Secure Transmission in Wireless Semantic Communications With Adversarial Training

Muhammed Yasinhan Yaşar
Computer Science
Ankara Yıldırım Beyazıt University
Ankara, Turkey
myyasar2001@gmail.com

***Abstract*—The Burgeoning technology of deep learning based semantic communications has significantly enhanced the efficiency and reliability of wireless communication systems by facilitating the transmission of semantic features. However, security threats, notably the interception of sensitive data, remain a sigfnificant challenge for secure communications. To safeguard the confidentiality of transmitted sematics and effectively counteract eavesdropping threats, this letter propose a secure deep learning-based semantic communication system, SecureDSC. It comprises semantic encoder/decoder, channel encoder/decoder, and encryption/decryption modules with a key processing network.**

***Index Terms*—Semantic communications, symmetric encryption, secure transmission**

I. Introduction

DEEP learning-based semantic communications have attracted much attention due to the focus on transmisson and interaction at the smeantic level [1]. Compared to traditional communication systems, sematic communications achieve higher transmission efficiency and lower bandwith with less susceptible to noise or other interference [2]. Nevertheless, the inherent openness and accessibility of wireless channels present a significant security risk to extracted semantic features transmitted in plaintext, enabling eavesdropping attacks and resulting in the disclosure of sensitive information. With the development of semantic communications, ensuring secure transmission is crucial for fostering trustworthy interactions within semantic communication systems and reliable evolution of wireless communication technologies.

Thanks for Muhammed Yasinhan Yaşar for their helps and contributions Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere.

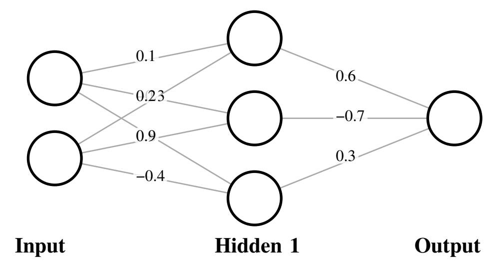

Fig. 1. The model of proposed secure text semantic communication system.

II. System Model

As shown in Fig. 1, Alice sends a message $\mathbf{m}$ to the legitimate receiver Bob, and both of them use the same shared session key $\mathbf{k}$ for encryption and decryption. The eavesdropping attacker Eve aims to reconstruct the original information communicated between legitimate users. As a black-box attacker, Eve lacks the knowledge of specific parameters used in the models employed by Alice and Bob. However, it can eavesdrop and analyze messages transmitted within the channel and leverage a large number of input-output pairs to invert the original network for private information.

Without loss of generality, we take the example of transmitting a text message i.e., $\mathbf{m} = [w_1, w_2, ..., w_L]$ where w_l denotes the l^{th} word in the sentence. At the sender end, the message passes through a semantic encoder to obtain a semantic feature $\mathbf{f}$, then $\mathbf{f}$ is input into a cipher encoder to generate ciphertext $\mathbf{c}$, and $\mathbf{c}$ is converted into asymbol stream $\mathbf{x}$ using a channel encoder, which is expressed as

$$\mathbf{x} = Ce_\gamma\big(En_\beta(Se_\alpha(\mathbf{m}), K_\kappa(\mathbf{k}))\big), \tag{1}$$

where $Se_\alpha(\cdot)$ is the semantic encoder network with parameter set $\boldsymbol{\alpha}$, $En_\beta(\cdot)$ is the encrypt network with parameter set β, $Ce_\gamma(\cdot)$ is the channel encoder network with parameter set γ and $K_\kappa(\cdot)$ is key processing network with parameter set κ.

References

[1] Z. Qin, X. Tao, J. Lu, W. Tong, and G. Y. Li, "Semantic Communications: Principles and Challenges." [Online]. Available: https://arxiv.org/abs/2201.01389

[2] H. Xie, Z. Qin, G. Y. Li, and B.-H. Juang, “Deep Learning Enabled Semantic Communication Systems,” *IEEE Transactions on Signal Processing*, vol. 69, no. , pp. 2663–2675, 2021, doi: 10.1109/TSP.2021.3071210.