양자 키 분배 프로토콜의 IPSec 적용 연구

손일권*, 이원혁, 이은주, 심규석
한국과학기술정보연구원
d2estiny@kisti.re.kr, livezone@kisti.re.kr, saranha@kisti.re.kr, kusuk007@kisti.re.kr

A study on the application of quantum key distribution to IPSec

Sohn Il Kwon*, Lee Wonhyuk, Lee Eunjoo, Shim Kyu-Seok
Korea Institute of Science and Technology Information

요 약

IPSec은 보안에 취약한 구조를 가진 IP의 보안을 위하여, 통신 세션의 IP 패킷을 각각 암호화하고 인증을 통해 안전한 IP 통신을 할 수 있게 하는 3계층 보안 프로토콜이다. 이러한 IPSec에서 키 교환을 위해 IKE 프로토콜을 사용하며, IKE 프로토콜은 Diffie-Hellman 알고리즘이나 공개키 방식 등을 사용하여 키를 교환한다. Diffie-Hellman 알고리즘, RSA(Rivest, Sharmir, Adleman) 기반 공개키 알고리즘, 타원곡선 암호(elliptic curve cryptography) 등은 모두 양자컴퓨터 개발 시 해독이 가능하다고 알려진 키 교환 알고리즘이기 때문에 양자컴퓨터의 공격에 안전한 키 교환 기법을 적용할 필요가 있다. 따라서 본 논문에서는 한국과학기술정보연구원에서 진행 중인 'DV-QKD 및 양자키 기반 보안장비(Q-IPSec) 연동 운영장비 제작' 사업을 소개한다. 해당 사업은 양자 키 분배 프로토콜(Quantum Key Distribution)을 IPSec 과정의 IKE에 적용하여 양자컴퓨터의 공격으로부터 취약한 부분을 보완할 수 있는 방법을 제시한다.

Ⅰ. 서 론

컴퓨터의 개발과 더불어 시작된 인터넷이 통신기술이 발전함에 따라 그 서비스 및 사용자가 점점 증가하여, 현재는 사물인터넷과 같이 거의 모든 기기가 인터넷에 접속 가능하게 되었다. 인터넷의 영향력이 증가함에 따라 통신망에 접속 가능한 정보가 급격히 증가하여, 적절한 보호가 없으면 저장 및 송수신 과정에서 유출, 수정, 삭제 등 허가되지 않은 작업이 이루어질 수 있다. 따라서 인터넷 프로토콜의 취약점을 해결하기 위해 보안 프로토콜들 또한 발전하였다. 보안 프로토콜 중 네트워크 보안 기술은 내부 사용자, DMZ, 서버망을 공유하는 사이트 사이의 네트워크에서 권한이 없는 사람의 접근, 우연 또는 의도적인 방해 및 파괴로부터 네트워크를 보호하는 기술을 총칭한다. 해당 기술들의 요구사항으로는 통신에 참여한 실체 인증, 데이터의 무결성 및 보안성, 데이터 인증, 부인 방지가 있으며, 이에 대한 보안 기술로 IPSec이 고안되었다[1].

이러한 IPSec 기술에 있어, 양자컴퓨터가 대두되면서 취약점으로 우려되는 부분이 있다. IKE 과정[2]에서 DH 알고리즘을 통해 Master Key를 생성하는 부분이다. DH 알고리즘이나 공개키 기반의 암호시스템의 보안성은 소인수 분해 알고리즘의 계산복잡도를 기반으로 하고 있다[3]. 양자컴퓨터의 경우 이러한 소인수 분해 능력이 기존 컴퓨터보다 지수적으로 향상될 수 있는 알고리즘을 수행할 수 있다. 이는 1984년 피터 쇼어가 제안한 쇼어 알고리즘으로, 양자 푸리에 변환을 통해 소인수분해 문제와 등가인 모듈러 함수의 오더를 찾는 문제를 다항 시간 내에 풀 수 있음을 보였다[4]. 따라서 양자컴퓨터로부터 안전한 대칭키 분배를 위하여 양자 키 분배 프로토콜이 고안되었다. 양자 키 분배 프로토콜은 양자는 복제할 수 없다는 성질과 측정 후 이전 상태로 되돌릴 수 없는 등의 양자역학적 특성을 이용하여 도청 시 이를 감지할 수 있는 키 분배 기술이다[5]. 본 논문에서는 이러한 QKD를 IPSec의 IKE 과정에 접목하여 양자컴퓨터의 공격에 취약할 수 있는 부분을 보완하는 방법을 알아보고 'DV-QKD 및 양자키 기반 보안장비(Q-IPSec) 연동 운영장비 제작' 사업을 소개한다.

Ⅱ. 본론

IPSec은 호스트 간, 호스트와 보안 게이트웨이 간 및 보안 게이트웨이 간의 경로를 보호할 수 있는 기술이다. 보안을 위하여 IKE(Internet Key Exchange)를 통해 두 통신단 사이의 암호키와 필요한 정보를 교환하며, 인증 헤더(Authentication Header) 프로토콜과 ESP(Encapsulated Security Payload) 프로토콜을 사용하여 보안을 제공한다. AH 프로토콜을 통해 출발지 인증, 데이터 무결성, 재현 공격 방지 서비스를 사용할 수 있으며, ESP 프로토콜을 통해 AH 프로토콜이 제공하지 않는 기밀성까지 확보할 수 있다. 또한, IPSec은 두가지 모드가 존재한다. 트랜스포트 모드는 호스트 간의 종단간 통신을 보호할 수 있으며, IP 상위의 프로토콜 정보를 인터넷을 통해 안전하게 전달할 수 있다. 이는 로컬 네트워크 내의 타 호스트들을 신뢰할 수 없을 때 특정 호스트 간 통신을 보호하기 위해 사용된다. 다른 모드로는 터널 모드가 있으며, 로컬 네트워크 간의 또는 로컬 네트워크와 호스트 간의 통신을 보호하기 위해 사용된다. 이를 통해 로컬 네트워크 내 모든 호스트들의 통신을 보호할 수 있다.

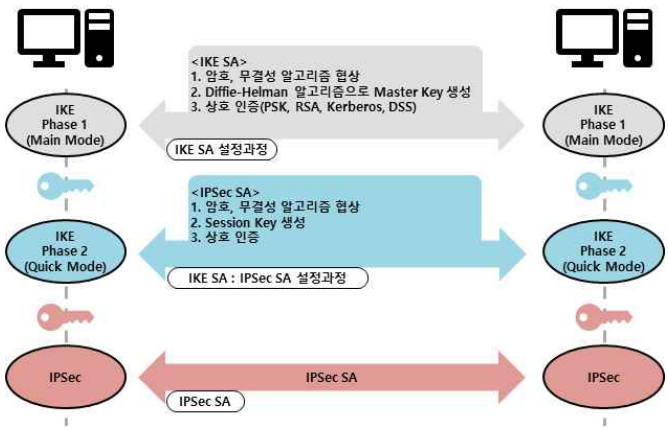

그림 1 IPSec 동작 과정

현재 RSA를 기반으로 한 비대칭 공개키 암호체계를 통해 대칭키 등을 나누어 가지고, 이후 대칭암호 체계를 통해 안전성이 보장된 암호통신을 수행한다. 하지만 앞서 설명하였듯이 대칭키를 나누어 가지는 과정이 양자컴퓨터에 의해 파훼 된다는 문제점이 있다. 양자키 분배 프로토콜은 이러한 대칭키를 양자역학적 특성을 통해 송수신자 사이에 안전하게 분배할 수 있다. 기본적으로 정해진 암호를 송신자가 수신자에게 전달하는 것이 아닌, 임의의 비트열로부터 송수신자가 서로 동일한 비트열을 뽑아내기 때문에 안전하다 할 수 있다. 양자 키 분배 프로토콜 중에서 가장 대표적인 방법은 Bennett과 Brassard가 1984년에 제안한 BB84 프로토콜로 그림 2.와 같은 과정을 통해 암호키를 분배한다[6].

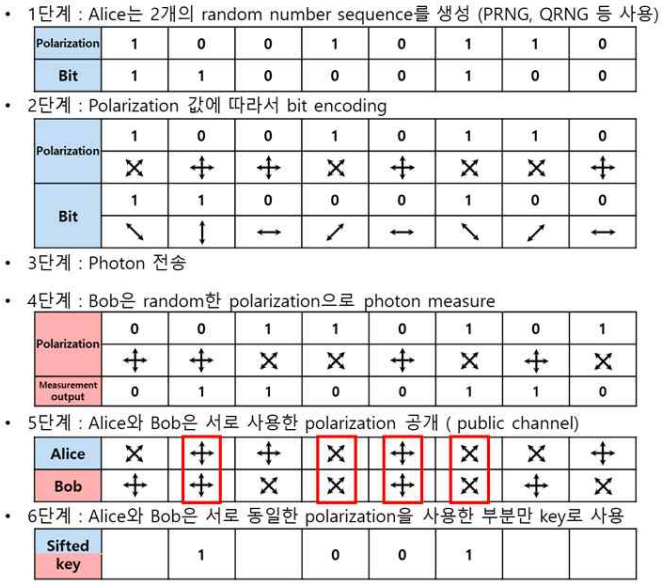

그림 2. 오류가 없는 양자채널에서의 BB84 프로토콜 동작 과정

IPSec의 IKE 과정에서는 QKD를 적용할 수 있는 과정이 두가지가 있다. 첫 번째로 QKD를 통해 생성된 양자키를 IKE SA의 공유 비밀을 설정하는 데 사용될 수 있다. IKE에서 DH 알고리즘을 통해 Master key를 생성하는 과정이 양자컴퓨터의 공격에 취약하므로 이 과정을 QKD로 대체함으로써 약점을 보완할 수 있다. 두 번째로는 IPSec SA의 session key 생성 과정을 QKD로 대체하는 것이다. 일반적인 IPSec의 경우 Phase 1에서 DH 알고리즘을 통해 교환한 Master key로부터 session key를 생성한다. 따라서 Master key로부터 session key를 생성하는 과정 전체를 QKD로 대체하면 보안상의 이슈를 최소화 할 수 있다. 이 경우 Phase 1에서의 Master key 교환 과정 또한 생략될 수 있다.

해당 사업에서는 두 번째로 설명한 IPSec SA의 session key 생성 과정을 QKD로 대체할 것이다. QKD 장비에 문제가 발생하였을 경우를 대비하여 기존의 IKE 과정 또한 수행할 수 있도록 할 것이다. 이때 IKE 알고리즘은 그림 3.과 같이 동작한다. 이를 통해 QKD를 통해 나누어가진 양자키를 IPSec에 연동하여 사용할 수 있다.

Ⅲ. 결론

본 논문에서는 QKD 기술을 IPSec의 IKE 과정에 적용하여, 양자컴퓨터의 공격으로부터 취약한 부분을 보완할 수 있는 'DV-QKD 및 양자키 기반 보안장비(Q-IPSec) 연동 운영장비 제작' 사업을 소개하였다. IKE에서 QKD를 적용할 수 있는 부분은 두 가지가 존재한다. Phase 1에서 DH 알고리즘을 사용하여 마스터 키를 생성하는 과정을 QKD로 대체할 수 있으며, Phase 2에서는 세션 키를 생성하는 과정을 대체하여 매 세션마다 QKD로 교환한 대칭키로 암호화하여 통신할 수 있다. 본 논문에서는 세션

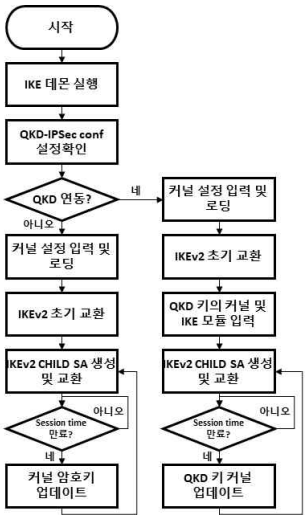

그림 3. QKD-IPSec에서의 IKE 동작 알고리즘

키 생성 과정을 QKD로 대체하는 방안을 사용하였으며 이를 통해 양자컴퓨터의 위협으로부터 취약한 부분인 DH 알고리즘을 사용하여 키를 나누어가지는 과정을 보완할 수 있는 IPSec을 제시하였다. 차후 시제품을 통해 IPSec에 QKD를 접목하였을 시의 통신 성능 저하 등의 발생 여부를 확인할 예정이며, 현재 단대단 통신만을 고려하고 있는 QKD 프로토콜을 사용하여 네트워크를 구축하기 위한 제반사항들을 연구할 예정이다.

ACKNOWLEDGMENT

본 연구는 2020년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다

참 고 문 헌

[1] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," IETF RFC 2401, November 1998.

[2] D. Harkins and D. Carrel, "The Internet Key Exchange," IETF RFC 2409, November 1998.

[3] J.L. Massey, "An Introduction to Contemporary Cryptography," Proc. of the IEEE, Vol.76, No.5, 1988, p.533

[4] P. Shor, in Proc. of the 35th Annu. Symp. on Foundations of Computer Science, edited by S. Goldwasser, IEEE Computer Society Press, Los Alamitos, California, 1994, pp.124.

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," Rev. Mod. Phys., Vol.74, No.1, 2002, p.145.

[6] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in Proc. of IEEE Int'l Conf. on Computers, Systems and Signal Proc., Bangalore, India, IEEE, New York, 1984, p.175.