(초)소형 국방 위성 통신 보안 및 신뢰성 향상 기법

김정수[1], 전수현[1], 이승현[2], 조현준[2], 염현식[2], 곽정호[1*], 하정석[2]

대구경북과학기술원[1], 한국과학기술원[2]

Enhancement of Communication Security and Reliability for (Ultra) Small Satellite Systems

Jeongsoo Kim[1], Suhyun Jeon[1], Seunghyun Lee[2], Hyunjun Joe[2], Hyeonsik Yeom[2], Jeongho Kwak[1*], and Jeongseok Ha[2]

Key Words : Communication security, Satellite edge computing, On-board processor, Communication reliability

서 론

본 연구팀은 (초)소형 국방 위성 통신 보안 및 신뢰성 향상 기법에 대한 연구를 진행하였고, 본 논문에서 해당 연구에 대한 결과를 소개한다. 구체적으로, 데이터 전송을 위한 암호화 및 물리계층보안 기법을 적용한 위성망 보안 기술연구와 저궤도 위성 엣지컴퓨팅 환경에서 보안성을 고려한 코드 오프로딩 기술 연구를 소개한다. 또한, AoI (Age of Information)을 최소화하기 위한 저궤도 위성통신기법에 대해 소개하고, OTFS (Orthogonal Time Frequency Space) 기반의 보안 저궤도 위성통신 기법에 대해 소개한다.

본 론

1. 국방 기밀 데이터 전송을 위한 암호화 및 물리계층보안 기법을 적용한 위성망 보안 기술

위성에서의 온보드 프로세서 (Onboard Processor)는 낮은 처리지연과 높은 전송속도를 보장하기 위해서 필수적이다. 하지만 위성 신호는 Broadcasting 특성으로 인해 도청에 매우 취약한 특성을 지니고 있다. 이러한 도청 위협을 해결하기 위해서 지금까지는 물리계층 보안 (PLS, Physical Layer Security)과 암호기술이 각각 독립적으로 개발되어 왔다. 하지만 전력 사용이 제한된 저궤도 위성에서 이러한 각 기술의 독립적인 사용은 추가적인 보안 비용과 PLS가 도청자의 성능에 의존함으로 인해서 자원 효율성과 보안성능의 트레이드-오프 이슈를 불러일으킨다. 본 연구에서는 다중빔을 사용하는 위성 네트워크 시스템에서 이러한 물리계층 보안과 암호기술을 통합한 통합 보안 프레임워크를 제안함으로써 자원효율성과 보안성능을 동시에 향상시킬 수 있음을 보인다. 또한, 온보드 프로세서의 전력사용을 분석하여 패킷 전송전력과 컴퓨팅 전력을 통합적으로 모델링하고 이를 효율적으로 사용하는 알고리즘을 제안하였다. 이를 위해 NOMA (Non Orthogonal Multiple Access) 시스템에서 공동 온보드 전력 할당, 빔 스케줄링과 보안 알고리즘을 결정하는 문제를 만들고, 이를 해결하는 준최적 알고리즘을 제안하였다.

2. 저궤도 위성 엣지컴퓨팅 환경에서 보안성을 고려한 코드 오프로딩 기술

최근 많은 모바일 어플리케이션들이 컴퓨팅 자원을 많이 요구함에 따라 지상에서의 엣지컴퓨팅 자원을 활용한 기술이 많이 개발되고 있다. 미래에 위성인터넷을 더욱 광범위하게 사용하게 되면, 저궤도 위성의 향상된 온보드 프로세서의 성능을 더욱 적극적으로 활용하는 엣지컴퓨팅 기술이 많은 주목을 받게 될 수 있다. 본 연구에서는 지상 단말이 프로세싱이 필요한 워크로드가 있을 때, 지상 단말 자체에서 워크로드를 처리하거나, 해당 워크로드를 단말 위에 떠있는 위성에 오프로딩하여 위성의 온보드 프로세서에서 처리하도록 하는 프레임워크를 고려하였다. 이 때, 지상 단말의 워크로드를 오프로딩 하는 상황에서 다른 위성이 해당 워크로드를 도청한다면, 위성망 환경에서 큰 피해가 갈 수 있기 때문에 도청 위성을 고려한 재밍신호 (Jamming Signal) 기반의 코드 오프로딩 알고리즘을 개발하는 연구를 제안하였다. 본 연구에서는 보안 신호와 비보안 신호를 나눔으로써 자원효율성을 향상시키는 아이디어를 적용하였다.

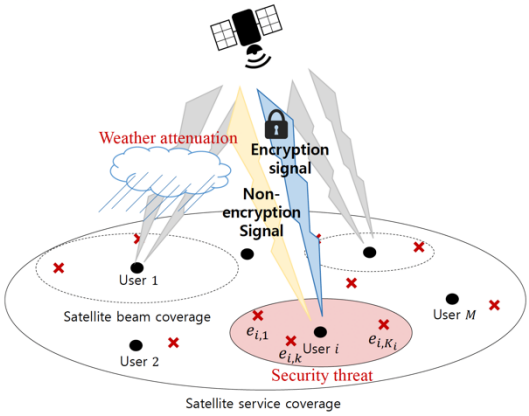

Fig. 1 Multibeam satellite system

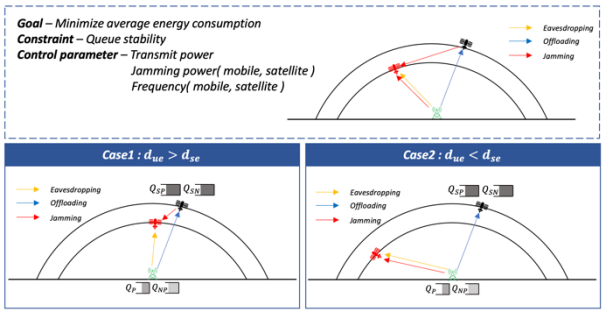

Fig. 2 Secure Code Offloading

3. AoI 최소화를 위한 저궤도 위성통신기법

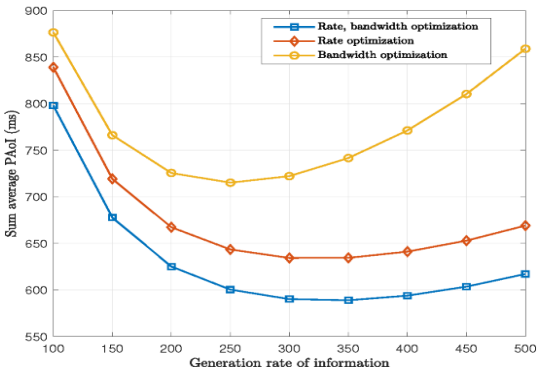

Fig. 3 Sum average PAoI with and without optimization of optimization variables

본 연구에서는 물리계층 보안 기법 연구를 위한 선행 연구로 도청자가 없는 상향링크 저궤도 위성 통신 환경에서 다수의 단말 간 각기 다른 전파지연, 전송지연을 고려한 평균 PAoI (Peak Age of Information)를 정보 처리 방식 및 통신 요소들에 대해 분석하였고, 이를 바탕으로 평균 PAoI를 최소화하기 위한 최적화 알고리즘을 제안하였다. Fig. 3은 최적화 기법 사용 유무와 정보의 생성율 (Generation rate of Information)에 따른 평균 PAoI를 나타낸 것으로, 제안한 최적화 기법을 사용하면 평균 PAoI를 획기적으로 경감시킴을 확인할 수 있다.

4. OTFS 기반의 보안 저궤도 위성통신 기법

현재 OTFS 기반의 저궤도 위성통신 시스템에 관한 많은 연구가 진행되어 왔지만, 물리계층보안에 대한 연구는 상대적으로 많이 진행되지 않았다. 본 연구에서는 AFF (Artificial Fast Fading)을 활용하여 OTFS 기반 보안 저궤도 위성 통신 성능을 향상시키는 기법을 제안하였다. AFF 기법은 적법 사용자의 채널 정보를 사용한 빔 형성 기법을 통해 적법 사용자에게는 deterministic한 유효채널을, 도청자에게는 임의의 유효채널을 형성하는 방식으로, 적법 사용자에게는 임의성이 사라지지만 도청자에게는 임의성이 존재하게 되어 보안 성능을 향상시키는 기법이다.

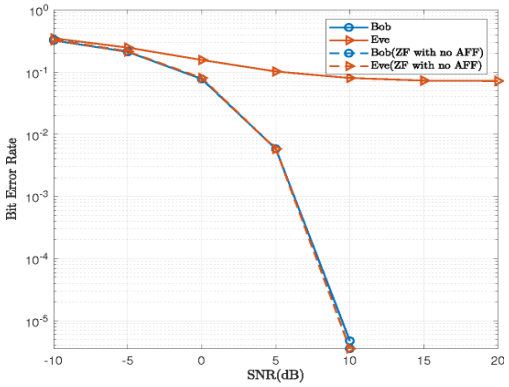

Fig. 4 BER between Bob and Eve

후 기

본 논문에서는 초소형 국방 위성의 통신보안 및 신뢰성을 향상하기 위한 네가지 기술들을 소개하였다. 앞으로 저궤도 위성에서의 통신보안 및 컴퓨팅보안이 점점 더 중요해지는 상황에서 본 논문에서 제안한 네가지 보안기술들이 실제 저궤도 위성에 적용되는 날을 기대해 본다. (이 논문은 2022년도 정부(방위산업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임 (KRIT-CT-22-040, 이종 위성군 우주 감시정찰 기술 특화연구센터)

참고문헌

1) M. Costa, M. Codreanu and A. Ephremides, "On the Age of Information in Status Update Systems With Packet Management," in IEEE Transactions on Information Theory, vol. 62, no. 4, pp. 1897-1910, April 2016