J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

기가비트 이더넷 망에서 OFB 방식을 이용한 물리 계층 프레임 보안 기법

Frame security method in physical layer using OFB over Gigabit Ethernet Network

임 성 렬1*
Sung-yeal Im

요 약

본 논문은 기가비트 이더넷 망에서 AES 알고리즘을 적용한 OFB 방식의 암호화/복호화를 이용한 물리 계층 프레임 보안 기법에 관한 것이다. 기가비트 이더넷 망에서 데이터 송수신시에 프레임을 보안 강도가 강력한 AES 알고리즘을 적용한 OFB 방식의 암호화/복호화를 수행하는 물리 계층에서의 데이터 보안 기법을 제안한다. 일반적으로 기가비트 이더넷망 운영 시에 보안 기능이 없으나 데이터 보안이 필요할 경우에 본 기법을 적용한 장치를 부가적으로 설치하여 보안 기능을 수행할 수가 있다. 기가비트 이더넷 망에서 데이터 전송 시에 이더넷 프레임은 IEEE 802.3 규격에 준하는 데 이 프레임에는 데이터 필드 외에도 수신 노드에서 데이터의 올바른 수신을 보장하기 위한 몇 개의 필드가 포함되어 있다. 암호화 시에는 이러한 영역을 제외한 데이터 영역만 암호화하여 실시간으로 전송하여 주어야 한다. 본 논문에서는 평문으로 구성된 IEEE802.3 프레임의 데이터 영역만 송신노드에서 암호화하여 전송한 프레임을 수신 노드에서 수신한 후 데이터 영역만 복호화하여 전송된 평문이 복구됨을 확인하여 암호화/복호화가 가능함을 보여준다. 일반적으로 보안 기능이 없이 운용하는 이더넷 망에서 데이터에 대한 보안이 요구될 시에 본 기법을 적용한 장치를 부가적으로 설치함으로서 시스템의 신뢰성을 높일 수 있다.

☞ 주제어 : 이더넷, 암호화, AES, OFB

ABSTRACT

This paper is about a physical layer frame security technique using OFB-style encryption/decryption with AES algorithms on Gigabit Ethernet network. We propose a data security technique at the physical layer that performs OFB-style encryption/decryption with AES algorithm with strong security strength when sending and receiving data over Gigabit Ethernet network. Generally, when operating Gigabit Ethernet network, there is no security features, but data security is required, additional devices that apply this technique can be installed to perform security functions. In the case of data transmission over Gigabit Ethernet network, the Ethernet frames conform to IEEE 802.3 specification, which includes several fields to ensure proper reception of data at the receiving node in addition to the data field . When encrypting, only the data field should be encrypted and transmitted in real time. In this paper, we show that only the data field of the IEEE802.3 frame is encrypted and transmitted on the sending node, and only the data field is decrypted to show the plain text on the receiving node, which shows that the encryption/decryption is carried out correctly. Therefore, additional installation of devices that apply this technique can increase the reliability of the system when security for data is required in Ethernet network operating without security features.

☞ keyword : ethernet, encryption, AES, OFB

1. 서 론

일반적으로 이더넷 망은 하나의 망을 여러 개의 노드가 공유하여 각 노드를 주소로 구분하여 사용함으로 보안에 취약할 수가 있다. 또한 이더넷 망을 사용하는 건물이나 캠퍼스 등에서는 외부에 노출되지 않는 공간이 많아 침입자가 망에 용이하게 접근하여 정보를 취득할 가능성이 있다. 이에 대한 대책으로 데이터를 암호화하여 전송하여 정보를 습득하더라도 해석이 불가능하게 한다.

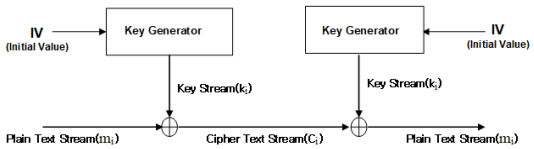
암호화 알고리즘 적용 시 소프트웨어 방식의 구현은 개발 및 수정이 용이하여 개발 기간이 단축되는 효과는

1 Office of General Education, Pusan National University, Busan, 46241, South Korea
* Corresponding author (syim7@pusan.ac.kr)
[Received 14 June 2021, Reviewed 16 July 2021(R2 17 August 2021, R3 7 September 2021), Accepted 11 September 2021]

있으나 하드웨어로 구현한 방식에 비해 암호화 처리 속도가 느리다. 알고리즘의 검증 단계 혹은 암호화 프로그램을 다운 받아 사용해야 하는 시스템에서는 소프트웨어적인 구현도 방책이나, 고속의 데이터 처리를 요구하는 통신망에서 데이터를 실시간으로 처리해 주기 위해서는 암호 알고리즘의 하드웨어적인 구현이 필수적이다[1, 2].

본 논문에서는 Gigabit 이더넷과 같은 고속 통신망에서 프레임 데이터 전송 시에[3] 프레임 데이터를 실시간적으로 암호화/복호화를 수행하는 데이터 보안 기법을 제안한다.

암호화 방식에는 블록 암호와 스트림 암호화 방식이 있으며[4] 스트림 암호화 방식의 장점은 변환 속도가 빠르다는 것이다. 스트림 암호화 방식은 다시 동기식 스트림 암호화 방식과 자기 동기식 스트림 암호화 방식으로 나눌 수 있다[5]. 이더넷 망에서 데이터 전송에서는 데이터 프레임의 수신 주기가 가변이므로 데이터가 손상되면 자기 동기식 암호화 방식에서는 다시 동기를 맞추기가 어렵다. 이러한 형태의 데이터에는 동기식 암호화 방식이 적합하다[6]. 키 생성 알고리즘은 약정되어 있어 수신 측에서 복호화 시에도 키의 재생성이 가능하다. 키 발생기의 초기 상태는 초기값 IV 로 초기화된다. 키 발생 스트림은 송신 측 암호화 키 생성 알고리즘과 수신 측 복호화 키 생성 알고리즘이 동일해야 한다.



(그림 1) 동기식 암호화 방식
(Figure 1) Synchronous stream cipher

그림 1에서 XOR 알고리즘을 이용한 동기식 스트림 암호화 방식의 원리를 보여주고 있다[7]. 동기식 암호화 방식에서는 1 비트나 1 바이트의 전송 에러가 연속된 다른 비트나 바이트에 영향을 미치지 않는다. 동기식 스트림 암호화 방식에서는 키스트림이 암호화할 평문 스트림과는 무관하게 생성되므로 암호화문이 전송 중에 손상되거나 분실되었을 때 다음 작업을 위해 송신 측과 수신 측에서 키 발생기를 다시 동기시켜야 한다[8].

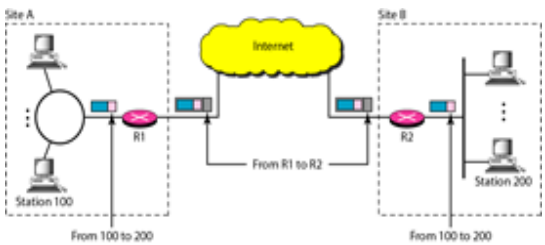
본 논문에서는 그림 1에서의 키 발생기를 OFB방식을 적용한 AES 알고리즘으로 구현하여 암호화 강도를 높였으며 입력되는 평문은 이더넷 프레임이며 암호화된 스트림은 이더넷 프레임의 페이로드만 암호화된 이더넷 프레임이 되게 된다.

이더넷 망은 데이터 프레임의 길이가 가변이므로 암호화 블록 길이가 정해진 AES같은 블록 암호를 직접 적용하기는 어려움으로 본 논문에서는 동기식 스트림 암호화 방식인 OFB 방식을 적용하여 블록암호인 AES 를 비트 단위의 스트림 암호화 방식으로 구현하여[9] 실험을 통해 암호화/복호화 과정을 검증하였다.

본 논문의 구성으로는 제2장에 기존 망의 암호화 운용 사례를 살펴보고 제3장에 AES 알고리즘과 OFB 암호화 방식을 소개하고 제4장에서는 이더넷 망과 이더넷 프레임의 구조에 대해 살펴보고 제5장에서 이더넷 망에서의 프레임 보안 기법에 대해 설명하며 제6장에서 결론을 맺는다.

2. 기존 망의 암호화 운용 사례

이더넷 망은 외부 망 또는 인터넷과 연결이 되지 않은 유선으로 연결된 근거리 통신망(LAN)으로 단일 사설망이다. 이에 비해 가상사설망(VPN)은 수 개의 근거리 통신망을 인터넷망에 연결하여 보안알고리즘으로 데이터의 인증, 무결성, 프리이버시를 보장하기 위해 IPSec을 사용하여 터널(tunnel) 방식으로 데이터그램을 교환하는 방식이다[10]. 그림 2에 VPN망의 개념도를 도시하였다. 이 방식에서는 A 사이트에서 발생한 IP 다이어그램은 IPsec 으로 캡슐화 하여 수신자를 R2로 하는 헤더 주소만 추가하여 외부 인터넷 망으로 전송하여 주는 데, 그림 2에서 동작원리를 보여주고 있다. R1 게이트웨이에서는 R2로 전송되는 패킷에 수신자를 R2로 하는 헤더 주소만 추가하여 인터넷 망으로 전송하여 준다. 인터넷 망에서는 이 패킷의 헤더 주소를 판별하여 R2 게이트웨이로 전달하여 준다. R2 게이트웨이에서는 이 다이어그램을 복호화하여 패킷의 수신주소를 판별하여 수신 단말로 전달하여 준다. 이와 같은 VPN 망에서는 R1이나 R2의 네트워크 계층에서 통신 세션의 개별 IP 패킷을 인증하고 암호화 기능을 수



(그림 2) 가상사설망(VPN)
(Figure 2) Virtual Private Network

행하는 IPSec를 이용하여 인터넷 망으로 전송되는 패킷의 암호화 과정이 있음으로 데이터의 보안이 가능하다. 하지만 이더넷 망 자체에서 발생된 데이터는 평문의 패킷이므로 LAN을 단일망으로 운용할 경우에는 데이터의 암호화가 필요할 수도 있으므로 본 논문에서 기술하는 보안 기법을 제안합니다.

3. AES 알고리즘과 OFB(Output Feedback) 암호화 방식

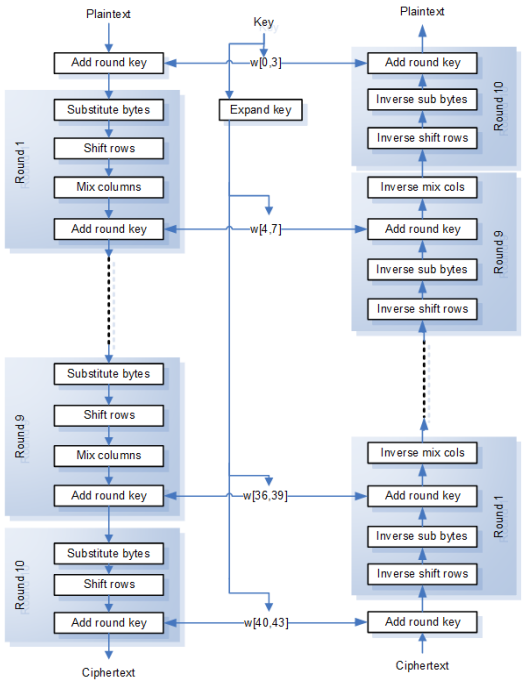
3.1 AES 알고리즘

AES 알고리즘은 미국 NIST에서 차세대 암호 알고리즘으로 1997년 AES를 공모하여 2000년에 최종 알고리즘으로 채택하여[11, 12] 현재까지 블록 암호의 표준으로 사용되어 오고 있다. AES 암호 알고리즘은 대칭키 블록 암호 알고리즘으로서 대칭키 길이와 암호화/복호화의 기본 단위인 블록의 크기를 128, 192, 256 비트 중에서 선택할 수 있는 알고리즘으로 알려진 공격에 강하고[13] 블록의 크기에 따라 총 라운드 수를 달리하는 데 각 라운드는 3개의 독립된 변환으로 구성되어 있다.

각 라운드는 바이트 치환, 행의 쉬프트, 열의 혼합 등으로 구성된 단계를 갖는 데, AES 암호 알고리즘은 128, 192 및 256 비트 단위의 가변 키 길이와 블록 길이를 가질 수 있으며 이에 따라 라운드 수가 결정된다[14]. 본 논문에서는 키 길이를 128 비트, 블록의 길이를 128 비트 단위로 암호화하는 AES를 선택하며 이 경우 암호화 알고리즘의 라운드 수는 10이 된다. 그림 2에 암호화 알고리즘의 라운드가 10인 AES 알고리즘의 암호화/복호화 과정을 보여주고 있다.

3.2 OFB(Output Feedback) 암호화/복호화 방식

본 논문에서는 이더넷 망의 데이터 프레임의 길이가 패킷에 따라 가변이므로 블록암호인 AES 방식에 스트림 암호화 방식인 OFB 방식을 적용하여 스트림 암호화 방식으로 데이터 프레임의 암호화를 구현한다[9]. OFB방식은 현재단의 평문이 암호화된 내용이 다음 단의 평문의 입력으로 인가되어 다시 암호화 과정을 거친다.[15] 그림 3에 스트림으로 인가되는 평문의 데이터의 바이트 단위의 스트림 암호화 데이터로 변환하는 OFB 방식의 암호화 과정을 보여주고 있다. 그림 3에서 각 단계의 Encryrt 박스의 암호화 알고리즘은 AES 이며 암호화 과정은 식(3)과 같이 기술되며



(그림 2) 암호화 라운드가 10인 AES 알고리즘
(Figure 2) AES algorithm with 10 cryptographic rounds

$$C_j = P_j \oplus E(K,[C_{j-1} \oplus P_{j-1}]) \quad (3)$$

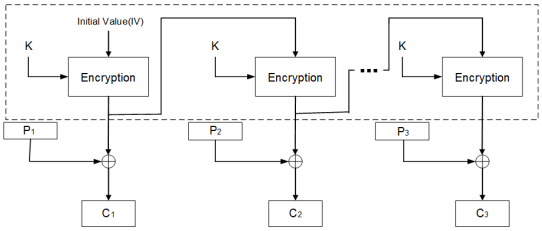
식(4)의 과정을 거쳐 복호화된다.

$$P_j = C_j \oplus E(K,[C_{j-1} \oplus P_{j-1}]) \quad (4)$$

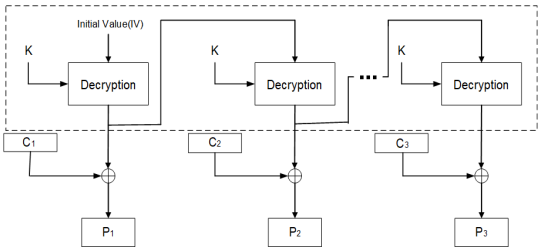
OFB 방식에서의 암호화/복호화 과정은 표 1과 같이 정리할 수 있다. OFB 방식의 유리한 점은 전송중의 비트 에러가 전파되지 않는다는 것이다. 그림 3의 a에서 암호문에서 C_1 바이트에서 1비트의 에러가 발생하면 복호화된 평문의 P_1 바이트에만 영향을 미친다[16].

(표 1) OFB 방식의 암호화/복호화 과정
(Table 1) OFB-based encryption/decryption

OFB	$IV = Nonce$ $I_j = O_{j-1} \quad j = 2, \ldots, N$ $O_j = E(K, I_j) \quad j = 1, \ldots, N$ $C_j = P_j \oplus O_j \quad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus MSB_u(O_N)$	$IV = Nonce$ $I_j = O_{j-1} \quad j = 2, \ldots, N$ $O_j = E(K, I_j) \quad j = 1, \ldots, N$ $P_j = C_j \oplus O_j \quad j = 1, \ldots, N-1$ $P_N^* = C_N^* \oplus MSB_u(O_N)$

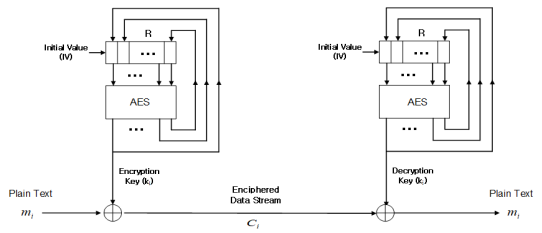


(a) 암호화 과정



(b) 복호화 과정

(그림 3) Output feedback(OFB) 방식
(Figure 3) Output feedback(OFB) method



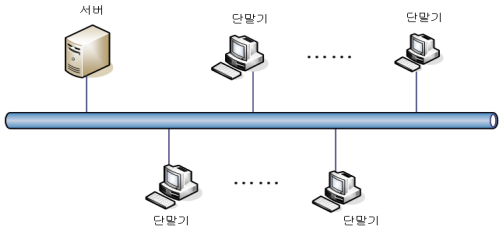
(그림 4) 스트림 데이터 암호화/복호화가 가능한 OFB(Output Feedback)방식
(Figure 4) OFB(Output Feedback) method with stream encryption/decryption

3.3 스트림의 비트 단위로 암호화/복호화가 가능하도록 OFB(Output Feedback)로 구현한 방식

그림 3과 같이 OFB 방식을 구현하여 바이트 단위로 암호화된 데이터를 비트 단위로 변환하여 전송이 가능하나 이와 같이 구현하면 여러 단의 암호화 과정이 필요하며 이는 AES 암호하 소자가 각 단마다 필요하게 되어 암호화 강도면에서는 잇점이 있을지 모르나 회로 구현도 복잡하여 비용 측면에서도 구현 시 경쟁력이 약화될 수가 있다. 그래서 본 논문에서는 송신단과 수신단에서 AES 소자를 한 개씩만 사용하여 암호화 키 발생과 복호화 키 발생용으로 사용하여 OFB 방식을 구현한다. 그림 4는 스트림으로 입력되는 데이터를 비트 단위로 암호화/복호화가 가능하도록 OFB(Output Feedback)이용하여 구현한 것이다[17]. 초기화값(Initala Value)은 난수이며 송신단과 수신단의 값이 일치하여야 하며 키 값은 동일하여야 한다[18].

4. 이더넷 망과 이더넷 프레임의 구조

ISO 9160에서는 물리 계층 데이터 처리 시의 기준을 명시하고 있다. 이더넷 프레임 데이터를 암호화하여 보낼 시에는 데이터 자체를 암호화하여 보낼 수도 있으나, 데이터 단말 장치(Data Terminal Equipment)에서는 일반 데이터 형태로 전송하고 특별히 암호화된 데이터를 필요로 하는 경우에 대비하여 데이터 보안 장치(Data Encipherment Equipment)를 부가 장치로 구성하는 것도 가능하다[19]. 그림 5는 이더넷 망의 개념도이다.



(그림 5) 이더넷 망의 개념도
(Figure 5) Conceptual diagram of Ethernet

OSI의 데이터 링크 계층은 IEEE 표준에서는 논리 링크 제어(Logical Link Control; LLC) 계층과 매개 접근 제어(Media Access Control; MAC) 계층인 두 계층으로 나누어진다. 이 표준은 IEEE 802로 명명되어 있으며 이더넷 관련 표준은 802.3으로 명명되어 있다[20].

이더넷 MAC계층은 상위 계층으로부터 받은 데이터를 프레임 처리하여 물리 계층으로 전달하여 준다. 이더넷 망에서 데이터 전송 시에 프레임은 IEEE802.3규격에 준하는 데 이 프레임에는 데이터 필드 외에도 수신 노드에서 데이터의 올바른 수신을 보장하기 위한 몇 개의 필드가 포함되어 있다. 이더넷 MAC 계층으로부터 전달 받은 이더넷 MAC 프레임에 물리 계층 헤더를 부가하여 이더넷 프레임을 구성하며 그림 6과 같이 7개의 영역이 있다. 이는 프리앰블, 프레임시작구분자, 수신주소, 발신주소, PDU의 길이와 순환여유검사영역이다[21]. 이더넷 프레임 암호화 시에는 다른 영역을 그대로 둔채 데이터 영역만 구분하여 암호화하여야 한다.

(그림 6) 이더넷 프레임
(Figure 6) Ethernet frame

- 프리앰블: 56 비트의 1 과 0의 반복으로 구성되어 있으며 수신 단에 프레임이 입력되는 것을 알리며, 입력 데이터의 타이밍을 동기화한다.
- 프레임 시작 구분자: 1바이트의 비트 패턴(10101011)으로 프레임의 시작을 알린다. 단말기들에 프레임의 동기를 맞출 마지막 신호임을 알려준다. 마지막 2비트의 11은 수신단에 다음의 영역이 수신주소임을 알려준다.
- 수신주소: 6바이트로 구성되어 있으며 프레임을 수신할 단말의 주소를 포함하고 있다.
- 발신주소: 경계를 구분하여 데이터 영역을 암호화한다. 목적지 주소는 프레임을 수신할 노드의 물리 주소이며 출발지 주소는 프레임을 송신하는 노드의 물리 주소이다. 길이 영역은 데이터 영역의 길이를 바이트 수로 표시한 영역이며 그 범위는 46~1500이다.

5. 이더넷 망에서 프레임 보안 기법

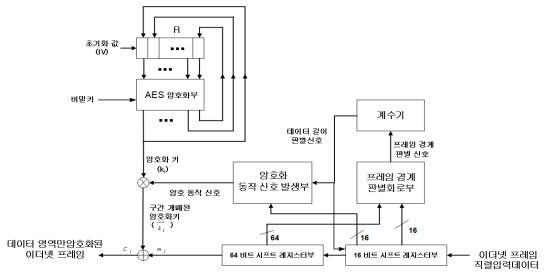
5.1 개요

본 논문에서는 이더넷 망에서의 송수신되는 데이터에 대한 보안을 제공하기 위해 물리 계층에서 이더넷 프레임을 암호화/복호화하는 방법을 기술한다. 이를 위해 프레임 형태로 전송되는 이더넷 LAN 프레임의 여러 필드 중 프레임의 송수신에 관련한 필드 등을 제외한 데이터 영역만 암호화해 주어야 하므로 프레임의 경계를 판별한 후 데이터 영역의 크기를 판별하여 데이터 영역만 암호화/복호화하여야 한다. 이더넷 망에서 이더넷 프레임의 물리 계층 데이터 보안장치는 이더넷 망에서 송신 단에서 송신하는 이더넷 프레임의 데이터 부분만 암호화하여 전송하고 수신 단에서는 수신한 프레임의 경계를 판별하여 전체 프레임에서 암호화된 데이터 영역만 복호화하여 원래 데이터를 복원하는 기능을 수행한다. 이러한 기법을 응용한 장치를 이더넷 망 운용에 있어서 보안 기능을 필요로 할 시에 부가적으로 설치하여 기능을 수행할 수 있도록 모듈 형태로 하여 운용의 편리성을 기할 수 있도록 구성할 수 있다. 이더넷 망에서 전송 데이터는 프레임의 형태로 전송되는 데 본 논문에서는 이 프레임을 구성하는 여러 영역 중 프레임의 송수신에 관련한 영역 등을 제외한 데이터 영역만 암호화한다.

5.2 이더넷 프레임 보안 장치의 구성도

이더넷 프레임 보안장치의 송신측 블록도를 그림 7에 도시하였다. 송신축 데이터 보안장치에서 수행하는 기능은 다음과 같다.

- 64 비트로 구성된 48 비트 시프트 레지스터부와 16 비트 시프트 레지스터부로 구성된 이더넷 데이터 입력 회로
- 데이터 프레임 입력 회로의 비트 패턴을 판별하여 프레임의 경계를 판별하기 위한 프레임 경계 판별 기능
- 프레임 경계 판별 회로부가 발생한 프레임 경계 판별 신호에 준해 인가된 초기값으로 계수하여 개폐 신호 발생부 동작 신호를 발생하여 주는 계수기 기능
- 계수기부가 발생한 개폐 신호 발생부 동작 신호에 따라 이더넷 데이터 프레임의 데이터 영역만 암호화하여 주기 위한 신호 발생을 위한 암호화 동작 신호 발생 기능
- 프레임 경계 판별 회로부가 발생한 프레임 경계 판별 신호에 따라 인가된 암호화 초기값을 이용하여 암호화 키를 발생하여 주는 암호화 키 생성 기능
- 암호화 키와 암호화 동작 신호를 논리적(AND) 연산하여 이더넷 프레임의 데이터 영역에서만 암호화 키를 열어주는 역할을 하는 논리적(AND) 회로 기능
- 이더넷 프레임의 데이터 영역과 암호화 키를 배타적 논리합으로 암호화하여 주는 배타적 논리합(XOR) 회로 기능으로 구성되어 있다.



(그림 7) OFB 방식을 이용한 이더넷 프레임의 암호화
(Figure 7) Encryption of Ethernet frames using OFB

5.3 이더넷 데이터의 암호화 과정

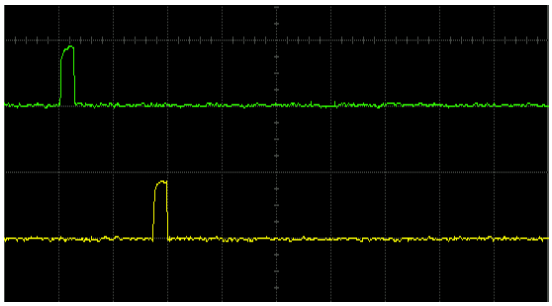
그림 7의 OFB방식을 이용한 이더넷 프레임의 암호화 블록도에서 암호화 원리를 설명한다. 그림 6의 이더넷 프레임의 구조에서 프레임의 경계를 알려주는 패턴인 물리 계층 헤더와 프레임 송수신에 관련된 수신주소와 발신 주소 및 순환 여유 검사부를 제외한 데이터 영역만 암호화 하여야 한다. 이더넷 프레임의 데이터 영역은 최소 46바이트에서 최대 1500바이트인 가변 길이이며 데이터 길이 영역에 데이터 영역의 바이트 수를 그 값으로 가지고 있다. 암호화할 시 직렬로 입력되는 이더넷 프레임에서 데이터 영역의 길이 동안만 암호화해 주어야 하므로 데이터 영역의 길이를 판별한 후 그 데이터 영역 길이에 해당하는 부분의 프레임(m_i)를 구간 개폐된 암호화 키($\overline{k_i}$)와 식 $C_i=m_i \otimes \overline{k_i}$ 에 준해 암호화하여 전송한다. 그림 7의 기능 블록도에서 직렬로 입력되는 이더넷 프레임에서 프레임의 경계를 판별하여 데이터 영역의 길이에 해당하는 부분만 암호화하여 전송하여 준다. 이하 그림 7의 각 블록의 기능을 상세히 설명한다.

5.3.1 64 비트 레지스터부

64 비트 시프트 레지스터부와 16 비트 시프트 레지스터부는 비트 단위로 입력되는 이더넷 프레임의 통로 역할을 하며 이중 64 비트 레지스터부는 이더넷 프레임 직렬 입력 데이터가 직렬로 입력되어 이때 프레임의 물리 계층 헤더에 해당하는 프리앰블(56비트의 1과 0의 반복)과 프레임 시작 구분자에 해당하는 패턴(10101011) 패턴이 64 비트 시프트 레지스터에 입력될 때 이 데이터를 프레임 경계 판별 회로부로 전달한다.

5.3.2 프레임의 경계 판별 회로부

64 비트 시프트 레지스터부에 프레임의 물리 계층 헤더에 해당하는 프리앰블과 프레임 시작 구분자 패턴이 64 비트 시프트 레지스터에 입력되어 검출될 시에 새로운 프레임이 입력된다는 것은 인지하여 프레임 경계 판별 회로부가 프레임의 경계임을 알리는 프레임 경계 판별 신호를 발생시킨다. 이 신호가 계수기부에 인가되면 계수기부에 십진수 14 가 로딩되어 이더넷 프레임의 각 바이트가 입력될 때 마다 1 씩 감소하도록 구성한다. 십진수 14 값의 의미는 그림 3의 이더넷 프레임에서 보듯이 이더넷 프레임 경계 판별 후에 입력되는 프레임의 데이터 길이값 영역의 2 바이트의 위치이다. 이는 프레임의 경계 판별 후 이더넷 프레임의 13-14 번째 바이트에 위치하는 길이 영역이 16 비트 시프트 레지스터부에 도달하는 데 걸리는 클록(clock) 수를 의미한다.



(그림 8) 프레임 경계 판별신호 및 16 비트 레지스터 데이터 길이 전달신호

(Figure 8) Frame boundary detection signal and data length transfer signal of 16 bit register

그림 8의 프레임 경계 판별 회로부에서 경계를 판별한 프레임 경계 판별 신호를 보여주고 있다. 이 신호에 의해 계수기부에서 발생시킨 16 비트 레지스터 데이터 길이 전달 신호를 발생시킨다. 그림 8은 오실로스코프로 측정한 프레임 경계 판별신호 및 16 비트 레지스터 데이터 길이 전달 신호이다.

5.3.3 16 비트 시프트 레지스터부

16 비트 시프트 레지스터부는 비트 단위로 입력되는 프레임의 데이터 길이 영역이 16 비트 시프트 레지스터의 내용으로 도달하였을 때 계수기부에서 발생되어 인가되는 데이터 길이 전달 신호에 따라 프레임에서 데이터 영역의 길이값을 암호화 동작 신호 발생부로 전달하여 주는 역할을 한다. 암호화 동작 신호 발생부에서는 이 데이터의 길이 값에 해당하는 동안만 암호화 동작 신호를 1 로 유지하고 나머지 구간은 0 이 되는 신호인 암호화 동작 신호를 생성한다.

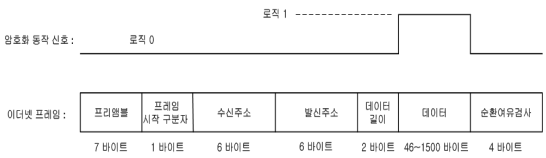
5.3.4 계수기부

계수기부는 프레임 경계 판별 신호에 준해 십진수 14를 초기값으로 설정하여 이더넷 프레임의 각 바이트가 입력될 때 마다 1 씩 감소하여 주며 이 값이 0 이 될 때 데이터 길이 전달 신호를 발생시킨다. 이 신호가 발생될 시

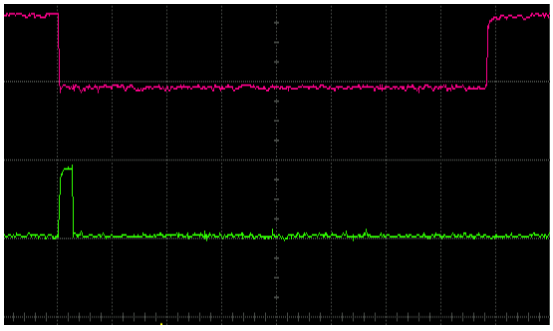
점에 이더넷 프레임의 길이 영역이 16 비트 시프트 레지스터의 내용으로 들어와 있으므로 이 신호를 이용해 16 비트 시프트 레지스터의 내용을 암호화 동작 신호 발생부로 전달하여 준다.

5.3.5 암호화 동작 신호 발생부

암호화 동작 신호 발생부에서는 데이터 길이 판별 신호가 인가되면 16비트 레지스터부로부터 데이터 길이 영역의 값을 전달받아 그 값을 내부 계수기의 초기값으로 설정한 후 이더넷 프레임의 한 바이트가 입력될 때마다 1씩 감소시키며 내부 계수기의 값이 0 이 될 때까지 암호화 동작 신호의 값을 1로 유지하며 그 외 구간은 0 이 되는 암호화 동작 신호를 발생시킨다. 이는 암호화 동작 신호는 이더넷 프레임의 데이터 영역에 해당하는 구간만 로직 1이고 그 외 그간은 로직 0인 신호임을 의미한다. 그림 9에 암호화 동작 신호의 타이밍 도를 도시하였으며, 그림 10에 오실로스코프로 측정한 데이터 프레임 경계 판별 신호와 반전된 암호화 동작 신호를 보여주고 있다.



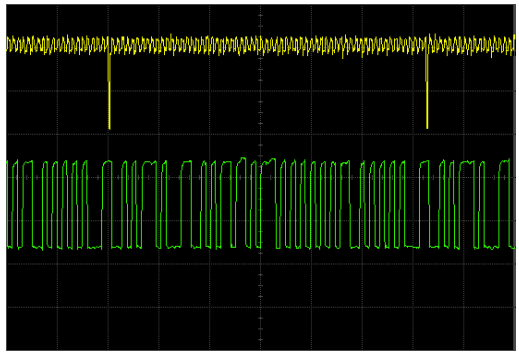
(그림 9) 암호화 동작 신호
(Figure 9) Encryption enable siganl



(그림 10) 반전된 암호화 동작 신호와 데이터 길이 전달 신호
(figure 10) Inverted encrypion enable signal and data length transfer signal

5.3.6 AES 암호화부

AES 암호화부는 OFB 방식으로 구현하여 키 스트림을 발생시키며 프레임 경계 판별 회로부에서 발생되는 프레임 경계 판별 신호에 준해 초기화 레지스터(R)에 초기값을 인가하여 AES 암호화부의 동작을 시작한다. 이는 수신 측에서 복호화 시에 송신 측과 동기를 맞추어 주기 위함이다. 발생된 암호화 키(k_i)가 암호화 동작 신호와 논리적(AND) 연산을 거치면 구간 개폐된 암호화 키($\overline{k_i}$) 가 생성된다. 그림 9에서 보듯이 암호화 동작 신호는 이더넷 프레임의 데이터 구간 동안만 로직 1 이고 나머지 구간은 로직 0 이므로 암호화 키(k_i)와 논리적 연산을 거친 구간 개폐된 암호화 키($\overline{k_i}$) 는 이더넷 프레임의 데이터 영역 구간에서는 $\overline{k_i}$=k_i 이고 나머지 구간에서는 $\overline{k_i}$=(로직 0) 이다. 이 구간 개폐된 암호화 키($\overline{k_i}$)는 이더넷 프레임(m_i)과 비트 단위로 배타적 논리합(XOR) 연산을 하는 회로를 거친다. 구간 개폐된 암호화 키($\overline{k_i}$) 는 이더넷 프레임의 데이터 영역 구간에서는 $\overline{k_i}$=k_i 이므로 이더넷 프레임의 데이터 영역 구간에서는 $C_i = m_i \otimes \overline{k_i}$ 연산에 의해 암호화되고 이더넷 프레임의 나머지 구간에서는 $\overline{k_i}$=(로직 0) 이므로 $C_i = m_i \oplus 0$ 연산을 하면 C_i=m_i 이므로 이는 암호화하지 않은 것과 같다. 이더넷 프레임(m_i)과 구간 개폐된 암호화 키($\overline{k_i}$)는 프레임 경계 판별 신호에 동기가 맞은 상태이므로 이더넷 프레임(m_i)과 구간 개폐된 암호화 키($\overline{k_i}$)를 배타적 논리합(XOR) 연산을 하면 이는 이더넷 프레임 중에서 데이터 영역만 암호화된 프레임이 전송됨을 의미한다.



(그림 11) 프레임 경계 판별 신호와 암화화되어 전송되는 프레임 데이터
(Figure 11) Frame boundary detection signal and transmitted data frame after encryption

그림 11에 오실로스코프로 측정한 프레임 경계판별 신호와 암화화되어 전송되는 프레임 데이터를 보여주고 있다.

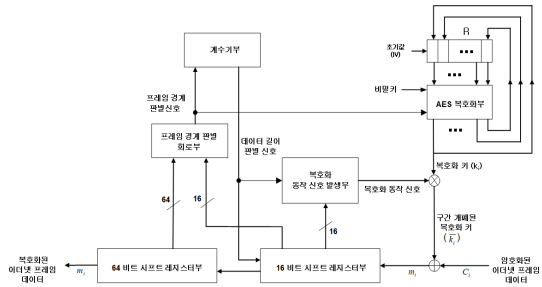
5.4 수신측의 이더넷 데이터의 복호화 과정

수신 측의 복호화 과정도 송신측의 암호화 과정과 유사한 과정을 거친다. 그림 12는 수신측의 복호화 장치의 블록도이다. 전송로를 거쳐 들어오는 암호화된 이더넷 프레임(C_i)이 비트 단위로 직렬로 입력 단에 인가되면 64 비트 시프트 레지스터에서 프레임 데이터의 경계를 판별한다. 프레임의 경계가 판별되면 암호화단과 동일한 원리로 이더넷 프레임의 데이터 영역만 복호화하여 배타적 논리합(XOR) 회로의 출력단에서 복호화된 이더넷 프레임(m_i)이 출력되게 된다.

이더넷 프레임은 비동기 방식으로 전송되므로 프레임의 경계를 구분하여 프레임 내의 데이터 영역만 암호화하여야 한다. 이를 위해 프리앰블과 프레임 시작 구분자의 비트 패턴을 이용한다. 프레임 시작 구분자 영역 다음 12 바이트 후에 데이터의 길이를 나타내는 영역이 나오므로 이 길이 값을 이용하여 암호화할 데이터의 길이를 결정한다. 그림 12는 이더넷 프레임의 복호화를 위한 블록도이다. 직렬로 입력되는 이더넷 프레임이 64비트 시프트레지스터에 입력된 값이 1과 0의 반복인 프리앰블의 패턴과 프레임 시작 구분자의 비트 패턴(10101011)과 일치하면 프레임 경계 판별회로에서는 프레임 경계 판별신호를 발생한다. 프레임 경계판별신호를 이용하여 계수기 초기값으로 발신주소 영역의 바이트 수(6 바이트), 수신주소 영역의 바이트 수(6 바이트) 및 길이 영역의 바이트 수(2 바이트)를 합한 값에 해당하는14를 로드하여 프레임의 각 바이트가 입력될 때 마다 1씩 감소하도록 구성한다. 이 값이 0이 될 때 16비트 시프트 레지스터에 입력된 데이터가 프레임 중 데이터 영역의 바이트 단위의 길이이다.

이때 16 비트 시프트 레지스터의 내용을 복호화 키 개폐 신호 발생기에 전달되도록 한 후, 복호화 키 개폐 신호 발생기에서는 이 값을 초기치로 하여 내부의 계수기를 동작시켜 데이터의 길이 동안만 복호화를 수행하도록 하는 복호화 키 개폐 신호를 만들어 이 신호를 이용하여 데이터 영역에 해당하는 구간만 암호화한다. 복호화 키 개폐 신호는 복호화해야 할 구간에서는 로직 ´1´ 값이고 그 외 구간은 로직 ´0´ 값인 신호이다.

복호화 키 발생회로는 IV를 초기화 값으로 하여 OFB 방식 출력의 일부인 한 바이트를 암호화 키(k_i)로 취하여 이를 복호화 키 개폐 신호와 바이트 단위로 논리적(AND)한 값 $\overline{k_i}$는 복호화 키 개폐 신호가 로직 ´1´ 인 구간에서는 복호화 키(k_i)와 동일하고 나머지 구간에서는 로직 ´0´ 이다. C_i 와 $\overline{k_i}$의 배타적 논리합(XOR) m_i는 복호화 구간에서는 $m_i = C_i \oplus \overline{k_i} = C_i \oplus k_i$가 되어 프레임의 데이터 영역이 복호화되고 프레임의 나머지 영역에서는 $\overline{k_i} = 0$이므로 $m_i = C_i$가 된다.



(그림 12) OFB 방식을 이용한 이더넷 프레임의 복호화
(Figure 12) Decryption of Ethernet frames using OFB

5.5 실험 결과

OFB를 적용한 블록 암호화 알고리즘인 AES의 동작 검증용 평문 벡터와 키 값을 입력하여 송신단에서 이더넷프레임으로 구성하여 전송한 데이터가 암호화를 거쳐 복호화가 되는 것을 검증하기 위해 AES의 초기화(IV)값과 비밀키 값을 지정하여 검증용 입력 평문을 전송하여 알고리즘에서 예상되는 값으로 암호화되는 것을 확인하였다.

먼저 전송한 프레임의 데이터 영역만 암호화되고 그외 영역은 암호화되지 않는 것을 검증하고 지정된 수신주소로 데이터 프레임이 수신되어 데이터 영역을 복호화하여 송신한 평문 벡터가 복원되는 것을 검증하였다. 본 논문에서는 AES의 암호화 블록 길이가 128 비트, 키의 길이가 128 비트로 하고 이더넷 프레임의 데이터 길이는 46~1500 바이트까지 가능하나 검증의 용이성을 위해 128 비트(16 바이트)의 배수인 48 바이트로 구성하여 같은 입력 값이 16 바이트 단위로 반복되는 값으로 구성하여 검증하였다.

- IV 벡터:000102030405060708090a0b0c0d0e0f0
- 비밀키: 00010203040506070809 0a0b0c0d0e0f
- 평문 입력 벡터:00112233445566778899aabbccddeeff

본 실험에서는 데이터 영역이 네 개의 128 비트 검증용 벡터인 48 바이트로 데이터 프레임을 구성하여 송신하여 출력 벡터가 나오는 가를 확인하고, 지정된 수신단에서 수신된 데이터 프레임의 복호화 여부를 검증하였다.

- 송신측 데이터
  00112233445566778899aabbccddeeff
  00112233445566778899aabbccddeeff
  00112233445566778899aabbccddeeff
  00112233445566778899aabbccddeeff

- 송신측 암호화를 거친 전송 데이터
  5e0d96780797c4e7f39e025b3d7c9b37
  5e0d96780797c4e7f39e025b3d7c9b37
  5e0d96780797c4e7f39e025b3d7c9b37
  5e0d96780797c4e7f39e025b3d7c9b37

- 수신단 측의 복호화된 데이터
  00112233445566778899aabbccddeeff
  00112233445566778899aabbccddeeff
  00112233445566778899aabbccddeeff
  00112233445566778899aabbccddeeff

위의 데이터는 송신측 데이터가 암호화를 거쳐 수신단 측에서 복호화되어 원래의 데이터가 복원됨을 보여주고 있다.

6. 결론 및 향후 과제

본 논문에서는 이더넷 프레임을 암호화하기 위해 스트림 암호를 적용한 물리 계층에서의 암호화 기법을 기술하였다. 암호화 기법 중 암호화 강도가 강한 AES 기법을 적용하며 원래 AES는 블록 단위의 암호화를 수행하는 알고리즘이나 AES에 OFB방식을 적용하여 직렬 스트림으로 입력되는 이더넷 프레임을 암호화/복호화가 가능함을 검증하였다. 본 방식에서는 시스템 운용 중에 암호화/복호화를 필요로 하는 단말에만 별도의 모듈 형태로 부가하여 운용할 수 있는 장점을 지닐 뿐만 아니라 OFB 방식을 적용한 AES알고리즘을 적용하여 구현함으로써 암호화 강도 측면에서도 강점을 지닌다. 암호화 시에 이더넷 프레임의 프리앰블, 수신 주소, 발신 주소, 데이터 크기 및 순환여유검사 영역은 그대로 두고 데이터 영역만 암호화 하기 위해 이더넷 프레임의 경계를 판별하여 이 경계를 기준으로 데이터 영역의 위치를 파악하여 데이터 영역의 길이에 해당하는 암호 키 개폐신호를 발생시켜 주어 이 영역만 암호화가 가능함을 보여준다. 본 논문에서는 IEEE 802.3 프레임의 데이터 영역만 암호화하여 전송한 후 수신단에서 데이터 영역의 복호화 과정을 거친 후 암호화/복호화가 가능함을 기술하였다. 본 논문의 기법은 내부의 근거리 망이 내부인이나 외부인을 대상으로 보안을 필요로 하는 곳에서 적용이 가능할 것이다. 향후 과제로는 ATM 셀 데이터의 스트림 암호화 구현에 관한 것이다.

참고문헌(Reference)

[1] Lee Kun-bae, Lee Byung-wook, “Hardware implementation of 128-bit encryption algorithm using FPGA,” Journal of the Information Processing Society, Vol. C, 8-C (No. 3), pp.277-286 Jun. 2001. https://www.koreascience.or.kr/article/JAKO200111920780446.page

[2] Im Sung-Yeal, Chung Ki-Dong, “ATM Cell Encryption Method using Rijndael Algorithm in Physical Layer,” JIPS, VOL. 13-C, pp 84, Feb., 2006. https://doi.org/10.3745/KIPSTC.2006.13C.1.083

[3] Forouzan, B., Data Communications and Networking,Mc Graw Hill, pp. 397-398, 2007.

[4] William Stallings, “Cryptography and Network Security”, Pearson Education Inc., pp.63, 2013.

[5] Denning, D. E., “Cryptography and Data Security”, Addison-Wesley Publishing Co., pp. 135-138, 1983.

[6] Branstad, D. K., “Security of Computer Communication,” IEEE, Comm. Soc. Mag. Vol. 16, No 6, pp. 33-40, Nov. 1978.

[7] Denning, D. E., “Cryptography and Data Security”, Addison-Wesley Publishing Co., pp. 138-139, 1983.

[8] S. W., “Shift Register sequences,” Holden-Day, San Fransico, Calif., 1967.

[9] William Stallings, “Cryptography and Network Security”, Pearson Education Inc., pp.185-192, 2013.

[10] Forouzan, B., Data Communications and Networking,Mc Graw Hill, pp. 1006-1008, 2007.

[11] NIST, “Announcing the Advanced Encryption Standard(AES),” FIPS PUB-197, Nov., 2001.

[12] Daemon, J., and Rijmen, V., “Rijndael: The Advanced Encryption Standard,” Dr Dobb’s Journal, Mar., 2001.

[13] E. Biham, “New types of cryptanalytic attacks using related keys,” Advances in Cryptology, Proceedings Eurocrypt’93, NCS 765, T. Helleseth, Ed., Springer-Verlag, pp. 398-409, 1994.
https://link.springer.com/content/pdf/10.1007%2F3-540-48285-7_34.pdf

[14] Daemen, J., and Rijmen, V. “The Design of Rijndael: The Wide Trail Strategy Explained,“ NewYork, Springer-Verlag, 2002.

[15] Davies, D. W., Price W.L. “Security for Computer Network”, John Wiley & Sons, pp. 93-94, 1989.

[16] William Stallings, “Cryptography and Network Security,” Pearson Education Inc., pp.187-189, 2013.

[17] Forouzan, B., “Security for Computer Networking,” John Willy & sons, pp. 93-95, 1989.

[18] Bright, H. S.and Enison, R. L., “Cryptography Using Modular Software Elements,” Proc. NCC, Vol. 45, AFIPS Press, Montvale, N. J., pp. 113-123, 1976.
https://doi.org/10.1145/1499799.1499816

[19] ISO 9160, “Information processing – Data encipherment – Physical layer interoperability requirement,” International Standards Organization, 1988.
https://www.iso.org/obp/ui/fr/#iso:std:iso:9160:ed-1:v1:en

[20] IEEE Std. 802.3, “Part3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical layer Specification,” 2008.

[21] Forouzan, B., “Data Communications and Networking,” Mc Graw Hill, pp. 397-398, 2007.

◐ 저 자 소 개 ◑

임 성 렬(Sung-yeal Im)
1983년 서울대학교 전자공학과(공학사)
1992년 포항공과대학교 대학원 전기전자공학과(공학석사)
2005년 부산대학교 대학원 이학박사
2012년~현재 부산대학교 교양교육원 비전임교수
관심분야 : 암호용 ASIC 설계, 네트워크 보안, 암호 알고리즘
E-mail : syim7@pusan.ac.kr