무선 센서 네트워크를 위한 비잔틴 공격에 강인한 새로운 다중 패스 키 설정 방법

정회원 김 영 식*, 장 지 웅**, 임 대 운***°

New Byzantine Resilient Multi-Path Key Establishment Scheme for Wireless Sensor Networks

Young-Sik Kim*, Ji-Woong Jang**, Dae-Woon Lim***° *Regular Members*

요 약

무선 센서 네트워크(wireless sensor network)에서 센서간 비밀키를 설정하는 단계 중 패스키를 구축하는 단계는 비잔틴 공격(Byzantine attack)에 매우 취약하다. Huang과 Hedhi는 RS 부호를 사용해서 비잔틴 공격에 대한 대응법을 제시하였지만[1], 전송되는 메시지가 공격자(adversary)에게 노출될 뿐만 아니라 전송 효율이 크게 떨어지는 단점을 갖고 있다.

본 논문에서는 Huang과 Hedhi의 방법의 단점을 극복하여, 공격자에게 직접적으로 전송되는 메시지의 정보를 노출하지 않고서도 효율적으로 비잔틴 공격을 막고 변조된 패스의 위치를 알아내는 방법을 제시한다. 이 방법에서는 non-systematic RS 부호를 사용하며 가용한 패스 상으로 서로 다른 RS부호의 부호어(codeword)의 심볼을 전송하게 된다. 이 방법을 사용하면 Huang과 Hedhi의 방법에 비해서 엔트로피 측면에서 보안성이 더 높고 전송 효율이 더 우수해 진다.

Key Words : Byzantine attack, multi-path key establishment, perfectly secure message transmission, Reed-Solomon code, wireless sensor network

ABSTRACT

The path key establishment phase in the wireless sensor network is vulnerable to Byzantine attack. Huang and Hedhi proposed a Byzantine resilient multi-key establishment scheme using a systematic RS code, which has shortcomings of exposing a part of message symbols and inefficient transmission.

In this paper, we propose a new Byzantine resilient multi-path key establishment scheme in which direct message symbols are not exposed to an adversary and are more efficiently transmitted the RS-encoded symbols to the destination node. In the proposed scheme, a non-systematic RS code is used to transmit a generated indirect secret key and each encoded symbol is relayed through available paths between two sensor nodes. If enough symbols are collected at the destination node, it is possible to reconstruct the secret message through RS decoding.

Ⅰ. 서 론

무선 센서 네트워크(Wireless sensor network)는 공간적으로 분포된 자발적인(autonomous) 센서들로 이루어진 무선 네트워크로서 각 센서에서는 물리적, 환경적 데이터를 수집하게 된다. 무선 센서 네트워크

* 삼성전자 (mypurist@gmail.com), ** UCSD 전기컴퓨터공학부 (stasera.jang@gmail.com),
*** 동국대학교 정보통신공학과 (daewoonlim@gmail.com, ° : 교신저자)
논문번호 : KICS2009-05-217, 접수일자 : 2009년 5월 28일, 최종논문접수일자 : 2009년 8월 31일

는 주로 군사적인 목적으로 전쟁지역에 무작위로 살포되어 여러 정보를 수집할 목적으로 개발되었지만, 오늘날에는 환경 및 동물 서식지 감시, 건물 내 동작 감시, 홈 자동화, 헬스케어 시스템에 응용되고 있다[2]. 각각의 센서들은 계산 능력이 크지 않을 뿐만 아니라 저비용으로 구현하기 위해서 조작방지(tamper-resistant) 기술이 적용이 되지 않기 때문에 외부의 공격이나 침입에 취약한 특성을 갖는다. 군사적 산업적 응용에서 잘못된 센싱 정보를 수집하는 경우 잘못된 결론으로 이어질 수 있기 때문에, 센서 네트워크에서는 이러한 외부의 공격에 대응할 수 있는 보안 체계가 필수적으로 갖추어져야한다.

하지만 센서 네트워크는 기존의 Ad-Hoc 네트워크에 비해서 노드의 개수가 수천 개 규모로 더 많을 뿐만 아니라 센서들이 조밀하게 배치된다. 또한 센서들은 계산능력과 메모리 및 배터리 용량이 제한되어 있고, 여러 요인에 의해 각 센서들이 고장을 일으키기 쉬워서 센서 네트워크 토폴로지(network topology)가 자주 변경이 된다[3]. 이러한 여러 제약들로 인해서 센서 네트워크에서 구현되는 보안 체계는 기존의 Ad-Hoc 네트워크에서 사용하는 보안 기법들을 그대로 사용할 수가 없다.

더욱이 제한된 계산능력과 메모리 용량은 센서 네트워크에서 공개키 암호 방식을 통해 보안 체계를 수립하는 것을 불가능하게 만든다. 그리고 모든 센서에서 하나의 비밀키를 공유하는 방식은 센서가 하나라도 공격자(adversary)에게 손상 및 노출되어 내부 정보가 드러나는 경우에는 전체 네트워크의 보안 체계가 무너지는 문제를 갖고 있다. 또한 모든 센서들이 각각의 고유한 비밀키를 소유하는 경우 역시 결국 무작위로 살포되는 센서들의 특성상 모든 센서들과 통신이 가능하기 위해서는 다른 센서의 비밀키를 대량으로 공유하고 있어야 하기 때문에 실제로 적용이 불가능하다.

이러한 문제를 절충하여서 Eschenauer와 Gligor는 센서 노드에서 사용할 전체 비밀키 군을 생성한 후에 각각의 센서들에게 무작위로 일부 비밀키들을 분배하는 확률적 키 선분배 방식(probabilistic key pre-distribution)을 제안하였다[4]. 이 방식에서는 전체 키 집합의 일부 부분집합을 각각의 센서들에게 무작위로 선분배한 후에 센서가 배치된 후에는 각 센서들이 이웃한 센서들을 감지하여 서로가 확률적으로 공유하고 있는 공통의 키를 찾는 과정을 거친다. 이렇게 되면 통신 가능 거리상에 놓인 센서들 상에서 확률적으로 일정한 개수 이상의 센서들은 서로 공통으로 소유한 키를 찾을 수가 있다. 그러면 물리적으로 인접하였지만 실제 네트워크상으로는 공통의 키가 없는 노드들에 대해서는 2번, 혹은 3번 정도의 Hop을 통한 패스가 형성이 되는데 이 패스를 이용해서 노드들 간의 새로운 키를 생성하여 공유하는 과정을 거치게 된다. Chan, Perrig, 그리고 Song은 Eschenauer-Gligor의 방법을 일반화시켜서 q개의 공통의 키를 소유한 경우에만 공유키를 갖는 새로운 방법을 통해서 성능을 개선시켰다[5].

그러나 패스키를 생성할 때 패스 상에 있는 노드들이 공격자에게 침해되어 조작되는 비잔틴 공격(Byzantine attack)에 노출된 경우에는 공격자에게 새롭게 생성하는 노드간 비밀키에 대한 정보를 노출하거나 패스키의 생성을 방해받을 수가 있다. 예를 들면 공격자가 패스상의 센서 노드를 소유하고 전달되는 통신 정보를 가로채어 전혀 다른 정보로 전송하는 경우에는 두 노드 사이에 공통의 키를 소유할 수가 없게 되며, 어떤 노드가 공격자에게 공격을 받았는지도 알 수가 없게 된다.

이러한 비잔틴 공격에 대응하여 Huang 과 Medhi는 systematic RS 부호를 사용해서 패스키를 생성하는 방법을 제안하였다[1]. 이 방법을 사용하게 되면 공격자가 자신이 소유한 노드에서 전송되는 데이터를 변조하더라도 최종 노드에서 원래의 값으로 수정할 수 있을 뿐만 아니라, 어떤 노드에서 변조가 일어났는지도 알 수가 있다. 하지만 systematic RS 부호를 사용하기 때문에 공격자 역시 패스키에 대한 일정 수준 이상의 정보를 획득하는 것이 가능하며, 같은 값을 여러 번 반복하게 보내게 되므로 효율성이 크게 떨어진다는 단점을 갖고 있다.

본 논문에서는 Huang과 Medhi의 방법의 단점을 극복하여, 공격자에게 직접적으로 전송되는 메시지의 정보를 노출하지 않고서도 효율적으로 비잔틴 공격을 막고 변조된 패스의 위치를 알아내는 방법을 제시한다. 또한 non-systematic RS 부호를 사용하며 가용한 패스 상으로 서로 다른 RS부호의 부호어(codeword)의 심볼을 전송하는 경우 엔트로피 측면에서 보안성이 더 좋고 전송 효율이 더 높음을 보일 것이다.

본 논문의 구성은 다음과 같다. 먼저 제 2장에서 사전 지식으로 비잔틴 공격과 RS 부호를 소개한 후, 제 3장에서는 Huang과 Medhi가 제시한 방법을 설명하고 그들의 논문에서는 제시되지 않은 다른 형태의 분석을 제시한다. 다음으로 제 4장에서는 시한 제시한 방법에 대해서 소개하며, 제 5장에서는 두 가지 방법을 비교하고 마지막으로 제 6장에서 결론을 맺는다.

Ⅱ. 사전지식

2.1 비잔틴 공격에 대한 개요

비잔틴 공격자(Byzantine adversary)는 네트워크상으로 임의의 패킷을 주입하거나 패킷 조작이 가능하며, 공격자가 획득한 노드로 지나가는 패킷의 내용을 도청(eavesdropping)하는 것이 가능한 능력을 지닌 공격자를 의미한다. 비잔틴 공격은 원래 시스템의 각 구성요소들 중에 일부 요소에서 문제가 발생하더라도 정상적인 동작이 가능한 내고장성(fault tolerant)을 갖는 시스템 구축을 위해 연구되었고[6], 오늘날에는 네트워크 보안 측면에서 많은 연구가 이루어지고 있다.

Dolev, Dwork, Waarts, 그리고 Yung은 비잔틴 공격자가 존재하는 환경에서 안전한 메시지 전송에 대한 연구를 수행하였다[7]. 그 결과 전체 n개의 패스가 존재하고 그 중에서 t개의 패스가 공격자에게 침해되어 전송되는 데이터가 변조된다고 했을 때, 2-round의 PSMT (perfectly secure message transmission)가 가능할 필요조건은 $n > 2t$를 만족하는 것임을 보였다[7]. 그리고 Fitzi 등은 1-round PSMT의 경우는 $n > 3t$가 되어야 가능하다는 것을 보였다[8].

Huang와 Medhi은 1-round PSMT의 특별한 경우로서 p개의 다중 Hop 패스가 두 센서 노드 사이에 형성된 경우에 systematic RS 부호를 사용해서 두 센서 노드 사이에 간접 비밀키를 구축하는 방법을 제시하였다[1].

2.2 Non-systematic RS 부호

RS 부호는 순회 부호의 일종으로 부호어(codeword)의 각 심볼이 q개의 원소로 이루어진 확장체(extension field) F_q상의 원소이다. 여기서 소수 p와 정수 s에 대해 $q = p^s$이다. 이 때 부호어의 길이는 $q-1$의 약수이지만, 순회부호의 부호 길이를 조절하는 shortening, extending, puncturing 등의 널리 알려진 여러 방법에 의해서 여러 가지 값으로 확장이 가능하다. 기본적으로 부호 길이가 n이고 메시지 심볼의 길이가 k인 RS 부호를 (n,k) RS 부호라 부른다.

t개의 오류를 정정할 수 있는 RS부호의 생성 다항식(generator polynomial)은 다음과 같다.

$$g(x) = \prod_{i=0}^{2t-1} (x - \beta^{b+i}) \quad (1)$$

여기서 β는 F_q상의 원시원(primitive element)이다. 이 때 메시지의 크기를 나타내는 차원(dimension)은 $k = n - 2t$이다. 부호어에서 메시지가 겉으로 보이도록 인코딩(encoding)된 경우를 systematic 인코딩이라 부르고 그렇지 않은 경우를 non-systematic 인코딩이라 부른다. 많은 응용에서 RS 부호는 systematic 인코딩을 사용한다. Systematic RS 부호는 메시지와 패리티가 부호어 상에서 명확하게 구분되어 있어, 오류가 적은 환경이거나 오류 정정이 실패하는 경우에는 디코딩이 없이도 메시지만 잘라서 그대로 사용할 수 있으며 구현도 비교적 쉽다.

그러나 이 논문에서는 non-systematic 인코딩을 사용해서 무선 센서 네트워크의 패스키 설정 단계의 보안을 높이는 방법을 제안한다. non-systematic 인코딩에서는 메시지와 패리티가 서로 섞여 있기 때문에 부호어만 봐서는 메시지를 바로 알 수가 없다. 따라서 전송되는 각각의 심볼이 공격자에게 노출될 수 있는 상황에서는 원래의 메시지 자체를 보내는 systematic 인코딩 보다는 원래의 메시지가 직접적으로 드러나지 않는 non-systematic 인코딩을 사용하는 것이 더 바람직하다.

RS 부호를 인코딩 하는 방법은 다음과 같다. 우선 메시지를 차수가 k인 다항식 $m(x)$로 나타내자. 이 때 메시지 다항식 $m(x)$는 유한체 F_q 상의 다항식이기 때문에 각 항의 계수는 F_q 상의 원소로 이루어져 있다. 이 때 non-systematic 인코딩은 (1)에서 주어진 생성 다항식과 메시지 다항식을 다음과 같이 곱함으로써 이루어진다.

$$c(x) = m(x)g(x) \quad (2)$$

그리고 systematic 인코딩은 (1)에서 주어진 생성 다항식으로 메시지 다항식에 x^{n-k}를 곱한 다항식을 나눈 나머지가 패리티 다항식이 된다.

$$c(x) = x^{n-k}m(x) + p(x) = q(x)g(x)$$

이 때 오류(error)의 개수를 e라 하고 손실(erasure)의 개수가 r이라고 하면 다음과 같은 부등식을 만족하는 경우 RS 부호는 메시지를 오류 없이 디코딩하는 것이 가능하다.

$$2e + r \leqq n - k = 2t \quad (3)$$

여기서 t는 오류 정정 능력(error correction capability)을 의미한다. Non-systematic RS 부호의 복호 방법은 [9]를 참고하라.

Ⅲ. HM 방식 및 분석

Huang과 Medhi는 systematic RS 부호를 사용해서 비잔틴 공격에 강인한 패스키 설정 방법을 제시하였다[1]. 이 논문에서는 Huang과 Medhi의 방법을 [1]에서 분석하지 않은 다른 방식으로 분석해 본다.

Eschenauer와 Gligor의 키설정 방법에서는[4] 무선 센서 네트워크에서 센서들이 무작위로 배치되고 난 후에는 센서 노드들 각각에서 통신 가능 거리상에 존재하는 인접한 노드들과 각 노드가 소유하고 있는 비밀키의 정보를 교환하여 공통으로 소유한 비밀키를 찾게 된다. 이 때 일정한 확률로 공통의 비밀키를 공유하게 되는 노드들 사이의 1-hop 패스가 형성이 된다. 이렇게 형성된 공통의 비밀키를 소유한 노드 사이에는 안전하게 정보를 송수신하는 것이 가능하다.

그림 1에서는 센서 노드들 사이의 비밀키를 이용한 1-hop 패스를 도식화 해서 보여주고 있다. 여기서 점선으로 된 원은 센서 노드에서 통신 가능한 거리를 의미한다. 그림 1에서는 네 개의 노드가 통신 가능한 거리에 존재하고 있고, A-C, A-D, B-C, B-D간에는 안전한 1-hop 채널이 형성되어 있다. A-B사이에는 공통의 비밀키가 없지만 A-C-B, A-D-B로 이어지는 두 개의 패스가 존재하여 이런 패스를 통해서 공통의 간접 비밀키를 공유할 수가 있다.

이 때 두 센서 노드 사이의 패스의 개수를 p개라 하자. 그러면 이 중에서 e개가 ($e < p$) 공격자에 의해서 침해되어 데이터가 조작된다고 가정하자. 그러면 Huang과 Hedhi의 방법에서는 먼저 센서 노드 A에서 공통으로 소유할 비밀 메시지를 생성한다. 이 비밀 메시지는 k개의 F_q 상의 원소들로 이루어져 있다. 이

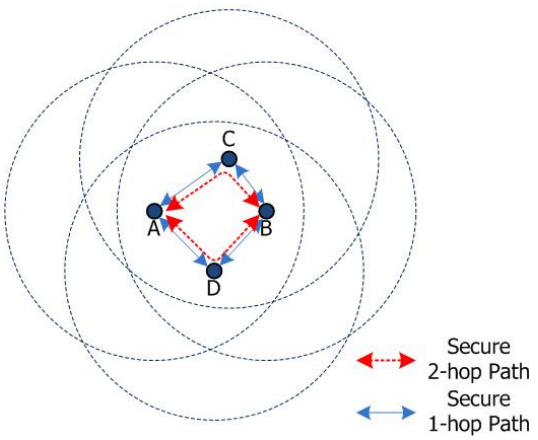

그림 1. 무선 센서 네트워크의 키 설정 과정에서 다중 Hop 패스

때 systematic RS 인코딩을 통해서 $2t$개의 패리티 심볼을 만들 수 있다. 그러면 각각의 패스로 한 번에 하나의 메시지 심볼과 $2t$개의 패리티 심볼을 연접해서 전송하게 된다.

모든 패스로 동일한 $2t$개의 패리티 심볼이 전송되고 1-round PSMT의 조건에 의해 $p > 3e$를 만족한다고 가정하면 HM 방식에서는 다수결에 의해서 패리티 비트를 항상 정확하게 복호할 수 있다.

그러면 p개의 패스는 각 패스마다 최대 t번의 전송을 통해서 메시지를 전송하게 되므로 $pt \geq ek$가 성립한다. p개의 패스 중에서 e개의 패스가 공격자에 의해서 변조가 된 것으로 간주하였으므로 RS부호의 성질에 의해서 변조된 심볼의 개수가 오류 정정 능력 t보다 작은 경우에는 원래의 오류를 모두 정정하면서 동시에 어떤 패스에서 변조가 일어났는지까지 알아낼 수가 있다.

그러나 이 방법이 가진 문제점으로는 매번 $2t$개의 패리티 심볼을 재전송하기 때문에 전송 효율이 급격히 떨어진다는 것이 있다. 뿐만 아니라 매 전송마다 패리티에 추가되어 전송되는 1개의 메시지 심볼은 systematic RS 부호의 특성으로 인해 비밀키에 대한 직접적인 정보를 제공하게 된다. 물론 하나의 센서 노드라도 공격자에게 침해받는 경우에는 $2t$개의 패리티 심볼도 모두 노출이 된다.

HM 방법의 경우 l번째 패스로 전달되는 심볼의 개수를 $r_{HM}(l)$이라 하자. 그러면 $p < k$인 경우 $r_{HM}(l)$은 최대 $\lceil k/p \rceil$ 개가 된다. 그리고 p가 k의 배수가 아니면 일부는 $\lfloor k/p \rfloor$ 개의 심볼을 전송하게 된다. 그러면 p개의 패스 중에서 e개가 공격자가 소유한 패스이고 공격자가 소유한 패스의 인덱스를 a_i, $(0 \leq i < e)$)로 나타내자. 그러면 공격자가 수신하는 총 메시지 심볼의 개수 E_{HM}은 다음과 같이 나타낼 수 있다.

$$E_{HM} = \sum_{i=0}^{e-1} r_{HM}(a_i)$$

그러면 E_{HM}은 다음과 같은 범위 안에 존재한다.

$$ek/p - e < E_{HM} < ek/p + e \tag{4}$$

여기서 센서 노드 B가 정확히 복호를 하기 위해서는 (n,k) RS 부호의 특성에 의해서

$$2E_{HM} \leq n - k = 2t \tag{5}$$

를 만족해야 한다. 다시 말해 공격자가 소유한 패스를 지나온 심볼들은 모두 오류로 간주할 수 있고 이 심볼들의 개수는 오류 정정 능력보다 작아야 한다. 반면에 공격자의 입장에서는 자신이 수신한 메시지 이외의 나머지는 손실(erasure)로 간주할 수 있으므로 다음과 같은 식을 만족하는 경우 공격자 역시 자신이 수신한 정보를 이용해서 비밀키를 복구하는 것이 가능해 진다.

$$n - E_{HM} - 2t \leqq n - k = 2t \tag{6}$$

이 경우 $2t$개의 패리티는 고정된 위치로 매번 전송되기 때문에 공격자도 항상 정확하게 패리티 정보를 얻을 수가 있다. 따라서 (5)와 (6)로부터 $n \leqq 5t$ 인 경우 공격자와 센서 노드 B 모두 비밀키를 복구할 수가 있으므로 공격자가 키를 완전히 복구하는 것을 방지하기 위해서는 다음이 성립하고

$$n > 5t \geqq 5E_{HM} \tag{7}$$

이것은 다음 관계를 함축한다.

$$k > 3E_{HM} \tag{8}$$

그리고 (4)와 (5)로부터 다음이 성립한다.

$$n + 2e \geqq (p + 2e)k/p \tag{9}$$

이 때 센서 노드 A가 전송하는 총 데이터 심볼의 개수는 $N_{HM} = (2t+1)k$이다. 설령 공격자가 충분한 심볼 수를 확보하지 못한 경우에도 E_{HM} 개의 메시지 심볼과 $2t$개의 패리티 심볼을 정확하게 알고 있기 때문에 실제로 새로 설정된 센서 노드 A와 센서 노드 B 사이의 패스키에 남아 있는 엔트로피 $H_{HM}(p,e)$는 그만큼 더 줄어들게 된다. 이 때 심볼의 비트수를 $q = 2^s$라 하면 패스키에 남아 있는 엔트로피는 $H_{HM}(p,e) = (k - E_{HM})s$비트이다.

Ⅳ. 비잔틴 공격에 강인한 새로운 패스키 설정 방법

앞에서 살펴본 HM 방식에서는 패스를 통해 전송되는 일부의 비밀키가 공격자에게 그대로 노출이 될 뿐만 아니라 패리티를 반복적으로 전송하기 때문에 그 만큼 효율이 떨어진다는 문제를 갖고 있었다. 이러한 문제를 해결하기 위해서 이 장에서는 non-systematic RS 부호를 사용하는 패스키 설정 방법을 제시하고 보안 특성을 분석한다.

이 방법에서도 패스키를 설정하는 단계까지는 기본적으로 Eschenauer와 Gligor가 제시한 방법을 그대로 따른다[4]. 센서 노드 A와 센서 노드 B는 서로 통신이 가능한 거리에 놓여 있지만 사전에 공유된 비밀키를 발견하지 못한 노드들이라 가정하자. 그리고 두 노드를 연결하는 2-hop 이상의 패스들이 p개 존재한다고 가정하자.

그러면 센서 노드 A에서는 센서 노드 B와 공유할 비밀 정보를 생성하여 이것을 non-systematic RS 부호를 사용해서 인코딩 한다. 그런 후 부호어의 각각의 심볼을 p개의 패스를 통해서 차례로 센서 노드 B로 전달한다. $n > p$인 경우 우선 p개의 심볼을 p개의 패스로 전달한 후 다시 첫 번째 패스부터 그 다음 p개의 심볼을 전달하게 된다.

그림 2 에서는 새로 제안하는 다중 패스키 설정 방법을 도식화해서 보여주고 있다. 이 그림에서는 센서 노드 A에서 센서 노드 B까지 총 8개의 다중 Hop 패스가 존재하고 각각의 패스로 순차적으로 RS 부호를 한 심볼씩 전송하게 된다. 이런 방법으로 l번째 패스상으로 총 $r(l)$개의 심볼이 전송이 된다고 가정하자. 이 때 $r(l) \leqq \lceil n/p \rceil$ 이다. 앞에서와 마찬가지로 공격자가 소유하게 되는 노드의 인덱스를 a_i $(0 \leqq i < e)$로 나타내면 부호어 심볼의 개수 E_N를 다음과 같이 나타낼 수 있다.

$$E_N = \sum_{i=0}^{e-1} r(a_i)$$

그러면 오류 정정 능력은 $t \geqq E_N$이 되어야 하고

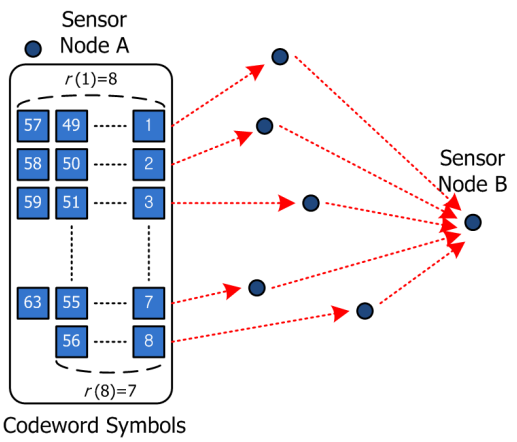

그림 2. 새로운 다중 패스키 설정 방법

그리고 각 패스상으로 전달되는 총 심볼의 개수 N은 다음과 같다.

$$N=\sum_{i=0}^{p-1} r(i) \leqq n$$

이제 센서 노드 B에서 수신된 정보를 통해 원래의 비밀 메시지를 다시 복호할 수 있기 위해서는 다음과 같은 조건을 만족해야만 한다.

$$k \leqq N-2E_N \tag{10}$$

여기서 공격자는 e개의 패스를 소유하고 있어서 전송되는 메시지들을 자유롭게 조작할 수 있다고 가정하자. 그러면 변조된 심볼은 그대로 통신 오류로 간주할 수 있고 p개의 패스로 r번의 전송을 통해서 전송되지 못한 심볼은 손실로 간주할 수 있다.

반면에 공격자가 복호가 가능하려면 다음과 같은 식을 만족해야 한다. 공격자가 확보한 심볼의 개수는 E_N개 이므로 나머지 $n-E_N$개를 공격자의 입장에서는 손실로 간주할 수 있고 오류는 없다. 따라서

$$k \leqq E_N$$

이다. 그러므로 공격자는 복호할 수 없으면서 센서 노드 B에서만 복호가 가능할 조건은 다음과 같다.

$$k > E_N$$
$$n = k+2t > 3E_N$$

여기서 손실이 없는 경우 $r(l)$은 n과 p에 의해서 결정이 된다. n은 RS 부호의 부호 길이이고 p는 무선 센서 네트워크를 설계할 때 도출되는 파라미터이다. 확률적으로 p의 기댓값을 구할 수 있다.

그러면 무선 센서 네트워크에서 몇 개의 센서 노드를 공격자가 소유하더라도 패스키를 안전하게 전달할 수 있는지는 파라미터 E_N의 최대값을 기준으로 t값을 정해 줌으로써 설계가 가능하다.

그리고 공격자가 자신이 소유한 센서 노드를 통해 수신한 심볼의 개수는 최대 E_N개이지만 non-systematic RS 부호의 특성상 모두 직접적으로 메시지를 나타내는 심볼이 아니기 때문에 공격자에게 직접적으로 노출되는 메시지는 없다. 하지만 엔트로피 측면에서는 $n-E_N$개의 심볼을 모르는 상황이 되므로 $q=2^s$라 하면 최소 $H(p,e)=(n-E_N)s$비트의 엔트로피가 패스키에 남아 있게 된다.

정리 1. $2t \geqq 3e$라 하자. p가 전체 패스의 개수이고 e가 공격자가 획득한 패스의 개수라 하자. $H_{HM}(p,e)$을 HM 방식에서의 엔트로피라 하고 $H(p,e)$를 새로운 방식에서의 엔트로피라 하면 다음 식이 성립한다.

$$H(p,e) > H_{HM}(p,e)$$

증명) 앞에서 두 엔트로피 값은 다음과 같이 주어졌다.

$$H_{HM}(p,e)=k-E_{HM}$$
$$H(p,e)=n-E_N$$

이 때 k는 HM 방식에 의해서 결정되는 메시지 심볼의 개수이다. 이제 $2t \geqq 3e$라는 조건을 이용하면 다음과 같은 부등식을 얻을 수 있다.

$$\begin{aligned} H(p,e)-H_{HM}(p,e) &= [n-k'-E_N+E_{HM}]s \\ &> [(n-k')-\frac{e}{p}(n-k')-2e]s \\ &= [(n-k')(1-\frac{e}{p})-2e]s \\ &> \frac{2s}{3}(n-k'-3e) \geqq 0 \end{aligned}$$

□

다음 장에서 나타난 것처럼 일반적으로 e가 커지게 되면 설계하는 시스템의 안정성을 높이기 위해서 더 높은 오류 정정 능력 t를 갖는 부호를 사용하게 되므로 $2t \geqq 3e$는 일반적인 환경에서 언제나 성립한다. 따라서 정리 1은 새로 제안한 방법에서 패스의 개수 p와 공격자가 획득한 패스의 개수 e의 크기가 같을 때 언제나 새로 제안한 방법의 엔트로피가 더 크다는 것을 보여준다.

Ⅴ. 성능 비교 분석

이 장에서는 HM 방식과 새로운 방식의 성능을 비교 분석할 것이다. 시뮬레이션을 위해서 $n=63$인 RS 부호를 가정하였다. 센서 네트워크에서 암호화를 위해서 대칭키 암호 시스템을 사용한다고 하자. 이 때 대칭키 알고리즘의 경우 오늘날 80비트에서 128비트 정도의 보안성이면 많은 공격으로부터 안전하다고 가정

할 수 있다. 따라서 $n=63$이면 $q=2^6$으로 $k \geq 22$이상만 되면 모든 비밀키를 한 번의 인코딩과 디코딩으로 전달하는 것이 가능하다. 이 때 n에 의해서 시스템 설계시에 가정된 p값과 e값에 따라서 필요한 메시지 심볼의 크기 k및 오류 정정 능력 t를 설계하는 것이 가능하다.

그림 3과 그림 4는 두 가지 방식에서 노드 사이의 패스의 개수가 $p=4,...,10$까지 변하고 공격자가 획득한 최대의 노드의 개수가 $e=1,2$일 때 메시지 심볼의 최소 크기와 그에 따른 오류 정정 능력 t를 비교해서 보여주고 있다.

그림에서 확인할 수 있는 것처럼 새로 제안한 방법의 오류 정정 능력의 크기가 기존의 방법보다 더 커야 하고 그에 따라서 부호어에서 차지하는 메시지 심볼의 크기 k는 작아지게 된다. 하지만 매 전송시 패리티 심볼을 반복해서 전송하는 기존의 방법에 비해서 이번에는 모든 심볼을 최대 한 번씩만 전송하기 때문에 전체 전송 효율은 그림 5에서 볼 수 있는 것처럼 훨씬 더 높다.

그림 5에서는 새로운 방식에서의 전송되는 심볼의 총 개수를 기존의 방법에서 전송되는 심볼의 총 개수로 나눈 값을 퍼센트로 표시해 주고 있다. 여기서 가

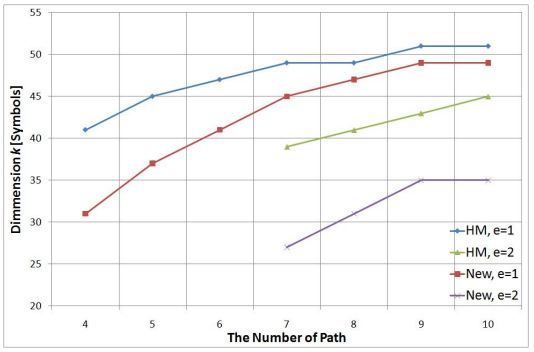

그림 3. 패스의 개수에 따른 메시지 심볼의 크기 비교

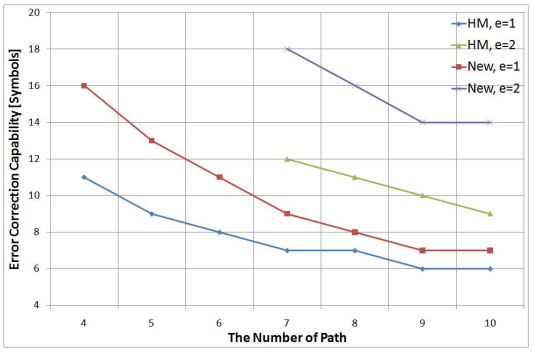

그림 4. 패스의 개수에 따른 필요한 오류 정정 능력 비교

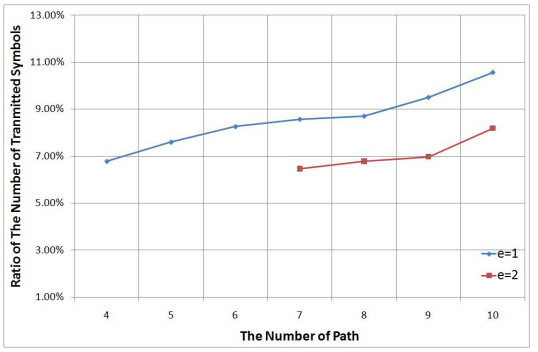

그림 5. 패스의 개수에 따른 전송되는 심볼의 총 개수

능한 패스의 크기를 $p=4,...,10$으로 하고 공격자가 획득한 최대의 노드의 개수를 $e=1,2$로 설정했을 때 모두 새로운 방법이 HM 방식에 비해서 더 적은 비율의 심볼만을 전송하고 있음을 볼 수 있다.

마지막으로 그림 6에서는 두 가지 전송 방식에서 최소의 엔트로피를 비교해 주고 있다. 여기에서 새로운 방법에서의 엔트로피가 기존에 비해서 패스의 개수가 작을 때에는 두 배 이상 더 크다는 것을 확인할 수 있다.

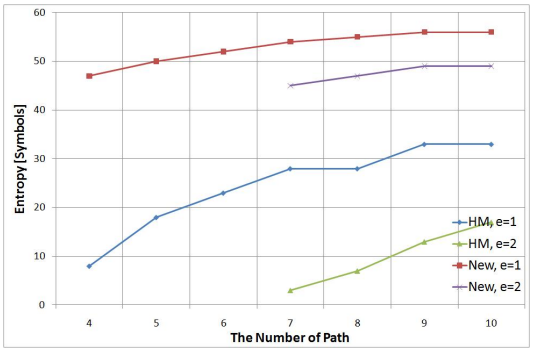

그림 6. 패스의 개수에 따른 최소 엔트로피에 대한 비교

Ⅵ. 결 론

본 논문에서는 non-systematic RS 부호를 이용하여 Huang과 Hedhi 방식 보다 안전하고 효율적인 무선 센서 네트워크의 다중 패스키 방식을 제안하였다. 새로 제안된 방식은 non-systematic RS부호를 이용하므로 패스키가 직접적으로 드러나지 않으며, 동일한 패리티 심볼을 매번 전송하지 않으므로 기존 방식보다 효율적인 전송이 가능하다. 또한 모의실험을 통하여 새로 제안된 방식이 기존의 방식보다 우수한 성능을 가짐을 보였다.

참 고 문 헌

〔1〕 D. Huang and D. Medhi, "A Byzantine resilient multi-path key establishment scheme and its robustness analysis for sensor network," in *Proc. IEEE IPDPS 2005*, 4-8 Apr. 2005.

〔2〕 S. Hadim and N. Mohamed, "Middleware challenges and approaches for wireless sensor networks," *IEEE Distributed Systems Online*, vol. 7, no. 3, pp. 1-1, Mar. 2006.

〔3〕 Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor network," *IEEE Commun. Survey & Tutorials*, vol. 8, no. 2, pp. 2-23, 2nd Quater 2006.

〔4〕 L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor network," in *Proc. 9th ACM Conf Computer, Commun. Security*, Nov. 2002, pp. 41-47.

〔5〕 H. Chan, A. Perrig, and D. Song, "Random key predistribution scheme for sensor networks," in *Proc. IEEE Symp. Security and Privacy (SP 2003)*, 11-14 May 2003, pp. 197-213.

〔6〕 L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Programming Languages and Systems*, vol. 4, no. 3, pp. 382-401, July 1982.

〔7〕 D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly Secure Message Transmission," *J. ACM*, vol. 40, no. 1, pp. 17-47, Jan. 1993.

〔8〕 Matthias Fitzi, Matthew Franklin, Juan Garay, and S. Harsha Vardhan, "Towards optimal and efficient perfectly secure message transmission," *IACR Theory of Cryptography Conference (TCC 2009)*, *LNCS 4392*, pp. 311-322, 2007.

〔9〕 A. Shiozaki, T. K. Truong, K. M Cheung, and I. S. Reed, "Fast transform decoding of nonsystematic Reed-Solomon codes," *IEE Proc.*, vol. 137, no. 2, pp. 139-143, Mar. 1990.

김 영 식 (Young-Sik Kim) 정회원

2001년 2월 서울대학교 전기공학부 공학사
2003년 2월 서울대학교 전기·컴퓨터공학부 석사
2007년 2월 서울대학교 전기·컴퓨터공학부 박사
2007년 3월~현재 삼성전자
<관심분야> 암호학, 시퀀스, 오류정정부호, 디지털 통신

장 지 웅 (Ji-Woong Jang) 정회원

2000년 2월 서울대학교 전기공학부 공학사
2002년 2월 서울대학교 전기컴퓨터공학부 석사
2006년 2월 서울대학교 전기컴퓨터공학부 박사
2006년 3월~2008년 6월 삼성전자 책임연구원
2008년 8월~현재 UCSD(postdoc)

임 대 운 (Dae-Woon Lim) 정회원

1994년 2월 한국과학기술원 전기및전자공학과 학사
1997년 2월 한국과학기술원 전기및전자공학과 석사
2006년 8월 서울대학교 전기·컴퓨터공학부 박사
1995년 9월~2002년 8월 LS산전(주) 중앙 연구소 선임 연구원
2006년 9월~현재 동국대학교 IT학부 조교수
<관심분야> OFDM, 부호 이론, 시공간 부호