情報保護學會論文誌
第19卷 第4號, 2009. 8

무선 센서 네트워크에서 경계값 결정을 위한 재귀적 계약망 프로토콜의 적용*

서 희 석†‡
한국기술교육대학교

Application of the Recursive Contract Net Protocol for the Threshold Value Determination in Wireless Sensor Networks*

Hee-Suk Seo†‡
Korea University of Technology and Education

요 약

유비쿼터스 센서 네트워크에서 센서 노드들은 불리한 환경에 배치되므로 공격자에 의해 훼손될 수 있다. 훼손된 노드들은 허위 감지 보고서들을 네트워크에 주입하는데 사용할 수 있는데, 이러한 허위 보고서들은 허위 경보를 유발할 수 있을 뿐만 아니라, 네트워크의 제한된 에너지 자원도 고갈시킬 수 있다. 허위 보고서 여과를 위한 보안 기법들에서, 보안성을 결정하는 보안 경계 값의 선택은 매우 중요하다. 기존의 적응적 보안 기법들에서는 경계 값의 결정이 전체 노드들에게도 적용되어 에너지 자원을 불필요하게 소모하는 문제점을 가진다. 본 논문에서는 충분한 보안성을 제공하면서 에너지를 절약할 수 있는 보안 경계 값 결정을 위하여 재귀적 계약망 프로토콜 적용 기법을 제안한다. 보다 효과적으로 네트워크를 운용하기 위하여, 네트워크를 계층적으로 그룹핑하고, 각 그룹에 대하여 재귀적으로 계약 망 프로토콜이 적용된다. 이를 통해 베이스 스테이션에서 퍼지 로직을 사용하여 결정된 경계 값은 보안 공격이 발생한 지역에 국한되어 적용된다.

ABSTRACT

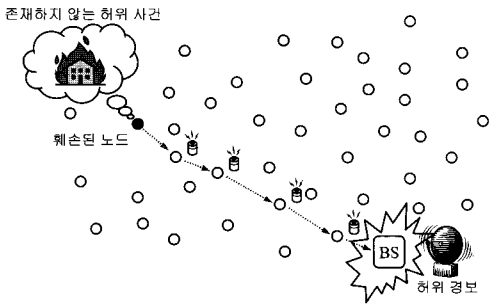
In ubiquitous sensor networks, sensor nodes can be compromised by an adversary since they are deployed in hostile environments. False sensing reports can be injected into the network through these compromised nodes, which may cause not only false alarms but also the depletion of limited energy resource in the network. In the security solutions for the filtering of false reports, the choice of a security threshold value which determines the security level is important. In the existing adaptive solutions, a newly determined threshold value is broadcasted to the whole nodes, so that extra energy resource may be consumed unnecessarily. In this paper, we propose an application of the recursive contract net protocol to determine the threshold value which can provide both energy efficiency and sufficient security level. To manage the network more efficiently, the network is hierarchically grouped, and the contract net protocol is applied to each group. Through the protocol, the threshold value determined by the base station using a fuzzy logic is applied only where the security attack occurs on.

Keywords: Ubiquitous Sensor Networks, Contract Net Protocols, DEVS, Fuzzy Logic, Security

접수일(2009년 4월 27일), 게재확정일(2009년 6월 9일)
* 이 논문은 2008년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임. (KRF-2008-331-D00575)
† 주저자, histone@kut.ac.kr
‡ 교신저자, histone@kut.ac.kr

I. 서 론

유비쿼터스 센서 네트워크(ubiquitous sensor network: 이하 USN)는 주변 환경 정보를 수집할 수 있는 감지 기능, 정보 처리 기능, 무선 통신 기능을 가지는 다수의 소형 센서 노드(sensor node)들과 감지 정보들의 집중국 역할 및 사용자와 노드간의 게이트웨이 역할을 하는 단일 또는 소수의 베이스 스테이션(base station: 이하 BS)들로 구성된다[1]. 각 센서 노드는 대상이 되는 사건(예를 들어, 적군의 출현 또는 사용자의 요청)이 발생한 경우, 사건 감지 보고서를 생성하여 BS로 전달한다. 일반적으로 USN에서는 노드들이 개방된 환경에 배치되므로 물리적인 위협에 취약할 수밖에 없다[2]. 악의적인 공격자는 노드를 물리적으로 취하여 데이터 인증에 사용하는 인증키들과 같은 보안 정보들을 획득할 수 있다[3]. 공격자는 <그림 1>과 같이 포획된 노드(훼손된 노드: compromised node)들을 통해 허위 감지 보고서들을 네트워크에 쉽게 주입할 수 있는데, 이러한 허위 보고서들은 네트워크 운영상의 허위 경보를 유발시킬 수 있을 뿐만 아니라, 센서 네트워크의 수명과 직결된 에너지의 고갈을 유발할 수 있다[4].



[그림 1] 허위 보고서 주입 공격

허위 보고서들을 전달 과정에서 탐지하여 폐기하기 위한 다양한 보안 기법들[5-11]이 제안되고 있는데, 이러한 기법들에서 네트워크의 보안을 강화하기 위하여 보안성을 강화하면(보안 경계 값을 높게 설정), 허위 보고서들의 전달 중 여과 확률은 증가하지만, 인증에 참여하는 노드들의 수가 증가하여 노드들의 에너지 소비가 증가하게 된다[4]. 반대로 보안성을 낮추게 되면(보안 경계 값을 낮게 설정), 인증에 참여하는 노드들의 수가 감소하여 에너지 소모는 줄어들지만, 허위 보고서들의 여과 확률이 떨어지므로, 결과적으로 불필요하게 에너지를 소모하게 될 수도 있다[8-11]. 즉, 보고서 생성에 참여하는 노드들의 수를 나타내는 보안 경계 값의 결정은 매우 중요하다.

기존의 적응적 보안 기법들[10-12]에서는, 결정된 경계 값에 따라 여과를 수행하여 BS에 보고를 하고, BS에서는 보고 받은 결과에 따라서 새로운 경계 값을 결정한다. BS는 이 새로운 경계 값을 네트워크에 브로드캐스트하는 방식을 취하므로, 실제 허위 보고서들의 보고 및 여과에 참여하지 않았다 하더라도 BS의 내용을 수신하여 경계 값을 바꾸게 된다. 그러므로 이러한 노드들의 에너지 자원을 불필요하게 소모하게 되는 문제점을 가진다.

본 논문에서는 충분한 보안성을 제공하면서 에너지를 절약할 수 있는 보안 경계 값 결정을 위하여 재귀적 계약망 프로토콜(contract net protocol: 이하 CNP)[6]을 적용한다. BS는 노드가 훼손되지 않은 인증 키들을 가지고 있을 확률, 훼손된 노드들의 수, 노드의 잔여 에너지 수준 등을 고려하여 경계 값을 결정한다. 보다 효과적으로 네트워크를 운용하기 위하여, 네트워크를 계층적으로 그루핑하고, 각 그룹에 대하여 순차적으로 CNP가 적용되는 재귀적인 방법을 제안한다. 계약망 프로토콜은 에이전트들이 계약에 의하여 분산된 문제를 해결하기 위해서 협상하고 통신하는 메커니즘을 제공한다.

논문의 구성은 다음과 같다. 2장에서는 관련 연구로, DEVS 모델링 방법론, CNP, 및 허위 보고서 여과 기법들을 간략히 소개하며, 3장에서는 제안 기법을 자세하게 설명한다. 4장에서는 시뮬레이션 결과를 분석하고, 5장에서 결론을 맺는다.

II. 관련연구

2.1 DEVS 모델링 방법론

Zeigler에 의해 정립된 DEVS(discrete event system specification) 방법론[13-14]은, 연속적인 시간상에서 발생되는 이산 사건을 처리하는 시스템을 시뮬레이션하기위하여 이론적으로 정립된 모델링 방법론이다. 이는 모델의 구조와 행동을 시뮬레이션 수행으로부터 추상화시키기 위하여 모델을 집합 이론적 방법으로 이용한 것으로, 시스템을 계층적(hierarchical)이고 모듈화(modular)된 형식으로 기술한다.

DEVS에서는 기본 모델(basic model)과 결합 모델(coupled model)을 정의한다. 기본 모델은 시

스템의 동적인 특성을 표현하기 위한 모델이고, 결합 모델은 시스템의 구성 요소간의 상호 작용을 표현하기 위한 모델이다. 기본 모델 M은 다음의 항들로 명세할 수 있다.

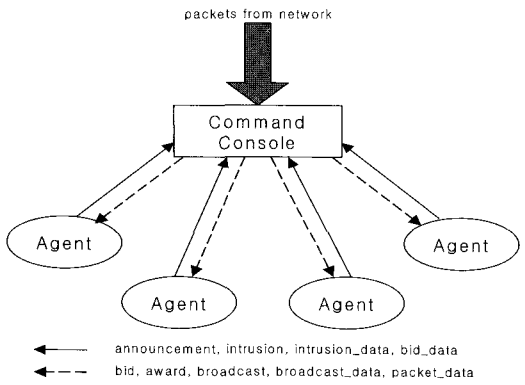
$M = \langle X, S, Y, \delta_{int}, \delta_{ext}, \lambda, ta \rangle$

- X : 외부 입력 집합
- S : 연속하는 상태 집합
- Y : 외부 출력 집합
- δ_{int} : 내부 전이 함수
- δ_{ext} : 외부 전이 함수
- λ : 출력 함수
- ta : 시간 전진 함수

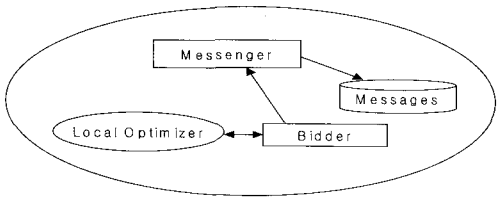
결합 모델 DN은 다음의 항들로 명세할 수 있다.

$DN = \langle D, \{M_i\}, \{I_i\}, \{Z_{i,j}\}, select \rangle$

- D : 컴포넌트 이름 집합
- M_i : 컴포넌트 기본 모델
- I_i : I의 영향 집합
- $Z_{i,j}$: 출력 해석(output translation)
- $select$: 타이-브레이킹 함수(tie-breaking function)



〔그림 2〕 CNP의 구조 및 자료의 흐름



〔그림 3〕 에이전트의 구조 및 자료의 흐름

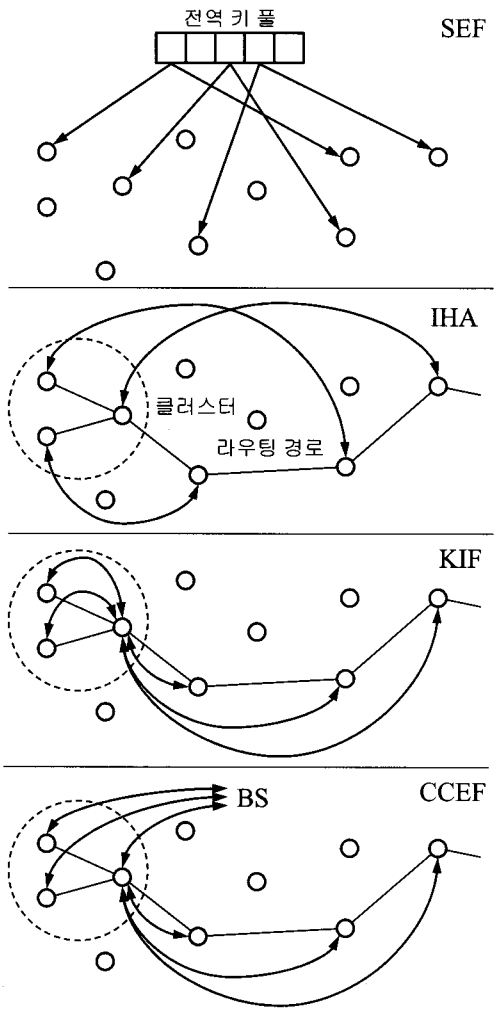
2.2 계약망 프로토콜

CNP[6]는 모듈화와 객체지향설계에 근거한다. 에이전트 모듈은 도메인에 독립적인 모듈과 도메인에 의존적인 모듈로 구성되는데 도메인에 독립적인 모듈에는 중앙 콘솔(command console), 메신저(messenger), 그리고 비더(bidder)가 있고, 도메인에 의존적인 모듈로 응용 프로그램에 의존적인 함수들을 호출하는 지역 옵티마이저(local optimizer) 모듈과 친밀하게 작동한다. 〈그림 2〉와 〈그림 3〉은 각각 CNP의 구조와 에이전트의 구조를 나타내며, 각 모듈들은 다음과 같이 동작한다. 중앙 콘솔은 에이전트들의 위치에 대한 정보를 가지고 있으며, 모든 에이전트들을 중앙에서 통제한다. 메신저는 에이전트들 사이에 메시지를 주고받는 것을 관리한다. 중앙 콘솔에서 선택된 에이전트로 어워드(award) 메시지를 받아들이며, 공고(announcement) 메시지를 중앙 콘솔에 보낸다. 에이전트의 위치를 알기 위해 중앙 콘솔에 질의(query)한다. 비더는 수신한 공고에 대한 응답으로 지역 옵티마이저로부터 에이전트의 상태 정보를 받아서 중앙 콘솔에 제출할 비드(bid)를 만든다. 지역 옵티마이저는 비드의 정보가 되는 정보를 계산하고 상태에 따라 갱신된 최신의 정보를 유지한다 (Seo 2005).

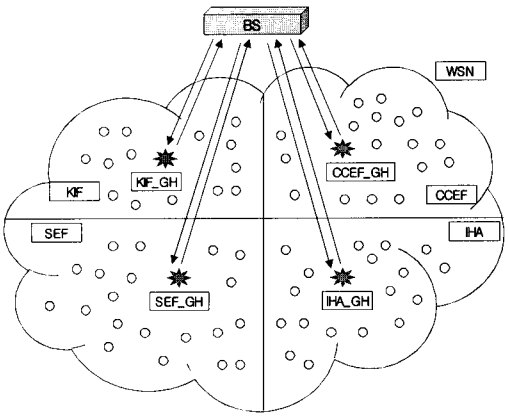
2.3 허위보고서 여과 기법들

허위 보고서들을 전달 과정 중 탐지하여 폐기위한 다양한 보안 기법들이 제안되고 있다. 대표적인 여과 기법들로는 통계적 전달 중 여과 기법(statistical en-route filtering scheme; 이하 SEF)[4], 인터리브드 홉-바이-홉 인증 기법(interleaved hop-by-hop authentication scheme; 이하 IHA)[3], 동적 전달 중 여과 기법(dynamic en-route filtering scheme; DEF)[7], 키 상속 기반 여과 기법(key inheritance-based filtering scheme; 이하 KIF)[9], 가환 암호 기반 전달 중 여과 기법(commutative cipher-based en-route filtering scheme; 이하 CCEF)[5] 등이 있다. 이들은 보고서 생성 노드들과 전달 노드들과의 키 공유를 통하여 허위 보고서 주입 공격에 대응한다. 각각은 고유의 키 공유 방법을 사용한다. 〈그림 4〉는 대표적인 여과 기법들에서의 키 공유 방법을 보인다. SEF에서 각 노드는 전역 키 풀에서 일부의 키들을 배치 전에 적재한다. IHA에서 각 노드는 일정 홉 떨어진 노드들과 키들을 공유한다.

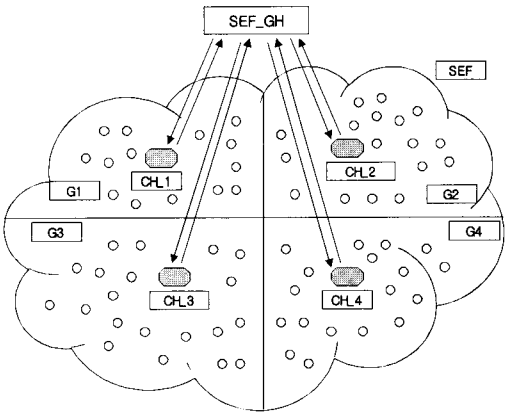
KIF에서 각 노드는 일정 홉 이내의 모든 노드들과 키들을 공유한다. CCEF에서는 질의가 클러스터 헤드(cluster head; 이하 CH)로 전달될 때, 암호 키는 CH에게, 복호 키는 전달 노드들에게 전달된다. 그러나 보고서들의 생성 및 검증 과정은 유사하다. 어떤 사건이 일어난 경우, 다수의 감지 노드들이 협력하여 사건 감지 보고서를 생성한다. 보고서는 그들의 키들로 생성된 메시지 인증 코드(message authentication code; 이하 MAC)들을 보고서에 덧붙임으로써 인증된다. 보고서가 BS를 향해 다수의 홉들을 지나 전달됨에 따라, 각 전달 노드는 보고서의 일부 MAC들을 자신의 키들을 사용하여 검증한다. 만약 검증이 실패하면, 보고서는 즉각 폐기된다.



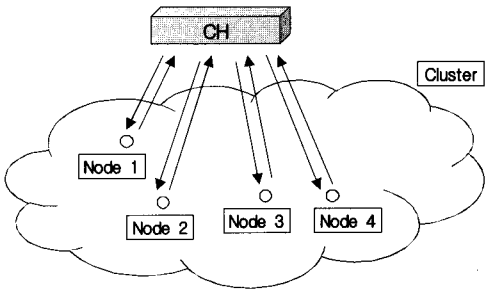
〔그림 4〕 허위 보고서 여과 기법들에서의 암호 키 공유



〔그림 5〕 대상 네트워크의 구조도



〔그림 6〕 그룹의 구조도



〔그림 7〕 클러스터의 구조도

본 연구에서는 대상 네트워크를 크게 〈그림 5〉와 같이 4개의 큰 그룹으로 구분하였다. 각 그룹을 다시 〈그림 6〉과 같이 여러 개의 클러스터로 구분하였으며, 각 클러스터는 〈그림 7〉과 같이 구성되어 재귀적으로 네트워크 단위가 선택되도록 구성하였다.

III. 경계 값 결정을 위한 재귀적 CNP의 적용

본 논문에서는 대규모 USN을 가정한다. 네트워크에서는 허위 보고서들을 여과하고, 정상 보고서들을 BS로 전달하기 위하여, 다양한 구조들을 사용한다. 본 논문에서 네트워크는 〈그림 5〉와 같이 SEF, IHA, CCEF, KIF 4개의 구조들로 그루핑된다고 가정한다. 이는 센서 노드들의 위치와 역할에 따라 허위 보고서들의 에너지 효율적인 여과 방법이 다르기 때문이다. SEF의 경우, 비용(overhead)은 작지만, 여과 성능이 떨어지고 훼손의 결과가 전역적으로 영향을 미치므로, 상대적으로 안전한 지역에 적합한 반면, IHA나 KIF는 여과 성능이 좋고 훼손 결과가 지역적으로만 영향을 미치지만, 비용이 높아 위험한 지역에 보다 적합하다 (Lee 등, 2007a). 각 그룹에는 구조를 대표하는 그룹 헤드(group head; 이하 GH)가 존재한다 (그림 6 참조). BS는 이러한 GH들을 통하여 데이터를 송신하거나 수신한다. 각 그룹은 노드들의 수와 특성에 따라서 여러 개의 클러스터(서브 그룹)들을 가진다. 각 클러스터에는 〈그림 7〉과 같이 CH가 존재하며, GH는 이 CH들을 통하여 데이터를 주고받는다. 각 클러스터에는 경계 값에 해당하는 말단 노드(terminal node)들이 존재하게 되며, CH와 노드들이 통신한다.

3.1 퍼지 기반 경계 값 결정

제안 기법에서는 BS에서 퍼지 로직을 사용하여 경계 값을 구한다. 경계 값 결정에는 훼손된 노드들의 수, 노드가 훼손되지 않은 키들을 가질 확률, 그리고 에너지 수준이 사용된다.

허위 보고서들의 여과를 위한 보안 기법들에서 보안 경계 값은 공격자에게 노출된 노드들, 즉 훼손된 노드들의 수보다 커야 한다[3]. 만약 훼손된 노드들의 수가 경계 값을 초과하게 되면, 공격자는 허위 보고서들에 포함되어야 할 모든 인증 키 정보를 얻을 수 있으므로, 보안 기법들은 더 이상 허위 보고서들에 대한 여과 기능을 수행할 수 없을 수 있다. 따라서 훼손된 노드들의 수를 고려해 경계 값을 결정해야 한다.

그리고 노드들이 공격자에게 노출되지 않은, 즉 훼손되지 않은 인증 키들을 가지고 있을 확률 역시 고려되어야 한다. 왜냐하면 이 확률은 각 노드의 개별 여과 능력을 보여주는 값으로써 현재 네트워크 환경에 적용돼 있는 보안 경계 값이 현재 훼손도에서 어느 정도의 여과 수준을 제공할 수 있는지를 보여줄 수 있는 값이기에 이 정보를 기반으로 경계 값을 더 증가시킬지, 감소시킬지를 결정할 수 있기 때문이다.

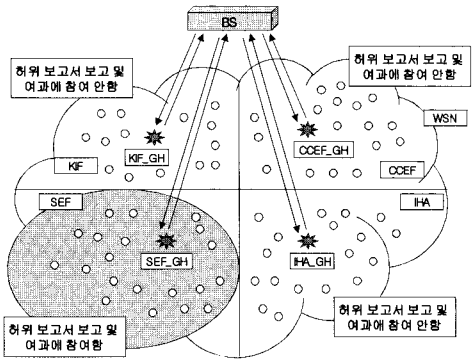
에너지는 USN에서 반드시 고려해야할 중요한 자원이다. 일반적으로 센서 노드들은 제한된 능력을 가지고 방치되므로, 전원에 제약이 있으며 교체가 불가능하다[14]. 에너지 수준이 매우 낮은 경우에는, 보안 기법의 가동을 중지하는 편이 에너지 효율적일 수 있다[8-9]. 그러므로 에너지 수준을 고려하여 경계 값을 결정해야 한다.

이러한 요소들은 명확한 값이 아닌 확률로서 존재하는 경우가 많으므로, 퍼지 로직을 적용하여 경계 값을 효과적으로 구할 수 있다.

3.2 계약망 프로토콜의 재귀적 적용

제안 기법에서는 각 계층의 통신에 CNP를 재귀적으로 적용함으로써, 통신에 참여하는 노드의 수를 최소화하며, 보다 효과적으로 허위 보고서들을 여과하게 된다[15].

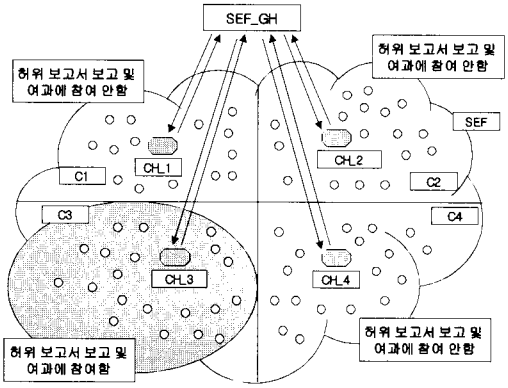
〈그림 8〉과 같은 1차 CNP의 적용은, BS와 허위 보고서들이 발생한 그룹(구조)들만의 경계 값 변경을 위한 통신을 가능하게 하므로, 그 외의 다른 그룹들에 속한 노드들은 에너지를 보존할 수 있다.



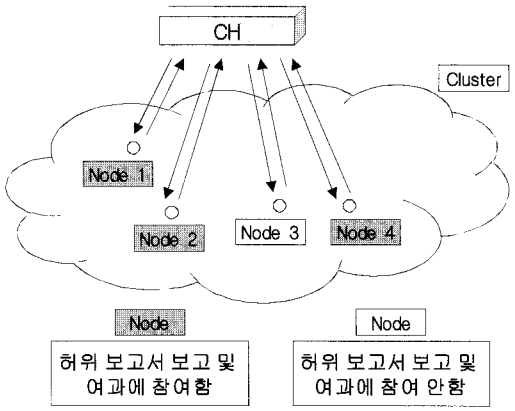
〔그림 8〕 1차 CNP 적용

동일 그룹 내에서도 허위 보고서들의 보고 및 여과에 참여하지 않은 클러스터들이 생겨나게 되고, 이러한 클러스터들에 속한 노드들은 경계 값을 변경할 필요가 없다. CNP의 2차 적용으로, 〈그림 9〉와 같이 허위 보고서들의 보고 및 여과에 참여하는 클러스터들만이 통신에 참여하게 되어, 경계 값 변경이 불필요한 클러스터들에 속한 노드들의 에너지 소모를 방지할 수 있다.

허위 보고서들의 여과에 참여하는 각 클러스터에서, 클러스터 노드들은 BS에서 통보한 경계 값에 따라 데이터를 BS에 전송하기 전에 자신의 MAC들을 보고서에 추가하여 전송하게 된다. 〈그림 10〉과 같은 3차 CNP의 적용으로, 자신의 에너지 수준이 충분하지 않고, 현재의 보고에 자신이 결정적인 여과 역할을 수행할 수 없다고 판단하는 노드들(예를 들어, 노드 3)은 비드에 참여하지 않을 수 있으며, 결국 이러한 노드들의 생존성을 높일 수 있다.



〔그림 9〕 2차 CNP 적용

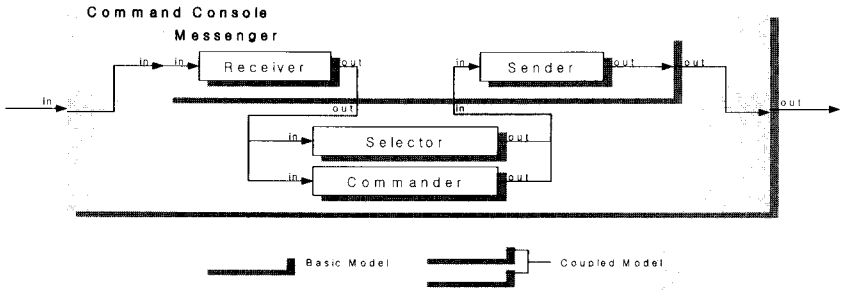


〔그림 10〕 3차 CNP 적용

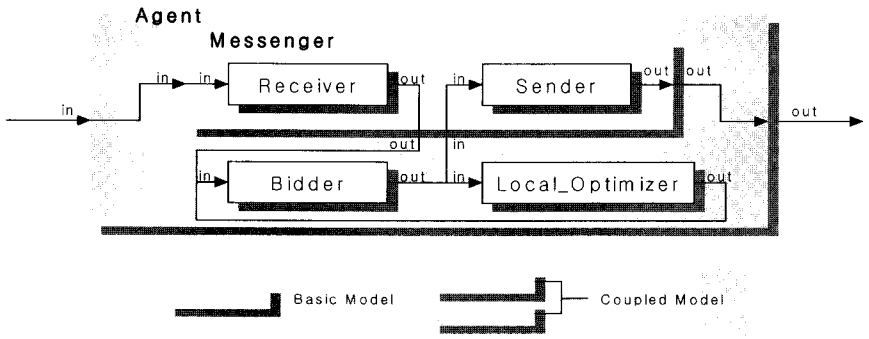
3.3 구성 요소들의 DEVS 모델링

〈그림 11〉과 〈그림 12〉는 각각 CNP의 주요 구성요소인 중앙 콘솔과 에이전트의 DEVS 모델이다. 중앙 콘솔 모델은 'Messenger', 'Selector', 및 'Commander'의 서브 모델들로 구성되며, 각각의 기능은 다음과 같다.

■ Messenger : 메시지의 송수신을 관리한다.



〔그림 11〕 중앙 콘솔 모델의 구조도



〔그림 12〕 에이전트 모델의 구조도

- Receiver : 에이전트들이 보낸 메시지들을 수신한다.
- Sender : 'Selector'나 'Commander'가 생성한 메시지들을 해당 에이전트나 모든 에이전트들에게 보낸다(유니캐스트, 멀티캐스트, 브로드캐스트).

■ Selector : 모든 에이전트들이 보낸 비드로 허위 보고서들의 보고 및 여과를 수행할 에이전트를 선택한다.

■ Commander : 네트워크의 상태에 따라 에이전트들을 통제하는 커맨드를 결정한다.

각 에이전트 모델은 'Messenger,' 'Bidder,' 및 'Local_Optimizer'의 서브 모델들로 구성되며, 각각의 기능은 다음과 같다.

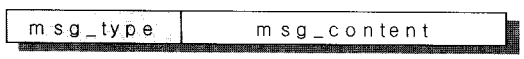
■ Messenger : 메시지의 송수신을 관리한다.
- Receiver : 중앙 콘솔에서 보낸 메시지들을 수신한다.
- Sender : 'Bidder'가 생성한 메시지들을 보낸다.

■ Bidder : 'Local_Optimizer'와 통신하여 비드를 만들고, 보안 기법 모델을 중앙 콘솔의 명령에 따라 통제한다.

■ Local_Optimizer : 서브 네트워크의 상태와 같이 비드를 위해 제공되는 정보를 관리하고 최적화한다. 훼손된 노드들의 수, 노드가 훼손되지 않은 키들을 가질 확률, 에너지 수준에 대한 상태 정보를 관리한다.

3.4 구성 요소들 간의 통신

〈그림 13〉은 구성 요소들 간의 통신을 위한 메시지의 구조와 종류이다. 메시지의 종류는 크게 컨트롤 메시지와 데이터 메시지로 나뉘며, 'msg_type' 필드의



	msg_type	메 시 지 종 류
Control Message	0	Broadcast
	1	Announcement
	2	Bid
	3	Award
	4	Intrusion
Data Message	5	broadcast_data
	6	bid_data
	7	packet_data
	8	intrusion_data

〔그림 13〕 메시지 구조

값에 의해 판단한다.

컨트롤 메시지에는 다음의 다섯 가지가 있다. 'Bid' 메시지는 비드를 제출하도록 모든 에이전트들에게 알린다. 'Award' 메시지는 중앙 콘솔에서 선택된 에이전트에게 여과 에이전트로 선택된 것을 알린다. 'Intrusion' 메시지(허위 보고서 경보)는 허위 보고서 탐지 시 해당 에이전트가 중앙 콘솔에 알린다. 'Announcement' 메시지는 에이전트에서 여과를 수행할 수 없는 상황이 되거나 상태 전이로 에이전트 선택을 다시 해야 할 경우 중앙 콘솔에 알린다. 'Broadcast' 메시지는 에이전트가 허위 보고를 탐지하면 탐지에 대한 정보를 받은 중앙 콘솔이 모든 에이전트에 탐지 정보를 보낸다는 것을 알린다.

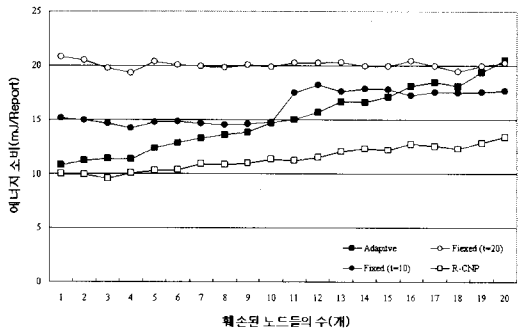
데이터 메시지는 네 가지가 있다. 비드 데이터 'bid_data'는 입찰 과정에서 에이전트를 선택하기 위해 필요한 정보를 가지며, 'intrusion_data'는 허위 보고서를 탐지하한 에이전트의 정보를 가진다. 'packet_data'는 네트워크로 유입되는 패킷의 정보를 가지고 있다. 마지막으로 'broadcast_data'는 허위 보고서 관련 정보를 포함한다.

IV. 시뮬레이션 결과

제안 기법의 효율성을 보이기 위하여 시뮬레이션을 수행하였다. 기존 연구에서 사용하였던 시뮬레이션 환경을 사용하여, 본 제안 기법의 우수성을 보이고자 한다[8-11]. 시뮬레이션에서는 제안 기법, 기존의 보안 경계 값 결정 기법, 그리고 경계 값이 고정된 경우를 비교하였다. 각 노드는 초기에 2,500mJ의 에너지 자원을 가지며, 1 바이트 송/수신에 각각 16.25μJ/12.5μJ을, 1개의 메시지 인증 코드 생성에는 15μJ을 소비한다. 하나의 메시지 인증 코드는 1 바이트이며, 원본 보고서의 크기는 24 바이트이다. 각 클러스터에서 단말 노드들의 수는 최대 20개이다.

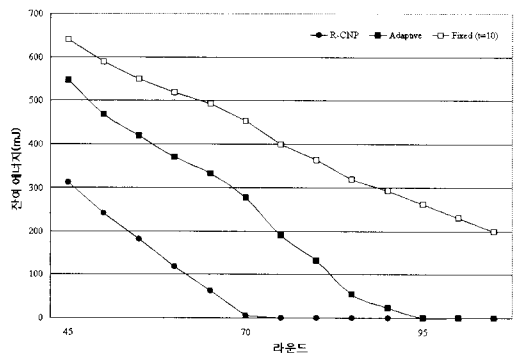
〈그림 14〉는 훼손된 노드들의 수가 0에서 20까지 한 보고서 전달에 소비된 평균 에너지 소비량이다. 〈그림 14〉에서 보듯이, 경계 값이 고정된 경우(빈 원 및 채워진 원), 훼손된 노도들의 수와 관계없이 일정한 에너지를 소비함을 알 수 있다. 특히, 훼손된 노드들의 수가 경계 값을 초과하면 에너지 소비가 증가함을 알 수 있다. 이 경우, 어떠한 허위 보고서들도 탐지되지 못하므로, 결과적으로 에너지를 불필요하게 낭비하게 된다. 기존의 보안 경계 값 결정 기법(빈 사각형)은 훼손된 노드들의 고려하여 경계 값을 조정함으로써, 경

계 값이 고정된 경우보다 에너지 효율적이다. 특히 제안된 기법(채워진 사각형)은 네트워크를 계층적으로 나누고 CNP를 적용함으로써 기존의 기법들에 비해 보다 적은 에너지를 소비함을 알 수 있다. 이는 기존 기법들과는 다르게, 제안 기법에서는 보안 경계 값의 변경이 반드시 필요한 클러스터 또는 그룹(허위 보고서들이 발생한 지역)에만 적용되기 때문이다.



〔그림 14〕 보고서 당 에너지 소비량

〈그림 15〉는 라운드에 따른 노드의 평균 잔여 에너지량의 변화를 보인다. 〈그림 15〉에서 보듯이 제안 기법 및 기존의 경계 값 결정 기법이 경계 값이 고정된 경우(빈 사각형)보다 에너지를 절약함으로써 네트워크의 수명을 늘릴 수 있음을 보인다. 특히 제안 기법의 경우, 경계 값 변경을 위한 통신에 참여하는 노드들을 최소화하여, 네트워크의 수명을 보다 더 늘릴 수 있음을 알 수 있다.



〔그림 15〕 라운드에 따른 잔여 에너지량 변화

V. 결 론

본 논문에서는 충분한 보안성을 제공하면서 에너지를 절약할 수 있는 보안 경계 값 결정을 위한 재귀적 CNP 적용 기법을 제안하였다. BS는 퍼지 로직을 활용하여 경계 값을 결정하며, 노드가 훼손되지 않은 인증키들을 가지고 있을 확률, 훼손된 노드들의 수, 노드의 잔여 에너지 수준을 입력으로 사용한다. 네트워크를 보다 효율적으로 운용하기 위하여, 네트워크를 계층적으로 그루핑하고, 각 그룹에 대하여 순차적으로 CNP가 적용되는 기법을 제안하였다. 시뮬레이션 결과를 통하여 제안 기법이 기존 기법들에 비해 에너지 효율적이며, 네트워크의 수명을 늘릴 수 있음을 보였다.

참 고 문 헌

〔1〕 I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirici, "A Survey on Sensor Networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

〔2〕 W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach," Proc. INFOCOM, pp. 503-514, Mar. 2005.

〔3〕 S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," Proc. S&P, pp. 259-271, May 2004.

〔4〕 F. Ye, H. Luo, and S. Lu, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 4, pp. 839-850, Apr. 2005.

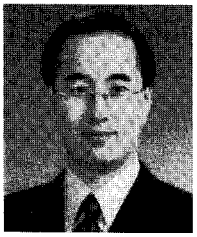
〔5〕 H. Yang and S. Lu, "Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks," Proc. VTC, pp. 1223-1227, Sep. 2004.

〔6〕 J. Yang, R. Havaldar, V. Honavar, L. Miller, and J. Wong, "Coordination of Distrbuted Knowledge Networks Using Contract Net Protocol," Proc. ITC, pp. 71-74, Sep. 1998.

〔7〕 Z. Yu and Y. Guan, "A Dynamic En-route Scheme for Filtering False Data Injection

in Wireless Sensor Networks," Proc. SenSys, pp. 294-295, Nov. 2005.
[8] H.Y. Lee and T.H. Cho, "Fuzzy Adaptive Threshold Determining in the Key Inheritance Based Sensor Networks," Lecture Notes in Artificial Intelligence, vol. 4570, pp. 64-73, July 2007.
[9] H.Y. Lee and T.H. Cho, "Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks," IEICE Transactions on Communications, vol. 90, no. 12, pp. 3346-3353, June 2007.
[10] S.J. Lee, H.Y. Lee, and T.H. Cho, "A Threshold Determining Method for the Dynamic Filtering in Wireless Sensor Networks Based on Fuzzy Logic," International Journal of Computer Science and Network Security, vol. 8, no. 4, pp. 155-159, Apr. 2008.
[11] H.Y. Lee and T.H. Cho, "Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks," Lecture Notes in Computer Science, vol. 4317, pp. 116-127, Dec. 2006.
[12] S.R. Kim and T.H. Cho, "Application of Fuzzy Logic for Adaptive Filtering in the Statistical Filtering based Sensor Networks," Proc. NMC, p. 18, Aug. 2006.
[13] B.P. Zeigler, H. Praehofer, and T.G. Kim, Theory of Modeling and Simulation, ACADEMIC PRESS, pp. 53-89, Jan. 2000.
[14] S.H. Chi and T.H. Cho, "Fuzzy Logic based Propagation Limiting Method for Message Routing in Wireless Sensor Networks," Lecture Notes in Computer Science, vol. 3983, pp. 58-64, May 2006.
[15] H.S. Seo, "Network Security Agent DEVS Simulation Modeling," Simulation Modelling Practice and Theory, vol. 14, no. 5, pp. 481-492, Aug. 2005.

〈著者紹介〉



서 희 석 (Hee Suk Seo) 종신회원
2000년 2월: 성균관대학교 산업공학과 (공학사)
2002년 2월: 성균관대학교 전기전자및컴퓨터공학과 (공학석사)
2005년 2월: 성균관대학교 전기전자및컴퓨터공학과 (공학박사)
2005년 3월 ~ 현재: 한국기술교육대학교 인터넷미디어공학부 정보보호전공 조교수
〈관심분야〉 악성코드 분석, 네트워크보안, 보안 시뮬레이션, USN