양자통신 환경 상에서의 가용성 침해 공격

권혁동* 김현준* 김경호* 서화정*†

*한성대학교 IT융합공학부

An Availability Attacks on a Quantum Communication Environment

Hyeok-Dong Kwon* Hyun-Jun Kim* Kyung-Ho Kim* Hwa-Jeong Seo*†

*Division of IT convergence engineering, Hansung University.

요 약

패킷 스니핑 공격은 보안의 3요소로 알려진 기밀성, 무결성, 가용성 중 기밀성을 침해하는 공격으로 분류된다. 스니핑 공격은 통신 주체가 아닌 제 3자가 패킷을 감청하는 공격으로 일반적으로 피해자에게 직접적인 피해가 발생하지 않기에 공격 상황을 인지하기 어렵다. 양자 통신은 전기 신호를 대신 양자를 활용한 새로운 통신으로 기존 통신보다 월등한 처리 속도를 보여줄 것으로 기대되는 기술로 여기서 양자는 외부 관측 시 붕괴된다는 특성을 활용하여 스니핑 공격을 방어할 수 있다. 하지만 이러한 특성으로 인해 스니핑 공격이 양자 통신상에서는 가용성 공격으로 재분류될 수 있다. 본 논문에서는 전술한 상황이 발생하는 원인을 서술하며 이에 대한 대처 기법 및 향후 과제에 대해 확인한다.

I. 서론

사이버 보안은 각종 보안 위협으로부터 정보를 보호하기 위해 기밀성, 무결성, 가용성 세 가지를 보안 요소로 제시하게[1] 되었으며 각각의 의미는 다음과 같다. 첫째로 기밀성은 인가되지 않은 제 3자가 데이터를 열람하거나 확인할 수 없다는 속성이고 둘째로 무결성은 전송된 데이터가 원본과 동일하며 수정되지 않았음을 보장하는 성질이다. 마지막으로 가용성은 허가된 사용자에 한해 자유롭게 데이터에 접근 가능한 환경을 제공함을 의미한다. 이러한 보안 요소에 따라 표 1과[2] 같이 여러 보안 위협을 분류할 수 있다.

양자통신은 전기 신호를 이용한 고전통신과 다르게 양자를 활용한 것으로 0과 1의 이진 정보뿐만 아니라 중첩된 상태의 정보를 전송할 수도 있다. 양자통신의 장점 중 하나는 스니핑 공격에 강하다는 것으로, 양자는 외부에서 관측 시 붕괴되기 때문에 스니핑 공격 발생 시 양자 붕괴 여부로 공격 상황을 빠르게 파악할 수 있다. 하지만 이러한 양자통신의 특성으로 인해 스니핑 공격은 양자통신상에서 가용성 공격으로 분류될 수 있다.

표. 1. 보안 공격의 분류

Attack type	Attack name
Confidentiality	Sniffing, Scanning, Traffic analysis
Integrity	Spoofing, Modification, Fabrication, Masquerading, Replaying
Availability	Denial of Service, Interruption

본 논문에서는 양자통신상에서 스니핑 공격이 가용성 공격으로 분류될 수 있는 사유에 대해 분석하며 이에 따른 대처 방안과 앞으로 준비해야 할 방향에 대해서 제안한다.

II. 관련 연구 동향

2.1 양자

양자는 1899년 독일의 물리학자 막스 플랑크(Max Planck)가 흑체 복사와 관련된 문제를 연구하던 도중 플랑크 상수를 발견하였고 이 법칙을 설명하기 위해 양자의 개념을 제시하였다[3]. 양자는 더 이상 나눌 수 없는 에너지 최소량의 단위로 정의되어 있으며 원자가 물질의 기초 단위라면 양자는 에너지의 기초 단위가 된다.

2.2 양자붕괴

양자역학에서는 모든 상태가 확률에 기반하기 때문에 양자는 측정하기 전까지 확률적으로 중첩된 상태로 존재한다. 만약 양자를 관측한다면 그 순간 하나의 상태로 확정적으로 존재하게 되며 다른 상태로 될 가능성은 사라진다. 특히 양자 붕괴는 정보에도 영향을 끼치며 측정으로 인하여 정보가 붕괴하게 된다면 기존 상태로 되돌릴 수 없기에 정보가 유실되는 효과를 볼 수 있다[4].

현실 세계에서 그림 1과 같이 양자 붕괴와 비슷한 현상을 확인할 수 있다. 육면체 주사위를 굴릴 때 각각의 눈을 획득할 확률은 모두 1/6이다. 이때 주사위를 굴려서 5가 나온 것을 확인했다면, 그 순간 5가 나올 확률은 1이 되며 다른 눈이 나올 확률은 0으로 붕괴한다[5].

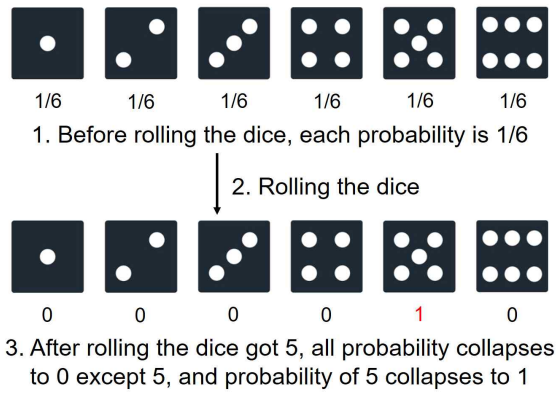

그림. 1. 양자붕괴의 예시

2.3 양자통신 프로토콜

BB84 프로토콜은 1984년 찰스 H. 베넷과 질 브라사드가 제안한 양자통신 프로토콜로서 송신자와 수신자간 OTP(One Time Pad)를 생성하는 프로토콜로[6] 가장 널리 알려진 최초의 양자 키 분배(Quantum Key Distribution, QKD) 프로토콜이다.

대략적인 통신 과정은 그림 2와 같다. 송신자는 양자 편광에 정보를 인코딩하여 값을 전송하고 수신자는 임의의 기저(basis)를 사용하여 값을 측정한다. 이후 송수신 양측은 일반 공개 채널을 통해 서로 사용한 기저 정보를 공유하고 일치하는 기저로 측정한 값만 취하여 시프트키(shifted key)를 생성한다. 본 과정까지 이상이 없었다면 마지막으로 시프트키에서 비밀키를 도출한다.

시프트키 생성 과정에는 도청의 가능성이 있기 때문에 송수신 양측은 오류의 비율을 계산하며 이를 QBER(Quantum Bit Error Rate)라 칭한다. 만약 특정 비트의 QBER가 임계점을 넘어선다면 공격받은 것으로 간주하고 시프트키를 파기한다.

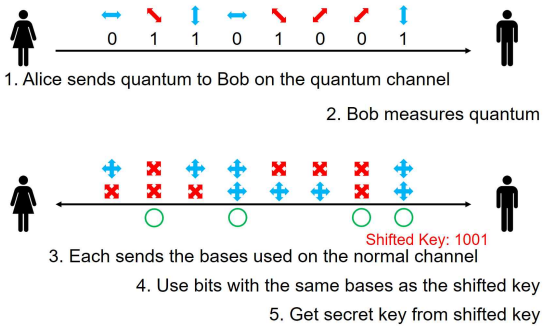

그림. 2. BB84 프로토콜 동작 과정

III. 공격 시나리오

2장에서 확인한 양자통신 프로토콜 BB84의 동작에 따르면 공격 대상은 일반채널과 양자채널 두 가지로 나눌 수 있으며 공격 대상에 따라 상이한 결과를 확인할 수 있다.

3.1 일반채널에 대한 공격

일반채널의 용도는 통신 주체가 서로 사용했던 기저 정보를 교환하기 위함으로 공격자가 일반채널을 공격하는데 성공하면 기저 정보를 획득할 수 있다.

기저 정보는 송신자 측에서는 비트를 인코딩 할 때 사용하며 수신자 측에서는 값 측정에 필터처럼 사용한다. 따라서 공격자가 기저 정보를 획득하더라도 이를 통해 추가적인 정보를 유추할 수가 없으며 일반채널에서는 키 생성을 위한 값이 전송되지 않으므로 일반채널 공격으로 유의미한 공격이 어렵다.

3.2 양자채널에 대한 공격

양자채널 상에는 송신자가 수신자 측에 비트를 담아 전송하는 양자가 존재한다. 따라서 공격자가 양자채널을 공격하는데 성공한다면 양자에 담긴 비트 값을 획득할 수 있다.

하지만 2.2절의 설명에서처럼 양자는 관측하는 순간 붕괴하여 하나의 상태로 확정적으로 존재하게 되며 기존 상태로 되돌릴 수 없게 된다. 즉, 그림 3과 같이 중간자가 양자채널을 도청하고 있다면 송수신자는 공격자가 있음을 인지할 수 있고, 키 교환을 중단할 수 있다.

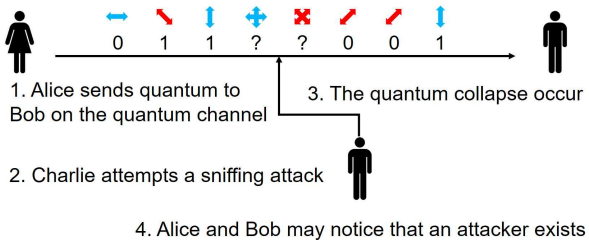

그림. 3. BB84 프로토콜의 공격자 감지 기법

결과적으로 공격자는 양자채널을 도청하더라도 공격 대상이 공격 상황을 인지하기 때문에 공격이 어려울 뿐더러 관측한 값에 양자붕괴가 발생하므로 원본 값에 손실이 발생한다. 때문에 정확한 값 확보 역시 어렵다.

IV. 공격 유형 재분류

우리는 3장에서 양자통신 프로토콜이 스니핑 공격을 어떻게 방어하는지 확인하였다. 하지만 스니핑 공격이 양자채널 상에서는 새로운 유형의 공격으로 적용될 가능성이 있으며 본 장에서 주제에 관한 확인을 한다.

우선 스니핑 공격의 가장 큰 특징은 공격 대상에 직접적인 피해를 가하지 않는다는 점이다. 스니핑 공격은 통신채널을 감시함으로써 패킷을 획득하는 공격으로, 획득한 패킷의 의미를 확보하는 것과 무관하게 비인가자가 통신에 접근한 것이므로 기밀성 공격에 해당된다.

반면에 양자통신상에서 스니핑 공격을 시도하면 그림 3에서 확인하였듯 양자붕괴 현상으로 인해 획득한 값은 의미를 상실할 가능성이 높다. 따라서 고전채널 상의 스니핑 공격은 복호화가 가능하다면 원본 값을 획득할 수 있지만, 양자채널 상의 스니핑 공격은 이것이 불가능하기에 정보 획득의 측면에서 성과를 보기 힘들다. 하지만 양자붕괴 현상으로 인하여 특별한 성질을 지니게 된다.

고전채널에서 스니핑 공격 발생 시 송수신 측은 공격자를 인지하지 못하더라도 통신 자체에는 지장이 생기지 않는다. 스니핑 공격은 패킷을 감청만 할 뿐 통신 상태에는 영향을 끼치지 않기 때문이다. 하지만 양자채널에서는 양자붕괴로 인해 송수신 측이 공격당함을 인지할 기회를 주지만 반대로 송수신 측의 정상적인 정보 교환을 방해하는 작용도 한다.

이는 양자채널을 관측하는 것만으로도 정상적인 통신을 방해할 수 있음을 시사한다. 이처럼 송수신 서로에게 통신 장애를 일으키므로 양자통신 상에서 스니핑 공격이 가용성 공격으로 분류 될 수 있다. 스니핑 공격이 환경에 따라 미치는 영향은 표 2를 통해 확인할 수 있다.

표. 2. 통신 환경 별 스니핑 공격의 영향 비교

	Classic Ch.	Quantum Ch.
Wiretapping	○	○
Decryptabili-ty	△	×
Original packet loss	×	○
Cause a communicati-ons failure	×	○

○: Possible
△: Conditionally possible
×: Impossible

V. 결론

본 논문에서는 고전채널 상에서 기밀성 침해 공격으로 분류되는 스니핑 공격이 양자채널 상에서는 가용성 침해 공격으로 재분류될 수 있는 가능성에 대해서 살펴보았다.

가용성 침해 공격은 사용자가 쉽사리 피해 상황을 인지할 수 있는 공격 유형이다. 이는 대체로 피해자가 인지하기 어려운 환경에서 수동적인 공격을 구사하기 때문이다. 반면에 가용성 침해 공격은 피해자의 통신사용을 방해하거나 정보 접근을 제한하는 등 눈에 보이는 피해가 즉각적으로 발생한다. 따라서 공격으로 인해 서비스가 중지되는 등 피해가 발생한다면 대부분의 사용자는 공격자를 비난하기보다 서비스 제공 주체를 비난하는 경우가 많으며 서비스 제공자는 원활한 서비스 제공 의무를 저버린 상황이 된다. 이러한 상황을 예방하기 위해 가용성 침해 공격에 속하는 서비스 거부 공격을 감지 또는 회피하기 위한 다양한 솔루션이 제시되어 있다[7].

양자 통신은 아직 활성화된 상태도 아니며 이에 따라 실제 사례도 발생하지 않았다. 하지만 앞으로 다가올 양자 통신 환경에서 가용성 침해 공격이 발생한다면 현재와 마찬가지로 많은 사용자들이 불만을 표할 것이다. 이와 같은 상황을 방지하기 위해서는 각종 수단이 필요할 것이다. 가령 양자채널 자체를 관측하지 못하도록 은닉하는 회피 기법, 공격 발생 시 우회할 수 있는 채널을 형성하는 대처 기법 등이 예시가 될 수 있다.

현재 양자 컴퓨터가 상용화되지 않았지만 양자 내성 암호에 대한 연구가 활발하듯이, 양자채널에서 가용성 침해 공격을 예방하기 위한 대응 방안도 미리 제시한다면 미래에 발생할 수 있는 피해를 줄이거나 방지할 수 있을 것으로 사료된다.

[참고문헌]

[1] National Institute of Standards and Technology government. Systems Security Engineering: Considerations for a Multidisciplinary Approachin the Engineering of Trustworthy Secure Systems [Internet]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

[2] Information and Communication Technology Glossary. Security Attack [Internet]. Available: http://www.ktword.co.kr/abbr_view.php?m_temp1=2288

[3] M. Planck, “On the Law of Distribution of Energy in theNormal Spectrum,” Annalen der Physik, vol. 4, pp. 553-563, Jan. 1901.

[4] J. H. Shin and J. Heo, “Quantum information theory and fault-tolerant quantum computing,” The Magazine of the Institute of Electronics and Information Engineers, vol. 45, no. 4, pp. 49-57, April. 2018.

[5] The Information Philosopher. Collapse of the Wave Function [Internet]. Available: http://www.informationphilosopher.com/solutions/experiments/wave-function_collapse/

[6] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore: India, pp. 175-179, 1984.

[7] Korea Internet and Security Agency. DDoS attack response guide [Internet]. Available: https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=21616