(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년03월31일
(11) 등록번호 10-1507572
(24) 등록일자 2015년03월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2014-0032957
(22) 출원일자 2014년03월20일
심사청구일자 2014년03월20일
(56) 선행기술조사문헌
KR1020100095653 A

(73) 특허권자
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
성순화
대전광역시 유성구 은구비남로 34, 새미래아파트 812-802 (노은동, 열매마을8단지)
(74) 대리인
김원준

전체 청구항 수 : 총 6 항 심사관 : 문형섭

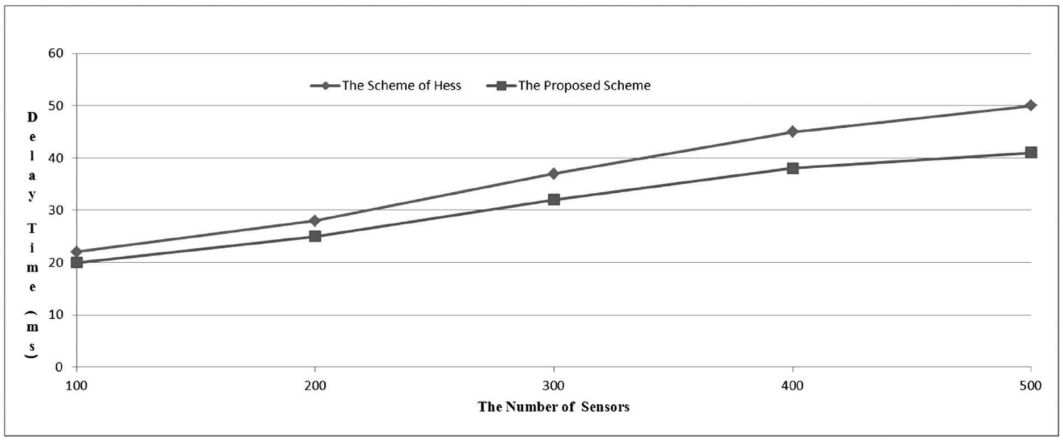
(54) 발명의 명칭 **센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법**

(57) 요 약

본 발명은 신뢰할 수 있는 제3의 기관인 키 생성 센터(KGC)와, 상호간에 신뢰관계가 수립되어 있는 복수개의 센서 노드들을 포함하는 센서 네트워크의 특성과 구조, 보안상 취약점을 고려한 센서 네트워크의 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법으로서, 보다 상세하게는 (A) 상기 키 생성 센터(KGC)가, 알고리즘 K-

(뒷면에 계속)

대 표 도 - 도8



proxies에 의해 생성된 ID를 네트워크 부트스트래핑(Bootstrapping) 단계에서, 또는 새로운 노드가 네트워크에 추가되거나 시스템 고장으로 노드의 ID의 갱신이 필요한 때에 상기 각 센서 노드에게 할당하고, 만약 센서 노드의 ID가 손상되었다면, counter-ID에서 철회되어 폐기되는 ID 생성, 갱신 및 철회 단계; (B) 상기 키 생성 센터(KGC)가, 라우팅 함수 R( ) 적용시에 유일한 "1"인 값이 출력되도록 복소수를 포함한 ID 1, -1, i, $-i$ 의 주소인 공개키를 부여하고, 공개키와 그 쌍인 비밀키를 의사 랜덤 이진 수열 생성기의 $\{0,1\}^*$ 이진 비트 스트링으로 생성하여 CH(Cluster Head)를 포함하는 각 센서 클러스터(Ri)를 구성하는 한편, CH의 마스터 키를 생성함으로써 클러스터 내 노드들의 비밀키에 대한 세션키를 만들기 위한 키 데이터의 마스터 준비 작업 수행하는 단계; 및 (C) 셋업 절차, 철회 절차가 필요 없는 쓰레시홀드 링 서명을 통해 센서 노드의 키를 인증하는 단계;를 포함하는 것을 특징으로 하는 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법에 관한 것이다.

특허청구의 범위

청구항 1

신뢰할 수 있는 제3의 기관인 키 생성 센터(KGC)와,

상호간에 신뢰관계가 수립되어 있는 즉, 평문의 정보를 상호교환할 수 있는 복수개의 센서 노드들을 포함하는 센서 네트워크의 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법으로서,

(A) 상기 키 생성 센터(KGC)가, 알고리즘 $K\text{-}_{proxies}$에 의해 생성된 ID를 네트워크 부트스트래핑(Bootstrapping) 단계에서, 또는 새로운 노드가 네트워크에 추가되거나 시스템 고장으로 노드의 ID의 갱신이 필요한 때에 상기 각 센서 노드에게 할당하고, 만약 센서 노드의 ID가 손상되었다면, counter-ID에서 철회되어 폐기되는 ID 생성, 갱신 및 철회 단계;

(B) 상기 키 생성 센터(KGC)가, 라우팅 함수 R( ) 적용시에 유일한 "1"인 값이 출력되도록 복소수를 포함한 ID 1, -1, i, $-i$ 의 주소인 공개키를 부여하고, 공개키와 그 쌍인 비밀키를 의사 랜덤 이진 수열 생성기의 $\{0,1\}^*$ 이진 비트 스트링으로 생성하여 CH(Cluster Head)를 포함하는 각 센서 클러스터(Ri)를 구성하는 한편, CH의 마스터 키를 생성함으로써 클러스터 내 노드들의 비밀키에 대한 세션키를 만들기 위한 키 데이터의 마스터 준비 작업 수행하는 단계;

(C) 셋업 절차, 철회 절차가 필요 없는 쓰레시홀드 링 서명을 통해 센서 노드의 키를 인증하는 단계;

를 포함하는 것을 특징으로 하는 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법.

청구항 2

제 1 항에 있어서,

상기 (C) 단계는,

셋업 단계, 추출 단계, 암호 단계, 복호 단계의 4 단계로 구성되며, 이를 기반으로 한 ID 기반 암호 알고리즘을 생성하는 것을 특징으로 하는 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법.

청구항 3

제 2 항에 있어서,

상기 셋업 단계는, 새로운 노드 N_{new}가 클러스터에 추가될 때 이루어지는 것으로서,

새로운 노드 N_{new}가 KGC로부터 ID를 부여 받아 그 이웃 노드들에게 Hello 메시지를 브로드캐스트하고, 이웃 노드들은 Hello 메시지를 받은 후, 새로운 노드가 정당한 노드인지 아닌지를 검증하기 위해 ID를 교환하는 것을 특징으로 하는 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법.

청구항 4

제 2 항에 있어서,

상기 추출 단계는, 센서 노드가 시스템의 다른 클러스터로 이동하는 이동 노드 N_m가 있을 때 이루어지는 것으로서,

이동 노드 N_m은 KGC로부터 입력 k, 마스터 키, 공개키로 사용되는 임의의 스트링인 임의 ID를 받고, CH에게 복호화 키인 비밀키 K_{priv}를 돌려주는 것을 특징으로 하는 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법.

청구항 5

제 2 항에 있어서,

상기 암호 단계에서,

일반 노드는 KGC로부터 입력 k, ID, m∈M를 전달받고 암호화한 암호문 c∈C를 돌려주는 것을 특징으로 하는 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법.

청구항 6

제 2 항에 있어서,

상기 복호 단계에서,

일반 노드는 KGC로부터 입력 k, c∈C, 비밀키 K_{priv}를 전달받고 복호화한 평문 m∈M 를 돌려주는 것을 특징으로 하는 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법에 관한 것으로, 보다 상세하게는 센서 네트워크의 특성과 구조, 보안상 취약점을 고려한 센서 데이터 통신의 보안을 위한 ID 기반 키 인증 방법에 관한 것이다.

배 경 기 술

[0002] 최근 무선 센서 네트워크는 사물 정보 및 환경 정보까지 실시간으로 관리하게 됨으로써 서비스 영역을 확장해 나가고 있다. 센서 노드의 위치는 미리 결정될 필요가 없어 접근이 어려운 영역이나 재난 구조를 위한 응용을 위해 임의로 배치되므로, 센서 네트워크 구성은 자가 구성 능력 및 센서 노드들의 협력 동작을 필요로 한다. 센서 네트워크를 구성하는 센서 노드들은 그 수가 매우 많고 각 센서 노드들은 제한된 자원과 컴퓨팅 능력을 가지며, 빈번한 센서 노드들의 삽입과 제거로 센서 네트워크 토폴로지가 쉽게 변화되는 특성을 가지고 있다.

[0003] 무선 센서 네트워크에서는 수많은 센서 노드들이 미리 결정된 형태 없이 배치될 수 있고, 이웃한 센서 노드들이 유사한 정보를 감지하는 특성에 의해 임의의 센서노드 동작이 실패하거나 기능이 소멸되는 경우에도 네트워크 전체적인 동작에는 영향을 미치지 않는 장점이 있는 반면, 무선 매체의 저속, 오류가 심한 전송 특성, 제한된 전원 공급, 센서 노드의 임의 배치로 인한 교체 불가능 등의 문제점을 가진다.

[0004] 한편, 센서 네트워크는 기존 통신 인프라가 없는 무선센서 네트워크로부터 정보 수집을 위해서 기존 무선 네트워킹 적용으로는 적합하지 않으며, 센서 네트워킹을 위한 에너지 소비가 네트워크 전체에 영향을 주어 전체적 시스템 수명을 증가시키는 방향으로 설계되어야 하며, 센서노드들의 동적인 변화에 빠르게 대응할 수 있어야 한다.

[0005] 따라서 센서 노드들의 자기 제어 능력, 제한된 전력과 데이터 중심적 특성을 고려한 라우팅 기법이 요구된다[비특허문헌 1참조]. 센서 네트워크의 안전성 측면에서는 이러한 센서 노드의 특성, 구조 형태, 보안 상 취약성으로 말미암아 안전한 통신을 위한 필요성이 절실함에도 불구하고 그 특성과 형태에 맞는 센서 데이터 보호를 만족시키지 못하는 것이 현실이다. 최근 USN(Ubiquitous Sensor Networks) 서비스 구성 시 센서 노드의 이동성 지원이 중요 이슈로 떠오름에 따라 센서 네트워크나 클러스터 내 노드 추가에 따른 인증과 노드 이동성 지원이 필요하게 되었다.

[0006] 처음 연결된 노드의 경우, 공유된 정보가 존재할 확률이 매우 낮을 뿐 아니라, 노드들의 삽입 및 제거와 같은 빈번한 이동성 때문에 각 노드들의 식별이 빨라야 되며, 이에 대한 키 관리 역시 빠른 대응으로 이루어져야 한다. 또한, 예상치 못한 악의적인 공격으로 인한 노드의 비밀키 혹은 마스터키가 노출될 경우, 키 관리 시스템을 복구할 수 있어야 한다.

[0007] 빠른 노드 식별과 계산량이 적은 키 관리를 위한 ID기반 키 관리에 관한 연구는 각 노드를 식별하고 키를 생성하여 노드 간의 통신에 대한 안전성을 제공할 수 있는 방안으로 연구가 진행되어 왔다. 이는 사전의 공유키 및 신뢰기관의 필요성을 언급하고 있으며, 최근 ID기반 연구[비특허문헌 2,3참조]는 키 분배가 없으며 클러스터 헤드의 부담을 분산시킬 수 있는 ID 기반 인증 기법을 제안하였으나, 노드들 간의 자기 제어 능력 부재로 클러스터 노드의 위임 인증 역할이 과중 되어 있다. 게다가 ID 기반 공개키 방식을 사용하여 겹선형 암호 시스템을 사용한 [비특허문헌 4]는 ID 기반 공개키 방식을 사용하여 계산량을 줄이려고 하였으나, 쌍(the Weil pairing) 기법을 사용함으로써 기존 공개키 방식과 유사한 연산량을 나타내었다.

[0008] 센서 네트워크 노드들의 암호 부담을 분석한 [비특허문헌 5]에서, 센서 노드의 인증과 암호에 사용하는 비대칭키(공개키) 기술은 대칭 키(공유키 혹은 비밀키) 기술과 비교하면, 센서 노드의 인증과 암호에 사용한 계산 비용이 적다는 장점이 있으나, 선 분산(predistribution) 키 과정이 필요하며 완전한 통신 연결을 보장하지 못한다는 단점을 가진다. 뿐만 아니라, 최근 많은 연구[비특허문헌 6-8참조]가 센서 네트워크의 공개키 암호를 사용하기 위한 실제적인 방법을 찾기 위해 수행되어 왔으나, 센서 노드의 인증과 암호에 사용한 계산량이 많다는 공개키 암호 기술의 중대한 문제점을 가지고 있다.

[0009] 그리고 현재 센서 네트워크의 특성으로 인한 보안 기법 적용이 어려워 메시지 기밀성, 무결성, 노드 인증 등의 보안요소 구현을 위해 경량화 된 키 분배 및 인증 기법 연구가 진행되고 있다.

[0010] 이러한 연구들은 키 분배가 필요하므로 메시지 전송 횟수가 증가하는 단점이 있어 그 해결책으로 ID 기반 기법[비특허문헌 2-4, 9참조]이 연구되고 있다. ID 기반 암호화(Identity-based Encryption, IBE)는 1984년 Shamir[비특허문헌 10참조]가 처음 제안하였으나, 그 스킴은 서명 스킴으로만 사용할 수 있어 ID 기반 암호화는 다루어지지 않았고, 2001년 Boneh와 Franklin이 Weil Pairing으로부터 ID 기반 암호화[비특허문헌 4참조]를 처음 소개하게 되었다.

[0011] 그 후, Weil과 겹선형(bilinear) 쌍으로부터 ID 기반 스킴의 많은 연구들이 암호화, 서명, 인증 스킴[비특허문헌 11,12참조]을 포함하여 수행되었다.

[0012] Horwitz 외[비특허문헌 13참조]의 계층적 ID 기반 암호(HIBE: Toward Hierachical Identity-Based Encryption)는 위 계층의 루트 개인키 생성기(PKG)와 아래 계층의 원시 ID(PID)로 구성된 2 레벨 계층적 ID 기반 암호(HIBE)를 제안하여, 위 레벨의 전체적 충돌 저항과 아래 레벨의 부분적 충돌 저항을 가진 2 레벨 계층적 ID 기반 암호 스킴이 BDH(Bilinear Diffie-Hellman) 가정 아래 안전하다는 것을 보이고 이와 관련된 보안 정의를 소개하였다.

[0013] 가능한 공격에 대비한 많은 스킴, ID 기반 암호의 실적, 그리고 전통적 대칭 암호는 ID 기반 암호가 그 성과를 상당히 향상시킬 것을 요구한다. 그러나 그들은 지역의 키들이 어떻게 생성되고 전송되어 그 패킷이 암호 되고 서명되는지를 상세히 설명하지 못하고 있다.

[0014] 국내에 개시된 등록특허 제10-1046992호인 "센서데이터 보안유지 방법, 시스템 및 기록매체"의 구성은 "시간 키 기반의 키 생성 다항식으로부터 센서데이터와 어플리케이션에서 공통의 암호키를 유도함으로써 센서노드에서 어플리케이션 시스템으로 센서데이터를 안전하게 전송할 수 있게, 센서노드가 가진 초기 그룹 키 및 개인키 값이 노출되어 난수값이 노출되어도 센서데이터를 암호화 또는 인증할 키 값이 노출되지 않도록 한" 것으로, 센서데이터의 기밀성과 무결성을 향상 시킬 수는 있어도 경량화를 벗어나지는 못하였다.

선행기술문헌

특허문헌

[0015] (특허문헌 0001) 국내 등록 특허 제10-1046992호

비특허문헌

[0016] (비특허문헌 0001) Akyildiz, I., Su, W., Sankarasubramaniam, Y., and Cayirci, E., "A Survey on Sensor Networks," IEEE Communications Magazine, Aug. 2002.

(비특허문헌 0002) Geng YANG, Chun-ming RONG, Christian VELGNER, Jiang-tae WANG and Hong-bing CHENG, "Identity-based key agreement and encryption for wireless sensor networks," The Journal of China Universities of Posts and Telecommunications, China, 2007.

(비특허문헌 0003) T.T. Huyen and Eui-Nam huh, "A reliable 2-mode authentication framework for Ubiquitous sensor network," Journal of Korean Society for Internet Information, 2008.

(비특허문헌 0004) D.Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology-Crypto 2001, LNCS 2139, Springer-Verlag, pp.213-229, 2001.

(비특허문헌 0005) P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, San Diego, California, USA, Sep. 2003.

(비특허문헌 0006) G. Gaubatz, J. Kaps, and B. Sunar, "Public keys cryptography in sensor networks-revisited," in The Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS), 2004.

(비특허문헌 0007) D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in Tiny OS based on elliptic curve cryptography," in The First IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, pp.71-79, Oct. 2004.

(비특허문헌 0008) W. Du, R. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks," MobiHoc 05, May 25-27, 58-67, UrbanaChampaign, Illinois, USA, 2005.

(비특허문헌 0009) X. Boyen, "Multipurpose Identity-based signcryption, a Swiss army knife for identity-based cryptography," in Proceedings of the 23rd Interna. Cobf. On Advances in Cryptology, Lecture Notes in Computer Science, vol.2729, pp.383-399, 2003.

(비특허문헌 0010) Shamir, A., "Identity-based cryptography and signature schemes," Advances in Cryptology Prc. of International Conference on Advances in Cryptology CRYPTO'84, Aug. 1984.

(비특허문헌 0011) F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," Selected Areas in Cryptology-SAC 2002, LNCS 2595, pp.310-324, 2003.

(비특허문헌 0012) B. Lynn, "Authenticated Identity-based Encryption," Cryptology e Print Archive, Report 2002/072, 2002.

(비특허문헌 0013) Jeremy Horwitz and Ben Lynn, "Toward Hierarchical Identity-Based Encryption," Stanford University, Stanford, CA 94305, USA, 2002.

(비특허문헌 0014) Soonhwa Sung, "A Threshold Ring Group Signature for Ubiquitous Electronic Commerce," Korea Information Processing Society Journals D, vol.14-D, no.4, ISSN 1598-2866, pp.373-380, Jun. 2007.

(비특허문헌 0015) Xuan Hung Le, Sungyoung Lee, Ismail Butun et al., "An Energy Efficient Access Control Scheme for Wireless Sensor Networks based on Elliptic Curve Cryptography," JCN, vol.11, no.6, pp.599-606, Dec. 2009.

(비특허문헌 0016) Fei Hu and Sunil Kumar, "Wireless Sensor Networks for Mobile Telemedicine: QoS support," IEEE Transactions on Information Technology in Bioinformatics, (under final review), 2003.

(비특허문헌 0017) Tiny OS, TinyOS1.1.0, [Online]. Available: http://tinyOS.net (downloaded 2012, Dec. 17)

(비특허문헌 0018) A. L. Alberto Medina, Ibrahim Matta, and John Byers, "BRITE: An approach to universal topology generation," In MAS-COTS, 2001.

(비특허문헌 0019) Liqun Chen and Caroline Kudla, "Identity-based authenticated key agreement protocols from pairing," Cryptology e Print Archive, Report 2002/184, http://eprint.iacr.org/2002/184, 2002.

(비특허문헌 0020) K. Lauter, "The advantages of elliptic curve cryptography for wireless security," IEEE Wireless Communications, vol.11, no.1, pp.62-67, Feb. 2004.

발명의 내용

해결하려는 과제

[0017] 본 발명은 전술한 종래기술의 문제점을 해결하고자, 센서 노드가 물리적인 환경 공격에 그대로 노출되어 전송 정보가 쉽게 변경되거나 정당하지 않은 노드가 데이터를 전송함으로써 전체 정보의 무결성을 쉽게 무너뜨리며, 악의적인 노드가 정당한 센서 노드로 가장하여 필요한 정보를 계속 발생시켜 중간 노드의 자원을 고갈시킴으로써 네트워크의 수명이 단축되는 것을 방지하도록 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법을 제공하는 것을 목적으로 한다

[0018] 또한, 본 발명은 센서 네트워크의 특성으로 인한 보안 기법 적용이 어려워 메시지 기밀성, 무결성, 노드 인증 등의 보안요소 구현을 위해 경량화에 중점을 둔 ID 기반 키 인증 방법을 제고하고자 함을 목적으로 한다.

[0019] 또한 본 발명은 ID 기반 암호 시스템을 바탕으로 센서 노드들의 빠른 이동성을 고려한 라우팅과 선 분산 키 과정이 필요 없는 클러스터 내 능동적인 키 인증이 가능한 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법을 제공하는 것을 목적으로 한다

과제의 해결 수단

[0020] 전술한 목적을 달성하기 위한 본 발명은, 신뢰할 수 있는 제3의 기관인 키 생성 센터(KGC)와, 상호간에 신뢰관계가 수립되어 있는 즉, 평문의 정보를 상호교환할 수 있는 복수개의 센서 노드들을 포함하는 센서 네트워크의 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법으로서, (A) 상기 키 생성 센터(KGC)가, 알고리즘 $K\text{-}_{proxies}$에 의해 생성된 ID를 네트워크 부트스트래핑(Bootstrapping) 단계에서, 또는 새로운 노드가 네트워크에 추가되거나 시스템 고장으로 노드의 ID의 갱신이 필요한 때에 상기 각 센서 노드에게 할당하고, 만약 센서 노드의 ID가 손상되었다면, counter-ID에서 철회되어 폐기되는 ID 생성, 갱신 및 철회 단계; (B) 상기 키 생성 센터(KGC)가, 라우팅 함수 R( ) 적용시에 유일한 "1"인 값이 출력되도록 복소수를 포함한 ID 1, -1, i, $-i$ 의 주소인 공개키를 부여하고, 공개키와 그 쌍인 비밀키를 의사 랜덤 이진 수열 생성기의 $\{0,1\}^*$ 이진 비트 스트링으로 생

성하여 CH(Cluster Head)를 포함하는 각 센서 클러스터(Ri)를 구성하는 한편, CH의 마스터 키를 생성함으로써 클러스터 내 노드들의 비밀키에 대한 세션키를 만들기 위한 키 데이터의 마스터 준비 작업 수행하는 단계; 및 (C) 셋업 절차, 철회 절차가 필요 없는 쓰레시홀드 링 서명을 통해 센서 노드의 키를 인증하는 단계;를 포함하는 것을 특징으로 하는 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법에 관한 것이다.

발명의 효과

[0021] 이상과 같이 본 발명에 의하면, ID 기반 키 인증은 이전의 연구보다 선 분산 키 과정이 필요 없으며, ID 종류가 간단하여 ID를 코드할 바이트 수를 줄일 수 있으며, ID 기반 암호 알고리즘의 공개키, 비밀키 연산량이 적을 뿐만 아니라, 클러스터 내 인증 프로세스에 의한 노드 인증으로 빠른 노드의 삽입과 제거에 대처할 수 있는 능동적인 키 인증을 이룰 수 있게 된다.

[0022] 또한, 경량화에 중점을 둔 ID 기반 키 인증 기법은 3 계층의 상호 작용으로 제한된 자원 하의 암호화, 복호화에 사용된 CPU 시간을 이전 연구보다 줄일 수 있으며, 센서 노드의 빠른 위상 변화에도 불구하고 이전 연구보다 전송 지연이 향상되게 된다.

도면의 간단한 설명

[0023] 도 1은 본 발명에 의한 존에서의 3 계층 상호 작용을 나타낸 도면.

도 2는 본 발명에 의한 대리 노드 층을 나타낸 도면

도 3은 본 발명에 의한 라우팅 함수 R()을 나타낸 플로챠트.

도 4는 본 발명에 의한 은닉 층을 나타낸 도면.

도 5는 본 발명에 의한 ACL의 예를 나타낸 도면.

도 6은 본 발명에 의한 ID기반 키 분포를 나타낸 도면

도 7은 본 발명에 의한 ID기반 노드 인증을 나타낸 도면

도 8은 본 발명에 의한 선서 노드 밀도에 따른 전송성과를 나타낸 그래프.

발명을 실시하기 위한 구체적인 내용

[0024] 이하 첨부된 도면을 참조하여 본 발명을 보다 상세히 설명한다. 그러나 첨부된 도면과 그에 대한 설명은 본 발명의 기술적 사상의 내용과 범위를 쉽게 설명하기 위한 예시일 뿐, 이에 의해 본 발명의 기술적 범위가 한정되거나 변경되는 것은 아니다. 또한 이러한 예시에 기초하여 본 발명의 기술적 사상의 범위 안에서 다양한 변형과 변경이 가능함은 당업자에게는 당연할 것이다.

[0025] 전술한 바와 같이 본 발명은, 신뢰할 수 있는 제3의 기관인 키 생성 센터(KGC)와, 상호간에 신뢰관계가 수립되어 있는 즉, 평문의 정보를 상호교환할 수 있는 복수개의 센서 노드들을 포함하는 센서 네트워크의 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법으로서,

[0026] (A) 상기 키 생성 센터(KGC)가, 알고리즘 $K\text{-}_{proxies}$에 의해 생성된 ID를 네트워크 부트스트래핑(Bootstrapping) 단계에서, 또는 새로운 노드가 네트워크에 추가되거나 시스템 고장으로 노드의 ID의 갱신이 필요한 때에 상기 각 센서 노드에게 할당하고, 만약 센서 노드의 ID가 손상되었다면, counter-ID에서 철회되어 폐기되는 ID 생성, 갱신 및 철회 단계; (B) 상기 키 생성 센터(KGC)가, 라우팅 함수 R( ) 적용시에 유일한 "1"인 값이 출력되도록 복소수를 포함한 ID 1, -1, i, $-i$ 의 주소인 공개키를 부여하고, 공개키와 그 쌍인 비밀키를 의사 랜덤 이진 수열 생성기의 $\{0,1\}^*$ 이진 비트 스트링으로 생성하여 CH(Cluster Head)를 포함하는 각 센서 클러스터(Ri)를 구성하는 한편, CH의 마스터 키를 생성함으로써 클러스터 내 노드들의 비밀키에 대한 세션키를 만들기 위한 키 데이터의 마스터 준비 작업 수행하는 단계; 및 (C) 셋업 절차, 철회 절차가 필요 없는 쓰레시홀드 링 서명을 통해

센서 노드의 키를 인증하는 단계;를 포함하는 센서 데이터 통신의 보안을 위한 ID기반 키 인증 방법에 관한 것이다.

[0027] 상기 알고리즘 $K\text{-}_{proxies}$는 배치 전 센서 노드들의 신뢰 관계를 바탕으로 임의의 노드 4개에 ID 1,-1, i, $-i$ 를 할당하는 알고리즘으로서 종래 당업계에서 비교적 널리 알려진 알고리즘이다. 알고리즘 $K\text{-}_{proxies}$에 의해 ID의 대리 노드가 할당된다. 할당된 ID의 대리 노드를 생성하는 이 알고리즘은 은닉층 노드로 상호 작용하기 위한 대리 노드층을 구성함으로써, ID 주소인 공개키를 4개로 할당하는 역할을 한다. 따라서 공개키의 갯수를 줄일 수 있는 알고리즘으로 공개키 관리 자원 즉 센서 데이터를 위한 에너지 및 비용을 줄일 수 있는 알고리즘이다.

[0028] 본 발명에서는 자기 제어 기능을 가진 ID 기반 암호의 키들이 어떻게 전송되는지를 설명하기 위해 임계 암호를 가진 링 서명[비특허문헌 14참조]을 고려한다. 만약 그룹에서 임계를 넘는 파티들이 암호화된 메시지를 복호화하기 위해 복호화 프로토콜에서 서로 협력한다면 임계 암호 시스템이라 하며, 이때 메시지는 공개키로 암호화되고 이와 일치하는 비밀키는 참여하는 파티들 사이에 공유된다.

[0029] 즉 n 파티를 가진 그룹에서 적어도 t 파티가 암호문을 효율적으로 복호화할 수 있다면 (t,n) 임계 암호시스템이라 한다.

[0030] 한편, 링 서명은 그룹 사용자들 중 각각의 키들을 가지고 있는 어떤 구성원에 의해 형성되는 디지털 서명의 한 형태로 서명 생성에 사용된 구성원 멤버 키가 누구의 것인지 판단하기 어려워야 한다. 그룹 각각은 공개키, 비밀키 쌍 (P_{K1}, S_{K1}), (P_{K2}, S_{K2}), …, (P_{Kn}, S_{Kn})을 가진다고 가정하면, 파티 i 는 입력(m, S_{Ki}, P_{K1}, …, P_{Kn}) 으로 메시지 m 에 관한 링 서명을 계산할 수 있다.

[0031] 이러한 링 서명의 유효성은 어느 누구나 확인할 수 있어야 하며, 어느 누구도 어떤 그룹의 비밀키를 알지 못한 채 어떤 메시지의 유효한 링 서명을 생성하기가 어려워야 한다. 그리고 이는 그룹 서명과 비슷하나, 그룹관리자가 없으므로 각각 서명의 익명성을 철회할 방법이 없으며, 사용자들의 어떤 그룹이 부가적인 셋업 없이 즉흥적인 그룹으로서 사용될 수 있다.

[0032] 따라서 (t,n) 임계 암호 시스템은 익명적인 방법에서 권위 있는 비밀을 누설할 방법과 바라지 않은 부작용 없이 인증할 수 있는 지정된 검증자를 검증할 수 있다.

[0033] 본 발명에서는 대리 노드 층, 은닉 층 및 자기 제어층의 상호 작용으로 상기 각 단계를 수행하도록 함으로써 USN 서비스에서 이동 노드의 이동성 지원을 할 뿐만 아니라, 계산량도 줄어들도록 하였다.

[0034] **(A) ID 생성단계 : 대리 노드 층에서 수행됨**

[0035] 센서 노드들은 보통 같은 관리상의 실체에 속해 있으므로 배치 이전에 노드들은 이미 서로 만난 사실이 있으므로 인터넷 환경과는 다르다. 즉, 센서 노드들은 배치 이전에 평문의 정보를 교환할 수 있는 초기 환경에 있어 그들 사이의 신뢰 관계를 수립할 수 있다.

[0036] 따라서 배치 전 센서 노드들의 신뢰 관계를 바탕으로, 알고리즘 $K\text{-}_{proxies}$로 생성, 갱신, 철회의 간단한 ID 할당을 한다.

[0037] (1) ID 생성

[0038] 신뢰할 수 있는 제3의 기관인 키 생성 센터(KGC)는 알고리즘 $K\text{-}_{Proxies}$에 의해 생성된 ID를 네트워크 부트스트래핑(Bootstrapping) 단계에서 노드에게 부여한다. ID를 부여 받은 노드는 전체 네트워크의 신뢰를 얻게 되며, 1

홉 주변 노드로 전송되어 ID 재생성을 할 수 있는 링 구조를 가지게 된다. 따라서 노드가 네트워크에 추가되거나, 시스템 고장으로 ID를 갱신하기를 원한다면, 알고리즘 $K_{-Proxies}$는 네트워크가 형성되기 전 결정되어야 한다.

[0039] KGC는 복소수를 포함한 ID 1, -1, i, $-i$ 의 주소인 공개키를 부여하고, 공개키와 그 쌍인 비밀키를 의사 랜덤 이진 수열 생성기(pseudorandom binary sequence generator)의 $\{0,1\}^*$ 이진 비트 스트링으로 생성하며, 도 2와 같이 CH(Cluster Head)를 포함한 크기에 제한이 없는(노드의 이동성을 배려하기 때문) 클러스터 R_i를 구성한다. 또한, KGC는 ID 생성과 함께 CH의 마스터키를 생성함으로써, 클러스터 내 노드들의 비밀키에 대한 세션키를 만들기 위한 키 데이터의 마스터 준비 작업을 한다. ID 생성은 기술적으로 ID 갱신과 같으나 더 많은 보안이 필요하다.

[0040] (2) ID 갱신

[0041] 최초의 ID가 노드에 생성된 후, 새로운 노드가 네트워크에 추가되거나, 시스템 고장으로 노드의 ID를 갱신하기를 원한다면, 그것은 T_{renew} 시간 이내에 갱신되어야 하며, 노드의 키 쌍이 업데이트되면 그의 ID 역시 갱신되어야 한다. ID를 갱신하기 위해, 노드는 현재의 유효한 ID와 새로운 ID를 위한 미래 만기 시간 T<(current time + T_{renew})를 만족해야 한다.

[0042] (3) ID 철회

[0043] 만약 ID가 손상되었다면, counter-ID에서 철회되어 스스로 폐기되며, 과거 T_{renew} 시간 이내에 counter-ID의 부분 집합을 유지해야 한다.

[0044] ID 할당을 위한 대리 노드 생성 알고리즘은 다음과 같다.

Define:

w, x, y, z: Four end-nodes to set up ID assignment
v: Proxy candidate
ID_1: ID for the node w
ID_i: ID for the node x
ID_{-1}: ID for the node y
ID_{-i}: ID for the node z
ID_{self}: ID for one node of itself
N_x: 1-hop neighbors of any node x
Re: Request to set up ID assignment
K: The number of proxies need to be found
Proxies(k): Executed at random node among w, x, y, z
  for i=1 to k **do**
    Randomly select a node in N_x, and send R
  end for
  if Receive positive ACK from node v **then**
    Register v as a proxy
  end if
Check(Re): Executed at all nodes receiving Re
  if Re is not seen before **then**
    if $ID_{self} \cap ID_w$ is not empty **then**
      if $ID_{self} \cap ID_x$ is not empty **then**
        if $ID_{self} \cap ID_y$ is not empty **then**
          if $ID_{self} \cap ID_z$ is not empty **then**
            Register itself as a proxy for node $w, x, y,$ and z
            Send back positive ACK to node w, x, y and z
            Exit the procedure
          end if
        end if
      end if
    end if
  end if
  Randomly select a neighbor other than the sender to forward Re.

[0045]

[0046] **(B) 간단한 라우팅 단계 : 은닉 층에서 수행**

[0047] 은닉 층은 노드의 빠른 이동과 ID 노출을 보호하기 위해 복소수를 포함한 4개의 ID 1,-1, i, $-i$ 를 입력으로 한 유일한 "1"인 값을 출력 하는 라우팅 함수 R( )을 사용한다.

[0048] 도 3의 라우팅 함수 R( )은 해쉬 함수처럼 가변의 값을 입력으로 일정 값의 출력을 내는 함수로서, 입력으로는 ID 1,-1, i, $-i$ 의 4개 중 어느 것이 될 수 있는 가변의 수가 된다. 단, 클러스터 크기에 따라 가변 크기는 비례하며, 클러스터 크기 제한은 없다. 그 출력으로는 임의의 클러스터 내 노드 ID 각각의 4제곱한 값인 "1"이 된다. 즉, $1\times1\times1\times1=1$, $-1\times-1\times-1\times-1=1$, $i\times i\times i\times i=1$, $-i\times-i\times-i\times-i=1$이 되므로 라우팅 함수 R( )은 다음과 같다.

[0049] $R_1(1) = R(1)\times R(1)\times R(1)\times R(1) = 1$

[0050] $R_{-1}(-1) = R(-1)\times R(-1)\times R(-1)\times R(-1) = 1$

[0051] $R_i(i) = R(i)\times R(i)\times R(i)\times R(i) = 1$

[0052] $R_{-i}(-i) = R(-i)\times R(-i)\times R(-i)\times R(-i) = 1$

[0053] $Rx_k(\ ) = \prod_{k=1}^{4} R_{x_k}$ x=1, -1, i, $-i$ k=k+1 ($1 \leq k \leq 4$)

[0054] 따라서 도 4의 클러스터 내 모든 ID 값은 유일한 "1"을 소유하게 되어 ID를 코드할 라우팅 테이블이 필요 없으며, 노드가 쉽게 떠나고 추가되더라도 전체 노드 ID 값이 모두 같기 때문에 라우팅 설정이 필요 없을 뿐만 아니라, 각 노드의 삽입 제거와 같은 이동성에 제한을 받지 않으며 공격자로부터 ID 노출을 보호할 수 있다.

[0055] 라우팅 함수 결과 모든 노드 ID가 "1"로 셋팅되는 것은 각 노드 수명 주기에 단 한 번만 주어진다. 이후 각 노드는 대리 노드 층에서 생성된 ID의 주소가 공개키가 되고 그 쌍인 비밀키는 KGC로 부터 받게 된다. 따라서 은닉 층은 효율적인 라우팅을 위해 일시적인 라우팅 함수를 사용하며, 자기 제어층과 상호 작용으로 센서 데이터를 인증할 키 인증 준비를 한다.

[0056] **(C) 키 인증 단계 : 자기 제어 층에서 수행**

[0057] 자기 제어 층은 센서 노드의 특성으로 셋업 절차, 철회 절차 등이 필요 없는 자기 제어 능력으로 키 인증이 이루어진다. 이러한 키 인증은 클러스터의 최소 노드들이 부분 그룹의 정확한 멤버십을 숨긴 채 키를 인증하기 위해 협력해야만 하는 쓰레시홀드 링 서명[비특허문헌 14참조]을 사용한다.

[0058] 이상과 같은 본 발명에 의하면, ID 기반 센서 노드 인증은 대리 노드 층과 은닉 층의 상호 작용을 바탕으로 한 키 생성과 자기 제어층의 ID 기반 키 동의 알고리즘으로 ID 기반 센서 노드인증 프로토콜이 이루어진다. 이하에서 이들을 구분하여 상세히 설명한다.

[0059] **(1) 키 생성**

[0060] 이전의 센서 네트워크 키 동의[비특허문헌 15참조]는 각 노드와 KGC사이에서 이루어졌으나, 제안된 키 동의에서는 CH와 KGC 사이에서 이루어진다. 즉, CH는 KGC와 독립적으로 쓰레시홀드 링 서명을 사용하여 클러스터 내 각 노드의 키를 인증한다. 따라서 이전의 KGC 관리 하에 있던 비밀키, 마스터 키 노출 문제를 해결할 수 있다. 센서 노드는 KGC로부터 공개키, 비밀키를 부여 받아, 접근을 위한 정당한 노드로 허락을 받은 CH와 통신을 한다. CH가 KGC로부터 받은 클러스터 마스터 키는 클러스터 내 각 노드의 키 쌍 값을 변화시킬 수 있는 키 관리를 하지만, KGC는 단지 키들을 생성만 한다.

[0061] 센서 노드의 역동적 위상 변화를 위한 주기적인 키업데이트는 이동성 인자[비특허문헌 16참조]를 바탕으로 계산되며, 두개의 키를 업데이트한다. 먼저, 각 CH와 모든 클러스터멤버와 공유한 클러스터 마스터 키, 그리고 클러스터 마스터 키를 생성하기 위해 사용되는 클러스터 멤버의 공개키와 비밀 키인 키 쌍을 업데이트함으로써 클러스터 마스터 키를 통한 센서 데이터 집합 보안이 이루어진다.

[0062] 각 클러스터에서 CH는 각 노드의 ID와 전체 센서 네트워크 수명에서 오직 한번만 사용되는 K_{pub} 시퀀스를 포함한 Hello 메시지를 이웃하는 모든 센서 노드에게 브로드캐스트 한다. 이웃하는 센서가 이 메시지를 받을 때, 이웃하는 센서는 키 쌍으로 암호화된 메시지 인증코드(MAC)를 CH에게 되돌려 준다. 그래서 CH는 그 자신과 이 센서 사이의 새로운 키 쌍을 재생성 할 쓰레시홀드 링 서명을 사용한다. 클러스터 내 모든 키 쌍이 한번 업데이트 되면, 새로운 클러스터 마스터 키는 업데이트된 키 쌍과 함께 각 클러스터 멤버에게 전송된다.

[0063] CH는 대리 노드 층에서 KGC에 의해 생성된 키 쌍과 클러스터 마스터 키가 정당한 노드로서의 접근을 위해 접근 제어 리스트(ACL)를 관리한다.

[0064] 도 5에서와 같이 ACL은 ID, 공개키, 개인키, 접근특권 마스크(APM)로 구성되며, 노드 정보와 서비스 승인을 명시하는 이진 비트 집합으로 이루어진다.

[0065] 클러스터 공개키(K_{pub})는 클러스터 각 노드의 공개키를 더한 후 해쉬함으로써 생성되며, 그 시점의 클러스터노드 수인 클러스터 크기에 의존된다. 클러스터 비밀키(K_{priv})는 클러스터 각 노드의 비밀키를 XOR한 후 해쉬하여 생성되며, 클러스터 마스터 키는 클러스터 각 노드의 비밀키를 해쉬하여 XOR한 후 다시 해쉬하여 생성된다.

[0066] - 클러 스터 공개키:

[0067] $$K_{pub} = H(\sum_{k=1}^{i/4} K_{pub}(1) + \sum_{k=1}^{i/4} K_{pub}(-1) + \sum_{k=1}^{i/4} K_{pub}(i) + \sum_{k=1}^{i/4} K_{pub}(-i))$$

[0068] - 클러스터 비밀키 :

[0069] $$K_{priv} = H(K_{priv(1)} \oplus K_{priv(2)} \oplus K_{priv(3)} \oplus \cdots\cdots \oplus K_{priv(i)})$$

[0070] - 클러스터 마스터 키 :

[0071] $$Km_{priv} = H\{(H(K_{priv(1)}) \oplus H(K_{priv(2)}) \oplus H(K_{priv(3)}) \oplus \cdots\cdots \oplus H(K_{priv(i)})\}$$

[0072] 도 6에서와 같이 ID 기반 키 분산은 클러스터 키와 같은 방법으로 존의 키 생성을 지원하며, 그 방법은 다음과 같다.

[0073] - 존 공개키:

[0074] $$K_{pub} = H(\sum_{k=1}^{i/4} K_{pub}(1) + \sum_{k=1}^{i/4} K_{pub}(-1) + \sum_{k=1}^{i/4} K_{pub}(i) + \sum_{k=1}^{i/4} K_{pub}(-i))$$

[0075] - 존 비밀키:

[0076] $$K_{priv} = H(K_{priv(1)} \oplus K_{priv(2)} \oplus K_{priv(3)} \oplus \cdots\cdots \oplus K_{priv(r)})$$

[0077] - 존 마스터 키:

[0078] $$Km_{priv} = H\{(H(K_{priv(1)}) \oplus H(K_{priv(2)}) \oplus H(K_{priv(3)}) \oplus \cdots\cdots \oplus H(K_{priv(r)})\}$$

[0079] **(2) ID 기반 센서 키 동의 알고리즘**

[0080] ID 기반 센서 키 동의는 셋업 단계, 추출 단계, 암호단계, 복호 단계의 4 단계로 구성되며, 이를 기반으로 한 ID 기반 암 호 알고리즘을 생성한다.

[0081] ① 셋업 단계

[0082] 새로운 노드 N_{new}는 KGC로부터 ID를 부여 받아 그 이웃 노드들에게 Hello 메시지를 브로드캐스트 한다. 이웃

노드들은 Hello 메시지를 받은 후, 새로운 노드가 정당한 노드인지 아닌지를 검증하기 위해 ID를 교환한다. 만약 ID가 손상되었다면, CH는 ACL로부터 ID를 철회시킨다. 왜냐하면 CH는 KGC로부터 키 생성 정보를 바탕으로 한 ACL을 감독하기 때문이다. 만약 CH의 마스트 키가 s일 때 ID의 $K_{priv} = (K_{pub})^s$이면, 통신 채널을 설정한다. 보안을 위한 re-keying에서 KGC는 새롭고 짧은 수명을 가진 임의의 노드 K'_{priv}를 선택하여 클러스터 내 모든 노드에게 브로드캐스트한 후, 만 약 ID의 $K'_{priv} = (K'_{pub})^s$이면, 통신 채널을 설정한다.

[0083] 임의 노드 NR은 KGC로부터 공개키와 비밀키를 받고 보안 매개 변수 $k \in Z^+$를 가진 후, 임의 노드의 비밀키와 k 시스템 매개 변수를 다시 KGC에게 돌려준다. 시스템 매개 변수로 유한 메시지 공간 M과 유한 암호문 공간 C는 공개적이며, 마스터 키는 KGC와 CH에게만 알려지나, 마스터 키는 KGC에서 생성된 후에는 CH에서만 관리된다.

[0084] ② 추출 단계

[0085] 이동 노드 N_m은 KGC로부터 입력 k, 마스터 키, 임의 ID를 받고, CH에게 비밀키 K_{priv} 를 돌려준다. 이때 ID 주소는 공개키로 사용되는 임의의 스트링이며, K_{priv}는 비밀키인 복호화 키이다.

[0086] ③ 암호 단계

[0087] 일반 노드는 입력 k, ID, $m \in M$ 를 가지고 암호문 $c \in C$ 를 돌려준다.

[0088] ④ 복호 단계

[0089] 일반 노드는 입력 k, $c \in C$, 비밀키 K_{priv} 를 가지고 평문 $m \in M$를 돌려준다.

[0090] $\forall\ m \in M$: 복호(k, c, K_{priv}) = m, c = 암호(k, ID, c)

[0091] 이상 ①~④의 과정에 대한 ID 기반 암호 알고리즘은 다음(라인 *******과 ******** 사이)과 같다.

[0092] 기호는 각각 다음을 의미한다.

G^*	집합 G^* = G|O (O은 그룹 G 의 식별 요소이다.)
Z^+	양의 정수 집합
H	해쉬 함수

[0093]

[0094] **********

[0095] 셋업: 보안 매개 변수 $k \in Z^+$ 가 주어지면, 알고리즘은 다음과 같이 진행된다.

[0096] Step 1: 임의의 $\alpha \in G$ 를 선택한다.

[0097] Step 2: 임의의 $s \in Z^+$를 선택한다.

[0098] Step 3: 어떤 n을 위한 암호학적 해쉬 함수를 선택한다.

[0099] (n: 평 문의 길이)

[0100] $H_1 : \{0,1\}^* \rightarrow G^*$ $H_2 : G \rightarrow \{0,1\}^n$

[0101] 보안 증명을 위해, 램덤 오라클로 모든 해쉬 함수를 관찰한다.

[0102] 메시지 공간 $M=\{0,1\}^n$. 암호문 공간 $C = G^* \times \{0,1\}^n$. 출력 시스템 매개변수 = {G, n, α, H_1, H_2}. 마스터 키 $s \in Z^+$. 추출: 주어진 스트링 $ID \in \{0,1\}^*$ 에 대하여 알고리즘은 다음과 같다:

[0103] Step 4: 공개키 $K_{pub} = H_1(ID) \in G$ 를 계산한다.

[0104] Step 5: 비 밀키 K_{priv} 가 $K_{priv} = (K_{pub})^s$ 되게 설정한다(s는 마스트 키).

[0105] 암호: 공개키 ID에서 $m \in M$을 암호하기 위해, 다음과 같이 진행한다.

[0106] Step 6: 공개키 $K_{pub} = H_1(ID) \in G$ 를 계산한다.

[0107] Step 7: 임의의 $\alpha \in \{0,1\}^n$을 선택한다.

[0108] Step 8: $r = H_2(\sigma, m)$을 설정한다.

[0109] Step 9: $\forall c \in C$가 되게 암호를 설정한다. $ID \in G$일 때, $c = (k, ID, m \oplus H_1(ID)^s)$.

[0110] 복호: 개인키 $K_{priv} \in G^*$를 사용하여, $c \in C$를 복호하기 위해 다음과 같이 진행한다:

[0111] Step10: $c \oplus H_2(K_{priv}) = \sigma$를 계산한다.

[0112] Step11: $c \oplus H2(\sigma) = m$을 계산한다 .

[0113] Step12: $r = H2(\sigma, m)$을 설정하고, $c = r\alpha$ 를 시험한다. 만약 $c \neq r\alpha$이면, 암호문을 거절한다.

[0114] Step13: c 의 복호화로 m을 출력한다.

[0115] **********

[0116] **(3) ID기반 센서 노드 인증 프로토콜**

[0117] 일반적인 암호 시스템에서는 마스트 키가 노출되면 모든 사용자의 비밀키가 노출된다. 그러나 제안된 연구는 마스트 키가 노출되더라도 모든 노드의 비밀키는 노출되지 않으며 그 반대도 마찬가지다. 그 이유는 노드의 이동성으로 인한 다중 i 가 항상 변함에 따라 KGC는 키만 생성하는 반면, CH는 키들을 위한 일방향 해쉬 함수로부터 ACL을 관리하기 때문이다. 그러므로 CH는 KGC와 독립적으로 키 인증을 할 수 있다.

[0118] [표 1]을 참조한 도 7에서, KGC는 키 쌍(K_{pub}, K_{priv})을 생성하여 임의(새로운) 노드 N_R(N_{new})과 이동 노드 N_m에게 보낸다. 임의 노드 N_R은 CH에게 클러스터링 요청 메시지(RQC)를 보내고 CH 는 NR의 ID 주소를 포함한 최초의 키 정보를 KGC에게 보낸다. KGC는 N_R의 ID 주소를 포함한 최초의 비밀키를 확인한 후, 키 정보가 정확하면 CH에게 인증 응답 메시지(RPA)를 보낸다.

[0119] 만약 키 정보가 정확하지 않으면 KGC는 CH에게 클러스터링 응답 메시지(RPC)를 보낸다. 새로운 노드 N_{new}가 네트워크에 추가되면 정당한 노드인가를 확인해야함으로, 만약 N_{new}가 인가된 N_R과 같은 ID를 가지면, CH는 N_{new} 에게 RPA를 보낸다.

[0120] 만약 CH가 N_m이 공격자로 의심이 가면, KGC에게 긴급 클러스터링 요청 메시지(ERQC)를 보낸다. KGC는 CH에게

N_m의 ID 주소를 포함한 키 정보를 가진 긴급클러스터링 응답 메시지(ERPC)를 보낸 후, CH는 마스터 키로 N_m 의 비밀키를 인증한다. 만약 CH가 ACL에 의해 그 노드를 인증했다면, N_m에게 RPA를 보내고, 인증하지 못했다 면 N_m 그 자신은 제거된다.

[0121] 같은 방법으로, N_{m1}이 N_{m2}가 공격자로 의심이 가면, N_{m1}은 CH에게 ERQC를 보낸다. CH는 KGC의 키 생성을 바탕으로 구성된 N_{m2}의 ACL 정보와 비교한다. 만약 N_{m2}의 값이 ACL 정보와 일치 하지 않는다면, CH는 KGC에게 ERQC를 보낸 후, KGC는 N_{m2}의 키 생성 정보를 제거하고 CH에게 ERPC를 보낸다. ERPC를 받은 CH는 ACL로부터 N_{m2}를 제거시키는 한편, KGC는 CH에게 N'_{m2}의 업데이트된 키 정보를 포함한 RPC를 보낸다.

[0122] [표 1]

[0123]

Symbol	Meaning	Symbol	Meaning
ID	node ID	RPC	Clustering response message
N_{new}	New node	ERQC	Emergency clustering request message
N_m	Mobile node	ERPC	Emergency clustering response message
N_R	Random node	K_{pub}	Public key
R( )	Routing function	K_{priv}	Private key
H( )	Hash function	K_{pub} sequence	Public key sequence
CH	Cluster Head	KGC	Key Generation Center
RQA	Authentication request message	NBR(N)	The number of neighbor nodes
RPA	Authentication response message	NBR(CH)	The number of neighbor CH
RQC	Clustering request message	ACL	Access control list
s	Master key	APM	Access privilege mask

실 시 예 1

[0124] 시뮬레이션을 통해 본 발명에 의한 키 인증 방법을 평가하였다.

[0125] 시뮬레이션 환경을 위해 컴퓨터 시스템 모델은 Intel Pentium E2220 2 .40GHz, 1.75GB RAM과 운영체제(OS)는 Tiny OS[비특허문헌 17참조]로 하며, 임의의 클러스터 센서 노드수를 500개, 센서 노드 배치 영역은 100m× 100m, 각 노드의 무선 통신 범위는 10m이며, 각 CH는 존의 임의 위치로 한다. 시뮬레 이션은 600초 동안 계속 진행되며, BRITE v2.1b[비특허문헌 18참조]에 의한 정사각형에 임의로 분산된 토폴로지를 생성하며, 센서 노드 간 충돌과 혼잡은 고려하지 않는다.

[0126] 제안된 IBE 스킴의 시뮬레이션은 Chen 외[비특허문헌 19참조]와 Hess[비특허문헌 11참조]의 제안된 스킴과 비교하여 암호화와 복호화의 키 연산에 필요한 CPU 시간과, 센 서 노드의 전송 지연을 분석하였다. [비특허문헌 20]을 참조로 한, 제안된 IBE 스킴의 비교 분석은 [표 2]와 같다. [표 2]는 제안된 IBE 스킴과 페어링으로부터 ID 기반 키 인증의 Chen 스킴[비특허문헌 19참조]의 키 길이에 대한 암호화와 복호화에 필요한 CPU 시간을 나타낸 것으로 시뮬레이션 환경에서 20번 시행한 평균값을 나타내며, 키 길이 160비트의 제안된 IBE 스킴의 암호화, 복호화에 필요한 CPU 시간은 각각 5.7초, 4.3초가 필요하며, 키 길이 1024비트에서[비특허문헌 19참조]의 암호화, 복호화에 필요한 CPU 시간은 각각 11.7초, 19.5초로 계산 시간이 키 길이에 비례함을 알 수 있다. [표 2]의 결과는 [비특허문헌 19참조]스킴이 페어링 키가 각 노드에 저장되어 다른 노드와 통 신을 할 때, 키 발견 연산이 이루어져야 하나, 제안된 IBE는 각 노드가 단지 공개 요소와 비밀키만 연산하기 때문이다.

[0127] [표 2]

[0128]

키 길이(비트)		암호화(초)		복호화(초)	
제안된 IBE스킴	Chen 스킴	제안된 IBE스킴	Chen 스킴	제안된 IBE스킴	Chen 스킴
64	128	3.1	2.8	2.9	3.1
128	256	5.1	3.2	4.2	4.5
160	512	5.7	8.3	4.3	12.3
256	1024	8.3	11.7	6.1	19.5

[0129] 도 8에서 고정된 100m×100m 라우팅 영역의 센서수는 100에서 500까지 100씩 증가하면서 변 한다. 도 8은 제안된 IBE 스킴과 Hess 스킴에서 센서 밀도에 따른 네트워크 전송 지연 시간을 나타내며, 제안된 IBE스킴과 Hess 스킴은 센서 밀도가 증가함에 따라 전송지연 시간이 증가함을 보인다.

[0130] 제안한 I BE 스킴에서는 센서 밀도가 증가할 때, 각 클러스터에 있는 센서 노드 수가 더 많이 있으며, CH에게 전달할 패킷 수가 더 많이 있다는 것을 알 수 있다. 그 이유는 센서 밀도가 증가함에 따라 제안한 IBE 스킴에서의 암호화, 복호화에 필요한 키 연산 증가로 전송지연 시간이 증가함을 알 수 있다. 또한 Hess 스킴은 페어링 기반의 효율적인 ID 기반 서명에도 불구하고 제안한 IBE 스킴보다 전송 지연 시간이 증가함을 보인다.

[0131] 이는 제안한 IBE 스킴이 간단한 라우팅과 3계층의 상호 작용으로 센서 노드의 이동성에 대비하고 안전성을 만족시키기 때문이다.

[0132] 전술한 바와 같이, 센서 노드는 물리적인 환경 공격에 그대로 노출되어 전송 정보가 쉽게 변경되거나 정당하지 않은 노드가 데이터를 전송함으로써 전체 정보의 무결성을 쉽게 무너뜨리며, 악의적 인 노드가 정당한 센서 노드로 가장하여 불필요한 정보를 계속 발생시켜 중간 노드의 자원을 고갈시킴으로써 네트워크 수명을 단축시킬 수 있다.

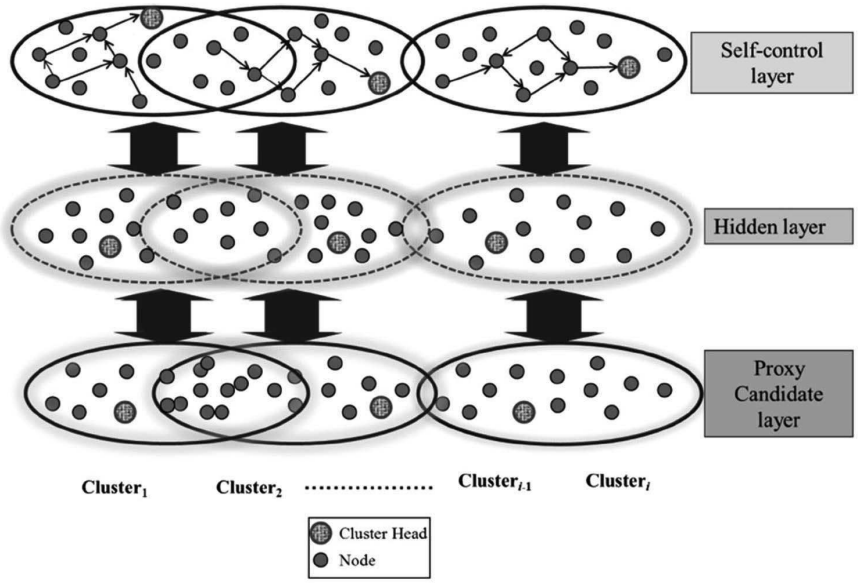
[0133] 그러므로 본 발명은 이러한 문제를 바탕으로 한, 경량화에 중점을 둔 ID 기반 키 인증 기법을 제안한다. 이 기법의 장점으로는 3 계층의 상호 작용으로 제한된 자원 하의 암호화, 복호화에 사용된 CPU 시간을 이전 연구보다 줄일 수 있으며, 센서 노드의 빠른 위상 변화에도 불구하고 이전 연구보다 전송 지연이 향상됨을 보였다.

[0134] 뿐만 아니라, 이전의 키 동의는 각 노드와 KGC에서 이루어지나, 제안된 키 동의는 KGC와 CH에서 키 동의가 이루어지며, KGC는 키 생성만 하고 키 생성 이후키 관리는 CH에서 KGC와는 독립적이며 자율적으로 이루어지므로, 이전의 키 생성기관의 비밀키, 마스터 키노출 문제를 해결할 수 있게 되어, 센서 노드 특성에 적응할 수 있는 키 인증 프로세스를 구축할 수 있다.

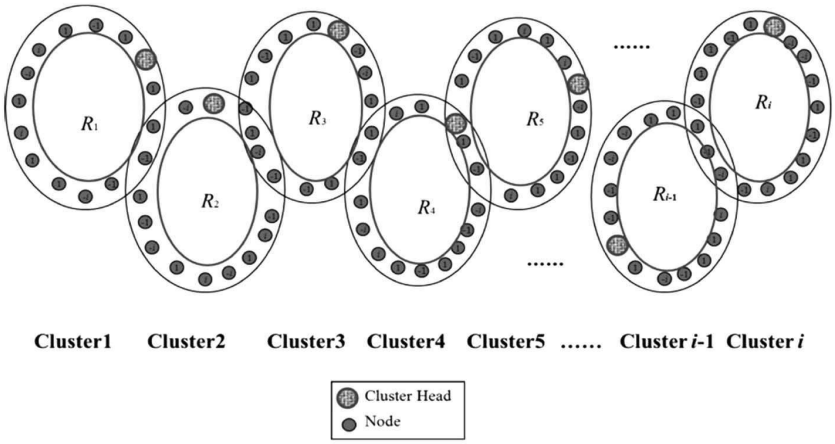
[0135] 따라서 본 발명의 ID 기반 키 인증은 이전의 연구보다 선 분산 키 과정이 필요 없으며, ID 종류가 간단하여 ID를 코드할 바이트 수를 줄일 수 있으며, ID 기반 암호 알고리즘의 공개키, 비밀키 연산량이 적을 뿐만 아니라, 클러스터 내 인증 프로세스에 의한 노드 인증으로 빠른 노드의 삽입과 제거에 대처할 수 있는 능동적인키 인증을 이룰 수 있다.

도면

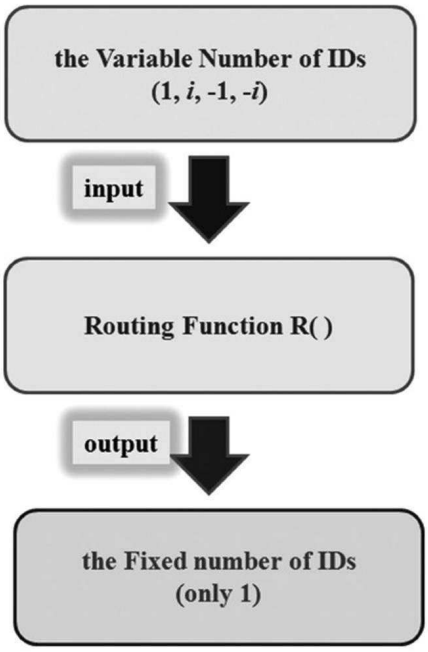
도면1


Self-control layer
Hidden layer
Proxy Candidate layer
Cluster1
Cluster2
Clusteri-1
Clusteri
Cluster Head
Node

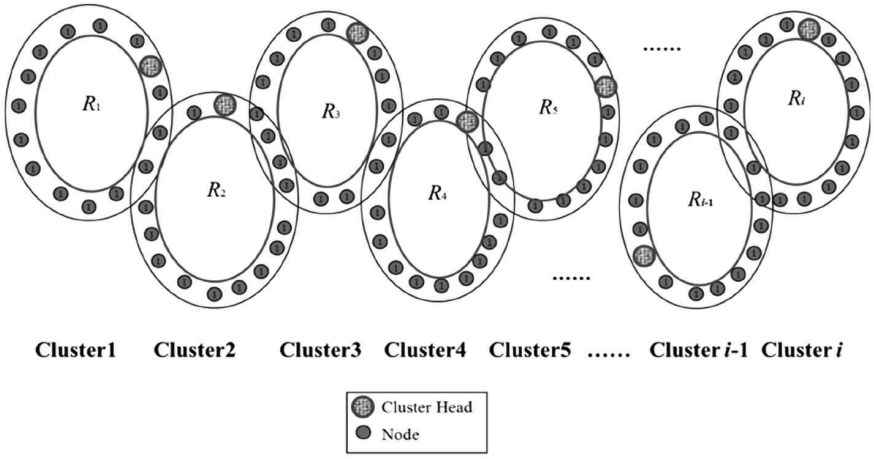
도면2


R1
R2
R3
R4
R5
Ri-1
Ri
Cluster1
Cluster2
Cluster3
Cluster4
Cluster5
Cluster i-1
Cluster i
Cluster Head
Node

도면3


the Variable Number of IDs
(1, i, -1, -i)
input
Routing Function R( )
output
the Fixed number of IDs
(only 1)

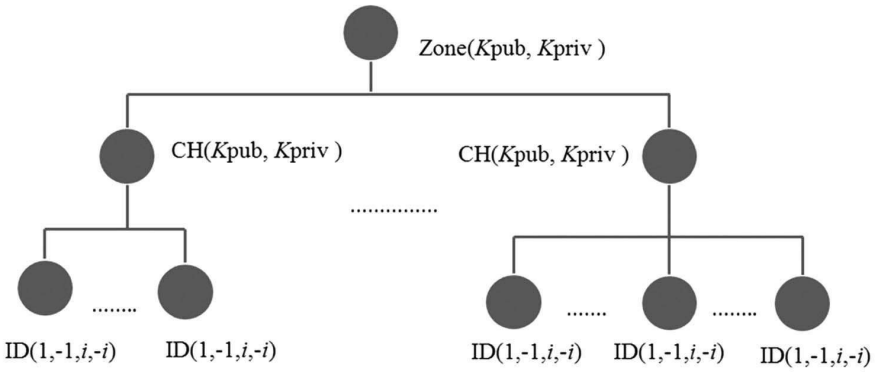
도면4


R1
R2
R3
R4
R5
Ri
Ri-1
.....
.....
Cluster1
Cluster2
Cluster3
Cluster4
Cluster5
.....
Cluster i-1
Cluster i
Cluster Head
Node

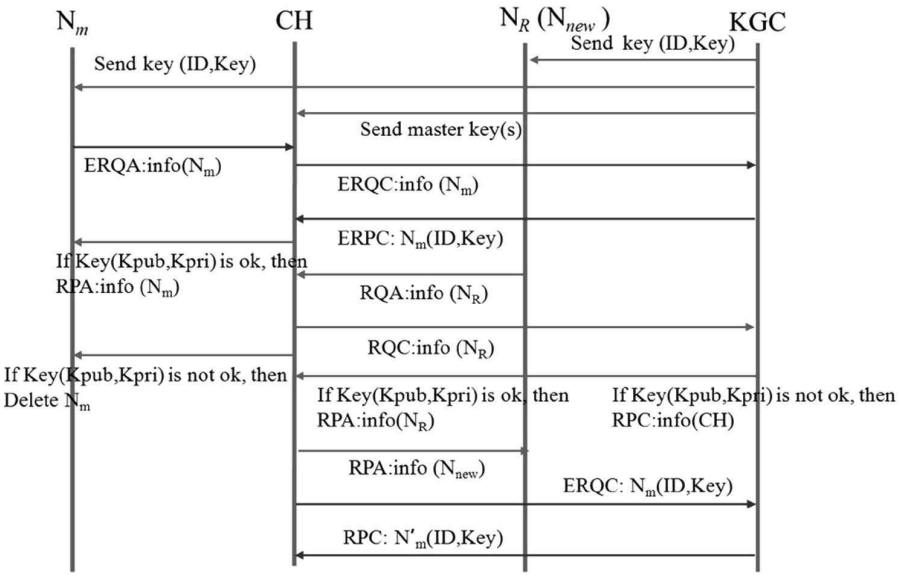
도면5


37459:
13578:
45289:
01: 05: D2: E5: 37: F1
식별자(ID)
공개키(Kpub)
비밀키(Kpriv)
접근 특권 마스크(APM)

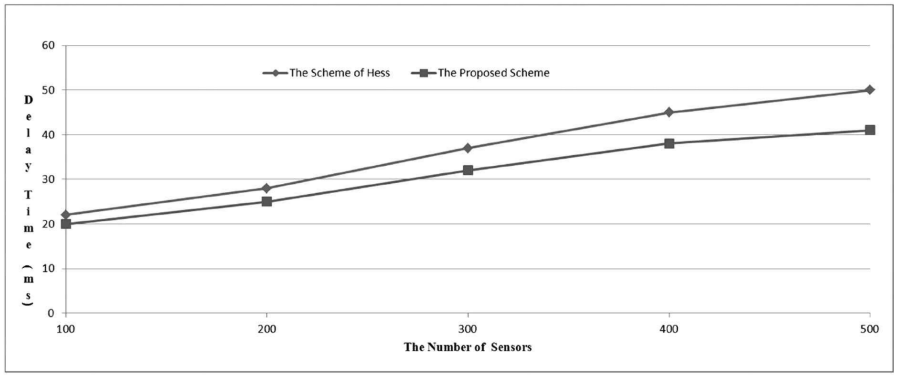
도면6


Zone(Kpub, Kpriv)
CH(Kpub, Kpriv)
CH(Kpub, Kpriv)
ID(1,-1,i,-i)
ID(1,-1,i,-i)
ID(1,-1,i,-i)
ID(1,-1,i,-i)
ID(1,-1,i,-i)

도면7


N_m
CH
N_R (N_{new})
KGC
Send key (ID,Key)
Send key (ID,Key)
Send master key(s)
ERQA:info(N_m)
ERQC:info (N_m)
ERPC: N_m(ID,Key)
If Key(Kpub,Kpri) is ok, then
RPA:info (N_m)
RQA:info (N_R)
RQC:info (N_R)
If Key(Kpub,Kpri) is not ok, then
Delete N_m
If Key(Kpub,Kpri) is ok, then
RPA:info(N_R)
If Key(Kpub,Kpri) is not ok, then
RPC:info(CH)
RPA:info (N_{new})
ERQC: N_m(ID,Key)
RPC: N'_m(ID,Key)

도면8


The Scheme of Hess
The Proposed Scheme
Delay Time (ms)
0
10
20
30
40
50
60
100
200
300
400
500
The Number of Sensors