USN 환경에서의 위험분석을 위한 효율적인 자산분석 방법론에 관한 연구*

*조준식, *박선호, *엄정호, **정태명
*성균관대학교 컴퓨터공학과 **성균관대학교 정보통신공학부
e-mail : *{jscho, shpark, jheom}@imtl.skku.ac.kr **tmchung@ece.skku.ac.kr

A Study on Efficient Asset Analysis Methodology for Risk Analysis On Ubiquitous Sensor Network Environments*

*Joonsic Cho, *Sunho Park, *Jungho Eom, **Taimyoung Chung
*Department of Computer Engineering, Sungkyunkwan Univ.
**School of Information and Communication Engineering, Sungkyunkwan Univ.

요 약

정보통신 인프라가 유비쿼터스 컴퓨팅 환경으로 확장됨에 따라 정보시스템의 종류가 급격히 증가하고, 이에 해당하는 위험 역시 커지고 있는 상황이다. 현재 국내 위험관리 수준은 외국의 위험관리 방법론을 도입하거나, 은행에서 사용되고 있는 재무위험관리를 정보시스템에 맞도록 수정하여 사용하고 있는 수준이다. 더구나 유비쿼터스 컴퓨팅 환경에 맞는 위험관리 기법들은 연구되고 있지 않으며, 인프라 구축에만 힘을 기울이고 있는 현실이다. 이에 따라 본 논문에서는 유비쿼터스 컴퓨팅 환경에서의 체계적인 위험관리를 위해 효율적인 자산분석 프레임워크를 제시하고, 유비쿼터스 컴퓨팅 환경에서의 적용에 있어서 최적화된 자산분석 방법론을 제시하였다.

1. 서론

오늘날 정부기관 및 기업에서 정보시스템을 보호하기 위한 정책 및 투자가 증대되고 있는 가운데 효율적인 보안대책을 수립할 수 있도록 정보시스템에 대한 위험관리 분야의 관심이 높아지고 있다[1]. 위험관리의 핵심이라 불리는 위험분석의 분야는 정보시스템의 자산의 정확한 분석을 토대로, 자산을 위협하고 있는 요소들과, 그에 해당하는 대응책을 분석하여 비용대비 효과가 뛰어난 대응책을 수립하는데 목적을 두고 있다[2]. 그러나 이러한 정보시스템 환경이 유비쿼터스 센서네트워크(Ubiquitous Sensor Network) 환경으로 확장됨에 따라 기존의 위험분석 방법론으로 USN 환경의 시스템을 위험분석을 수행하기에는 자산의 정의에 어려움이 있다. USN 은 각종 센서에서 수집한 정보를 무선으로 수집할 수 있도록 구성한 네트워크로서 WPAN(Wireless personal area network), ad-hoc network 등의 기술이 발전함에 따라 센서 네트워크 기술이 매우 활성화되고 있다[3]. 기존의 위험분석 방법론으로는 이러한 센서들을 분류하고 정량적, 정성적 가치를 판단하는데 있어 센서가 내재하고 있는 취약점 및 위협요소들을 판단할 수 있는 방법이 없다.

따라서, 본 논문에서는 USN 에서의 자산의 분류와 센서의 기능별 자산분석을 수행하고, 기존의 방법론에서 제시한 정성적 가치평가의 문제점을 해결할 수 있는 새로운 방법론을 제시한다.

2. 일반적인 위험분석 방법론

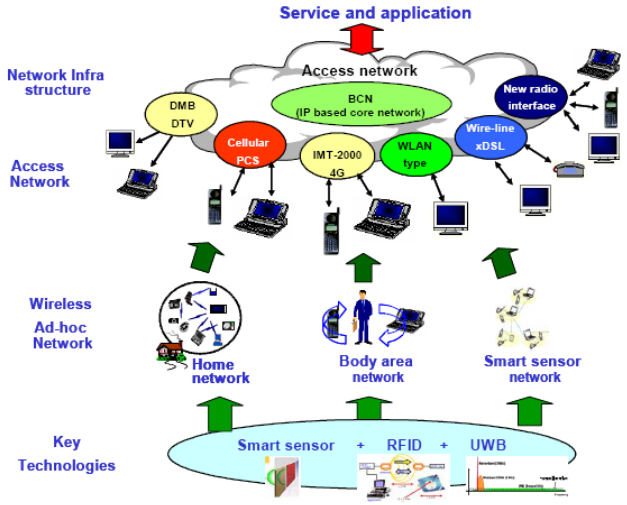
위험분석은 보안관리를 수행하기 위한 필수적인 과정이고 시스템의 위험을 평가하고, 비용효과적인 대응책을 제시하여 시스템 보안정책과 보안대응책 구현계획을 수립하는 위험관리의 핵심적인 부분이다[4]. 위험분석의 목적은 보호되어야 할 대상 정보시스템과 조직의 위험을 측정하고, 이 측정된 위험이 허용 가능한 수준인지 아닌지 판단할 수 있는 근거를 제공하는 것이다. 위험분석이란 정보시스템과 그 자산의 비밀성, 무결성, 가용성, 기록추적성에 영향을 미칠 수 있는

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성・지원사업의 연구결과로 수행되었음.

다양한 위협에 대해서 정보시스템의 취약성을 식별하고, 이로 인해서 예상되는 손실을 분석하는 것이다.[5,6]

3. 유비쿼터스 센서네트워크의 특징

유비쿼터스 환경은 사용자가 컴퓨터를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 정보통신환경을 말한다[2]. USN 은 일반적으로 [그림 1]와 같이 센서나 RFID 를 통하여 수집한 데이터를 광대역통신망을 통하여 사용자에게 서비스를 제공해주게 된다.



[그림 1] 유비쿼터스 센서네트워크 개요

기존의 정보통신 인프라에서 구축되어있던 자산들 이외에 무선망을 기반으로 하는 센서나 RFID, 블루투스, 적외선통신등의 정보기기들과 센싱된 데이터를 모으고, 서비스를 제공해주는 미들웨어 기술이나 서비스 제공을 담당하는 응용프로그램 등의 자산이 존재한다. 이러한 특징으로 인해 USN 은 기존의 정보시스템 자산과 다른 특성을 갖고 일반적인 위험분석 모델을 통해서 USN 환경에서의 자산의 정확한 식별이 불가능하다[7].

4. 센서네트워크에서의 자산분석 방법론

4.1 기존의 자산분류 체계의 문제점

기존의 자산분류는 유형 자산을 중심으로 자산의 가치를 산정하였다. 이는 분석하려는 자산이 내재하고 있는 역할이나 정보의 가치를 평가하고, 이를 자산의 가치에 적용해 정확한 자산의 가치를 산출하지 못하는 단점을 갖고 있다. TTA 국내 표준 “공공정보시스템 보안을 위한 위험분석 표준 - 위험분석 방법론 모델” 은 ISO 13335 GMITS(Guidelines for the Management of IT Security)의 기반으로 작성이 되어있고, 이 위험분석 방법론의 특징은 자산의 분류방법에 있어서 최상위 단계에 IT 정보 시스템을 기준으로 나누기 때문에 정보통신 자산 개별 가치를 판단하는데 적합하지만, 이 개별적 자산이 내재하고 있는 무형의 가치, 즉 정보의 가치나, 제공 서비스의 가치판단에 부적합한 요소를 갖고 있다[5].

4.2 USN 환경에서의 자산분석 수행 문제점

USN 환경에서의 자산은 센서단위가 주체로 볼 수 있으나 현재 나와 있는 자산분석 방법론을 그대로 적용하게 된다면 서비스를 제공해주기 위한 데이터들에 대한 가치평가를 할 수 없고, 앞에서 언급한 일반적인 자산분석의 문제점이 그대로 나타나게 된다.

센서의 정량적인 가치는 작기 때문에 센서가 감지하고 있는 무형의 가치에 대해서는 판단할 근거가 없다. 예를 들어, 위치판단을 하는 센서가 존재한다고 가정해보자. 이 센서가 존재하는 위치에 따라서 필요한 서비스를 제공하는 것이 목적이다. 여기서 위치판단을 하는 센서의 가격이 400$이라 가정하면, 정량적 가치판단 기준에 의해 초기 구입비용과 비슷한 수준의 가치로 계산된다. 그러나 이 센서가 중요 서비스를 제공하는 웹서버 근처나, 사내 금고의 근처에 있을 경우, 혹은 허락되지 않은 서비스로의 접근을 요구하는 경우 센서의 해당 정보인식을 통해서 제어해야 하는 서비스의 종류를 나타내야 할 것이다. 이 센서가 특수한 권한을 갖고 있는 사용자가 사용할 경우, 제공해야 하는 서비스의 민감도는 높아지기 마련이다. 즉, 정량적 가치 400$ 이상의 가치를 갖고 있다는 말이다.

이밖에 센서들의 유지 보수비용에 대한 비용과, 같은 역할을 하는 여러 종류의 센서 중 혹은 같은 종류의 여러 센서 중 어떤 센서에 가중치를 두어 가치판단을 해야 하는지에 대해서 정확한 자산분석이 요구된다. 즉, 센서의 정량가치의 판단과 센서들의 기능에 기반을 두는 정성가치의 판단의 자산분석이 수행되어야 한다.

5. USN 환경에서의 자산분석을 수행 프레임워크

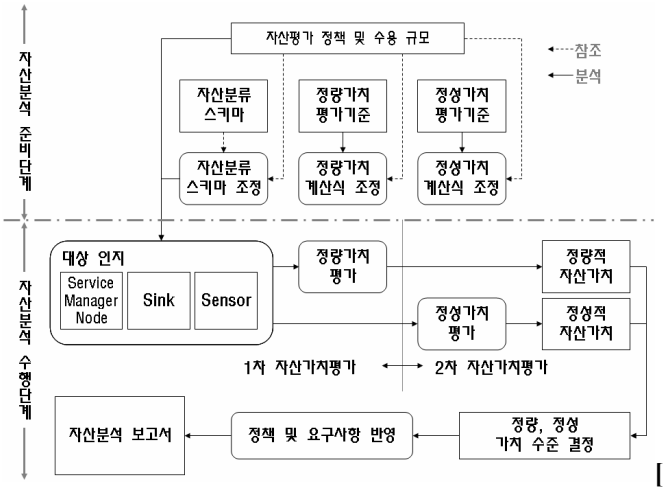


그림 2] USN환경에서의 자산분석 프레임워크

앞에서 말한 일반적인 자산분석에서의 문제점과 USN 환경의 센서 자체를 자산을 인식하였을 경우 문제점 해결하기 위해서는 센서의 역할기반의 서비스 제공을 기준으로 자산분석을 수행해야 할 것이다. 기본적으로 센서의 정량적 가치판단 후 가중치 계산을

통해 센서가 내재하고 있는 정성적 가치판단의 효율성을 제공하는 것이 목적이다.

[그림 2]는 센서네트워크에서의 자산분석을 수행하기 위한 자산평가 방법론 구조이다. 본 논문에서는 USN 환경에서의 자산분석 수행을 위해 센서에 대한 유형 자산 및 센서에 대한 인적 요소가 내재하고 있는 무형자산 요소가치판단을 할 수 있는 프레임워크를 제공한다.

5.1 자산분석 준비단계

정확한 자산분석을 수행하기 위해서 4 단계의 평가 준비단계를 거친다.

① 자산평가 정책 및 수용 규모

기존의 USN 의 운영 정책 및 자산평가를 수행하기 위한 보안정책들을 분류하고, 자산분석을 수행하기 위한 대상을 분류하여 자산분석을 수행하기 위한 사전 준비 작업을 수행한다.

② 자산분류 스키마 조정

기존의 자산분류표에 유형자산인 Sink, SMN, 센서를 추가하여 <표 1>에서와 같이 구성한다. 요소들로는 개발/구입비용과 운영에 필요한 비용, 그밖에 보안정책이나, 다른 컴포넌트와의 연결 요소들을 필요로 한다.

<표 1> 자산 및 분류 및 평가요소

자산		평가요소		
자산분류	자산컴포넌트	개발/구입	운영	기타
유형 자산	Sink			
	SMN			
	센서			

③ 정량가치 계산식 조정

단순히 자산이 내재하고 있는 정량적 가치를 평가하기 위해 수행하는 과정이며, 센서네트워크 환경의 시스템의 정량가치 평가를 위해 다음과 같은 요소들을 기반으로 아래와 같은 자산에 대한 정량가치 계산식을 정의한다.

- ✓ $f_{quwantity}$ - 정량분석 기본식 (Quantitative Analysis Function)
- ✓ SMN - 서비스관리노드(Service Manager Node)
- ✓ S - 싱크서버(Sink)
- ✓ SNG - 센서노드그룹(Sensor Node Group)
- ● PDC - 구입개발비용(Purchase & Development Cost)
- ● YOC - 연간운영비용(Yearly Operation Cost)
- ● OC - 기타비용(Other Cost)
- ✓ RV - 잔존가치(Residual Value)
- ✓ SL - 내용연수(Service Life)
- ✓ RSL - 잔여내용연수(Remain Service Life)
- ✓ DC – 감가상각비(Depreciation Cost)
- ✓ $DC = \dfrac{RSL}{SL(SL+1)/2}$

$$f_{quwantity}(SMN \parallel S) = (PDC + YOC + OC - RV)DC$$

$$f_{quwantity}(SNG) = (\sum_{i=1}^{n} SN_i + YOC + OC - RV)DC$$

④ 정성가치 계산식 조정

<표 2> 센서 그룹 및 평가표

자산		평가요소				종합
		Fnc 1	Fnc 2	...	Fnc n	
Sensor	Sensor Node Group 1					

센서노드를 제외한 기타 자산 컴포넌트는 기존의 위험분석 방법론으로 자산의 정성적 평가가 가능하다. 그러나 센서노드에서는 인식하는 데이터와 사용자에게 제공하는 서비스 기준으로 정성가치를 계산한다. 센서 하나에서 인식하는 데이터는 센서의 기능에 따라서 같은 종류의 센서라 할지라도 큰 차이를 가지고 있다. 이러한 차이점들을 적용하기 위해 <표 2>와 같이 같은 기능을 제공 센서노드를 그룹별로 분류하고, 센서들의 역할별 항목을 세분화하여 표로 작성한다. 작성한 표를 중심으로 다음과 같은 정성가치 계산식을 정의한다.

- ✓ $f_{quality}$ - 정성분석 기본식 (Qualitative Analysis Function)
- ✓ Fnc - 기능(Function)
- ✓ CS - 기능별 민감도 Context Sensitive(기본값 1 로 하여 <표 3>의 민감도에 따라 작성한다)

<표 3> 평가요소 기능별 CS 값

Fnc	설명	수준	비고
Fnc 1	사용자 위치	최소접근권한을 1 로 하여 센싱 위치에 따른 권한의 증감을 0.5 로 한다	근무시간 이외에는 관리자 이외의 접근을 금한다 CS+2
Fnc 2	온도	(현재온도 - 20)/50 + 1	관리자가 상주할 경우 CS-0.2 화재위험 있을경우 CS+2
Fnc 3	센서 위치	센서가 놓여진 위치에 따라 1 의 증감을 보인다.	최대값 5
Fnc 4	습도	Abs((현재습도-70)/5)+0.8	습도가 너무 낮으면 화재위험, 너무 높으면 기기의 고장 위험
Fnc 5	이동 센서	센싱된 위치에 따른 등급설정	사용자 위치별 가중치 중복산정
…	…	…	…
Fnc n	사용자	접근불가:0.4 접근가능:1 수정가능:2	시스템자체의 Admin 일 경우 5 로 설정

- ✓ N - 역할 분할 총 개수

$$f_{quality}() = Fnc_1 \sum_{i=1}^{N} \frac{CS_i}{N} \times Fnc_2 \sum_{i=1}^{N} \frac{CS_i}{N} \times \cdots \times Fnc_n \sum_{i=1}^{N} \frac{CS_i}{N}$$

5.2 자산분석 수행단계

자산분석 준비단계에서 정의한 자산분석 대상 항목과 계산식을 바탕으로 실질적인 자산분석을 수행하는 과정이다. 총 6 단계의 과정을 거치며, 해당 자산에 대

한 정성적, 정량적 분석을 수행하여 추가 요구 항목을 적용할 수 있도록 한다. 앞에서 정의한 자산분류표를 바탕으로 자산분석을 수행할 대상 파악한 후, 정량가치, 정성가치 평가 후 <표 4>와 같은 자산가치 평가표를 도출한다. 정량가치와 정성가치의 곱으로 종합 자산 가치를 측정할 수 있으며 자산평가를 수행하는 조직의 보안정책과 맞는지 확인을 하고, 후에 관리자 및 CEO 의 요구에 맞도록 계산식을 수정하고 자산평가를 재수행 할 수 있는 구조를 갖는다.

<표 4> 자산가치 평가표

자산		평가표		종합
		정량가치	정성가치	
Sensor	Sensor Node Group 1			
	Sensor Node Group 2			
	Sensor Node Group 3			
Sink				
SMN				

6. GMITS 와 USN 환경에서의 자산분석 방법론 비교

<표 5>는 표준문서 ISO/IEC TR 13335, Guidelines for the Management of IT Security 의 위험분석 방법론과 본 논문에서 제안한 USN 기반 자산분석 방법론 비교 표이다. 정확한 비교를 위하여 모든 정량가치와 정성가치의 값은 평균값을 갖도록 하였다. 자산의 평가는 해당 자산의 적용 후 6 개월을 기준으로 하였다.

GMITS 의 경우 정량적인 평가에서 자산 복구비용과 자산 교체비용만을 추가 항목으로 자산의 정량적 평가를 수행한다. 이러한 요소가 없다면 초기 구입 비용 그 자체가 정량적 가치가 된다. 이에 반해 SN 기반 자산분석 방법론은 자산 복구비용 및 자산 교체비용을 수반하며 감가상각비(본 논문에서는 연간 10%로 설정)를 따져 정량적 수치는 위와 같이 도출된다.

모든 정성적 가치는 기본수준으로 설정할 경우 SN 기반 자산분석의 평균은 <표 3>의 기능별 민감도에 따라 정성가치가 바뀌게 된다. SNG1 의 기능은 엘리베이터에서 온도 및 사용자를 인식하는 센서라 할 때, 평균온도일 경우 1 의 가중치와 사용자 인식의 기본값 1 의 가중치를 갖는다. 그러나 사용자 인식에 있어서 근무시간 이외에는 2 의 가중치를 갖게 되므로 이 센서의 정성가치는 다음과 같다.

$$f_{quality}(SNG1) = Fnc_1 \sum_{i=1}^{24} \frac{1}{24} \times Fnc_2 (\sum_{i=1}^{12} \frac{2}{24} + \sum_{i=1}^{12} \frac{1}{24})$$

$$f_{quality}(SNG1) = 1 \times 2$$

이런 방법으로 나머지 자산에 관해서 정성가치 기본식을 적용하여 계산한다. GMITS 의 경우 정성가치의 기준은 단일기준으로 5 단계의 평가만을 가지고 있지만, 본 논문에서 제안한 USN 기반 자산분석 방법론은 세분화된 정성가치의 다양한 방법의 정성가치 평가가 가능하다.

<표 5> GMITS 와 USN 기반 자산분석 방법론 비교

자산		GMITS		USN 환경 자산분석		
		정량 가치	정성 가치	정량 가치	정성 가치	종합
Sensor	SNG1	100$	3	95$	2	190$
	SNG2	200$	3	190$	0.8	152$
	SNG3	300$	3	285$	1.5	427$
Sink		500$	3	475$	3	1425$
SMN		800$	3	760$	5	3800$

7. 결론

기존의 위험분석 평가모델에서 제시한 자산분석 방법론을 보다 구체화시켜 자산의 가치를 산정하였다. 평가모델에서 제시한 방법들은 모두 정량적인 자산의 가치와 정성적인 자산의 가치를 분리시켜 따로 제시하였지만, 본 논문에서는 이러한 가치들을 그대로 적용함과 동시에 정성적인 가치평가 부분에 다양한 기능별 정성적 가치평가 모델을 제시하였다.

자산의 정량적 가치와 정성적 가치의 모호함을 해결하기 위해 정량적 가치는 평가자의 주관이 들어갈 수 없는 가치평가 구조를 가지고, 정성적 가치평가에 각 기능별 가중치를 세분화시켜 적용시킬 수 있도록 하였다. 이러한 정량적 가치와 정성적 가치의 분할은 마지막에 자산가치 평가표를 통해 하나로 만들 수 있으며, 자산의 보다 정확한 가치평가를 내릴 수 있도록 하였다.

제시한 유비쿼터스 센서네트워크 환경의 자산평가 방법론을 실제의 다수의 센서네트워크 환경에 적용하여 문제점을 발견하고, 정량평가 계산식 및 정성평가 기능별 평가요소들을 조정, 보완하여 자산분석뿐만 아니라 위험분석 전반에 걸쳐 센서네트워크가 가지고 있는 내재적인 위험을 탐지 예방할 수 있는 방법론 설계 등은 향후 연구과제로 남긴다.

참 고 문 헌

[1] NIST, "An Introduction to Computer Security : The NIST Handbook", NIST Special Publication 800-12, 1996.
[2] NIST, "Risk Management Guide for Information Technology Systems", NIST Special Publication 800-30, August 2001.
[3] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, August 2002.
[4] Fussell L., Field S., "The role of the risk management database in the risk management process", Systems Engineering, 2005. ICSEng 2005. 18th International Conference p.364 - 369, Aug. 2005.
[5] ISO/IEC TR 13335, "Guidelines for the Management of IT Security", ISO/IEC, 1997.
[6] British Standards Institution(BSI), "BS7799", BS7799, 1999