Journal of the Korea Academia-Industrial cooperation Society
Vol. 23, No. 11 pp. 1-7, 2022

https://doi.org/10.5762/KAIS.2022.23.11.1
ISSN 1975-4701 / eISSN 2288-4688

스마트 더스트 환경을 고려한 경량화 키 관리 및 인증 기법

민소연[1*], 이재승[2]
[1]서일대학교 정보통신공학과, [2]숭실대학교 컴퓨터학과

Lightweight Key Management and Authentication Scheme for Smart Dust Environments

So-Yeon Min[1*], Jae-Seung Lee[2]
[1]Dept. of Information and Communication Engineering, Seoil University
[2]Dept. of Computer Science and Engineering, Soongsil University

요 약 무선 통신과 센서 디바이스의 발전으로 센서를 이용한 사물인터넷(Internet of Things) 환경이 다양한 분야에 적용되고 있다. 사물인터넷 환경은 다양한 분야에서 수많은 데이터들을 수집하고, 가공하여 사용자에게 지능형 서비스를 제공해 준다. 최근에는 초소형 센서, 나노 기술 등의 발전으로 스마트 더스트(Smart Dust)의 관심이 높아지고 있다. 스마트 더스트는 먼지 크기의 센서 디바이스를 사람이 접근하기 어려운 군사 지역이나 산간, 사막 등에 배치하고 무선 통신을 통해 데이터를 수집하는 방법이다. 초기에는 군사적인 목적으로 개발되었으나 현재에는 실생활에서도 활용도가 높아지고 있다. 그러나, 먼지만한 크기의 센서 디바이스를 사용함에 따라 메모리나 연산 능력, 파워 등에 한계점을 가지고 있어 기존의 일반적인 보안 프로토콜을 사용하기에는 무리가 있다. 제안하는 논문에서는 스마트 더스트 환경에 적합한 안전성과 경량화를 적용한 보안 프로토콜을 제안한다. 제안하는 논문은 비트 단위의 인증 기법인 Distance-Bounding 프로토콜과 LEACH 라우팅 프로토콜, 해시 등을 환경에 맞게 개선하여 활용하였으며, 성능 평가를 통해 기존 프로토콜과의 보안성을 확인했다. 또한, 성능적인 측면에서 LEACH 프로토콜과는 약 9%, 기존 보안 프로토콜과는 1.5~4배 정도의 효율성이 있음을 검증하였다.

Abstract With the development of wireless communication and sensor devices, the IoT(Internet of Things) environment has been applied to various fields using sensors. This environment provides users with an intelligent service by collecting and processing data from many sources. Due to the recent microsensor and nanotechnology developments, the Smart Dust method has attracted considerable attention. This method provides a means of collecting data through wireless communication from dust-sized sensor devices located in inaccessible areas such as deserts, mountains, or military zones. This technology was initially developed for military purposes, but it is now being utilized in the civilian sector. However, dust-sized sensor devices have limited memories, computing abilities, and powers and thus are incompatible with existing general security protocols. In this study, we propose a security protocol suitable for smart dust environments based on an improved bit-unit authentication technique called Distance-Bounding Protocol, LEACH Routing Protocol, and Hash. Performance assessments verified the security and performance of this protocol.

Keywords : Smart Dust, IoT Authentication, IoT Security, Key Management, IoT

본 논문은 서일대학교 학술지원비에 의해 연구되었음.
*Corresponding Author : So-Yeon Min(Seoil Univ.)
email: symin@seoil.ac.kr
Received September 20, 2022 Revised October 31, 2022
Accepted November 4, 2022 Published November 30, 2022

1. 서론

사물인터넷은 네트워크를 통해 사물들을 연결하여 사람과 사물 혹은 사물들 간의 상호 통신으로 정보를 공유하는 지능형 기술 및 서비스를 의미한다. 사물인터넷은 다양한 환경에서 지능형 서비스를 제공하기 위해 데이터를 수집하고, 사용자의 정보, 요구사항, 환경 등을 고려하여 서비스를 제공하며 디바이스를 제어한다. 최근에는 무선 통신 기술의 발전과 소형 센서를 포함한 디바이스들의 발달로 기존 무선 센서 네트워크 환경을 기반으로 한 사물인터넷 환경이 홈 네트워크나 웨어러블 서비스와 같은 일상적인 서비스는 물론 군사 및 산간 지역, 의학, 상업적인 용도 등 폭넓게 활용되고 있다. 특히, 초소형 센서를 통해 활용되는 똑똑한 먼지, 즉 스마트 더스트의 개념이 활용 가능해짐에 따라 사람들이 접근하기 쉽지 않은 군사 지역이나 산간 지역 등에 센서를 배치하고 해당 지역 데이터를 수집하는 등 다양한 활용 가능성을 보여주고 있다. 이러한 스마트 더스트를 활용한 IoT 환경은 무선 센서를 이용해 데이터를 감지하고 이 정보를 BS(Base Station)이나 중간 센서 노드들로 전송하는 센서 노드로 구성되어 있다. 이때, 스마트 더스트와 같은 환경에서 활용하는 센서 디바이스들의 경우 초소형으로 이루어져 있어 한정된 메모리로 인한 저장 및 처리능력, 에너지 효율성의 한계를 가지고 있고, 이로 인해 제한된 자원을 활용하기 위한 다양한 연구가 진행되고 있다[1-3].

따라서, 본 논문에서는 제한된 환경에서 보안성 및 에너지 효율성을 고려하여 처리 능력 및 계산 속도, 저장 공간 등에 크게 제약이 없는 해시함수를 활용한 경량화된 상호인증 및 키 관리 방법을 연구하였다.

2. 관련 연구

2.1 사물인터넷

사물인터넷은 1999년 MIT Auto-ID Center 설립자인 Kevin Ashton에 의해 최초로 개념 및 용어가 제안된 후 통신 및 센서 디바이스의 발전을 거쳐 현재는 일상생활에서 여러 방면에서 활용되고 있다[4].

사물인터넷에 기반한 서비스는 일상생활에서 쉽게 찾아볼 수 있다. 스마트 홈이나 스마트 카, 웨어러블, e-헬스케어 등 다양한 방면에서 서비스가 상용화 되고 있으며, 활용 범위 또한 지속적으로 늘어나고 있다. 해당 서비스를 활용하기 위해서는 디바이스 간의 통신이 필요하며 많은 제품들이 M2M(Machine-to-Machine) 기술에 기반 하여 서비스 되고 있다.

최근에는 초소형 센서를 이용한 스마트 더스트 환경이 주목받고 있으며, 초소형 센서를 활용하는 만큼 메모리 공간이나 연산 등을 효율적으로 수행하기 위한 연구들이 진행되고 있다.

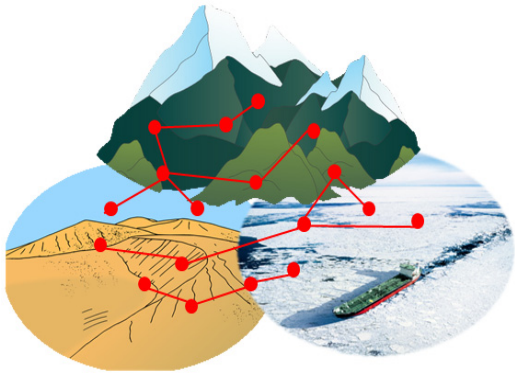

Fig. 1. Examples of Smart Dust Utilization

2.2 스마트 더스트(Smart Dust)

통신 기술과 초소형 센서, 나노 기술 등의 발전으로 스마트 더스트의 개념이 다양한 분야에서 활용되고 있다. 스마트 더스트는 미국 캘리포니아 대학의 크리스 피스터 교수가 1~2mm 먼지 크기의 초소형의 센서를 개발하고, 그 이름을 '스마트 더스트'라고 지칭한 데서 유래되었다. 먼지 크기만큼 작은 이 초소형 센서는 아주 작은 크기에도 불구하고 컴퓨팅 능력을 가지고 있으며, 통신 기술을 이용하여 데이터를 주고받는 등 상호 소통이 가능하다는 장점을 가지고 있다. 스마트 더스트는 초기에 군사적 목적으로, 적군의 위치를 파악하기 위해 고안되었으나, 현재는 사람들이 접근하기 어려운 산간 지역의 산불이나 홍수 같은 자연재해 예방이나 생태 관측 등에 활용되고 있으며, 보통 하나의 센서 디바이스는 다른 디바이스들과 함께 네트워크를 형성하고, 상호 작용을 통해 유의미한 정보를 도출하여 사용자 에게 제공된다[5-7].

스마트 더스트 센서 디바이스의 경우 앞서 서술한 것처럼 먼지 크기의 센서를 이용해 다양한 데이터를 수집할 수 있다는 장점이 있지만, 보안상의 취약점이 존재한다. 크기가 작아진 만큼 센서 디바이스들은 메모리 공간이나 파워 등의 한계로 저성능으로 이루어져 있으며, 이는 인증 절차에 문제를 일으킬 수 있다. 안전한 인증 프로토콜을 이용한다면, 디바이스의 성능 한계로 인해 시간이 지연될 수 있으며 이때 인증정보의 노출 등이 문제

가 발생할 수 있다. 경량화 인증을 이용할 경우 빠른 상호작용이 가능하지만 인증절차 간소화로 인한 보안 문제가 발생할 수 있다.

즉, 한정된 자원으로 센서 디바이스가 가지는 한계점을 고려한 안전한 인증 기법이 중요하게 대두되고 있다.

3. 제안 내용

제안하는 프로토콜은 Distance-Bounding와 LEACH 라우팅 프로토콜을 환경에 맞게 개선하고[7,8], 해시 함수 및 XOR 연산을 통해 저연산 인증 방법을 제안하였다. 센서 디바이스들은 특정 주기에 거쳐 대표 디바이스를 선정하고 그룹을 형성 한다. 그룹 내에서는 대칭 키를 이용한 데이터 통신을 하며, 대표 디바이스는 게이트웨이와 비대칭 통신을 통해 데이터를 전송한다. 대표 디바이스는 지속적으로 변경되어 특정 디바이스에 가중되는 부담을 분산 한다.

Table 1. Proposed Notation

Notation	Meaning
N_v, N_p	Nonce
SN	Serial Number
GW	Gateway
$E()$	Encryption
$D()$	Decryption
ID	Sensor ID
C_{id}	Middle Node ID
R_i^n	3n Bit Divided Value
p, q, z	Prime Number
R	Random Number

3.1 디바이스 초기인증

본 논문에서 제안하는 프로토콜의 그림에서는 GW의 광고를 수신하여 대표 디바이스가 GW에 접속 하는 절차는 생략하였다. 라우팅 프로토콜을 통해 대표 디바이스를 선출하고 지역 내 광고를 통해 조인 메시지를 응답한 디바이스들과 함께 그룹을 형성한다. 그룹 내 데이터 수집 및 인증 절차는 대표 디바이스를 통해 이루어지며, 특정 주기로 그룹을 재선정한다. 인증 및 키 교환 과정은 다음과 같으며, 해당 과정에서 암·복호화, 난수를 이용한 해시 절차, 비트 교환을 통한 인증 방법에 대한 자세한 수식은 그림을 통해 자세히 설명하였다.

Step 1. 대표 디바이스로부터 광고를 수신한 센서 디바이스는 본인 인증을 위한 정보로 M_0, H_0를 생성 후 전송한다.

Step 2. M_0, H_0 수신한 디바이스는 M_1, H_1를생성하여 전송한다.

Step 3. GW는 암호화 하여 Provider에게 전송하며, 전송된 데이터는 복호화를 통해 H_0과 H_1를 검증한다. 이후, M_2, M_3를 생성한 후 GW를 통해 대표 디바이스로 전송한다.

Step 4. M_2, M_3를 대표 다비이스는 M_3를 복호화하여 R_1 값을 획득하고, 해시 함수를 사용해 해당 값의 무결성을 검증한다. 검증 후 Distance-Bounding절차를 위해 난수들의 조합으로 만든 3*n비트의 생성 및 저장한다. 센서 디바이스에게는 M_2를 전송한다.

Step 5. M_2를 수신한 센서 디바이스는 R_2를 이용해 해시로 전송된 값을 검증한다. 검증에 성공하면 Step 4. 절차와 마찬가지로 3*n비트를 저장한다.

Step 6. 센서 디바이스는 인증이 필요할 경우 대표 디바이스에 인증을 요청한다. 랜덤한 수 c_i를 생성하고 한 비트씩 송신을 통해 검증한다. 이때, Relay Attack 확인을 하기 위해 Time on 상태를 유지한다.

Step 7. 센서 디바이스로부터 비트를 받은 대표 디바이스는 c_i 값이 0과 1일 때에 따라 각각 R^c, R^1의 i번째 비트를 센서 디바이스에게 전송한다.

Step 8. 센서 디바이스는 송신 값 c를 기준으로 R_i^{cn}을 생성하고, 전송 받은 값들을 취합하여 R_i^{cn}값과 비교한다. 해당 절차를 통해 올바른 디바이스로부터 데이터를 수신했는지 확인하고, Time off 이후 시간 측정을 이용해 특정 이상 시간이 발생할 경우 통신을 중단한다.

Step 9. 디바이스들은 정상적으로 데이터가 확인 될 경우 R_i^{cn}를 함수를 통해 저장하고 3*n bit의 남은 비트 및 랜덤 정보를 이용하여 세션 키를 생성하고 데이터를 송수신 한다.

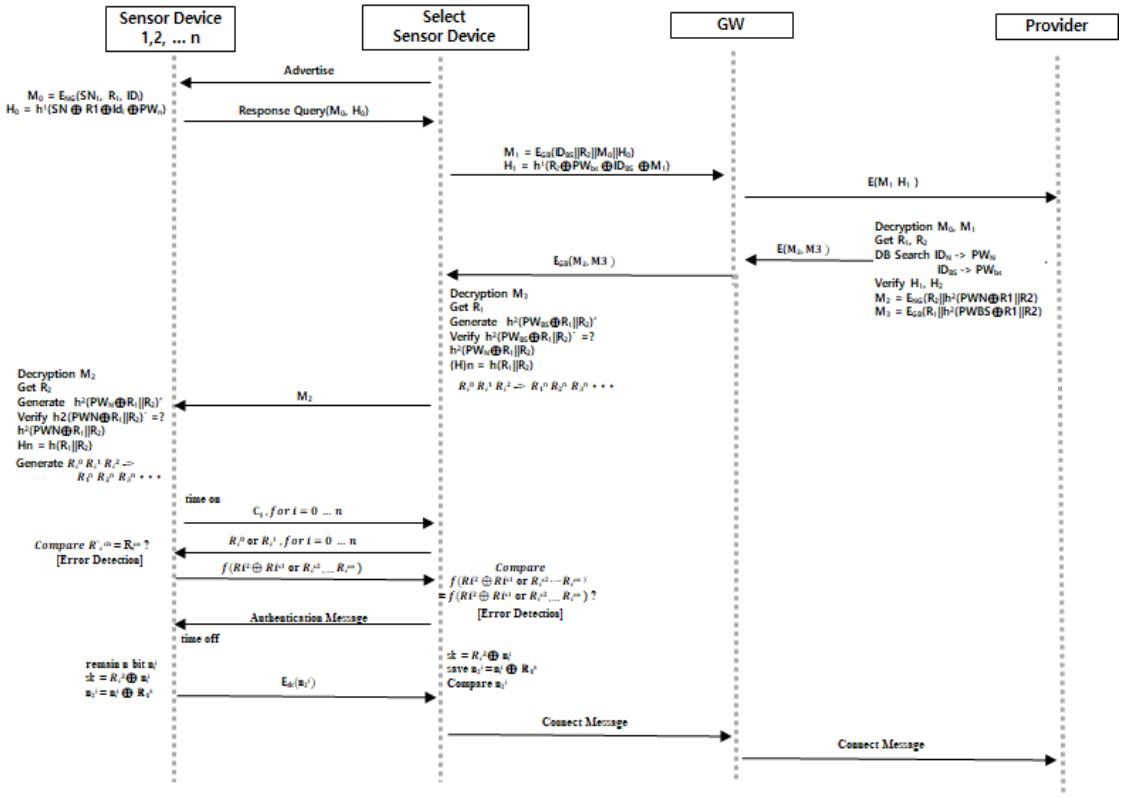

Fig. 2. Authentication Protocol

3.2 키 관리

그룹 내 센서 디바이스 간 통신을 위해 사용되는 그룹 키 관리는 다음과 같다.

Step 1. 센서 디바이스들은 P값을 대표 디바이스에 게 전송한다.

Step 2. 대표 디바이스는 센서들이 보낸 값을 이용하여 다항식을 통해 키 값을 생성한다.

Step 3. 공유된 키 값을 받은 센서노드들은 해당 키를 이용하여 데이터를 주고받으며, 키 노출, 분실등의 문제가 발생할 경우 대표 디바이스에게 키 갱신을 요청한다.

Step 4. 새로운 대표 디바이스가 선정될 경우 해당 키는 폐기 한다.

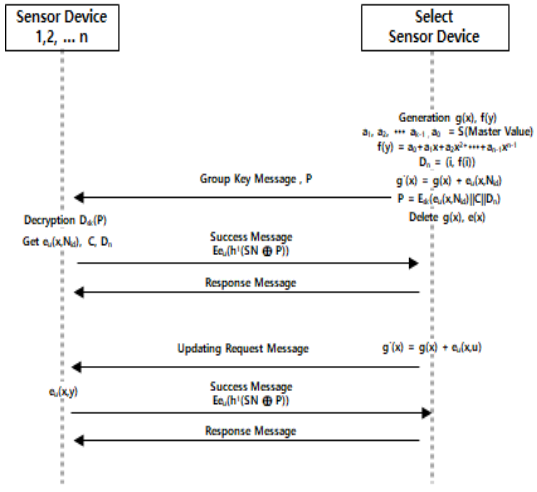

Fig. 3. Key Exchange Protocol

4. 성능 평가

본 절에서는 기존 사물인터넷 환경에서 제안된 키 관리 및 인증 프로토콜과의 비교를 통해 안전성을 검증한다. 검증 요소는 사물인터넷 환경에서 요구되는 보안 요구사항을 기준으로 작성되었다. 또한, 기존 프로토콜과의 성능 비교를 통해 에너지 효율성에 대해 검증하였다.

4.1 보안성 평가

보안성 평가를 위해 기존 경량화 인증 기법을 기준으로 비교하였으며, 경량화 인증의 경우 저성능 디바이스의 효율적 운용을 위해 보안성에 있어 취약점 부분들이 존재 하였다. 본 논문은 테스트 결과 IoT 환경에서의 보안 요구사항을 충족하였다.

Table 2. Security Analysis

	blundo's [9]	farash [10]	Dave's Protocol [11]	Khusvinder [12]	Proposed scheme
Relay attack	X	X	O	O	O
Replay attack	X	O	X	O	O
Eaves dropping	O	O	X	X	O
Leaked key	X	X	O	X	O
Mutual authentication	X	X	X	O	O

디바이스 간의 등록 과정에서는 사전 정보인 시리얼 값을 통해 등록하였으며, 비대칭 암호 프로토콜의 경우 대표 센서 디바이스를 기준으로만 사용되었다. 대표 센서의 인증절차 이후에는 해당 디바이스를 기준으로 그룹 키를 관리, 제안하는 대칭 암호화를 통해 성능 향상 및 기밀성과 무결성을 보장하였다. 제안하는 프로토콜은 향상된 LEACH 프로토콜을 활용하여 대표 디바이스가 지속적으로 변경되어 특정 디바이스의 부하가 집중되는 현상이 없도록 하였다. 또한, 대표 디바이스와 GW간 통신에서는 안전한 채널을 이용하고, 대표 디바이스와 일반 센서와의 통신에서는 합의된 그룹 키 및 파라미터의 hash함수를 이용하여 상호인증이 가능하도록 하였다. 내장된 시리얼 및 합의된 키 값으로 통신을 진행함으로 악의적인 사용자에 의해 메시지가 탈취되더라도 해독할 수 없으며 익명성 또한 보장된다.

4.2 효율성 검증

본 논문에서는 에너지 효율성 분석을 위해 표 3에서 기술된 환경에서 시뮬레이션을 진행하였다.

Table 3. Simulation Initial Settings

Simulation Initial Settings	
Number of Device	50 ~ 300
Placement Area	100m*100m~300m*300m
Control Center Location	X=50m, y=50m
ETX, ERX	50 nanoJ
Packet Size	5,000 bit

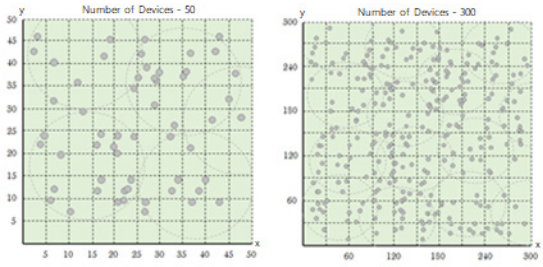

Fig. 4. Performance Simulation

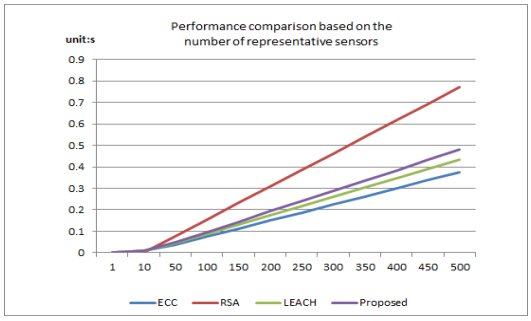

Fig. 5. Performance assessment of representative devices

디바이스의 개수와 배치 지역, 컨트롤 센터의 위치는 가변적으로 변경하며 진행하였고, 각각의 라운드는 기본 30sec에서 반경에 따라 변경했다. 기존의 보안 프로토콜과 비교했을 때, 에너지 효율성에서 대표 디바이스 기준 1.6배, 일반 센서 기준 2~4.5배의 큰 차이를 보이며, LEACH 프로토콜과는 큰 차이를 나타내지 않았다. 대표 디바이스와 일반 센서 기준으로 LEACH 프로토콜의 비해 약 9% 차이가 있지만, LEACH 프로토콜이 보안성이 아닌 라우팅 프로토콜임을 고려한다면 성능 면에서 우수함을 확인할 수 있었다.

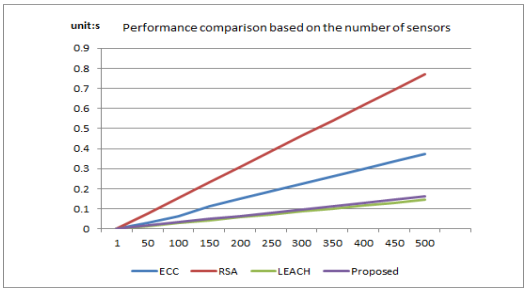

Fig. 6. Sensor Device Performance Assessment

5. 결론

본 연구에서는 사람이 쉽게 접근하기 힘든 산간 및 군사 지역, 사막 등과 같은 지역에서 데이터 수집에 용이한 스마트 더스트 환경을 고려한 효율적인 보안 프로토콜을 제안하였다. 즉, 에너지 효율성 향상을 위해 비트 단위 인증 기법인 Distance-Bounding 프로토콜과 LEACH 라우팅 프로토콜, 해시와 XOR 연산 등을 환경에 맞게 응용하여 활용하였으며, 그룹 키 관리 방법을 적용하여 효율적인 디바이스 관리 방안을 통해 성능적인 측면에서 단순 라우팅 프로토콜인 LEACH 프로토콜과 약 9% 정도의 차이를 나타냈다. 또한, 기존 보안 프로토콜과는 1.5~4배 정도의 효율성이 있음을 검증하였다. 제안하는 프로토콜을 활용한다면 센서 디바이스의 효율성을 향상시켜 안전하고 효율적인 지능형 서비스 제공이 가능함을 확인할 수 있었으며, 향후 에는 웨어러블 서비스와 같은 이동형 서비스와 접목하는 방안에 대해 연구할 예정이다.

References

[1] DI MARTINO, Beniamino, et al. Internet of things reference architectures, security and interoperability: A survey. Internet of Things, 2018, 1: 99-112.
DOI: https://doi.org/10.1016/j.iot.2018.08.008

[2] DA XU, Li; HE, Wu; LI, Shancang. Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 2014, 10.4: 2233-2243.
DOI: https://doi.org/10.1109/tii.2014.2300753

[3] ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. Computer networks, 2010, 54.15: 2787-2805.
DOI: https://doi.org/10.1016/j.comnet.2010.05.010

[4] CUI, Xiaoyi. The internet of things. In: Ethical ripples of creativity and innovation. Palgrave Macmillan, London, 2016. pp. 61-68.
DOI: https://doi.org/10.1057/9781137505545_7

[5] KAHN, Joseph M.; KATZ, Randy H.; PISTER, Kristofer SJ. Next century challenges: mobile networking for "Smart Dust". In: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking. 1999. pp. 271-278.
DOI: https://doi.org/10.1109/icn.2000.6596708

[6] NICCOLAI, Lorenzo, et al. A review of Smart Dust architecture, dynamics, and mission applications. Progress in Aerospace Sciences, 2019, 106: 1-14.
DOI: https://doi.org/10.1016/j.paerosci.2019.01.003

[7] BRANDS, Stefan; CHAUM, David. Distance-bounding protocols. In: Workshop on the Theory and Application of Cryptographic `Techniques. Springer, Berlin, Heidelberg, 1993. pp. 344-359.
DOI: https://doi.org/10.1007/3-540-48285-730

[8] SINGH, Sunil Kumar; KUMAR, Prabhat; SINGH, Jyoti Prakash. A survey on successors of LEACH protocol. Ieee Access, 2017, 5: 4298-4328.
DOI: https://doi.org/10.1109/access.2017.2666082

[9] BLUNDO, Carlo, et al. Perfectly-secure key distribution for dynamic conferences. In: Annual International Cryptology Conference. Springer Berlin Heidelberg, pp. 471-486. 1992.
DOI: https://doi.org/10.1006/inco.1998.2717

[10] Farash, Mohammad Sabzinejad, Turkanović Muhamed, Kumari Saru, and Marko Hölbl. "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment." Ad Hoc Networks 36 (2016): 152-176.
DOI: https://doi.org/10.1016/j.adhoc.2015.05.014

[11] SINGELEE, Dave; PRENEEL, Bart. Location verification using secure distance bounding protocols. In: IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005. IEEE, p. 7 p. 840. 2005.
DOI: https://doi.org/10.1109/mahss.2005.1542879

[12] Gill, Khusvinder, Shuang-Hua Yang, and Wan-Liang Wang. "Secure remote access to home automation networks."IET Information Security 7.2 (2013): 118-125.
DOI: https://doi.org/10.1049/iet-ifs.2011.0303

민 소 연(So-Yeon Min) [종신회원]

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신공학과 교수

〈관심분야〉
통신 및 신호처리, 정보통신, 임베디드 시스템

이 재 승(Jae-Seung Lee) [정회원]

- 2013년 2월 : 평생교육진흥원 컴퓨터학과 (공학사)
- 2015년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2017년 3월 : 숭실대학교 컴퓨터학과 박사수료
- 2019년 2월 ~ 2022년 3월 : (주) IOSYS 연구소 연구원

〈관심분야〉
시큐어코딩, Sensor Network, IoT Security