2015 IEEE 21st International Conference on Parallel and Distributed Systems

Jamming with Power Boost: Leaky Waveguide Vulnerability in Train Systems

Sang-Yoon Chang*, Bao Anh N. Tran§, Yih-Chun Hu†, Douglas L. Jones‡
*§†‡Advanced Digital Sciences Center †‡University of Illinois at Urbana-Champaign
Email: {sychg, baoanh.t, yihchun, jones}@adsc.com.sg

***Abstract*—Modern-day train operations rely on wireless communications. Unlike other mobile systems, the train vehicle operations are tightly interwound with and remain physically close to the railway and the trackside infrastructure, providing a suitable platform to deploy leaky-waveguide-based communication. Due to the train system's safety-critical application and its exposure to the public, it is critical to address security in train communications. To investigate the availability of leaky waveguide communications, we first study prior leaky waveguide implementations in train systems and, based on those studies, construct a model to characterize the path loss of inside-waveguide propagation and the repeater implementations. Using our model, we analyze the jamming impact and contrast with jamming in free space without a waveguide. As a result, we establish that jamming the waveguide takes advantage of the waveguide infrastructure to extend its impact beyond the traditional jamming range and breaks the spatial dependence on the jamming source.**

I. Introduction

With the advent of computing and machine automation, railway train operations are increasingly becoming human-independent. For example, fully automatic trains are running without on-board human drivers in the cities of Singapore, Shanghai, Dubai, Seoul, and Paris. Public train systems are quicker to adopt automation than other transportation applications because, unlike cars and airplanes (which in current practice rely more heavily on sensing capabilities to make individual actuation decisions), trains operate in a fixed routine and their mobility is restricted to one-dimensional rail lines. The trains's operational space being limited and consistently surrounded by the train infrastructure, e.g., railway track, enables centralized control of the train operations. The centralized controller, Operational Control Center (OCC), has a global view of the rail line network and controls the train vehicle operations for safety, traffic control, infotainment, and so on. As the control is dynamic, OCC and the train vehicles need to be in constant communication during the trains's operations. Communication-based train communication (CBTC) facilitates such control of train operations as it relies on telecommunication-based signalling.

The trains are mobile by design and adopt wireless communication to synchronize and communicate with the OCC, the stations, and other train vehicles. Therefore, there is an air gap between the mobile trains and the rest of the infrastructure (OCC, trackside equipments, stations, etc.). This gap space is shared by the human customers as they move between the train vehicles and the stations (which are parts of the train infrastructure). For communication across the air-gap, many train systems adopt leaky waveguide technology with the waveguide structure installed parallel to the railway tracks, so that the waveguide is always near the operating trainborne antennas (as the trains's operational scope is restricted along the railway tracks).

We study the security of communications systems for train applications. Public train systems are critical infrastructure. As availability and seamless operation is critical (e.g., even operational delays can cause societal dysfunction and public backlashes) and as CBTC-based train operations rely more heavily on wireless communication, we focus on securing communication availability. Although safety has been well-studied and multiple layers of redundancy is typically implemented to thwart natural accidents and failures, security measures have been lagging since most policy-makers and operators rely on the fact that the system is closed (in access) and the protocols proprietary and confidential. History has shown that such security-by-obscurity approach only provides weak security assurances, prompting many experts to adopt the Kerckhoff's principle (that system protocol and implementations are known to attackers) when they develop measures to secure systems. Previous failures in real-life train signaling operations [1], [2] demonstrate the vulnerability of wireless communication for train systems, and the recent threat demonstrations on car applications [3]–[5] are alarming to train system engineers considering that, unlike train systems, the wireless channels exploited for cars were not even designed to carry mission-critical operations (mission-critical car operation control lies within the car and is based more heavily on sensing than communication).

We investigate the security of the leaky waveguide communications system and make three major contributions. First, we discuss leaky waveguide systems and how it differs from the more traditional free wave model. Second, we construct a model to capture the leaky waveguide system, as the system parameters are sensitive to the system implementation and vary in real-life implementations. Third, we validate the impact of jamming on leaky waveguide (and contrast with the more traditional RF jamming on free air space) in theoretical analyses and simulation.

The rest of the paper is organized as follows. Section II discusses prior work in wireless jamming in open air space while Section III introduces the leaky waveguide communica-

1521-9097/15 $31.00 © 2015 IEEE
DOI 10.1109/ICPADS.2015.13

Fig. 1. Leaky waveguide deployment in railway systems (left) and the corresponding trainborne antenna (right)

tion system and discusses literature that studies it. We construct an implementation-independent model for leaky waveguides in Section IV and establish our threat model in Section IV-C. Afterward, we use the model to analyze the repeater effect and the SINR in Section V and simulate a waveguide implementation in train systems to contrast the impact of waveguide jamming with the open-air jamming in Section VI. Finally, Section VII concludes the paper.

II. Prior Work in Jamming

Before we study the train systems, we review the prior research in wireless jamming which is a threat to communication availability. The jamming threat, which injects noise or interference signals to disrupt the wireless communication, has been well-practiced, e.g., military applications and government censorship, and is well-studied, e.g., [6]–[11]. However, jamming signals are artificially generated at the point of attack and are subject to channel attenuation, limiting their propagation and impact to some distance from that point; as with any wireless signal emission, jamming has a finite transmission range from the signal source in free space. Thus, the prior literature assumes that the victim is within the jammer's physical transmission range and propose solutions based on virtual access and processing, such as spread spectrum [6]–[9], that increases the resistance to the noise and interference, effectively making the scenario a power game between the attacker (effective jamming power) and the legitimate user (effective signal power with processing gain relative to the jamming power). As we will see in the rest of the paper (especially in Section VI), jamming on leaky waveguide breaks this model, effectively extending the jamming transmission range to cover the entire network. To the best of our knowledge, we are the first to present such a wireless jamming threat and to investigate the security of leaky waveguide systems in train applications.

III. The System: Leaky Waveguide with Repeaters

A. Leaky Waveguide and Free Wave

To send signals over the air, the radio frontend takes the digital-domain samples, converts it into electromagnetic (EM) signal waves, and emits them through the antenna(s). To contrast leaky waveguide to the traditional *free wave* technology (where the EM signal is freely travelling over the open air space, e.g., without a waveguide), we highlight two features of free wave model. First, the signal naturally attenuates due to the RF expansion of the wavefront. Second, a radio transmitter sends the EM signal oblivious to its surroundings, making the channel characteristics very sensitive to the physical surroundings and the locations of both the transmitter and the receiver; such sensitivity creates variations known as *fading*.

Leaky waveguide is designed to limit these two aspects of the free wave model. As the name implies, waveguide technology guides the wave by restricting its propagation to one dimension (as opposed to having the wave propagate in three dimensions) to sustain the signal power over a long distance; the waveguide also physically establishes and fixes the path between two communication users to minimize the fading effect and have the propagation behavior become more uniform across the channel, e.g., no moving objects between the users. The wave-guiding structure is typically an air-filled metal structure that extends between the two users. Figure 1 depicts a waveguide deployed for trains and the train-borne radio that communicates with the waveguide.

While the waveguide structure may be sufficient to communicate longitudinally between stations, the train communication needs to extend outside of the waveguide for the train vehicles (which cannot have a probe inside the waveguide as it moves) and the trackside equipments to access the communication. Thus, train systems make the waveguide *leaky* by introducing slot gaps on the guide surfaces, and the travelling wave that used to be restricted within the guide structure without the slot gaps now travels to outside of the guide; each slots acts like a dipole for signal radiation according to the Small-Hole Theory [12], [17]. The wave-guiding structures are built parallel to and near the railway tracks (so that the leaked waves do not need to travel far away from the guide), and the signal-receiving antennas on train experience homogeneous signals as the train moves parallel to the waveguide because of the following two factors when designing slotted waveguides: the inter-slot distance is small relative to the distance between the waveguide and the receiving antenna, creating a dense array of slot sources [12], [13], [16]; and cavity-backed rectangular slots are used for broad radiation pattern and quick attenuation orthogonal to the waveguide-longitudinal axis [18]. Such slotted waveguide design enables a simpler model in Section IV-B in the following ways: it enables the adaptation of the well-studied free-wave model (discussed in Section IV-A) to characterize the propagation of the signal that exits the waveguide; the power loss is largely dominated by the radial distance from the waveguide; and fading from the tunnel and other train environments becomes marginal.

Because of the leaky nature, leaky waveguide communication introduces occasional wireless repeaters when supporting longer distances. To compensate with the loss, the *repeaters* amplify the signal received from one side of the waveguide and re-

Reference	Longitudinal loss (dB/km)	Radial loss	Analyzed Parameters	Testbed country
[12]	17 ± 1	62dB at 30cm	$f,\ f_{co},\ \rho_{wg},\ b,\ a,\ l_x,\ l_y$	France
[13]	14 ± 1	53dB at 25cm	$l_x,\ l_y$	France
[14]	3 ± 1	22-27dB (distance not specified)	$f,\ f_{co}$	Japan
[15]	13.9	63dB at 32cm	$f,\ f_{co},\ \rho_{wg},\ b,\ a$	China
[16]	20	60dB at 20cm	(N.A.)	China

TABLE I
PRIOR STUDY OF LEAKY WAVEGUIDE IN TRAIN APPLICATIONS AND THEIR SYSTEM-BASED MEASUREMENT RESULTS

transmit it to the other side.

B. Leaky Waveguide and Leaky Coaxial Cable

A closely related technology to leaky waveguide is *leaky coaxial cable* or *leaky feeder* where the guiding structure is replaced by coaxial cables; to contrast, the waveguide lacks the cable dielectric material and the inner conductor of coaxial cable and is thus empty inside. Although our model in Section IV-B can be adapted to leaky coaxial cables (as they too use repeaters to deal with the signal loss across the coaxial cables), we focus on leaky waveguide because the following aspects make it more suitable for train applications: first, the metal guide structure for leaky waveguide is more physically robust than coaxial cables and is thus more suitable for static environment of train and railways and makes the maintenance of the system easier (by application design, train systems require industrial-grade equipments and the infrastructure to be physically robust); second, leaky waveguide has less propagation loss in the longitudinal direction than leaky coaxial cables, especially at frequencies above 1GHz (for example, at 2.5GHz, a 42-mm-diameter cable attenuation is about 80 dB/km [12]), making leaky waveguide more suitable for distances in the order of hundreds of meters or kilometers for human transport applications of train, as we will see in greater detail in Section III-C.[1] For signaling and communication redundancy, leaky waveguide, leaky coaxial cable, and free wave antennas are sometimes used in combination.

C. Prior Work in Leaky Waveguide

Leaky waveguide communication in trains are less studied than the traditional wireless communication (that assumes free wave) due to their infrastructure-heavy applications and limited access to the research community (because the implementation is often proprietary and the details confidential to the system builder who is contracted by the government that owns the public train systems). Nevertheless, Table III reviews prior work in leaky waveguide in train applications and lists the system measurement results. The table includes the power loss over distance in the longitudinal (along the wave guide) and radial directions (moving away from the center of the wave guide's cross section) and the parameters that were analyzed to study the wireless propagation characteristics (in addition to the travelled distance); the parameters are the wave's carrier frequency (f), the cutoff frequency (f_{co}) which is a lower bound on the operating frequency for signal propagation and is determined by the cross-sectional dimensions of the waveguide, the resistivity of the wave-guide material (ρ_{wg}), the width and height of the wave-guide structure (b and a respectively), the width and height of the slots (l_x and l_y respectively). We denote the longitudinal loss rate and the radial loss α and $\overline{\text{PL}_r}$, respectively, and revisit them in Section IV and in Section V, respectively. The wave propagation characteristics are sensitive to the implementation details such as the physical nature of the wave-guide structure and the physical properties of the wave signal (e.g., carrier frequency and bandwidth), and the implementation varies from one operator to another depending on the application requirements and design decisions. Therefore, we construct a model that can embrace the dependency on these system design parameters in Section IV-B and study the model.

[1]The leaky coaxial cable finds greater use in applications such as building indoors, airplanes, and mines, and its research focus is more on the propagation characteristics outside of the coaxial cable (as opposed to within and along the wave guide) [19], [20].

IV. OUR SYSTEM MODEL

As in Section III, we limit our discussions to those relevant to our work. Since our contribution lies in studying multiple coexisting users (in order to study interference and jamming impact in leaky waveguides) we focus on the *path loss*, the propagation attenuation while the signal travels from one user (the transmitter) to another (the receiver). We abstract the design parameters in the physical structure of the leaky waveguide (e.g., the dimensions and the material of the metal and the slot length) and the parameters for the communication protocol (e.g., carrier frequency and bandwidth) from our analyses; these parameters, studied in the prior work in Section III-C, are static and fixed after the system implementation.

A. Traditional Free Wave Model

As defined in Section III-A, to contrast with waveguide, we define *free wave* to be the signal wave propagation over the open air space. The basic path loss model has the path loss (PL) inversely proportional to some exponent (γ) of the travelled distance (d), i.e., PL $\propto \frac{1}{d^\gamma}$. The path loss is the ratio between the transmitter power (P) and the received power ($\tilde{P}$), i.e., PL $= \frac{P}{\tilde{P}}$ (path loss is typically greater than one as signal naturally attenuates), and the exponent, γ is called path loss exponent. In decibels (dB), this is rewritten as:

$$\text{PL} = 10\gamma \log_{10}(d) + C \tag{1}$$

where C is a constant, e.g., fixed by the system implementation. From Equation 1, the *log-distance path loss model* abstracts away from the other parameters, such as the frequency and the

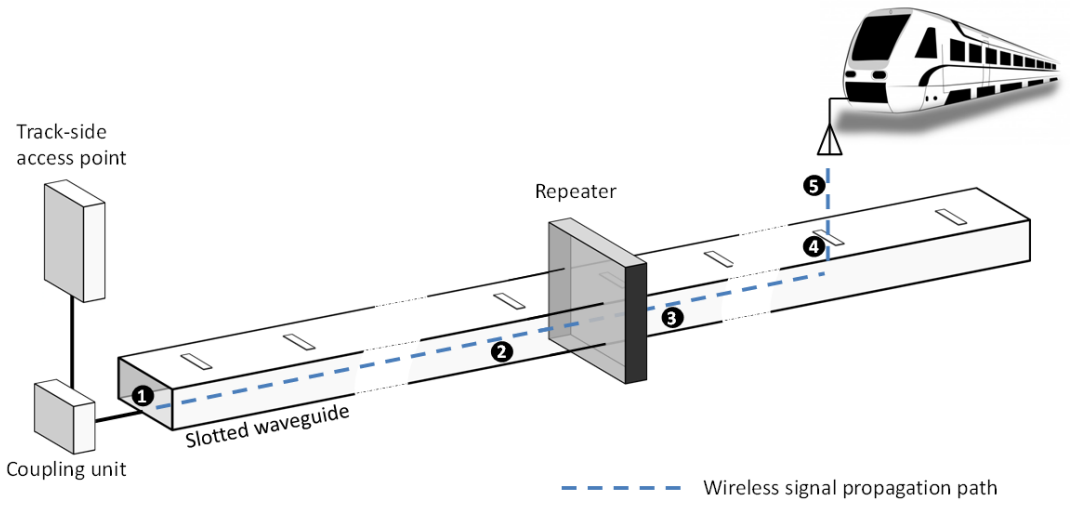

Fig. 2. An illustration of the signal propagation path on a leaky waveguide

antenna size, by introducing a reference path loss (PL_0) and defining the path loss with respect to the reference [21]; it also introduces a random variable (X) to capture the fading effect:

$$\text{PL} = \text{PL}_0 + 10\gamma \log_{10}(d) + X \tag{2}$$

where X is a Gaussian random variable, i.e., $X \sim \mathcal{N}(0, \sigma^2)$. There are other models which capture the fading effect in a system that supports more complicated mobility pattern, e.g., in car-baesd vehicular ad hoc network (VANET) applications [22], [23], but log-distance path loss model works well with the one-dimensionally limited mobility of trains [15].

B. Our Model for Leaky Waveguide with Repeaters

In leaky waveguide system, the signal does not only stay within the waveguide but also leaks outside of the waveguide to reach the train-borne antenna (which is positioned outside of the waveguide). As Figure 2 illustrates, the signal propagation path of leaky waveguide system consists of the followings: (1) on one end, the track-side access point (which is connected via internal wired communication to the rest of the infrastructure, such as the station and the OCC) is connected to the leaky waveguide via a coupling unit; (2) the signal propagates longitudinally along the waveguide; (3) to compensate with the longitudinal loss, wireless repeaters amplify and re-transmit the signal; (4) some signal leaks through the slots by design; and (5) the leaked signal propagates through free wave to reach the train-borne antenna.

Thus, the path consists parts of both inside of the waveguide in the longitudinal direction and outside of the waveguide in the radial direction; the path loss and the distance travelled in the longitudinal direction are denoted as PL_l and d_l, respectively, and those in the radial direction are PL_r and d_r, respectively. The loss by the repeater is denoted as PL_{rptr}. Thus, the path loss of waveguide (PL) is:

$$\text{PL} = \text{PL}_l + \text{PL}_{rptr} + \text{PL}_r \tag{3}$$

By design, the repeater amplifies the signal and thus PL_{rptr} is negative, i.e., $\text{PL}_{rptr} = -C_{rptr}\lfloor \frac{d_l}{d_{rptr}} \rfloor$ where $\lfloor x \rfloor$ is the ceiling of some x (the largest integer not greater than x) and C_{rptr} and d_{rptr} are the system design parameters of the wireless repeater amplifying gain and the distance between consecutive repeaters, respectively; C_{rptr} is the effective gain, i.e., the power ratio between the output of the repeater and the input.

Now we dissect the terms in Equation 3 and investigate PL_l and PL_r. As discussed in Section III-C, the longitudinal loss is the focus of study in the waveguide and is linear in dB [12]–[15]. Thus, $\text{PL}_l = C_{cplng} + \alpha d_l$ where C_{cplng} is the coupling loss and α is the rate of loss over d_l. As for the radial loss with leaking signal, the slot is functionally equivalent to a magnetic dipole [12], [15] and thus it follows the free wave model of Equation 2 after the signal escapes from the waveguide, as discussed in Section III-A. Thus, $\text{PL}_r = \text{PL}_{0,r} + 10\gamma \log_{10}(d_r) + X_r$ where $\text{PL}_{0,r}$ corresponds to that of the leakage through the slot and X_r accounts for the fading of the free wave after the leakage. Then, the path loss (PL) becomes:

$$\begin{aligned} \text{PL} &= \text{PL}_l + \text{PL}_{rptr} + \text{PL}_r \\ &= C_{cplng} + \alpha d_l - C_{rptr}\lfloor \frac{d_l}{d_{rptr}} \rfloor \\ &\quad + \text{PL}_{0,r} + 10\gamma \log_{10}(d_r) + X_r \end{aligned} \tag{4}$$

C. Our Threat Model

We consider a malicious attacker that threatens the availability of train communication system. In specific, the attacker injects jamming signals to disrupt the mission-critical communication for the CBTC train operations. This threat is distinct from accidental interference, which has recently been studied for train systems [24], [25]. As many countries do not assign separate frequency band for train communications, the train system experiences in-band interference and is designed accordingly; the system designers build robustness against natural

interference by implementing virtual protection via filtering and spread spectrum. However, even though such measures are effective against natural interference, it does not defeat sophisticated attacker who a priori knows the protocol measure by Kerchkoff's principle (which is a standard assumption in computer security research), can sense the spectrum for reactive jamming, and can breach the spreading pattern (if proactive spreading/hopping is used); in short, the measure is not designed for security (against a malicious and resource-capable attacker) but for safety. Real-life incidents of disruption due to accidental interference, e.g., [1], show the potential vulnerabilities that modern-day train communications have against a more advanced threat/failure scenario.

The attacker can also beamform its signal for greater impact, whether the beamforming direction is along the railway trajectory toward the travelling train (for free-wave jamming) or pointing downward toward the railway-adjacent waveguide (for waveguide jamming). For example, prior work in CBTC signalling proposes using beamforming radar for better performance in longitudinal loss rate α [26].

Radio-based attacks are feasible in train systems because, unlike other critical infrastructure applications (where the control system access is far away from the general public), the train system shares space with the public, and the consumers are in close proximity to the system communication infrastructure (as they are within the train). This significantly lowers the cost of wireless signal and interference injection, as has happened with a TV remote controller-based frontend [2]. Even though the attacker spatially coexists with the train infrastructure and can affect it remotely using the air medium, it does not need to physically compromise the infrastructure, e.g., by penetrating the waveguide and probing or emitting signals from within it.

V. Analyses

We constructed a path loss model that captures the waveguide propagation, repeaters, and the radial loss from the slots in Section IV-B and contrasted it with free wave model that does not have a waveguide infrastructure, which is discussed in Section IV-A. In this section, we study and use the model to provide insights about leaky waveguide communication system.

A. Repeater Effect

To compensate with the path loss, leaky waveguide incorporates repeaters for long-distance train systems. The repeaters, by design, take the input signal from one side and amplify and re-transmit the signal to the other side. We capture this effect in our model in Section IV-B. In Figure 3, the repeater impact corresponds to a non-increasing step function where the decreasing step sizes are constants of C_{rptr}; as a consequence, the loss in the longitudinal direction ($\text{PL}_l + \text{PL}_{rptr}$) experiences C_{rptr} drop whenever it encounters an amplifying repeater; the horizontal axis is in units of the inter-repeater distance, d_{rptr}. Aside from the waveguide propagation, the use of repeaters is critical in determining the jamming impact, as we will see in Section V-B.

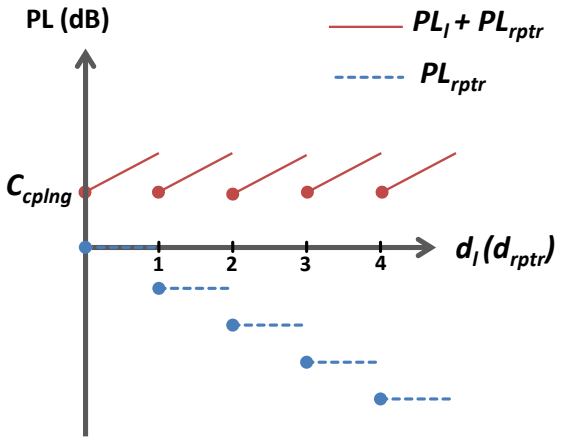

Fig. 3. The repeater effect of the path loss

B. Jamming and SINR

Signal-to-noise ratio (SNR) is a widely used metric to characterize the wireless channel quality and affects the channel capacity, which is an upper bound on the reliable communication rate, e.g., $R < B\log_2(1+\text{SNR})$ by Shannon. Given a communication protocol that fixes the data bit rate (R) and the bandwidth (B), SNR effectively decides whether reliable communication is possible, regardless of how the signal is processed afterward. Thus, the attacker's goal is to lower the SNR by injecting noise-like interference, making the effective SNR to be signal-to-interference-and-noise ratio (SINR). If the attacker reduces the SINR, so that the capacity is lower than the transmission data rate R (i.e., $R > B\log_2(1+\text{SNR})$), then it successfully disrupts the communication. Thus, the attacker goal is to reduce the receiver SINR below a threshold τ' (e.g., $\tau' = 2^{\frac{R}{B}} - 1$):

$$\text{SINR} < \tau' \tag{5}$$

Given that $\tilde{P}'$ is the received power,

$$\text{SINR} = \frac{\tilde{P_S}'}{\tilde{P_I}' + \tilde{P_N}'} < \frac{\tilde{P_S}'}{\tilde{P_I}'} < \tau' \tag{6}$$

The first inequality is a tight bound because it is an interference-limited system due to the jammer, i.e., $\tilde{P_I}' > \tilde{P_N}'$; it also provides a conservative solution for the jammer that makes SINR $< \tau'$ regardless of the noise power. In dB, Equation 6 becomes:

$$\tilde{P_I} - \tilde{P_S} > \tau \tag{7}$$

where $\tau = 10\log_{10}\tau'$, $\tilde{P_I} = 10\log_{10}\tilde{P_I}'$, and $\tilde{P_S} = 10\log_{10}\tilde{P_S}'$. Since $\tilde{P_I} = P_I - \text{PL}_{I,R}$ and $\tilde{P_S} = P_S - \text{PL}_{S,R}$, where $\text{PL}_{I,R}$ is the path loss the jammer's interference experiences at the victim receiver and $\text{PL}_{S,R}$ is the path loss for the signal to the same receiver, Equation 7 becomes the following:

$$P_I - P_S > \text{PL}_{I,R} - \text{PL}_{S,R} + \tau \tag{8}$$

Now, we study $\text{PL}_{I,R}$ and $\text{PL}_{S,R}$ in greater details. We first study the radial component of path loss from the waveguide

to the trainborne antenna, PL_r, which affects both $\text{PL}_{I,R}$ and $\text{PL}_{S,R}$, and establish that it is constant in train implementations.

When using waveguide-based communication in general settings, as can be seen in Equation 4, PL_r depends on the radial direction d_r and the fading X_r, i.e., $\text{PL}_r = \text{PL}_{0,r} + 10\gamma \log_{10}(d_r) + X_r$. However, in train systems where the waveguide and the train motion trajectory are parallel, the distance d_r between the (closest part of) waveguide and the receiver remains constant; also, $\sigma = 0$ and thus $X_r = 0$ as the line-of-sight dominates because of the leaky-slot design as discussed in Section III-A. Thus, PL_r is constant in train implementations, which corroborates prior studies in waveguide (e.g., Table III) which fixes the radial loss between the waveguide and the trainborne radio. Compared to the signal travelling through and inside the waveguide, the signal that takes the free-wave path and travels outside of the waveguide (in which case the channel loss is described in Equation 2) quickly attenuates and becomes marginal as the distance increases[2]; we further analyze this effect in Section VI. If we denote $\overline{\text{PL}_r}$ to capture the independence of PL_r with respect to d_r and X_r and $\text{PL}_{I,\text{wg}}$ to correspond to the loss of the signal path from jammer to the waveguide (i.e., $\text{PL}_{I,\text{wg}} = \text{PL}_{0,r} + 10\gamma \log_{10}(d_{I,\text{wg}}) + X_r$), the path loss between the jammer and the receiver becomes:

$$\begin{aligned} \text{PL}_{I,R} &= \text{PL}_{I,\text{wg}} + \alpha d_{I,R} - C_{rptr} \lfloor \frac{d_{I,R}}{d_{rptr}} \rfloor + \overline{\text{PL}_r} \\ &= \text{PL}_{0,r} + 10\gamma \log_{10}(d_{I,\text{wg}}) + X_r \\ &\quad + \alpha d_{I,R} - C_{rptr} \lfloor \frac{d_{I,R}}{d_{rptr}} \rfloor + \overline{\text{PL}_r} \end{aligned} \tag{9}$$

In contrast to the jammer's interference path (that experiences $\text{PL}_{I,R}$ to enter the waveguide), the legitimate signal gets injected to the waveguide by wired connection and coupling, and thus the path loss becomes:

$$\text{PL}_{S,R} = C_{cplng} + \alpha d_{S,R} - C_{rptr} \lfloor \frac{d_{S,R}}{d_{rptr}} \rfloor + \overline{\text{PL}_r} \tag{10}$$

Using Equation 9 and Equation 10, the jamming power cost for successful attack in Equation 8 becomes:

$$\begin{aligned} P_I - P_S \; > \; & \text{PL}_{0,r} + 10\gamma \log_{10}(d_{I,\text{wg}}) + X_r \\ & + \alpha d_{I,R} - C_{rptr} \lfloor \frac{d_{I,R}}{d_{rptr}} \rfloor + \overline{\text{PL}_r} + \tau \\ & - \{ C_{cplng} + \alpha d_{S,R} - C_{rptr} \lfloor \frac{d_{S,R}}{d_{rptr}} \rfloor + \overline{\text{PL}_r} \} \\ = \; & - C_{cplng} + \text{PL}_{0,r} + X_r + 10\gamma \log_{10}(d_{I,\text{wg}}) + \tau \\ & + \alpha \left(d_{I,R} - d_{S,R} \right) - C_{rptr} \left(\lfloor \frac{d_{I,R}}{d_{rptr}} \rfloor - \lfloor \frac{d_{S,R}}{d_{rptr}} \rfloor \right) \end{aligned} \tag{11}$$

Thus, after the communication system is deployed, the jamming power cost relative to the signal power is dependent on the following parameters: the jammer's distance from the waveguide ($d_{I,\text{wg}}$), the distance between the jammer and the receiver relative to the source-receiver distance ($d_{I,R} - d_{S,R}$) and how many more times the jammer's interference signal encounters the repeater relative that of the source transmission ($\lfloor \frac{d_{I,R}}{d_{rptr}} \rfloor - \lfloor \frac{d_{S,R}}{d_{rptr}} \rfloor$).

[2]The train communication system that emulates physical waveguide in free wave, e.g., via directional antenna/beamforming and radar [26], and uses wireless relays/repeaters in open air is another promising direction for long-distance communication but is beyond the scope of this work.

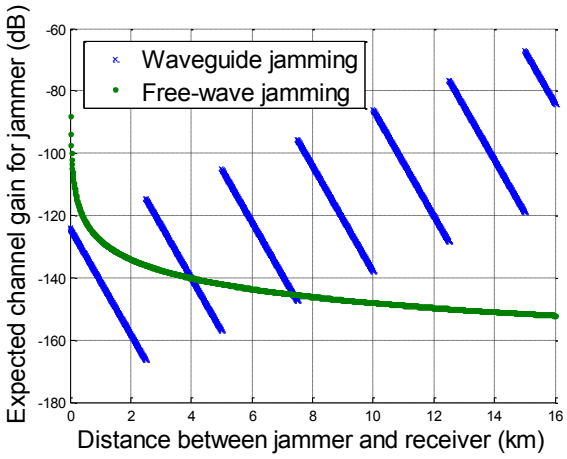

Fig. 4. Jammer's channel gain when jamming the waveguide and jamming on free wave

VI. Simulation

We simulate a train communication system to show the vulnerability of waveguide jamming. We adhere to the Electronic Industries Alliance Waveguide WR 430 (supporting 1.7 - 2.60GHz frequency band) and use the parameters and the measurements from [12], which yields $C_{cplng} = 0.3$dB, $\alpha = 17dB/km$, $\overline{\text{PL}_r} = 62$dB at $f = 2.4$GHz and $d_r = 30cm$[3]; we also use $C_{rptr} = 52$dB, $P_S = 23$dBm, and B =20MHz, which values fall in the range of typical train system design. For the free wave model, we use $\gamma = 2$, which corroborates with He et al. [27] when the free-wave radio transmitter is located at a comparable height to the receiver.

From the aforementioned parameters, we make a design choice of inter-repeater distance (d_{rptr}) for the repeater implementation, given that the receiver supports the SNR-threshold of $\tau = 10$dB and the noise experienced is dominated by the circuit noise (i.e., $\overline{P_N}$=-174+73 = -101dBm because the thermal noise level is -174dBm/Hz and B =20Hz=73dBHz). As discussed in Section V-B, the SNR at the receiver needs to be greater than τ anywhere in operation scope of CBTC (e.g., along the railway) and SNR $> \tau$, $\forall d_{S,R}$ yields:

$$P_S - C_{cplng} - \alpha d_{S,R} + C_{rptr} \lfloor \frac{d_{S,R}}{d_{rptr}} \rfloor - \overline{\text{PL}_r} - \tau - \overline{P_N} > 0, \; \forall d_{S,R} \tag{12}$$

Equation 12 with the aforementioned system parameters yields $-17 d_{S,R} + 52 \lfloor \frac{d_{S,R}}{d_{rptr}} \rfloor + 51.7 > 0$, and solving it results in: $d_{rptr} < 3.04$km, $\forall d_{S,R}$. We fix $d_{rptr} = 2.5$km to accommodate the signal fluctuation due to the wireless

[3]These values are affected by the system deployment and the corresponding parameters. In this case, the parameters (as defined in Section III-C) were: TE01 propagation mode, $f_{co} = 1.37$GHz, the waveguide surface made of aluminum alloy and with a size of 109.2mm×54.6mm (as defined in WR 430 standard), and the slot dimensions of 19mm×3mm.

channel, leaving 9.18dB error margin for the first repeater and 9.5dB margin for the rest of the repeaters (as the SNR reaches the minimum as it encounters the first signal-amplifying repeater). Using greater d_{rptr} (within the constraint of $d_{rptr} < 3.04$km for the first repeater and $d_{rptr} < 3.059$km for the rest of the repeaters) makes the system less tolerant to channel errors and signal fluctuations.

We study the jamming power behavior and contrast the two jamming strategies of using the waveguide and using free wave without the waveguide. Assuming that the jamming source is at the same height as the trainborne-antenna and the same distance from the waveguide, Figure 4 shows the result where the horizontal axis is the jammer-receiver distance ($d_{I,R}$) and the vertical axis is the expected jammer's channel *gain* (which is the inverse of loss). Given the same transmitting power, jamming the waveguide causes greater interference at the receiver than jamming on free wave when $d_{I,R} \in (2.5, 4) \bigcup (5, 7.375) \bigcup (7.5, \infty)$ due to the signal-amplifying repeaters in the waveguide communication infrastructure (which effect is discussed in Section V-A). Also, because the communication system needs to be conservative to tolerate the channel randomness and error, e.g., the repeater using smaller d_{rptr} to ensure that the (decodable) signal does reach the repeater, there is a positive drift in the channel gain, and the expected interference power by the jammer continues getting boosted as it travels in the waveguide. For example, after $d_{I,R} > 12.5$km, the interference power never becomes less than what the receiver would have experienced if it were at $d_{I,R} = 0$ (i.e., the point in the waveguide where jammer signal gets injected). Thus, jamming the waveguide takes advantage of the power-amplifying aspect of waveguide communication infrastructure to expand its impact throughout the CBTC communication scope, regardless of the jamming source's location, and challenges the jamming (transmission) range notion which the traditional free-wave-based jamming widely adopts.

VII. Conclusion

Jamming in open air is well-studied in wireless security. However, repeater-based leaky waveguide system is distinct from open air-based communications and is deployed for infrastructure-interwound train applications. To investigate the jamming vulnerability of leaky waveguide communication system, we study prior work in leaky waveguide and construct an implementation-independent model. Using that model, we show that the jamming impact extends throughout the train communication space, which is in contrast to the traditional model that adopts finite jamming range (due to the natural signal attenuation from the jamming source in the open air).

VIII. Acknowledgements

This work was supported by the National Research Foundation (NRF), Prime Ministers Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-31) and administered by the National Cybersecurity R&D Directorate.

References

[1] H. He, "Passenger wi-fi freezes third shenzhen metro train in a week." South China Morning Post. [Online]. Available: http://www.scmp.com/news/china/article/1078165/passenger-wi-fi-freezes-third-shenzhen-metro-train-week

[2] C. Squatriglia, "Polish teen hacks his citys trams, chaos ensues." Wired. [Online]. Available: http://www.wired.com/2008/01/polish-teen-hac/

[3] A. Greenber, "Hackers remotely kill a jeep on the highwaywith me in it," *Wired*. [Online]. Available: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[4] J. Finkle and B. Woodall, "Researcher says can hack gm's onstar app, open vehicle, start engine," *Reuters*. [Online]. Available: http://www.reuters.com/article/2015/07/30/us-gm-hacking-idUSKCN0Q42FI20150730

[5] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, "Fast and vulnerable: A story of telematic failures," in *9th USENIX Workshop on Offensive Technologies (WOOT 15)*. Washington, D.C.: USENIX Association, Aug. 2015. [Online]. Available: http://blogs.usenix.org/conference/woot15/workshop-program/presentation/foster

[6] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications–a tutorial," *IEEE Transactions on Communications*, pp. 855–884, May 1982.

[7] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread spectrum communications handbook*. McGraw-Hill: New York, Mar. 1994.

[8] S.-Y. Chang, Y.-C. Hu, and N. Laurenti, "Simplemac: A simple wireless mac-layer countermeasure to intelligent and insider jammers," *Networking, IEEE/ACM Transactions on*, vol. PP, no. 99, pp. 1–14, 2015.

[9] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pp. 64–78, May 2008.

[10] S.-Y. Chang, Y.-C. Hu, and Z. Liu, "Securing wireless medium access control against insider denial-of-service attackers," in *Proceedings of the IEEE Conference on Communications and Network Security*, ser. CNS '15. IEEE, 2015.

[11] T. Basar, "The gaussian test channel with an intelligent jammer," *Information Theory, IEEE Transactions on*, vol. 29, no. 1, pp. 152–157, Jan 1983.

[12] M. Heddebaut, "Leaky waveguide for train-to-wayside communication-based train control," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 3, pp. 1068–1076, March 2009.

[13] D. P. D. D. Heddbaut, M. and J. Mainardi, "I.A.G.O.: Command Control Link Using Coded Waveguide," *Journal of Transportation Engineering*, vol. 116, no. 4, pp. 427–435, July 1990.

[14] T. Kawakami, T. Maruhama, T. Takeya, and S. Kohno, "Waveguide communication system for centralized railway traffic control," *IRE Transactions on Vehicular Communications*, vol. 13, no. 1, pp. 1–18, Sep 1959.

[15] H. Wang, F. Yu, L. Zhu, T. Tang, and B. Ning, "Modeling of communication-based train control (cbtc) radio channel with leaky waveguide," *Antennas and Wireless Propagation Letters, IEEE*, vol. 12, pp. 1061–1064, 2013.

[16] L. Zhu, H. Wang, and B. Ning, "An experimental study of rectangular leaky waveguide in cbtc," in *Intelligent Vehicles Symposium, 2009 IEEE*, June 2009, pp. 951–954.

[17] H. A. Bethe, "Theory of diffraction by small holes," *Phys. Rev.*, vol. 66, pp. 163–182, Oct 1944. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRev.66.163

[18] R. Johnson and H. Jasik, "Antenna engineering handbook," *McGraw-Hill*, 1961.

[19] K. Carter, "Predicting propagation loss from leaky coaxial cable terminated with an indoor antenna," W. H. Tranter, T. S. Rappaport, B. D. Woerner, and J. H. Reed, Eds. Norwell, MA, USA: Kluwer Academic Publishers, 1999, pp. 71–82. [Online]. Available: http://dl.acm.org/citation.cfm?id=345514.345533

[20] I. E. Z.-H. J. A. Sesena-Osorio, A. Aragon-Zavala and G. Castanon, "Indoor propagation modeling for radiating cable systems in the frequency range of 900-2500 mhz," 2013, vol. 47, pp. 241–262. [Online]. Available: http://www.jpier.org/pierb/pier.php?paper=12102314

[21] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[22] S. ur Rehman, M. Khan, and T. Zia, "Wireless transmission modeling for vehicular ad-hoc networks," in *Parallel and Distributed Systems (ICPADS), 2014 20th IEEE International Conference on*, Dec 2014, pp. 398–403.

[23] H. Boeglen, B. Hilt, P. Lorenz, J. Ledy, A.-M. Poussard, and R. Vauzelle, "A survey of v2v channel modeling for vanet simulations," in *Wireless On-Demand Network Systems and Services (WONS), 2011 Eighth International Conference on*, Jan 2011, pp. 117–123.

[24] M. Li, H. shen Wang, H. li Zhao, and L. Zhu, "Test and analysis on the interference to the cbtc systems by wi-fi signals," in *International Journal of u- and e- Service, Science and Technology*, vol. 8, 2015, pp. 123–132.

[25] X. Li, Q. Song, H. Tao, X. Liu, S. Zhang, X. Wang, Q. Luo, and X. Peng, "Evaluation on anti-interference to wlan equipments for spatial deployment of cbtc systems in tunnels," in *Communications in China (ICCC), 2014 IEEE/CIC International Conference on*, Oct 2014, pp. 47–52.

[26] M. Lienard, P. Degauque, and P. Laly, "Long-range radar sensor for application in railway tunnels," *Vehicular Technology, IEEE Transactions on*, vol. 53, no. 3, pp. 705–715, May 2004.

[27] R. He, Z. Zhong, B. Ai, and J. Ding, "An empirical path loss model and fading analysis for high-speed railway viaduct scenarios," *Antennas and Wireless Propagation Letters, IEEE*, vol. 10, pp. 808–812, 2011.