디지털산업정보학회 논문지 제4권 제4호 - 2008년 12월

계약망 프로토콜과 DEVS 모델링을 통한 센서네트워크 보안 모델의 설계

허 수 만* · 서 희 석**

Design of Sensor Network Security Model using Contract Net Protocol and DEVS Modeling

Hur, Suh Mahn · Seo, Hee Suk

<Abstract>

Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects forged reports into the network through compromised nodes. Such attacks by compromised sensors can cause not only false alarms but also the depletion of the finite amount of energy in a battery powered network. In order to reduce damage from these attacks, several security solutions have been proposed. Researchers have also proposed some techniques to increase the energy-efficiency of such security solutions. In this paper, we propose a CH(Cluster Header) selection algorithm to choose low power delivery method in sensor networks. The CNP(Contract Net Protocol), which is an approach to solve distribution problems, is applied to choose CHs for event sensing. As a result of employing CNP, the proposed method can prevent dropping of sensing reports with an insufficient number of message authentication codes during the forwarding process, and is efficient in terms of energy saving.

Key Words : Sensor Network, False Report, Filtering, Contract Net Protocol, Security Model

Ⅰ. 서 론

최근 무선 통신의 발전과 초미세 전자기계 시스템의 발전은 저 비용의 센서 네트워크 구성을 가능하게 하였다. 저 비용의 센서네트워크는 사람을 대신하여 위험한 군사 지역에 이용될 뿐만 아니라 유통관리, 생산 관리, 환경 및 재난 관리, 에너지 관리, 의료 및 건강 서비스, 지능형 교통시스템 등 수많은 분야에 응용될 것으로 예측되고 있다[1,2]. 이러한 무선 센서네트워크는 제한된 베터리 용량, 한정된 무선통신 범위 그리고 작은 메모리 공간을 가지고 있는 많은 센서노드들과 센서 네트워크를 인터넷과 같은 기존 통신 인프라와 연결하여 센서노드들이 센싱한 정보를 모아서 사용자에게 전달해주는 베이스 스테이션(Base station)으로 구성되어 있다[3].

* 한국기술교육대학교 정보미디어공학과 석사
** 한국기술교육대학교 인터넷미디어공학부 교수(교신저자)

많은 센서네트워크 응용분야에서 센서노드는 개별 관리가 어려운 개방된 환경에 배치된다. 이런 특징으로 인해, 공격자는 센서노드를 물리적으로 쉽게 획득(compromising)할 수 있으며 획득한 센서노드(compromised node)를 이용하여 허위보고서를 쉽게 베이스 스테이션으로 보낼 수 있다. 허위보고서는 제한된 에너지 자원을 가진 센서노드의 수명을 단축시킬 뿐만 아니라 베이스 스테이션과 관리자의 중요한 결정에 혼란을 유발 시킬 수도 있다. 이러한 허위보고서의 피해를 최소화하기 위해서는 허위보고서를 전송 중에 발견하여 걸러 내야하며, 걸러지지 않은 허위보고서는 베이스 스테이션에서 발견하고 제거해야 한다.

최근 이러한 허위 경고 공격을 막기 위해 몇몇의 필터링 기반 보안 기법이 제안되었다. 그중 하나가 Fan Ye et al.이 제안한 통계적 여과 기법 (SEF : Statistical En-route Filtering)[4] 이다.

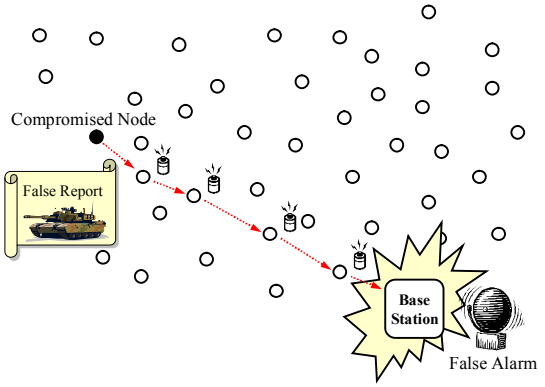
본 논문에서는 통계적 여과 기법을 센서네트워크 계약망 프로토콜 보안 모델의 위조 보고서 검출에 적용하고 그 과정에서 가장 적합한 클러스터헤드를 선출하는 알고리즘을 제안함으로써 에너지효율을 극대화 하고자 노력하였다.

본 논문은 다음과 같이 구성된다. 2장에서는 배경이론으로 공격모델과 통계적 여과 기법, k-covered 그리고 계약망 프로토콜에 대해서 간단히 설명하고, 3장에서는 동기와 센서네트워크의 계약망 프로토콜에 통계적 여과 기법을 적용함에 있어서 가장 최상의 클러스터헤드를 선출하는 알고리즘을 제안하며, 4장에서는 보안모델에 대한 DEVS 모델링을 적용해 보고 5장에서는 결론과 향후 연구 과제에 대해 논의한다.

Ⅱ. 관련연구

2.1 허위 경고 공격(False Positive Attack)

많은 센서네트워크 응용분야에서 센서노드는 센서노드별 관리가 어렵고, 개방된 환경에 배치된다. 이러한 센서노드의 취약점을 이용하여 공격자들은 배치된 센서노드를 물리적으로 쉽게 획득할 수 있으며, 획득한 센서노드가 가지고 있는 인증키를 이용하여 허위보고서를 만들어 센서네트워크에 전송할 수 있다.

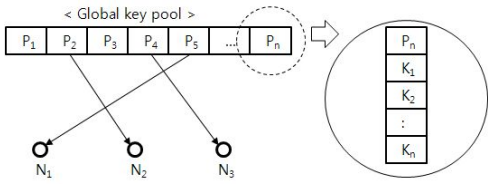


<그림 1> 허위 경고 공격

<그림 1>은 공격자가 포획한 센서노드를 이용한 허위 경고 공격을 보여주고 있다. 공격자에 의해 만들어진 허위보고서는 제한된 에너지 자원을 가지고 있는 센서노드의 수명을 단축시킬 뿐만 아니라, 베이스 스테이션에 전달되어 관리자의 판단에 혼란을 초래할 수도 있다.

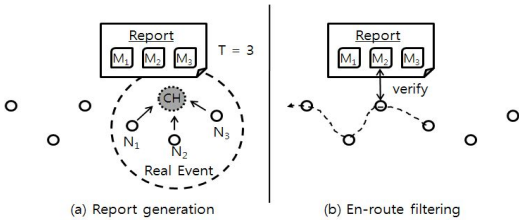
2.2 통계적 여과 기법(SEF : Statistical En-route Filtering Scheme)

통계적 여과 기법에서 노드들에게 키를 할당 방법은 <그림 2>와 같이 베이스 스테이션의 특정 구획의 키들 중 사용자가 지정한 개수의 키를 각 노드에 저장한 후 관심 지역에 배치하게 된다.



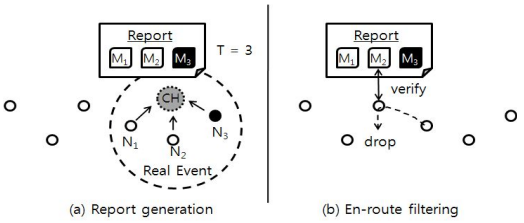
<그림 2> 배치 전에 각 노드들에게 키 할당

이벤트가 발생하면 이벤트를 탐지한 노드들 중 한 노드가 클러스터 헤드로 선택이 된다. 그 주변노드들은 감지한 이벤트 데이터 메시지와 각각 자신이 소유한 키들 중에서 하나의 키를 임의로 선택해서 이벤트 데이터에 대한 MAC을 생성한다. 그리고 두 메시지를 클러스터 헤드(CH: cluster head)로 선택된 노드에 전달하면, 클러스터 헤드가 이벤트에 관한 보고서를 생성한다. 이때 보고서는 서로 다른 구획의 키로 인증된 MAC으로 구성되어야 한다.



<그림 3> Report generation and En-route filtering

<그림 3>은 리포트 생성과 En-route 필터링 과정을 보여준다. T는 보안 임계값으로써 위 <그림 3>에서 T의 값은 3 이다. 클러스터 헤드에서 작성된 보고서는 멀티홉 방식으로 베이스 스테이션에 전달되며, 전달되는 동안 중간노드에서는 자신이 보유한 키들이 작성된 보고서에 사용되고 있는지 여부를 확인한다. 여기서 자신이 갖고 있는 키가 없으면 다음 노드로 전달하고, 그렇지 않으면 보고서에 관한 MAC을 구성하여 보고서에 사용된 메시지 인증코드와 비교하여 정상적인 MAC인 경우에만 다음 노드로 전달하게 된다.

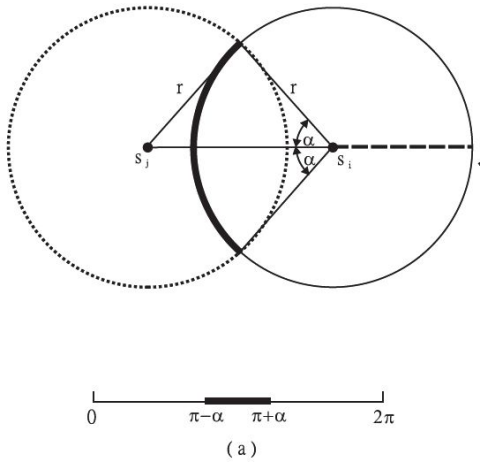


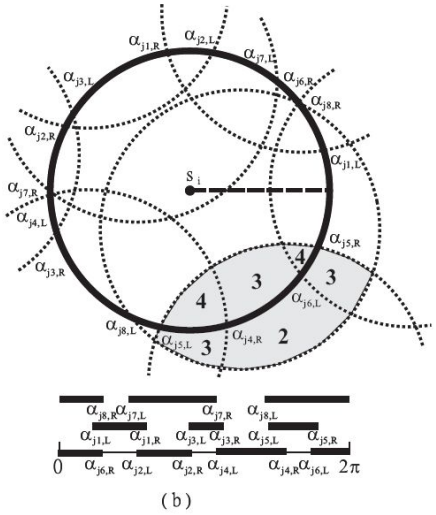
<그림 4> Forged report filtering

이와 같은 방법을 통하여 정상 메시지만 베이스 스테이션에 전달되고, <그림 4>와 같이 위조 메시지는 중간에서 여과되며 최악의 경우에는 모든 키를 소유한 베이스 스테이션에서 같은 방법으로 메시지에 사용된 모든 MAC을 증하게 된다. 이러한 방법을 통하여 위조 메시지 공격에 대응할 수 있으며, 전체 네트워크에서 사용되는 에너지 소모를 줄일 수 있다. <그림 4>는 계적 여과 기법의 여과과정을 보여주고 있다.

2.3 k-covered

Chi-Fu와 Yu-Chee[5]가 제안한 k-covered 개념은 아래 그림과 같이 어떤 지역의 중복된 Coverage를 구해 불필요한 노드를 사용하지 않음으로써 Power Saving 효과를 얻을 수 있다.





<그림 5> perimeter-coverage

두 개의 센서 노드 S_i와 S_j가 각각 $(X_i,\ Y_i)$, $(X_j,\ Y_j)$의 좌표에 있다면 두 노드 사이의 거리는 수식(1)같다.

$$d(S_i, S_j) = \sqrt{|X_i - X_j|^2 + |Y_i - Y_j|^2} \qquad \text{수식(1)}$$

조건 $d(S_i,\ S_j) \le 2r$에서 각도 α는 수식(2)와 같이 구해진다.

$$\angle \alpha = \arccos\left(\frac{d(S_i, S_j)}{2r}\right) \cdots\cdots \text{수식(2)}$$

한 원의 원주율은 π이므로 두 원의 원주율 2π를 직선상에 그리면 <그림 5>의 (a)와 같다. Si 노드가 Sj노드와 겹치는 원주율은 π-α에서 π+α가 된다. 이를 좀 더 복잡하게 실제 환경과 같이 그려보면 <그림 5>의 (b)와 같다.

관측지역의 모든 지역이 k개의 센서에 의해 센싱이 되는지에 관한 결정문제(decision problem)로써 k-UC (k-unit-disk Coverage)문제와 k-NC(k-non-unit-disk Coverage)문제로 나뉘게 되는데 두 문제의 차이점은 전자는 센싱 범위가 동일하며 후자는 동일하지 않음을 가정하고 있다.

2.4 계약망 프로토콜

계약망 프로토콜은 분산된 문제를 해결하는 것에 있어 통신하고 조정하기 위한 도구로서 제안되었다. 계약망 프로토콜의 사용은 분산감지 시스템과 분산전달 시스템을 위해서 시도되었다[6]. 계약망 프로토콜은 에이전트들이 계약(contract)에 의하여 분산된 문제를 해결하기 위해서 협상하고 통신하는 메커니즘을 제공한다[7]. 에이전트들은 수행될 필요가 있는 작업을 알리고 다른 에이전트들에 의해 공지된 작업들을 수행하기 위해 비드를 만들고, 중앙 콘솔은 각 에이전트들이 제출한 비드를 평가해서 계약을 체결한다.

Ⅲ. 계약망 프로토콜 적용 보안 모델

3.1 동 기

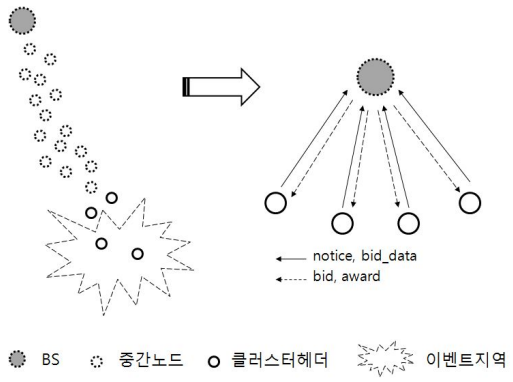
기존 필터링 보안 기법에서의 에너지 효율을 위한 여러 가지 방법들이 나오고 있다. 본 연구진은 에너지 효율을 위해 분산 문제 해결의 한 방법인 계약망 프로토콜을 적용하여 최적의 클러스터헤드를 선정하고자 한다.

계약망 프로토콜의 bid하는 과정에서 가장 적합한 클러스터헤드를 선정하고 클러스터 헤드 선택 알고리즘을 제안한다. 원 홉 관계로 클러스터링이 되는 통계적 여과 기법에서 최적의 클러스터헤드를 선정하는 것은 가장 중요한 요인이 된다.

k-covered 개념은 관측지역이 주어졌을 때, 해당 지역의 k-covered를 구하는 것이지만 본 논문에서는 이 원리를 이용해 클러스터 헤드와 겹치는 클러스터 노드의 개수를 구하고 클러스터헤드를 선정하는 지표로 사용한다. 클러스터헤드를 선정하고 선정된 클러스터헤드가 클러스터노드들의 MAC을 모아서 베이스 스테이션으로 리포트를 보내게 된다. 이 때 시스템에서 설정한 임계값보다 적으면 버려지게 된다. 임계값보다 많거나 적으면 에너

지효율 면에서 좋지 않다. 따라서 어떤 이벤트 지역을 탐지할 때 시스템에서 설정한 임계값을 만족하는 최소한의 클러스터노드를 가진 클러스터헤드를 선정하여 에너지 효율을 극대화 하고자 하였다.

3.2 메시지 구조와 가정사항



<그림 6> 센서네트워크의 예

본 논문은 모든 센서노드들의 센싱범위는 동일하고 센서노드들은 관심지역에 배치된 후에 원 홉의 클러스터링을 자동으로 형성할 수 있는 메커니즘을 가지고 있다고 가정한다. 또한, 모든 센서노드들의 위치를 알고 있다고 가정한다.

<그림 6>에서와 같이 최초 이벤트 발견 클러스터헤드는 베이스 스테이션에 이벤트가 발생했다고 notice 메시지를 보낸다. notice 메시지를 받은 베이스 스테이션은 해당지역의 클러스터헤드를 선정하기 위해 bid 메시지를 보낸다.

location	distance	nodes	power

<그림 7> bid_data 메시지 구조

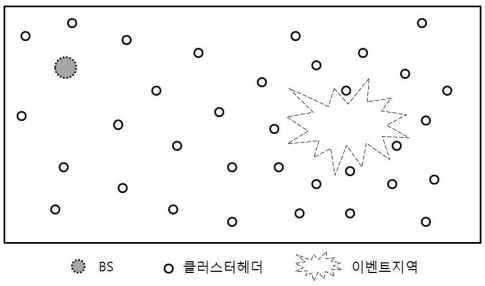
bid 메시지를 받은 클러스터헤드들은 베이스 스테이션에 bid_data 메시지를 보내게 되는데 bid_data는 <그림 7>와 같이 네 가지 필드로 구성된다. location 필드는 비드를 보내는 클러스터헤드의 위치를 나타내며 <표 1>과 같이 클러스터헤드가 이벤트 지역 안에 있으면 0, 밖에 있으면 1로 표시한다. distance 필드는 클러스터헤드와 Event 지역과의 거리이며 nodes 필드는 클러스터헤드와 클러스터 노드 간 센싱범위가 겹치는 클러스터 노드들의 수를 말한다. nodes 필드는 k-covered 개념을 사용하여 구한다. 그리고 Power 필드는 노드에 남아있는 에너지량을 수치화한 값이다.

<표 1> location field_type

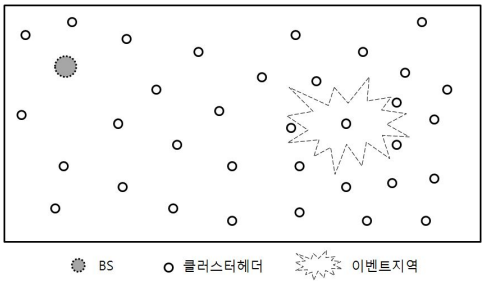
Field_type	필드 내용
0	이벤트지역 내
1	이벤트지역 밖

3.3 클러스터헤드 선택 알고리즘

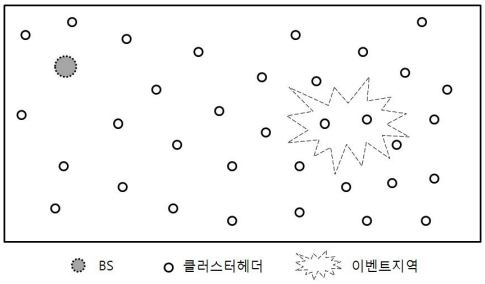
각 클러스터헤드는 nodes 필드의 값이 임계값을 넘을 경우에 bid_data를 베이스 스테이션에 보내게 되는데 첫 번째로 location 필드의 값을 기준으로 정렬하여 0(이벤트지역 내)과 1(이벤트지역 밖)이 있다면 0인 값이 선택이 된다. 이것은 이벤트지역내에 있는 클러스터헤드가 이벤트지역을 직접 탐지할 수 있는 확률이 높고 임계값을 만족하기 위한 클러스터노드수가 많기 때문이다. location 필드값으로 0이 2개 이상<그림 10>일 경우에는 nodes 필드로 가게 되고 1개 <그림 9>일 경우 클러스터헤드로 선택이 된다.



<그림 8> 이벤트지역 내 CH가 없을 경우



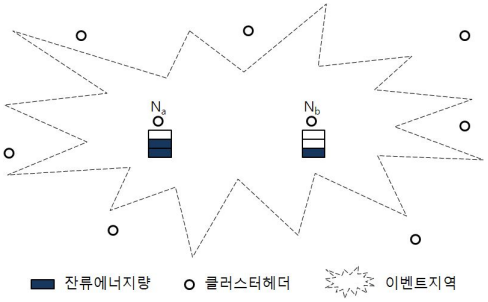
<그림 9> 이벤트지역 내 클러스터헤드가 1개인 경우



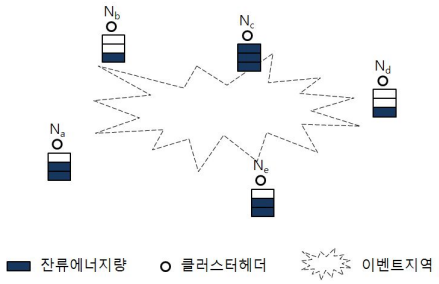
<그림 10> 이벤트지역 내 클러스터헤드가 2개인 경우

location 필드값으로 0은 없고 1이 2개 이상<그림 8>일 경우 distance 필드로 가게 되고 1개일 경우 클러스터헤드로 선택이 된다. nodes 필드에서는 클러스터 헤드와 센싱범위가 겹치는 클러스터 노드의 수가 나타내어진다. 이 중 가장 작은 클러스터 노드수를 가진 클러스터헤드가 선택이 된다. <그림 5>의 (b)그림은 클러스터헤드 S_i는 총 8개의 클러스터 노드들과 센싱범위가 겹치는 것을 알 수 있다. 만약 같은 클러스터 노드를 갖는 것이 있다면 클러스터헤드의 남아있는 전력량을 수치화한 power 필드를 보고 선택한다. <그림 11>는 이벤트지역 내 클러스터헤드가 2개 일때, 잔류에너지량을 나타낸 것이다. <그림 12>은 이벤트지역 내 클러스터헤드가 없고 이벤트지역 밖에 2개 이상일 때, 잔류에너지량을 나타낸 것이다. <그림 13>은 클러스터헤드의 선택 순서도이다.

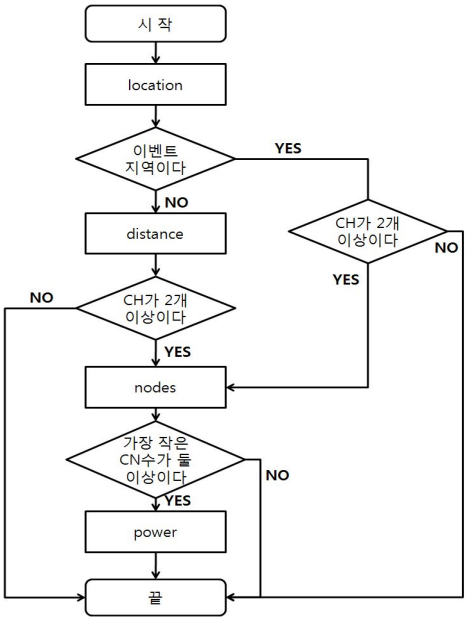
이런 과정이 끝나면 베이스 스테이션은 선택된 클러스터헤드에 award 메시지를 보내 최종적으로 이벤트 탐지 클러스터 헤드로 선택되었다는 것을 알린다.



<그림 11> 그림 8의 잔류에너지량



<그림 12> 그림 6의 잔류에너지량



<그림 13> 클러스터헤드 선택 순서도

Ⅳ. 보안 모델에 대한 DEVS 모델링

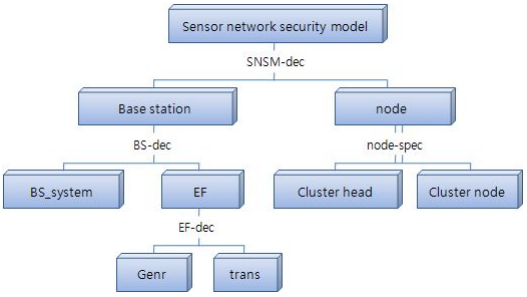
4.1 DEVS 방법론

Zeigler에 의해 정립된 DEVS 방법론은 연속적인 시간 상에서 발생되는 이산 사건을 처리하는 시스템을 시뮬레이션 하기 위해 이론적으로 정립된 모델링 방법론이다. 이는 모델의 구조와 행동을 시뮬레이션 수행으로부터 추상화시키기 위해 모델을 집합 이론적 방법으로 이용한 것으로, 시스템을 계층적(hierarchical)이고 모듈화(modular)된 형식으로 기술한다.[8,9,10]

DEVS에서는 기본 (Basic) 모델과 결합 (Coupled) 모델을 정의한다. 기본 모델은 시스템의 동적인 특성을 표현하기 위한 모델이고, 결합 모델은 시스템의 구성 요소 간의 상호 작용을 표현하기 위한 모델이다.

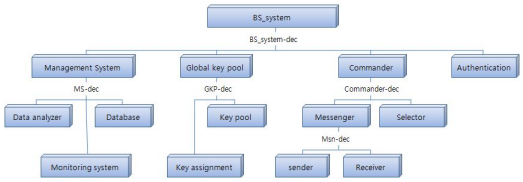
4.2 보안 시스템의 전체 구조

<그림 14>은 센서 네트워크 보안 모델에 대한 전체 구조도이다. SNSM (Sensor Network Security Model) 모델은 BS (Base Station) 모듈과 Node 모듈로 구성된다. BS 모듈은 노드들의 배치 전 키 분배 및 수신된 이벤트 리포트의 인증을 검사하는 모델로서 BS_system 모듈과 EF 모듈로 구성된다. Node 모듈은 실제 환경에 배치되는 모델로서 이벤트가 발생한 부분을 탐지, MAC을 생성하는 CN (Cluster Node) 모듈과 생성된 MAC을 송신받아 리포트를 생성하는 CH(Cluster Head) 모듈로 구성된다. BS_system 모듈은 BS 자체에 대한 모델이며 EF 모델은 시뮬레이션의 입력을 생성하는 모듈로서 시뮬레이션의 입력을 생성하는 Genr 모듈과 시뮬레이션의 통계 수집을 위한 Trans 모듈로 구성된다. 본 구조에 따른 시뮬레이션의 수행은 다음과 같다. 시뮬레이션 수행을 위해서 Genr 모듈에서는 노드의 수, 배치 지역의 크기, 이벤트의 범위, 이벤트 횟수 등의 환경에 따른 입력을 발생하여 BS_system 모듈로 전달하게 된다. BS_system 모듈은 이를 수신하여 자신의 각 영역에 입력값을 전달하여 시뮬레이션의 초기화를 수행한다.



<그림 14> 센서네트워크 보안 모델의 전체 구조도

4.3 베이스 스테이션 시스템의 모델링



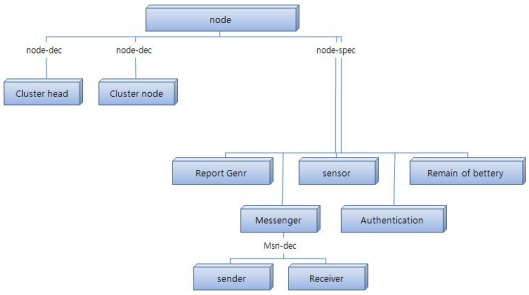
<그림 15> 베이스 스테이션 시스템의 구조도

<그림 15>는 베이스 스테이션 시스템에 대한 구조도를 상세하게 표현한 그림이다. 베이스 스테이션 시스템을 관리하는 Management System 부분은 Data analyzer, Monitoring system, Database 모듈로 구성된다. EF 모듈의 Genr 모듈이 전달해 주는 데이터를 이 모듈들이 받아서 전체적인 동작을 하게 된다. 이를 수신한 Global key pool 모듈은 전체 노드에게 key pool에 저장되어 있는 키를 랜덤하게 할당하고 해당 지역에 배치된다. 이벤트 발생 후 클러스터 헤드가 보내온 데이터를 Management System 모듈에서 분석하여 이를 Commander 모듈에 전송한다. Commander 모듈은 최종적으로 이벤트를 탐지할 클러스터 헤드를 Selector 모듈을 통해 선정하고 Messenger 모듈을 통해 해당 클러스터 헤드에 결과를 전송하게 된다. 베이스 스테이션 시스템의 Authentication 모듈은 node 모듈에 있는 Authentication

모듈과 같지만 최종적으로 리포트의 전체 MAC에 대해 인증한다는 특징이 있다.

4.4 노드의 모델링

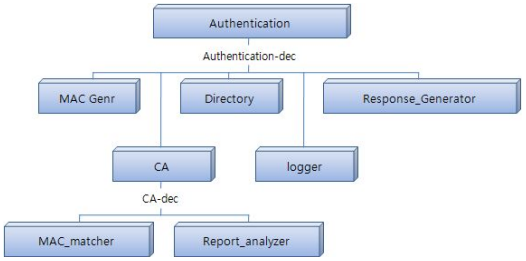
<그림 16>는 보안 모델 시스템의 노드 구조도이다. 각 노드는 리포트 생성기, 센서, 배터리, 메신저, 인증으로 구성된다. 센서는 이벤트를 탐지하기 위해서 필요한 모듈로서 센싱범위내에 이벤트가 발생되었는지 탐지하고 탐지되었다면 MAC 생성기 모듈을 통해 MAC을 생성한다. 메신저 모듈은 생성된 MAC을 CH로 보내거나 리포트를 BS로 보내는 역할을 한다. 배터리 모듈은 노드의 남아있는 에너지량을 파악하여 알려준다. 인증 모듈은 중간 노드의 리포트 인증, BS에서의 최종적인 리포트 인증을 담당하도록 구성한다.



<그림 16> 노드의 구조도

4.5 인증 시스템의 모델링

<그림 17>은 인증 모듈의 구조도이다. Directory 모듈은 배치되기 전에 할당 받았던 키와 key indices 등을 보관하는 역할을 수행하게 된다. MAC Genr 모듈은 Directory 모듈에서 키를 가져와 자신의 MAC을 생성한다. CA (Certification Authority) 모듈은 인증을 담당하는 역할을 수행하며 MAC_matcher 모듈과 Report_analyzer 모듈로 구성된다. 리포트를 송신받게 되면 Report_analyzer 모듈은 리포트를 분석하여 MAC을 추출하게 되고, MAC_matcher 모듈은 리포트에서 분석한 key indices에서 자신과 같은 key indices가 있는지 없는지 판단하여 있다면 자신이 만든 MAC과 비교하여 인증을 하게 된다. Response_Generator 모듈은 인증 결과에 따라서 패킷을 포워딩 할 것인지 버릴 것인지 결정하게 된다. logger 모듈은 이 모든 결과를 기록하는 역할을 수행한다.



<그림 17> 인증 모듈의 구조도

V. 결론 및 향후과제

센서 네트워크의 통계적 보안 기법에서는 적절한 클러스터헤드 선정에 관해 다루지 않았다. 클러스터헤드 선정을 위해 본 논문에서는 계약망 프로토콜을 적용하여 클러스터 헤드 선택 알고리즘을 제안하였다. 향후 과제는 계약망 프로토콜을 적용한 통계적 여과 기법의 에너지 효율과 필터링 효율 등의 성능을 분석하기 위한 시뮬레이션을 수행하는 것이다. 그리고 클러스터헤드 선택 알고리즘에서 예전 드롭되어진 리포트의 경험횟수(dropped report), 이벤트가 얼마나 발생했는지에 관한 이벤트횟수(event frequency)등을 고려한 클러스터헤드 선택 알고리즘 방법을 연구하여 보다 향상된 계약망 프로토콜을 적용한 센서 네트워크 보안 모델을 제안 하고자 한다.

참고문헌

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks," IEEE Commun. Mag, 2002, pp. 102-114.

[2] k. Akkaya, M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks," Ad hoc Netw. 3(3), 2004, pp.325-349.

[3] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," ACM,Proceeding of SenSys, 2003, pp. 255-265.

[4] F. Ye, H. Luo, S. Lu, and L. Zhang "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE J. Sel. Area Comm. 23(4), 2005, pp. 839-850.

[5] C.-F Huang, Y.-C Tseng "The Coverage Problem in a Wireless Sensor Network," In ACM International Workshop on Wireless Sensor Networks and Applications(WSNA), 2003, pp. 115-121.

[6] T. Sandholm, "An Implementation of the Contract Net Protocol based on Marginal Cost Calculations," in 11th National Conference on Artificial Intelligence (AAAI-93), Washington. DC, 1993.

[7] Jihoon Yang, Raghu Havaldar, Vasant Honavar, Les Miller and Johny Wong, "Coordination of Distrbuted Knowledge Networks Using Contract Net Protocol," Information Technology Conference, IEEE, 1998, pp. 71-74.

[8] Seo, Hee Suk and Cho, Tae Ho, "An application of blackboard architecture for the coordination among the security systems," Simulation Modelling Practice and Theory, Elsevier Science B.V., Vol. 11, Issues 3-4, Jul. 2003, pp. 269-284.

[9] Seo, Hee Suk and Cho, Tae Ho, "Simulation Model Design of Security System based on Policy-Based Framework," Simulation Transactions of The Society for Modeling and Simulation International, vol. 79, no. 9, Sep. 2003, pp. 515-527.

[10] Seo, Hee Suk, "Network security agent DEVS simulation modeling," Simulation Modelling Practice and Theory, Elsevier Science B.V., Vol. 14, Issues, Oct. 2005, pp. 481-492.

■ 저자소개 ■

허 수 만
Hur, Suhmahn

2007년 9월~현재
한국기술교육대학교
정보미디어공학과 정보보호전공
(공학석사)
2007년 2월 공주대학교 컴퓨터공학과 (공학사)

관심분야 : USN보안, 포렌식,
리버스엔지니어링
E-mail : acaciasu@kut.ac.kr

서 희 석
Seo, Heesuk

2005년 3월~현재
한국기술교육대학교 인터넷미디어
공학부 정보보호전공 교수
2005년 2월 성균관대학교 전기전자및컴퓨터공
학과 (공학박사)
2004년 3월~2005년 2월
(주)정보감리평가원 선임연구원
2002년 2월 성균관대학교 전기전자및컴퓨터공
학과 (공학석사)
2000년 2월 성균관대학교 산업공학과 (공학사)

관심분야 : 네트워크보안, 보안 시뮬레이션,
USN
E-mail : histone@kut.ac.kr

논문접수일 : 2008년 8월 11일
수 정 일 :
게재확정일 : 2008년 9월 10일