양자 공격에 대비한 스마트 그리드 시스템에 PQC암호화 적용 가능성 연구

안종민, 김태식 , 정재학*

인하대학교, Texas A&M kingsvile[1]

anjong3@naver.com, Taesic.Kim@tamuk.edu[1], *jchung@inha.ac.kr

A Study on the Applicability of PQC to Smart grid system

Jongmin Ahn, Teasic Kim, Jeahak Chung*

Inha Univ., Texas A&M kingsvile[1]

요 약

스마트 그리드 시스템의 발전에 따라 스마트 그리드의 네트워크 보안 또한 중요해 지고 있지만 양자 컴퓨팅 분야가 발전됨에 따라 기존 암호화 방법의 보안성이 위협받으며 스마트 그리드 네트워크의 안전 또한 위협받는 상황이다. 이에 따라 본 논문에서는 양자 컴퓨팅 공격에 대비한 기술인 PQC 암호화 방법이 현재 스마트 그리드에 적합한지 분석한다. 스마트 그리드에서 가장 많이 사용되는 스마트 미터는 저 전력, 저 사향의 small device 로 전력 소모에 따른 베터리 수명이 매우 중요하다. 이에 본 논문에서는 스마트 미터가 PQC를 사용하는 경우 기대되는 배터리 수명을 예측하여 PQC의 스마트 그리드 적용 가능성을 분석하였다.

Ⅰ. 서 론

최근 스마트 그리드 기술이 발전에 따라 그리드를 효과적으로 운용하고 관리하기 위해 최신 정보 통신 기술이 적용되고 있다. 이에 따라 스마트 그리드의 안정성을 위해서는 통신 네트워크의 보안성을 높여야한다[1]. 스마트 그리드 네트워크는 TLS를 이용해 보안을 유지한다. TLS는 수학적 난해함에 의존해 보안성을 유지하거나 decryption key가 많은 경우의 수에 의해 보안성을 유지한다. 그러나 양자 컴퓨터의 발달로 많은 수학적 난해한 문제가 빠르게 풀리고 연산속도가 비약적으로 증가하면서 보안성이 위협을 받고 있다. PQC 와 같은 새로운 암호화 방법이 개발되고 있다. 이에 따라 스마트 그리드 네트워크의 보안성을 높이기 위해 PQC를 적용한 연구가 필요하다. 따라서 본 논문에서는 스마트 그리드에서 양자공격으로부터 통신 보안을 유지하기 위해 PQC의 스마트 그리드 적용가능성에대해 알아본다.

Ⅱ. 본론

양자 컴퓨터의 개발에 따라 기존의 암호 기술의 보안성이 위협받으며 이에 맞춰 양자 컴퓨터의 연산 속도로도 해독할 수 없는 암호화 기술이 개발되고 있다. 그러나 이 PQC는 기존 암호화 알고리즘 보다 큰 계산 복잡도를 갖기 때문에 스마트 미터와 같이 전력 저전력을 요구하는 small device에 적합하지 않을 수 있다. 실제로 대다수의 스마트 미터는 16-bit/ 32-bit processor를 사용한다. 따라서 PQC 알고리즘의 에너지 소모량이 스마트 그리드에 미치는 영향을 알아보기 위해 에너지 사용량에 따른 스마트 미터 혹은 센서의 수명을 계산해 보았다. PQC를 용할 때 필요한 에너지가라 하면 아래 식과 같이 나타낼 수 있다[37].

$$_{ot} \quad E_{kgen} + E_{nc} + E_{Dec} + E_{comm}(L_{bit}) \qquad (1)$$

식 (1)에서 는E_{kgen} key를 generation할 때, E_{Enc}는 암호화로 만들 때, E_{Dec}는 복호화 소모되는 에너지를 말한다. 는$E_{comm}(L_{bit})$ 키 및 cipher text를 전송할 때 소모되는 에너지로 KEM알고리즘은 는 public key 길이와 cipher text의 합 Sig. 알고리즘은 public key 길이와 signature 길이의 합이다. PQC를 적용한 스마트 미터가 12v 100Ah의 battery를 사용할 때 기대 수명을 그림 1에 나타내었다.

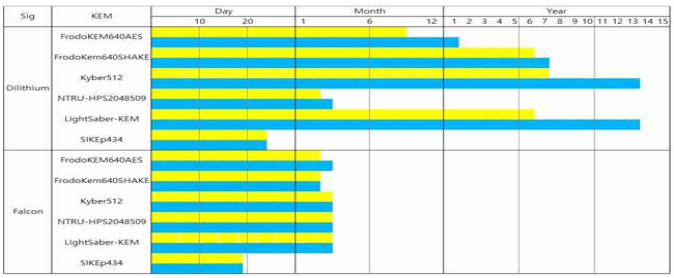

그림 1 PQC 적용 스마트 미터 배터리 수명

Ⅲ. 결론

일부 PQC 암호화는 1~5년의 수명을 보장하며 스마트 그리드에 적합한 것을 알 수 있다. 다수의 PQC가 적게는 수일에서 길어야 수십일의 수명을 보여 스마트 그리드에 적용하기에 어려운 결과를 보였다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음 (2020-0-01540)

참 고 문 헌

[1] B. Ahn, T. Kim, J. Choi, K. Park, and D. Won, “A cyber kill chain model for distributed energy resources (DER) aggregation systems,” in Proc. 2021 IEEE EEE Innovative Smart Grid Technologies Conference North America, in press.