8

융합소프트웨어 안전성을 위한 소프트웨어공학 기술 적용

고려대학교 ▌차성덕* · 최진영* · 김선한 · 이희조 · 장길수 · 남원홍
최재순 · 이정주 · 정세훈 · 황대연 · 송경섭 · 신병윤

1. 서 론

소프트웨어의 사용은 지금까지 컴퓨터, IT 산업 안으로만 국한되어 왔지만 최근에는 산업간 융·복합이 활발해지면서 다양한 산업들과 융합되어 사용되고 있다. 특히, 최근 범 정부 차원의 5대 주요 산업(자동차, 조선, 항공, 건설, 의료)과 소프트웨어 산업의 융합이 활발히 추진되고 있다. 이러한 융합 소프트웨어는 고신뢰 융합 소프트웨어 공학 기술을 통한 생산성과 품질 향상이 요구되고 있는데, 그 이유로 적용 분야의 대부분이 mission critical, safety critical 성격을 지니는 임베디드 시스템이라는 점과 기존의 국가 주력 산업 분야와 소프트웨어 산업의 융합을 통해 신 성장 동력을 창출할 수 있다는 점을 들 수 있다.

이러한 배경으로 본 논문에서는 다양한 융합 도메인들을 위하여 기존의 소프트웨어 공학 기술이 어떻게 효과적으로 사용될 수 있는지를 연구한다. 연구 대상 도메인으로는 그 중요성과 장래성을 고려하여 최근 정부 육성 5대 지원 사업 중 하나인 '의료산업'과 녹색 성장으로 인해최근 중요성이 강조되고 있는 '스마트 그리드'을 선정하였다.

본 연구에서는 일차적으로 각 도메인들을 연구하고 특성들을 분석한다. 이러한 분석을 통하여 각 도메인의 특성과 현안 문제에 적절한 소프트웨어 공학 기법들을 선정하여 각 도메인의 중요 이슈(안전성, 품질 향상 등)들을 해결한다. 즉 의료 산업 중 인공 심장 제어 소프트웨어를 분석하고 이 분야에서 가장 중요시 되는 안전성 확보를 위하여 테스팅과 정형 검증을 적용하여 해당 소프트웨어들의 무결점을 입증한다. 스마트 그리드 시스템 분야에서는 중요 component들의 안전성과 품질 향상을 위하여 통신 프로토콜을 정형적으로 검증하고 사이버 보안 문제에 대한 해결 방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 인공 심장 제어 소프트웨어 관련 테스팅과 정형검증 기법 적용을 설명하며, 3장에서는 스마트 그리드 시스템에 대한 설명과 스마트 그리드 시스템에서 사용되는 통신 프로토콜에 대한 정형 검증 및 사이버 보안 문제에 해결에 대해서 논한다. 끝으로 4장에서는 본 연구에 결론을 제시한다.

2. 인공 심장 제어 소프트웨어를 위한 소프트웨어공학 기술 적용

2.1 인공심장 제어 소프트웨어

해마다 발생하는 말기 심장 질환 환자의 절대적인 수와 그 증가 폭은 심장 기증자의 수에 비해 상당히 크다. 인공심장 기술은 적용 정도에 따라 심장 전체나 일부분을 대체할 수 있으므로, 심장 기증자의 부족에 대응할 수 있다. 인공심장은 그 장치의 고장이나 오작동이 인명의 손실과 직결되는 safety critical system 이라 할 수 있으며, 또한 이러한 이유로 제품의 기능과 새로운 기술의 적용 여부도 중요하지만, 설계와 검증 역시 매우 중요하다. 인공심장은 크게 혈액을 이송할 펌프와 그 펌프를 제어하는 소프트웨어로 이루어지며, 이러한 제어 소프트웨어는 인공심장 안전성을 위해서 정형 검증이 필수적이다.

본 연구가 대상으로 삼는 한국인공장기센터[1]에서 개발한 인공심장 H-VAD(Hybrid Ventricular Assist Device)의 제어 소프트웨어는 주로 event-driven 방식으로 작동하며 각종 센서를 통해 주기적으로 현재 인공심장과 사람의 상태를 파악한다. 외부에서 입력이 있을 경우, 그 입력과 현재의 상태 값을 조합하여 적합한 행동을 결정하며, 입력 값이 존재하지 않을 경우는 현재 상태 값을 이용하여 다음 행동을 결정한다. 그러므로, 인공심장 제어 소프트웨어는 현재 상태와 입

* 종신회원
† 본 과제는 정보통신산업진흥원의 SW공학 요소기술 개발과 전문인력 양성사업의 결과물임을 밝힙니다.

력 값의 실효 범위 및 획득 방법, 조합 알고리즘 등 다양한 검증 필요성을 가지고 있다.

2.2 테스팅 기법

테스팅은 소프트웨어의 동작이 부정확하거나 혹은 명세서와 일치하지 않는 소프트웨어의 결함을 발견하기 위한 절차이다. Code coverage는 소스 코드 상에 작성된 각 실행 명령이나 분기문 등이 테스트 케이스에 의해 얼마나 수행 되었는지를 나타내며, 그 주된 종류는 표 1과 같다.

소프트웨어 테스팅을 수행하기 위해서는 다양한 입력 값과 실행 환경을 필요로 한다. 그러므로, 효율적인 테스팅을 위해서는 체계적으로 입력 값과 수행 환경을 작성해야 하며, CASE(Computer-Aided Software Engineering) 도구들이 테스팅 수행에 상당한 도움을 줄 수 있다. 이러한 테스팅 CASE 도구에서 중요시 되는 기능은 테스팅 과정의 자동화와 가시적인 결과 표현이다. 그림 1은 SureSoft Tech사 에서 개발한 Code Scroll 테스팅 도구 실행 화면으로서 분기문 논리식의 경계 값을 기반으로 입력 값을 자동 생성하며 테스팅 결과를 가시화하여 직관적으로 보여준다.

Code coverage는 소프트웨어의 실질적인 수행 경로를 이용한 척도로서, 명세대로 수행되지 않은 코드나 분기문 등에 의해 발생할 수 있는 오류를 검증하는데 유용하다. 하지만, 실행 된 코드에 대한 행동 적합성이나 소프트웨어 시스템 전체에서 지켜야 할 특성 만족 유무를 검증할 수 없으므로, 모델 체킹과 같은 정형 검증 기법을 도입할 필요성이 있다.

표 1 Code coverage의 종류

이 름	설 명
Function coverage	모든 함수나 subroutine이 호출되었는지 여부
Statement coverage	모든 statement가 실행되었는지 여부
Branch coverage	모든 분기가 실행되었는지 여부
Condition coverage	모든 조건문의 각 논리식이 평가되었는지 여부
Path coverage	수행 가능한 모든 경로가 실행되었는지 여부

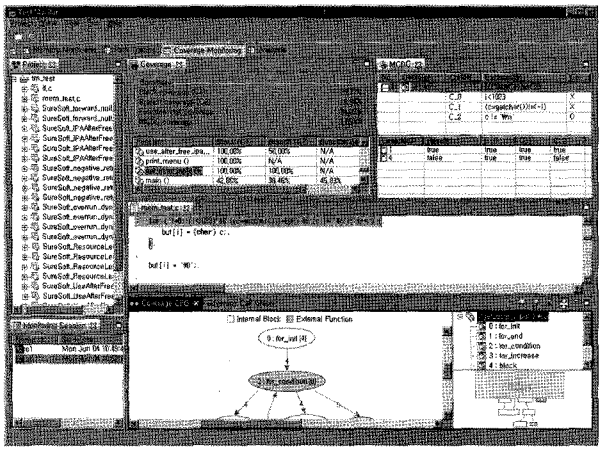


그림 1 Code Scroll Test Monitor

본 연구에서는 대상 인공심장 제어 소프트웨어에 대해 branch coverage를 code coverage의 척도로 사용한다. 테스팅을 효과적으로 수행하기 위해 대상 소프트웨어의 작동 환경에 맞춰 전용 CASE 도구인 H-VAD Path Logger를 구현하였으며 실행 화면은 그림 2와 같다.

H-VAD Path Logger는 대상 인공심장 제어 장비인 H-VAD와 통신하며 인공심장 제어 소프트웨어의 실행 경로 정보를 수집한다. 수집된 정보는 사전에 구축한 전체 탐침 코드 목록과 비교하여 branch coverage를 측정하고 그 결과를 가시적으로 보여준다. 그림 2는 현재 인공심장 제어 소프트웨어가 CDMA_Sub, main, DefaultIsr 등과 같은 소스코드로 이루어져 있으며 main 코드 내 main 함수에 있는 118라인 탐침이 수행되지 않은 경우를 보여 주고 있다. 실행 경로는 사전에 인공심장 제어 소프트웨어의 분기문에 따라 심어진 탐침 코드에 의해 측정된다. H-VAD Path Logger의 특징을 정리하면 다음과 같다.

① 대상 소프트웨어 실행 경로를 수집.
② branch coverage 척도를 측정 가능.
③ 소스 코드 및 함수 별 테스팅 수행 및 결과 분석을 효과적으로 수행할 수 있도록 GUI를 활용.

2.3 SATABS를 이용한 정형검증

모델 체킹 기법은 하드웨어 검증에 매우 효과적으

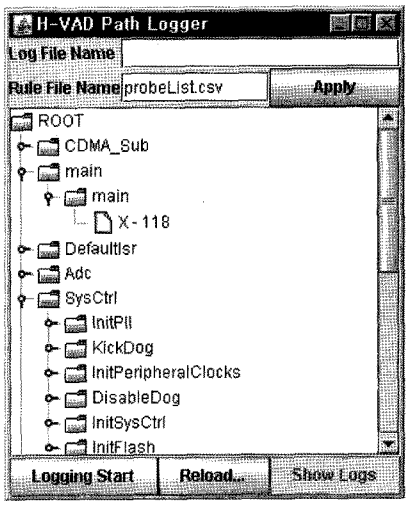


그림 2 인공심장 제어 소프트웨어 branch coverage 측정 도구 H-VAD Path Logger

로 사용되어 왔지만, 소프트웨어 검증에는 다음과 같은 이유로 제약점이 있었다. 즉, 대형 소프트웨어에 적용될 수 없었고, 대상 언어로 주요 프로그래밍 언어를 받아들이지 않았기 때문이다. 이러한 두 가지 제약점에 대해서 SATABS[2]는 counter-example guided abstraction refinement 기법을 이용하고 ANSI-C를 대상 입력 언어로 채택함으로써, 그러한 문제점들을 해결하였고, 따라서 대형 C 언어 소프트웨어 검증에 효과적으로 사용되고 있다.

SATABS는 abstract 모델을 생성하기 위해서 SAT 기반의 Boolean quantification을 이용하여, 본래 모델의 conservative abstraction(over-approximation)을 CNF (Conjunctive Normal Form) 식으로 생성한다. 생성된 CNF 식은 기존의 SAT solver 기반의 모델 체킹 툴에 의해서 검증된다. 검증 결과, abstract 모델에서 사용자가 검사하고자 하는 safety property가 만족되었다면, conservative abstraction을 사용했기 때문에, 본래 모델에서도 검증된 safety property가 만족되는 것을 알 수 있다. 하지만, 검사한 safety property가 위배된 경우에는 모델 체킹 툴이 생성한 counter-example이 실제 가능한 행위(behavior)인지 over-approximation에 의한 허구적인 행위인지 검사한다. 이러한 검사도 모델 체킹 도구에 의해서 자동적으로 이루어진다. 만약, 그 counter-example이 실제 행위라면, 원래 모델에서도 그 counter-example이 유효한 것이고, 그렇기 때문에 본래 모델은 주어진 safety property를 위반하는 것이다. 만약, 해당 counter-example이 허구인 것으로 판명되면, 현재 abstraction에 대한 refinement 단계를 거쳐, 보다 정확한 abstraction 모델을 생성하고, 위에서 설명한 모델 체킹 단계를 반복한다. SATABS는 이러한 반복 과정을 통해서, 본래 모델이 주어진 safety property를 만족하는지를 입증하거나, counter-example을 찾아낼 수 있으며, 최악의 경우는 여러 번의 refinement 단계 끝에 본래 모델에 대한 문제를 풀 수도 있다.

2.4 적용 결과 및 기대 효과

2.4.1 테스팅

본 연구에서 테스트 하고자 하는 인공 심장 제어 소프트웨어는 embedded software로서 실행과 테스팅 환경 구축에 제약 사항이 많다. 본 연구에서 다양한 테스팅 도구의 embedded software 적용 적합성을 조사한 결과, 목적 인공심장 제어 소프트웨어 작동 환경에 특화된 CASE 도구를 구현하기로 결정하여 현재 실험 단계에 있다.

향후 과제로서 code coverage 테스팅을 통해 작성된 인공심장 소프트웨어 코드가 현실적으로 발생할 수 있는 모든 입력 값과 환경 변화에 대해 안전하게 작동함을 보이고자 한다.

2.4.2 SATABS를 이용한 검증 결과

본 연구에서는 2.3절에서 소개한 SATABS를 이용하여 인공 심장 제어 소프트웨어에 대한 기본적인 safety property 검증을 수행한다. 검증 대상 코드로 main 함수와 주요 인터럽트 핸들러 함수(타임 인터럽트 함수인 T3INT_ISR, 6개의 버튼 인터럽트 함수, 4개의 센서 인터럽트 함수)들을 포함하며, 위의 함수들이 호출하는 모든 함수들도 포함한다. 그리고, 하드웨어에서의 인터럽트 발생을 모델링하기 위하여, main 함수의 while 문 안에서 다음과 같이 SATABS에서 제공하는 non-determinism[2]을 이용하여 인터럽트 핸들러 함수들을 호출하였다.

```
void main(void){
   ...
   while(1){
      ...
      int nd_intrpt = nondet_int();

      if(nd_intrpt<0) T3PINT_ISR();
      else if(nd_intrpt<1) CAPINT1_ISR();
      else if(nd_intrpt<2) CAPINT2_ISR();
      ...
      else if(nd_intrpt<6) CAPINT6_ISR();
      else if(nd_intrpt<7) CAPTURE1();
      ...
      else if(nd_intrpt<10) CAPTURE4();
      ...
   }
   ...
}
```

검증 property로는 35개의 '배열에 대한 underflow 및 overflow' 검사, 9개의 'division by zero' 검사를 수행하는 중이다. 그림 3은 검증 결과의 일부로서, 타임 인터럽트 함수 T3INT_ISR에 대한 모델 체킹 수행 화면을 보여준다. SATABS는 632초 동안 31번의 abstraction/refinement 단계를 수행하여, 위에서 설명한 property 주의 일부인 30개 safety property가 모두 만족함을 보였다. 현재, 전체 프로그램에 대한 모델 체킹이 진행 중이며, 향후 과제로서 프로그램 개발자나 검증자가 중요 변수들에 대한 assert 문을 삽입하여, 그 변수들의 값이 의도한대로 바뀌는지를 검증할 계획이다.

```
>satabs T3PINT_ISR.c --function T3PINT_ISR
file T3PINT_ISR.c: Parsing
R3PINT_ISR.c
Converting
Type-checking T3PINT_ISR
Generating GOTO Program
122 functions, 1288 instructions.
Removing function pointers

...

Verified 772 original clauses.
Verified 796 original clauses.
Verified 2544 original clauses.
Verified 772 original clauses.
Verified 798 original clauses.
Refining set of predicates according to
counterexample
*** CEGAR Loop Iteration 31
Computing Predicate Abstraction for Program
Running Cadence SMV: smv -force -sift
VERIFICATION SUCCESSFUL
Time: 632.437 total, 44.124 abstractor, ···
Iterations: 31
Predicates: 43
```

그림 3 SATABS 수행 결과

3. 스마트 그리드를 위한 소프트웨어공학 기술 적용

현대에 있어서 전기는 모든 분야의 바탕이 되는 중요한 자원으로 전력망에 문제가 생기면 곧바로 생활에 상당한 지장이 오게 된다. 이러한 이유로 차세대 성장 동력인 그린 IT 부문의 핵심 분야로 대두되고 있는 스마트 그리드에서 시스템의 신뢰성과 안전성을 확보하는 일은 매우 중요하다. 또한, 인터넷과 연동되기 때문에 보안 역시 중요한 문제로 대두되고 있다. 본 연구에서는 스마트 그리드 시스템의 특징을 분석하여 소프트웨어의 안전성을 높이고, 보안 문제를 해결 할 수 있는 기술들을 제시한다.

3.1 스마트 그리드

스마트 그리드는 '발전-송전-배전-판매'의 단계로 이루어지던 기존의 전력망에 정보기술(IT)을 접목하여, 전력공급자와 소비자가 양방향으로 실시간 정보를 교환, 에너지효율을 최적화하며 새로운 부가가치를 창출하는 차세대 전력망이다. 발전, 송전, 배전, 소비자를 양방향 통신망으로 연결하여 전력시스템 전체가 한 몸처럼 작동하는 것이 기본 개념이다.

이를 활용하여 전력 공급자는 전력 사용 현황을 실시간으로 파악하여 공급량을 탄력적으로 조절할 수 있다. 그리고, 전력 소비자는 현재 전력 요금을 실시간으로 파악하여, 요금이 비싼 시간대를 피하는 등 시간과 사용량을 조절할 수 있으며, 태양광 발전 등 가정에서 생산되는 전기를 판매할 수도 있게 된다.

또한, 스마트 그리드는 자동조정 시스템으로 운영

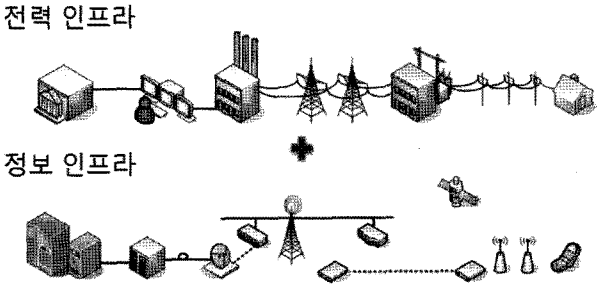


그림 4 스마트 그리드

되므로 고장 요인을 사전에 감지하여 정전을 최소화하고, 기존 전력시스템과는 달리 다양한 전력 공급자와 소비자가 직접 연결되는 분산형 전원체제로 전환되면서 풍량과 일조량 등에 따라 전력 생산이 불규칙한 한계를 지닌 신 재생에너지 활용도가 증대된다. 이러한 방법으로 신 재생에너지 활용도가 높아지면 화력발전소를 대체하여 온실가스와 오염물질을 줄일 수 있게 되어 환경문제를 해소하는데도 도움이 된다. 그림 4는 스마트 그리드의 개관을 보여 준다.

스마트 그리드는 이처럼 많은 장점을 지니고 있어, 세계 여러 나라들이 차세대 전력망으로 구축하기 위한 많은 사업들을 추진하고 있다. 우리나라도 가전제품과 네트워킹을 통하여 전력사용을 최적화하고, 소비자에게 실시간 전기요금 정보를 제공하는 전력관리장치 'Advanced Smart Meter'와 전기자동차 충전 인프라, 분산형 전원(배터리), 실시간 전기요금제, 전력망의 자기치유 기능, 신 재생에너지 제어 기능, 직류(DC) 전원 공급, 전력 품질 선택 등을 필수요소로 하는 '한국형 스마트 그리드 비전'을 발표하였다. 또한, 제주특별자치도를 스마트 그리드 실증단지로 선정하고, 2010년부터 본격적으로 기술 실증에 착수한 뒤 2011년부터 시범도시를 중심으로 대규모 보급을 시작하며, 2020년까지 소비자 측 지능화를, 2030년까지 전체 전력망 지능화를 완료할 계획이다.

스마트 그리드 시스템의 중요 요소 중의 하나인 Advanced Metering Infrastructure(AMI) 시스템은 고객의 계측기와 유틸릴티 사이에 상호 작용을 하기 위한 주요 수단이다. AMI의 양방향 통신은 기본적인 계측뿐만 아니라, 고객의 장치와 시스템 사이에서 정보를 교환하는 제3자(제3서비스 제공업체)에 의해서 수 많은 서비스와 기능을 제공 가능하게 한다. 그림 5는 AMI의 구성을 보여 준다.

3.2 모델 체킹

그림 5에서와 같이 스마트 그리드에서 고객과의 정보 교환 등을 담당하는 AMI 시스템에는 많은 구성요

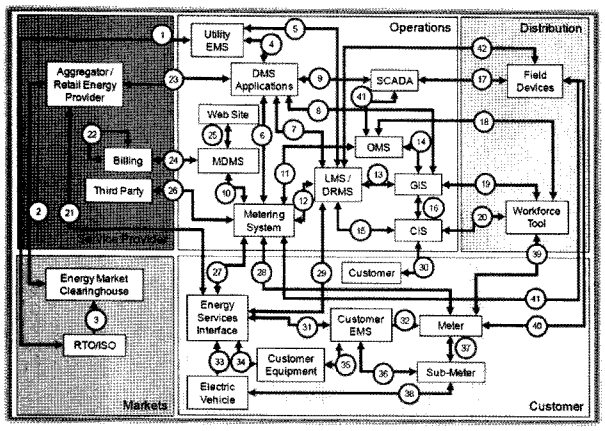


그림 5 AMI의 구성

소들이 존재하며, 서로가 다양한 방식으로 통신을 하고 있다. 이러한 AMI 시스템에 들어가는 소프트웨어의 안전성을 높이기 위한 방법으로 모델 체킹이 있다.

모델 체킹은 시스템을 수학적 모델로 기술하여 주어진 요구 사항을 만족하는지를 검증하는 정형 기법의 하나이며, 이미 많은 분야에서 고 등급의 소프트웨어 안전성 등급을 받기 위해서는 정형기법을 적용할 것을 요구하고 있다. 모델 체킹이 받아들이는 입력 두 가지는 정형적인 언어로 만들어져야 하며, 이러한 정형적 기술로 인해 모호함 없는 정확한 명세가 만들어지고 속성과의 관계를 수학적으로 증명할 수 있게 된다.

모델 체킹의 다른 특징으로 시스템 모델이 주어진 속성을 만족시키지 못했을 경우 만족 시키지 못한 이유를 보여주는 반례를 생성해 준다는 것이 있다. 이러한 반례의 존재로 인해 테스팅에서는 찾기 힘든 오류의 원인을 보다 쉽게 찾을 수 있게 해준다. 그림 6은 모델 체킹 기법의 high-level overview를 보여준다.

본 연구에서는 스마트 그리드, 특히 AMI 시스템의 안전성을 위해 모델 체킹 도구 중에서 SPIN[3] 모델 체커를 이용한 정형 검증을 제안한다.

SPIN(Simple Promela Interpreter) 모델 체커

SPIN은 Bell Labs에서 개발한 모델 체킹 도구로 통신 프로토콜과 같은 동시성 시스템의 논리적인 일관성을 분석하는 것을 목적으로 만들어졌으며, 많은 프로토콜의 검증에 사용되어 왔다.

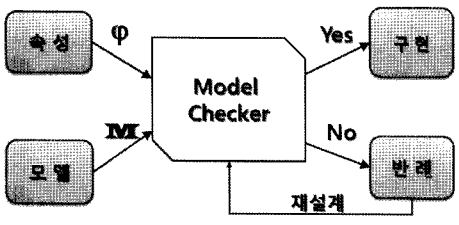


그림 6 모델 체킹

SPIN은 템플릿을 이용하여 프로세스의 행위들을 기술하고 이들 프로세스를 유한 오토마타로 변환 시킨다. 전체 시스템의 행위는 각 프로세스의 오토마타의 상태를 인터리브 방식으로 조합하여 산출한다. 이렇게 합쳐진 오토마타들은 전체 시스템의 행위를 나타내게 되며, 전역 도달성 그래프라고도 할 수 있다. 모델이 만족해야 할 속성은 시제 논리로 표현되어 다시 Buchi 오토마타로 변환된다. 이 Buchi 오토마타와 시스템의 그래프를 합하여 새로운 오토마타를 만들어 이를 만족하는 언어가 존재하는지를 검사하게 되면 원하는 모델이 속성을 만족하는지를 알 수 있게 된다.

그림 7은 SPIN을 이용한 검증을 하기 위해, 필요한 모델의 명세를 오토마타로 나타내고, 속성을 시제 논리로 표현한 것을 보여준다. 이 모델은 다시 SPIN의 입력 언어인 promela로 바꾸어서 검증을 하게 된다. 이러한 SPIN은 병렬적으로 행동을 하는 비동기적 프로세스들을 명세하기에 좋은 특성을 가지고 있기에 서로 독립적으로 행동을 하게 되는 프로토콜을 명세하게에 알맞다.

본 연구에서는 AMI 시스템의 주요 구성요소들의 모델을 SPIN의 입력언어인 promela로 기술하고, 중요 안전성 요구사항들을 선형시제 논리로 기술한 후, SPIN을 이용하여 검증하고자 한다.

3.3 스마트 그리드 보안

스마트 그리드 시스템(관련 SW 포함)은 안정적이고 신뢰할 수 있는 서비스를 제공하기 위해 네트워크로 고객의 개인정보, 실시간 요금정보 등 중요한 데이터를 송수신해야만 한다. 하지만, 2005년부터 진행된 대부분의 중대형 주요 전력 IT과제들이 하나같이 보안을 고려하지 않고 개발이 되어 왔으며, 이는 스마트 그리드 실용화 단계에 이르러 큰 문제점이 될 수 있다.

서비스 과정에 송수신되는 데이터가 손실, 도청 또는 위조되거나, DDoS 공격으로 인해 서비스가 마비된다면 현재 인터넷 환경에서보다 물리적/경제적으로 더 큰 피해가 예상됨을 표 2를 통해 알 수 있다.

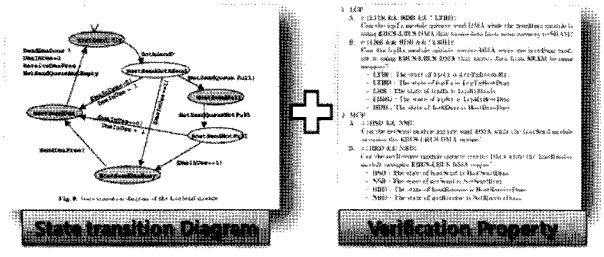


그림 7 SPIN을 이용한 검증

표 2 DDoS 공격 비교(인터넷 vs. 스마트 그리드)

인터넷 (7.7 대란)	구 분	스마트그리드
한국, 미국 주요 기관 사이트	목 표	발전소, 건물 등
DDoS 공격	공격방식	DDoS 공격
봇 넷	공격도구	봇 넷
악성코드 유포로 해킹경유지(봇넷) 확보 → 공격명령 하달 → 봇넷을 통해 DDoS 공격	공 격 시나리오	스마트 그리드 계량기에 악성코드 침투 → 다른 계량기로 전파 → 건물 전체 또는 NAN 규모 이상의 계량기 통제 → 봇넷을 통해 DDoS 공격
주요 사이트 서비스 중단 PC 하드디스크 자료 삭제	공격결과	도시 전 지역 정전

3.3.1 스마트 그리드 보안 위협

스마트 그리드의 중요 요소인 AMI와 EV(Electric Vehicle)는 스마트 그리드의 특성인 양방향통신과 개방성 등으로 인해 보안에 있어서 많은 위협이 존재한다.

① AMI 보안 위협
- 비인가 된 제어명령을 발생시켜 특정지역의 전기를 공급/차단
- 특정 사용자의 계정 정보를 조작하여 요금 수정
- 게이트웨이나 집중기로 많은 양의(전력)요청을 전송하는 등의 DoS 공격으로 서비스 마비를 유발

② EV 보안 위협
- EV : 운전자정보 및 차량등록정보 위조
- EV 충전 인프라 : 타인의 집(전용 충전장소)에서 충전하거나, 위조된 정보를 이용하여 충전소(주차장) 등 공공장소에서의 충전으로 비용지불을 회피

3.3.2 스마트 그리드 보안요구사항

스마트 그리드 시스템은 많은 부분에서 인터넷과 같은 보안조건을 요구하지만, 환경, 장비 등의 차이로 일부에서는 더 복잡하고 특별한 보안을 요구한다.

허가되지 않은 자의 정보접근 차단을 통한 기밀성(Confidentiality), 허가되지 않은 정보의 수정, 도청 방지를 통한 무결성(Integrity), 정상적인 사용자의 서비스 이용 및 DoS 공격 차단을 통한 가용성(Availability)을 보장해야만 하며, 이와 더불어 서비스 요청과 결재 등 재정적인 부분에 대한 문제 발생을 막기 위해, 책임성(Accountability) 또는 부인방지(Non-repudiation) 등이 요구되어진다.

본 연구에서는 인터넷 환경 하에서 위의 요구조건을 충족하기 위해 연구되었던 인증, 암호화, DDoS 공격탐지/차단 등 다양한 보안 메커니즘에 기반을 둔 추가적인 연구를 통해 스마트 그리드 시스템에 적용 가능한 보안메커니즘을 개발할 것이다. 특히 AMI 시스템의 사용자 단에서 공격 행위를 탐지/차단하기 위한 공격 근원지 기반 rate limiting 기법[4]과 HAN, NAN, WAN의 네트워크 단에서 봇들의 그룹 행위 탐지[5]는 DDoS 등의 공격을 AMI 시스템 내/외부에서 방어하기 위해 활용할 수 있을 것이다.

3.5 적용/기대 결과

많은 통신을 해야 하며 데이터가 매우 중요한 역할을 할 AMI 시스템에서 사용될 프로토콜이 요구사항을 만족하는지를 증명하는 것은 안전한 시스템을 제작하기 위한 기초가 된다. 이러한 이유로, SPIN을 이용한 AMI 안전성 검증은 스마트 그리드 품질 향상에 많은 도움이 될 것이라 예상할 수 있다.

또한, HAN에서의 공격 근원지 기반 탐지 기법, NAN과 WAN에서의 네트워크 기반 탐지 기법은 스마트 그리드 시스템의 총체적인 보안을 구축하여, 안정적인 서비스를 제공하고 피해를 최소화하는데 기여한다.

4. 결 론

본 논문은 다양한 산업들과 IT산업의 결합인 융합소프트웨어의 고신뢰도 달성을 위하여, 각 도메인에 맞는 소프트웨어공학 기술의 적용을 제안하였다. 이러한 적용은 각 도메인 융합소프트웨어의 품질 및 안전성을 높이는데 많은 기여를 할 것으로 기대된다. 향후 연구 과제로, 본 논문에서 제안한 소프트웨어공학 기술 적용을 완료하여, 그 결과를 구체적으로 분석하는 연구가 필요하다. 또한, 각 도메인에 알맞은 기술들을 타 도메인에 적용하는 연구 또한 상당한 가치가 있을 것으로 예상된다.

참고문헌

[1] 한국인공장기센터. Korea Artificial Organ Center. http://www.kaoc.or.kr/

[2] E. Clarke, D. Kroening, N. Sharygina, K. Yorav. SATABS: SAT-based Predicate Abstraction for ANSI-C. Tools and Algorithms for the Construction and Analysis of Systems(TACAS2005), pp.570-574, 2005.

[3] Gerard J. Holzmann: The Model Checker SPIN. IEEE Transactions on Software Engineering, vol.23(5): 279-295, 1997.

[4] Hyunsang Choi, Heejo Lee, Hyogon Kim. BotGAD: Detecting Botnets by Capturing Group Activities in Network Traffic. Int'l Conf. on Communication System software and middleware(COMSWARE), 2009.

[5] Keun Park, Dongwon Seo, Jaewon Yoo, Heejo Lee, Hyogon Kim. Unified Rate Limiting in Broadband Access Networks for Defeating Internet Worms and

DDoS Attacks, Information Security Practice and Experience Conference(ISPEC), pp.176-187, 2008.

차 성 덕

1983 University of California, Irvine 전산학 학사
1986 University of California, Irvine 전산학 석사
1991 University of California, Irvine 전산학 박사
현재 고려대학교 정보통신대학 교수
관심분야 : Software Engineering, Computer Security
E-mail : scha@korea.ac.kr

최 진 영

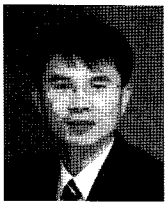
1982 서울대학교 컴퓨터공학 학사
1986 Derexel University 컴퓨터공학 석사
1993 University of Pennsylvenia 컴퓨터공학 박사
현재 고려대학교 정보통신대학 교수
관심분야 : 계산 이론, 수리 논리, 실시간 컴퓨팅, 정형기법, 프로그래밍 언어, 프로세스 대수, 소프트웨어 공학, 프로토콜 공학
E-mail : choi@formal.korea.ac.kr

김 선 한

1983 고려대 의학과 학사
1987 고려대 의학과 석사
1993 고려대 의학과 박사
현재 고려대학교 의과대학 교수
관심분야 : 로봇 수술, 직장 암
E-mail : drkimsh@korea.ac.kr

이 희 조

1993 포항공과대학교 컴퓨터공학 학사
1995 포항공과대학교 컴퓨터공학 석사
2000 포항공과대학교 컴퓨터공학 박사
현재 고려대학교 정보통신대학 부교수
관심분야 : 네트워크 보안, 악성 코드 탐지 및 분석, 스마트 그리드 보안
E-mail : heejo@korea.ac.kr



장 길 수

1991 고려대학교 전기공학 학사
1994 고려대학교 전기공학 석사
1997 Iowa State University 전기공학 박사
현재 고려대학교 전기전자전파공학부 교수
관심분야 : Power Quality, Power System Dynamics and Controls, Computer Applications in Power System Engineering, Distributed Energy Resources Integration
E-mail : gjang@korea.ac.kr

남 원 홍

1998 고려대 컴퓨터학과 학사
2001 고려대 컴퓨터학과 석사
2007 University of Pennsylvania 컴퓨터공학과 박사
현재 고려대학교 정보통신대학 연구교수
관심분야 : Formal Methods, Formal Verification
E-mail : whnam92@korea.ac.kr

최 재 순

1995 서울대학교 제어계측공학과 학사
1997 서울대학교 의공학과 석사
2003 서울대학교 의공학과 박사
현재 고려대학교 의과대학 연구교수
관심분야: 의료용 로봇, 바이오메카트로닉스, 인공장기
E-mail : aequitas@korea.ac.kr

이 정 주

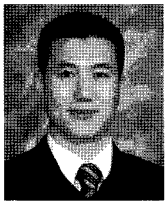
1998 한국과학기술원 전기 및 전자공학과 학사
2000 서울대학교 의공학과 석사
2004 서울대학교 의공학과 박사
현재 고려대학교 의과대학 연구교수
관심분야: 기계식 인공심장, 전자의료기기 제어, 외과수술 기기
E-mail : jungjoo.lee@gmail.com

정 세 훈

2010 고려대 컴퓨터학과 학사
현재 고려대학교 컴퓨터학과 석사과정
관심분야 : Testing, Requirement Engineering
E-mail : gifaranga@korea.ac.kr

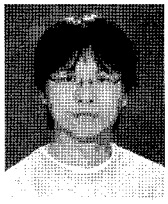
황 대 연

2002 고려대 컴퓨터학과 학사
2005 고려대 컴퓨터학과 석사
현재 고려대학교 컴퓨터학과 박사과정
관심분야: 정형기법, 수리 논리, 내장형 시스템, 소프트웨어 공학.
E-mail : dyhwang@formal.korea.ac.kr



송 경 섭

2002 공군사관학교 전산과학과 학사
현재 고려대학교 컴퓨터전파통신공학과 석사과정
관심분야 : 네트워크 보안, 스마트 그리드 보안
E-mail : cadetks@korea.ac.kr



신 병 윤

2007 고려대학교 전기전자전파공학부 학사
현재 고려대학교 전자전기공학과 석박사 통합과정
관심분야 : Distributed Energy Resources Integration, Smart Grid
E-mail : shinby@korea.ac.kr