위성 통신 보안을 위한 온보드 전송 및 계산 전력 최적화

전수현, 곽정호, 최지환*
대구경북과학기술원, *한국과학기술원

jsh6327@dgist.ac.kr, jeongho.kwak@dgist.ac.kr, *jhch@kaist.ac.kr

Onboard Transmission and Computation Power Optimization for Satellite Communication Security

Jeon Suhyeon, Kwak Jeongho, Choi Jihwan*
DGIST, *KAIST

요 약

본 논문은 다수의 도청자가 존재할 수 있는 위성 통신 환경에서 전송 및 컴퓨팅 파워를 동시에 고려한 위성 통신 보안 기법을 제안한다. 도청자 수를 바탕으로 한 보안 위협을 활용하여 위성의 온보드 전력을 비암호화 및 암호화 신호와 암호화 계산에 분배한다. 두 신호의 동시 전송을 위해서 비직교 다중접속 기술을 활용하여 보안 위협이 높아질수록 기존의 물리 계층 보안 기술보다 향상된 보안 성능을 달성한다.

Ⅰ. 서 론

저궤도 군집 위성을 활용한 인터넷 서비스가 상용화되면서 위성 통신의 수요가 높아지고 있다. 이러한 군집 위성은 감시/정찰과 음영지역 지원 등의 다양한 목적에 활용될 것으로 예상되며, 이는 복잡한 프로토콜의 활용을 초래한다. 또한, 신호의 브로드케스팅 특성에 의해, 위성은 재밍과 같은 보안 공격에 취약하고[1], 이에 따라 위성 통신 시스템에 향상된 보안 기술이 요구된다.

위성의 보안 기술로는 물리 계층 보안 기술과 암호화 기술이 서로 독립적으로 개발되어 왔다. 하지만, 전력 제한적인 위성 통신 시스템에서 두 기술 중 하나의 기술만 활용하는 것은 비효율적이다. 먼저, 암호화 활용으로 인해 발생하는 추가적인 계산 비용은 위성의 성능을 떨어뜨리는 요인이 된다. 대표적인 advanced encryption standard (AES) 암호화를 위해서 전송파워와 비교될 만한 큰 전력을 소모한다. 또한, 물리 계층 보안 기술을 사용하기 위한 도청자의 채널 정보 획득이 어렵다. 따라서, 본 논문에서는 암호화 신호와 비암호화 신호를 활용한 위성 통신 보안 기술을 제안한다. 이때, 위성의 온보드 전력을 암호화 및 비암호화 신호 전송과 암호화 및 메시지 인증 코드 계산에 대한 전력으로 분배한다. 위성이 전송하는 암호문에 대한 무결성을 제공하기 위해서 암호문과 메시지 인증 코드를 함께 전송한다. 두 신호를 중첩하여 한 유저에게 전송하기 위해서 비직교 다중접속 기술을 사용하고 두 신호의 채널 용량을 최대화하고 보안 알고리즘을 선택하는 공동 최적화 문제를 설계한다. 시뮬레이션을 통해 도청자가 많은 환경에서 제안된 기술이 기존의 물리 계층 보안 기술보다 높은 보안 성능을 제공함을 보인다.

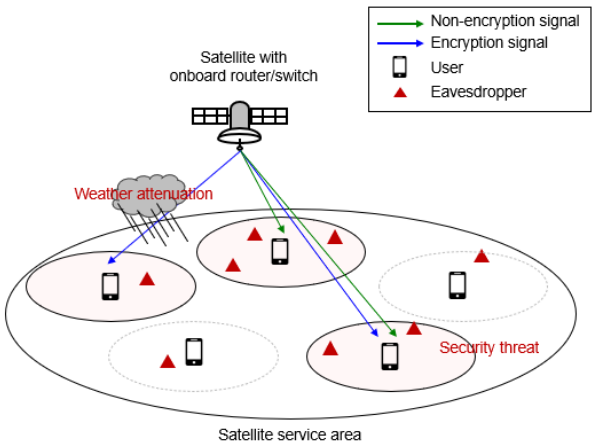

그림 1. 암호화 및 비암호화 신호 전송과 보안 기술 계산을 고려한 온보드 위성 통신 보안 기술.

Ⅱ. 본론

그림 1 은 잠재적 도청자들의 위협을 받고 있는 유저에게 비암호화 및 암호화 신호를 활용하는 위성 통신 보안 기술을 보여준다. 유저 i 에게 전송되는 위성 신호를 엿듣는 도청자 k 의 신호 대 잡음비(SNR) $\gamma_{i,k}$ 는 아래와 같다.

$$\gamma_{i,k} = \frac{nh_{i,k}^2 \bar{P}}{WN_0}, \quad (1)$$

이 때, n은 위성의 사용가능한 빔 수를 의미하고 $h_{i,k}$ 는 도청자의 multi-path fading 으로 Nakagami-m fading 을 따른다. $\bar{P}$는 모든 사용자들에게 균등하게 분배되는 전송 파워이고, W와 N_0는 각각 사용가능한 대역폭과 잡음 전력 스펙트럼 밀도를 나타낸다. 위성 통신 환경에서 보안

위협은 독립적인 도청자들의 SNR 을 바탕으로 다음과 같이 구할 수 있다 [2].

$$S_i = \mathbb{P}\left[\max_k \gamma_{i,k} \geq \gamma_t\right], \quad (2)$$

이 때, γ_t는 성공적인 디코딩을 위한 임계값을 나타낸다.

보안 위협을 바탕으로 위성의 온보드 전력은 비암호화 및 암호화 신호 전송 전력과 보안 알고리즘 계산 전력으로 분배된다:

$$P_i = \{1-(\phi+1)S_i\}P_i + S_iP_i + \phi S_iP_i, \quad (3)$$

두 신호를 중첩하여 한 유저에게 전송하기 위해서 비직교 다중접속 기술을 활용한다. 따라서, 각 신호에 대한 채널 용량 C_i^{ne}와 C_i^e는 다음과 같다:

$$C_i^{ne} = \begin{cases} \frac{W}{n}\log_2\left(1+\frac{nh_i^2\{1-(\phi+1)S_i\}P_i}{WN_0}\right), & P_i^{ne} \geq P_i^e \\ \frac{W}{n}\log_2\left(1+\frac{nh_i^2\{1-(\phi+1)S_i\}P_i}{WN_0+nh_i^2S_iP_i}\right), & P_i^{ne} < P_i^e \end{cases}, \quad (4)$$

$$C_i^e = \begin{cases} \frac{W}{n}\log_2\left(1+\frac{nh_i^2S_iP_i}{WN_0}\right), & P_i^{ne} \geq P_i^e \\ \frac{W}{n}\log_2\left(1+\frac{nh_i^2S_iP_i}{WN_0+nh_i^2\{1-(\phi+1)S_i\}P_i}\right), & P_i^{ne} < P_i^e \end{cases}, \quad (5)$$

이 때, h_i 는 유저 i 의 채널 이득을 의미하고, 역시 Nakagami-m fading 을 겪는다. 한 유저에게 전송된 두 신호는 같은 h_i를 겪기 때문에, 연속 간섭 제거(SIC) 기술의 디코딩 순서는 S_i가 결정한다. 따라서, S_i에 따라 두 신호의 채널 용량은 두 가지 경우로 나타낼 수 있다.

두 신호를 전송하기 전에 예측된 보안 위협을 바탕으로, 두 채널 용량의 합을 최대화하고 최적 보안 알고리즘을 선택하는 공동 최적화 문제는 아래와 같이 설계할 수 있다.

$$\text{maximize} \sum_{i=1}^{N} C_i^{ne} + C_i^e, \quad (6)$$

$$\text{subject to} \sum_{i=1}^{N} P_i \leq P_{total}, \quad (7)$$

$$\mathcal{SA}_i = \begin{cases} \text{no security}, & S_i = 0 \\ (\text{AES}_{128},\ \text{SHA}_{256}), & 0 < S_i \leq \frac{1}{\phi+2} \\ (\text{AES}_{196},\ \text{SHA}_{384}), & \frac{1}{\phi+2} < S_i \leq \frac{1}{\phi+1} \\ (\text{AES}_{256},\ \text{SHA}_{512}), & \frac{1}{\phi+1} < S_i \leq 1 \end{cases}, \quad (8)$$

식 (7)은 위성 온보드의 전체 전력에 대한 제약 조건이고, 식 (8) 보안 알고리즘 쌍이다. SHA 는 대표적인 메시지 인증 코드 알고리즘이며 AES 와 SHA 의 아래 첨자는 보안 강도를 의미하고 값이 커질수록 높은 보안 강도를 의미한다. 두 채널 용량의 합은 P_i에 대해서 concave 하기 때문에, 주어진 문제는 convex 최적화 문제를 만족한다 [3]. 따라서, 최적 온보드 전력은 아래와 같이 구할 수 있다.

$$P_i = \frac{W}{n}\left\{\frac{1}{\Lambda \ln 2} - \frac{N_0}{h_i^2(1-\phi S_i)}\right\}, \quad (9)$$

이 때, Λ는 전체 온보드 전력 조건에 대한 Lagrangian multiplier 이다. 그림 2 는 제안된 기법과 물리 계층 보안 기술의 보안 용량에 대한 유저i의 성능 비교를 보여준다. 보안 용량은 유저의 채널 용량과 도청자의 채널 용량의 차로 구할 수 있으며, 도청자 수가 많아질수록 도청 diversity 이득에 의해서 보안 용량이 급격하게 감소한다. 하지만, 제안된 기법은 도청자 수가 많아질수록 암호화 신호 전송에 많은 전력을 분배함으로써 향상된 보안 성능을 얻을 수 있다. 이 때, S_i에 의해 SIC 디코딩 순서가 바뀌기 때문에 제안된 기법의 보안 성능이 급격히 향상된다. 또한, 보안 위협이 낮은 환경에서는 비암호화 신호 전송에 많은 전력을 분배하기 때문에, 도청자 수와 관계없이 항상 높은 throughput 을 제공한다.

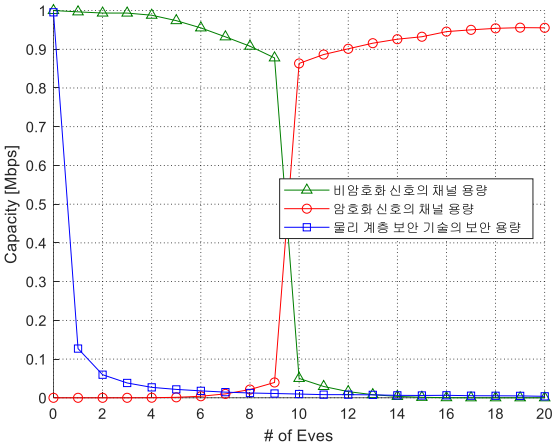

그림 2. 제안된 기법과 물리 계층 보안 기술의 성능 비교.

Ⅲ. 결론

본 논문에서는 비직교 다중 접속 기술을 바탕으로 비암호화 및 암호화 신호 전송과 보안 알고리즘 계산 파워를 고려한 온보드 위성의 보안 기술을 제안하였다. 전송 전 예측한 보안 위협을 활용하여 위성의 온보드 전력을 두 신호의 전송과 보안 알고리즘 계산에 대하여 분배하고 두 신호의 채널 용량 최대화 및 보안 알고리즘 쌍 선택에 대한 합동 최적화 문제를 설계하고 최적 온보드 전력 할당 전략을 도출하였다. 시뮬레이션을 통해 제안한 기술이 기존의 물리 계층 보안 기술보다 향상된 보안 성능을 달성하였다.

.

ACKNOWLEDGMENT

이 성과는 2021 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2021R1A2C1007729), 이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2022-0-00704, 초고속 이동체 지원을 위한 3D-NET 핵심 기술 개발).

참 고 문 헌

[1] Consultative Committee for Space Data Systems (CCSDS), Security threats against space mission, Imformational Report, Green Book, Dec. 2015

[2] S. Jeon, J. Kwak, and J. P. Choi, Optimal Joint User Selection and Beam Scheduling Based on Channel Conditions and Security Threats," 2021 Joint conference on Satellite Communications (JC-SAT 2021), 2021. 10.

[3] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.