위성 엣지 컴퓨팅 환경에서의 안전한 코드 오프로딩 기법

김정수, 전수현, 곽정호
대구경북과학기술원

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

Secure Code Offloading for Satellite Edge Computing System

Jeongsoo Kim, Suhyeon Jeon, Jeongho Kwak
DGIST

요 약

본 논문은 위성 엣지 컴퓨팅 환경에서 잠재적 도청 위성을 고려하여 에너지 효율적인 안전한 오프로딩 기법을 제안한다. 지상 게이트웨이에서 서비스 위성으로 오프로딩하는 상황을 고려하며 이 때 보안에 사용하는 에너지를 효율적으로 사용하기 위해 모바일 단말에 들어오는 작업의 종류를 보안이 필요한 작업과 그렇지 않은 작업으로 구분하였고 동적 전압 주파수 스케일링 기술을 적용하였다. 이 때, 지상 사용자 와 서비스 위성의 대기열 안정화를 보장하면서 안전한 오프로딩에 사용하는 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. 이 때, 지상 통신과 다르게 일정한 궤도를 따라 빠르게 이동하는 위성의 특성에 따라 동적인 채널을 고려한 동적 코드 오프로딩 기술이 필요하다.

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 모바일 단말의 데이터를 무선채널을 통해 그대로 전송하는 오프로딩의 특성에 의해 도청 가능성이 항상 존재한다. 대부분의 기존 연구에서 지상의 잠재적 도청자를 고려했지만 위성의 수가 빠르게 늘어나면서 잠재적 도청 위성에 대한 고려가 필요하다.

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 있거나 도청 위성의 고도가 낮을 때, 보안용량이 감소하여 사용자가 원하는 서비스를 제공할 수 없다. 이러한 문제를 해결하기 위해서 재밍신호를 통해 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 위성의 이동에 따른 동적인 채널 변화를 반영하지 못하는 문제가 있다. 또한 보안이 필요한 작업과 그렇지 않은 작업이 있는데 모든 작업에 대해 보안을 고려하는 것은 에너지를 비효율적으로 사용하는 것이다.

본 논문에서는 잠재적인 도청 위성이 존재할 때, 모바일 단말과 서비스 위성의 보안 작업 대기열, 비 보안 작업 대기열을 모델링하고 각 대기열의 안정성을 보장하면서 장기간 관점에서 전체 시스템 에너지를 최소화하는 안전한 동적 오프로딩 기술을 제안한다. 이를 위해 타임슬랏마다 오프로딩 정책을 결정하고 모바일 단말과 서비스 위성의 CPU 연산 에너지와 재밍 신호 에너지 및 게이트웨이의 전송 에너지를 조절하여 전체 시스템 에너지를 최소화하는 기법을 제안한다.

Ⅱ. 본론

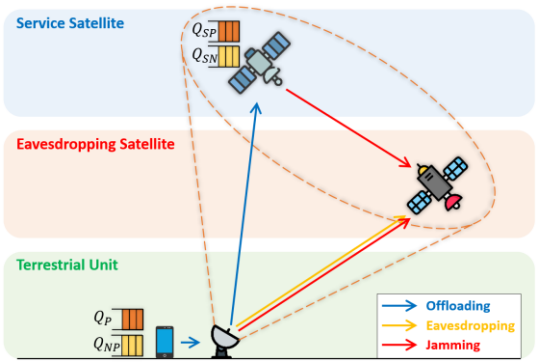

그림 1. 안전한 위성 엣지 컴퓨팅 시스템

그림 1 은 도청 위성이 존재하는 상황에 지상 게이트웨이에서 서비스 위성으로 오프로딩할 때 서비스

위성 혹은 게이트웨이에서 재밍 신호를 보내는 상황을 보여준다. 모바일 단말, 게이트웨이, 서비스 위성, 도청 위성을 각각 하나씩 고려하고, 지상 게이트웨이는 모바일 단말에게 받은 데이터를 그대로 서비스 위성에 전송하는 역할을 수행한다. 서비스 위성과 도청 위성의 수신 신호 대 간섭 및 잡음 비(SINR) $SINR_{us}, SINR_{ue}$은 아래와 같다.

$$SINR_{us}(t) = \frac{|h_{us}^H(t)w(t)|^2}{\rho\phi_J(t)h_{se}^H(t)n_J(t) + B\sigma_s^2}, \quad (1)$$

$$SINR_{ue}(t) = \frac{|h_{us}^H(t)w(t)|^2}{(\phi_J(t)h_{se}^H(t) + (1-\phi_J(t))h_{ue}^H(t))n_J(t) + B\sigma_e^2}, \quad (2)$$

이 때, B는 사용가능한 대역폭, w는 빔포밍 가중치, ρ는 전이중 통신(Full Duplex)방식에 의해 발생하는 자기 간섭의 제거성능을 나타낸다. 또한, ϕ_J 는 재밍 신호 생성 장치 선택을 나타낸다. h_{us}, h_{ue}, h_{se} 는 각각 게이트웨이와 서비스 위성, 게이트웨이와 도청 위성, 서비스 위성과 도청 위성 사이의 채널 이득을 나타내며 Nakagami-m fading 을 따른다. 식(1),(2)를 통해 채널용량 C_{us}, C_{ue}를 구할 수 있다:

$$C_{us}(t) = B\log_2(1 + SINR_{us}), \quad (3)$$

$$C_{ue}(t) = B\log_2(1 + SINR_{ue}), \quad (4)$$

또한, 두 채널 용량의 차이를 통해 보안용량 C_{sec} 를 구할 수 있다:

$$C_{sec}(t) = C_{us}(t) - C_{ue}(t). \quad (5)$$

위성의 이동에 따른 채널 상태와 모바일 단말의 서비스 요구의 동적인 특성으로 인해 위성과 모바일 단말의 보안 대기열과 비 보안 대기열 Q_P, Q_{NP}, Q_{SP}, Q_{SN}은 아래와 같이 설계된다:

$$Q_P(t+1) = \left[Q_P(t) - \phi_P(t)\theta_o(t)C_{SEC}(t) - (1-\phi_P(t))\theta_l(t)\frac{f_m(t)}{\gamma} + A_P(t)\right]^+, \quad (6)$$

$$Q_{NP}(t+1) = \left[Q_{NP}(t) - \phi_{NP}(t)\left((1-\theta_o(t))C_{SEC}(t) + C_{ue}(t)\right) - (1-\phi_{NP}(t))(1-\theta_l(t))\frac{f_m(t)}{\gamma} + A_{NP}(t)\right]^+, \quad (7)$$

$$Q_{SP}(t+1) = \left[Q_{SP}(t) - \theta_s(t)\frac{zf_s(t)}{\gamma} + \phi_P(t)\theta_o(t)C_{SEC}(t)\right]^+, \quad (8)$$

$$Q_{SN}(t+1) = \left[Q_{SN}(t) - (1-\theta_s(t))\frac{zf_s(t)}{\gamma} + \phi_{NP}(t)\left((1-\theta_o(t))C_{SEC}(t) + C_{ue}(t)\right)\right]^+, \quad (9)$$

이 때, f_m, f_s 는 모바일 단말과 서비스 위성의 모바일 CPU 의 1 초당 사이클 수를 나타내고, γ는 한 비트를 처리할 때 필요한 CPU 사이클 수를 나타낸다. 또한, ϕ_P, ϕ_{NP} 는 모바일 단말의 보안/비보안 대기열의 오프로딩 여부를 결정하는 결정계수이고, $\theta_l, \theta_o, \theta_s$는 보안 작업의 모바일 단말 처리, 오프로딩, 위성 처리 비율을 나타낸다. 식 (6), (7) 의 입력A_P, A_{NP}는 독립적이고 같은 확률 분포(i.i.d.)를 따르며. 이를 통해, 대기열 안정화를 만족하면서 안전한 오프로딩을 위한 장기간 시스템 에너지 소모 최소화 문제는 아래와 같이 설계할 수 있다.

$$\min_{\{f_s, f_m, P_u, P_J, \phi_P, \phi_{NP}, \phi_J\}} \lim_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\mathbb{E}\left[P_m(t) + \delta P_n(t) + \omega P_s(t)\right], \quad (10)$$

$$s.t. \lim_{t\to\infty}\frac{1}{t}\sum_{\tau=1}^{t-1}\mathbb{E}\left[Q_P(\tau)\right] < \infty, \quad (10a)$$

$$\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=1}^{t-1}\mathbb{E}\left[Q_{NP}(\tau)\right] < \infty, \quad (10b)$$

$$\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=1}^{t-1}\mathbb{E}\left[Q_{SP}(\tau)\right] < \infty, \quad (10c)$$

$$\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=1}^{t-1}\mathbb{E}\left[Q_{SN}(\tau)\right] < \infty, \quad (10d)$$

P_m 은 모바일에서 연산 파워와 전송 파워의 합이고, P_n은 게이트웨이의 전송 파워를 나타내며,P_s는 위성 연산 파워와 재밍 파워의 합을 나타내며 식 $(10a), (10b), (10c), (10d)$는 각 대기열에 들어온 입력을 유한시간 내에 처리할 수 있음을 의미한다.

위의 문제를 리아푸노프 최적화 식을 유도한 뒤 보안 대기열, 비 보안 대기열의 오프로딩 정책 변수를 대입한 뒤 그 중에서 최소 값을 가지는 정책을 선택하고 해당 정책에서 동적 전압 주파수 스케일링 기술을 적용해 문제를 해결하였다.

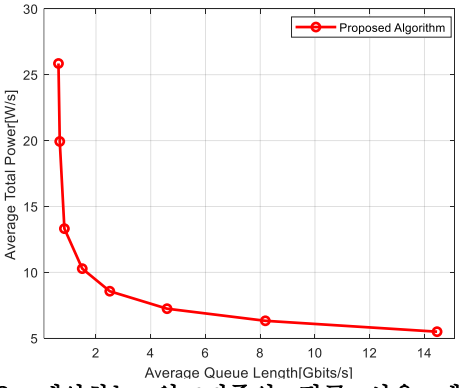

그림 2. 제안하는 알고리즘의 평균 사용 에너지와 평균 처리시간의 관계

그림 2 에서 제안하는 알고리즘이 평균 에너지 사용량과 평균 처리 시간 사이에 트레이드오프 관계가 있음을 알 수 있다. 평균 처리 시간이 작을 때는 약간의 시간 지연을 통해 많은 에너지를 아낄 수 있고, 반대로 평균 에너지 사용량이 작은 경우 약간의 에너지 사용을 통해 큰 평균 처리 시간 감소를 달성할 수 있다. 이에 따라 트레이드오프 변수를 조절하여 사용자의 요구사항에 맞게 자원할당을 할 수 있다.

Ⅲ. 결론

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

.

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).