



저작자표시-동일조건변경허락 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이차적 저작물을 작성할 수 있습니다.
- 이 저작물을 영리 목적으로 이용할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



동일조건변경허락. 귀하가 이 저작물을 개작, 변형 또는 가공했을 경우에는, 이 저작물과 동일한 이용허락조건하에서만 배포할 수 있습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

공 학 석 사 학 위 논 문

무선 센서네트워크에서 재밍 공격 방어를 위한
에너지 효율적인 라우팅 알고리즘



정 보 통 신 공 학 과

선 기 현

공 학 석 사 학 위 논 문

무선 센서네트워크에서 재밍 공격 방어를 위한
에너지 효율적인 라우팅 알고리즘

지도교수 김 성 운

이 논문을 석사학위논문으로 제출함.

2014년 2월

부 경 대 학 교 대 학 원

정 보 통 신 공 학 과

선 기 현

선기현의 공학석사 학위논문을 인준함.

2014년 2월 21일



주	심	공학박사	박 규 칠 (인)
위	원	공학박사	류 지 열 (인)
위	원	공학박사	김 성 운 (인)

목차

I. 서론	1
II. 관련 연구	4
2.1 재밍 정의 및 공격 종류	4
2.2 기존 재밍 감지 수단	5
2.3 기존 재밍 공격 방어 방법	6
2.4 기존 에너지 효율적인 라우팅 방법	10
2.5 본 논문의 접근 방법	12
III. 재밍 공격 방어를 위한 에너지 효율적인 라우팅 기법 ..	13
3.1 제안된 JARRA 기법	13
3.2 클러스터 형성 및 PDR 계산 단계	15
3.3 재밍 지역 우회 경로 선정 단계	18
IV. 성능평가	21
4.1 시뮬레이션 환경	21
4.2 시뮬레이션 결과	22
V. 결론	28
참고문헌	29

그림 목차

그림-1 재밍 공격 환경에서의 무선 센서네트워크 개념도	1
그림-2 PP(Proactive Protection)기법 개념도	7
그림-3 RP(Reactive Protection)기법 개념도	8
그림-4 FBL(Failure-Based Learning)기법 개념도	9
그림-5 DAP(Detour by Anchor Point)기법 개념도	10
그림-6 LEACH 개념도	11
그림-7 JARRA 개념도	13
그림-8 JARRA 기법 순서도	14
그림-9 JARRA 기법 전체 동작과정	15
그림-10 Hello 메시지 및 CH 메시지 구조	18
그림-11 무선 센서네트워크 환경에서 노드 및 재밍 배치	22
그림-12 JARRA 기법 성능평가 1	23
그림-13 JARRA 기법 성능평가 2	24
그림-14 JARRA 기법 성능평가 3	26
그림-15 JARRA 기법 성능평가 4	26

표 목차

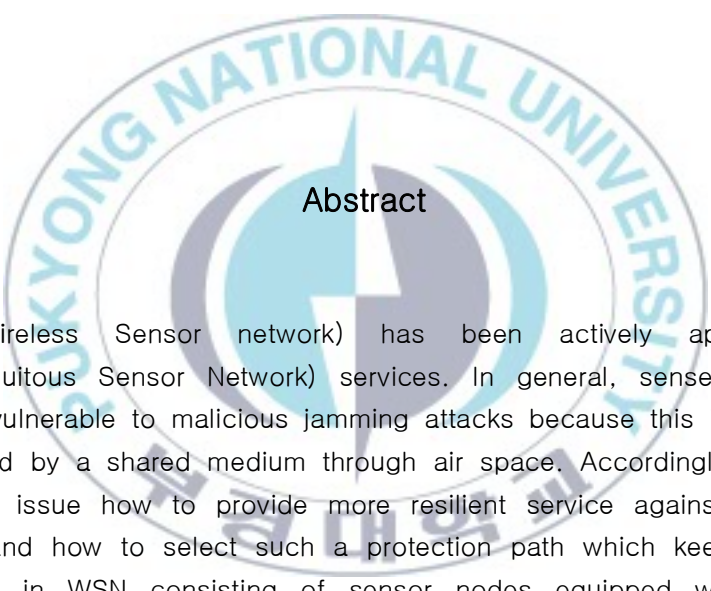
표-1 재밍 형태와 정의 및 해당 OSI 계층	5
표-2 재밍 공격 감지 수단 및 판단 방법	6
표-3 Hello 메시지 및 CH 메시지의 필드	18
표-4 JARRA 기법과 LEACH 기법 네트워크 종료 시점	24
표-5 JARRA 기법과 LEACH 기법 센싱 데이터 전송 성공률 비교	26



Energy efficiency Routing Algorithm for Defending Jamming Attacks in Wireless Sensor Networks

Ki-Hyun Seon

*Department of Telecommunication Engineering, The Graduate School,
Pukyong National University*



Abstract

WSN(Wireless Sensor network) has been actively applied for USN(Ubiquitous Sensor Network) services. In general, sensed data in WSN is vulnerable to malicious jamming attacks because this is normally transferred by a shared medium through air space. Accordingly, it is an important issue how to provide more resilient service against jamming attacks and how to select such a protection path which keeps energy efficiency in WSN consisting of sensor nodes equipped with limited power. In this thesis, we envisage the JARRA(Jamming Attack Resilient Routing Algorithm) scheme that detects jamming attacks and selects an optimal de-tour path guaranteeing energy efficiency and successful data delivery from the source node to the sink node. According to our simulation results, it is revealed that the JARRA scheme has superior resilience and energy efficiency compared with a method adapting LEACH(Low Energy Adaptive Clustering Hierarchy) routing scheme.

I. 서론

무선 센서네트워크는 한정된 에너지로 작동되는 작은 무선 센서들로 구성된다. 이 센서들은 서로 협력하면서 주위 환경으로부터 온도나 습도, 기상 데이터, 소음이나 진동 등 여러 정보들을 수집해서 싱크 노드(Sink node)에게 필요한 데이터를 제공한다[1][2]. 이런 센서 노드들은 보통 에너지를 충전하거나 교체하기 어려운 곳에 위치한 경우가 많으므로, 에너지 수명이 매우 큰 이슈로 작용한다. 때문에 에너지 사용의 효율성을 향상시켜 무선 센서네트워크의 수명을 늘리는 연구가 활발히 진행되고 있다[3][4]. 아래 그림-1은 이러한 개념을 도식화한 것이다.

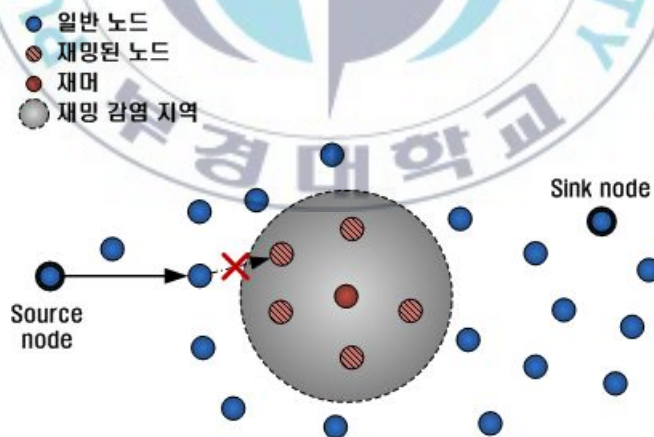


그림-1 재밍 공격 환경에서의 무선 센서네트워크 개념도

위의 그림에서 감지된 데이터들을 싱크 노드로의 전송은 일반적

으로 멀티 홉 기반의 가장 짧은 경로로 공기를 통해 무선으로 전송된다. 이 과정에서 의도적인 재머에 의한 공유된 공기 매체를 활용한 재밍 공격은 반복적인 데이터 전송 실패를 유발하여 무선 구간 통신 신뢰성 저하로 귀결되므로 악의적인 재밍 공격에 매우 취약하다[3][4][5][6].

여기서 재밍이란 무선통신의 신뢰성에 해로운 서비스 거부 공격의 종류로, 재머라 불리는 악의적인 공격자가 임의의 의미 없는 신호를 해당 무선 채널로 전송함으로써 통신을 방해하는 공격으로 노드들 간 통신을 방해하여 데이터 전송 실패를 야기하고, 이는 실패된 경로를 회복하기 위한 노드들의 지속적인 메시지 재전송 시도로 이어져 각 노드에서 많은 에너지를 소모하게 된다[5][6]. 결과적으로 한정된 전력을 갖는 센서 노드들로 구성된 무선 센서 네트워크에서 에너지 효율적이며 재밍 공격에 대한 방어를 효과적으로 고려하는 라우팅 기법 적용은 중요한 이슈이다[3][4].

본 논문에서는 무선 센서네트워크에서 재밍 공격 방어를 위한 에너지 효율적인 라우팅 알고리즘(JARRA: Jamming Attack Resilient Routing Algorithm)을 제안한다. 제안된 알고리즘은 성공적인 패킷 전달율(PDR : Packet Delivery Ratio)개념 적용으로 재밍 공격의 발생을 감지한 후 이를 피하는 목적지까지의 대체 경로를 에너지 효율적인 최적의 대체 경로를 계산하는 방법이다[5]. 제안된 방법은 재밍 상황에 대한 수학적 묘사를 기반으로 계산된 PDR을 활용하여 재밍을 감지하고, 또한 센서 네트워크에서 에너지 효율성을 높이는 대표적 라우팅 개념인 LEACH(Low Energy

Adaptive Clustering Hierarchy) 기법[7][8]을 개선하여 적용함으로써 다양한 재밍 공격(constant, deceptive, random 및 reactive 재밍)으로부터 무선 센서네트워크를 효과적으로 방어한다.

본 논문의 2장에서는 기존의 관련 연구 내용을 분석하고, 3장에서는 재밍 공격 방어를 위해 제안된 에너지 효율적인 라우팅 알고리즘인 JARRA 기법을 상세히 기술한다. 4장에서 시험 모델을 통한 시뮬레이션 및 성능 분석 결과를 제시하고 마지막으로 5장에서 결론을 맺는다.



II. 관련 연구

2.1 재밍 정의 및 공격 종류

본 논문에서 방어의 대상으로 하는 재밍은 무선 센서네트워크의 노드 간 무선통신에 피해를 가하는 일종의 서비스 거부 공격(Service Denial Attack)으로, 재머라 불리는 악의적인 공격자가 임의의 의미 없는 신호를 해당 무선 채널로 전송 및 통신 교란으로 데이터 전송 실패를 야기하게 된다. 결과적으로 무선 센서네트워크의 노드들은 실패한 무선 전송 경로를 회복하기 위해 노드들 간 추가적인 메시지 재전송 시도로 해당 노드에서 많은 에너지를 소모하게 된다. 이에 따라 한정된 전력을 갖는 센서 노드로 구성된 무선 센서네트워크의 수명을 단축시키고 센싱 데이터의 전송을 방해하여 신뢰성있는 서비스 제공에 문제가 생기는 결과가 생긴다 [3][4][5].

위에서 언급한 형태의 재밍은 여러 연구에서 다양하게 정의하였는데, 재밍의 형태 및 정의 그리고 해당 OSI 계층은 다음 표-1과 같이 요약된다[9].

표-1 재밍 형태와 정의 및 해당 OSI 계층

재밍 형태	방해 내용 정의	OSI 계층
Constant 재밍	공유된 매체로 의미없는 신호들을 계속해서 전송하여 정상적인 전송 동작을 방해함	물리 계층
Deceptive 재밍	프로토콜에 사용중인 패킷 형태와 맞지 않는 비정상적인 패킷 주입으로 네트워크 계층의 정상적인 동작을 방해함	네트워크 계층
Random 재밍	재밍 및 sleep모드를 오가며 Constant 재밍 공격을 랜덤하게 반복하여 방해함	물리 계층
Reactive 재밍	재밍 및 sleep모드를 오가며 Deceptive 재밍 공격을 반복하여 방해함	네트워크 계층

위의 표-1에서 요약된 재밍을 방지하기 위한 해결책을 찾기 위해서는 먼저 발생 여부를 판단할 수 있는 재밍 감지 수단이 필요하고 감지된 재밍에 대한 공격 방어 방법이 모색되어야 한다. 본 논문의 아래 2.2 소절은 기존에 연구된 재밍 감지 수단을 분석하고, 2.3 소절은 이들에 대한 재밍 공격 방어 방법을 요약한다.

2.2 기존 재밍 감지 수단

본 논문에서 연구 대상으로 하는 재밍에 대한 감지 수단은 [9]에서 정의하였는데, 대표적으로 신호강도(SS : Signal Strength)를 이용하는 방법, 캐리어 센싱 시간(CST : Carrier Sensing Time)을 비교하는 방법, 패킷 전달율(PDR : Packet Delivery Ratio)을 계산하고 기준치 달성 여부로 판단하는 방법, 신호강도 일관성(SSC : Signal Strength Consistency)을 분석하여 판단하는 방법 등으로 분류 할 수 있다. 이에 대한 요약은 아래 표와 같이 정리된다[9].

표-2 재밍 공격 감지 수단 및 판단 방법

감지 수단	동작 방법
신호강도 (SS : Signal Strength)	이웃 노드들 간의 송수신 신호강도가 -5db보다 낮은 경우 재밍으로 간주
캐리어 센싱 시간 (CST : Carrier Sensing Time)	일정기간이상 정상적인 캐리어센싱 타임과 비교하여 현재 캐리어 센싱 타임이 긴 경우 재밍으로 간주하여 감지
패킷 전달율 (PDR : Packet Delivery Ratio)	송신노드에서 송신한 패킷 수 대비 수신노드에서 성공적으로 수신한 패킷 수의 비가 16.77%(경험적 수치)보다 낮은 경우 재밍으로 간주
신호강도 일관성 (SSC : Signal Strength Consistency)	이웃 노드들의 평균 전송 신호 강도와 해당 전송 노드의 전송 신호강도를 비교하여 상대적으로 낮은 경우 재밍으로 간주

본 연구에서는 재밍 공격 감지 수단 및 판단 방법으로 패킷 전달율을 적용하는데, 이는 다른 방법에 비해 표-1에 정리한 모든 종류의 재밍을 감지할 수 있다[9]. 또한 한정된 에너지로 동작하는 무선 센서네트워크에서 최소의 메시지 교환을 통한 간단한 계산식을 통해 재밍 감지가 가능하기 때문에 다른 감지 수단을 활용하는 방법에 비해 에너지 효율적이다.

2.3 기존 재밍 공격 방어 방법

앞 2.2소절의 재밍 감지 수단으로 재밍 공격이 감지되면 이에 대한 방어 방법으로 다양한 연구가 진행되어왔다[5][10][11]. 관련 연구에 따르면 능동적인 공격 방어 방법과 수동적인 방어 방법으로 구분되며, 능동적인 방법은 재밍이 감지될 때 어떠한 기준에

의한 대체 가능한 전송 경로를 새로 설립하여 해당패킷을 전송하는 네트워크계층 기반 접근법이다[10]. 이러한 접근법의 예로는 PP(Proactive Protection)기법[5], RP(Reactive Protection)기법[5], FBL(Failure-Based Learning)기법[11] 그리고 DAP(Detour by Anchor Point)기법[11] 등이 있다.

먼저 PP기법은 아래 그림-2와 같은 개념을 가지며, 다중경로 라우팅 경로선택 기법 적용과 에너지 효율적인 경로선택 개념을 동시에 적용하여 가장 효과적인 (1+1) 데이터 전송 경로를 선택하는 기법이다. 이 방법은 다중 경로 선택에 관계된 시간적 오버헤드로 성능이 저하되고 탐색 단계에서 관련 패킷의 송수신등으로 에너지 소모가 심하여 무선 센서네트워크에서의 활용은 비효율적이다.

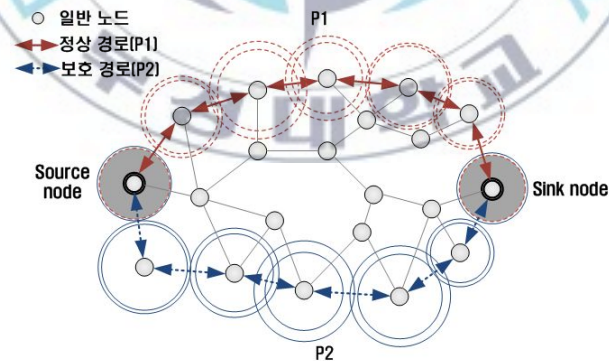


그림-2 PP(Proactive Protection)기법 개념도

둘째로 RP기법은 아래 그림-3과 같은 개념을 가지며, 주기적인 Hello 메시지를 주고 받음으로서 이웃 노드의 생존여부를 확인하

여 Hello 메시지에 대한 무응답 노드는 라우팅 테이블에서 삭제하는 방법으로 대체 경로선택에 활용하는 방법이다. 이 방법에서는 현재 데이터 전송 경로에서 재밍 공격으로 전송 실패가 발생하면 또 다른 대체 경로를 구성하는데, 즉 해당 재밍 된 노드와 다른 이웃노드로 Hello 메시지 전송과 응답 등을 최종목적노드에 도달할 때까지 반복하여 최적의 대체 경로를 구성하는 방법이다. 이 방법은 타 방법에 비해 최소 홉 수를 거치는 대체 경로를 활용하므로 패킷 전달과정에서 에너지 소모를 최소화할 수 있는 장점이 있다.

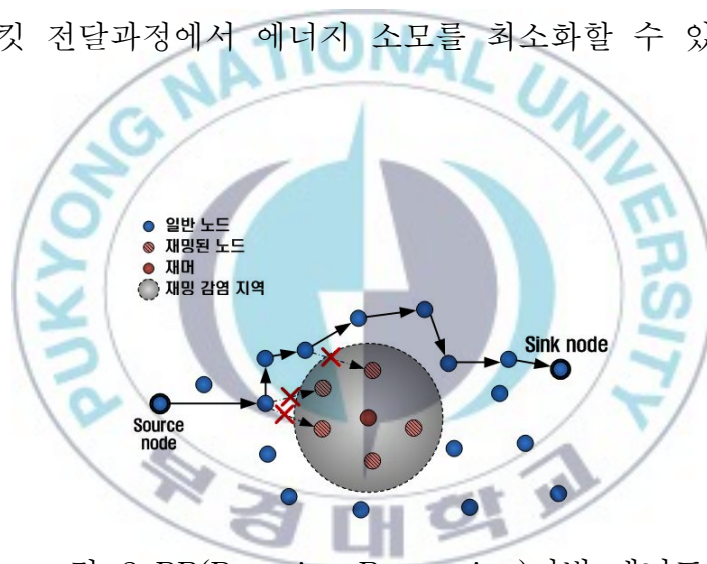


그림-3 RP(Reactive Protection)기법 개념도

셋째로 FBL기법은 아래 그림-4와 같은 개념을 가지며, 재밍 발생 시 대체 경로 선택을 위해 RP기법과 동일한 대체경로선택 접근 방법을 사용하지만, 이 방법의 주요 응용분야는 무선 네트워크에서 브로드캐스팅 용으로 목적지가 단일 노드가 아닌 복수의 목적지 노드를 대상으로 적용되는 방법이다. 여기서 복수의 대체 목적지 경로를 구할 때 Geocast Region 개념을 활용하는데, 무선

센서네트워크에서는 소스 노드와 목적지 노드 1:1 서비스 특성을 가지므로 그 목적에 부합되지 않는다.

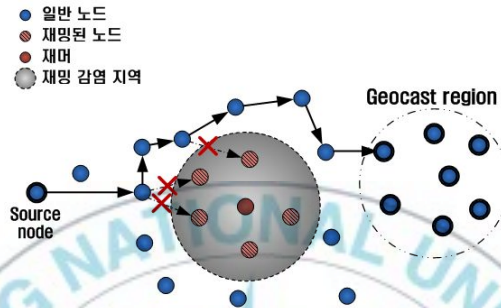


그림-4 FBL(Failure-Based Learning)기법 개념도

마지막으로 DAP기법은 아래 그림-5와 같은 개념을 가지며, 데이터 전송 중 재밍 공격 발생에 대한 대체 경로 설립으로 접근하는 개념은 앞에서 설명한 RP기법 및 FBL기법과 유사하다. 그러나 효율적인 대체 경로 설립을 위해 재밍 공격에 영향을 덜 받는 멀리 떨어진 고정지점(Anchor Point)을 거치는 우회경로를 선택하여 패킷을 전송하는 방법이다. 이 기법은 재밍 공격에 대비하여 신뢰성이 많은 대체 경로를 활용하지만 고정지점을 거치는 경로 설립 과정에서 노드들의 위치 및 각도 등 계산과정이 복잡하고, 또한 계산된 대체 경로가 타 방법에 비해 대체적으로 많은 홉 수를 거쳐 상대적으로 에너지 소모가 심한 단점이 있다.

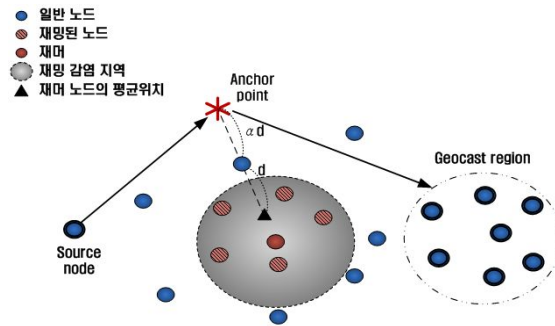


그림-5 DAP(Detour by Anchor Point)기법 개념도

본 논문에서는 재밍 공격에 대한 방어 방법으로 RP기법을 적용한 접근 방법을 제시한다. 이 접근방법의 주된 이유는 재밍 공격 발생시 최소 경로를 가지는 대체 경로 선택 및 최적의 루트를 통한 데이터 전달 과정을 통해 무선 센서네트워크의 생명 주기를 연장할 수 있다. 또한 주기적 라우팅 테이블 수정으로 재밍 공격에 대해 즉각적인 대응이 가능하고 RP기법에 비해 복구 개념을 적용하므로 무선 링크 자원 활용이 더 효율적이다. 일반적으로 무선 센서네트워크의 서비스 특성은 주기적인 센싱 데이터의 전달에 기초를 하기 때문에 (1+1) 보호 보다는 복구 개념이 더 효율적이다.

2.4 기존 에너지 효율적인 라우팅 방법

앞 소절에서 무선 센서네트워크에서의 센싱 데이터 전달과정에서 재밍 공격이 발생하면 RP기법을 활용한 최소 경로를 통한 대체 경로 채택 및 이를 통한 에너지 효율적인 데이터 전달로 무선 센서네트워크의 생명 주기를 연장하는 접근 방법을 선택하였다.

본 논문에서 제안하는 알고리즘은 무선 센서네트워크에서의 클러스터링 기반의 동작으로 전체 네트워크의 생명 주기의 최적화를 구현하고자 한다. 이에 본 논문에서는 무선 센서네트워크에서의 네트워크 수명 및 네트워크 확장성을 기반으로 라우팅을 달성하는 클러스터링 기법인 LEACH(Low Energy Adaptive Clustering Hierarchy) 기법을 또한 응용한다[7][8].

LEACH 기법은 센서네트워크 전체 영역을 여러 개의 클러스터 영역으로 나누고 각 클러스터별로 헤드 노드가 한번 선정되면 해당 클러스터내의 다른 모든 노드들이 헤드 노드로 선정된 후 다시 순번이 돌아오는 라운드 로빈 방법을 적용한다. 이는 임의적으로 클러스터 헤드 노드를 선정함에 있어 모든 노드가 균등하게 클러스터 헤드 노드로 선정되도록 하기 위함이다. 결과적으로 무선 센서네트워크에 있는 모든 센서 노드들이 클러스터 헤드 노드로 선정됨에 있어 무작위로 순환시켜 에너지 소비를 분산하고 클러스터 헤드 노드에 의해 형성된 클러스터를 지역적으로 관리하는 개념이다[7][8]. 아래 그림-6은 LEACH 기법의 동작 과정 개념을 도식화한 것이다.

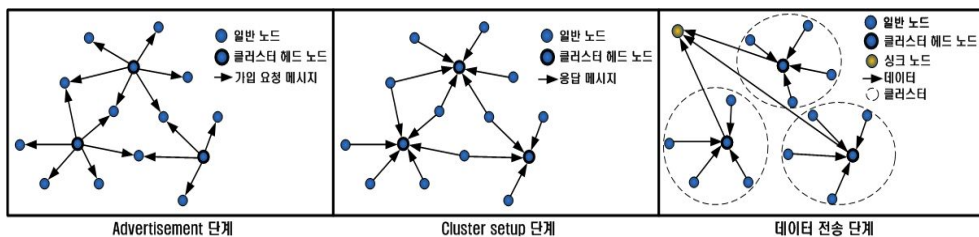


그림-6 LEACH 개념도

2.5 본 논문의 접근 방법

본 논문에서 제안하는 JARRA(Jamming Attack Resilient Routing Algorithm) 기법은 무선 센서네트워크내에서 다양한 재밍 공격에 대해 먼저 패킷 전달율을 활용하여 재밍을 효과적으로 감지하고, 둘째 가장 효율적인 재밍 지역 우회 경로를 계산하는 라우팅 기법을 포함한다. 재밍 발생시 재밍 지역 우회 경로 계산 과정에서는 LEACH 기법을 응용하지만 각 클러스터별 헤드 노드 선정 과정에서 라운드로빈 개념을 적용하는 것이 아니라 잔여 에너지가 가장 많은 노드를 선택하는 새로운 접근법을 제시한다. 이는 전체 노드들의 생존 시간을 늘려 전체 에너지 소비를 효과적으로 분산하고 각각의 클러스터를 지역적으로 관리함으로써 재밍 공격에 대해 안정적인 네트워크 운영을 기할 수 있다.

III. 재밍 공격 방어를 위한 에너지 효율적인 라우팅 기법

3.1 제안된 JARRA 기법

아래 그림-7은 제안된 JARRA 기법의 개념을 도식화한 것이다. 그 과정은 먼저 소스 클러스터 헤드 노드에서 수집한 센싱 데이터를 목적지 노드까지 전송하기 전에 재밍된 지역을 패킷 전달을 활용하여 감지한 후 정상 동작하는 다른 클러스터 헤드 노드들을 통해 재밍 지역 우회 경로를 선정한 후 수집된 센싱 데이터를 전송하는 개념이다. 여기서 에너지 효율적인 방법으로 라우팅 알고리즘을 구현하기 위해 클러스터 기반의 LEACH 변형 방법을 제안한다.

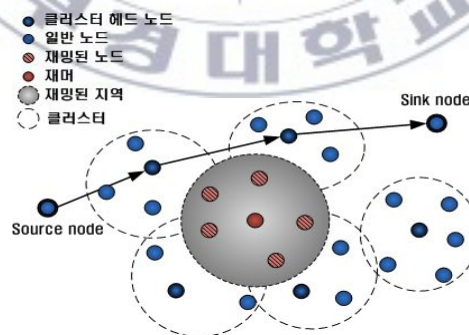


그림-7 JARRA 기법 개념도

JARRA 기법 동작의 상세한 절차는 아래 그림-8의 순서도와 같

으며 크게 클러스터 형성 및 PDR 계산 단계, 재밍 지역 우회 경로 선정단계로 구성된다.

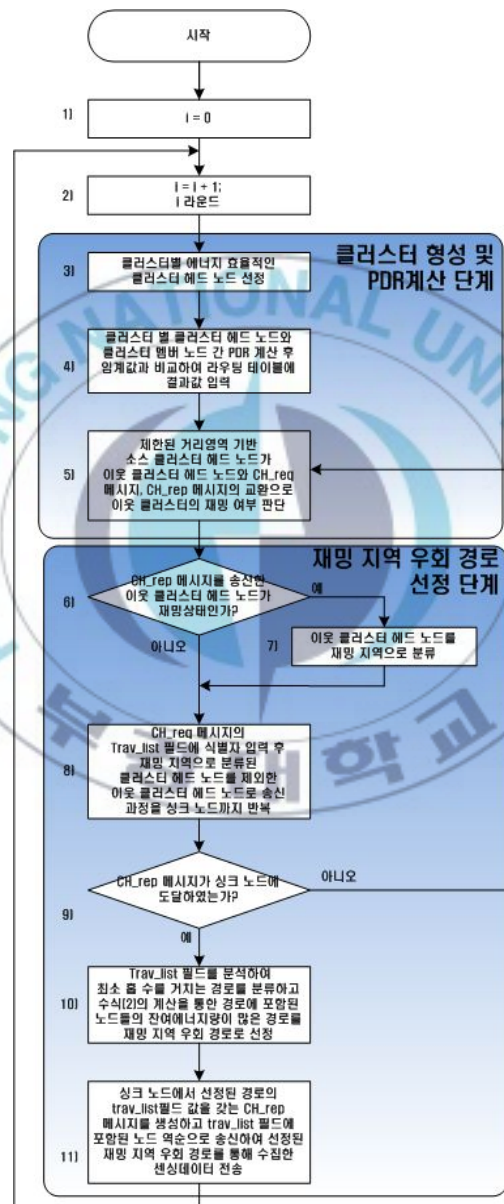


그림-8 JARRA 기법 순서도

아래 그림-9는 JARRA 기법의 전체 동작과정을 도식화한 것이다. 그림-9의 각 라운드 클러스터 형성과 Hello_req, Hello_rep 메시지 교환은 클러스터 형성 및 PDR 계산단계에서 동작하는 과정에 해당하며, CH_req, CH_rep 메시지 교환과 최소 홉수를 거치는 대체 경로를 통한 데이터 전송은 재밍 지역 우회 경로 선정 단계에서 동작하는 과정에 해당된다.

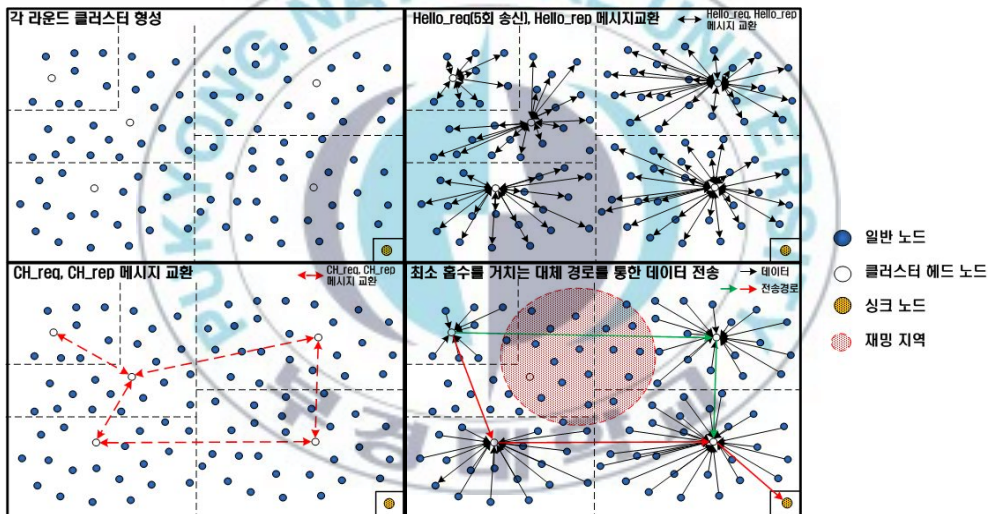


그림-9 JARRA 기법 전체 동작과정

3.2 클러스터 형성 및 PDR 계산 단계

먼저 클러스터 형성 및 PDR계산 단계에서는 주어진 무선 센서 네트워크를 클러스터로 구성하고 각 클러스터별로 잔여 에너지 량이 가장 많은 노드를 클러스터 헤드 노드로 선정 한다. 이 후,

PDR계산을 통해 재밍된 클러스터를 감지하고 재밍 지역을 우회하며 싱크 노드까지 가장 적은 홉 수를 거치는 에너지 효율적인 경로 선택의 개념을 사용한다.

클러스터 형성 및 PDR계산 단계의 동작 단계 중 클러스터 헤드 노드 선정 과정에서는 각 클러스터에 속한 노드들이 LEACH 기법과 같은 라운드로빈 개념을 통해 클러스터 헤드 노드를 선정하는 것이 아니라, 참여한 노드가 속해있는 해당 클러스터에서 각각의 노드 잔여 에너지량을 비교하여 가장 많은 에너지를 가지고 있는 노드가 클러스터 헤드 노드로 선정된다.

이후의 과정으로 PDR계산을 위해 각 클러스터 헤드 노드에서 클러스터 멤버 노드로 Hello_req 메시지를 5회 송신하고 이에 대한 응답메시지인 Hello_rep 메시지가 수신되는 비율을 활용하여 PDR을 계산한 후 결과값을 라우팅 테이블에 입력한다. 이 과정에서 활용되는 PDR의 수식은 다음 수식(1)로 정의된다[9].

$$PDR = \frac{N_{Hello-req}}{N_{Hello-rep}} \quad (1)$$

수식(1)의 $N_{Hello-req}$ 는 각 클러스터 헤드 노드에서 자신에 속한 클러스터의 타 노드들에게 재밍 여부를 판단하는 기초자료를 확보하기 위한 수단으로 송신되는 메시지의 수이고, $N_{Hello-rep}$ 는 클러스터 멤버 노드들로부터 응답된 메시지의 수이다.

수식(1)의 결과를 통해 클러스터 헤드 노드와 클러스터 멤버 노

드 간 PDR계산이 완료되면 임계값과 비교하여 재밍 여부를 판단한 후, 라우팅 정보로 활용해서 라우팅 테이블(그림 10의 J 필드 값을 '1'로 셋팅)을 유지한다. 비교 대상으로 하는 임계값은 수식에 의해 정해지는 것이 아니라 현장에서의 실험을 통해 주어진 경험적 수치로 Wang 외 저자들의 기존 연구에 따르면, constant, deceptive, reactive 그리고 random 재밍을 판단하기 위해 16.77%의 임계값이 사용되었다[9].

이후의 동작으로 이웃 클러스터 헤드 노드가 재밍된 지역에 포함되었는지를 판단하기 위해 제한된 거리에 위치한 이웃 클러스터 헤드 노드와 CH_req 메시지(자신의 식별자가 입력된 메시지), CH_rep 메시지를 교환한다. 이 과정에서의 제한된 거리는 각 클러스터간 거리가 200m를 초과하지 않기 때문에 한 홉의 거리에 위치한 이웃 클러스터 헤드 노드 간의 메시지 교환을 위해서 CH 메시지는 200m의 전송범위로 동작한다.

PDR 계산 및 재밍 지역 우회 경로 선정을 위한 라우팅 과정에서 활용되는 Hello 메시지와 CH 메시지는 그림 10과 같은 구조를 가지며 표-3과 같은 해당 필드로 구성된다.

type	src	dst	J	trav_list
------	-----	-----	---	-----------

그림-10 Hello 메시지 및 CH 메시지 구조

표-3 Hello 메시지 및 CH 메시지의 필드

Type	① : Hello_req		①, ②, ③, ④
	② : Hello_rep		
	③ : CH_req		
	④ : CH_rep		
src			①, ②, ③, ④
dst			①, ②, ③, ④
J	(0 : , 1 :)		④
trav_list			③, ④

3.3 재밍 지역 우회 경로 선정 단계

앞서 3.2절의 클러스터 형성 및 PDR계산 단계를 기술하였다. 이 과정에서 계산된 PDR 값을 임계값과 비교하고 재밍 여부를 판단한 후, 라우팅 정보로 활용하여 라우팅 테이블을 유지한다.

이후에 동작하는 그림-8의 재밍 지역 우회 경로 선정 단계에서는 이웃 클러스터 헤드 노드간의 CH_req 메시지와 CH_rep 메시지의 교환을 통해 수신되는 CH_rep 메시지의 J 필드 값이 '1'로 정의된 이웃 클러스터 헤드 노드가 발생하면 해당 클러스터 헤드 노드를 재밍된 지역으로 분류하고 해당 라운드의 라우팅 과정에서

제외한다. 이 과정에서도 재밍 지역 우회 경로 선정의 정보로 활용하기 위해 주변 클러스터 헤드 노드의 재밍 여부를 판단하기 위해 패킷 전달율인 PDR 개념을 활용한다.

수식(1)의 결과를 통해 소스 클러스터 헤드 노드는 재밍된 지역에 위치한 이웃 클러스터 헤드 노드를 분류하고 CH_req 메시지의 trav_list 필드에 자신의 식별자를 추가한 후 정상적으로 동작하는 이웃 클러스터 헤드 노드로 송신한다. 그리고 CH_req 메시지를 수신한 이웃 클러스터 헤드 노드들도 trav_list 필드에 자신의 식별자를 추가하고 다음 노드로 송신한다. 이 같은 과정이 소스 클러스터 헤드 노드에서 송신된 CH_req 메시지가 싱크 노드에 도달할 때까지 반복한다.

이러한 반복과정을 거쳐 싱크 노드에 CH_req 메시지가 도달하면 싱크 노드에서는 trav_list 필드를 분석하여 최소 홉 수를 거치는 경로를 분류하고 이 후에 수식(2)를 계산하여 경로에 포함된 클러스터 헤드 노드의 잔여 에너지량이 가장 많은 경로를 재밍 지역 우회 경로로 선정한다. 이 과정에서 활용되는 수식(2)는 아래와 같다.

$$Find(Shortest_path(i,j)) = MAX \sum_{k=i}^j E_k, \begin{cases} i = \text{소스 클러스터 헤드 노드} \\ j = \text{싱크 노드} \end{cases} \quad (2)$$

수식(2)의 E 는 소스 클러스터 헤드 노드에서 싱크 노드까지 재밍 지역 우회 경로에 포함되어 있는 라운드별 각 클러스터 헤드

노드들의 잔여 에너지 량이다.

앞의 과정을 통해 재밍 지역 우회 경로가 선정되면 싱크 노드에서는 선정된 경로의 trav_list 필드에 포함된 클러스터 헤드 노드 역순으로 확정된 경로를 trav_list 필드 값으로 갖는 CH_rep 메시지를 생성하고 송신한다. 결과적으로 CH_rep 메시지는 소스 클러스터 헤드 노드에 도달하게 되고 소스 클러스터 헤드 노드는 수신된 CH_rep 메시지의 trav_list 필드를 분석하여 선정된 재밍 지역 우회 경로를 통해 수집된 센싱 데이터를 전송한다.

결과적으로 재밍 지역 우회 경로 선정 단계에서는 소스 클러스터 헤드 노드에서 싱크 노드까지의 CH_req 메시지의 trav_list 필드 분석을 통한 최단 홉 수를 거치며 trav_list 필드에 포함되어 있는 클러스터 헤드 노드의 잔여 에너지 량의 합이 가장 많은 라우팅 경로를 선정하고 수집된 센싱 데이터를 전송하는 개념이다.

IV. 성능평가

4.1 시뮬레이션 환경

무선 센서네트워크에서 재밍 공격 방어를 위한 에너지 효율적인 JARRA 기법의 성능 평가를 위해서는 실제 환경에서 직접적인 실험이 요구되지만, 이는 실질적이고 비용적인 이유로 인하여 불가능하다. 대신 실험 상황을 쉽게 제어하기 적합한 시뮬레이션 환경을 아래 그림-11과 같이 구성하였다.

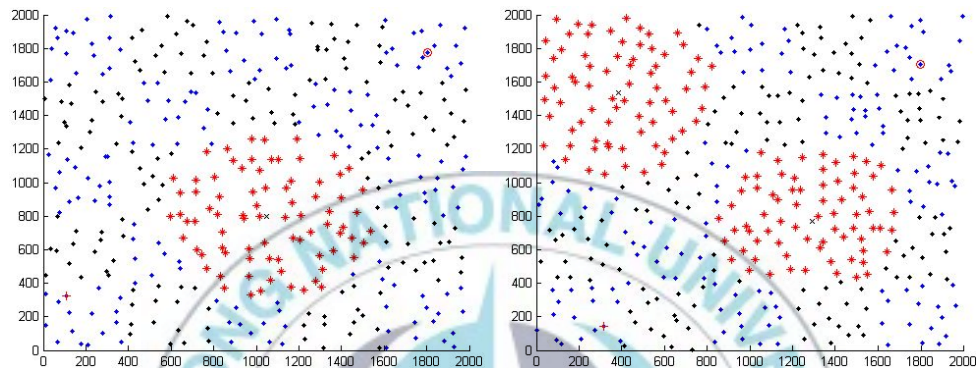
시뮬레이션 모델은 기존의 연구[11]와 동일한 $2000m \times 2000m$ 의 영역으로 설계하였고 여기에 400개의 노드들이 약 $100m^2$ 당 하나씩 무작위로 배치된다.

또한 클러스터 헤드 노드의 수는 비교대상으로 하는 LEACH 기법과 동일한 전체 노드 400개 중 5%에 해당하는 20개의 노드가 클러스터 헤드 노드로 동작하도록 한다[7][8]. 여기서 동작하는 클러스터 헤드 노드의 선정 방식은 라운드 로빈 개념을 활용하는 LEACH 기법과 다르게 해당 클러스터에 속한 노드들 중 잔여 에너지량이 많은 노드가 클러스터 헤드 노드로 선출 되도록 한다.

마지막으로 제안된 JARRA 기법에서 방어를 목적으로 하는 재밍 공격의 형태는 앞서 표-1에서 요약된 4가지의 형태를 가지며, 재밍 공격의 범위는 $500m$ 로 가정하고, 단일 재밍일 경우와 이중 재밍일 경우에 대해 각각 실험한다.

시뮬레이션 환경은 그림-11과 같이 “.”으로 표시되는 노드는

정상적인 노드를 나타내며, “*” 모양으로 표시되는 재밍 지역의 위치는 원활한 실험을 위해서 원형에 둘러 싸인 소스 클러스터 헤드 노드와 싱크 노드 사이에 위치시킨다.



(a) 단일 재밍 환경

(b) 이중 재밍 환경

그림-11 무선 센서네트워크 환경에서 노드 및 재밍 배치

이번 시뮬레이션에서 소스 클러스터 헤드 노드와 싱크 노드 사이에 위치한 재밍 공격이 3개 이상으로 발생하면 전체 영역을 가로지르는 형태로 인해 재밍 지역 우회 경로 선정이 불가하기 때문에 고려하지 않는다. 단, 단일 재밍이 발생한 경우와 이중 재밍이 발생한 경우의 차이를 비교하여 3개 이상의 재밍이 발생한 환경의 결과를 예측할 수 있다.

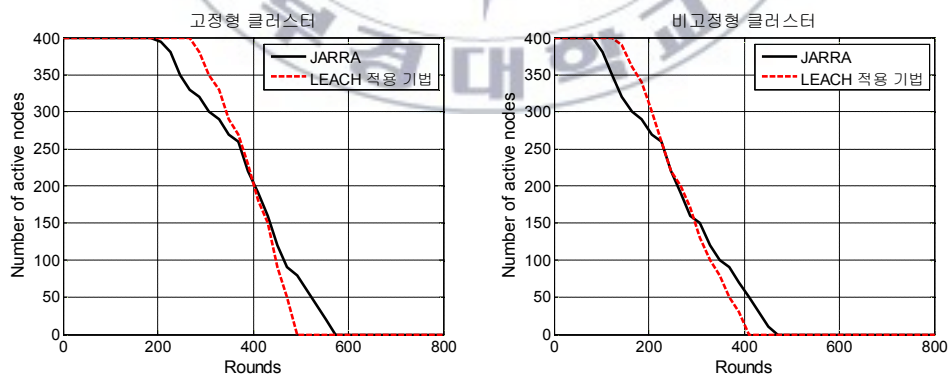
4.2 시뮬레이션 결과

제안된 JARRA 기법은 재밍 지역을 회피하여 최소 홉 수를 거치

는 재밍 지역 우회 경로를 통해 재밍 공격(constant, deceptive, reactive 그리고 random)으로부터 신뢰성 있고, 에너지 효율적인 라우팅을 목적으로 한다.

본 시뮬레이션에서는 제안된 JARRA 기법의 비교 대상으로 LEACH 변형 적용 기법을 채택하였으며, 성능평가 항목으로는 네트워크에서 각종 재밍 공격이 발생하였을 때에 800 라운드 동안의 센싱 데이터 전달 후 생존 노드의 수와 센싱 데이터 전송 성공률을 비교하여 성능 향상에 대한 근거를 제시한다.

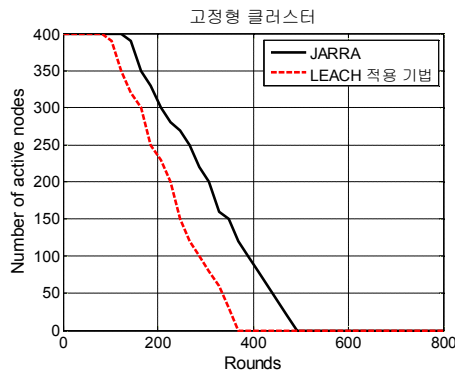
먼저 이에 대한 내용으로 클러스터 구성을 고정형인 경우(해당 클러스터에 속한 노드가 고정적인 경우)와 비고정형인 경우(해당 클러스터에 속한 노드가 유동적인 경우)로 형성할 때 단일 재밍과 이중 재밍에 대한 각각의 생존 노드 수를 비교한 결과는 아래 그림-12 및 그림-13과 표-4로 정리된다.



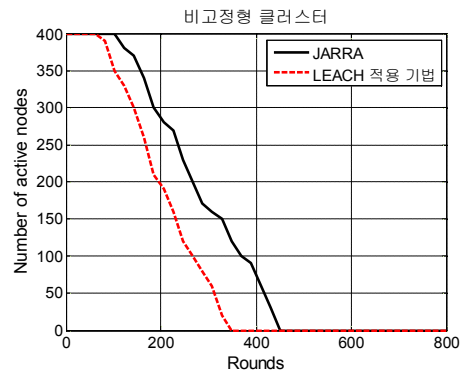
(a) 고정형 클러스터인 경우

(b) 비고정형 클러스터인 경우

그림-12 JARRA 기법 성능평가 1



(a) 고정형 클러스터인 경우



(b) 비고정형 클러스터인 경우

그림-13 JARRA 기법 성능평가 2

표-4 JARRA 기법과 LEACH 기법 네트워크 종료 시점

알고리즘	네트워크 종료 라운드			
	단일 재밍		이중 재밍	
	고정형	비고정형	고정형	비고정형
JARRA 기법	574	492	512	451
LEACH 기법	493	410	369	348

위의 그림-12 및 그림-13과 표-4는 JARRA 기법과 LEACH 변형 적용 기법의 고정형 클러스터의 경우와 비고정형 클러스터 경우의 환경에서 발생한 단일 재밍과 이중 재밍 각각에 대한 생존 노드 수를 비교한 결과 값이다.

라우팅 기법의 일반적 평가 기준인 네트워크 생존시간 즉, 400개의 노드 중 첫 번째 노드의 에너지가 고갈되는 시점을 비교하였을 때, 단일 재밍의 경우 JARRA 기법이 먼저 발생하였지만, 이중 재밍일 경우 LEACH 변형 적용 기법이 먼저 발생한다. 그러나 네

트위크에 속한 전체 노드가 동작하지 않는 경우는 JARRA 기법이 두 가지 종류의 메시지를 활용하는 LEACH 변형 적용 기법보다 두 가지의 메시지를 더 활용하여 총 네가지 종류의 메시지 활용에도 불구하고 재밍 우회 경로 성능을 갖추므로 인해 단일 재밍과 이중 재밍이 발생한 환경에서 향상된 성능을 보여준다.

따라서 라운드 로빈 방식으로 클러스터 헤드 노드를 선정하고 이전 라운드에서 클러스터 헤드 노드로 동작한 노드는 클러스터 헤드 노드 선정 과정에서 제외하는 방식인 LEACH 변형 적용 기법보다 잔여 에너지가 많은 노드를 클러스터 헤드 노드로 선정하는 JARRA 기법이 에너지 효율적인 측면에서 우수하다고 판단된다. 결과적으로 네트워크가 더 오래 지속된 JARRA 기법이 무선 센서네트워크 환경에서 LEACH 변형 적용 기법보다 각 노드들의 효율적인 에너지 소비가 가능하다.

이 후에 진행된 시뮬레이션은 앞서 실험한 환경과 동일한 상태에서 LEACH 적용 기법(직접 전송)과 LEACH 변형 적용 기법(최단 홉 수 경로 선정)과의 소스 클러스터 헤드 노드에서 싱크 노드까지의 센싱 데이터 전송 성공률을 비교하였으며, 결과는 아래 그림-14 및 그림-15와 표-5로 정리된다.

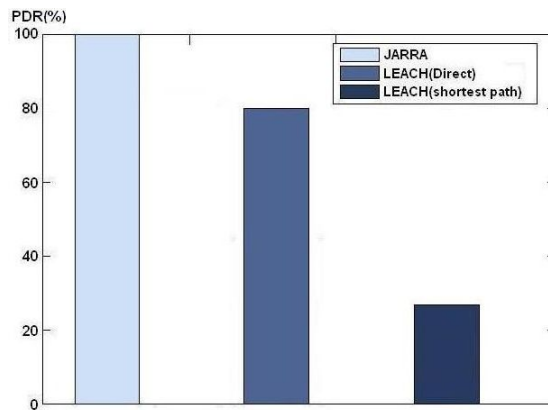


그림-14 JARRA 기법 성능평가 3

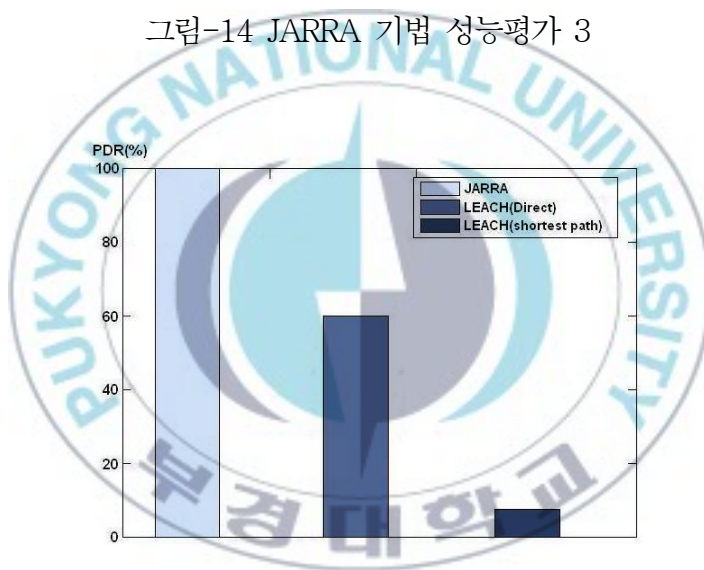


그림-15 JARRA 기법 성능평가 4

표-5 JARRA 기법과 LEACH 기법 센싱 데이터 전송 성공률 비교

알고리즘	센싱 데이터 전송 성공률	
	단일 재밍	이중 재밍
JARRA 기법	100%	100%
LEACH 기법 (직접 전송)	80%	60%
LEACH 기법 (최소 홉수)	27%	8%

위의 그림-14와 표-5의 결과로 단일 재밍의 경우 JARRA 기법의 센싱 데이터 전송 성공률은 재밍 지역을 우회하는 라우팅을 활용한 센싱 데이터 전송으로 인해 100%이고, LEACH 적용 기법(직접 전송)의 경우 재밍 지역에 포함된 클러스터는 센싱 데이터 전송이 불가능하여 그 성공률은 80%이다. 마지막으로 최단 홉수를 경유하여 센싱 데이터 전송을 전송하는 LEACH 변형 적용 기법은 성공률이 약 27%의 결과를 보였다.

또한 그림-15와 표-5의 결과로 이중 재밍의 경우 JARRA 기법은 단일 재밍과 마찬가지로 100%의 데이터 전송 성공률을 보이지만, LEACH 적용 기법의 경우 센싱 데이터 전송 성공률은 60%이며, 마지막으로 LEACH 변형 적용 기법은 약 8%의 성공률을 나타낸다.

결과적으로 보면 제안된 JARRA 기법 적용 시 기존의 LEACH 적용 기법 및 변형 적용 기법보다 더 나은 센싱 데이터 전송 성공률을 보인다. 즉, 제안된 방법이 기존의 LEACH 기법을 응용 및 변형 적용한 방법보다 우수한 회복력과 에너지 효율성을 가짐을 알 수 있다.

V. 결론

무선 센서네트워크는 공유된 매체 즉, 공기를 통해 통신 채널을 제공하는 특성으로 인해 악의적인 공격자에 의한 재밍 공격에 취약하다. 이러한 문제의 해결을 위해서는 다양한 종류의 재밍 공격을 보다 완벽하게 감지하고 방어 및 우회하는 방법이 요구된다.

본 논문에서는 무선 센서네트워크에서 에너지 효율적이며 재밍 지역 우회 경로 선정을 통한 재밍 방어 방법을 제안하였다. 해당 방법은 무선 센서네트워크 환경에서 각 노드들의 효율적인 에너지 소비를 위해 클러스터 기반으로 동작하며, PDR을 활용하여 소스 클러스터 헤드 노드에서 싱크 노드까지 재밍 지역 우회 경로를 선정하고 신뢰성있는 라우팅을 달성한다. 또한 재밍 지역 우회 경로는 최소 홉수를 경유하며, 경로에 포함된 클러스터 헤드 노드들의 잔여 에너지가 많은 경로를 선정하는 방식이다.

시뮬레이션에서 제안된 JARRA 기법의 성능을 측정하기 위해 기존의 클러스터 기반의 대표적인 에너지 효율적인 알고리즘인 LEACH 기법과 그 성능을 비교하였다. 결과적으로 시뮬레이션을 통한 성능 평가에 의하면 JARRA 기법이 단일 재밍과 이중 재밍이 발생한 환경에서 기존의 LEACH를 응용 및 변형 적용한 기법보다 재밍 공격에 대한 회복력과 네트워크 생존성 그리고 센싱 데이터 전송 성공률 측면에서 우수한 성능을 보였다.

결론적으로 제안된 기법은 악의적인 재밍 공격 환경에서 에너지 효율적인 방법으로 더욱 더 회복력이 강한 기법으로 평가된다.

참 고 문 헌

- [1] 김성운, 박선영, “수중 센서네트워크를 위한 에너지 효율적인 라우팅 방법 연구”, 한국정보기술학회논문지, 제 9권, 제 2 호, (2011) 95-104.
- [2] 김성운, 박선영, “BcN 기반 USN 서비스를 위한 라우팅 기술 연구”, 한국정보기술학회논문지, 제9권, 제3호, (2011) 119-129.
- [3] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, A survey on jamming attacks and countermeasures in WSNs, IEEE Communications Surveys and Tutorials 11 (4) (2009) 42-56.
- [4] X. Li, Y. Zhu, and B. Li, Optimal anti-jamming strategy in sensor networks, Proc. of IEEE ICC'12 Ad-hoc and Sensor Networking Symposium, (2012) 178-182.
- [5] U. Patel, T. Biswas, and R. Dutta, A routing approach to jamming mitigation in wireless multihop networks, Proc. of Local and Metropolitan Area Networks'11 (2011) 1-6.
- [6] S. Liu, L. Lazos, and M. Krunz, Thwarting control-channel jamming attacks from inside jammers, IEEE Trans. Mob. Comput. 11 (9) (2012) 1545-1558.

- [7] Abbasi, A.A and Younis, M, A Survey on Clustering Algorithms for Wireless Sensor Networks, Comput. Netw. (2007) 2826-2841.
- [8] 김대영, “계층적 센서 네트워크에서의 클러스터링 및 라우팅 알고리즘”, 경희대학교 석사학위 논문, (2006).
- [9] L. Wang and A. M. Wyglinski, A combined approach for distinguishing different types of jamming attacks against wireless networks, Proc. of Communications, Computers and Signal Processing'11 (2011) 809-814.
- [10] H. Sun, S. Hsu, and C. Chen, Mobile jamming attack and its countermeasure in wireless sensor networks, Proc. of Advanced Information Networking and Applications Workshops '07 (2007) 457-462.
- [11] S. Yoon and Y. Ko, JRGP: jamming resilient geocasting protocol for mobile tactical ad hoc networks, Proc. of Information and Communication Technology Convergence'10 (2010) 437-442.

감사의 글

학부생 시절 갖춰 놓은 것 없이 많이 부족했던 저를 프로토콜 공학 연구실에 받아주셔서 5년 동안 항상 아껴주시고 사랑으로 지도해주신 김성운교수님께 진심으로 감사드리며 앞으로 사회에 나가서도 항상 마음 속 깊이 그 뜻을 간직하겠습니다. 또한 많이 부족한 본 논문의 심사를 맡아 세심한 관심과 조언을 아끼지 않으신 박규철 교수님, 류지열 교수님께도 깊이 감사드립니다.

연구실에 처음 들어와 규칙적이고 어긋나지 않도록 잘 적응할 수 있게 도와주셨던 찬효 선배, 현수선배등 졸업한 선배들과 학부 및 석사 과정 동안 늘 함께했던 선영, 경호, 영준, 하선, 황원, 대명 등 프로토콜공학 연구실원들, 그리고 대학원 생활을 함께 하며 기쁨과 아픔을 함께 했던 나의 동기들과 후배들 동협, 철원, 상현, 철환, 명우, 승훈, 성규, 설봉, 민지, 주현, 희중과 석사 과정 중 행정적인 업무로 많은 도움을 준 학과사무실 조교 수정, 현정에게도 감사의 말을 전합니다. 동기들과 후배, 그리고 친구들 덕분에 항상 웃음 잃지 않으며 자신감 있고 즐겁게 석사생활을 할 수 있었다고 자부하며 진심으로 고마움의 마음을 전합니다.

끝으로 항상 저를 믿어주시고 아껴 주셨던 사랑하는 부모님, 형, 형수님, 지후, 소민, 여동생, 그리고 사랑하는 나의 와이프 정임이를 포함하여 항상 저를 응원해주신 모든 분들에게 감사하는 마음을 글로 대신 전합니다.

2014년 2월

선기현올림