<작성주의>
작성전에 전자출원명세서 작성방법 도움말을 충분히 숙지하고 명세서를 작성하기 바랍니다.
식별항목【 】은 내용이 없어도 삭제하지 말고 공란 또는 점(·)만 표시하기 바랍니다.
발명의 명칭은 서지사항의 명칭과 동일하게 입력해야 합니다.

【발명의 설명】

【발명의 명칭】

시간 동기화 기반 행렬 분할 키 교환 및 실시간 회전 방법{Time-Synchronized Matrix-Based Key Exchange and Real-Time Key Rotation Method}

【기술분야】

본 발명은 네트워크 보안 및 암호화(H04L9) 기술 분야에 속한다. 구체적으로, 시간 동기화와 임시 키 교환을 결합한 키 분배 및 키 회전 알고리즘에 관한 것이며, 통신 과정에서 사용되는 대칭/비대칭 키를 효율적이고 안전하게 교환하고, 실시간으로 키를 갱신(회전)함으로써 중간자 공격, 도청 및 양자 컴퓨터 공격에 대한 내성을 보완하고자 하는 기술이다.

【발명의 배경이 되는 기술】

현대 네트워크 보안 환경에서는 데이터 암호화를 위한 키 교환 및 키 회전 기술이 필수적이다. 기존의 키 교환 방식으로는 Diffie-Hellman(DH), Rivest-Shamir-Adleman(RSA), 타원곡선암호(ECC) 등이 널리 사용되고 있다. 그러나 이러한 방식은 대수적 난제(Mathematical Hard Problem)에 기반하고 있어, 양자 컴퓨터가 발전할 경우 Shor 알고리즘 등의 공격에 의해 보안성이 약화될 가능성이 크

다.

또한, 기존 키 교환 방식은 일정한 주기로 키 회전(Key Rotation)을 수행하지만, 키 회전 주기가 상대적으로 길거나 사전에 설정된 방식으로 이루어지는 경우가 많다. 이로 인해 장기간 동일한 키가 사용될 경우, 공격자가 키를 노출시킬 가능성이 증가하는 문제가 발생한다. 특히, 실시간성이 중요한 금융 거래, 온라인 인증, 보안 통신 환경에서는 키 회전 속도가 보안 수준에 직접적인 영향을 미친다.

이러한 문제를 해결하기 위해 일부 연구에서는 시간 동기화(Time Synchronization)를 이용한 키 교환 방식을 제안하였다. 예를 들어, Network Time Protocol(NTP) 및 Precision Time Protocol(PTP) 등을 활용하여 통신 양측의 시간을 동기화한 후, 이를 기반으로 키를 생성하는 방법이 연구된 바 있다. 그러나 기존 연구들은 단순히 시간 동기화를 활용하는 것에 그쳐 있으며, 키 회전 및 키 보정 연산을 통한 추가적인 보안 강화 방식은 제안되지 않았다.

또한, VPN, MPLS, SDN 등의 전용 네트워크 경로를 활용하여 통신 지연(Latency)을 일정하게 유지하는 기술이 존재하지만, 이를 활용한 키 교환 및 키 회전 알고리즘은 제안되지 않은 상태이다. 따라서, 실시간으로 보안성을 유지하면서도 네트워크 환경 변화에 강건한 키 교환 및 회전 기술이 필요하다.

(【선행기술문헌】)

문헌명: [국가R&D연구보고서] 양자 컴퓨팅 환경에 안전한 보안 프로토콜 개발에 관한 연구

(https://scienceon.kisti.re.kr/srch/selectPORSrchReport.do?cn=TRKO202000004195)

문헌명: 해쉬 체인 기반의 안전한 하둡 분산 파일 시스템 인증 프로토콜

(https://koreascience.or.kr/article/JAKO201334064305404.page?)

(【특허문헌】)

문헌명: KR101009420B1 - 통합네트워크에서 단말 시각 동기화 방법 및 장치

이 특허는 통합 네트워크 환경에서 단말 간의 시간 동기화 방법 및 장치를 제시한다. 특히, 체크 메시지 교환을 통해 양측의 시간을 동기화하는 기술을 다루고 있으며, 이는 본 발명의 시간 동기화 기반 키 교환 방식과 관련이 있다.

(【비특허문헌】)

문헌명: Windows 시간 서비스 도구 및 설정

(https://learn.microsoft.com/ko-kr/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings)

Microsoft의 공식 문서로, Windows 운영 체제에서 시간 동기화를 위한 다양한 도구와 설정 방법을 상세하게 설명하고 있다. 특히, NTP(Network Time Protocol)를 활용한 시간 동기화 설정 방법이 포함되어 있어, 본 발명의 시간 동기화 메커니즘 구현에 참고할 수 있다.

【발명의 내용】

【해결하고자 하는 과제】

본 발명은 상기 언급한 기존 키 교환 및 키 회전 방식의 한계를 극복하고자, 시간 동기화 기반 행렬 분할 및 실시간 키 회전 방법을 제안한다.

본 발명이 해결하고자 하는 주요 과제는 다음과 같다.

첫째, 양자 컴퓨터 공격에 대한 대응이 필요하다. 본 발명은 시간 동기화 및 물리적 네트워크 지연값(Latency)을 활용한 키 교환 방식을 통해, 수학적 난제에 의존하지 않는 보안성을 확보하는 것을 목표로 한다. 완전한 양자 내성을 보장하지 못하더라도, 기존의 대수적 난제 기반 암호화와 다른 방향을 제시하고자 한다.

둘째, 실시간 키 회전 방식의 최적화가 필요하다. 기존 키 회전 방식은 일정한 주기로 수행되며, 키 노출 위험을 줄이는 데 한계가 있다. 본 발명에서는 밀리초 단위의 실시간 시간 변화 감지를 통해 키 회전을 수행함으로써, 장기간 동일 키 사용으로 인한 보안 취약성을 최소화하는 것을 목적으로 한다.

셋째, 통신 환경 변화에 따른 보안성을 유지해야 한다. VPN, MPLS, SDN 등 고정 네트워크 경로를 활용하여 일정한 통신 지연(Latency)을 유지하고, 이를 기반으

로 키 검증 과정을 수행하여 중간자 공격(Man-in-the-Middle Attack)에 효과적으로 대응할 수 있도록 한다.

넷째, 계산 오버헤드 및 네트워크 부하를 최소화해야 한다. 기존 키 교환 방식에서 다수의 임시 키(TK)를 반복적으로 교환하는 경우, 통신 부하가 증가하는 문제가 발생할 수 있다. 본 발명에서는 TK를 단일 교환한 후, 행렬 분할 및 보정 연산을 수행하는 방식을 통해 네트워크 부하를 줄이고 실시간성을 확보하는 것을 목표로 한다.

본 발명의 해결 과제는 이상에서 언급한 과제로 제한되지 않고, 아래 내용들을 통해 다른 과제가 유추될 수 있으며, 이는 본 발명이 속한 기술분야에서 통상의 지식이 있을 경우 명확하게 이해될 수 있을 것이다.

【과제의 해결 수단】

본 발명은 위의 문제를 해결하기 위해 다음과 같은 기술적 수단을 적용한다.

첫째, 시간 동기화 기반의 임시 키(TK) 생성 기법을 적용한다. 사전 합의된 원자시계, GPS 시각 동기화, NTP/PTP 등을 이용하여 통신 양측의 시간이 동기화된 상태를 유지한다. 또한, 체크 메시지 교환을 통해 통신 경로상의 레턴시(Latency)를 밀리초(MMSSmmmm, 분/초/밀리초) 단위로 측정한 후, 이를 해시 함수에 적용하여

동일한 해시 값이 나올 경우 이를 임시 키(TK)로 확정한다.

둘째, 행렬 분할 및 키 보정 연산을 수행한다. 각 통신 당사자는 n×n 크기의 키 행렬을 생성하고, 이를 n^2 /8개의 섹션으로 분할한 후, 각 행렬 섹션에 대해 8자리 임시 키(TK)를 적용(합 연산)하여 보정된 키 행렬을 생성한다.

셋째, 보정된 키 행렬을 이용하여 키 교환을 수행한다. 보정된 키 행렬을 상호 교환한 후, 각 당사자는 상대방의 키 행렬을 받아 TK 값을 상쇄(차 연산)하는 방식으로 원본 난수 행렬을 복원한다. 이를 통해 수학적 난제에 의존하지 않는 새로운 키 교환 방식이 구현된다.

넷째, 실시간 키 회전 알고리즘을 적용한다. 통신 중 시간이 흐름에 따라, 기존 행렬 섹션을 신규 값으로 갱신한다. 이를 통해 장기간 동일한 키 사용으로 인한 보안 위험을 줄이고, 실시간 환경에서도 안전한 키 교환을 보장할 수 있다.

【발명의 효과】

본 발명을 통해 다음과 같은 효과를 기대할 수 있다.

첫째, 양자 컴퓨터 공격에 대한 저항성을 일부 확보할 수 있다. 기존 RSA, ECC 등의 암호 방식이 아닌 시간 동기화 및 물리적 네트워크 특성을 활용하는 방식

이므로, Shor 알고리즘 등의 양자 컴퓨터 공격에 대한 내성이 상대적으로 강화된다.

둘째, 실시간 보안성을 강화하고, 키 노출 위험을 감소시킬 수 있다. 기존 키 회전 방식은 정해진 주기로 수행되지만, 본 발명은 밀리초 단위의 시간 변화를 감지하여 실시간으로 키를 갱신하므로, 장기간 동일한 키 사용에 따른 보안 위험을 최소화할 수 있다.

셋째, 네트워크 부하 및 계산 오버헤드를 줄일 수 있다. 기존 방식 대비 TK 교환 횟수를 줄이고, 행렬 분할 및 보정 연산을 통해 효율적인 키 회전이 가능하다. 이를 통해 네트워크 트래픽 및 계산 비용을 최소화하면서도 강력한 보안성을 유지할 수 있다.

넷째, 중간자 공격을 효과적으로 방어할 수 있다. 고정된 네트워크 경로에서의 통신 지연(Latency)을 활용한 키 검증 기법을 적용하여, 외부 공격자가 네트워크 환경을 동일하게 재현하는 것이 어렵도록 설계되었다.

【도면의 간단한 설명】

도1은 전체 시스템의 개요를 나타낸다.

도2는 시간 동기화 및 RTT 계산 과정을 나타낸다.

도3은 키 교환 과정을 나타낸다.

【발명을 실시하기 위한 구체적인 내용】

본 발명은 시간 동기화 기반 행렬 분할 키 교환 및 실시간 키 회전 방법을 제공하며, 이를 실시하기 위해 시간 동기화 기법을 활용한 임시 키(TK) 생성, 행렬 분할을 통한 키 보정 연산, 고정 네트워크 경로를 이용한 키 검증 및 중간자 공격 방지, 실시간 키 회전 기법이 유기적으로 결합된다.

또한, 본 발명에서는 교환된 키를 활용하여 통신 메시지를 암호화하고, 수신자가 이를 복호화하는 방식을 포함하며, 행렬 연산을 기반으로 한 보안 강화를 실현한다. 다음에서 본 발명의 구체적인 실시 방법을 설명한다.

본 발명에서 사용되는 키 교환 방식은 통신 양측의 시간이 정확하게 동기화된 상태에서 수행된다. 이를 위해 다음과 같은 방법을 적용할 수 있다.

먼저, 본 발명에서는 네트워크 환경에 따라 GPS(Global Positioning System) 동기화, NTP(Network Time Protocol), PTP(Precision Time Protocol) 등을 이용하여 양측의 시간 흐름을 동기화한다.

인터넷 기반 환경에서는 공인 NTP 서버(예: time.google.com, time.windows.com)를 이용하여 밀리초(ms) 단위 정확도로 시각을 동기화할 수 있다. 데이터센터 및 클라우드 환경(AWS, Azure 등)에서는 VPC 내부 NTP 서버를 구축하여 내부 트래픽에서 정밀한 시간 동기화가 가능하다. 물리적 네트워크 환경(군

사, 금융 등 초정밀 보안이 필요한 경우)에서는 PTP(Precision Time Protocol)를 이용하여 마이크로초(μs) 단위까지 정밀한 시간 동기화를 수행하거나, 사전 합의된 원자 시계를 이용할 수 있다.

시간 동기화가 완료된 후, 체크 메시지(Check Message)를 이용하여 네트워크 경로의 레턴시 값을 측정한다. 통신 양측은 특수한 체크 메시지(비공개된 난수 값 포함)를 송수신하며, 송수신 지연 시간을 개별적으로 측정한다. 왕복 지연 시간(RTT, Round Trip Time)을 MMSSmmmm(분/초/밀리초)의 단위로 측정한 후, 해시 함수(SHA-256, SHA-3 등)를 적용하여 양측 간 동일한 해시 값이 생성될 경우 이 RTT 값을 임시 키(TK, Temporary Key)로 확정한다. 만약 RTT 값이 일정 범위를 초과하거나, 양측의 해시 값이 일치하지 않는다면, 재측정을 수행하여 임시 키를 교환할 수 있도록 한다. 그러나 무제한 무차별 대입 공격을 제한하기 위해 한 네트워크 경로당 시도 횟수는 최대 10회로 제한한다.

본 발명에서는 키 교환 과정에서 행렬 연산을 이용하여 보안성을 강화하며, 이를 위해 다음과 같은 과정을 포함한다.

각 통신 당사자는 난수 생성기를 사용하여 n×n 크기의 키 행렬을 생성한다. 여기서 n은 8의 배수(예: 8, 16, 32 등)로 설정되며, 이는 보안 강도를 유지하면서도 연산 효율성을 극대화할 수 있도록 하기 위함이다. 생성된 행렬은 n^2 /8개의 독립적인 섹션으로 분할되며, 각 섹션에 대해 8자리 TK 값을 연산하여 보정된 키 행렬을 생성한다.

보정된 키 행렬을 상호 교환한 후, 각 통신 당사자는 상대방이 제공한 행렬을 기반으로 자신의 행렬을 복원한다. 복원 과정에서는 상대방으로부터 전달받은 행렬에서 TK 값을 상쇄하는 연산을 수행하여 원본 난수 행렬을 복원한다. 이를 통해 수학적 난제에 의존하지 않고도 안전한 키 교환이 이루어진다.

본 발명에서는 고정 네트워크 경로를 활용하여 통신 경로의 무결성을 보장하며, 이를 통해 중간자 공격(MITM, Man-in-the-Middle Attack) 방어 메커니즘을 제공한다.

VPN 환경에서는 IPsec을 이용한 터널링 방식을 활용하여 송신자와 수신자 간의 경로를 고정하고, 특정 IP 범위 내에서만 키 교환이 가능하도록 제한할 수 있다. MPLS 환경에서는 사전 정의된 라벨(Label) 기반으로 트래픽을 라우팅하여 경로를 일정하게 유지할 수 있다. SDN 환경에서는 중앙 컨트롤러에서 보안 정책을 설정하고, 특정 네트워크 구간에서만 키 교환이 가능하도록 제한할 수 있다.

또한, 키 교환 과정에서 레턴시 값이 기준값을 벗어나면, 정상적인 네트워크 환경이 아닐 가능성이 높다고 판단하고, 키 교환을 자동 차단한다.

본 발명에서는 밀리초(ms) 단위의 시간 변화를 통해 실시간 키 회전을 수행함으로써 보안성을 강화한다.

네트워크 통신 중 시간의 흐름을 지속적으로 기록하며, 시간 흐름에 따라 키

회전이 자동으로 실행된다. 본 발명에서는 키 회전의 주기를 사전에 설정하는 것이 아니라, 네트워크 환경 및 시간 변화 값에 따라 동적으로 수행하도록 설계한다. 키 회전 시, 전체 행렬을 새로 생성하는 것이 아니라, 기존 행렬에서 시간 변화가 감지된 정도를 각 섹션에 반영하여 부분적인 갱신(MMSSmmmm 단위에 맞게 덧셈 연산)을 수행한다.

본 발명에서는 상호 교환한 키를 활용하여 메시지 데이터를 안전하게 암호화하고 복호화할 수 있도록 행렬 연산을 적용한다.

메시지 전송에 앞서, 송신자는 수신자에게 다시 체크 메시지를 전송하여 메시지를 전송할 것임을 알리고, 수신자와 송신자의 키는 업데이트가 중단된다. 수신자의 경우, 상기 구했던 RTT 값을 이용해 자신의 키를 보정(차 연산)한다.

송신자는 메시지를 n×n 크기의 메시지 행렬로 변환한 후 자신이 보유한 수신자의 키 행렬과 행렬곱 연산(Matrix Multiplication)을 수행하여 암호화된 메시지를 생성한다. 이때, 메시지의 길이에 따라, n×n 크기보다 작은 경우, 패딩(padding)을 통해 나머지 부분을 채운다. 또, 메시지의 길이가 n×n 크기보다 큰 경우, 메시지를 분할하여, 다음 통신 때 전송한다.

수신자는 송신자로부터 암호화된 메시지를 수신한 후, 송신자가 사용한 키 행렬(수신자의 키 행렬)의 역행렬을 계산하여 행렬곱 연산을 수행함으로써 원본 메시지를 복호화할 수 있다.

이와 같은 방식은 키를 직접적으로 메시지에 적용하는 것이 아니라, 행렬 연산을 기반으로 변형된 형태로 사용함으로써 전통적인 대칭키 및 비대칭키 암호 방식과 비교하여 보안성을 강화할 수 있다.

본 발명은 시간 동기화 기반 임시 키(TK) 생성, 행렬 분할을 통한 키 보정 연산, 고정 네트워크 경로를 이용한 키 검증 및 중간자 공격 방지, 실시간 키 회전 기법을 유기적으로 결합하여 보안성이 강화된 키 교환 및 회전 방법을 제공한다. 또한, 교환된 키를 활용한 메시지 암·복호화 방식을 포함하여, 키 교환 후 통신 과정에서도 강력한 보안성을 유지할 수 있도록 한다. 이를 통해 기존 RSA, ECC 등 수학적 난제 기반 암호 방식의 한계를 극복하고, Shor 알고리즘에 비교적 강력한 보안성을 유지할 수 있다.

(【실시예】)

본 실시예에서는 본 발명의 동작 과정을 보다 직관적으로 설명하기 위해 Alice(100)와 Bob(200)이 보안 통신을 수행하는 과정을 예제 값과 함께 제시한다. Alice와 Bob은 본 발명의 시간 동기화 기반 행렬 분할 키 교환 및 실시간 키 회전 방법을 활용하여 안전하게 키를 교환한 후, 교환된 키를 이용하여 메시지를 암호화하고 복호화한다. 또한, 중간자 공격(Man-in-the-Middle Attack)이 발생할 경우 이를 탐지하는 과정도 포함하여 실시예를 설명한다.

Alice와 Bob은 보안 통신을 수행하기 전에, 먼저 시간을 동기화하고 키 교환을 수행한다. 본 발명의 시간 동기화 과정은 일반적인 네트워크 시간 동기화 방식과 달리, 절대적인 시간값을 일치시키는 것이 아니라 시간이 흐르는 속도를 동기화하는 것을 목적으로 한다. 이를 위해 Alice와 Bob은 NTP(Network Time Protocol) 또는 PTP(Precision Time Protocol) 등을 이용하여 각자의 클럭 속도를 조정하여 동일한 시간 흐름을 유지하도록 한다. PTP를 사용할 경우 마이크로초(μs) 단위까지 정밀하게 동기화가 가능하며, NTP를 기반으로 동기화하는 환경에서는 밀리초(ms) 수준에서 동기화를 제공할 수 있다.

시간 동기화가 완료되면, Alice와 Bob은 체크 메시지를 교환하여 네트워크 경로의 왕복 지연 시간(RTT, Round Trip Time)을 측정한다. Alice와 Bob이 서로에게 체크 메시지를 전송한 뒤, 응답한 시간과의 차를 구해 RTT 값을 계산한다. 예를 들어, Alice와 Bob 간의 RTT 값이 57.32ms로 측정되었다고 가정하면, MMSSmmmm(분/초/밀리초) 단위에 맞게 조정하면 [0 0 0 0 0 5 7 3]으로 TK를 나타낼 수 있고, 이를 해시 함수(SHA-256 등)에 적용하여 이 값을 상호 간 비교한다. 만약 일치할 경우, 위 TK를 확정한다.

Alice와 Bob은 각각 난수 생성기를 사용하여 n×n 크기의 키 행렬을 생성한다. 여기서 n은 8의 배수(예: 8, 16, 32 등)로 설정되며, 이는 보안 강도를 유지하면서도 연산 효율성을 극대화할 수 있도록 하기 위함이다. 예를 들어, Bob이

생성한 키 행렬 B가 다음과 같다고 가정한다.

B =

[4 1 3 5 2 8 6 9]

[7 5 2 3 8 6 4 1]

[9 3 6 1 5 2 7 8]

[2 8 5 6 3 7 1 9]

[6 4 9 7 1 3 2 5]

[8 7 1 2 9 5 3 6]

[3 9 7 8 6 1 5 2]

[5 2 4 9 7 8 1 3]

각자의 행렬을 n^2 /8 개의 섹션으로 분할한 후, 임시 키(TK)를 활용하여 일부 값을 조정한다. 여기에서는 섹션이 행 단위로 나눠지고, 숫자 단위로 나누어진 섹션에 MMSSmmmm 형식의 RTT 값을 자리에 맞게 더한다. 그렇게 하면 보정된 키 행렬 B’ 은 다음과 같다.

B’ = [4 1 3 5 2 13 13 12]

[7 5 2 3 8 11 11 4]

[9 3 6 1 5 7 14 11]

[2 8 5 6 3 12 8 12]

[6 4 9 7 1 8 9 8]

[8 7 1 2 9 10 10 9]

[3 9 7 8 6 6 12 5]

[5 2 4 9 7 13 8 6]

이 보정된 행렬을 서로 교환한 후, Alice는 Bob의 행렬을 받고, Bob은 Alice의 행렬을 받아 TK 값을 상쇄하는 방식으로 원래 난수 행렬을 복원한다. 이를 통해 Alice와 Bob은 서로의 난수 행렬을 알게 되고, 이 행렬을 최종 키 행렬로써 사용한다.

키 교환이 완료된 후, Alice는 Bob에게 보낼 메시지를 암호화한다. 본 발명에서는 교환된 키 행렬을 활용하여 행렬 연산을 기반으로 메시지를 암호화하고 복호화할 수 있다. 예를 들어, Alice는 "HELLO"라는 메시지를 Bob에게 전송하려고 한다고 가정한다. 메시지 전달에 앞서, Alice, Bob의 업데이트 중인 키 A,B 의 업데이트를 상기 언급한 방식에 따라 고정한다. Alice는 ASCII 코드 값을 사용하여 각 문자에 대한 숫자 값을 정의한 후, 이를 r×n(n은 8의 배수로, 키 행렬에서의 n과 같다. r은 자연수로, 메시지 길이에 따라 동적으로 설정한다.) 메시지 행렬로 변환할 수 있다. 그런데 "HELLO"의 경우 문자열의 길이가 5밖에 되지 않아 r×n 크기의 행렬보다 길이가 짧게 된다. 이 경우에 남은 공간을 0으로 패딩(Padding)하여 길이를 맞춘다. 이 과정을 통해 변환된 메시지 행렬을 M이라고 하며, “HELLO”의 경우, 패딩을 하면 M = [72 69 76 76 79 0 0 0] 으로

나타내진다. 그 다음, Bob의 상기 키 행렬 B에 Alice가 공유할 M을 곱하여 암호화된 메시지 C를 생성한다. 행렬곱의 정의에 따라 C의 크기는 r×8 이다.

$$
\begin{aligned}
C &= M \times B \\
&= [72\ 69\ 76\ 76\ 79\ 0\ 0\ 0] \times \\
&\quad [4\ \ 1\ \ 3\ \ 5\ \ 2\ \ 8\ \ 6\ \ 9] \\
&\quad [7\ \ 5\ \ 2\ \ 3\ \ 8\ \ 6\ \ 4\ \ 1] \\
&\quad [9\ \ 3\ \ 6\ \ 1\ \ 5\ \ 2\ \ 7\ \ 8] \\
&\quad [2\ \ 8\ \ 5\ \ 6\ \ 3\ \ 7\ \ 1\ \ 9] \\
&\quad [6\ \ 4\ \ 9\ \ 7\ \ 1\ \ 3\ \ 2\ \ 5] \\
&\quad [8\ \ 7\ \ 1\ \ 2\ \ 9\ \ 5\ \ 3\ \ 6] \\
&\quad [3\ \ 9\ \ 7\ \ 8\ \ 6\ \ 1\ \ 5\ \ 2] \\
&\quad [5\ \ 2\ \ 4\ \ 9\ \ 7\ \ 8\ \ 1\ \ 3] \\
&= [2081\ 1569\ \ 1901\ \ 1652\ \ 1383\ \ 1911\ \ 1474\ \ 2404]
\end{aligned}
$$

Alice는 암호화된 메시지 행렬 C를 네트워크를 통해 Bob에게 전송한다. Bob은 Alice로부터 암호화된 메시지를 수신한 후, 자신의 키 행렬의 역행렬 B^{-1} 을 계산하여 복호화를 수행한다. 역행렬 연산은 생략한다.

$$M = C \times B^{-1}$$

이와 같은 방식으로 Bob은 원래 메시지 행렬 M을 복원할 수 있으며, 이를 다시 ASCII 코드로부터 변환하면 "HELLO"라는 원래의 메시지를 확인할 수 있다.

본 발명은 또한 중간자 공격(Man-in-the-Middle Attack, MITM) 발생 시 이를 감지하는 기능도 포함한다. Alice와 Bob은 키 교환 전에 고정 네트워크 경로에서 예상되는 지연값(RTT 값)을 사전 측정하여 기준값으로 저장한다. 만약 제3자가 중간에서 공격을 시도하여 트래픽을 가로채거나 변경하려 하면, 네트워크 경로의 레턴시 값이 변동되며, 본 발명에서는 이 변동을 감지하여 키 교환을 무효화한다. 예를 들어, 기존 체크 메시지(메시지를 전송하기 전, 키 업데이트를 멈추기 위해) RTT 값이 57.32ms로 예상되었으나, 공격으로 인해 89.13ms로 변경된다면, 이를 감지하여 키 교환을 중단할 수 있다.

본 실시예에서는 Alice와 Bob이 본 발명을 활용하여 키 교환을 수행하고, 이를 이용하여 메시지를 안전하게 암호화하고 복호화하는 과정을 설명하였다. 본 발명은 시간 동기화를 기반으로 안전한 키 교환을 수행하며, 행렬 연산을 활용하여 메시지를 암호화 및 복호화함으로써 보안성을 강화할 수 있다. 또한, 중간자 공격이 발생할 경우 네트워크 지연값 검증을 통해 이를 감지하고 키 교환을 차단하는 기능도 포함하여 보안성이 더욱 향상된다. 본 발명의 방법은 금융 거래, 블록체인, 군사 통신, 클라우드 보안 등 다양한 산업 분야에서 활용될 수 있으며,

기존 암호화 방식 대비 효율적이고 강력한 보안성을 제공할 수 있다.

(【산업상 이용가능성】)

본 발명은 시간 동기화 기반 키 교환 및 행렬 연산을 활용한 보안 기술로서, 기존 암호화 및 보안 프로토콜 대비 보안성, 실시간성, 효율성이 개선되었다. 이를 통해 금융, 클라우드 보안, 군사 통신, 사물인터넷(IoT), 블록체인 등 다양한 산업 분야에서 활용될 수 있다.

금융 및 핀테크(FinTech) 산업에서는 본 발명을 적용하여 온라인 금융 거래 및 전자결제 시스템에서 안전한 키 교환을 수행할 수 있다. 금융 기관 및 핀테크 기업에서는 온라인 뱅킹, 모바일 결제, 블록체인 기반 송금 시스템 등에서 암호 키 교환의 보안성을 강화할 필요가 있으며, 본 발명을 적용하면 키 교환 과정에서 중간자 공격을 방지하고 보안성을 높일 수 있다. 신용카드 결제 및 디지털 서명 시스템에서도 본 발명의 키 회전 기술을 적용하여 장기간 동일한 키 사용으로 인한 보안 취약점을 줄일 수 있다.

클라우드 보안 및 데이터센터 환경에서도 본 발명을 활용할 수 있다. 클라우드 서비스 제공업체에서는 사용자의 민감한 데이터를 보호하기 위해 암호화 키 관리(KMS, Key Management Service)를 운영하고 있으며, 본 발명을 적용하면 클라우드 환경 내에서 보안 키 관리의 효율성을 높이고 보안성을 강화할 수 있다. 특히, 서버 간 보안 통신 및 데이터 암호화에도 적용할 수 있으며, 클라우드 기반 사물인터넷(IoT) 시스템에서도 안전한 키 교환을 가능하게 한다.

군사 및 방위산업 분야에서도 본 발명의 활용이 가능하다. 군사 네트워크에서

는 외부 도·감청을 방지하기 위해 통신 키를 지속적으로 갱신할 필요가 있으며, 본 발명의 실시간 키 회전 기술을 적용하면 키가 노출될 가능성을 줄이고 통신 보안을 강화할 수 있다. 또한, 정부 기관의 기밀 문서 전송 및 국가 정보망 보호에도 본 발명을 적용할 수 있으며, 네트워크 경로를 기반으로 한 동적 키 검증 기능을 통해 중간자 공격을 감지하고 대응할 수 있다.

사물인터넷(IoT) 환경에서도 본 발명을 적용할 수 있다. 사물인터넷 기기는 제한된 연산 성능과 배터리 용량을 가지는 경우가 많으므로, 본 발명의 경량 키 교환 방식을 적용하면 IoT 기기 간 보안 통신을 보다 효율적으로 수행할 수 있다. 또한, IoT 네트워크에서 키 교환 시 기존의 중앙 집중형 방식이 아닌, 시간 동기화 기반 키 교환을 활용하면 기기 간의 보안성을 높이고 네트워크의 안정성을 유지할 수 있다.

블록체인 및 분산 원장 기술에서도 본 발명을 활용할 수 있다. 블록체인 네트워크에서는 노드 간의 보안 통신 및 키 교환이 중요한 요소이며, 본 발명을 적용하면 블록체인 네트워크 내에서 더욱 안전한 노드 간 인증 및 서명 키 교환이 가능해진다. 또한, 프라이빗 블록체인 환경에서는 운영 주체가 중앙에서 키를 관리하는 경우가 많아 키 유출 시 전체 네트워크가 손상될 가능성이 있지만, 본 발명을 적용하면 노드 간의 키 교환을 더욱 안전하게 수행할 수 있다.

본 발명은 이러한 다양한 산업 분야에서 활용될 수 있으며, 기존의 대칭키 및 비대칭키 기반 보안 체계를 보완하는 역할을 수행할 수 있다. 특히, 본 발명에서 제안하는 시간 동기화 기반 보안 키 교환 및 실시간 키 회전 기술은 기존 암호화

시스템과 병행하여 적용할 수 있으므로, 기존 네트워크 및 보안 인프라를 변경하지 않고도 보안성을 강화할 수 있다. 따라서, 본 발명은 금융, 클라우드 보안, 군사 보안, 사물인터넷, 블록체인 등 다양한 응용 분야에서 높은 활용 가치를 가진다.

(【부호의 설명】)

100 - 사용자 ALICE

200 - 사용자 Bob

300 - 사용자 간 네트워크

400 - 시간 동기화 과정

410 - 사용자의 시간 동기화 요청

420 - 사용자의 시간 동기화 응답

430 - 사용자 간 보정된 시간 계산

500 - RTT 측정 및 임시키(TK) 검증 과정

510 - 체크 메세지 송신

520 - RTT 측정

530 - 해시 함수(SHA256) 적용

540 - 해시 값 비교

541 - 해시 값 일치 시

542 - 해시 값 불일치 시

550 - 임시 키 확정

600 - 키 교환 수행 과정

610 - 사용자 각자 키 행렬 생성

620 - 사용자 각자 키 행렬과 TK 합 계산

630 - 사용자 간 키 행렬과 TK의 합 교환

640 - 사용가 간 키 복구(차 연산)

700 - 메시지 암호화 및 복호화 과정

(【수탁번호】)

(【서열목록 자유텍스트】)

.

【청구범위】

【청구항 1】

시간 동기화 기반의 키 교환 방법에 있어서,

(a) 첫 번째 통신 장치와 두 번째 통신 장치가 각각 클럭 주파수를 조정하여 동일한 시간 흐름을 유지하는 단계,

(b) 상기 첫 번째 통신 장치와 두 번째 통신 장치가 서로 체크 메시지를 주고받으며 통신 경로의 왕복 지연 시간(RTT, Round Trip Time)을 측정하는 단계,

(c) 상기 측정된 RTT 값을 임시 키(TK, Temporary Key)로 정하고, 해시 함수에 적용하여 비교하는 단계,

(d) 상기 첫 번째 통신 장치와 두 번째 통신 장치가 각각 난수 생성기를 이용하여 n×n 크기의 키 행렬을 생성하는 단계,

(e) 상기 생성된 난수 행렬을 n^2 /8개의 섹션으로 분할한 후, 상기 임시 키(TK)를 적용(합 연산)하여 행렬 값을 조정하는 보정 연산을 수행하는 단계,

(f) 상기 보정된 행렬을 서로 교환한 후, 상대방으로부터 전달받은 행렬에서 TK 값을 상쇄하는 연산(차 연산)을 수행하여 원래 난수 행렬을 복원하는 단계,

(g) 복원된 난수 행렬을 키 행렬(A,B)로 확정하는 단계를 포함하는 것을 특징으로 하는 키 교환 방법.

【청구항 2】

청구항 1에 있어서,

상기 클럭 주파수 조정은 NTP(Network Time Protocol) 또는 PTP(Precision

Time Protocol)을 이용하여 수행되는 것을 특징으로 하는 키 교환 방법.

【청구항 3】

청구항 1에 있어서,

상기 해시 함수는 SHA-256, SHA-3 또는 이에 준하는 보안 해시 알고리즘을 사용하는 것을 특징으로 하는 키 교환 방법.

【청구항 4】

청구항 1에 있어서,

상기 난수 행렬의 크기 n×n에서,

n은 8의 배수로 설정되는 것을 특징으로 하는 키 교환 방법.

【청구항 5】

청구항 1에 있어서,

10회 연속으로 두 통신 장치 간 해시값이 일치하지 않을 경우,

상기 첫 번째 통신 장치와 두 번째 통신 장치 간의 네트워크 경로가 정상적이지 않다고 판단하여 키 교환을 중단하는 것을 특징으로 하는 키 교환 방법.

【청구항 6】

시간 동기화 기반의 실시간 키 회전 방법에 있어서,

(a) 첫 번째 통신 장치와 두 번째 통신 장치가 키 교환을 수행하여 키 행렬(A, B)을 확정하는 단계,

(b) 상기 키 행렬(A, B)을 이용하여 메시지를 암호화 및 복호화하는 단계,

(c) 상기 키 행렬(A,B)을 시간의 흐름에 따라 키 행렬의 섹션에 MMSSmmmm 단위로 반영하는 방법.

【청구항 7】

청구항 6에 있어서,

실시간으로 시간의 흐름에 따라 업데이트하는 것을 특징으로 하는 실시간 키 회전 방법.

【청구항 8】

네트워크 경로 기반의 보안 검증 방법에 있어서,

(a) 메시지 행렬 전송 전, 첫 번째 통신 장치와 두 번째 통신 장치가 체크 메시지를 송수신하여 RTT(왕복 지연 시간, Round Trip Time)를 측정하는 단계

(b) 상기 측정된 RTT 값을 사전에 저장된 기준값과 비교하는 단계,

(c) 상기 RTT 값이 기준값과 10% 이상 차이나는 경우, 중간자 공격 가능성이 있는 것으로 판단하여 키 교환을 중단하는 단계를 포함하는 것을 특징으로 하는 보안 검증 방법.

【청구항 9】

청구항 8에 있어서,

상기 네트워크 경로는 VPN(Virtual Private Network), MPLS(Multi-Protocol Label Switching) 또는 SDN(Software-Defined Networking)을 이용하여 설정되는 것을 특징으로 하는 보안 검증 방법.

【청구항 10】

행렬 연산을 이용한 메시지 암호화 및 복호화 방법에 있어서,

(a) 두 통신 장치가 키 교환을 수행하여 서로의 키 행렬(A,B)를 확보하는 단계,

(b) 송신할 메시지를 n×n 크기의 메시지 행렬(M)로 변환하는 단계,

(c) 메시지 송신 전, 체크 메시지를 통해 키 업데이트를 멈추는 단계,

(d) 상기 메시지 행렬(M)에 키 행렬(A,B)을 곱하여 암호화된 메시지 행렬(C)을 생성하는 단계,

(e) 상기 암호화된 메시지 행렬(C)을 네트워크를 통해 두 번째 통신 장치로 전송하는 단계,

(f) 두 번째 통신 장치가 상기 암호화된 메시지 행렬(C)을 수신한 후, 사전에 공유한 키 행렬(A,B)의 역행렬을 계산하는 단계,

(g) 상기 역행렬을 암호화된 메시지 행렬(C)에 곱하여 원본 메시지 행렬(M)을 복원하는 단계를 포함하는 것을 특징으로 하는 메시지 암호화 및 복호화 방법.

【청구항 11】

청구항 10에 있어서,

상기 메시지 행렬(M) r×n(r은 자연수이고, n은 상기 키 행렬의 크기인 n이다)의 크기로 설정되는 것을 특징으로 하는 메시지 암호화 및 복호화 방법.

(【서열목록】)

【요약서】

【요약】

본 발명은 네트워크 통신에서 시간 동기화 기반의 키 교환 및 실시간 키 회전 방법에 관한 것이다. 본 발명에서는 통신 양측이 동일한 시간 흐름을 유지하도록 클럭 주파수를 조정한 후, 네트워크 경로의 왕복 지연 시간(RTT, Round Trip Time)을 측정하여 임시 키(TK)를 생성한다. 이후, 난수 행렬을 생성하고, 행렬 분할 및 보정 연산을 통해 보안성을 강화한 키 교환을 수행한다.

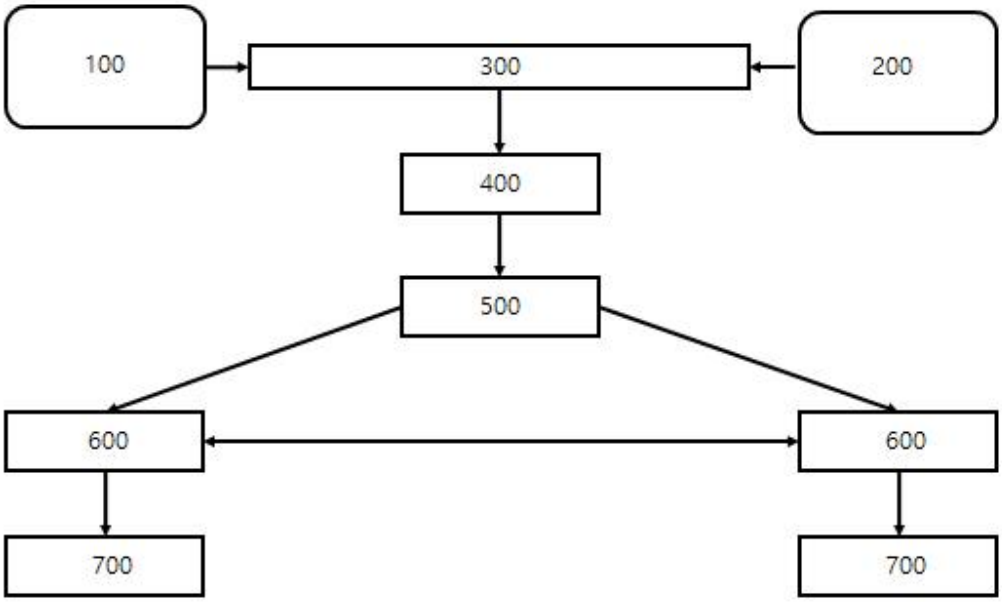
또한, 본 발명은 시간 동기화 및 네트워크 환경의 변화를 실시간으로 감지하여 키 회전을 수행함으로써, 중간자 공격(Man-in-the-Middle Attack), 도청에 대한 내성을 강화한다. 더 나아가, 기존의 대수적 난제 기반 암호와는 다른 접근법을 제공한다. 본 발명의 방식은 기존의 RSA, ECC와 같은 수학적 난제 기반의 암호 기법과 달리, 네트워크 물리적 특성(네트워크 시간 동기화 및 RTT)을 활용하여 보안성을 유지하는 것이 특징이다. 이를 통해 금융, 클라우드 보안, 군사 통신, 사물인터넷(IoT), 블록체인 등의 다양한 분야에서 강력한 보안성을 제공할 수 있다.

(【대표도】)

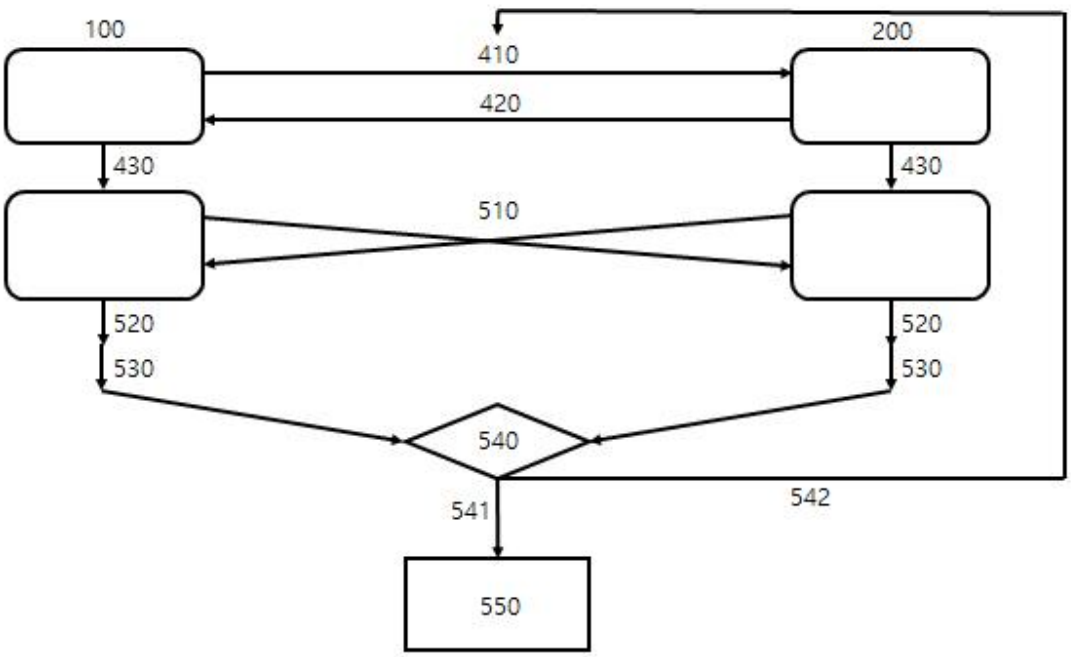
도1

【도면】

【도 1】


100
300
200
400
500
600
600
700
700

【도 2】


100
200
410
420
430
430
510
520
520
530
530
540
541
542
550

【도 3】