ABSTRACT

Semantic communication is an important component in the next generation of wireless networking. Enabled by this novel paradigm, the conventional Internet-of-Things (IoT) is evolving toward the semantic IoT (SIoT) to achieve significant system performance improvements. However, traditional wireless communication security techniques for bit transmission cannot be applied directly to the SIoT that focuses on semantic information transmission. One key reason is the lack of new security performance indicators. Thus, we have to rethink the wireless communication security in the SIoT. As such, in this article, we analyze and compare classical security techniques, such as physical layer security, covert communications, and encryption, from the perspective of semantic information security. We highlight the differences among these security techniques when applied to the SIoT. Novel performance indicators, such as semantic secrecy outage probability (for physical layer security techniques) and detection failure probability (for covert communication techniques), are proposed. Considering that semantic communications can raise new security issues, we then review attack and defense methods at the semantic level. Lastly, we present several promising directions for future secure SIoT research.

INTRODUCTION

The advancement of semantic communications technique has significantly changed nearly all aspects of wireless communication networks. As a new communication paradigm, semantic communications no longer focus on the accurate transmission of bits, but on transmitting task-related semantic information [1]. As semantic models become lightweight, deploying semantic encoders and decoders in network edge devices is also practical. Thus, the conventional IoT is evolving toward the SIoT, enabling more efficient and energy-saving information interaction [2]. For example, the Semantic Internet-of-Vehicles (SIoV) is a new approach to interconnecting vehicles with the semantic communications. The information transmitted between vehicles is in the form of semantic information, such as features extracted by neural networks, rather than raw road images, enabling intelligent, timely, and efficient interactions.

Data security is an enduring topic in wireless communication networks. When network devices transmit sensitive data, there is a high risk of eavesdropping or jamming/interference attacks by malicious third parties. A straightforward approach is to encrypt the data by using complex algorithms. Although various encryption algorithms have been proposed, the effectiveness of encryption and the complexity of computation are positively correlated. To improve the security of communication networks, high complexity in encryption put much pressure on network edge devices with insufficient computing power. Fortunately, besides traditional encryption methods, the physical layer security (PLS) technique is considered to be an essential driver enhancing 6G security [3]. Without requiring actual key distribution, PLS can achieve high-quality network security performance with low computational complexity. A common disadvantage of encryption and PLS is that they can only guarantee that the information will not be decrypted. However, a malicious third party can still use the detected wireless signals to locate the transmitter in the network and, thus, perform jamming. To solve this problem, the covert communication techniques are proposed as a more demanding PLS technique. In order not to be detected by malicious nodes in the act of transmitting data, transmitters can hide the transmitting activities by designing a suitable power allocation scheme or by using friendly jammers. A comparison of the aforementioned wireless communication security techniques is presented in Fig. 1.

However, current research on PLS, covert communications, and encryption is mainly carried out in the conventional IoT without considering the new features of SIoT. Moreover, the study of the security of semantic communications techniques is still in its infancy [4–6]. The application of classical wireless communication security techniques in SIoT has not been clearly discussed. Specifically, the following questions have not been answered:

Q1 How do wireless communication security techniques differ in the SIoT compared to those in the conventional IoT?

Q2 What are the security performance indicators in SIoT?

Q3 What are the new security issues does semantic communication technology bring while improving the efficiency of the network?
As such, we revisit classical communication security techniques from the perspective of semantic networks, and discuss the novel attack and defense methods brought about by the semantic communications techniques. Our contributions are summarized as follows:

- We revisit three security techniques, such as PLS, covert communications, and encryption. For each technique, we discuss its new features in SIoT (For Q1).

- To quantify the new characteristics brought by the SIoT to PLS and covert communications, we propose two new performance indicators, that is, semantic secrecy outage probability (SSOP) and detection failure probability (DFP), respectively (For Q2).

- We discuss the semantic attack schemes caused by semantic communications technique, which can be divided into targeted and untargeted semantic attacks (For Q3). Furthermore, we propose training-based and training-free defense schemes.

**Revisiting Conventional Security Techniques**

In this section, we revisit wireless communication security techniques, including PLS, covert communications, and encryption techniques (Table 1). We present the definitions, features, and common security performance indicators. We then discuss the differences between these techniques when applied in the SIoT and in the conventional IoT, and propose novel performance indicators.

**Physical Layer Security**

**Definition:** The PLS is built upon the information-theoretic level using physical layer technologies, e.g., friendly jammer. Unlike the encrypt method, PLS independent of device computing capability, which not only enables it to achieve effective security but also gives it a natural advantage in saving resources. Moreover, such a technique is able to adjust transmission strategies according to the physical layer characteristics to adapt to physical medium [3]. The eavesdroppers could be malicious mobile devices or wireless sniffers with malicious plugins [3].

![FIGURE 1. Rethinking physical layer security technique in the semantic Internet of Things. A novel security performance indicator, such as semantic secrecy outage probability, is proposed.](image)

| Security Techniques | Physical Layer Security | Covert Communications | Encryption |
|---------------------|-------------------------|-----------------------|------------|
| Purpose             | Avoid the eavesdropper to obtain the content of the source message | Avoid the warden to detect the occurrence of wireless transmitting activities | Prevent the eavesdropper to obtain the content of the source message |
| Performance Indicators | 1. Secrecy Outage Probability | 1. Detection Error Probability | 1. Encryption/decryption Time |
|                     | 2. Probability of Non-zero Secrecy Capacity | 2. Covert Rate | 2. Crack Time |
|                     | 3. Average Secrecy Capacity | | 3. Power Consumption |
| Protocol Layer      | Physical Layer | Physical Layer and Network Layer | Mainly Upper Layer |
| Security Level       | Medium | High |
| Major features       | 1. Guarantee security at the information-theoretic level using physical layer technologies, e.g., friendly jammer | 1. Securing data by hiding the wireless transmitting activities using physical layer technologies, e.g., friendly jammer | 1. Data security is ensured by encrypting the data, mainly with the help of upper layer encryption algorithms |
|                     | 2. The malicious third party can detect communication activities | 2. The malicious third party cannot detect communication activities | 2. The malicious third party can detect communication activities |
| Role in the Slot Network | Protect semantic information from being decoded successfully by the eavesdropper | Hide the transmission of semantic information from detection by warden | Encryption protection of semantic information |
| New Performance Indicator | Semantic secrecy outage probability, which describes the probability that the eavesdropper successfully obtains the semantic information sent by the transmitter and accurately performs the semantic decoding | Detection failure probability, which describes the probability that no transmission activity is detected by warden during the transmission time of the data |

**TABLE 1.** Comparison of physical layer security, covert communications, and encryption techniques, as well as our proposed new performance indicators for the SIoT.
Based on the above discussion, one can conclude that the metrics reflecting the security performance of the SIoT are not only SOP at the communication level, but also the semantic decoding error probability (SDEP) at the semantic level. Here, SDEP describes the probability that the eavesdropper can successfully decode the information that it needs from the intercepted semantic information.

The wireless channel changes. According to the working principles of PLS methods, the security performance indicators mainly include secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), and the average secrecy capacity (ASC) [7].

**Average Secrecy Capacity:** The secrecy capacity can be obtained by calculating the difference between the main channel capacity and wiretap channel capacity. For a given constraint of perfect secrecy, the average secrecy capacity provides a criterion for capacity limit in an accounting point of view. For instance, if the legitimate user is able to obtain the perfect channel state information (CSI) of the eavesdropper’s channel, then the coding scheme can be flexibly adjusted to adapt to different fading coefficients. In principle, therefore, one can realize any average secure communication rate, which is below the average secrecy capacity of the channel.

**Secrecy Outage Probability:** The SOP is defined as the probability that the instantaneous secrecy capacity falls less than the target secrecy rate [7]. The SOP first provides the conditions that the wireless channel needs to meet to support the specified secure rate. Second, it gives a security measure for cases where legitimate users have no CSI about the eavesdropper. Therefore, as long as the secrecy capacity is larger than the target secrecy rate, the eavesdropper’s channel is worse than legitimate users’ estimation and the secrecy of the network is ensured.

**Probability of Non-Zero Secrecy Capacity:** If the main channel capacity is larger than that of the eavesdropper’s channel, the eavesdroppers are unable to decode the transmitted information. Here, the occurrence probability of such an event is defined as the PNZ. On this basis, according to the definition, the PNZ equals the probability that the instantly received signal-to-noise ratio (SNR) of the legitimate users is greater than that of the eavesdropper.

**Physical Layer Security in SIoT Network:** In a conventional IoT, an eavesdropper is considered successful if it can obtain the source message sent by the transmitter. However, in the SIoT, semantic information is transmitted in the wireless channel and decoding is required to obtain the original source message, as shown in Fig. 1 (Part A). Therefore, even if the eavesdropper intercepts the semantic information sent by the transmitter, it may still not obtain the required information, as shown in Fig. 1 (Part B). According to the characteristics of semantic communication, we discuss possible scenarios in which the eavesdropper succeeds in eavesdropping on information but fails to decode it as follows:

- **Semantic decoding failure caused by background knowledge difference between the eavesdropper and the legitimate receiver.** In the SIoT, legitimate communication participants will share background knowledge for semantic encoding and decoding. The eavesdropper might have the different background knowledge to decode the intercepted semantic information. For example, the semantic information “Mouse” could be decoded as an animal or a computer device, in which the eavesdropper may not be able to decode this meaning correctly. Moreover, the dataset used for semantic encoder and decoder training can be regarded as the shared background knowledge which may not be unavailable to the eavesdropper.

- **The objectives of the eavesdropper are different from those of the legitimate receiver,** resulting in the eavesdropper unable to obtain the desired information. For example, a transmitter is a camera in the SIoT that captures street-view photos. With the help of semantic communication technique, the camera acts as a transmitter to send the photos to a legitimate receiver. The owner of the legitimate receiver is a vehicle company interested in the number and type of cars on the street, while the same camera wants to steal pedestrians’ information on the road from images. However, the transmitter, through the semantic encoder, transmits only the semantic information that satisfies the task of the legitimate receiver, for example, image segmentation of vehicles. Therefore, even if the eavesdropper has perfect access to the images transmitted in the wireless environment, its objective is not met in this case.

- **Mismatch between semantic encoding of the transmitter and semantic decoding of the eavesdropper.** In semantic communication, semantic encoding and decoding at the transmitter and receiver have to be jointly trained. This process can be used as a mechanism to secure semantic communication further. For example, for image-based semantic extraction, the legitimate transmitter’s encoding engine is trained with human-based datasets (e.g., human faces), while the eavesdropper’s decoding is trained with animal-based datasets. Thus, due to this model mismatch, even though the eavesdropper can intercept the transmitted data, it may not be able to decode the human-based semantic information correctly.

Based on the above discussion, one can conclude that the metrics reflecting the security performance of the SIoT are not only SOP at the communication level, but also the semantic decoding error probability (SDEP) at the semantic level. Here, SDEP describes the probability that the eavesdropper can successfully decode the information that it needs from the intercepted semantic information. For example, in a semantic communications system with visual question answering (VQA) task [8], SDEP can be the probability that the eavesdropper can successfully eavesdrop on information. For example, a transmitter is a camera in the SIoT that captures street-view photos. With the help of semantic communication technique, the camera acts as a transmitter to send the photos to a legitimate receiver. The owner of the legitimate receiver is a vehicle company interested in the number and type of cars on the street, while the same camera wants to steal pedestrians’ information on the road from images. However, the transmitter, through the semantic encoder, transmits only the semantic information that satisfies the task of the legitimate receiver, for example, image segmentation of vehicles. Therefore, even if the eavesdropper has perfect access to the images transmitted in the wireless environment, its objective is not met in this case.

**Remark 1:** As shown in Fig. 1 (Part C), SSOP describes the probability that the eavesdropper in the SIoT successfully eavesdrops on the semantic information sent by the transmitter and successfully performs the semantic decoding. Therefore, SSOP is defined as the product of SOP and one minus SDEP.

Note that when the task or interest of the eavesdropper is unknown, SSOP cannot be calculated accurately by the SIoT designer. However, our proposed SSOP can still be used for theoretical upper-bound performance analysis to verify the robustness of the proposed system design. Another possible
research direction is to use statistical methods to estimate the semantic information that eavesdroppers may wish to obtain. Thus, the system designer can estimate SSOP to facilitate secure SIoT design, for example, to minimize SSOP given certain resource constraints. Moreover, because the wireless transmission and the semantic encoding/decoding schemes can be jointly optimized, a cross-layer algorithm is expected to reduce the SSOP.

Figure 2 shows the SOP and the SSOP versus the signal-to-noise ratio of the transmitter-receiver link with different values of SDEP. We can observe that the probability that the eavesdropper fails to decode the semantic information reduces the SSOP. Specifically, when an eavesdropper in the semantic IoT has a 30 percent probability of not being able to decode successfully semantic information, that is, SDEP = 30 percent, the transmitter can use an SNR roughly 1 dB lower to achieve the same SSOP as the SOP in a conventional IoT.

An essential motivation for secure SIoT research is to perform cross-layer co-design. Although semantic communications can enhance system security and reduce the transmit power required to achieve a certain SSOP, the encoding and decoding of semantic information consume computational resources of the network. Therefore, the trade-off between SIoT performance and security should be considered. A more secure and more efficient IoT can be achieved by designing joint transmit and jamming power allocation schemes in the physical layer and the semantic encoding/decoding scheme in the semantic layer. Moreover, because the specific definition of SSOP could be different in different systems, the model of SSOP needs further verification and study for future work by considering the difference in background knowledge shared by the transmitter and receiver and the matching degree of the training model.

**Covert Communications**

**Definition:** So far, the PLS has been applied at large to boost wireless transmission security. Despite its effectiveness, PLS still has certain limitations in other aspects. By analyzing the wireless signal, for instance, the user's location may be exposed, which poses threat to user privacy. Such problems cannot be solved by PLS techniques, triggering the proposal of covert communications. Also known as low probability of detection communications, covert communications aim to deliver information to a legitimate user without being caught by the warden, who attempt to detect such transmission [9]. The covert communications can include two major aspects: The first one focuses mainly on analyzing and exploiting the uncertainty of the average power of malicious wardens. Another one is to send the signal covered by high-power signals, so as to improve covertness. It is not difficult to see that covert communication never relies on the adversary's competence, indicating that transmission security can be perfectly guaranteed even if the attacker has a strong processing capability. According to the above discussion, the covert rate and DEP, which are detailed as follows, are used to characterize the performance of covert communications.

**Detection Error Probability:** The warden needs to make a binary choice between silent and transmitting via hypothesis testing. Therefore, the detection error probability (DEP) is defined as the likelihood of the warden making a wrong decision, which contains two cases. The first one is that the warden chooses non-null-decision (transmitting) while the null hypothesis (silent) is accurate, which is called false alarm. Another one is that the warden sides with a null hypothesis when the non-null hypothesis is true, which is known as miss detection. The value of DEP is the sum of the probabilities of making the above two wrong decisions.

**Covert Rate:** Besides DEP, the covert rate, which describes the data transmission rate when the DEP of the warden is close to one, is also vital. The covert rate of any user can be calculated based on the well-known Shannon–Hartley theorem [10].

**Covert Communications in SIoT Network:** In a covert communication system, the objective of the warden is to detect whether the transmission is taking place with or without concerning what data is being transmitted. Therefore, encoding the source message to be transmitted into semantic information will not improve the DEP of the warden. If the warden successfully detects that wireless communication is taking place, it can analyze and obtain the transmitter’s information, such as the location, and then apply interference to block the semantic communications. To make the DEP converge to 1 arbitrarily, the solutions are to design a reasonable transmitting power allocation scheme and/or to use a friendly jammer or a reconfigurable intelligent surface, as in the conventional IoT. The covert rate in the semantic IoT is the same as

![Figure 2](image-url)
in the conventional IoT.

However, because the warden can perform multiple detections during the data transmission process, a failure of one detection does not mean that the warden cannot discover the transmitting activity. Although the DEP can be arbitrarily close to 1 with covert communication techniques, the DEP is typically set as 90 to 95 percent in practical communication systems [11]. Even if we consider that the DEP is 99 percent, the probability that a warden who can detect the wireless environment five times per second finds a transmitting activity that lasts 10 seconds is approximately 39.5%. When the warden finds a transmitting activity five times per second, the warden can detect the wireless environment, the shorter the transmission time of the data. Therefore, as shown in Fig. 3, the probability of the wireless transmission being successfully detected by the warden is lower in the SLoT than in the conventional IoT. The reason is that in the SLoT, the transmitter can encode articles into semantic information without affecting task completion, for example, knowledge graphs, which have fewer bytes than the original article. Therefore, with the same covert rate, transmitters in the SLoT can complete information transmission faster, as shown in Fig. 3. Because there is an upper limit to the frequency of the warden’s detection of the wireless environment, the shorter the transmission time is, the lower the probability that the transmitting activity will be detected.

However, there is no effective performance indicator to describe the covert communication security performance improvement by decreasing the transmitted data amount with semantic communications technique. This research gap exists because all source messages are encoded in the conventional IoT, and there are no differences in the amount of data. To fill this gap, we propose a new performance indicator for covert communications, such as detection failure probability (DFP), as follows:

**Remark 2:** DFP describes the probability that the warden detects no transmitting activity during the transmission time of the data. Therefore, as shown in Fig. 3, DFP can be defined as a power function of DEP, where the power is the number of detections. Considering that the warden performs f detections per unit of time due to energy constraints, the number of detections can be calculated as the data amount divided by the covert rate and then multiplied by f.

Figure 4 illustrates the detection failure probability versus the ratio of the data volume of semantic information to that of the source message. We can observe that although the warden’s DEP is the same in both the SLoT and conventional IoT, that is, 90 percent as is set in much of the literature [11], a great gap exists in the achievable DFP. For example, if the semantic encoder can reduce the number of bits of the source message by half to obtain the semantic information, the DFP can be improved by 69 percent.

An interesting insight is that there is a trade-off between the semantic encoder computing resource and the physical layer transmit power resource. However, unlike the trade-off we discussed earlier, for the semantic encoder in the covert communication system, the information transmission time in SLoT is shorter than that in conventional communication systems, higher jamming power can be used. On the other hand, smart jamming power allocation schemes can be designed according to the transmitted semantic information.

**Encryption**

**Definition:** Encryption is one of the most classical techniques to ensure secure transmission, which operates in the upper layers of the communication system. For encryption techniques, there are comprehensive metrics for performance evaluation, including, but not limited to, crack time, the throughput of encryption/decryption, and power consumption. The crack time and the computational resources to be used by the eavesdropper are positively related to the key size.

**Encryption in SLoT Network:** In the SLoT, encryption techniques can be seen as a “second layer” of protection for the transmitted data. The reason is that the input of the encryption algorithm can be semantic information obtained through semantic coding, and semantic information itself has encryption properties. Even if the eavesdropper succeeds in breaking the encryption, it may not succeed in decoding the semantic information to obtain the source message, as we discussed above.
A general design is to integrate cryptography as an option with semantic communication systems [4]. In SIoT, if the transmitter and receiver want to hide the information from a potential eavesdropper, the goal is to minimize the error between the transmitter and receiver while maximizing the error between the transmitter and eavesdropper. Following this idea, an encrypted semantic communication system is designed in [4]. However, the authors in [4] only considered symmetric encryption, and related work is still in the early stage. Moreover, an interesting future research direction is to optimize the encryption schemes dynamically according to the semantic information of the data. Specifically, a more efficient and sophisticated encryption scheme can be used to protect more critical semantic information.

**New Security Issues**

In this section, we discuss the new security issues arising from the introduction of semantic communication techniques in the IoT.

**Semantic Attack in SIoT Network**

Unlike the bit streams transmitted in conventional IoT, the semantic information in SIoT is largely task-related and dependent on the design of the semantic encoder and decoder. However, a variety of error-correcting coding methods have been designed to correct bit errors; methods that can reduce semantic noise have rarely been investigated. Semantic noise in communication is defined as a type of disturbance caused by misunderstandings about the meaning of messages, which cause a mismatch between the source message and the obtained information by semantic encoding [5, 6].

The semantic noise can have a small or large impact on system performance. For example, because of the small deviation of the text semantic vectors, the receiver decodes “bike” into “bicycle” when recovering the text message. The receiver’s judgment will not be affected. However, the disturbance of some semantic information may seriously affect the communication system. For example, if the images are incorrectly semantic encoded and uploaded to a dataset, the quality of the artificial intelligence model trained by the dataset may be affected.

In the SIoT, some semantic noise is naturally present, for example, different users have different interpretations of the same word and require better semantic encoding and decoding design to overcome. However, some semantic noise is generated by attackers with the aim of disrupting the semantic communication system. For source messages in text form, synonym substitution or reversing the order of certain letters may cause the deep learning-based semantic model to misinterpret the semantics of the sentence. For source messages in image form, only by changing some pixels in an irrelevant image, the semantic information extracted by a well pre-trained semantic encoder can be completely inconsistent with the real content of the image [12]. Regardless of the modality of the source message, the goal of the semantic attack can vary and corresponds to different loss function optimization.

**Targeted Semantic Attack:** The goal is to generate semantic tampered source messages with a given target semantic information. Here, the target semantic information is the semantic information that the receiver in the SIoT wants to receive. For example, a digital twin service provider wants to collect some images with snowy mountain as semantic information to build a virtual object. The attacker can change some pixels in an irrelevant image to make the semantic information of the irrelevant image very close to snowy mountain. Therefore, the loss function could be the cosine similarity of the semantic vectors of the irrelevant pictures and the snowy mountain pictures. As shown in Fig. 5, as the number of iterations increases, the semantic similarity of the two images gradually increases. If the digital twin service provider cannot correctly detect the semantic tampered images, its database will be contaminated. Therefore, this type of attack can be called semantic data poisoning attack. Such a semantic tampering approach can also be used for man-in-the-middle attacks. A malicious intermediate node capable of intercepting the wireless communication channel can replace the images to be transmitted, without affecting the semantic information.

**Untargeted Semantic Attack:** Similar to the approach of the target semantic attack, but with a different objective function, the aim of the untargeted semantic attack is to minimize the similarity between the semantic information of the tampered source message and its true semantic information. In this case, the devices in the SIoT are unable to perform properly the semantic encoding of the maliciously tampered source message. For example, the semantic feature of the attack image in Fig. 5 is not iterating to be closer to the “snowy mountain,” but as far from the “baseball player” as possible.

**Defense Methods**

**Training-Based Defense:** By considering that a large part of the semantic communication encoders and decoders are functioned by deep learning methods, a feasible solution to reduce semantic noise is to improve the robustness of semantic models during the training process. Specifically, there have been some training-based methods,
for example, defensive distillation [13], weight perturbation [14], and adversarial training [15]. Although several approaches have been made to improve model robustness using adversarial samples in natural language and image processing [15], semantic noise-resistant models in wireless communication have not been sufficiently studied. Fortunately, researchers can draw inspiration from existing adversarial training methods and consider the impact of wireless transmission in the SIoT. Recently, to reduce the impact of semantic noise on the system, a masked vector quantized-variational autoencoder (VQ-VAE) is developed as the robust semantic communication system [5]. To improve the system robustness, a feature importance module is proposed to suppress noise-related and task-independent features. It is shown that the proposed masked VQ-VAE requires 0.36 percent transmitted symbols of the conventional “joint photographic experts group (JPEG) + low-density parity-check coding” method [5], while improving the system robustness by reducing the impacts of semantic noise. **Training-Free Defense:** Research on training-free defense methods remains to be developed. There are different defense methods for data with different modalities. Taking image data as an example, a possible defense solution is to use the visual invariance of the semantic tampered images for correct semantic extraction. As shown in Fig. 5, although the semantic similarity between the two images is high for a semantic encoder, the human eye can easily see the difference between them. The reason is that only some pixels in the attack image have been adjusted. Inspired by this, we try to blur both images by using Gaussian method, and find that the semantic similarity between them can be reduced from 0.987 to 0.78 without retraining the semantic model. As a future research direction, more pre-processing solutions could be investigated to defend against this kind of semantic attack.

**Future Direction**

**Explainable AI-Aided Semantic Communications**

The past few years have witnessed the rapid development of machine learning (ML) technologies, especially deep learning, which has shown significant advantages in various applications. Most of them, however, are often unable to explain their decisions and actions during the operation process, triggering the research on explainable artificial intelligence (XAI). The XAI aims to provide users with detailed explanations of how the decision is made or the result is obtained. For semantic communications, which rely on ML, the XAI can make the training of transceiver pairs change from black box to white box, making the training process clearer and easier to understand. Such an improvement allows semantic communication system designers to identify and fix potential vulnerabilities or threats and helps users understand and trust these semantic communications better. Therefore, studying explainable AI-aided semantic communications is indispensable to improving its security.

**Blockchain-Aided Semantic Internet of Things Network**

The blockchain is a chain of blocks that store all committed transactions in a decentralized and distributed network. Unlike the conventional ways, the blockchain realizes the peer-to-peer digital assets transfer without any intermediaries, and the features of decentralization, immutability, audit-ability, and transparency drive the transactions' security. Considering the above advantages, the stored and shared transaction information in the blockchain can be replaced with semantic information that needs to be transmitted. In this way, not only the storage consumption of the blockchain is reduced, but also, the decentralized blockchain verification mechanism would further improve the security of semantic content. Therefore, how to better integrate blockchain and the IoT is also worthy of further study.

**Secure Semantic Communications for Metaverse**

To provide an ideal immersive experience for users in Metaverse, the data that describes the user and physical world must be transmitted to the virtual world efficiently and accurately. Semantic communication is one of the best-suited techniques for this task. Considering the data characteristics and appl-
The Role of Physical Layer Security,” IEEE Commun. Stand. Mag., vol. 6, no. 1, Jan 2022, pp. 102–08.
[4] X. Luo et al., “Encrypted Semantic Communication Using Adversarial Training for Privacy Preserving,” arXiv preprint arXiv:2209.09008, 2022.
[5] Q. Hu et al., “Robust Semantic Communications With Masked VQ-VAE Enabled Codebook,” arXiv preprint arXiv:2204.01311, 2022.
[6] W. Yang et al., “Semantic Communications for Future Internet: Fundamentals, Applications, and Challenges,” IEEE Commun. Surveys Tuts., to appear, 2022.
[7] A. Muldharjee et al., “Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey,” IEEE Commun. Lett., vol. 11, no. 3, Mar. 2021, pp. 553–57.
[8] T.-X. Zheng et al., “Wireless Covert Communications Aided by Distributed Cooperative Jamming Over Slow Fading Channels,” IEEE Trans. Wireless Commun., vol. 20, no. 11, Nov. 2021, pp. 7026–39.
[9] C. Szegedy et al., “Intriguing Properties of Neural Networks,” Proc. Int’l Conf. Learn. Represent., 2014.
[10] N. Papernot et al., “Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks,” Proc. IEEE Symp. Secur. Priv., 2016, pp. 582–97.
[11] D. Wu, S.-T. Xia, and Y. Wang, “Adversarial Weight Perturbation Helps Robust Generalization,” Proc. Adv. Neural Inf. Process. Syst., vol. 33, 2020, pp. 2958–69.
[12] Y. Bai et al., “Improving Adversarial Robustness via Channel-Wise Activation Suppressing,” arXiv preprint arXiv:2103.08307, 2021.

**Biographies**

**HONGYANG DU** is working toward his Ph.D. at the School of Computer Science and Engineering, the Energy Research Institute @ NTU, Interdisciplinary Graduate Program, Nanyang Technological University, Singapore. His research interests include semantic communications, Metaverse, and communication theory.

**JIACHENG WANG** is a Research Associate in Computer Science and Engineering, at Nanyang Technological University, Singapore. Prior to that, he received his Ph.D. at the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China. His research interests include wireless sensing and semantic communications.

**DUSIT NIYATO** is a Professor at the School of Computer Science and Engineering, at Nanyang Technological University, Singapore. He received his Ph.D. in electrical and computer engineering from the University of Manitoba, Canada, in 2008. His research interests are in the areas of sustainability, edge intelligence, decentralized machine learning, and incentive mechanism design.

**JIAXING KANG** received his Ph.D. from the Guangdong University of Technology, China, in 2018. He has been a postdoc at Nanyang Technological University, Singapore from 2018 to 2021. He is currently a Full Professor at Guangdong University of Technology, China. His research interests focus on blockchain, security, and privacy protection.

**ZEHUI XIONG** is an Assistant Professor at Singapore University of Technology and Design, and an Honorary Adjunct Senior Research Scientist with Alibaba-NTU Singapore Joint Research Institute, Singapore. He received his Ph.D. at Nanyang Technological University (NTU), Singapore. His research interests include wireless communication, blockchain, edge intelligence, and Metaverse.

**MOHSIN GULZAN** is currently a Professor of Machine Learning and the Associate Provost at Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE. His research interests include applied machine learning, artificial intelligence, Internet of Things, smart city, and cybersecurity. He was elevated to the IEEE Fellow in 2009 and was listed as a Clarivate Analytics Highly Cited Researcher in Computer Science in 2019, 2020 and 2021.

**DONG IN KIM** received his Ph.D. in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1990. He is a Professor with the College of Information and Communication Engineering, Sungkyunkwan University, Suwon, South Korea. His research interests include Internet of Things, wireless power transfer, and connected intelligence.