https://doi.org/10.7840/kics.2023.48.2.185

NDN 환경에서 형태보존암호를 이용한 Content 기밀성 보호 기법

이 상 현◆, 정 다 윗*, 이 선 영°

Content Confidentiality Protection in NDN Based on Format-Preserving Encryption

Sang Hyeon Lee◆, Da Wit Jeong*, Sun-Young Lee°

요 약

NDN (Named-Data Networking)은 콘텐츠의 효율적인 배포를 위해 콘텐츠 이름을 주소로 사용한다. 그러나 평문 상태로 동작해 민감 정보를 포함한 경우 데이터의 추측, 누출 등 기밀성이 파괴되는 보안 위협이 존재한다. 본 논문은 NDN 아키텍처의 변경을 최소화하면서 기존에 발생하는 보안 위협으로부터 콘텐츠를 보호하기 위해 형태보존암호를 이용하여 콘텐츠 이름을 암호화하는 기법을 제안하였다. 암호화되더라도 정상적인 통신이 가능하고 기밀성이 보호됨을 시험을 통해 보였다. 그리고 형태보존암호를 블록 암호 AES와 비교하였을 때 네트워크 지연시간이 약 1.3%로 짧음을 확인하였다.

키워드 : 엔디엔, 형태보존암호, 콘텐츠 이름 암호화, 기밀성 보호, 네트워크 지연시간
Key Words : NDN, FPE, Encrypted Content Name, Confidentiality Protection, Network Latency

ABSTRACT

Named-Data Networking (NDN) uses Content names as address for efficient distribution of content. However, since it operates in plain-text state, there are security threats that destroys confidentiality, such as data guessing and leaking, when sensitive information is included. This paper proposes a method of encryption the Content name using Format-Preserving Encryption to protect Content name from existing security threats while minimizing changes of NDN architecture. Experiments results showed that communication is possible, and confidentiality is protected, even though Content name is encrypted. In addition, it confirmed that the network latency was about 1.3% shorter than when encrypted with AES.

Ⅰ. 서 론

인터넷은 IP, TCP, UDP에 대한 IETF RFC를 통해 구조가 정리되었고, ARPANET의 NCP 프로토콜을 TCP/IP 체계로 전환함으로써 지금의 인터넷이 탄생하였다[1,2]. 하지만 모바일 네트워크의 활성화와 비디오 스트리밍 서비스의 증가로 가용성, 보안, 위치 의존성과 같은 구조적 문제점이 드러났다. 또한, 다양한

※ 본 연구는 2018년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF2018R1D1A1B07047656).
◆ First Author : Soonchunhyang University Department of Information Security Engineering, cpd4268@sch.ac.kr, 학생회원
° Corresponding Author : Soonchunhyang University Department of Information Security Engineering, sunlee@sch.ac.kr, 종신회원
* Soonchunhyang University Department of Information Security Engineering, djung0605@sch.ac.kr, 학생회원
논문번호 : 202211-284-B-RN, Received November 28, 2022; Revised December 22, 2022; Accepted January 7, 2023

IoT 기기와 서비스의 증가로 기존 인터넷의 문제점이 심화하였다. 이러한 문제를 해결하기 위해 미래 인터넷 기술로서 ICN (Information-Centric Network)이 연구되고 있다. ICN은 기존 인터넷의 문제점을 해결하기 위한 새로운 형태의 네트워크 패러다임으로서[3], 효율적인 콘텐츠 배포를 위해 웹 서비스, 비디오, 이미지와 같은 NDO (Named-Data Object)를 기반으로 하는 네트워크 아키텍처이다[3,4]. TCP/IP 체계와 달리 호스트 중심이 아닌 데이터에 중점을 두어 통신하는 구조이며, P2P (Peer-to-Peer) 오버레이 시스템, 콘텐츠 배포 네트워크와 같은 전용 플랫폼에서만 사용할 수 있는 통신 시스템을 일반 플랫폼에서 제공하여 효율적이고 안정적인 콘텐츠 배포를 목표로 한다[3-5].

대표적인 ICN 아키텍처 중 하나인 NDN (Named-Data Networking)은 TCP/IP의 강점을 활용하면서 IP 주소 체계의 요구사항으로 발생하는 약점을 해결하는 것을 목표로 한다. TCP/IP와 동일하게 Thin Waist 구조를 따르면서 데이터그램을 송수신하고 종단간 법칙을 따른다[6]. 또한, 기존 IP 주소 체계의 통신 방식에서 콘텐츠 이름(Content Name)에 기반한 통신 방식을 가지므로 효율적인 콘텐츠 배포 및 제어가 가능하다[7]. 즉, NDN은 IP가 아닌 콘텐츠를 중심으로 통신하는 네트워크이다. 콘텐츠 소비자(Consumer)는 원하는 콘텐츠를 검색하기 위해 네트워크 내 위치를 알고 있을 필요가 없으며 콘텐츠 이름이 포함된 Interest 패킷을 전송, Data 패킷을 수신해 접근한다[5-7]. 콘텐츠 이름은 가변적인 길이를 가지며 계층적으로 구조화된 데이터 형식으로 구성된다[8]. 그러나 민감한 콘텐츠 데이터를 갖는 경우 공격자가 평문 상태인 콘텐츠 이름에서 데이터의 유형을 추측할 수 있는 등 기밀성이 파괴되는 위험성을 갖는다. 본 논문에서는 NDN 환경에서 콘텐츠 이름을 형태보존암호를 이용해 암호화하여 악의적인 사용자로부터 정보의 기밀성을 보호하기 위한 콘텐츠 이름 암호화 기법을 제안한다.

본 논문은 다음과 같이 구성한다. 2장에서는 NDN과 형태보존암호에 대해 서술하고, 3장에서 NDN 환경에서의 콘텐츠 기밀성 보호 기법을 제안한다. 4장에서는 제안하는 기법을 가상 환경에서 구현하여 블록암호 AES와 성능을 비교 평가한다. 5장에서 본 논문의 결론을 서술한다.

Ⅱ. 관련 연구

2.1 NDN

NDN (Named-Data Networking)은 IP 주소 기반 아키텍처와 달리 콘텐츠를 중심으로 통신하는 패러다임을 갖는 미래 인터넷 아키텍처이다. NDN은 콘텐츠 소비자(Consumer)가 콘텐츠 생산자(Producer)에게 데이터를 요청하고, 콘텐츠 이름(Content Name)에 따라 데이터를 응답 받는다. 이때 전송되는 Interest 패킷은 IP 주소와 같은 호스트 인터페이스 정보를 포함하지 않고, 콘텐츠의 이름으로만 데이터를 송신한다. 콘텐츠 생산자는 소비자로부터 전달된 Interest 패킷과 전자서명 과정을 거쳐 공개키를 Data 패킷 내 Signature 필드에 포함하여 전달한다[6]. 이를 통해 현재 인터넷 아키텍처에서 발생하는 스푸핑과 같은 네트워크 공격으로부터 안전하면서 데이터의 무결성이 보장되는 장점이 있다. 또한, 콘텐츠 중심의 네트워크 통신 구조에 따라 빠른 데이터 검색이 가능하다.

NDN 네트워크에서는 데이터 요청과 응답을 위해 Interest 패킷과 Data 패킷을 사용한다. 각 패킷은 [그림 1]과 같은 구조를 가지며, 데이터 검색을 위해 동일한 콘텐츠 이름을 식별자로써 Content Name 필드에 담아 사용한다.

NDN 라우터는 효율적인 통신을 위해 PIT (Pending Interest Table)와 FIB (Forwarding Information Base)를 기반으로 패킷을 포워딩하는과정을 갖는다. 라우터 노드에 Interest가 요청되었을 때 패킷 포워딩 과정을 거친 후 콘텐츠를 CS (Content Store)에 캐시하고, 앞으로 전달될 Interest 패킷을 만

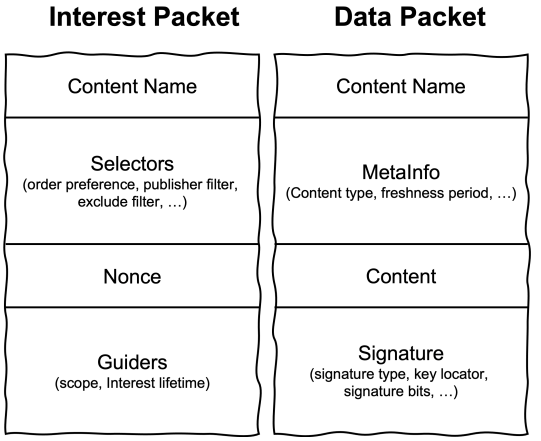

그림 1. NDN 네트워크의 패킷 구조[6]
Fig. 1. Packet Specification of NDN Network

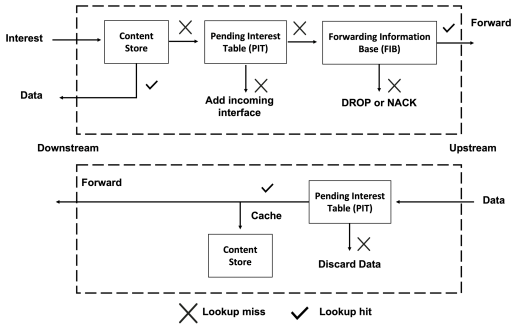

그림 2. NDN의 패킷 포워딩 과정[6]
Fig. 2. Packet Forwarding Process

족시키기 위해 이용된다. PIT는 라우터가 콘텐츠 소비자로부터 수신한 Interest에 대한 패킷 정보와 콘텐츠 이름을 캐시한다. FIB는 라우터의 적응형 전달 전략(Strategy)에 따라 요청된 Interest를 전달하기 위한 목적으로 사용된다. 이때 Interest 패킷이 CS와 PIT에서 만족하지 않으면 라우터의 적응형 전달 전략과 FIB를 기반으로 다음 노드로 포워딩한다. [그림 2]는 NDN의 패킷 포워딩 과정이다.

2.2 형태보존암호

형태보존암호 (Format-Preserving Encryption) [9,10]는 암호문이 평문의 형태와 길이를 그대로 유지하는 암호 알고리즘으로 1997년 Michael Brightwell에 의해 처음으로 제안되었다[11]. 10진수로 이루어진 신용카드, 개인 식별 번호와 같이 구조화된 정보에서 비식별화 기술의 암호화 도구로써 사용되고 있다. 또한, 다양한 암호로의 설계가 가능한데 Prefix Cipher, Cycle-Walking Cipher, Generalized-Feistel Cipher 구조가 있다[12]. 형태보존암호는 기존의 블록 암호와 달리 Tweak이라 지칭되는 부가 정보를 함께 사용하여 암호화를 진행한다. Tweak은 비밀키와 달리 반드시 보호되어야 하는 정보는 아니며 동일한 평문이 여러 번 암호화될 때 서로 다른 Tweak을 적용하면 다른 암호문이 생성되는 특징이 있다. 형태보존암호는 평문의 길이와 형태를 그대로 유지하기 때문에 데이터베이스, 네트워크 프로토콜 구조의 변경 없이도 사용 가능하다. 형태보존암호 FF3-1에서 사용되는 라운드 함수는 AES와 같은 블록 암호나 해시 함수를 기반으로 동작한다[13].

형태보존암호 중 NIST에서 권장하는 FF3-1은 특정 연산을 수행하는 라운드 함수가 반복되는 Feistel 구조를 사용한다. [그림 3]은 형태보존암호화 시 사용되는 Feistel 구조이다. FF3-1은 입력 값으로 평문 X,

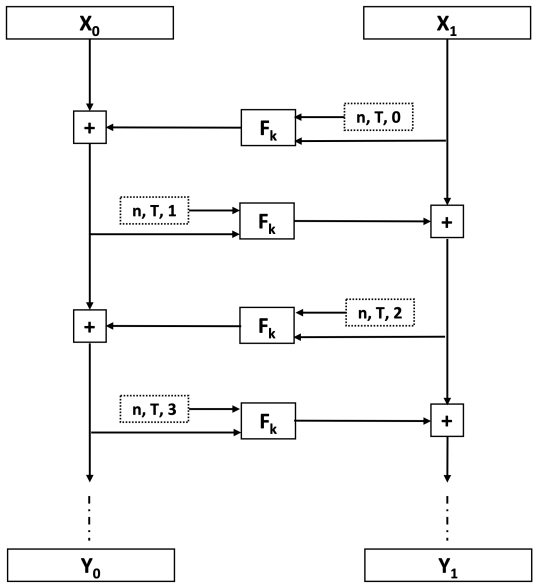

그림 3. FF3-1에서 사용되는 Feistel 구조
Fig. 3. FF3-1 Using Feistel Structure

비밀키 K, Tweak T를 갖는다. 이때 평문 X를 분할해 왼쪽 값 X_0, 오른쪽 값 X_1으로 구분한다. 평문 길이 n이 짝수인 경우 양 값의 길이는 $X_0 = X_1$로 같고, 홀수인 경우 $X_0 = X_1 + 1$로 정의한다. 또한, Tweak T는 56-bit로 왼쪽 값 T_0, 오른쪽 값 T_1으로 구분하며 각 28-bit의 길이를 갖는다. 이후 평문 길이 n와 Tweak T, 라운드 수 i를 라운드 함수 F_K에 인자 로서 적용한다. 이때 라운드 키 (Round Key)가 만들어진다. 짝수 라운드에서는 T_1을 홀수 라운드에서는 T_0을 사용해 암호화한다. 라운드 함수 F_K의 결과 값과 덧셈 (+) 연산을 진행한 뒤 나온 각 결과 값을 스왑(Swap)하는 과정을 거친다. 복호는 위와 반대되며 덧셈 (+)이 아닌 뺄셈 (-)으로 진행된다.

2.3 NDN의 Content 기밀성 보호 연구

NDN은 콘텐츠가 중심이 되는 네트워크로 콘텐츠 이름을 기반으로 데이터를 전달한다. 또한, 콘텐츠 데이터가 라우터 노드 내 CS에 캐시 상태로 기록되고, 콘텐츠와 관련된 모든 정보가 평문 상태로 전달된다. 콘텐츠가 민감한 정보를 포함하는 경우 공격자가 콘텐츠 이름 또는 데이터 자체에서 정보를 획득할 수 있어 기밀성이 파괴되는 등의 프라이버시 문제가 발생한다. 이에 따라 NDN 프로젝트에서는 NDN의 보안 위협에 관한 연구를 진행 중이다. 2010년 Name Privacy에 대한 문제점이 언급되었고[14], 2021년 NDN 소프트웨어의 취약점 분석 연구 결과가 발표되

었다[15]. 현재까지 NDN 아키텍처에 대해 다양한 네트워크 공격 문제와 콘텐츠 정보의 기밀성 보호를 위한 연구가 진행되고 있다 [8,16,17,18].

Kyi Thar Ko 등은 NDN에서 공개키 기반 암호인 PEKS를 사용해 NDN의 새로운 포워딩 전략을 제안하였다[19]. Nikolai Leshov 등은 NDN 기반 전술 네트워크에서 공격자가 평문 상태의 콘텐츠 이름에서 정보를 획득할 수 없도록 CoNaP (Content Name based Privacy) Schema를 제안하였다[20].

Ⅲ. 형태보존암호를 이용한 Content 기밀성 보호 기법

본 장에서는 NDN 환경에서 평문 상태로 통신하는 콘텐츠 정보의 기밀성을 보호하기 위해 형태보존암호를 이용한 Content Name 암호화 기법을 제안한다. 제안하는 기법은 형태보존암호를 적용하여 효과적으로 콘텐츠의 기밀성을 보호하기 위해 키 관리 노드(Key Management Node)를 추가하였다. 콘텐츠 생산자와 소비자가 중개 라우터를 통해 콘텐츠 정보를 등록, 검색할 때 기밀성을 보장하기 위해 콘텐츠 정보의 암호화 키를 관리, 분배한다. 키 관리 노드는 노드 간 인증과 키 교환을 진행하고, 콘텐츠 이름이 암호화되더라도 중개 라우터를 통한 흐름제어 및 캐시 기능이 상실되지 않는다.

3.1 NDN 노드 인증 및 키 관리 절차

NDN 네트워크 상에서 노드 간 암호화된 Content Name을 이용하여 통신하기 위해 인증 및 키 관리 프로토콜을 사용한다. [표 1]은 형태보존암호화 수행 시 인증 및 키 관리 절차에 대한 용어의 정의이다.

[그림 4]는 NDN 노드 간 인증 및 키 관리 절차로 이에 대한 과정은 다음과 같다.

표 1. 용어 정리
Table 1. Notations

Defining	Description
PU(N)	Node's Public Key
PR(N)	Node's Private Key
PU(KM)	Key Management Node's Public Key
PR(KM)	Key Management Node's Private Key
SK	Session Key
Token	Authorization Token
FPE_K	Format-Preserving Encryption Key
T_K	Format-Preserving Encryption Tweak

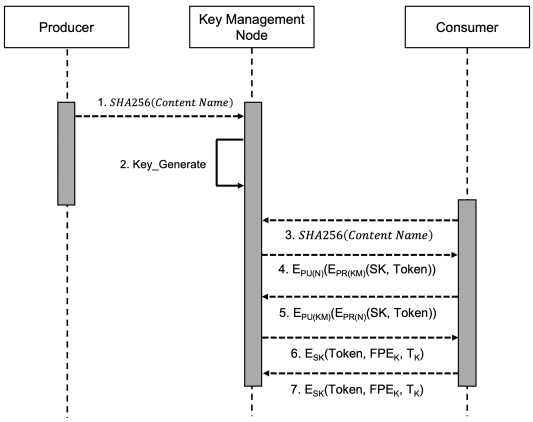

그림 4. 형태보존암호가 적용된 NDN 노드 인증 및 키 관리 절차
Fig. 4. Process of Authentication and Key Management Protocol in FPE-NDN

1. 콘텐츠 생산자가 Content Name의 해시 값을 키 관리 노드에 전송한다.
2. 키 관리 노드는 수신된 값을 기반으로 형태보존암호에 사용될 키를 생성한다.
3. 콘텐츠 소비자는 통신을 시작하기 전 인증을 수행하기 위해 Content Name의 해시 값을 키 관리 노드에 전송한다.
4. 키 관리 노드는 자신의 개인키 *PR(KM)*로 암호화된 세션키 *SK*와 *Token*을 콘텐츠 소비자의 공개키 *PU(N)*로 암호화하여 전송한다. 이때 소비자의 개인키 *PR(N)* 로 암호문을 복호화하고 이를 다시 키 관리 노드의 공개키 *PU(KM)*로 인증하여 세션키 *SK*와 *Token*을 얻는다.
5. 콘텐츠 소비자는 키 관리 노드에게 통신이 준비됨을 알리기 위해 세션키 *SK*와 *Token*을을 자신의 개인키 *PR(N)*로 암호화하고 이를 다시 키 관리 노드의 공개키 *PU(KM)*로 암호화하여 전송한다.
6. 키 관리 노드는 세션키 *SK*로 *Token*을, FPE_K, T_K를 암호화하여 콘텐츠 소비자에게 전송한 다. 소비자는 수신한 암호문을 세션키 *SK*로 복호해 FPE_K, T_K을 얻는다.
7. 콘텐츠 소비자는 키 관리 노드에게 세션키 *SK*로 FPE_K, T_K를 암호화하여 전송함으로 키 교환 과정이 완료되었음을 알린다.

3.2 형태보존암호를 이용한 Content Name 암호화 과정

본 논문에서 제안하는 형태보존암호를 이용한 NDN 네트워크의 구성 방식은 [그림 5]와 같다. 네트

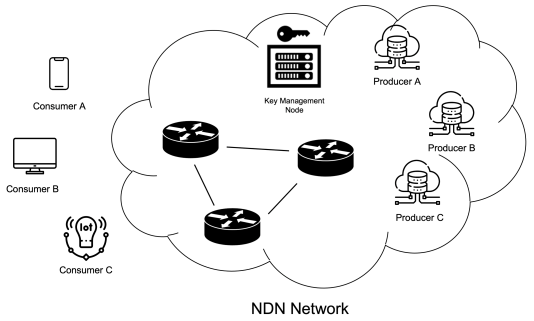

그림 5. 제안 방식 구성도
Fig. 5. Proposed NDN Environment

워크 내 구성은 콘텐츠 소비자, 라우터, 키 관리 노드, 콘텐츠 생산자로 각 노드는 NDN 네트워크 환경에서 통신한다. 이때 라우터는 원활한 흐름제어와 FIB의 포워딩 복잡도를 줄이기 위해 패킷이 수신되었을 때 키 관리 노드와 통신하여 인증 및 키 교환 절차를 수행하고 복호된 콘텐츠 이름을 캐시한다. 이를 통해 기존의 암호화 키가 만료되어도 라우터 내 CS와 PIT에 캐시된 데이터는 영향을 받지 않아 평상 동일한 흐름제어가 가능하다. 또한, 노드 간 인증 과정을 통신 전 수행해 신뢰성 있는 통신이 가능하다.

[그림 6]은 형태보존암호를 이용한 NDN 네트워크에서 콘텐츠 소비자와 생산자 간 통신 과정이다. 두 노드 간 네트워크 통신 과정은 다음과 같다.

1. 콘텐츠 생산자는 키 관리 노드와 인증 및 키 교환 절차를 수행한다.
2. 암호화된 콘텐츠 이름을 라우터 노드(NDN Router A)에 Broadcasting하고, Interest 패킷에 대응하기 위해 대기한다.
3. 콘텐츠 소비자는 키 관리 노드와 인증 및 키 교환 절차를 수행하고, 발급된 암호화 키를 이용해 콘텐츠 이름을 암호화한다.
4. 암호화된 콘텐츠 이름을 Interest 패킷에 담고 라우터 노드(NDN Router B)에 포워딩한다.
5. 라우터는 요청된 Interest의 콘텐츠 이름을 복호하고 NDN 컴포넌트에 캐시한다. 단, 컴포넌트에 이전 기록된 정보가 있는 경우 Data 패킷에 캐시 된 콘텐츠 정보를 포함하여 컨텐츠 소비자에게 전달한다.
6. 이후 라우터는 Interest를 적응형 전달 전략과 FIB에 따라 다음 노드에 포워딩하고 통신을 마무리한다.
7. 콘텐츠 생산자는 Interest가 요청되면 콘텐츠 이름의 생명주기를 확인하고, 패킷 내 콘텐츠 이름을 복호한다. 단, 콘텐츠 이름 복호 실패 시 Interest를 폐기한다.
8. 이후 컨텐츠 생산자는 콘텐츠 정보를 Data 패킷에 포함하고 패킷을 라우터 노드(NDN Router A)에 전송한다.
9. 라우터는 Data 패킷이 들어오면 컴포넌트에 기록

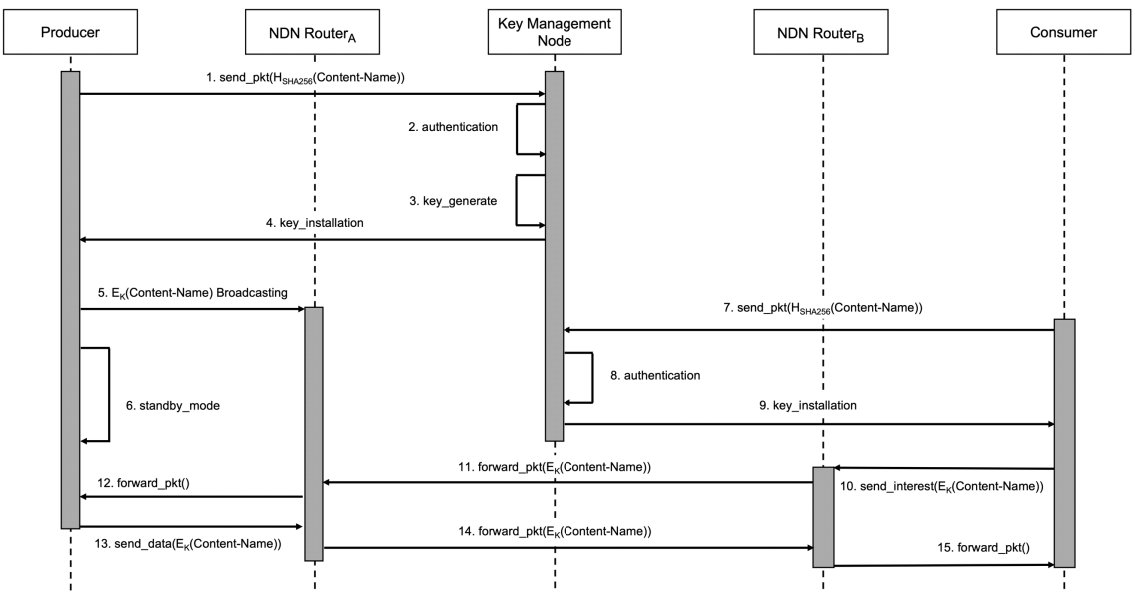

그림 6. 형태보존암호화가 적용된 NDN 네트워크의 패킷 통신 과정
Fig. 6. Process of Packet Communication in NDN Network based on Format-Preserving Encryption

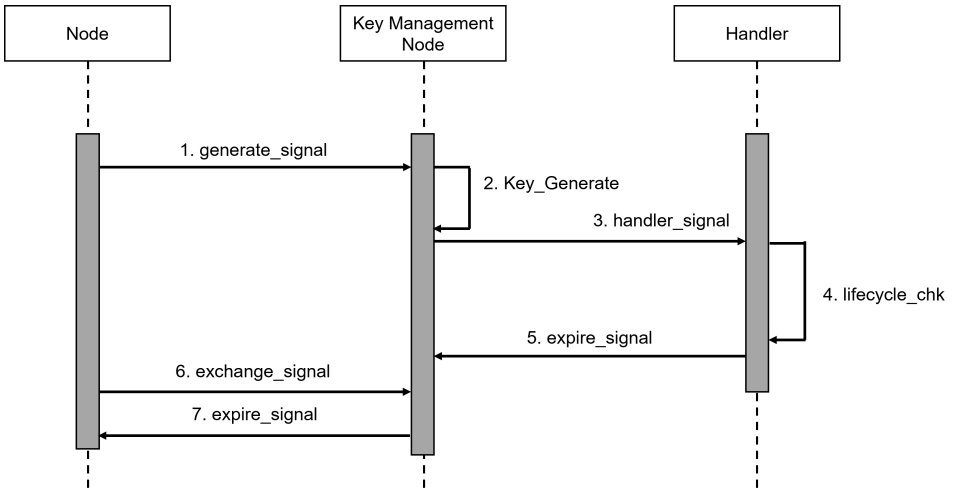

그림 7. 암호화된 콘텐츠 이름의 암호화 키 생명 주기
Fig. 7. Lifecycle of Encrypted Content Name via FPE Key

된 엔티티에 콘텐츠 이름을 검색하고, 인터페이스에 따라 콘텐츠 소비자에게 포워딩한다.

[그림 7]은 통신 중 사용하는 생명주기 메커니즘으로 콘텐츠 생산자는 이를 기반으로 주기적으로 키를 재생성해 보안도를 높이고 콘텐츠의 기밀성을 보호한다. 또, 통신 상태를 유지하고 있는 노드가 있는 경우 생명주기 갱신을 통해 가용성을 유지하고 콘텐츠 정보의 손실을 막는다. 생명주기 메커니즘의 동작 과정은 다음과 같다.

1. 콘텐츠 생산자로부터 생성 신호를 수신한 키 관리 노드는 키를 생성하고, Handler에 생명주기를 등록한다.
2. Handler는 등록된 주기를 지속적으로 검증하고, 만료 시점에 키 관리 노드에게 expire 신호를 전송한다. 이때 만료된 키는 폐기한다.
3. 노드가 키 관리 노드에 만료된 키에 대해 교환 신호를 보내오면 해당 키에 대한 expire신호를 전송하고 통신을 종료한다.
4. 콘텐츠 생산자는 expire 신호를 받은 시점에서 키 관리 노드에게 키 생성 신호를 전달한다.

Ⅳ. 구현 및 성능 평가

본 장에서는 형태보존암호를 이용한 Content Name의 암호화 기법의 구현과 성능 평가를 진행한다. 구현에서는 형태보존암호가 적용된 NDN 시스템의 구조를 설명하고, 이를 바탕으로 구현 과정과 알고리즘을 보인다. 성능 평가에서는 형태보존암호 FF3-1과 블록암호 AES[21]를 이용해 동일한 구현 환경에서 비교, 평가한다. 형태보존암호를 이용하였을 때 네트워크 동작 여부와 패킷 전달이 가능함을 실험을 통해 보인다. 제안 기법의 실험 환경은 [그림 5]와 같이 구성하였으며 가상 네트워크를 기반으로 구현하였다. 제안 기법은 Intel i7-8700 @3.20GHz CPU 와 32GB 램 환경에서 Ubuntu 20.04 LTS 운영체제와 오픈소스 NDN Forwarding Daemon (NFD), NDN C++ library (ndn-cxx)를 이용해 구현하였다. 또한, 콘텐츠 생산자는 1000 bytes 크기의 콘텐츠를 갖도록 하였고, 콘텐츠 소비자는 1,000개의 Interest 패킷을 전송하도록 구성하였다.

4.1 구현

미래 인터넷 아키텍처인 NDN은 오픈소스 형태로 온라인 코드 저장소(GitHub)에 공개되어 있다. 본 논문에서 제안하는 형태보존암호를 이용한 시스템은 NDN 프로젝트를 기반으로 구현하였다. 제안하는 방식의 NDN 아키텍처는 [그림 8]와 같다.

발급된 형태보존암호화 키를 사용해 콘텐츠 이름을 암호화, Interest 패킷의 Content Name 필드에 넣어 전송한다. 모든 노드는 패킷 전송 전 키 관리 노드와의 인증 및 키 교환 절차를 수행하고, 이 과정에서 발급된 형태보존암호 키를 기반으로 암호화를 진행한다. NDN 프로젝트는 Name 컴포넌트 구조를 자체적으로 구현해 사용한다. 이로 인해 특정 암호화 시 값이 16

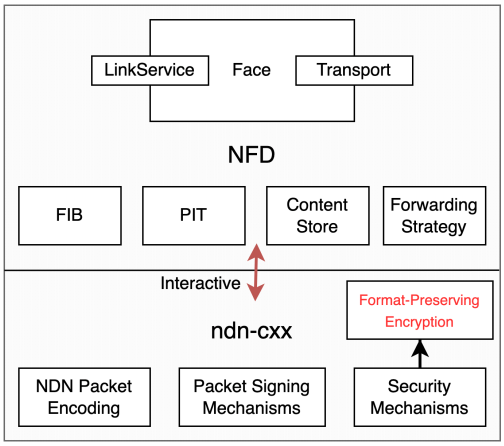

그림 8. 제안하는 NDN 시스템의 아키텍처
Fig. 8. Architecture of Proposed NDN System

진수 또는 이진 값으로 나오는 경우 사용할 수 없다. 하지만 제안하는 기법은 Name 컴포넌트 규약을 그대로 사용할 수 있으면서 암호화되므로 제약이 없다. 소비자 노드에서 콘텐츠 이름 암호화 과정에 대한 구현 코드는 [Algorithm 1]와 같다.

NDN의 콘텐츠 이름은 계층 구조로 문자 '/'를 기준으로 각 계층을 구분한다. 콘텐츠 소비자와 라우터 노드에서 사용되는 알고리즘은 인증, 키 교환 절차를 거친 후 Boolean 체크를 진행한다. 문제가 없는 경우 콘텐츠 이름을 입력 X로 받는다. 입력 X로부터 문자열 인덱스 0을 기준으로 문자 '/'의 인덱스 번호를 찾아 각 계층을 구분하고, 발급된 키로 암호화한 뒤 재조립하여 NDN의 Name 컴포넌트로 구성한다. 이러한 과정을 반복 수행 후 마지막 계층이 암호화된 후 While Loop를 종료한다. 콘텐츠 생산자의 경우 Real-Application을 통해 콘텐츠를 제공할 때 키 관리 노드에 키 생성 신호를 전달한 후 키 교환 절차를 밟는다.

[표 2]는 제안하는 기법에서 구현된 암호화 방식에 따라 콘텐츠 이름의 값을 비교한 결과이다. 평문 상태의 경우 30 bytes 크기를 가지는 "/sch.ac.kr/calab/research.file"의 콘텐츠 이름을 사용하였다. 또한, 형태보존암호가 적용된 경우 "/jwelvrtpw/4jbyh/jncvnntvdqpxu"로 평문과 동일한 형태와 길이를 갖는다. 반면, 블록 암호 AES는 블록 단위로 암호문을 생성하여 입력의 길이에 상관없이 블록 길이 128bit의 암호문 블록을 생성한다. 이때 암호문에 특수 문자와 같은 값이 포함되어 Name 컴포넌트에서 사용할 수 없거나 통신 시 손실되는 등 문제

Algorithm 1: Node in Real-Application of NDN

Prerequisites:
Designed function for Consumer and Router, and it must be used in all communications;

Key, K. for the block cipher;
Base, radix;
Tweak bit string, T. such that LEN(T) = 64;

Inputs:
Uri bit string, X. in base radix of length n, such that n ∈ [minlen...maxlen];

Steps:
1. **Let** auth = authentication(X).
2. **Let** pkE = pubKeyExchange(auth).
3. **Let** kE = KeyExchange(auth, pkE).
4. **Let** iCompStart = 0.
5. **If** pkE **and** kE **is False**, **Return** error.
6. **While** iCompStart **from** X.size():
   i. iCompEnd = X.find('/', iCompStart).
   ii. **If** iCompEnd **is equal to** 0xffffffff, iCompEnd = X.size().
   iii. **Let** Y_i = X.substr(iCompStart, iCompEnd – iCompStart).
   iv. FF3-1.Encrypt(FPE_K, T_K, Y_i).
   v. append(Component::fromEscapedString(Y_i)).
   vi. iCompStart = iCompEnd + 1.

표 2. 암호화 방식에 따른 Content Name 비교
Table 2. Comparison Content Name by Encryption Type

Type	Content Name	Length (Byte)
Non-Encrypted	/sch.ac.kr/calab/research.file	30
FPE	/jwelvrtpw/4jbyh/jncvnntvdqpxu	30
AES	/WclmKYz1x1ZNiG3xmLyGUw/o2be1ktIzO3v/O+iEwKbbw/LOfVT3e5Gyegvhgd NIqRxw	69

가 발생한다. 또, 비교적 큰 용량을 갖는 콘텐츠 이용 시 패킷 분할에 따른 네트워크 비용이 증가한다.

4.2 성능 평가

4.2.1 네트워크 통신 실험

NDN 네트워크는 콘텐츠 생산자가 콘텐츠를 네트워크상에 업로드하면 소비자는 필요로 하는 콘텐츠를 이용하는 구조다. 콘텐츠 이름 암호화 시 사용된 키에 따라 결과 값이 달라지는데 이는 라우터에서 흐름제어 확보 불능 상태로 빠질 수 있고, 궁극적으로 패킷 손실로 이어진다. 또, 암호화 키에 따른 결과 값이 모

두 노드 내 컴포넌트에 기록되는 등 네트워크 자원에서 문제가 발생한다. 따라서 암호화를 적용하더라도 네트워크 흐름제어를 확보하면서 통신할 수 있어야 한다. 제안하는 기법은 이러한 콘텐츠 이용 과정에서 발생할 수 있는 프라이버시 문제를 해결하고, 기밀성 보호를 위해 콘텐츠 이름을 암호화하였다. 또, 흐름제어 확보를 위해 라우터 상에서 콘텐츠 이름을 복호한 뒤 캐시해 키 교환 절차에 따른 문제 해결이 가능하다. [그림 9]은 형태보존암호와 블록 암호 AES를 이용하여 구현된 NDN 네트워크에서 왕복 시간(Round-Trip Time, RTT)에 따른 패킷 전달을 표현하였다. 콘텐츠 소비자와 생산자 노드 간 통신 중 RTT의 값이 0.5~0.75ms인 구간에서 형태보존암호가 적용된 경우(FPE-NDN) 최초 41개 패킷이 전달되었고, AES가 적용된 경우(AES-NDN) 0개의 패킷이 전달되었다. 이러한 결과는 통신 속도 관점에서 형태보존암호가 우위에 있음을 증명한다. 또, RTT 0.75~1.0ms에서는 대부분의 패킷이 전달되는 경향을 보였다. FPE-NDN이 791개, AES-NDN이 116개로 형태보존암호가 적용된 NDN 네트워크가 가장 많은 패킷이 전달되었다. 따라서 두 암호화 타입 모두 통신이 가능하지만 형태보존암호가 적용된 NDN이 통신상 자원 사용 측면에서 우위를 점한다.

4.2.2 네트워크 비교 및 기밀성 보호 평가

NDN의 보안성은 콘텐츠 이름 보안성, 라우팅 및 포워딩, 애플리케이션 보안 등으로 나누어져 있다[15]. NDN에서의 보안은 통신상에서 사용되는 데이터 자체에 내장되어 제공하고 있다[22]. 제안하는 방법은 패킷의 Content Name 필드에 들어갈 데이터를 통신 전 직접 암호화함으로써 기밀성을 보호한다. 네트워크의 기밀성 보호는 암호화 방식에 따라 평가한다. 또, 암호별 패킷내 필드의 크기 비교를 통해 제안하는 기법의 타당성을 보인다.

암호화 방식 별 기밀성 보호 평가는 [표 3]와 같다.

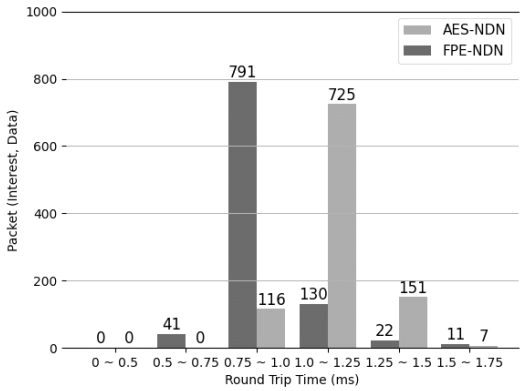

그림 9. 왕복 시간에 따른 패킷 전달 비율
Fig. 9. Ratio of Packet Communication by RTT

O는 기밀성이 보호됨을, X는 그렇지 않음 을 의미한다. 형태보존암호와 블록 암호 AES가 적용된 경우 기밀성 보호로 안전한 통신이 능하다는 공통점이 있다. 하지만 AES의 경우 형태보존암호와 달리 암호화 시 데이터 형태와 길이가 변화하여 패킷 크기에 영향을 미친다. 그러나 제안하는 기법은 평문의 형태와 길이를 그대로 유지하고 있고, 기밀성 보호를 제공해 공간 자원에 영향을 미치지 않는다.

4.2.3 통신 지연 평가

본 실험은 제안하는 기법이 콘텐츠 이름의 암호화에 따라 네트워크 성능에 얼마나 영향을 미치는지 확인하기 위함이다. 이를 위해 네트워크의 성능 판단 요소 중 패킷의 왕복 시간 (Round-Trip Time, RTT)을 이용해 지연 시간을 측정하였다. 제안한 기법과 블록 암호 AES를 적용한 NDN을 동일 환경에서 구현하여 비교하였다. 실험 결과는 [그림 10]과 같다.

형태보존암호와 블록 암호 AES를 적용한 NDN 기법의 패킷 왕복 시간을 측정한 결과 약 93%가 0.8~1.2ms의 값으로 측정되었다. 시간을 비교했을 때 형태보존암호 기법이 AES 기법보다 최대 0.4ms, 최

표 3. 암호화 스키마 별 패킷 정보와 기밀성 보호 평가
Table 3. Packet Information and Evaluation of Confidentiality Protection

Data Type		Packet Size	Length Breakdown (Byte)			Schema Confidentiality		
Non-Encrypted	Interest	125	Content Name	Content	Sig Value	Consumer	Router	Producer
	Data	1243	30	1000	71	X	X	X
FPE	Interest	125	Content Name	Content	Sig Value	Consumer	Router	Producer
	Data	1243	30	1000	71	O	O	O
AES	Interest	194	Content Name	Content	Sig Value	Consumer	Router	Producer
	Data	1341	99	1000	71	O	O	O

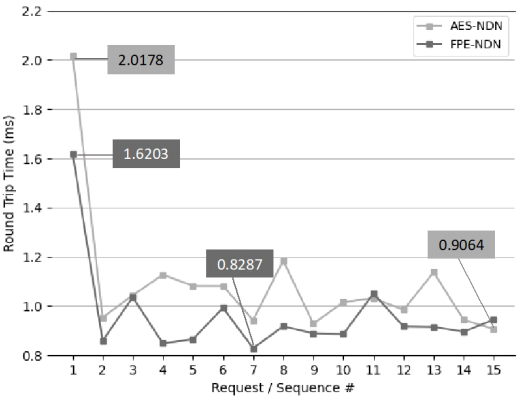

그림 10. FPE와 AES 기법의 왕복 지연 시간 비교
Fig. 10. Comparison Latency between FPE and AES

소 0.08ms로 지연 속도가 개선되었다. NDN 네트워크의 특징 중 하나로 첫 통신에서는 NDN 컴포넌트의 캐시 된 정보가 없고 흐름제어를 확보하는 과정을 거치기 때문에 첫 번째 패킷은 긴 시간이 소요된다. 반면, 두 번째 패킷에서는 짧은 시간이 소요된다. 그 이유는 NDN에서 캐시되는 정보를 갖는 노드가 많을수록 속도가 빨라지는 특징이 있기 때문이다[23].

V. 결 론

NDN은 기존의 IP 주소 체계를 갖는 네트워크의 약점을 해결하면서 효율적인 콘텐츠 배포 및 제어가 가능하다. 하지만 사용되는 콘텐츠의 이름과 데이터가 평문 상태로 네트워크상에서 이동하기 때문에 콘텐츠에 대한 기밀성 보호가 불가능해 프라이버시 문제가 발생한다. 이에 본 논문에서는 NDN 환경에서 형태보존암호를 이용해 콘텐츠 이름 암호화 기법을 제안하였다. 콘텐츠의 이름에 대한 형태보존암호 적용, 패킷의 포워딩에 따른 흐름제어, 키 관리 기법으로 구성된다. 제안하는 기법은 콘텐츠에 대한 기밀성 보호와 속도 비교 실험을 통해 블록 암호 AES를 적용하였을 때보다 지연시간이 약 1.3% 짧음을 보였다. 또, 기밀성 보호를 통해 콘텐츠의 프라이버시 보호가 가능함을 확인하였다.

References

[1] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, and S. Wolff, “A brief history of the internet,” *SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 5, pp. 22-31, 2009. (http://doi.org/10.1145/1629607.1629613)

[2] D. Clark, “The design philosophy of the DARPA internet protocols,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 18, no. 1, pp. 106-114, 1988. (https://doi.org/10.1145/52325.52336)

[3] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlmann, “A survey of information-centric networking,” *IEEE Commun. Mag.*, vol. 50, no. 7, pp. 26-36, Jul. 2012. (https://doi.org/10.1109/MCOM.2012.6231276)

[4] S. H. Byun, “Trends in future internet architecture research,” *Electronics and Telecommun. Trends*, vol. 24, no. 3, pp. 1-12, 2009. (https://doi.org/10.22648/ETRI.2009.J.240301)

[5] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs, and R. Braynard, “Networking named content,” in *Proc. 5th Int. Conf. Emerging Netw. Experiments and Technol.*, pp. 1-12, 2009. (https://doi.org/10.1145/1658939.1658941)

[6] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, kc claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, “Named data networking,” *Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66-73, Jul. 2014. (https://doi.org/10.1145/2656877.2656887)

[7] A. Afanasyev, J. Burke, T. Refaei, L. Wang, B. Zhang, and L. Zhang, “A brief introduction to named data networking,” *MILCOM 2018*, pp. 1-6, 2018. (https://doi.org/10.1109/MILCOM.2018.8599682)

[8] N. Kumar, A. K. Singh, A. Aleem, and S. Srivastava, “Security attacks in named data networking: A review and research directions,” *J. Comput. Sci. and Technol.*, vol. 34, no. 6, pp. 1319-1350, Nov. 2019. (https://doi.org/10.1007/s11390-019-1978-9)

[9] TTA, *Format-Preserving Encryption Algorithm FEA*(2015), Retrieved Sep. 6, 2022, from https://www.tta.or.kr.

[10] NIST, *Special Publication 800-38G Revision*

1: Recommendation for Block Cipher Modes of Operation-Methods for Format-Preserving Encryption(2019), Retrieved Sep. 2, 2022, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38Gr1-draft.pdf. (https://doi.org/10.6028/NIST.SP.800-38Gr1-draft)

[11] B. Michael and S. Harry, "Using datatype-preserving encryption to enhance data warehouse security," *20th NISSC*, pp. 141-149, 1997.

[12] B. John and P. Rogaway, "Cipher with arbitrary finite domains," *RSA Data Secur. Conf. Cryptographer's Track (RSA CT '02)*, 2271, pp. 114-130, 2002. (https://doi.org/10.1007/3-540-45760-7_9)

[13] W. Jang and S.-Y. Lee, "Implementation and performance evaluation of the format preserving encryption FEA algorithm," *J. KICS*, vol. 46, no. 3, pp. 420-429, 2020. (https://doi.org/10.7840/kics.2021.46.3.420)

[14] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, kc claffy, D. Krioukov, D. Massey, C. Papadopoulos, T. Abdelzaher, L. Wang, P. Crowley, and E. Yeh, *Named Data Networking (NDN) Project*(2010), Retrieved Jul. 2022, from https://named-data.net/techreport/TR001ndn-proj.pdf

[15] A. Chavez, P. Cordeiro, G. Huang, P. Kitsos, T. La Pay, A. Short, and A. Summers, *Named Data Networking for DER Cybersecurity* (2021), Retrieved Aug. 20, 2022, from https://www.osti.gov/biblio/1820522. (https://doi.org/10.2172/1820522)

[16] Z. Zhang and K. Zhang, "Research on security and privacy issues of NDN," in *Proc. 2nd Int. Conf. Soft Comput. in Inf. Commun. Technol.*, pp. 67-71, May 2014. (https://doi.org/10.2991/scict-14.2014.17)

[17] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, and L. Zhang, "An overview of security support in named data networking," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 62-68, Nov. 2018. (https://doi.org/10.1109/MCOM.2018.1701147)

[18] T. Chatterjee, S. Ruj, and S. D. Bit, "Security issues in named data networks," *IEEE Comput.*, vol. 51, no. 1, pp. 66-75, Jan. 2018. (https://doi.org/10.1109/MC.2018.1151010)

[19] K. T. Ko, H. H. Hlaing, and M. Mambo, "A PEKS-Based NDN strategy for name privacy," *Feture Internet (MDPI)*, vol. 12, no. 8, pp. 1-22, Jul. 2020. (https://doi.org/10.3390/fi12080130)

[20] N. Leshov, M. A. Yaqub, M. T. R. Khan, S. Lee, and D. Kim, "Content name privacy in tactical named data networking," *IEEE 2019 Eleventh ICUFN*, pp. 570-572, 2019. (https://doi.org/10.1109/ICUFN.2019.8805919)

[21] NIST Federal Inf. Process. Stds., *Advanced Encryption Standard (AES)*(2001), Retrieved Aug., 29, 2022, from https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[22] V. Jacobson, D. K. Smetters, J. D. Thornton, M. Plass, N. Briggs, and R. Braynard, "Networking named content," *Commun. ACM*, vol. 55, no. 1, pp. 117-124, 2012. (https://doi.org/10.1145/2063176.2063204)

[23] S. Choi, "Data pre-caching and cached data lifetime increase methods in NDN-based drone networks," M.S. Thesis, University of Hanyang, 2019.

이 상 현 (Sang Hyeon Lee)

2020년 3월~현재 : 순천향대학교 정보보호학과 학사과정

<관심분야> 정보보안, NDN, 암호응용, 취약점분석

[ORCID:0000-0002-5475-4778]

정 다 윗 (Da Wit Jeong)

2019년 3월~현재 : 순천향대학교 정보보호학과 학사과정

<관심분야> 정보보안, 네트워크보안, 취약점분석, 딥러닝

[ORCID:0000-0002-7915-7160]

이 선 영 (Sun-Young Lee)

1993년 2월 : 부경대학교 전자계산학과(이학사)

1995년 2월 : 부경대학교 전자정보공학과(이학석사)

2001년 3월 : 일본도쿄대학 전자정보공학과(공학박사)

2004년 3월~현재 : 순천향대학교 정보보호학과 교수

<관심분야> 콘텐츠보안, 암호이론, 정보이론, 정보보안

[ORCID:0000-0002-4686-9436]