논문 2013-50-10-6

무선 센서 네트워크를 위한 신뢰 기반의 안전한 클러스터 헤드 선출 (Secure Cluster Head Elections Based on Trust for Wireless Sensor Networks)

왕 기 철*, 조 기 환**

(Gicheol Wang and Gihwan Cho[©])

요 약

클러스터 구조를 가진 센서 네트워크에서 클러스터 헤드는 그 멤버들로부터 데이터를 모아서 모아진 데이터를 싱크에 보내는 역할을 수행하기에, 오염된 노드들이 클러스터 헤드 선출에 개입하여 선출결과를 조작하거나 변경하지 못하도록 막아야 한다. 오염된 노드들로부터 클러스터 헤드 선출 과정을 보호하기 위해서는 선출과정의 비예측성, 비조작성, 그리고 일치성을 보존해야 한다. 하지만, 기존의 클러스터 헤드 선출 방법들은 지능화된 오염노드들이 상호 협력을 통해 위의 속성들을 교묘하게 손상시키는 것을 막지 못한다. 본 논문에서는 이러한 지능화된 오염노드들을 식별하고 제거함으로써 클러스터 헤드 선출과정을 보호하는 방법을 제안한다. 클러스터 헤드 선출 라운드 마다 각 멤버는 다른 멤버들의 행위에 따라 그들에게 직접적인 신뢰값을 부여한다. 각 멤버는 자신이 부여한 직접신뢰값과 다른 멤버들에 의해 부여된 간접신뢰값을 묶어서 멤버들의 실제 신뢰값들을 추출한다. 이후에 각 멤버는 추출된 다른 멤버들의 실제 신뢰값을 평가하고 낮은 신뢰값을 가진 멤버들은 클러스터 헤드 후보자에서 제거한다. 이를 통해 제안방법은 다른 경쟁방법에 비해 클러스터 헤드 선출 결과의 비조작성과 일치성을 크게 향상시킨다. 또한, 제안방법은 메시지 손실이 발생하는 환경에서도 다른 방법들에 비해 높은 비조작성과 일치성을 제공한다.

Abstract

In clustered sensor networks, since a CH (Cluster Head) collects data from its members and delivers the collected data to the sink, it is very important to prevent compromised nodes from joining a CH election and manipulating and fabricating the election result. In order to protect CH elections from compromised nodes, unpredictability, non-manipulability, and agreement property should be guaranteed in CH elections. However, existing CH election schemes cannot prevent intelligent compromised nodes from skilfully violating those properties via their cooperation. In this paper, we propose a scheme which protects the CH election process by detecting intelligent compromised nodes and excluding them. For every CH election round, each member gives a direct trust value to other members according to their behavior. Then a real reputation value is given to each member by combining the direct trust value and indirect trust values provided by other members. Then, each node evaluates the real reputation values of members in its cluster and excludes some untrustable nodes from CH candidates. The scheme greatly improves the non-manipulability and agreement property of CH election results compared to other rival schemes. Furthermore, the scheme preserves the high non-manipulability and the high agreement property even in an environment where message losses can happen.

Keywords : 클러스터 헤드 선출, 센서 네트워크 보안, 클러스터 구조, 노드 신뢰도 평가

* 정회원, 한국과학기술정보연구원 첨단연구망서비스실

(Dept. of Advanced KREONET Service, Korea Institute of Science and Technology Information)

** 정회원, 전북대학교 컴퓨터공학부, 영상정보통신기술연구센터

(Div. of Computer Science and Engineering, CAIT, Chonbuk National University)

© Corresponding Author(E-mail: ghcho@chonbuk.ac.kr)

접수일자: 2013년3월21일, 수정완료일: 2013년9월27일

I. 서 론

무선 센서 네트워크는 많은 수의 센서노드들로 구성되어 있으며 이들 센서노드들 간에는 무선으로 통신을 수행한다. 임의의 센서 노드는 마이크로 컨트롤러, 무선 송수신기, 센서들, 그리고 특정한 양의 전원을 가진 배터리로 구성되어 있다. 센서노드들의 임무는 온도, 소리, 빛, 진동과 같은 환경적 요소들을 감지하고 싱크로 전달하여 이들을 이용하고자 하는 사용자의 의사결정을 돕는 것이다. 무선 센서 네트워크는 험준한 산악 지역이나 화산활동 지역과 같은 사람이 근접하기 어려운 환경에 설치되어 동작하므로 대부분의 동작시간 동안 보호되지도 않고 관리되지도 않는다^[1]. 이러한 이유로 센서노드들이 보유한 에너지는 일정 시간 동안만 동작할 수 있도록 제한되어 있으며, 배터리는 재충전되지 않는다. 따라서, 센서노드들이 이러한 희박한 에너지 자원을 보존할 수 있는 방법이 요구되고 있으며, 클러스터링은 이 요구를 충족시킬 수 있는 훌륭한 방법들 중 하나이다.

무선 센서 네트워크에서 클러스터링은 인접한 센서노드들을 논리적인 그룹(cluster)으로 묶어서 관리하고 이 그룹내에서 리더 역할을 수행할 노드(CH: Cluster Head)를 선출하는 일련의 과정을 의미한다^[2]. 임의의 클러스터 내에서 노드들은 자신이 감지한 데이터를 오직 그룹리더인 CH에게만 전송하고, CH는 모여진 데이터를 집약하여 싱크에게 전송함으로써 네트워크 내에서 전체적인 전송횟수를 줄일 수 있는 이점을 지닌다^[3]. 즉, 노드들의 데이터 전송횟수가 감소함으로써 노드들의 수명이 증가하고 이를 통해 다시 네트워크의 수명이 증가하는 이점을 유발한다.

그러나 클러스터 구조가 센서 네트워크의 에너지를 절약하는 이점을 유발하지만, CH들은 데이터의 수집점이자 수집된 데이터를 싱크로 전달하는 원천지이기에 공격자들에게는 더 없이 좋은 공격 목표가 된다. 즉, 공격자들은 CH들을 오염시킴으로써 일반 노드들로부터 전달되는 데이터를 빠짐없이 수신할 수 있고 더불어 변조된 데이터를 싱크에게 전달함으로써 데이터의 수요자가 잘못된 의사결정을 하도록 유도할 수 있다. 만일, 공격자들이 네트워크 내의 모든 CH들을 오염시킨 경우에 그들은 전체 네트워크를 그들의 이익에 따라 조정할 수 있다. 한편, 클러스터 구조 하에서 CH들은 일반 노드들

에 비해 에너지 소모가 많기 때문에 주기적으로 CH 역할을 수행하는 노드들을 변경할 필요가 있다. CH 역할 노드의 변경은 노드들이 CH 선출 프로토콜을 주기적으로 수행하는 것에 의해 구현된다. 이때 오염노드들은 틀림 없이 CH가 되려고 시도할 것이다. 따라서, CH 선출 프로토콜이 수행되는 동안에 오염된 노드들을 식별하고 이들이 CH로 선출되지 않도록 막는 기법이 필요하다. 기존에 제안된 CH 선출 보안 기법들 중에서 공유키 기반의 방법들^[4~5]은 네트워크 외부의 공격자로부터 CH 선출을 잘 보호하지만 내부 오염노드들의 이상행위를 막을 수 없다. 난수 기반의 방법들^[6]과 키체인 기반의 방법^[7]은 오염노드들이 메시지를 선택적으로 전송하여 CH 선출 결과를 분할시키거나 혹은 메시지 전송을 고의로 회피하여 CH 선출 결과를 변경시키는 공격에 취약하다. 마지막으로, 은닉 기반의 CH 선출 방법^[8]은 공유키 기반의 방법들 처럼 내부 오염노드들의 이상행위를 막지 못한다.

본 논문에서는 난수에 기반하여 CH를 선출하되 난수 기반의 방법들이 가지는 선택적 전송 공격 및 고의적 전송회피 공격에 대한 취약점을 해결하기 위하여 신뢰도 기반의 후보제외 기법을 CH 선출에 도입한다. 제안 방법에서 각 멤버는 다른 멤버들의 행위에 기반하여 그 노드들의 신뢰값을 부여한다. 즉, CH 선출 과정에서 메시지 전송을 하지 않는 노드들에게는 낮은 신뢰값을 부여함으로써 정상노드들이 의심스러운 노드들을 식별하고 그들을 CH 후보에서 제외할 수 있게 한다. 제안하는 방법에서 노드들에게 부여되는 신뢰값은 3가지로 구분된다. 먼저, 각 노드가 프로토콜 과정에서의 직접 관찰을 통해 부여하는 직접 신뢰값이 있다. 각 노드가 직접 신뢰값을 부여할 때, 프로토콜 동작 동안에 성공한 전송횟수, 실패한 전송횟수를 고려하는데, 이때 최근에 연속적으로 성공 혹은 실패한 시간간격을 고려하여 신뢰값을 부여한다. 반면, 자신의 클러스터에 있는 멤버들이 관찰한 신뢰값들을 통합하여 부여하는 간접 신뢰값이 있다. 마지막으로, 직접 신뢰값과 간접 신뢰값을 평균을 내서 부여하는 통합 신뢰값이 있다. 통합 신뢰값들을 평균을 내면 멤버들의 실제 신뢰값들이 생성되고 부여된다. 멤버들에게 부여되는 실제 신뢰값들의 평균보다 낮은 실제 신뢰값을 가지는 노드는 CH 후보에서 제외된다.

본 논문의 구성은 다음과 같다. II장에서는 안전한

CH 선출과 관련된 기존 연구들을 살펴본다. III장에서는 네트워크와 공격 모델을 살펴본다. IV장에서는 제안된 방법을 상세히 살펴보고 V장에서는 실험결과를 통해 CH 선출 방법들을 비교한다. VI장은 결론을 내린다.

II. 관련 연구

LEACH(Low-Energy Adaptive Clustering Protocol)^[3]는 모든 노드가 번갈아가면서 CH 역할을 수행하도록 함으로써 네트워크의 수명을 연장하고자 하였다. 이는 CH가 자신의 멤버들로부터 데이터를 수집하고 이를 집약해서 싱크에게 원거리로 전송하기 때문이다. 이 방법에서, 임의의 임계치보다 낮은 확률을 가지는 노드는 자신을 CH로 선언하고 다른 노드들은 이들 중에서 하나에 가입한다. 그러나 이 방법은 모든 노드들이 정상으로 동작하는 환경을 가정하기에 오염 노드의 불법적인 CH 선언에 대처할 수 없다.

F-LEACH^[4]는 LEACH의 CH선출을 보호하기 위하여 제안되었다. 이 방법에서 노드들은 임무현장에 배치되기 전에 미리 임의의 개수 만큼 키들을 분배받는다. 그리고 CH자격을 가지는 노드는 싱크와 공유된 키들을 이용해서 자신을 CH로 선언하며 싱크는 같은 키들을 이용해서 그 CH선언을 검증한다. 이후에 싱크는 검증된 CH들을 μ TESLA^[9]를 이용하여 방송하고, 일반 노드들은 그들 중에서 하나의 CH에 가입한다. 하지만 이 방법은 일반노드들의 클러스터 가입을 검증하지 않기 때문에 무자격 노드들이 클러스터에 자유롭게 가입할 수 있다. SecLEACH^[5]는 이 문제를 해결하기 위해 싱크가 CH 선언노드들을 인증하고 CH들이 일반노드들의 가입을 인증한다. F-LEACH와 SecLEACH는 CH선언 및 클러스터 가입을 인증하기 위해 미리 분배된 키들을 이용하므로, 분배된 키들을 가지지 않은 공격자들로부터만 프로토콜을 보호할 수 있다. 즉, 두 방법은 임무현장에 배치된 후에 오염된 노드들이 프로토콜에 참여하고 불법적인 CH선언 및 클러스터 가입을 수행하는 것을 막을 수 없다.

Liu 등은 미리 정해진 노드들이 CH로 선언하고 나머지 노드들이 하나의 클러스터에 직접 혹은 중계노드를 통해 가입하는 방법^[10]을 제안하였다. 여기서 CH 선언이나 클러스터 가입은 미리 분배된 다항식 배당 (polynomial share)에 의해 인증된다. 따라서 다항식 배

당을 가지지 않은 외부 공격자는 클러스터 생성에 참여할 수 없다. 또한 많은 이웃을 가진 정상노드는 스스로 네트워크에서 탈퇴하고 싱크는 탈퇴하지 않는 의심스러운 노드를 강제로 퇴출시키는 워홀 방지 기법을 사용한다. 그러나, 임의의 중계노드가 공격자에 의해 오염되면 그 중계노드는 해당 CH와 멤버노드들 사이에서 DoS(Denial of Service)공격을 일으킬 수 있다. 또한 임의의 오염된 노드는 중계노드 설정을 방해하거나 CH와 멤버노드들 사이의 연결을 단절시킬 수 있다.

[11]과 [12]에서는 CH를 선출하기에 앞서서 먼저 의심스러운 노드들을 제거하고 안전한 멤버들만을 클러스터 멤버로 편입시켜서 클러스터를 생성하는 방법을 제안하였다. 이 방법의 장점은 클러스터 생성 과정에서 포함된 오염노드들이 CH 선출 과정에서도 계속해서 활동하는 것을 방지할 수 있다는 점이다.

Sirivianos등은 난수 기반의 안전한 CH선출 방법인 SANE(Secure Aggregator Node Election)^[6]을 제안하였다. SANE은 Merkle의 퍼즐 기반 방법, commitment 기반의 방법, 그리고 seed 기반 방법으로 구성되어 있다. Merkle의 퍼즐 기반 방법에서 현재의 CH는 먼저 Merkle의 퍼즐을 이용하여 다른 멤버들과 pairwise키들을 생성한다. 이후에 각 멤버는 자신의 난수를 생성하여 pairwise키로 암호화한후 다른 멤버로부터 전달된 난수의 합에 더한후에 또 다른 멤버에게 전달한다. 이 과정은 모든 멤버들이 자신의 암호화된 난수를 난수들의 합에 누적시킬 때까지 반복한다. 마지막 난수 누적자는 그 난수의 합을 방송하고 현재의 CH는 멤버들과 공유된 pairwise키들을 모든 멤버들에게 분배한다. 모든 노드들은 암호화된 난수의 합을 그 키들을 이용하여 평문 난수의 합으로 변환할 수 있다. 각 노드는 그 평문 난수의 합에 기반하여 CH를 선출한다.

commitment 기반의 방법에서 매 CH 선출 라운드마다 각 노드는 자신의 commitment를 다른 멤버들에게 일대일로 전송한다. 이때 commitment는 각 노드가 생성한 난수를 공유된 키에 의해 암호화된 것이다. 이후에 각 노드는 자신의 commitment에 대한 이행값, 즉 자신의 난수를 다시 다른 멤버들에게 분배한다. 멤버들은 공유된 키들을 이용하여 난수들을 검증하고 이를 통해 난수의 합을 생성한다.

seed 기반의 방법에서 각 노드는 자신의 seed 값을 생성하고 이를 방송형태로 모든 다른 멤버들에게 분배

한다. 이 seed 값은 매 CH 선출 라운드마다 새로운 난수를 생성하기 위해 사용되는 초기난수이다. 매 CH 선출 라운드마다 각 노드는 availability 메시지를 방송하는데 이 메시지는 전송자의 CH 선출에의 참여 의지를 나타낸다. Availability 메시지를 수신하는 멤버들은 메시지 전송자를 저장하고 전송자의 seed 값과 현재 CH 선출 라운드 수를 이용하여 전송자의 새로운 난수를 생성한다. 그래서 모든 멤버들의 availability 메시지를 수신한 후에 각 노드는 전송자들의 리스트와 새로운 난수들의 합을 얻게 되고 이를 CH 선출을 위한 공통값으로 활용한다.

Merkle의 puzzle 기반 방법은 pairwise키 설정, 난수 분배, 그리고 키분배로 인한 통신 및 계산 오버헤드가 크다. Commitment 기반의 방법과 seed 기반의 방법은 Merkle의 puzzle 기반 방법에 비해 오버헤드를 감소시키지만 공통적인 문제점을 가지고 있다. 즉, 두 방법 모두에서 난수의 합의 생성에 기여하는 마지막 노드는 CH 선출 결과를 예측하고 조작할 수 있으며 심지어는 멤버들이 공유하고 있는 난수의 합의 여러개 생성되도록 해서 클러스터를 분할시킬 수 있다.

Dong 등은 두 개의 키체인을 이용한 CH 선출 기법^[7]을 제안하였다. 네트워크 구성 초기에 클러스터 내의 각 멤버는 두개의 키체인 (즉, Yes 키체인과 No 키체인)을 생성하고 이들의 마지막 키를 방송한다. 이 마지막 키들은 노드의 ID를 검증하는데 사용될 뿐만 아니라 CH 선출과정에서 각 멤버가 전송하는 키체인 값의 전송자를 확인하는데도 이용된다. 이후의 CH 선출 라운드마다 각 키체인의 나머지 값들이 차례로 이용된다. 따라서 이 방법은 키체인 기반의 방법이라고 불린다. 이 방법에서 CH 후보들이 선정된 후에 실제 CH는 번갈아 가면서 선정된다. CH 선출 과정 동안에 각 멤버는 CH 선출에 참여하고자 하는 경우에는 Yes 키체인 값을 그렇지 않은 경우에는 No 키체인 값을 전송한다. 만일 임의의 멤버가 No 키체인 값을 전송하면 그 멤버는 CH 후보에서 완전히 제외된다. 만일 임의의 멤버가 Yes 키체인 값을 전송하지 않으면 일단은 CH 후보에서 제외하고 그 멤버가 CH로 선출될 차례인 경우에는 다음 후보에게 역할이 넘겨진다. 임시로 CH 후보에서 제외된 멤버는 다음 CH 선출 라운드에서 다시 선출에 참여할 기회를 가지게 된다. 그러나 이후에도 계속 Yes 키체인 값을 전송하지 않으면 이 멤버는 완전히 CH 후

보에서 제외된다. 이렇게 각 멤버에게 여러 번의 기회를 주는 이유는 메시지 손실이 발생하는 환경에 대비하기 위해서다. 이 방법은 외부 공격자에 대한 강력한 대비책을 제시하는 반면에 오염된 노드의 공격에 취약하다. 즉, 임의의 오염노드는 자신의 Yes 키체인 값 전송을 고의로 계속해서 회피함으로써 CH 선출 결과를 쉽게 변경할 수 있다. 오염노드는 또한 자신의 Yes 키체인 값 전송을 CH 후보들의 일부에게만 전송함으로써 여러 개의 CH 선출 결과들을 생성할 수 있다. 비록 이 기법이 여러 개의 CH 선출 결과들을 병합하는 병합 알고리즘을 가지고 있지만, 그 알고리즘은 CH 후보들의 자발적인 참여를 필요로 한다. 하지만, 오염노드들의 입장에서 자신의 이익과 반대되는 알고리즘에 참여하지 않을 것이므로, 이 알고리즘은 오염노드들이 증가할수록 제대로 동작하지 않는다.

Buttayan 등은 메시지 암호화 및 복호화를 이용하여 외부노드들로부터 CH 선출과정을 숨기는 CH 선출 기법^[8]을 제안하였다. 이 방법에서 외부노드는 어떤 노드가 CH로 선출되는지 알 수 없지만 내부에서 오염된 노드는 CH 선출결과를 외부로 유출할 수 있다. 더구나, 오염노드는 그 자신의 적격성에 상관없이 스스로를 CH로 선언할 수도 있다.

III. 네트워크 및 위협 모델

1. 네트워크 모델

본 논문에서 우리는 모든 노드들이 임무현장에 무작위로 배치된다고 가정한다. 모든 노드들은 거의 움직이지 않으며 어떤 노드이든지 CH 역할을 수행할 수 있다고 가정한다. 노드들이 임무현장에 배치된 후에 모든 노드들은 초기 클러스터들을 생성하기 위해^[2]와 같은 클러스터 생성 기법을 수행한다. 네트워크 동작은 라운드들로 구성되며 각 라운드는 CH 선출 단계와 통신 단계로 나뉘어 진다. CH 선출 단계에서는 모든 노드들이 하나의 노드를 CH로 선출한다. 통신 단계에서는 모든 멤버들이 자신의 감지 데이터를 CH에게 전송하고 CH는 데이터를 집약하고 이를 싱크에게 전송한다.

2. 위협 모델

서론에서 이미 언급한 것처럼 네트워크 내에 존재하는 오염노드들은 CH가 되기 위해 노력할 것임에 틀림

없다. 따라서 오염노드들의 위협에 대처하기 위해 임의의 CH 선출 기법이 만족시켜야 할 속성에는 다음과 같은 것들이 있다. 먼저, CH 선출 기법은 비예측성을 만족해야 한다. 즉, 임의의 노드가 CH 선출 결과를 예측하기 어려워야 한다. 두 번째, CH 선출 기법은 비조작성을 만족해야 한다. 즉, 임의의 노드가 자신의 이익을 위하여 CH 선출 결과를 조작할 수 없어야 한다. 세 번째, CH 선출 기법은 일치성을 만족해야 한다. 즉, 클러스터 내의 모든 멤버들이 같은 선출결과를 가져야 한다. 마지막으로 CH 선출 기법은 메시지 손실에 대한 면역이 있어야 한다. 이는 무선 네트워크에서 간섭이나 장애물, 신호감쇠로 인해 메시지 손실이 자주 발생하기 때문이다.

우리는 제안하는 CH 선출 기법이 [6]의 방법들 처럼 난수에 기반하여 동작한다고 가정한다. 표 1은 제안하는 방법에서 사용되는 값들의 정의와 그들의 목적을 요약해서 보여준다. 임의의 클러스터에서 모든 멤버들은 자신만의 난수를 생성하고 그 값을 분배하는 것에 의해 공통값의 생성에 기여한다. 이때 각 멤버가 생성하는 난수를 이후부터는 공헌값이라 부르기로 한다. 공통값의 생성은 모든 멤버들의 공헌값을 더하는 것에 의해 계산되기에 마지막으로 공헌값을 전송하는 노드는 공통값을 미리 예측할 수 있다 (비예측성 훼손). 또한, 이 오염노드는 자신의 공헌값 전송을 회피하는 것에 의해 CH 선출 결과를 손쉽게 바꿀 수 있다 (비조작성 훼손). 즉, 정상노드가 CH로 선출될 것 같으면 자신의 공헌값 전송을 회피함으로써 공통값의 변경을 만들어 내고 이를 통해 오염노드들 중 하나가 CH로 선출되도록 할 수

있다. 이러한 공격을 본 논문에서는 침묵 공격이라고 부르기로 한다. 일반적으로 정상노드들은 자신의 메시지가 클러스터내의 모든 노드들에게 전달되도록 전송전력을 조절할 수 있다. 그래서 정상노드들의 전송전력은 클러스터내의 최대 홉 거리와 같으며 이는 클러스터 생성 과정에서 결정이 된다. 본 논문에서는 이러한 클러스터내의 최대 홉 거리를 클러스터 직경으로 부르기로 한다. 오염노드들은 자신의 공헌값을 전송할 때 전송전력 레벨을 낮추어서 전송할 수 있다. 이를 통해 일부 멤버들에게만 그 공헌값이 전송되고 따라서 멤버들이 가진 공헌값의 합이 달라지게 된다. 따라서 여러개의 공헌값의 합이 생성되어 CH 선출 결과도 여러 개로 나뉘게 된다 (일치성 훼손). 이러한 공격을 이후부터는 선택적 전송 공격이라 부르기로 한다. 무선 네트워크 환경에서 메시지 손실은 자주 발생되며 이를 오염노드의 고의적인 전송회피와 구분하기는 매우 힘들다. 따라서 임의의 멤버로 부터의 메시지 미수신을 모두 공격으로 간주하면 선의의 피해자가 발생하게 된다. 반면에, 오염노드는 이러한 특성을 이용하여 자신의 악의적인 행위를 은닉할 수 있다.

IV. 신뢰 기반의 CH 선출 기법

본 논문에서 우리는 외부의 공격자들이 초기 클러스터 생성 과정에서 모두 제거 되었다고 가정한다. 결과적으로 본 논문에서의 공격자는 오염된 내부의 노드들을 의미한다. 제안된 CH 선출 기법은 3단계로 구성되어 있다. 첫 번째 단계에서는 각 멤버가 자신의 공헌값(난수)을 생성하고 이를 방송한다. 이후에 각 멤버는 같은 클러스터에 있는 다른 멤버들의 공헌값 전송 여부에 따라 신뢰값들을 부여한다. 이러한 메시지 수신 성공 및 실패 횟수는 클러스터 내의 각 멤버가 얼마나 CH 선출 프로토콜에 순응하는지를 나타낸다. 이는 3.2절의 위협모델에서 밝힌 것처럼 오염노드들은 선택적 전송 공격 혹은 침묵공격을 통해 CH 선출결과와 비조작성 및 일치성을 훼손하기 때문이다. 이 횟수들은 시간이 지날수록 누적되며 더 정확한 순응성을 나타낸다. 또한 마지막으로 성공한 두 전송 사이의 시간 간격 및 마지막으로 실패한 두 전송 사이의 시간 간격에 따라 가중치를 부여하면 최신성을 고려한 신뢰값을 구할 수 있다. 즉, 전송 성공 횟수와 전송 실패 횟수가 같을 경우

표 1. 제안방법에서 이용되는 값의 정의 와 목적
Table 1. Definition and purpose of values used in the proposed scheme.

값	정의
	목적
공헌값	각 멤버에 의해 생성된 난수
	모든 멤버의 공헌값이 더해져서 하나의 공통된 난수(공통값) 생성
공통값	각 멤버의 공헌값이 더해진 합
	공통값을 멤버수로 나누어 나머지를 CH 위치로 선정
신뢰값	각 멤버가 다른 멤버들에게 부여하는 0에서 1사이의 값
	다른 멤버들에 대한 신뢰도를 수치로 계량화

그림 1. 공헌값 생성 및 전송의 순서도

Fig. 1. Flow chart for generation and transmission of contribution value.

에 최근에 전송에 성공했는지 혹은 실패했는지를 따지게 된다. 결국, 각 멤버는 다른 멤버들의 메시지 전송횟수 및 비전송 횟수 그리고 최근의 전송 및 비전송 간격을 고려한 식을 이용하여 다른 멤버들에게 0에서 1사이

의 신뢰값을 부여한다. 각 멤버가 클러스터내의 다른 멤버들에게 신뢰값을 부여한 후에, 각 멤버는 신뢰값 리스트를 방송한다. 우리는 IV.1 절에서 제안된 방법의 첫 번째 단계를 자세히 기술한다. 두 번째 단계에서 각

그림 2. 신뢰값 리스트 생성 및 방송의 순서도

Fig. 2. Flow chart for generation and broadcast of trust value list.

멤버는 수신한 신뢰값 리스트를 이용하여 다른 멤버들의 간접 신뢰값들을 유도하고 그들의 통합된 신뢰값들을 계산하여 통합 신뢰값 테이블에 저장한다. 그 후에 각 멤버의 실제 신뢰값은 해당 멤버의 통합 신뢰값들을

평균을 구함으로써 얻을 수 있다. 마지막으로 각 멤버는 모든 멤버들에 대한 실제 신뢰값들의 평균을 구하고 그 평균 아래의 값을 가진 멤버들을 CH 후보에서 제외한다. 제안방법의 두 번째 단계는 IV.2절에서 자세히 기

술된다. 세 번째 단계에서 모든 멤버들은 남은 CH 후보들로부터의 공헌값들을 모두 더함으로써 공통값을 생성하고 그 공통값을 이용하여 CH를 선출한다. 제안된 방법의 세 번째 단계는 IV.3절에서 자세히 기술된다.

1. 공헌값 및 신뢰값 리스트의 전송

그림 1은 제안된 방법의 1단계에서 공헌값의 생성과 전송에 관한 순서도를 보여준다. 매 CH 선출 라운드마다 각 노드는 공통값의 생성을 위한 자신의 공헌값을 생성하고 방송한다. 모든 노드들이 공헌값을 전송하고 나면 각 노드는 다른 멤버들의 메시지 전송 여부와 전송 간격을 체크하여 그들에 대한 신뢰값을 계산한다. 또한 그 횟수들은 최근에 성공한 두 전송 사이의 간격 및 최근에 실패한 두 전송 사이의 간격을 반영함으로써 전송 성공 혹은 전송 실패에 대하여 최신성을 반영할 수 있다. 식 (1)은 위의 사항들을 반영하여 신뢰값을 구하기 위한 식이다.

$$T_{i,j}^D = 1 - \frac{1}{\max[w_{i,j}^s st_{i,j} - w_{i,j}^u ut_{i,j}, 0] + 1} \quad (1)$$

식 (1)에서 $st_{i,j}$ 와 $ut_{i,j}$ 는 노드 i 에 의해 계수된 노드 j 의 전송 성공 횟수 및 전송 실패 횟수를 의미한다. 또한 $w_{i,j}^s$ 와 $w_{i,j}^u$ 는 각각 노드 j 의 성공 횟수 및 실패 횟수에 대한 가중치를 의미한다. 이 가중치들은 전송 성공 혹은 실패에 대한 최신성을 반영하기 위해 이용되며 식 (2)와 식 (3)에 의해 결정된다. 또한 식 (2)와 식 (3)에서 $\Delta_{i,j}^s$ 와 $\Delta_{i,j}^u$ 는 각각 노드 j 가 최근에 성공한 두 전송사이의 간격과 노드 j 가 최근에 실패한 두 전송사이의 간격을 의미하고 T_{CH} 는 CH 선출 주기를 의미한다.

$$w_{i,j}^s = \begin{cases} 3 & \Delta_{i,j}^s \leq T_{CH} \\ 2 & T_{CH} < \Delta_{i,j}^s \leq 2 \times T_{CH} \\ 1 & \Delta_{i,j}^s > 2 \times T_{CH} \end{cases} \quad (2)$$

$$w_{i,j}^u = \begin{cases} 3 & \Delta_{i,j}^u \leq T_{CH} \\ 2 & T_{CH} < \Delta_{i,j}^u \leq 2 \times T_{CH} \\ 1 & \Delta_{i,j}^u > 2 \times T_{CH} \end{cases} \quad (3)$$

다른 멤버들에 대한 신뢰값을 계산한 후에, 각 노드는 신뢰값 리스트를 다른 멤버들과 공유하기 위해 방송한다. 신뢰값 리스트를 수신할 때 마다 각 노드는 0보

다 작거나 1보다 큰 신뢰값이 포함되었는지 검사한다. 만일 그러한 신뢰값이 하나라도 포함이 되었으면 CH 선출 라운드의 수를 점검한다. 첫 번째 선출 라운드인 경우에 수신자는 신뢰값 리스트를 모두 1로 채운후에 신뢰값 테이블에 저장한다. 첫 번째 선출 라운드가 아니면 신뢰값 테이블에 저장되어 있던 이전의 신뢰값 리스트를 그대로 보존한다. 만일 전송자의 신뢰값 리스트가 모두 0과 1사이의 값이면 수신자는 전송자의 이전 신뢰값 리스트를 지금 수신한 신뢰값 리스트로 치환한다. 만일 특정한 시간 동안 기다려도 아무런 메시지도 수신하지 못하면 제안 방법의 첫 번째 단계는 종료된다. 그림 2는 제안 방법의 첫 번째 단계에서 신뢰값 리스트의 생성 및 방송의 순서도를 보여준다.

2. CH 후보들의 재선정

그림 3은 제안된 방법의 두 번째 단계에 대한 순서도를 보여준다. 먼저, 각 노드는 클러스터 내에서 임의의 노드가 신뢰값 리스트의 전송을 회피했는지 조사한다. 이는 멤버의 신뢰값 리스트 전송 여부 또한 신뢰값 계산에 반영하기 위해서이다. 만일 신뢰값 리스트의 전송 여부를 신뢰값 계산에 포함시키지 않으면 이기적인 노드들은 공헌값 전송만 수행하고 신뢰값 리스트의 전송을 기피할 수 있다. 이 경우에 각 멤버는 다른 멤버들의 평가 결과에 대한 표본을 많이 얻을 수 없게 되고 따라서 정확한 신뢰도를 구할 수 없게 된다. 임의의 노드가 신뢰값 리스트의 전송을 회피했다면, 각 노드는 회피자의 비전송 횟수를 1만큼 증가시킨다. 그후에 각 노드는 회피자의 비전송 시간 간격을 바꾸기 위해 이전 비전송 시간과 최근 비전송 시간을 업데이트 한다. 또한 각 멤버 i 는 같은 클러스터 내에 있는 다른 멤버 j 의 간접 신뢰값들을 식 (4)를 이용하여 계산한다. 여기서 간접 신뢰값이란 자신이 아닌 다른 멤버가 자신을 포함한 멤버들에게 부여한 신뢰값을 이용하여 만들어 낸 신뢰값을 의미한다. 간접 신뢰값을 만들어내기 위해 각 멤버는 자신이 다른 멤버에게 직접 부여한 신뢰값과 그 멤버가 모든 멤버들에게 부여한 신뢰값을 동시에 고려한다. 식 (4)에서 m 은 클러스터 내에 있는 멤버들의 수를 의미한다. 이어서 각 노드 i 는 같은 클러스터 내에 있는 임의의 멤버 j 의 신뢰값과 간접 신뢰값을 통합하여 j 의 통합된 신뢰값을 계산한다. 식 (5)는 임의의 노드 j 에 대한 통합된 신뢰값을 계산하는 식을 보여준다. 각 노드는

그림 3. CH 후보들의 재선정을 위한 순서도
Fig. 3. Flow chart for reselection of CH candidates.

멤버들에 대한 통합된 신뢰값을 구하여 통합 신뢰값 테이블에 저장한다. 마지막으로, 각 노드는 클러스터 내에서 멤버들에 의해 배정된 모든 통합 신뢰값들을 식 (6)을 이용하여 평균을 산출함으로써 실제 신뢰값들을 추출해낸다. 각 노드는 실제 신뢰값들의 평균을 내고 그

평균 보다 낮은 실제 신뢰값을 가진 노드들을 CH 후보에서 제외한다.

$$T_{i,j}^{IND} = \frac{\sum_{k=1}^{m-1} T_{i,k}^D T_{k,j}^D}{m-1} \quad (4)$$

$$T_{i,j} = \frac{T_{i,j}^D + T_{i,j}^{IND}}{2} \quad (5)$$

$$T_{real}^i = \frac{\sum_{j=1}^m T_{j,i}}{m} \quad (6)$$

3. CH 선출

그림 4는 제안된 방법의 세 번째 단계를 보여준다. 각 노드는 생존한 CH 후보들이 전송한 공헌값들을 모두 더함으로써 공통값을 생성한다. 그리고 각 노드는 그 공통값을 생존한 CH 후보들의 수로 나누고 그 나머지를 CH 후보리스트에서 실제 CH 역할을 수행할 노드의 위치로 정한다.

그림 4. CH 선출의 순서도
Fig. 4. Flow chart for CH election

V. 평 가

본 장에서 우리는 제안된 방법의 안전성과 효율성을 ns-2^[13] 네트워크 시뮬레이터를 이용하여 평가한다. 실험 환경에서 100 개의 노드가 랜덤하게 100m×100m.

영역에 배치되었다. 각 노드는 [3]에서의 에너지 모델을 사용하여 에너지를 소모하였다. 우리는 각 노드가 CH 선출을 위해 통신할 때 충돌이 발생하지 않는다고 가정한다. 만일 각 노드가 CSMA (Carrier Sense MultipleAccess) 기반의 MAC (Medium Access Control)을 이용한다면 이 가정은 꽤 비현실적이다. 하지만, TDMA (Time Division Multiple Access) 기반의 MAC과 여러개의 DSSS (Direct Sequence Spread Spectrum) 코드들을 이용한다면 충돌을 회피할 수 있다. 따라서 본 논문에서는 각 노드가 TDMA와 CSMA의 두 가지 MAC프로토콜을 이용한다고 가정한다. 실험은 1800초 동안 수행되며 오염노드들은 3초에서 900초 사이에 랜덤하게 결정된다. 또한 초기 클러스터들은 네트워크가 생성된 후에 한번만 생성되며 이후에 각 노드는 30초 마다 자신의 클러스터에서 CH를 선정한다. CH 선출 프로토콜에 집중하기 위해 CH 선출사이에 이루어지는 멤버들과 CH간의 통신 및 CH와 싱크간의 통신은 구현하지 않았다. 표 2는 실험에 사용되었던 파라미터들과 그 값들을 보여준다.

제안된 방법은 seed기반의 방법, commitment 기반의 방법, 그리고 키체인 기반의 방법과 비교되었다. 이들과의 비교 이유는 이들이 서로 간에 유사한 방법으로 공통값을 생성하고 그 공통값을 이용하여 CH를 선출하기 때문이다. 또한, 그들은 같은 유형의 공격에 취약하다. 우리는 특정한 수의 오염노드에 대해 각 방법을 20번씩 실행시켜서 그 결과들의 평균을 산출하였다. 우리는 각 방법의 매 실행마다 오염노드와 네트워크의 위상이 달라지게 만들었다. 또한 하나의 클러스터 내에서는

표 2. 실험에 사용된 파라미터와 값들.
Table 2. Simulation parameters and values.

파라미터	값
실험영역	100m.×100m.
노드수	100
오염노드수	10~50
초기 에너지량	10 Joules
에너지 소모 모델	[3]의 에너지 모델
대역폭	1Mbps
패킷 헤더 사이즈	25 bytes
전송범위	30 meter
MAC 프로토콜	비영속적 CSMA, TDMA
실험시간	1800초
노드 오염시간	3~900초
CH 선출 주기	30초

오직 하나의 공격 (침묵공격 또는 선택적 전송 공격)만이 수행되도록 하였다. 이는 두 공격의 목표가 서로 다르기 때문이다. 본 논문에서 소개된 CH 선출 방법들의 비교를 위해 우리는 다음의 실험 척도들을 사용하였다.

- 클러스터당 생성된 CH수 : 이 척도는 하나의 클러스터에서 오염노드들의 선택적 전송 공격에 의하여 야기되는 CH들의 수를 의미한다. 이 척도는 임의의 CH 선출 방법이 일치성을 얼마나 보존하는지를 나타내는 척도이다. 공격이 없다면, 클러스터당 생성된 CH의 수는 1이 되어야 한다.
- 선출당 오염노드의 CH 선출 빈도 수 : 이 척도는 한번의 CH 선출 라운드에서 오염노드들의 침묵공격에 의해 그들이 CH로 당선되는 빈도수를 의미한다. 이 척도는 임의의 CH 선출 방법이 오염노드의 조작성을 얼마나 제한할 수 있는지를 나타내는 척도이다. 이 척도는 작을수록 좋지만 공격이 없다고 해서 이 값이 0이 되지는 않는다.
- 노드당 에너지 소모량 : 이 척도는 각 노드가 네트워크 운영 기간 동안에 소모한 에너지를 의미한다. 이 척도는 임의의 CH 선출 방법이 각 노드에게 얼마만큼의 에너지 소모를 유발하는지를 나타내는 척도이다. 이 척도가 작을수록 에너지 효율적인 방법이 된다.

그림 5는 오염노드의 수가 증가함에 따라 클러스터 내에서 얼마나 많은 수의 CH들이 생성되는지를 보여준다. Seed 기반의 방법과 commitment 기반의 방법은 오염노드들의 선택적 전송 공격에 잘 대처하지 못하기에 그들은 오염노드 수가 작다고 하더라도 CH들의 수를 크게 증가시킨다. 키체인 기반의 방법은 오염노드의 수가 작을 때는 분리된 클러스터들을 병합하는 알고리즘을 통해 CH들의 증가를 완화시킨다. 하지만 오염노드의 수가 증가할수록 병합 알고리즘의 동작을 와해시킬 수 있는 문제점을 지니고 있다. 즉, 클러스터 내의 오염노드 수가 많아지면 클러스터 병합 알고리즘이 동작하지 않으므로 분할된 클러스터들이 그대로 남게 된다. 신뢰 기반의 방법은 그림 5에서 보는 것처럼 오염노드의 수가 증가하더라도 CH들의 수를 거의 증가시키지 않는다. 비록 키체인 기반의 방법이 오염노드의 수가 작을 때는 신뢰 기반의 방법과 거의 유사한 정도

그림 5. 클러스터당 생성된 CH수 vs. 오염노드수

Fig. 5. The number of CHs per cluster vs. the number of compromised nodes

의 안전성을 제공하지만, 오염노드의 수가 증가할 수록 안전성이 점차로 저하됨을 그림 5를 통해서 알 수 있다.

그림 6은 오염노드 수의 증가에 따른 오염노드가 CH로 선출되는 빈도를 보여준다. 그림 6에서 보는 것처럼, seed 기반 방법과 commitment 기반 방법은 오염노드의 증가와 함께 그들의 CH 선출 확률도 크게 높인다. 이것은 오염노드들이 쉽게 CH 선출 결과를 예측할 수 있고 자신들의 공헌값 전송을 회피하는 것에 의해 CH 선출 결과를 변경할 수 있기 때문이다. 키체인 기반의 방법은 이전의 두 방법에 비해 나은 보안성을 제공하는데 이는 그 방법이 공헌값 전송을 두 번 이상 회피하는 노드들을 CH 후보에서 완전히 배제하기 때문이다. 하지만 오염노드들이 교대로 공헌값 전송을 회피하는 경우에 그들은 이러한 배제 전략으로부터 생존할 수 있다. 따라서 키체인 방법도 오염노드의 증가에 취약하다. 특히, 오염노드의 수가 크면 클수록 commitment 나 seed 기반의 방법과 거의 유사한 정도로 오염노드를 CH로 선출한다. 이는 키체인 기반의 방법이 가지는 또 하나의 취약점을 그대로 보여주는 것이다. 즉, 임의의 클러스터 내에 오염노드 수가 많아지면 그들은 상호협력해서 CH 선출 결과를 자신들에게 유리한 결과로 변경할 수 있다. 예를 들어 현재 임의의 오염된 노드가 CH로 선출될 차례인 경우에 그들은 추천 메시지를 모두 전송

그림 6. 선출당 오염노드의 CH 선출 빈도수 vs. 오염노드수

Fig. 6. CH winning frequency of compromised nodes per election vs. the number of compromised nodes.

해서 그 노드가 CH로 선출되도록 하는 반면에, 정상노드가 CH로 선출될 것 같으면 오염노드들이 모두 추천 메시지를 전송하지 않음으로써 그 노드의 CH 선출을 방해한다. 이렇게 추천 메시지의 비전송이 CH 선출에 영향을 미침에도 불구하고 키체인 기반의 방법은 이러한 악의적인 행위에 대한 대비책을 가지고 있지 않다. 반면에, 신뢰 기반의 방법은 공헌값의 전송은 물론 신뢰값 리스트의 전송 또한 멤버의 신뢰도 계산에 고려함으로써 모든 형태의 메시지 비전송에 대해 대비한다. 따라서 신뢰 기반의 방법은 오염노드의 증가에 따라 그들의 CH 선출 빈도를 높이지는 하지만 그 증가율은 키체인 방법에 비해 월등히 낮은 편이다.

그림 7은 CH 선출들을 위해 각 노드에 의해 소모된 평균 에너지량을 보여준다. Seed 기반 방법은 임의의 CH 선출에서 각 노드가 짧은 길이의 메시지만을 오직 전송하기에 다른 방법들에 비해 월등히 낮은 양의 에너지를 소모한다. 키체인 기반의 방법은 오염노드의 수가 증가하면 오히려 노드들의 에너지 소모량이 감소한다. 이는 키체인 기반의 방법에서 임의의 오염노드가 두 번 이상 메시지 전송을 회피하면 그 노드는 CH 후보에서 완전히 퇴출되기 때문이다. 퇴출된 노드는 더 이상 CH 선출에 참여할 수 없기 때문에 CH 선출을 위해 에너지를 소모할 이유가 없다. 반면에 신뢰 기반의 방법은 거

그림 7. 노드당 에너지 소모량(J.) vs. 오염노드수
Fig. 7. Energy consumption per node(J.) vs. the number of compromised nodes.

의 일정한 양의 에너지를 소모한다. 이는 신뢰기반의 방법에서 오염노드는 현재의 CH 선출에서 배제되었다 하더라도 다음 CH 선출에 참여할 수 있기 때문이다. 이러한 전략은 제안방법이 메시지 손실이 자주 발생하는 무선 네트워크 환경에 적절함을 알려준다.

그림 8은 메시지 손실률의 증가가 어떻게 클러스터 당 생성되는 CH들의 수에 영향을 미치는지 보여준다. 메시지 손실률에 의한 영향을 평가하기 위한 실험에서 오염노드들의 수는 30개로 고정되었다. 그림 8에서 보는 것처럼 commitment 기반 방법과 seed 기반 방법은 메시지 손실률이 증가함에 따라 더 많은 수의 CH들을 생성한다. 이는 CH 선출을 위한 CH 후보리스트의 상이성이 증가하기 때문이다. 이는 다시 클러스터 내에 공유된 공통값의 수를 증가시키고 따라서 CH들의 수도 증가하게 된다. 키체인 기반의 방법은 두 방법에 비해 우수한 보안성을 제공하는 것처럼 보이지만 실제로는 단언하기 힘들다. 이는 키체인 기반의 방법이 CH들을 가지지 않은 클러스터들을 많이 생성하기 때문이다. 그림 8에서 보는 것 처럼 키체인 기반의 방법은 메시지 손실률이 2% 이상이 되면 두 개의 클러스터 중 하나가 CH를 가지지 못하게 된다. 이 방법에서 CH를 가지지 못하는 클러스터가 발생하는 이유는 임의의 노드가 자신을 CH로 선언하기 위해서는 멤버들의 절반이상으로부터 추천메시지를 수신해야 하기 때문이다. 하지만 메시지 손실이 자주 발생하는 경우에 유력한 CH 후보자

그림 8. 클러스터당 생성된 CH수 vs. 메시지 손실률(%)
Fig. 8. The number of CHs per cluster vs. message loss rate(%)

그림 9. 선출당 오염노드의 CH선출 빈도수 vs. 메시지 손실률(%)
Fig. 9. CH winning frequency of compromised nodes per election vs. message loss rate(%)

들은 과반이상의 추천메시지를 수신하는데 실패하게 된다. 신뢰 기반의 방법은 메시지 손실률이 증가하더라도 CH들의 수를 거의 증가시키지 않으며 다른 방법들에 비해 가장 좋은 보안성을 제공한다.

그림 9는 메시지 손실률의 증가가 오염노드들이 CH로 선출되는 빈도에 어떤 영향을 미치는지 보여준다.

그림 10. 노드당 평균 에너지 소모량(J.) vs. 메시지 손실률(%)

Fig. 10. Average energy consumption per node(J.) vs. message loss rate(%)

Seed 기반의 방법과 commitment 기반의 방법은 메시지 손실률의 증가에 따라 클러스터 내에 많은 수의 CH들을 생성한다. 이는 다시 오염노드들의 CH 선출 빈도를 증가시킨다. 눈여겨 볼 점은 키체인 기반의 방법이 메시지 손실률이 증가하면 오염노드들의 CH 선출 빈도를 감소시킨다는 것이다. 이는 그림 8에서 본 것처럼 메시지 손실률이 증가함에 따라 CH를 선출하지 못하는 클러스터들이 증가하기 때문이다. 즉, 메시지 손실률이 증가하면 정상적인 노드들은 물론 오염노드들조차도 같은 클러스터 내의 다른 멤버들로부터 과반수 이상의 추천 메시지를 수신하기가 힘들게 되므로, 이들의 CH 선출 빈도수 또한 감소하게 되는 것이다. 신뢰기반의 방법은 다른 방법들에 비해 오염노드들의 CH 선출 빈도를 크게 감소시킨다. 더구나 신뢰기반의 방법은 메시지 손실률에 상관없이 오염노드들의 CH 선출 빈도를 특정한 수(그림 9에서는 2) 이하로 항상 유지시킨다는 장점을 지닌다.

그림 10은 메시지 손실률의 증가가 노드의 에너지 소모량에 미치는 영향을 보여준다. 모든 방법들은 메시지 손실률의 증가에 따라 노드의 에너지 소모량을 작은 비율로 감소시킨다. 이는 노드들이 수신하는 메시지들의 수가 감소하기 때문이다. 특히, commitment 기반의 방법은 다른 방법들에 비해 더 많이 영향을 받는데 이는

이 방법에서 노드들이 더 많은 수의 메시지들을 전송하기 때문이다. Seed 기반의 방법은 임의의 CH 선출 라운드에서 각 노드가 짧은 길이의 메시지를 한번만 전송하기에 여타 방법들에 비해 에너지 소모량이 작다. 키체인 기반의 방법은 메시지 손실에 대처하기 위한 메시지의 중복 전송 강제화 그리고 클러스터 병합 알고리즘 수행으로 인하여 seed 기반의 방법에 비해 많은 양의 에너지를 소모한다. 신뢰 기반의 방법에서 각 멤버는 CH 선출 라운드 마다 한번의 랜덤값 전송과 한번의 신뢰값 리스트 전송을 수행하므로 seed 기반의 방법에 비해서는 많은 양의 에너지를 소모한다. 하지만, 신뢰 기반의 방법은 메시지의 중복 전송이나 클러스터 병합 알고리즘을 수행하지 않기에 키체인 방법에 비해서는 작은 양의 에너지를 소모한다.

VI. 결 론

클러스터 구조를 가진 센서 네트워크에서 오염노드들은 CH 선출 결과를 예측하고 조작할 수 있으며 때로는 CH 선출 결과의 일치성을 훼손하기도 한다. 본 논문에서 우리는 그러한 오염노드들을 식별하고 CH 후보에서 제거하는 효과적인 방법을 제시한다. 먼저, 제안방법은 각 CH 후보가 다른 후보들의 행위를 직접 평가하고 그에 따라 신뢰값을 부여한다. 그후에 그 신뢰값들의 리스트는 다른 노드들에게 분배되고 수신자들은 수신된 직접 신뢰값 리스트를 이용하여 간접 신뢰값 리스트를 생성하고 두 신뢰값 리스트의 통합버전인 통합신뢰값 리스트를 생성한다. 이후에 각 멤버는 통합신뢰값 리스트를 통합신뢰값 테이블에 저장하고 각 열에 대한 평균값을 계산하여 실제 신뢰값 리스트에 저장한다. 마지막으로 실제 신뢰값 리스트의 평균을 구하고 그 평균 보다 낮은 실제 신뢰값을 가진 노드를 CH 후보에서 제외한다. 또한 제안방법은 제외된 노드가 이후의 CH 선출에 다시 참여하게 함으로써 메시지 손실에 유연하게 대처할 수 있다. 실험결과는 제안방법이 다른 방법들에 비해 CH 선출 결과의 일치성을 19%에서 68%까지 향상시킴을 보여주었다. 또한 제안방법은 다른 방법들에 비해 CH 선출 결과의 비조작성을 56%에서 65%까지 향상시켰다. 한편, 메시지 손실이 발생하는 상황에서 제안방법은 다른 방법들에 비해 CH 선출 결과의 일치성을 14%에서 83%까지 향상시켰다. 또한 메

시지 손실이 발생하는 상황에서 제안방법은 CH 선출 결과의 비조작성을 다른 방법들에 비해 55%에서 80%까지 향상시켰다.

REFERENCES

- [1] G. Wang, K. Song, and G. Cho, "DIRECT: Dynamic Key Renewal Using Secure Cluster Head Election in Wireless Sensor Networks," *IEICE Transactions on Information and Systems*, Vol. E93-D, No. 6, pp. 1560-1571, Jun. 2010
- [2] 왕기철, 조기환, "무선 센서 네트워크에서 안전한 클러스터 구성 방안," 대한전자공학회 논문지, 제 49권 TC편, 제8호, 84-97쪽, 2012년 8월
- [3] W. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Transactions on Wireless Communications*, Vol. 1, No. 4, pp. 660-670, Oct. 2002.
- [4] A. C. Ferreira, M. A. Vilaca, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. Loureiro, "On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks," in Proc. of 4th IEEE Int'l Conf. on Networking, Vol. 3420, pp. 449-458, 2005.
- [5] L. B. Oliveira, H. C. Wong, M. W. Bern, R. Dahab, and A. A. Loureiro, "SecLEACH-A Random Key Distribution Solution for Securing Clustered Sensor Networks," in Proc. of 5th IEEE Int'l Symposium On Network Computing and Applications, pp. 145-154, Cambridge, MA, USA, Jul. 2006.
- [6] M. Sirivianos, D. Westhoff, F. Armknecht, and J. Girao, "Non-manipulable Aggregator Node Election Protocols for Wireless Sensor Networks," in Proc. of Int'l Symposium On Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, pp. 1-10, Apr. 2007.
- [7] Q. Dong and D. Liu, "Resilient Cluster Leader Election for Wireless Sensor Networks, in Proc. of IEEE 6th Annual Communication Society Conf. on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 108-116, Rome, Italy, Jun. 2009.
- [8] L. Buttyan and T. Holczer, "Private Cluster Head Election in Wireless Sensor Networks," in Proc. of the 5th IEEE Int'l Workshop on Wireless and Sensor Network Security (WSNS '09), IEEE, pp. 1048-1053, 2009.
- [9] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, Vol. 8, No. 5, pp. 521-534, Sep. 2002.
- [10] D. Liu, "Resilient Cluster Formation for Sensor Networks," in Proc. of 27th Int'l Conf. on Distributed Computing Systems, pp. 40-48, Toronto, ON, Canada, Jun. 2007.
- [11] G. Wang, D. Kim, and G. Cho, "A Secure Cluster Formation Scheme in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, Vol. 2012, Article ID 301750, 14 pages, Oct. 2012
- [12] K. Sun, P. Peng, P. Ning, and C. Wang, "Secure Distributed Cluster Formation in Wireless Sensor Networks," in Proc. of the 22nd Annual Conf. on Computer Security Applications, pp. 131-140, Miami, FL, USA, Dec. 2006.
- [13] Network Simulator ns-2. (2012, Dec. 20). [Online]. Available: <http://www.isi.edu/nsnam/ns>

— 저 자 소 개 —

왕 기 철(정회원)

1997년 광주대학교 전자계산학과
학사 졸업2000년 목포대학교 전산통계학과
석사 졸업2005년 전북대학교 컴퓨터 통계
정보 학과 박사 졸업

2006년~2007년 전북대학교 Post-doc 연구원

2008년 전남대학교 Post-doc 연구원

2009년~현재 한국과학기술정보연구원

선임연구원

<주관심분야 : Ad hoc 네트워크, 센서 네트워크,
무선네트워크 보안, 이동 컴퓨팅>

조 기 환(정회원)

1985년 전남대학교 계산통계학과
학사 졸업1987년 서울대학교 계산통계학과
석사 졸업1996년 영국 Newcastle 대학교
전산학과 박사 졸업

1987년~1997년 한국전자통신연구원 선임연구원

1997년~1999년 목포대학교 컴퓨터과학과
전임강사

1999년~현재 전북대학교 컴퓨터공학부 교수

<주관심분야 : 이동컴퓨팅, 컴퓨터통신, 무선네트
워크 보안, 센서네트워크, 분산처리시스템>