양자키 분배망에서의 시간 주도형 동기화 기법에 관한 연구

이상주

썬웨이브텍

angelet86@sunwave.co.kr

A Study on Server-Initiated Time Synchronization in Quantum Key Distribution Networks

Lee Sangju

SunwaveTech

요 약

본 논문은 양자키분배망(QKDN) 환경에서 기존 client-initiated 시간 동기화 방식의 한계를 분석하고, 서버 주도형 시간 동기화(SITS) 기법을 제안하였다. ITU-T SG13에서 논의 중인 SITS 개념을 기반으로 계층적 QKDN 운영 모델을 정립하고, 3계층 시뮬레이션을 통해 성능을 정량적으로 비교하였다. 실험 결과, 제안 기법은 Client 계층에서 시간 동기화 정확도와 장애 복구 성능을 유의미하게 향상시킴을 확인하였다.

Ⅰ. 서 론

본 논문에서는 양자키분배(QKD)는 양자역학적 원리를 이용하여 도청 여부를 물리적으로 검출할 수 있는 보안 기술로, 차세대 국가·공공 통신 인프라의 핵심 요소로 주목받고 있다. 최근에는 단일 링크 중심의 QKD를 네트워크 형태로 확장한 양자키분배망(QKDN)이 제안되고 있으며, 이 과정에서 시간 동기화는 키 생성 성공률과 네트워크 안정성을 좌우하는 핵심 요소로 작용한다. 특히 QKD 시스템은 시간 창(time window) 기반 검출 방식을 사용하므로, ms 수준의 오차만으로도 키 폐기율 증가 및 재전송 비용 상승이 발생할 수 있다.

현재 대부분의 QKDN은 NTP 기반 client-initiated 동기화 방식을 사용하고 있으나, 이 방식은 네트워크 혼잡, 비대칭 경로, GNSS 장애 상황에서 시간 정확도가 급격히 저하되는 문제가 보고되고 있다. 이러한 한계를 극복하기 위해 본 논문에서는 서버가 능동적으로 시간 정보를 배포하는 server-initiated 동기화 모델을 QKDN 환경에 적용하고 그 효과를 분석한다.

Ⅱ. 관련연구

본 논문에서는 ITU-T Y.3800 시리즈는 QKDN의 기능 구조와 관리 모델을 정의하고 있으며, Supplement 89는 QKD 시스템에서 요구되는 시간 동기화 요소를 기술하고 있다. 그러나 기존 표준 문서는 client-initiated 방식 중심으로 구성되어 있어, 서버 주도형 시간 배포 모델에 대한 체계적인 논의는 부족하다.

한편 NTP 및 IEEE 1588(PTP)은 범용 네트워크 환경에서 높은 정확도를 제공하지만, QKDN이 요구하는 패킷 인증, 무결성 보호, 재생 공격 방지와 같은 보안 요구사항을 완전히 만족하기에는 구조적 한계가 존재한다. 이러한 배경에서 ITU-T SG13에서는 QKDN 특화 시간 동기화 모델로서 SITS를 Supplement 형태로 논의하고 있다.

Ⅲ. 본문

본 논문에서는 양자키분배망(QKDN) 환경에 적합한 서버 주도형 시간 동기화(Server-Initiated Time Synchronization, SITS) 구조를 기반으로 한 운영 모델을 제안한다. SITS는 상위 시간 서버가 하위 노드에 대해 시간 정보를 능동적으로 배포하는 방식으로, 기존 client-initiated 방식과 달리 하위 노드의 요청 없이도 시간 동기화가 수행되는 구조적 특징을 가진다. 이러한 구조는 다수의 노드가 계층적으로 연결된 QKDN 환경에서 시간 편차 누적을 방지하고, 노드 간 시간 일관성을 유지하는 데 유리하다.

제안하는 SITS 구조에서 최상위 계층(L1)은 GNSS 또는 국가 표준시와 동기화된 신뢰 가능한 기준 시각을 확보한다. 이후 해당 기준 시각은 중간 계층(L2, L3)을 거쳐 최종 Client 노드로 계층적으로 전달된다. 각 계층은 상위 계층으로부터 수신한 시간 정보를 기반으로 로컬 시각을 보정하며, 이를 다시 하위 계층으로 전달하는 중계 역할을 수행한다. 이러한 계층적 전달 구조는 QKDN의 확장성을 고려한 설계로, 네트워크 규모가 증가하더라도 시간 동기화 관리 복잡도를 효과적으로 제어할 수 있다.

또한 SITS는 주기적 배포 방식과 이벤트 기반 배포 방식을 모두 지원한다. 정상 동작 상태에서는 사전에 정의된 주기에 따라 시간 패킷이 주기적으로 전송되며, 이를 통해 지속적인 시간 동기화 상태를 유지한다. 반면 네트워크 장애, 시간 편차 급증, 상위 계층과의 연결 복구와 같은 특정 이벤트가 발생할 경우에는 이벤트 기반 동기화가 수행된다. 이 방식은 장애 이후 빠른 시간 수렴을 가능하게 하여, 기존 주기 기반 방식 대비 복구 시간을 단축시키는 효과를 가진다.

보안 측면에서 QKDN 환경의 시간 정보는 단순한 관리 데이터가 아닌 보안 자산으로 간주될 수 있으므로, SITS에서는 시간 패킷에 대한 엄격한 보안 검증 절차를 포함한다. 각 노드는 수신한 시간 패킷에 대해 메시지 인증 코드(MAC) 또는 디지털 서명을 검증함으로써 패킷의 무결성과 송신자의 신뢰성을 확인한다. 이를 통해 위·변조된 시간 정보가 적용되는 것을 방지할 수 있다.

아울러 재생 공격(replay attack)을 방지하기 위해 sequence number 또는 타임스탬프 기반 검증 메커니즘을 적용한다. 각 노드는 이전에 처리된 패킷보다 오래된 시간 패킷을 자동으로 폐기함으로써, 공격자가 과거의 시간 정보를 재전송하여 시스템 동작을 교란하는 것을 차단한다. 이러한 보안 메커니즘은 QKDN 환경에서 요구되는 높은 신뢰성과 안전성을 충족하기 위한 필수 요소이다.

종합적으로 제안하는 SITS 기반 시간 동기화 구조는 계층적 QKDN 환경에서 시간 일관성 유지, 장애 복구 성능 향상, 그리고 보안 요구사항 충족이라는 측면에서 기존 client-initiated 방식 대비 구조적 이점을 제공한다. 이는 이후 장에서 제시하는 시뮬레이션 기반 성능 평가를 통해 정량적으로 검증된다.

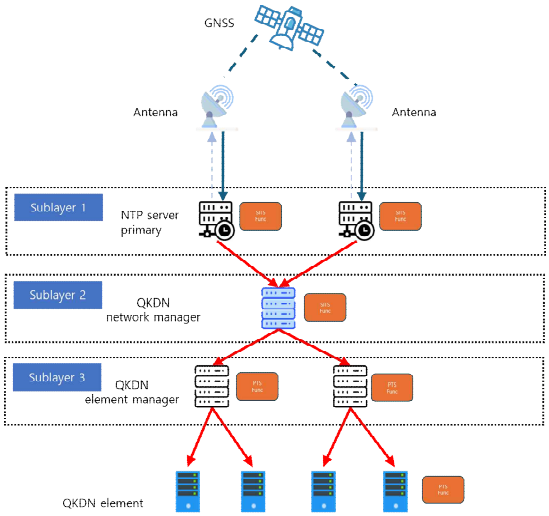

그림 1 Server-Initiated Time Synchronization 구조도

Ⅳ. 성능평가

본 논문의 성능 평가는 L1 - L2 - L3 - Client로 구성된 3계층 시뮬레이션 환경에서 수행되었다. 각 계층은 QKDN의 계층적 시간 전달 구조를 모사하며, 상위 계층의 시간 서버가 하위 노드에 시간 정보를 전달하는 구조로 구성된다. 시뮬레이션은 총 2.5시간 동안 Δt = 0.1 s 간격으로 수행되었다.

네트워크 장애 상황을 고려하기 위해 1800 - 2400 s 구간에서는 패킷 손실률을 정상 상태 대비 8배 증가시키고, 전송 지연을 50 ms 추가하여 네트워크 혼잡 및 링크 품질 저하 상황을 모델링하였다. 이는 실제 QKDN 환경에서 발생 가능한 링크 장애 및 트래픽 집중 상황을 반영하기 위한 설정이다.

시간 동기화 성능을 정량적으로 평가하기 위해 RMS 오차와 P95 오차를 정확도 지표로 사용하였다. RMS 오차는 평균적인 시간 편차를 나타내며, P95 오차는 오차 분포의 상위 값을 통해 극단적인 시간 오차 발생 가능성을 평가한다. 또한 장기적인 시간 동기화 품질을 평가하기 위해 AUC(Area Under the Curve)를 사용하였다.

장애 이후의 회복 특성을 분석하기 위해 임계치 초과 시간(AOT)과 장애 복구 시간을 추가적으로 평가하였다. AOT는 시간 오차가 특정 임계값을 초과한 상태로 유지된 누적 시간을 의미하며, 장애 이후 시스템의 안정화 정도를 평가하는 지표이다.

시뮬레이션 결과, 서버 주도형 시간 동기화 기법은 기존 client-initiated 방식 대비 Client 계층에서 RMS 및 P95 오차가 감소하는 경향을 보였으며, 장애 이후 빠른 시간 수렴 특성을 나타냈다. 특히 AOT가 감소하여 시스템이 허용 가능한 시간 오차 범위로 복귀하는 데 소요되는 시간이 단축됨을 확인하였다. 이러한 결과는 제안 기법이 QKDN 환경에서 단기 정확도와 장애 복구 성능 측면에서 효과적임을 보여준다.

임계값	Client-Initiated	Server-Initiated	Δ(%)
1ms	32284.8	22159.6	-31.4%
2ms	27484.9	17368.0	-36.8%
5ms	13087.0	5211.4	-60.2%

표 1 Area-Over-Threshold after Outage

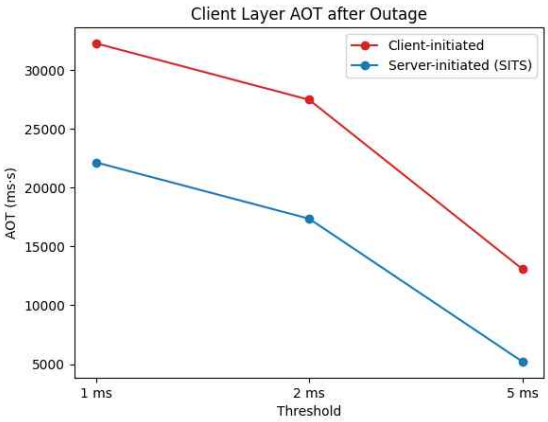

그림 2 Area-Over-Threshold after Outage 그래프

Ⅴ. 결론

본 논문에서는 양자키분배망(QKDN) 환경에서 서버 주도형 시간 동기화 기법의 구조적 특징과 성능 효과를 분석하였다. 제안 기법은 상위 시간 서버가 시간 정보를 능동적으로 배포하는 구조를 통해 기존 client-initiated 방식에서 발생하는 시간 편차 누적 문제를 완화하며, 계층적 QKDN 환경에서 노드 간 시간 일관성을 유지하는 데 효과적임을 확인하였다.

시뮬레이션 결과, 제안 기법은 특히 Client 계층에서 시간 동기화 정확도를 향상시키고, 네트워크 장애 이후 빠른 시간 수렴 특성을 보여 장애 복구 성능 측면에서 유의미한 개선 효과를 나타냈다. 이는 QKDN 운영 환경에서 키 정합 실패율 감소 및 서비스 안정성 향상으로 이어질 수 있음을 의미한다.

향후 연구에서는 제안 기법의 실용성을 보다 명확히 검증하기 위해 실증망 기반 평가를 수행하고, 대규모 노드 확장 환경에서의 성능 특성을 분석할 예정이다. 또한 시간 패킷 인증 및 무결성 검증 과정에서 발생하는 암호 오버헤드를 최소화하기 위한 최적화 방안과, 기존 시간 동기화 메커니즘과의 상호 운용성에 대한 추가 연구를 진행할 계획이다.

참 고 문 헌

[1] ITU-T Recommendation Y.3800, Overview on networks supporting quantum key distribution, 2019.

[2] ITU-T Supplement 8, Time synchronization aspects in QKD systems, 2023.

[3] ITU-T SG13 TD327/WP4, Draft Supplement Y.supp.QKDN-SITS, 2025.