COVERT WIRELESS COMMUNICATION IN DENSE IOT NETWORK USING THZ BAND

M.Venkata Rathnam1[st], Y.Tejaswi[2],K.Mahesh Babu[3],A.Mahesh Babu [4]

T.Rohith[5],SK.Ruksana[6]

[1]Associate Professor ,Dept of ECE, PBR VITS ,Kavali, Andhra Pradesh-524201
[2,3,4,5,6]UG students ,Dept of ECE,PBR VITS,Kavali,Andhra Pradesh-524201 India.

Abstract - The Covert communication is a valuable tool in preventing an adversary from detecting that the transmission has occurred between two users. The covert wireless communication in an IoT network with dense deployment, where an IoT device is subjected to both the background noise and the aggregate interference from other transmitting devices. In an IoT network with THZ(Terahertz) band, the covert communication becomes more challenging as Willie can position as receiver in the narrow beam between Alice and Bob to detect or block their LOS communications. Even in the LOS communication the covert communication is still possible by using Specular reflection or Diffuse scattering methods. Covert communication enhances the security of IoT networks.

Index Terms – Terahertz Bands, Covert communication, Line of Sight, Internet of Things.

I. INTRODUCTION:

The Internet of Things (IoT) is dramatically changing our daily lives [1]. Meanwhile, security issue is becoming oneof the primary tasks of IoT in the coming years [2][3][4]. Traditional cryptography methods for network security cannotsolve all security problems. If a user wishes to communicate covertly (without being detected by other detectors), encryption to preventing eavesdropping is not enough [5]. Even if a message is encrypted, the metadata, such as network traffic pattern, can reveal some sensitive information [6]. Ina battlefield, soldiers hope to hide their tracks so they needto communicate stealthy. Furthermore, if an adversary cannot detect the transmissions, he has no chance to launch the "eavesdropping and decoding" attack even if he has boundlesscomputing and storage capabilities.

Covert communication at physical-layer has a long history. It is always related with "wireless steganography", i.e., hiddeninformation is embedded into a cover signal to construct a covert channel, such as encoding information on top of the training sequences of Wi-Fi [7], the cyclic prefix of Wi-Fi OFDM symbols [8], or a dirty Wi-Fi QPSK constellation [9]. Inthis paper, we consider physical-layer covert communication that employs the background noise and the aggregate interference in a dense IoT network to hide user's transmission attempts. Consider a scenario that a transmitter Alice would like to send a message to a receiver Bob covertly over a wireless channel in order to not being detected by a warden Willie. Alice can use the noise in the channel instead of the statistical properties of the cover signal to hide information. Seminal work of Bash *et al.* [10] initiated the research on howthe covert throughput scales with *n*.

II. LITERATURE SURVEY

[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 end users, 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 real world applications.

[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 aim of guiding future research directions.

[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.

[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 full update 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 (Fair Dyn DSF) in the multi owner setting. Using Fair Dyn DSF, one can check the correctness of search results, achieve fair arbitration, multi-keyword search, and dynamic update. We also prove that Fair Dyn DSF is secure against inside keyword guessing attack and demonstrate its efficiency by evaluating its performance using various datasets.

[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.

III. **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 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

IV. **PROPROSED 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 $d_{\alpha,\omega}= \omega(n^{1/2\alpha})$.(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, mm Waves (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-of Sight) 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.

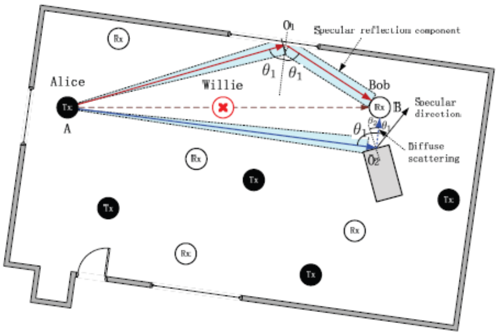


Fig. Covert communication in a THz Band IoT network.

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

$$G_k = \frac{2}{1 - \cos(\phi/2)}$$

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

$$P_{Rx} = Ad_{a,b}^{-2} \exp(-Kd_{a,b})$$

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,

$$H = P_{Tx}c^2/(16\pi^2 f^2).$$

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

$$S_{JN}(f) = \frac{hf}{\exp(hf/k_B T) - 1}$$

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

$$\mathbb{P}_B(x) = 1 - \exp[-\lambda(x - r_B)r_B]$$

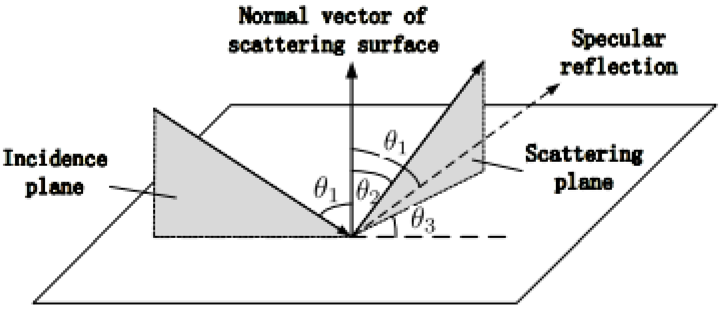


Fig. The model of scattering at a rough surface

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

$$\mathbb{P}_C = \frac{\phi}{2\pi}$$

then the aggregate interference at Bob is

$$I_{THz}^{(b)} = A \sum_{i=1}^{\infty} \left[r_i^{-2} \exp(-Kr_i) \cdot \mathbf{1}_{\{I_i > 0\}} \right]$$

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{I I>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.

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)

V. **ASSESMENT METRICS:** 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:

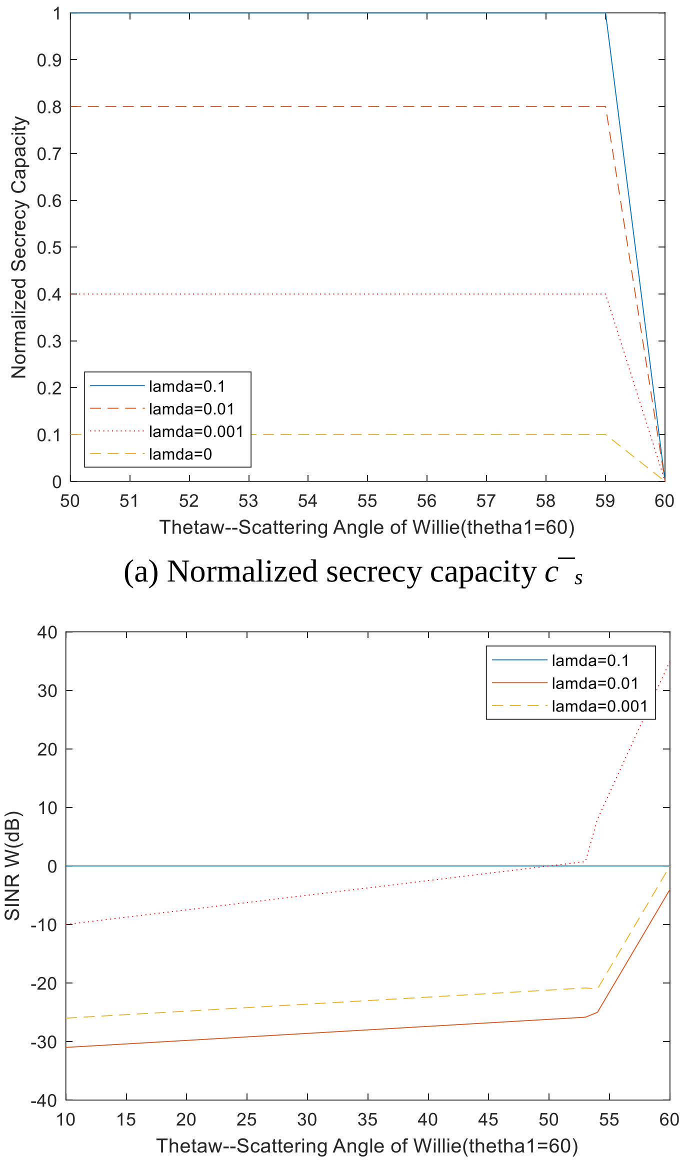
$$\bar{c}_s = \frac{\log(1+SINR_B)-\log(1+SINR_W)}{\log(1+SINR_B)}$$

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:

$$\begin{aligned} SINR_B &= \frac{Ad_{a,b}^{-2}\exp(-Kd_{a,b})\cdot G_B}{S_{JN}(f)+I_{THz}^{(b)}} \\ SINR_W &= \frac{Ad_{a,w}^{-2}\exp(-Kd_{a,w})\cdot G_W}{S_{JN}(f)+I_{THz}^{(w)}} \end{aligned}$$

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.

VI. **RESULTS AND DISCUSSION:**



(a) Normalized secrecy capacity $\bar{c}_s$

(b)SINRW(dB)

Fig. (a) The normalized secrecy capacity $\bar{c}_s$ and (b) $SINR_W$ versus the scattering angle of Willie θ_W for different network density λ. Here the incidence angle of Alice θ_1 = 60◦, the surface height variation σ_h = 0.088mm, and the operating frequency f = 500GHz.

The Effect of Network Density λ: As illustrated in Fig. (a), if the incident angle of Alice $\theta_1 = 60^{\circ}$ and Bob's antenna is located exactly at the specular reflection direction of Alice's signal, the closer Willie's scattering angle θ_W to θ_1, the smaller $\bar{c}_s$ we can get. This is obvious because the scattering coefficient G_W approximates to G_B when $\Delta = \theta_1 - \theta_W$ 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 ($\lambda = 0$), the normalized secrecy capacity is so small that covert communication is practically impossible for a predefined threshold. Fig. (b) also confirms this result from another aspect. The smaller the density λ is, the higher the $SINR_W$, which means the reduction of the interference will increase the likelihood of exposure. This also implies that the interference is helpful to covert communication.

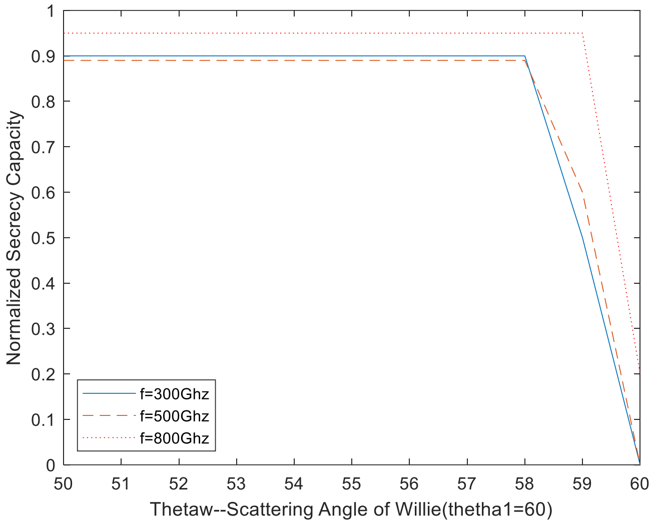


Fig. The normalized secrecy capacity $\bar{c}_s$ versus the scattering angle of Willie θ_W for different operating frequencies. Here the incidence angle $\theta_1 = ^{60}\circ$, $\sigma_h = 0.058$mm, and $\lambda = 0.01$.

The Effect of Operating Frequency: Fig. shows the comparison when different operating frequencies are taken into account. One can notice that $\bar{c}_s$ 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.

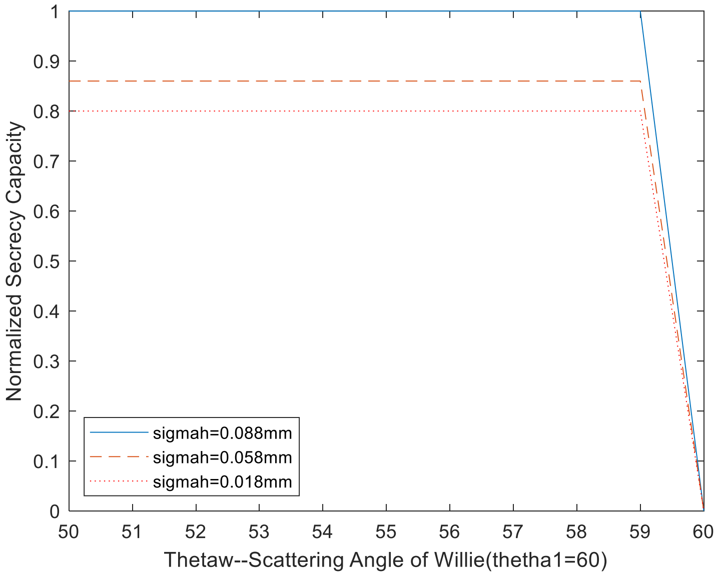


Fig. The normalized secrecy capacity $\bar{c}_s$ versus the scattering angle of Willie θ_W for different surface rough nesses σ_h. Here the incidence angle $\theta_1 = 60\circ$, $f = 500$GHz, and $\lambda = 0.01$.

The Effect of Surface Roughness: The effect of surface roughness on $\bar{c}_s$ is illustrated in Fig. In this measurement, we fix the surface correlation length l_c, only change the standard deviation of the surface height distribution σ_h. We notice that the larger value of σ_h results in lower $\bar{c}_s$. The underlying reason is that, for smaller value of σ_h, the surface is a more smooth surface with a purely specular reflection, a larger value of σ_h represents a relatively more rough surface with a stronger diffuse scattering contribution.

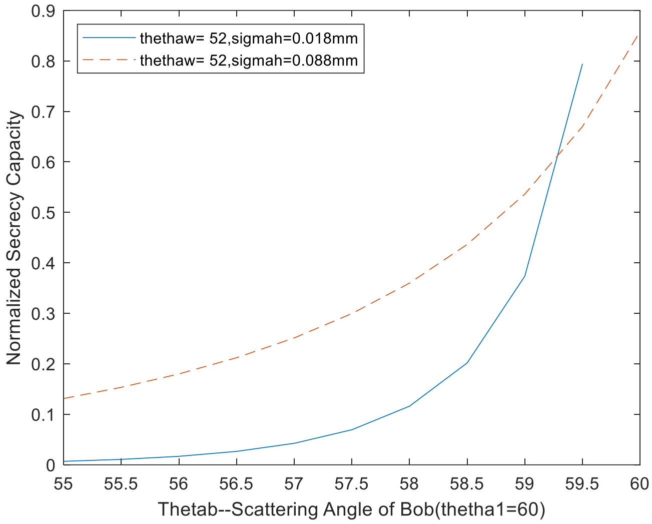


Fig. The normalized secrecy capacity $\bar{c}_s$ versus the scattering angle of Bob θ_B for different surface roughness σ_h. Here $\theta_1{}^{=60}$∘, $f = 500$GHz, and $\lambda = 0.01$.

The Effect of Bob's Scattering Angle: In practice, Alice and Bob cannot always find a specular reflection path to perform their NLOS communication. As an alternative, Alice and Bob use diffuse scattering to communicate covertly. Fig. demonstrates the effect of Bob's scattering angle θ_B on $\bar{c}_s$. Given the incidence angle $\theta_1 = 60^\circ$, we fix the receiver angle of Willie θ_W at 52° and 55°, then calculate the value $\bar{c}_s$ at different scattering angle of Bob $\theta_B(55^\circ \cdots 60^\circ)$. The results show that, the closer Bob's scattering direction to the specular reflection direction, the larger the value of $\bar{c}_s$. On the other. However, if the scattering angle deviates from the direction of reflection for several degrees, the value of $\bar{c}_s$ will decrease rapidly, especially when the surface is rougher.

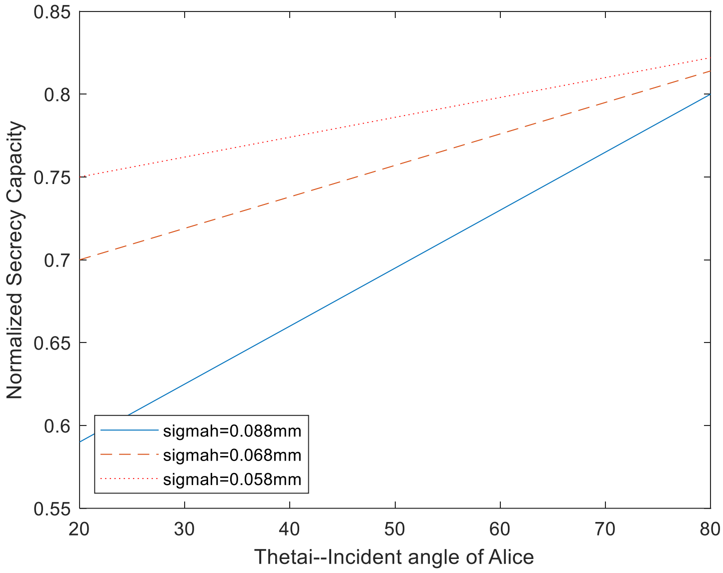


Fig. The normalized secrecy capacity $\overline{c}_s$ versus the incident angle of signal θ_1 for different surface rough nesses σ_h. Here the scattering angle of Willie $\theta_W = \theta_1 - 5^\circ$, $f = 500$GHz, $\lambda = 0.01$.

The Effect of Incident Angle: Fig. depicts the ten- dency of $\overline{c}_s$ with the incident angle θ_1. In the measurement setup, we assume Bob is located in the reflected direction ($\theta_B = \theta_1$), and Willie's receiver angle is fixed to be $\theta_W = \theta_B \quad 5^\circ$. When the incident angle θ_1 increases, the value of $\overline{c}_s$ increases as well. However, this growth is slow. Besides, themore smooth the surface, the higher the value of $\overline{c}_s$. This is due to the fact that a smooth surface has a stronger specularreflection component.

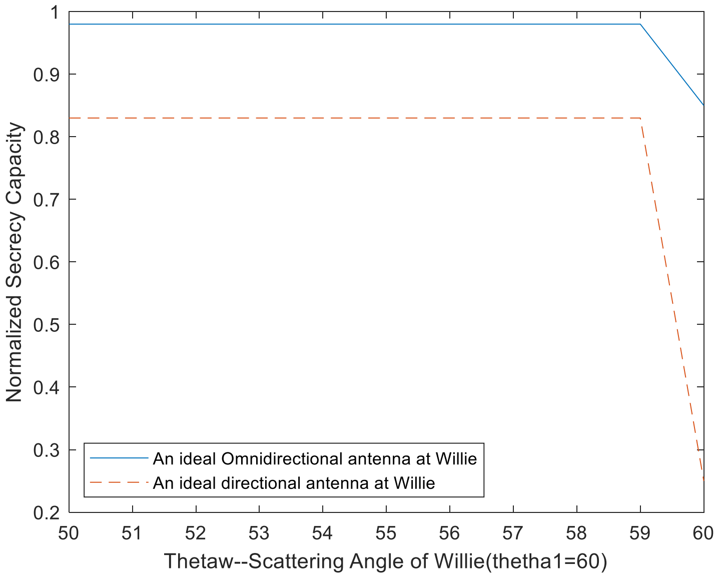


Fig. The normalized secrecy capacity $\overline{c}_s$ versus the scattering angle of Willie θ_W for different antennas of Willie. Here $\theta_1 = 60^{\circ}$, $\sigma_h = 0.058$mm, and $f = 800$GHz.

The gain of an omnidirectional antenna is much lower than a directional antenna with a small directivity angle. Then, the omnidirectional antenna willexperience more interference from other Tx in the vicinity. Fig. 14 also shows the normalized secrecy capacity Aliceand Bob can get when Willie adopts an omnidirectional or directional antenna. It is important to note that the omni-directional antenna has relatively lower detection capability compared with the directional antenna. However, if Williehas no knowledge about the direction of Alice’s signal, awrong receiving direction of his directional antenna would be counterproductive.

VII. **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.

VIII. **REFERENCES:**

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A surveyon 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 informationin 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 asymmetricshift 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.

[13] B. A. Bash, S. Guha, D. Goeckel, and D. Towsley, "Quantum noise limited optical communication with low probability of detection," in *IEEEISIT 2013*, 2013, pp. 1715–1719.

[14] B. A. Bash, D. Goeckel, and D. Towsley, "Covert communication gains from adversarys ignorance of transmission time," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8394–8405, 2016.

[15] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1195–1205, October 2015.

[16] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Communications Letters*, vol. 21, no. 4, pp.941–944, April 2017.

[17] Z. Liu, J. Liu, Y. Zeng, J. Ma, and Q. Huang, "On covert communication with interference uncertainty," in *IEEE ICC*, Kansas City, MO, USA, May2018.

[18] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *ACM SIGCOMM*, New York, NY, USA, 2011, pp. 2–13.

[19] X. Fang, N. Zhang, S. Zhang, D. Chen, X. Sha, and X. Shen, "On physical layer security: Weighted fractional fourier transform based user cooperation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5498–5510, August 2017.

[20] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEETransactions on Wireless Communications*, vol. 16, no. 9, pp. 6193–6206,2017.

[21] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Trans- actions on Wireless Communications*, vol. 17, no. 11, pp. 7252–7267, November 2018.

[22] B. He, S. Yan, X. Zhou, and H. Jafarkhani, "Covert wireless communi- cation with a poisson field of interferers," *IEEE Transactions on WirelessCommunications*, vol. 17, no. 9, pp. 6005–6017, 2018