# *SOS*: Dynamic Secure Code Offloading for Power Minimization in LEO Satellite Edge Computing

Jeongsoo Kim, Suhyeon Jeon, and Jeongho Kwak
Department of Electrical Engineering and Computer Science, DGIST, Korea
Email: jeongsoo98@dgist.ac.kr, jsh6327@dgist.ac.kr, jeongho.kwak@dgist.ac.kr

***Abstract*—The satellite edge computing (SEC) has recently received considerable attention thanks to its wide area service around the world. However, this also creates a risk of exposing private user data to eavesdroppers. Physical layer security can help prevent this, yet it requires extra usage of network resources. Hence, efficient management of these resources is essential for saving power and ensuring secure code offloading. Moreover, from the perspective of mobile devices that request services, the level of security demands is quite different for various services, yet current studies have not fully considered this aspect. In this paper, we propose a secure code offloading framework for an SEC system with a jamming strategy in the existence of eavesdropping satellite. We formulate an average power minimization problem of an LEO satellite, a gateway, and a mobile device while ensuring security and the stability of queues. This includes making decisions of code offloading, computing/network resource allocation, and jamming unit selection. As a solution of this problem, we propose an SOS algorithm by invoking stochastic optimization theory. Finally, via extensive simulations, we demonstrate that the proposed SOS algorithm can save up to 60% of average power compared to existing algorithms while maintaining the same delay and zero leakage of information toward eavesdropper.**

## I. Introduction

Recently, as many applications requiring high processing capability have emerged, the burden on the limited resources of mobile devices is increasing. To address the computing capability problem of mobile devices, mobile edge computing (MEC) technology can play an essential role by leasing the abundant resources of MEC servers to mobile devices via code offloading [1], [2]. However, there are limitations in fully exploiting MEC offloading when the communication infrastructure is inferior due to low population density or physical constraints (e.g., sea, air, and desert). Therefore, satellite edge computing (SEC) technology, which offloads workloads to satellites, has a lot of attention from industry and academia.

Moreover, recently, the commercial internet service market utilizing satellites has been rapidly growing [3]. This remarkable growth will lead to improvement of computing capability of satellite onboard processors which, in turn, enables general usage of SEC technology [4]. Especially in SEC, due to the high mobility property of satellites, which move quickly along a preset orbit, and weather attenuation, dynamic code offloading should be considered under extremely time-varying wireless channels [5]–[7].

Meanwhile, edge computing technology always has the possibility of eavesdropping due to the broadcasting nature of transmitting raw data from mobile devices via wireless channels. In particular, since satellite communication has broader coverage and higher accessibility, the threat of eavesdropping by potential eavesdroppers would be higher than terrestrial communication. The concept of secrecy capacity was introduced to cope with the threat of eavesdropping. According to Wyner *et al.* [8], the difference between the channel capacity of receiver and the channel capacity of the eavesdropper is defined as the secrecy capacity that can transmit data without information leakage. Based on this secrecy capacity theory, many studies about secure code offloading were conducted to minimize information leakage and maximize secrecy capacity by modeling service channels and wiretapping channels in terrestrial communication [9], [10].

However, most existing secure code offloading studies have only considered potential eavesdroppers of ground in the terrestrial code offloading environment. Whereas, in a satellite code offloading environment, the potential eavesdroppers can exist not only on the ground but also in air (e.g., UAVs) and space (e.g., satellites) [11]. Furthermore, as the cost burden for launching satellites has reduced significantly, launching a satellite for eavesdropping becomes easier. Eavesdropping satellite moves with a constant speed along a predetermined orbit and can be located at various altitudes. If the eavesdropping satellite is at the same angle with the serving satellite or the altitude of the eavesdropping satellite is lower, then the threat of eavesdropping increases due to the matched antenna angle. In this case, the jamming signal can deteriorate the channel capacity of the eavesdropper by sending an interference signal to the eavesdropper, but needs an additional jamming power [10]–[12]. Hence, it is crucial to efficiently optimize jamming signal transmission.

Existing studies of secure code offloading in an SEC environment modeled secrecy capacity in static systems (i.e., wireless channels are fixed) and proposed algorithms aimed to maximize the secrecy capacity [9], [11]. Moreover, these studies assumed homogeneous service model regardless of different security requirement of different services. However, in real-world scenarios, different services would require different levels of security. For example, according to the *AppStore* and

This work was supported by Korea Research Institute for defense Technology planning and advancement (KRIT) grant funded by the Korea government (DAPA (Defense Acquisition Program Administration)) (KRIT-CT-22-040, Heterogeneous Satellite constellation based ISR Research Center, 2022).

ISBN 978-3-903176-65-2 © 2024 IFIP