논문 22-47-02-08 The Journal of Korean Institute of Communications and Information Sciences '22-02 Vol.47 No.02
https://doi.org/10.7840/kics.2022.47.2.269

저궤도 군집 위성망에서 재생공격 대응을 위한 동적 타임스탬프 기반 인증 기법

현 준 열◆, 이 민 우°, 임 재 성*

Dynamic Timestamp-Based Authentication Techniques for Anti-Replay Attacks in LEO Satellite Networks

Junyeol Hyun◆, Minwoo Lee°, Jaesung Lim*

요 약

저궤도 군집 위성망의 광범위한 접근성과 노출된 링크는 네트워크 공격 위협을 증가시키는 주요 요인이다. 특히 대형 저궤도 군집 위성은 우주 공간에서 광범위하게 통신 링크를 구성하기 때문에 네트워크 공격에 더욱 취약하다. 구체적으로 대형 저궤도 군집 위성 네트워크의 종단 간 전파지연은 거리에 따라서 가변하는데, 이는 인증 과정에서 재생공격의 위협을 증가시킨다. 본 논문은 대형 저궤도 군집 위성 네트워크에서 재생 공격에 내성을 갖는 동적 타임스탬프(Timestamp)를 이용하는 기법을 제안한다. 이를 위해 위성간 링크에서의 지연시간을 활용하여 동적 타임스탬프의 허용 범위를 산출하는 방법을 제안한다. 또한 타임스탬프의 허용 범위를 동적으로 설정할 수 있도록 안전하게 인증 절차를 개선하였다. 모의실험을 통하여 제안된 기법이 재생공격의 위협을 감소시킬 수 있음을 확인하였다.

Key Words : LEO Satellite Mega-Constellation, Authentication, Replay Attack, Propagation Delay

ABSTRACT

The wide accessibility of LEO satellites networks and exposed links are main factors that increase the threat of network attacks. An LEO satellite mega-constellation networks are more vulnerable to network attacks because they constitute extensive communication links in outer space. Especially the characteristics of dynamically varying propagation delay time between end-to-end constellation in LEO satellite networks increase the threat of replay attacks in authentication. This paper proposes a technique to use dynamic timestamps resistant to network replay attacks. To this end, this paper suggests the technique to calculate the allowable range of dynamic timestamps using the delay of inter-satellite links. And the authentication procedure was improved to use the dynamic timestamps. Through simulations, it was confirmed that the proposed technique could reduce the threat of regenerative attacks.

※ 이 논문은 2021년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.NRF2021R1I1A1A01047914)
◆ First Author : Ajou University Department of Military Digital Convergence, june7944@ajou.ac.kr, 학생회원
° Corresponding Author : Ajou University Department of Military Digital Convergence, iminu@ajou.ac.kr, 종신회원
* Ajou University Department of Military Digital Convergence, jaslim@ajou.ac.kr, 종신회원
논문번호 : 202110-299-B-RN, Received October 28, 2021; Revised November 26, 2021; Accepted November 26, 2021

Ⅰ. 서 론

최근 대형 저궤도 군집 위성 네트워크(Low Earth Orbit Satellite Mega-Constellation Network, LEO MCN)에 대한 연구가 활발하게 진행되고 있다. 전 세계를 초저지연으로 연결할 수 있는 LEO MCN을 구축하기 위해 Starlink, OneWeb, Kuiper와 같은 저궤도 위성 통신 시스템이 빠른 속도로 구축되고 있으며, 상용 서비스 개시를 앞두고 있다[1,2].

위성 통신을 이용하면 지구 어디에서나 통신이 가능하다. 특히 정지궤도 위성과 달리 LEO MCN을 이용하면 저궤도 위성이 지구 전역에 걸쳐서 연결되어 있기 때문에 적은 지연 시간으로 통신이 가능하다. 또한 LEO MCN에서는 여러 개의 위성이 사용자의 시야에 존재하기 때문에 음영지역 없이 통신이 가능하다[2].

위성 통신의 대표적인 취약점은 통신 링크가 노출되어 있다는 것이다[3,4]. 통신 링크가 노출되어 있으면 공격자가 인증 과정에서 메시지를 탈취할 수 있기 때문에 재생공격이나 중간자 공격에 취약하다[3]. 따라서 저궤도 위성 네트워크에서 인증 및 키 교환 프로토콜이 활발하게 연구되고 있다[5-9].

재생공격은 공격자가 인증 과정에서 정상 메시지를 탈취하여 재전송함으로써 DoS(Denial of Service) 공격을 일으킬 수 있는 큰 위협이다. 타임스탬프는 인증 프로토콜에서 재생공격을 방지하기 위한 대표적인 방법이다[10]. 실제로 많은 저궤도 위성 통신의 인증 및 키 교환 프로토콜에서 재생 공격을 방지하기 위한 방법으로 타임스탬프를 활용하고 있다[5-9]. 대표적으로 위성, MANET, Zigbee와 같은 여러 분야에서 타임스탬프를 개선하여 보안 위협을 감소시키기 위한 연구가 이루어졌다[9,11,12].

재생공격을 방지하기 위해서는 타임스탬프의 허용 범위를 적정 수준으로 설정하는 것이 중요하다[11]. 타임스탬프의 허용 범위를 크게 설정할 경우 공격자가 메시지를 탈취하여 재전송하기 위한 충분한 시간이 주어지기 때문에 재생 공격의 위협이 증가한다. 반면에 정상 메시지가 여러 변수로 인하여 수신측에 늦게 도착할 수 있다. 만약 타임스탬프가 작다면 이런 경우에 불필요하게 정상 메시지가 폐기될 수 있다.

그런데 LEO MCN의 인증 프로토콜에서 타임스탬프를 개선시키기 위한 연구는 아직 이루어지지 않았다. 특히 LEO MCN은 위성간 링크(Inter-Satellite Link, ISL)의 길이가 다양하고, 잦은 핸드오버가 일어나기 때문에 라우팅 정보가 자주 변화한다[4]. 그리고 전 세계에 걸쳐서 네트워크가 연결되어 있기 때문에 종단 간 전파 지연의 범위가 두 노드의 상대적인 위치에 따라서 크게 달라진다. 이러한 경로 지연에 대한 여러 변수들로 인하여 메시지가 전달되는 시간이 달라지기 때문에 고정된 값으로 타임스탬프의 허용 범위를 설정하면 효과적으로 재생공격을 방지하기 어렵다.

그러나 기존의 인증 프로토콜에서는 타임스탬프 조건 설정에 대한 언급이 없거나[5,8,9] 위성과 지상 사용자 사이의 시간 동기화와 RTT(Round-Trip Time)만을 고려하여 타임스탬프 허용 범위를 설정하였다[6]. 이러한 방식은 LEO MCN에서의 지연 시간을 고려하지 않았기 때문에 종단 간 전파 지연이 크게 변화하는 경우 문제가 된다.

본 논문에서는 LEO MCN에서의 종단 간 지연 시간에 따라서 타임스탬프의 허용 범위를 동적으로 설정하는 방법을 제안한다. 또한 종단 간 지연 시간에 따라서 타임스탬프 허용 범위가 변화하더라도 안전한 인증 절차를 제시한다. 그리고 제안된 방법이 재생 공격의 위협을 감소시킬 수 있음을 모의실험을 통하여 보인다.

논문의 구성은 다음과 같다. 2장에서는 LEO MCN의 구조와 네트워크 모델을 설명한다. 3장에서는 동적으로 타임스탬프 허용 범위를 설정하는 방법에 대하여 설명하고, 동적인 타임스탬프를 안전하게 전달할 수 있도록 개선된 인증 절차를 제안한다. 4장에서는 모의실험을 통해 제안 기법이 재생 공격을 방지하는데 효과적임을 보인다. 그리고 5장에서 결론으로 마무리한다.

Ⅱ. 시스템 모델

2.1 대형 저궤도 군집 위성 네트워크

대부분의 Mega-Constellation Network(MCN)는 하나 또는 여러 층의 Walker Constellation으로 이루어져 있다[1]. 본 논문에서는 한 층의 Walker Delta Constellation 모델을 활용한다. Walker Delta Constellation에서는 서로 다른 궤도에 위치한 인접한 위성이 ISL을 통해 연결되어 지구를 공전한다[13]. Walker Delta Constellation은 N_P개의 궤도 평면으로 구성되고, 각 궤도 평면 내에는 M_P개의 위성이 있다. 따라서 총 $N_P \times M_P$개의 위성으로 구성된다.

본 논문에서 궤도 평면은 모두 동일한 간격으로 떨어져 있다고 가정한다. 또한 궤도 평면 내의 인접 위성 사이의 거리도 일정하다고 가정한다. 각 궤도 평면

은 동일한 기울기로 기울어져 있으며 인접 궤도 위성과의 위상 차이를 나타내는 위상인자(Phasing Factor, F)는 0으로 설정한다[1].

본 논문에서 LEO MCN은 OBP(On-Board Processing) 능력을 갖춘 저궤도 위성들로 구성되며, 각각의 위성은 위성간 통신 링크(ISL)로 통신이 가능하다[1]. OBP 능력은 위성에서 라우팅과 메시지 처리가 가능함을 의미한다. 위성 중에서 특별히 지상의 사용자 또는 NCC 사이에서 메시지를 중계하는 것을 접근위성(Access Satellite)이라고 한다.

ISL은 FSO(Free Space Optical)을 사용하는 통신 링크로 구현이 된다[14]. ISL은 동일한 궤도 평면 내부의 인접한 위성끼리 연결하는 궤도 내 위성간 링크(Intra-plane ISL)와 인접한 궤도 평면의 위성끼리 연결하는 궤도 간 위성간 링크(Inter-plane ISL)로 분류할 수 있다. 하나의 위성은 Intra-plane ISL과 Inter-plane ISL을 각각 2개씩 갖추어 인접 위성과 연결되어 이동한다.

2.2 네트워크 모델

인증을 위해서 사용자는 NCC(Network Control Center)와 메시지를 주고받는다. 지상에 있는 사용자가 보낸 메시지는 LEO MCN을 거쳐서 NCC에 전달된다. 사용자는 상공에 위치한 접근위성(Access satellite of User, SAT-User)에 메시지를 전송한다. LEO MCN에 진입한 메시지는 라우팅 프로토콜에 따라서 NCC의 접근위성(Access Satellite of NCC, SAT-NCC)까지 전달된다. 이 과정에서 NCC와 사용자가 같은 위성의 지상 수신범위(Footprint) 안에 위치할 경우, SAT-User와 SAT-NCC는 동일하므로, SAT-User는 NCC에 메시지를 바로 전송할 수 있다. 그러나 사용자와 NCC의 거리가 먼 경우에는 여러 홉의 ISL을 거쳐서 SAT-NCC에 메시지를 전달해야 한다. 그리고 SAT-NCC는 지상에 있는 NCC에 메시지를 전송한다. 이때 LEO MCN 내부의 ISL은 FSO 통신 링크로 이루어져 간섭이 적고 공격 위협으로부터 안전하다[14].

그러나 무선 링크의 속성상 지상과 접근위성 사이 통신 링크는 공격자에게 노출되어 있다. 사용자와 NCC는 각 접근위성의 지상 수신범위 안에 포함되어 있다. 접근위성의 지상 수신범위 내부의 공격자는 사용자와 SAT-User 사이 또는 NCC와 SAT-NCC 사이에서 인증 메시지를 가로채서 재생 공격과 중간자 공격을 수행할 수 있다. 이때 공격자의 최대 고도를 대기권 상에서 비행이 가능한 10km로 제한하면, 사용자

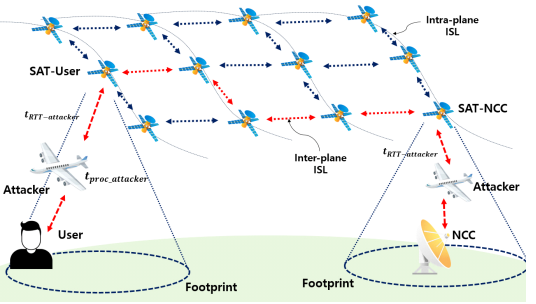

그림 1. 사용자와 NCC가 LEO MCNs으로 연결되는 경로
Fig. 1. A multi-hop path connecting between user and NCC in LEO MCNs

와 공격자 또는 NCC와 공격자 사이의 전파지연이 충분히 작다고 가정할 수 있다. 공격자의 시스템 내에서의 처리지연 시간은 $t_{proc-\text{attacker}}$로 나타내고, 공격자와 위성 사이의 전파지연 시간은 위성과 공격자 사이의 RTT($t_{RTT-\text{attacker}}$)의 1/2로 표현할 수 있다.

Ⅲ. 전파지연을 고려한 동적 타임스탬프 기법

3.1 전파 지연을 고려한 타임스탬프 허용 범위

인증 과정에서 재생공격을 방지하기 위해서는 타임스탬프의 유효성을 확인해야 한다. 타임스탬프의 유효성을 확인하기 위해서는 수식 (1)을 활용한다. 메시지를 보내는 시각(t_s)과 메시지를 수신한 시각(t_d)의 차이가 타임스탬프의 허용 범위($\triangle T$)보다 작은지 확인한다. 수식 (1)을 만족하는 경우 다음 단계로 진행하고, 그렇지 않은 경우 메시지를 폐기한다.

$$|t_s - t_d| \leq \triangle T \tag{1}$$

이때 $\triangle T$를 적절하게 설정하는 것이 매우 중요하다. 따라서 이번 절에서는 사용자와 NCC 사이의 종단 간 지연시간에 따라서 동적으로 $\triangle T$를 산출할 수 있는 방법을 설명한다. $\triangle T$는 수식 (2), (3)으로 나타낼 수 있다.

$$\triangle T = \frac{1}{2}t_{RTT-NCC} + \frac{1}{2}t_{RTT-User} + t_{ISL} \tag{2}$$

$$t_{ISL} = H_{\text{inter}}\, t_{\text{inter}} + H_{\text{intra}} t_{\text{intra}} + (H_{inter} + H_{\text{intra}} + 1)t_{proc} \tag{3}$$

수식 (2)에서는 위성-지상 링크에서의 지연 시간과 LEO MCN에서의 지연 시간(t_{ISL})을 이용하여 동적인

타임스탬프 허용 범위를 산출한다. 위성-지상 링크에서의 지연 시간은 NCC와 SAT-NCC 사이의 RTT($t_{RTT-NCC}$)와 사용자와 SAT-User 사이의 RTT($t_{RTT-User}$)를 이용하여 구할 수 있다. 그리고 LEO MCN에서의 지연 시간은 수식 (3)을 통해 구할 수 있다.

수식 (3)은 LEO MCN의 지연 시간을 전파 지연(Propagation delay)과 처리 지연(Processing delay)으로 표현한다. 전파 지연은 메시지가 지나 온 ISL의 홉 수와 단일 ISL의 평균 전파 지연을 곱하여 나타낼 수 있다. 그리고 이 계산 과정을 Inter-plane ISL과 Intra-plane ISL에서 각각 수행한 후 더하면 LEO MCN에서의 전체 전파 지연이 된다. 처리 지연은 지나온 위성 노드의 수($H_{inter}+H_{\text{intra}}+1$)를 단일 위성에서 처리 지연과 곱한 값으로 나타낸다. 이때 각 위성에서 처리 지연은 t_{proc}으로 동일하다고 가정한다.

ISL에서 평균 전파 지연은 수식 (4), (5), (6)으로 계산할 수 있다. 이때 수식 (5), (6)에서 c는 빛의 속도를 의미한다.

$$l = 2Rsin(\frac{\Pi}{N}) \tag{4}$$

$$t_{interISL} = \frac{2(R_E+h)\sin(\frac{\Pi}{N_P})}{c} \tag{5}$$

$$t_{intraISL} = \frac{2(R_E+h)\sin(\frac{\Pi}{M_P})}{c} \tag{6}$$

수식 (5), (6)은 각각 Inter-plane ISL과 Intra-plane ISL의 평균 경로 지연을 의미한다. ISL의 평균 경로 지연은 ISL의 평균 길이를 빛의 속력으로 나눈 값이다. ISL의 평균 길이를 구하기 위해서 수식 (4)를 활용한다. 수식 (4)는 반지름의 길이가 R인 원에 내접하는 정N각형의 한 변의 길이(l)을 표현한 수식이다. 그림 2는 N_P개의 궤도 평면이 동일한 적경(Right ascension of ascending node, RAAN) 차이($\frac{2\Pi}{N_P}$)로 떨어져 있는 상황을 표현한 것이다[1]. 이때 지구 반지름(R_E)과 위성의 고도(h)를 더한 값을 원의 반지름으로 하여 계산하면 수식 (5)에서 Inter-plane ISL의 평균 길이를 구할 수 있다. 또한 하나의 궤도 평면 내에서 M_P개의 위성이 $\frac{2\Pi}{M_P}$ 간격으로 위치한다고 할 때, 동일한 방식으로 수식 (6)의 intra-plane ISL의 평균 길이를 구할 수 있다.

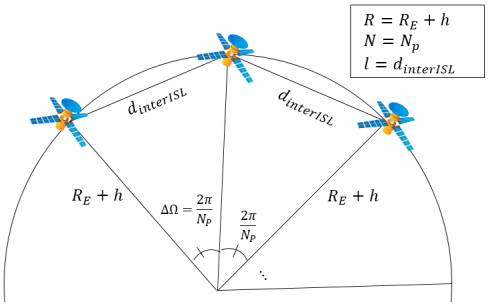

그림 2. 동일한 간격으로 떨어져 있는 궤도 평면 내 위성
Fig. 2. Evenly distributed satellites in each orbit planes

NCC는 지상에 고정되어 있고 지속적으로 위성과의 RTT를 측정하기 때문에 $t_{RTT-NCC}$를 알고 있다. 그러나 메시지를 주고받는 시간동안 위성과 사용자 사이의 상대적인 위치가 변하기 때문에 위성과 사용자 사이의 RTT($t_{RTT-User}$)는 일정하지 않다. 따라서 $t_{RTT-User}$는 사용자가 위성의 지상 수신범위 가장 바깥에 위치한다고 가정하여 최댓값으로 설정한다. 수식 (7)은 사용자와 위성 사이의 RTT를 계산하는 방법이다[15]. 수식 (7)에서 h는 위성의 고도, c는 빛의 속도, ε는 고도각(Elevation angle), R_E는 지구 반지름을 의미한다.

$$t_{RTT-User} = \frac{2\sqrt{2R_Eh+h^2+(R_E\cos(\varepsilon))^2}-2R_E\cos(\varepsilon)}{c} \tag{7}$$

모든 수식을 종합하면 $\triangle T$는 다음과 같이 수식 (8)로 정리할 수 있다.

$$\begin{aligned}\triangle T = &\frac{\sqrt{2R_Eh+h^2+(R_E\cos(\varepsilon))^2}-R_E\cos(\varepsilon)}{c} \\ &+\frac{1}{2}t_{RTT-User}+H_{inter}\frac{2(R_E+h)\sin(\frac{\Pi}{N_P})}{c} \\ &+H_{\text{intra}}\frac{2(R_E+h)\sin(\frac{\Pi}{M_P})}{c}+(H_{inter}+H_{\text{intra}}+1)t_{proc}\end{aligned} \tag{8}$$

3.2 동적 타임스탬프 허용 범위를 적용한 인증 절차

LEO MCN에서의 지연 시간을 고려하여 동적으로 타임스탬프 허용 범위($\triangle T$)를 설정하기 위해서는 LEO MCN의 지연 시간 정보를 NCC 또는 사용자에

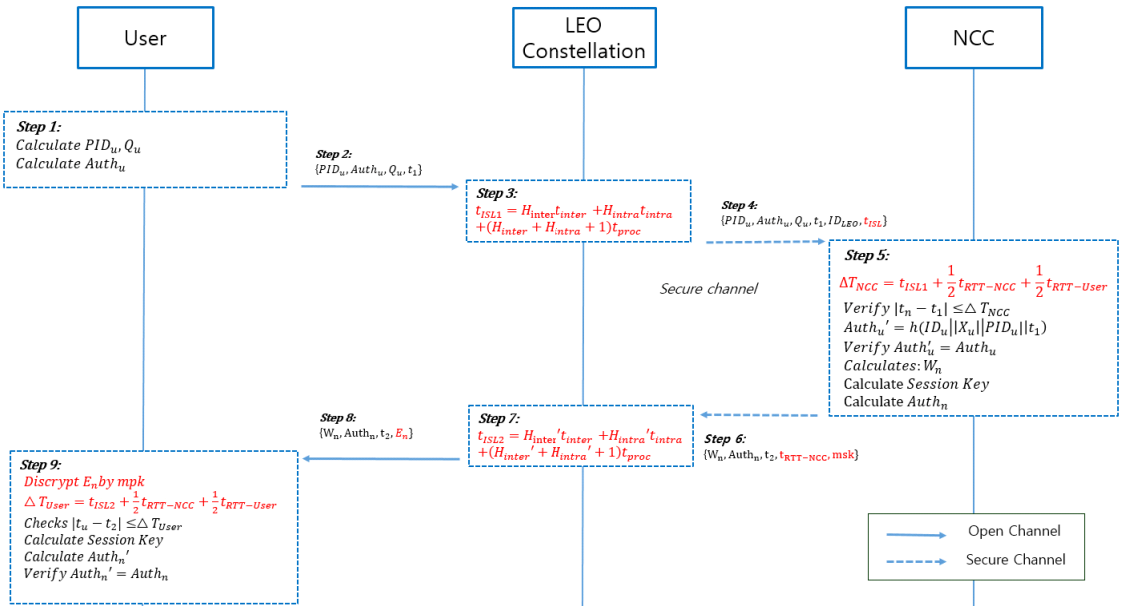

그림 3. 공격자가 타임스탬프를 조작하지 못하도록 수정한 인증 절차
Fig. 3. Modified login and authentication phase for anti-tampering timestamp

게 전달해야 한다. 이 과정에서 $\triangle T$에 관련된 정보를 보낼 때, 메시지의 무결성을 보장할 수 있어야 한다. 그러나 인증 메시지를 보내는 시점에서는 사용자와 NCC는 상호인증이 완료되지 않았기 때문에 안전한 채널이 형성되지 않았다. 상호 합의된 세션키를 통해 암호화하지 않고 평문으로 $\triangle T$와 관련된 정보를 보낼 경우 무결성을 보장할 수 없다. 이런 경우 공격자는 $\triangle T$와 관련된 정보를 변경하여 DoS 공격을 할 수 있다. 따라서 LEO MCN의 지연 시간을 사용자 또는 NCC에게 안전하게 전달하는 절차가 필요하다.

다음은 동적으로 $\triangle T$를 설정하기 위해서 Altaf[3]의 인증 프로토콜을 수정한 인증 절차이다. 그림 3에서 기존 프로토콜에서 수정된 부분은 적색으로 표시하였다.

3.2.1 Registration Phase

Registration Phase는 사용자가 NCC에 사용자 정보를 등록하는 과정이다. 이 단계에서는 사용자는 사용자 정보를 NCC에게 전달하고 이후 단계에서 필요한 로그인 및 인증 정보를 NCC로부터 안전한 채널을 통하여 받는다.

3.2.2 Login and Authentication Phase

Login and Authentication Phase에서는 그림 3의 절차에 따라서 사용자와 NCC 사이의 상호인증이 이루어진다.

Step 1: 사용자는 인증을 하는데 필요한 정보 ($Auth_u$, PID_u, Q_u)를 생성하고 메시지를 보내는 시간 t_1와 함께 SAT-User에 전송한다. 여기서 $Auth_u$는 t_1가 포함된 해시함수로 생성된다. 따라서 만약 공격자가 t_1를 변경한다면 수신 측에서 이를 탐지하여 메시지를 폐기한다.

Step 2: SAT-User가 LEO MCN 내의 여러 ISL을 통해서 SAT-NCC에게 인증 메시지를 전달한다. 이 과정에서 기존 프로토콜과 달리 메시지가 지나가는 Inter-plane ISL의 홉 수(H_{inter})와 Intra-plane ISL의 홉 수(H_{intra})가 메시지에 포함되어 전달된다. 이때 LEO MCN 내부의 ISL은 FSO 통신을 이용하기 때문에 간섭이나 탈취로부터 안전하다고 가정한다[14].

Step 3: SAT-NCC는 인증 메시지를 받으면 H_{inter}와 H_{intra}를 활용하여 수식 (3)을 통해 t_{ISL1}을 계산한다.

Step 4: SAT-NCC는 Secure Channel을 통하여 인증 메시지와 함께 t_{ISL1}을 NCC에게 전달한다. NCC와 SAT-NCC는 Secure Channel을 이용할 수 있다고 가정한다[6]. 일반적으로 NCC는 SAT-NCC와 상호인증이 완료되었기 때문에 Secure Channel을 이용할 수 있다.

Step 5: NCC에서는 메시지가 도착하면 도착시간

(t_n)을 기록한다. 또한 NCC는 기존 프로토콜과 달리 t_{ISL1}를 이용하여 수식(2)에 따라 $\triangle T_{NCC}$를 생성한다. 그리고 수식 (1)를 만족하는지 확인하여 만족하는 경우에만 다음 단계로 진행하고 그렇지 않으면 메시지를 폐기하고 인증 절차를 중단한다. 다음으로 NCC는 수신한 인증정보($Auth_u$, PID_u, Q_u)를 통하여 적법한 사용자인지 확인한다. 인증에 성공하면 인증에 필요한 인증 정보(W_n, $Auth_n$)를 생성한다.

Step 6: NCC는 SAT-NCC에게 인증 메시지를 Secure Channel로 보낸다. 이때 인증 메시지에는 기존 프로토콜과 다르게 인증 정보와 메시지의 전송 시각(t_2)과 함께 NCC의 RTT($t_{RTT-NCC}$), 서버의 개인키(msk)를 추가하여 전송한다.

Step 7: SAT-NCC는 인증 메시지를 LEO MCN을 통하여 SAT-User에게 전달한다. 이때도 메시지가 지나오는 ISL 홉 수(H_{inter}', H_{intra}')가 함께 전달된다. SAT-User는 H_{inter}'와 H_{intra}'를 이용하여 수식 (3)에 따라 t_{ISL2}를 계산한다. 그리고 기존 프로토콜과 달리 NCC로부터 전달 받은 서버의 개인키(msk)를 이용하여 t_{ISL2}과 $t_{RTT-NCC}$를 수식 (9)와 같이 비대칭키 암호화한다.

$$E_n = E_{msk}(t_{ISL2} + \frac{1}{2}t_{RTT-NCC}) \quad (9)$$

Step 8: SAT-User는 사용자에게 인증 메시지와 t_2 그리고 비대칭키 암호화된 값(E_n)를 전송한다. 이때 통신 링크는 공격자에게 노출되어 있다. 그러나 공격자는 서버의 개인키를 알 수 없기 때문에 E_n를 변경할 수 없다. 또한 $Auth_n$은 t_2가 포함된 해시함수에 의해 생성되기 때문에 공격자는 t_2를 변경할 수 없다. 따라서 사용자는 메시지의 무결성을 확인할 수 있다.

Step 9: 사용자는 메시지를 수신하면 수신시각(t_u)를 기록한다. 그리고 사용자는 서버의 공개키(mpk)를 이용하여 E_n을 복호화한다. 그 결과를 이용하여 사용자는 수식 (2)에 따라 $\triangle T_{User}$를 계산한다. 그리고 수식 (1)에 따라 재생 공격이 일어났는지 확인하고 수식을 만족하는 경우에만 다음 단계로 진행한다. 마지막으로 NCC에서 보낸 인증 정보를 통해 NCC와 사용자의 상호인증이 완료되면 이후의 암호 통신에 사용되는 세션키가 생성된다.

Ⅳ. 모의실험

4.1 모의실험 모델 및 파라미터

본 논문에서는 모의실험을 통해 고정된 값의 타임스탬프 허용 범위를 사용하는 경우와 제안기법을 사용하는 경우를 비교하여 제안기법이 재생공격을 방지하는데 효과적임을 보였다. 모의실험을 위하여 LEO MCN을 그림 4와 같이 모델링하였다. 인증 메시지가 전송되는 시간은 위성이 이동하는 시간보다 충분히 짧기 때문에 실험 과정 중에 위성의 상대적인 위치는 변화하지 않는다고 가정한다. 따라서 실험 중 ISL의 길이는 고정되어 있다. 모의실험에 활용한 파라미터는 표 1에 정리하였다.

그림 4는 LEO MCN의 일부를 격자 모양으로 간소화시킨 모델이다. LEO MCN은 15개의 Inter-plane ISL과 15개의 Intra-plane ISL로 이루어져 있다. 모든 ISL의 길이는 2900km로 동일하게 설정하였다.

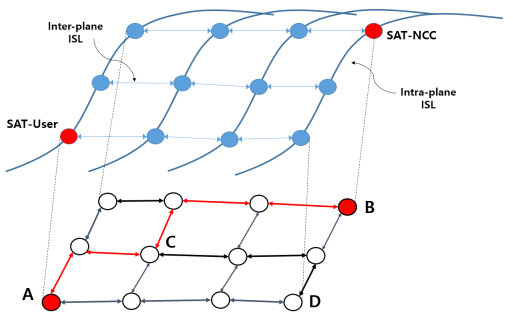

그림 4. 간소화된 LEO MCN 모델
Fig. 4. Simplified LEO MCN Model

표 1. 모의실험 파라미터
Table 1. Simulation parameters

환경변수	값
저궤도 위성의 고도(h)	550km
공격자의 최대 고도	10km
N_p	15
M_p	15
Phasing Factor (F)	0
$t_{RTT-NCC}$	10ms
$t_{RTT-\min}$	3.7ms
$t_{RTT-MAX}$	18.2ms
ISL Processing delay(t_{proc})	1.0ms
Attacker processing delay($t_{proc-※acker}$)	10ms

SAT-User는 SAT-NCC에게 인증 메시지를 전송한다. 메시지가 이동하는 경로는 메시지를 전송할 때의 ISL의 링크 상태에 따라서 달라진다. 따라서 메시지가 가장 적은 홉 수로 전송되지 않을 수도 있다. 이를 구현하기 위해서 전송된 메시지는 0.9의 확률로 SAT-NCC와 가까운 방향으로 이동하지만 0.1의 확률로 반대 방향으로 이동하도록 설정하였다. 예를 들어 그림 4에서 A에서 B로 이동할 때, C에서는 오른쪽과 위쪽으로 이동할 확률은 각각 0.45이고 왼쪽과 아래쪽으로 이동할 확률은 각각 0.05이다. 그리고 D에서는 0.9의 확률로 위쪽으로 이동하고 나머지 방향으로는 동일하게 1/30의 확률로 이동한다.

4.2 모의실험 결과

모의실험에서는 고정된 타임스탬프 허용 범위를 사용했을 때와 제안기법을 사용했을 때 공격자가 재생공격에 성공할 확률을 비교한다. 또한 고정된 타임스탬프 허용 범위와 제안기법을 사용했을 때 메시지가 폐기될 확률에 대해서도 비교한다. 그리고 Inter-plane ISL과 Intra-plane ISL의 홉 수를 변화시키면서 실험을 진행하여 홉 수의 변화에 따른 제안기법의 효과성을 확인하였다. 이때 고정된 타임스탬프 허용 범위 값은 수식 (10), (11)이다.

수식 (10)은 타임스탬프 허용 범위를 큰 고정값($\triangle T_{large\,fixed}$)으로 설정하는 수식이고, 수식 (11)은 작은 고정값($\triangle T_{small\,fixed}$)으로 설정하는 수식이다. 수식 (10), (11)에서 타임스탬프의 허용 범위는 위성의 지상 수신범위 내에서 RTT의 최댓값($t_{RTT-MAX}$)과 위성의 고도(h)으로 구성되기 때문에 저궤도 위성의 고도가 일정하다면 고정된 값이 된다.

$$\triangle T_{large\,fixed} = 2t_{RTT-MAX} + \frac{7\pi(R_E+h)}{4c} \quad (10)$$

$$\triangle T_{small\,fixed} = t_{RTT-MAX} + \frac{5\pi(R_E+h)}{4c} \quad (11)$$

$$t_{ISL} + \frac{1}{2}t_{RTT-NCC} + \frac{1}{2}t_{RTT-attacker} + t_{proc-attacker} < \triangle T \quad (12)$$

$$t_{ISL} + \frac{1}{2}t_{RTT-NCC} + \frac{1}{2}t_{RTT-User} > \triangle T \quad (13)$$

수식 (12)는 공격자가 재생공격을 하는데 걸리는 시간이 타임스탬프 허용 범위보다 작은 상황을 의미한다. 공격자가 재생공격을 하는데 걸리는 시간은 LEO MCN에서의 지연 시간(t_{ISL})과 공격자와 위성 사이의 지연 시간($t_{RTT-\mathrm{attacker}}$), 공격자의 처리 지연($t_{proc-\mathrm{attacker}}$)을 합한 값으로 나타낼 수 있다. 따라서 수식 (12)를 만족하는 경우 공격자의 메시지가 타임스탬프 허용 범위 안에 들어왔기 때문에 재생공격에 성공했다고 볼 수 있다. 이때 공격자와 사용자는 충분히 가깝기 때문에 공격자와 사용자 사이의 경로 지연은 매우 작으며, 공격자의 처리 지연($t_{proc-\mathrm{attacker}}$)은 10ms로 가정한다. 또한 공격자와 위성 사이의 경로지연은 수식 (7)을 활용하여 계산했을 때 최댓값 8.8ms, 최솟값 1.5ms를 갖는다.

모의실험에서는 100번의 시행 중에서 수식 (12)를 만족하는 횟수를 확률로 나타내고 이를 10회 수행한 평균값을 구한다. 그림 5은 Intra-plane ISL의 홉 수를 4로 고정하고 Inter-plane ISL의 홉 수를 3부터 7까지 변화시켰을 때 재생공격 성공 확률을 나타낸 것이다.

$\triangle T_{large\,fixed}$를 사용할 경우 항상 재생공격이 성공할 확률이 높다. 그리고 $\triangle T_{small\,fixed}$을 사용하는 경우, Inter-plane ISL 홉 수가 6 이하일 때는 효과적으로 재생공격을 방지할 수 없었다. 왜냐하면 LEO MCN에서 지연이 짧기 때문에 공격자가 재생공격을 할 수 있는 충분한 시간이 주어지기 때문이다.

그러나 제안된 $\triangle T$를 사용할 경우 ISL 홉 수에 상관없이 항상 재생공격이 성공할 확률이 0임을 확인할 수 있다.

그림 6은 Inter-plane ISL의 홉 수를 4로 고정하고

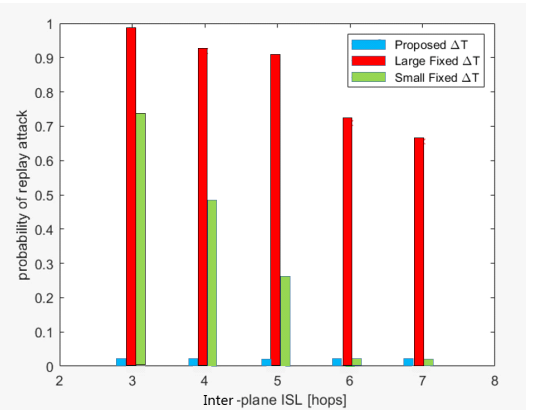

그림 5. Inter-plane ISL의 홉 수를 변화시켰을 때 공격 성공 확률
Fig. 5. Probability of attack, when the number of inter-plane ISL hops changes

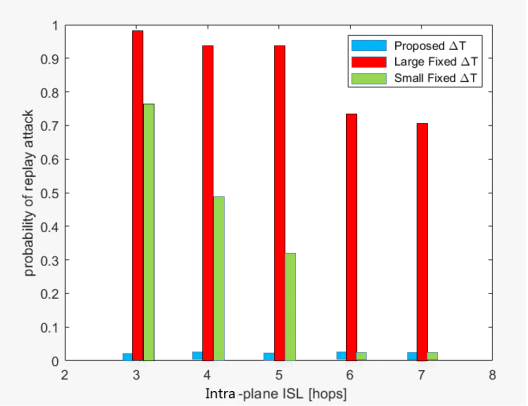

그림 6. Intra-plane ISL의 홉 수를 변화시켰을 때 공격 성공 확률
Fig. 6. Probability of attack, when the number of intra-plane ISL hops changes

Intra-plane ISL의 홉 수를 3부터 7까지 변화시켰을 때 재생공격 성공 확률을 나타낸 것이다. 마찬가지로 $\triangle T_{large\,fixed}$를 사용하면 항상 재생공격의 위협이 크다. 그리고 $\triangle T_{small\,fixed}$를 사용하면 Intra-plane ISL의 홉 수가 5 이하일 때는 재생공격을 효과적으로 방지할 수 없었다. 그러나 제안된 $\triangle T$를 사용하면 항상 재생공격에 성공할 확률이 0임을 확인할 수 있다. 따라서 고정된 타임스탬프 허용 범위를 사용할 때와 달리 제안기법을 사용하면 메시지가 이동하는 거리와 상관없이 재생공격을 방지할 수 있음을 알 수 있다.

수식 (13)은 정상 사용자가 메시지를 보냈을 때 타임스탬프의 허용 범위를 넘어서서 메시지가 폐기되는 상황을 의미한다. $\triangle T$를 작게 설정하면 재생공격의 확률은 낮출 수 있지만 정상 메시지도 폐기되어 통신의 품질이 저하된다. 따라서 재생공격의 성공 확률을 낮추는 것과 함께 정상 메시지의 폐기 확률을 낮추는 것 역시 중요하다. 정상 사용자가 보낸 메시지가 도착하는 시간은 수식 (13)의 좌변처럼 LEO MCN에서의 지연 시간(t_{ISL})과 사용자와 SAP-User 사이의 지연 시간, NCC와 SAP-NCC 사이 지연 시간의 합으로 나타낼 수 있다. 모의실험에서는 100번의 시행 중에서 수식 (13)을 만족하는 횟수를 확률로 나타내고 10회 수행한 평균값을 구한다. 이때 $t_{RTT-User}$는 $t_{RTT-\min}$와 $t_{RTT-MAX}$ 사이에서 무작위로 설정된다.

그림 7은 Intra-plane ISL의 홉 수를 4로 고정하고, Inter-plane ISL의 홉 수를 3부터 7까지 변화시켰을 때 정상 메시지가 폐기될 확률을 나타낸 것이다. $\triangle T_{small\,fixed}$를 사용하면 정상 메시지가 폐기될 확률

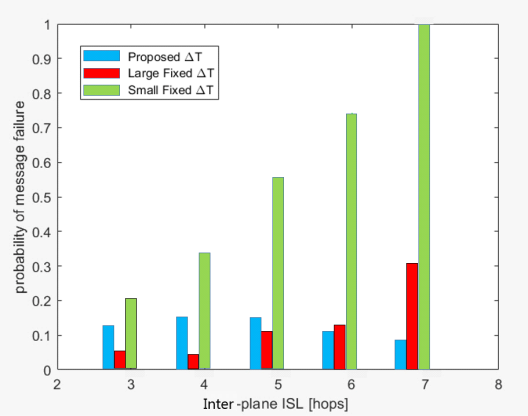

그림 7. Inter-plane ISL의 홉 수를 변화시켰을 때 메시지 폐기 확률
Fig. 7. Probability of message failure, when the number of inter-plane ISL hops changes

이 높게 나타난다. 그리고 $\triangle T_{large\,fixed}$를 사용하면 대체적으로 낮은 메시지 폐기 확률을 보였으나, Inter-plane ISL의 홉 수가 증가할수록 정상 메시지의 폐기 확률이 증가하였다. 반면에 제안된 $\triangle T$는 모든 홉 수에서 0.1 내외의 낮은 메시지 폐기 확률을 나타냈다.

그림 8는 Inter-plane ISL의 홉 수를 4로 고정하고, Intra-plane ISL의 홉 수를 변화시키면서 정상 메시지가 폐기될 확률을 나타낸 것이다. $\triangle T_{small\,fixed}$를 사용했을 때는 정상 메시지의 폐기 확률이 항상 높았다. 그리고 $\triangle T_{large\,fixed}$를 사용할 때는 홉 수가 증가할수록 정상 메시지의 폐기 확률이 증가하였다. 그러나 제안 기법을 사용할 경우 항상 메시지의 폐기 확률이 낮

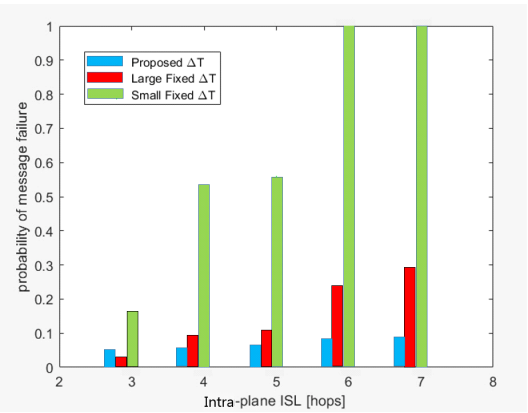

그림 8. Intra-plane ISL의 홉 수를 변화시켰을 때 메시지 폐기 확률
Fig. 8. Probability of message failure, when the number of intra-plane ISL hops changes

은 것을 확인할 수 있었다.

모든 결과 그래프를 종합했을 때, 제안 기법을 사용하면 고정된 타임스탬프 허용 범위를 사용할 때보다 효과적으로 재생공격을 방지할 수 있었다. 또한 $\triangle T$가 너무 작게 설정되어 정상 메시지가 폐기되는 경우도 방지할 수 있었다. 그리고 제안기법은 고정된 $\triangle T$와 달리 종단 간 거리에 상관없이 적용 가능함을 확인할 수 있었다.

V. 결 론

본 논문에서는 대형 저궤도 군집 위성 네트워크에서 종단 간 전파 지연을 고려하여 동적으로 타임스탬프 허용 범위를 설정하는 방법을 제안하였다. 또한 이 제안 기법을 실용적으로 사용할 수 있도록 인증 과정에서 동적인 타임스탬프 허용범위를 사용할 수 있는 절차를 제안하였다. 그리고 모의실험을 통하여 제안기법이 종단 간 거리에 상관없이 재생공격의 위협을 감소시키면서, 동시에 타임스탬프 기법으로 인하여 정상 메시지가 폐기되는 문제도 방지할 수 있음을 확인하였다.

References

[1] Q. Chen, G. Giambene, L. Yang, C. Fan, and X. Chen, “Analysis of inter-satellite link paths for LEO mega-constellation networks,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2743-2755, Mar. 2021.

[2] G. Z. Qu, H. Cao, and J. Xie, “LEO satellite constellation for internet of things,” *IEEE Access*, vol. 5, pp. 18391-18401, Aug. 2017.

[3] B. Li, Z. Fei, C. Zhou, and Y. Zhang, “Physical layer security in space information networks: A survey,” *IEEE Internet of Things J.*, vol. 7, no. 1, pp. 33-52, Jan. 2020.

[4] C. Jiang, X. Wang, J. Wang, H. Chen, and Y. Ren, “Security in space information networks,” *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 82-88, Aug. 2015.

[5] I. Altaf, M. A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary, and C. Chen, “A lightweight key agreement and authentication scheme for satellite-communication systems,” *IEEE Access*, vol. 8, pp. 46278-46287, Mar. 2020.

[6] K. Xue, et al., “A secure and efficient access and handover authentication protocol for internet of things in space information networks,” *IEEE Internet of Things J.*, vol. 6, no. 3, pp. 5485-5499, Jun. 2019.

[7] J. Guo and Y. Du, “A novel RLWE-Based anonymous mutual authentication protocol for space information network,” *Secur. and Commun. Netw.*, pp. 1-12, Aug. 2020.

[8] J. Guo and Y. Du, “A secure three-factor anonymous roaming authentication protocol using ECC for space information networks,” *Peer-to-Peer Netw. Appl.*, vol. 14, pp. 898-916, Jan. 2021.

[9] I.-A Song and Y.-S. Lee, “Timestamp based key exchange protocol for satellite access network,” *J. KIIECT*, vol. 9, no. 2, pp. 162-170, Apr. 2016.

[10] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, “A survey of Internet of Things (IoT) authentication schemes,” *Sensors*, vol. 19, no. 5, pp. 1141-1180, Mar. 2019.

[11] A. Baayer, et al., “Enhanced timestamp discrepancy to limit impact of replay attacks in MANETs,” *J. Inf. Secur.*, vol. 3, no. 3, pp. 224-230, May 2012.

[12] F. Farha and H. Ning, “Enhanced timestamp scheme for mitigating replay attacks in secure ZigBee networks,” *IEEE Int. Conf. SmartIoT*, pp. 469-473, Aug. 2019.

[13] Y. Su, Y. Liu, Y. Zhou, J. Yuan, H. Cao, and J. Shi, “Broadband LEO satellite communications: Architectures and key technologies,” *IEEE Wireless Commun.*, vol. 26, no. 2, pp. 55-61, Apr. 2019.

[14] M. Motzigemba, H. Zech, and P. Biller, “Optical inter satellite links for broadband networks,” *Int. Conf. RAST*, pp. 509-512, Jun. 2019.

[15] N. J. H. Marcano, L. Diez, R. A. Calvo, and R. H. Jacobsen, “On the queuing delay of time-varying channels in low earth orbit satellite constellations,” *IEEE Access*, vol. 9, pp. 87378-87390, Jun. 2021.

현 준 열 (Junyeol Hyun)

2022년 2월 : 아주대학교 국방디지털융합학과 졸업

<관심분야> 위성통신, 사이버전, 네트워크 보안

[ORCID:0000-0001-8661-3040]

이 민 우 (Minwoo Lee)

1998년 2월 : 한국항공대학교 항공통신정보공학과 졸업

2013년 2월 : 아주대학교 일반대학원 NCW공학 박사 졸업

2019년 3월 : 아주대학교 국방디지털융합학과 대우교수

<관심분야> 위성통신, 네트워크 보안, 사이버전자전

[ORCID:0000-0001-7109-4700]

임 재 성 (Jaesung Lim)

1983년 2월 : 아주대학교 전자공학 학사

1985년 2월 : KAIST 영상통신 석사

1994년 8월 : KAIST 디지털통신 박사

1995년 9월~1998년 2월 SK텔레콤 중앙연구원 책임연구원

1998년 3월~현재 : 아주대학교 국방디지털융합학과 정교수

2006년 8월~현재 : 아주대학교 국방전술네트워크 연구센터장

<관심분야> 이동 및 위성통신, 무선네트워크, 국방전술통신

[ORCID:0000-0003-0080-9398]