**COVERT WIRELESS COMMUNICATION IN IOT NETWORK: FROM AWGN CHANNEL TO THZ BAND**

**Abstract:** Covert communication can prevent an adversary from knowing that a transmission has occurred between two users. In this paper, we consider covert wireless communications in an IoT network with dense deployment, where an IoT device experiences not only the background noise, but also the aggregate interference from other Tx devices. Our results show that, in a dense IoT network with lower frequency AWGN channels, when the distance between Alice and the adversary Willie =), Alice can reliably and covertly transmit O(log2 √ n) bits to Bob in n channel uses. In an IoT network with THz (Terahertz) Band, covert communication is more difficult because Willie can simply place a receiver in the narrow beam between Alice and Bob in order to detect or block their LOS communications. We demonstrated that covert communication is still possible in this occasion by utilizing the reflection or diffuse scattering from a rough surface. From the physical-layer security perspective, covert communication can enhance the security of IoT network from the bottom layer.

.

**Keywords**: Terahertz communications, Covert communications, Physical layer security, Internet of Things;

**Existing System:**

Bash, Goeckel, and Towsley’s work [10] is the first work that puts information theoretic bound on covert wireless communication. A square root law is found over noisy AWGN channels and quantum channels [13]. In a different model, if Alice transmits only once in a long sequence of possible transmission slots and Willie does not know the time of transmission attempts, Alice can reliably transmit O(min{ √ n log(T(n)), n}) bits to Bob with a slotted AWGN channel [14]. To improve the performance of covert communication, Lee et al. [15] found that, Willie has measurement uncertainty about its noise level due to the existence of SNR wall, then they obtained an asymptotic privacy rate which approaches a non-zero constant. Following Lee’s work, He et al. [16] defined new metrics to gauge covertness of communication, and Liu et al. [17] took the interference measurement uncertainty into considerations. In general, the covertness is due to the existence of noise, and Willie cannot accurately distinguish it from user’s signals. Cooperative jamming is regarded as a prevalent physical-layer security approach [18][19] which can increase the measurement uncertainty of the adversary. Sobers et al. utilized cooperative jamming to carry out covert communications. To achieve the transmission of O(n) bits covertly to Bob over n uses of channel, they added a “jammer” to the environment to help Alice for security objectives. Soltani et al. [21] considered a network scenario where multiple “friendly” nodes generate artificial noise to hide the transmission from multiple adversaries. He et al. studied covert communication in wireless networks in which Bob and Willie are subject to uncertain shot noise from interferers.

**Disadvantages:**

1.Low Security

2.Low frequency bands.

**Proposed System:**

In this work, we consider covert communication in a dense IoT network with THz (Terahertz) Band. AWGN channel is the standard model for a free-space RF channel, although the noise is unpredictable to some extent, the aggregate interference in a noisy IoT network is more difficult to be predicted. In a dense IoT network with lower frequency AWGN channels, we found that covert communication is still possible. Alice can reliably and covertly transmit O(log2 √ n) bits in n channel uses when the distance between Alice and Willie =).(α is path loss exponent). Increasing demand for larger bandwidths for IoT network has turned the interest from lower frequency UHF (0.3-3GHz) towards higher frequencies, mmWaves (30-300GHz) and THz Band (0.1-10THz). THz Band signals are often assumed to be more secure than lower frequency signals due to the more directional transmission and the more narrow beams. However this makes covert communication more difficult. In THz Band, Willie can simply place a receiver in the LOS (Line-of-Sight) path between Tx and Rx to find or block their communications. Hence Alice and Bob need resorting to the aggregate interference and the NLOS (Non-Line-ofSight) communication to improve the security and hiding. In a THz Band IoT network, although the LOS communications can be detected easily by Willie, we found that the communication based on reflection or diffuse scattering is a feasible information hiding method. As depicted in Fig., the communication via specular reflection A-O1-B or diffuse scattering A-O2-B can evade the detection. The scattering signals Willie eavesdropping are masked by the background noise and the aggregate interference in a dense IoT network.

To bypass the detection of Willie, Alice and Bob should resort to the reflection or diffuse scattering NLOS transmission link, • Specular Reflection: At first, Alice and Bob try to find a surface in the surroundings that the THz beam from Alice can be specularly reflected to the antenna of Bob, i.e., the specular reflection path AO1 and O1B in Fig., and SINR at Bob is above a predefined threshold. Diffuse Scattering: If a specular reflection path does not exist, Alice and Bob find a diffuse scattering path so that Bob’s received signal strength is above a threshold, such as the scattering path AO2 and O2B in Fig.

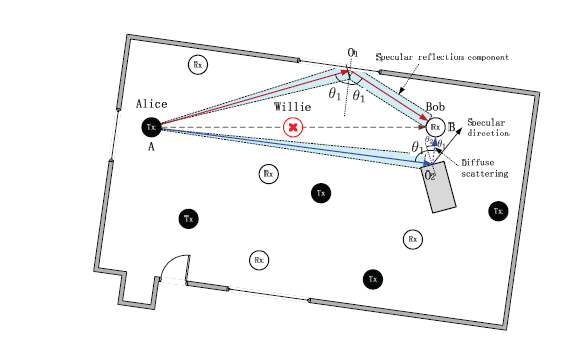


Fig. Covert communication in a THz Band IoT network.

**Advantages:**

* Increase signal covertness.
* High frequency bands.

**Applications:**

* Military Applications
* E-mail,
* Virtual private networks (VPNs),
* Internet browsers (Secure Sockets Layer and Transport Layer Security Protocols)

**Software & Hardware Requirements:**

**Software:** Matlab 2018a

**Hardware:**

**Operating Systems:**

• Windows 10

• Windows 7 Service Pack 1

• Windows Server 2019

• Windows Server 2016

**Processors:**

Minimum: Any Intel or AMD x86-64 processor

Recommended: Any Intel or AMD x86-64 processor with four logical cores and AVX2 instruction set support

**Disk:**

Minimum: 2.9 GB of HDD space for MATLAB only, 5-8 GB for a typical installation

Recommended: An SSD is recommended a full installation of all MathWorks products may take up to 29 GB of disk space

**RAM:**

Minimum: 4 GB

Recommended: 8 GB