

낮은 복잡도의 보안 네트워크 부호화

김 영 식*

New Secure Network Coding Scheme with Low Complexity

Young-Sik Kim*

요 약

네트워크 부호화는 중간 노드에서 데이터의 변환을 허용함으로써 전송률 높일 수 있는 방식이지만, 중간 노드에 대한 도청이나 데이터 변조에 취약해지는 문제가 발생한다. 이를 위해 정보이론적 관점에서 또는 암호학적 관점에서 도청 또는 데이터 변조에 저항할 수 있는 다양한 부호화 방식들이 제안되었다. 최근에 암호학적 관점에서 랜덤 네트워크 부호화에도 안전한 네트워크 부호화 방식이 제안되었지만, 안전한 해쉬 함수와 같은 암호학적 도구들의 사용은 센서 노드와 같은 낮은 연산능력을 보유한 장비에서는 적용이 어려운 문제를 지닌다. 이 논문에서는 선형 변환 및 간단한 테이블 룩업을 기반으로 랜덤 네트워크 부호화 사용할 때 n 개의 패킷 중에서 공격자가 최대 $n-1$ 개의 패킷을 도청하는 경우에도 $n-1$ 개까지의 사용자 메시지를 동시에 안전하게 전송할 수 있는 안전한 네트워크 부호화 방식을 제안한다. 제안하는 방식은 암호학적으로 전부-또는-전무 변환(all-or-nothing transform) 형태를 가지면서도 정보이론적으로 완료된 조건에서 안전한 네트워크 부호화 방식임을 증명할 것이다.

Key Words : Random Network Coding, Secure Network Coding, Weakly Secure Network Coding, All-or-Nothing Transform (AONT), Cryptography, Hash Function

ABSTRACT

In the network coding, throughput can be increased by allowing the transformation of the received data at the intermediate nodes. However, the adversary can obtain more information at the intermediate nodes and make troubles for decoding of transmitted data at the sink nodes by modifying transmitted data at the compromised nodes. In order to resist the adversary activities, various information theoretic or cryptographic secure network coding schemes are proposed. Recently, a secure network coding based on the cryptographic hash function can be used at the random network coding. However, because of the computational resource requirement for cryptographic hash functions, networks with limited computational resources such as sensor nodes have difficulties to use the cryptographic solution. In this paper, we propose a new secure network coding scheme which uses linear transformations and table lookup and safely transmits $n-1$ packets at the random network coding under the assumption that the adversary can eavesdrop at most $n-1$ nodes. It is shown that the proposed scheme is an all-or-nothing transform (AONT) and weakly secure network coding in the information theory.

I. 서 론

네트워크 부호화는 기존의 라우팅 기법에서 데이터를 저장한 후에 재전송하는 방식을 일반화시킨 방식

으로 중간 노드에서 입력받은 데이터를 결합시켜 새로운 데이터를 생성할 수 있도록 하고 있다. 그 결과 네트워크의 처리량은 높아졌지만 보안 측면에서는 여러 가지 문제점이 지적되고 있다^[1-5,12].

※ 본 연구는 한국연구재단 중견연구지원사업(과제번호 2011-0016664)의 지원을 받아 수행되었습니다.
* 주저자 : 조선대학교 정보통신공학과 정보이론 및 정보보안 연구실, iamyskim@chosun.ac.kr, 정희원
논문번호 : KICS2013-02-079, 접수일자 : 2013년 2월 1일, 최종논문접수일자 : 2013년 3월 27일

안전한 네트워크 부호화 문제는 Cai 등이 처음에 소개하였다^[4]. 이 논문에서는 소스 노드가 n 개의 패킷을 여러 싱크 노드로 전송하는 네트워크 부호화가 구현된 네트워크를 가정했다. 이 때 오류는 발생하지 않는 것으로 가정하며, 그 대신 공격자가 네트워크상의 $\mu (< n)$ 개의 링크를 관찰하고 있다고 가정한다. 이 때 안전한 네트워크 부호화에서 해결하고자 하는 문제는 보호하고자 하는 메시지를 n 개의 전송되는 패킷 속으로 공격자에게 드러나지 않도록 안전하게 숨기는 것이다. 이 때 도청하고 있는 공격자가 전송되는 비밀 정보에 대해서 정보이론적인 관점에서 어떠한 정보도 얻을 수 없도록 해야 한다. 이러한 안전한 네트워크 부호화 문제는 wiretap 채널 II의 일반화된 것으로 알려져 있다^[4]. 따라서 안전한 네트워크 부호화에서 비밀은 n 개의 전송되는 패킷에 랜덤성을 추가함으로써 달성될 수가 있다.

안전한 네트워크 부호화를 위해서 특별한 형태의 오류정정부호를 사용할 수 있음이 잘 알려져 있다^{[1],[10]}. 네트워크에 대한 공격은 전달되는 정보의 내용을 파악하는 도청과 같은 수동적 공격과 정보 전달을 방해하기 위한 재밍이나 오류 주입과 같은 능동적 공격으로 나눌 수 있다. 이 중에서 능동적 공격 모델인 비잔틴 공격 하에서의 안전한 네트워크 부호화를 위해 Jaggi 등은 새로운 랜덤 네트워크 부호 설계 알고리즘을 제시하였고^[11], Koetter와 Kschischang은 오류정정부호의 하나인 rank metric 부호를 이용해서 비잔틴 공격에 대응할 수 있음을 보였다^[10].

도청 공격에 대응하기 위해서도 오류정정부호를 이용하거나 네트워크 부호 설계 단계에서 보안을 고려하여 설계할 수 있다. 그러나 강한 조건의 안전한 네트워크 부호화의 경우에는 l 개의 비밀 메시지를 n 개의 패킷에 실어 안전하게 보낸다고 할 때, 그리고 공격자가 $\mu = n - l$ 개 이하의 패킷만을 관찰할 수 있다고 할 때, 달성 가능한 것이 정보이론적으로 증명되었다. 즉, 아무리 노력하더라도 l 개의 비밀 정보를 전달하기 위해 네트워크 처리량은 $l = n - \mu$ 로 줄어들게 된다.

따라서 Bhattad 등은 문제의 조건을 완화시켜서 완화된 조건의 안전한 네트워크 부호화 (weakly secure network coding) 방식을 제안하였다^[5]. 이 조건 하에서는 송신하는 비밀 정보의 임의의 원소들과 네트워크를 통해서 전송되는 임의로 선택한 최대 $\mu = n - 1$ 개의 링크 정보 사이에서의 상호 정보 (mutual information)가 0이 되도록 만들어야한다. 즉, 공격자는 네트워크에서 정보를 관찰하기는 하지만 네

트워크에 대한 어떠한 의미 있는 정보도 얻을 수 없도록 만들어야 한다.

네트워크 구조를 미리 알고 있는 경우에는 관찰자가 최대 $n - 1$ 개의 노드만을 관찰할 수 있다고 하면, 최대 $l = n$ 개의 데이터를 전송하는 것도 가능해진다. 그러나 이런 방식의 문제는 네트워크 구조가 사전에 알려져 있어야 하고, 그에 상응하는 정확한 네트워크 부호를 사용해야한다는데 있다. 만일 네트워크 부호가 랜덤 네트워크 부호에서처럼 분산된 환경에서 생성이 되는 경우에는 Bhattad 등이 제안한 네트워크 부호로는 이러한 조건을 만족시킬 수가 없다.

따라서 정보이론적인 보안이 아니라 암호학적인 보안을 제공하고자 하는 노력이 별도로 이루어졌다. 그 시작의 하나로 Zhang 등은 one-time pad를 사용해서 안전한 네트워크 부호화를 구성하였다. 그러나 암호화 키를 전송하기 위해서 전체 메시지 패킷 중 절반에 해당되는 패킷을 사용해야한다는 문제가 있다^[6]. 이런 문제를 해결하기 위해 Adeli 와 Liu는 해쉬 함수를 이용한 방식으로 변경하여, 전송해야할 비밀 패킷의 수를 한 개로 줄였다^[7]. 그러나 이 방법에서는 네트워크 부호의 특정한 전역 부호화 벡터를 사용하는 경우에 보안 취약점이 발생할 수 있다. Kim 은 이를 보완하여 모든 전역 부호화 벡터에 대해 보안 취약점이 발생하지 않는 방식을 제안하였다^[8].

Kim의 방식에서는 네트워크 구조를 사전에 알지 못한 상태로 랜덤하게 네트워크 부호를 생성하는 경우에도 취약점이 생기지 않도록 할 수 있지만, 암호학적 해쉬 함수를 송신측과 수신측이 사용해야한다는 계산적인 부담은 여전히 존재한다.

이 논문에서는 도청 공격에 대한 대응 방법으로서 해쉬함수를 사용하지 않는 낮은 복잡도의 안전한 네트워크 부호화 방식을 제안한다. 이 방식에서는 관찰자가 최대 $n - 1$ 개의 링크를 관찰할 수 있다고 할 때 n 개의 패킷에 $n - 1$ 개의 비밀 정보를 전달하는 것이 가능하다. 본 논문에서 제안하는 방식은 별도의 변환이나 장치의 변경 없이 Koetter와 Kschischang의 rank-metric 부호와 직접 연결해서 사용이 가능하다^[10].

II. 사전 지식

이 논문에서 사용하는 네트워크 모델은 다중 전송(multicast) 네트워크 모델로서 다음과 같은 구성요소를 갖는다. 우선 네트워크는 다음과 같은 지향성 비순회 그래프 $G = (V_G, E_G)$ 로 구성된다. 여기

에서 V_G 는 그래프 상의 vertices의 집합이고 E_G 는 그래프의 각 edge의 집합이다. 또한 전체 송신 메시지의 길이는 n 이고 각각의 메시지 심볼은 원소가 $q=2^d$ 개인 유한체 $GF(q)$ 상의 원소라 가정한다. 그리고 소스 노드와 싱크 노드의 집합을 각각 S_G 와 T_G 로 나타낸다. 마지막으로 그래프 G 의 edge는 단위 시간 당 $GF(q)$ 의 원소 중 하나를 전송할 수 있다고 가정한다.

소스 노드 집합 S_G 에서 다음과 같이 길이가 n 인 정보 벡터를 생성한다고 하자.

$$m = (m_1, m_2, \dots, m_n)^T$$

여기에서 $m_i \in GF(q)$ 이고 $|S_G| \leq n$ 이다. 선형 네트워크 부호에서 길이가 n 인 부호화 벡터가 각 edge에 할당된다. 그래프 G 에서의 edge의 수가 l 이라고 하자. 그러면 전역 부호화 벡터 v_i 가 각 edge에 할당이 된다.

$$v_i = \{v_{i1}, v_{i2}, \dots, v_{in}\}$$

여기에서 전역 부호화 벡터 역시 $GF(q)$ 상에 존재한다고 가정한다. 이 때 공격자는 유한한 계산 능력을 가졌으며 한 번에 최대 $n-1$ 개의 노드만을 동시에 얻을 수 있다고 가정한다.

이 때 Kim은 다음과 같은 방식을 제안하였다. 임의의 입력 길이 v 비트를 갖는 데이터에 대해 u 비트의 출력을 생성하는 암호학적으로 안전한 해쉬 함수를 $H(\cdot) : \{0,1\}^v \rightarrow \{0,1\}^u$ 로 나타내자. 그리고 I_i 를 인덱스 값이고 a 는 $GF(q)$ 상에서 랜덤하게 생성한 임의의 원소라고 하자. 그러면 Kim의 방식에서는 소스 노드에서 다음과 같이 메시지를 처리한다.

$$\hat{m} = (m_1 \oplus H(a \| I_0), m_2 \oplus H(a \| m_1 \| I_1), \dots, m_{n-1} \oplus H(a \| m_{n-2} \| I_{n-2}), a \oplus H(m'))^T$$

여기에서 m' 은 다음과 같이 주어진다.

$$m' = (m_1 \oplus H(a \| I_0)) \| (m_2 \oplus H(a \| m_1 \| I_1)) \| \dots \| (m_{n-1} \oplus H(a \| m_{n-2} \| I_{n-2}))$$

III. 새로운 안전한 네트워크 부호 설계

본 논문에서는 Kim의 방식과는 달리 해쉬 함수나 암호화 알고리즘을 사용하지 않고 일반적인 선형 변환을 이용해서 하나의 전부-또는-전무(all or nothing) 변환을 새롭게 정의할 것이다.

먼저 이 논문에서도 기존의 논문과 마찬가지로 $GF(q)$ 상의 랜덤하게 생성한 임의의 심볼 a 를 전송하는 것으로 가정한다. 이 때 $q=2^d$ 에서 $d \geq 128$ 이고, $d=8k$ ($k \geq 16$ 인 짝수)이다. 안전한 네트워크 부호 구성을 위해 사전 변환이 필요한데, 사전에서 사용하는 연산을 설명하면 다음과 같다.

$l_i(x)$ 를 d 비트의 x 를 i 비트만큼 왼쪽으로 순회 시프트(cyclic shift)하는 연산자로, $x = x_0x_1 \dots x_{d-1}$ ($x_i \in \{0,1\}$)일 때 $l_i(x) = x_i x_{i+1} \dots x_{d-1} x_0 \dots x_{i-1}$ 가 된다.

또한 $v(b)$ 를 4비트 단위의 $x^4 + x + 1 = 0$ 을 생성 다항식으로 갖는 $GF(2^4)$ 상에서의 곱의 역원을 수행하는 함수라고 하자. 즉, $v(\cdot)$ 는 b 를 4비트 단위로 $b_0b_1 \dots b_{2k-1}$ 의 블록으로 나눈 후에 각각의 b_i ($0 \leq i \leq 2k-1$)에 대해서 $b_i b_i^{-1} = 1$ 가 되도록 b_i^{-1} 를 $GF(2^4)$ 에서 계산해 $b^{-1} = b_0^{-1} b_1^{-1} \dots b_{2k-1}^{-1}$ 를 만들어 내는 함수이다. $GF(2^4)$ 상에서의 곱의 역원 관계는 표 1에 나타내었다. 표 1에서 우측의 4비트 데이터는 $GF(2^4)$ 의 곱의 역원에 의해 좌측의 4비트 데이터로 변환이 된다.

표 1. $GF(2^4)$ 상에서의 곱의 역원 관계
Table 1. Multiplication Inverses over $GF(2^4)$

| | |
|---------------|---------------|
| (0000)↔(0000) | (1000)↔(1111) |
| (0001)↔(0001) | (1001)↔(0010) |
| (0010)↔(1001) | (1010)↔(1100) |
| (0011)↔(1110) | (1011)↔(0101) |
| (0100)↔(1101) | (1100)↔(1010) |
| (0101)↔(1011) | (1101)↔(0100) |
| (0110)↔(0111) | (1110)↔(0011) |
| (0111)↔(0110) | (1111)↔(1000) |

그러면 사전변환은 다음 과정과 같이 수행된다.

<사전 변환>

- 1) 랜덤 데이터 a 는 다음과 같이 k 개의 8비트 블록들로 나타낼 수 있다. $a = (a_0 a_1 \dots a_{k-1})$. 그

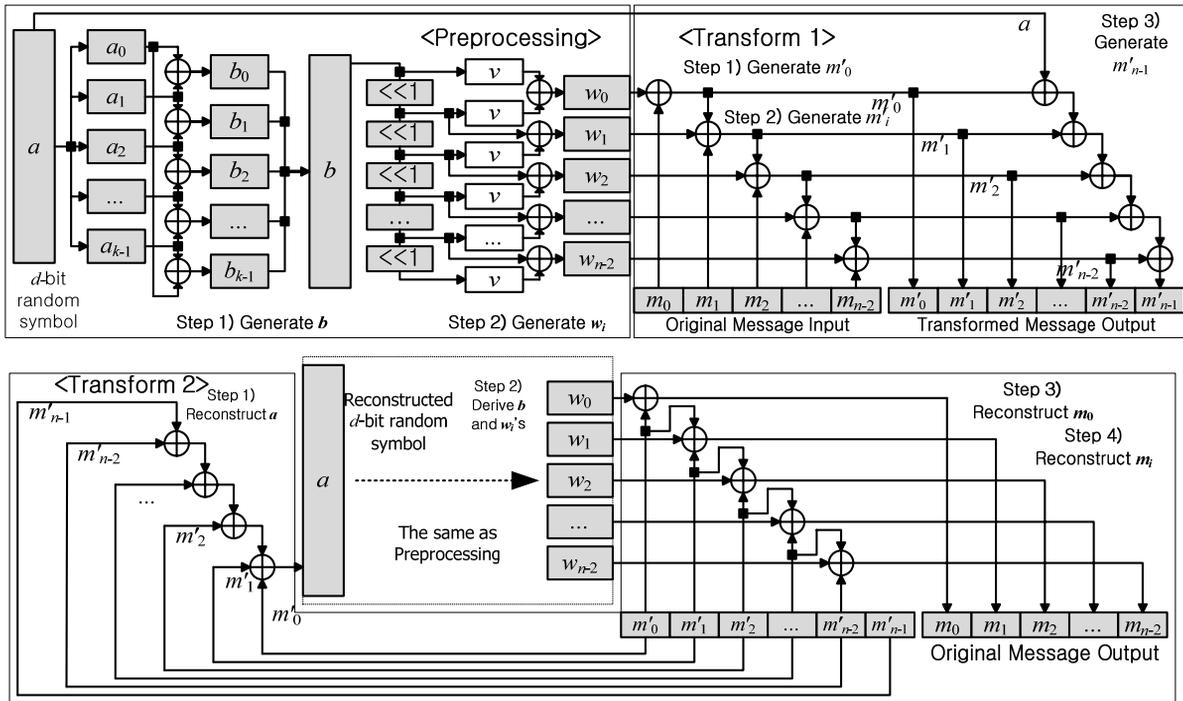


그림 1. 사전 변환 및 변환 1과 변환 2의 동작 블록도
 Fig. 1. Block diagrams for Preprocessing, Transform 1, and Transform 2.

러면 8비트 블록을 이용해서 다음과 같이 새로운 데이터 $b = (b_0 \dots b_{k-1})$ 를 생성한다. 여기에서 $b_i = a_i \oplus a_{(i+1) \bmod k}$ 이고 \oplus 는 비트 단위의 XOR을 의미한다.

- 2) b 로부터 새로운 $n-1$ 개의 랜덤 심볼 $w_i = l_i(b) \oplus v(l_{i+1}(b))$ ($1 \leq i \leq n-2$)를 얻는다. 단 예외적으로 $w_0 = v(l_1(b)) + v(b)$ 이다.

이제 하나의 랜덤 심볼 a 와 $n-1$ 개의 w_i 를 사용해서 총 $n-1$ 개의 심볼로 구성된 메시지 $m = m_0 m_1 \dots m_{n-2}$ 를 전부-또는-전무 변환해서 총 n 개의 $m' = m'_0 m'_1 \dots m'_{n-1}$ 를 얻는 과정과 같이 나타낼 수 있다.

<변환 1>

- 1) 먼저 초기값 $m'_0 = m_0 \oplus w_0$ 를 계산한다.
- 2) 연속적으로 그 이후의 값 $m'_i = m_i \oplus w_i \oplus m'_{i-1}$ ($1 \leq i \leq n-2$)를 계산한다.
- 3) 마지막으로 $m'_{n-1} = a \oplus m'_0 \oplus \dots \oplus m'_{n-2}$ 를 계산한다.

이에 대한 역변환은 다음과 같이 이루어진다. 일

단 모든 변환된 심볼 m' 을 전부 가지고 있다고 하자.

<변환 2 (변환 1의 역변환)>

- 1) $a = m'_{n-1} \oplus m'_0 \oplus \dots \oplus m'_{n-2}$ 를 계산해서 랜덤 심볼 a 를 복구한다.
- 2) a 로부터 b 를 구하고 다시 $n-1$ 개의 w_i 를 유도한다.
- 3) 먼저 첫 번째 심볼 $m_0 = m'_0 \oplus w_0$ 를 통해서 복구한다.
- 4) 연속적으로 심볼 $m_i = m'_i \oplus w_i \oplus m'_{i-1}$ 을 복구한다.

그러면 $n-1$ 개의 모든 심볼 $m = m_0 \dots m_{n-2}$ 를 다시 복구할 수가 있다. 그림 1은 사전 변환 및 변환 1과 변환 2의 동작을 블록별로 나타내었다. 이제는 이러한 변환이 정말로 전부-또는-전무 변환임을 증명하자. 그 전에 전부-또는-전무에 대한 정확한 정의를 내리도록 하자.

정의 1. [9] 메시지 $m = (m_0, m_1, \dots, m_{n-2}, a)$ 에서 변환된 메시지 $m' = (m'_0, m'_1, \dots, m'_{n-1})$ 로의 변환 f 가 다음과 같은 조건을 만족시키면 f 를 전부-또는-전무 변환이라 부른다.

- 1) 변환 f 는 가역적이다. 즉, 변환된 메시지 m' 이 모두 주어지면, 본래의 메시지를 얻을 수 있다.
- 2) 변환 f 와 그 역변환은 효율적으로 계산이 가능하다.
- 3) 변환된 메시지 m' 의 블록 중에서 하나라도 없다면 본래의 메시지 m 을 계산하는 것이 계산적으로 불가능하다.

이제 다음과 같은 정리를 얻을 수 있다.

정리 2. 변환 1과 변환 2는 전부-또는-전무 변환이다.

증명) 우선 변환 2로부터 변환 1을 적용하기 전 본래의 모든 데이터 m 과 a 를 얻을 수 있음은 자명하므로 정의 1의 1)번은 쉽게 증명된다. 그리고 2)번은 변환 1과 변환 2 모두 비트 단위의 XOR 내지는 i 비트의 순회 시프트 변환만을 이용하므로 역시 효율적인 계산이 가능하다. 문제는 3)번의 성질을 증명하는 것이다.

우선 최악의 경우로 다음과 같은 두 가지 경우를 생각할 수 있다.

경우 1) m'_{n-1} 를 제외하고 총 $n-1$ 개의 심볼을 갖는 경우

이 경우에는 m'_{n-1} 을 알지 못하기 때문에 본래의 심볼 a 를 직접적인 방법으로는 알 수 없다. 따라서 $m'_0 \cdots m'_{n-2}$ 의 블록을 통해서 찾아야 한다. 이 경우 메시지를 임의로 조절할 수 있다고 가정하고 메시지 값을 모두 0으로 세팅하였다고 해 보자. 이 경우 $m'_0 = 0 \oplus w_0$ 으로 w_0 은 쉽게 얻을 수 있지만, $w_0 = v(l_1(b)) + v(b)$ 로 b 가 통계적으로 랜덤하다면 b 를 정확히 알아낼 수가 없다. 마찬가지로 $m'_i = m_i \oplus w_i \oplus m'_{i-1}$ 로부터 $w_i \oplus w_{i-1} \oplus \cdots \oplus w_0$ 을 얻을 수 있지만, 이 경우 i 값에 따라서 다음과 같이 정해진다.

$$w_i \oplus \cdots \oplus w_0 = \left(\bigoplus_{t=1}^i l_t(b) \right) \oplus \left(\bigoplus_{t=1}^{i+1} v(l_t(b)) \right)$$

즉, b 를 1부터 i 만큼 순회 시프트 시킨 값들의 XOR에 언제나 $v(\cdot)$ 가 적용된 값들의 XOR 합이 더해지는 형태를 갖는다. 따라서 선형 변환 $l_i(\cdot)$ 값이 다른 값과 XOR되지 않고 단독으로 노출되는 일이 존재하지 않게 된다. 따라서 이 경우도 본래의 b 값을 알아내기가 어렵다.

경우 2) m'_{n-1} 를 포함해 총 $n-1$ 개의 심볼을 갖고 있는 경우

이 경우에는 일단 m'_{n-1} 을 알고는 있지만 m'_i ($0 \leq i \leq n-2$) 중에서 하나의 심볼 값을 알지 못하게 된다. 미지의 값을 m'_j 라 하자. 그러면 변환 2의 1)단계에서 $a \oplus m'_j$ 를 얻게 된다. 여기에서도 모든 메시지가 0인 경우 $a \oplus \left(\bigoplus_{t=0}^j w_t \right)$ 가 되어 언제나 랜덤 값의 변환 값인 w_i 의 XOR 합이 더해져 있으므로 정확한 a 를 알아낼 수가 없다. 따라서 b 값이나 거기에서 파생되는 w_i 들을 알아낼 수 없다.

따라서 변환 1과 변환 2는 하나의 전부-또는-전무 변환을 이룬다.

전부-또는-전무 변환의 성질을 통해서 이러한 변환의 역할을 확인할 수 있다. 전부-또는-전무 변환을 사용하면 네트워크상으로 변환된 모든 데이터를 온전하게 수신할 수 있는 정상적인 수신자만 데이터를 복구하는 것이 가능하다. 그러나 공격자는 적어도 하나 이상의 변환된 패킷을 정상적으로 수신하지 못하기 때문에, 전체 데이터를 복구하는 것이 불가능하다.

IV. 특성 분석

이 장에서는 새로 제안한 방식의 다양한 보안 특성 및 계산적 복잡도를 분석할 것이다.

4.1. 보안 분석

먼저 새로운 제안에서 네트워크 부호의 기본 유한체의 크기는 $q = 2^d$ 로 $d = 8k \geq 128$ 인 값으로 가정하였다. 이것은 한 번에 128비트 이상의 데이터를 묶어서 처리하는 것을 의미한다. 만일 a 를 쉽게 추측할 수 있다면 본 논문에서 제안한 전부-또는-전무 변환을 하더라도 본래의 메시지를 쉽게 추측할 수가 있다. 그러나 이 논문에서 사용하는 유한체는 2^{128} 이상의 원소를 갖기 때문에 추측을 통해서 알아낼 수 있는 확률은 평균적으로 $1/2^{127}$ 이하로 매우 안전한 수준임을 알 수 있다.

또 다른 가능한 공격으로 중간 노드에서 일부 알아낸 변환된 메시지의 네트워크 부호 값을 다양하게 선형 결합을 시킴으로써 본래의 메시지가 드러날 가능성을 생각해 볼 수 있다. 그러나 메시지 비트는 언제나 파생된 랜덤 심볼 w_i 들의 XOR 합에 의해서 더해져 있다. 이것을 일반적으로 모든 메시

지 심볼에 대해서 랜덤한 심볼 r_i 들이 다음과 같이 더해져 있는 것으로 볼 수 있다.

$$m' = (m_0 \oplus r_0, \dots, m_{n-2} \oplus r_{n-2}, a \oplus r_{n-1})$$

여기서 r_0 는 a 로부터 파생된 w_0 이고, r_i 는 이전의 m'_{i-1} 와 w_i 의 XOR 합으로 구성된다. 랜덤성에 의해서 w_i 들의 XOR 합이 우연히 모든 비트가 0이 될 가능성이 존재하므로 정확한 분석이 필요하다.

만일 a 가 좋은 난수 발생장치로부터 추출한 모든 비트가 0이 아닌 랜덤 값이라고 하면 b 는 자명하게 0이 아닌 랜덤 값이 된다. 왜냐하면 0이 아닌 a 에서 모든 비트가 0인 b 가 나온다는 의미는 a 를 8비트로 나눈 a_i 들이 모두 같은 값을 갖는다는 의미이고 이것은 a 가 좋은 난수 발생장치에서 추출한 랜덤 값이라는 가정에 모순이 되기 때문이다.

더 나아가서 0이 아닌 b 로부터는 언제나 0이 아닌 $l_i(b)$ 값과 $v(l_i(b))$ 값을 자명하게 얻는다. 이제 두 0이 아닌 값이 더해져서 우연히 0이 나올 확률은 0과 1이 같은 확률을 가질 때 $1/2^{128}$ 이 되어 매우 작다. 따라서 높은 확률로 모든 메시지들에 0이 아닌 랜덤 파생값 w_i 의 XOR이 더해져 있으므로 선형 결합을 통해서도 우연히 메시지들이 드러날 확률도 매우 작다.

마지막으로 제안된 보안 기술은 완화된 조건 하에서 안전한 네트워크 부호라는 사실을 증명할 수 있다. 이를 위해서 다음과 같은 보조정리가 필요하다.

보조정리 3. [8] r 이 $GF(q)$ 상에서의 임의의 원소라고 하자. 그리고 m 이 r 과는 통계적으로 독립인 $GF(q)$ 상에서 균일하게 분포를 통해 추출된 값이라 하자. 그러면 $r+m$ 의 분포는 r 과는 독립이다.

정리 4. 변환 1과 변환 2는 완화된 조건의 안전한 네트워크 부호를 구성한다.

증명) 안전한 네트워크 부호에 의해서 네트워크로 전송되는 메시지 심볼은 $m_i \oplus r_i$ 가 되고, 네트워크 부호를 통해서 이 메시지들의 선형결합들이 임

의로 $\sum_{i=0}^t \alpha_i (m_i + r_i) = \sum_{i=0}^t \alpha_i m_i + \sum_{i=0}^t \alpha_i r_i$ 와 같이 생성된다. 여기에서 α_i 는 네트워크 부호에 의해 생성

되는 $GF(2^d)$ 상의 임의의 계수이고 덧셈은 $GF(2^d)$ 상의 덧셈 (즉, 비트 단위의 XOR)로 가정한다. 만일 메시지 심볼이 $GF(2^d)$ 이다. 이 때 만일 메시지 심볼이 $GF(2^d)$ 상에서 균일한 분포를 갖는다면, 보조정리 3으로부터 랜덤 네트워크 부호에서 생성되는 메시지 심볼의 선형 결합 값은 랜덤 값 r_i 들의 선형결합과 통계적으로 독립이 된다. 이러한 통계적 독립성으로 인해, 공격자가 획득한 변환된 메시지들의 선형 결합의 집합 W 와 각 변환된 메시지들 사이의 상호 정보는 $I(m'; W) = 0$ 이 된다.

4.2. 복잡도 분석

이제 이 논문에서 제안한 방식의 계산적인 복잡도를 분석해 보자. 이 논문에서 일어나는 연산중에서 d 비트의 XOR 연산의 계산량을 X_d 라 하고 i 비트 왼쪽 순회 시프트 연산의 계산량을 L 이라 하고, 4비트 블록 단위로 이루어지는 $GF(2^4)$ 상에서의 곱의 역원 연산의 총 계산량을 V 로 나타내자. 전송되는 패킷 수를 n 개라고 하면, 표 2와 같이 계산적 복잡도를 나타낼 수 있다.

표 2. 제안한 방식의 계산적 복잡도
Table 2. Computational Complexity of the Proposed Scheme.

| Stage | Computational Complexity |
|---------------|---------------------------|
| Preprocessing | $nX_d + nV + 2(n-2)L$ |
| Transform 1 | $(2n-3)X_d$ |
| Transform 2 | $(n-3)X_d + nV + 2(n-2)L$ |

실제 구현에 있어서의 복잡도는 i 비트 순회 시프트와 d 비트의 XOR 합은 모두 소프트웨어나 하드웨어로 쉽게 구현이 될 수 있다. 가장 복잡한 연산은 비선형적인 $GF(2^4)$ 상에서의 곱셈의 역원 연산이지만, 총 원소의 개수가 16개인 유한체 상에서 일어나는 곱셈이기 때문에 총 64비트의 메모리를 사용해서 룩업표로 구성할 수가 있다.

Kim의 방식과 비교해 보면, Kim의 방식에서는 일반적인 암호학적 해쉬 함수의 사용을 가정하고 있다. 제안된 방식과 Zhang^[6], Adeli-Liu^[7], 그리고 Kim^[8] 방식의 특성을 표 3에서 비교하였다. 이 때 해쉬 함수는 SHA-1이나 SHA-2 family 등 임의의 함수를 선택할 수 있을 뿐만 아니라 구현 방식에 따라서 연산량이 다르기 때문에 해쉬 함수를 호출

하는 회수를 별도로 표시하였다.

일반적으로 해쉬 함수는 암호화 알고리즘보다 경량으로 여겨지지만, 일방향성, 약한 충돌저항성, 강한 충돌 저항성 등의 강한 요구조건들을 만족해야 하기 때문에, SHA-1의 경우만 하더라도 하나의 블록에 대한 해쉬 값을 연산하기 위해 80번의 반복 연산을 수행해야 한다. 그러나 제안된 방식에서는 전부-또는-전무 조건만 만족시키는 것으로 충분하기 때문에 이러한 조건을 완화시켜서, 간단한 선형 연산 및 테이블 룩업으로 변환 과정을 완료하는 것이 가능하다. 따라서 센서 네트워크와 같은 작은 연산 능력만을 보유한 분산 네트워크에서도 작은 비용으로 보안 방식을 구현하는 것이 가능하다.

V. 결 론

이 논문에서는 선형 변환과 룩업표를 이용해서 암호학적 해쉬 함수에 비해 적은 계산량을 사용해서 메시지를 변환할 수 있는 안전한 네트워크 부호를 제안하였다. 제안된 방식에서는 n 개의 전송되는 메시지 중에서 최대 $n-1$ 개의 사용자 메시지를 전송하는 것이 가능하다. 이 때 공격자가 최대 $n-1$ 개까지의 노드를 관찰하더라도 사용자 메시지는 공격자에게 유출되지 않고 안전하게 전송이 될 수 있다. 새로운 안전한 네트워크 부호는 전부-또는-전무 변환에 기반을 둔 것으로 정보이론적으로 완전한 조건의 안전한 네트워크 부호화의 조건을 만족하는 것을 증명하였다. 향후에는 오류가 존재하는 환경에서도 도청 공격에 안전하면서도 낮은 복잡도를 갖는 네트워크 부호에 대한 연구가 필요하다.

References

[1] S.-Y. R. Li, R. W.-H. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 1111 - 1120, Feb. 2003.

[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W.-H. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204 - 1216, Apr. 2000.

[3] T. Ho, R. Koetter, M. Medard, M. Effros, J. Shi, and D. Karger, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413 - 4430,

Oct. 2006.

[4] N. Cai and R. W.-H. Yeung, "Secure network coding," in *Proc. 2002 IEEE Int. Symp. Inf. Theory (IEEE ISIT 2002)*, p. 323, Lausanne, Switzerland, July 2002.

[5] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," in *Proc. Workshop Network Coding, Theory, and Applications (NetCod 2005)*, Riva del Garda, Italy, Apr. 2005.

[6] Y. Zhang, C. Xu, and Wang, "A novel scheme for secure network coding using one-time pad," in *Proc. Int. Conf. Networks Security, Wireless Commun. and Trusted Computing*, pp. 92 - 98, Hubei, China, Apr. 2009.

[7] M. Adeli and H. Liu, "Secure network coding with minimum overhead based on hash functions," *IEEE Commun. Lett.*, vol. 13, no. 12, pp. 956 - 958, Dec. 2009.

[8] Y.-S. Kim, "Refined secure network coding scheme with no restriction on coding vectors," *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1907 - 1910, Nov. 2012.

[9] R. L. Rivest, "All-or-nothing encryption and the package transform," in *Proc. Fast Software Encryption'97 (FSE'97)*, pp. 210 - 218, Haifa, Israel, Jan. 1997.

[10] R. Kötter and F. R. Kschischang, "Coding for Errors and Erasures in Random Network Coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579 - 3591, Aug. 2008.

[11] S. Jaggi, M. Langberg, S. Katti, S., T. Ho, D. Katabi, and M. Medard, "Resilient Network Coding in the Presence of Byzantine Adversaries," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2596 - 2603, June 2008.

[12] M. Park, I. Choi, M. Ahn, and I. Lee, "Exact BER analysis of physical layer network coding for two-way relay channels." *KICS Inform. Mag.*, vol. 37A, no.5, pp. 317 - 324, May 2012.

김 영 식 (Young-Sik Kim)



2001년 2월 서울대학교 전기공학부 학사

2003년 2월 서울대학교 전기컴퓨터공학부 석사

2007년 2월 서울대학교 전기컴퓨터공학부 박사

2007년 3월~2010년 8월 삼성

전자 책임연구원

2010년 9월~현재 조선대학교 정보통신공학과 조교수

<관심분야> 암호학, 정보보호, 정보이론, 오류정정부호, 하드웨어 보안