http://dx.doi.org/10.5392/JKCA.2012.12.01.048

무선 센서 네트워크 환경에서 단-방향 해쉬 함수 기반 다중 경로 보안 전송 기법

A Secure Multipath Transmission Scheme Based on One-Way Hash Functions in Wireless Sensor Networks

이윤정*, 김동주*, 박준호*, 성동욱**, 유재수*
충북대학교 정보통신공학부*, 한국과학기술원 전산학과**

Yunjeong Lee(sky86861026@gmail.com)*, Dongjoo Kim(dongjoo.k@gmail.com)*, Junho Park(junhopark@chungbuk.ac.kr)*, Dong-ook Seong(doseong@dbserver.kaist.ac.kr)**, Jaesoo Yoo(yjs@chungbuk.ac.kr)*

요약

다양한 센싱 모듈의 개발과 무선 통신 기술의 발달로 인해, 한정된 통신 능력과 제한된 연산 능력을 갖춘 다수의 센서 노드를 활용하여 무선 센서 네트워크를 구성하는 것이 가능하게 되었다. 이러한 센서 노드는 무인 환경이나 적지와 같은 환경에 배포되기 때문에 보안에 취약하다. 특히 실생활 응용에 사용될 때, 데이터가 노출되면 치명적인 피해를 입을 수 있기 때문에 보안에 대한 고려는 필수적이다. 하지만 기존 네트워크에서의 보안 기법은 센서 노드의 제한된 성능을 고려하지 않기 때문에, 무선 센서 네트워크에 적용하는 것은 한계가 있다. 이러한 점을 해결하기 위해, 본 논문에서는 무선 센서의 제한된 성능을 고려한 에너지 효율적인 보안 기법을 제안한다. 제안하는 기법은 원본 데이터의 해독을 어렵게 하기 위해 단-방향 해쉬 함수인 MD5를 기반으로 데이터를 변환 후, 분할하여 다중 경로를 통해 전송함으로써 보안성을 강화하는 것이 가능하다. 성능 평가 결과, 제안하는 기법은 기존 기법의 약 6%의 에너지만 소비하였다.

■ 중심어 : | 무선 센서 네트워크 | 보안 | 단 방향 해쉬 함수 | MD5 | 다중 경로 전송 |

Abstract

With the development of sensing devices and wireless communication technologies, wireless sensor networks are composed of a large number of sensor nodes that are equipped with limited computing performance and restricted communication capabilities. Besides, the sensor nodes are deployed in hostile or unattended environments. Therefore, the wireless sensor networks are vulnerable to security. In particular, the fatal damage may be occurred when data are exposed in real world applications. Therefore, it is important for design requirements to be made so that wireless sensor networks provide the strong security. However, because the conventional security schemes in wired networks did not consider the limited performance of the sensor node, they are so hard to be applied to wireless sensor networks. In this paper, we propose a secure multipath transmission scheme based on one-way hash functions in wireless sensor networks considering the limited performance of the wireless sensor nodes. The proposed scheme converts a sensor reading based on one of one-way hash functions MD5 in order to make it harder to be cracked and snooped. And then, our scheme splits the converted data and transfers the split data to the base station using multi-path routing. The experimental results show that our proposed scheme consumes the energy of just about 6% over the existing security scheme.

■ keyword : | Wireless Sensor Networks | Security | One-Way Hash Functions | MD5 | Multi-path Routing |

* 본 연구는 2011년 교육과학기술부로부터 지원(지역거점연구단육성사업/충북BIT연구중심대학육성사업단)과 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업의 결과임.(No. 2009-0080279)
접수번호 : #111202-001
접수일자 : 2011년 12월 02일
심사완료일 : 2011년 12월 20일
교신저자 : 유재수, e-mail : yjs@chungbuk.ac.kr

I. 서 론

무선 센서 네트워크는 환경 정보 수집, 연산, 무선 통신이 가능한 수많은 센서 노드로 구성된 네트워크이다. 무선 센서 네트워크는 센서 노드를 이용하여 환경 정보를 수집하고 수집된 정보에 대한 분석을 통해 정보를 활용할 수 있도록 한다[1]. 이와 같은 특징으로 인해 무선 센서 네트워크는 차세대 핵심 응용 분야 중 하나로 주목 받고 있으며, 생태계 감시, 군사지역 감시, u-City 응용 등과 같은 다양한 분야에서 폭넓게 응용되고 있다. 무선 센서 네트워크는 관심 지역에 수십에서 수 만 개의 센서 노드를 광범위 하게 배포하여 노드 간 멀티-홉 통신을 통해 정보를 수집한다. 광범위한 센서 네트워크를 구성하기 위해서는 크기가 작고 저렴한 센서가 요구된다. 이로 인해 센서 네트워크에서 사용되는 센서는 에너지, 연산 능력, 통신 반경, 저장 메모리 측면에서 제한적인 성능을 가진다. 따라서 무선 센서 네트워크에서 사용하는 모든 기법은 제한적인 센서의 성능을 고려하여 에너지를 효율적으로 사용할 수 있는, 즉 에너지 소모량이 적은 알고리즘에 대한 연구가 요구된다[2].

무선 센서 네트워크는 주로 환경 정보나 군사 지역을 감시하기 위해 무인 환경에 구축되고, 센서 노드는 수집한 데이터를 기지국으로 전송하기 위해 무선 통신을 사용하기 때문에 외부의 공격으로부터 취약하다[3]. 이러한 특성으로 인해 데이터 전송 시에 데이터가 쉽게 노출될 가능성을 가지고 있다. 이는 군사 정보나 개인의 프라이버시를 다루는 응용에서는 큰 문제가 발생할 수 있다. 이런 문제점을 해결하기 위한 많은 보안 기법들의 연구가 활발하게 진행되고 있다.

일반적으로 안전한 센서 네트워크의 구성을 위해, 정보를 전달하는 기본적인 요소인 라우팅 프로토콜에 키 교환, 인증과 같은 암호 프로토콜을 결합하여 사용할 수 있다[4]. 최근에는 암호 알고리즘을 기반으로 실제 데이터와 가상 데이터를 일정 주기로 동시에 수집하여 전송하는 기법과 신뢰 레벨을 사용한 데이터 전송 기법 등이 제안되었다[5][6]. 하지만 이러한 기법들은 데이터를 전송하는 데 있어서 보안성을 높이기 위해 노드 간의 통신량이 많고, 불필요한 정보의 전송으로 인한 에너지 소모가 발생하기 때문에 제한된 성능을 바탕으로 동작하는 센서 네트워크에는 효율적이지 않다. 그러므로 센서 네트워크의 특성을 고려한 에너지 효율적인 보안 기법에 대한 연구가 요구된다.

본 논문에서는 센서 네트워크에서 전송 데이터가 노출되더라도 실제 정보에 대한 분석을 어렵게 하면서도 통신 에너지 소모량을 줄여 에너지 효율성을 향상시킨 단-방향 해쉬 함수 기반의 다중 경로 보안 전송 기법을 제안한다. 제안하는 기법은 데이터를 전송하는 과정에서 실제 데이터에 대한 분석을 어렵게 하기 위해 센싱 데이터를 변환하여 전송한다. 하지만 변환 데이터라고 할지라도 전체 데이터가 노출되면 분석이 가능하다는 점을 고려하여 데이터를 분할하여 전송한다. 제안하는 기법의 기본 개념은 단 방향 해쉬 함수인 MD5가 복호화 방법이 존재하지 않고[7], 변환한 데이터의 정보의 일부로는 전체 데이터에 대한 정보를 파악하는 것이 불가능하다는 특징을 기반으로 하여 MD5를 이용한 변환 데이터를 분할하여 전송하는 다중 경로 전송을 사용한다. 기본적으로 본 논문에서 제안하는 기법은 GPSR 기법을 기반으로 작동을 하기 때문에 보안성을 높이면서도 센서 노드 간의 통신량을 최소화 하는 것이 가능하다[8].

본 논문의 구성은 다음과 같다. 제2절에서는 기존 보안 기법의 분석을 통해 문제점과 연구 목적을 설명한다. 제3절에서는 제안하는 단-방향 해쉬 함수 기반 다중 경로 보안 전송 기법에 대해 기술한다. 제4절에서는 제안하는 기법의 보안 수준에 대한 분석을 수행하고, 제5절에서는 기존 기법과의 성능평가를 통해 제안하는 기법의 우수성을 보인다. 마지막으로 제6절에서는 결론과 향후 연구 방향에 대하여 기술한다.

II. 관련 연구

무선 센서 네트워크의 보안성을 높이기 위한 다양한 기법들이 제안되었다. 최근에는 암호 알고리즘을 기반으로 실제 데이터와 가상 데이터를 일정 주기로 동시에 수집하여 전송하는 TESP^2[5]와 신뢰 레벨을 사용하여

데이터를 전송하는 S-GPSR[6]이 제안되었다.

TESP^2 (Timed Efficient Source Privacy Preservation Scheme) [5]는 기본적인 데이터 보안을 위해 타원 곡선 암호 즉, ECC(Elliptic Curve Cryptography)를 사용하여 데이터를 암호화 한다. [그림 1]은 TESP^{2}의 구조를 나타난다.

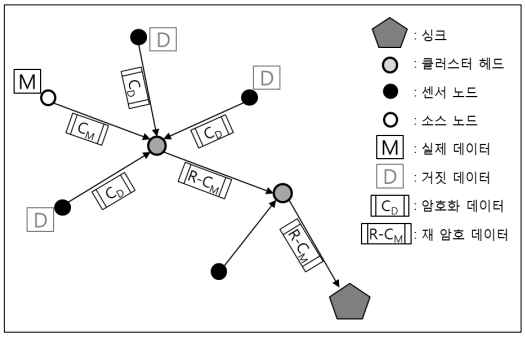


그림 1. TESP^2 구조

[그림 1]에서 어떤 상황을 감지한 소스 노드가 데이터를 싱크로 전송할 때, 클러스터 헤드 노드는 실제 데이터와 소스 노드를 은닉하기 위해 자신에게 연결된 센서 노드로부터 주기적으로 데이터를 수집한다. 이 때, 실제 데이터가 발생한 소스 노드에서만 데이터를 수집하지 않고 다른 센서 노드에서도 동등하게 데이터를 수집한다. 데이터가 발생하지 않은 센서 노드는 거짓 데이터를 암호화하여 클러스터 헤드 노드로 전송한다. 암호 데이터를 전송 받은 클러스터 헤더 노드는 거짓 데이터를 필터링하여 실제 데이터를 분리한 후 복호화하고, 클러스터 헤드 노드가 일정 주기에 따라 데이터를 수집할 때 실제 데이터를 다시 암호화하여 상위 클러스터 헤드 노드로 전송하게 된다. TESP^{2}는 실제 데이터와 데이터가 발생한 센서 노드를 최대한 은닉함으로써 보안성을 보완하였다. 하지만 거짓 데이터 자체는 필요 없는 데이터이기 때문에 이를 사용함으로써 에너지 소모가 발생하고, 클러스터를 구축할 때 센서 간의 통신량이 증가하여 에너지 효율적이지 않다는 문제점을 가지고 있다.

S-GPSR[6]은 기존의 GPSR[8] 기법에 보안성을 추가적으로 고려한 라우팅 프로토콜이다. GPSR(Greedy Perimeter Stateless Routing)은 모든 센서 노드가 목적지의 지리적 위치 정보를 알고 있고, 위치 정보를 이용하여 목적지까지 그리디 포워딩으로 데이터를 전송하는 기법이다. 그리디 포워딩은 데이터가 발생한 센서 노드가 자신의 전송 범위 안에 있는 이웃 노드 중 목적지와 가장 가까운 거리에 있는 이웃 노드로 데이터를 전송한다. S-GPSR은 데이터 보안성을 위하여 신뢰 레벨이라는 개념을 도입하였다. [그림 2]는 S-GPSR의 흐름도를 보여준다.

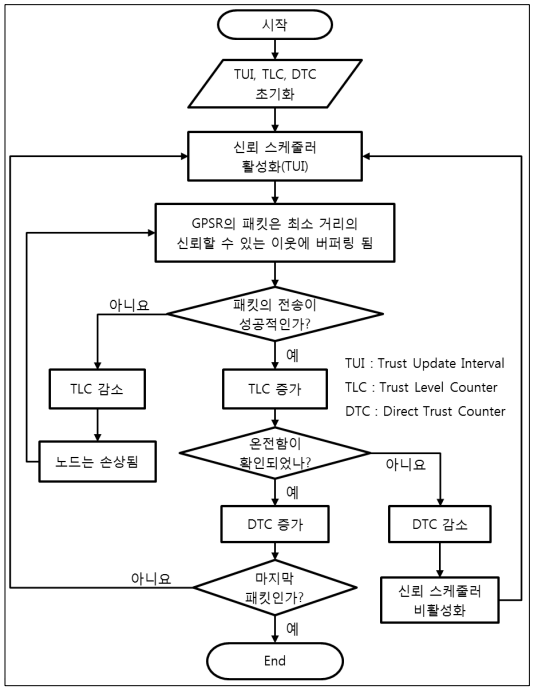


그림 2. S-GPSR 흐름도

[그림 2]에서 TUI는 신뢰도 갱신 주기로 이 주기에 의해 신뢰도가 변화된다. TLC는 신뢰 레벨 카운터로 패킷을 전송했을 때 전송된 패킷이 성공적으로 전송 됐는지의 여부를 확인하여 카운터의 수치를 결정한다. DTC는 직접 신뢰 카운터로 전송 노드가 패킷의 온전함을 확인하여 카운터의 수치를 결정한다. 패킷의 온전함은 원본 패킷과 패킷이 전송된 노드의 확인 메시지를 통해 원본 패킷과 확인 메시지의 비교를 수행하여 결정한다. 이 기법은 기존에 제안된 기법인 신뢰 모델과

T-GPSR을 참조하여 수행된다[9][10]. 신뢰 레벨은 이웃 노드와 통신을 통해 메시지를 전송하고 수신하는 과정에서 데이터가 수정이 됐는지의 여부를 판단하여 결정된다. 결정된 신뢰 레벨을 사용하여 고-신뢰 레벨을 가지고 있는 노드를 통해서만 데이터를 전송함으로써 데이터의 보안성을 높인다. 이 기법 또한 신뢰 레벨을 결정하는 과정에서 고-신뢰 이웃을 판별하기 위해 노드 간에 지속적인 통신이 이루어진다. 센서 네트워크에서 통신 모듈의 사용은 가장 많은 전력을 사용하기 때문에 지속적인 패킷 송수신 때문에 에너지가 빠르게 소모된다는 단점을 가지고 있다.

본 논문에서는 기존 기법의 에너지 손실 문제를 해결하기 위해 MD5 해쉬 함수를 사용한 보안 기법의 연구를 진행한다. 뿐만 아니라, 보안성을 강화하기 위한 분산 데이터 전송 기법의 연구를 추가적으로 수행한다.

III. 제안하는 다중 경로 보안 전송 기법

본 논문에서는 기존 보안 기법의 문제점을 해결하기 위한 단 방향 해쉬 함수 기반의 다중 경로 보안 전송기법을 제안한다. MD5는 입력된 다른 두 개의 메시지가 동일한 메시지 축약을 결과로 내거나 같은 메시지가 서로 다른 메시지 축약을 만들어지는 것은 연산적으로 불가능하다고 알려져 있다[7][11]. MD5는 단-방향 해쉬 함수로, 복호화 알고리즘이 따로 없이 매칭 복호화 방법을 사용하기 때문에 전체 데이터에 대한 MD5 값이 같아야만 하는 특징이 있다. 실제 보안 시스템에서는 이러한 특징을 이용하여 비밀번호를 데이터베이스에 저장할 때 MD5를 사용하여 그 변환 값을 저장하고, 입력한 값의 MD5 변환 값이 저장된 MD5 변환 값과 같은지를 확인하는 형태로 많이 활용된다. MD5는 해쉬 알고리즘 중 연산 속도가 가장 빠르기 때문에 가장 널리 사용된다. 본 논문에서는 보안성을 높이기 위한 연산이 많이 발생하고, 암호화에 필요한 키 값의 저장 용량이 요구되는 데이터의 암호화 대신에 MD5 알고리즘을 사용하여 데이터를 변환하였다. 여기에 MD5는 전체 데이터가 모두 존재할 때 데이터 해독이 가능하다는 문제점을 가지기 때문에 전체 데이터를 한 번에 보낼 경우 보안성이 높지 않다. 따라서 MD5 변환 데이터를 분할하여 각각 다른 경로를 통해 전송함으로써 보안성을 강화하였다. 또, 데이터를 분할하여 전송함으로써 발생하는 에너지 소모량을 줄이기 위해 GPSR을 사용함으로써 이웃 노드와의 통신량을 최소화 하였다[12].

제안하는 기법은 크게 3단계로 이루어진다. 1단계는 센서 노드에서 데이터를 처리하는 과정으로, 단 방향 해쉬 함수 MD5를 이용하여 데이터를 변환하고, 분산 전송에 필요한 전처리 과정을 수행한다. 2단계는 센서 노드에서 기지국으로 데이터를 분산 전송하는 과정으로 분할 데이터는 GPSR을 기반으로 전송한다. 3단계는 기지국에서 데이터를 처리하는 과정으로, 수집된 분할 데이터를 원본 데이터로 복구한다. [그림 3]은 위에서 설명한 제안하는 기법의 전체적인 모습을 보여준다.

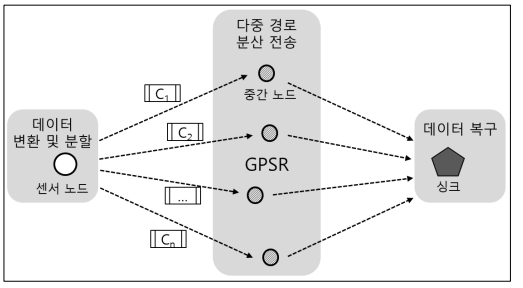


그림 3. 제안하는 기법

1단계는 데이터를 단 방향 해쉬 함수인 MD5 알고리즘을 이용하여 데이터를 변환하고 분할 처리하는 과정이다. [표 1]는 주어진 데이터 구조를 나타낸다. 이 데이터는 해쉬 함수 MD5에 의해 고정된 길이(128비트)로 변환된다.

표 1. 데이터 구조

ID	*x*	*y*	*온도*	*습도*

예를 들어 ID가 Sen_1_22 이고, x좌표 값이 73, y좌표 값이 493, 온도가 23, 습도가 42로 주어졌다고 할 때, 전체 데이터는 [Sen_1_22, 73, 493, 23, 42]이고, MD5 변환 값은 [ac237b3ce685e55b4ee37e9880529643]로 나타

난다. 데이터 변환 과정을 마친 변환 데이터는 분산 전송을 하기 위한 전처리 과정을 수행하게 된다. MD5를 통해 변환된 데이터 값은 임의의 수 2^n개로 분할된다. 이때의 n값은 임의의 값으로 사용자의 정의에 의해 결정된다. 분할한 변환 데이터는 기지국에 전송 된 후 복구된다. 이때, 데이터 복구를 위해 분할 데이터의 순서 정보가 요구된다. 따라서 순서 정보와 오류 검출을 위한 패리티 비트를 전송 데이터에 추가 한다. 1단계 과정을 모두 마친 데이터는 [표 2]의 데이터 구조와 같이 나타난다.

표 2. 전처리 과정 후 전송 데이터 구조

순서 정보	*분할된 MD5 변환 값*	*패리티 비트*

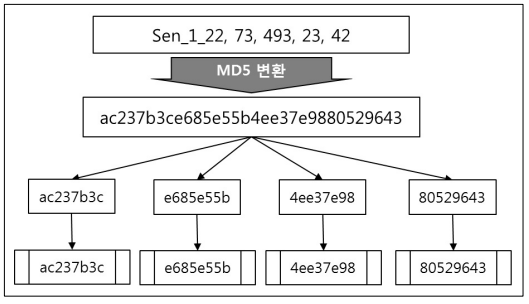


그림 4. 데이터 처리 및 분할

[그림 4]는 위의 예제를 이용하여 데이터 처리 단계를 도식적으로 나타낸다. 2단계는 데이터를 기지국으로 전송하는 과정이다. 이 단계에서는 데이터를 서로 다른 경로를 통해 전송하기 위해 중간 노드의 개념을 사용한다[13]. 분할 데이터가 같은 경로를 통해 전송되고 인근 경로 상에 악의적인 노드가 배치 될 경우 다수의 데이터가 노출될 가능성이 있기 때문에 랜덤 분산 전송을 사용하여 전체 데이터 노출을 방지한다.

분산 전송을 위해 분할 데이터가 서로 다른 위치의 중간 노드를 경유하게 하여 다중 경로를 통해 기지국으로 전송한다. 각 센서 노드는 자신과 기지국의 좌표 값을 알고 있고, 그 값을 이용해 자신과 기지국의 중심 좌표를 계산한다. 계산된 값을 기준으로 하여 중심 좌표와의 거리가 일정 범위(α, β)에 포함되는 중간 좌표 범위를 산출한다. 여기에서 α, β 값은 중간 좌표 범위의 설정 값으로 네트워크의 크기나 보안성을 고려하여 결정되는 임의의 값이다. 중간 좌표 범위 안에서 2^n개의 좌표를 산출한다. 소스 노드에서는 중간 좌표 정보를 통해 분할 데이터를 각각 다른 경로로 전송한다. 위에서 설명한 2^n개의 중간 좌표 선정 방법은 아래 식 (1)-(3)와 같이 나타난다.

$$\text{중심 좌표} = \left(\frac{\text{싱크 } x\text{좌표} + \text{소스 } x\text{좌표}}{2}, \frac{\text{싱크 } y\text{좌표} + \text{소스 } y\text{좌표}}{2}\right) \quad (1)$$

$$\text{중간좌표} = Random(\text{중간 좌표 범위}, 2^n) \quad (2)$$

$$\text{중간 좌표 범위} = \begin{cases} x\text{범위} = \text{중심 } x\text{좌표} \pm \alpha \\ y\text{범위} = \text{중심 } y\text{좌표} \pm \beta \end{cases} \quad (3)$$

위의 식을 통해 산출된 중간 좌표에 가장 인접한 노드가 중간 노드가 된다. 소스 노드에서는 중간 좌표 정보를 이용하여 분할 데이터를 전송하게 되고, 데이터가 중간 노드에 도달하면 중간 노드부터는 싱크의 좌표 정보를 이용하여 전송한다. 데이터 분산 전송 과정은 [그림 5]와 같이 나타난다.

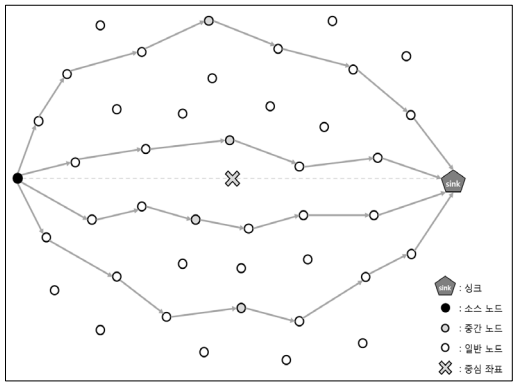


그림 5. 분산 전송 기법

센서 노드에서 중간 노드, 중간 노드에서 기지국으로의 데이터 전송은 모두 GPSR 기법을 기반으로 수행한다.

기지국에 전송된 데이터는 3단계를 통해 원래 데이터로 복구된다. 데이터의 순서와 상관없이 수신되는 데이터를 순서 정보에 의해 순서대로 배치하고, 분할된 변환 값만을 추출하여 병합한다. MD5로 변환한 데이터는 복구를 위해 매칭 복호화 과정을 수행하여 원본 데이터로 복구한다. [그림 6]은 위의 예제를 이용하여 데이터 복호화 과정을 나타낸 것이다.

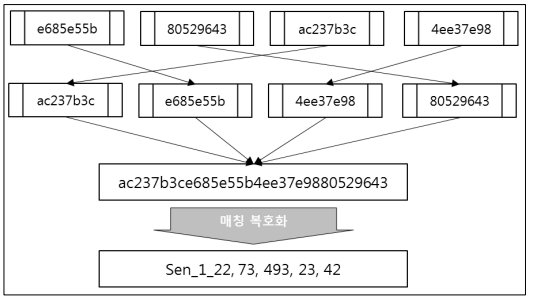


그림 6. 데이터 복호화

단-방향 해쉬 함수는 복호화 알고리즘이 존재하지 않기 때문에 데이터 매칭을 통해 데이터를 복구하게 된다. 하지만 데이터를 매칭하는 과정에서 원래 데이터를 찾기 위해 수많은 데이터를 발생시켜 MD5값으로 변환한 후 원본 데이터의 MD5 값과 일일이 매칭 해봐야 하기 때문에 이로 인한 부하가 발생한다. 이와 같은 부하를 줄이기 위해서 환경 정보는 일반적으로 일정 범위 내에서만 발생한다는 특징을 이용한다. 각 속성 값에 범위를 정하여 데이터 발생 경우의 수를 줄여 줌으로써 매칭 연산량을 줄인다. 또, 빈번하게 발생하는 값들은 저장소에 따로 저장하여 그 값을 먼저 매칭 해봄으로써, 더 빠른 복구 과정을 수행하는 것이 가능하다.

IV. 제안하는 기법의 보안 분석

보안 기법은 보안성에 대한 성능 평가가 어렵다. 따라서 제안하는 기법의 보안성에 대한 분석을 수행한다. 제안하는 기법에서 사용하는 MD5는 단-방향 해쉬 함수이다. 해쉬 함수에서 사용되는 해쉬 코드는 다음 식과 같은 함수 H 에 의해서 만들어진다[14].

$$h = H(M) \quad (4)$$

여기서 M은 가변 길이의 메시지이다. 해쉬 함수의 목적은 원래 데이터의 지문을 만드는 것으로, 메시지 인증에 주로 사용된다. 따라서 해쉬 함수 H는 다음과 같은 특징을 가져야 한다. 첫째, $H(x)$는 주어진 x에 대해서 계산하는 것이 비교적 쉽다. 둘째, 어떤 주어진 코드 m에 대해서 $H(x) = m$인 x를 찾는 것은 계산적으로 실행 불가능하다. 셋째, 어떤 주어진 블록 x에 대해서 $H(y) = H(x)$인 y, x를 찾는 것이 계산적으로 실행 불가능하다. 넷째, $H(x) = H(y)$인 어떤 (x, y)짝을 찾는 것이 계산적으로 불가능하다.

이와 같은 특징을 고려하여 개발된 MD4 해쉬 함수는 통상적인 해쉬 함수의 안전성을 확보하고 있지만 그 알고리즘이 해독되어 MD5가 개발되었다. MD5는 대문자와 소문자, 띄어쓰기 공백과 같이 아주 작은 차이에 대해서도 MD5 값이 전혀 다른 값으로 변환된다. 따라서 데이터에 대한 패턴을 파악하기 어렵기 때문에 암호화 기법과 같이 사용될 수 있다. 또, MD5의 알고리즘은 복호화 알고리즘 자체가 아예 존재 하지 않기 때문에 데이터 해독에 많은 시간에 걸린다. 웹상에 MD5 복호화 기능을 제공하는 많은 페이지가 존재하는데, 이는 단지 기존의 MD5 암호화에서 변환한 데이터를 저장하고 이를 바탕으로 비교 연산을 수행하여 일치하는 데이터의 존재 시에 결과를 보여주는 형식이다. 실제로 다른 MD5 복호화 알고리즘으로 변환한 MD5값을 복호화 페이지에 입력 값으로 넣으면 데이터를 찾지 못한다.

컴퓨터 성능의 발전으로 기존의 알고리즘이 점차 풀리고 있는 상황에서 MD4는 아주 간단하게 원본 메시지 값을 알아낼 수 있게 되었다[15]. MD5 역시 펜티엄급 컴퓨터에서 연립 방정식을 이용하여 충분한 시간만 주어진다면 인위적으로 풀어낼 수 있다. 또, 인위적이 아니더라도 비밀번호와 같은 8자리 정도의 숫자를 해쉬 한 값들은 이미 단순한 반복 대입에 의해 어느 정도 무력화되어 있다. 대소문자 52자, 특수문자 30자 정도가 대부분의 시스템이 사용하고 있는 비밀번호 집합이며, 2,044,140,858,654,976 정도의 조합이 나타난다. 이 숫자의 절반이 기대 값이므로, 만약 초당 1백만 번 MD5 연

산이 가능하다면 단순한 대입으로도 8개월 내에 비밀번호를 해독할 수 있다. 더구나, 가능성이 높은 비밀번호 위주로 조합한다면 이보다 훨씬 짧은 시간 내에 알고리즘을 깰 수 있다. 하지만 데이터를 해독하는데 엄청난 시간이 소요 되고, 유출되었던 비밀번호 값이 제한된 데이터 길이를 가진다는 점을 고려해 보면, 비밀번호보다 길이가 긴 다른 데이터에 대한 해독은 더 어려울 것이다.

특히 우리가 사용할 데이터는 길이가 제한되어 있지 않고, 속성 값이 센서에 장착된 모듈에 따라 발생하기 때문에 더욱 해독하기 어렵다. 뿐만 아니라, 더 높은 보안성을 위해 MD5값을 분할하여 전송하기 때문에 만약에 데이터가 노출이 되었더라도 모든 분할 데이터를 획득하지 못하면 원본 데이터는 해독이 불가능하다.

V. 성능 평가 및 분석

1. 성능 평가 환경

본 논문에서는 시뮬레이션 실험을 수행하여 기존 보안 기법인 TESP[2]을 본 논문에서 제안하는 기법과 시뮬레이션을 통해 결과를 비교 분석 하였다. 제안하는 기법의 성능을 평가하기 위해 기존 기법과 제안하는 기법에 대해 에너지 효율 측면에서 성능을 비교하였다. 센서 네트워크는 400m×400m ~ 1200m×1200m의 정사각형 형태를 가진다. 가로의 길이를 W미터, 세로 길이를 H미터라고 할 때, 센서 네트워크에 존재하는 노드의 개수 N은 $N = W \times H$ 개로 나타난다. 센서 네트워크상에 N개의 노드를 무작위로 배치하여 구성하고, 기지국은 전체 네트워크의 오른쪽 중간에 위치한다.

각 센서 노드들은 통신 반경 내의 이웃 노드들과 서로 통신할 수 있으며, 통신은 무 손실 통신을 가정한다. [표 3]은 실험에 사용된 기반 환경을 나타낸다. 실험은 다양한 센서 네트워크의 크기를 기준으로 진행하였으며, 전체 배포된 센서 노드의 개수는 네트워크의 크기에 따라 400개에서 3600개 사이 값으로 값을 변화시키면서 성능 평가를 수행하였다. 라우팅 시뮬레이션은 400개의 센서 노드가 배포된 환경을 기준으로 수행하였다. 센서 노드의 데이터 전송 크기는 4바이트로 가정하였고, 각 센서 노드의 통신 반경은 35m로 가정하였다.

표 3. 성능 평가 파라미터 및 값

파라미터	값
센서 네트워크 크기 (m)	400x400 ~ 1200x1200
센서 개수 (개)	400 ~ 3600
센서 통신 반경 (m)	35
데이터 전송 크기 (Byte)	4

본 논문에서 사용하는 에너지 소모 모델은 아래와 같은 모델을 사용하였다.

$$R_{cost} = 50 \times 0.000000001\,[J]$$
$$T_{cost} = 50 \times 0.000000001\,[J]$$
$$T_{amp} = 0.0013 \times 0.000000000001\,[J]$$

$$Receive_{cost} = MSG_{size} \times R_{cost} \quad (5)$$

$$Trans_{cost} = MSG_{size} \times (T_{cost} + T_{amp} \times T_{dist}{}^2) \quad (6)$$

2. 시뮬레이션 결과

[그림 7]은 제안하는 기법을 가상 환경에서 수행한 시뮬레이션 결과이다. 네트워크의 전체 센서 노드 수는 400개로 수행하였다. 다음 절에 서술한 에너지 소모량 시뮬레이션 환경은 전체 노드 수가 1600~2500개인 환경에서 수행 하였지만, 분산 라우팅 결과를 표현하기 위해 400개로 수행하였다. 왼쪽에 있는 삼각형이 센싱 데이터를 전송할 소스 노드, 중간 4개의 원 안에 해당하는 노드가 중간 노드, 오른쪽에 사각형이 기지국을 각각 나타낸다. X 표시는 소스 노드와 기지국의 좌표를 이용하여 계산한 중심 좌표 값이다. 소스 노드로부터 센싱된 데이터는 임의의 중간 노드를 경유하여 기지국으로 전송된다.

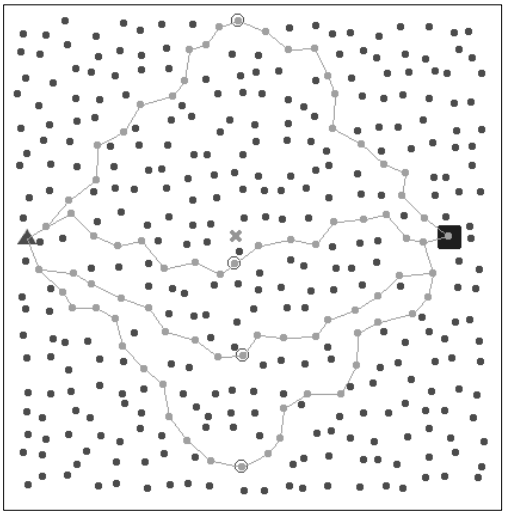
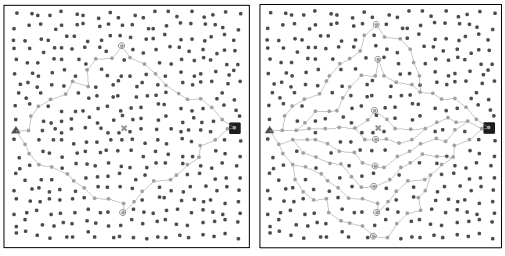


그림 7. 제안하는 기법의 라우팅 시뮬레이션

[그림 7]은 네트워크의 전체 노드 수가 400개 일 때, 중간 노드의 수 2^n에서 n(n=1,2,3, …)의 값을 변화시키면서 라우팅 시뮬레이션 결과를 살펴 본 것이다. [그림 8]-a는 n이 1일 때, [그림 8]-b는 n=3일 때의 결과이다. n=2일 때의 결과는 [그림 7]과 같이 나타난다.



a. 중간 노드 수 : 2개 b. 중간 노드 수 : 8개

그림 8. 중간 노드 개수에 따른 시뮬레이션 결과

[그림 9]는 n=4일 때 즉, 중간 노드 개수가 16개일 때의 결과이다. [그림 7]이나 [그림 8]과 같은 크기의 시뮬레이션 환경에서는 중간 노드의 수가 16개일 때의 라우팅 결과를 제대로 표현하지 못하여, 전체 노드 수가 1000개인 환경에서 수행하였다.

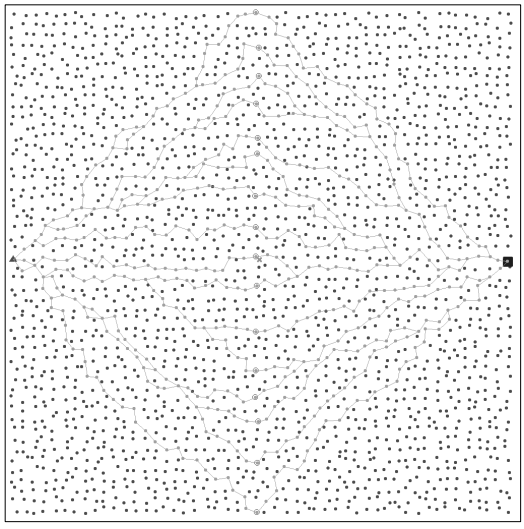


그림 9. 중간 노드 수 : 16개

3. 성능 평과 결과

[그림 10]은 수행 기법에 따른 데이터 전송 시에 소모된 에너지를 나타낸 결과이다. TESP[2]는 클러스터 환경을 기반으로 하여 데이터를 ECC로 암호화 하여 클러스터 헤더 노드를 통해 전송한다. 제안하는 기법은 다중 경로로 분산 전송을 사용함에도 기존 기법에 비해 소모 에너지가 적다. 기존 기법의 경우 거짓 데이터의 전송으로 인한 에너지 소모가 발생하고 소스 노드 데이터의 보안을 위해 클러스터 헤더를 사용함으로써 클러스터를 구축하는 과정에서 메시지 송수신으로 인해 에너지 소모가 크다.

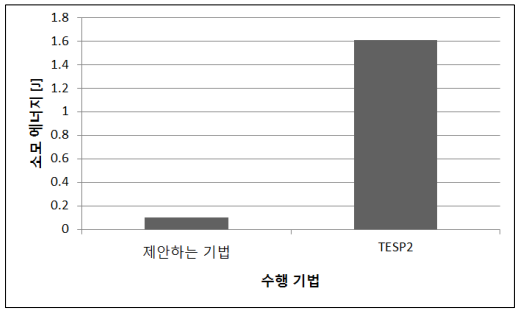


그림 10. 수행 기법에 따른 에너지 소모량 비교

[그림 11]은 센서 네트워크를 구성하는 노드 수에 따른 데이터 전송 시에 소모된 통신 에너지를 나타낸 결과이다. 제안하는 기법은 GPSR을 기반으로 데이터를 전송하기 때문에 센서 노드의 수가 증가할수록 목적지로 가는 센서 노드의 수가 늘어나기 때문에 소모되는 에너지가 점차 증가한다. 기존 기법의 에너지 소모량은 어떤 클러스터 기법을 사용하느냐에 따라 결과가 달라질 수 있다. 성능 평가 결과, 제안하는 기법이 기존 기법의 약 6%의 에너지만 소비하였다.

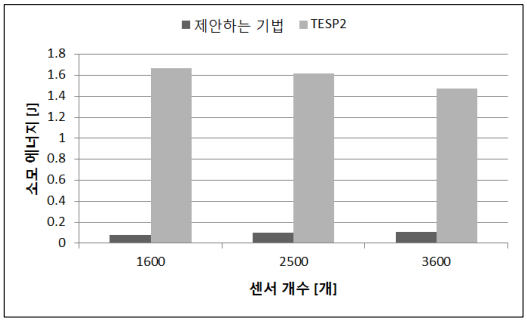


그림 11. 센서 노드 수에 따른 에너지 소모량 비교

VI. 결론

본 논문에서는 기존에 제안된 보안 기법의 문제점을 해결하는 새로운 보안 기법을 제안하였다. 기존 기법의 경우 데이터 보안을 위해 이웃 노드와의 통신이 과도하게 사용되는 문제점이 있다. 또한, 불필요한 정보의 전송으로 인한 에너지 소모가 발생한다. 이러한 문제점을 해결하기 위해 본 논문에서 단-방향 해쉬 함수 기반 다중 경로 보안 전송 기법을 제안하였다. 제안하는 기법에서는 GPSR을 기반으로 데이터를 전송하기 때문에 이웃 노드와의 통신을 최소로 사용한다. 또한, 해쉬 함수를 이용하여 실제 데이터의 크기와 관계없이 전송되는 데이터 크기가 일정하기 때문에 실제 데이터의 크기가 커지더라도 센서에서의 통신량에는 영향을 미치지 않는다. 뿐만 아니라, 데이터를 분할하여 전송함으로써 에너지를 효율적으로 사용하면서 보안성을 강화하였다. 성능 평가 결과, 제안하는 기법이 기존 기법의 약 6%의 에너지만 소비하였다. 향후 연구로는 MD5 데이터를 효율적으로 복구하기 위한 복구 알고리즘과 악의적인 센서 노드에 의한 데이터 변경 인지 및 처리 기법에 대하여 추가적인 연구를 진행하는 것이다.

참 고 문 헌

[1] Telecommunications Technology Associations, *Security Requirements for USN services*, 2009. (in Korean)

[2] 박준호, 여명호, 성동욱, 권현호, 이현정, 유재수, "센서 네트워크 환경에서 가상 식별자를 이용한 에너지 효율적인 다중 경로 데이터 라우팅 기법", *한국콘텐츠학회논문지*, 제11권, 제7호, pp.70-79, 2011.

[3] 성동욱, 이윤정, 박준호, 유재수, "무선 센서 네트워크 환경에서 반발력 기반 고-신뢰 데이터 라우팅 기법", *한국컴퓨터종합학술대회 논문집*, 제38권, 제1호(D), pp.171-174, 2011

[4] 황정연, "암호 프로토콜", *한국물리학회 특집호*, 제16권, 제3호, pp.17-21, 2007.

[5] R. Lu, X. Lin, H. Zhu, and X. Shen, "TESP^2: Timed Efficient Source Privacy Preservation *Scheme for Wireless Sensor Networks,*" *Proc. of the IEEE International Conference on Communications(ICC'10)*, pp.105-110, 2010.

[6] P. Samundiswary, D. Sathian, and P. Dananjayan, "Secured Greedy Perimeter Stateless Routing for Wireless Sensor Networks," *International Journal of Ad Hoc, Sensor & Ubiquitous Computing (IJASUC)*, Vol.1, No.2, pp.9-20, 2010.

[7] R. Rivest, "The MD5 Message-Digest Algorithm," *MIT Laboratory for Computer Science and RSA Data Security Inc.*, 1992.

[8] B. Karp and H. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," *Proc. of the 6th Annual International Conference on*

Mobile Computing and Networking(MobiCom '00), pp.243-254, 2000.

[9] A. Pirzada and C. McDonald, "Establishing Trust In Pure Ad-hoc Networks," *Proc. of Australasian Conference on Computer Science (ACSC)*, Vol.26, pp.47-54, 2004

[10] A. Pirzada and C. McDonald, "Trusted Greedy Perimeter Stateless Routing," *Proc. of the ICON*, pp.206-211, 2007.

[11] http://mytears.org/resources/doc/Encode/md5.html.

[12] 김재현, 김석규, 이재용, "무선 센서 네트워크에서의 에너지 효율성을 고려한 MAC/라우팅 프로토콜", *전자공학회지*, 제32권, 제7호, pp.57-73, 2005.

[13] Y. Li and J. Ren, "Source-Location Privacy through Dynamic Routing in Wireless Sensor Network," *Proc. of IEEE International Conference on Computer Communications (INFOCOM '10)*, pp.1-9, 2010.

[14] 우찬일, 김범식, "MD5 해쉬 함수와 대칭형 암호 시스템을 이용한 인증용 디지털 워터마킹", *전자공학회논문지*, 제41권(TE), 제3호, pp.95-101, 2004.

[15] 윤현경, 김완경, 소우영, "MD5와 Crypt를 이용한 안전한 웹 인증 시스템의 설계 및 구현", *한국멀티미디어 학회 춘계 학술 발표 대회 논문집*, pp.87-90, 2004.

저 자 소 개

이 윤 정(Yunjeong Lee) 준회원

- 2011년 2월 : 충북대학교 정보통신공학과 (공학사)
- 2011년 3월 ~ 현재 : 충북대학교 정보통신공학과 석사과정

<관심분야> : 무선 센서 네트워크, 네트워크 보안, 데이터베이스 시스템, 위치 기반 서비스, 클라우드 컴퓨팅 등

김 동 주(Dongjoo Kim) 준회원

- 2011년 2월 : 충북대학교 정보통신공학과(공학사)
- 2011년 3월 ~ 현재 : 충북대학교 정보통신공학과 석사과정

<관심분야> : 무선 센서 네트워크, 데이터베이스 시스템, 클라우드 컴퓨팅 등

박 준 호(Junho Park) 정회원

- 2008년 2월 : 충북대학교 정보통신공학과(공학사)
- 2010년 2월 : 충북대학교 정보통신공학과(공학석사)
- 2010년 3월 ~ 현재 : 충북대학교 정보통신공학과 박사과정

<관심분야> : 무선 센서 네트워크, 데이터베이스 시스템, RFID, 차세대 웹, LMS/LCMS, 바이오인포매틱스 등

성 동 욱(Dong-ook Seong) 정회원

- 2005년 2월 : 충북대학교 정보통신공학과(공학사)
- 2007년 2월 : 충북대학교 정보통신공학과(공학석사)
- 2011년 2월 : 충북대학교 정보통신공학과(공학박사)
- 2011년 3월 ~ 현재 : 한국과학기술원 전산학과 연수연구원

<관심분야> : 무선 센서 네트워크, 데이터베이스 시스템, FLASH 메모리 저장 시스템, LCMS/LMS, 위치 기반 서비스 등

유 재 수(Jaesoo Yoo) 종신회원

- 1989년 2월 : 전북대학교컴퓨터공학과(공학사)
- 1991년 2월 : 한국과학기술원 전산학과(공학석사)
- 1995년 2월 : 한국과학기술원 전산학과(공학박사)
- 1995년 3월 ~ 1996년 8월 : 목포대학교 전산통계학과 (전임강사)
- 1996년 8월 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 및 컴퓨터정보통신연구소 교수

<관심분야> : 데이터베이스시스템, 정보검색, 센서네트워크 및 RFID, 멀티미디어데이터베이스, 분산객체컴퓨팅, 바이오 인포매틱스 등