무선 센서 네트워크에서 데이터 무결성을 보장하기 위한 다중 해쉬 체인 기법

박길철* · 정윤수** · 김용태*** · 이상호****

A Multi-hash Chain Scheme for Ensure Data Integirty Nodes in Wireless Sensor Network

Gil-Cheol Park* · Yoon-Su Jeong** · Yong-Tae Kim*** · Sang-Ho Lee****

이 논문은 2010년도 한남대학교 학술연구조성비 지원에 의하여 연구되었음.

요 약

최근 무선 센서 네트워크에서는 센서 노드의 에너지 소모뿐만 아니라 센서 노드에서 수집된 데이터의 무결성을 보장하기 위한 연구가 진행되고 있다. 그러나 기존 연구에서는 센서 노드로부터 데이터를 병합하는 클러스터 헤드의 오버헤드 및 데이터의 무결성을 보장하지 못하고 있다. 이 논문에서는 센서 노드로부터 전달된 데이터를 클러스터 헤드가 병합할 때 클러스터 헤드의 오버헤드를 줄이고 병합된 데이터의 무결성을 보장하기 위한 다중 경로 해쉬 체인 기법을 제안한다. 제안된 기법은 데이터 병합시 클러스터 헤드의 데이터 무결성을 보장하기 위해서 주경로와 보조경로로 나누어 다중 해쉬 체인을 형성한다. 주경로 이외에 사용되는 보조 경로는 센서 노드의 인증 시 클러스터 헤드의 오버헤드를 최소화하면서 센서 노드의 무결성을 지원한다.

ABSTRACT

Recently, In the wireless sensor network, a study which guarantees integrity of not only data gathered from sensor node but also energy consumption of it is now going on. However, the existing study cannot guarantee data integrity and overhead of cluster head which merges data from sensor node. This paper proposes multi-path hash chain technique which guarantees integrity of merged data and reduces overhead of cluster head when cluster head merges with data transmitted from sensor node. The proposed technique forms multi-hash chain dividing main-path and assistance-path to guarantee data integrity of cluster head, when merges data. The assistance-path ,which is used when main-path is not, supports integrity of sensor node while minimizing overhead of cluster head when sensor node is authenticate.

키워드

무선 센서 네트워크, 다중해쉬체인, 데이터 무결성

Key Word

wireless sensor network, multi-hash chain, data integrity

* 한남대학교 공과대학 멀티미디어학부 교수(제1저자)
** 한남대학교 산업기술연구소 전임연구원 (교신저자, bukmunro@gmail.com)
*** 한남대학교 공과대학 멀티미디어학부 교수
**** 충북대학교 전자정보대학 컴퓨터공학부 교수

접수일자 : 2009. 12. 31
심사완료일자 : 2010. 06. 28

Ⅰ. 서 론

최근 저 전력 통신과 관련된 무선 센서 네트워크는 다양한 센서와 접목하여 낮은 에너지 소비(low-power)와 저비용(low-cost)을 목적으로 개발되고 있으며, 그 응용 범위가 군사적인 목적에서부터 환경/생태 감시 분야, 에너지 관리 분야, 물류/재고 관리 분야, 전투지역 관리 분야, 의료 모니터링 분야, 보안, 헬스케어 등의 응용 분야까지 크게 확장되고 있어 무선 센서 네트워크의 이용성과 중요성이 대두되고 있다[1].

무선 센서 네트워크에서는 수 많은 센서 노드들이 미리 결정된 형태없이 배치될 수 있고 근접한 센서 노드들이 유사한 정보를 감지하는 특성에 의해 임의의 센서 노드의 동작이 실패하거나 기능이 소멸되는 경우에도 네트워크의 전체적인 동작에는 영향을 미치지 않는 장점이 있다. 그러나 무선 센서 네트워크는 무선 매체의 저속, 오류가 심한 전송 특성 및 제한된 전원 공급, 센서 노드의 임의 배치로 인한 교체 불가능 등의 문제점을 가진다. 이러한 무선 센서 네트워크의 문제점을 해결하기 위해서는 센서 노드의 에너지 소비를 네트워크 전체에 분산시켜 전체적 시스템의 수명을 증가시키는 방향으로 설계되어야 하며, 센서 네트워크의 동적인 변화에 빠르게 대응하여 수집된 정보를 안전하게 전달할 수 있어야 한다[2,3].

또한, 무선 센서 네트워크가 신뢰할 수 없고, 위험 환경에 노출되고 있으나 기존 데이터 병합 기법은 센서 노드와 베이스 스테이션 종단간 데이터 프라이버시(데이터 기밀성 및 무결성)를 제공하지 못하는 문제점이 있다.

이 논문에서는 데이터 병합시 수집된 데이터의 무결성을 보장하기 위한 다중 경로 해쉬 체인을 제안한다. 제안된 기법은 데이터 병합시 클러스터 헤드의 오버헤드를 최소화하기 위해서 주경로와 보조경로로 나누어 다중 해쉬 체인을 형성한다. 또한, 제안 기법에서 주경로 이외에 사용되는 보조 경로는 클러스터의 오버헤드를 최소화하면서 센서 노드의 인증 및 무결성을 지원한다.

이 논문의 구성은 다음과 같다. 2장에서는 해쉬 체인 기법과 기존 데이터 병합 기법에 대해서 분석한다. 3장에서는 다중 경로 해쉬 체인 기법을 제시하고, 4장에서는 제안 기법의 성능평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

Ⅱ. 관련 연구

2.1 해쉬 체인

해쉬체인은 랜덤한 seed를 이용하여 연속적으로 해쉬값을 계산하여 생성하는 기법으로써 one-time passwords의 효율적인 인증을 Lamport가 처음 제안하였다[4]. 해쉬 체인은 seed가 s이면 길이가 n인 해쉬체인을 생성하기 위해서 (식 1)과 같이 계산된다.

$$c_n = H(s),\ c_{n-1} = H(H(s)),\ ...,\ c_1 = H^n(s),$$
$$c_0 = H^{n+1}(s) \qquad \text{(식 1)}$$

여기서 $c_{n-i+1} = H^i(s)$는 s를 i번 해쉬한 값을 의미하고 $c_0 = H^{n+1}(s)$는 해쉬체인의 루트 값을 의미한다.

해쉬체인은 해쉬함수의 일방향 특성 때문에 $H^i(s)$를 알고 있어도 $H^{i-1}(s)$는 계산할 수 없다. 하지만 $H^i(s)$를 알고 있으면 $H^{i-1}(s)$의 유효성은 한번의 해쉬연산을 통해 확인할 수 있다.

2.2 기존 연구

무선 센서 네트워크에서 안전하게 데이터를 병합하기 위한 알고리즘은 다양한 방법으로 연구되고 있다. 데이터 병합 기법은 무선 센서 네트워크에서 센서 노드가 데이터를 전송할 때 소요되는 에너지를 줄이기 위한 기법 중에 하나이다. 그러나 기존 데이터 병합 연구는 센서 노드와 베이스 스테이션 종단간 데이터 프라이버시를 제공하지 못하고 있어 암호화 기법이 데이터 병합에 접목되어 연구되고 있다.

Peter et al.[5]은 무선 센서 네트워크에서 데이터를 숨긴 병합 기법을 제안하였다. 이 기법은 동형 수집 속성을 추가한 3가지 암호 알고리즘기술을 사용하여 데이터의 기밀성을 보장하고 있지만 데이터를 숨길때마다 난수의 사용이 증가하는 단점이 있다.

Girao et al.[6]은 Domingo-Ferrer로 불리우는 대칭 암호시스템을 기반으로 한 덧셈과 곱셈의 연산을 수행하는 동형 병합 기법을 제안했다. 그러나 Domingo-Ferrer 기법[7]은 대칭이기 때문에 이 시스템을 WSN에 배치할 때 정보는 쉽게 노출될 수 있는 단점이 있다. Mykletun과 Girao[8]는 감처진 데이터를 동형으로 수집할 수 있는 공개 키 기법을 제시하였고 병합 방법은 덧셈이나 곱셈의 단일 연산만을 사용했다.

Ⅲ. 다중 경로 해쉬 체인을 이용한 데이터 병합 기법

이 절에서는 데이터 병합을 수행하는 클러스터 헤드의 오버헤드를 줄이면서 센서 노드의 인증 및 무결성을 보장하기 위한 다중 경로 해쉬 체인을 이용한 데이터 병합 기법을 제안한다.

3.1 용어 정의

제안 기법에서 사용하는 주요 용어를 정의하면 표 1과 같다.

표 1. 제안 메커니즘의 용어 정의
Table 1. Parameter of Proposed Mechanism

Notaion	Definitions
n	해쉬 체인 길일
k_n	주 경로에서 생성되는 해쉬 체인 키
x_n, y_n	보조 경로에서 생성되는 해쉬 체인 키
‖	연접(concatenate) 연산

3.2 네트워크 모델

제안 기법의 네트워크 모델은 그림 1과 같이 베이스 스테이션, 클러스터 헤드, 센서 노드로 구성된다.

네트워크에 배치된 센서 노드는 에너지가 남아있는 동안 센서 노드 자신의 위치를 유지한다. 센서 노드들은 클러스터 기반으로 네트워크를 구성되며 클러스터 헤드와 센서 노드간 거리는 1 홉으로 구성된다. 센서 노드로부터 수집된 데이터는 클러스터 헤드가 1차 수집하고 수집된 데이터는 클러스터 헤드가 베이스 스테이션에게 직접 전달하거나 인접한 클러스터에게 전달하여 베이스 스테이션에게 전달하도록 한다. 베이스 스테이션으로부터 멀리 떨어진 클러스터 헤드를 위해 그림 1에서는 멀티 홉 라우팅 기법을 통해 데이터를 포워드하며 각 클러스터의 데이터 수집 결과는 다중 경로 해쉬 체인을 이용하여 다른 중간 수집자에 의해 다시 수집하지 않고 베이스 스테이션에게 보내진다.

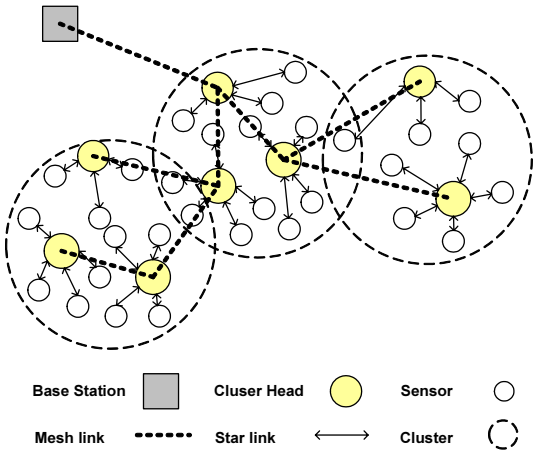

그림 1. 네트워크 모델
Fig 1. Network Model

3.3 다중 경로 해쉬 체인 기법

이 절에서는 무선 센서 네트워크에서 데이터 수집 역할을 수행하는 클러스터 헤드의 오버헤드를 최소화면서 센서 노드로부터 수집된 데이터의 병합을 효율적으로 수행하기 위한 다중 경로 해쉬 체인 기법을 제안한다. 제안 기법에서 데이터 병합시 클러스터 헤드의 오버헤드를 최소화하기 위해서는 경로를 주경로와 보조경로로 나누어 다중 해쉬 체인을 형성한다. 제안 기법에서 주경로 이외에 사용되는 보조 경로는 센서 노드의 인증 및 무결성을 위해 사용되며 이 때 보조 경로를 통해 생성된 해쉬 체인의 결과 값은 x_n과 y_n을 통해 센서 노드를 인증한다.

해쉬 체인의 길이를 n이라고 가정하면 생성자는 먼저 주 경로에서 사용할 랜덤 키 k_n을 생성한 후 2개의 보조 경로 x_n과 y_n을 n의 값이 짝수와 홀수일 경우로 나누어 주 경로와 XOR을 수행한다.

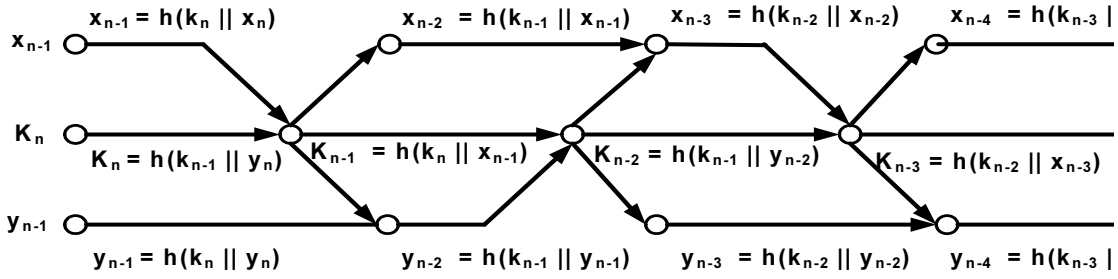

그림 2. 다중 경로 해쉬 체인
Fig 2. Multipash Hash Chain

이 때, x_n의 초기값은 k_{n+1}으로 할당하고, y_n의 초기값은 k_n과 동일하게 할당한다. 해쉬 함수에 사용되는 ‖는 연접(concatenate) 연산을 의미한다.

그림 2는 센서 네트워크의 임의 센서 노드에서 데이터를 병합하려고 할 때 데이터를 전달한 센서 노드의 인증과 무결성을 보장하기 위해 다중 경로 해쉬 체인으로 키를 생성하여 데이터를 병합할 수 있다. 그림 2와 같은 방법은 다중 경로 해쉬 체인을 수행함으로써 주경로와 보조경로를 사용하게 되는데 주 경로 k_n은 데이터 병합과 관련하여 데이터의 병합 유・무를 판단하는데 사용되며 보조 경로 x_{n-1}과 y_{n-1}은 데이터를 송・수신하는 노드들의 인증과 무결성을 판단하게 된다.

(식 1)은 데이터 병합을 수행하는 노드의 해쉬체인 값을 나타내고 있다. 이 때, 해쉬 체인 값은 n의 값에 따라 짝수인 경우에는 $h(k_{n-1} \| y_n)$와 같은 해쉬 값이 생성되고, 홀수인 경우에는 $h(k_n \| x_{n-1})$와 같은 해쉬 값이 생성된다.

$$k_n = \begin{cases} h(k_{n-1} \| y_n) & n\text{=짝수} \\ h(k_n \| x_{n-1}) & n\text{=홀수} \end{cases} \quad \text{(식 1)}$$

이 때, 보조 경로 x_n과 y_n은 (식 2)~(식 3)과 같이 $n-1$번째 키 값을 해쉬 함수에 적용한다.

$$x_n = h(k_{n-1} \| x_{n-1}) \quad \text{(식 2)}$$

$$y_n = h(k_{n-1} \| y_{n-1}) \quad \text{(식 3)}$$

생성자(generator)는 n의 값이 0일 될 때까지 다음의 4단계 처리과정을 반복적으로 수행한다.

• 단계 1 : 생성자는 송신 노드로부터 전달된 n의 값을 1씩 감소시킨다.

• 단계 2 : 송신 노드로부터 전달된 n의 값이 짝수일 경우 생성자는 $h(k_{n-1} \| y_n)$을 계산하고 홀수일 경우 생성자는 $h(k_n \| x_{n-1})$을 계산한다.

• 단계 3 : 이전 노드의 인증과 무결성을 체크하기 위해서 보조 경로 x_n 은 k_{n+1}를 해쉬함수에 적용한 값으로 계산한다.

$$x_n = h(k_{n+1}) \quad \text{(식 4)}$$

• 단계 4 : 생성자는 주 경로 k_n을 계산하기 위해서 보조 경로 y_n을 보조 경로 x_n으로 해쉬함수에 적용한 값으로 계산한다.

$$y_n = h(x_n) \quad \text{(식 5)}$$

Ⅳ. 평가

이 절에서는 제안 기법의 성능을 평가하기 위해 [9]에서 사용된 방법을 통해 해쉬 체인 키 길이에 따른 키의 변화수, 키의 평균변화 확률, 키의 변화에 따른 표준분산 그리고 표준 분산 확률에 대한 성능 평가를 수행한다.

4.1 실험 평가 항목

실험 평가를 위해 해쉬 체인에 대한 키 비트 수의 평균 변화, 평균 키 변화 확률, 키 비트 수의 표준 분산 그리고 평균 변화의 분산 확률 등의 4가지 항목을 사용한다. 실험 평가에 사용되는 4가지 항목은 [9]에서 사용된 내용을 기반으로 다음과 같이 정의한다.

$\overline{K}$는 해쉬 체인에서 변환된 평균 키 길이 수를 의미한다.

$$\overline{K} = \frac{1}{N}\sum_{i=1}^{N} K_i \qquad \text{(식 6)}$$

여기서 K_i는 i번째 해쉬 체인의 키 길이를 의미하고 N은 실험의 반복 횟수를 의미한다. P는 해쉬 체인에서 변환된 평균 키 변화 확률을 의미한다.

$$P = \frac{\overline{K}}{128} \times 100\% \qquad \text{(식 7)}$$

$\triangle K$과 $\triangle P$는 해쉬 체인에서 변환된 키 길이의표준분산 및 확률을 의미한다.

$$\triangle K = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(K_i - \overline{K})^2} \qquad \text{(식 8)}$$

$$\triangle P = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left(\frac{K_i}{128} - P\right)^2} \times 100\% \qquad \text{(식 9)}$$

4.2 실험 결과

그림 3은 센서 노드가 해쉬 체인 키 길이를 128 비트와 256 비트로 데이터를 클러스터 헤드에게 전달하였을 경우 클러스터 헤드가 데이터 병합을 수행할 때 발생하는 센서 노드 수 변화에 따른 클러스터 헤드의 오버헤드 변화율을 보여주고 있다. 그림 3의 결과처럼 키 길이에 따라 오버헤드의 크기는 다르지만 노드 수 증가에 따른 오버헤드의 변화는 노드 수가 작은 경우 오버헤드의 변화가 크지만 노드 수가 증가 할수록 오버헤드의 변화는 일정한 크기로 작게 증가하였다.

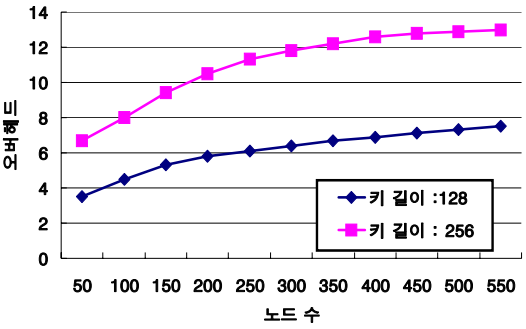

그림 3. 클러스터 헤드의 오버헤드
Fig 3. Overhead of Cluster Head

표 2는 센서 노드에서 클러스터 헤드까지 해쉬 체인의 생성자가 생성한 키의 길이가 변환될 경우 변환된 평균 키 길이의 수와 평균 키 변화 확률, 평균 키 변화 확률의 표준 분산 및 확률 등을 보여주고 있다.

표 2. 해쉬 값에 따른 키 길이의 변화율
Table 2. Number of changed key bit in hash values

평가항목 (Items)	키 길이				
	256	512	1024	2048	4096
$\overline{K}$	64.396	64.724	64.066	64.097	64.019
$P(\%)$	50.309	50.565	50.052	50.076	50.015
$\triangle K$	5.6124	5.3541	5.8421	5.7743	5.7114
$\triangle P(\%)$	4.5246	4.3015	4.7565	4.7072	4.6784

표 2의 결과처럼 키 길이에 따라 변환된 평균 키 길이의 수는 반복적으로 N번 실험을 반복하여도 64비트에

밀접하게 나타났으며 64비트에 해당하는 분산값은 매우 낮게 나타났다.

V. 결 론

무선 센서 네트워크에서 수집되는 데이터는 센서 노드로부터 클러스터 헤드가 데이터를 병합하여 싱크 노드에게 전달한다. 그러나 클러스터 헤드는 센서 노드로부터 중복되게 데이터를 수집하기 때문에 데이터 병합이 많아질수록 오버헤드 높아진다. 이 논문에서는 센서 노드로부터 전달된 데이터를 클러스터 헤드가 병합할 때 클러스터 헤드의 오버헤드를 줄이고 병합된 데이터의 무결성을 보장하기 위한 다중 경로 해쉬 체인 기법을 제안했다. 제안된 기법은 클러스터 헤드의 오버헤드를 줄이면서 병합된 데이터의 무결성을 보장하기 위해서 해쉬 체인을 주경로와 보조경로로 나누어 센서 노드의 인증 및 무결성을 지원한다. 실험 결과 해쉬 체인의 키 길이를 256, 512, 1024, 2048, 4096로 구분하여 N번 실험을 반복하여도 변환된 키 길이는 64비트에 부합되게 나타났으며 64비트에 해당하는 분산값 또한 매우 낮게 나타났다. 향후 연구에서는 제안된 기법을 실제 환경에 적용하여 실험된 결과가 동일한지에 대해서 연구를 계속 수행할 계획이다.

참고문헌

[1] N. Xu, S. Rangwala, K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, D. Estrin, “A Wireless Sensor Network for Structural Monitoring,” In Proceedings of the ACM Conference on Embedded Networked Sensor Systems, November 2004.

[2] 정윤수, 김용태, 박길철, 이상호, “WSN의 확장성과 에너지 효율성을 보장하는 라우팅 프로토콜”, 한국컴퓨터정보학회 논문지, pp. 105-113, 2008년 7월.

[3] 정윤수, 김용태, 박길철, 이상호, “노드간 에너지 소비를 효율적으로 분산시킨 PRML 메커니즘”, 한국해양정보통신학회 논문지, pp. 774-784, 2009년 4월.

[4] L. Lamport, ″Password authentication with insecure communication″, Communicatios of the ACM, vol. 24, no. 11, pp. 770-772, Nov. 1981.

[5] S. Peter, K. Piotrowski, P. Langendoerfer, ″On Concealed Data Aggregation for Wireless Sensor Networks″, Consumer Communications and Networking Conference, 2007.

[6] J. Girao, D. Westhoff, and M. Schneider, ″CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor networks″, International Conference on Communication(ICC2005), vol. 5, pp. 3044-3049, 2005.

[7] J. D. Ferrer, ″A Provably Secure Additive and Multiplicative Privacy Homomorphism″, In Information Security Conference, LNCS 2433, pp. 471-483, 2002.

[8] E. Mykletun, J. Girao, and D. Westhoff, ″Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks″, International Conference on Communications(ICC2006), vol. 5, p. 2288-2295, 2006.

[9] D. Xiao, X. F. Liao, and S. J. Deng, “One-way hash function construction based on the chaotic map with changeable-parameter”, Chaos, Solitons & Fractals, 2005, vol.24, no. 1, pp. 65-71. 2005.

저자소개

박길철(Gil-Cheol Park)

1983. 한남대학교 전자계산학과 학사.
1986. 숭실대학교 전자계산학과 석사.
1998. 성균관대학교 전자계산학과 박사.
2006. UTAS, Australia 교환교수
1998. 8.~ 현재 한남대학교 공과대학 멀티미디어학부 교수
2005. 2. 한국정보기술학회 이사 멀티미디어 분과 위원장

※관심분야 : multimedia and mobile communication, network security

정윤수(Yoon-Su Jeong)

1998. 청주대학교 전자계산학과 학사
2000. 충북대학교 대학원 전자계산학과 석사
2008. 충북대학교 대학원 전자계산학과 박사
2009.9 ~ 현재 한남대 산업기술연구소 전임연구원
※관심분야 : 유・무선통신보안, 암호이론, 정보보호, Network Security, 이동통신

김용태(Yong-Tae Kim)

1984. 한남대학교 계산통계학과 학사.
1988. 숭실대학교 전자계산학과 석사.
2008. 충북대학교 전자계산학과 박사.
2002. 12. ~2005.2 (주)가림정보기술 이사
2010.3 ~ 현재 한남대학교 공과대학 멀티미디어학부 교수
※관심분야 : 모바일 웹서비스, 정보 보호, 센서 웹, 모바일 통신보안

이상호(Sang-Ho Lee)

1976. 숭실대학교 전자계산학과 학사.
1981. 숭실대학교 전자계산학과 석사.
1989. 숭실대학교 전자계산학과 박사.
1981. 3. ~ 현재 충북대학교 전자정보대학 컴퓨터공학부 교수
※관심분야 : 네트워크보안, Protocol Engineering, Network Management