위성 엣지 컴퓨팅 환경에서의 안전한 오프로딩 프레임워크 제안

김정수, 전수현, 곽정호
대구경북과학기술원

jeongsoo98@dgist.ac.kr, jsh6327@dgist.ac.kr, jeongho.kwak@dgist.ac.kr

Secure Task Offloading Framework for Satellite Edge Computing System

Kim Jeongsoo, Jeon Suhyeon, Kwak Jeongho
DGIST

요 약

본 논문은 위성 엣지 컴퓨팅 환경에서 오프로딩 데이터의 도청 위협을 고려하여 보안 성능이 낮을 때 재밍 신호를 통해 보안 성능을 향상시키는 효율적인 오프로딩기법을 제안한다. 도청 위성이 존재할 때, 지상 터미널에서 서비스 위성으로 오프로딩하는 상황을 고려하며 이 때 지상 유저와 위성의 큐를 안정화 하면서 전체 시스템의 에너지 사용량을 최소화하는 것을 목표로 한다.

Ⅰ. 서 론

최근 높은 계산능력을 요구하는 어플리케이션이 많이 출시되고 있으나 현재의 모바일 단말의 자원만으로 이를 처리하기에 힘든 부분이 있다. 이러한 문제는 모바일 엣지 컴퓨팅 기술을 통해 풍부한 엣지 서버의 자원을 사용하여 해결할 수 있다. 하지만 낮은 인구 밀도 혹은 물리적 제약으로 인해 통신 인프라를 갖추지 못한 경우 모바일 엣지 컴퓨팅 기술을 이용하는 데에 제한이 있다. 이 경우 위성으로 오프로딩을 하는 위성 엣지 컴퓨팅 기술을 사용하는 것이 해결책이 될 수 있다.

일정한 궤도를 따라 지구를 도는 위성의 특성에 따라, 위성 통신은 끊김 없는 서비스를 제공할 수 있다. 또한, 높은 위성의 고도로 인해 넓은 서비스 범위를 가진다. 최근 위성의 온보드 프로세서의 성능이 증가함에 따라 위성을 활용한 인터넷 서비스가 상용화 되면서 위성이 엣지 서버의 역할을 대신하는 위성 엣지 컴퓨팅 기술을 고려할 수 있게 되었다. 하지만 유저의 데이터를 무선채널을 통해 그대로 전송하는 오프로딩의 특성에 의해 도청 가능성이 항상 존재한다. 특히, 낮은 고도에 도청 위성이 존재할 때, 도청 가능성이 높아진다.

정보이론을 바탕으로, 물리계층 보안 방식은 위성의 채널용량과 도청자의 채널용량의 차를 보안용량으로 정의하고 보안용량만큼의 데이터를 정보유출 없이 전송할 수 있다 [1]. 도청 위성이 서비스 위성 가까이 있을 때, 보안용량이 감소하여 유저가 원하는 서비스를 제공할 수 없다. 이러한 문제를 해결하기 위해서 서비스 위성에서 재밍신호를 전송하여 도청 위성에 간섭을 발생시켜 보안용량을 향상시킬 수 있다. 기존의 위성 엣지 컴퓨팅 환경에서 안전한 오프로딩을 고려한 연구는 정적인 시스템에서 보안용량의 최소값을 만족하기 위한 방법을 제안한 연구가 있다 [2]. 하지만 잠재적인 도청자의 위치를 고려하지 않았고, 위성의 이동에 따른 동적인 채널 변화를 반영하지 못하여 장기간 관점으로 봤을 때 에너지를 비효율적으로 사용하는 문제점이 있다.

본 논문에서는 잠재적인 도청 위성이 존재할 때, 유저와 위성의 큐를 모델링 하고 두 큐의 안정성을 보장하면서 장기간 관점에서 전체 시스템 에너지를 최소화하는 실시간 안전한 오프로딩 기술을 제안한다. 이 때 위성의 이동에 따른 채널 상태 변화와 보안용량 및 큐 상태를 고려한다. 이를 위해 유저와 위성의 CPU 연산 에너지와 재밍신호 에너지 및 지상의 전송 에너지를 조절하여 전체 시스템 에너지를 최소화하는 최적화 문제를 설계한다.

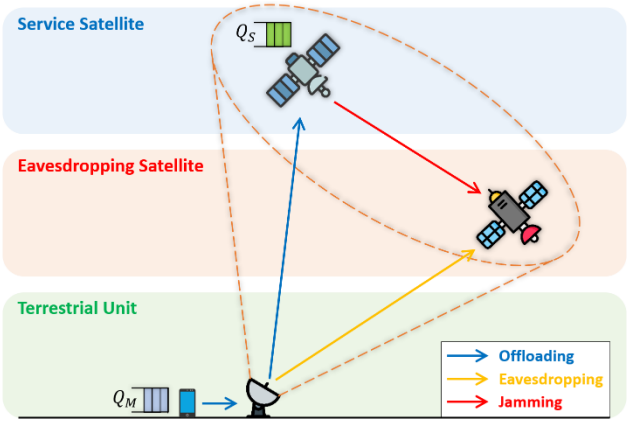

그림 1. 물리 계층 보안 기술을 적용한 위성 엣지 컴퓨팅 시스템.

Ⅱ. 본론

그림 1 은 도청 위성이 존재하는 상황에서 지상에서 위성으로 오프로딩할 때 서비스 위성이 재밍 신호를 전송하여 보안용량을 향상시키는 안전한 오프로딩

시스템을 보여준다. 한명의 유저와 하나의 서비스 위성, 도청 위성, 지상 터미널을 고려하고, 지상 터미널은 유저에게 받은 데이터를 그대로 서비스 위성에 전송하는 역할을 수행한다. 서비스 위성, 도청 위성의 수신 신호 대 간섭 및 잡음 비(SINR) $SINR_{us}, SINR_{ue}$은 아래와 같다.

$$SINR_{us} = \frac{\alpha^2 h_{us}^2(t) l_{us}(t) P_u(t)}{\rho P_J(t) + B\sigma_s^2}, \quad (1)$$

$$SINR_{ue} = \frac{\alpha^2 h_{ue}^2(t) l_{ue}(t) P_u(t)}{h_{se}^2(t) l_{se}(t) P_J(t) + B\sigma_e^2}, \quad (2)$$

이 때, B는 사용가능한 대역폭, l은 경로 손실 함수, P_u는 전송 파워, α^2 는 날씨 감쇠를 나타낸다. 또한, ρ 는 전이중 통신(Full Duplex)방식에 의해 발생하는 자기 간섭의 제거성능을 나타낸다. h_{us}, h_{ue}, h_{se} 는 각각 터미널과 서비스 위성, 터미널과 도청 위성, 서비스 위성과 도청 위성 사이의 채널 이득을 나타내며 Nakagami-m fading 을 따른다 [3]. 따라서, 식 (1),(2)를 통해 채널용량 C_{us}, C_{ue}를 구할 수 있다.

$$C_{us} = B\log_2\left(1 + \frac{\alpha^2 h_{us}^2(t) l_{us}(t) P_u(t)}{\rho P_J(t) + B\sigma_s^2}\right), \quad (4)$$

$$C_{ue} = B\log_2\left(1 + \frac{\alpha^2 h_{ue}^2(t) l_{ue}(t) P_u(t)}{h_{se}^2(t) l_{se}(t) P_J(t) + B\sigma_e^2}\right), \quad (5)$$

또한, 두 채널용량의 차이를 통해 보안용량 C_{sec}를 구할 수 있다.

$$C_{sec} = C_{us} - C_{ue}, \quad (6)$$

위성의 이동에 따른 채널 상태와 유저의 서비스 요구가 동적으로 변하기 때문에, 다음 타임슬랏에서의 위성과 유저의 큐인 Q_S, Q_M을 설계하면 아래와 같다.

$$Q_S(t+1) = \left[Q_S(t) - \frac{8f_s(t)}{\gamma} + \phi_o(t) C_{sec}(t)\right]^+, \quad (7)$$

$$Q_M(t+1) = \left[Q_M(t) - \phi_o(t) C_{sec}(t) - (1-\phi_o(t))\frac{f_m(t)}{\gamma} + A_M\right]^+, \quad (8)$$

이 때, f_s, f_m은 위성과 모바일 CPU 의 1 초당 사이클 수를 나타내고, γ 는 한 비트를 처리할 때 필요한 CPU 사이클 수를 나타낸다. 또한, ϕ_o는 유저의 오프로딩 여부를 결정하는 결정계수이고, 식 (8)의 입력 A_M 은 독립적이고 같은 확률 분포를 따르며. 이를 통해, 큐 안정화를 만족하면서 안전한 오프로딩을 위한 장기간 시스템 에너지 소모 최소화 문제는 아래와 같이 설계할 수 있다.

$$\min_{\{f_s, f_m, P_u, P_J, \phi_o\}} \lim_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \mathbb{E}\left[P_m(t) + P_s(t)\right], \quad (9)$$

$$s.t. \lim_{t\to\infty} \frac{1}{t}\sum_{\tau=1}^{t-1} \mathbb{E}\left[Q_M(\tau)\right] < \infty, \quad (9a)$$

$$\lim_{t\to\infty} \frac{1}{t}\sum_{\tau=1}^{t-1} \mathbb{E}\left[Q_S(\tau)\right] < \infty, \quad (9b)$$

P_m 은 모바일에서 연산 파워와 오프로딩전송 파워의 합이고, P_s 는 위성 연산 파워와 재밍 파워의 합을 나타내며 식 (9a),(9b)는 각 큐에 들어온 입력을 유한시간 내에 처리할 수 있음을 의미한다.

Ⅲ. 결론

본논문에서는 위성 엣지 컴퓨팅 환경에서 발생할 수 있는 도청 위협에 대해 안전한 오프로딩기술을 제안한다. 모바일 단말과 서비스 위성에 큐를 모델링하고 동적인 채널 환경을 고려하여 실시간 안전한 오프로딩 정책 결정 문제를 설계하였다.

.

ACKNOWLEDGMENT

이 논문은 2024 년도 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임 (KRIT-CT-22-040, 이종 위성군 우주 감시정찰 기술 특화연구센터)

참 고 문 헌

[1] Wyner, Aaron D. "The wire-tap channel." Bell system technical journal 54.8 (1975): 1355-1387.

[2] Wang, Dawei, et al. "Double-edge Computation Offloading for Secure Integrated Space-air-aqua Networks." IEEE Internet of Things Journal (2023).

[3] Zhang, Haoxing, et al. "On Secure Uplink Transmissions in Satellite-Aerial Systems." IEEE Transactions on Aerospace and Electronic Systems (2022).