위성 통신망 보안 기술 당면 과제 및 향후 발전 방향 분석

최지환* 정회원, 주창희**

Present and Future Technologies of Satellite Communication Network Security

Jihwan Choi*, *Member*, Changhee Joo**

요 약

위성 통신은 무선 채널을 통한 광역 브로드캐스팅 특성으로 인하여 보안에 취약한 약점을 가지고 있음에도 불구하고, 위성 통신을 위한 보안 기법으로는 지상 통신에서 사용해 오던 상위 계층에서의 암호화를 제외하고 많은 방법이 알려져 있지 않다. 특히 물리 계층에서의 재밍, 스푸핑 신호 공격 빈도가 증가함에 따라 이에 대한 대응 기술 개발이 중요하다고 할 수 있다. 본 논문에서는 위성 통신망 보안 문제에 대해서 상위 계층과 물리 계층에서의 대응책에 대해 각각 정리하고, 사물인터넷 등의 지상망 적용을 위해 정보 이론 관점에서 개발되고 있는 물리 계층 보안 기법의 최근 연구 결과에 대해 알아본다. 교차 계층 접근 방식을 포함하여, 위성 통신 보안을 향상시킬 수 있는 향후 연구 방향을 제시한다.

Key Words : satellite communications; network security; encryption; anti-jamming; physical layer security

ABSTRACT

Satellite communications are vulnerable to malicious eavesdroppers and interceptors due to wide coverage and broadcasting applications. However, technologies for securing satellite networks have yet to be more articulated beyond high-layer packet encryption. As attempts for jamming and spoofing attacks spread out, it is extremely critical to invest on the development of physical layer security solutions. In this paper, we review current technologies for satellite communication network security both in high and physical layers. We also present recent research results on physical layer security in the fields of information theory and wireless networks. We suggest a future direction for satellite communication security, including a cross-layer approach.

I. 서 론

위성 통신망을 사용하면 넓은 영역에 있는 많은 수의 사용자들을 별도의 지상 인프라 설치 없이 서비스할 수 있는 장점이 있다. 현재 국내 위성 통신 사업은 상업적으로 지상망과의 치열한 경쟁에서 틈새시장을 찾고 있으며, 군사적으로는 북한의 재밍 교란 위협 및 주변 우주군사대국 사이에서의 우주영토 확보라는 어려운 문제에 직면해있다. 위성 통신의 효율성과 경쟁력을 높이기 위해서 사물인터넷(IoT), 초고주파대역 고속 이동통신, 초고화질 TV방송, 유/무인기 연동, 태양광 에너지 전송 등의 새로운 서비스 시장을 개척함과 동시에, 디지털 온보드 신호처리(OBP), 대규모 다중빔, 초저궤도용 초경량 위성, 지상망 프로토콜 연동, 등의 첨단 위성 통신 기술 개발에도 많은 투자를 기울여야 할 시점이라 할 수 있다.

위성 통신망 사용자들이 점점 다양화, 대규모화 되고 사용 기술 및 프로토콜이 복잡해짐에 따라 위성 통신망의 보안 문제가 더욱 중요해지고 있다. 위성 통신은 넓은 영역의 브로드캐스팅에 최적화되어있다는 특성 때문에 비인가 사용자들이 망에 침입하여 허가받지 않은 사용을 하거나 다른 사용자들의 서비스를 방해하는 상황에 취약하다는 약점이 있다. 앞으로 사물인터넷 및 초저궤도 위성 분산 시스템 등의 서비스 대중화와 함께 위성 및 사용자 수가 급증함에 따라 위성 통신망 보안 관련 문제 역시 급증할 것으로 예상된다.

※ 이 논문은 방위사업청 및 국방과학연구소의 재원에 의해 설립된 신호정보 특화연구센터 사업의 지원을 받아 수행되었음.
*대구경북과학기술원(DGIST) 정보통신융합전공 (jhchoi@dgist.ac.kr)
**울산과학기술원(UNIST) 전지전자컴퓨터공학부 (cjoo@unist.ac.kr)
접수일자 : 2017년 9월 8일, 수정완료일자 : 2017년 9월 19일, 최종게재확정일자 : 2017년 9월 20일

위성 통신을 위한 보안책은 전통적으로 상위 계층에서 패킷 암호화와 사용자 인증을 위해 패킷에 redundancy를 더하는 방식으로 이루어졌다[1-3]. 군통신에서는 상위계층 보안 기법을 보완하기 위해서 물리계층 해법을 함께 적용하는 것이 일반적으로서, 특정한 신호 파형을 독자적으로 사용하는 방식을 적용하고 있다. 최근 물리 계층 보안 연구가 많은 관심을 가짐에 따라 물리 계층 보안 기법을 항재밍용으로 사용하려는 기술이 민간 통신 위성에도 많이 고려되고 있다. 하지만 아직도 상위 계층과 물리 계층 보안 기술은 분리된 채로 적용되고 있고, 항해킹과 항재밍 대응에 관하여 정확한 수학적 모델링이나 경제적 타당성 분석이 필요한 상황이다.

본 논문에서는 현재 위성통신망에서 널리 쓰이고 있는 상위 및 물리 계층 보안 기술에 대해 정리하고, 이기종 지상망에서 활발히 연구되고 있는 첨단 물리 계층 보안 기술의 위성 통신망 적용 여부에 대해 검토한다. 향후 연구 방향으로서, 상위 계층과 물리 계층 기술을 접목하는 교차 계층 접근 방식에 대하여 간단히 소개한다.

Ⅱ. 위성 통신망 보안 기술

1. 상위 계층 보안 기술

위성 통신망을 위한 상위 계층 보안 기술의 목적 및 기본 원칙은 지상 통신망과 크게 다르지 않다. 전달하고자 하는 내용을 왜곡 없이 원하는 사용자들만 들을 수 있도록, 패킷을 암호화하고(packet encryption), 메시지가 변경되지 않았음을 확인하며(message integrity), 송수신자가 맞는지 확인한다(authentication).

하지만, end-to-end 일관성이 보장되는 유선망에서 쓰이는 프로토콜이 위성 연동 이기종망에서 쓰일 경우 문제가 발생할 수 있다. IPSec (Internet Security Protocol)과 SSL (Secure Socket Layer) 같은 보안 프로토콜의 종단 보안성 보장과 위성망에서의 proxy 사용을 통한 효율 향상 사이에 충돌이 생기게 되는데[4], 위성 PEP (performance enhancing proxy) 사용 시 TCP (Transmission Control Protocol)의 end-to-end 일관성이 위배되는 것과 비슷한 문제라 할 수 있다. 해결을 위하여, IPSec과 SSL 암호화 및 패킷화 과정를 분할하여, 중간 proxy의 활용성을 잃지 않으면서도 전체 패킷의 end-to-end 연결성을 최대한 보장하는 방식을 취할 수 있다. 암호화가 여러 번 이루어지므로, 암호 키도 여러 개 필요하고, 이에 따른 키 생성 및 분배 문제가 더욱 복잡해지게 된다.

패킷 암호화를 위한 키 생생 및 분배는 위성망뿐 아니라 전반적인 통신망에서 복잡한 문제로 인식된다. 해독이 쉽지 않은 랜덤성을 가지는 암호 키를 생성한 후, 상호 먼 거리에 위치하고 있는 사용자들에게 나눠주는 방식은 기술적, 경제적으로 쉽지 않고, 중간 과정에서 도난당할 위험이 적지 않다. 한 가지 해법으로서, 양자역학에서 알려져 있는 양자 얽힘(quantum entanglement) 현상을 보안키에 사용하려는 시도가 계속 이루어지고 있다. 올해 6월 중국에서 “묵자” 위성을 이용하여, 양자쌍둥이 하나의 상태를 결정할 경우 1,200 km 거리에 떨어져 있는 다른 양자쌍둥이의 상태도 동시에 결정됨을 실험으로 보였다[5]. 상용화, 실용화되기까지는 기술적으로 아직 많은 이슈가 남아있으나, 양자 암호키는 물론, 양자컴퓨터, 양자통신의 가능성을 보여준다는 의미가 있다. 특히 양자 통신이 실현될 경우, 위성 통신, 우주 통신의 가장 큰 한계점이라 할 수 있는 거리 지연을 극복할 수 있게 된다.

2. 물리 계층 보안 기술

위성 통신망에서 물리 계층 보안 기술 적용의 가장 큰 목적은 항재밍이라 할 수 있다. 항재밍 세부기술로는 주파수 hopping, spread spectrum, 에러 정정 부호(error correction code, ECC), agile/narrow 다중빔 등이 널리 쓰이고 있고 안테나 어레이, successive interference cancellation (SIC) 등의 첨단 MIMO (multi-input multi-output) 안테나 기술을 도입하기 위한 시도도 확산되고 있다. 다중 안테나를 사용함으로써, nullling, 빔포밍 등의 SDMA (space division multiple access) 기술로 원하는 위치의 사용자는 높은 수신율을 보이게 하면서, 도청자가 있거나 신호를 보내고 싶지 않은 지역에는 송신 널링을 달성할 수 있게 된다.

최근 물리 계층 보안 기술이 많이 적용되는 위성 분야는 GPS 항법 신호라 할 수 있다. 특히 GPS 공격의 경우, 단순 재밍을 넘어 위성신호 파형을 동일하게 모방하여 사용자를 속이는 기만신호(spoofing)의 사용 빈도도 증가하고 있어, 기만신호의 특성을 파악하고 이에 대비하는 기술의 필요성이 점점 높아지고 있다[6]. 재밍 및 기만신호 공격 여부는 신호 세기뿐 아니라 신호 세기의 변화율, 도플러 변화, 다른 주파수 신호(GPS의 L1, L2) 사이의 cross-correlation, 차이점 등 여러 파라미터를 바탕으로 복합 판단하여야 한다[7]. 최근 많은 각광을 받고 있는 머신러닝, 딥러닝 기법을 적용할 수 있는 분야의 한 예가 될 수 있을 것이다.

아래의 표 1은 위성 통신망에 적용되는 상위 계층과 물리 계층 보안 기술의 주요 목적, 대표 기술, 당면 문제점, 그리고 미래 적용 기술을 비교 정리한다.

표 1. 상위 계층과 물리 계층 보안 기술 비교

	상위 계층	물리 계층
주요 사용 목적	패킷 암호화	항재밍
대표 기술	보안 프로토콜 (IPSec, SSL 등)	신호 랜덤화 에러 정정 부호 다중 안테나
당면 문제점	유선망 프로토콜의 이기종망 적용 및 효율적이고 안전한 암호키 생성	기만신호 공격의 증가
미래 적용 기술	양자 암호키 생성 및 분배	머신러닝, 딥러닝 적용

Ⅲ. 최신 물리 계층 보안 기술

최근 무선 디바이스 사용 확산과 이를 바탕으로 한 무선 서비스의 폭발적인 증가에 따라, 암호화 및 알고리즘 연산 기반 상위 계층 보안 기술의 한계점을 극복하려는 시도로써, 물리 계층 보안 기술 연구 및 상용화 구현이 진행되고 있다. 정보이론 관점에서 원하는 수신자와 도청자의 채널용량 차이로 secrecy capacity를 정의하고, 도청자가 얻지 못하는 수신자의 정보량을 극대화하는 방향으로 송수신 기법을 최적화하게 된다. 연구 차원에서 고려되고 있는 기법은 다중안테나 빔포밍, 협력 빔포밍, 릴레이 전송, full duplex 등 최신 통신 네트워크 송수신 기술을 포함한다.

송신기가 전달하고자 하는 신호 외, 수신기 주변의 도청자들을 방해하기 위하여 재밍 신호(friendly 재밍)를 부가적으로 송출할 수 있다. 이 경우, 수신자가 송신자의 재밍 신호를 상쇄할 수 있는 능력(그림 1에서 Ic로 표현)을 갖추는 것이 중요하고, 이 상쇄 능력이 송신단에서 재밍 신호와 원하는 신호의 파워비(jamming to signal ratio: JSR)를 결정하는 데 중요한 요인이 된다(그림 1). 또한, 도청자의 채널 정보(그림 2에서 Eve Channel Gain으로 표현)를 모르는 것은 통신 보안 성능에 큰 영향을 미치지 않는다(그림 2)[8]. 특히 이 문제는 송신기 스케줄러의 입장에서 수신자에게 원하는 신호를 보내는 작업과 도청자의 수신을 방해하는 작업 사이의 우선순위를 정하고, 한정된 송신 자원(파워, 타임슬랏, 주파수대역, 안테나 등)을 효율적으로 배분하는 MAC(medium access ccontrol) 계층 자원 배분 및 스케줄링 문제와도 연결된다.

물리 계층에서 사용하는 기법 중 수도랜덤코드를 활용한 주파수 hopping, spread spectrum이나 friendly 재밍 신호 발생의 경우, 송신자와 수신자가 수도랜덤코드를 사전에 생성하여 서로 알고 있어야한다는 점에서, 상위 계층 보안 기법에서의 암호키 생성 및 분배 문제와 본질적으로 다를 바가 없다고 볼 수 있다. 수도랜덤코드 생성 및 분배의 효율과 보안성을 높이기 위해 무선 채널 페이딩의 랜덤성을 이용하는 등의 연구가 이루어지고 있다[9].

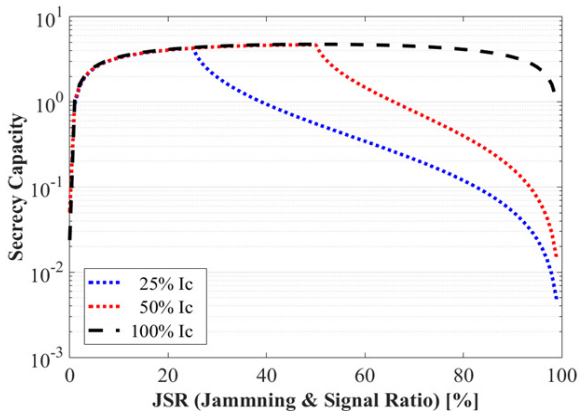

그림 1. 수신자의 재밍신호 상쇄능력(Ic)이 다른 경우, 재밍-신호 파워비(JSR)에 따른 통신 보안 성능(Secrecy Capacity) 비교[8]

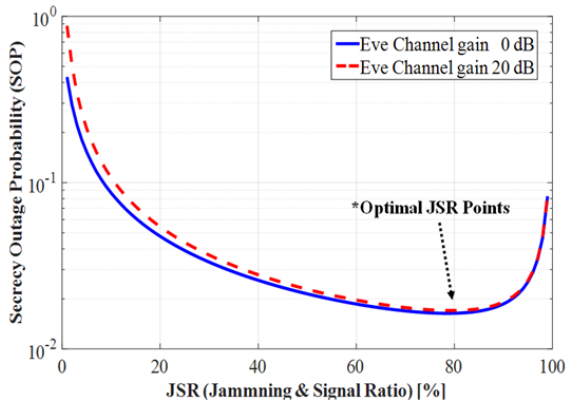

그림 2. 도청자의 채널 환경(Eve Channel Gain)이 다른 경우, 재밍-신호 파워비(JSR)에 따른 통신 보안 성능 (Secrecy Outage Probability) 비교[8]

Ⅳ. 결론 및 향후 연구 방향 제언

본 논문에서는 위성 통신망 보안 기술에 대하여, 항해킹, 항재밍 관점에서 각각 상위 계층 보안 기술과 물리 계층 보안 기술을 검토하고, 현재 지상망 및 정보이론 관점에서 진행되고 있는 첨단 물리 계층 보안 기술에 대하여 간단히 정리해 보았다. 위성망 트래픽 중 지상 인터넷에서와 같은 IP 패킷의 비중이 점점 더 많이 늘어남은 물론, 위성이 지상망과 연동된 이기종 네트워크의 중요 부분을 담당함에 따라, 통신 위성망 또한 지상망이 겪는 보안 문제-재밍, 해킹, 도청, 스푸핑, DDoS (distributed denial of service) 공격 등-에 노출되고 있다. 통신 보안 문제가 군용은 물론 민간 상용 위성에까지 중요해지면서, 상위 계층 암호화 및 물리 계층 항재밍, 항스푸핑 신호 기술 개발 및 실제 적용이 널리 연구되고 있다.

하지만, 상위 계층과 물리 계층을 아우르는 교차 계층 보안 기술 논의는 아직 요원한 상태이다. 교차 계층 보안 기술은 정의 자체도 확립되어 있다고 보기 힘든 상황이지만, 앞에서 보았듯이 물리 계층 보안 문제가 MAC 계층 자원 배분 문제로 치환된다든지, 항재밍 기법 적용을 통해 상위 암호화 처리 과정의 복잡성을 조절할 수 있음을 생각할 때, 교차 계층 보안 문제 분석 및 기술 개발의 여지는 충분하다고 할 수 있다. 특히 위성을 포함하는 복잡한 다중경로 멀티합 네트워크에서 여러 항재밍 기법 적용 시 TCP/IP 등의 상위 계층에서 일어나는 혼잡 제어 및 라우팅 알고리즘 수행 결과 변화를 예상할 때, 통신망 보안을 위한 교차 계층적 접근은 반드시 필요하다고 볼 수 있다.

다른 이슈로서, 태양풍과 같은 우주환경 요인으로 인한 위성 오작동 모델링 및 분석, 대응기법에 관한 연구가 전자회로 및 천제물리 분야에서 진행되고 있다[10, 11]. 자연적인 우주환경 요인을 의도된 재밍 신호로, 일반적인 위성 온보드 시스템을 위성 통신 시스템으로 대체할 경우, 위성 통신에서의 물리 계층 보안 연구와의 접목을 시도할 수 있을 것이다.

마지막 빼놓을 수 없는 최신 통신망 기법으로서, software defined network (SDN)와 software defined radio (SDR)를 들 수 있다. control plane과 data plane을 분리하는 SDN의 경우, 채널 지연 시간이 긴 위성망의 특성 상 지상망에 비하여 구현되기가 쉽지는 않겠지만, 그럼에도 위성의 소형화, 대규모화, 저궤도화 및 민간 제작 추세를 감안할 때, 경제적으로 매우 관심을 끄는 대상이다. SDN이 위성 통신망에 구현될 때의 보안 문제 및 대응 기술 연구 개발은 위성 통신 연구자들에게 상당히 흥미 있는 분야라고 할 수 있을 것이다.

참 고 문 헌

[1] Gerard Maral and Michel Bousquet, Satellite Communications Systems: Systems, Techniques and Technology, 5th ed., Wiley, 2010, pp.115-117.

[2] James Kurose and Keith Ross, Computer Networking: A Top-Down Approach, 6th ed., Pearson, 2013, pp. 671-705.

[3] Adam Hudaib, Satellite Network Threats Hacking & Security Analysis, CreateSpace Independent Publishing Platform, 2016.

[4] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," IEEE Wireless Communications, vol. 12, no. 6, pp. 50-61, Dec. 2005.

[5] Juan Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers,"Science, vol. 356, no. 6343, pp. 1140-1144, June 2017.

[6] Mark L. Psiaki and Todd E. Humphreys, "GNSS spoofing and detection,"*Proceedings of the IEEE,* vol. 104, no. 6, pp.1258-1270, April 2016.

[7] Jon S. Warner and Roger G. Johnston, "GPS Spoofing Countermeasures," *Journal of Homeland Security*, LA-UR-03-6178, 2003, http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-6178

[8] Jongyeop Kim and Jihwan P. Choi, "Cancellation-Based Friendly Jamming for Physical Layer Security," Proceeding of *IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, 2016.

[9] Yi-Sheng Shiu *et al.*,"Physical layer security in wireless networks: a tutorial,"*IEEE Communications Magazine*, vol. 18, no. 2, pp. 66 - 74, Apr. 2011.

[10] Joshua Engel, *et al.* "Predicting on-orbit static single event upset rates in xilinx virtex FPGAs." Los Alamos National Laboratory Report, 2006, http://scholarsarchive.byu.edu/facpub/1307/

[11] Melanie D. Berg, Kenneth A. Label, and Jonathan Pellish. "New Developments in FPGA: SEUs and Fail-Safe Strategies from the NASA Goddard Perspective." NASA Technical Report, 2016. https://ntrs.nasa.gov/search.jsp?R=20150023390

저자

최 지 환(Jihwan Choi)

- 1998년 2월 : 서울대학교 전기공학부 (공학사)
- 2000년 6월 : MIT EECS(공학석사)
- 2006년 9월 : MIT EECS(공학박사)
- 2006년 9월 ~ 2012년 12월 : Principal Ssytems Engineer, Marvell Semiconductor, Inc.
- 2013년 1월 ~ 현재 : 대구경북과학기술원, 정보통신융합전공, 부교수
- 2016년 1월 ~ 현재 : 정보통신기술진흥센터, 위성 분야 RP(비상근)

<관심분야> : 위성-지상 연동망, 교차 계층 최적화, 기계학습

주 창 희(Changhee Joo)

- 1998년 2월 : 서울대학교 전기공학부 (공학사)
- 2000년 2월 : 서울대학교 전기공학부 (공학석사)
- 2005년 2월 : 서울대학교 전기공학부 (공학박사)
- 2005년 9월 ~ 2007년 6월 : Post-doc Purdue Univ.
- 2007년 7월 ~ 2010년 2월 : Research Scientist, OSU.
- 2010년 3월 ~ 2011년 8월 : 한국기술교육대학교, 정보통신학과, 조교수
- 2011년 9월 ~ 현재 : 울산과학기술원, 전기전자컴퓨터공학부, 부교수

<관심분야> : 위성네트워크, 무선자원할당, 시스템 최적화