Hidden Terminal Emulation: An Attack in Dense IoT Networks in the Shared Spectrum Operation

Moinul Hossain and Jiang Xie
Department of Electrical and Computer Engineering
The University of North Carolina at Charlotte
Email: {mhossai4, Linda.Xie}@uncc.edu

***Abstract*—The Internet of Things (IoT) has been rapidly taking steps towards commercialization. However, the dense deployment of IoT nodes—that may follow different wireless technologies—in the shared spectrum creates a new challenge to solve: secure coordination among co-located IoT nodes from different IoT networks. In this paper, we shed light on this unique challenge, and we illustrate how this challenge has the potential to create a novel vulnerability where an attacker can pose as a hidden terminal (by manipulating its radiation patterns) and interfere with transmissions from its hidden counterparts, namely *hidden terminal emulation* (HTE) attack. As the dense deployment of IoT nodes will aggravate such hidden terminal interference, it facilitates the HTE attacker plausible deniability to interfere with its hidden counterparts. This paper is the first to present a theoretical analysis of the feasibility of HTE attacks (i.e., successful impersonation of hidden terminals), to illustrate how it is affected by the density of IoT nodes, and to provide insights on secure IoT deployment.**

I. Introduction

A new path to infinite possibilities has emerged with the advent of the Internet of Things (IoT) [1]. IoT consists of devices that possess the ability to generate, to process, and to exchange data. This data encompasses critical control, privacy-sensitive, and security information; hence, IoT requires thorough security analysis before its widespread deployment.

IoT is envisioned as a ubiquitous technology that will intricately integrate our surrounding devices and solve complex real-life problems. Such a broad scope requires an enormous amount of IoT deployment. As a result, it creates a unique situation where there will be *numerous IoT devices in a small physical space*, and these IoT devices will vie for the radio resource. Researchers have developed different solutions to this radio resource challenge [2]–[5], and spectrum sharing stands out as one of the prominent solutions because of its greater impact on efficient use of the radio resource [6], [7].

Intuitively, proprietary users can manage the network operation efficiently because of their sole control over their own licensed spectrum. However, heterogeneous wireless networks and technologies who share the same spectrum, require an appropriate global solution for secured coordination among them. Otherwise, it may potentially create new security vulnerabilities and hinder the spectrum sharing process [8]–[15].

Motivations: The dense deployment of IoT devices can bring a new vulnerability where attackers can exploit *natural hidden terminal interference* to corrupt transmissions of particular victim IoT devices [11]. Fig. 1 provides an illustration of this natural interference, where nodes $B2$ and $B4$ are hidden terminals to nodes $A1$, $A3$, and $A5$, and vice versa. These two sets of nodes belong to two different networks, and each of these two sets is unknown to transmissions of the other set. Therefore, it is highly probable that if nodes of these two sets utilize the same radio channel at the same time, they can create interference with the reception of nodes $A2$ and $A4$.

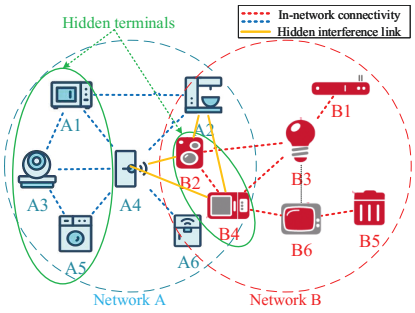


Fig. 1. Hidden terminal interference between coexisting IoT networks.

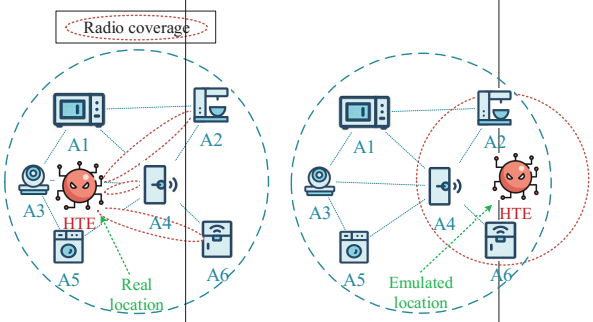
The concurrent transmissions from hidden nodes act as an interference at the corresponding exposed receiver(s), and it is difficult to differentiate between a benign node (i.e., benign hidden terminal) and a malicious interference source. Moreover, traditional IoT devices cannot incorporate sophisticated localization mechanisms [16]–[18] to probe and detect location spoofing because of their hardware constraints. Therefore, if an attacker can impersonate a hidden node to a particular IoT node (by manipulating radiation pattern), it can capitalize on this natural interference scenario to corrupt the attempted transmissions from the IoT node. This can be a *life-threatening attack* if a perpetrator compromises a critical medical IoT device (e.g., oxygen pump, pacemaker) or a vehicle operation controller [19]–[21]. Hence, there is an urgent need for a comprehensive and rigorous investigation of this vulnerability.

Challenges: The underlying principle of the HTE attack is to spoof a different location where it can emulate the physical behavior of a benign hidden node. In Fig. 2(a), the attacker tries to impersonate a hidden terminal to nodes $A1$, $A3$, and $A5$; it exposes its identity only to nodes $A2$, $A4$, and $A6$ through smart array antennas. The intelligent exploitation of smart array antennas enables the attacker to create a different physical scenario than the real one, which is represented in Fig. 2(b). Here, the attacker tries to interrupt packets from $A1$, $A3$, and $A5$ to $A2$ and $A4$. Though location spoofing attacks have been studied for quite a few years, to the best of our knowledge, no work considered spoofing a location that will create a hidden terminal scenario. In addition, creating such a scenario in a dense IoT network offers additional challenges

This work was supported in part by the US National Science Foundation (NSF) under Grant No. 1718666, 1731675, 1910667, and 1910891.

978-1-7281-0962-6/19/$31.00 ©2019 IEEE

and raises a feasibility question of perpetrating this attack.



(a) The real scenario. (b) The emulated scenario.

Fig. 2. The hidden terminal emulation attack.

Contributions: In this paper, we study these challenges and propose solutions. The novel contributions of this paper are summarized in the following:

1. We propose a reactive attack model based on location spoofing, where the HTE attacker attacks by impersonating a hidden terminal to the victim. In the proposed model, the attacker emulates a hidden terminal by manipulating its antenna radiation pattern.
2. We formulate HTE as a nonlinear feasibility problem that is based on smart antenna array synthesis. We solve the problem using semidefinite relaxation (SDR) in conjunction with a heuristic local-search algorithm.

Related Work on Location Spoofing: As discussed, an HTE attacker tries to emulate the radiation characteristics of a hidden terminal and creates a different physical scenario than the actual one (Fig. 2). Thereby, we compare it to conventional location spoofing attacks in the localization paradigm, especially with received signal strength (RSS) based methods. In [16], it is experimentally shown that, by manipulating the RSS at the anchors, the localization method can be made futile. Directional antennas are exploited in [22], where the attackers have the ability to bias the location estimation to a direction of their choice. In [23], a mathematical analysis of beamforming-based perfect location spoofing against RSS-based localization techniques is proposed, where an attacker mimics the path-loss signature at the anchor nodes to manipulate the results of RSS-based localization algorithms. The vulnerability of WLAN-based Skyhook positioning system [24] is investigated in [25] where authors demonstrated the susceptibility of Skyhook against location spoofing attacks.

However, location spoofing is more challenging in an exponentially denser network environment. Unlike previous works, we address these challenges and formulate a mathematical model to test the feasibility of the HTE attack.

II. The Hidden Terminal Emulation Attack

In the literature, location forging is considered a localization problem, and anchor nodes—specially equipped to locate any node—play an important role in detecting location forging attacks. However, in most IoT applications, IoT nodes may not be equipped with localization capabilities; hence, in dense IoT scenarios, off-the-shelf location spoofing detection methods cannot be directly applied. Thereby, a different approach is taken [11] to analyze the HTE attack, which is conducted in two sequential phases: the reconnaissance and emulation phase and the reactive interference phase.

The Reconnaissance and Emulation Phase: In this phase, the primary task of an HTE attacker is to successfully emulate the radiation characteristics of a benign hidden terminal to the neighbors of the victim(s). In this paper, we consider the *exposed node(s) as victim(s)* (e.g., $A2$ and/or $A4$ in Fig. 2), and the attacker is motivated to reactively interfere with transmissions originating from the hidden nodes (e.g., $A1$, $A3$, and/or $A5$ in Fig. 2) that are destined for the victim node(s).

With conventional omnidirectional radios, realizing HTE attack is not possible because the path-loss vector would be the same at each direction. An attacker, however, can use smart antenna's beamforming capability to solve this problem and mimic the signal characteristics of the spoofed location. To achieve this, the attacker first obtains the geometric locations of the IoT nodes by wardriving [26] and other off-the-shelf techniques, such as the angle of arrival and distance to the transmitter. Then, it deduces an optimal antenna configuration that enables the emulation of a hidden terminal. Please note that, as complex localization schemes are highly unlikely to be present in general IoT nodes, an attacker does not require to mimic the exact RSS signature of the spoofed location; instead, it must maintain an average signal strength equal to or above R_{th} (i.e., the receiver sensitivity threshold) at the exposed node(s) and an average signal strength lower than S_{th} (i.e., the carrier sensing threshold) at the hidden nodes.

The Reactive Interference Phase: In this phase, the HTE attacker continues to sense the operating band through wide-band sensing and sniffs the band for request-to-send (RTS) and clear-to-send (CTS) messages addressed to or from the victim node, respectively. Afterward, it deliberately interferes transmissions from nodes $A1$, $A3$, and $A5$, that are destined to the victim node (e.g., $A4$). However, the choice of interference rate depends on the strategy of the attacker; it may interfere with each transmission or randomly choose to jam. An interference strategy is proposed in [11].

Summary: The HTE attacker utilizes the smart antenna array technology that is widely available for communication purposes and weaponizes this technology to perpetrate the attack. A wide range of distinct attack strategies can be studied from the proposed generalized attack strategy.

III. The Reconnaissance and Emulation Phase

As discussed, in reality, IoT nodes are unlikely to have necessary tools to analyze RSS readings that are received from different IoT nodes of different networks, and this makes low-powered, computationally limited IoT nodes more vulnerable to the HTE attack. In the remainder of this work, we consider that the HTE attacker is equipped with a circular smart antenna array that consists of N_{ele} isotropic elements put on a circle with a radius r, and the i^{th} antenna element is placed with the phase angle ϕ_i. The beamforming-pattern for the circular smart antenna is characterized by,

$$G(\theta) = \sum_{i=1}^{N_{ele}} w_i \exp\left[j\frac{2\pi}{\lambda} r\cos(\theta - \phi_i)\right], \quad (1)$$

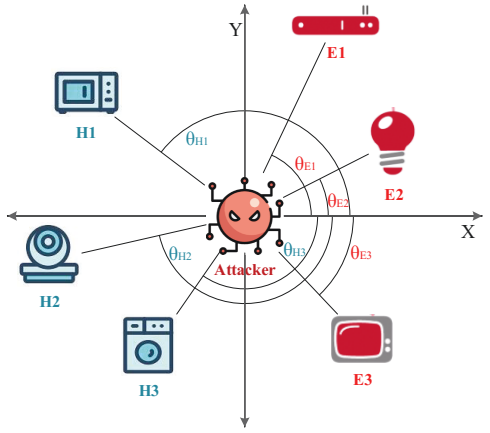


Fig. 3. Problem formulation of the HTE attack.

where λ is the signal wavelength, θ represents the direction to the respective IoT node, and $\mathbf{w} = [w_1, w_2, \cdots, w_{N_{ele}}]$ is the complex weight vector that can be tuned to change the radiation pattern. Here, the circular array antenna is chosen to illustrate the formulation of the analysis because it can produce flexible asymmetric radiation patterns and can deflect a beam through 2π. Nonetheless, the analysis is not limited to circular antenna array; a different antenna model with a different geometric form can be incorporated by replacing its corresponding beamforming equation in (1).

However, designing such an attack model requires realistic limitations to consider, such as smart antenna design and relative distances to each IoT nodes. Therefore, it is probable that not all locations are feasible to perpetrate this attack.

A. Problem Overview

To understand how we analyze the condition that an attacker at a certain location can launch the HTE attack, let us look at the illustration in Fig. 3 where an attacker is trying to reveal its transmission to nodes $E1$, $E2$, and $E3$ and to hide its transmission from nodes $H1$, $H2$, and $H3$. In order to reduce the radio coverage at unwanted directions and to steer the radio transmission to intended directions, we use the log-distance path-loss model to infer the mean RSSs at given distances. According to the log-distance path-loss model, the mean path-loss at distance d is,

$$PL_d(dB) = 10\alpha \log_{10} d + PL_{d_0}(dB), \tag{2}$$

where PL_{d_0} is the path loss at the reference distance $d_0 = 1m$ and α is the path-loss exponent. Moreover, the path-loss at distance d can be expressed as,

$$PL_d(dB) = P_0(dBm) - P_{R_d}(dBm), \tag{3}$$

where P_0 is the required transmission power to keep a good connection with the receiver if omni-directional antenna is used and P_{R_d} is the received signal strength at distance d. Therefore, combining (2) and (3), we have,

$$P_{R_d} = \frac{P_0}{PL_0 d^\alpha}. \tag{4}$$

For a smart antenna with steering capacity, the transmission power in direction θ is represented by $P_0|G(\theta)|^2$ instead of P_0. So we rewrite (4) as,

$$P_{R_d}(\theta) = \frac{P_0|G(\theta)|^2}{PL_0 d^\alpha}, \tag{5}$$

where $P_{R_d}(\theta)$ represents the received signal strength at distance d along the direction θ. Now, for m exposed nodes and n hidden nodes,

$$P_{R_{d_i}}(\theta_{E_i}) = \frac{P_0|G(\theta_{E_i})|^2}{PL_0(d_{E_i})^\alpha}, \tag{6}$$

$$P_{R_{d_j}}(\theta_{H_j}) = \frac{P_0|G(\theta_{H_j})|^2}{PL_0(d_{H_j})^\alpha}, \tag{7}$$

where $i = 1, 2, \cdots, m$ and $j = 1, 2, \cdots, n$.
From (1), the beamforming directional gain in the direction of the i_{th} node can be written as,

$$|G(\theta_{E_i})|^2 = |\mathbf{w}\mathbf{c_i}|^2, \tag{8}$$

where

$$\mathbf{c}_i = \begin{bmatrix} \exp[j\frac{2\pi}{\lambda} r\cos(\theta_{E_i} - \phi_1)] \\ \exp[j\frac{2\pi}{\lambda} r\cos(\theta_{E_i} - \phi_2)] \\ \cdot \\ \cdot \\ \cdot \\ \exp[j\frac{2\pi}{\lambda} r\cos(\theta_{E_i} - \phi_{N_{ele}})] \end{bmatrix}. \tag{9}$$

Letting,

$$\begin{aligned} \mathbf{h}_i &= \left[\frac{P_0}{PL_0(d_{E_i})^\alpha}\right]^{\frac{1}{2}} \mathbf{c}_i, \quad i = 1, 2, \cdots, m \\ \mathbf{g}_j &= \left[\frac{P_0}{PL_0(d_{H_j})^\alpha}\right]^{\frac{1}{2}} \mathbf{c}_j, \quad j = 1, 2, \cdots, n \end{aligned} \tag{10}$$

the feasibility of HTE attack can be modeled as,

$$\begin{aligned} &\text{find any} && \mathbf{w} \\ &\text{subject to} && |\mathbf{w}^H \mathbf{h}_i|^2 \geq R_{th}, \quad i = 1, \cdots, m \\ &&& |\mathbf{w}^H \mathbf{g}_j|^2 < S_{th}, \quad j = 1, \cdots, n \end{aligned} \tag{11}$$

where R_{th} and S_{th} represent the receiver sensitivity and carrier sensing threshold, respectively. It can be seen that the above problem belongs to the class of quadratically constrained quadratic programming (QCQP) problems. The constraints are concave homogeneous quadratic constraints. The problem contains a special case of the problem considered in [27]; hence, it is NP-hard.

B. Solving HTE Problem

As the feasibility problem of HTE defined in (11) is an NP-hard problem, it is not possible to analyze the properties of HTE by directly solving it. Therefore, we first formulate the derivation of a relaxed problem, which will incorporate a solution that provides an upper bound for the feasibility answers to the HTE problem; that is, if the relaxed problem is infeasible, (11) is definitely infeasible. Afterward, we provide a randomization technique, which in most of the cases finds a feasible solution through a local search around the point generated by the relaxed problem. This randomization algorithm essentially serves with a lower bound on the HTE problem (11); that is, if the randomization algorithm can find a feasible solution, (11) is certainly feasible.

Relaxation: To deduce the relaxed problem, first, we include an objective function to the problem (11); therefore, when multiple solutions exist, the one with the minimum objective

value is returned. We reformulate the HTE feasibility problem to minimizing the transmission power problem,

$$\begin{aligned} &\text{minimize}_{\mathbf{w}} && ||\mathbf{w}||_2^2 \\ &\text{subject to} && |\mathbf{w}^H\mathbf{h}_i|^2 \geq R_{th}, \;\; i = 1, \cdots, m \\ &&& |\mathbf{w}^H\mathbf{g}_j|^2 < S_{th}, \;\; j = 1, \cdots, n \end{aligned} \tag{12}$$

where $||\cdot||_2$ stands for the Euclidean norm of a vector.

Now using the fact that $\mathbf{h}^H\mathbf{w}\mathbf{w}^H\mathbf{h} = \text{trace}(\mathbf{h}^H\mathbf{w}\mathbf{w}^H\mathbf{h})$ where $\text{trace}(\cdot)$ represents the trace of a matrix, (11) can recast as,

$$\begin{aligned} &\text{minimize}_{\mathbf{X}} && \text{trace}(\mathbf{X}) \\ &\text{subject to} && \text{trace}(\mathbf{X}\mathbf{Q}) \geq R_{th}, \;\; i = 1, \cdots, m \\ &&& \text{trace}(\mathbf{X}\mathbf{Q}) < S_{th}, \;\; j = 1, \cdots, n \\ &&& \mathbf{X} \succeq 0, \\ &&& \text{rank}(\mathbf{X}) = 1, \end{aligned} \tag{13}$$

where $\mathbf{X} = \mathbf{w}\mathbf{w}^H$, $\mathbf{Q} = \mathbf{h}\mathbf{h}^H$, $\text{rank}(\cdot)$ denotes the rank of a matrix, and $\mathbf{X} \succeq 0$ means that $\mathbf{X}$ is a Hermitian positive semidefinite matrix.

Note that since (11) is an NP-hard problem, so is (13). Therefore, in the following, a heuristic solution is utilized to analyze a relaxed version of (13). The relaxation is based on the observation that (13) is almost similar to a semidefinite programming problem except for the last constraint; that is, $\text{rank}(\mathbf{X}) = 1$, which is non-convex. As a semidefinite problem can be solved in polynomial time, we relax (13) by discarding the rank constraint and deduce an SDR problem,

$$\begin{aligned} &\text{minimize}_{\mathbf{X}} && \text{trace}(\mathbf{X}) \\ &\text{subject to} && \text{trace}(\mathbf{X}\mathbf{Q}) \geq R_{th}, \;\; i = 1, \cdots, m \\ &&& \text{trace}(\mathbf{X}\mathbf{Q}) < S_{th}, \;\; j = 1, \cdots, n \\ &&& \mathbf{X} \succeq 0 \end{aligned} \tag{14}$$

The optimal solution $\mathbf{X}_{opt}$ of the SDR problem provides a lower bound for the objective value of (12). If the problem does not yield in a solution, (11) is infeasible. This is because the feasible region of the actual problem (11) is actually a subset of the feasible region of the relaxed problem (14). However, the solution $\mathbf{X}_{opt}$ of the SDR problem does not necessarily solve the NP-hard problem. Nonetheless, the rank relaxation of a general QCQP problem results in the Lagrange bi-dual problem, which is the closest convex problem to the original NP-hard problem. Therefore, though $\mathbf{X}_{opt}$ may not be the optimal solution for the HTE problem, it conforms to other constraints in (13), which means that it could be close to the feasible region of the original HTE problem. Based on this observation, we employ a local-search based randomization algorithm to search for a feasible solution to (11).

Randomization Algorithm: If the solution $\mathbf{X}_{opt}$ is rank-one, $\mathbf{w}$ can be deduced by finding the principal eigenvector corresponding to only the non-zero eigenvalue. However, as the SDR relaxes the rank-one constraint, $\mathbf{X}_{opt}$ may not be rank-one in reality. Similar to [27], once the SDR problem is solved, a randomized technique can be used to obtain an approximate solution to the original HTE feasibility problem. Numerous randomization techniques have been proposed so far, and we modify the one proposed in [27]. The general idea of this method is to create a set of candidate vectors $\{\tilde{\mathbf{w}}_{can,i}\}_{i=1}^{L}$ (L = number of randomizations) using $\mathbf{X}_{opt}$ and choose the optimal solution from these candidate vectors.

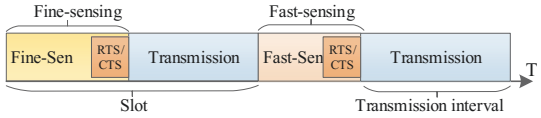


Fig. 4. The channel access schedule.

In our application, first, to deduce the candidate vectors, the eigencomposition of $\mathbf{X}_{opt}$ is expressed in the form,

$$\mathbf{X}_{opt} = \mathbf{A}\mathbf{V}\mathbf{A}^H, \tag{15}$$

and the candidate beamforming vector in the form,

$$\tilde{\mathbf{w}}_{can,i} = \mathbf{A}\mathbf{V}^{1/2}\lambda_l, \tag{16}$$

is selected as a candidate vector, where $\mathbf{A}$ is a unitary matrix of eigenvectors, $\mathbf{V}$ is a diagonal matrix of eigenvalues, and λ_l is the random vector that consists of uniformly distributed independent random variables on the unit circle in the complex plane. It helps us to ensure that $\tilde{\mathbf{w}}_{can,i}\tilde{\mathbf{w}}_{can,i}^H = \mathbf{A}\mathbf{V}^{1/2}\lambda_l\mathbf{A}^H(\mathbf{V}^{1/2})^H{\lambda_l}^H = \text{trace}(\mathbf{V}\lambda_l{\lambda_l}^H) = \text{trace}(\mathbf{V}) = \text{trace}(\mathbf{X}_{opt})$. If any constraint in (12) is not met by $\tilde{\mathbf{w}}_{can,i}$, a new randomization round begins. If multiple feasible candidates are found, the one with the smallest norm is selected.

Summary: We formulate a numerical method to test the feasibility of the emulation phase. (11) belongs to the class of QCQP problems. It contains a special case of the problem considered in [27]; hence, it is NP-hard, and it is not possible to analyze the properties by directly solving it. Therefore, we first formulate the derivation of a relaxed problem which will provide an upper bound for the feasibility answers to the emulation problem; that is, if the relaxed problem is infeasible, (11) is definitely infeasible. Afterward, we use a randomization technique which finds a feasible solution through a local search around the point generated by the relaxed problem. This randomization algorithm essentially serves as a lower bound on the HTE problem (11); that is, if the randomization algorithm can find a feasible solution, (11) is certainly feasible.

IV. Performance Analysis

In this section, we simulate the SDR problem and the randomization algorithm described in Section III to analyze the feasibility of HTE attack under different scenarios.

A. Simulation Setup

In the simulation, this work considers a possible beamforming aiming error ($\gamma_\theta = 1^o$) when the attacker directs its beam towards a certain direction. Hence, $G(\theta)$ is replaced by $G(\theta \pm \gamma_\theta)$. First, we analyze the feasibility of HTE attacks with the fixed location of the victim or exposed nodes and under randomly generated locations of the hidden nodes. We consider a 20×20 2-D space. The path-loss exponent $\alpha = 3.5$, victim's true location is $(0, 0)$ (with two victims $(0, 5)$ and $(0, -5)$), the required transmit power when omnidirectional antenna is used $P_0 = 10$ dBm, receiving antenna sensitivity $R_{th} = -70$ dBm, carrier sensing threshold $S_{th} = -100$ dBm, and the path loss at $d_o = 1m$ is $P_d = 30$ dB.

IoT Node Model: We consider that the victim IoT node has n neighbors in its radio range, and they use omnidirectional antennas for communications. Every benign IoT node is equipped with one radio for spectrum sensing and one radio for control information exchange and data transmission.

Channel Access: In shared spectrum operations, each transmission attempt of an IoT node must be preceded by a sensing interval. As shown in Fig. 4, IoT nodes employ longer fine-sensing to sense the current channel before initiating a transmission, and they continue to sense the channel—using shorter fast-sensing—during the transmission to negate the collision with co-located IoT nodes. An IoT node is allowed to access a channel when it finds the channel available. After accessing the channel, two IoT nodes exchange RTS/CTS messages to reserve the channel.

Though the scope of this paper is to illustrate the PHY-layer constraints and configurations of the attacker (i.e., the reconnaissance and emulation phase), we incorporate MAC-layer information to help readers grasp a more comprehensive overview of the HTE attack.

B. Success Rate of HTE

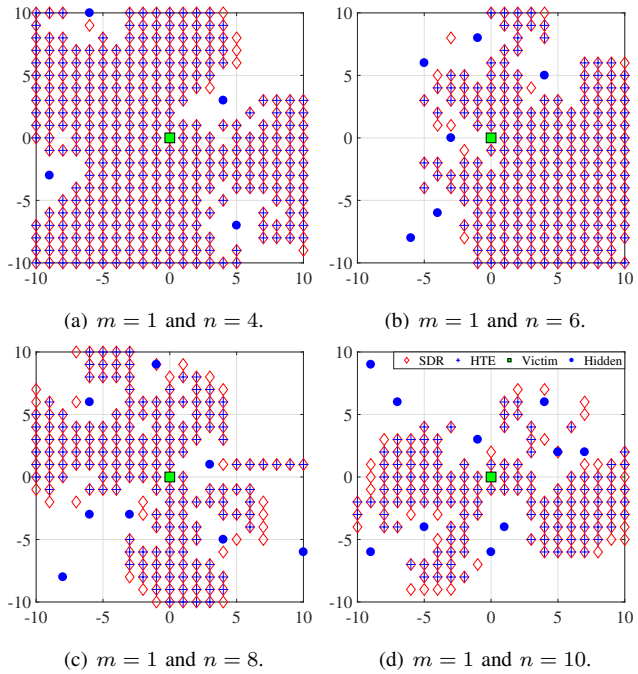
We use the Monte Carlo simulation to estimate the success rate of HTE attacks—in terms of successfully impersonating as a hidden terminal—with different combinations of the number of antenna elements (N_{ele}) and the number of hidden nodes (n). In each simulation, the location of each node is randomly generated, except the victim node (i.e., $(0, 0)$).

For each combination, totally 1000 trial runs are launched, and the values in Table I represent the average of these trials. The table contains the number of times where the SDR problem finds a solution (A_{SDR}), the number of times where the randomization algorithm finds a feasible solution (A_{local}), and how tightly these two results are bounded (A_{local}/A_{SDR}). As the SDR solution provides an upper bound and the local-search provides a lower bound on the original HTE feasibility problem, the number of times that the original problem has feasible solutions lie between A_{SDR} and A_{local}.

TABLE I
SUCCESSFUL CASES

n	$N_{ele} = 4$	$N_{ele} = 6$	$N_{ele} = 8$	$N_{ele} = 10$
4	84/80 95%	141/137 97%	154/149 97%	310/303 98%
5	71/65 92%	112/107 96%	121/113 93%	289/271 94%
6	62/53 85%	98/92 94%	117/102 87%	258/230 89%
8	2/0	14/12 86%	73/60 82%	217/186 86%
10	0/0	5/3 60%	29/22 77%	91/67 74%

Table I demonstrates two important trends. First, both A_{SDR} and A_{local} increases as we increase the number of antenna elements (N_{ele}). It happens because a smart array antenna with more antenna elements offers more flexibility in tuning the radiation pattern; hence, it makes an attacker more capable to perpetrate HTE attacks. In addition, mathematically, more antenna elements means that $\mathbf{w}$ is more tunable and hence larger degree of freedom in solving the problem. Second, both A_{SDR} and A_{local} decrease as n increases. Intuitively, we can understand that adding more hidden nodes represents adding more constraints to the original problem; hence, reducing the feasible space. We can also observe the feasibility of HTE attack with a comparatively lower number of antenna elements than the number of hidden nodes. In the simulation, we observe only two cases where HTE is not feasible, i.e., $n = \{8, 10\}$ and $N_{ele} = 4$. It signifies the weakness of dense IoT deployment against the HTE attack.



(a) $m = 1$ and $n = 4$. (b) $m = 1$ and $n = 6$. (c) $m = 1$ and $n = 8$. (d) $m = 1$ and $n = 10$.

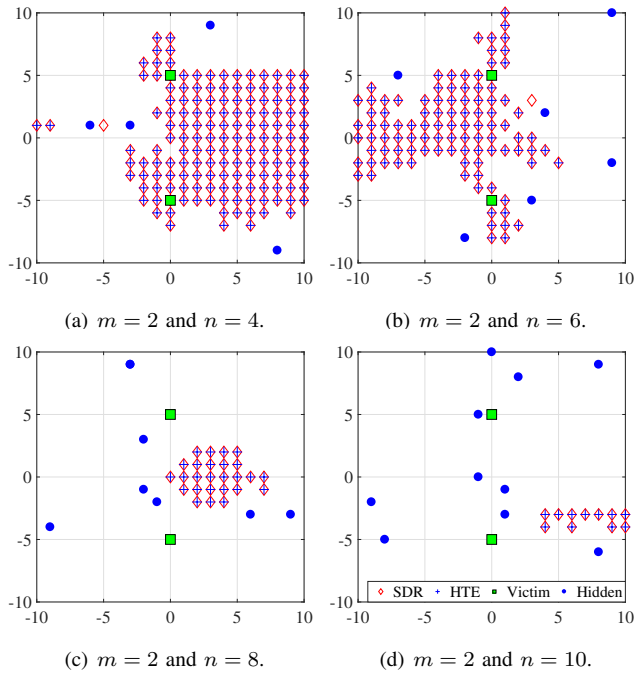
Fig. 5. The geometric statistics of HTE feasibility problem.

C. Impact of Exposed and Hidden Node Density

In this part, we investigate how the feasibility of HTE is impacted by the number of exposed or victim nodes (m) and hidden nodes (n), more importantly, how the relative positions and angles of all nodes impact the feasibility problem. In the simulation, all nodes are fixed, and we vary the true location of the attacker along a square grid in the simulated 2-D space to identify the location where the attacker can find a feasible solution and can launch HTE attacks. A group of simulations are shown in Fig. 5. The parameters used in generating the figure are $N_{ele} = 10$, $m = 1$, and $n = \{4, 6, 8, 10\}$. In Fig. 5 and 6, the locations marked by green filled squares, blue filled circles, red unfilled diamonds, and blue pluses represent the location of the victim(s) (m), hidden nodes (n), SDR feasible points, and HTE feasible points, respectively.

Hidden Node Density: In the figure, most of the locations where SDR is feasible, are also marked by blue pluses; it means that solutions to the HTE feasibility problem are tightly bounded by solutions to the SDR and the randomization algorithm. By comparing the figures in Fig. 5, we can observe that as the number of hidden nodes in the attacker's transmission range increases, the number of locations where HTE is feasible decreases. It indicates that the higher density of IoT nodes is less susceptible to HTE attacks. Thereby it provides an important understanding of secure IoT deployments.

Guard Against HTE Attacks: This analysis is insightful to trace the physical location of HTE attackers. If we can determine the presence of the HTE attacker (using a different method), this analysis has the potential to help us narrow down possible hiding locations of the HTE attacker, as HTE can be launched from only certain places. Furthermore, this



(a) $m = 2$ and $n = 4$. (b) $m = 2$ and $n = 6$.

(c) $m = 2$ and $n = 8$. (d) $m = 2$ and $n = 10$.

Fig. 6. Attack efficiency vs risk of detection.

analysis is also helpful for finding the weaknesses in critical IoT infrastructure in the shared spectrum operation; therefore, it can help design a robust IoT network.

Attack Efficiency vs Risk of Exposure: Intuitively, an attacker must utilize its resources to maximize its attack objective, i.e., attacking more IoT nodes. However, it must also take into account the risk of detection. From Fig. 5 and Fig. 6, we can observe that, as we increase the number of victim nodes or exposed nodes from $m = 1$ to $m = 2$, the feasible space to launch the attack decreases. Thereby, it also increases the risk of exposing the attacker's location. Hence, considering this observation, an attacker must trade-off between the reward of attack and the cost of exposure.

V. Conclusion

In this paper, we discussed a vulnerability that the dense IoT deployment will likely bring, i.e., interference from impersonating hidden terminals of external IoT networks, and we illustrated how an HTE attacker can exploit this vulnerability by manipulating its antenna radiation pattern. This work is among the first to foresee this vulnerability of IoT deployment, study it, and, to the best of our knowledge, the first to propose an attack feasibility study based on array antenna synthesis. We utilized the SDR technique and a randomization algorithm to efficiently solve the HTE feasibility problem. Simulation results indicate that the proposed method provides a strong approximation to the HTE feasibility problem. In addition, the observation from the simulation results provides an attacker's conundrum to trade-off between the attack efficiency (i.e., attacking more victims) and the risk of exposure. Lastly, the analysis and observation provide insightful guidance to narrow down the probable locations of an HTE attacker.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Elsevier Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[3] D. Bharadia *et al.*, "Full duplex radios," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 375–386, 2013.

[4] Y. Saito *et al.*, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE Vehicular Technology Conference (VTC Spring)*, pp. 1–5, 2013.

[5] S. K. Sharma, T. E. Bogale, L. B. Le, S. Chatzinotas, X. Wang, and B. Ottersten, "Dynamic spectrum sharing in 5G wireless networks with full-duplex technology: Recent advances and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 674–707, 2018.

[6] G. Ding, J. Wang, Q. Wu, Y.-D. Yao, R. Li, H. Zhang, and Y. Zou, "On the limits of predictability in real-world radio spectrum state dynamics: From entropy theory to 5G spectrum sharing," *IEEE Communications Magazine*, vol. 53, no. 7, pp. 178–183, 2015.

[7] X. Liu and J. Xie, "A practical self-adaptive rendezvous protocol in cognitive radio ad hoc networks," in *Proc. IEEE INFOCOM*, pp. 2085–2093, 2014.

[8] M. Hossain and J. Xie, "Impact of off-sensing attacks in cognitive radio networks," in *Proc. IEEE GLOBECOM*, pp. 1–6, 2017.

[9] M. Hossain and J. Xie, "Covert spectrum handoff: An attack in spectrum handoff processes in cognitive radio networks," in *Proc. IEEE GLOBECOM*, pp. 1–6, 2018.

[10] M. Hossain and J. Xie, "Off-sensing and route manipulation attack: A cross-layer attack in cognitive radio based wireless mesh networks," in *Proc. IEEE INFOCOM*, pp. 1376–1384, 2018.

[11] M. Hossain and J. Xie, "Detection of hidden terminal emulation attacks in cognitive radio-enabled IoT networks," in *Proc. IEEE ICC*, pp. 1–6, 2019.

[12] M. Hossain and J. Xie, "Hide and seek: A defense against off-sensing attack in cognitive radio networks," in *Proc. IEEE INFOCOM*, pp. 613–621, 2019.

[13] U. Narayanan and J. Xie, "Signaling cost analysis of handoffs in a mixed IPv4/IPv6 mobile environment," in *Proc IEEE GLOBECOM*, pp. 1792–1796, 2007.

[14] A. M. Srivatsa and J. Xie, "A performance study of mobile handoff delay in IEEE 802.11-based wireless mesh networks," in *Proc. IEEE ICC*, pp. 2485–2489, 2008.

[15] Y. Song and J. Xie, "Finding out the liars: Fighting against false channel information exchange attacks in cognitive radio ad hoc networks," in *Proc IEEE GLOBECOM*, pp. 2095–2100, 2012.

[16] Y. Chen, W. Trappe, and R. P. Martin, "Attack detection in wireless localization," in *Proc. IEEE INFOCOM*, pp. 1964–1972, 2007.

[17] X. Li, Y. Chen, J. Yang, and X. Zheng, "Designing localization algorithms robust to signal strength attacks," in *Proc. IEEE INFOCOM*, pp. 341–345, 2011.

[18] Z. Li, Z. Xiao, Y. Zhu, I. Pattarachanyakul, B. Y. Zhao, and H. Zheng, "Adversarial localization against wireless cameras," in *Proc. International Workshop on Mobile Computing Systems & Applications (HotMobile)*, pp. 87–92, 2018.

[19] The 7 craziest IoT device hacks, "https://threatpost.com/pair-of-bugs-open-honeywell-home-controllers-up-to-easy-hacks/113965/," Accessed April 2019.

[20] When the IoT attacks: Four examples of the highest security stakes we've seen, "https://www.aberdeen.com/techpro-essentials/when-the-iot-attacks-four-examples-of-the-highest-security-stakes-weve-seen/," Accessed April 2019.

[21] The 5 worst examples of IoT hacking and vulnerabilities in recorded history, "https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/," Accessed April 2019.

[22] K. Bauer *et al.*, "The directional attack on wireless localization: how to spoof your location with a tin can," in *Proc. IEEE GLOBECOM*, pp. 4125–4130, 2009.

[23] T. Wang and Y. Yang, "Analysis on perfect location spoofing attacks using beamforming," in *Proc. IEEE INFOCOM*, pp. 2778–2786, 2013.

[24] Inc. Skyhook, "http://www.skyhookwireless.com," Accessed April 2019.

[25] N. O. Tippenhauer *et al.*, "iPhone and iPod location spoofing: Attacks on public WLAN-based positioning systems," *Technical Report/ETH Zürich, Department of Computer Science*, vol. 599, 2012.

[26] D. Han *et al.*, "Access point localization using local signal strength gradient," in *Proc. International Conference on Passive and Active Network Measurement*, pp. 99–108, 2009.

[27] N. D. Sidiropoulos, T. N. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Transactions on Signal Processing*, vol. 54, no. 6-1, pp. 2239–2251, 2006.