https://doi.org/10.5392/JKCA.2020.20.08.359

무선 센서 네트워크 위치 검증 기법 분류

Classification of Location Verification in WSNs

김인환
연세대학교 컴퓨터과학과

In-hwan Kim(inhwan.kim00@gmail.com)

요약

IoT(Internet of Things)의 주요기술인 WSNs(Wireless Sensor Networks)는 위치를 기반으로 정보를 전달하거나 인증을 하는 경우가 많기에 잘못된 위치 정보는 서비스에 큰 위험이 된다. 따라서 위치 정보를 검증하는 방법은 필수적이다. 목적에 적합한 기법을 설계하기 위해서는 기존 연구들에 대한 통합적인 분석과 분류 결과가 중요하다. 본 논문은 WSN 를 대상으로 개발된 위치 검증 기법들의 특징에 대해 통합적인 분석 및 분류 결과를 제시하는 것을 목표로 한다. 이를 위해 기발표된 주요 위치 검증 기법들의 특징 분석 결과를 바탕으로 분류 기준을 설정한다. 그리고 설정한 분류 기준에 따라 기존 연구 결과를 분류하고 각각의 특징과 발전 방향을 기술한다. 본 논문의 결과는 기존의 위치 검증 기법 분석 및 분류 연구와 비교해, 보다 다양한 기준을 제시하고 있다는 점에서 신규 기법의 설계시 유용한 참고자료가 될 것으로 기대된다.

■ 중심어 : | 분류기준 | 특징분석 | 위치검증 | 무선센서네트워크 | 과학기술 |

Abstract

WSNs as the main technology of IoT often deliver information or authenticate based on location. Thus, verifying location information is essential. This paper aims to present the comprehensive analysis and classification of location verification techniques in WSN. For this, classification criteria are suggested based on the result of feature analysis of existing techniques. In addition, the existing techniques are classified according to the suggested criteria, and each characteristic and development direction are described. The result of this paper is expected to be a useful reference material when designing a new technique.

■ keyword : | Classification Criteria | Feature Analysis | Location verification | Wireless Sensor Networks | Science Technology |

I. 서 론

WSN(Wireless Sensor Networks)은 수많은 센서들로 구성된 네트워크이다. 센서들은 온도나 움직임 감지, 데이터 처리, 무선 통신과 같은 능력을 갖고 있다. 이같은 능력을 활용해 타겟 환경에서 발생하는 데이터를 수집할 수 있다. 수집된 데이터는 일반적으로 무선 통신을 이용해 주변 노드와 협력하여 싱크 노드(Sink node)라 불리는 센서로 전달된다. WSN은 사람이 접근하기 어려운 환경에 배치되어 물건, 환경, 사람 등에 대한 상태 모니터링이나 추적을 위한 어플리케이션에 사용된다[1]. 이러한 어플리케이션은 보통 지리 기반 라우

접수일자 : 2020년 07월 14일
수정일자 : 2020년 08월 10일
심사완료일 : 2020년 08월 10일
교신저자 : 김인환, e-mail : inhwan.kim00@gmail.com

팅[2]이나 위치 기반 인증[39] 등을 바탕으로 구현된다.

센서의 위치를 획득하는 잘 알려진 방법은 GPS (Global Positioning System)[4]를 이용하는 것이다. 그러나 모든 센서에 GPS를 장착하는 것은 비용 측면에서 효과적이지 못하다[5]. 위치를 획득하는 또 다른 방법은 위치 계산법(Localization)[6]을 이용하는 것이다. 위치계산법은 보통 자신의 위치를 알고 있는 앵커(Anchor) 노드를 기준으로, 자신의 위치를 알지 못하는 위치불명센서(Unknown Sensor)의 위치를 계산한다.

위치 정보는 에러 혹은 악의적인 사용자에 의해 변조될 가능성이 있다. 시빌(Sybil) 공격, 웜홀(Wormhole) 공격 등에 의해 조작된 위치 정보가 사용되는 경우 WSN의 미션 성공에 매우 치명적인 영향을 준다[3]. 예를 들어, 군사 작전 지역에 배치된 센서를 통해 측정된 환경의 변화를 바탕으로 작전을 수행하는 상황에서, 위치 정보의 훼손 여부 검증은 매우 중요하다. 또 다른 예로, 빌딩 내에서만 접근을 허용하는 자원이 있을 때, 해당 자원에 대한 사용요청을 허가하기 위해 사용자의 위치 정보 검증은 필수라 할 수 있다.

본 논문은 WSN 환경을 대상으로 한 주요 위치 검증 기법(Location Verification)들의 특징에 대해 통합된 분석과 분류 결과를 제시하는 것을 목표로 한다. 이를 위해 먼저 기발표된 위치 검증 기법의 특징을 분석한다. 분석된 특징을 바탕으로 기반 기술들을 확인하고 분류 기준을 세운다. 마지막으로 정의된 분류 기준의 특징을 정리하고 이에 따라 기존 연구 결과를 분류하고 발전방향을 기술한다. 제시된 분류 기준과 분석 결과는 새로운 위치 검증 기법 설계에 기여할 수 있을 것으로 기대된다.

본 논문의 II 장에서는 주요 위치 검증 기법과 이를 분류한 연구에 대해 소개한다. III 장에서는 주요 위치 검증 기법의 특징에 대해 분석하고 이를 바탕으로 분류 기준을 정의한다. 또한, 제시된 분류 기준에 따라 기존의 기법들을 분류하고 발전방향을 정리한다. 마지막으로 IV 장에서는 결론을 기술한다.

II. 관련 연구

위치 정보를 보호하는 방법은 [그림 1]처럼 안전한 위치 계산법(Secure Localization)과 위치 검증 기법으로 분류할 수 있다. 두 방법은 궁극적으로 모두 신뢰할 만한 위치 정보를 제공하는 것을 목표로 하지만 사용 측면에서 차이가 있다.

안전한 위치 계산법은 각종 공격으로부터 위치 측정 과정을 보호해 올바른 위치 정보를 계산하는 것에 중점을 두고 연구가 이루어졌다[7]. 그러나 위치 정보를 사용하는 시점에서는 악의적으로 잘못된 정보를 사용할 가능성이 있으므로, 이를 막기 위해 위치 검증 기법에 대해서도 많은 연구가 이루어졌다[8-22].

위치 정보 검증은 인증 프로토콜을 보완하는 과정에서 시작되어 여러 가지 방식으로 연구가 이루어졌다. 초기에는 Fiat-Shamir 인증 프로토콜[23]의 취약점을 보완하는 Chaum 의 논문에서 언급된 Distance Fraud 에 대한 방어법으로 Distance Bounding (DB) [24]이 소개되었다. DB 프로토콜은 증명자(Prover)와 검증자(Verifier) 간에 주고받는 암호학적인 Challenge-Response 메시지의 왕복시간을 이용해 증명자 위치의 Upper Bound 를 계산하는 방법이다. 메시지 왕복시간 이외에도 무선 신호 감쇠 현상, 신호 수신 소요 시간, 신호 수신 각도 등의 위치계산법을 이용하기도 하는데, 이 때에는 보다 정확한 위치 검증이 가능하다. 그 밖에도 센서 간의 관계를 바탕으로 논리적인 연결성을 검증함으로써 목적을 달성하기도 한다.

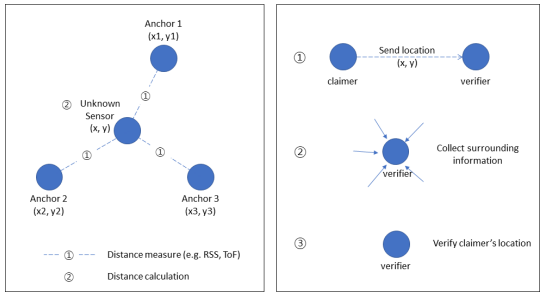

그림 1. Localization 과 Location verification

이처럼 다양한 방식으로 개발되어온 위치 검증 기법들의 특징을 분석하고 분류하는 연구는 보다 향상된 기법의 개발 혹은 특정 어플리케이션에 적합한 기법의 개발에 있어 매우 중요한 시작점이 될 수 있다. 이런 관

점에서 위치 검증 기법에 대한 분석 및 분류 연구가 있었다[3][25].

Jiang[3]은 안전한 위치 계산이라는 관점에서 안전한 노드 인증 기법과 위치 검증 기법에 대해 분석 및 분류했다. 위치 검증 기법에 대해서는, 잘못된 위치 정보를 처리하는 방법을 기준으로 정보의 필터링과 검증으로 분류 기준을 제시했다. 그리고 각각의 분류 기준에 맞춰 기개발된 기법들의 특징을 소개했다. 하지만 위치 계산과 위치 검증을 모두 다루었기 때문에 위치 검증에 대한 보다 세부적인 분류는 미흡한 부분이 있었다. 즉, 두 가지 큰 분류 기준을 제시한 것 이외에는 각 기법의 기반 기술에 대한 분석과 특징을 간단하게 소개하는 정도에 그쳤다.

Zeng[25]은 안전한 위치 계산법과 위치 검증 기법을 분리해서 센서의 위치 정보 보안에 대해 통합적인 리뷰를 수행했다. 위치 검증 기법은 목적에 따라 In-region 과 Single-point 검증으로 구분하고, 각각에 대해 한 번에 검증 가능한 수에 따라 Batch 와 One-by-one 검증으로 구분했다. 그리고 위치 계산 시스템에 수행 가능한 기본 공격과 복합 공격을 자체적으로 정의하고 기존 연구들의 방어 가능 여부를 판단해 제시했다. 하지만, 각 기법의 기반 기술에 대해서는 분석이 미흡했으며, 특성에 대해서는 추가 H/W에 대한 내용만 간단히 언급하는데 그쳤다.

III. 위치 검증 기법 분석 및 분류

본 논문에서 분석한 위치 검증 기법들은 기존의 분석 및 분류 논문에서 다룬 기법들을 공통적으로 포함했으며 추가적으로 최근 논문들을 대상으로는 분야의 키워드가 일치하며 인용수가 있는 기법을 대상으로 했다. 다만, WSN을 대상으로 한 위치 검증 기법들이 많지 않은 관계로 논문의 선정에는 제약이 있었다.

1. 위치 검증 기법 특징 분석

Sastry는 DB 프로토콜을 기반으로 목표 영역 내 대상의 존재여부를 확인할 수 있는 Echo 프로토콜을 제안했다[8]. Echo 프로토콜은 암호화를 사용하지 않아 CPU와 메모리 요구사항을 낮출 수 있었고, 전파와 울트라사운드를 사용해 DB 프로토콜 대비 안전성을 확보함과 동시에 증명자에서의 프로토콜 처리시간 지연을 일정 부분 수용하도록 설계되었다. 또한, 노드 간의 시간 동기화를 필요로 하지 않아 보다 가벼워졌다.

Du는 위치 정보 이상 여부를 Anomaly Intrusion Detection 문제로 정의하고 Location Anomaly Detection (LAD) 기법을 제안했다[10]. 이 기법은 센서의 배치 상태 사전 지식과 센서의 추정 위치 불일치 여부를 바탕으로 거짓 위치 주장(Claim)을 탐지한다. 하지만 앞서 언급한 것처럼 센서 배치 정보가 필요하며 많은 노드가 위치 검증 프로세스에 참여해야 하는 문제가 있다. 이와 유사하게 [17-19] 에서도 위치 검증을 탐지 시스템의 일종으로 형식화해 문제를 해결하고자 했다. 이같은 방식에서는 검증 문제를 수학적으로 표현 가능하므로 보다 명확한 알고리즘 검증이 가능하다. 그러나 이 기법들은 검증자 역할을 하는 고정 노드가 필요하다는 조건이 있다.

Hwang 의 팬텀 노드(Phantom node) 탐지 기법은 노드의 위치 대신 이웃 노드 간의 거리를 이용해 생성한 로컬 맵을 위치 검증에 이용했다[11]. 이 기법은 위치 정보를 직접 사용하지 않기 때문에 공격자가 검증 기법을 통과하는 가짜 위치를 계산하기 어려우며, 공격자가 정직한 노드보다 많은 상황에서도 대부분의 공격자들을 걸러낼 수 있다. 다만, 검증을 위해서는 모든 노드가 주변 노드와의 거리를 계산해서 보내야 하므로 통신 부하가 있으며, 협력 공격자 모델에 대해서는 안전성이 확인되지 않았다.

Ekici는 센서간 홉-거리(Hop-Distance)를 이용하는 확률 위치 검증 기법을 제안했다[12]. 일련의 검증자는 증명자로부터 패킷을 수신하고, 패킷이 이동한 유클리드 거리와 홉 카운트 간의 통계적 확률, 즉 홉-거리를 계산해 중앙 노드로 전송한다. 이 기법은 특별한 하드웨어가 필요치 않으나, 고정된 증명자가 필요하고 믿을 만한 제 3자가 최종 검증 연산을 수행해야 한다는 제약이 있다.

Wei는 이웃 노드의 관측 결과를 이용한 위치 검증 기법을 제안했다[13]. 이 기법은 각 센서가 브로드캐스트 신호를 바탕으로 주변 노드 관측 결과를 매트릭스

형태로 구성해 보내는 역할만 하고 최종 연산은 중앙 서버에서 처리하도록 설계되었다. 연산 부담을 중앙 서버로 대체함으로써 센서의 부담을 줄였으며 특별한 하드웨어나 사전 지식을 필요로 하지 않는다는 장점이 있다. 반대로 이웃 노드들의 관측 결과가 필수이므로 노드들의 능동적인 참여가 필요하며 검증자 역할에 신뢰할 수 있는 제 3자가 필요하다. 또한 팬텀 노드[11] 와 같이 검증에 모든 노드가 참여해야 하는 구조이므로 특정 노드 하나만 검증이 필요할 때는 오버헤드가 크다.

Miao는 VF(Virtual Force) 모델을 이용한 협력 위치 획득 및 검증 기법을 제시했다[15]. VF 모델은 센서간 측정 거리와 추정 거리에 따라 작용하는 가상의 힘을 모델링한 것으로 센서의 위치를 점진적으로 정제하는데 이용된다. 또한, 위치가 틀어진 앵커의 위치를 조정하기 위해 Localization Reliability 모델을 이용한 앵커 프로모션(Anchor Promotion) 알고리즘을 제안했다. 이 기법은 분산 방식으로 동작한다는 장점이 있으나, 앵커의 의존성이 높아 앵커에 대한 위협에 취약하다.

또한, Miao는 센서간 거리를 바탕으로 한 평판 기반의 분산 위치 검증 기법을 개발했다[16]. 이 기법은 RSS(Received Signal Strength), 삼변측량(Trilateration) 기술을 이용한다. 센서 움직임을 탐지할 수 있다는 장점이 있으나, 역시 고정된 앵커를 필요로 한다.

Wu는 이동하는 장애물(MO: Moving Object)과 RSS를 이용한 위치 검증 기법을 제안했다[20]. 이 기법에서 노드는 위치 검증 시 일정 시간동안 위치와 RSS를 전달하도록 요청 받는다. AP(Access Point)는 보고받은 RSS의 변화와 장애물 이동 정보를 바탕으로 노드의 위치를 검증한다. 즉, MO가 신호를 막지 않을 때는 상대적으로 높은 RSS 를 받고, 반대의 상황에서는 낮은 RSS 를 받는다는 점을 이용하는 것이다. 단점으로는 빠르게 이동하는 환경에서는 사용하기 어렵다.

Wang 은 WBAN(Wireless Body Area Network) 환경에서 BAV (Barometric Altimetry Verification)와 RSSI-based Left/Right Indication 알고리즘을 제안했다[21]. 제안 기법을 이용하면 센서 주변의 순간 기압으로 센서의 수직 위치를 측정하고, 센서가 어떤 팔다리에 설치되어 있는지 확인할 수 있어 환자의 몸에 잘못 부착된 센서를 찾을 수 있다. 응용 측면에서 새로운 시도였지만 공격자를 가정하지 않은 기본적인 위치 확인 방법이기에 여러 가지 공격에 취약하다는 문제가 있다.

Nosouhi 는 블록체인 기반이며 프라이버시를 고려한 분산형 위치 검증 기법을 제안했다[22]. 제안 기법은 지리적인 위치 정보와 시간 정보를 포함한 Location Proof (LP) 생성과 검증에 블록체인 기술을 이용했다. LBS(Location Based Service)에서 공격자가 위치를 속여 바우처 같은 리워드를 획득할 수 있는 것처럼, 검증자에게도 보상(Crypto Currency)을 제공함으로써 사용자가 자발적으로 시스템에 참여할 동기를 제공했다. 또한, 대부분의 기법들이 최종적인 위치 검증에 신뢰할 수 있는 인증자(authority)가 필요하다는 한계를 해결했다. 하지만, 블록 체인의 취약점이나 속도 문제는 해결이 필요한 부분이라 할 수 있다.

2. 위치 검증 기법 분류 기준

위치 검증 기법은 Zeng [25]의 제안처럼 어플리케이션 목적에 따라 분류 기준을 설정할 수 있다. 또한, 각 기법들의 특징을 바탕으로 공통된 부분을 정리함으로써 추가적인 기준을 도출할 수 있다.

표 1. 위치 검증 기법 분류 기준 및 특징

분류기준	방식	특징
Location Precision	In-region	위치를 정확하게 계산할 필요가 없으므로 유연한 시나리오 적용 가능
	On-spot	정확한 위치 확인 필요한 시나리오에 적합, 연산이 상대적으로 복잡할 가능성이 있음
Verification scale	One-by-one	적은 수의 악의적인 센서가 있을 때 유용, 많은 노드를 검증하려면 비용 오버헤드가 커짐
	Batch	많은 수의 악의적인 센서가 있을 때 유용, 많은 노드를 한 번에 검증하므로 악의적인 센서가 적다면 탐지 비용 오버헤드가 커짐
Architecture	Distributed	노드 실패나 단일지점 실패로 인한 영향이 적음, 연산 비용이 높은 편임
	Centralized	센서 자체의 연산 부하를 줄일 수 있음, 신뢰할 수 있는 제 3자가 필요
Anchor Usage	Anchor-based	다양한 localization 과 연동 가능, anchor 역할을 할 센서 노드를 정의해야 함
	Anchor-free	homogeneous 센서로 구성된 환경에 적합, 네트워크에 대한 사전 지식이 필요함
Ranging Technology	Range-based	높은 정확도 달성 가능, 기반 기술에 따라 추가 H/W 필요함
	Range-free	추가 H/W 가 불필요함, 보통 네트워크에 대한 사전 지식이 필요함

이에 따른 첫 번째 위치 검증 기법의 분류 기준은 (1)

위치 정확도(Location Precision)이다. 즉, 정확한 지점에 대한 검증인지 혹은 특정 영역 내의 존재 여부에 대한 검증인지에 따른 것이다. 전자는 On-spot 검증이라고 불리며, 후자는 In-region 검증이라고 불린다.

Zeng[25]이 제안한 또 다른 기준은 (2) 검증 대상 규모(Verification Scale)에 따른 것이다. 한 번에 검증 가능한 노드의 개수에 따른 기준으로, One-by-one 혹은 Batch 방식으로 구분할 수 있다. [25]에서는 검증 대상 규모를 위치 정확도의 하위 기준으로 분류했으나, 앞 장의 분석 결과에 따르면 위치 정확도가 항상 검증 대상 규모를 결정하지는 않으므로 독립적인 어플리케이션 목적에 따른 분류로 보는 것이 적합하다.

세 번째로는 기반 기술이나 특징에 따라 분류 가능하다. 위치 검증에는 최종 검증을 수행할 신뢰할만한 제3자 혹은 인프라가 필요하지만, 최근 논문에서는 분산 방식도 연구되고 있다. 이를 바탕으로 (3) 위치 검증 기법의 설계 구조(Architecture)에 따라 중앙집중형 방식과 분산형 방식으로 분류가 가능하다. 이 분류는 앵커의 사용 여부와도 연관이 있어 보이지만, 실질적으로 앵커는 위치 검증의 보조 역할만 수행[15][16]할 수 있다는 점에서 (4) 앵커 사용 여부를 별도의 기준으로 분류했다.

기존 검증 기법들의 특징에 따른 마지막 분류 기준은 (5) 범위 측정 기술(Ranging Technology)에 의한 분류이다. 위치 검증은 본질적으로 위치 계산법과 연관이 있다. 이 기준은 세부적으로 Range-based와 Range-free 로 나눌 수 있다. Range-based 는 RSS, ToF(Time of Flight), AoA(Angle of Arrival) 등의 기술을 이용해 거리를 측정하는 방법을 의미하며, Range-free 는 이러한 거리 측정 기술이 아닌 주변 노드와의 연결성(Connectivity) 같은 논리적인 정보를 이용하는 방법을 의미한다. 이 기준은 위치 정확도와 연관이 있지만, 각 기술의 조합에 따라 정확도 여부가 달라지므로 항상 위치 정확도의 하위 분류로 보기는 어렵다. [표 1]은 앞서 정리한 위치 검증 기법 분류 기준과 특징에 대한 요약이다.

2.1 위치 정확도

첫 번째 기준은 필요한 위치의 정확도이다. 보다 구체적으로, 관심영역(ROI: Region of Interest) 내에 타겟 센서 존재 여부를 확인하는 In-region 방식[8][13][26]과 타겟 센서가 리포트한 위치가 맞는지 확인하는 On-spot 방식[10-16]으로 나뉜다. 이 기준은 서비스의 요구 사항에 따른 것으로 볼 수 있다.

In-region 방식은 대부분 상대방까지의 Upper Bound 거리를 계산하는 DB 프로토콜[24]을 사용하지만, 특별한 역할의 센서들을 이용해 논리적인 경계를 만들고 경계에 도달하는 패킷을 바탕으로 위치를 확인하거나[26], 센서들의 통신 범위 중첩 정보를 바탕으로 타겟 센서가 ROI에 위치할 확률을 계산[13]함으로써도 구현 가능하다.

반면에 On-spot 방식은 센서가 주장한 (x, y) 위치에 해당 센서가 실제로 존재하는지 확인하기 위해 네트워크 내 센서들의 배치 상태[10], 홉-거리 정보[12], 나노 초의 패킷 왕복 시간을 측정[11][14], 이웃 노드 관측 결과의 불일치 여부[13]와 같은 정보를 이용해 구현된다. 특정한 좌표에의 위치 여부를 확인하는 것이 목적이므로 일반적으로 위치 정확도가 높다.

2.2 검증 대상 규모

두 번째 기준은 검증 대상의 규모이다. 검증 과정에서 한 번에 다수의 센서를 검증하는 Batch 방식[11][13][14][20][21]과 한 번에 관심 대상인 센서 하나씩을 검증하는 One-by-one 방식[8][10][12][15][16][20][22][26]으로 나뉜다. 이 기준 역시 위치 정확도와 마찬가지로 서비스의 요구 사항에 따라 구분 가능하다.

Batch 방식은 다수의 센서를 한번에 검증하는 것을 목표로 한다. 이 방식은 보통 연관된 모든 센서로부터 필요한 정보를 수집하는 특징이 있다. 수집된 정보는 센서 간의 거리[11][14], 이웃 센서의 관측 결과[13], 신호의 블록 현상[20], 공기압이나 RSSI 모음[21] 등이 될 수 있다. 위치 검증은 수집된 정보를 바탕으로 센서가 직접 수행하거나 신뢰할 수 있는 제 3자에 의해 이루어진다. 센서가 직접 위치 검증을 수행하는 분산형 방식이라면, 네트워크 내의 전체 센서가 아닌 특정 그룹의 센서들을 검증 대상으로 본다[21]. Batch 방식은 특성상 네트워크 내에 발생한 다수의 위치 이상을 탐지하는데 효과적이지만, 반대로 특정 센서의 검증만 필요

한 상황에서는 오버헤드가 크다.

반면에, One-by-one 방식은 적은 수의 노드 위치를 검증하는데 적합하다. 이 방식은 거리 측정 정보 활용[8][16][26], 계획된 지역에 특별한 역할을 하는 센서를 배치[26], 이웃 노드 상태 정보의 일치 여부를 확인[10], 홉-거리 정보를 활용[12]함으로써 그 목적을 달성한다. 일반적으로 batch 방식보다는 검증 오버헤드가 적은 편이다. 하지만 검증하고자 하는 노드의 개수가 증가할수록 선형적으로 오버헤드가 늘어난다.

2.3 위치 검증 기법 설계 구조

세 번째 분류 기준은 위치 검증 기법의 설계 구조이다. 즉, 위치 검증 시, 센서가 모두 동일한 역할을 수행하는 형태의 Distributed 방식과, 특정 센서 혹은 제 3자가 검증을 전담하는 형태의 Centralized 로 나눌 수 있다.

Distributed 방식은 각 센서가 검증 과정을 수행한다[8][10][11][15][16][26]. 센서는 검증에 필요한 정보를 수집하고, 수집된 정보를 바탕으로 수신한 위치 정보를 검증한다. 따라서 센서 각각이 복잡한 연산을 처리하는 경우가 많다. 이는 곧 센서의 연산 부담으로 이어질 수 있으므로 이를 고려해 기법을 설계할 필요가 있다.

Centralized 방식은 각 센서가 정보 수집 역할을 담당하고, 검증 역할을 수행하는 중앙 서버 혹은 특별한 센서를 사용한다[12-14]. 위치 검증 역할의 센서 혹은 서버는 신뢰할 수 있다고 가정한다. 이같은 방식은 센서의 연산 부담을 최소화하는 대신 이 부담을 서버 혹은 특별 센서로 전가한다. 따라서 센서의 연산 부하를 줄이는데는 효과적일 수 있으나, 반드시 통신 부하까지 줄이는 것은 아니란 점을 염두에 두어야 한다.

표 2. 위치 검증 기법 분류 및 요약

Category	App. scenario				Underlying tech.						Note
	Location precision		Verification scale		Architecture		Anchor usage		Ranging tech.		
	In-region	On-spot	One-by-one	Batch	Centralized	Distributed	Anchor-based	Anchor-free	Range-based	Range-free	
Echo [8]	O		O			O		O	O		Using intersection would help to extend to more precise region verification.
Acceptor [26]	O		O			O	O			O	Carefully considering the placement of the required verifiers would enchance the distributed property of the protocol.
WBAN [21]	O			O	O			O	O		Adopting more accurate ranging technique rather than RSSI only would help the protocol to be extended to the on-spot implementation.
Lightweight-1 [13]	O			O	O			O		O	Considering majority of attackers would help to enhance the robustness of the protocol.
LAD [10]		O	O			O		O		O	Analyzing and reenforcing the depency to deployment knowledge model would help to achieve better accuracy.
Virtual Force [15]		O	O			O	O		O		Considering the mobility of anchor would make the algorithm more robust.
UNDA [16]		O	O			O	O		O		Considering combination with range-free localization would make the usage of the idea to become wider.
Blockchain [22]		O	O			O	O			O	Adopting the range-based tech would help to wider application of the scheme.
MO [20]		O	O		O			O	O		Considering multihop relay would resolve the limitation of RSS usage for deep fading sensors.
PLV [12]		O	O		O		O			O	Reenforcing the integrity of hop count and content would help to strengthen the range-free nature of the protocol.
Verifier Bee [14]		O		O	O		O		O		Considering non-line-of-sight situation would enhance the downside of using drone as an anchor.
Lightweight-2 [13]		O		O	O			O		O	Considering the mobility of sensors would help wider application of the idea.
Phantom [11]		O		O		O		O	O		Considering collaborative attackers would help to enhance the distributed nature of the idea.

2.4 앵커 사용 여부

위치 검증 기법은 본질적으로 위치 계산과도 연관이 있다. 따라서 위치 계산법에서 자주 사용되는 앵커의 사용 여부가 분류 기준이 될 수 있다.

Anchor-based 방식[12][14-16][26]은 특별한 역할을 하는 앵커가 다른 센서들에게 기준 위치 정보를 전송[14-16]하거나, 위치 검증에 필요한 정보를 제공하는 참조 노드 역할을 수행[12][26]하는 방식으로 구현된다. 많은 위치 계산법이 앵커의 사용을 가정하고, 위치 검증 기법 역시 위치 계산법을 활용하는 경우가 많으므로 이 방식은 위치 검증에 자연스럽게 적용될 수 있다는 장점이 있다.

Anchor-free 방식에서는 위치 검증에 필요한 정보를 얻는 기준점이 없으므로, 상대 거리 혹은 센서 간 연결성(Connectivity) 정보를 활용한다[8][10][11][13]. 즉, 센서들이 서로 협력해서 필요한 데이터를 수집하고 때로는 검증을 직접 처리해야 하는 부담이 있다. 거리의 측정은 범위 측정 기술(Ranging)을 이용할 수 있으며, 연결성 정보는 이웃 센서로부터 발생하는 라디오 신호의 관측 결과를 이용할 수 있다.

2.5 범위 측정 기술

범위 측정 기술(Ranging)은 센서 간 거리를 측정할 때 사용되는 방법이며 위치 계산법에서 많이 사용되는 방법 중 하나이다. 이 기술의 사용 유무에 따라 Range-based 와 Range-free 로 분류할 수 있다.

Range-based 기법은 정확한 수치를 바탕으로 위치를 계산하므로 높은 정확성을 보장한다[8][11][14-16]. RSS, ToA(Time of Arrival), TDoA(Time Difference of Arrival), AoA(Angle of Arrival) 기술을 통해 상호 간의 거리를 계산한다. RSS 를 제외한 범위 측정 기술들은 라디오 신호의 왕복 시간 혹은 수신 각도를 측정해야 하므로 특별한 H/W 가 필요하다. 예를 들어, DB 프로토콜에서는 ToA 기술을 이용하기 때문에 센서가 나노 초 단위의 시간을 측정할 수 있어야 한다.

Range-free 방식은 센서 배치 사전 지식, 홉-거리, 이웃 노드 관측 결과로 측정한 연결성 정보를 이용한다[10][12][13][26]. 추가적인 H/W를 필요로 하진 않으나 검증에 활용할 수 있도록 사전 지식을 미리 검증자에게 제공하거나 운영 중 이같은 정보를 획득할 방법이 있어야 한다.

3. 기존 연구 분류 및 요약

앞서 분류한 기준에 따라 기존 연구들을 분류하고 그 특징을 정리함으로써 통합적인 분석 결과를 제공한다. [표 2]는 기존 기법들의 분류 결과와 각 기법의 발전방향에 대한 요약을 포함한다. 표에서 볼 수 있듯, 분류의 주요 기준을 어플리케이션 시나리오에 따른 기준으로 둠으로써 각 기술들의 적용 방법에 따른 독립성을 확인할 수 있다. 분류된 각 기법은 [표 1]의 위치 정확도와 검증 대상 규모 특징에 따라 위치 기반 자원 접근 혹은 위치 기반 체크인 서비스 등에 다양하게 활용 가능하다.

[표 2]에서 제시한 분류 결과는 각 시나리오 별 조합 가능한 기술들의 확인을 도움으로써, 신규 기법 설계 시 참고자료로서의 역할을 할 수 있을 것으로 기대된다. 또한, [표 2]에 포함되지 않은 기법에 대해서는 그 기법의 특징을 바탕으로 기준을 적용함으로써 신규 기법 설계의 가능성을 확인할 수도 있을 것으로 기대된다.

IV. 결론

위치가 중요한 역할을 하는 서비스에서 잘못된 위치는 서비스 품질에 영향을 줄 뿐만 아니라 큰 손실을 초래하기도 한다. 따라서 위치 정보의 검증 방법은 필수적이다. 위치 정보 검증 기법을 설계함에 있어 기존 연구의 분석과 분류는 매우 중요한 과제이다. 본 논문에서는 WSN 환경의 위치 검증 기법 특징에 대해 통합적인 분석 결과 및 분류 기준을 제시했다. 또한, 각 기법의 분류 결과와 발전방향을 제공함으로써 신규 기법 개발의 참고자료 역할을 할 수 있을 것으로 기대된다. 다만, 본 연구에서는 프라이버시 특성은 고려하지 않았다. 콘텐츠 서비스에서 중요한 부분을 차지할 프라이버시에 대한 분석이 추가되면 보다 유용할 것으로 예상된다.

참 고 문 헌

[1] L. Borges, F. Velez, and A. Lebres, "Survey on the Characterization and Classification of Wireless Sensor Networks Applications," IEEE Communications Surveys & Tutorials, Vol.16, No.4, pp.1860-1890, 2014.

[2] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," Ad Hoc Networks, Vol.3, No.3, pp.325-349, 2005.

[3] J. Jiang, G. Han, C. Zhu, Y. Dong, and N. Zhang, "Secure Localization in Wireless Sensor Networks: A Survey (Invited Paper)," JCM, Vol.6, No.6, pp.460-470, Sep. 2011.

[4] U.S. a Department Of Defense, "Global Positioning System Standard Positioning Service," Www.Gps.Gov, No.September, pp.1-160, 2008.

[5] A. Srinivasan and J. Wu, "A Survey on Secure Localization in Wireless Sensor Networks," CRC Press, Taylor and Francis Group: Florida, USA, p.26, Oct. 2017.

[6] J. Bachrach and C. Taylor, "Localization in Sensor Networks," Handbook of Sensor Networks: Algorithms and Architectures, pp.277-310, 2005.

[7] M. S. Chebli, H. Mohammad, and K. A. Amer, "An Overview of Wireless Indoor Positioning Systems: Techniques, Security, and Countermeasures," in Internet and Distributed Computing Systems, Cham, pp.223-233, 2019.

[8] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in Proceedings of the 2nd ACM workshop on Wireless security. ACM, pp.1-10, 2003.

[9] S. Capkun and J. P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., Miami, FL, USA, Vol.3, pp.1917-1928, 2005.

[10] W. Du, L. Fang, and P. Ning, "LAD: Localization anomaly detection for wireless sensor networks," in Parallel and Distributed Processing Symposium, 2005, Proceedings, 19th IEEE International. IEEE, pp.41a-41a, 2005.

[11] J. Hwang, T. He, and Y. Kim, "Detecting Phantom Nodes in Wireless Sensor Networks," in IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications, Anchorage, AK, USA, pp.2391-2395, 2007.

[12] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks," Ad Hoc Networks, Vol.6, No.2, pp.195-209, Apr. 2008

[13] Y. Wei and Y. Guan, "Lightweight Location Verification Algorithms for Wireless Sensor Networks," IEEE Trans. Parallel Distrib. Syst. Vol.24, No.5, pp.938-950, May. 2013.

[14] P. Perazzo, K. Ariyapala, M. Conti, and G. Dini, "The verifier bee: A path planner for drone-based secure location verification," 2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Boston, MA, pp.1-9, 2015.

[15] C. Miao, G. Dai, K. Ying, and Q. Chen, "Collaborative Localization and Location Verification in WSNs," Sensors, Vol.15, No.5, pp.10631-10649, May. 2015.

[16] C. Miao, G. Dai, L. Chen, H. Jin, and Q. Chen, "A Node Localization Verification Model for WSN," in Human Centered Computing, vol. 9567, Q. Zu and B. Hu, Eds. Cham: Springer International Publishing, pp.296-309, 2016.

[17] J. T. Chiang, J. J. Haas, J. Choi, and Y. C. Hu, "Secure location verification using simultaneous multilateration," IEEE Transactions on Wireless Communications, Vol.11, No.2, pp.584-591, Feb. 2012.

[18] S. Yan, I. Nevat, G. W. Peters, and R. Malaney, "Location verification systems under spatially

correlated shadowing," IEEE Transactions on Wireless Communications, Vol.15, No.6, pp.4132-4144, Jun. 2016.
[19] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "Optimal information theoretic wireless location verification," IEEE Transactions on Vehicular Technology, Vol.63, No.7, pp.3410-3422, Sep. 2014.
[20] D. Wu, D. Zhu, Y. Liu, and D. Zhao, "Location Verification Assisted by a Moving Obstacle for Wireless Sensor Networks," IEEE Internet Things J., Vol.5, No.1, pp.322-335, Feb. 2018.
[21] H. Wang, Y. Wen, and D. Zhao, "Location verification algorithm of wearable sensors for wireless body area networks," Technology and Health Care, Vol.26, No.S1, pp.3-18, Jan. 2018.
[22] M. R. Nosouhi, S. Yu, W. Zhou, M. Grobler, and H. Keshtiar, "Blockchain for secure location verification," Journal of Parallel and Distributed Computing, Vol.136, pp.40-51, Feb. 2020.
[23] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identication and signature problems," In Advances in Cryptology - CRYPTO'86, Vol.263, pp.186-194.
[24] S. Brands and D. Chaum, "Distance-Bounding Protocols," in Advances in Cryptology — EUROCRYPT '93, Vol.765, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, pp.344-359, 1994.
[25] Y. Zeng, J. Cao, J. Hong, S. Zhang, and L. Xie, "Secure localization and location verification in wireless sensor networks: a survey," J Supercomput, Vol.64, No.3, pp.685-701, Jun. 2013.
[26] Adnan Vora and Mikhail Nesterenko, "Secure location verification using radio broadcast," Dependable and Secure Computing, IEEE Transactions on, Vol.3, No.4, pp.377-385, 2006.

저 자 소 개

김 인 환(In-hwan Kim) 정회원

- 2007년 2월 : 아주대학교 정보및컴퓨터공학부(공학사)
- 2009년 2월 : 아주대학교 정보통신공학원(공학석사)
- 2017년 8월 : 연세대학교 컴퓨터과학과(공학박사)
- 2017년 9월 ~ 현재 : 삼성전자

〈관심분야〉 : 위치검증, 컴퓨터 네트워크, 컴퓨터 보안