[10-54]

센서 네트워크에서의 고장을 허용하는 견고한 인증기법

*윤미연 *이광겸 *손상철 *신용태
*숭실대학교 일반대학원 컴퓨터학과
{myyoon, goodwin77, yelhorse, shin}@cherry.ssu.ac.kr

Robust Authentication Mechanism allowing node failure for sensor network

*Miyoun Yoon *KwangKyum Lee *Sangchol Son *Yongtae Shin
*Dept. of Computing, Soongsil University

요약

본 논문에서는 센서 네트워크에서 계층적인 인증 메커니즘에 대해서 제안한다. 센서 노드에서는 적은 배터리 용량과 메모리 사이즈 때문에 인증 기법이 경량화 되어야 한다. BS(base station)는 어떤 상황에서든 센서 노드가 확실하게 맞다는 가정 하에 수집된 정보로 결정되고, 배터리의 문제나 다른 이유로 센서가 고장을 일으키더라도 매커니즘이 수행되어야 하기 때문이다. 따라서 메시지가 교환될 때 간단한 계산과 적은 메모리를 요구하는 센서가 내장된 경량화 된 인증 메커니즘을 제안하고 나아가 버스트 패킷의 손실과 센서의 고장, 메시지 중복으로 인한 위조된 센서가 발생하더라도, 지정된 센서들이 적당한 선택을 할 수 있는 기법을 제안하고, 각 보안성의 제공여부를 분석하고, 기존연구와의 비교분석을 수행한다.

1. 서론

센서 네트워크는 ad-hoc 네트워크와 비슷하지만 많은 측면에서 여러 가지 다른 사항들을 볼 수 있다. 예를 들어 네트워크상에서 센서 노드는 서로간의 통신 중에 탈퇴할 수 없지만 ad-hoc 노드는 ad-hoc 네트워크 내에서 동적으로 탈퇴할 수 있다. 또한 센서 노드는 이동성을 지원하지만 어플리케이션에는 의존하지 않는 특징을 갖고 있고, ad-hoc 노드는 항상 모바일 노드를 취해야 하는 특징을 갖고 있다. 그리고 센서 노드는 배터리의 제약과 낮은 프로세스 파워, 저용량의 메모리에서 사용되지만, ad-hoc 노드는 노트북이나 PDA와 같이 높은 프로세싱 파워와 대용량의 메모리가 사용되는 기기에서 사용될 수 있다. 마지막으로 센서 네트워크는 BS(base station) 노드를 가지고 있지만 ad-hoc 네트워크에선 BS(base station)가 없다. 따라서 본 논문에서는 인증을 위한 센서 노드의 이런 특징들을 살펴본다.

센서 네트워크의 총체적인 정보는 센서 노드의 부분적인 정보가 집결되어 만들어 진다. 그래서 위조된 센서는 허용될 수 없고, 인증되지 않은 센서로 전달된 데이터는 수행되지 않는다. 그런 이유로 제대로 된 센서 노드들 간의 인증이 성립되기 위해선 신뢰적인 통신이 꼭 필요하고 따라서 센서 노드의 물리적인 특성들을 고려한 경량화 된 인증에 대해서 제안한다. 본 논문의 2장에서 센서 네트워크나 ad-hoc 네트워크에 관련 있는 몇몇의 연구에 대해서 소개하고 그것들의 장·단점을 분석하며 3장에서는 인증 메커니즘을 제안하고 4장에서는 본 논문에서 제안하는 보안성을 분석하고, 기존연구[3]와의 비교분석을 수행한다. 마지막으로 5장에서 결론과 향후 연구과제에 대해 제시하고 설명한다.

2. 관련연구

[1]은 비상시 센서 네트워크의 지역 탐색 메커니즘을 제안하였다. 이것은 identify code 알고리즘[]에 기초하며, 장애물이나 센서의 어떤 위치든 상관하지 않는다. 예를 들어 꼭 그리드 구조에 기초할 필요는 없다는 뜻이다. 입력 순서 포인트가 {f, g, d, e, a, b, c} 일 때 센서 위치 포인트 {a, b, c}로 목표 영역을 충분히 발견해 낼 수 있고, 어느 영역이든 배치될 수 있다. 그러나 필수조건으로 각 센서들의 감지 포인트를 알아야 하고, 프로시져는 O(nk)의 저장 장소와 계산시간 O(n)을 필요로 한다. 여기서 n은 입력 포인트의 순서 사이즈, k는 각 센서의 자식 프로시져 숫자이다. 따라서 센서가 아니라 기법의 수행 BS(base station)로 하는 것이 더 효율적이다. 더군다나