Node Compromise에 대한 무선 센서 네트워크의 취약성 및 위험 평가*

박종서** · 서윤경*** · 이슬기*** · 이장세**** · 김동성***

요 약

현재 다양한 공격 대응을 위해 효과적이고 효율적인 방법으로 네트워크와 정보시스템의 취약성을 평가하는 일은 매우 중요하게 여겨지고 있다. 그러나 네트워크와 정보시스템의 취약성 및 위험 평가 방법론은 센서 네트워크에 직접 적용하기가 어렵다. 왜냐하면 센서 네트워크는 전통적인 네트워크와 정보시스템과 비교해 다른 특성을 지니고 있기 때문이다. 본 연구 논문은 클러스터 기반 센서 네트워크에서의 취약성 평가 프레임워크를 제안하고 있다. 센서 네트워크에서 취약성을 평가하며 몇 가지 케이스를 통해 클러스터 기반 센서 네트워크의 취약성 평가 프레임워크의 실효성을 증명해 보인다.

Assessing Vulnerability and Risk of Sensor Networks under Node Compromise

Jong Sou Park** · Yoon Kyung Suh*** · Seulki Lee***
Jang-Se Lee**** · Dong Seong Kim***

ABSTRACT

It is important to assess vulnerability of network and information system to countermeasure against a variety of attack in effective and efficient way. But vulnerability and risk assessment methodology for network and information systems could not be directly applied to sensor networks because sensor networks have different properties compared to traditional network and information system. This paper proposes a vulnerability assessment framework for cluster based sensor networks. The vulnerability assessment for sensor networks is presented. Finally, the case study in cluster based sensor networks is described to show possibility of the framework.

Key words : Sensor Network Security Management, Vulnerability Analysis for Sensor Network

---

* 이 논문은 2006년도 한국항공대학교 교비지원 연구비에 의하여 지원된 연구의 결과임.
** 한국항공대학교 컴퓨터공학과 교수
*** 한국항공대학교 컴퓨터공학과
**** 한국해양대학교 컴퓨터제어전자통신공학부

1. 서 론

오늘날 센서 네트워크의 취약성을 분석하는 것에 대한 필요성은 점점 더 중요한 이슈가 되고 있다. 그러나 현재는 센서 네트워크의 취약성을 평가하는 데에 매우 미약한 연구만이 진행되고 있다. 최근, Anand[4]의 연구가 센서 네트워크에서 도청에 관한 취약성을 확률론적으로 정량화하는 것을 제안했다. 그 제안론은 확률론적인 방법으로 실현가능성을 보였고 특히, 도청 중인 공격자의 공격시 데이터 통합의 측면에서 접근하였다. Kannan[6]의 연구는 게임 이론적 관점을 이용했다. 취약성에 대응하여 최적의 센서 배치와 연관된 형식적인 프레임워크를 제안했다. 그러나 Kannan[6]의 연구는 엄밀히 말하면 센서 네트워크의 취약성을 따지기 보다는 센서 네트워크의 배치에 관한 것이다.

본 논문에서는, 노드 침해에 포커스가 맞춰진 취약성 분석 프레임워크를 제안한다. 즉, 센서 노드가 공격자에 의해 완전히 포획되고 조작 될 수 있는 상황을 고려하는 것이다[3]. 가장 먼저, 네트워크 안의 클러스터에 속해 있는 센서 노드 각각의 위상을 반영한 센서 노드 취약성을 표시한다. 이는 각각의 센서 노드의 취약성 값과 파급효과 값에 따른다. 특히, 다음의 관련연구를 통해 센서 노드의 취약성을 정량적인 어떤 범위 안에 들 수 있음을 보일 수 있다. Hartung의 연구[2]는 공격자가 센서 노드를 포획한 후 1분 안에 노드 안의 저장된 정보를 알아낼 수 있음을 나타낸다. Alarifi의 연구[1]는 노드 침해 공격의 대응을 위한 센서 네트워크의 탄력성을 강화시키기 위해 센서 노드에 다양한 변화를 준다. 제안한 방법 중에는 데이터를 알기 어렵게 뒤섞는 방법도 있다. 이런 경우, 센서 노드로부터 저장된 정보를 빼내는 데는 어느 정도 시간이 걸리게 된다. 두 연구를 통해 센서 노드의 탄력성을 고려하면 센서 노드 취약성의 정량화가 가능하게 된다. 두 번째로, 센서 노드 취약성을 센서 링크 단위, 센서 클러스터 단위, 센서 네트워크 단위로 확장 할 수 있다. 그 중에서도, 링크 취약성을 계산하기 위해서 두 가지 방법을 제안한다. 세 번째는, 센서 네트워크의 자산의 중요도에 대한 파급효과를 고려한 취약성 식으로 확장하였다.

본 논문의 구성은 다음과 같다. 관련 연구를 소개하고, 센서 네트워크의 취약성 및 위험 평가 프레임워크를 제안한다. 센서 네트워크의 취약성 평가 프레임워크의 검증을 위해 시나리오 별 시뮬레이션 한 것을 나타내고, 마지막으로 결론과 향후 연구에 대해 기술한다.

2. 취약성 분석

현재 위험분석은 보안 관리를 수행하기 위한 필수적인 과정으로 시스템의 위험을 평가하고, 비용효과적인 대응책을 제시하여 시스템 보안정책과 보안 대응책 구현계획을 수립하는 위험관리의 핵심적인 부분이다. 이는 정보시스템과 그 자산의 비밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협에 대해서 정보시스템의 취약성을 식별하고, 이로 인해 예상되는 손실을 분석하는 것으로서, 위험분석의 3대 요소인 자산, 위협, 취약성의 관계분석을 통해 조직에 효과적인 보안 대책을 수립한다. 다음은 위험분석의 3대 요소인 자산, 위협, 취약성에 대한 설명이다.

• 자산(Asset)

자산은 조직의 입장에서 가치를 갖는 모든 것을 통칭한다. 단, 정보시스템 환경에서 지칭하는 자산은 조직의 정보시스템 관련 자산들로 그 의미가 축소된다. 자산 분석을 통하여 보호해야할 자산들을 식별하고 체계적으로 분류하여, 소유하고 있는 자산들의 가치를 평가하게 된다.

• 위협(Threat)

위협은 시스템 또는 조직에 손실을 초래할 수

있는 원치 않는 사건을 일으키는 잠재적인 원인으로서, 자산에 해를 줄 수 있는 위험의 원천을 말한다. 위협분석은 이렇게 위협을 식별하고 분류하여, 발생 빈도와 손실 정도를 측정한다.

• 취약성(Vulnerability)

위협에 의해 이용될 수 있는 자산이 내포하고 있는 약점을 말한다. 다시 말해 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어 등에 존재하는 약점을 뜻한다. 취약성 분석은 이렇게 약점을 확인하고 분류하여 위협을 감소시키는 과정을 말한다. 효율적인 위험분석을 위해서는 자산 분석 후 취약성 분석과 위협 분석을 하게 된다. 이를 바탕으로 대응책을 모색하여 분석한 후 종합적인 위험평가를 거치게 되는 것이다[7, 8].

3. 센서 네트워크의 취약성

최근에 제안 된 센서 네트워크에 관한 취약성 연구 중 Anand의 연구가 있다[4]. 보안에 관하여, 센서 네트워크는 기존 분산 시스템과는 다르게 고려해야 할 것을 다음과 같이 제시하였다. 먼저, 센서 장비들은 물리적인 공격에 대해 취약하다. 두 번째로, 센서 장비들은 파워 공급과 프로세싱 제약이라는 매우 주요한 문제를 안고 있다. 세 번째로, 시스템의 데이터 집합 시 발생하는 보안 문제가 있다. 이들 중 마지막 문제에 집중한 Anand의 연구는 데이터 집합에 관한 취약점을 다룬다. 그의 연구는 전통적인 보안 기술들을 다시 살펴보아, 암호학적으로 보안을 강화시키는 것이 아닌 다른 방법으로 제약 조건들을 검토하였다. 공격자가 타겟에 기반을 둔 공격들의 분류를 시작으로, 도청을 위해 센서 네트워크의 취약성을 어떻게 평가하는지를 다루었다. 다음은 센서 장비에 가해지는 공격들을 세 가지로 분류한 것이다.

• 도청(Eavesdropping)

공격자(도청자)는 센서 네트워크의 출력 집합 데이터 결과를 노린다 : 이것은 시스템이 무엇을 관찰하고 있는지 보는 것이다. 즉, 센서 네트워크의 주체가 어떻게 반응하는지를 예상하는 것이다. 공격자는 노드로부터 전달된 메시지를 듣거나 직접 그 노드들과 타협한다. 다음은 도청의 두 가지 유형이다.

(a) 수동적 도청 : 공격자는 센서 노드에게 자신을 숨기고, 메시지를 도청하기 위한 중간 통신만을 한다.

(b) 적극적 도청 : 공격자는 센서나 데이터를 통합하는 어떠한 지점으로 쿼리를 보내면서 정보를 알아내기 위해 적극적으로 시도한다.

• 붕괴(Disruption)

공격자의 목표는 센서 응용 프로그램을 방해하는 것이다. 이는 두 가지 기술의 결합으로 이뤄질 수 있다.

(a) 의미론적 분열 : 공격자는 변질되거나 사용할 수 없게 된 데이터 집합을 제공하기 위해 메시지를 주입하고, 데이터를 매수하고, 값들을 변화 시킨다.

(b) 물리적 분열 : 공격자는 직접적으로 환경을 조작함으로써 센싱 데이터를 뒤엎는다. 예를 들면, 센서 부근에 열을 발생시켜 잘못된 값이 보고되도록 하는 것이다.

• 가로채기(Hijacking)

붕괴된 모델의 변질은 공격자가 그 선택 값에 따라 센서 응용 프로그램의 출력 집합을 통제하는 경우를 말하는 것이다. 만약 공격자의 선택 값이 가장 크다면 공격자가 충분한 센서들을 조정할 수 있게 되는 것이다.

Anand의 연구는 공격자가 센서 네트워크의 출력 집합 값을 확인하는 것이 목표인 경우를 다룬다. 그리고 시스템이 보고 있는 것을 보호하는 즉,

시스템의 유저가 어떻게 반응하는지를 예측하는 능력을 보호하는 것이다. Anand의 제안 방법은 환경에 대해 가능한 한 가장 정확한 정보를 돌려받기 위해 센서 네트워크 응용 프로그램을 작동시킬 때의 취약성을 다루는 것이다. 따라서 그의 연구는 기밀성 평가를 위한 정량적인 접근 방법이라 할 수 있다. 또한 시스템의 출력 집합을 보호하는 것으로 제한되고 도청 취약성만을 계산 한다.

4. 센서 node compromise에 대한 취약성 분석 제안 방법론

센서 네트워크는 전통적인 컴퓨터 네트워크에 비교하여 많은 제약조건을 가진 특별한 네트워크다. 이러한 제약들 때문에 기존에 써오던 보안 방법론을 센서 네트워크 영역에 바로 적용하기에는 어려움이 따른다. 센서 적용에 있어서 많은 부분들 특히, 다중의 동적인 특징들, 이들의 상관관계와 데이터 분배에 대한 시간적인 측면들이 고려되어야 한다[4]. 다음의 절에서는 센서 네트워크의 본질적인 특징들을 고려한 취약성 식을 새롭게 정의하였다. 먼저 센서 네트워크의 토폴로지는 계층적이고 동적인 클러스터 구조로 되어 있다고 가정한다. 이 토폴로지는 가장 에너지 효율적이고 센서 네트워크에서 광범위하게 사용되는 토폴로지이다.

4.1 센서 네트워크의 취약성 식

4.1.1 센서 노드 취약성

$$NV_{ijk} = \sum_{l=1}^{n} (\omega_{ijkl} \times vul_{ijkl}) / \sum_{l=1}^{n} \omega_{ijkl} \quad (1)$$

w_{ijkl}와 vul_{ijkl}는 i번째 네트워크 안에 있는 j번째 클러스터에 속한 k번째 노드의 l번째 취약성 항목의 파급효과와 평가된 값을 나타낸다. 그리고 n은 i번째 네트워크 안에 있는 j번째 클러스터에 속한 k번째 노드의 취약성 항목들의 총 개수를 의미한다. 센서 노드의 취약성은 Hartung의 연구[2]와 Alarifi의 연구[1]에 관련시켜 좀 더 간단한 방법으로 계산 될 수 있다. 예를 들면,

$$NV'_{ijk} = [a, b] \quad (2)$$

여기서, a와 b는 $a = \alpha * t_{compromise}$, $b = \beta * t_{compromise}$ 이다. 식 (2)에서, a는 센서 노드 취약성의 낮은 한도를 의미하며, b는 센서 노드 취약성의 높은 한도를 의미한다. 그리고 α, β는 센서 노드로부터 정보를 빼 내는 데 걸리는 총 시간 $t_{compromise}$에 관련된 특정 상수라 할 수 있다.

4.1.2 센서 링크 취약성

$$LV_{im} = (n_{success})_{im} / (n_{trial})_{im} \quad (3)$$

$(n_{success})_{im}$는 성공한 공격 시나리오 수를 의미한다. $(n_{trial})_{im}$는 adversary 모델로부터의 타겟 구성 요소들로 실행 된 공격 시나리오 수를 의미한다. 이 둘은 모두 i번째 네트워크 안 m번째 링크를 통하는 것이다. 또한, LV_{im}는 랜덤 그래프[3, 5]와 상호 연관되어 다른 방법으로 계산 될 수 있다.

4.1.3 센서 클러스터 취약성

$$CV_{ij} = \sum_{k=1}^{n} (\omega_{ijk} \times NV_{ijk}) / \sum_{k=1}^{n} \omega_{ijk} \quad (4)$$

w_{ijk}는 i번째 네트워크에 있는 j번째 클러스터의 k번째 노드의 중요도 가중치를 나타낸다. 그리고 n은 i번째 네트워크에 있는 j번째 클러스터의 타협된 노드들의 총 수를 의미한다.

4.1.4 센서 클러스터 취약성

$$Net\,V_i = \sum_{j=1}^{n} (\omega_{ij} \times CV_{ij}) / \sum_{j=1}^{n} \omega_{ij} \quad (5)$$

w_{ij}는 i번째 네트워크에 있는 j번째 클러스터의 중요도 가중치를 나타낸다. 그리고 n은 i번째 네트워의 타협된 클러스터들의 총 수를 의미한다.

4.2 위험 파급 효과를 고려한 센서 네트워크의 취약성 평가

기존 네트워크에 해당하는 취약성 분석 방법론의 가용성을 높이기 위해서는 w에 위험의 파급효과 값을 대입할 수 있다.

$$\omega_{ijkl} = IR_{ijkl} = IT_{ijkl} \times IV_{ijkl} \quad (6)$$

IR_{ijkl}, IT_{ijkl}, IV_{ijkl}는 i번째 네트워크 안, j번째 클러스터 안, k번째 노드의 l번째 취약성 항목의 위험 파급효과, 위협 파급효과, 취약성 파급효과이다.

$$\omega_{ijk} = IR_{ijk} = IT_{ijk} \times IV_{ijk} \quad (7)$$

IR_{ijk}, IT_{ijk}, IV_{ijk}는 i번째 네트워크 안, j번째 클러스터 안, k번째 노드의 위험 파급효과, 위협 파급효과, 취약성 파급효과이다.

$$\omega_{ij} = IR_{ij} = IT_{ij} \times IV_{ij} \quad (8)$$

IR_{ij}, IT_{ij}, IV_{ij}는 i번째 네트워크 안, j번째 클러스터의 위험 파급효과, 위협 파급효과, 취약성 파급효과이다.

다음 장에서는, 각각의 클러스터와 수집된 정보의 중요도에 대한 취약성 값의 변화를 다룬다.

4.3 센서 네트워크 자산의 중요도

4.3.1 구성 요소의 중요도

일반적으로, 싱크 노드는 보통의 leaf 노드보다는 훨씬 중요하다. 왜냐하면 싱크 노드가 데이터의 통합 점이기 때문이다. 파급 효과는 다음과 같이 공식화 하여 나타난다.

$p_{ijk} \times \omega_{ijk}$: p_{ijk}는 i번째 네트워크 안, j번째 클러스터 안, k번째 노드의 지위 값을 나타낸다.

$p_{ij} \times \omega_{ij}$: p_{ij}는 i번째 네트워크 안, j번째 클러스터의 지위 값을 나타낸다.

4.3.2 수집되는 정보의 중요도

훨씬 중요한 정보를 센싱하는 센서 노드들은 높은 weight 값을 갖는다. 파급 효과는 다음과 같이 공식화 되어 나타난다.

$q_{ijk} \times \omega_{ijk}$: q_{ijk}는 i번째 네트워크 안, j번째 클러스터 안, k번째 노드로 수집된 정보들의 중요도 값을 나타낸다.

$q_{ij} \times \omega_{ij}$: q_{ij}는 i번째 네트워크 안, j번째 클러스터의 싱크 노드로 수집 된 정보들의 중요도 값을 나타낸다.

4.3.3 센서 노드 중요도를 이용한 링크 취약성

다른 두 개의 노드 취약성 set이 주어졌을 때, $p_n w_n$와 $p_m w_m$를 이용해 링크 취약성을 고려할 수 있다. p_n와 p_m는 유저의 정책에 따라 다르게 할 수 있다.

$$LV_{k_n k_m} = (NV_{ijn} p_{ijn} \omega_{ijn} + NV_{ijm} p_{ijm} \omega_{ijm}) / (p_{ijn} \omega_{ijn} + p_{ijm} \omega_{ijm}) \quad (9)$$

NV_{ijn}와 NV_{ijm}는 각각 i번째 네트워크 안, j번째 클러스터의 n번째 노드와 m번째 노드의 노드 취약성을 나타낸다. 주어진 노드 취약성 NV_{ijn}, NV_{ijm}을 이용하여, 링크 취약성 LV_{knkm}이 노드 중요도 $p_n w_n$와 $p_m w_m$에 기반한 weight를 고려하여 산술 평균을 구할 수 있다. 일정한 파급 효과를 가진 센서 네트워크의 특별한 경우, $p_n w_n$와 $p_m w_m$는 파급 효과 x와 y로 정의 할 수 있다. 다음의 식은 모든 두 개의 노드들이 $p_n w_n$와 $p_m w_m$를 가지고 있다고 본다.

$$LV_{k_n k_m} = (NV_{ijn} x + NV_{ijm} y)/(x+y) \quad (10)$$

다음 장에서는, 각각의 시나리오가 어떻게 노드와 클러스터와 네트워크의 취약성에 영향을 미치는지와 더불어 자산의 중요도 중 구성 요소의 중요도에 관련된 파급 효과를 적용한 취약성 식이 사용 가능할 만큼 정확한지 검증한다.

5. 평가 및 검증

이 장에서는, 취약성 및 위험 평가 식들을 다음의 시나리오들을 이용하여 평가한다. 모든 센서 노드들이 간섭 저항자 역할을 하지 않고, 노드 타협에 대해 취약하다고 가정한다. 또한 베이스 스테이션은 공격에 대해 안전하다고 가정한다. 네 개의 시나리오에서 예로 든(데이터) 통합 트리는 계층적인 그룹의 s1부터 s10까지의 노드들이 주어진다. 각각의 노드 s1 ; ::: ; s10은 하위 클러스터 그룹의 데이터를 모으는 작업을 수행하며 노드 s10으로 데이터를 보내기 전에 그들이 모은 데이터를 결합한다[4].

예를 들면, 테이블 1은 monte carlo 시뮬레이션을 통해 만들어진다. 이것은 노드 s1이 타협되었을 때 두 노드의 취약성에 연관된 링크 취약성을 보여준다.

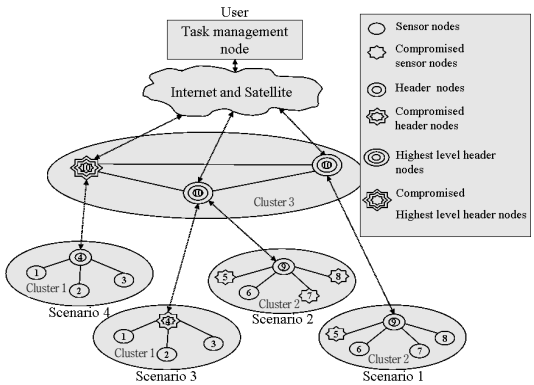
〈표 1〉 센서 링크의 취약성

S	1	2	3	4	5	6	7	8	9	10
1	0.0	6.3	6.4	6.1	6.3	6.3	6.4	6.3	6.3	6.1
2	6.3	0.0	2.9	2.4	2.5	2.5	2.9	2.5	2.5	2.4
3	6.4	2.9	0.0	2.8	2.9	2.9	3.0	2.9	2.9	2.8
4	6.1	2.4	2.8	0.0	2.4	2.4	2.8	2.4	2.4	2.0
5	6.3	2.5	2.9	2.4	0.0	2.5	2.9	2.5	2.5	2.4
6	6.3	2.5	2.9	2.4	2.5	0.0	2.9	2.5	2.5	2.4
7	6.4	2.9	3.0	2.8	2.9	2.9	0.0	2.9	2.9	2.8
8	6.3	2.5	2.9	2.4	2.5	2.5	2.9	0.0	2.5	2.4
9	6.3	2.5	2.9	2.4	2.5	2.5	2.9	2.5	0.0	2.4
10	6.1	2.4	2.8	2.0	2.4	2.4	2.8	2.4	2.4	0.0

<표 1> 을 통해서 센서 노드 s4와 s6사이에 있는 링크의 취약성이 2.4임을 알 수 있다. 이 때, 취약성 값은 0~10사이로 두며 0인 경우는 피해 가능성이 없는 안전한 상태를 의미하고, 5의 경우 일반 정보 유출이 가능한 정도의 취약함을 의미하며, 10은 시스템의 완전한 통제 권한 획득 또는 마비가 가능함을 의미한다. 이는 센서 노드 취약성, 센서 클러스터 취약성, 센서 네트워크 취약성 값에도 적용된다. <표 1>은 다음의 시나리오 1에 따른 결과이다. 따라서 센서 노드 s1에 연결된 링크들의 취약성 값이 다른 링크들 보다 높게 측정된다.

5.1 시나리오 설정

여기서 제시하는 네 개의 시나리오에서는 위의 monte carlo 링크 취약성 계산 시 적용된 가정과는 달리 클러스터 별로 노드들이 그림과 같이 연결되어 있음을 가정한다. 그리고 (그림 1)에서 숫자로 표시한 센서 노드들은 앞으로 s를 붙여 설명하겠다.



(그림 1) Concept 시나리오

시나리오 1 (그림 1)에서는, 클러스터 1에 속해 있는 센서 leaf 노드 s1이 공격당한다[1]. 클러스터 1은 s1에서부터 s4까지를 클러스터 한 것으로 구성된다. 시나리오 1에서는, 클러스터 1의 취약성과 전체 센서 네트워크의 취약성을 계산할 수 있다.

시나리오 2 (그림 1)에서는, 여러 개의 센서 leaf 노드들 (s5, s7, s8)이 타협 되었을 경우를 다룬다. 센서 노드 (s5, s7, s8)을 포함하여 s6, s9가 클러스터 2에 속해 있다. 센서 노드 s5는 hash function을 이용해 뒤섞인 데이터 구조를 지닌 채[1]

공격당한다. 반면 s7, s8은 데이터가 섞인 후, 코드 소스를 어렵게 바꿔주어[1] 공격당하는 것으로 설정하였다. 시나리오 2를 설정한 목적은 하나의 클러스터 안에 단일의 센서 leaf 노드가 공격당한 경우와 여러 개의 센서 leaf 노드가 공격당한 경우를 비교하기 위함이다.

시나리오 3에서는, 첫 번째 레벨의 클러스터에 속해 있는 센서 header 노드가 공격당한 경우이다. 여기서 첫 번째 레벨의 클러스터는 클러스터 1, 2를 의미하고, 두 번째 레벨의 클러스터는 클러스터 3을 의미한다. 시나리오 3에서 s9는 s7, s8에 가한 보안 기법과 동일하게 hash function을 이용해 뒤섞인 데이터 구조와 함께 코드도 뒤섞는다[1]. 이 시나리오는 leaf와 header 노드가 공격당할 때를 비교하기 위해 시도하였다.

시나리오 4에서는, 두 번째 레벨 클러스터에 속해 있는 센서 header 노드가 공격당한다. s10은 s7, s8, s9에 가한 보안 기법에 한 가지를 더 추가한다. 코드의 control flow를 임의로 하여[1] 공격당한다고 보았다.

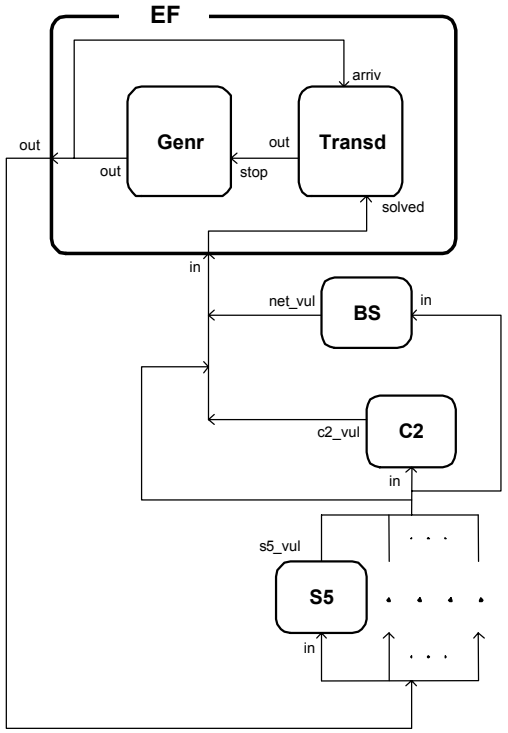
5.2 시나리오 구현

시뮬레이션의 목적은 취약성 및 위험 평가 식들을 다음의 시나리오들을 이용하여 평가하는 것이다. 또한 위의 시나리오 1에서 4의 경우와 마찬가지로 모든 센서 노드들이 간섭 저항자 역할을 하지 않고, 노드 타협에 대해 취약하다고 가정한다. 또한 베이스 스테이션은 공격에 대해 안전하다고 가정한다. 네 개의 시나리오에서 예로 든 (데이터) 통합 트리는 계층적인 그룹의 s1부터 s10까지의 노드들이 주어진다. 각각의 노드 s1 ; ::: ; s10은 하위 클러스터 그룹의 데이터를 모으는 작업을 수행하며 노드 s10으로 데이터를 보내기 전에 그들이 모은 데이터를 결합한다[4].

다음은 시뮬레이션을 수행하기 위한 test bed의 구조도를 나타낸 것이다.

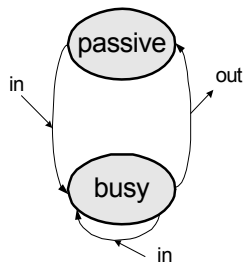
5.2.1 Test bed 모델

아래의 test bed 모델은 EF(experimental frame)의 Genr(Generator) 모델에서 공격 신호를 발생하면 이를 input으로 받는 모든 모델들은 동작을 시작한다. 즉, s1, …, s4 모델이 반응하게 되고, 일정 시간이 경과하면 s1, …, s4 모델은 output을 발생하여 c1 모델과 bs 모델과 EF 모델에게 전달한다. c1 모델은 받은 값을 이용해 클러스터 1의 취약성 값을 계산하고, 이 output은 bs 모델과 EF 모델에게 전달한다. bs 모델은 input 값을 이용해 네트워크의 취약성 값을 계산하여 net_vul(output)을 EF에게 전달한다. 그러면 EF의 Transd(transducer) 모델은 받은 값을 모두 출력해주고, 동작이 끝나면 Genr 모델에게 stop 신호를 보낸다. 이렇게 되면 모델의 상태 변화가 모두 끝나게 된다[9].

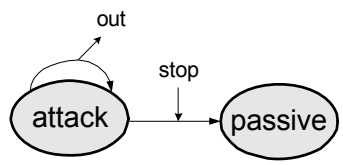


(그림 2) Test bed 모델의 부분 구조도

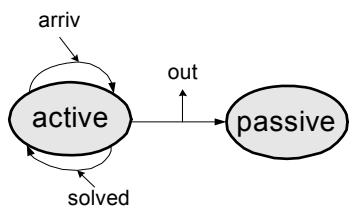
(그림 2)은 클러스터 2의 진행 사항을 구조화 한 것이다. 여기서 attack을 감지하는 모델은 S5, S6, S7, S8, S9 모델이다. S5, …, S9 모델들이 자신의 S5_vul, …, S9_vul 값을 C2 모델과 BS 모델과 EF 모델의 in port로 보낸다.



(a) BS / C1-3 / S1-10의 STD



(b) EF Genr의 STD



(c) EF Transd의 STD

(그림 3) 최하위 엔티티에 대한 상태 전이도

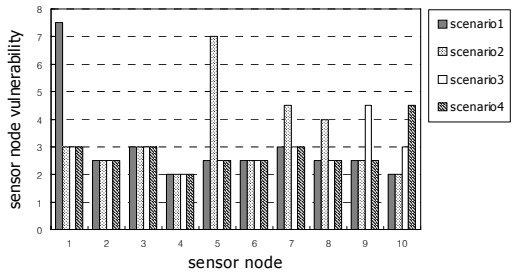
(그림 2)에서 BS 모델과 C1, C2, S1, …, S9 모델의 상태 전이도[9]를 (그림 3)(a)와 같이 표현하였다. (그림 3)(b)는 EF 모델 내부 모델인 Genr 모델의 상태 전이도이며, (c)는 EF 모델 내부 모델인 Transd의 상태 전이도이다. (그림 3)을 이용하여 <표 2>의 Model을 설계한다. 시뮬레이션은 DEVS 기반의 DeSim-VC++을 이용했다[9]. <표 2>는 필요한 구성요소들이다.

〈표 2〉 DeSim 기본 구성 요소

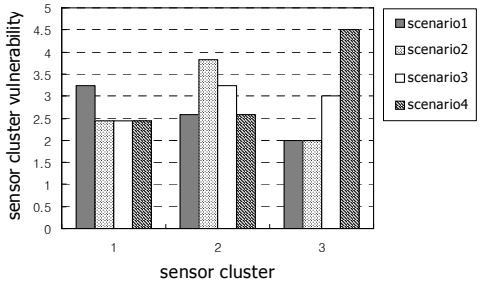
Library Files		Model	
Atomic.cpp, Coupled.cpp Digraph.cpp, Entities.cpp Entstr.cpp, List.cpp	Message.cpp, Mlist.cpp Models.cpp Port.cpp Output.cpp, Main.cpp Tglobal.h	ExtTransitionFN, ContentPort(), IntTransitionFN, ContentValue(), OutputFN, MakeContent("out", & JobID) ;,	InitializeFN, HoldIn("busy", PTime) ;, StartSimulation : EFP.Restart() ;, Continue();

5.2.2 구성 요소에 대한 취약성 값

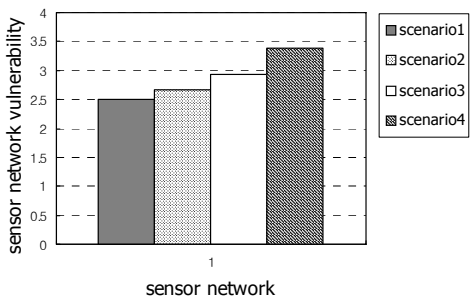
(그림 4)~(그림 6)은 센서 네트워크의 노드, 클러스터, 네트워크 취약성을 식 (6), 식 (8), 식 (9)를 이용해 정량화 한 그래프이다. 식 (6), 식 (8), 식 (9)에 (그림 1)의 시나리오에 맞춰 임의의 값을 지정하여 보았다. 시나리오 1에서는 다른 센서 노드들이 안전하지 않은 상태에서 첫 번째 레벨 클러스터에 속한 센서 leaf 노드 s1만이 공격을 당한다. 시나리오 2에서는 첫 번째 레벨 클러스터에 속한 여러 개의 센서 leaf 노드들이 공격을 당한다. 시나



(그림 4) 센서 노드와 센서 노드 취약성



(그림 5) 센서 클러스터와 센서 클러스터 취약성



(그림 6) 센서 네트워크와 센서 네트워크 취약성

리오 3은 첫 번째 레벨 클러스터의 센서 header 노드 하나가 공격을 당하고 마지막 시나리오에서는 두 번째 레벨 클러스터의 센서 header 노드 하나가 공격을 당하는 구성이다. 각각의 시나리오는 최소한의 센서 노드들로 구성된 네트워크에서 여러 다양한 경우를 보여준다.

(그림 5)에서 센서 클러스터 1와 센서 클러스터 2는 첫 번째 레벨의 클러스터 나타내고, 센서 클러스터 3은 두 번째 레벨의 클러스터를 나타낸다. 본 논문에서는 센서 네트워크의 계층적인 특징을 반영하여 센서 노드의 레벨에 따라 다른 weight 값을 부여하였다. 높은 레벨에 있는 센서 노드들은 큰 weight 값을 가지게 되고, 같은 레벨에 있는 센서 노드들은 동일한 weight 값을 가지게 된다. 시나리오 1, 2를 통해 클러스터 2의 취약성이 클러스터 1의 취약성 보다 높음을 확인 할 수 있다. 즉, 같은 레벨에 있는 센서 노드일 경우 공격당한 센서 노드의 개수가 많은 센서 클러스터의 취약성이 더 높아짐을 볼 수 있다. 또한 시나리오 3과 4를 통해 두 번째 레벨의 센서 노드가 공격당할 때가 첫 번째 레벨의 센서 노드일 때 보다 훨씬 취약성 값이 올라감을 알 수 있었다. (그림 6)에서는 시나리오 4의 경우가 가장 네트워크에 미치는 충격이 크다는 것을 알 수 있다. 즉, 시나리오 상 가장 높은 레벨의 센서 header 노드가 공격 받는 경우이다.

6. 결 론

본 논문에서는 센서 네트워크에서 클러스터를 기반으로 한 취약성 및 위험 평가 프레임워크를 제안하였다. 노드 타협이 발생할 경우, 센서 노드와 센서 링크, 센서 클러스터와 이를 모드 아우르는 센서 네트워크의 취약성 값을 계산하였다. 또한 다양한 접근 방법을 통해 센서 노드 취약성과 센서 링크 취약성을 구하는 방법을 소개하였다. 본 논문에서는 컨셉 시나리오를 바탕으로 센서 네트워크 모델을 만들어 제안한 방법을 평가하였다. 시뮬레이션 tool을 이용해 구성하여 컨셉이 바뀌어도 평가가 가능할 수 있게 제안하였다. 따라서 본 논문에서 제안하였지만 검증하지 못한 취약성 및 위험 식들을 이용해 앞으로 확장 및 평가가 가능하다 하겠다.

참 고 문 헌

[1] A. Alarifi and W. Du, “Diversify Sensor Nodes to Improve Resilience Against Node Compromise”, In Proc. of the fourth ACM Workshop on Security of Ad Hoc and Sensor Networks, Virginia, USA, pp. 101-112, 2006.

[2] C. Hartung, J. Balasalle, and R. Han, “Node Compromise in Sensor Networks : The Need for Secure Systems”, Technical Report CU-CS-990-05, Department of Computer Science University of Colorado at Boulder, USA, 2005.

[3] H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan, “On the Distribution and Revocation of Cryptographic Keys in Sensor Networks”, IEEE Transactions on Dependable and Secure Computing, Vol. 2, pp. 233-247, 2005.

[4] M. Anand, Z. G. Ives, and I. Lee, “Quantifying Eavesdropping Vulnerability in Sensor Networks”, In Proc. of the 2nd Int. Workshop on Data Management for Sensor Net-

works, Trondheim, Norway, pp. 3-9, 2005.
[5] P. De, Y. Liu, and S. K. Das, "Modeling Node Compromise Spread in Wireless Sensor Networks Using Epidemic Theory", In Proc. of the 2006 Int. Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 237-243, 2006.
[6] R. Kannan, S. Sarangi, S. Ray, and S. S. Iyengar, "Minimal Sensor Integrity : Measuring the Vulnerability of Sensor Deployments", Information Processing Letters, pp. 49-55, 2003.
[7] ISO/IEC JTC 1/SC27, Guidelines for the Management of IT System Security(GMITS) 1996~1997.
[8] OECD, OECD Guidelines for the Security of Information Systems and Networks Towards a culture of security, 2002.
[9] S. D. Chi, "Model-Based Reasoning Methodology Using the Symbolic DEVS Simulation", Trans. of the Society for Computer Simulation International, Vol. 14, No. 3, 1996.

박 종 서

1983년 한국항공대학교 항공통신학과(공학사)
1986년 노스캐롤라이나대학 전기 컴퓨터공학과 (공학석사)
1994년 펜실베니아주립대학교 컴퓨터공학부(공학박사)
1994년~1996년 펜실베니아주립대학교 컴퓨터 공학과 조교수
1996년~현재 한국항공대학교 컴퓨터공학과 교수

서 윤 경

2005년 한국항공대학교 항공우주및 기계 공학부(공학사)
2006년~현재 한국항공대학교 컴퓨터공학과 석사과정

이 슬 기

2006년 한국항공대학교 컴퓨터 공학과(공학사)
2006년~현재 한국항공대학교 컴퓨터공학과 석박사통합과정

이 장 세

1997년 한국항공대학교 컴퓨터 공학과(공학사)
1999년 한국항공대학교 컴퓨터 공학과(공학석사)
2003년 한국항공대학교 컴퓨터 공학과(공학박사)
2004년~현재 한국해양대학교 컴퓨터제어전자통신 공학부 조교수

김 동 성

2001년 한국항공대학교 전자 공학과(공학사)
2003년 한국항공대학교 컴퓨터 공학과(공학석사)
2003년~현재 한국항공대학교 컴퓨터공학과 박사과정