Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.4, August 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.4.639

ACT를 이용한 AMI 보안 분석

위 미 선,[1†‡] 김 동 성,[2] 박 종 서[1]
[1]한국항공대학교, [2]캔터베리대학교

Security Analysis of AMI Using ACT

Miseon Wi,[1†‡] Dong Seong Kim,[2] Jong Sou Park[1]
[1]Korea Aerospace University, [2]University of Canterbury

요 약

스마트 그리드는 기존 전력망에 IT 기술을 접목하여 에너지 효율을 최적화하는 차세대 지능형 전력망으로 미국, 유럽, 일본 등 전 세계적으로 기술개발이 이루어지고 있으며 실증사업을 추진하고 있다. 최근 스마트 그리드에 대한 공격 사례가 증가되고 있으며 개인정보의 사용 및 유출의 피해가 높아지고 있다. 전력망이 더욱 복잡해지고 상호 연결됨에 따라 보안 분석과 평가에 대한 노력이 점차 중요해지고 있다. 본 논문에서는 스마트 그리드의 핵심 기술인 AMI(Advanced Metering Infrastructure)의 공격과 공격에 대한 대응책을 ACT(Attack Countermeasure Tree)를 이용하여 모델링 하였다. 보안 분석은 확률이 있는 경우와 확률이 없는 경우로 나누어서 수행하였다. 이러한 모델을 가지고 SHARPE(Symbolic Hierarchical Automated Reliability and Performance Evaluator)로 구현하여 다양한 경우의 확률과 ROA, ROI, Structure Importance, Birnbaum Importance에 대해 계산하였다.

ABSTRACT

Smart grid is a network of computers and power infrastructure that monitor and manage energy usage efficiently. Recently, the smart grid demonstration projects around the world, including the United States, Europe, Japan, and the technology being developed. The protection of the many components of the grid against cyber-threats has always been critical, but the recent Smart grid has been threatened by a variety of cyber and physical attacks. We model and analyze advanced metering infrastructure(AMI) in smart grid. Using attack countermeasure tree(ACT) we show qualitative and probabilistic security analysis of AMI. We implement using SHARPE(Symbolic Hierarchical Automated Reliability and Performance Evaluator) tool and calculate probability, ROA, ROI, Structure Importance, Birnbaum Importance.

Keywords: Smart grid, ACT, AMI

I. 서 론

스마트 그리드란 기존 전력망에 IT 기술을 접목하여 에너지 효율을 최적화 하는 새로운 형태의 차세대 전력 인프라이다. 스마트 그리드는 재생에너지 보급을 위한 인프라를 구축함으로써 산업 전반에 걸쳐 커다란 파급효과를 가져올 수 있는 신 성장 동력을 제공한다. 최근 스마트 그리드에 대한 공격으로 개인정보의 사용 및 유출, 정전사태 등 공격의 종류가 다양해지고 공격의 수준 또한 높아지고 있다. 전력 공급의 중추인 스마트 그리드가 사이버 공격에 피해를 입으면 국가 전력 마비와 같은 심각한 피해를 입게 될 것이다. 스마트 그리드의 공격 사례들은 점차 증가하고 있는 추세이며 이에 대한 보안 분석과 평가의 필요성이 높아지

접수일(2013년 2월 15일), 수정일(2013년 6월 10일), 게재확정일(2013년 6월 13일)
† 주저자, pingsue@kau.ac.kr
‡ 교신저자,pingsue@kau.ac.kr(Corresponding author)

고 있다.

본 논문의 스마트 그리드 ACT(Attack countermeasure tree)에서의 공격은 주로 스마트 미터 공격 위주로 되어있으며, 현재 스마트 그리드 보안의 주요 이슈도 스마트 미터에 집중되어 있다. 스마트 미터는 수 천 만개의 기기가 국가 전역에 배치되고, 보안에 취약한 장소에 배치 될 수 있기 때문에 해커들의 표적이 되기 쉽다. 또한 스마트 미터에 대한 다양한 공격들이 존재하고 이로 인해 단순한 공격에 대해서는 분석할 수 있지만 복잡하고 수준 높은 공격들의 분석에 관해서는 어렵다.

Patrick McDaniel은 스마트 그리드 등 다양한 분야에 대한 보안을 연구하기 위해서 공격 트리(attack tree)를 사용하였다[1]. 공격 트리는 시스템의 다양하고 복잡한 공격에 대해 보안 대책을 수립할 수 있도록 규칙적이고 체계적인 방법을 제공할 수 있다[2].

본 논문에서는 [1]의 공격 트리에 탐지와 완화 방법을 고려하여 AMI에 대한 ACT를 구현하였다. ACT는 공격뿐만 아니라 공격에 대한 탐지와 완화 방법까지 고려하여 공격 트리보다 다양한 분석이 가능하다. AMI에서 발생하는 다양한 공격들은 구조가 복잡하고 변수가 많기 때문에 각각의 이벤트(공격, 탐지, 완화)에 대한 확률을 명확하게 규정하기 힘들다. 따라서 AMI에 대한 보안 분석으로 확률이 있는 경우와 확률이 없는 경우로 나누어 수행하였다. 확률이 없는 경우의 보안 분석에는 Mincuts, Structure Importance Measures등을 사용하였다. 스마트 그리드의 시범단지나 테스트 베드를 통하여 스마트 미터 환경에서 발생하는 이벤트에 대한 확률을 구할 수 있으면 Risk, Cost, Impact, ROI, ROA, Birnbaum Importance Measures 등을 계산할 수 있음을 보였다. 이러한 모델을 가지고 SHARPE(Symbolic Hierarchical Automated Reliability and Performance Evaluator)를 이용하여 구현하고 위에서 언급한 metrics를 계산하였다.[3]

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구 및 배경 지식을 소개하고 3장에서는 AMI 시스템에 대한 ACT를 소개한다. 4장에서는 제안된 ACT를 이용한 보안 분석이 소개된다. 5장에서는 논문을 마무리하고 향후 연구에 대해서 기술한다.

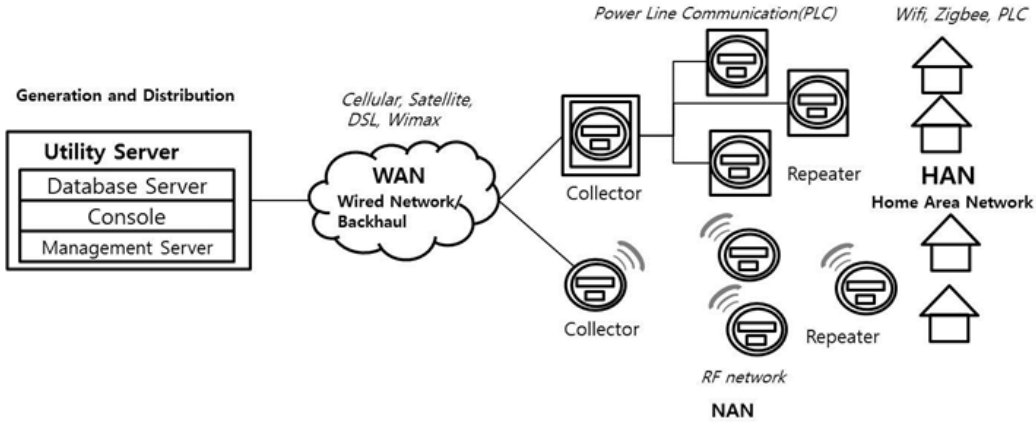
II. 배경지식 및 관련 연구

2.1 스마트 그리드

스마트 그리드는 전력망에 통신망을 접목시켜 전력계통 시스템의 제어를 통해 발전, 송전, 변전, 배전 등 전 과정에 대한 통제가 가능하고, 이를 통하여 에너지 사용의 효율성을 높이는 것이 궁극적인 목표이다. 스마트 그리드는 AMI(Advanced Metering Infrastructure)를 기반으로 미터와 유틸리티 서버 간에 통신이 이루어진다. AMI는 센서를 기반으로 한 컴퓨터 시스템이며 스마트 미터와 유틸리티간의 상호 정보교환이 가능한 통신 인프라이다. AMI는 공급자와 수요자간의 양방향 통신이 가능하며 원격으로 데이터를 수집하고, 실시간 통신 서비스, 광 대역 데이터 전송, 다양한 통신망을 이용할 수 있다[1].

AMI의 네트워크 구조는 [그림 1]과 같다. 로컬 네트워크 NAN(Neighborhood Area Network)에 스마트 미터가 배치되어 있으며 사용량을 수집한다. 리피터(repeater)는 총 사용량 데이터를 콜렉터(collector)에 전송한다. 콜렉터는 데이터를 유틸리티에 전송하는 역할을 한다. NAN은 단거리 통신 기술인 RF와 PLC(Power Line Communication)를 사용하여 메쉬 네트워크에서 스마트 미터를 연결하는데 사용한다. WAN(Wide Area Network)은 전달받은 데이터를 유틸리티 서버로 전송한다. WAN은 높은 대역폭의 원거리 통신 기술이 필요하며 사용하는 통신 기술은 PLC, cellular 기술, WiMAX등이 있다. WAN과 NAN을 연결하는 엑세스 포인트는 서로 다른 통신 기술 사이의 게이트웨이로서 동작한다. 콜렉터와 리피터는 마이크로 컨트롤러 유닛으로 구성되어 있으며 플래시 메모리, 스토리지, 통신 모듈로 구성되어 있다[4]. AMI는 대규모의 장비들이 서로 복잡하게 연결되어 있고 인증과 암호화의 구축이 완전하지 않기 때문에 해커의 타겟이 되기 쉽다. 따라서 이에 관련된 에너지 관련 범죄가 늘어나고 있는 추세이다.

AMI의 핵심 구성 요소인 스마트 미터(Smart Meter)는 자동으로 에너지를 계량 및 관리하는 기기로 CPU, 스토리지, 통신 인터페이스, 소켓으로 구성되어 있다. 전통적인 아날로그 미터 시스템은 한 달 또는 두 달에 한번 미터에 기록된 에너지 사용량을 검침원이 직접 체크한다. 이에 반해 스마트 미터는 실시간 에너지 측정 및 양방향 통신이 가능하며, 시간대별



〔그림 1〕 AMI 네트워크

측정되는 전력요금과 현재까지 사용한 에너지 사용량에 대한 정보를 사용자에게 제공한다. 유틸리티는 스마트 미터에서 수집한 데이터와 로그 정보를 통해 에너지 수요 현황을 파악함으로써 효율적이고 유동적인 전력 요금의 책정이 가능하다. 아울러 스마트 미터는 플랫폼의 무결성을 위해 유틸리티에 의해 플랫폼 상태가 관리되어야 한다. 따라서 유틸리티는 갑작스러운 에너지 공급 중단 현상 혹은 스마트 미터 내부의 기능적 문제가 생겼을 경우 펌웨어를 업데이트 하거나 저장되어 있는 임시 배터리로 전환시킴으로써 플랫폼의 무결성을 유지한다.

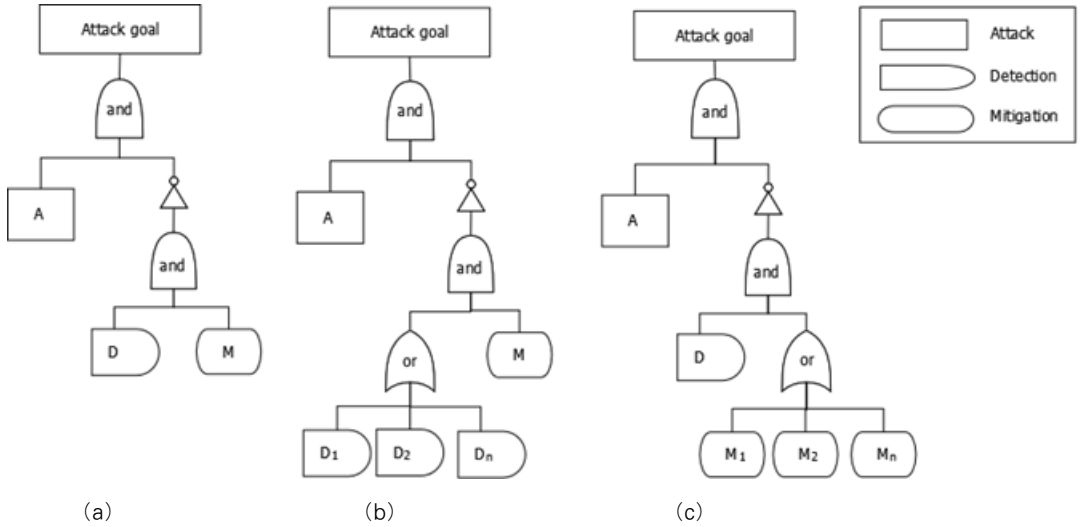
전력 송배전망에서는 대표적으로 SCADA (Supervisory Control And Data Acquisition) 제어 기술을 사용한다. SCADA 시스템은 원격으로 데이터를 수집하여 전력문제를 감시하고 제어하며 중앙위치로부터 명령을 내린다. 보통 SCADA는 네트워크로 상호 연결된다. 직접적인 발전 설비 운영은 디지털 제어 시스템에 의하여 제어되지만 전송, 배전 명령과 생산 출력을 조정하기 위해 SCADA 시스템과 통신하여야 한다. 이와 같이 스마트 그리드는 물리적이고 또한 수많은 정보 통신 기술을 이용하여 복잡하게 고도로 연결되어 있으며 상호 의존적이다. 스마트 그리드의 핵심 기술인 AMI의 취약성을 이용하면 금전적인 이득을 취할 수 있고, 발전 에너지 미터 수치를 조작 할 수 있다. 아날로그 미터에서 디지털 미터로 전환됨에 따라 공격 행위가 단순한 물리적인 공격에서 원격 침투와 복잡하고 여러 가지 상태 정보를 보유한 컴퓨터의 조작으로 이동하게 될 것이다. 최근 분산 서비스 거부 공격(DDos), 사용 기록기, 지능형 스마트 미터 Rootkit, 스마트 미터 기반 바이러스 및 다른 악성 소프트웨어 공격 등 지능적이고 수준 높은 공격들이 증가하고 있다. 이에 대비하여 기존 IT의 보안문제와 마찬가지로 스마트 그리드 또한 사이버 보안문제가 해결 되어야 한다.〔5〕

ACT는 특정 시스템에 대한 보안 모델을 디자인 할 때 사용 할 수 있는 하나의 모델로 공격 메커니즘과 방어 메커니즘이 결합된 트리 형태의 모델이다. 각 이벤트를 논리회로로 이용하여 조합하고, 공격 순서를 체계적으로 구현한다. 그에 대한 탐지나, 완화 방법에 대해서도 고려함으로써 보다 효과적인 보안 모델링을 할 수 있다〔3〕.

2.2 관련 연구

스마트 그리드는 복잡한 구조로 이루어져 있으며 상호간 프로토콜이 다르고, 데이터의 암호화와 인증 부분이 완전히 구축되어 있지 않다. 또한 시스템 설계상의 결함 등으로 인한 여러 가지 보안 문제점이 상당수 제기되고 있다. 스마트 그리드에 대한 보안 연구로 Robin Berthier는 AMI에 대한 대응책으로 침입 탐지 기반의 센서를 사용하는 것을 제안 하였다〔4〕. 이 센서를 사용함으로써 실시간으로 모니터링이 가능하고, 다수의 스마트 미터를 원격으로 공격하는 경우를 방지 할 수 있다.

송배전망을 제어하는 SCADA 시스템에 대한 보안 연구를 위해 공격 트리를 이용한 사례가 있다〔6〕. SCADA 시스템의 공격들에 대한 대응책을 공격 이벤트의 하위 리프 노드로 설정 하였다. 하지만 이 모델로 모든 공격의 취약점이 관측되지 않았다. 공격 트리 구조를 사용하여 대응책에 대해 분석하는 것은 한계가



〔그림 2〕 (a) 각각 하나의 공격 이벤트, 탐지 이벤트, 완화 이벤트로 구성된 ACT (b) 하나의 공격 이벤트와 여러 개의 탐지 이벤트, 하나의 완화 이벤트로 구성된 ACT (c) 하나의 공격 이벤트와 여러 개의 완화 이벤트, 하나의 탐지 이벤트로 구성된 ACT

있기 때문에 이를 보완하기 위해 ACT 모델을 사용하여 공격에 대한 대응책의 심층적인 분석을 할 수 있다. ACT에 대한 연구로 BGP 공격과 SCADA 시스템 공격, Malicious insider 공격 트리를 ACT를 구현하여 공격에 대한 탐지와 완화 방법의 효율성을 평가하였다. 세 가지 ACT를 이용하여 공격 트리보다 다양한 관점에서 분석이 가능함을 보였다[3]. AMI의 공격들을 확인할 수 있는 방법으로 AMI-Analyzer 툴을 제시하였다[7]. Abhishek Rakshit은 모든 호스트의 데이터를 중앙에서 관리하여 스마트 그리드의 공격을 탐지하는 구조를 제안하였다. 복잡한 구성의 AMI의 다양한 공격들에 대해 분석 할 수 있고 보안 지침에 따라 제대로 동작하고 있는지 확인함으로써 공격을 미연에 방지할 수 있다[8]. 하지만 프로그램 상의 결함이 많아 완벽한 탐지가 어렵고 보안 모델에 대한 보완이 필요하다. 현재 ACT를 이용한 스마트 그리드의 보안 연구가 많지 않아 기존의 공격 트리를 이용한 스마트 그리드 보안 분석에서 대응 대책을 추가한 ACT를 사용하여 보안 연구를 수행한다.

III. ACT를 이용한 모델링과 분석

3.1 ACT

ACT는 특정 시스템의 공격에 대한 탐지 방법이나 완화 방법을 적용하여 공격 메커니즘과 방어 메커니즘을 동시에 적용시킨 트리 구조 모델이다. ACT는 취약점 측정에 대한 Frame work로 사용될 수 있으며 각 대책의 유형의 개수나, 탐지와 완화 방법에 대해 알 수 있고 그럼으로써 구조, 대응을 더 쉽게 할 수 있다. 결론적으로 시스템의 보안 분석을 체계화 할 수 있다는 장점이 있다. ACT 모델은 다양한 metrics을 SHARPE 툴을 이용하여 계산할 수 있으며 이를 이용하여 여러 가지 분석이 가능하다. 공격과 보안에 대한 비용 측정과, Impact. Risk, ROI, ROA등을 구하여 확률적인 분석이 가능하며, 공격(attack)이나 탐지(detection), 완화(mitigation) 이벤트들의 구조적인 중요도를 판별하는 분석 또한 가능하다. ACT의 기본적인 구조는 〔그림 2〕와 같다. ACT는 공격, 탐지, 완화 이벤트로 구성되어 있고 보통 공격에 대한 탐지 이벤트가 수행 된 뒤에 완화 이벤트가 수행되므로 공격 이벤트를 왼쪽에 놓고 그 다음 탐지와 완화 이벤트 순서로 배열한다[3].

공격에 성공 했을 때의 확률은 게이트에 따라 계산 방법이 다르다. AND 게이트로 이벤트가 조합되었을 때 공격에 성공 할 확률은 $\prod_{i=1}^{n} P(i)$ 이다. 반면 OR 게이트로 이벤트가 조합되었을 때 공격에 성공할 확률은 $1-\prod_{i=1}^{n}(1-P(i))$이다. 〔그림 2〕의 a는 보통 ACT에서 자주 쓰이는 연산 구조로 goal에 도달하기 위한 확률식은 다음과 같다.

$$P_{goal} = P_A(1-P_D+P_D(1-P_M)) = P_A(1-P_D \times P_M) \quad (1)$$

〔그림 2〕의 a는 하나의 공격 이벤트와 탐지와 완화 이벤트로 이루어진 경우로 P_{goal}은 공격이 성공할 확률을 나타낸다. 이 수식은 공격이 탐지가 되지 않은 경우의 수식 $P_{UD}= P_A(1-P_D)$와 공격이 감지되었으나 완화 이벤트가 이루어지지 않은 경우의 수식인 $P_{DUM}= P_AP_D(1-P_M)$두 가지 경우를 고려한다. 〔그림 2〕의 b의 P_{goal}에 대한 식은 다음과 같다.

$$P_{goal} = P_A(1-(1-\prod_{i=1}^{n}(1-P_{D_i}) \times P_M) \quad (2)$$

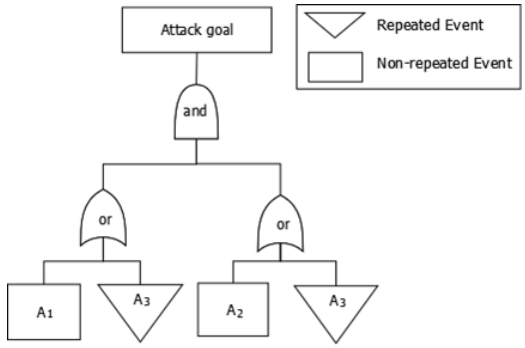
〔그림 2〕의 b는 하나의 공격 이벤트와 다수의 탐지 이벤트, 그리고 하나의 완화 이벤트로 이루어진 경우이다. 이 경우에도 공격이 탐지되지 않아 성공한 경우와 탐지는 되었지만 완화가 되지 않았을 때 $P_{DUM} = (P_A(1-\prod_{i=1}^{n}(1-P_{D_i})) \times (1-P_M)$를 나누어 고려한다. 〔그림 2〕의 c의 P_{goal}에 대한 식은 다음과 같다.

$$P_{goal} = P_A(1-P_D \times (1-\prod_{i=1}^{n}(1-P_{M_i}))) \quad (3)$$

〔그림 2〕의 c는 하나의 공격이벤트와 하나의 탐지 이벤트, 그리고 다수의 완화 이벤트로 이루어진 경우이다. 이 경우에도 공격이 탐지되지 않아 성공한 경우 $P_{DUM}= P_AP_D\prod_{i=1}^{n}(1-P_{M_i})$와 탐지는 되었지만 완화가 수행되지 않은 경우를 나누어서 고려한다. 지금 현재 모델에서는 고려하지 않았지만 ACT에서는 하나의 공격 이벤트에 대해서 다수의 완화와 탐지이벤트가 고려될 수 있다. 하나의 공격 이벤트와 m개의 탐지 이벤트, n개의 완화 이벤트로 이루어질 경우 식은 다음과 같다.

$$P_{goal} = P_A(1-(1-\prod_{i=1}^{m}(1-P_{D_i})) \times (1-\prod_{i=1}^{n}(1-P_{M_i}))) \quad (4)$$

〔그림 3〕은 공격 이벤트 중 반복되는 공격 이벤트가 포함된 공격 트리이다. 공격 트리를 설계할 때 리프 노드의 공격 이벤트 중 중복되는 이벤트가 있을 경우 위의 그림과 같이 표기한다. ACT 내에 반복되는 이벤트가 있는 경우에도 확률 계산은 AND 게이트와



〔그림 3〕 반복되는 이벤트(repeated event)가 포함되어 있는 공격 트리

OR 게이트의 조합에 따른 계산식을 이용하며, 〔그림 2〕와 동일한 방식으로 구한다. 〔그림 3〕의 경우 goal에 도달할 확률은 $P_{goal} = (1-(1-P_{A_1})(1-P_{A_3})) \times (1-(1-P_{A_2})(1-P_{A_3}))$이다. ACT를 이용하여 비용과 Impact에 대한 보안 분석을 할 때 반복되는 이벤트가 있는 경우와 반복되는 이벤트가 없는 경우의 계산 방식이 다르다. 반복되는 이벤트가 있는 경우 다음 장에서 소개할 Mincuts의 Boolean Function 이용하여 구한다.

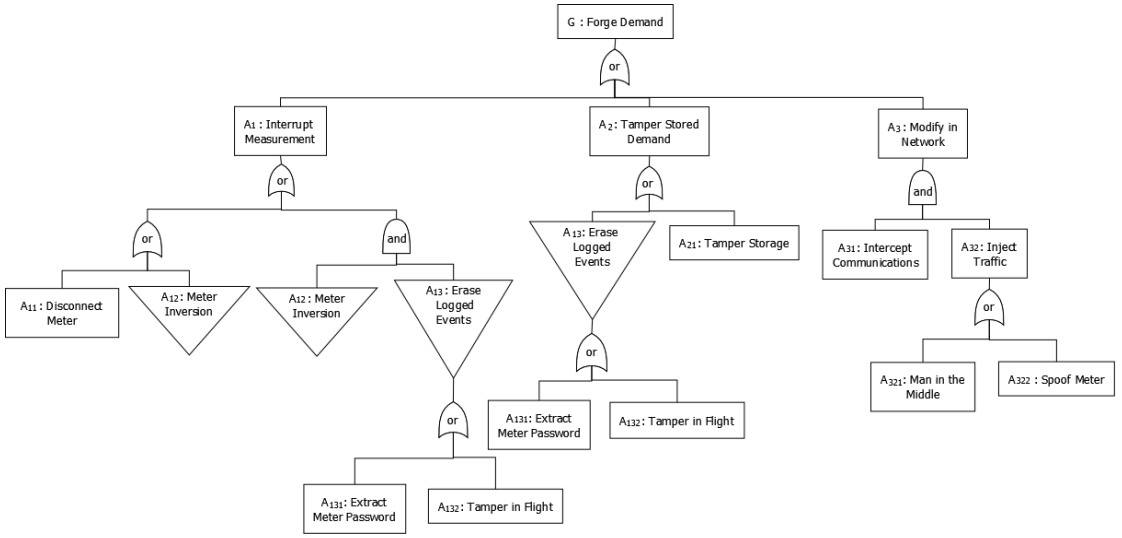
IV. ACT를 이용한 AMI 보안 분석

이번 장은 ACT를 구현함으로써 할 수 있는 보안 분석에 대해 설명한다. 보안 분석으로는 크게 확률이 없는 경우와 있는 경우로 나뉜다.

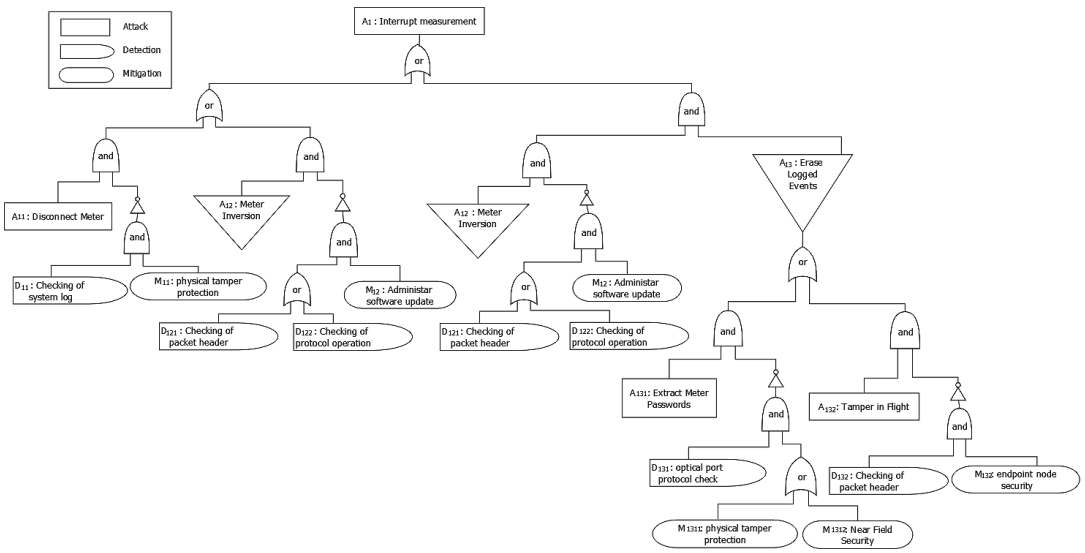
4.1 AMI에 대한 ACT

AMI의 공격과 대응책에 대한 보안 분석을 하기 위해 논문 〔1〕의 AMI 공격 트리(Attack Tree)를 이용하여 ACT로 구현하였다. 공격 트리의 노드들은 일반적으로 선택 가능한 OR 게이트와 목적을 달성하기 위해 반드시 수행해야 하는 AND 게이트로 연결된다. 공격 트리가 설계되면 여러 하위 노드들에게 가치를 할당하여 각각의 노드들의 가치를 계산하고 그 가치에 따라 보안 대책을 수립하게 된다〔9〕. 본 논문에서는 〔1〕의 AMI 공격 이벤트에 대한 탐지와 완화 이벤트 〔10〕를 추가하여 ACT를 구성하였다.

〔그림 4〕는 AMI에 대한 공격 트리로 하위 노드를 세 가지로 구분하였다. 스마트 미터가 사용량을 측정하기 전에 일어나는 공격(Interrupt Measurement),



〔그림 4〕 스마트 그리드에 대한 공격 트리



〔그림 5〕 A_1에 대한 ACT

스마트 미터가 사용량을 저장하기 전과 저장하는 과정에서 일어나는 공격(Tamper Stored Demand), 스마트 미터에서 데이터와 로그 정보를 유틸리티에 전송 할 때 일어나는 공격(Modify in Network)으로 구분하였다. 각각의 하위 노드에 탐지와 완화 이벤트를 적용하여 ACT를 구성하였으며, 공격에 대한 이벤트는 A, 탐지에 대한 이벤트는 D, 완화에 대한 이벤트는 M으로 표기하였다. 측정 방해 공격은 A_1, 스토리지에 대한 공격은 A_2, 데이터 전송 시 네트워크에서 일어나는 공격은 A_3으로 표기하였다. 루트 노드(root node)는 Forge Demand로 에너지 사용량 데이터와 로그 값을 읽어와 공격에 성공하는 것을 의미하며, 이것을 공격 트리의 최종 목적으로 정의하였다. 루트 노드는 G로 표기하였다.

각각의 리프 노드는 루트 노드에 도달하기 위한 이벤트를 의미한다. AND 게이트와 OR 게이트의 계산식을 이용하여 P_{goal}을 구할 수 있다. 반복되는 이벤트는 〔그림 3〕과 같이 표기한다.

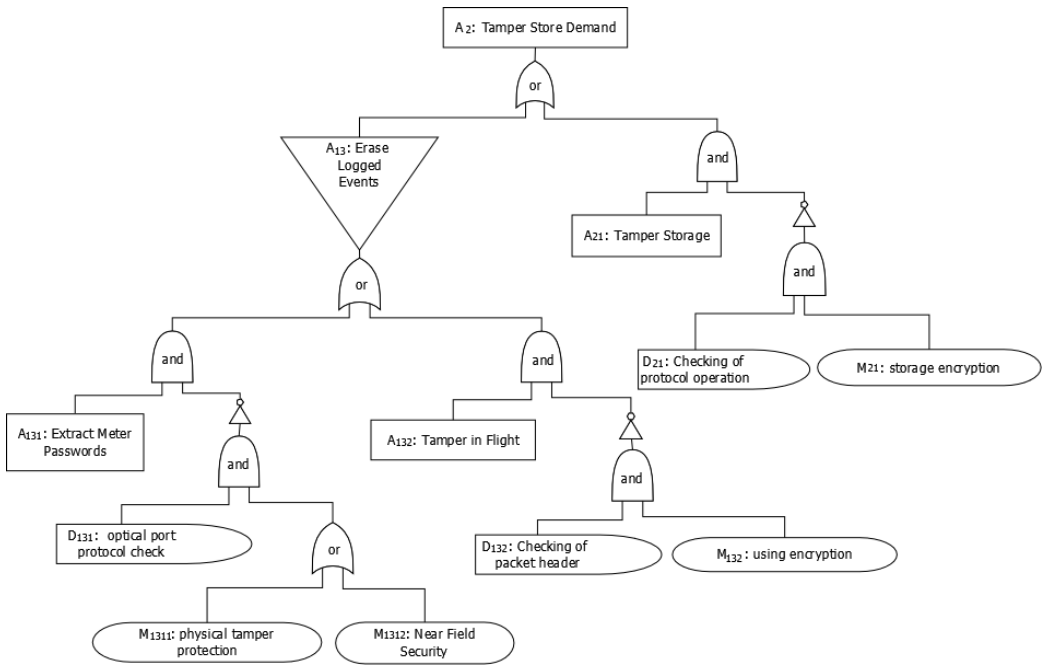
〔그림 5〕, 〔그림 6〕, 〔그림 7〕은 앞의 공격 트리에 탐지나 완화 이벤트를 추가한 ACT이다. 세 개의 ACT가 상위에 OR 게이트로 결합하여 루트 노드에 도달하게 된다.

〔그림 5〕는 A_1의 어택 트리에 탐지와 완화 이벤트를 추가한 ACT이다. 주로 에너지 사용량을 측정하기 전에 일어나는 공격이다. 대부분 물리적인 공격으로 해커가 직접 부품들을 제거하거나 주사기를 삽입해 전기신호를 빼내는 공격, 스마트 미터의 물리적 흐름을 방해하기 위한 연결 분리 공격(A_{11})과 스마트 미터 소켓 내의 사용 측정기를 되감는 공격(A_{12})이 있다. 모든 스마트 미터는 이벤트나 로그 정보를 유틸리티에 전달하기 때문에, 이 두 가지의 공격이 성공하려면 이런 이벤트에 대한 로그를 지우는 작업(A_{13})이 필요하다. A_{11}는 시스템 로그를 확인하는 것으로 탐지 가능하며(D_{11}), 스마트 미터의 물리적 공격 보완(M_{11})으로 완화한다. A_{12}는 데이터의 패킷 헤더 확인(D_{121})과 프로토콜 동작 모니터링(D_{122}) 함으로써 탐지 가능하며 스마트 미터의 주기적인 소프트웨어 업데이트(M_{12})로 완화 할 수 있다.

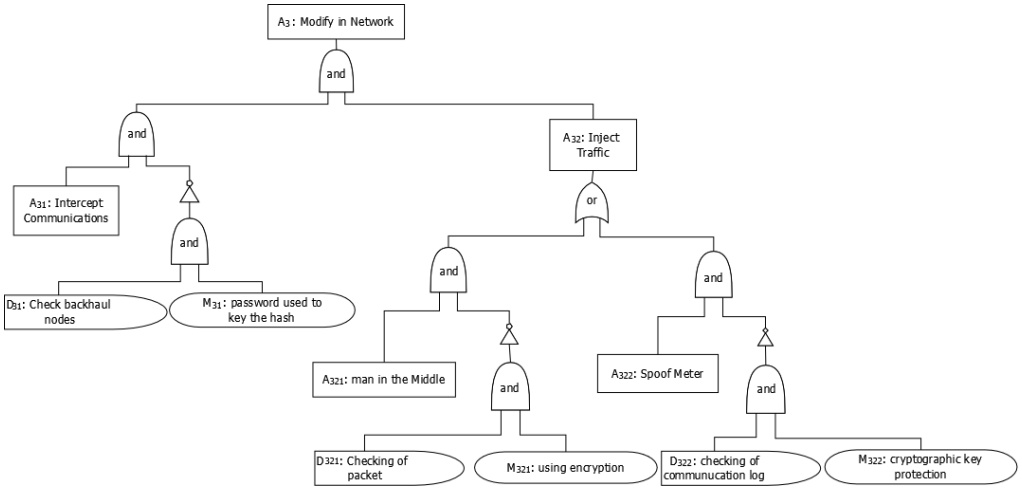
〔그림 6〕과 〔그림 7〕의 경우에는 스마트 미터와 AMI가 포함된다. AMI의 경우 스마트 미터의 전원이 갑자기 꺼지거나 반대의 에너지 흐름이 발생할 때, 센서 데이터를 로깅하여 이에 대한 대응을 하기 때문에 공격이 성공하기 힘들다. 이 공격이 탐지되지 않으려면 공격한 기록을 없애기 위하여 미터의 패스워드를 얻어 로그가 유틸리티로 전송되기 전에 지우는 작업이 수행 되어야 한다. 이에 대한 탐지 방법으로는 패킷 헤더와 시스템 로그, 해당 프로토콜을 체크하는 방법이 있다. 탐지 후 공격에 대한 완화 방법으로는 우선 대부분 물리적인 공격이기 때문에 주변의 물리적인 보안을 강화시키는 것이 첫 번째로 수행되어야 한다. 또한 데이터의 암호화가 이루어져야 할 것이다. 관리자 소프트웨어를 상시 업데이트 하는 것도 완화 방법 중 하나이다.

〔그림 6〕은 A_2의 어택 트리에 탐지와 완화 이벤트를 추가한 ACT이다. 스마트 미터는 스토리지에 많은 양의 데이터를 저장한다. 사용량의 값을 매기는 관세표가 저장되어 있으며, 물리적인 이벤트, 명령어 실행에 관한 로그, 사용량 기록, 스마트 미터 자체의 프로그램 또한 저장되어 있다. 스마트 미터의 행동은 모두 스토리지에 의해 제어되기 때문에 많은 양의 데이터가 저장되어야 한다.

스토리지 공격(A_{21})은 스토리지 내의 감사 로그와, 전체 사용량 기록 데이터가 공격 대상이 된다. 이런



〔그림 6〕 A_2에 대한 ACT



〔그림 7〕 A_3에 대한 ACT

값은 관리자 인터페이스를 통해 접근할 수 있으며, 접근 시 패스워드를 필요로 한다. 그러나 해커가 패스워드를 얻어(A_{131}) 감사로그를 완전히 지우고 사용량을 조작(A_{132})할 때, 사용량을 0으로 초기화 시키는 것은 제한되어 있다. 악의적인 사용자가 미터의 패스워드를 얻었을 때를 고려한 것이다. 사용자의 전기요금은 결제주기의 X%의 사용량 후에 수요 재설정 작업을 실행하여 X%를 감소시킬 수 있다. 스마트 미터의 관리자 인터페이스는 로그인 자격을 요구하기 때문에, 패스워드를 얻어내는 작업이 먼저 필요하다. A_{131} 공격은 스마트 미터의 optical port pin이나 optical lens 에서 reader 장비를 삽입하여 스누핑 공격으로 패스워드를 얻어 스토리지에 접근한다. 또 다른 공격으로 스토리지에 대한 권한을 얻은 후 스토리지 펌웨어에 접근하여 값을 조작하는 방식이 있다. 스토리지 공격에 성공하면 해커가 원하는 작업을 수행하기 위한 모든 제어가 가능하기 때문에 자주 일어나며, 또한 hack kit를 판매하기 위한 목적으로도 수행된다. 위의 공격이 성공하려면 로그와 이벤트 정보를 지우는 작업이 수행되어야 한다. 스토리지 조작 공격에 대한 탐지 방법으로는 패킷 헤더(D_{132})와 스토리지 통신 프로토콜(D_{21}), 데이터 송수신시 상호 인증 과정에서 optical port 프로토콜 동작을 확인(D_{131})하는 방법이 있다. 그에 대한 완화 방법으로는 미터내의 스토리지 주변 구성품에 대한 보안 강화(M_{1311}), 미터 자체의 물리적인 보안 강화(M_{1312})와 스토리지 데이터의 암호화(M_{21}), 패스워드의 암호화(M_{132})가 수행되어야 한다.

〔그림 7〕은 A_3의 어택 트리에 탐지와 완화 이벤트를 추가한 ACT이다. 주로 스마트 미터와 유틸리티가 통신할 때 일어나는 공격이다. 네트워크 공격은 스마트 미터의 위치와 상관없이 스마트 미터와 유틸리티 사이의 어떠한 노드에서도 공격 가능하다. AMI의 콜렉터 노드에서 각 리피터의 전체 사용량을 조정할 수 있기 때문에 보통 공격은 콜렉터 노드에서 일어날 확률이 높다. 스마트 미터와 유틸리티 사이의 트래픽에 침입(A_{31})하기 위해서는 우선 스마트 미터와 유틸리티 사이의 프로토콜을 리버스 엔지니어링을 통해 확인해야 한다. AMI 시스템이 메시지 무결성 및 인증을 위해 암호화를 사용하는 경우, 스마트 미터 스토리지에서 패스워드를 추출하는 것이 필요하다.

스마트 미터와 유틸리티 사이의 인증 혹은 무결성 프로토콜에 결함이 있는 경우, 위조된 데이터와 이벤트 로그를 전송할 수 있는 미터 스푸핑 공격(A_{322})이 가능하다. 만약 인증 메커니즘에 결함이 있지만 스마트 미터와 유틸리티 사이의 암호화 채널이 있다면 Man in the middle(A_{321}) 공격이 가능하다. A_{321}은 ARP 스푸핑 방식을 이용하여 공격자의 IP 주소를 상대방의 IP 주소인 것처럼 위장하여 통신 중간에 중계자 역할을 하는 공격이다. Man in the middle 공격과 스푸핑 공격을 완벽히 막을 수 있는 해결책은 없지만 백홀 노드의 주기적인 탐지(D_{21})와 패킷(D_{321}), 통신 로그(D_{322})를 체크하여 공격을 탐지한 후에 데이터의 암호화(M_{321})와 암호화된 키를(M_{322}) 사용하는 완화 방법이 이루어져야 한다[1].

4.2 확률이 없는 경우의 보안 분석

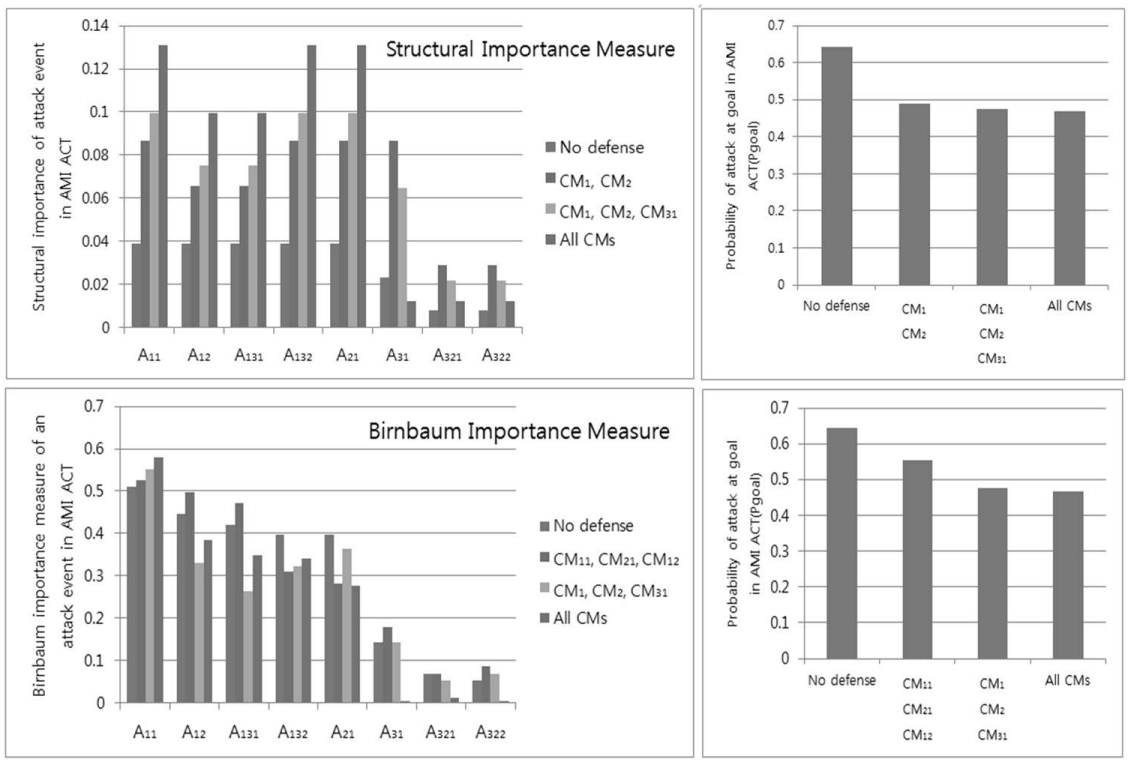
확률이 없는 경우의 보안 분석으로는 Mincuts과 Structure importance measurement가 있다.

4.2.1 Mincuts

ACT는 루트 노드에 도달하기 위한 Mincuts의 집합으로 정의할 수 있다. Mincuts은 ACT의 경우 공격-대책 시나리오를 의미하며 공격 트리의 경우 공격 시나리오를 의미한다. ACT의 루트 노드를 표현할 때 리프 노드들의 집합을 Boolean 함수 $\overline{(\Phi(X))}$로 표현한다. Boolean 함수란 함수 및 변수가 취할 수 있는 값이 참과 거짓의 값만을 가질 수 있는 함수를 의미한다. 변수 X는 ACT의 상태 벡터 x_{A_i}로 공격이 성공했을 때 1, 실패 하였을 때 0으로 정의한다. Boolean 연산자는 and, or, not으로만 이루어져 있으므로 그 결과 또한 참 또는 거짓이다. 다음은 위의 ACT의 Mincuts의 집합이다.

$$
\begin{aligned}
&\{(A_{12},\overline{D_{122}M_{12}}),(A_{12},\overline{D_{121}M_{12}}),(A_{11},\overline{D_{11}M_{11}}),\\
&(A_{131},\overline{D_{131}M_{1311}}),(A_{131},\overline{D_{131}M_{1312}}),\\
&(A_{21},\overline{D_{21}M_{21}}),\\
&(A_{12},\overline{D_{121}M_{12}},A_{131},\overline{D_{131}M_{1311}}),\\
&(A_{12},\overline{D_{121}M_{12}},A_{131},\overline{D_{131}M_{1312}}),\\
&(A_{12},\overline{D_{121}M_{12}},A_{132},\overline{D_{132}M_{132}}),\\
&(A_{12},\overline{D_{122}M_{12}},A_{131},\overline{D_{131}M_{1311}}),\\
&(A_{12},\overline{D_{122}M_{12}},A_{131},\overline{D_{131}M_{1312}}),\\
&(A_{12},\overline{D_{121}M_{122}},A_{132},\overline{D_{132}M_{132}}),\\
&(A_{31},\overline{D_{31}M_{31}}),\\
&(A_{31},\overline{D_{31}M_{31}},A_{321},\overline{D_{321}M_{321}},A_{322},\overline{D_{322}M_{322}})\\
&\}
\end{aligned}
$$

위의 Mincuts을 Boolean 함수로 표현하면 다음과 같다. Mincuts으로 ACT에 대한 모든 공격, 대책 시나리오를 확인할 수 있다. 스마트 그리드 ACT의 최종 목적에 도달하기 위한 시나리오로 14가지의 경우를 확인할 수 있다.



〔그림 8〕 (a) 스마트 그리드 ACT 의 각 공격이벤트의 Structure Importance Measure에 따른 변화 (b) 그에 따른 P_{goal} 의 변화 (c) 각 공격 이벤트의 Birnbaum importance measure에 따른 변화 (d) 그에 따라 대응책을 수행하면서 나타나는 P_{goal} 의 변화

$$\overline{\Phi(X)} = x_{A_{12}}x_{D_{122}}x_{M_{12}} + x_{A_{12}}x_{D_{121}}x_{M_{12}} + x_{A_{11}}x_{D_{11}}x_{M_{11}} + x_{A_{131}}x_{D_{131}}x_{M_{1311}} + x_{A_{131}}x_{D_{131}}x_{M_{1312}} + x_{A_{21}}x_{D_{21}}x_{M_{21}} + x_{A_{132}}x_{D_{132}}x_{A_{132}} + x_{A_{12}}x_{D_{121}}x_{M_{12}}x_{A_{131}}x_{D_{131}}x_{M_{1311}} + x_{A_{12}}x_{D_{121}}x_{M_{12}}x_{A_{131}}x_{D_{131}}x_{M_{1312}} + x_{A_{31}}x_{D_{31}}x_{M_{31}}x_{A_{321}}x_{D_{321}}x_{M_{321}}x_{A_{322}}x_{D_{322}}x_{M_{322}} + x_{A_{12}}x_{D_{122}}x_{M_{12}}x_{A_{131}}x_{D_{131}}x_{M_{1311}} + x_{A_{12}}x_{D_{122}}x_{M_{12}}x_{A_{131}}x_{D_{131}}x_{M_{1312}} + x_{A_{12}}x_{D_{122}}x_{M_{12}}x_{A_{132}}x_{D_{132}}x_{M_{132}} \quad (5)$$

4.2.2 Structural importance measurement

스마트 그리드에서 발생하는 다양한 공격들은 구조가 복잡하고 변수가 많기 때문에 각각의 이벤트(공격, 탐지, 완화)에 대한 확률을 명확하게 규정하기 힘들다. Structural importance measurement는 확률을 이용하지 않고 트리 구조만으로 각각의 이벤트에 중요도를 매긴다. 어떤 이벤트가 ACT에서 가장 중요한지를 판별하는 작업은 보안 분석을 하는데 있어 매우 중요한 부분이다. 만약 공격 이벤트의 확률이 주어지고 탐지, 완화 이벤트들의 확률이 주어지지 않을 때 주어진 ACT에서 Boolean structure function 을 정의할 수 있다. 공격이 성공했을 때는 $\overline{\Phi(X)}=1$, 반면 공격이 실패 했을 때를 $\overline{\Phi(X)}=0$ 으로 간주한다. 이를 이용하여 두 가지의 상태 벡터를 정의하고 식은 다음과 같다.

$$X = (x_{A_1}x_{A_2}\cdots x_{A_{k-1}}x_{A_k}x_{A_{k+1}}\cdots x_{A_N})$$
$$\acute{X} = (x_{A_1}x_{A_2}\cdots x_{A_{k-1}}\acute{x}_{A_k}x_{A_{k+1}}\cdots x_{A_N}) \quad (6)$$

Structural importance measure는 Boolean 구조 함수에 대한 상태 벡터의 정규화 된 수로 정의한다. 두 가지 상태벡터를 이용하여 Structural importance의 수식을 정의하며 식은 다음과 같다.

$$I_{A_k}^{ST} = \frac{\sum_X \overline{\Phi(X)}_{A_k} - \overline{\Phi(\acute{X})}_{A_k}}{2^n} \quad (7)$$

공격 이벤트(A_k)는 상태벡터 X와 연관되어 있으며, Boolean 값 $\overline{\Phi(X)}$이 A_k 이벤트에 따라 1에서 0으로 변화한다. 만약 위의 식에서 $\overline{\Phi(X)}_{A_k} - \overline{\Phi(\acute{X})}_{A_k} = 1$ 이면 A_k는 상태벡터 X와 연관되어 있다고 할 수 있다. 시스템에서 가장 중요한 이벤트가 결정되면, 해당 구성 요소에 적합한 탐지 와 완화 방법을 수행할 수 있다. 다음 수식을 이용하여 AMI ACT의 Structure importance를 〔표 1〕에 표시하였다.

〔표 1〕 AMI ACT의 Structure importance measure

Event	Importance
A_{11}, A_{132}, A_{21}	0.065585
A_{12}, A_{131}	0.049686
M_{12}, D_{131}	0.029811
$D_{11}, M_{11}, D_{132}, M_{132}, D_{21}, M_{21}$	0.021862
$D_{121}, D_{122}, M_{1311}, M_{1312}$	0.009937
A_{31}, A_{321}, A_{322}	0.006085
$D_{31}, M_{31}, D_{321}, M_{321}, D_{322}, M_{322}$	0.002028

〔표 1〕을 보면 주로 공격 이벤트가 주로 중요도가 높음을 확인할 수 있으며, 주로 스마트 미터와 스토리지 공격 이벤트의 중요도가 높게 나타났다. 공격 이벤트에 비해 탐지와 완화 이벤트의 중요도는 낮은 것을 확인 할 수 있다.

4.3 확률이 있는 경우의 보안 분석

확률이 있는 경우의 보안 분석은 주로 해커의 관점, 보안 전문가의 관점 두 가지로 나누어진다. ACT를 이용하여 분석 하게 되면 각각의 공격 혹은 탐지와 완화 방법을 수행 하였을 때 투자비용이나, 공격 혹은 대응책이 성공 했을 때 서로가 입을 수 있는 Risk나 Impact, ROA, ROI 등을 분석 할 수 있다.

〔표 2〕에서 공격 이벤트의 확률과 비용, Impact 파라미터 값을 지정해 주었다. 〔표 3〕은 공격 이벤트의 탐지와 완화 이벤트의 확률과 비용의 파라미터 값을 지정해 준 표이다.

〔표 2〕 AMI ACT의 공격 이벤트 수행 시 확률, 투자비용, Impact

ACT node	Prob. of attack	Attak cost	Attack impact
A_{11}	0.3	70	80
A_{12}	0.2	100	50
A_{131}	0.15	30	200
A_{132}	0.1	50	170
A_{21}	0.1	150	140
A_{31}	0.2	200	150
A_{321}	0.1	100	100
A_{322}	0.3	70	80

〔표 3〕 AMI ACT의 탐지와 완화 이벤트를 수행 시 일어날 확률과 투자비용

ACT node	Prob. of countermeasure success	Security investment cost
D_{11}	0.5	20
M_{11}	0.4	40
D_{121}	0.7	10
D_{122}	0.6	15
M_{12}	0.5	30
D_{131}	0.7	10
M_{1311}	0.4	40
M_{1312}	0.6	30
D_{132}	0.7	10
M_{132}	0.6	20
D_{21}	0.7	10
M_{21}	0.5	20
D_{31}	0.6	15
M_{31}	0.5	30
D_{321}	0.7	10
M_{321}	0.5	20
D_{322}	0.7	10
M_{322}	0.4	40

4.3.1 비용

ACT의 경우 비용은 공격 수행 시 투자비용, 대응책 수행 시 투자비용으로 나누어서 분석한다. 이벤트가 어떠한 게이트로 조합되었는가에 따라서 비용을 계산하는 방법이 다르다. 반복되는 이벤트가 없는 경우 AND 게이트일 경우에는 게이트의 합인 $\sum_{i=1}^{n} C_{A_i}$로 계산하고, OR 게이트의 경우 $\min^{n_{i=1}} C_{A_i}$로 게이트 중에서 가장 낮은 비용을 선택한다. 여기에서 C_{A_i}는 특정 공격(A_i)을 수행할 때 드는 비용을 의미한다. ACT에 반복 이벤트가 있다면 Mincuts을 이용하여 비용을 계산한다. AMI ACT의 Boolean 함수에서 가장 낮은 비용의 공격을 합산하여 구한다. 이는 해커 혹은 보안 관리자가 가장 최선책을 선택한다고 가정했을 때의 경우에 해당된다. 우리는 임의의 해커가 어떠한 능력을 가지고 있는지 알 수 없기 때문에 이를 전제로 한다. 보안에 대한 비용의 경우 탐지와 완화 방법을 수행할 때의 비용을 모두 더하여 계산한다. 전체 공격에 대한 비용은 Mincuts을 이용하여 구할 수 있다.

4.3.2 Birnbaum importance measure

공격에 대비하기 위한 방어 메커니즘에 대해 중요도를 매기는 작업으로 확률을 이용해서 공격과 탐지, 완화이벤트의 중요도를 측정 할 수 있으며 그 수식은 다음과 같다.

$$I^{B_{A_k}} = \frac{\delta P_{goal}}{\delta P_{A_k}} \tag{8}$$

그림 8.(a)는 Structural importance measure의 변화를 나타낸 그래프이다. 어택 트리의 경우 (no defense) Structural Importance Measure를 측정하였을 때 값이 가장 높은 이벤트는 $A_{11}, A_{12}, A_{131}, A_{132}, A_{21}$이다. 이를 참고하여 중요도가 높은 순서대로 탐지와 완화 이벤트를 추가해야 한다. CM_i(countermeasure)는 탐지와 완화 이벤트를 간략화하기 위해 사용한 것으로 A_i 공격에 대한 탐지 및 완화 방법을 뜻한다. 따라서 CM_1과 CM_2를 동시에 수행한다. 〔그림 8〕의 a는 각 공격 이벤트의 Structural importance measure의 변화를 나타낸 것이고 〔그림 8〕의 b는 Structural importance measure이 가장 높은 순서대로 공격 이벤트에 대한 탐지, 완화 이벤트를 추가할 때 마다 변하는 P_{goal}을 나타낸 것이다. 〔그림 8〕의 c는 각 공격 이벤트의 Birnbaum importance measure의 변화를 나타낸 것이고 〔그림 8〕의 d는 Birnbaum importance measure이 가장 높은 순서대로 공격 이벤트에 대한 탐지, 완화 이벤트를 추가할 때 마다 변하는 P_{goal}을 나타낸 그래프이다. 〔그림 8〕의 b와 d의 그래프에서 탐지와 완화 이벤트를 추가할 때 마다 P_{goal}이 낮아지는 것을 확인할 수 있다. 〔그림 8〕의 c그래프를 보면 A_{11}의 중요도가 가장 큰 것을 확인할 수 있다. 그러므로 가장 먼저 CM_1를 수행한다. 앞과 같이 공격(A_i)에 대한 탐지와 완화 이벤트를 수행할 때(CM_i) 중요도가 가장 높은 공격의 이벤트부터 수행해야 한다.

4.3.3 Risk

Risk는 해커에게 가해지는 Risk, 시스템에 가해지는 Risk 두 가지의 관점으로 나누어 해석한다. 해커의 Risk는 수행한 공격의 탐지와 완화 이벤트의 확률과 연관되며 시스템에 대한 Risk는 시스템의 공격 시나리오와 연관된다. 시스템의 Risk는 총 Impact

(I_{goal})와 P_{goal}을 곱한 값으로 정의되며 식은 다음과 같다.

$$Risk_{sys} = P_{goal} \times I_{goal} \quad (9)$$

모든 공격에 대한 탐지, 완화 이벤트를 고려하지 않은 Risk에서 특정 공격의 탐지, 완화 이벤트를 적용했을 때 감소하는 Risk의 변화량을 구하는 식은 다음과 같다.

$$\begin{aligned} \triangle Risk_{CM_i} &= Risk_{without S_{CM}} - Risk_{with CM_i} \\ &= I_{goal} \times (P_{goal_{without CM_i}} - P_{goal_{with CM_i}}) \end{aligned} \quad (10)$$

특정 탐지, 완화 이벤트의 집합을 S_{CM}라고 했을 때, S_{CM}을 적용하여 감소한 Risk를 구하는 식은 다음과 같다.

$$\begin{aligned} \triangle Risk_{S_{CM}} &= Risk_{without S_{CM}} - Risk_{with S_{CM}} \\ &= I_{goal} \times (P_{goal_{without S_{CM}}} - P_{goal_{with S_{CM}}}) \end{aligned} \quad (11)$$

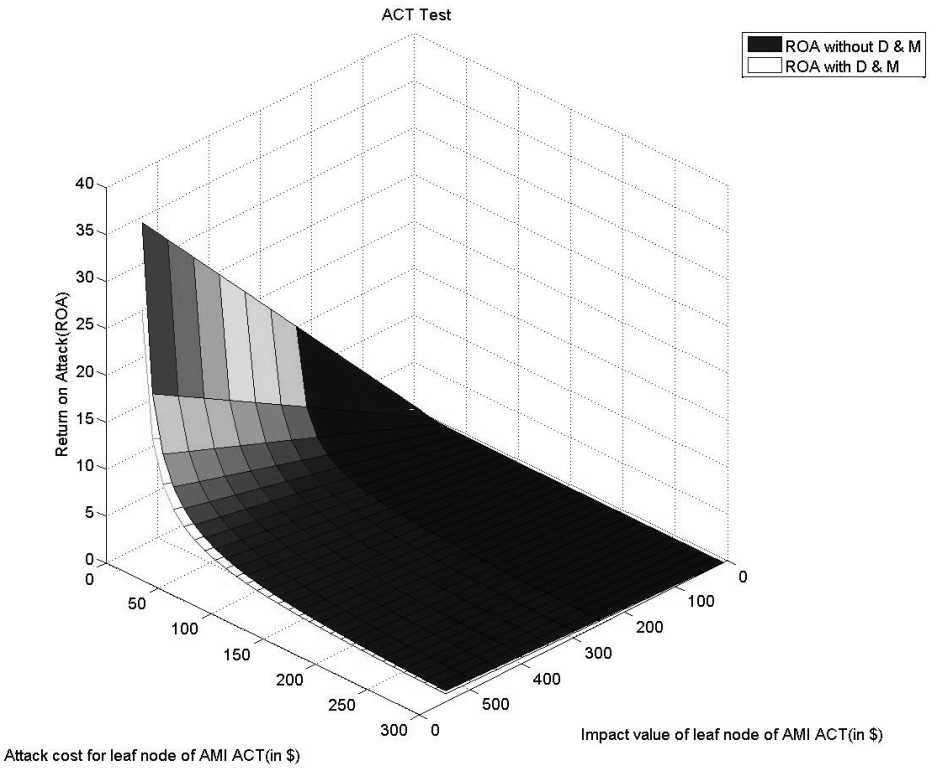
4.3.4 ROA and ROI

ROI와 ROA는 경제 분야에서 사용되는 측정 기준으로 보안 분석에도 이를 사용할 수 있다. ACT의 경우 이를 이용하여 해커와 보안 관리자 사이에 생길 수 있는 수익을 계산하여 비교 할 수 있다.

ROA(Return on attack)는 해커가 공격에 성공할 때 얻는 이익을 의미한다. ROA는 공격에 어떠한 탐지, 완화 방법을 사용했는가에 따라서 값이 달라질 수 있다. ROA는 공격시 Risk에 대해 해커가 부담하는 비용을 나누어 계산하며 그 수식은 다음과 같다.

$$ROA = \frac{Risk_{sys}}{C_{※acker}} = \frac{I_{goal} \times P_{goal}}{C_{※ackerr}} \quad (12)$$

ROI(Return on investment)는 보안 관리자가 공격에 대한 탐지, 완화 방법을 수행할 때 얻는 이익을 의미한다. 해당 시스템의 보안 정책의 효율성을 평가하는 방법으로, 경제 분야나 보안 분야에서도 널리

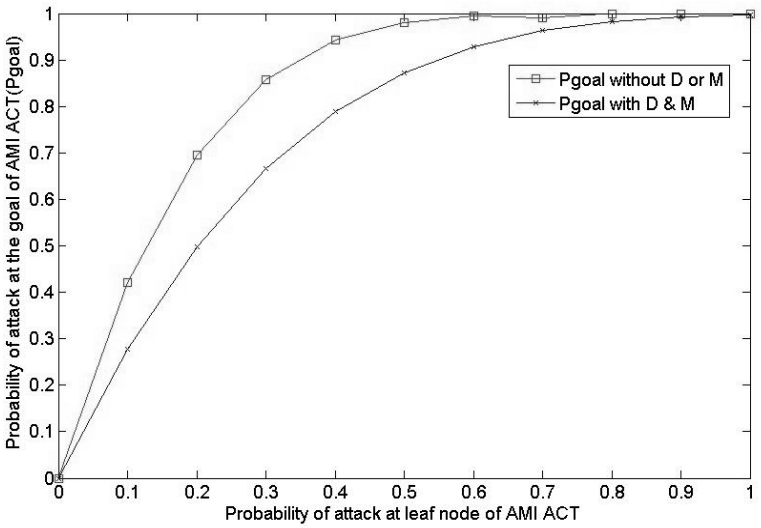


〔그림 9〕 스마트 그리드 ACT의 노드 중 하나인 의 impact 값(x축)과 공격 했을 때 드는 비용(y축) 에 따라서 변화 하는 ROA의 변화

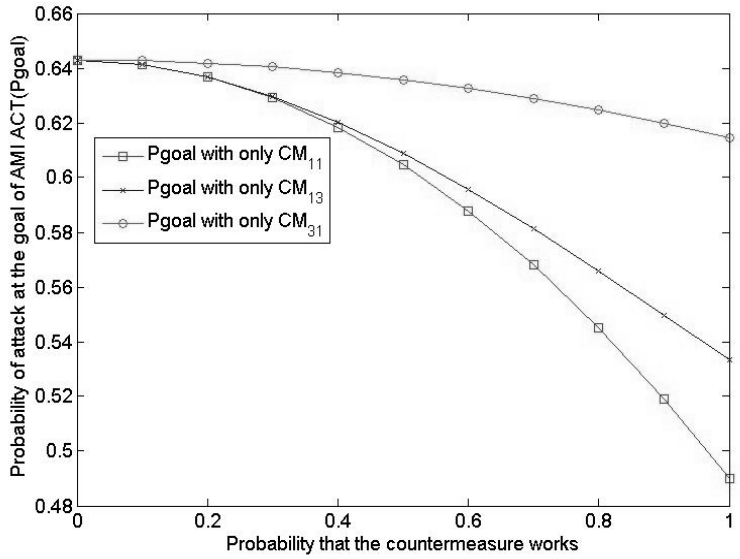
사용되고 있다. ROI에 관한 식은 (13) 과 같다. 식 (13)는 특정 공격(A_i)에 대응하기 위해서 보안 관리자가 공격에 대한 탐지 및 완화 이벤트(CM_i)를 수행하였을 때 생기는 이익을 의미한다. CM_i에 관한 ROI는 CM_i을 수행함으로써 감소하는 확률의 변화량과 CM_i에 투자하는 데에 드는 비용, Impact를 이용하여 계산 하며 그 수식은 다음과 같다.

$$ROI_{CM_i} = \frac{I_{goal} \times \triangle P_{goalCM_i} - c_{CM_i}}{c_{CM_i}} \quad (13)$$

〔그림 9〕는 AMI ACT 중 공격 이벤트 의 impact 값을 〔0, 500〕까지 변화시키고 A_{131}의 비용을 〔0, 300〕$로 변화 시키면서 ROA 값을 관찰 한 그래프이다. $Risk_{SYS}$가 적을수록 ROA값이 적은 것을 확인 할 수 있다. 그래프에서 탐지와 완화 이벤트를 추가하게



〔그림 10〕 스마트 그리드 ACT의 리프 노드 중 공격 이벤트의 확률이 변화할 때 변화하는 P_{goal}의 그래프



〔그림 11〕 스마트 그리드 ACT의 탐지, 완화 이벤트의 확률이 변화할 때 P_{goal}의 변화 그래프

되면 전체적으로 ROA 값이 감소하는 것을 확인할 수 있다. 탐지와 완화 이벤트가 없을 때 ROA의 최대값은 35 이고 탐지와 완화 이벤트를 추가 했을 때는 25로 해커가 얻을 수 있는 이익이 적어지는 것을 확인할 수 있다.

〔그림 10〕은 스마트 그리드 ACT의 리프 노드 중 모든 공격 이벤트의 확률이 각각 〔0, 1〕 범위로 변화할 때 P_{goal}의 변화를 나타낸 것이다. 공격 이벤트의 확률이 증가할수록 전체 공격에 성공할 확률이 높아지는 것을 확인할 수 있다. 탐지와 완화 이벤트를 추가하게 되면 P_{goal}이 감소하는 것을 확인 할 수 있다. 이 그래프에서 AMI ACT의 탐지와 완화 이벤트가 제대로 동작 하고 있다고 판단 할 수 있다.

〔그림 11〕은 스마트 그리드 ACT의 특정 탐지, 완화 이벤트의 확률이 〔0, 1〕의 범위에서 변화 할 때 P_{goal}의 변화를 나타낸 것이다. 전체적으로 특정 탐지, 완화 이벤트의 확률(P_{CM_i})이 증가할수록 공격에 성공할 확률이 낮아지는 것을 확인 할 수 있다. 이 그래프에서는 공격 트리에서 $CM_{11}, CM_{13}, CM_{31}$을 수행하여 $P_{CM_{11}}, P_{CM_{13}}, P_{CM_{31}}$이 〔0, 1〕로 변화 하였을 때 P_{goal}의 변화를 관찰하였다. $P_{CM_{11}}$이 〔0, 1〕로 변화할 때가 가장 변화의 폭이 크고 그 다음은 $P_{CM_{13}}$, 가장 변화의 폭이 적은 것은 $P_{CM_{31}}$이다. 이 결과로 보았을 때 세 가지 탐지, 완화 방법 중에 CM_{11}이 가장 공격에 대한 효과적인 탐지, 완화 방법 이라고 할 수 있다.

V. 결 론

본 논문에서는 AMI의 필수 요소인 스마트 미터에 대한 공격을 중심으로 AMI에 대한 공격과, 공격에 대한 탐지와 완화 방법을 고려한 ACT 모델을 구현하여 보안 분석을 수행하였다. 보안 분석의 경우에서 이에 대한 분석으로는 확률이 있는 경우와 없는 경우로 나누어서 수행하였다. 확률이 있는 경우로는 Risk, Impact, ROA, ROI, Birnbaum Importance 등을 계산할 수 있으며 확률이 없는 경우는 Structure Importance와 Mincuts을 계산할 수 있다. 이러한 보안 분석을 통해 AMI의 공격에 대한 탐지와 완화 방법의 효율성을 평가하였다. 앞으로 세부적인 공격, 탐지, 완화 방법을 수집하여 세밀한 보안 분석에 대해 추가 연구가 필요하며, 최종적으로 논문에 제시된 ACT를 침입 탐지 시스템(IDS)와 관련성을 지어서 실제 스마트 그리드 보안에 적합하도록 적용하는 연구를 수행할 것이다.

참고문헌

〔1〕 Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel, "Energy Theft in the Advanced Metering Infrastructure," In Proc. of 4th international conference on Critical information infrastructures security (CRITIS 2009), pp.176-187, 30 Sep 2009.

〔2〕 엄정호, "공격 트리를 이용한 위협평가 방법에 관한 연구," 보안공학연구회, 9(1), pp. 45-52 , 2012년 2월.

〔3〕 Arpan Roy, Dong Seong Kim, and Kishor S. Trivedi, "Attack Countermeasure Trees (ACT): towards unifying the constructs of attack and defense trees," Security and Communication Networks, pp. 929-943, 2 FEB 2011.

〔4〕 Robin Berthier, William H. Sanders, "Specification-based Intrusion Detection for Advanced Metering Infrastructures," In Proc. of First IEEE International Conference on Smart Grid Communications (Smart Grid Comm 2010), pp. 350-355, Oct 2010.

〔5〕 에너지포럼, "스마트 그리드의 단점," http://cafe.naver.com/energystory.cafe?iframe_url=/ArticleRead.nhn%3Fclubid=23592913%26page=4%26menuid=48%26boardtype=L%26articleid=736%26referrerAllArticles=false, 2011년 12월.

〔6〕 Chee-Wooi Ten, Chen-Ching Liu, and Manimaran Govindarasu, "Vulnerability Assessment of Cyber security for SCADA Systems Using Attack Trees," In Proc. of IEEE Power Engineering Society General Meeting, pp. 24-28, JUN 2007.

〔7〕 Mohammad Ashiqur Rahman, EhabAl-Shaer, "AMIAnalyzer: Security Analysis of AMI Configurations," In Proc. 4th Symposium on Configuration Analytics and Automation (SAFECONFIG 2011),

pp. 1-2, Oct 2011.
〔8〕 Abhishek Rakshit and Xinming Ou, "A Host-based security Assessment Architecture for Industrial Control Systems," In Proc. of 2nd International Symposium on Resilient Control Systems 2009 (ISRCS 2009), pp. 13-18, Aug 2009.
〔9〕 Patrick McDaniel & Stephen McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security and Privacy, Vol.7, No.3, pp. 75-77, 2009.
〔10〕 Todd Baumeister, "Literature Review on Smart Grid Cyber Security," Technical Report, University of Hawaii, http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf, Dec 2010.
〔11〕 Xinming Ou, Sudhakar Govind avajhala and Andrew W. Appel, "MulVAL: A Logic-based Network Security Analyzer," In Proc. of the 14th conference on USENIX Security Symposium(SSYM 2005), pp. 8-8, 2005.

〈저자소개〉

위 미 선 (Miseon Wi) 학생회원
2012년 2월: 한국항공대학교 전자 및 항공전자공학과 졸업
2012년 3월~현재: 한국항공대학교 컴퓨터공학과 석사과정
〈관심분야〉 스마트 그리드, 네트워크 보안

김 동 성 (Dong Seong Kim) 정회원
2003년: 한국항공대학교 컴퓨터공학과 석사
2008년: 한국항공대학교 컴퓨터공학과 박사
2008년~2011년: Duke University 박사후 연구원
2011년~현재: 캔터베리대학교 컴퓨터과학 및 소프트웨어 공학과 조교수
〈관심분야〉 고신뢰 시스템, 네트워크 보안

박 종 서 (Jong Sou Park) 종신회원
1986년: 노스캐롤라이나대학 전기 컴퓨터공학과 석사
1994년: 펜실베이나주립대학교 컴퓨터공학과 박사
1996년~현재: 한국항공대학교 컴퓨터공학과 교수
〈관심분야〉 네트워크 보안, 임베디드 시스템