**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.

Index Terms—Terahertz communications, Covert communications, Physical layer security.,Internet of Things;

**CHAPTER 1**

**INTRODUCTION**

Wireless communications have already penetrated into all corners of our society, with the increasing tides of 5G/B5G, internet of things, ubiquitous access, and cloud computing . Accordingly, the covertness of today’s wireless communications attracts unprecedented interest, when facing great risks to individual privacy and government and military security. As such, the covert wireless communication to achieve a reliable information transmission from transmitter to receiver with low probability of interception has been the focus of academic, industrial, and military communities. Traditionally, besides the encryption methods for content protection, the communication covertness can be enhanced through the electromagnetic signal protection in the physical layer . Hiding the transmitting signal deeply under the noise or interference background is one of the prevailing methods to reinforce the physical layer security .Furthermore, if the interceptor cannot detect the underlying signal transmission between the transmitter and the receiver, there is no opportunity to launch an “eavesdropping and decoding” attack, even with unlimited computing resource or decryption codes .In general, the deeper the transmitting signal is hid under the noise background with a worse signal-to-noise ratio (SNR), the lower the interception probability for the adversary. This ensures a higher transmission covertness between transmitter and receiver.

An emerging technology and, really, a revolution, the Internet of Things (IoT) has brought tremendous changes to end users in their daily lives. For individuals, their living, studying, and working are all involved in the IoT network, taking advantage of smart environments (home and city), eHealth, and transportation systems. For businesses or institutions, innovations like advanced automation and industrial manufacturing, knowledge sharing and data management, and smart and self-modifying mechanisms and systems are becoming more and more popular. INTERNET of Things (IoT) is fast, and can be found in a broad range of applications ranging from consumers (e.g., smart homes) to organizations (e.g., Industry 4.0) to governments (e.g., Internet of Battlefield/Military Things)– collectively, this can be referred to as Internet of Everything (IoE) . Due to the rapid development in telecommunication systems, IoT can collaborate with Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), things, and networks in any form, at any time, and anywhere. Cyber security is the inevitable problem that must be solved in the development of IoT. If the issue is not well managed, hackers will take advantage of the defects and weaknesses of devices or objects and then will distort data or disrupt systems through the global IoT network. IoT attacks and failures may outweigh any of its benefits. In addition, traditional security protocols and mechanisms are not suitable because existing devices are limited in their low levels of scalability, integrity, and interoperability. Therefore, new methodologies and technologies should be developed to meet the security, privacy, and reliability requirements of IoT.

IoT involves so many different things, especially heterogeneous devices. By 2015, IoT connected 4.9 billion things and will connect 25 billion things by 2020 . IoT has great flexibility and scalability, but this huge number also may predict a security disaster. The more devices a person connects, the greater the risk to the individual and to the network, and the higher the cyber security risk to the global infrastructure. In 2003, each person had only fewer than 0.08 devices. In 2010, the number increased to 1.84. By 2020, there will be 6.58 devices per person. Devices of all types are developing widely and rapidly across the global IoT network, but these devices are easily attacked and are considered as vulnerable points in the IoT network. Thus, the IoT cyber security infrastructure ensures that devices are maintained in a secure environment and that users can use them appropriately. The scale of IoT smart devices is very broad, and includes computers, smart phones, communication interfaces, operating systems, lightweight services, and preloaded applications. Equipped with RFID sensors or actuators, intelligent devices can execute accordingly, make decisions autonomously, and disseminate information to users safely. With the advancement of internet and wireless communication, smart devices and things, and IP protocol and sensor network technologies, more and more network-based objects have been involved in IoT cyber security. These advanced technologies also are having a huge impact on new ICT and on Industry 4.0 . Cyber security is spread across the IoT network, a global infrastructure of heterogeneous smart devices that integrate sensory, communications, networking, and information processing technologies. In addition, many other technologies and devices, such as barcodes, smart phones, social networks, and cloud computing, that are used in IoT influence cyber security, to some extent. The cyber security of IoT is often cited by countries and institutions to implement standards and laws in order to achieve a high degree of cyber security. The United States, China, and the United Kingdom are the three largest countries affected by IoT cyber security threats, especially by smart home attacks [10]. In the U.S., the Cyber security for the Internet of Things (IoT) program has been implemented to control and to improve the cyber security of smart devices and the entire environments by standards and guidelines [11]. China Cyber security Law (CSL) was initiated on June 1, 2017. The Cyberspace Administration of China (CAC) is the primary governmental authority to supervise and enforce the CSL. The CSL regulates cyber security from different aspects, including network operation security and network information security, as well as managing monitoring, early warning, and emergency responses within mainland China. Europe has made progress in various sectors, such as energy, vehicles, and residential, in cyber security.

First, IoT is the extension of the net or Internet, meaning that, in IoT, various networks should coexist, and the interoperability among these networks is critical for information delivery and supporting applications .Interconnection is a critical architecture issue in IoT . Second, things connected in IoT are no longer limited to devices or objects, but can also be information, human behaviors, etc. , Thus, IoT should include mechanisms that handle the connection of objects in a broader manner. There have been a number of research efforts devoted to developing IoT prototypical systems .Nonetheless, most of the systems that focus on specific applications are implemented within extranet or intranet, and have no interaction with each other. Based on the features of IoT that interconnection is a critical architecture issue, strictly speaking, these systems or applications are not ‘Internet of Things’, but the ‘Net of Things’, or can even be considered as ‘Net of Devices’, and the interactions between these extranets and intranets were missed .Thus, IoT should cover all things in large scale networks, in which various networks should coexist, and are able to interact with each other via various gateways and middle wares, supported by the complex control plane . One vision is that a generalized network infrastructure that integrates various networks should be designed, and all IoT based systems or applications can provide their services by efficiently sharing network resources and information across the generalized network infrastructure. For example, in smart cities [156], [14], if a generalized network infrastructure can be implemented and is able to cover all regions in a city, applications (smart grid, smart transportation, smart healthcare, etc.) can share their individual network infrastructures to enable data collection and information delivery. In this vision, everything that is inter-connected in the network can be realized because all applications can interact with each other easily and share the resources effectively. The implementation of generalized network infrastructure can reduce the cost of network deployment as well. In the next future, the Internet of Things (IoT) paradigm will involve billion of smart-devices with processing, sensing and actuating capabilities able to be connected to the Internet. Integrating social networking concepts into the IoT has led to the Social IoT (SIoT) concept which enables people and connected devices to interact, facilitating information sharing . However, interoperability , security, and privacy issues are a great challenge for IoT but they are also enabling factors to create a “trust and interoperable ecosystem.” In fact, not solving these issues, the SIoT paradigm will not reach enough popularity and all its potential can be lost. Security issue is emphasized by the lack of standards specifically designed for devices with limited resources and heterogeneous technologies. In addition, these devices, due to many vulnerabilities, represent a “fertile ground” for existing cyber threats. As the demand for smaller devices that can offer higher speed wireless communication any time and anywhere is growing relentlessly, the need for higher frequency bands with wide unregulated bandwidth that can support multi-Gigabits/s data rates have become essential. The opening up of carrier frequencies in the THz-range, such as D-band (i.e., 110 GHz–170 GHz) and around 300 GHz, is the most promising approach to provide sufficient bandwidth required for ultra-fast and ultra-broadband data transmission. This large bandwidth paired with higher speed wireless links can open the door to a large number of novel applications such as ultra-high-speed pico-cell cellular links, Terabits/s (Tbps) WLAN and WPAN, secure wireless communication for military and defense applications, and on-body communication for health monitoring systems.

**CHAPTER 2**

**LITERATURE REVIEW**

**[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao:** Fog/edge computing has been proposed to be integrated with Internet-of-Things (IoT) to enable computing services devices deployed at network edge, aiming to improve the user’s experience and resilience of the services in case of failures. With the advantage of distributed architecture and close to endusers, fog/edge computing can provide faster response and greater quality of service for IoT applications. Thus, fog/edge computing based IoT becomes future infrastructure on IoT development. To develop fog/edge computing-based IoT infrastructure, the architecture, enabling techniques, and issues related to IoT should be investigated first, and then the integration of fog/edge computing and IoT should be explored. To this end, this paper conducts a comprehensive overview of IoT with respect to system architecture, enabling technologies, security and privacy issues, and present the integration of fog/edge computing and IoT, and applications. Particularly, this paper first explores the relationship between Cyber-Physical Systems (CPS) and IoT, both of which play important roles in realizing an intelligent cyber physical world. Then, existing architectures, enabling technologies, and security and privacy issues in IoT are presented to enhance the understanding of the state of the art IoT development. To investigate the fog/edge computing-based IoT, this paper also investigate the relationship between IoT and fog/edge computing, and discuss issues in fog/edge computing-based IoT. Finally, several applications, including the smart grid, smart transportation, and smart cities, are presented to demonstrate how fog/edge computing-based IoT to be implemented in rea lworld applications.

**Summary:** In this paper, a comprehensive review of IoT has been presented, including architectures, enabling technologies, and security and privacy issues, as well as the integration of fog/edge computing and IoT to support diverse applications. Particularly, the relationship and difference between IoT and CPS has been clarified at the outset. Possible architectures for IoT have been discussed, including the traditional three-layer architecture and the SoA-based four-layer architecture.

**[2] M. Frustaci, P. Pace, G. Aloi, and G. Fortino**,**:** Social Internet of Things (SIoT) is a new paradigm where Internet of Things (IoT) merges with social networks, allowing people and devices to interact, and facilitating information sharing. However, security and privacy issues are a great challenge for IoT but they are also enabling factors to create a “trust ecosystem.” In fact, the intrinsic vulnerabilities of IoT devices, with limited resources and heterogeneous technologies, together with the lack of specifically designed IoT standards, represent a fertile ground for the expansion of specific cyber threats. In this paper, we try to bring order on the IoT security panorama providing a taxonomic analysis from the perspective of the three main key layers of the IoT system model: 1) perception; 2) transportation; and 3) application levels. As a result of the analysis, we will highlight the most critical issues with the aimof guiding future research directions.

**Summary:** Here, it is shown that that IoT system model has many security issues among which threats that can exploit some possible weaknesses. For these reasons, it is necessary to appropriately enforce trust management and security in the IoT world starting from the characterization of the different threats related to each specific level of the general IoT system model.

**[3] Y. Lu and L. D. Xu:** As an emerging technology, the Internet of Things (IoT) revolutionized the global network comprising of people, smart devices, intelligent objects, information, and data. The development of IoT is still in its infancy and many directly related issues need to be solved. IoT is a unified concept of embedding everything. IoT has a great chance to make the world a higher level of accessibility, integrity, availability, scalability, confidentiality, and interoperability. But, how to protect IoT is a challenging task. System security is the foundation for the development of IoT. This article systematically reviews IoT cyber security. The key factors of the paradigm are the protection and integration of heterogeneous smart devices and information communication technologies (ICT). Our review applies to people interested in cyber security of IoT, such as the current research of IoT cyber security, IoT cyber security architecture and taxonomy, key enabling countermeasures and strategies, major applications in industries, research trends and challenges

**Summary:** we have vigorously surveyed the important aspects of IoT cyber security, specifically, the state-of-the-art of the current position and potential future directions, the major

Counter measures against IoT attacks, and the applications in industries. In addition, we introduced and discussed a possible four-layered IoT cyber security infrastructure and a taxonomy of attacks on IoT cyber security.

**[4] Y. Miao, X. Liu, K. R. Choo, R. H. Deng, H. Wu, and H. Li:** Cloud-assisted Internet of Things (IoT) is increasingly prevalent in our society, for example in home and office environment; hence, it is also known as Cloud-assisted Internet of Everything (IoE). While in such a setup, data can be easily shared and disseminated (e.g., between a device such as Amazon Echo and the cloud such as Amazon AWS), there are potential security considerations that need to be addressed. Thus, a number of security solutions have been proposed. For example, Searchable Encryption (SE) has been extensively studied due to its capability to facilitate searching of encrypted data. However, threat models in most existing SE solutions rarely consider the malicious data owner and semi-trusted cloud server at the same time, particularly in dynamic applications. In a real-world deployment, disputes between above two parties may arise as either party will accuse the other of some misbehavior. Furthermore, efficient fullupdate operations (e.g., data modification, data insertion, data deletion) are not typically supported in the cloud-assisted IoE deployment. Therefore, in this paper, we present a Fair and Dynamic Data Sharing Framework (FairDynDSF) in the multi owner setting. Using FairDynDSF, one can check the correctness of search results, achieve fair arbitration, multi-keyword search, and dynamic update. We also prove that FairDynDSF is secure against inside keyword guessing attack and demonstrate its efficiency by evaluating its performance using various datasets.

**Summary:** In thispaper, we proposed an efficient and practical FairDynDSF, which supports result verification, dispute arbitration, dynamic update, decryption authorization and expressive keyword search simultaneously. In addition, FairDynDSF is also designed to be resilient to data corruption attacks and sufficiently lightweight for deployment on resource-constrained IoT devices. The formal security analysis showed that FairDynDSF is secure against inside KGAs, and the empirical examination using various datasets demonstrated that FairDynDSF is practical and scalable in practice.

**[5] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha:** Covert communication, also known as low probability of detection (LPD) communication, prevents the adversary from knowing that a communication is taking place. Recent work has demonstrated that, in a three-party scenario with a transmitter (Alice), intended recipient (Bob), and adversary (Warden Willie), the maximum number of bits that can be transmitted reliably from Alice to Bob without detection by Willie, when additive white Gaussian noise (AWGN) channels exist between all parties, is on the order of the square root of the number of channel uses. In this paper, we begin consideration of network scenarios by studying the case where there are additional “friendly” nodes present in the environment that can produce artificial noise to aid in hiding the communication. We establish achievability results by considering constructions where the system node closest to the warden produces artificial noise and demonstrate a significant improvement in the throughput achieved covertly, without requiring close coordination between Alice and the noise-generating node. Conversely, under mild restrictions on the communication strategy, we demonstrate no higher covert throughput is possible. Extensions to the consideration of the achievable covert throughput when multiple wardens randomly located in the environment collaborate to attempt detection of the transmitter are also considered.

**Summary**: In this paper, first step in establishing low probability of detection (LPD) communications in a network scenario. We established that Alice can transmit O(mγ/2√ n) bits reliably to the desired recipient Bob in n channel uses without detection by an adversary Willie if randomly distributed system nodes of density m are available to aid in jamming Willie; conversely, no higher covert rate is possible.

.

**CHAPTER 3**

**EXISTING METHOD**

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 etal. [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. [20] 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. [22] 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 are used

**CHAPTER 4**

**PROPOSED METHOD**

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.

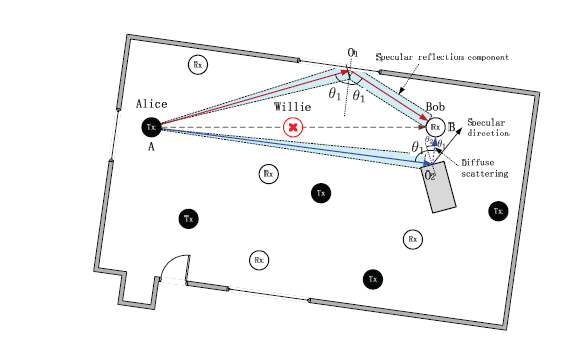
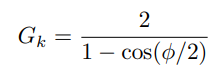


Fig. Covert communication in a THz Band IoT network.

Next we briefly look into the THz Band model, network and blocking model, and rough surface scattering theory. 1) Channel Model :Suppose each device in THz Band is equipped with a directional antenna, and the antenna radiation pattern is the cone model, i.e., a single cone-shaped beam, whose width determines the antenna directivity. The antenna gain Gk for the main lobe of device k is given by



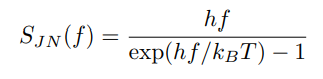
where ϕ is the directivity angle of antenna. When Alice transmits a message, the power of received signal at Bob is given by



where PT x is the transmit power of Tx, GT x and G Rx are the antenna gain of Tx and Rx, c is the speed of EM wave, and f is the operating frequency,



In addition to path loss, any receiver will suffer from Johnson-Nyquist noise generated by thermal agitation of electrons in conductors, which can be represented



where h is Planck’s constant, kB is Boltzmann constant, and T is the temperature in Kelvin.

Network and Blocking Model: In a dense THz Band IoT network, transmitters form a stationary PPP Π = {Xi} with the density λ, receivers experience not only the noise, but also the aggregate interference from other transmitters. However, due to the directionality of antenna in THz Band, users themselves may act as blockers to interference. We use the blocking model proposed in [23] to analyze the aggregate interference. For any interferer located at a distance x from the receiver Bob, the blocking probability of the interference from this interferer can be estimated as follows



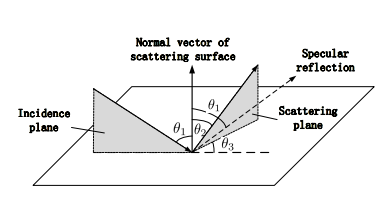
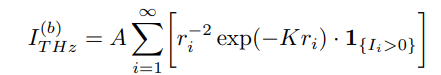


Fig. The model of scattering at a rough surface

where rB is the blocker radius. Besides, if Bob is not in the coverage of an interferer J, then J does not contribute to the aggregate interference at Bob. Given the antenna directivity angle ϕ, the probability that Bob is located in coverage of an interferer is



then the aggregate interference at Bob is



where ri is the distance between i-th interferer and Bob. 1{Ii>0} is an indicator function, 1{Ii>0} = 0 if the signal from this interferer is blocked, or Bob’s antenna directivity is not in coverage of this interferer, 1{Ii>0} = 1 if Bob is interfered by i-th interferer, P{1{Ii>0} = 1} = PC (1 − PB).

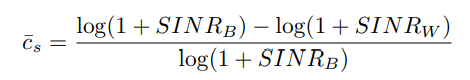
Rough Surface Scattering Model: The general surface scattering model is shown in Fig. 3. A wave, which is incident on a rough surface under an angle θ1, is scattered into the direction given by the angles θ2 and θ3. Kirchhoff scattering model [24] gives the expression of the scattering path gain, G(f, σh, lc, θ1, θ2, θ3), describing the scattered with respect to the incident power. In the expression of Kirchhoff approximation, parameters lc (the surface correlation length) and σh (the standard deviation of surface height variation) describe the surface properties. Fig. shows the path gain at f = 500GHz as a function of angles θ1 and θ2 with θ3 = 0.

Specular reflection, or regular reflection, is the mirror-like reflection of waves, such as light, from a surface

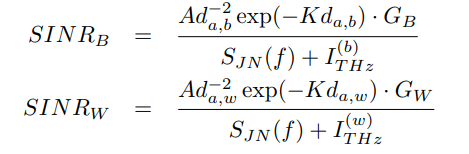
Diffuse scattering refers to signals that are scattered in many directions, including the usual specular direction. These signals are generated because of gaps and sharp changes in the walls of a building that destroy its flat layer (e.g., windows, balconies, brick or stone decorations, beams). Last but not least, the type of material matters, creating an effective roughness parameter [4] for each wall that can be used with ray-based propagation tools.

Kirchhoff model is yet another model used for the general scattering geometry in which a wave is incident on a rough surface under angle θ with the normal to that surface, and is scattered to a direction given by elevation and azimuth angles. According to, this model provides good results if the surface does not contain sharp edges, spikes or other sharp irregularities, which is totally impossible to eliminate in many real use-case scenarios.

Assessment Metric: To quantify the detection ability of Willie, we assess a normalized secrecy capacity [25], which relates the strength of Willie’s signal to Bob’s signal as follows:



where SINRB and SINRW represent Bob and Willie’s signal to interference plus noise ratio on linear scale, respectively. Given the reflecting path gain of Bob GB and scattering path gain of Willie GW , SINRB and SINRW can be estimated as follows:

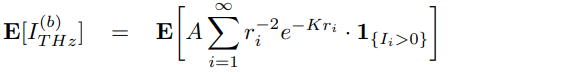


The quantity c¯s is a metric which can be used to assess the likelihood of a successful covert communication. If c¯s is above a predefined threshold, we presume that covert communication is feasible. On the other hand, SINRW can also be used to quantify the Willie’s detection ability. If SINRW << 0 dB, the signal Willie eavesdropped will be overwhelmed by the noise and the aggregate interference.

In THz Band IoT network ,Willie is located in the path of LOS link between Alice and Bob, and tries to detect the possible transmission between them. 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 A-O-1 and O-1-B, 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 A-O-2 and O-2-B

In this subsection we use the normalized secrecy capacity c¯s to assess the likelihood of covert communication. To estimate c¯s, we need to calculate I (b) THz, I (w) THz and SINRB, SINRW

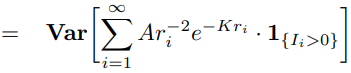
Next, we estimate the mean of the aggregate interference I (b) THz Bob observed (in below Eqn) as follows,

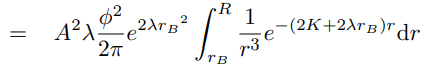


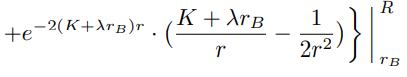
 

where Ei(·) is the exponential integral function, R is the radius of the zone that the signal that comes from Tx farther than R is considered as the background noise. Eq. (a) follows directly after Campbell’s theorem [26] for the mean of a sum function of a stationary PPP Π = {Xi}.

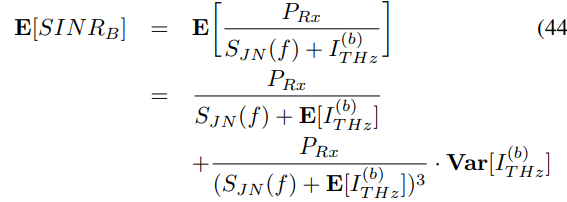
Similarly, the variance of the aggregate interference I (b) THz can be obtained as follows,



here Eq. (a) also follows directly after Campbell’s theorem for the variance of a sum function of a stationary PPP Π = {Xi}. Next we estimate the mean of SINRB by Taylor expansion technique [23] as follows,



here PRx is the received signal strength of Bob, , GB is the reflecting path gain of Bob, which is obtained from Kirchhoff scattering model and SJN (f) is Johnson-Nyquist noise, Similarly, we can get the approximation of the mean of SINRW in the same way.

Now we assess the effects of the operating frequency, network density, the surface roughnesses, and the scattering angle on the normalized secrecy capacity c¯s. Throughout this subsection, we assume that interference coming from the nodes R = 10m away is zero, the coefficient H introduced in Eq. (10) is set to 1. The blocker radius of every node rB = 0.1m, the distance between Alice and Bob da,b = 5m, the absorption coefficient is assumed to be a constant K = 0.01. All devices in the IoT network are equipped with directional antennas (Tx and Rx) with directivity angle ϕ = π/18. Also, the illuminated area of the reflection surface is approximately 4cm2 , the surface correlation length lc = 1.8mm.

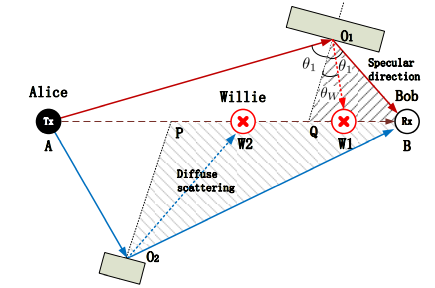


Fig: The selection of reflection points. O1 and O2 are two reflection points, O1B and O2B are their specular reflection directions, O1Q and O2P are the normal vectors of two scattering surfaces, respectively.

THz signal path loss is the major constraints for the realization of the terahertz wireless communications [9]. However, as the distance increases, the pathloss for the terahertz link increases at a faster rate than for the mmWave one, Materials characterization in terahertz frequency band is becoming progressively more important due to a vast variety of applications [12]. Due to absorption attenuation of oxygen molecules and water vapors in the air, THz signal experience harsh path losses that restrict the wireless communication to few meters. Wireless communication in THz band has very high molecular absorptions as well as molecular noise generated by water vapors in response to attenuation of electromagnetic radiation. Besides molecular absorption THz signals may suffer reflection and scattering losses in multipath propagation.

The molecular absorption loss is a function of the carrier frequency and the communication distance and is mainly due to water vapor molecules [11], [16], [17]. The high attenuation absorption peaks due to excited molecule vibrations at specific THz resonant frequencies result in multiple transmission windows [54], each having a bandwidth that shrinks with communication distance. Moreover, higher gas mixing ratios and densities result in stronger and wider spectral peaks. Molecular absorption thus results in frequencyselectivity even in LoS scenarios.

Other parameters such as the line intensity for the reference temperature, 𝑆 (𝑖,𝑔) 0 , the air- and self-broadened half-widths, 𝛼 (air) 0 and 𝛼 (𝑖,𝑔) 0 , and the temperature broadening coefficient, 𝜄, are directly retrieved from the high-resolution transmission molecular absorption (HITRAN) database .The distance-dependent path loss is illustrated in Fig. 8, in which we plot the total path loss, i.e., the spreading and the molecular losses, as a function of frequency–increasing the communication distance results in more severe losses.

**CHAPTER 5**

**ADVANTAGES AND APPLICATIONS**

**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)

**CHAPTER 6**

**7.1 INTRODUCTION TO MATLAB**

**What Is MATLAB?**

MATLAB is an elite dialect for specialized registering. It incorporates calculation, representation, and programming in an easy to-utilize condition wherein issues and preparations are communicated in herbal numerical documentation. Run of the mill utilizes comprise

• Math and calculation

• Algorithm advancement

• Data obtaining

• Modeling, re-enactment, and prototyping

• Data examination, investigation, and representation

• Scientific and designing illustrations

• Application advancement, including graphical UI building

MATLAB is an intuitive framework whose important statistics aspect is an show off that does not require dimensioning. This allows you to tackle several specialized processing issues, particularly those with framework and vector info, in a small quantity of the time it'd take to compose a program in a scalar non intuitive dialect, as an instance, C or FORTRAN.

The call MATLAB stays for grid studies facility. MATLAB changed into first of all composed to present easy access to framework programming created by way of the LINPACK and EISPACK ventures. Today, MATLAB motors fuse the LAPACK and BLAS libraries, inserting the cutting side in programming for network calculation.

MATLAB has advanced over a time of years with contribution from several customers. In university situations, it's far the usual academic apparatus for early on and propelled guides in mathematics, designing, and science. In enterprise, MATLAB is the tool of choice for excessive-profitability studies, advancement, and exam.

MATLAB highlights a collection of more utility-specific arrangements known as tool booths. Important to most clients of MATLAB, device kits permit you to learnandapply particular innovation. Tool compartments are exhaustive accumulations of MATLAB capacities (M-records) that reach out the MATLAB condition to take care of precise training of problems. Territories in which tool stash are reachable include flag coping with, manipulate frameworks, neural structures, fluffy reason, wavelets, pastime, and severa others.

**The MATLAB System:**

The MATLAB system consists of five main parts.

**Development Environment:**

 This is the set of tools and centres that help you operate MATLAB features and files. Many of that gear are graphical person interfaces. It includes the MATLAB desktop and Command Window, a command history, an editor and debugger, and browsers for viewing assist, the workspace, files, and the hunt direction.

**The MATLAB Mathematical Function:**

This is a great collection of computational algorithms ranging from standard capabilities like sum, sine, cosine, and complex arithmetic, to extra sophisticated features like matrix inverse, matrix eigen values, Bessel functions, and speedy Fourier transforms.

**The MATLAB Language:**

This is a high-level matrix/array language with control flow statements, functions, data structures, input/output, and object-oriented programming features. It allows both "programming in the small" to rapidly create quick and dirty throw-away programs, and "programming in the large" to create complete large and complex application programs.

**Graphics:**

MATLAB has considerable centres for displaying vectors and matrices as graphs, as well as annotating and printing those graphs. It consists of high-stage functions for 2-dimensional and 3-dimensional records visualization, photograph processing, animation, and presentation graphics. It also consists of low-stage capabilities that will let you absolutely customise the appearance of graphics as well as to construct complete graphical person interfaces for your MATLAB programs.

**The MATLAB Application Program Interface (API):**

This is a library that allows you to put in writing C and Fortran applications that have interaction with MATLAB. It consists of facilities for calling workouts from MATLAB (dynamic linking), calling MATLAB as a computational engine, and for studying and writing MAT-documents.

**7.2 MATLAB WORKING ENVIRONMENT:**

## MATLAB DESKTOP:

Matlab Desktop is the principle Matlab application window. The desktop consists of five sub windows, the summon window, the workspace program, the existing catalog window, the order records window, and at the least one figure home windows, which can be proven simply while the consumer suggests a sensible.

The order window is the area the customer sorts MATLAB orders and expressions at the initiate (>>) and wherein the yield of these fees is shown. MATLAB characterizes the workspace because the association of factors that the customer makes in a work session. The workspace software demonstrates these elements and some statistics approximately them. Double tapping on a variable within the workspace application dispatches the Array Editor, which may be applied to get data and salary instances modify sure homes of the variable.

The present Directory tab over the workspace tab demonstrates the substance of the existing registry, whose way is seemed within the present index window. 1For case, within the windows running framework the manner may be as consistent with the subsequent: C:MATLABWork, demonstrating that registry "paintings" is a subdirectory of the primary catalog "MATLAB", which is delivered in pressure C. Tapping on the bolt inside the present index window demonstrates a rundown of as of past due utilized approaches. Tapping at the seize to one aspect of the window enables the client to exchange the existing catalog.

MATLAB utilizes an inquiry way to discover M-data and different MATLAB related documents, which might be sort out in catalogs within the PC file framework. Any file keep strolling in MATLAB must dwell inside the ebb and go with the flow registry or in an index that is on are trying to find manner. Of direction, the statistics supplied with MATLAB and math works device kits are included into the inquiry way. The least stressful method to look which indexes are at the inquiry manner. The handiest method to peer which catalogs are soon the quest way, or to encompass or regulate an inquiry manner, is to pick set manner from the File menu the computer, and after that utilization the set way exchange container. It is exquisite exercise to add any typically utilized catalogs to the pursuit way to hold a strategic distance from again and again having the exchange the existing index.

The Command History Window contains a record of the orders a client has entered in the charge window, including both present and past MATLAB sessions. Already entered MATLAB orders can be chosen and re-executed from the charge history window by right

tapping on a summon or arrangement of orders. This activity dispatches a menu from which to choose different choices notwithstanding executing the orders. This is helpful to choose different choices notwithstanding executing the summons. This is a valuable component while trying different things with different orders in a work session

**Using the MATLAB Editor to create M-Files:**

The MATLAB manager is both a word processor unique for making M-statistics and a graphical MATLAB debugger. The proofreader can display up in a window without everybody else, or it could be a sub window in the laptop. M-facts are intended by means of the expansion .M, as in pixelup.M. The MATLAB editorial manager window has various draw down menus for errands, for instance, sparing, seeing, and troubleshooting documents. Since it plays out a few basic checks and furthermore utilizes shading to separate between exclusive additives of code, this content device is suggested as the equipment of selection for composing and changing M-capacities. To open the proofreader, sort regulate at the incite opens the M-report filename.M in a supervisor window, organized for altering. As referred to before, the record has to be inside the momentum catalog, or in an index within the pursuit manner.

**Getting Help:**

The important technique to get help on line is to utilize the MATLAB assist application, opened as a exclusive window both via tapping at the query mark image at the computing device toolbar, or by using writing help program on the provoke within the order window. The help Browser is an internet application coordinated into the MATLAB computing device that shows a Hypertext Markup Language (HTML) statistics. The Help Browser contains of two sheets, the assistance pilot sheet, used to find out data, and the show sheet, used to look the statistics. Clear as crystal tabs aside from pilot sheet are applied to play out a pursuit. Second, within the motion pictures taken via transferring camera setup, the state of affairs becomes extra complex because the heritage may additionally exchange by using shifting shot, we cannot tune item motion exactly inside the sum of distinction map. Therefore, in this situation, the purpose is executed through reusing the previous seam and applying it to the cutting-edge body. In order to discover the seams, we use the preceding seam from previous body to look the modern-day seam in contemporary frame. our method is using a seam computed in frame1 (in crimson) to go looking a comparable seam in frame2. For the pixels close by the area of previous seam, we decide how a lot the selected pixel might vary from the pixel of preceding seam. We use difference of the 2 pixels as the degree of temporal coherence. If the distinction value of first seam pixel is over the threshold, we can keep to go looking the next seam pixel on three feasible pixels (in yellow, blue and brown) in subsequent row, until we discover 5 consecutive pixels that also exceed the threshold.

When we can't search the matching seam, we recalculate the energy for a new seam. We assume a seam 𝑆l-1 has been calculated inside the previous body, and a seam must be calculated for the contemporary frame. For preserving the temporal coherence, we want to make a new seam close to the previous seam with the identical index. We use the distinction among preceding seam and all pixels at the current body as the measure

Thus we upload temporal coherence price Tc(i,j) to the strength map earlier than calculating a seam 𝑆L. The price Tc is zero while the body pixels have the equal fee as previous seam pixels. Using our temporal coherence price, we will calculate the seam which has least electricity and is more close to the preceding seam in previous frame. Consequently, we will decrease the jittery artifacts inside the films.

**COMMUNICATION:**

Communications System Toolbox™ offers algorithms and gear for the layout, simulation, and analysis of communications systems. These capabilities are furnished as MATLAB ® features, MATLAB System gadgets™, and Simulink ® blocks. The machine toolbox includes algorithms for source coding, channel coding, interleaving, modulation, equalization, synchronization, and channel modeling. Tools are supplied for bit blunders charge evaluation, producing eye and constellation diagrams, and visualizing channel characteristics. The machine toolbox additionally provides adaptive algorithms that allow you to version dynamic communications structures that use OFDM, OFDMA, and MIMO techniques. Algorithms support fixed-point facts arithmetic and C or HDL code era.

**Key Features**

▪ Algorithms for designing the physical layer of communications systems, which includes supply coding, channel coding, interleaving, modulation, channel fashions, MIMO, equalization, and synchronization

▪ GPU-enabled System objects for computationally intensive algorithms together with Turbo, LDPC, and Viterbi decoders

▪ Interactive visualization equipment, consisting of eye diagrams, constellations, and channel scattering capabilities

▪ Graphical tool for evaluating the simulated bit mistakes rate of a machine with analytical outcomes

▪ Channel models, consisting of AWGN, Multipath Rayleigh Fading, Rician Fading, MIMO Multipath Fading, and

LTE MIMO Multipath Fading

▪ Basic RF impairments, along with nonlinearity, section noise, thermal noise, and section and frequency offsets

▪ Algorithms available as MATLAB features, MATLAB System objects, and Simulink blocks

▪ Support for fixed-point modeling and C and HDL code technology

**System Design, Characterization, and Visualization:**

The layout and simulation of a communications gadget requires analyzing its reaction to the noise and interference inherent in real-world environments, reading its behavior the usage of graphical and quantitative manner, and determining whether the resulting overall performance meets requirements of acceptability. Communications System Toolbox implements a selection of obligations for communications machine layout and simulation. Many of the functions, System objects™, and blocks inside the device toolbox perform computations associated with a specific thing of a communications gadget, consisting of a demodulator or equalizer. Other talents are designed for visualization or evaluation.

**System Characterization**

The system toolbox offers several standard methods for quantitatively characterizing system performance:

▪ Bit error rate (BER) computations

▪ Adjacent channel power ratio (ACPR) measurements

▪ Error vector magnitude (EVM) measurements

▪ Modulation error ratio (MER) measurements

Because BER computations are fundamental to the characterization of any communications system, the system toolbox provides the following tools and capabilities for configuring BER test scenarios and accelerating BER simulations:

**BER tool**— A graphical user interface that enables you to analyze BER performance of communications systems. You can analyze performance via a simulation-based, semi analytic, or theoretical approach.

**Error Rate Test Console** — A MATLAB object that runs simulations for communications systems to measure error rate performance. It supports user-specified test points and generation of parametric performance plots and surfaces. Accelerated performance can be realized when running on a multi core computing platform.

**Multi core and GPU acceleration** — A capability provided by Parallel Computing Toolbox™ that enables you to accelerate simulation performance using multi core and GPU hardware within your computer.

**Distributed computing and cloud computing support** — Capabilities provided by Parallel Computing Toolbox and MATLAB Distributed Computing Server™ that enable you to leverage the computing power of your server farms and the Amazon EC2 Web service. Performance Visualization. The system toolbox provides the following capabilities for visualizing system performance:

**Channel visualization tool** — For visualizing the characteristics of a fading channel

**Eye diagrams and signal constellation scatter plots** — for a qualitative, visual understanding of system behavior that enables you to make initial design decisions

**Signal trajectory plots** — for a continuous picture of the signal’s trajectory between decision points

**BER plots** — for visualizing quantitative BER performance of a design candidate, parameterized by metrics such as SNR and fixed-point word size

**Analog and Digital Modulation**

Analog and digital modulation strategies encode the facts circulation into a sign this is appropriate for transmission. Communications System Toolbox presents some of modulation and corresponding demodulation abilities. These talents are available as MATLAB features and gadgets, MATLAB System Modulation sorts provided by the toolbox are:

**Analog,** including AM, FM, PM, SSB, and DSBSC

**Digital,** including FSK, PSK, BPSK, DPSK, OQPSK, MSK, PAM, QAM, and TCM



**Source and Channel Coding**

Communications System Toolbox affords source and channel coding talents that can help you develop and compare communications architectures fast, enabling you to discover what-if eventualities and avoid the need to create coding competencies from scratch.

**Source Coding**

Source coding, also referred to as quantization or signal formatting, is a manner of processing facts a good way to lessen redundancy or prepare it for later processing. The system toolbox offers a diffusion of styles of algorithms for imposing source coding and interpreting, inclusive of:

▪ Quantizing

▪ Companding (*µ*-law and A-law)

▪ Differential pulse code modulation (DPCM)

▪ Huffman coding

▪ Arithmetic coding

**Channel Coding**

▪ orthogonal area-time block code (OSTBC) (encoder and decoder for MIMO channels)

▪ Turbo encoder and decoder examples

The gadget toolbox offers application functions for developing your personal channel coding. You can create generator polynomials and coefficients and syndrome deciphering tables, in addition to product parity-take a look at and generator matrices.

The system toolbox additionally presents block and convolutional interleaving and deinters leaving functions to reduce facts errors as a result of burst mistakes in a conversation machine:

**Block,** including General block interleaver, algebraic interleaver, helical scan interleaver, matrix interleaver, and random interleaver.

**Convolutional,** including General multiplexed interleaver, convolutional interleaver, and helical interleaver

**Channel Modeling and RF Impairments**

Channel Modeling

Communications System Toolbox provides algorithms and tools for modeling noise, fading, interference, and different distortions which might be commonly found in communications channels. The system toolbox supports the subsequent styles of channels:

▪ Additive white Gaussian noise (AWGN)

▪ Multiple-enter multiple-output (MIMO) fading

▪ Single-enter single-output (SISO), Rayleigh, and Rician fading

▪ Binary symmetric

A MATLAB channel object provides a concise, configurable implementation of channel models, enabling you to

specify parameters such as:

▪ Path delays

▪ Average path gains

▪ Maximum Doppler shifts

▪ K-Factor for Rician fading channels

▪ Doppler spectrum parameters

For MIMO systems, the MATLAB MIMO channel object expands these parameters to also include:

▪ Number of transmit antennas (up to 8)

▪ Number of receive antennas (up to 8)

▪ Transmit correlation matrix

▪ Receive correlation matrix

To combat the effects noise and channel corruption, the system toolbox provides block and convolutional coding and decoding techniques to implement error detection and correction. For simple error detection with no inherent correction, a cyclic redundancy check capability is also available. Channel coding capabilities provided by the system toolbox include:

▪ BCH encoder and decoder

▪ Reed-Solomon encoder and decoder

▪ LDPC encoder and decoder

▪ Convolutional encoder and Viterbi decoder

****

**RF Impairments**

To model the effects of a non-ideal RF front end, you can introduce the following impairments into your communications system, enabling you to explore and characterize performance with real-world effects:

▪ Memory less nonlinearity

▪ Phase and frequency offset

▪ Phase noise

▪ Thermal noise

You can include more complex RF impairments and RF circuit models in your design using SimRF™.

****

**Equalization and Synchronization**

Communications System Toolbox lets you discover equalization and synchronization strategies. These techniques are usually adaptive in nature and tough to design and symbolize. The machine toolbox affords algorithms and tools that will let you swiftly select the proper approach on your communications machine. Equalization To compare one-of-a-kind techniques to equalization, the device toolbox offers you with adaptive algorithms which include:

▪ LMS

▪ Normalized LMS

▪ Variable step LMS

▪ Signed LMS

▪ MLSE (Viterbi)

▪ RLS

▪ CMA

These adaptive equalizers are available as nonlinear decision feedback equalizer (DFE) implementations and as

Linear (symbol or fractionally spaced) equalizer implementations.

**Synchronization**

The device toolbox provides algorithms for each service segment synchronization and timing phase synchronization. For timing section synchronization, the machine toolbox presents a MATLAB Timing Phase Synchronizer object that offers the following implementation techniques:

▪ Early-late gate timing method

▪ Gardner’s method

▪ Fourth-order nonlinearity method

**Stream Processing in MATLAB and Simulink**

Most verbal exchange structures cope with streaming and frame-primarily based statistics using a aggregate of temporal processing and simultaneous multi frequency and multichannel processing. This form of streaming multidimensional processing can be visible in superior communication architectures consisting of OFDM and MIMO. Communications System Toolbox enables the simulation of advanced communications structures via helping move processing and frame-based simulation in MATLAB and Simulink. In MATLAB, circulate processing is enabled by way of System items™, which use MATLAB objects to symbolize time-based and facts-driven algorithms, sources, and sinks. System objects implicitly manipulate many information of flow processing, including information indexing, buffering, and management of set of rules state. You can mix System gadgets with fashionable MATLAB functions and operators. Most System items have a corresponding Simulink block with the identical abilities. Simulink handles circulation processing implicitly with the aid of coping with the float of information thru the blocks that make up a Simulink model. Simulink is an interactive graphical environment for modeling and simulating dynamic systems that uses hierarchical diagrams to symbolize a machine version. It includes a library of widespread-reason, predefined blocks to represent algorithms, resources, sinks, and device hierarchy.

**Implementing a Communications System**

Fixed-Point Modeling Many communications systems use hardware that requires a fixed-point representation of your design.

Communications System Toolbox supports fixed-point modeling in all relevant blocks and System objects™ with tools that help you configure fixed-point attributes.

Fixed-point support in the system toolbox includes:

▪ Word sizes from 1 to 128 bits

▪ Arbitrary binary-point placement

▪ Overflow handling methods (wrap or saturation)

▪ Rounding methods: ceiling, convergent, floor, nearest, round, simplest, and zero

Fixed-Point Tool in Simulink Fixed Point™ facilitates the conversion of floating-point data types to fixed point. For configuration of fixed-point properties, the tool tracks overflows and maxima and minima.

**Code Generation**

Once you've got advanced your set of rules or communications device, you can robotically generate C code from it for verification, rapid prototyping, and implementation. Most System gadgets, functions, and blocks in Communications System Toolbox can generate ANSI/ISO C code the use of MATLAB Coder™, Simulink Coder™, or Embedded Coder™. A subset of System gadgets and Simulink blocks also can generate HDL code. To leverage present highbrow belongings, you can choose optimizations for specific processor architectures and integrate legacy C code with the generated code.

You can also generate C code for both floating-point and fixed-point data types.

DSP Proto typing DSPs are used in communication system implementation for verification, rapid prototyping, or final hardware implementation. Using the processor-in-the-loop (PIL) simulation capability found in Embedded Coder, you can verify generated source code and compiled code by running your algorithm’s implementation code on a target processor. FPGA Prototyping

FPGAs are used in communication systems for implementing high-speed signal processing algorithms. Using the FPGA-in-the-loop (FIL) capability found in HDL Verifier™, you can test RTL code in real hardware for any existing HDL code, either manually written or automatically generated HDL code.

**CHAPTER -7**

**HARDWARE & SOFTWARE REQUIREMENTS:**

**Software:**

• Matlab R2018a.

**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 Math Works products may take up to 29 GB of disk space

**RAM:**

Minimum: 4 GB

Recommended: 8

**CHAPTER 8**

**EXPERIMENTAL RESULTS**

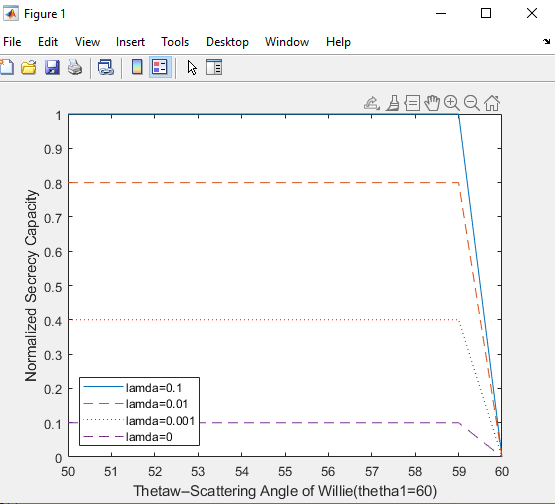


Fig: Normalized secrecy capacity c¯s

. if the incident angle of Alice θ1 = 60◦ and Bob’s antenna is located exactly at the specular reflection direction of Alice’s signal, the closer Willie’s scattering angle θW to θ1, the smaller c¯s we can get. This is obvious because the scattering coefficient GW approximates to GB when ∆ = θ1 − θW is very small. On the other hand, the higher the network density λ, the larger the normalized secrecy capacity and the covert communication is more likely to succeed. Indeed, if there is no interferer in the surroundings (λ = 0), the normalized secrecy capacity is so small that covert communication is practically impossible for a predefined threshold.

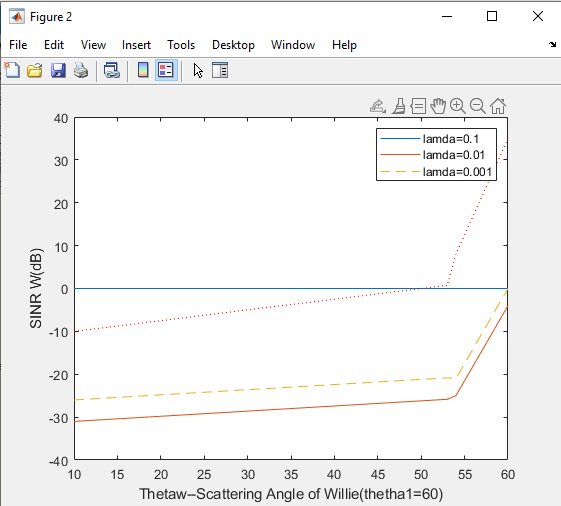


Fig:SINRW (dB)

The smaller the density λ is, the higher the SINRW , which means the reduction of the interference will increase the likelihood of exposure. This also implies that the interference is helpful to covert communication.

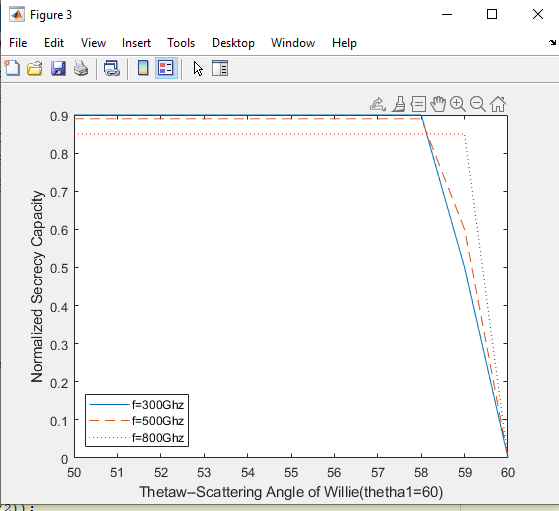


Fig.. The normalized secrecy capacity c¯s versus the scattering angle of Willie θW for different operating frequencies

when different operating frequencies are taken into account. One can notice that c¯s increases with the frequency when the scattering angle is close to the specular reflection direction, but decreases when the receiver angle of Willie gradually deviates from the reflection direction. This is reasonable since the scattering always increases with the operating frequency

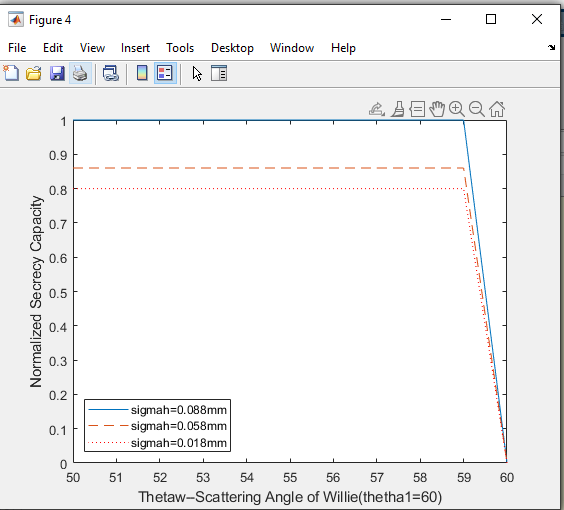


Fig. The normalized secrecy capacity c¯s versus the scattering angle of Willie θW for different surface roughnesses σh. H

In this measurement, we fix the surface correlation length lc, only change the standard deviation of the surface height distribution σh. We notice that the larger value of σh results in lower c¯s. The underlying reason is that, for smaller value of σh, the surface is a more smooth surface with a purely specular reflection, a larger value of σh represents a relatively more rough surface with a stronger diffuse scattering contribution

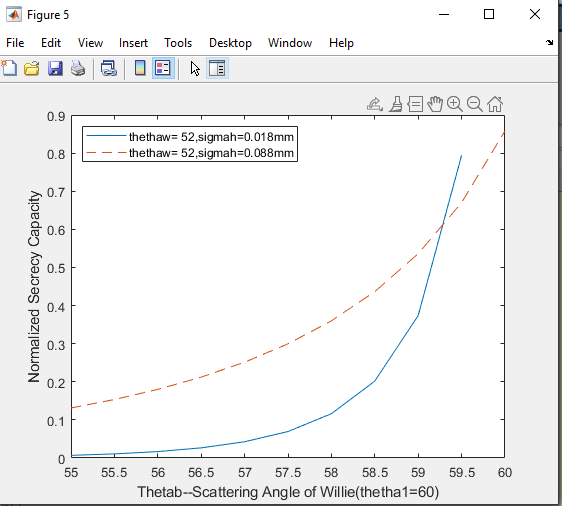


Fig. The normalized secrecy capacity c¯s versus the scattering angle of Bob θB for different surface roughness σh

s the effect of Bob’s scattering angle θB on c¯s. Given the incidence angle θ1 = 60◦ , we fix the receiver angle of Willie θW at 52◦ and 55◦ , then calculate the value c¯s at different scattering angle of Bob θB(55◦ · · · 60◦ ). The results show that, the closer Bob’s scattering direction to the specular reflection direction, the larger the value of c¯s. On the other hand, a more smooth surface (with less σh) will have less scattering strength and therefore will have larger c¯s.

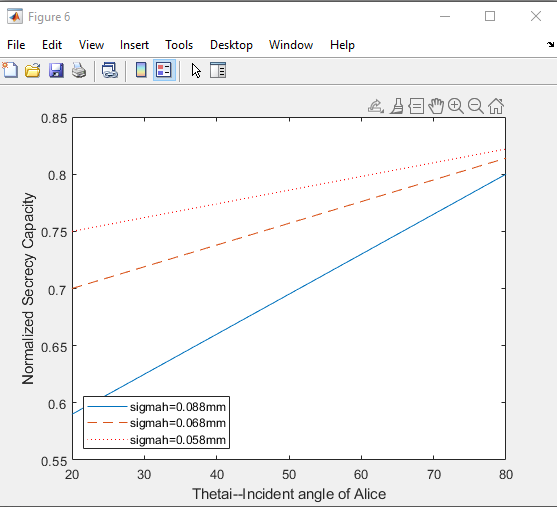


Fig.. The normalized secrecy capacity c¯s versus the incident angle of signal θ1 for different surface roughnesses σh

In the measurement setup, we assume Bob is located in the reflected direction (θB = θ1), and Willie’s receiver angle is fixed to be θW = θB −5 ◦ . When the incident angle θ1 increases, the value of c¯s increases as well. However, this growth is slow. Besides, the more smooth the surface, the higher the value of c¯s. This is due to the fact that a smooth surface has a stronger specular reflection component

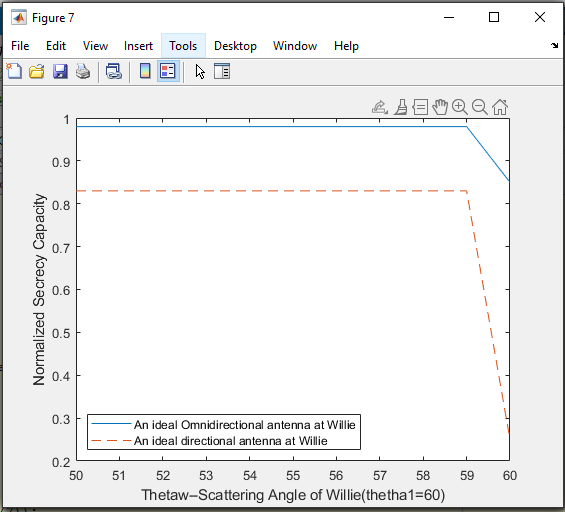


Fig. The normalized secrecy capacity c¯s versus the scattering angle of Willie θW for different antennas of Willie

the normalized secrecy capacity Alice and Bob can get when Willie adopts an omnidirectional or directional antenna. It is important to note that the omnidirectional antenna has relatively lower detection capability compared with the directional antenna.

**CHAPTER 9**

**CONCLUSION**

Security is the foundation for the development of IoT network. However, how to protect IoT is a challenging task and many related issues need to be solved. From the physical layer security perspective, this paper introduces covert communication into IoT network to enhance the security from the bottom layer. If the adversary cannot detect user’s transmission behavior, he has no chance to launch other attacks. What he sees is merely a shadow noisy wireless network.

**CHAPTER 10**

**FUTURE SCOPE**

Willie is faced with a dilemma of how to determine the type of antenna.so ,the The future scope is that which type of antenna is used or what particular antenna should be used ,and further different modulations can be used.

**CHAPTER 11**

**REFERENCES**

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, October 2017.

[2] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating critical security issues of the iot world: Present and future challenges,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483–2495, August 2018.

[3] Y. Lu and L. D. Xu, “Internet of things (iot) cybersecurity research: A review of current research topics,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2103–2115, April 2019.

[4] Y. Miao, X. Liu, K. R. Choo, R. H. Deng, H. Wu, and H. Li, “Fair and dynamic data sharing framework in cloud-assisted internet of everything,” IEEE Internet of Things Journal, vol. 6, no. 4, pp. 7201–7212, Aug 2019.

[5] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, “Hiding information in noise: Fundamental limits of covert wireless communication,” IEEE Communications Magazine, vol. 52, no. 12, pp. 26–31, December 2015.

[6] J. Hu, C. Lin, and X. Li, “Relationship privacy leakage in network traffics,” in 25th International Conference on Computer Communication and Networks, ICCCN, August 2016, pp. 1–9.

[7] J. Classen, M. Schulz, and M. Hollick, “Practical covert channels for wifi systems,” in 2015 IEEE Conference on Communications and Network Security (CNS), Sep. 2015, pp. 209–217.

[8] S. Grabski and K. Szczypiorski, “Steganography in ofdm symbols of fast ieee 802.11n networks,” in 2013 IEEE Security and Privacy Workshops, May 2013, pp. 158–164.

[9] S. DOro, F. Restuccia, and T. Melodia, “Hiding data in plain sight: Undetectable wireless communications through pseudo-noise asymmetric shift keying,” in IEEE INFOCOM 2019, April 2019, pp. 1585–1593.

[10] B. Bash, D. Goeckel, and D. Towsley, “Limits of reliable communication with low probability of detection on awgn channels,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 1921–1930, September 2013.

[11] W. Wu, N. Cheng, N. Zhang, P. Yang, W. Zhuang, and X. Shen, “Fast mmwave beam alignment via correlated bandit learning,” IEEE Transactions on Wireless Communications, pp. 1–1, 2019.

[12] I. F. Akyildiz, J. M. Jornet, and C. Han, “Terahertz band: Next frontier for wireless communications,” Physical Communication, vol. 12, pp. 16– 32, 2014.