d''_{Ti}. 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 UOV public cryptosystem the minimum number of legitimate nodes required per trusted node is four. In addition, it is important to note that in practice, the underground-to-underground wireless channel (e.g., M-T) has a limited communication range (i.e., less than 10m [17]).

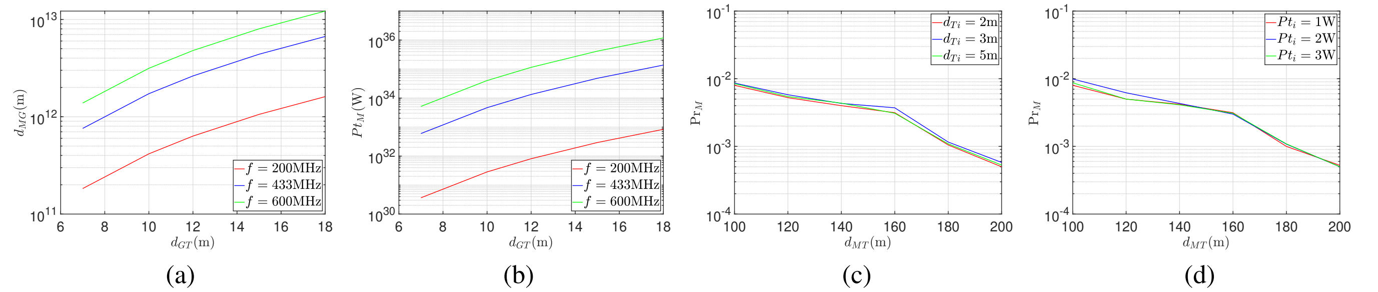


Fig. 6. Plots of (a) the distance between a type 1 M from G against the distance between T and G, (b) the required power transmitted by the type 1 M to defeat Step 3 of STUN, (c) the success probability of the type 2 M against the distance between M and T, and (d) the success probability of the type 2 M against the distance between M and T.

Experimental Evaluation: We evaluated the success probability of a type 2 adversary transmitting at any random transmit power by selecting from a uniform distribution between $[1-10]$W in an attempt to defeat Step 3 of STUN. The adversary is successful if the received power of the trusted node is between $\tau^T_{low} = 2.512 \times 10^{-7}$mW and $\tau^T_{high} = 6.309 \times 10^{-7}$mW as obtained in Section III-B. We emulated the adversary's pathloss according to (3) with the soil parameters obtained from the testbed. We ran the experiment 10,000 times. In Fig. 6(c) and (d) we plot the success probability of the type 2 adversary against the distance between the adversary and the trusted node. From both the plots, we observe that the success probability for the type 2 adversary is between 8.6×10^{-3} and 5.8×10^{-4}. STUN primitive is a single-use system, where the adversary has a single online chance to inject the message m_M. Thus, even for a larger probability of success of adversary is tolerable as compared to the well-known cryptographic security system. Similar security values have been deemed acceptable for pairing protocols utilizing short authentication strings [18].

V. Conclusion

We address the problem of a secret-free secure bootstrapping for COTS underground nodes with an aboveground gateway. We propose STUN, which can achieve node authentication and secret establishment in-band with the assistance of a trusted underground node by utilizing hard-to-forge underground wireless propagation laws. We theoretically prove that STUN has security equivalent to the UOV scheme in public cryptography. We also validate our theoretical results with experiments in an underground wireless testbed. In the future, we plan to experimentally evaluate and optimize the placements of the trusted nodes to cover an agricultural farm. Also, develop security for G-to-$\mathbf{L}$ communication link.

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. 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] A. Salam, M. C. Vuran, and S. Irmak, "Di-sense: In situ real-time permittivity estimation and soil moisture sensing using wireless underground communications," *Computer Networks*, vol. 151, pp. 31–41, 2019.

[2] 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.

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

[4] X. Liang, T. Yun, R. Peterson, and D. Kotz, "LightTouch: Securely connecting wearables to ambient displays with user intent," in *Proc. of INFOCOM*. IEEE, 2017, pp. 1–9.

[5] N. Ghose, L. Lazos, and M. Li, "HELP: Helper-enabled in-band device pairing resistant against signal cancellation," in *Proc. of 26th USENIX Security Symposium*, 2017, pp. 433–450.

[6] ——, "In-band secret-free pairing for cots wireless devices," *IEEE Transactions on Mobile Computing*, 2020.

[7] 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.

[8] 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.

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

[10] 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.

[11] M. Wilhelm, J. B. Schmitt, and V. Lenders, "Practical message manipulation attacks in IEEE 802.15. 4 wireless networks," in *Proc. of MMB & DFT 2012 Workshop*, 2012, pp. 29–31.

[12] 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.

[13] A. Sampath and C. Tripti, "Synchronization in distributed systems," in *Proc. of Advances in Computing and Information Technology*. Springer, 2012, pp. 417–424.

[14] 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.

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

[16] 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.

[17] 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.

[18] L. H. Nguyen and A. W. Roscoe, "Authentication protocols based on low-bandwidth unspoofable channels: a comparative survey," *Journal of Computer Security*, vol. 19, no. 1, pp. 139–201, 2011.