해쉬체인을 이용한 센서네트워크의 디지털서명 모델

김영수* · 조선구**

Digital Signature Model of Sensor Network Using Hash Chain

Young-soo Kim* · Seon-Goo Cho**

요 약

센서네트워크에서는 패킷 포워딩과 라우팅 기능을 전담하는 노드나 서버가 존재하지 않고 네트워크 통신에 참여하는 센서노드들이 이러한 기능을 수행한다. 따라서 센서노드들이 패킷 포워딩과 라우팅 과정에서 패킷의 위변조에 대한 공격이 취약하다. 이의 해결책으로 라우팅과 포워딩 메시지에 대한 인증과 무결성을 보장하는 보안기능이 요구된다. 이를 위해서 공개키기반 전자서명 모델에 비해서 디지털 서명을 생성하고 검증하는데 계산적인 부담이 적은 해쉬체인 기반 디지털서명 모델을 제안하고 연산횟수의 비교를 통하여 모델의 적합성을 검증하였다.

ABSTRACT

In sensor network there are no nodes or servers that are exclusively responsible for packet forwarding and routing. Instead, sensor nodes participating in network communications perform these activities. Thus, they are vulnerable to the alteration and forgery of message in the process of packet forwarding and routing. To solve this problem, a security to ensure authentication and integrity of routing and forwarding messages should be required. To do this, we propose the hash chain-based digital signature model where it takes less time to compute in generating and verifying the digital signature model, unlike the public key-based digital signature model, and verify if this model is proper by comparing computation times between tow models.

키워드

센서네트워크, 해쉬체인, 디지털 서명

Key word

Sensor Network, Hash Chain, Digital Signature

* 충북대학교 컴퓨터공학과

** 나사렛대학교 호텔관광경영학과

접수일자 : 2009. 09. 07

심사완료일자 : 2009. 10. 06

Ⅰ. 서 론

유비쿼터스 시대를 위한 기반기술로서 무선통신을 지원하는 센서네트워크의 중요성이 커지고 있다. 센서네트워크의 라우팅 프로토콜로서 클러스터링 기반 라우팅 프로토콜이 널리 사용되고 있다. 클러스터링 기반 라우팅 프로토콜은 센서네트워크를 클러스터라는 작은 영역으로 분할하고 각 클러스터에는 클러스터 헤드가 존재하여 클러스터 멤버인 센서노드로부터 데이터를 수집하고 이를 모아서 싱크노드로 전달하는 역할을 수행한다[1].

센서네트워크에서는 메시지의 라우팅과 포워딩을 전담하는 노드나 서버가 존재하지 않고 네트워크 통신에 참여하는 센서노드 가운데 클러스터 헤드로 선출된 노드가 이러한 기능을 수행한다. 이처럼 클러스터 헤드가 메시지의 라우팅과 포워딩을 동시에 수행하기 때문에 클러스터링 기반 라우팅 프로토콜은 인증과 무결성에 취약하다[2]. 악의적인 노드에 의한 라우팅과 포워딩 메시지의 위변조는 센서네트워크를 마비시킬 수 있고 센서네트워크의 기능을 심각하게 훼손할 수 있다. 따라서 라우팅과 포워딩 메시지에 대한 인증과 무결성을 보장하는 보안기능이 요구된다[3]. 공개키 기반 전자서명 모델은 서명을 생성하고 확인하는데 계산적인 부담이 높기 때문에 제한된 전력으로 운용되는 센서네트워크에서는 부적절하다[4]. 따라서 이의해결을 위해서 본 논문에서는 해쉬키 체인을 이용한 전자서명 모델을 제안한다. 해쉬키 체인을 이용한 전자서명 모델에서는 해쉬함수를 반복 적용하여 생성한 해쉬값을 체인화 함으로써 체인의 앞뒤에 있는 해쉬값을 서명과 검증을 위한 키로 사용한다.

본 논문은 다음과 같이 구성한다. 2절에서는 해쉬코드기반 메시지 인증모델과 공개키기반 디지털서명모델을 분석하고 3절에서는 해쉬체인기반 센서네트워크의 디지털서명 모델을 제안한다. 4절에서는 모델의 실용성을 검증하기 위하여 성능분석을 한다. 5절에서는 결론과 시사점을 기술한다.

Ⅱ. 공개키 기반 디지털서명 모델

2.1 해쉬코드기반 메시지 인증 모델

메시지 인증은 전달되는 메시지의 이상 유무를 확인할 수 있는 기능으로 전송중 발생할 수 있는 메시지 변경과 위조여부를 확인하는 기능이다. 수신자가 수신한 메시지가 송신자가 전송한 메시지와 동일한 메시지임을 확인할 수 있는 기능으로 전송중 메시지의 불법변경여부를 확인할 수 있다.

(그림 1)과 같이 일방향 해쉬함수로 생성한 메시지 압축기능을 갖고 있는 해쉬코드를 메시지에 부착해서 전송하면 이를 수신한 수신자는 메시지로부터 해쉬코드를 계산해서 수신한 해쉬코드와 비교해서 메시지 인증을 한다[5].

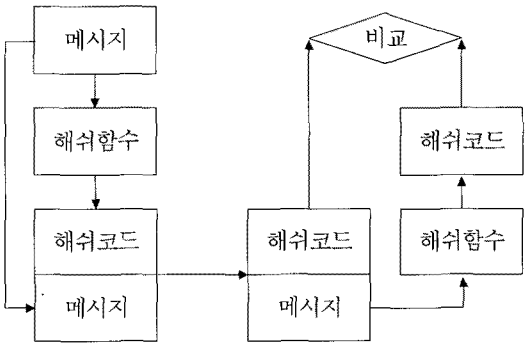

그림 1. 해쉬코드기반 메시지인증 모델
Fig. 1 Hash code based message authentication model

그러나 해쉬함수가 공개되어 있으므로 제삼자가 송신자로 가장하여 임의의 메시지를 정당한 메시지인 것처럼 인증을 하면 수신자는 검증시 제삼자의 위조인증임을 알수가 없다. 제삼자의 위조인증을 막기 위해서는 (그림 2) 같이 송신자와 수신자가 사전에 비밀정보를 교환해 갖고 있으면 쉽게 방지가 가능하다. 송신자는 인증하려는 메시지와 비밀정보를 연결한 후 해쉬함수에 입력해서 해쉬코드를 계산하여 수신한 해쉬값과 비교하여 메시지인증을 검증한다. 동일한 해쉬값을 갖는 경우 메시지의 변경이 없었음을 확신한다.

제삼자가 위조인증을 생성하려고 해도 송신자와 수신자 사이의 비밀정보를 모르기 때문에 수신자를 속일 수 있는 위조인증을 만들 수 없다[6].

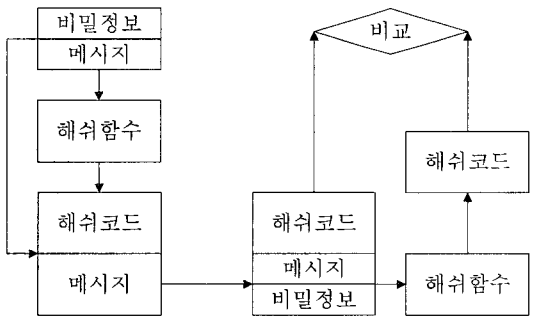

그림 2. 비밀정보기반 메시지인증 모델
Fig. 2 Secret-based message authentication model

2.2 공개키기반 디지털서명 모델

디지털 서명은 송신자가 보낸 메시지를 수신자가 송신자이외의 사람에 의해서 서명되지 않았음을 검증하는 메커니즘이다. (그림 3)와 같이 디지털서명방식은 송신자가 자신의 개인키를 사용하여 생성한 서명값을 전송하면 수신자는 수신자의 공개키를 사용하여 서명값을 복호화하여 검증한다[7]. 디지털 서명을 하는 경우에는 메시지에 직접 서명하는 것보다는 해쉬함수에 의해 구해진 해쉬코드에 서명하는 것이 서명을 위한 처리시간이 적게 소요된다.

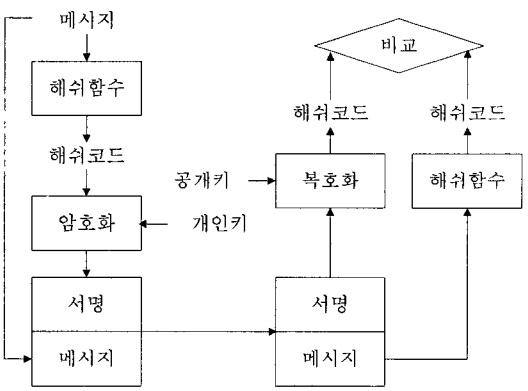

그림 3. 공개키기반 디지털서명 모델
Fig. 3 Public key based digital signature model

하지만 해쉬함수에 비해서 공개키 연산은 계산 부하를 유발하고 소요시간이 길다. 따라서 제한된 전력으로 운용되는 센서노드에게 이러한 공개키 연산은 부적절하다. 공개키기반 디지털서명은 서명을 생성하고 확인하는데 계산적인 부담이 높기 때문에 자원이 제약되어 있는 센서네트워크에서는 적합하지 않다[8].

Ⅲ. 해쉬체인기반 센서네트워크의 디지털서명 모델

3.1 클러스터기반 라우팅 프로토콜의 메시지 전송 모델

센서네트워크 라우팅 프로토콜의 하나인 클러스터기반 라우팅 프로토콜은 일련의 노드들을 하나의 클러스터 헤드와 다수의 클러스터 멤버로 이루어진 클러스터로 묶어 라우팅한다. (그림 4)와 같이 클러스터링 기반 라우팅 프로토콜은 센서네트워크를 클러스터라는 작은 영역으로 분할하고 각 클러스터에는 클러스터 헤드가 존재하여 클러스터 멤버인 센서노드로부터 데이터를 수집하고 이를 모아서 싱크노드로 전달하는 역할을 수행한다[9].

여기서 클러스터 헤드는 aggregation을 통하여 통신비용을 줄일 수 있는 구조를 말한다. 즉 각 노드들이 센싱한 정보를 자신이 속한 클러스터의 클러스터헤드로 보내면 클러스터 헤드는 노드들이 보내온 메시지를 집성하여 메시지의 사이즈를 줄이게 된다. 클러스터 헤드는 메시지의 라우팅과 포워딩을 동시에 수행하기 때문에 무결성에 취약하다. 악의적인 노드가 클러스터헤드를 공격해서 쉽게 라우팅과 포워딩 메시지를 변조해서 무결성을 손상시키는 위협에 노출되어 있다[10]. 이의 해결을 위한 공개키 기반 디지털서명은 계산비용이 비싸다는 점과 디지털 서명을 생성하고 검증하는 과정에 소요되는 시간이 크다는 단점을 가진다. 따라서 라우팅과 포워딩 메시지에 대한 인증과 무결성을 보장하는 보안기능이 요구된다[11]. 본 논문에서는 해쉬키 체인을 사용하는 디지털서명방식을 사용해서 이의 해결책을 제시한다.

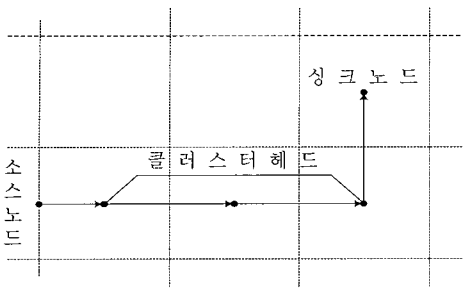

그림 4. 클러스터기반 메시지 전송 모델
Fig. 4 Cluster-based Message transit model

3.2 해쉬키체인 기반 전자서명 모델

일반적인 해쉬체인은 초기값을 기반으로 반복적인 일방향 해쉬함수를 적용하여 생성되는 값들의 체인을 의미한다. 해쉬키 체인은 (그림 5)와 같이 해쉬함수에 적용하여 얻은 값을 키로 사용하고 다시 해쉬함수에 적용하여 그 다음 키값을 얻는 방법으로 해쉬함수의 연산을 여러번 반복해서 얻은 값의 리스트를 말한다.

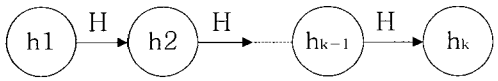

그림 5. 해쉬키 체인 모델
Fig. 5 Hash key chain model

해쉬함수를 반복 적용하여 생성한 해쉬값을 체인화함으로써 체인의 앞뒤에 있는 해쉬값을 서명과 검증을 위한 키로 사용하기 위해서 센서네트워크의 싱크노드는 메시지 전송경로상의 모든 노드에게 배분한다.

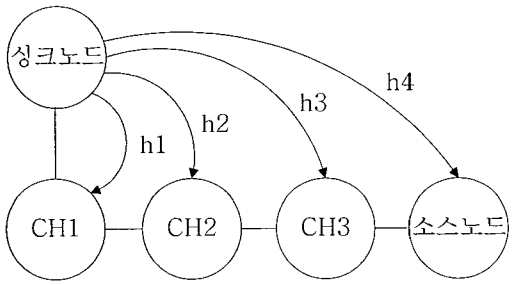

그림 6. 해쉬키 분배모델
Fig. 6 Hash key distribution model

(그림 6)과 같이 싱크노드는 메시지 전송경로상에 있는 노드의 수만큼 해쉬키를 갖는 해쉬체인을 생성하고 싱크노드에 바로 인접한 클러스터 헤드 CH1, CH2, CH3로부터 소스노드까지 순차적으로 해쉬키체인의 해쉬키를 전달한다.

송신노드는 싱크노드로부터 해쉬키를 전달받은 후 (그림 7) 과 같이 해쉬키를 서명값으로 메시지에 부착해서 수신노드로 전달한다. 수신노드는 싱크노드로 부터 전달받은 해쉬키를 해쉬함수에 입력하여 계산한 해쉬키와 메시지와 함께 수신한 해쉬키를 비교하여 인증과 무결성을 확인한다.

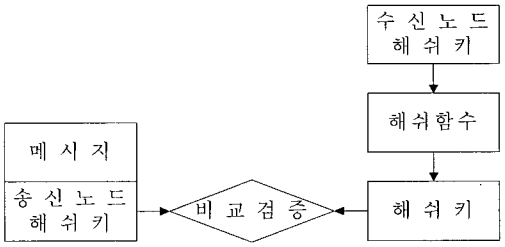

그림 7. 해쉬키체인기반 전자서명모델
Fig. 7 Hash key chain based digital signature model

Ⅳ. 성능평가 및 분석

공개키기반 디지털 서명 모델과 해쉬체인기반 디지털서명 모델의 서명과 검증의 연산 횟수를 비교하여 성능을 분석하였다. 싱크노드와 소스노드사이에 3개의 클러스터 헤드가 존재하는 라우팅 경로를 갖는 센서네트워크에 대해서 분석하였다. <표 1>과 같이 공개키기반 디지털서명 모델에서는 싱크노드는 검증을 위해서, 소스노드는 서명을 위해서 공개키 연산을 수행하고 중간 경유 노드인 클러스터 헤드는 서명과 검증을 위해서 각각 공개키 연산을 수행한다. 반면 해쉬키체인 디지털서명 모델에서는 서명을 위해서 분배받은 해쉬키를 부착하면 되므로 해쉬함수를 수행하지 않고 검증을 위해서 소스노드를 제외한 전체노드가 해쉬함수를 한번 수행한다.

공개키기반 디지털서명모델은 공개키 연산횟수가 8번으로 해쉬체인 기반 디지털서명모델에 비해서 상당한 처리시간과 연산비용이 요구됨을 알 수 있다.

해쉬체인기반 전자서명 모델은 공개키연산을 사용하지 않고 해쉬함수의 수행횟수가 4번으로 공개키 연산이 해쉬함수의 연산에 비해서 일반적으로 100~1000배 정도의 걸린다는 걸 고려하면 성능이 뛰어나다는 걸 알 수 있다.

표 1. 디지털서명 모델의 성능비교표
Table. 1 Parameters Comparing Performances of Digital Signature Model

		해쉬함수연산		공개키연산	
		생성	확인	암호	복호
공개키기반 디지털서명	전체노드			4	3
	싱크노드				1
해쉬체인기반 디지털서명	전체노드		3		
	싱크노드		1		

V. 결 론

센서네트워크에서는 패킷 포워딩과 라우팅 기능을 전담하는 노드나 서버가 존재하지 않고 네트워크 통신에 참여하는 센서노드들이 이러한 기능을 수행한다. 따라서 센서노드들이 패킷 포워딩과 라우팅 과정에서 패킷의 위변조에 대한 공격이 취약하다. 이의 해결책으로 라우팅과 포워딩 메시지에 대한 인증과 무결성을 보장하는 보안기능이 요구된다. 이를 위해서 공개키기반 전자서명 모델에 비해서 디지털 서명을 생성하고 검증하는데 계산적인 부담이 적은 해쉬체인 기반 디지털서명 모델을 제안하고 연산횟수의 비교를 통하여 모델의 적합성을 검증하였다.

본 논문은 센서네트워크의 라우팅과 포워딩 메시지에 대한 인증과 무결성을 보장하기 위한 해쉬체인기반 전자서명 모델에 대해서 제안하였다. 공개키 기반 디지털 서명의 사용은 비용이 비싸다는 것과 디지털 서명을 생성하고 검증하는 과정에서 소요되는 시간이 크다는 단점을 갖는다. 따라서 라우팅과 포워딩 메시지의 전송이 빈번한 센서네트워크에 대해서 해쉬체인기반 디지털서명모델의 사용이 적합하다는 것을 확인하였다.

제안된 해쉬체인 기반 디지털서명모델은 싱크노드로부터 분배된 해쉬키를 이용하여 메시지를 전달하기 때문에 서명을 위한 연산 부담이 공개키기반 디지털서명모델보다 훨씬 적다. 서명과 검증을 위한 연산횟수를 통해서 공개키기반 디지털서명모델보다 해쉬체인기반 전자서명 모델의 성능이 뛰어나다는 것을 확인하였다.

참고문헌

[1] Jamil Ibriq and Imad Mahgoub "Cluster-Based Routing in Wireless Sensor Networks: Issues and Challenges," SPECTS 2004.

[2] Hu, F., et al., "Secure wireless sensor networks: problems and solutions," J. of SCI, to appear, 2004

[3] Karlof C. and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Networks, vol, 1, issues 2-3(Special Issue on Sensor Network Applications and Protocols), Elsevier, pp. 293-315, Sep. 2003.

[4] Gaubatz, G., et al., "Public key cryptography in sensor networks-revisited," 1st European Workshop on Security in Ad-Hoc and Sensor Networs, 2004.

[5] Schneier, B., One-Way Hash Function, Dr. Dobb's Journal, pp. 148-151 September, 1991.

[6] Wang X. and H. Yu, "How to Break MD5 and Other Hash Functions, Advances in Cryptology-Eurocrypt," '2005, LNCS 3494, Springer-Verlag, pp. 19-35, 2005.

[7] Rivest, R., A. Shamir, and L. Adleman, "A method for obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21, pp. 120-126, 1978.

[8] Krzysztof Piotrowski et al., "How public key cryptography influences wireless sensor node lifetime," Proceedings of the fourth ACM workshop on Security of ad-hoc and sensor networks, Alexandria, Virginia, USA, 2006.

[9] Handy M. J., et al., Low Energy Adaptive "Clustering Hierarchy with Deterministic Cluster-Head Selection," IEEE, 2002.

[10] Bechler M., et al., "A Cluster-Based security architecture for ad hoc networks," in: Proceedings of IEEE Conference on Computer Communications Hong Kong, March 2004.

[11] Perrig A., et al., "Security in wireless sensor networks," Commun. OF ACM, 47(5), pp. 53-57, June 2004.

저자소개

김영수(Young-Soo Kim)

2003년 2월 : 국민대학교 정보관리학박사
2008년 ~ 현재 : 충북대학교 포닥

※ 관심분야 : 인터넷, 정보보안, 보안공학

조선구(Seon Goo Cho)

2000년 2월 : 국민대학교 정보관리학박사
현재 나사렛대학교 경영학부 부교수

※ 관심분야 : 전자상거래, 인터넷응용