2011년 2월
박사학위 논문

환경 감시 센서 네트워크를 위한 저에너지 고신뢰성 라우팅 프로토콜

조선대학교 대학원
컴 퓨 터 공 학 과
최 동 민

환경 감시 센서 네트워크를 위한 저에너지 고신뢰성 라우팅 프로토콜

An Energy-Efficient and Reliable Routing Protocol for Environment Monitoring Sensor Networks

2011년 2월 25일

조선대학교 대학원

컴 퓨 터 공 학 과

최 동 민

환경 감시 센서 네트워크를 위한 저에너지 고신뢰성 라우팅 프로토콜

지도교수 정 일 용

이 논문을 컴퓨터공학 박사학위신청 논문으로 제출함

2010년 10월

조선대학교 대학원

컴 퓨 터 공 학 과

최 동 민

최동민의 박사학위논문을 인준함

위원장	조선대학교	교수	모 상 만 (인)
위 원	조선대학교	교수	강 문 수 (인)
위 원	조선대학교	교수	신 석 주 (인)
위 원	국가보안연구소	박사	이 철 원 (인)
위 원	조선대학교	교수	정 일 용 (인)

2010년 12월

조선대학교 대학원

목 차

표 목 차

도 목 차

ABSTRACT

An Energy-Efficient and Reliable Routing Protocol for Environment monitoring Sensor Networks

Dongmin Choi

Advisor : Prof. Il Yong Chung, Ph.D.
Department of Computer Engineering,
Graduate School of Chosun University

Wireless sensor networks(WSNs) consist of numerous sensor nodes equipped with a radio transceiver, a small microcontroller, and non-rechargeable batteries. The nodes are deployed over a large area and communicate with each other via wireless links. It has been widely recognized that energy-efficient and security are important design issues in WSNs. The disposable sensor nodes with non-rechargeable batteries have serious energy constraints and, thus, the energy-efficient and energy-balanced design of protocols is necessary for prolonging network lifetime. On the other hand, security-sensitive networks such as military applications, the interception of information can cause serious problems. So it is important to ensure that the data arrive at their destinations safely and reliably.

For energy-efficient networks, dynamic clustering is an effective technique to prolong network lifetime, achieve scalability, and balance load, which are important requirements. When this method is applied, however, some nodes consume energy unnecessarily because the environment is such that the data collected from the sensor nodes often overlap. Moreover, this unnecessary

energy consumption increases energy consumption at the cluster-head node. Thus, such a protocol must change the cluster formation and cluster-head node in each round to prolong the network's lifetime. Nevertheless, this method also consumes a lot of energy during the set-up process of cluster formation. To cope with such problems, we propose a novel cluster-based protocol. For secure communications in cluster-based sensor networks, key pre-distribution methods using a polynomial key pool are more suitable than other methods to guarantee reliable and stable operation. With this method, however, some nodes cannot join each other because of the probability of pairwise key establishment. Moreover, a hierarchical structure requires a differentiated security level in each part. To cope with such problems, we propose a key management method with an authentication method.

In this study, we propose an energy-efficient and reliable routing protocol for environment monitoring sensor networks to prolong the network's lifetime. First, we propose a clustering method that reduces unnecessary data transmission among nodes by eliminating the duplication of data. Our method alleviates the problem of nearby nodes collecting the same data from adjacent areas by electing all the nodes that form a cluster with consideration of their sensing coverage. Furthermore, it introduces relay nodes, also called repeaters, which help to hop the data transmission along to cluster head nodes in order to cope with energy-hole and link-failure problems. This method prevents data loss caused by node link disconnections, thus it collects the data reliably. Second, to achieve a secure network, we propose a key management scheme that is appropriate for hierarchical sensor networks. Our proposed scheme is based on the polynomial key pool pre-distribution scheme, and sustains the network's stability through a key authentication process.

According to the performance analysis results, ARCS reduces the energy consumption and increases the transmission efficiency of; consequently, it prolongs the network lifetime by about 61%, 49%, 36% and 21% compared to LEACH, TEEN, APTEEN and ARCT, respectively. The simulation and analytical comparison results show that the proposed scheme has higher resiliency than key pool, grid and location-based schemes, and it provides an authentication

method.

제1장 서 론

제1절 연구의 배경 및 목적

무선 센서 네트워크는 최근 대두되고 있는 유비쿼터스 컴퓨팅의 연구에 힘입어, 광범위하게 설치되어 있는 유무선 네트워크 인프라에 상황인지를 위한 다양한 센서 디바이스를 결합하여 감지된 환경데이터를 응용서비스 서버와 연동하는 기술이다. 센서 노드가 온도센서와 같은 표준 센서와 다른 점은 바로 지능형 클러스터에서의 상호 연결성과 집단적으로 데이터를 수집·처리하는 능력이다. 정보통신부(MIC)와 정보통신연구진흥원(IITA) RFID/USN 기술로드맵[1] 에 의하면 USN은 어느 곳에나 부착된 태그와 센서 노드로부터 사물 및 환경 정보를 감지, 저장, 가공, 통합하고 상황인식 정보 및 지식 콘텐츠 생성을 통하여 언제, 어디서, 누구나 원하는 맞춤형 지식 서비스를 자유로이 이용할 수 있는 첨단 지능형 사회의 기반 인프라이며, RFID/USN에서는 사물의 이력정보뿐만 아니라 사물을 둘러싸고 변화하는 물리 환경계의 다양한 정보를 획득하여 생산성, 안전성 및 인간생활수준의 고도화를 실현함에 그 목적이 있음을 정의하고 있다.

이 기술을 통해 공공, 민간분야에 걸쳐 재난방제, 환경감시, 지능형 물류관리, 실시간 시큐리티, 모바일 헬스케어 등의 여러 응용 환경에 적용을 시도하고 있다 ([표 1] 참고).

센서 네트워크는 물리 또는 환경계의 현상을 정량적으로 측정하는 소자인 센서와 환경, 물리계에서 센싱된 정보 또는 센서에 관련된 특정 이벤트를 유무선 통신 기술 기반으로 하여 전달하거나 컴퓨팅을 수행하는 센서, 프로세서, 통신소자, 전지 등으로 구성되는 시스템으로 데이터 처리, 통신경로 설정, 미들웨어 처리 등을 수행하는 센서 노드, 그리고 센서 노드에서 감지된 센싱 정보를 취합하거나, 이벤트성 데이터를 센서

네트워크 외부로 연계하고 관련 센서 네트워크를 관리하는 시스템으로 '베이스 스테이션'으로 불리기도 하며, 대체로 하드웨어/소프트웨어적으로 센서 노드보다 역량이 큰 시스템인 싱크 노드 등으로 구성되는 네트워크이며, 이 네트워크를 구성하는 노드들은 광범위한 지역에 감시임무를 목적으로 배포되며 이들 센서 노드를 통해 감지된 데이터는 네트워크 내부에서 데이터 처리를 통해 보다 상위의 이벤트로 변화된 후 원격의 관리자에게 전달된다. 이때, 저가, 저 전력의 단일 홉 또는 멀티 홉 무선 네트워

크를 통해 데이터가 전송된다.

[표 1] USN 기술 분류

USN 기술	공공분야	지형 탐사
		생화학 가스 탐지
		차량의 위치 및 이동경로 확인
		도로 교통 상황 감시
		산불 감지 등 방재 재해
		해양/대기 환경감시
		환경 및 동식물 모니터링 시스템
		축산물 관리 시스템
	민간분야	자동 감시 및 경보
		도난/침입 감시
		농수산물 유통환경 감시
		농산물에 대한 생산 환경 정보 센싱
		빌딩 등 구조물 안전 감지
		고가 장비의 진동 감지
		FA/HA/BA 등
		각종 위치 추적
		원격탐사 및 데이터 수집
		각종 서식지 등 환경 정보 수집
		의료 보건 분야
		차량위치 및 이동 경로확인 시스템
		홈 네트워킹
		노인 위치 추적 및 건강관리 시스템

이러한 센서 네트워크 관련 기술은 크게 센서 네트워크 노드, 센서 네트워킹, 보안 기술로 구분된다 ([표 2] 참고).

이러한 센서 네트워크는 일반적인 네트워크와 다르게 여러 가지 제약사항이 존재한다[2].

전력제한 - 센서 노드는 일회성으로 재충전이 불가능한 배터리로 동작한다[3][4].

계산능력 - 저가격 및 저전력의 요구사항을 만족시키기 위해 계산능력이 제한된 프로세서를 사용하므로 일반 네트워크와 다른 적용이 필요함.

통신능력 - 센서 노드의 전송 범위는 제한되어 있다.[5]

[표 2] 센서 네트워크 관련기술

센서네트워크	센서 네트워크 노드 (센서/싱크/USN게이트웨이)	센서 기술
		근거리 무선통신 기술
		에너지 Harvesting 기술
		초소형 운영체제 기술
		SiP/SoC 기술
		센싱 정보 전달망 엑세스 기술
		TCP/IPv6 적응 기술
	센서 네트워킹	저전력 기술
		노드 위치 검출 밑 동기 기술
		멀티 홉 라우팅 기술
		네트워크 동기 기술
		Self-organizing 기술
		저전력 네트워킹 기술
		센서 데이터 처리 및 관리 기술
	보안기술	경량 센서 노드 보안 기술
		보안 라우팅 프로토콜 및 게이트웨이 보안 기술
		취약성 방지 기술
		키 분배 및 관리 기술
		프라이버시 보호 기술

에너지 효율의 관점에서 센서 네트워크의 가장 큰 이슈는 네트워크의 수명 연장이다. 네트워크의 수명 연장을 위해 노드 각각의 전력을 효율적으로 사용할 수 있는 방법이 필요하며, 이러한 효율적인 전력 사용은 결과적으로 전체 네트워크의 수명을 연장시킬 수 있다. 센서 노드의 에너지 소모는 크게 두 부분으로 나누어지며 이는 데이터 감지 및 처리와 전송으로 구분된다. 그러나 몇몇 선행 연구에 의하면 데이터 전송에 소비되는 에너지는 노드 내부 데이터 처리에 소비되는 에너지보다 상당히 큰 것으로 알려져 있다[6][7].

보안상의 관점에서 가장 이슈가 되는 센서 네트워크의 주요 특징은 센서 노드의 제한된 능력, 센서 노드들에 대한 물리적 보안의 취약성, 그리고 브로드캐스팅을 주 통신수단으로 하는 멀티 홉 라우팅 및 데이터 융합 등이 있다. 센서 네트워크의 실효성을 위해서는 센서들이 매우 제한된 연산, 통신, 저장능력 및 에너지원만을 가질 수 있어 정상적인 동작을 위한 프로토콜뿐만 아니라 보안 기능의 사용에도 많은 제약이 따른다. 이러한 제한된 자원은 일반적인 네트워크에서 사용되는 알고리즘의 적용이 불가능하게 된다. 또한 센서 네트워크는 사람의 접근이 어려운 지역에 설치되어 장기간 방

치된 상태로 운영되므로 물리적인 공격에 매우 취약하다. 센서의 제한된 전력과 통신 능력은 인접 노드로의 제한된 브로드캐스팅을 주요 통신방식으로 사용하도록 하여 일대일 통신에 비해 훨씬 많은 취약성과 보안상의 어려움을 가중시키고, 특히 전력이나 대역폭의 효율적인 사용을 위해 중간 노드들이 경유하는 메시지에 대한 부분적인 프로세싱을 해야 하는 특성은 보안능력을 더욱 더 어렵게 만든다[8][9][10].

노드 포획 - 센서 네트워크는 수천 또는 수 만개의 소형 센서들이 넓은 지역에 흩어져 설치되므로 운영자가 각 센서 노드들을 관리하고 감시하는 것은 불가능하다. 따라서 공격자는 쉽게 센서 노드에 물리적으로 접근하여 비밀키나 중요 데이터를 추출해 낼 수 있으며, 프로그램을 수정하여 네트워크에 재투입하거나 보다 강력한 노드로 교체시켜 공격에 이용할 수 있다. 하드웨어적으로 공격에 강인한 센서 노드를 값싸게 만드는 것은 매우 어려워 현실성이 없다. 따라서 센서 네트워크를 설계할 때 소수의 악의적인 노드가 존재하더라도 전체 네트워크가 안정적으로 동작하도록 탄력적인 네트워크를 구축한다.

프라이버시 - 센서 네트워크는 쉽게 악의적인 목적의 감시 네트워크로 악용될 수 있다. 은밀한 센서 네트워크를 통해 직원들의 동태를 감시하거나 백화점의 고객들을 감시할 수도 있고, 정보기관의 경우 각종 공중 장소에 감시 네트워크를 설치하여 시민의 프라이버시를 침해할 수도 있다. 기존의 CCTV 카메라가 유사한 목적으로 합법적으로 사용되고 있으나 센서 네트워크의 경우는 이를 쉽게 감출 수 있고, 또한 완전 자동화된 방법으로 원격에서 대량의 정보 수집 및 가공이 용이하다는 사실이 문제를 더욱 악화시키는 것이다. 또한 합법적으로 설치/운영되는 센서 네트워크라 하더라도 여기서 수집된 정보들이 불법적으로 악용될 수 있는 소지는 존재한다. 불법적인 센서들을 찾아내는 센서 탐지 장치의 보급이 한 방어책이 될 수 있다. 그러나 기술적인 방법으로 프라이버시 문제를 해결하기는 어려우므로 사회규범이나 법/제도적인 장치의 확립이 선행되어야 한다. 센서 노드의 존재를 인지시키고 수집된 정보의 사용 목적을 명시하여 거부감을 줄여 주는 노력도 필요하다. 다음은 센서 네트워크의 보안을 위한 요구사항을 나타

낸다.

보안과 인증 - 민감한 센싱 데이터의 도청이나 프로토콜 메시지의 조작 등 일반적인 통신 보안을 위해 다양한 암호학적인 보안 기법들이 사용될 수 있다. 센서 네트워크의 경우 데이터 융합, 단대단 보안은 대부분의 경우 불가능하므로 링크계층 보안 프로토콜, 버클리 모트가 가장 일반적인 보안 대책이 될 것이다. 대표적인 프로토콜로 버클리 모트에서 채택한 TinySec을 들 수 있다. 여기서 가장 중요하며 또한 어려운 문제는 센서 네트워크의 제한된 자원을 고려하여 계산량이나 통신량에 있어 얼마나 효율적으로 보안기능을 추가하는가이다.

라우팅 보안 - 센서 네트워크의 동작에 근간이 되는 것은 라우팅 프로토콜이다. 기존의 애드 혹 라우팅 프로토콜들은 대부분 센서 네트워크에 사용되기에 너무 무겁거나 또한 센서 네트워크의 특성상 사용이 불가능하다.

키 관리 - 센서 네트워크는 전혀 혹은 거의 네트워크 인프라가 없는 상태에서 무작위로 배포된 센서들이 라우터의 역할을 겸하여 안전한 네트워크 인프라를 구축하여 모든 다른 보안목적에서 사용될 비밀 키를 설정하고 관리하는 것이다. 센서 네트워크의 다양한 특성들은 특히 키 관리 문제에 중대한 도전이 되어 센서 네트워크의 보안에서 가장 어려우며 또한 중요한 보안의 출발점이 된다.

보안 데이터 융합 - 센서 네트워크의 센싱 데이터는 센서의 밀집한 배치로 인한 거리의 인접성에 의해 많은 부분 중복이나 불필요한 부분이 존재하여 원래 데이터를 그대로 전송하면 귀중한 에너지나 대역폭 등 자원을 낭비하게 된다. 따라서 일부의 중간 노드들이 데이터를 취합하여 중복을 제거하고 특징적인 데이터만을 추출하여 압축된 형태로 전송하게 된다. 문제는 이러한 데이터 융합 노드들이 공격의 주요 목표가 되고 이들이 공격자의 수중에 들어간다면 질의를 무시하거나 거짓의 위조된 융합 결과를 보고하

여 센서 네트워크의 기능을 심각하게 훼손시킬 수 있다. 이는 라우팅 공격이나 서비스 거부 공격 등에 대한 보안과는 다른 데이터 융합 결과 정확성을 보장할 수 있는 보안대책이 필요하다.

서비스 거부 공격 - 센서 네트워크는 매우 제한된 자원만을 갖는 수많은 소형 센서들로 순간적으로 형성되는 네트워크이다. 따라서 기반구조 자체가 매우 취약하며 물리적인 공격에도 무방비 상태이므로 다양한 형태의 서비스 거부공격이 가능하다. 열악한 환경에서 동작하는 센서 네트워크는 일부 오류가 발생하더라도 지속적으로 동작하도록 설계되지만 이들은 지능적이고 결정적인 공격자들에 대해서는 거의 제 기능을 발휘하지 못한다. 특히 센서의 수명은 곧 전원의 수명과 동일하므로 다양한 방법으로 센서의 전원을 고갈시키는 서비스 거부 공격은 가장 막기 어려우며 치명적이다.

센서 네트워크에 대한 서비스 거부 공격은 다양한 계층에서 이루어질 수 있다. 물리계층에서의 전파방해나 센서 노드의 물리적인 파괴를 필두로 링크 계층 및 네트워크 계층에서의 다양한 자원 고갈 공격들이 가능하다.

키 분배와 관련된 센서 네트워크의 한계 및 이에 따른 요구조건은 다음과 같다.

노드 포획 - 센서 노드들은 공공장소나 적대적인 환경에 설치될 수 있고 또한 관리되지 않는 상태로 운용되므로 공격자에 의한 물리적 접근 및 공격에 취약하다. 센서 노드 내에 저장된 비밀키는 센서가 물리적으로 안전한 메모리를 갖추지 않는 한 물리적인 공격에 의한 노출은 피할 수 없다. 따라서 일부 센서 노드내의 비밀정보가 노출되더라도 해당 노드나 그 주위의 노드들을 제외하고는 전체 네트워크의 안전성이 유지되어야 한다.

네트워크 설정 정보 – 센서 노드들은 무작위로 설치되므로 설치 후의 네트워크 구조에 대한 정보를 미리 알 수는 없다. 비록 수작업으로 하나씩 설치한다고 하더라도 수많은 노드들의 개별적인 위치를 사전에 결정하는 것은 거의 불가능하다. 따라서 설치 후의 네트워크 토폴로지에 대한 사전 지식을 바탕으로 하는 키 관리 방식은 바람직하지 않다.

노드 제한 – 센서 노드들은 매우 제한된 계산력, 전송전력 및 대역폭을 가지므로 프로토콜에 필요한 통신량이나 저장량을 최소화해야 한다. 특히 저가의 소형 센서들에서 계산량이 많이 소요되는 공개키 암호를 자유로이 이용하는 것은 아직까지는 현실적으로 불가능에 가깝다.

동적 토폴로지 변화 – 센서 노드들은 초기 설치 후 다양한 이유로 추가 설치하거나 네트워크에서 제외시켜야 한다. 따라서 노드가 추가 설치되더라도 기존의 노드들과 키 설정이 가능하여야 하며, 또한 비정상적인 행위를 하는 노드가 탐지되면 다이내믹하게 이를 네트워크로부터 제거해야 한다. 그러므로 위의 센서 네트워크의 보안요구사항을 만족하기 위해 센서 네트워크에 특화된 보안 설계가 필요하며, 특히 보안키의 관리 및 운용 방법이 중요하다.

제2절 연구의 범위 및 논문의 구성

본 연구에서는 1절에서 언급한 센서 네트워크의 에너지 효율과 보안 문제를 다루고자 한다. 세부적으로는 센서네트워크의 응용환경인 환경데이터 수집을 목적으로 하는 센서 네트워크의 에너지 효율성을 극대화하는 방안과, 해당 응용환경에서 발생할 수 있는 다양한 공격에 보안상 안전한 키 분배 및 관리 기법을 제안함으로써 센서 네트워크에서 발생할 수 있는 보안 위협[11]을 제거하고, 기존의 키 분배 방법들에 비해 높은 효율성과 보안성을 제공하고자 한다.

에너지 효율의 관점에서, 최근에 제안된 라우팅 기법들[12]은 평면, 계층적, 위치기반, 실시간 등으로 분류된다. 이러한 기법들 중 계층적 라우팅 알고리즘은 클러스터링을 기반으로 한 데이터 모음을 하는 기법으로, 노드들은 다른 역할을 수행하여 데이터를 재처리 하여 에너지의 중복 소비를 줄이는 방법으로 감시를 목적으로 하는 센서 네트워크의 수명을 향상시키는데 적합한 라우팅 기법이다.

그러나, 클러스터링 방식은 클러스터 헤드 노드에 부하가 집중되어 클러스터 헤드 노드의 에너지가 급격히 소모되므로 전체 네트워크 잔여 에너지의 불균형이 커지게 된다. 이러한 에너지의 불균형을 해소하기 위해 클러스터 헤드 노드의 역할을 주기적으로 바꾸는 여러 가지 방법들이 제안되었으나 이들 역시 클러스터 헤드 노드 부하 분산의 문제와 클러스터 헤드 노드 최적화 및 에너지 홀과 같은 문제가 있다[13][14][15].

보안상의 관점에서 볼 때, 센서 네트워크에서 안전한 통신을 위해서는 노드들 사이에 전송되는 메시지를 암호화하는 것이 중요하며, 특히 에너지 효율을 목적으로 설계된 클러스터 기반 프로토콜에서 충분한 데이터 안정성을 보장하기 위해서는 클러스터 구조에 적합한 키 관리 및 인증 기법이 필요하다. 이러한 클러스터 기반 프로토콜은 selective forwarding, HELLO flood attack, sybil attack 과 같은 보안상 취약점이 존재한다.

본 연구에서는 위의 에너지와 보안 측면에서 발생할 수 있는 문제점들을 개선할 수 있는 새로운 라우팅 기법으로서 에너지 효율적이면서 안전한 클러스터 기반 라우팅 및

키 분배 및 인증 기법을 제안하고자 한다.

제안하는 방법은 에너지 측면에 있어 멀티 홉 기반 센서 네트워크의 데이터 중복 수집 및 전송 문제를 완화하고, 노드 및 영역별 에너지 불균형 문제를 완화하였으며, 클러스터 헤드 노드의 잘못된 위치로 인한 네트워크 링크 단절 문제와 수집된 데이터의 정확도를 개선하였다. 보안 측면에 있어 계층 클러스터 구조를 갖는 센서 네트워크에 적합한 키 관리 기법을 적용하였다. 이 방법은 다항식 키 풀 기반 기법에 기초하며 키 인증 절차를 통해 안정된 네트워크를 유지한다.

또한, 이 방법은 클러스터 네트워크의 주기적인 노드의 연결을 쉽게 이루고, 여기에 신뢰할만한 베이스 스테이션 또는 싱크에 의한 클러스터 헤드 노드의 인증을 매 라운드마다 반복함으로써 안정적인 클러스터의 유지가 가능하며, 각 클러스터에 사용하는 개별 키를 할당함으로써 클러스터 내 보안이 향상되었다. 여기에 더해 클러스터 헤드 노드들 사이의 멀티 홉 전송에 사용되는 키를 별개로 지정하여, 멀티 홉 전송 중 발생할 수 있는 외부 공격에 대한 보안성을 향상시켰다.

이 논문의 구성은 다음과 같다.

제 2장에서는 기 제안되었던 센서 네트워크의 다양한 라우팅 기법들을 그 분류에 따라 비교 및 분석한다. 특히 클러스터 기반 라우팅 기법은 세부 분류에 따라 특징을 비교함으로써 이 연구에서 제안하는 에너지 효율적인 라우팅 기법에 대해 고찰한다.

또한 다양한 키 분배 기법들을 소개하며 해당 기법들의 특징과 문제점에 대해 분석함으로써 이 연구에서 제안하는 클러스터 기반 키 관리 및 인증 기법을 고찰한다.

제 3장에서는 노드 경쟁을 통한 에너지 홀 문제와 네트워크 단절 문제의 완화 및 수명 증대의 결과를 보이는 클러스터 기반 멀티 홉 클러스터링 기법과 높은 보안성 및 인증을 통한 노드 포획 및 키 유출에 대한 안전성을 갖는 클러스터 기반 센서 네트워크에 적합한 키 관리 및 인증 기법에 대해 기술한다.

제 4장에서는 제안하는 클러스터링 기반 라우팅 기법의 성능을 키 관리 기법의 유무에 따라 데이터 수집률과 정확도, 네트워크 연결도, 영역별 에너지 소비 평준화 정도, 고립 노드의 수, 네트워크의 생존시간과 관련하여 평가하며, 키 관리 기법의 안전도를 측정한다.

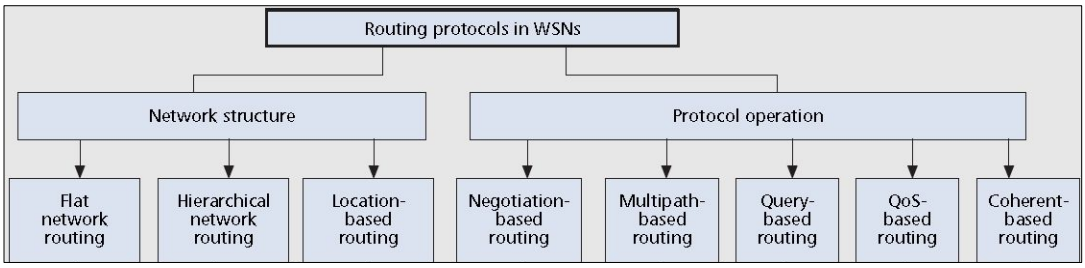
마지막으로 5장에서는 본 연구의 결론 및 향후 연구 과제에 대해 논의한다.

제2장 관련 연구

제1절 센서 네트워크 라우팅

센서 네트워크 환경에서는 노드들 상호간의 무선 통신을 통해 네트워크를 구성하고 데이터를 싱크 또는 베이스 스테이션에 전달하는 구조를 갖는다. 이러한 정보 전달을 위해서는 적합한 라우팅 기법이 요구된다. 그러나 센서 네트워크의 특성상 일반적인 네트워크 라우팅 프로토콜은 적용에 어려움이 있다. 따라서 센서 노드의 제한된 자원 특성과 환경을 고려한 라우팅 기법이 필요하다.

아래의 [그림 1] 은 센서 네트워크의 라우팅 프로토콜을 네트워크 구조와 프로토콜 동작에 의해 구분한 것이다.



[그림 1] 센서 네트워크 라우팅 프로토콜의 분류

이중 네트워크의 구조에 의한 라우팅 기법은 다음과 같이 분류된다.

평면 라우팅 기법(Flat network routing)

· Direct diffusion[16]
· Sensor protocols for Information via nego-tiation(SPIN)[17][18]
· Rumor routing[19]
· Minimum cost forwarding algorithm[20]

· Gradient-based routing[21]
· Information-driven sensor querying(IDSQ)
  Constrained anisotropic diffusion routing(CADR)[22]
· COUGAR[23]
· Routing protocols with random walks[24]
· ACQUIRE[25]
· Energy-aware routing[26]

계층적 라우팅 기법(Hierarchical network routing)

· Low-energy adaptive clustering hierarchy protocols(LEACH)[27]
· LEACH-C[28]
· PEGASIS[29]
· HEED[30]
· BCDCP[31]
· Threshold-sensitive energy efficient protocols(TEEN)[32]
· Adaptive periodic TEEN[33]
· VAR[34]
· TVAR[35]
· ARCT[36]
· Small minimum energy communication network(MECN)[37]
· Self-organizing protocol[38]
· Sensor aggregates routing[39]
· Virtual grid architecture routing[40]
· Hierarchical power-aware routing[41]
· Two-tier data dissemination[42]

위치 기반 라우팅 기법(Location based routing)

· Geographic adaptive fidelity[43]
· Geographic and energy aware routing[44]

· MFR, DIR, and GEDIR[45]
· The greedy other adaptive face routing[46]
· SPAN[47]

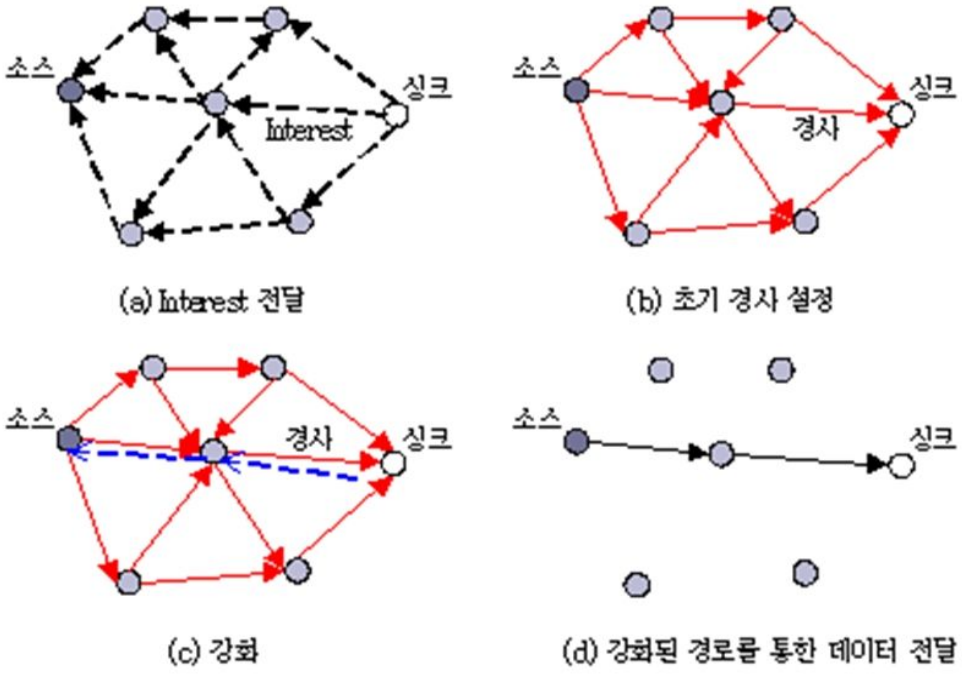
위의 네트워크 구조에 의한 기법 분류들 중 대표적인 몇 가지 기법들을 기술한다.

1. 평면 라우팅

가. Direct diffusion

수집 노드가 원하는 정보를 얻기 위해 전체 센서 노드에 쿼리를 전송한 후 질의에 해당하는 노드들이 데이터를 수집 노드에 전송하는 데이터 중심적 라우팅 기법이다.
DD의 동작단계는 아래의 [그림 2] 와 같다.

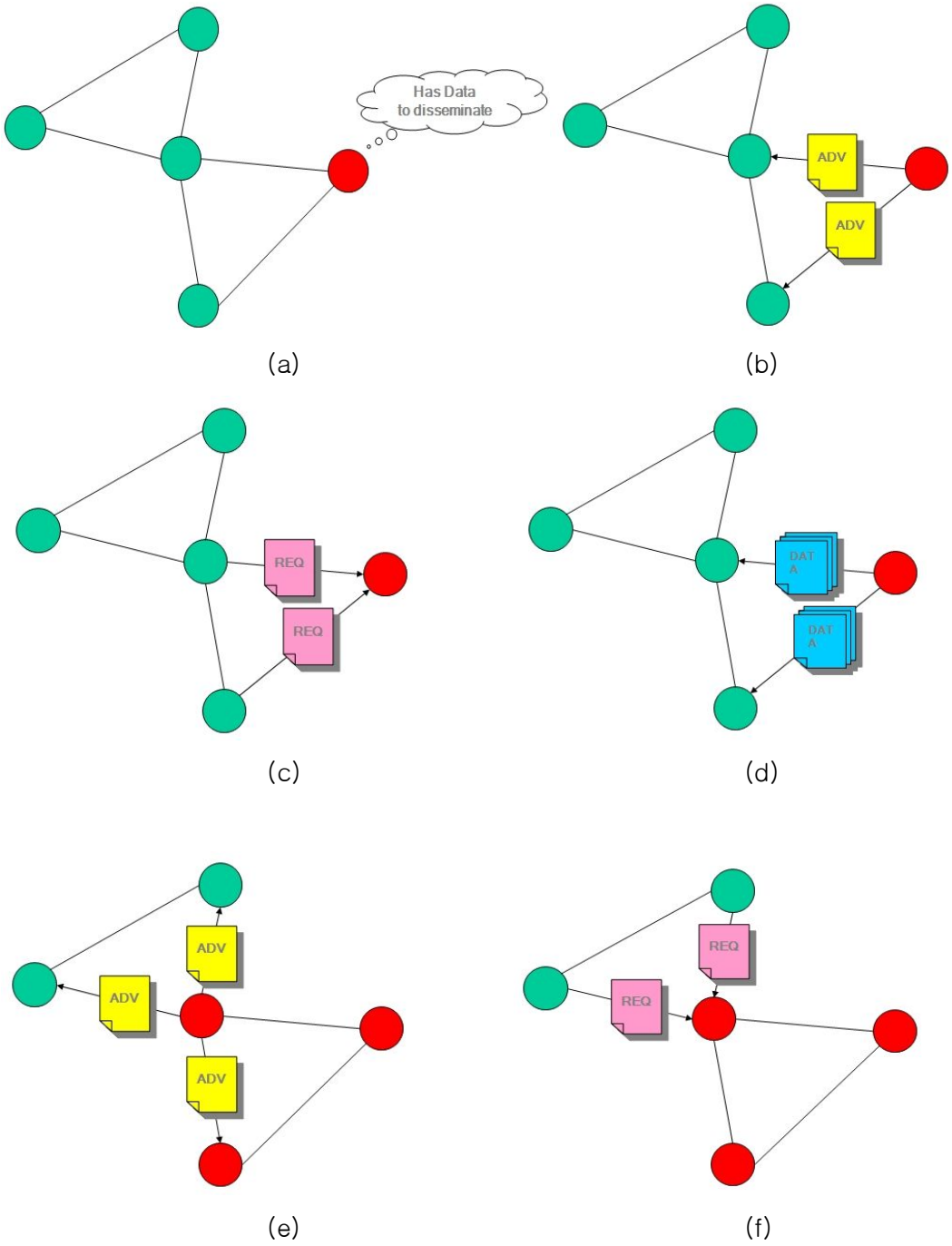
(a) 수집노드는 특정 쿼리를 전체 센서 노드에 전달한다.
(b) 쿼리를 받은 노드는 관련된 데이터가 있을 경우 수집 노드에 그 데이터를 전송한다. 이 데이터는 다중 경로를 통해 전송되며 이때 경사도가 설정된다.
(c) 수집노드는 이러한 경로의 강화를 통해 단일화된 경로를 설정한다.
(d) 강화된 경로를 통해 데이터의 전달이 이루어진다.



[그림 2] Direct diffusion 기법의 동작

나. SPIN

SPIN은 flooding 기법의 단점을 보완하기 위해 만들어졌다. 이 기법은 센서 노드가 자신의 데이터를 광고하고 싱크로부터 요청을 기다리는 형태의 데이터 중심적 라우팅 기법이다. 이 기법의 동작은 아래의 [그림 3] 과 같다.



[그림 3] SPIN 기법의 동작

(a,b) 데이터를 가지고 있는 센서 노드는 패킷 광고를 통해 (ADV broadcast) 데이

터를 가지고 있음을 알린다.

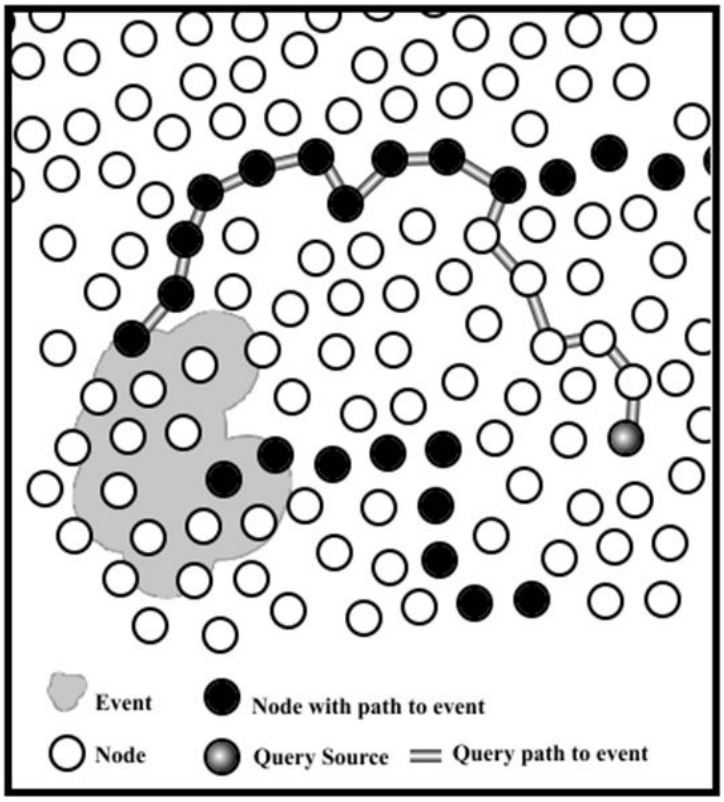
(c) ADV를 수신한 이웃 노드들 중 이 데이터를 수신하기 원하는 노드는 REQ로 응답한다.

(d) 데이터를 가지고 있는 노드는 REQ 수신 후, REQ를 보냈던 노드들에게 DATA를 송신한다.

(e) (a-d)의 반복을 통해, 데이터 수신을 원하는 노드는 데이터를 받을 수 있다.

다. Rumor routing

이 기법은 쿼리와 이벤트 플러딩의 혼합된 형태이며 아래의 [그림 4] 와 같다.



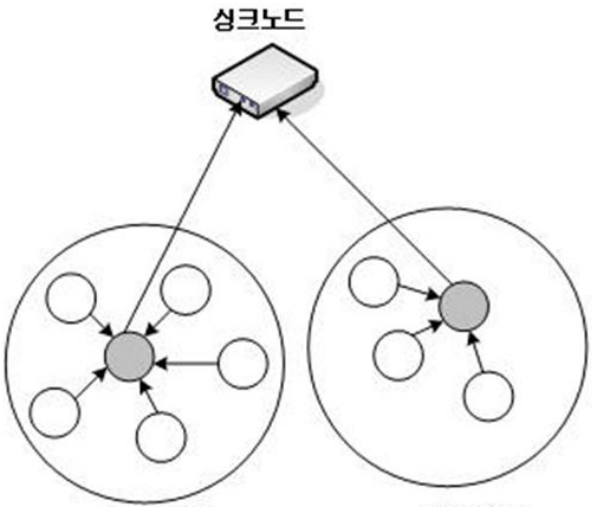
[그림 4] Rumor routing 기법의 동작

이 기법에서 데이터를 필요로 하는 노드 즉 데이터를 수신받기 원하는 노드인 query

source는 쿼리를 발생하여 인접 노드에 전송하며, 데이터가 발생된 노드, 즉 이벤트를 감지하여 데이터를 전송하고자 하는 노드는 이벤트를 발생하여 전송한다. 이 두 쿼리와 이벤트는 네트워크내부를 노드들 간의 중계에 의해 네트워크 내부를 이동하다가 특정 지점에서 만나게 되고, 이때 경로를 생성하여 쿼리를 발생한 노드와 이벤트를 전송하는 노드들 간에 경로가 설정되는 기법이다.

2. 계층적 라우팅

이 기법은 센서 네트워크에서 쉽게 발생할 수 있는 인접 노드들 사이의 유사 데이터 생성과 중복 전송에 소비되는 에너지를 줄이기 위해 데이터 모음과 압축을 통한 클러스터 기반 데이터 전송 및 라우팅 기법이다 ([그림 5] 참고). 즉, 이 기법은 다수의 지역 클러스터를 구성하며 클러스터 외부와의 통신 및 클러스터 내부 노드들의 데이터 모음 및 압축을 클러스터 헤드 노드가 담당하는 기법이다. 이러한 기법은 대규모의 센서 네트워크에 적용이 가능하며 노드의 전력 소비 효율 측면에서도 강점을 가진다.



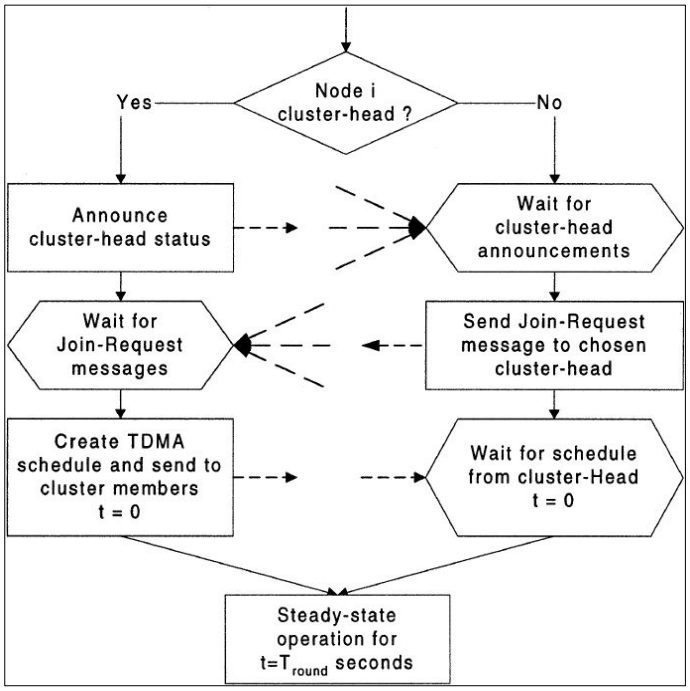
[그림 5] 클러스터의 기본 구조

가. LEACH

클러스터 기반의 계층적 라우팅 프로토콜인 LEACH(Low Energy Adaptive Clustering Hierarchy)는 센서 네트워크의 대표적인 클러스터링 방법으로 클러스터 헤드가 클러스터 내 멤버노드로부터 데이터를 수집하여 통합한 후 싱크 또는 베이스 스테이션에 전송을 한다. 이 방법은 클러스터 헤드 노드의 에너지 소비가 크므로 전체 네트워크의 노드에 에너지 소비를 분산시키기 위해 클러스터 헤드 노드의 역할을 주기적으로 바꾼다. 매 라운드마다 시행되는 클러스터 헤드 선정 $P_i(t)$는 아래의 식과 같다.

$$P_i(t) = \begin{cases} \dfrac{k}{N - k^*(r \bmod \frac{N}{k})} : C_i(t) = 1 \\ 0 : C_i(t) = 0 \end{cases} \quad (1)$$

N은 네트워크의 총 노드의 개수, r은 현재 라운드, t는 현재 시간, k는 전체 노드들 중 클러스터 헤드로 선정되는 노드의 비율을 나타낸다. $P_i(t)$는 클러스터 헤드가 되기 위한 임계값이 되며 이 값을 기준으로 하여 노드는 자신이 클러스터 헤드가 될지 여부를 결정한다. 이 방법은 최근에 클러스터 헤드가 되었던 노드는 $P_i(t)$값이 0이 되어 클러스터 내의 모든 노드가 클러스터 헤드가 될 수 있다. [그림 6] 은 한 라운드 진행에서 클러스터 헤드 노드로 선정된 노드의 동작 과정과 클러스터 헤드 노드에 종속되는 클러스터 내 노드의 동작 과정을 보인다.



[그림 6] LEACH의 클러스터 헤드 선정

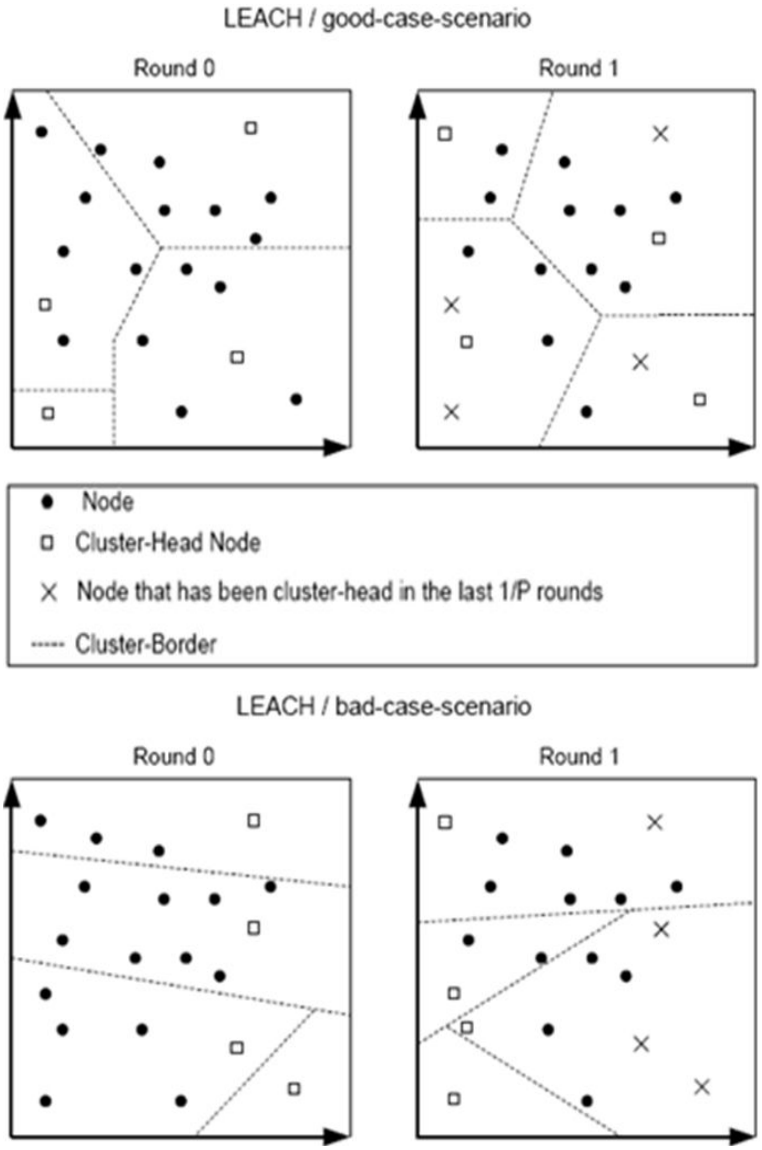
아래의 [그림 7] 은 일정한 간격을 갖는 라운드로 구성된 LEACH의 동작을 나타낸다. 한 라운드는 setup과 steady로 나누어지며 이러한 과정은 매 라운드마다 반복된다. 따라서 이 방법은 사전에 정해진 주기에 따라 데이터의 측정이 가능하다.

[그림 7] LEACH의 타임라인

그러나 이 방법은 클러스터 헤드 노드가 네트워크에 고르게 분포되지 못할 확률이 있다.

LEACH는 노드들 사이의 다른 통신 거리를 고려하지 않았다. 그러므로 이 방법의 라운드 진행에 따라 주기적으로 바뀌는 클러스터와 클러스터 헤드 노드의 선정은 네트워크의 상태를 잘 반영하지 못한다. 아래의 [그림 8] 과 같이 클러스터 헤드로부터 멀

리 위치한 클러스터 헤드 및 일반 노드는 통신 거리가 멀기 때문에 그 만큼 큰 전송 에너지를 소모하게 되어 전체적인 네트워크 수명이 짧아진다.



[그림 8] LEACH에서 발생할 수 있는 클러스터 헤드 노드의 분포 문제

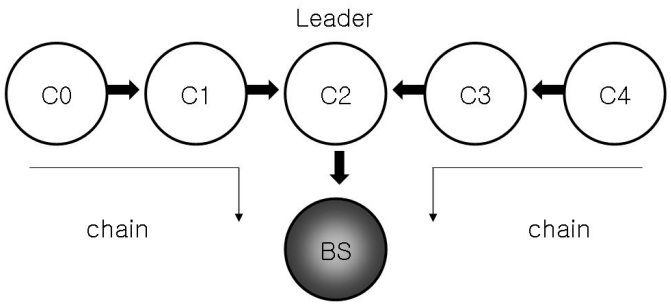
나. LEACH-C

LEACH의 비효율적인 클러스터 구성 문제를 해결하기 위하여 LEACH-C(Low Energy Adaptive Cluster Hierarchy-Centralized)가 제안되었다.

LEACH-C는 클러스터를 싱크 또는 베이스 스테이션의 주도로 구성하게 된다. 네트워크의 모든 노드는 자신의 위치정보와 에너지 정보를 싱크에 알리고 싱크는 이 정보를 다른 모든 노드에게 알려주어 최적의 클러스터를 구성하도록 하여 LEACH에서 발생하는 클러스터 헤드의 배치 문제를 해결하려고 하였다. 이 방법은 네트워크의 모든 노드가 싱크와 통신하는데 따른 오버헤드와 위치 계산에 따른 클러스터 선정에 소모되는 에너지가 추가적으로 필요하다.

다. PEGASIS

PEGASIS(Power-Efficient Gathering in Sensor Information Systems)는 LEACH 프로토콜에 chain 개념을 도입하여 보다 에너지 효율을 향상시킨 프로토콜이다. 이 네트워크에서는 싱크에서 가장 멀리 떨어진 노드부터 체인이 시작되어 싱크에 가장 가까운 노드까지 이어진다. 모든 데이터(토큰)를 통하여 이동하며 체인 중 한 노드가 리더가 되어 취합한 데이터를 싱크에 전송하는 구조이다 ([그림 9] 참조).



[그림 9] PEGASIS의 데이터 전송 경로

이 방법은 매 라운드마다 무작위로 리더가 선정되는 방법을 취하고 있으며 LEACH에 비해 에너지 효율 면에서는 나은 성능을 보이고 있지만 데이터의 적시성에 있어 많은 전송 지연이 있으며 데이터 유실시 추가적인 에너지의 소모가 크므로 효율적이지

못하다.

라. HEED

LEACH의 클러스터 헤드 선정 방법에 변인을 추가하여 클러스터 구성에 에너지 측면을 고려할 수 있도록 한 HEED(Hybrid, Energy-Efficient. Distributed)는 LEACH의 클러스터 헤드 선정 알고리즘에 노드의 가용 에너지 량을 고려함으로써 가용 에너지 량이 많은 노드가 클러스터 헤드가 되도록 하여 네트워크 수명을 증가시키도록 한 알고리즘이다. 이 방법의 헤드 선정을 위한 확률 함수는 아래의 식과 같다.

$$CH_{prob} = C_{prob} \times \frac{E_{residual}}{E_{\max}} \quad (2)$$

$E_{residual}$은 노드에 남아있는 가용한 에너지를 말하며, $E_{\max}$는 노드가 초기 배치될 때 가지고 있는 총 에너지 량을 말한다. C_{prob}는 네트워크 노드들 중 클러스터 헤드 노드의 비율을 나타내며, 노드의 잔여 에너지 량이 같은 후보가 여럿 있는 경우 클러스터 내 통신비용을 두 번째 기준 값으로 하여 클러스터 헤드를 선정하도록 하였다.

마. BCDCP

BCDCP(Base Station Controlled dynamic clustering Protocol)은 베이스 스테이션이 복잡한 계산을 대부분 수행한다는 가정을 둔다는 점에서 LEACH-C와 유사한 부분이 있다.

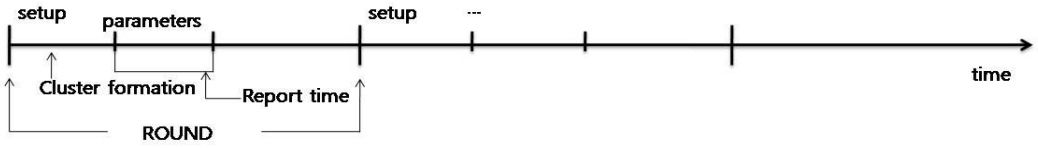
이 프로토콜은 setup과 data communication 이라는 두개의 단계를 가지고 있으며 클러스터 형성에 있어 클러스터 헤드의 후보 집합 S를 설정하여 이 집합에서 클러스터 헤드를 결정하며 클러스터 분할 알고리즘으로 네트워크를 정해진 숫자의 클러스터가 될 때 까지 계속 두 개로 나누는 과정을 반복한다.

또한 이 방법은 클러스터에서 노드들의 데이터를 취합한 헤드가 직접 싱크에 데이터를 전송하는 방식이 아닌 클러스터 헤드에서 클러스터 헤드로 데이터를 전송하여 결국 최종 데이터 수집자인 싱크에 데이터를 전달하는 방식을 취하고 있다. 이 방법도

LEACH-C와 같이 각 라운드마다 모든 노드의 정보(잔여 에너지와 위치 정보)를 전송하는 형태를 띈다.

바. TEEN

TEEN(Threshold sensitive Energy Efficient sensor Network protocol)은 센서 노드들이 임계 데이터를 처리하는 반응적 네트워크이다. 이 방법은 임계값을 이용한 데이터 전송을 제외한 동작은 LEACH와 같다. 아래의 [그림 10] 은 TEEN의 동작을 나타낸다.



[그림 10] TEEN의 타임라인

이 방법은 클러스터 형성에 LEACH와 동일한 방법을 사용하며 클러스터 형성 이후 클러스터 헤드 노드가 측정하는 데이터의 parameter들, 즉 hard threshold값인 H_T와 soft threshold값인 S_T를 멤버 노드에 전송한다. 멤버 노드들은 이 값을 기준으로 report time내에 할당된 시간에 데이터 전송을 한다.

이 방법은 노드들이 측정한 값이 H_T 값을 초과할 때 데이터를 수집하여 전송이 이루어지며, H_T를 초과한 이후에 측정하는 데이터가 S_T를 초과할 때에만 데이터를 수집하고 전송한다.

결과적으로 report time에서 모든 노드가 동작하지는 않으며 낭비되는 에너지가 줄어든다. 또한 이 방법은 클러스터를 다시 구성할 때 사용자가 임의로 임계값을 재설정 할 수 있다. 따라서 이 값을 변경하여 수집 데이터의 빈도와 노드의 수명을 조절이 가능하다. 그러나 수집되는 데이터가 H_T를 초과하지 않으면 노드가 데이터를 전송하지 않으므로 데이터의 수집이 이루어질 수 없고, S_T를 초과하지 않는다면 초기값 이후의 데이터 변동, 특히 임계값 이하 데이터 변동에 대해서는 알 수 없다.

그러므로 전체 네트워크를 구성하는 노드의 생존 여부를 판단하기 어려운 문제가 있으며, 수집한 데이터가 모든 임계값을 초과한다고 하더라도 서로 인접한 노드들에게서 수집된 데이터는 클러스터 헤드에 의해 통합되는 과정을 거치므로 수집 데이터의 중복

처리에 소모되는 에너지를 고려해야 한다.

사. APTEEN

LEACH의 proactive network의 장점과 TEEN의 reactive network의 장점을 결합한 형태의 APTEEN(A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks)은 TEEN의 임계값에 의한 데이터 전송과 LEACH의 데이터 전송 주기를 융합한 형태의 하이브리드 프로토콜로서 임계값 전송이 갖는 데이터 수집과 네트워크 구성 노드의 상태 인식의 어려움을 완화한다.

APTEEN은 클러스터 형성 후 클러스터 헤드가 임계값, TDMA 스케줄과 카운트 시간 등을 포함하는 parameter들을 멤버 노드에 전송한다. 모든 노드는 parameter에 의해 정해진 시간에 수집된 데이터를 클러스터 헤드에 전송하며 데이터가 임계값을 넘었을 경우에도 데이터를 수집하여 전송한다. 그러므로 이 방법은 TEEN의 임계값 이하의 데이터 변동에 대한 데이터 수집 문제와 노드의 생존 여부 판단의 문제를 개선했다.

아. ARCT

이 방법은 2가지 종류의 클러스터를 구성하며 이를 통해 데이터를 수집한다. 2가지의 클러스터 중 첫 번째인 지역 클러스터(regional cluster)는 클러스터에 참여하는 모든 노드가 동일한 값의 센싱 데이터를 갖고 있다. 다시 말해서, 이 클러스터에 참여하는 멤버 노드가 되기 위한 조건은 노드가 수집한 센싱 데이터의 일치하는지의 여부이다. 이렇게 구성된 클러스터에서 클러스터 헤드 노드를 제외한 멤버 노드는 슬립(sleep)하여 에너지를 절약하는 구조이다.

이 방법을 이용하면 지역 클러스터는 전체 네트워크에서 한 개의 노드처럼 동작하게 되며 지역 클러스터의 에너지 소모량이 적어지게 되며 전체 네트워크 트래픽이 줄어든다. 다시 말해서, 모든 노드가 한 지역에 고르게 분포한다고 가정할 때, 이 지역 클러스터에 참여하는 노드가 증가할수록 전체 네트워크의 에너지 보존량은 높아지며 이는 곧 네트워크의 수명과 직결된다. 지역 클러스터링 후, 이 클러스터에 참여하지 못하는 노드들 - 동일한 값을 갖지 못하는 노드들 - 은 두 번째로 구성되는 클러스터인 일반 클러스터를 구성하는 후보노드가 된다. 이 클러스터는 데이터 수집과 전송을 결정하는

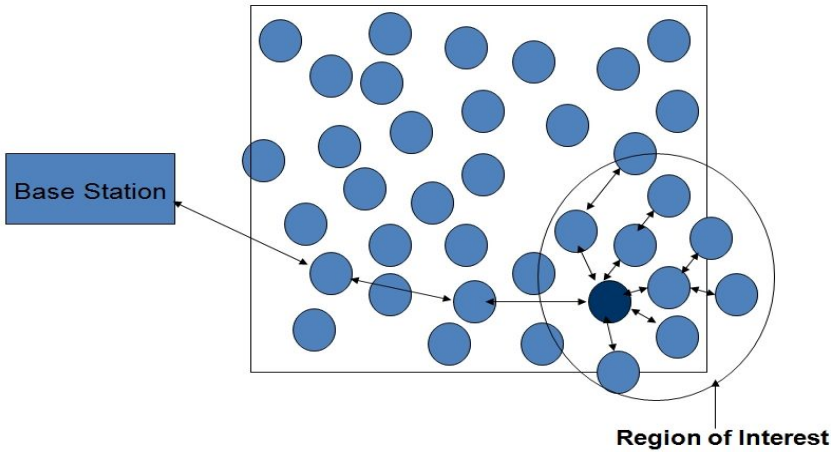
데 있어 사전에 결정된 다수의 문턱값을 이용하며, 이 문턱값은 모든 노드가 사전에 테이블로 저장하여 유지한다.

위의 두 가지 클러스터를 통해 수집 데이터의 중복을 피하면서 네트워크의 수명을 연장시키는 것이 이 방법의 목적이며 기존의 방법들에 비해 낮은 에너지 소모와 높은 네트워크 연결도, 연장된 네트워크 동작 시간, 높은 데이터 수집률을 보인다. 그러나 이 방법은 중앙의 싱크로부터 1-hop 거리 이내에 있는 노드들의 에너지 소모를 고려하지 않아 에너지 홀 문제가 발생할 경우 1-hop 거리 밖의 노드들의 가용자원 여부와 관계없이 네트워크를 유지하지 못하게 된다. 또한 지역 클러스터 선정에 있어 참여 노드 선정을 위한 파라미터가 수집되는 데이터의 특성을 정확하게 반영하지 못하는 문제가 있어 이러한 문제를 수정할 필요성이 제기된다.

3. 위치 기반 라우팅

가. GEAR

이 방법에서 노드들이 이용하는 쿼리는 위치 정보가 포함되어 있으며, 네트워크의 특정 지역으로 전파된다. 목표 지역으로 쿼리를 전송하기 위한 이웃노드들은 확률적으로 선정되며 목표지역으로만 쿼리가 플러드 된다. 이 방법에서 모든 노드는 이웃노드 테이블을 관리 및 유지하고 있으며 이 테이블에는 이웃노드들의 에너지 준위와 위치 정보가 포함되며 각 이웃 노드들의 전송비용도 저장된다. 패킷 포워드시 최소의 비용을 갖는 이웃노드를 통해 전송된다. 아래의 [그림 11] 은 GEAR의 쿼리 전송 및 최소 코스트 전송 경로에 의한 동작을 나타낸다.



[그림 11] GEAR의 동작

이 방법은 모드는 노드가 이웃노드 테이블을 유지하고 있으므로 목표 지역으로 패킷을 전송할 때 더욱 근접한 최소비용의 이웃노드를 선정하여 패킷을 포워딩 할 수 있으며, 모든 이웃노드의 거리가 멀 경우 최소 비용을 고려하여 이웃 노드 선정이 가능하다.

제2절 센서 네트워크 라우팅에서의 보안 취약성

센서 네트워크의 라우팅 기법들은 상당 부분 보안상 취약점이 존재하며, 가능한 공격은 아래와 같다. 이러한 공격 유형별로 각각의 프로토콜에 대한 보안상 취약점은 아래의 표와 같이 분류할 수 있다.

- Bogus routing information
  라우팅 메시지를 스푸핑, 변경 또는 재전송하여 라우팅을 교란시켜서 에러를 고의로 발생시키거나 라우팅 루프를 형성하거나 라우팅 정보의 전송을 지연시켜 통신을 방해한다.
- Selective forwarding
  특정 메시지(또는 노드)에 대한 전달을 거부하거나 삭제하는 공격이다.
- Sinkholes
  selective forwarding과 같이 사용 하여 라우팅 정보를 변경하여 공격자의 노드(sinkhole)로 모든 데이터들이 지나가도록 조작하여 엿듣기가 가능하다.
- Sybil
  하나의 노드가 다른 노드에게 여러 식별자로 인식하도록 하는 공격으로 geographic routing에 치명적인 공격이다.
- Wormholes
  실제로는 존재하지 않는 노드 연결이 있는 것처럼 인식하게 하는 공격으로 엿듣기 공격이나 selective forwarding과 같이 활용된다.
- HELLO floods
  멀리 있는 공격자가 강한 강도의 신호로 HELLO 패킷을 보냄으로써 가까운 곳에 위치하지 않는 공격자에게 패킷을 보내도록 하는 방법이다.

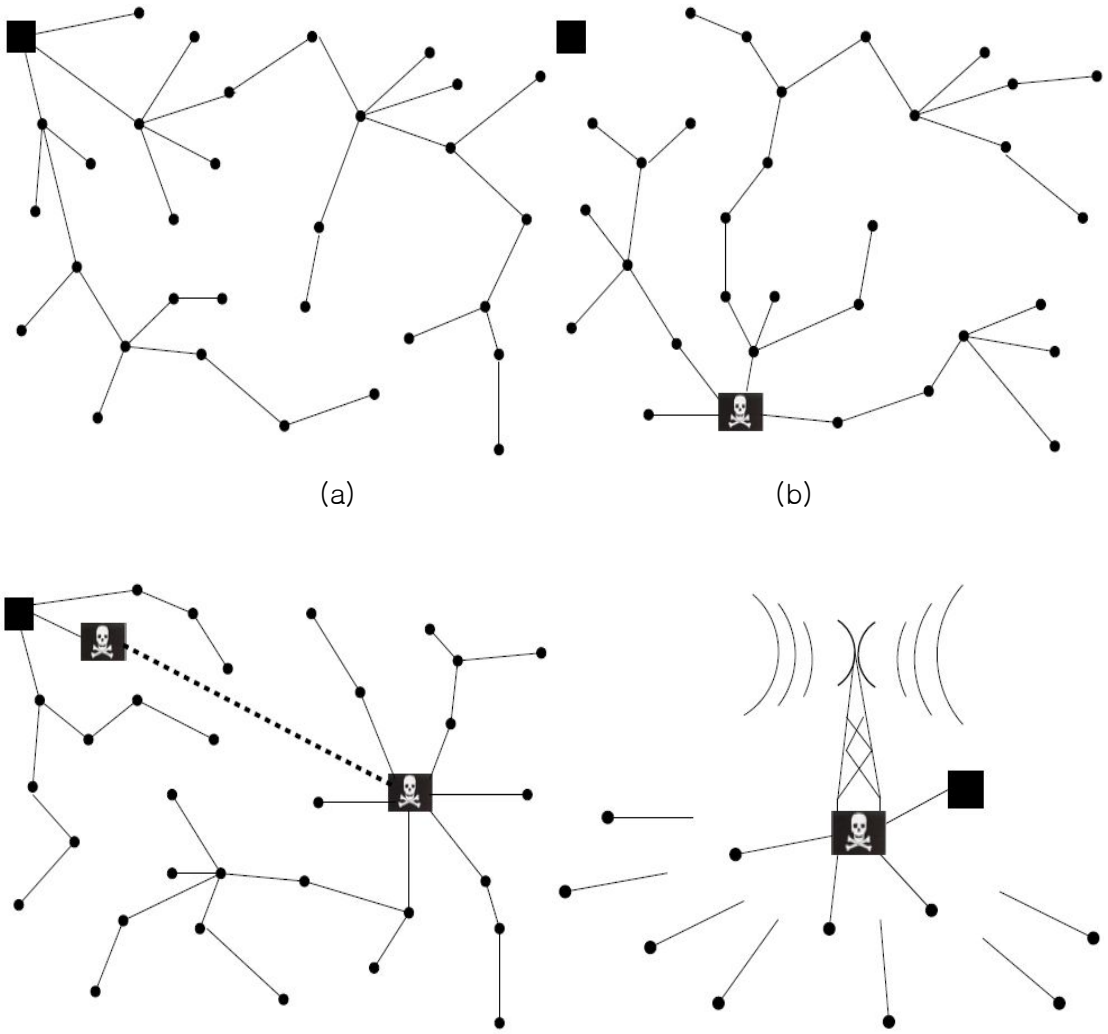
[표 3] 센서 네트워크 라우팅 프로토콜과 관련 공격유형

Protocol	Relevant attacks
TinyOS beaconing	bogus routing information, selective forwarding, sinkholes, sybil, wormholes, HELLO floods
Directed diffusion and its multipath variant	bogus routing information, selective forwarding, sinkholes, sybil, wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	bogus routing information, selective forwarding, sinkholes, sybil, wormholes
Clustering based protocols (LEACH, TEEN, PEGASIS)	selective forwarding, HELLO floods
Rumor routing	bogus routing information, selective forwarding, sinkholes, sybil, wormholes
Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA)	bogus routing information, sybil, HELLO floods

1. TinyOS 비코닝

이 기법에 관련된 공격으로는 bogus routing information, selective forwarding, sinkholes, sybil, wormholes, HELLO floods 이 있다. 특히 공격 노드가 인증되지 않은 경로 업데이트 신호를 만들었을 경우 이 공격 노드는 베이스 스테이션으로 위장이 가능하다. 그러므로 전체 네트워크의 안전성과 신뢰성 보장이 불가능하게 된다.

아래의 [그림 12] 는 정상적인 경우와 악의적인 노드의 공격을 받은 경우의 스패닝 트리를 나타낸다.



[그림 12] TinyOS beaconing 의 가능한 공격

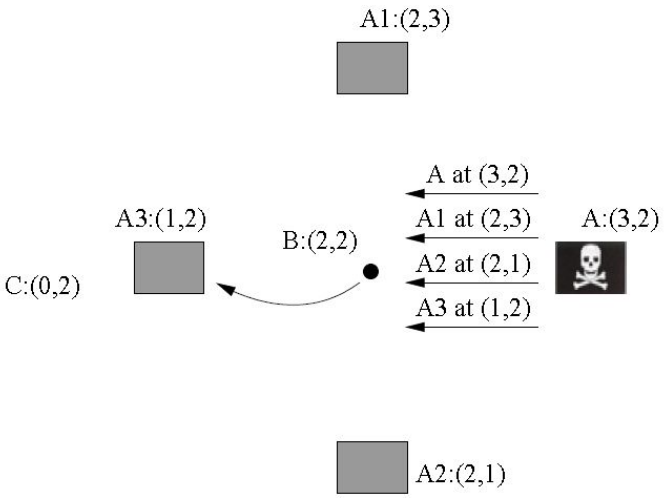
(a)는 정상적인 경우이며, (b)는 공격 노드에 의한 인증되지 않은 경로 업데이트 신호에 의한 스푸핑이며, (c)는 웜홀을 이용한 싱크홀 공격, (d)는 HELLO flood 공격을 나타낸다.

2. Direct diffusion

이 기법은 interest 정보에 대한 replay 공격, 경로 강화단계에 대한 스푸핑 공격, selective forwarding 공격, data 위변조 공격, wormhole 공격, sybil 공격에 취약하다.

3. GEAR

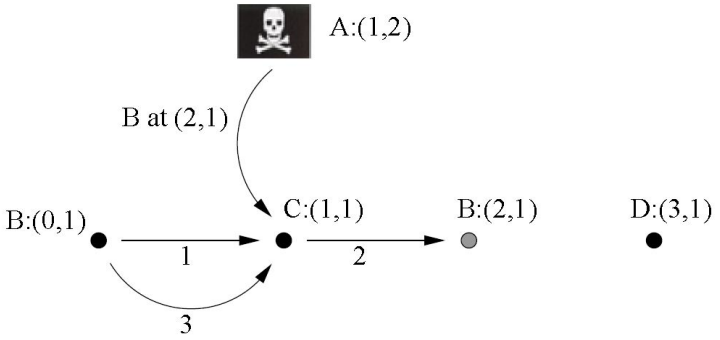
이 기법은 위치 정보에 대한 공격에 취약하다. 공격 노드는 자신이나 특정 노드의 잘못된 위치 정보를 제공함으로써 라우팅을 방해할 수 있다. 아래의 [그림 13] 은 GEAR의 가능한 공격인 sybil 공격에 대해 나타낸다.



[그림 13] 위치 기반 라우팅 기법의 가능한 sybil 공격

(3,2) 위치에 존재하는 노드 A는 자신이 마치 (2,3), (2,1), (1,2)에 존재하는 A1, A2, A3인 것처럼 B에 속인다. 그러면 노드 B는 C(0,2)에 정보를 전달하기 위해 (1,2)에 존재하는 A3를 경유해서 C에 정보를 전송해야 하지만, A의 sybil 공격에 의해 A3로 정보를 전달하지 못하고 A에 전달하게 된다. 이 경우, A는 C에 정보를 전송할 수 없기 때문에 정상적인 라우팅을 수행할 수 없게 된다. 아래 [그림 14] 는 bogus

routing information 공격을 나타낸다.

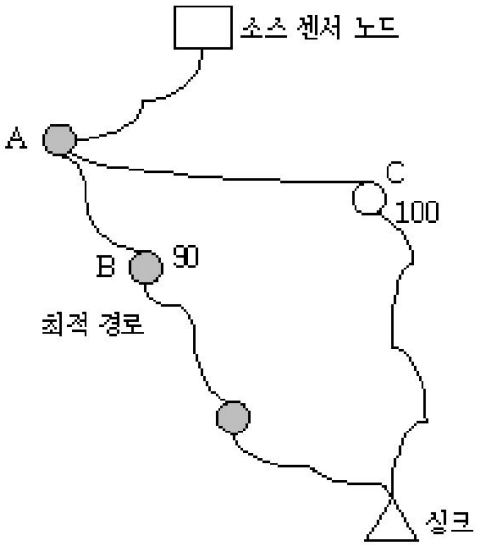


[그림 14] 위치 기반 라우팅 기법의 가능한 bogus routing information 공격

1,2 는 노드의 정상적인 동작을 나타낸다. 그러나 공격 노드 A가 노드 C에게 노드 B의 위치가 (0,1)이 아닌 (2,1)이라는 정보를 제공할 경우, C는 B에게 신호를 보내려고 시도하나 B는 신호를 받을 수 없게 된다.

4. 최소비용 포워딩

이 기법은 노드 to 싱크 사이의 코스트에 기초한 데이터 전송 알고리즘이다 ([그림 15] 참조). 이 기법에서는 라우팅 경로가 결정되면 최소 코스트를 갖는 경로를 통해 데이터를 전송한다. 이 기법은 sinkhole, HELLO flood, bogus routing information, selective forwarding, wormhole 공격에 취약하다.



[그림 15] Minimum cost forwarding 기법의 동작

5. LEACH

이 기법은 HELLO flood 와 selective forwarding 공격에 취약하다. LEACH의 클러스터 헤드 노드 선정과정에서 클러스터 헤드 노드의 멤버 노드가 되려고 하는 노드들은 인접 클러스터 헤드 노드의 신호들 중 그 신호 세기가 가장 큰 노드의 멤버노드가 된다. 이때 공격 노드가 더 강한 신호세기로 패킷을 전송할 경우 공격 노드가 클러스터 헤드 노드가 될 수 있다.

제3절 센서 네트워크 보안 기법

1. 공격 대응 기술

센서 네트워크 환경에서는 노드의 에너지 제약을 이용한 슬립거부 공격이 위협적인 공격의 하나로 대두되고 있어 이에 관련된 기술이 연구되고 있으며[48], 센서 노드의 각 레이어별로 서비스거부 공격의 가능성이 있으므로 이에 대한 대응 기술이 연구되고 있다[49].

또한 sybil 공격, 개인 프라이버시 침해와 같은 공격에 대한 대응 기술도 연구되고 있다[50][51][52][53].

2. 공통 보안 기법

다음은 공격에 대한 공통적인 대응 기법들을 나타낸다.

· Fake routing information 공격
  - 공유키를 이용한 노드간 상호인증을 한다. 외부 공격자는 공유 키 값을 알 수 없으므로 공격은 무의미하다.

· HELLO flood 공격
  - 공격 노드의 메시지를 수신한 노드는 특정 패킷을 보내 응답여부를 확인한다.
  - 신뢰할 만한 3rd party를 이용하여 인증을 수행한다.

· Selective forwarding 공격
  - 다중 경로를 이용한다.
  - 동적으로 경로선택을 한다.

· Sybil 공격
  - 모든 노드들이 유일한 키를 보유한다.
  - 이웃 노드의 수에 제한을 둔다.

· Sinkhole 공격
  - 사전 감지는 어렵다. 네트워크 트래픽 분석을 위한 사후처리가 가능하다.
  - 공격 패턴 분석 및 공격 지점 확인 기법의 연구 필요.

3. 인증 기법

대표적인 인증 기법인 SPINS(Security Protocols for Sensor Networks)[54]는 센서 네트워크의 특성에 맞도록 설계한 보안 프로토콜로서 UC Berkely에서 설계하여 제안한 프로토콜이다. SPINS 프로토콜은 다음과 같은 센서 네트워크의 특성을 고려하여 설계하였다.

- 센서 네트워크의 통신 방식인 무선 통신은 많은 전력을 소모 시키는 방식이므로 통신 오버헤드를 최소화 하는 것이 필요하다.
- 제한된 파워를 갖는 센서의 특성상 기존의 보안 알고리즘을 그대로 적용하기는 불가능하다.
- 제한된 메모리를 갖는 센서의 특성상 비대칭형 알고리즘을 적용하기 위한 변수를 저장하기 위한 공간의 마련에 어려움이 있다.
- 전원공급에 제한이 많다.
- 인증된 데이터가 전체 센서 네트워크에 브로드캐스트 되는 센서 네트워크의 특성상 비대칭형 디지털 서명 방식의 적용은 적합하지 않다.

SPIN 프로토콜의 프로토타입은 UC berkeley에서 개발한 Smart dust 노드에 적용하여 개발되었으며, SPIN 프로토콜의 설계 자체도 Smart dust 노드를 염두에 두고 개발한 것이다. Smart dust 노드의 하드웨어 사양은 [표 4] 와 같다.

[표 4] Smart dust 하드웨어 사양

CPU	8-bit, 4MHz
Storage	8KB instruction flash
	512 bytes RAM
	512 bytes EEPROM
Communication	916 MHz radio
Bandwidth	10Kilobits per second
Operating System	TinyOS
OS code space	3500 bytes
Available code space	4500 bytes

SPINS에서 대상으로 하는 센서 네트워크는 노드와 베이스 스테이션(BS)으로 구성된 네트워크로서, 기본적인 통신 방식은 노드에서 BS로, BS에서 노드로, BS에서 모든 노드로의 통신, 이 세 가지로 가정하고 있다.

센서 노드가 생성되는 시점에서 각 노드는 BS와 공유하는 마스터 키를 받는다는 가정과 BS는 기본적으로 신뢰할 수 있다는 가정을 두고 있다.

SPINS는 SNEP 프로토콜과 μTESLA 프로토콜로 구성되는데, SNEP(Secure Network Encryption Protocol)은 통신 데이터의 암호화, 인증 등의 서비스를 제공하기 위한 프로토콜이다.

가. SNEP 프로토콜

SNEP(secure Network Encryption Protocol)프로토콜은 다음과 같은 특성을 가진다.

· Semantic security

counter 값은 메시지가 전송될 때마다 증가되고, encryption 할 때 counter 값이 사용되므로, 동일한 메시지라도 전송되는 시점에 따라 다르게 암호화 되어 semantic security가 보장된다고 볼 수 있다.

· Data authentication

MAC 검증이 정확하다면 수신자는 요청된 송신자로부터의 메시지인지 확인할 수 있다.

· Replay protection

MAC의 counter 값은 old message의 반복을 막을 수 있다.

· Weak freshness

메시지 검증이 정확하다면, 수신자는 지금 수신한 메시지가 자신이 수신한 이전 메시지 이후에 보내진 메시지라는 것을 확인 할 수 있다.

· Low communication overhead

counter 값은 양단에서 관리하고 메시지에 실어 전송하지 않으므로 통신 오버헤드를 줄일 수 있다.

A에서 B로 전송하는 SNEP 프로토콜이 적용된 메시지는 아래와 같이 구성된다.

$$A \rightarrow B: \{D\}_{<K_{encr}, C>},\ MAC(K_{mac}, C \mid \{D\}_{<K_{encr}, C>})$$

D는 데이터(메시지), K_{encr}는 encryption key, C는 counter 이다.

MAC은 $MAC(K_{mac}, C \mid E)$ 인데 여기서 E는 K를 encryption key 로 하고 C를 counter로 하여 D를 encrypt한 메시지를 의미한다.

K_{encr}와 K_{mac}는 A와 B가 공유하는 master secret key를 돌려서 생성한 key가 된다. 아래의 수식은 노드 A가 임의의 N_A를 생성하여 노드 B의 응답으로부터 strong data freshness의 확립을 보여 준다.

$$A \rightarrow B: N_A, R_A$$
$$B \rightarrow A: \{R_B\}_{<K_{encr}, C>},\ MAC(K_{mac}, N_A \mid C \mid \{R_B\}_{<K_{encr}, C>})$$

N_A는 예측 불가능한 임의의 숫자, R_A는 요청 메시지를 의미한다.

MAC 검증이 정확하다면 노드 A는 요청에 대한 응답이 노드 B에서 생성되었다는 것을 알 수 있다. 첫 message에 기밀성이나 데이터 인증이 요구될 때 보통의 SNEP를 사용할 수도 있다.

아래는 counter exchange protocol의 동작을 보여준다.

$$A \rightarrow B: C_A$$
$$B \rightarrow A: C_B,\ MAC(K'_{BA}, C_A \| C_B),$$
$$A \rightarrow B: MAC(K'_{AB}, C_A \| C_B)$$

counter exchange protocol은 어떠한 이유로든 공유되고 있는 counter의 상태가 일치하지 않게 되는 경우가 발생하면 구동 된다.

다음은 request of current counter 동작을 보여준다.

$$A \rightarrow B : N_A$$
$$B \rightarrow A : C_B, MAC(K'_{BA}, N_A \| C_B)$$

나. μTESLA 프로토콜

μTESLA 프로토콜은 TESLA 프로토콜의 micro version 으로 이해할 수 있다. TESLA 프로토콜은 제한된 컴퓨팅 환경을 기초로 개발되지 않았기 때문에 센서 노드에 적용하기에는 무리가 있다. 이 TESLA 프로토콜을 센서 노드에 적용하기 위해 변형한 프로토콜이 μTESLA 프로토콜이다. TESLA 프로토콜과 μTESLA 프로토콜의 주요 차이점을 기술하면 다음과 같다.

TESLA 프로토콜은 디지털 서명을 사용하여 initial packet을 인증하는데 이 방법은 센서 노드에 적용하기에 비용부담이 크고 symmetric mechanism 만을 사용한다. 이 기법은 각각의 패킷을 주고받는 과정에서 키를 노출하므로 대량의 에너지가 필요하며 특정한 시기에 키를 노출한다. 또한, 센서 노드에 one-way key chain을 저장하는 비용부담이 크며, 인증된 전송자의 수에 제약이 있다.

μTESLA 프로토콜은 sender setup, sending authenticated packets, bootstrapping new receivers, authenticating packets 의 과정으로 나누어진다.

4. 그룹 키 관리 기법

그룹 키 관리 기법인 LEAP[55] 는 4개의 암호키와 키 설정 프로토콜로 구성된다. 각각의 키는 다음과 같다.

개인키 : 베이스 스테이션과 모든 노드가 공유하는 개인키
그룹키 : 네트워크의 모든 노드와 공유하는 브로드캐스팅 키
pairwise 키 : 임의의 노드 u,v 간의 공유를 위해 사용하는 키
클러스터 키 : 임의의 노드 u가 이웃 노드와 클러스터 키를 설정에 사용하는 키.

이 방법은 공격 노드는 개인키를 알 수 없으며, pairwise 키와 클러스터 키는 주위의 이웃 노드를 인증하기 위해서만 사용되며 그룹키는 브로드캐스트 되는 메시지의 복호화에만 사용되므로 공격 노드가 존재하는 센서 네트워크의 생존성을 극대화 할 수 있다.

5. 키 분배 및 관리 기법

가. Key infection

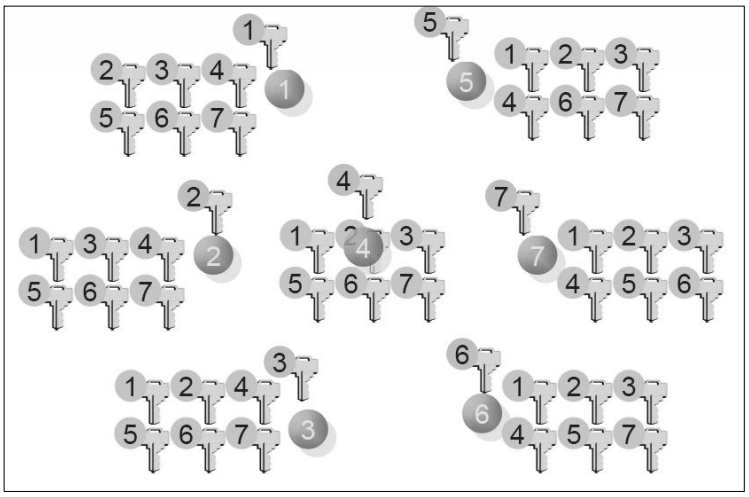
이 방법은 비밀키를 평문상태로 교환한다[56].

즉, 공격자가 최소한 센서 네트워크의 초기 네트워크 구성시 발생하는 노드들 간의 키 교환 과정 동안만은 네트워크의 전 영역을 동시에 도청하는 것이 어렵다고 가정하면 센서 노드의 초기화시 각 노드들이 랜덤하게 생성한 세션키를 이웃 노드들과 평문상태로 교환해도 대부분의 세션키들은 안전할 수 있다. 이러한 가정은 이후 네트워크의 정상 운영 중에는 공격자에 대한 아무런 제한이 없다는 가정을 전제한다.

이 방법은 실제로 중요하거나 민감하지 않은 응용 분야의 경우 안전성과 효율성 사이의 하나의 타협이 된다. 물론 공격자가 일부의 소수 노드들만이라도 전복시켜 자신의 통제하에 두는 경우 라우팅 공격이나 DoS 공격이 가능하므로 이러한 위험부담은 감수해야 한다.

나. Network-wide shared key

이 방법은 [그림 16] 과 같이 네트워크의 모든 노드들이 동일한 키를 갖는다.



[그림 16] 키 관리 기법

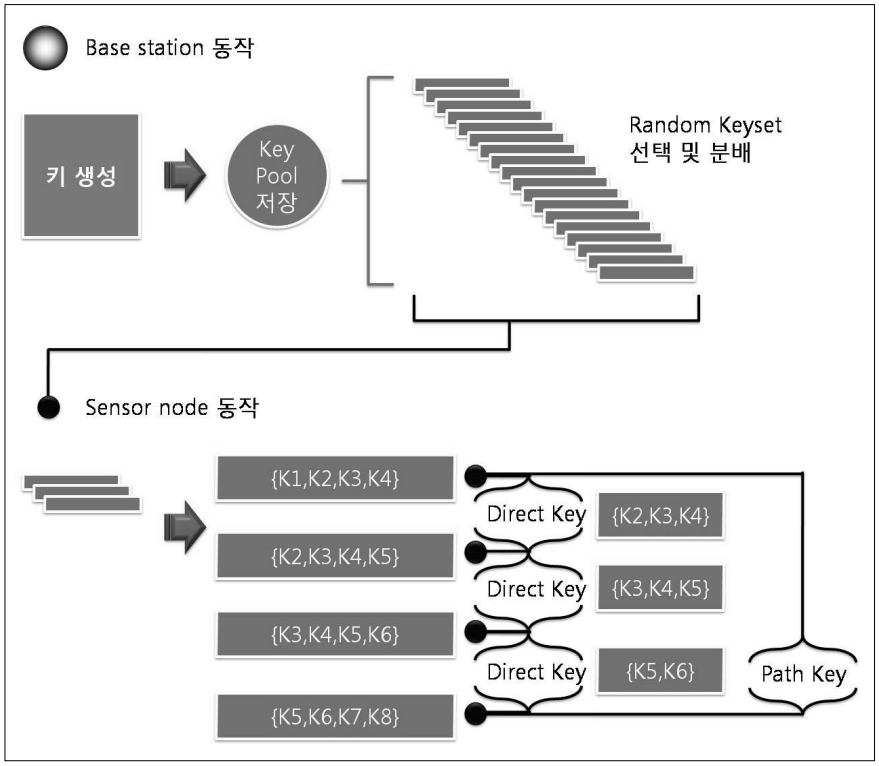
이 방법은 노드가 필드에 배치되기 전에 모든 센서 노드에 동일한 비밀키를 주입하며, 필드에 노드가 배치된 이후에는 이 비밀키를 이용하여 암호화 및 인증을 수행한다.

이는 효율성 면에서는 월등하지만 센서 노드가 물리적으로 안전하지 않는 한 하나의 노드만이라도 공격자에 의해 전복된다면 전체 네트워크의 안전성이 파괴되는 문제점이 있다. 비록 하나의 공유키를 이용하는 것이 문제점은 있으나 키 관리의 효율성으로 인해 많은 기존 네트워크 프로토콜들에서 이 방식을 가정하고 있다. 이와 같이 전체 네트워크에서 공통의 비밀키를 이용하는 경우 공격당한 노드가 탐지되거나 그렇지 않더라도 주기적으로 이 키를 갱신시키는 프로토콜이 필요하다.

한편 미리 주입된 마스터키를 사용하여 링크키를 교환한 후 마스터키를 메모리에서 지움으로써 위 방식의 문제점을 상당부분 제거할 수 있다. 즉 센서 노드가 처음에 배치될 때 인접 노드들과의 인증 및 링크키 교환 과정 동안만 마스터키가 노출되지 않는다고 가정하면 하나의 마스터키만을 이용하여 안전하고 효율적인 키 관리가 가능하며 이와 같은 가정은 LEAP (Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks)에서 사용하고 있다.

다. Key pool을 이용한 랜덤 키

센서 노드들 사이에 pair-wise key 설정 프로토콜[57]로서 초기 노드가 필드에 배치되기 전의 임의의 키 셋을 분배하여, 노드들이 필드에 배치된 이후 노드들 사이에 pair-wise key를 생성하는 형태이다. [그림 17] 은 베이스 스테이션과 센서 노드들의 키 셋을 이용한 직접 키 및 간접 키 설정 형태를 보이고 있다.



[그림 17] 랜덤 키 분배 기법

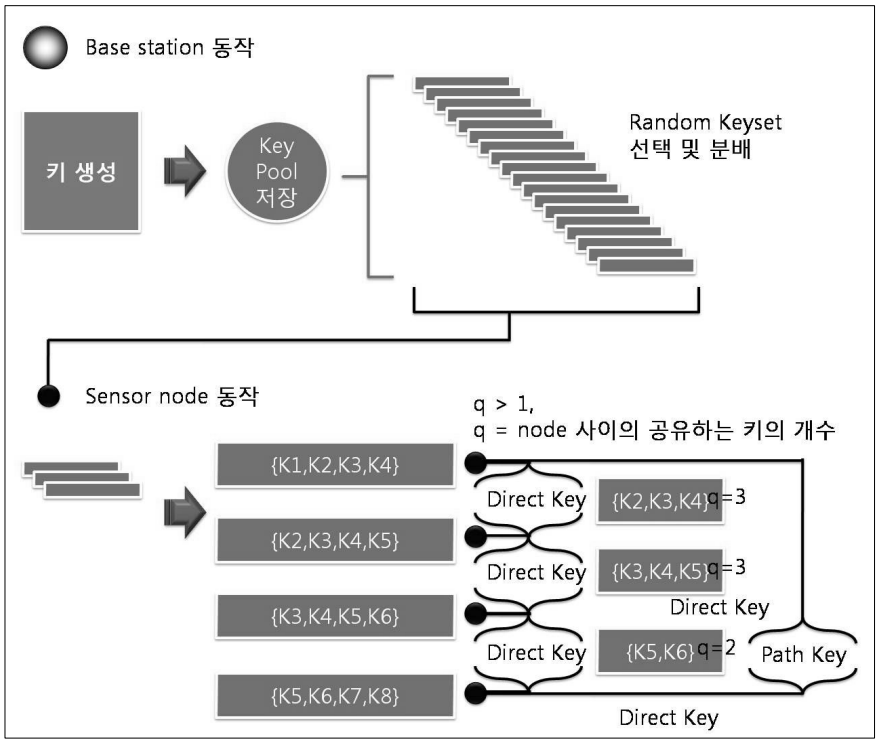
베이스 스테이션 동작 - 초기 노드를 필드에 배치하기 전 베이스 스테이션은 랜덤 키를 생성하여 키 풀에 저장한다. 키 풀에 저장된 키들 중 랜덤하게 키 셋을 선정하고 이 키 셋을 각각의 노드들에 저장한다.

노드 동작 - 필드에 배치된 각각의 노드들은 자신이 가지고 있는 키 셋을 이용하여 인접한 노드들과 일치하는 키를 찾아 pair-wise key로 사용한다. 일치

하는 키가 없을 경우 인접한 다른 노드들과의 일치하는 킷값의 중계를 통해 경로키를 설정하여 pair-wise key로 사용한다.

이는 키 풀에서 랜덤하게 키를 설정하는 형태에 보안성을 증대시키기 위한 방법으로 두 노드사이에 공유하는 키의 개수를 q로 하여 공유하는 키의 숫자를 조정함으로서 보안 레벨을 조정하는 방법[58]이다.

다음의 [그림 18] 은 베이스 스테이션의 랜덤 키 셋 생성에 관련된 동작과 센서 노드들의 키 셋을 이용한 직접 키 및 간접 키 설정 형태를 보이고 있다.



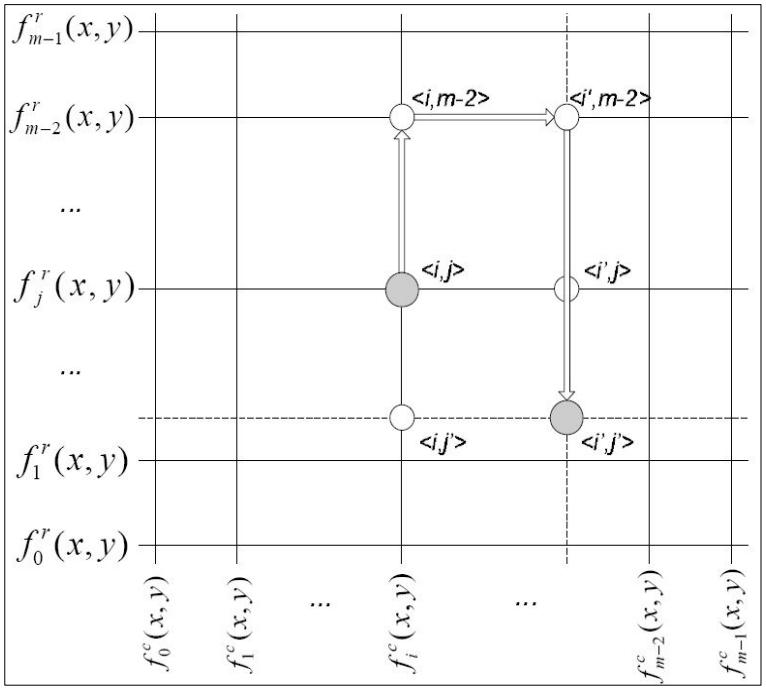
[그림 18] Q 합성수 키 분배 기법

이 방법은 확률을 이용하는 키 분배 방법에서 q가 증가할 경우 노출되어야 하는 키의 개수가 증가하므로 공격에 대한 보안 효과는 높아지나 공유하는 키의 개수도 증가하여야 하므로 노드들 사이의 키 공유 연결도가 낮아지게 되어 전체 네트워크의 구성이 어려워지므로 보안과 연결도 사이의 적절한 값을 정하여 보안과 네트워크 연결도

사이의 최적값을 찾아야 한다.

라. Grid 기반 키

[그림 19] 의 방법은 논리적 그리드 형태를 정하고 각 그리드의 행과 열에 키를 할당[59]하는 pair-wise key 설정 프로토콜이며 키 대신 키를 유도하는 다항식을 분배한다.

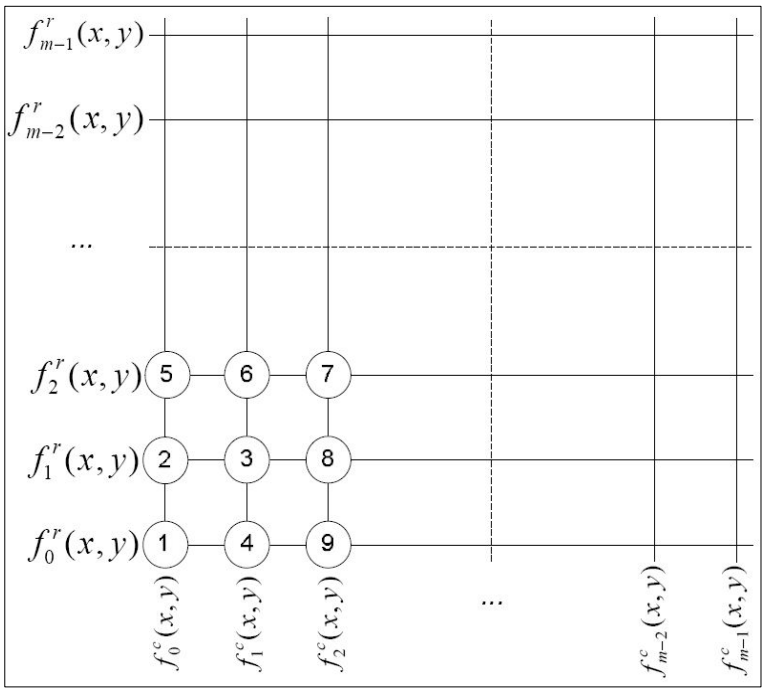


[그림 19] 그리드 키 할당

이 방법은 센서 노드들을 $m \times m$ 크기를 가지는 그리드의 행과 열이 교차하는 지점에 위치시키고 $2m$개의 다항식 $\{f_i^c(x, y), f_i^r(x, y)\}_{i=0, \ldots, m-1}$을 생성하여 i열 j행에 있는 노드에게 두 개의 다항식 $f_i^c(x, y)$와 $f_j^r(x, y)$를 배분한다. 이렇게 할당된 키는 각 교차점에 두 개씩 할당되며 이 교차점에 노드들을 위치하게 하여 노드가 두 개의 키 쌍을 갖는다.

[그림 20] 에서 나타내는 그리드에 노드의 ID가 할당된 예와 같이 생성된 논리적 그리드의 각 교차점에 ID를 할당하는데 이 할당하는 ID는 각 교차점에 할당된 두 개

의 키 쌍을 갖는 노드의 ID로 사용되어 노드들을 구분하는 역할을 한다.

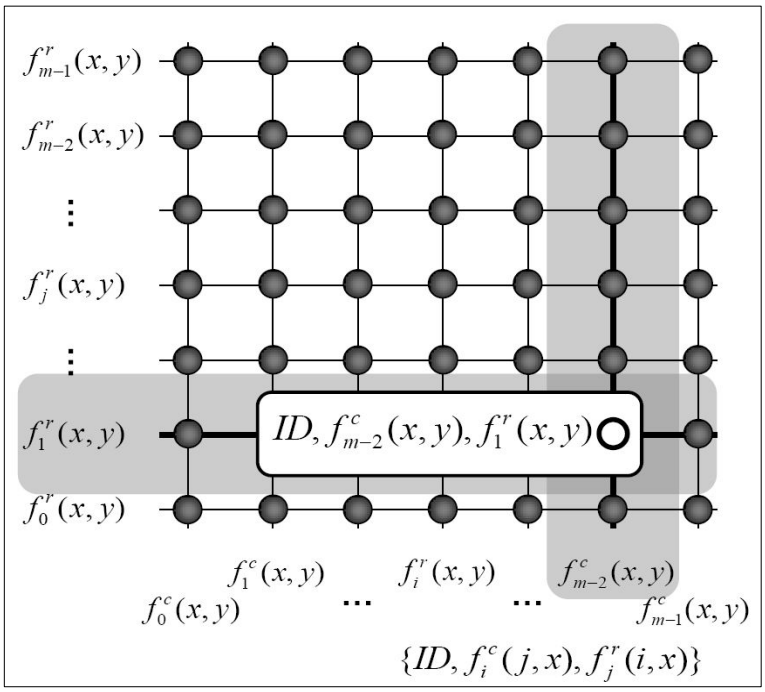


[그림 20] 노드의 ID 할당

[그림 19] 와 [그림 20] 에서 생성된 키 쌍과 노드의 ID를 정리하면 [그림 21] 과 같은 형태로 한 노드에 할당된다.

$ID=<i,j>$인 다항식 공유키 $\{ID, f^c_i(j,x), f^r_j(i,x)\}$를 할당받은 노드는 자신이 위치한 행 또는 열에 있는 노드들과는 동일한 다항식 공유키를 갖고 있으므로 pair-wise key를 바로 생성할 수 있으며, 동일한 행이나 열에 위치하지 않는 경우 동일한 행이나 열에 위치한 노드들의 중계를 통하여 경로키를 생성하고, 이때 노드의 위치 정보를 이용하므로 쉽게 찾을 수 있다.

그러나 행과 열에 위치한 노드 중 한 개의 노드의 다항식 공유키가 공격자에 노출되었을 경우, 노출된 키를 사용하여 pair-wise를 이룬 전체 네트워크의 행과 열의 모든 노드는 공격자에 노출된다.



[그림 21] 노드에 할당되는 키

마. Location 기반 키

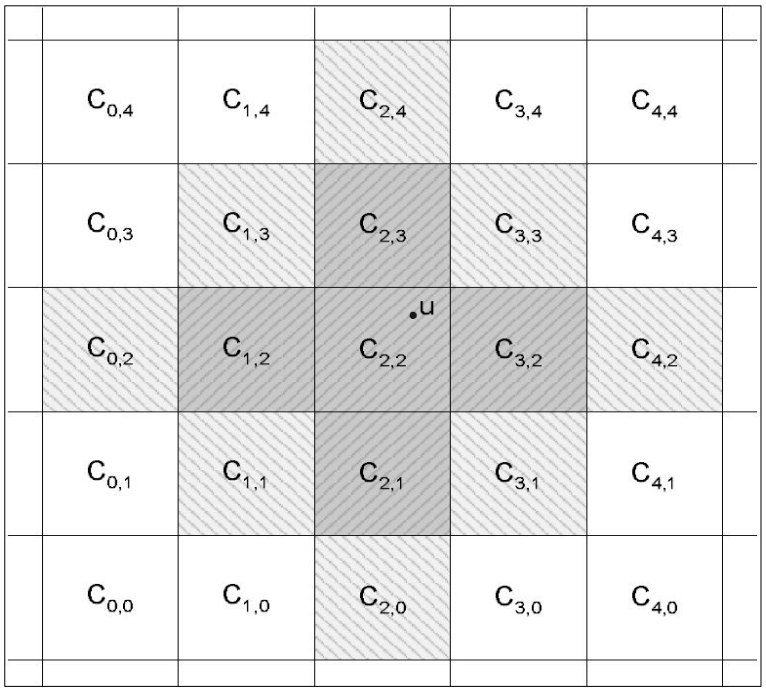
다음의 [그림 22] 는 네트워크 필드를 일정한 정사각형의 셀로 구분하여 pair-wise key를 설정하는 프로토콜이다. 이 방법도 다항식[60]을 사용하여 pair-wise key를 생성한다.

앞의 그리드 기반 방법에서와 달리 노드가 배치될 필드를 셀로 나누어 각각의 셀에 다항식을 할당하며, 특정한 셀에 배치되는 노드는 인접한 4개 셀의 다항식을 포함한 총 5개의 다항식을 할당받는다. 센서 노드가 필드에 설치되기 전에 센서 노드들이 위치할 필드를 정사각형의 셀로 구분되는 영역 $\{C_{i_c,\ i_r}\}_{\ i_c=0,\ 1,\ \ldots,\ C-1,\ i_r=0,\ 1,\ \ldots,\ R-1}$로 나누고 다항식 $\{f_{i_c,\ i_r}(x,y)\}_{\ i_c=0,\ 1,\ \ldots,\ C-1,\ i_r=0,\ 1,\ \ldots,\ R-1}$을 각 셀에 할당하여 해당 셀에 위치한 노드는 그 셀에 할당된 다항식 $\{f_{i_c,\ i_r}(x,y)\}$과 인접한 4개 셀의 다항식을 할당받는다.

예를 들어 아래의 [그림 22] 에서 센서 노드 u가 셀 $C_{2,\,2}$에 배치되면 $C_{2,\,2}$는 이 센

서 노드의 홈 셀이 되며, 이 셀에 인접한 4개의 셀 $C_{1,2}$, $C_{2,3}$, $C_{3,2}$, $C_{2,1}$는 홈 셀의 인접 셀이 된다. 따라서 노드 u는 $C_{2,2}$, $C_{1,2}$, $C_{2,3}$, $C_{3,2}$, $C_{2,1}$의 다항식 공유키인 $f_{2,2}(u,y)$, $f_{1,2}(u,y)$, $f_{2,3}(u,y)$, $f_{3,2}(u,y)$, $f_{2,1}(u,y)$를 할당받는다.

이 방법의 취약점은 한 셀의 한 노드가 공격을 받아 키가 노출되었을 때, 자신이 위치한 셀의 모든 노드도 공격자에 노출이 되며 인접한 4개 셀에 위치한 모든 노드들도 노출된다.



[그림 22] 위치기반 키 분배 기법

하드웨어적인 한계에도 불구하고 공개키 암호 연산을 센서 네트워크에 접목시키려는 연구도 진행 중에 있다. 센서 네트워크 환경에서 공개키 암호 연산은 불가능하게 생각되어왔으나 최근 몇몇 연구들은 센서 노드에서도 공개키 암호의 구현이 가능할 수 있음을 보이고 있다[61].

그러나 실용화에는 하드웨어 자원적인 한계로 인해 무리가 있고 공개키 기반구조 확립의 문제도 있으므로 논외로 한다.

Ngo Trong Canh[62]등이 제안한 기법은 위치 기반 기 분배기법의 인접 셀을 8개

로 정하고 인접하는 두 셀 (i,j)와 (u,v)는 동일한 키 $f_{(u,v)(i,j)} = f_{(i,j)(u,v)}$를 사용하여 보안성은 향상 시키면서 사용되는 키의 개수는 상대적으로 적게 사용하도록 하였다.

그러나 이 기법 역시 위치 기반 기법과 동일한 보안 취약점이 존재하며 동일한 크기의 셀일 경우 더욱 큰 피해를 초래할 수 있다.

제3장 센서 네트워크 라우팅의 에너지 효율성 및 보안 신뢰성 향상

제1절 고려 요소

본 장에서는 센서 네트워크 환경의 효율적이고 안정적이며 안전한 클러스터 기반 네트워크 구성을 위해 고려해야하는 몇 가지 요소에 대해 언급하며, 제안하는 기법에서 네트워크를 구성할 때 고려하는 수집된 데이터 값, 고도, 센서 감지범위와 클러스터 헤드 노드 부하의 분산과 노드의 연결도 향상을 위해 도입한 요소들에 대해 기술한다.

이후 이상의 에너지 효율적이며 안정적인 네트워크 유지가 가능한 라우팅 기법 상에서 동작 가능한 키 관리 기법 및 인증 기법에 대해 기술한다.

센서 네트워크는 그 동작에 있어 아래의 3가지를 만족해야 한다.

효율 - 최소의 노드 활용, 노드 전송의 최소화, 데이터 중복 회피, 부하 분산
안정 - 브로드캐스트 문제 고려, 에너지 홀 문제 고려
안전 - 동적인 네트워크 변화에 맞는 키 분배 및 인증 기법

· 효율

센서 노드는 데이터를 수집하고자 하는 지역에 밀집되게 분포한다. 이러한 이유로 각 노드들이 수집하는 데이터는 중복되기 쉬워 중복된 데이터 전송에 낭비되는 에너지가 많다. 또한 센서 노드에서 메시지 송수신에 소모되는 에너지는 데이터 처리에 소모되는 에너지에 비해 상대적으로 크다.

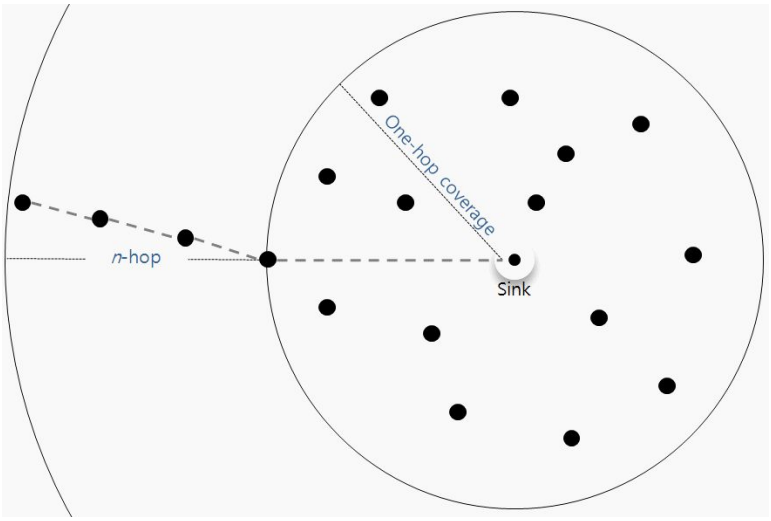
이와 같은 네트워크에서 발생할 수 있는 브로드캐스트 문제와 에너지 홀 문제를 고려하여 최소의 노드만 동작하는 방법이 데이터 수집에 있어 효율적이고 안정적인 결과를 갖는다. 따라서 평면 라우팅 방식[63]보다는 클러스터링[64]을 이용한 계층적 구조가 더 적합하다.

또한, 노드가 데이터를 전송할 때 소비하는 에너지가 노드 전체 보유 에너지에서 차지하는 비율[65][66][67][68]을 고려하면 멤버 노드로부터 데이터를 전송받아 데이터 취합을 하여 상위 계층으로 전송하는 클러스터링 방식이 보다 효율적인

에너지 관리가 가능하다.

· 안정

멀티 홉 전송에서 발생하는 문제들 중 에너지 홀 문제는 네트워크 수명을 결정하는 중요한 요소이다. 센서 네트워크는 다중 홉 전송을 기반으로 동작하는 네트워크이다. 이러한 다중 홉 전송에서 싱크와 직접 전송이 가능한 1-hop 거리에 위치한 노드들은 싱크 노드와 직접 전송이 불가능한 위치에 있는 노드들의 릴레이 노드로서 동작하므로 에너지 소모가 큰 편이다. 이는 싱크 주변에 에너지 홀을 생성하게 되어, 네트워크의 단절로 인한 수명 단축을 야기한다 ([그림 23] 참조).



[그림 23] 에너지 홀 문제

본 연구는 센서 모듈의 감지범위[69]와 수집 데이터의 중복성을 고려하였으며, 네트워크 성능 평가에 실제 기상 데이터[70]를 이용하였다.

이 방법은 특정 지역에 배치된 노드들이 동일한 데이터를 중복 수집하는 문제를 최소화하고, 수집하는 데이터의 정확도를 높이며, 네트워크를 구성하는 노드들 사이의 링크단절을 완화시킨다. 제안하는 방법은 ARCT에서 사용했던 지역 클러스터의 개념을 토대로 한 클러스터와 중계기를 이용한 클러스터링 방법이다.

ARCT의 지역 클러스터링에서, 모든 노드는 초기 수집된 데이터 값의 일치 여부로 지역클러스터를 형성하였다.

그러나 제안하는 방법은 여기에 동일한 고도 값을 고려하였으며, 지역 클러스터를 형성하는 범위를 한 노드의 전송 범위가 아닌 노드의 센서 디바이스의 감지 범위로 한정하여 데이터 수집의 오차를 줄였다. 또한 수집된 데이터의 멀티 홉 전송에 발생하는 링크 단절 현상을 억제하기 위해 중계 노드를 이용하였다. 이는 데이터의 중복 수집을 피하고 네트워크의 수명을 연장시키며 링크 단절 현상을 완화시킨다.

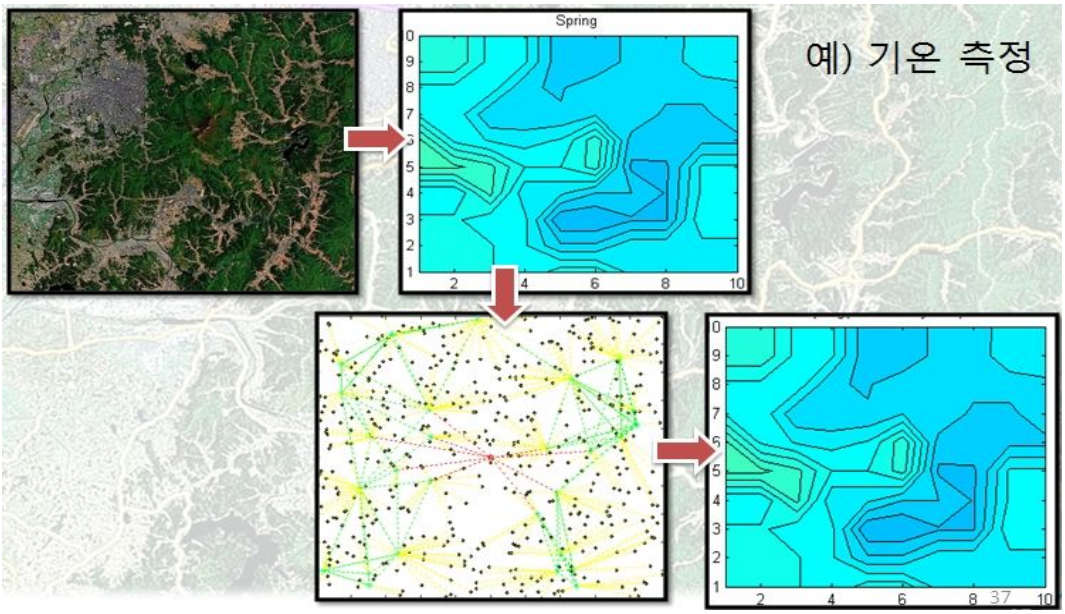
제2절 에너지 효율성 향상

1. 기본 가정

센서 네트워크는 그 응용에 따라 다양한 환경이 존재하며, 제안하는 방법은 기상감시 센서 네트워크와 같은 응용에 적합한 클러스터 기반 멀티 홉 라우팅 프로토콜이다([그림 24] 참조). 이 방법은 아래와 같은 기본가정을 갖는다.

기본가정

- 모든 노드는 멀티 홉 기반 전송을 한다.
- 노드들의 위치는 고정되어 있다.
- 모든 노드들은 시간적으로 동기화되어 있다.
- 모든 노드들의 초기 에너지는 동일하다.
- 모든 노드들의 에너지는 제한되어 있다.
- BS는 에너지 제약이 없으며, 통신 커버리지는 전체 네트워크 필드를 포함한다.
- 센서 노드는 전송 세기의 조절이 가능하다.
- 모든 노드는 자신의 고도를 측정 가능한 센서가 있다.
- 노드의 센서 감지범위는 노드의 전송범위보다 작다.
- 노드 A의 신호를 노드 B가 성공적으로 수신했다면
  노드 B의 신호 또한 노드 A에 의해 성공적으로 수신된다.



[그림 24] 기상 관측용 센서 네트워크의 예

가. 노드 선별을 위한 파라메터

ARCT의 지역 클러스터(region cluster)에서 클러스터에 참여하는 모든 노드는 동일한 수집 데이터 값을 갖고 있다. 다시 말해서, 이 클러스터에 참여하는 조건은 초기에 수집된 데이터의 일치 여부이다. 그러나, 제안하는 방법은 ARCT의 기본 지역 클러스터 형성 조건인 동일한 초기 수집데이터 값 이외에 두 가지를 도입하였다. 이 두 가지는 다음과 같다 ([그림 25] 참조).

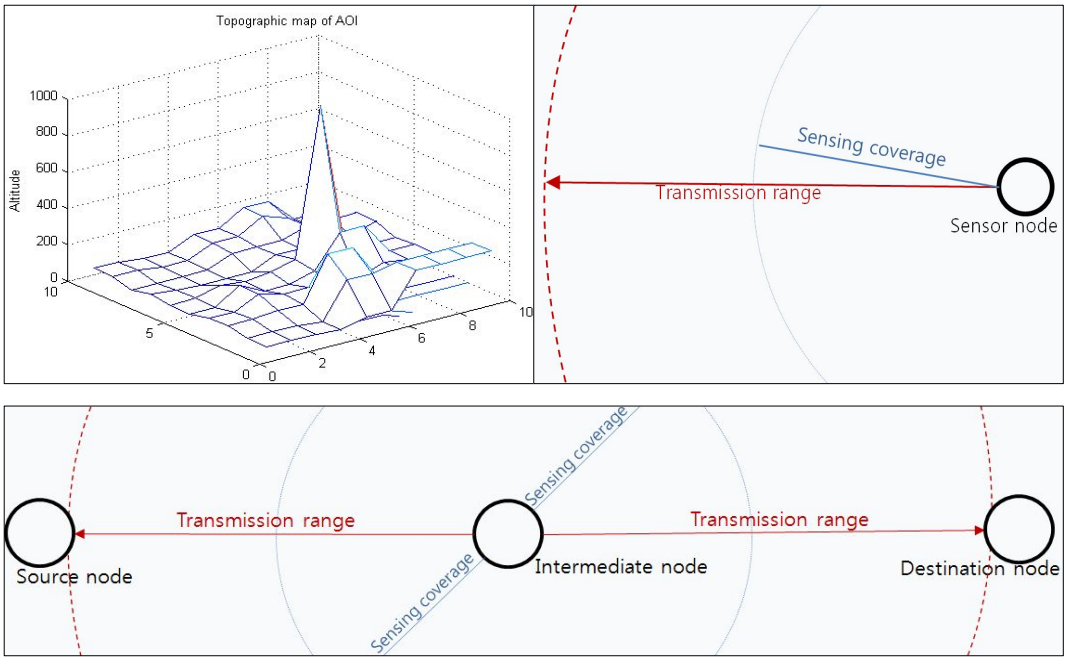
· 고도

- 초기 인접 클러스터의 형성 조건에 동일한 고도 또한 포함된다. 비록 초기 기온이 같을 지라도 고도의 차이는 수집되는 기후데이터에 영향을 미치는 요인이므로 정확한 데이터 수집에 문제가 된다.

· 센서의 감지범위

- 지역 클러스터는 동일 데이터의 중복을 피하기 위한 방법이다. 따라서 센서의 감지 범위 이내에 다수의 센서 노드가 데이터 수집을 하는 것은 바람직하지 않다.

정해진 필드에 random distributed된 노드들은 위의 조건을 바탕으로 하여 선별된다.



[그림 25] 고도와 센서의 감지범위

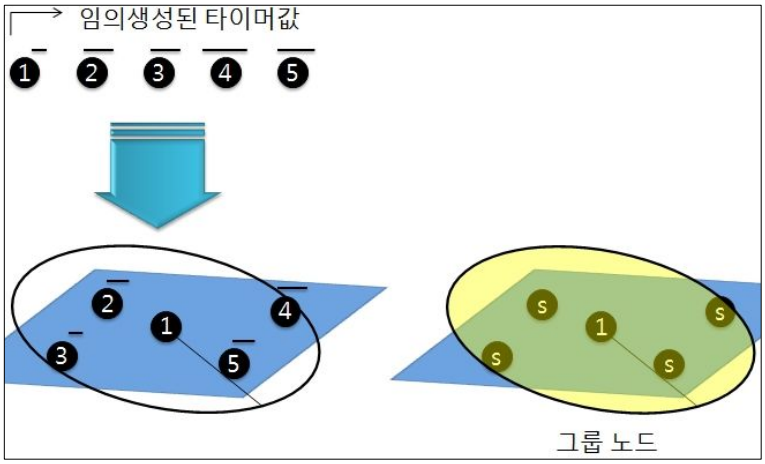
2. 네트워크 셋업

가. 지역 선별 노드 (그룹) 선정

그룹 노드 선정 과정은 아래와 같다 ([그림 26] 참조).

(1) 모든 노드는 필드에 배치되기 전 임의로 설정된 노드의 동작 지연시간을 설정하여 저장한다.
(2) 초기 모든 노드가 필드에 무작위로 뿌려진 이후, 사전에 임의로 할당된 노드 동작을 위한 타이머를 갖는 노드는 자신의 동작시간에 깨어 동작한다.
(3) 동작을 시작한 노드는 즉시 자신이 위치한 곳의 고도 데이터와 기후 데이터를 수

집하여 기후 데이터 수집 센서의 유효 감지 범위에 맞는 전파세기로 패킷을 전송한다.



[그림 26] 노드의 동작 타이머 결정 및 노드 경쟁에 의한 그룹 형성

(4) 이 패킷을 수신한 센서의 유효감지 범위에 위치한 인접한 노드들 중 위의 두 가지 조건, 즉 고도와 기후데이터 값이 일치하는 모든 노드는 동작을 중지하고 슬립모드로 들어간다.
(5) 위의 두 가지 조건들 중 하나라도 일치하지 않을 경우 슬립하지 않고 자신에게 할당된 시간에 동작하여 (3)의 동작을 한다.

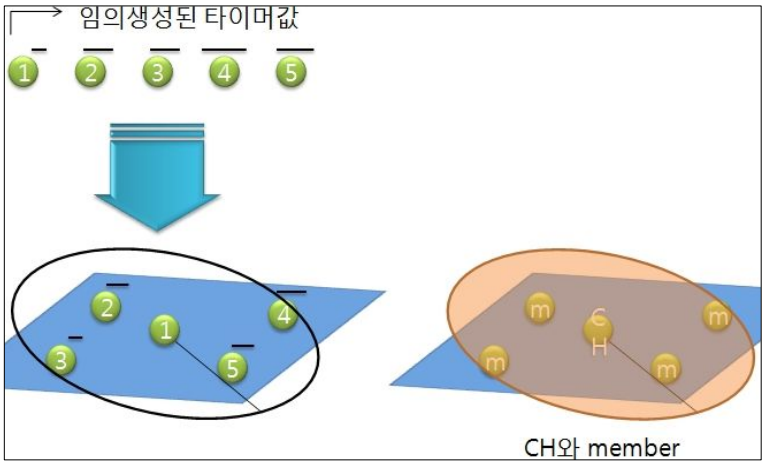
이렇게 하여 선정된 노드군은 지역 선별 노드가 되며, 다음 과정으로 진행하여 지역 클러스터와 데이터 중계기로서 선정되어 동작한다. 지역 선별 노드 선정을 위한 할당된 시간이 종료된 후, 선별된 지역 노드는 (1)의 시간을 임의로 재설정하고 클러스터 헤드 노드 선정에 참여한다.

나. 클러스터 헤드 노드 선정

클러스터 헤드 노드 선정과정은 다음과 같다.

(1) 사전에 정해진 클러스터 헤드 노드 선정 구간 내에서 설정된 시간이 빠른 노드부터 시작하여 자신이 클러스터 헤드 노드임을 알리고 클러스터 헤드 노드의 전송

반경 내에 있는 모든 노드를 멤버 노드로 하는 지역 클러스터를 형성한다. 여기에서도 역시 노드 선별과정의 (4)와 같이 아직 자신의 동작 시간에 도달하지 못한 모든 노드는 클러스터 헤드노드가 되려는 시도를 포기하고 현재 클러스터 헤드노드의 멤버 노드가 된다 ([그림 27] 참조). 이때, 클러스터 헤드 노드의 멤버 노드가 되는 모든 노드들은 자신의 주변에 위치한 클러스터 헤드 노드의 패킷을 카운트하여 인접한 클러스터 헤드노드의 수를 저장한다.

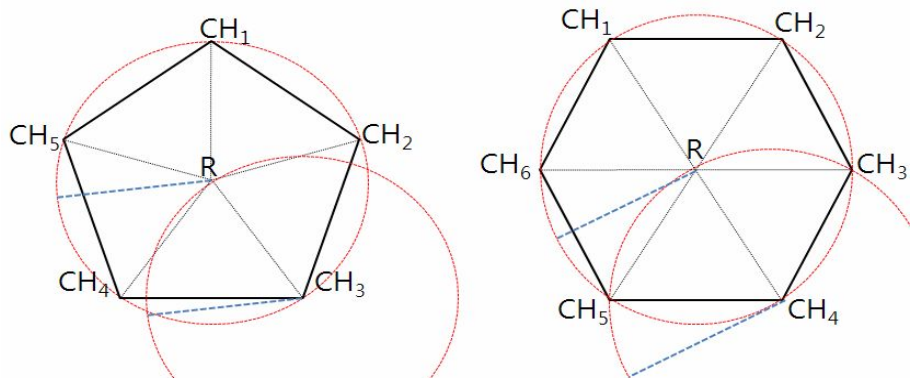


[그림 27] 노드 경쟁에 의한 클러스터 형성

(2) 지역 클러스터링이 완료된 후, 모든 클러스터 멤버 노드들 중 인접한 클러스터 헤드 노드의 수가 2개 이상 5개 이하인 멤버 노드는 클러스터 헤드 노드의 멀티 홉 전송에 데이터 전송 중계 노드의 후보가 된다.

다. 전송 중계 노드 선정

인접 클러스터 헤드 노드의 수가 2개 이상 5개 이하인 이유는 다음과 같다.
중계노드는 두 인접하지 않는 노드들 사이의 성공적인 데이터 중계를 그 목적으로 한다. 따라서 최소 2개의 노드가 필요하다. 또한 최대 5개의 노드를 허용하는 이유는 아래의 [그림 28] 과 같다.



(a) CH가 5개일 때 (b) CH가 6개 일때

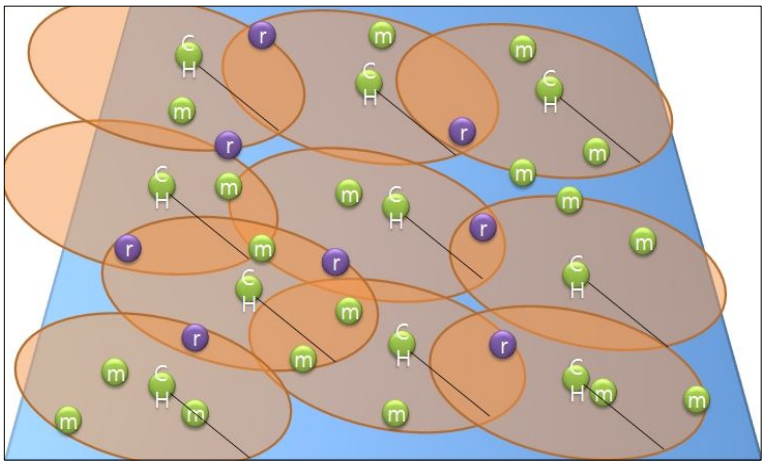
[그림 28] 클러스터 헤드 노드가 5개와 6개일 때
노드들의 이상적인 배치 형태와 통신 거리

위의 그림에서 R은 리피터, 즉 중계 노드를 의미하며, CH는 클러스터 헤드 노드를 의미한다. 위의 그림과 같이 클러스터 헤드 노드가 이상적으로 배치됨을 가정했을 때, 클러스터 헤드 노드들 간의 원활한 통신을 위해서는 클러스터 헤드 노드가 5개일 때까지 중계 노드가 패킷 중계를 해야 한다.

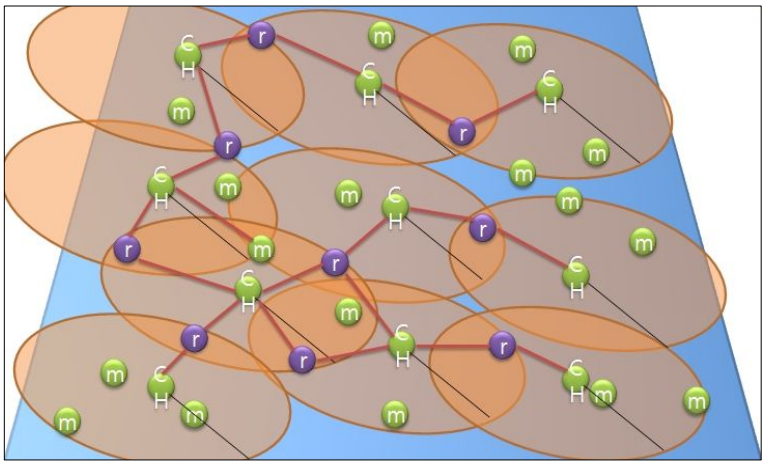
그러나 클러스터 헤드 노드가 6개 이상일 경우, 클러스터 헤드 노드들 사이에 연결이 가능하므로 6개 이상인 경우는 중계 노드가 필요하지 않다.

위의 그림은 어디까지나 이상적인 경우를 가정했을 때이며, 실제 그 이하 개수의 클러스터 헤드 노드로도 멀티 홉 통신이 가능하다. 따라서 중계 노드로 선정될 노드에 사용자에 의해 정의된 중계노드 선정 비율을 적용하여 일부의 노드만 중계 노드로서 동작하도록 하였다.

데이터 전송 중계 노드의 후보 노드가 된 모든 노드들 중 사용자에 의해 사전에 설정된 비율을 토대로 임의 선정된 노드들은 데이터 전송 중계 노드가 되며, 이 노드들은 클러스터 헤드 노드와 같은 레벨에서 동작하여 클러스터 헤드 노드 사이의 멀티 홉 전송을 중계하는 역할을 한다 ([그림 29] 참조).



(a)확률에 의한 리피터 선정



(b) 리피터를 이용한 네트워크 연결

[그림 29] 리피터의 선정과 네트워크 연결

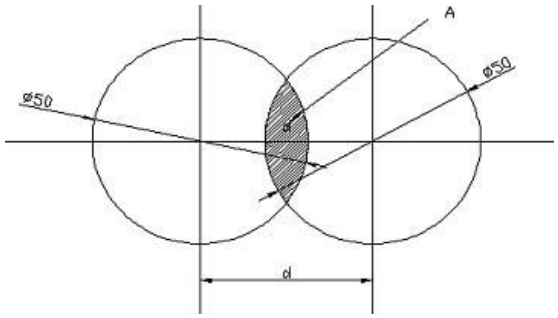
라. 중계노드 선정 비율 결정

두 클러스터 사이의 중첩된 영역 (음영지역)에서 중계노드를 선정하기 위해, 사전에 중계노드 선정 비율을 결정해야 한다. 센서 노드가 주어진 지역에 균일하게 분포함을 가정했을 때, 네트워크에서 평균적으로 생성되는 클러스터 또한 균일하게 배치됨을 가정하고 아래 [그림 30] 에서 보이는 두 클러스터 사이의 중첩된 면적을 구한 후 해당 면적에 배치되는 노드들의 수를 구하여 중계노드 선정 비율을 결정한다.

d를 두 클러스터 헤드 노드사이의 거리, 클러스터 크기를 50pi로 했을 때 중첩 영역의 면적을 구하는 식은 다음과 같다.

$$1250acos(\frac{d}{50}) - \sqrt{25^2 - (\frac{d}{2})^2} \times d \quad (3)$$

이 식에 의해 면적을 구하고 네트워크 크기에 비례한 노드의 밀도를 적용하면 전송 중계노드 선정 확률을 결정 할 수 있다.



[그림 30] 두 클러스터의 중첩 영역

마. 노드의 부하 균형을 위한 가중치 부여 및 갱신

클러스터 네트워크의 단점인 에너지 부하 분산을 위해 제안하는 방법에서는 아래와 같은 최대 지연시간 가중치 부여 및 최소·최대 지연시간 가중치 부여 방법을 택하였다. 기존에 제안되었던 방법들은 노드의 부하 분산을 위해 노드 자신의 잔여에너지와 인접 노드의 잔여에너지를 참고로 하는 방식을 사용한다. 그러나 이러한 방법은 노드 자신의 인접 환경에 대한 잔여에너지를 고려할 수 있을 뿐이며, 전체 네트워크의 에너지 소모량은 알 수 없다. 이러한 문제를 해결하려는 노력의 일환으로 전체 네트워크를 총괄하는 BS를 이용하여 노드의 잔여에너지를 고려하며 노드의 역할을 할당하는 방법들이 제안되었다. 그러나 이 방법은 BS가 네트워크에 자주 개입하게 되어 오히려 네트워크의 가용 에너지 자원이 낭비되는 문제가 발생한다. 이에 제안하는 방법에서는 노드의 부하균형을 효율적으로 조정하기 위해 다음과 같은 제안을 하였다. 우선 노드의 네트워크 참여를 조정하는 지연시간을 두었다. 이 지연시간을 통해 노드가 네트워

크에 동시에 참여하지 않고 자신의 지연시간이 만료된 후 참여하는 경쟁적 참여를 통해 네트워크를 구성하게 된다. 그리고 이러한 지연시간을 결정하는 노드가 부하를 받는 정도는 모든 네트워크에 동일한 기준으로 적용되어야 한다. 이러한 기준은 네트워크에서 노드의 역할과 노드가 소모한 에너지 량 등에 의해 결정 될 수 있다.

이러한 기준은 네트워크의 특성에 맞게 고려되어야하고 선택되어야 한다. 네트워크의 수명이 크게 고려되지 않고 모든 노드가 네트워크에서 동작하며 최대의 해상력을 갖는 조건이 필요한 네트워크에서는 노드의 지연시간 설정에 노드가 소모한 에너지 량을 이용할 수 있다. 노드의 전체 에너지 량을 지연시간의 최대값과 맵핑을 하고 소모 에너지 량에 따라 지연시간을 조정하면 노드의 부하 균형을 이룰 수 있으며 이런 종류의 네트워크는 거의 모든 노드의 수명이 균일하게 조절되어 네트워크 수명 그래프가 수직에 가깝게 나타나게 된다.

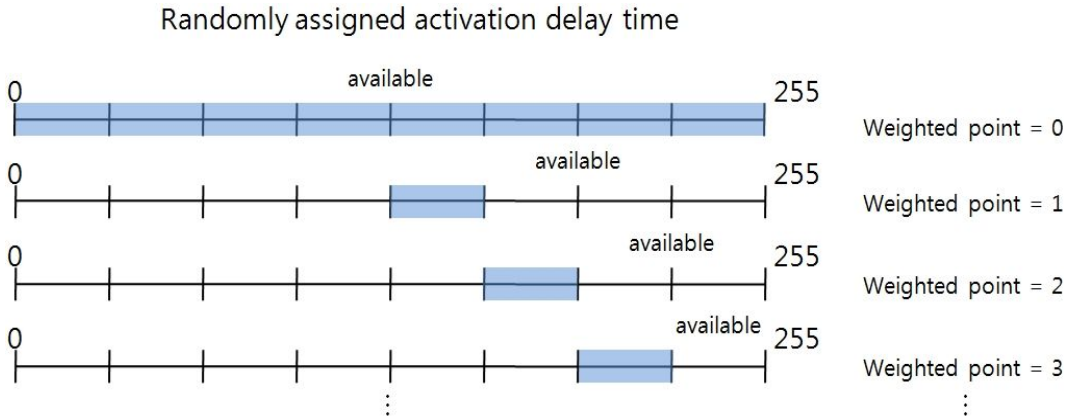
제안하는 방법은 모든 노드가 동작할 필요가 없는 네트워크이며 수집하는 데이터의 특성상 높은 해상력을 요구하지 않는다. 그러나 네트워크 환경을 고려하면 최대한의 수명을 가져야 한다. 이러한 조건에서 부하 균형이 갖는 의미는 모든 노드가 동일한 수명을 가져야 한다는 조건과는 약간 다른 조건을 요구한다. 이러한 환경에서 말하는 부하균형의 의미는 다음과 같다. 즉, 요구조건을 만족하기 위해 최소의 노드가 동작하여 에너지 소비를 최소화 하며, 이 최소의 노드가 부하균형을 이루는 형태이다. 따라서 네트워크 전체의 부하균형이 아니므로 네트워크의 수명 그래프는 수직 형태가 아닌 계단식 하향 곡선을 그리게 된다. 따라서 제안하는 방법은 이러한 결과를 얻기 위해 BS의 개입이 없는 상태에서 전체 네트워크의 에너지 잔량을 가늠할 수 있는 방법인 노드의 역할에 의한 설정을 적용하였다. 이 방법은 노드의 지연시간을 결정할 때 노드의 역할에 따라 가중치를 차등 적용하여 구분하는 방법이다. 이는 BS의 개입이 없어도 노드의 역할별로 가중치가 달라지므로 개별 노드 또는 BS의 관점에서 전체 네트워크 노드의 잔여 에너지 정보를 알지 못하더라도 네트워크 부하균형을 위한 지연시간 설정에 적절한 구분 기준이 될 수 있으므로 응용환경에 맞는 부하균형 설정 방법이 될 수 있다.

제안하는 방법은 노드의 역할이 4가지로 구분된다. 노드가 동작하지 않는 상태 즉 슬립 상태가 있다. 또한 노드가 동작하는 상태인 네트워크에 일반노드로 참여하는 형태가 있으며, 리피터 노드로 동작하는 상태, 그리고 클러스터 헤드 노드로 동작하는 상태가 있다. 노드가 동작하는 상태에서는 최대 지연시간 가중치 부여방법을 적용하며 노드가 동작하지 않는 상태에서는 최소 지연시간 가중치 부여방법을 적용한다.

(1) 최대 지연시간 가중치 부여

Heterogeneous sensor network에서 노드의 역할에 따른 에너지 소모량을 비교하면 지역 선별 노드< 전송 중계 노드 < 클러스터 헤드 노드의 순으로 나타낼 수 있다. 우리는 이 비율을 단순화하여 가중치에 적용하였다.

노드 선정과정에서, 지역 선별 노드로 선정된 노드들은 가중치 1을 받는다.
클러스터 헤드 노드 선정과정에서 선정된 클러스터 헤드 노드는 가중치 2를 받는다.
클러스터 헤드 노드 선정과정에서 선정된 전송 중계 노드는 가중치 1을 받는다.



[그림 31] 최대 지연시간 가중치 값에 의해 결정되는
할당 가능한 동작 지연시간의 범위

사용자에 의해 사전에 설정된 전체 동작 지연시간을 R_t 라고 하고, 이 지연시간의 최소값을 m_{R_t}, 최대값을 M_{R_t}, 노드들이 할당 가능한 동작 지연시간 구간을 r_t, 노드의 최대 지연시간 가중치 값을 W_{Mdp}, 지연시간을 구간별로 나눈 슬롯의 개수를 n_s라고 하면, 실제로 노드가 사용 가능한 지연시간 구간 r_t의 최소값 m_{r_t}를 결정하는 식은 다음과 같으며 이 구간 r_t내에서 랜덤 지연시간 값을 선정한다.

$$\text{최소값 : } m_{r_t} = \frac{1}{2} M_{R_t} + \frac{r_t (W_{Mdp} - 1)}{n_s} \quad (4\text{-}1)$$

$$\text{최대값 : } M_{r_t} = \frac{1}{2} M_{R_t} + \frac{r_t W_{Mdp}}{n_s} \quad (4\text{-}2)$$

위의 [그림 31] 과 식에 의하면 가중치는 다음과 같은 의미를 갖고 있음을 알 수 있다.

가중치 1 - 다음 라운드에서 선택 가능한 지연시간 범위 중 하위 절반의 구간
가중치 2 - 다음 라운드에서 선택 가능한 지연시간 범위 중 하위 구간 첫 번째 슬롯
가중치 3 - 다음 라운드에서 선택 가능한 지연시간 범위 중 하위 구간 두 번째 슬롯

예를 들어, 첫 라운드에서 클러스터 헤드 노드로 동작한 노드가 있다고 하자.
그렇다면 이 노드의 현재 가중치는 다음과 같다. 가중치 = 3

이 가중치 포인트에 의해, 이 노드는 다음 라운드에서 지역 노드로 선별되기 위한 임의의 시간을 할당받을 때 아래와 같은 불이익을 받는다.

0부터 255중 임의로 선정되는 동작 지연시간 중에서 노드가 선택 가능한 수의 집합에 가중치 3이 적용되므로 이 노드는 후반 7/8 구간, 즉 192-224 구간에서 시간을 임의로 선정하게 된다. 이는 이 노드가 현재 라운드에서 sleep 할 수 있는 확률을 높여주어 과도한 에너지가 집중되어 소모되지 않게 하는 효과가 있다.

또한 할당 시간 선정이 끝난 노드는 자신이 이번 라운드에서 네트워크의 노드로 활동할 확률이 줄어들게 되므로 다른 노드들과의 형평성을 위해 자신의 가중치 포인트를 1포인트 낮추게 되며, 자신의 가중치가 0이 될 때까지 매 라운드마다 반복한다.

(2) 최소 지연시간 가중치 부여

이 방법은 최대 가중치 부여 방법에 최소 가중치 부여 방법을 결합한 것이다.
이 방법에서 노드들이 생성하는 지연시간의 범위는 네트워크에 참여하지 못하는 노드에 의해 발생하며, 이 노드들은 매 라운드마다 네트워크에 참여하지 못한 횟수를 카운

트하여 이를 최소 지연시간의 가중치로 사용한다. 이 값이 증가할수록 다음 라운드에서 이 노드가 생성하는 지연시간의 범위가 빠르고 좁게 설정되므로 다음 라운드에서 네트워크에 참여할 수 있는 확률이 높아지게 된다. 이렇게 네트워크에 참여했던 노드는 자신의 최소 지연시간 가중치 값을 초기화 하여 네트워크에 부하가 분산될 수 있도록 한다.

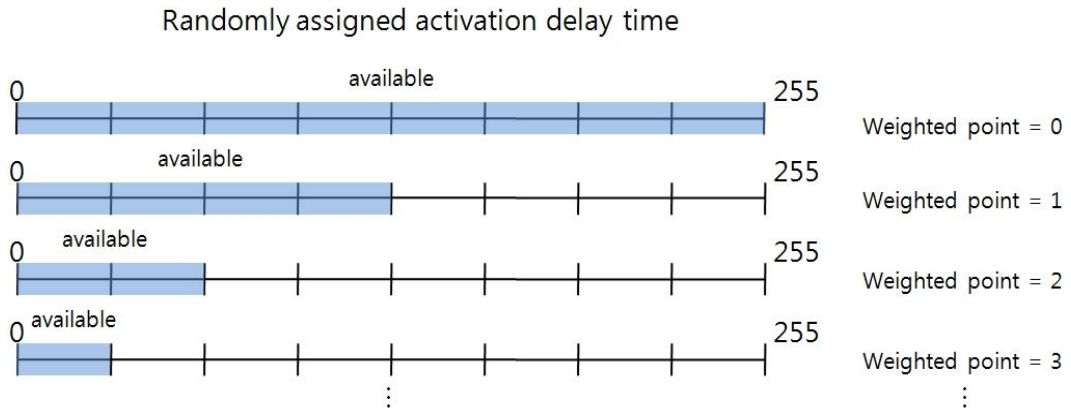
아래의 [그림 32] 는 최소 지연시간의 가중치 값에 의해 결정되는 할당 가능한 동작 지연시간의 범위를 나타낸다.

사용자에 의해 사전에 설정된 전체 동작 지연시간을 R_t 라고 하고, 이 지연시간의 최소값을 m_{R_t}, 최대값을 M_{R_t}, 노드들이 할당 가능한 동작 지연시간 구간을 r_t, 노드의 최소 지연시간 가중치 값을 W_{mdp}라고 하면, 실제로 노드가 사용 가능한 지연시간 구간 r_t의 최대값 M_{r_t}를 결정하는 식은 다음과 같으며 이 구간 r_t내에서 랜덤 지연시간 값을 선정한다.

$$\text{최소값 : } m_{r_t} = m_{R_t} \tag{4-3}$$

$$\text{최대값 : } M_{r_t} = \frac{M_{R_t}}{2^{W_{mdp}}} \tag{4-4}$$

가중치 값에 의해 결정되는 최소지연시간은 노드가 네트워크에 참여하지 않았던 라운드가 많을수록, 즉 네트워크 불참회수가 많을수록 감소하며, 이 네트워크 불참회수가 가중치가 된다. 이 값에 의해 최소지연시간의 범위가 결정된다.



[그림 32] 최소 지연시간 가중치 값에 의해 결정되는
할당 가능한 동작 지연 시간의 범위

가중치 1 - 다음 라운드에서 선택 가능한 지연시간 범위 중 상위 절반의 구간
가중치 2 - 다음 라운드에서 선택 가능한 지연시간 범위 중 상위 1/4 구간
가중치 3 - 다음 라운드에서 선택 가능한 지연시간 범위 중 상위 1/8 구간

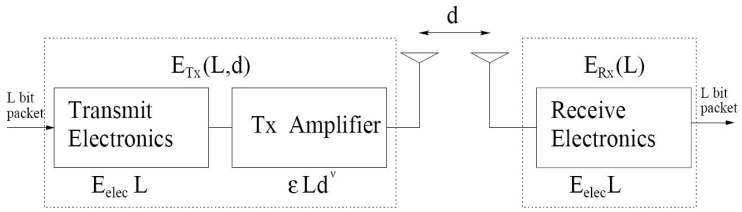
예를 들어, 이전 3라운드 동안 네트워크에 참여하지 못한 노드가 있다고 하자.
그렇다면 이 노드의 현재 가중치는 다음과 같다. 가중치 = 3

이 가중치 포인트에 의해, 이 노드는 다음 라운드에서 지역 노드로 선별되기 위한 임의의 시간을 할당받을 때 아래와 같은 이익을 받는다.

0부터 255중 임의로 선정되는 동작 지연시간 중에서 노드가 선택 가능한 수의 집합에 가중치 3이 적용되므로 이 노드는 전반 1/8 구간에서 시간을 임의로 선정하게 된다. 이는 이 노드가 현재 라운드에서 네트워크에 참여할 수 있는 확률을 높여준다.
또한 할당 시간 선정이 끝난 노드는 자신이 이번 라운드에서 네트워크의 노드로 활동할 확률이 줄어들게 되므로 다른 노드들과의 형평성을 위해 자신의 가중치 포인트를 초기화하게 된다.

3. 소비 에너지 식 유도

제안하는 방법은 매 라운드 당 한번의 setup과 한번의 steady 상태가 반복되며 setup은 송수신 과정과 스케쥴 연산을 포함한다.



[그림 33] 무선 통신 에너지 소비 모델

[그림 33] 의 에너지 소비 모델을 참고하여 제안하는 방법의 에너지 소모량을 아래의 식(5), (6) 으로 표기하였다. 이후 식에 사용되는 변수는 [표 5] 와 같다.

$$E_{tx}(l,d) = \begin{cases} lE_{elec} + lE_{mp}d^4 & : to\ \ sink \\ lE_{elec} + \dfrac{lE_{fs}M^2}{2\pi k} & : in\ \ cluster \end{cases} \quad (5)$$

$$E_{rx}(l) = lE_{elec} \quad (6)$$

제안하는 방법은 클러스터 내 지역 선별 노드의 개수인 N_{R_C}값에 의해 네트워크의 수명이 결정된다.

[표 5] 기호 표기법

E_{elec}	전자 에너지
E_{fs}	free space model 의 증폭에너지
E_{mp}	multipath model 의 증폭 에너지
$E_{schedule}$	노드의 scheduling 소모 에너지
E_{da}	데이터 병합 소모 에너지
l	데이터의 크기
N	전체 노드
N_R	지역 선별 노드
N_r	지역 선별 노드에 포함되는 노드
N_C	클러스터에 포함되는 노드
d	sink까지 거리
M	네트워크 면적의 한 변의 길이
C	클러스터
C_h	클러스터 헤드 노드
N_{R_C}	클러스터 내 지역 선별 노드
N_{rep}	전송 중계 노드
N_u	단위면적($1m \times 1m$) 당 위치하게 될 노드
U_{th}	사용자가 지정한 데이터 수집 단위면적의 배수값
A_C	N_C개의 노드가 위치하는 면적

가. N_{R_C}값 설정

N_{R_C}는 다음과 같은 방법으로 구한다. 우선, 필드에 노드들이 일정한 간격으로 배치되어있다고 가정하고 노드가 배치될 장소의 전체 면적에서 단위면적을 정한다. 단위면적이 $1m \times 1m$라고 할 때, 단위면적에 위치하게 될 노드의 수 N_u를 구하고 전체 네트워크에 생성될 C 값을 구하여 한개 클러스터에 포함되는 노드의 수 N_C를 구한다.

수식에 의한 분석은 인접 노드와의 데이터 비교가 어려우므로 인접 노드와 동일 데이터를 유지하는 기본면적을 정하여 사용자가 지정한 데이터 수집의 기본면적이 단위면적의 몇 배수인지 U_{th}를 구하고 이를 클러스터 내 노드수로 나눔으로서 N_R을 구할 수 있다.

$$A_C = \frac{N_C}{N_u} \tag{7}$$

$$N_R = \frac{A_C}{U_{th}},\ 1 \leqq N_R \leqq N_C \tag{8}$$

나. 셋업 단계

(1) 지역 선별 노드 셋업

지역 선별 노드 선정 과정은 지역 선별 후보 노드의 송신 1회로 이루어진다. 송신은 초기 패킷 광고와 1회의 초기 수집 정보의 전송이다. 에너지 소모량은 아래와 같이 나타낼 수 있으며, 이 식은 (5)와 (6)을 이용하여 나타내었다.

$$E_{N_R} = E_{schedule}(l) + \frac{N}{CN_{R_C}} \times E_{tx}(l,d) \tag{9}$$

$$E_{N_r} = E_{rx}(l) \tag{10}$$

지역 선별 노드의 에너지 소모량E_{N_R}은 식 (9)로 유도되며, 지역 선별 노드에 포함되는 노드 N_r 에너지 소모량E_{N_r}은 식 (10)로 유도된다. 식 (9)와 (10)을 이용하여 지역 선별 노드와 지역 선별 노드에 포함되는 노드의 소모 에너지를 합산하면 한 개의 지역 선별 노드 그룹에서 setup시 소모되는 에너지$E_{N_{R+r}}$인 식 (11)로 나타낼 수 있으며, 전체 네트워크에 생성된 지역 선별 노드의 수인 CN_{R_C}를 곱하면 전체 네트워크의 지역 선별 노드 선정에 소모되는 에너지$E_{all-N_{R+r}}$는 식 (12)로 나타낼 수 있다.

$$E_{N_{R+r}} = ((E_{N_R}) + (E_{N_r}) \times (\frac{N}{CN_{R_C}} - 1)) \quad (11)$$

$$E_{all-N_{R+t}} = CN_{R_C}(E_{N_{R+r}}) \quad (12)$$

(2) 클러스터 셋업

클러스터 셋업 과정은 클러스터 헤드 노드의 송신 2회, 수신 1회 스케쥴 연산으로 이루어진다. 송신은 초기 패킷 광고와 스케쥴 정보를 전송하는 것이고, 수신은 참여희망 노드의 메시지를 수신하는 것이다. 아래에 식 (5)와 (6)을 이용하여 식으로 나타내었다.

$$E_{cs-ch} = lE_{elec}(N_{R_C} - 1) + lE_{schedule}N_{R_C} + lE_{elec} + lE_{mp}d^4 + lE_{elec} + lE_{fs}\frac{M^2}{2\pi C} \quad (13)$$

$$E_{cs-mn} = lE_{elec} + lE_{fs}\frac{M^2}{2\pi C} + 2lE_{elec} \quad (14)$$

클러스터 헤드 노드의 에너지 소모량 E_{cs-ch}은 식 (13)으로 유도되며, 클러스터 멤버 노드의 에너지 소모량 E_{cs-mn}은 식 (14)로 유도된다. 식 (13)과 (14)을 이용하여 하나의 클러스터 헤드와 멤버 노드의 소모 에너지를 합산하면 한 개의 클러스터 셋업에 소모되는 에너지E_{cs}인 식 (15)으로 나타낼 수 있으며, 네트워크에 생성된 클러스터의 수인 C를 곱하면 전체 네트워크의 클러스터 셋업에 소모되는 에너지 E_{all-cs}는 식 (16)로 나타낼 수 있다.

$$E_{cs} = ((E_{cs-ch}) + (E_{cs-mn}) \times (N_{R_C} - 1)) \quad (15)$$

$$E_{all-cs} = C(E_{cs}) \quad (16)$$

(3) 전송 중계 노드 셋업

전송 중계 노드 셋업과정은 전송 중계노드의 송신 1회, 수신 1회로 이루어진다.

$$E_{repeater} = E_{rep}(lE_{elec} + lE_{fs}\frac{M^2}{2\pi C}) \quad (17)$$

다. Steady 단계

(1) 지역 선별 노드

제안하는 방법은 steady 단계에서 지역 선별 노드만 자신의 역할대로 동작한다. 이를 식으로 나타내면 steady 단계에서 그룹의 AN의 에너지 소모량E_R는 식 (18)로 유도되며, 지역 선별 노드의 인접 노드는 sleep 상태이므로 에너지 소모가 없어 E_r는 0이다.

$$E_{R-std} = lE_{elec} + lE_{fs}\frac{M^2}{2\pi c} \quad (18)$$

(2) 클러스터 노드

클러스터에서 에너지 소비는 LEACH의 에너지 소비 모델이 적용된다. 그러나 클러스터의 멤버 노드로 참여하는 지역 선별 노드의 중복된 에너지 소비는 제외한다. 클러스터의 헤드 노드는 상위의 sink로 전송하는 송신1회와 클러스터 내 멤버 노드로부터 수신하는 수신1회, 그리고 수신한 데이터를 처리하는 data aggregation 1회로 구성되며 이는 식(19)로 유도된다.

$$\begin{aligned} E_{C_h-std} &= E_{tx}(l,d) + E_{rx}(l)\times(E_{R_C}-1) + E_{da}(l)\times(E_{R_C}-1) \\ &= lE_{elec} + lE_{mp}d^4 + lE_{elec}(E_{R_C}-1) + lE_{da}(E_{R_C}-1) \end{aligned} \quad (19)$$

식 (18)와 (19)을 이용하면 steady 단계의 한 프레임에서 한 개의 클러스터가 소모하는 에너지 E_{C-std}는 식 (20)으로 나타낼 수 있다.

$$E_{C-std} = (E_{C_h-std} + E_{r-std}\times(E_{R_C}-1)) \quad (20)$$

그러므로 클러스터 하나의 프레임에서 전체 에너지 소모량$E_{C-allstd}$은 클러스터 개수인 c를 곱하면 식 (21)로 나타낼 수 있다.

$$E_{C-allstd} = C(E_{C-std}) \tag{21}$$

라. 전체 네트워크

setup 전체 소모에너지와 steady 전체 소모에너지의 합은 전체 네트워크의 소모에너지이며 이는 앞의 식 (12), (16), (21)을 이용하여 아래의 식(22)로 나타낼 수 있다.

$$E_{tvar} = E_{all-N_{R+t}} + E_{all-cs}\frac{CN_{R_C}R}{N} + lE_{elec}N + (E_{C-allstd})f \tag{22}$$

이는 기 제안되었던 방법[71][72]와 유사한 형태이나 그룹노드와 지역선별노드의 선정과정의 차이가 크므로 다른 에너지 소비 그래프를 나타내게 된다.

아래의 [그림 34] 는 제안하는 기법의 클러스터 형성 알고리즘을 나타낸다.

$CH_{regional}$: regional cluster head node
Repeater : relay node
N_{RCH_member} : regional cluster member node
N_{normal} : normal node before joining the cluster
$N_{regional}$: regional node
N_{sleep} : sleep node

Initialize :
1. generate(random_delay Time) /by normal nodes

Main Processing: /clustering process by normal nodes
1. if(nodes weight value > 0)
2. decrease weight value by 1 point
3. end if
4. Calculate available time slot period by weight value

```
5.  delay Time <- generate( random_delay Time)
6.  wait for delay Time or until receiving {any advertisement message}
7.  if( delay Time_Expired)
8.      if( nodeID == Nnormal )
        become N_regional
        broadcast( the Advertisement Message {nodeID, the 1st sensing value,
    position, altitude} )
9.      else
        cancel the delay Time
10.     end if
11.else
12.     if( receive the Advertisement Message{the 1st sensing value, altitude} ==
      the 1st sensing value, altitude )
        become N_sleep
            else
                wait for delay Time or until receiving {any
advertisement Message}
13.     end if
14.end  if
15.if( nodeID == N_regional )
        increase weight value by 1 point
 delay Time <- generate(random_delay Time)
16.     wait for delay Time or until receiving {any advertisement message}
17.if( delay Time_Expired)
18.     if( nodeID == N_regional )
        become CH_regional
        increase weight value by 2 points
        broadcast( the Advertisement Message {NodeID, position} )
19.     else
        cancel the delay time
20.     end if
21.else
22.     if( receive the Advertisement Message )
        cancel the delay time
                become N_RCH_member
            else
    wait for delay Time or until receiving {any advertisement Message}
23.     end if
24.end  if
25.if( nodeID == N_RCH_member )
26.     if( # of neighbor CH_regional) > 2 &&
27.       # of neighbor CH_regional < 6 )
28.       become repeater
29.       broadcast( the Advertisement Message {NodeID, position} )
30.   end if
```

31.end if

$CH_{regional}$

1. broadcast(the Advertisement Message {nodeID, the 1st sensing value, position})
2. accept(join Message)
3. aggregate sensing data
4. transmit_data_to_Sink (sensing value, nodeID, position)

N_{RCH_member}

1. join to cluster(CHnodeID, nodeID, position)

Repeater

1. join to cluster(CHnodeID, nodeID, position)
2. relay data

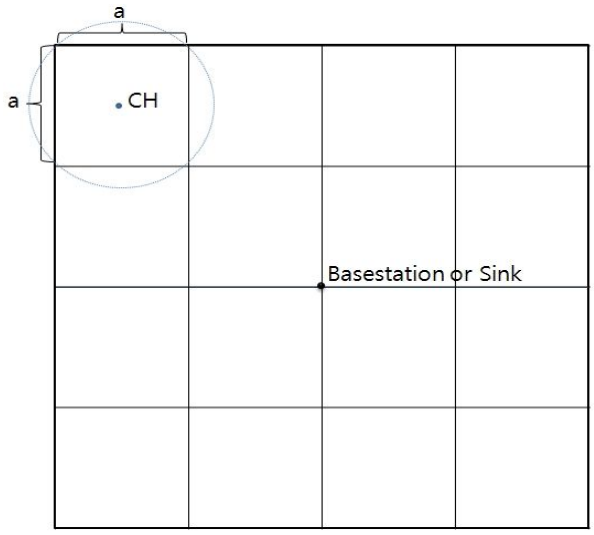
[그림 34] 제안하는 기법의 의사코드

제3절 보안 신뢰성 향상

1. 기본 가정

제안하는 방법은 다음과 같은 가정을 갖는다. 센서 노드들이 초기에 필드에 위치하여 네트워크를 이룰 때에는 공격을 받지 않는다. 모든 노드는 한번 필드에 deployment된 후 고정되어 있다. 베이스 스테이션으로부터 one-hop 거리 밖에 위치한 모든 노드는 multi-hop 기반 통신을 한다. 클러스터 형성 시 클러스터 헤드는 one-hop거리의 노드들과 클러스터를 형성한다. 한 클러스터에 속한 노드는 클러스터 헤드 및 클러스터 내의 노드와 통신한다.

2. 네트워크 구조



[그림 35] 제안하는 기법의 네트워크 구조

[그림 35] 에서 노드가 배치되게 되는 필드는 노드가 배치된 후 클러스터로 구분된다. 클러스터의 이상적인 배치, 그리고 필드에 배치되는 모든 노드는 골고루 분포된다는 가정을 하면 각 클러스터에는 평균 N_c개의 노드가 분포하고 있다. 클러스터의 지름

이 a라고 정하고, 노드의 전파 전달 거리 R 안에 위치하는 노드의 수가 m개라고 가정하면, R 내에 위치하는 노드의 수는 m+1개이다. 이것으로부터 네트워크 내부의 센서 노드의 밀도N_d 를 계산하면 노드의 밀도는

$$N_d = \frac{(m+1)}{\pi R^2} \tag{23}$$

이며, 이 식으로부터 한 개의 클러스터에 위치한 노드의 개수는

$$N_c = N_d a^2 = \frac{(m+1)a^2}{\pi R^2} \tag{24}$$

로 나타낼 수 있다.

3. 공격 유형

위와 같은 계층적 클러스터 센서 네트워크에서 가능한 라우팅 공격 유형을 보면 다음과 같다.

· Selective forwarding

- 공격 노드가 특정 메시지의 전송을 거부하거나 삭제하는 공격이다. 이 공격은 특정 노드로의 전달이나 데이터를 거부함으로써 노드들의 통신을 단절시키거나 베이스 스테이션으로 수집되는 정보의 신뢰성을 저하시킨다.

· HELLO flood attack

- 노드들의 경로 설정 단계에서 멀리 있는 공격자가 강한 강도의 HELLO 패킷을 보냄으로써 일반 노드들의 경로 설정 시 공격 노드가 라우팅에 참여를 시도하는 형태의 공격이며 센서 노드들의 라우팅을 혼란시킨다.

· Sybil attack

- 공격 노드가 많은 수의 노드 ID를 가지고 이를 공격에 사용하는 방법이다. 이 공격

은 정상 노드가 공격 노드인 것으로, 또는 공격 노드가 정상 노드인 것으로 가장할 수 있으며 라우팅 경로를 변경하여 공격 노드가 라우팅 경로에 포함되게 할 수 있다.

4. 키 분배 및 인증 기법 제안

위와 같은 유형의 공격은 비밀키 공유와 인증을 통해 대응이 가능하다. 제안하는 기법은 이변수 다항식을 이용한 pair-wise key를 생성하는 키 선분배 기법이며 키의 추출은 키 풀에서 생성된 키를 노드에 할당하는 형식이다.

이 기법은 크게 키 사전 키 배포 단계, 공유키 설정 단계, 경로키 생성의 3단계로 이루어진다. 또한 계층적 클러스터 네트워크 구조에 의하면 노드는 그 역할에 따라 3가지 레벨로 구분이 가능하며 각 레벨에 요구되는 키는 다음과 같다.

level 1에서 사용되는 키의 요구사항 - 사전에 분배된 키 셋을 이용해 확률적인 링크를 구성한다. 가장 기본이 되는 키이다. 클러스터 내의 멤버 노드가 이에 해당한다.

level 2에서 사용되는 키의 요구사항 - level 1의 키와는 다른 키를 상위 레벨로부터 받아 사용한다. level 2가 된 노드는 BS의 인증 절차를 거쳐 level 2로 동작하게 된다. CH 및 리피터 노드가 이에 해당한다.

level 3에서 사용되는 키의 요구사항 - 모든 키를 알고 있으며 키를 만들 수 있다. 베이스 스테이션 및 싱크가 이에 해당한다.

가. 사전 키 배포 단계

베이스 스테이션은 아래와 같이 P 개수를 갖는 임의의 t차 이변 다항식 pool을 생성하여 랜덤하게 k개의 키를 각각의 노드에 할당한다. 이때 베이스 스테이션은 두 개의 키 풀을 유지하며, 각각 일반 노드와 상위 노드의 키 설정에 사용한다. 이 두 개의 풀에서 생성되는 키는 중복 사용되지 않는다. 이렇게 사용하는 키를 구분함으로써 일

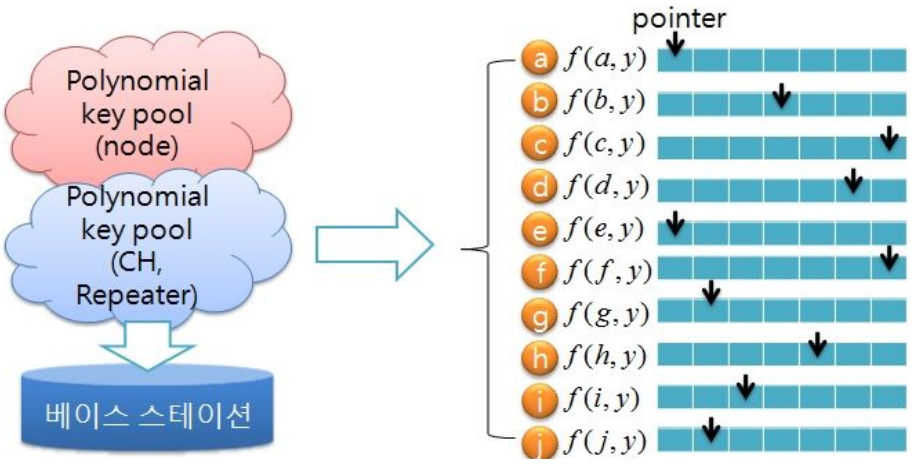
반 노드에서 누출되는 키로 인해 상위 레벨의 노드가 포획되는 문제를 완화하는 효과가 있다.

$$f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^{i}y^{j} \ , \ f(x,y)=f(y,x) \tag{25}$$

이 k개의 키를 이용하여 모든 노드들은 공유키를 설정하여 인접하는 노드들 사이에 확률적인 연결을 한다. 이 확률은 다음의 식에 의해 계산할 수 있다.

$$p'=1-\frac{((P-k)!)^2}{(P-2k)!P!},\ 0\le p'\le 1 \tag{26}$$

또한 각 노드에 할당된 k개의 키는 임의로 생성된 포인터를 가지고 있다. 이 포인터는 매 라운드 마다 이동하여 다른 키를 가리킨다. 각 노드별 k개의 키와 포인터 위치는 BS가 생성하여 배포하는 것으로 BS는 사전에 모든 정보를 알고 있다. BS는 이 포인터 정보를 이용하여 CH 후보 노드의 인증을 수행한다. 아래 [그림 36] 은 BS가 키 풀에서 노드에게 임의로 할당한 k개의 키와 포인터를 나타낸다.



[그림 36] 베이스 스테이션에서 노드에 임의로 할당된 키와 키 포인터

나. 공유키 및 경로키 설정 단계

제안하는 방법은 계층적 클러스터링 기법 중 ARCT 와 ARCS 방법을 기초로 한 키 분배 및 공유이므로 ARCT, ARCS의 클러스터 생성 절차에 맞추어 키를 분배한다.

ARCT에서 CH 후보 노드는 자신이 CH임을 자신의 전송반경 이내에 위치한 인접 노드에 알리며, 이 신호를 수신한 인접노드 중 공유키를 발견한 노드와 발견하지 못한 노드 모두 CH가 되기를 포기하고 멤버노드가 되기 위한 대기상태로 들어간다. 이후 BS의 인증을 마친 CH가 멤버노드에 클러스터 내부에서 사용할 공유키를 전달하면 이 키를 공유하여 클러스터 내 멤버 노드로 동작한다. 이 때 공유키를 소유하는 멤버노드들은 CH와 공유하는 키를 이용하여 클러스터 공유키를 받으며, 공유키를 소유하지 못한 멤버노드는 인접한 멤버노드와 경로키 설정을 통해 클러스터 공유키를 받아 CH와 키를 설정하게 된다.

· Level 1 노드

- 사전에 키를 배포받은 노드들은 주어진 영역에서 상호 공유키를 설정하는 과정을 거쳐 클러스터를 구성한다. 이 클러스터는 해당 라운드만 유지되며 매 라운드마다 변경되므로 주기적인 클러스터 재설정이 필요하다. 이때 노드들 사이에 반복적인 공유키 설정이 필요하게 되며, 이 공유키 설정은 노드들이 사전에 분배받은 k개의 키를 이용한 확률적인 공유를 하게 된다.

(1) 클러스터 설정시 CH후보 노드는 자신이 소유하고 있는 k개의 키 부분정보를 포함한 패킷을 자신의 전송 반경 내에 위치한 인접 노드들에게 브로드캐스트한다.

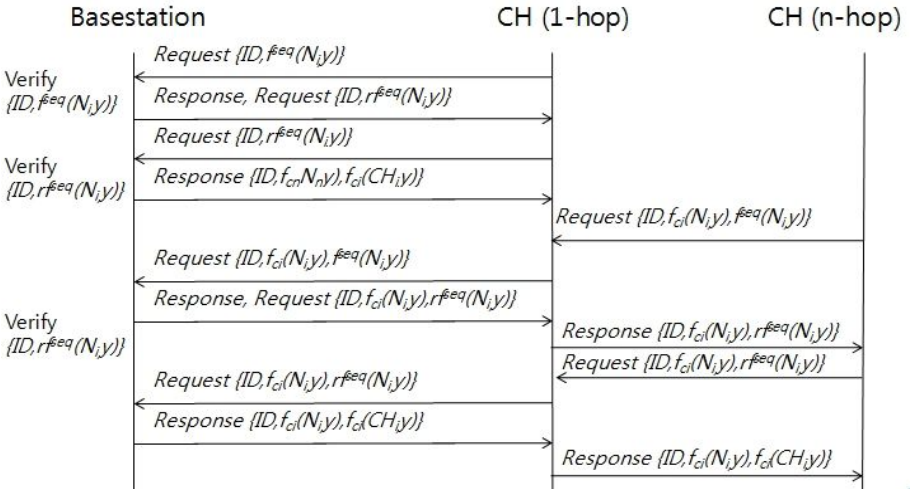
(2) 인접 노드들 중 공통의 키를 소유한 노드들은 자신이 CH가 되려던 시도를 포기하고 CH의 BS인증 후 클러스터 내 공유키를 전송받을 때까지 대기한다.

(3) 공통의 키를 소유하지 못한 노드들 또한 대기한다. 그러나 공격자에 의한 공격일 수 있으므로 이를 구분하기 위해 클러스터 내 공유키와 경로키 설정이 되기까지 대기시간을 더 연장한다. 클러스터 내 공유키와 경로키 설정이 이루어지지 않을 시 다시 CH가 되기 위한 타이머를 동작한다.

· Level 2 노드

- CH후보로 선정된 노드는 자신이 소유한 k개의 키들 중 포인터가 위치하지 않은 $k-1$개의 키들 중 임의의 키를 이용하여 BS과 통신을 시도한다. ARCS의 경우 리피터로 선정된 노드도 동일한 절차로 동작하며, 이는 통신 도중 키의 유출이 발생할 경우 포인터의 위치를 숨기기 위한 것이다.

아래의 [그림 37] 은 BS과 1홉 거리 이내에 위치한 CH 후보노드와 BS과 1홉 거리 밖에 위치한 CH 후보노드의 BS에 의한 인증 절차를 나타낸 것이다.



[그림 37] 베이스 스테이션에 의한 클러스터 헤드 노드의 인증 절차

· Level 3 노드

- BS은 하위 레벨 1, 2의 노드들과 인증을 통한 안정된 네트워크를 구성하며, 레벨 2의 모든 노드는 네트워크의 안정된 동작을 위해 BS의 인증이 꼭 필요하다. 또한, 클러스터 내부에서 사용하는 클러스터 내 공유 키와 클러스터 헤드 노드들 사이의 멀티 홉 통신을 위한 클러스터 헤드 노드 간 공유 키를 생성하여 분배하는 역할을 한다.

(1) 노드의 삽입

새로운 노드를 네트워크에 삽입시, 새로운 노드 또한 BS로부터 k개의 키와 포인

터를 받는다. 이 키에 의해 인접 노드와 클러스터 형성 시 확률적 키 공유 확률에 의해 키를 설정한다.

(2) 노드의 삭제

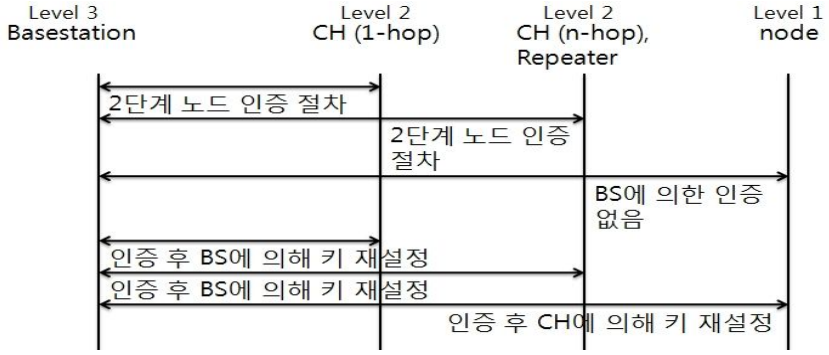
노드의 경우, 외부 공격에 의한 노드의 손실이 감지되면 해당 노드가 보유한 k개의 키 정보는 폐기해야 하므로 BS에 의해 전체 네트워크의 노드에 해당하는 키의 폐기를 요청하는 패킷을 브로드캐스트 하며 폐기 요청을 수신한 모든 노드는 해당하는 키를 리스트에서 삭제한다.

다. 노드 인증 단계

계층적 센서 네트워크에서 step 3은 일반 노드에게는 적용되지 않는다.
일반 노드는 최하위 계층으로서 내 외부로부터의 공격에 취약하며 이 노드들을 모두 인증하기 위해서는 상당한 자원의 소모가 필요하며 노드의 숫자에 비례해 요구 시간 및 자원이 증가하므로 사실상 불가능하다.

상위레벨의 CH 노드는 클러스터 단위의 데이터 수집자 역할을 하며 데이터 중계의 역할을 담당한다. 따라서 상대적으로 높은 보안 안전성을 요구하며 그 숫자도 일반 노드에 비해 상당히 적다. 그러므로 안전한 데이터 취합과 전송을 위해 CH 노드 레벨부터 BS의 인증이 필요하다.

아래 [그림 38] 은 계층적 센서 네트워크의 일반적인 레벨 구분과 인증 및 키 재설정 과정을 나타낸다.



[그림 38] 네트워크의 레벨 구분과 키 분배 및 인증 절차

제4장 성능 평가

본 장에서는 제안한 지역 클러스터 기반 라우팅 기법과 키 관리 기법을 에너지 측면에서 센서 네트워크의 기본 기능인 데이터 수집에 대해 성능을 측정한다. 또한 멀티홉으로 연결된 센서 네트워크의 네트워크 연결률을 측정하며, 네트워크의 생존 시간 동안 생성된 클러스터 헤드 노드의 수 및 모든 노드들의 에너지 소비 평준화 정도, 고립된 노드들의 수, 그리고 마지막으로 전체 네트워크의 생존시간을 측정한다.

보안 측면에서 노드간 연결도, 키 유도 방식, 최대 노출키 수 (키 노출에 따른 견고성), 키 노출 피해범위, 키의 갱신 오버헤드, 노드에 저장되는 키의 메모리 오버헤드, 노드 포획에 대한 안전성에 대해 평가한다.

제1절 실험 환경

이 실험에는 밀집 센서 네트워크와 키 분배의 구현을 위해 MATLAB7.0이 사용되었으며 실험환경은 아래의 표와 같다.

[표 6] 시뮬레이션 파라미터

Item	Value
전자 에너지	$E_{elec} = 50nJ/bit$
증폭 에너지 (free space model)	$E_{fs} = 10pJ/bit/m^2$
증폭 에너지 (multipath model)	$E_{mp} = 0.0013pJ/bit/m^4$
Scheduling 에너지	$E_{schedule} = 5nJ/bit/signal$
데이터 병합 에너지	E_{da}=$5nJ/bit/signal$
데이터 크기	$l = 1000bit$
전체 노드 수	$N = 1000$
네트워크 면적 한 변의 길이	$M = 200m$
임계값	$-3 \leq H_{th} \leq 3, S_{th} = 0.2$

모든 기법의 측정 기본 단위는 라운드이며 1번의 라운드 내에 1번의 셋업과 3번의 고정전송 주기를 갖는다. 하이브리드형 기법인 APTEEN의 고정 주기 전송 횟수는 3라운드마다 1회의 전송을 적용하였다. 이 측정에 사용하기 위해 센서 노드들이 취급하는 온도변화 데이터 값은 실제 환경에서 발생하는 온도변화와 유사한 조건을 주기 위해 기상청에서 제공하는 기온 변화 데이터베이스에서 추출한 지역별 기온변화 데이터 셋을 이용하였다.

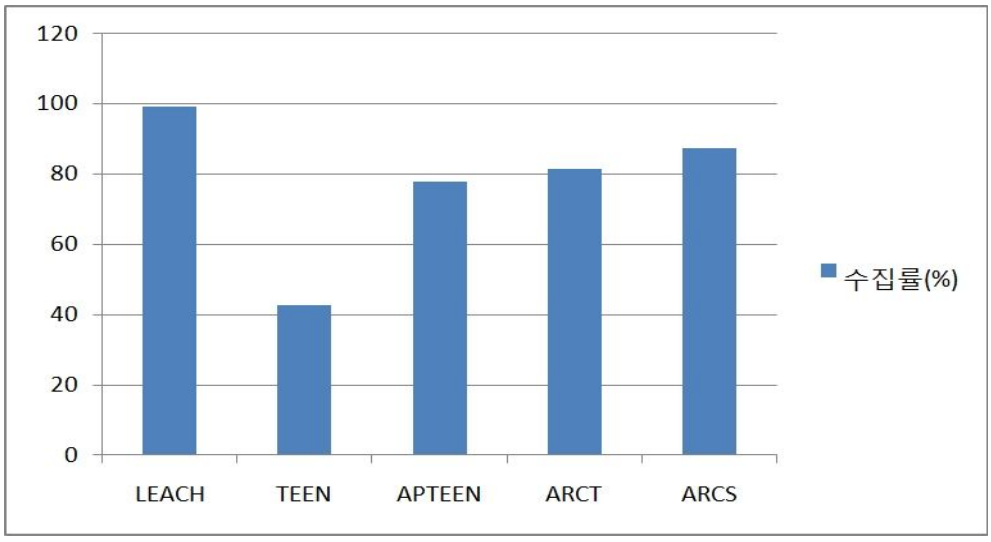
제2절 라우팅 기법 에너지 효율성 평가

1. 수집 데이터 정확도 평가

다음의 [표 7] 과 [그림 39] 는 각 클러스터링 기법의 네트워크 생존 시간 동안 노드에 의해 수집된 데이터를 원시 데이터와 비교한 수집 데이터의 정확도이다.

[표 7] 프로토콜별로 수집한 데이터의 정확도

프로토콜 / 기온 데이터	수집 데이터 정확도 (%)				
	LEACH	TEEN	APTEEN	ARCT	ARCS
봄	99.21	36.74	73.80	81.04	87.48
여 름	99.24	48.15	76.82	84.08	87.74
가 을	99.20	47.90	74.64	75.78	87.08
겨 울	98.65	37.40	85.72	84.83	86.99
평 균	99.08	42.55	77.75	81.43	87.32



[그림 39] 프로토콜별 평균 데이터 수집률

표에 의하면 평균 정확도에 있어 LEACH가 가장 높은 것을 알 수 있다. 이러한 결과는 LEACH가 proactive network이며 네트워크의 모든 노드가 데이터 전송에 관여하기 때문에 가능하다.

TEEN은 다른 4가지 방법에 비해 상당히 낮은 수준의 정확도를 보임을 알 수 있다. 이는 TEEN의 특성상 실제 수집된 값을 전송하는 것이 아닌 2가지의 문턱값을 사용하여 전송을 조절하는 형태이기 때문이며, 이로 인해 사실적인 데이터를 재구성하는데 어려움이 있다. 또한, 봄과 겨울의 정확도가 낮게 나타남을 알 수 있는데 이것은 일부 지역이나 일정 시간동안 수집 데이터가 문턱값에 미달되어 데이터 전송이 없었음을 간접적으로 짐작하게 하는 부분이다. 결국 TEEN에 있어 노드의 에너지 소비는 줄어드나 데이터 수집 자체가 어렵게 되는 결과를 갖게 된다.

APTEEN의 경우 중간 정도의 정확도를 보인다. 이는 APTEEN의 고정 주기 전송 메커니즘으로 인한 결과이며 이로 인해 TEEN보다 상대적으로 높은 데이터 정확도를 보인다.

ARCT의 경우 TEEN과 APTEEN보다는 높으나 LEACH에 비해 낮은 정확도를 보인다. 이는 지역 클러스터 멤버 노드의 수집 데이터를 무시하고 클러스터 헤드 노드가 수집한 데이터에 의존하였기 때문으로 보인다. 그럼에도 불구하고 LEACH에 근접한 수준의 정확도를 보이는 것은 상당히 높은 데이터 정확도를 갖고 있음을 의미한다. 그러나 여전히 20%대의 오차가 존재한다.

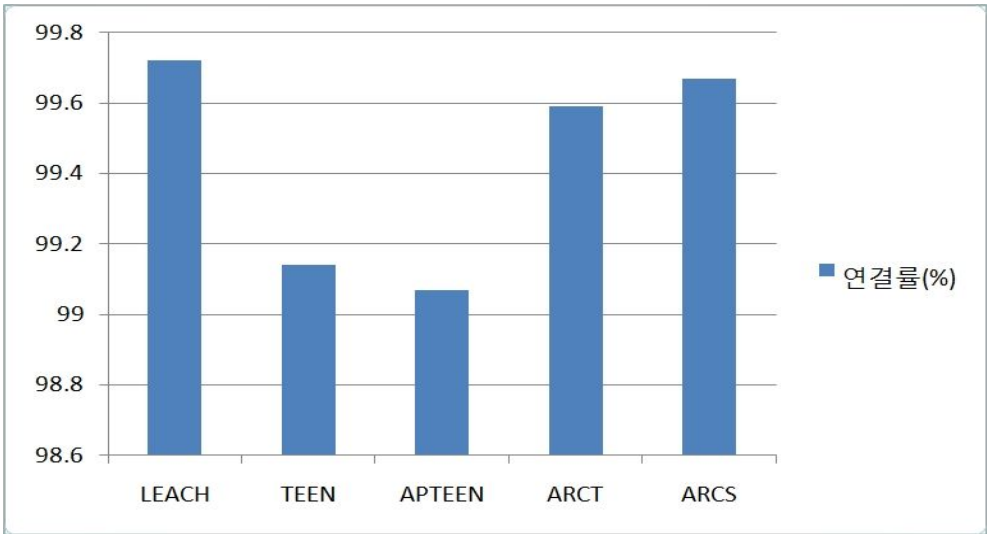
ARCS의 경우 90%에 근접한 결과를 보여주며 ARCT에 비해 개선되었음을 알 수 있다.

2. 네트워크 연결도 평가

아래의 [표 8] 과 [그림 40] 은 전체 네트워크 생존시간 동안 프로토콜별로 측정한 평균 네트워크 연결도를 나타낸다.

[표 8] 프로토콜별로 측정한 네트워크 평균 연결도

프로토콜 / 기온 데이터	네트워크 연결도 (%)				
	LEACH	TEEN	APTEEN	ARCT	ARCS
봄	99.53	99.72	99.32	99.69	99.55
여 름	99.79	98.47	99.08	99.63	99.81
가 을	99.79	98.71	98.20	99.62	99.68
겨 울	99.77	99.63	99.67	99.39	99.61
평 균	99.72	99.13	99.07	99.58	99.66



[그림 40] 프로토콜별 평균 네트워크 연결률

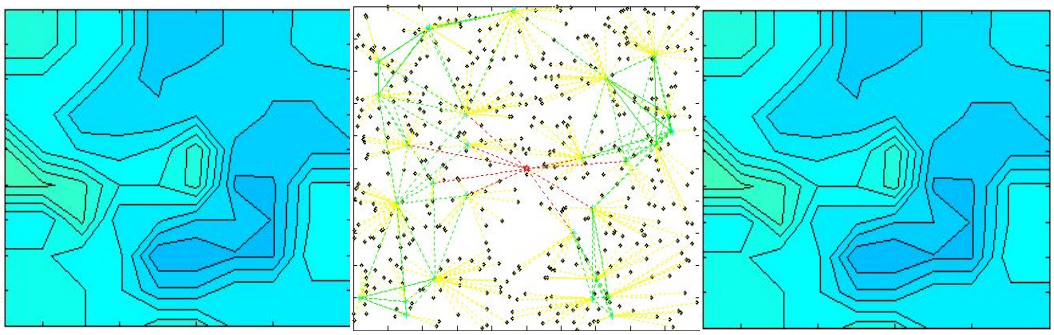
표에 의하면 LEACH, TEEN, APTEEN 모두 계절 데이터에 관계없이 비슷한 수준의 평균 연결률을 보임을 알 수 있다.

클러스터 기반 프로토콜에서는 클러스터 헤드 노드가 소스 노드와 싱크 사이의 데이터 전달자 역할을 하기 때문에 클러스터 헤드 노드의 개수가 가장 중요하다. 확률에

기초한 클러스터 헤드 노드 선정에 있어 클러스터 헤드 노드의 개수가 많을수록 싱크와의 연결확률이 높아지기 때문에 클러스터 헤드 노드의 개수가 많을수록 네트워크 연결 확률은 높아진다. 그러나 클러스터 헤드 노드는 에너지 소모량이 크기 때문에 여기에 트레이드오프가 존재한다.

이전의 연구 결과에서는 적절한 수준이 전체 노드의 5% 정도라고 알려져 있다. 그러나 제안한 방법은 지역 클러스터의 에너지 소모율이 크지 않기 때문에 더욱 많은 수의 클러스터 헤드 노드를 설정할 수 있다. 따라서 전체 네트워크의 연결도는 높아지게 되며 전체 네크워크의 동작 시간 동안 평균 99%이상의 연결률을 보인다.

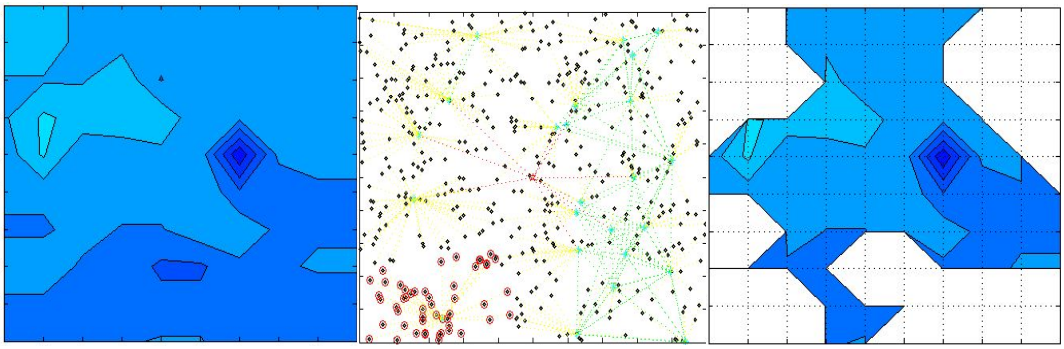
아래의 [그림 41] 은 네트워크가 정상적으로 연결되었을 때의 데이터 수집과 복원 과정을 나타낸 것이다. 네트워크가 정상적으로 링크 단절이 없이 동작할 경우 (a)의 원시 데이터는 정상적인 수집과정 (b)를 거쳐 싱크노드에 전달되게 되고 이는 정상적으로 복원되어 (c)와 같이 사용자에게 제공되게 된다.



(a) 원시 데이터 (b) 정상적으로 연결된 네트워크 (c) 완전한 데이터 복원

[그림 41] 프로토콜에 의한 일반적인 데이터 수집과 복원의 예

그러나 아래의 [그림 42] 와 같이 데이터 수집을 담당하는 네트워크의 일부가 단절되는 현상이 나타날 경우 원시 데이터 (a)의 일부 데이터는 (b)의 링크가 단절된 노드들(붉은 색 노드들)이 데이터 전송을 할 수 없으므로 해당 지역의 데이터가 소실되게 되며, 싱크 노드가 재구성 한 맵은 (c)와 같이 나타나게 되어 정상적인 데이터 복원이 어렵게 된다.



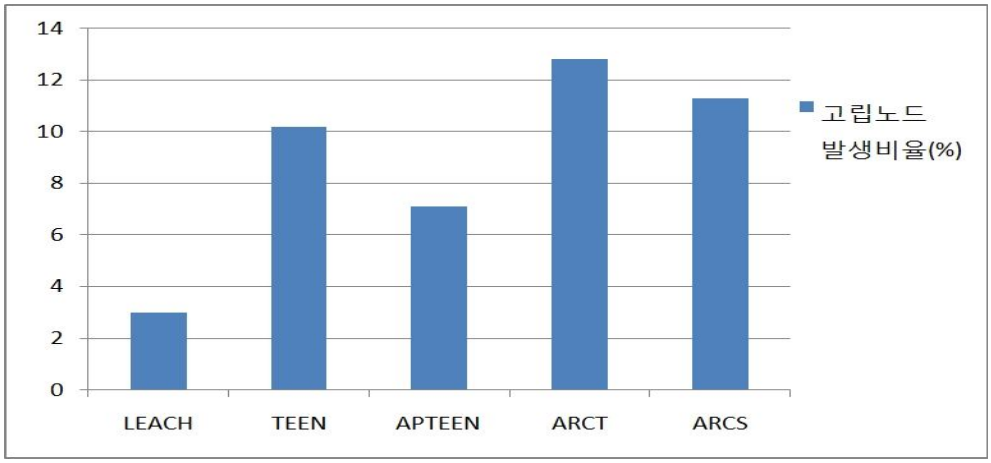
(a) 원시 데이터 (b) 일부 링크가 단절된 네트워크 (c) 불완전한 데이터 복원

[그림 42] 네트워크 단절시 발생하는 문제의 예

아래의 [표 9] 와 [그림 43] 은 전체 네트워크 생존시간 동안 고립된 노드가 발생한 라운드를 측정하여 비교한 것이다.

[표 9] 네트워크 수명에 대한 고립노드 발생비율

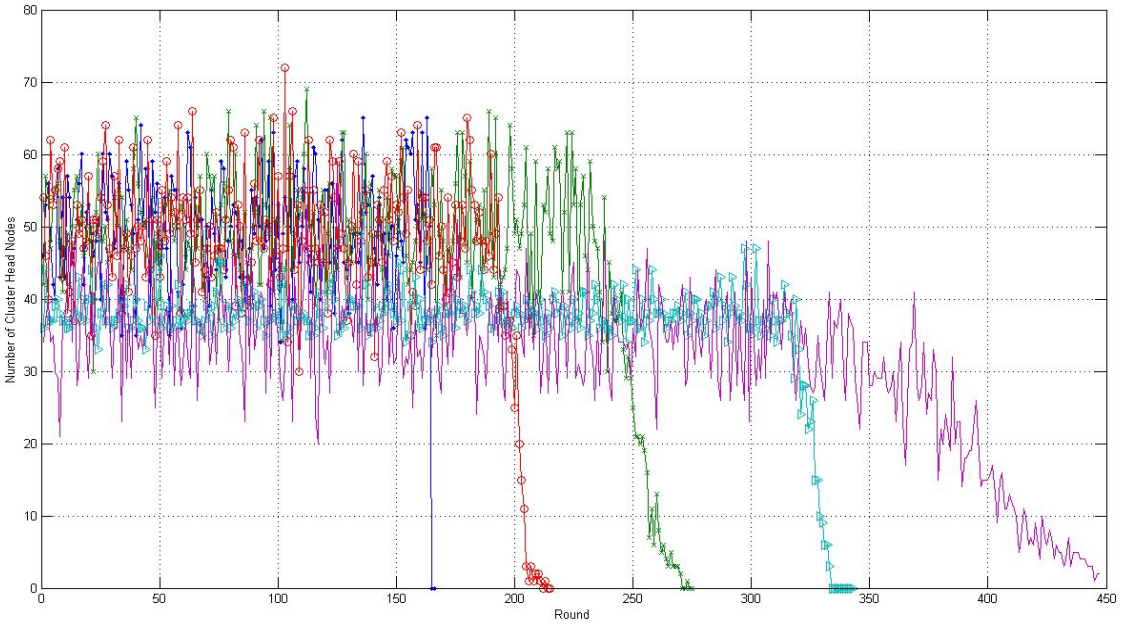
	LEACH	TEEN	APTEEN	ARCT	ARCS
네트워크 수명 (라운드 수)	169	275	212	345	443
고립노드 발생횟수	5	28	15	44	50
고립노드 발생비율 (%)	3	10.2	7.1	12.8	11.3
정상 전송 비율 (%)	97	89.8	92.9	87.2	88.7



[그림 43] 고립노드 발생 비율

3. 클러스터 헤드노드의 수

클러스터 헤드 노드의 수는 네트워크의 연결도와 관계가 있다. 따라서 확률에 기반한 클러스터 헤드 노드 선정방법에서 클러스터 헤드 노드의 수를 일정하게 유지하는 것은 꼭 필요하다. 아래의 [그림 44] 는 네트워크 생존시간 동안에 생성되었던 클러스터 헤드 노드의 수를 각 프로토콜별로 나타낸 것이다.



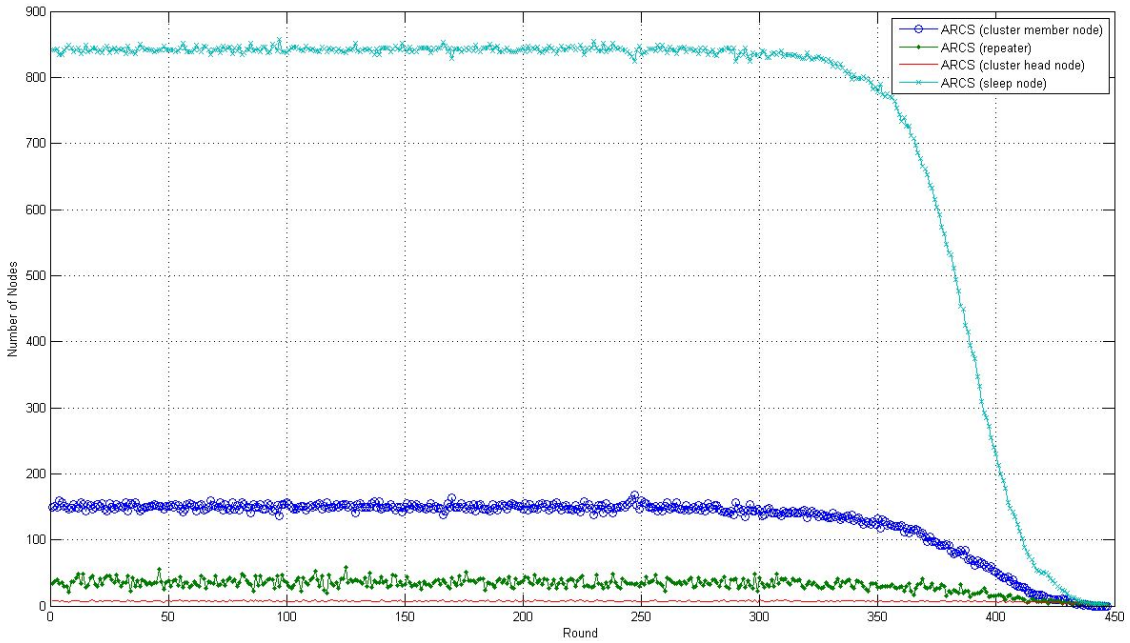
[그림 44] 프로토콜별로 생성된 클러스터 헤드 노드의 수

LEACH, TEEN, APTEEN은 동일한 방식으로 클러스터 헤드 노드를 선정한다. 이 방법들은 동일한 5%의 클러스터 헤드노드 선정확률이 적용되며 이 확률에 의해 클러스터 헤드 노드가 선정된다. 그러나 그래프에서 보이는 바와 같이 클러스터 헤드 노드는 약 40개에서 60개 정도로 최대 20개의 오차범위로 생성됨을 알 수 있다. LEACH, TEEN, APTEEN의 방법은 기준 값에 미달되는 클러스터 헤드노드가 자주 생성될 경우 노드들 사이의 연결도가 낮아지게 되어 데이터 수집에 문제가 발생할 확률이 커지게 된다.

이에 비해 제안한 방법과 같이 랜덤 시간에 의한 노드들의 경쟁을 통해 클러스터 헤드를 선발하는 경우 일정한 개수의 클러스터 헤드 노드의 수를 유지한다. ARCT는 클

러스터 헤드 노드의 수가 35개에서 40개 정도로 유지되어 앞의 세 가지 방법에 비해 오차 범위가 줄어든 것을 알 수 있다. 제안한 방법인 ARCS도 역시 유사한 수준의 클러스터 헤드 노드의 수를 유지하고 있음을 알 수 있다.

그러나, 아래의 [그림 45] 에 의하면 제안하는 방법은 데이터 전송을 위해 클러스터 헤드 노드와 중계 노드가 존재한다. 이들 중 에너지 소모가 큰 클러스터 헤드 노드의 비율은 약 20%이다. 결과적으로 제안하는 방법은 클러스터 헤드 노드가 전체 네트워크의 에너지 소비에 미치는 영향이 적다.

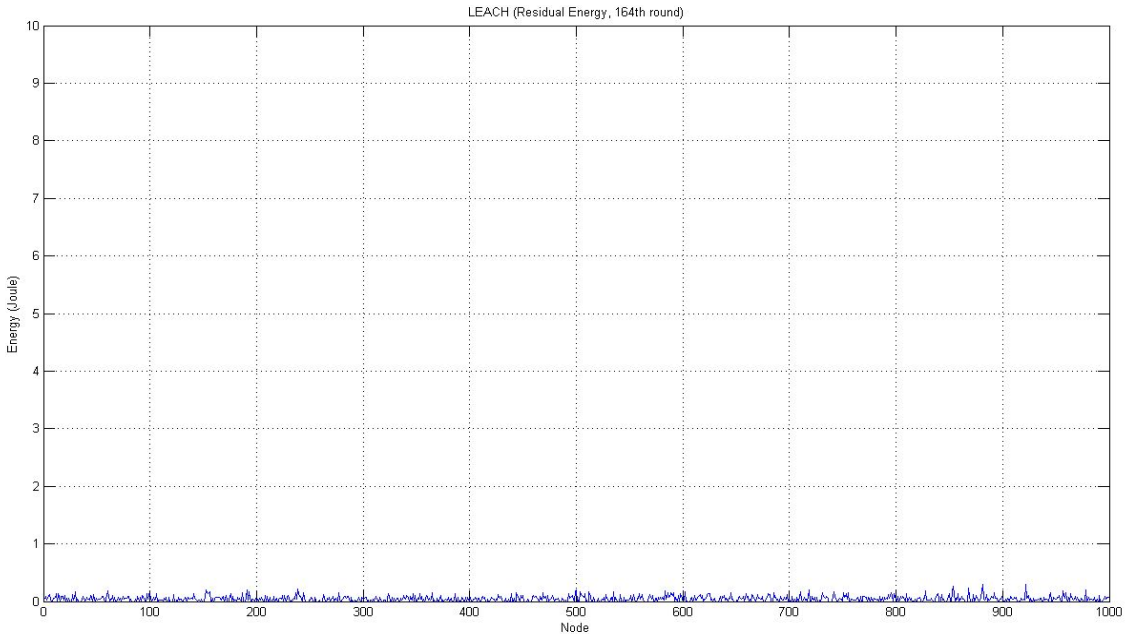


[그림 45] 제안한 방법의 클러스터 헤드 노드와 중계 노드의 생성 비율

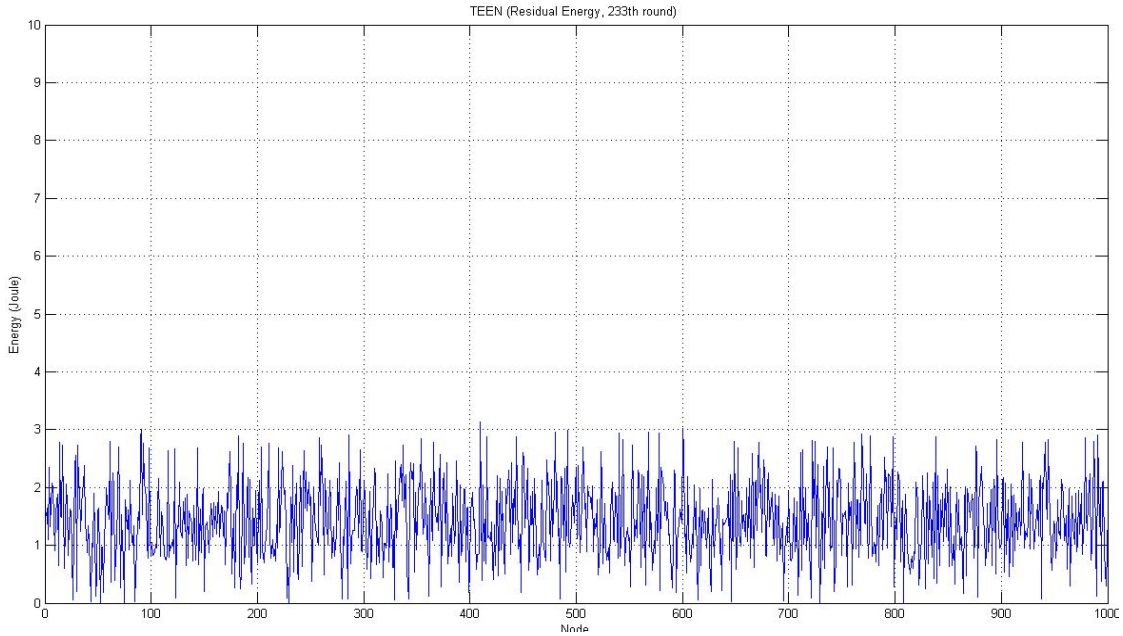
4. 네트워크 잔여 에너지 측정

가. 노드별 잔여 에너지

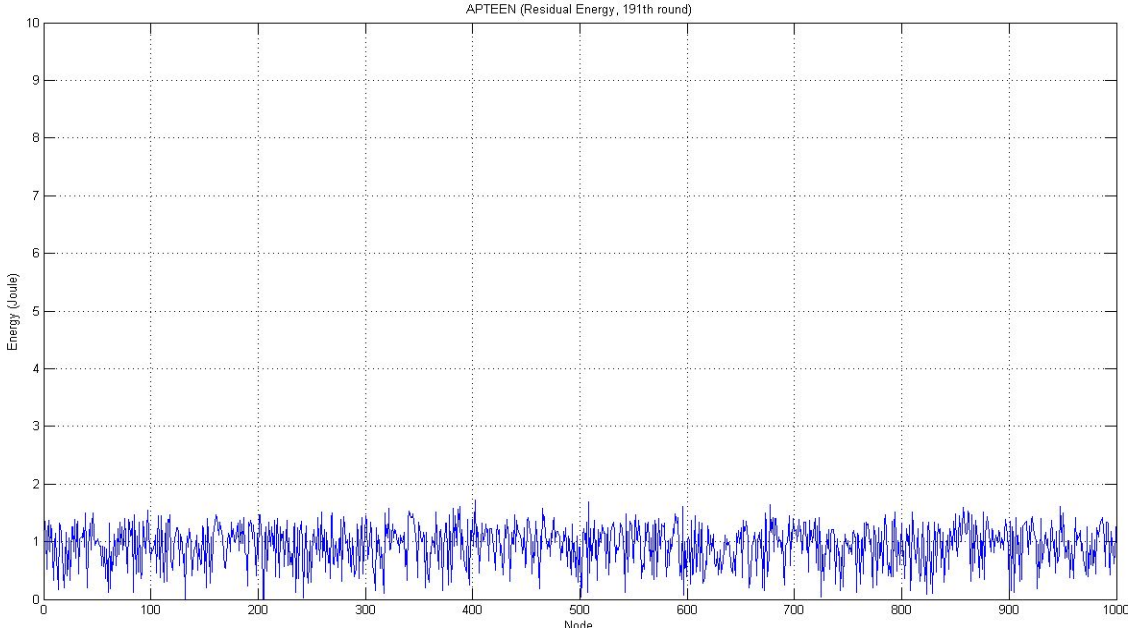
아래의 [그림 46] 은 각 프로토콜별로 네트워크를 구동했을 때, 네트워크에서 에너지가 고갈된 노드가 최초로 발생하는 시점에 측정한 노드별 잔여에너지 그래프이다.



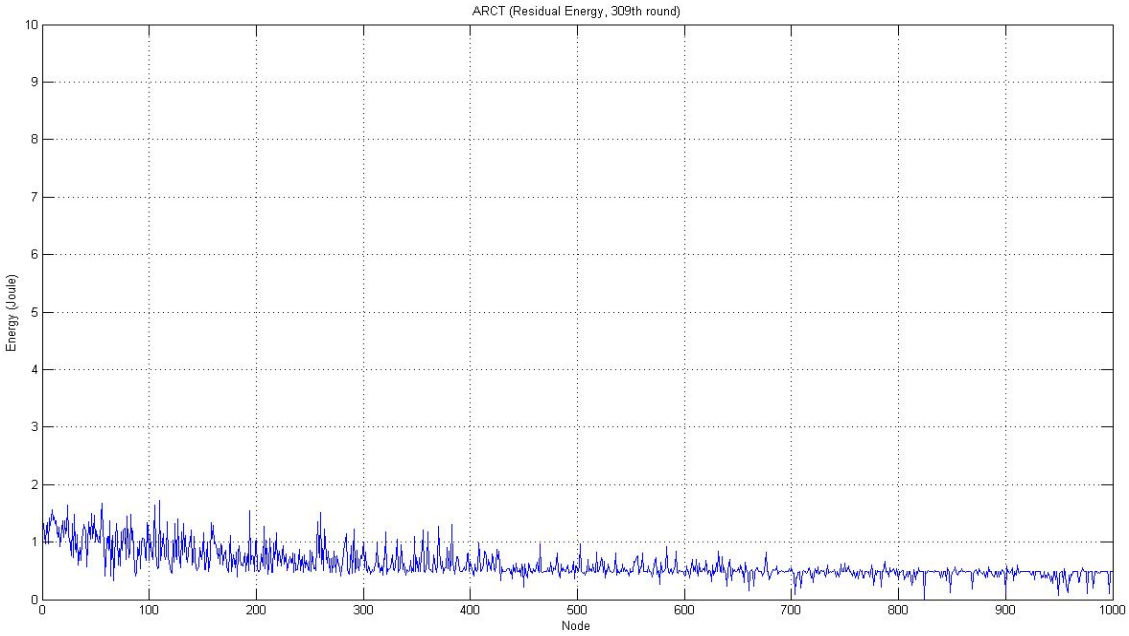
(a) LEACH



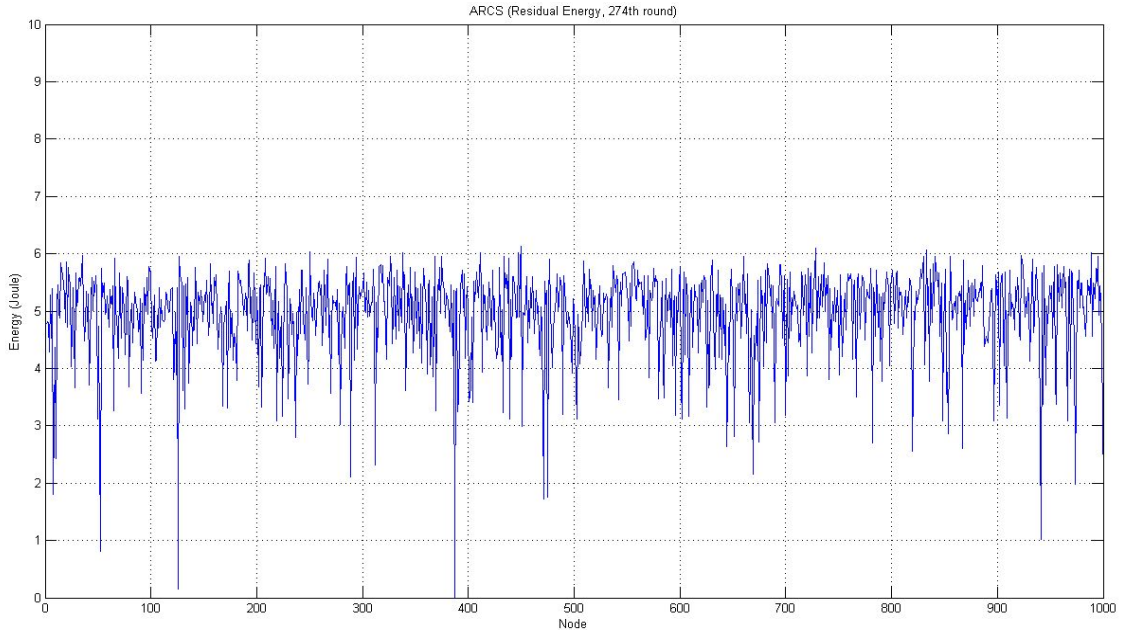
(b) TEEN



(c) APTEEN



(D) ARCT



(e) ARCS

[그림 46] 에너지가 고갈된 노드가 최초로 발생한 시점의
노드별 잔여 에너지 그래프

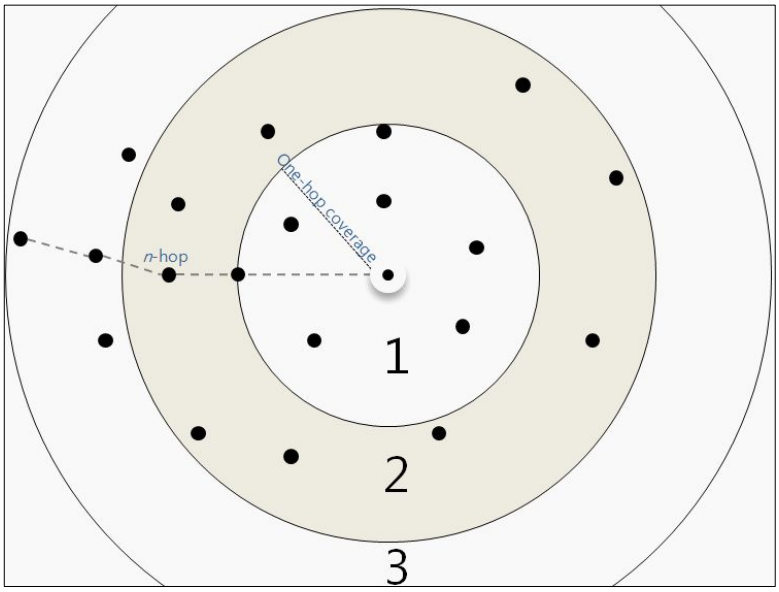
위의 그래프에 의하면 최초 에너지 고갈 노드가 발생했을 때 TEEN과 제안하는 방법이 가장 불균등한 에너지 소비를 보인다. TEEN은 데이터 수집에 있어 프로토콜 특성상 문턱값에 의해 노드의 동작이 제어되는 부분이 많다. 따라서 데이터 수집 구역 중 특정 부분에서 수집되는 데이터가 일정 시간 동안 변화가 없을 경우 노드가 동작하지 않아 이러한 에너지 불균형이 나타나는 것으로 보인다.

제안하는 방법은 가중치에 의해 노드의 역할을 할당하는 방법을 사용하므로 에너지 소비가 큰 역할을 중복하여 할당받은 노드가 낮은 확률로 발생하는 구조이다. 따라서 노드별 에너지 불균형이 나타나게 된다. 나머지 3개의 방법은 1~2J 정도로 비슷한 수준의 잔여 에너지 분포를 보인다. 그러나 노드별 에너지 불균형이 네트워크의 에너지 불균형을 의미하지는 않는다. 다음의 영역별 소비 에너지 그래프에 의하면 제안하는 방법은 매우 우수한 결과를 보인다.

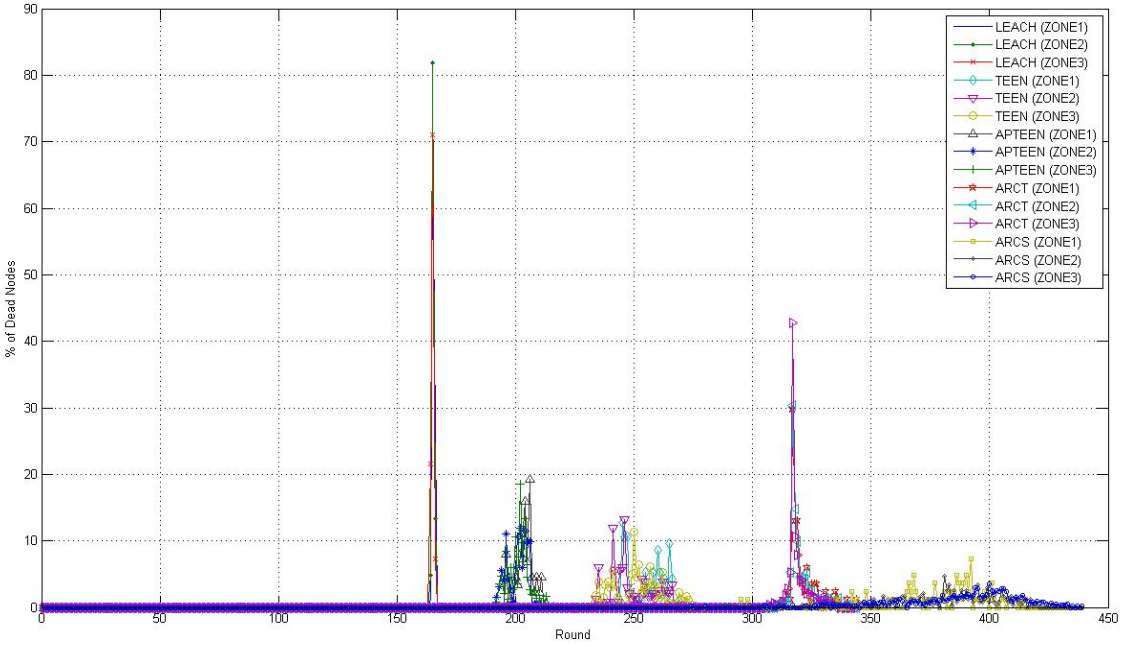
나. 영역별 소비 에너지

멀티 홉 기반 네트워크에서 전체 네트워크의 수명은 싱크 노드와 1홉 거리로 인접하는 노드들의 수명에 의해 결정된다. 이를 감안하여 싱크 노드와 인접한 노드와 그렇지 않은 노드들과의 영역별 에너지 소비 비율을 측정하기 위해 아래의 [그림 47] 과 같이 영역을 분할하였다.

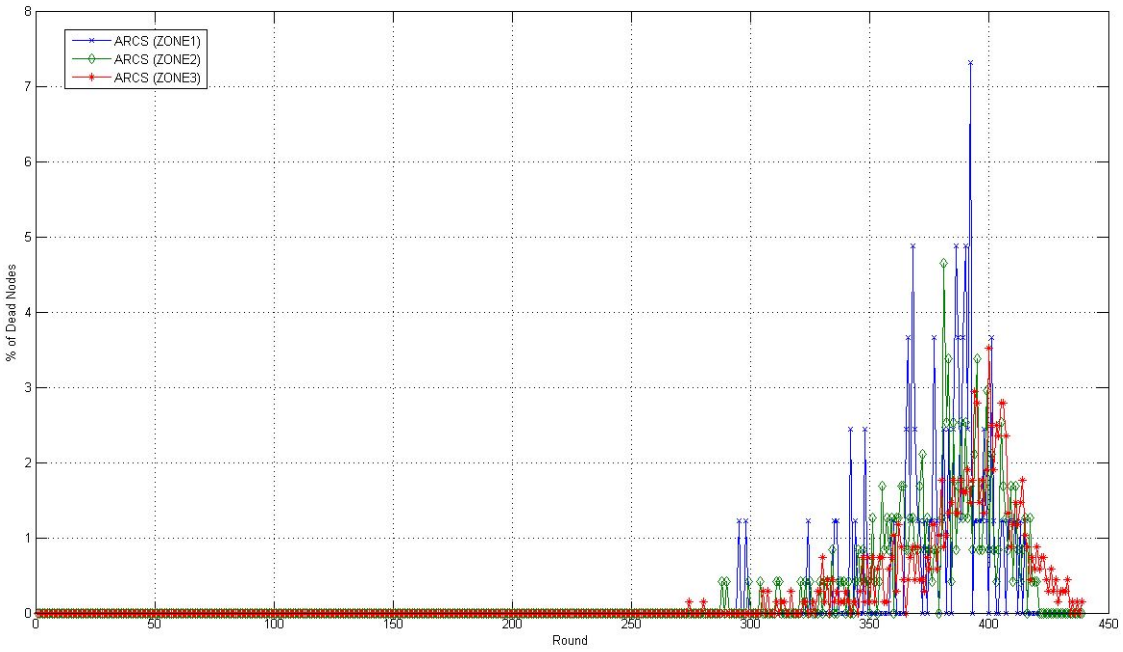
에너지 홀 문제는 싱크와 1-hop 거리 이내로 인접한 노드들에게서 주로 발생한다. 따라서 아래의 그림에서 1영역에 해당하는 부분의 에너지 소비율을 다른 영역의 에너지 소비율과 비교해 보면 네트워크의 영역별 에너지 소비율을 알 수 있다.



[그림 47] 에너지 소비 측정을 위한 영역 분할



[그림 48] 분할된 각 영역에서 측정한 사망 노드 발생 비율



[그림 49] 제안 방법의 영역별 사망 노드 발생 비율

[그림 48] 에 의하면 LEACH의 경우 모든 영역에서 약 90%의 노드들이 사망한 것을 알 수 있다. 이는 링크 단절이 발생하기 쉬운 환경을 의미하며 생존한 노드들은 네트워크를 유지하기 어렵게 된다.

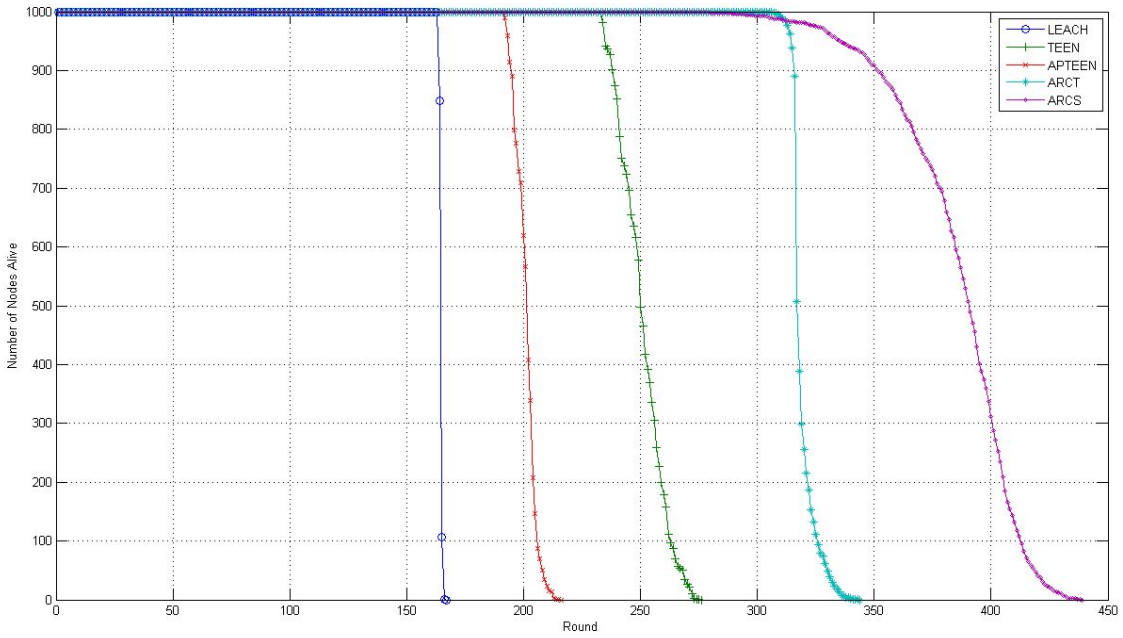
TEEN과 APTEEN의 경우, 최대 20%이내의 노드가 사망함을 알 수 있다. 이는 LEACH에 비해 네트워크 단절이 적게 발생함을 의미한다.

제안하는 방법 ARCS의 경우, 250라운드 이후부터 사망 노드가 발생함을 알 수 있다. 그러나 이 노드의 수는 극히 적어 각 영역별로 3% 이내의 발생률을 보이고 있으며, 최대 7% 이내의 노드가 사망함을 알 수 있다.

특히 [그림 49] 에 의하면 에너지 홀 문제와 네트워크 수명에 큰 영창을 미치는 1 영역에 해당되는 노드의 사망률이 7% 정도로 발생함을 알 수 있다. 이는 센서 네트워크에서 링크 단절이 발생할 확률이 낮음을 의미하며 네트워크의 수명과도 깊은 관련이 있다.

5. 네트워크 생존시간

아래의 [그림 50] 은 프로토콜별로 측정된 네트워크 수명이다. LEACH는 최초로 제안된 방법으로 가장 낮은 네트워크 생존시간을 보여주며, 반응적 네트워크인 TEEN의 경우 LEACH에 비해 2배 가까이 연장된 수명을 보여준다. APTEEN은 TEEN의 단점을 보완하는 형태로 LEACH의 고정된 주기 전송을 TEEN에 포함하여, 그 수명이 약간 짧게 나타난다. 제안한 방법의 경우 앞의 세 방법과는 다른 데이터 수집 방식을 사용하여 LEACH와 같이 고정된 주기 전송을 갖으나 ARCT와 같이 데이터 수집 영역의 노드 밀도를 낮춤으로서, 실제 데이터 전송에 참여하는 노드의 수를 줄여 네트워크의 수명이 연장되었다.



[그림 50] 프로토콜별 네트워크 생존 시간

6. 동일한 클러스터 수를 적용했을 때 비교

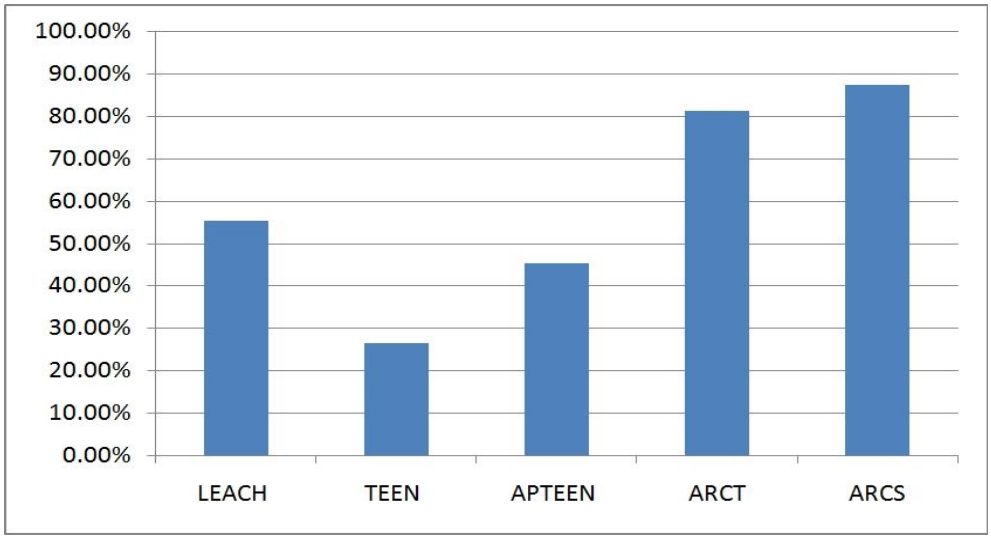
다음은 동일한 클러스터 헤드 노드의 수를 적용했을 경우에 측정되는 결과이다.

가. 수집된 데이터의 정확도 비교

아래의 [표 10] 및 [그림 51] 에 의하면 클러스터 헤드 노드의 수가 동일한 조건에서 데이터를 수집했을 경우 나타나는 데이터 수집 정확도가 상당한 차이를 보임을 알 수 있다. 이는 전송 중계노드가 없이 모든 전송 중계를 클러스터 헤드 노드에 의지하는 LEACH, TEEN, APTEEN의 특징에 의한 결과이다. ARCT 및 제안 기법은 네트워크의 크기 및 노드의 최대 전송거리에 의해 클러스터의 크기가 정해지는 특징을 갖고 있다.

[표 10] 동일한 수의 클러스터 헤드노드일 경우 수집 데이터 정확도 비교

수집 데이터 정확도 (%)				
LEACH	TEEN	APTEEN	ARCT	ARCS
55.30	26.50	45.32	81.44	87.33



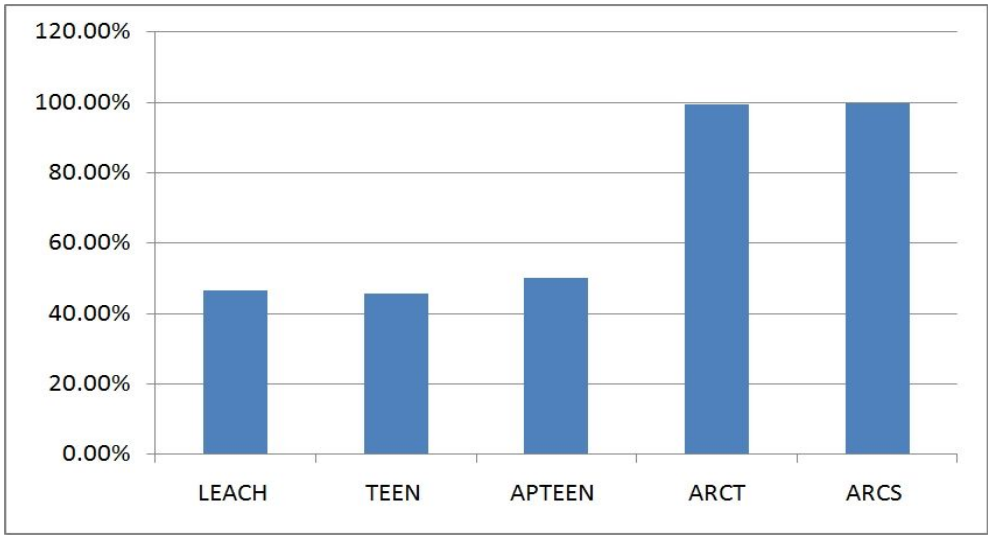
[그림 51] 동일한 수의 클러스터 헤드노드일 경우 데이터 수집률 비교

나. 네트워크 연결도 비교

네트워크 연결도 비교 결과는 아래의 [표 11] 및 [그림 52] 와 같다.

[표 11] 동일한 수의 클러스터 헤드노드일 경우 네트워크 연결도

네트워크 연결도 (%)				
LEACH	TEEN	APTEEN	ARCT	ARCS
46.71	45.79	50.11	99.59	99.67



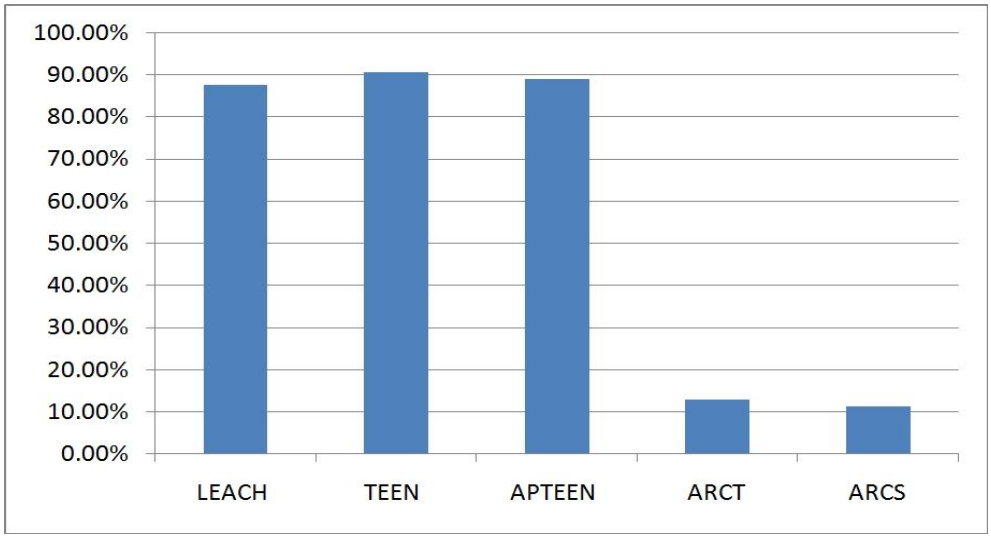
[그림 52] 동일한 수의 클러스터 헤드노드일 경우 네트워크 연결도 비교

LEACH, TEEN, 그리고 APTEEN의 경우 클러스터 헤드노드 선정 알고리즘의 선정을 위한 동작은 동일하다. 그러나 TEEN의 경우 문턱값에 의해 노드의 동작여부가 결정되는 부분이 있어 다른 두 가지 방법에 비해 낮은 네트워크 연결률을 보임을 알 수 있다. 또한 위의 세 가지 방법들은 클러스터 헤드노드가 클러스터 헤드노드간의 멀티 홉 중계 임무도 감당하고 있기 때문에 클러스터의 크기가 클러스터 헤드노드의 최대 전송거리보다 작아야 한다. 만약 클러스터의 크기가 클러스터 헤드노드의 최대전송거리와 같다면 해당 클러스터는 네트워크와 단절된다.

다. 고립노드 발생 비율

[표 12] 동일한 수의 클러스터 헤드노드일 경우 고립노드 발생 비율

고립노드 발생 비율 (%)				
LEACH	TEEN	APTEEN	ARCT	ARCS
87.60%	90.70%	89.05%	12.80	11.30



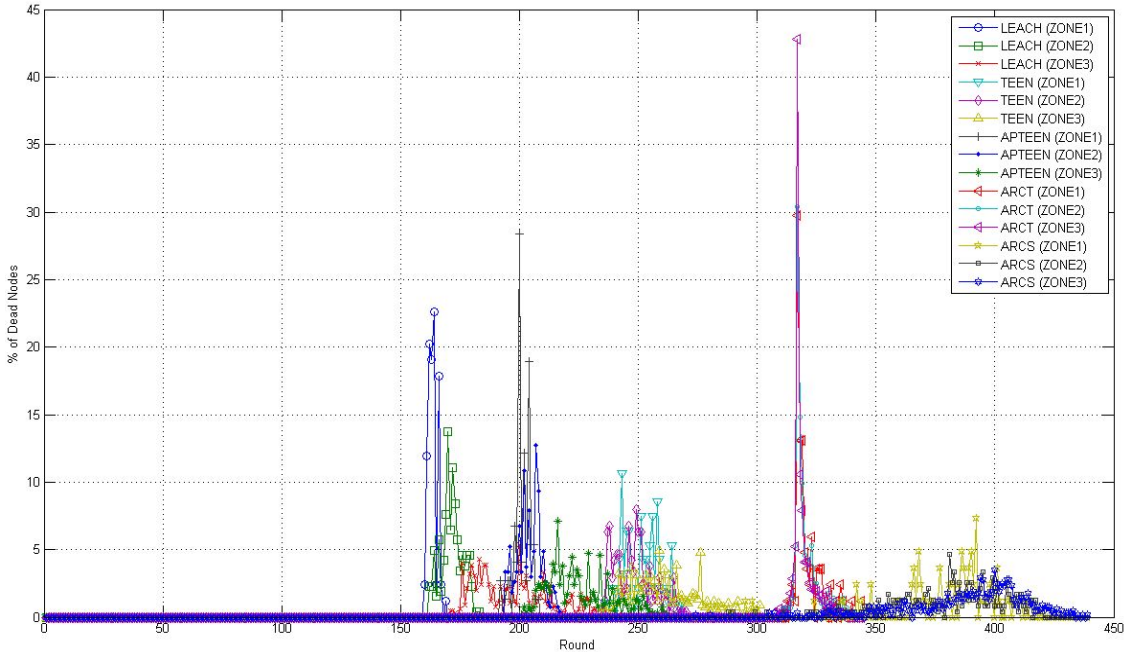
[그림 53] 동일한 수의 클러스터 헤드노드일 경우 고립노드 발생 비율

결과적으로 적은 수의 클러스터 헤드 노드로 전체 네트워크를 관리하기에는 문제가 발생한다. 따라서 위의 세 가지 기법, LEACH, TEEN, 그리고 APTEEN은 네트워크 연결에 문제가 있으며 네트워크 연결이 불안전해지면 네트워크에 참여하지 못하고 고립되는 노드 또한 많아지고 횟수 또한 빈번하게 발생하게 된다.

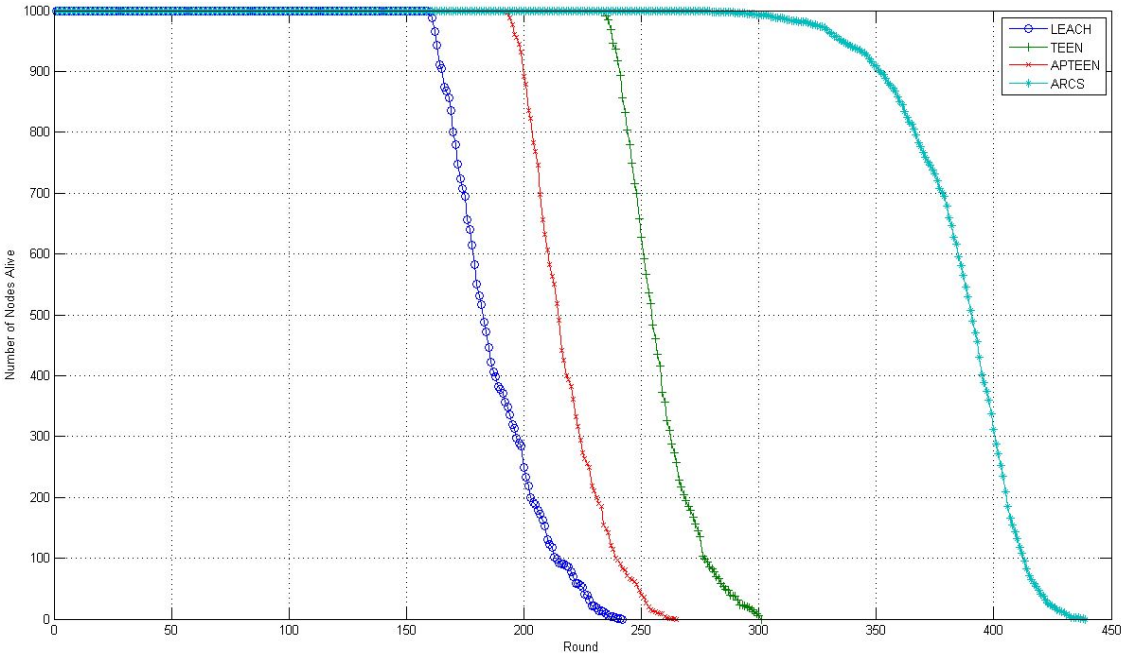
라. 영역별 소비 에너지 비교

아래의 [그림 54] 의 결과에 의하면 LEACH, TEEN, APTEEN은 선정되는 클러스터 헤드 노드의 수가 기존에 비해 1/4 이하로 줄어들었으므로 상대적으로 노드의 부하가 많이 줄어들었다. 따라서 에너지가 고갈되는 노드의 비율은 이전에 비해 많이 줄어든 것을 확인할 수 있다. 그러나 LEACH와 APTEEN의 경우 제 1영역에서 멀티홉 중계를

담당하는 노드들의 대다수가 다른 영역에 비해 높은 비율로 사망하는 것을 알 수 있다. 이는 2,3영역의 에너지 소비는 많이 낮추었으나 1영역의 에너지 소비로 인해 에너지 홀이 발생할 확률이 높아 네트워크가 안정적으로 유지되지 못할 가능성이 높음을 의미한다.



[그림 54] 동일한 수의 클러스터 헤드노드일 경우 영역별 사망노드 발생 비율



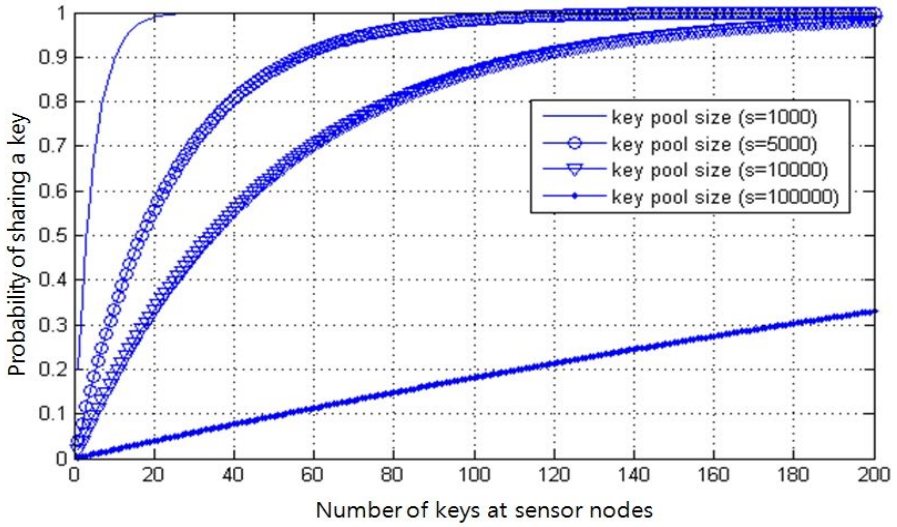
[그림 55] 동일한 수의 클러스터 헤드노드일 경우 네트워크 수명 비교

위의 [그림 55] 는 동일한 클러스터 헤드 노드 수를 적용했을 경우 측정된 네트워크 수명을 나타낸다. 결과 그래프에 의하면 기본 클러스터 헤드 노드 수를 적용한 이전의 LEACH, TEEN, APTEEN에 비해 수명이 연장된 것을 볼 수 있다. 그러나 연장된 수명이 비해 낮은 네트워크 연결도와 데이터 수집률, 그리고 높은 비율의 고립노드 발생율과 1영역에서의 높은 노드사망률로 인해 단순히 네트워크의 수명 증가만으로는 프로토콜의 성능을 측정할 수 없음을 알 수 있다.

제3절 키 관리 기법 안전성 평가

1. 노드간 연결도

확률기반 키 분배 기법들은 [그림 56] 에서 보이는 바와 같이 키 풀에서 임의로 선택된 서브키 셋을 노드들에게 분배하는 기법을 사용하므로 전체 네트워크에 분포된 모든 노드들에 대해 완벽한 연결을 보장할 수 없다.



[그림 56] 확률기반 기법에서 노드 사이에 1개의 키를 공유할 확률

2. 오버헤드

· 노드의 키 저장 오버헤드

확률기반 키 분배 기법에서 메모리 오버헤드 C는 s'를 노드에 할당되는 subset의 크기로 가정하면 다음의 식 $C = s'(t+1)\log_2 q$과 같다.

· 키의 갱신 오버헤드

동일한 다항식을 사용하여 polynomial share를 생성한 노드들이 해당된다.

· 노드의 키 계산 오버헤드
클러스터를 구성하는 센서 노드의 수를 클러스터에 할당된 t차 이변 다항식의 차수를 넘지 않도록 제한한다면 이웃 노드의 수를 최대 t-1개까지 제한할 수 있으므로 작은 오버헤드를 가진다.

3. 키의 견고성

임의의 t차 이변 다항식을 사용한 키 생성 및 분배 방법을 사용하는 모든 방법들은 노드의 ID를 이용하여 polynomial share를 생성하고 이 polynomial share에 상대 노드의 ID를 입력하여 pair-wise key를 생성한다. 이러한 기법은 t차 이변 다항식의 차수 t개 까지는 노드가 노출되어도 다항식이 노출되지 않으며 t+1개가 노출되었을 때 다항식이 노출된다.

4. 키의 노출시 피해범위

동일한 키를 가지고 있는 노드들은 동일한 다항식을 사용하므로 다항식의 노출 피해범위에 해당된다.

5. 노드 포획에 대한 안전성

앞의 조건에 의해 t차 이변 다항식의 차수 t개 까지는 노드가 노출되어도 다항식이 노출되지 않으며 t+1개가 노출되었을 때 다항식이 노출된다.

한 개의 클러스터에 위치한 노드의 개수 N_c가 다음과 같을 때

$$N_c = N_d a^2 = \frac{(m+1)a^2}{\pi R^2} \tag{27}$$

이므로, 특정 클러스터에 위치하며 다항식을 공유할 센서노드의 수 N_s는 전송 범위를 기본 단위로 놓았을 때 공유하는 polynomial의 개수에 대해 공유하는 클러스터를 입력한 아래의 식으로 나타낼 수 있으며 N_s의 개수를 t개까지 제한하면 다항식의 노출시 사용되는 다항식에 대한 안전성을 갖는다.

$$N_s = \frac{C_s(m+1)a^2}{\pi} \quad < (t+1) \tag{28}$$

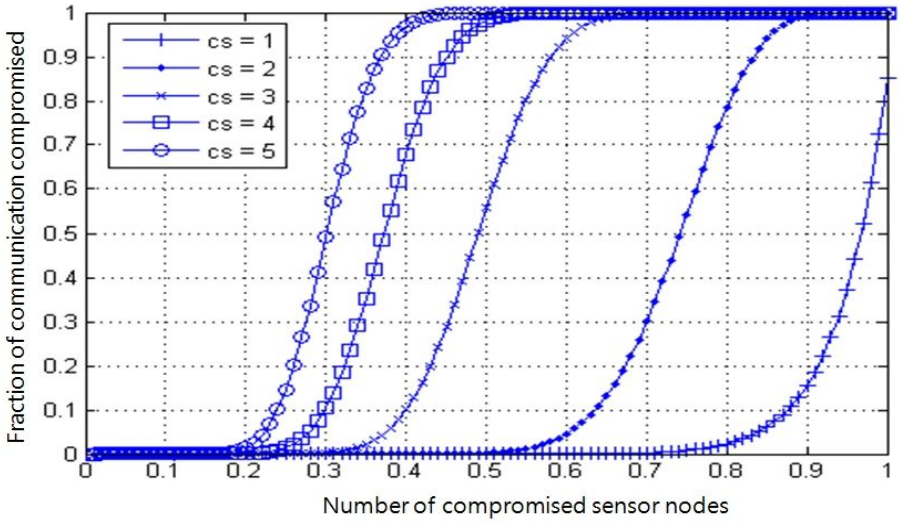
공격자에 의해서 노출되는 네트워크의 센서 노드의 비율을 p_c라고 가정하자. 이것은 각각의 센서 노드가 노출될 확률 p_c를 가지고 있는 것을 의미한다. 그러므로 특정한 클러스터에서 같은 다항식을 공유하는 센서 중 i개 센서가 노출될 확률은 다음과 같다.

$$P_c(i) = \frac{N_s!}{(N_s-i)!i!} p_c^i (1-p_c)^{N_{s-i}} \tag{29}$$

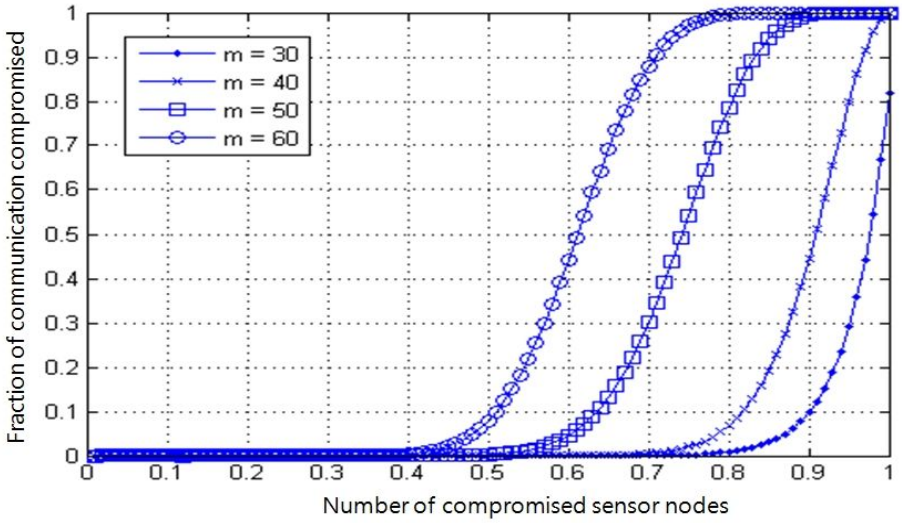
따라서 이 클러스터에 할당된 다항식이 노출된 확률은 전체에서 노출된 노드에 할당된 다항식을 제하므로 다음과 같다.

$$P_c = 1 - \sum_{i=0}^{t} P_c(i) \tag{30}$$

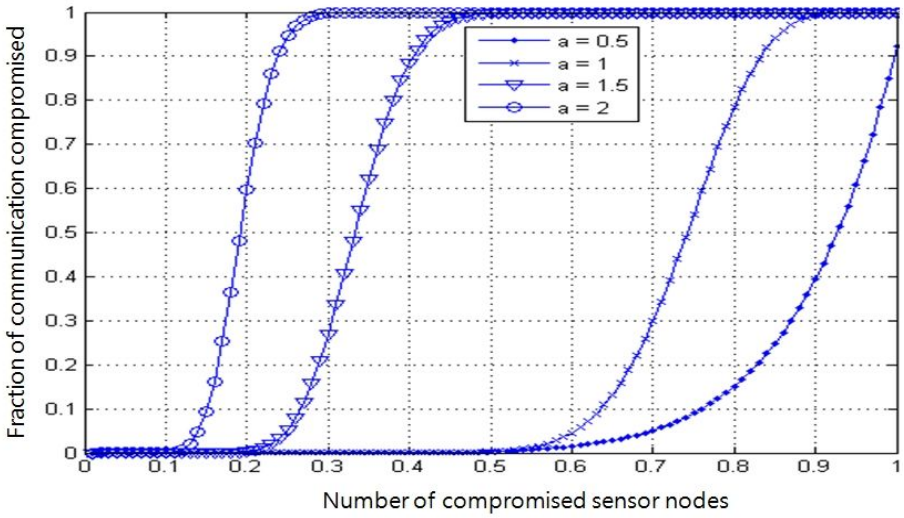
다음의 [그림 57] 은 포획된 노드의 비율과 노출된 키의 비율에 대한 관계를 나타낸다.



(a) a=1, m=50



(b) a=1, C_s=2



(c) m=50, C_s=2

[그림 57] 포획된 노드와 노출된 키의 관계

a는 클러스터의 크기를 나타내며, C_s는 다항식을 공유하는 클러스터의 개수를, m은 노드의 수를 나타낸다. 위의 그래프에서 우리는 다항식을 공유하는 클러스터가 적을수록, 노드의 수가 적을수록, 클러스터의 크기가 작을수록 더 견고함을 알 수 있다. 특히 (a)의 공유하는 클러스터에 따른 견고성의 변화그래프는 인접 셀과 동일 다항식을 공유하는 기존의 셀 기반 기법들에 취약점이 된다.

제안하는 기법은 BS로부터 받은 다항식을 인접노드와 키 공유에 사용하므로 공유하는 클러스터에 대해 키 누출위험을 감소시킬 수 있다. 아래의 [표 13] 은 제안하는 기법의 안전성에 대해 비교한 비교표이다.

[표 13] 제안하는 방법의 안전성 및 효율 비교

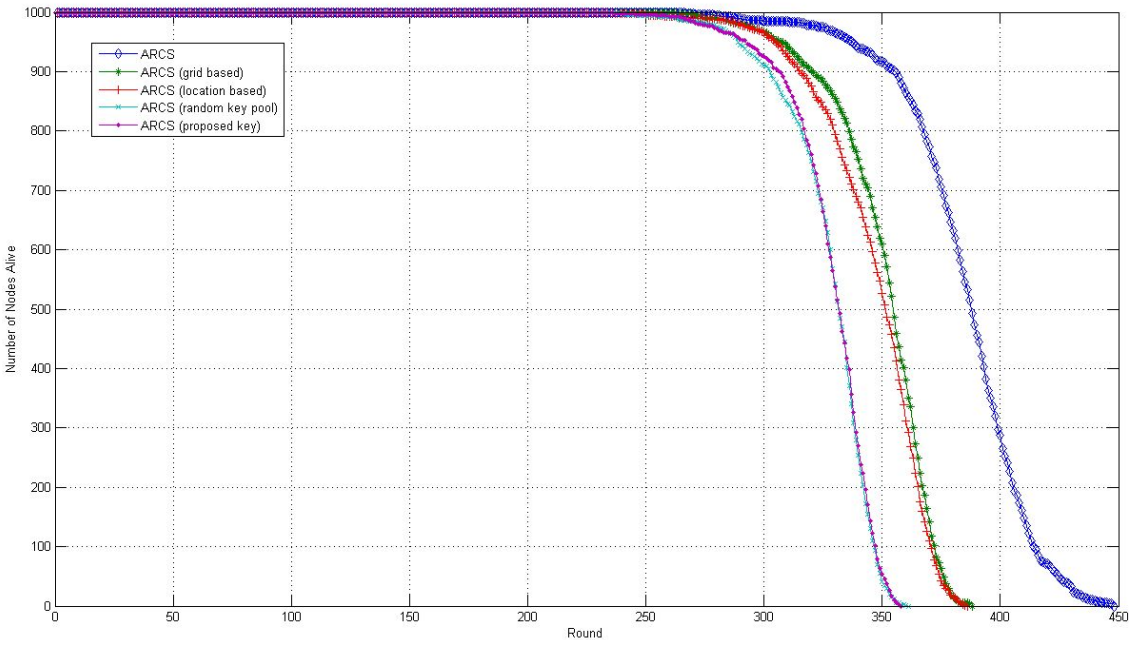
항목	Random (pool) [6]	Polynomial (pool) [9]	Polynomial (Grid) [9]	Polynomial (Location) [12]	Polynomial (Location) [13]	Proposed Scheme
pair-wise key 설정확률	0.99	0.99	1	1	1	0.99
키 유도 방식	키	t차 이변 다항식	t차 이변 다항식	t차 이변 다항식	t차 이변 다항식	t차 이변 다항식
최대 노출키 수 (키 노출에 따른 견고성)	1개	t(다항식의 차수)+1개	t(다항식의 차수)+1개	t(다항식의 차수)+1개	t(다항식의 차수)+1개	t(다항식의 차수)+1개
키의 노출 피해범위	동일키 공유 센서	동일 다항식 공유 센서	전체 네트워크의 동일 다항식을 사용한 행, 열	5개 셀 (홈 셀과 인접 4개 셀)	8개 셀	동일 다항식 공유 센서
키의 갱신 오버헤드	동일키 사용 센서	동일 다항식 사용 센서	동일 다항식을 사용한 행, 열	5개 셀 (홈 셀과 인접 4개 셀)	8개 셀	동일 다항식 사용 센서
노드의 저장 오버헤드	임의의 개수의 키	임의의 개수의 polynomial share	2개의 polynomial share	5개의 polynomial share	8개의 polynomial share	임의의 개수의 polynomial share +1 or +2
노드의 키 계산 오버헤드	없음	이웃 노드수(전체 네트워크) X 다항식 부분정보 계산량	이웃 노드수(전체 네트워크) X 다항식 부분정보 계산량	이웃 노드수(전체 네트워크) X 다항식 부분정보 계산량	이웃 노드수(전체 네트워크) X 다항식 부분정보 계산량	이웃 노드수(단일 클러스터 내) X 다항식 부분정보 계산량
Base station 인증	최초 1회	최초 1회	최초 1회	최초 1회	최초 1회	최초 1회, 매 라운드 1회

6. 네트워크 수명

키 분배 및 인증 기법이 네트워크 수명에 미치는 영향을 알아보기 위해 랜덤 키 풀 기반 기법, 그리드 기반 기법, 위치 기반 기법을 제안하는 라우팅 기법에 적용하여 실험하였다. 위의 세 가지 기법 중 그리드와 위치 기반 기법은 베이스 스테이션에 의한 사전 키 분배 및 위치 선정이 끝난 상태를 전제 조건으로 하여 실험하였다.

아래의 [그림 58] 에 의하면 제안하는 키 관리 및 인증 기법은 다른 기법을 적용한

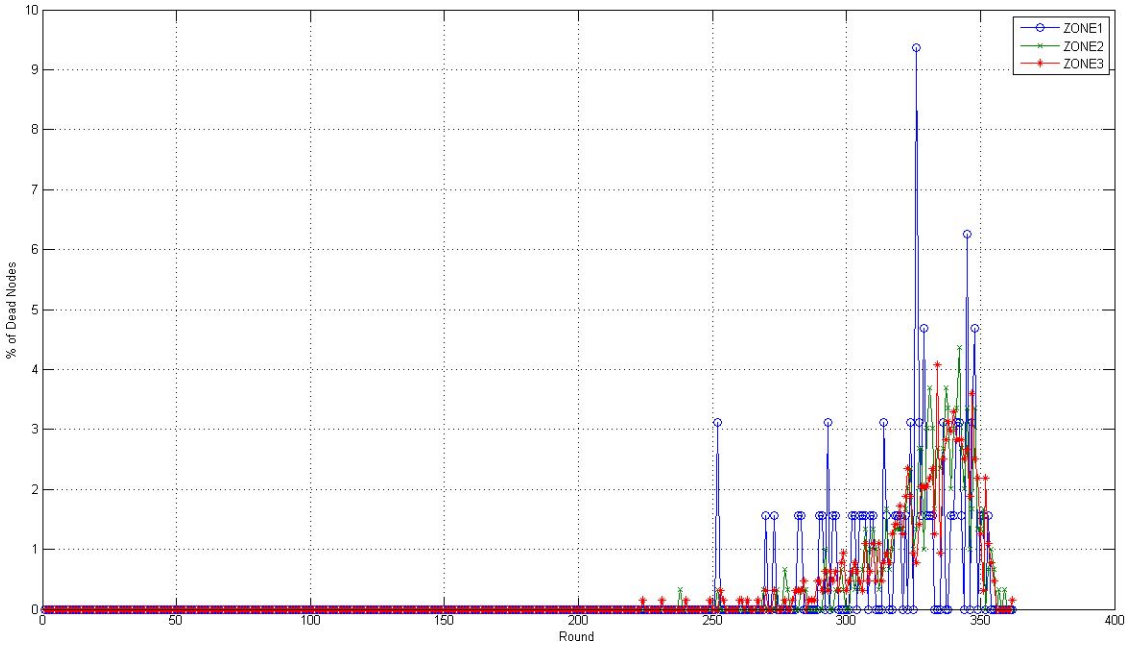
결과와 비교하여 볼 때 랜덤 키 기반 기법에 약간 못 미치는 수명을 나타내며 그리드 기법에 비해 최대 9% 정도의 수명 손실을 보임을 알 수 있다. 또한 이 기법은 키 관리 기법을 적용하지 않은 ARCS 기법에 비해 약 20%낮은 네트워크 수명을 나타내며 이는 베이스 스테이션에 의한 노드의 인증 절차가 포함되어 있기 때문으로 보인다. 이상의 실험 결과에 의하면 제안하는 키 분배 및 인증 방법의 장점은 다음과 같다. 먼저, 노드의 키 분배 및 키 성립 과정에 있어 BS의 개입이 필요하지 않다. 이는 그리드와 위치 기반 방법들이 요구하는 BS의 개입이 필요하지 않음을 의미한다. 따라서 노드의 자원이 낭비되지 않는다. 그리고 라운드의 변경시 매번 셋업 단계에서 상위 레벨의 노드에 대한 인증이 이루어진다. 이는 다른 기법들이 고려하지 못한 클러스터 네트워크의 특성을 고려한 것이다. 또한, 클러스터 단위에서 사용하는 키는 BS로부터 재분배 받는 과정을 거치므로 다른 기법에서 사용하는 키를 이용한 클러스터 형성보다 외부 공격에 대해 안전하다. 비록 주기적인 노드의 인증, 그리고 확률기반 키 분배에 의한 최대 9%의 에너지 손실이 있다 하더라도 안전한 네트워크 유지를 고려한다면 제안하는 방법은 다른 방법들에 비해 우월한 결과를 보임을 알 수 있다.



[그림 58] ARCS 기법에 적용시 네트워크 수명 변화 비교 그래프

7. 영역별 소비에너지

아래의 [그림 59] 에 의하면 제안하는 방법은 특정 라운드에서 발생한 9%대의 사망노드 발생률을 제외한 노드 사망의 평균값이 키 관리 기법을 적용하지 않은 ARCT에 크게 다르지 않은 결과를 보이는 것을 알 수 있다. 그러므로 부하 분산이 이루어진 ARCS에 제안하는 키 관리 기법을 적용하는데 큰 문제가 없음을 알 수 있다.



[그림 59] 보안 기법 적용시 제안하는 방법의 영역별 사망 노드 발생비율

8. 취약한 공격에 대한 저항성

Selective forwarding

- Selective forwarding을 위해 공격 노드가 발생하는 조건을 고려하면, 일반 노드의 경우 베이스 스테이션의 인증을 거치지 않으므로 발생 가능하며 이때 공격 가능한 범위는 클러스터 내부가 될 수 있다. 그러나 이때에도 베이스 스테이션의 인증을 받는 클러스터 헤드 노드의 인증을 거쳐야 하기 때문에 노드의 모든 키와 포인터 정

보가 누출되지 않는다면 해당 공격은 불가능하며, 발생할 경우에도 단일 클러스터 영역 내부로 제한된다.

HELLO flood attack

- 네트워크 노드의 경쟁기반 셋업에서 HELLO flood attack 이 발생할 경우 유출된 키와 동일 정보를 공유하는 네트워크의 모든 노드는 sleep 모드로 전환하여 네트워크에 참여하지 않는다. 또한, 다항식 기반 키를 이용하므로 t+1개의 키가 노출되지 않는다면 공격으로부터 안전하게 된다. 네트워크 셋업 이후는 베이스 스테이션의 인증을 거치므로 사실상 불가능하다.

Sybil attack

- 셋업 구간에서 공격이 발생할 경우, 네트워크 셋업이 노드의 시간 경쟁에 기초하므로 공격이 제한된다. 또한 베이스 스테이션의 인증을 받은 클러스터 헤드 노드의 인증 절차가 있으므로 공격이 불가능하다.

제5장 결 론

센서 네트워크의 클러스터링 방법에 대한 연구는 상당부분 진행되었으며 실제적인 응용에 맞춘 연구가 필요하다. 이에 본 연구는 클러스터링을 이용한 센서 네트워크를 실제 환경 감시 네트워크에 적용했을 때 발생하는 문제들과 이에 대한 보완을 다루었으며 해당 응용에 효과적인 클러스터링 기법을 제안하였다. 에너지 효율 면에서 보았을 때, 성능평가 결과에 의하면 제안한 방법에서 제시한 2가지의 클러스터를 이용한 클러스터링 방법은 기온 측정 분야에 적용할 경우 기존 방법에 비해 높은 정확도, 높은 연결도, 낮은 오류율, 긴 네트워크 수명을 제공함을 알 수 있다. 그러나 제안한 방법은 기온 데이터의 특성에 맞추어 이에 대해 최적화를 한 방법이므로 다른 형태의 데이터 수집에 동일한 결과를 낼 수는 없을 것으로 본다. 가장 중요한 점은 환경 감시를 목적으로 하는 센서 네트워크의 프로토콜 설계에 있어 수집 데이터의 특성과 환경을 사전에 파악하는 것이 센서 네트워크의 성능 향상에 미친다는 것이다. 또한, 무선 센서 네트워크에서 에너지 효율과 보안은 개별적으로 생각할 수 없다. 따라서 위와 같은 클러스터 네트워크의 키 분배 방법을 제안하게 되었다.

이 기법은 t차 2변 다항식의 polynomial share를 이용한 키 선분배 기법으로 클러스터 네트워크의 주기적인 노드의 연결을 쉽게 이루고, 여기에 신뢰할만한 베이스 스테이션에 의한 클러스터 헤드 노드 및 리피터 노드의 인증을 매 라운드마다 반복함으로써 안전한 클러스터의 유지가 가능하게 되었으며, 각 클러스터에 사용하는 개별 키를 할당함으로써 클러스터 내 보안이 향상되었다. 또한 클러스터 헤드 노드들 사이의 멀티홉 전송에 사용되는 키를 별개로 지정하여 클러스터 헤드 노드의 멀티홉 전송에 발생할 수 있는 외부 공격에 대한 보안성을 향상시켰다.

따라서 기존의 그리드 기반 키 분배 방법이나 위치 기반 키 분배 방법, 고정 클러스터 기반 키 분배 방법들을 고려하면 에너지 보존이나 클러스터 내 보안의 향상에 있어 상대적으로 우수함을 알 수 있다.

연구 결과에 의하면 향후 다음과 같은 연구가 필요함을 알 수 있었다.

첫째, 센서 네트워크는 응용환경의 영향을 많이 받는 네트워크에 속한다. 취급하는 데이터의 특성과 네트워크의 환경을 고려하는 라우팅 설계가 해당 응용환경에 최적화된 라우팅 프로토콜 설계에 큰 비중을 차지한다. 센서 네트워크를 응용 환경에 최적화하는 것이 우선적인 목표가 될 수 있으나, 범용으로 사용이 가능하고 다양한 응용환경을

감안한 환경변수를 두어 이를 네트워크 구성에 적용하는 방법도 충분히 고려가 가능하다. 일례로 산불 감시나 물체 추적 등 노드들이 실시간으로 특정지역에서 발생하는 일을 오차 없이 전송해야하는 경우, 그리고 기상감시와 같이 어느 정도 느슨한 데이터 수집이 허용되는 경우와 같이 서로 상반된 응용환경에서도 사용자가 조정이 가능한 환경 변수값에 의해 네트워크 구조를 쉽게 변경할 수 있는 네트워크 라우팅 기법에 대한 연구가 필요하다. 둘째, 보안의 측면에서 네트워크 구조의 변경은 보안의 구조 또한 변경됨을 의미한다. 변경이 가능한 네트워크의 구조에 대한 사전연구를 통해 해당 구조들에 최적화된 보안 기법을 연구하여 네트워크 구조가 변경될 때 유동적으로 변경 가능한 보안 기법의 연구가 필요하다. 셋째, 센서 네트워크 라우팅 프로토콜을 실제 환경에서 적용하여 검증하는 작업이 필요하다 .

참고 문헌

[1] 정보통신부, 정보통신연구진흥원, “RFID/USN 기술로드맵”, ITRM2012, January 2007.

[2] S. A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," *Rensselaer Polytechnic Inst., Comput. Sci. Dept., Troy, NY, Technical Report TR-05-07*, 2005.

[3] J. Kahn, R. Katz, and K. Pister, "Next Century Challenges: Mobile Networking for Smart Dust," *Proceedings of IEEE International Conference on Mobile Computing and Networking*, pp. 271-278, 1999.

[4] D. Ganesan, B. Krishnamachari, A. Woo, D. Culler, D. Estrin, and S. Wicker, "Complex Behavior at Scale: An Experimental Study of Low-Power Wireless Sensor Networks," *UCLA CS Technical Report UCLA/CSD-TR02-0013*, 2002.

[5] B. Krishnamachari, *Networking Wireless Sensors*, Cambridge University Press, 2005.

[6] G.J. Pottie and W.J. Kaiser, "Wireless Integrated Network Sensors," *Communications of ACM*, vol.43, no.5, pp. 51-58, 2000.

[7] Y. Yao and J. Gehrke, "Query Processing for Sensor Networks," *Proceedings of the 2003 CIDR Conference of Linux or Windows CE .NET*, pp. 491-502, 2003.

[8] R. J. Watro, D. Kong S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: Securing Sensor Networks with Public Key Technology," *In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004)*, pp. 59-64, October 2004.

[9] D. W. Carman, P. S. Kruus, and B. J. Matt, Constraints and Approaches for Distributed Sensor Network Security, *NAI Labs Technical Report #00-010, 3060 Washington Road (Rt. 97) glenwood*, 2000.

[10] 임채훈, “유비쿼터스 센서 네트워크 보안”, 한국통신학회지(정보통신), 제22권, 제8호, pp. 35-50, 2005.

[11] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks:

Attacks and Countermeasures," *First IEEE International Workshop on Sensor Network Protocols and Applications*, pp.113-127, May 2003.

[12] J. Al-karaki and A. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Communications,* vol. 11, pp. 6-28, December 2004.

[13] Y. Tseng, S. Ni, Y. Chen, and J. Sgeu, "The Broadcast Strom Problem in a Mobile Ad Hoc Network," *The Journal of Mobile Communication Computation and Information*, vol. 8, no1-2, pp.153-167, 2002.

[14] Jian Li and Mohapatra, P. "An analytical model for the energy hole problem in many-to-one sensor networks," *Proceedings of Vehicular Technology Conference 2005 IEEE 62nd*, vol.4, pp. 2721-2725, 2005.

[15] X. Wu, G. Chen and S. Das, "Avoiding Energy Holes in Wireless Sensor Networks with Nonuniform Node Distribution," *IEEE Transactions on Parallel and Distributed Systems*, Vol.19, No.5, pp. 710-720, 2008.

[16] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: a Scalable and Robust Communication Paradigm for Sensor Networks," *Proceedings od ACM Mobi-Com 2000, Boston, MA*, pp. 56-67, 2000.

[17] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," *Proceedings of 5th ACM/IEEE Mobicom, Seattle, WA*, pp. 174-185, August 1999.

[18] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks," *Wireless Networks*, vol. 8, pp. 169-185, 2002.

[19] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," *Proceedings of 1st Wksp. Sensor Networks and Apps., Atlanta, GA*, pp.1528-1545 October 2002.

[20] F. Ye et al., "A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks," *Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on*, pp. 304-309, 2001.

[21] C. Schurgers and M.B. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks," *itary Communications Conference, 2001. MILCOM 2001.*

Communications for Network-Centric Operations: Creating the Information Force. IEEE, vol. 1, pp.351-361, October 2001.

[22] M. Chu, H. Haussecker, and F. Zhao, "Scalable Information Driven Sensor Querying and Routing for Ad Hoc Heterogeneous Sensor Networks," *International Journal of High Performance Computing Applications*, vol. 16, no. 3, August 2002.

[23] Y. Yao and J. Gehrke, "The Cougar Approach to Innetwork Query Processing in Sensor Networks," *SIGMOD Record*, vol. 31, no. 31, pp. 9-18, September 2002.

[24] S. Servetto and G. Barrenechea, "Constrained Random Walks on Random Graphs: Routing Algorithms for Large Scale Wireless Sensor Networks," *Proceedings of 1st ACM International Workshop. Wireless Sensor Networks and Apps., Atlanta, GA,* pp. 12-21, 2002.

[25] N. Sadagopan et al., "The ACQUIRE Mechanism for Efficient Querying in Sensor Networks," *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, pp.149-155, May 2003.

[26] R. C. Shah and J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE,* pp.350-355, March 2002.

[27] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, vol. 2, pp.10 ,January 2000.

[28] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *in IEEE Transactions on Wireless Communications*, vol. 1, pp. 660-670, October 2002.

[29] S. Lindsey, C. Raghavendra, and K. M. Sivalingam, "Data Gathering Algorithms in Sensor Networks using Energy Metrics," *IEEE Transactions Parallel and Distributed System*, vol. 13, no. 9, pp. 924-935, September

2002.

[30] O. Younis and S. Fahmy, "Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach," *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, pp. 629-640, 2004.

[31] S.D. Muruganathan at al., "A centralized energy-efficient routing protocol for wireless sensor networks," *IEEE Communications Magazine*, vol. 43, pp. s8-s13, March 2005.

[32] A. Manjeshwar and D. P. Agarwal, "TEEN: a Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," *Parallel and Distributed Processing Symposium., Proceedings 15th International*, pp.30189a ,April 2001.

[33] A. Manjeshwar and D. P. Agarwal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," *Parallel and Distributed Processing Symposium., Proceedings International, IPDPS 2002,* pp. 195-202, 2002.

[34] D. Choi, S. Moh, and I. Chung, "Variable Area Routing Protocol in WSNs: A Hybrid, Energy-Efficient Approach," *High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on*, pp. 397-403, 2008.

[35] D. Choi and I. Chung, "An Analysis of Threshold-Sensitive Routing Protocol in Wireless Sensor Networks," *Proc. of the 21st IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS 2009),* pp.158-164, November 2009.

[36] D. Choi, S. Moh, and I. Chung, "Regional Clustering Scheme in Densely Deployed Wireless Sensor Networks for Weather Monitoring Systems," *High Performance Computing and Communications (HPCC), 2010 12th IEEE International Conference on*, pp. 497-502, 2010.

[37] V. Rodoplu and T. H. Meng, "Minimum Energy Mobile Wireless Networks," *ISelected Areas in Communications, IEEE Journal on*, vol. 17, no. 8, pp. 1333-1344, August 1999.

[38] L. Subramanian and R. H. Katz, "An Architecture for Building Self

Configurable Systems," *Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC. 2000 First Annual Workshop on*, pp. 63-73, August 2000.

[39] Q. Fang, F. Zhao, and L. Guibas, "Lightweight Sensing and Communication Protocols for Target Enumeration and Aggregation," *MobiHoc '03 Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pp. 165-76, 2003.

[40] J. N. Al-Karaki et al., "Data Aggregation in Wireless Sensor Networks — Exact and Approximate Algorithms," *High Performance Switching and Routing, 2004. HPSR. 2004 Workshop on*, pp. 241-245, 2004.

[41] Q. Li, J. Aslam, and D. Rus, "Hierarchical Power-Aware Routing in Sensor Networks," *Proceedings of the DIMACS Workshop on Pervasive Networking*, May 2001.

[42] F. Ye et al., "A Two-Tier Data Dissemination Model for Large-Scale Wireless Sensor Networks," *MobiCom '02 Proceedings of the 8th annual international conference on Mobile computing and networking,* pp. 148-159, 2002.

[43] Y. Xu, J. Heidemann, and D. Estrin, "Geographyinformed Energy Conservation for Ad-hoc Routing," *Proceedings of 7th Annual ACM/IEEE International Conference Mobile Comp. and Net.*, pp. 70-84, 2001.

[44] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," *UCLA Comp. Sci. Dept. technical report, UCLA-CSD TR-010023,* May 2001.

[45] I. Stojmenovic and X. Lin, "GEDIR: Loop-Free Location Based Routing in Wireless Networks," *International Conference Parallel and Distrib. Comp. and Sys., Boston, MA,* pp. 3-6, November 1999.

[46] F. Kuhn, R. Wattenhofer, and A. Zollinger, "Worst-Case Optimal and Average-Case Efficient Geometric Ad Hoc Routing," *Proceedings of 4th ACM International. Conference Mobile Comp. and Net.*, pp. 267-78, 2003.

[47] B. Chen et al., "SPAN: an Energy-efficient Coordination Algorithm for Topology Maintenance in Ad-Hoc Wireless Networks," *Wireless Networks*,

vol. 8, no. 5, pp. 481-94, September 2002.

[48] D. Raymond et al., "Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols," *Proceedings of 7th Annual IEEE systems, Man, and Cybernetics (SMC) Information Assurance Workshop(IAW), IEEE Press*, pp. 297-304, 2006.

[49] D. Raymond and S. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," *IEEE Pervasive Computing*, Vol.7, No.1, pp.74-81, 2008.

[50] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor netwroks: analysis & defenses," *Proceedings of the third international symposium on Information processing in sensor netwroks, ACM Press*, pp.259-268, 2004.

[51] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis in wireless sensor networks," *Technical Report CU-CS-987-04, University of Colorado at Boulder*, 2004.

[52] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor netwroks," *Proceedings of IEEE Symposium on Security and Privacy*, pp. 49-63, May 2005.

[53] H. Chan and A. Perrig, "Security and Privacy in sensor networks," *IEEE computer Magazine*, pp.103-105, 2003.

[54] A. Perrig and R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "SPINS: Security Protocols for Sensor Networks," *Proceedings of the 7th ACM/IEEE International Conference on MobiCom*, pp. 156-163, 2001.

[55] S. Zhu, S. Setia, and S. Jaodia, "LEAP: efficient security Mechanisms for Large Scale Distributed Sensor Netwroks," *Proceedings of the 10th ACM Conference on Computer and Communication Security(CCS),* pp.62-72, October 2003.

[56] R. Anderson, H. Chan, and A. Perrig, "Key Infection : Smart Trust for Smart Dust", *Proceedings of the 12th IEEE International Conference on*, pp. 206-215, 2004.

[57] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed

sensor networks," *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41-47, 2002.

[58] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *IEEE Symposium on Security and Privacy,* pp. 197-213, 2003.

[59] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine*, Vol. 44, pp. 122-130, 2006.

[60] D. Liu and P. Ning, "Location-Based pair-wise Key Establishments for Relatively Static Sensor Networks," *First ACM Workshop on the Security of Ad-Hoc and Sensor Networks*, pp. 72-82, 2003.

[61] D. Malan, M. Welsh, and M. D. Smith, "A Public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," *2004 First Annual IEEE Communications Society Conference on*, pp.71-80, October 2004.

[62] N. Canh, T. Phuong, Y. Lee, S. Lee, and H. Lee, "A Location-aware Key Predistribution Scheme for Distributed Wireless Sensor Networks," *Proceedings of the 15th IEEE International Conference on*, pp. 188-193, 2007.

[63] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D. Culler, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, Vol. 8, No.5, pp. 521-534, 2002.

[64] M. Rajiullah and S. Shimamoto, "An Energy-Aware Periodical Data Gathering Protocol Using Deterministic Clustering in Wireless Sensor Networks (WSN)," *Proceedings of Wireless Communications and Networking Conference*, pp. 3014-3018, 2007.

[65] J. Hill and D. Culler, "A wireless-embedded Architecture for System Level Optimization," *UC Berkeley Technical Report*, 2002.

[66] W. Ye, J. Heidemann, and D. Estrin, "An Energy Efficient MAC Protocol for Wireless Sensor Networks," *Proceedings of INFOCOM 2002*, Vol.3, pp. 1567-1576, 2002.

[67] Crossbow, "MPR-MIB Users Manual," www.cs.ucsb.edu/~nchohan/docs/moteManual.pdf, June 2007.

[68] Maxfor, "MTM-CM5000-MSP Users Manual," www.maxfor.co.kr/datasheet/MTM-CM5000-MSP_Manual_ver1.0.pdf, December 2010.

[69] 우성일렉트레이드, 자동화용 센서 ,http://www.photosensor.co.kr/, March 2009.

[70] 기상청 일기예보 지상관측자료, http://www.kma.go.kr, March 2009.

[71] 최동민, 모상만, 정일용, " 무선 센서 네트워크에서 에너지 효율적인 가변 영역 라우팅 프로토콜", 멀티미디어학회 논문지, 11권, 18호, pp. 1082-1092, August 2008.

[72] 최동민, 모상만, 정일용, " 무선 센서 네트워크 환경의 Threshold-sensitive 가변 영역 클러스터링 프로토콜에 관한 분석", 멀티미디어학회 논문지, 12권, 11호, pp. 1609-1622, November 2009.

저작물 이용 허락서

학 과	컴퓨터공학과	학 번	20077540	과 정	박사
성 명	한글: 최 동 민	한문: 崔 東 珉	영문: Dongmin Choi		
주 소	광주광역시 남구 주월동 해태아파트 201동 1502호				
연락처	e-mail : cdm1225@gmail.com				
논문제목	한글: 환경 감시 센서 네트워크를 위한 저에너지 고신뢰성 라우팅 프로토콜				
	영문: An Energy-Efficient and Reliable Routing Protocol for Environment Monitoring Sensor Networks				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건 아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함.
2. 위의 목적을 위하여 필요한 범위 내에서의 편집과 형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물 이용의 허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음.
7. 소속 대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의( ) 반대( )

201 년 월

저작자 : (인)

조선대학교 총장 귀하