정 보 보 호 학 회 지
제24권 제5호, 2014. 10

에너지 사용 맥락을 통한 AMI 네트워크에서의 데이터 이상 감지 방법론 제안

강 동 주*, 김 발 호**, 김 휘 강***

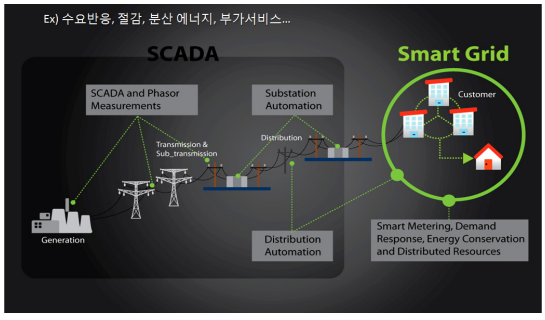
요 약

현재 우리나라는 2013년 제주 스마트그리드 실증단지사업을 완료한 이후, 현재 AMI 및 ESS 보급사업을 진행 중이고 더불어 주요 7~8개 도시에 대한 스마트그리드 시티 사업도 준비 중에 있다. 스마트그리드 인프라의 본격적인 확산과 더불어 가장 우려되는 사안 중의 하나가 사이버 보안 이슈이며, 이는 기존의 주요 전력망 보안정책이 폐쇄망 운영을 골자로 하고 있다는 점에서 볼 때 상충되는 측면이 있다. 스마트그리드의 중심이 기존의 대형 전력망 중심에서 스마트 홈 기반 중심으로 옮겨가면서, 전력망은 외부 네트워크와의 연결성이 강화되고 있으며 통신 분야에서 진행되어 오던 사물통신(Internet of Things: IoT) 개념과 결합하면서 그 개방성의 진행이 가속화되고 있다. 따라서 기존의 폐쇄망 정책만으로는 보안성을 확보하는데 명확한 한계가 존재하며 시대적 조류에도 부합하지 않기 때문에, 새로운 패러다임이 필요한 때라고 판단된다. 그 대안 중의 하나로 개방 네트워크로 인해 증가하는 연결성을 보안 위협의 루트가 아닌 보안성을 강화하기 위한 환경으로 활용하는 것이다. 촘촘히 연결된 네트워크를 통해 각 개체가 서로를 상호 모니터링 함으로써 전체 시스템이 오염되는 것을 막을 수 있다. IoT의 도입을 통해 기기 간에는 사회적 연결성이 강화될 것이며, 이러한 연결성과 그 안에 숨겨진 맥락을 통해 이상 여부를 사전에 감지해낼 수 있다. 본 논문에서는 그러한 사회적 관계성에 근거하여 AMI 네트워크에서의 이상 징후를 감지하기 위한 기본적 방법론을 제안하고자 한다.

Ⅰ. 서 론

스마트그리드의 본래 목적 중의 하나는 최종 소비자를 전력시스템 운영의 능동적 주체로 끌어들이는 것이었다. 그러나 국내외를 막론하고 최근 5~6년의 스마트그리드 사업은 기존 대규모 시스템의 고도화와 새로운 인프라의 확충에 초점이 맞추어져 있었다. 이러한 정책은 새로운 산업과 시장을 창출하는데 명확한 한계를 보였고, 이로 인해 새로운 접근법에 대한 필요성이 꾸준히 제기되어 왔으며, 그 중심에 소비자 중심적인 접근법이 포함되어 있다. 스마트그리드 초기에는 주로 신재생에너지, 계통운영자동화, 전기자동차 인프라 등에 초점이 맞추어져 왔지만, 최근에는 소비자 참여(consumer engagement) 이슈로 초점이 수렴되고 있다. 무엇보다 지속적인 투자와 발전이 있기 위해서는, 민간분야의 지속적 투자가 발생할 수 있는 유인이 필요하고 이를 위해서는 최종 소비자를 참여시키는 방안이 궁극적인 해결책이라 볼 수 있다.

그러나, 소비자의 참여를 적극적으로 이끌어내는 과정에서 주요한 장벽 중의 하나는 사이버 보안과 프라이버시 이슈이다. 스마트 미터를 기반으로 개인의 에너지



〔그림 1〕 스마트그리드와 소비자 참여

* 한국전기연구원 선임연구원
** 홍익대학교 전자전기공학부 교수
*** 고려대학교 정보보호대학원 조교수

사용량이 노출되면, 이를 기반으로 생활 패턴과 프라이버시를 유추할 수 있기 때문이다. 따라서 소비자의 적극적 참여를 이끌어내기 위해서는 스마트 폰의 경우와 마찬가지로 매력적인 부가서비스를 만들어냄과 동시에 사이버 보안에 대한 우려를 완화하여야 한다.

Ⅱ. AMI 보급 추이

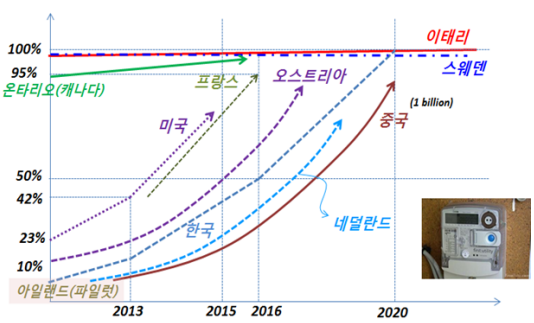
현재 우리나라는 스마트 미터 보급 사업을 진행 중이고, 2020년까지 100%를 보급한다는 계획을 수립하고 있다. 스마트 미터에 통신 인프라를 결합한 것이 AMI (Advance Metering Infrastructure)이며, 우리나라는 모든 가정용 수용가를 포함하는 최종 소비자 단에 100% AMI를 보급하는 계획을 수립하고 진행 중이다. 더불어, 다른 주요 국가들의 경우도 2020년까지 100% 보급을 계획하고 있으며, 이태리와 스웨덴의 경우는 이미 100% 보급을 달성하였다. 이러한 상황에서, 전력시스템은 스마트 미터를 통해 개방망과의 연계가 강화될 수 밖에 없으며, 이러한 맥락에서 가장 중요한 문제 중의 하나가 보안이 될 수 밖에 없다. 실제로 네덜란드의 경우, 스마트 미터 강제 보급 정책을 시행했다 취소한 적이 있는데, 스마트 미터로 인한 사생활 침해와 사이버 보안에 대한 우려로 소비자들의 저항이 강화되었기 때문이다.

보안성 확보가 중요한 이슈이긴 하지만, AMI를 보급하는 정부나 사업자 입장에서는 그에 따라 비용 역시 상승하기 때문에 사업성을 떨어뜨리고 그로 인해 보급 유인을 떨어뜨릴 수 있다. 기존의 보안정책이나 솔루션을 적용할 경우, 연결성이 증가하면 그만큼 많은 수의 강화된 보안 솔루션이 필요하기 때문이다. 따라서 변화된 환경에서는 새로운 접근 방법이 필요하며 본 논문에서는 그러한 방법의 일환으로, 기기들의 증가된 연결성을 보안을 강화하기 위한 수단으로 활용하고자 한다. 스마트 홈과 더불어 IoT의 유입이 강화되면서, 스마트 가전기기의 도입도 가속화되고 있으며, 이는 기기 간의 연결성이 더욱 사회적 관계성을 띄는 계기가 될 것이다. 이러한 사회적 관계망 속에서 기기는 서로를 감시할 수 있으며, 전체적인 맥락을 이해하는 도구로 활용될 수 있다. 이는 다시 빅 데이터(big data) 기반의 접근 방법과도 조우하게 된다.

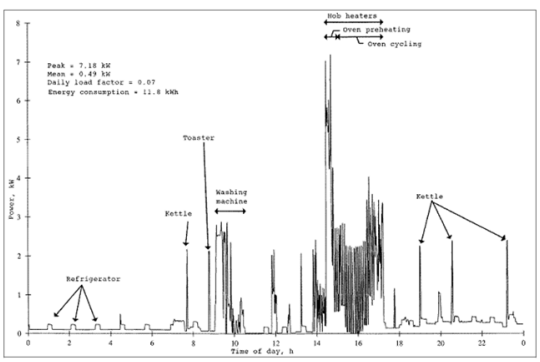
Ⅲ. 에너지 사용 맥락(context)

에너지 네트워크에서는 특정 시간대의 수요와 공급 균형이 이루어져야 하고, KCL, KVL 법칙에 의해 특정 노드에서의 에너지 입력과 출력이 동일해야 하기 때문이다. 이는 일종의 대칭성으로 이해할 수 있고, 이러한 속성을 이용하면 개별 기기 간의 관계성이 보다 명료해지고 그에 기반하여 현재 상태의 이상 여부를 검증할 수 있다. 이러한 접근방법은 이미 다양하게 연구되고 있으며, Brandon J. Murill 등의 연구도 그 중의 하나이다. 개별 가전기기는 고유의 전력사용패턴(사용시간 및 사용전력량)이 존재하며, 이는 개별 기기의 측정 데이터가 참인지 거짓인지를 검증하는데 활용될 수 있다. 예를 들어, 밤에 주로 커져있어야 되는 조명기기가 낮에 계속 전기를 사용하고 있거나, on-off 모드가 자주 발생한다면 그것은 뭔가 이상이 있다는 신호로 해석될 수 있다.

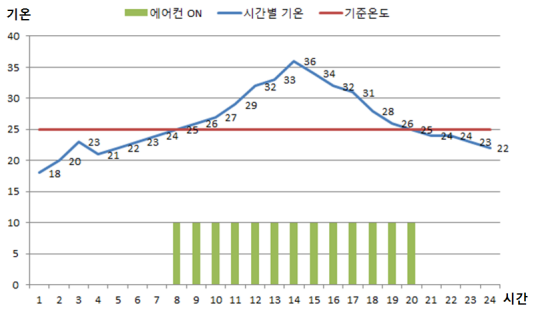
에어컨을 예로 들어 본다면, 에어컨은 여름 시즌, 늦은 아침부터 오후를 거쳐, 초저녁에 주로 많이 가동되는 특성이 있다. 그리고 이러한 패턴이 항상 일정하게 발생



〔그림 2〕 주요 국가들의 AMI 보급 계획



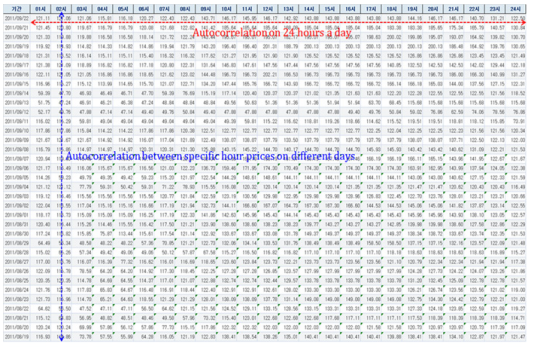
〔그림 3〕 전력기기의 고유 전력사용패턴 사례



〔그림 4〕 에너지 사용 패턴 사례

했는데, 특정일에 완전히 다른 패턴을 보인다면, 데이터의 이상이든 실제 에어컨이 선택으로 커졌는지에 대한 검증이 필요하고 이러한 과정에서 이상 여부를 판단할 수 있다.

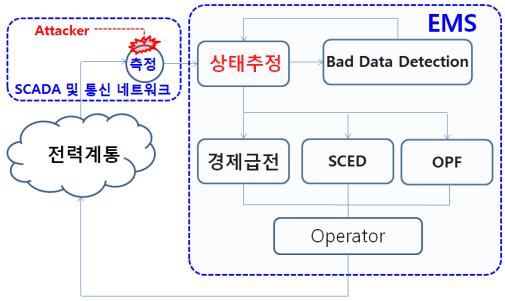
에너지 사용패턴은 다음 그림과 같이 매트릭스 형태로 정량화될 수 있다. 전력 데이터의 경우는 요일별 특성과, 시간별 특성이 공존하므로, 다음과 같이 일(date)과 시간(hour)으로 구성된 행렬로 표현할 수 있다. 이러한 행렬을 통해 에너지 사용량에 대한 맥락을 정량화할 수 있다.



〔그림 5〕 에너지 사용 맥락의 정량적 표현

Ⅳ. 상태추정 및 상관관계 도출 개념

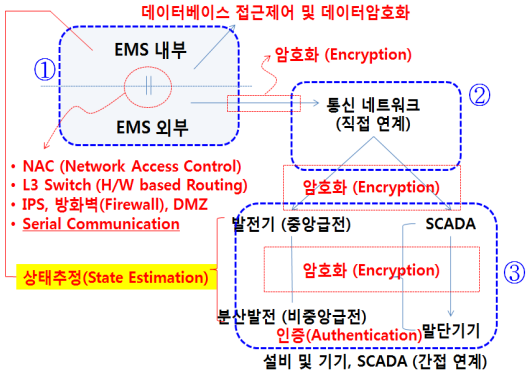
데이터의 무결성을 검증하기 위한 '상태추정(state estimation)' 이라는 방법으로 이미 대규모 전력계통운전에서도 이용되고 있다. [그림 6]은 상태추정 기능의 개념을 보인 것으로 계측 데이터를 실제 계통운영에 활용하기 전 상태추정 기능을 통해 데이터를 검증하는 과정을 보인 것이다.



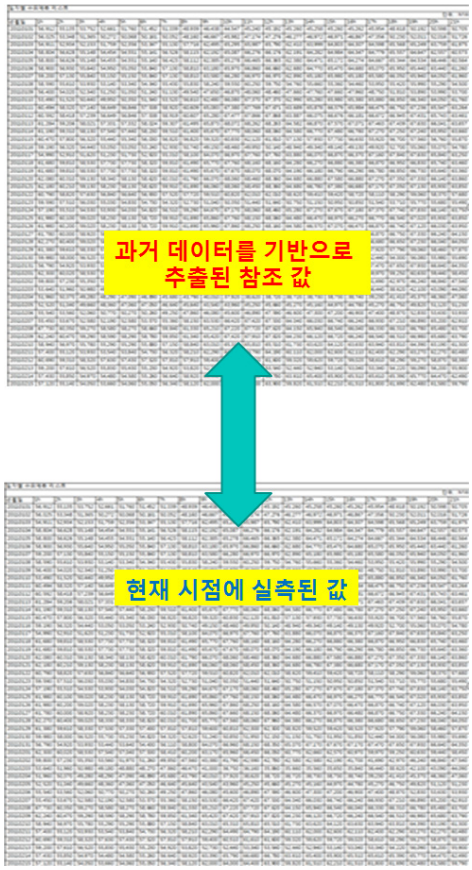
〔그림 6〕 전력계통의 상태추정(SE) 기능

상태추정은 사이버 보안을 위한 솔루션은 아니지만, 중앙제어센터가 RTU로부터 받는 데이터의 무결성을 검증하기 위한 수단으로, 측정 데이터의 리던던시(redundancy)를 활용하여 방정식을 수립하고, 측정값과 방정식의 해를 상호 검증하는 형태로 이루어진다. 이는 현재 계측오류를 검증하는데 사용되고 있지만, 다음 그림과 같이 기존의 보안 관련 정책 및 솔루션과 혼용되어 사용될 수 있다.

상태추정 기능을 AMI 기반 네트워크에도 적용한다면, 기기별로 [그림 5]와 같은 고유 정보를 추출할 수 있다. 이러한 데이터가 누적되면, 일정한 패턴으로 수렴할 것이고 에너지 기기별, 혹은 사용자별 고유 정보로 활용할 수 있다. 이러한 개념은 정보보호 분야에서의 사이버 게놈(cyber genome) 개념과도 결부하여 적용될 수 있다. 기기별로 추출된 게놈 정보를 기준으로 실측 데이터와의 비교를 통해 상관관계를 도출하고, 실측치가 상관관계 대비 일정수준 이상 오차를 보인다면 데이터 무결성이 훼손된 것으로 간주할 수 있다. [그림 8]은 그러한 개념을 보인 것으로, 행렬 형태로 표현할 경우



〔그림 7〕 사이버 보안 측면의 상태추정 활용



〔그림 8〕 행렬연산 기반의 상관관계 도출

MATLAB 등의 툴을 활용하여 선형대수 형태로 쉽게 연산할 수 있다는 장점이 있다.

과거 데이터를 통해 추출된 값은 일종의 미래 예측값으로도 인식할 수 있다. 과거 데이터에 기반하여 의례적으로 특정 미래시점에 특정 패턴을 보여야 하는데, 실측 데이터와의 오차가 허용 오차 범위 이상으로 커질 경우 데이터에 대한 검증이 사전적으로 이루어질 수 있다. 예측에 대한 값은 자기상관관계에 의한 측면과, 타 변수와의 상관관계에 의한 상관지수를 구하는 것으로 나누어질 수 있고 다음 식과 같은 형태로 모델링 될 수 있다.

기준시점 대비 증가예상변량을 더함으로써 특정 미래 시점의 값을 추정하는 형태이다. 이렇게 예측된 값이 일종의 상태 추정값으로 볼 수 있다. 아래의 식은 전력사용량을 의미하는 것으로, 전력사용량의 경우, 시간별, 일별, 주간, 월간, 계절 단위의 주기성을 보이므로, 각 주기별 변량을 독립적으로 적용한 사례라고 볼 수 있다.

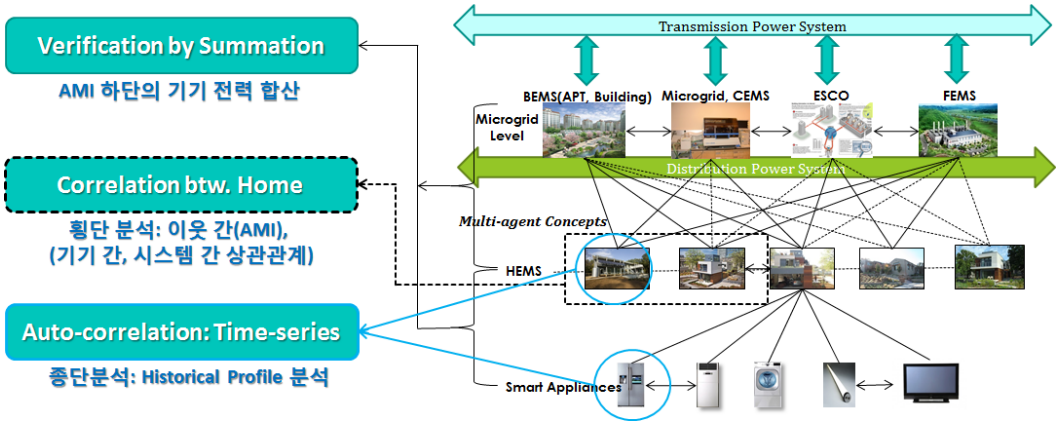
$$
\begin{aligned}
P_{future} &= P_{current} + \Delta P_{time\ domain} + \Delta P_{structural\ domain} \\
&= P_{current} + \Delta P_{hourly} + \Delta P_{daily} + \Delta P_{weekly} \\
&\quad + \Delta P_{monthly} + \Delta P_{seasonal} + \Delta P(L_{hourly}) + \Delta P(L_{daily}) \\
&\quad + \Delta P(L_{weekly}) + \Delta P(L_{monthly}) + \Delta P(L_{seasonal}) \\
&\quad + \Delta P(FC_{yearly}) + \Delta P(C_{yearly}) + \cdots \\
&\quad + \epsilon_h + \epsilon_d + \epsilon_w + \epsilon_m + \epsilon_s + \epsilon_{L_h} + \epsilon_{L_d} + \epsilon_{L_w} + \epsilon_{L_m} \\
&\quad + \epsilon_{FC_y} + \epsilon_{C_y} + \cdots
\end{aligned}
$$

현재 시점으로부터 미래 시점이 멀리 있으며, 즉 상태추정 이격시간(Δt)가 커지면 미래예측 속성에 가까울 것이고, 이격시간이 줄어들수록($\Delta t \to 0$) 전력계통 운영에 사용되는 실시간 상태추정의 개념과 유사해진다. 또한 이격시간이 줄어들수록 상태추정의 정확성은 증가하게 될 것이다.

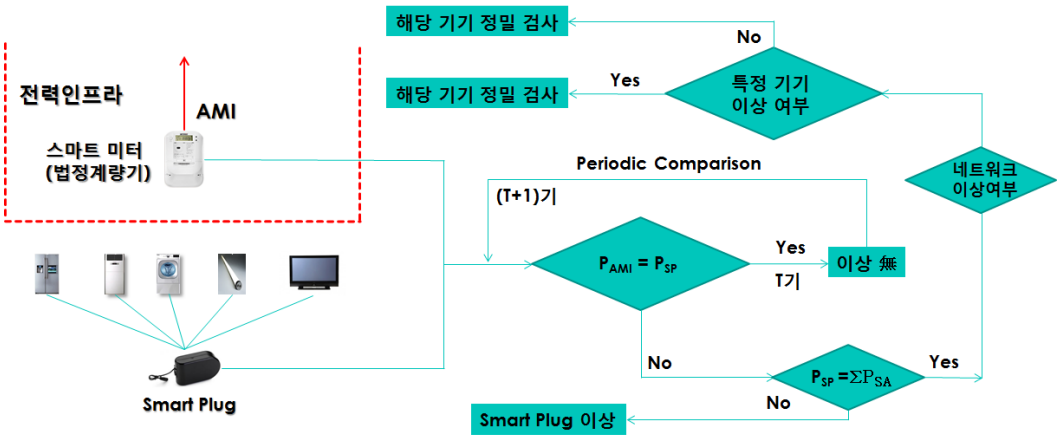
Ⅴ. 컨텍스트 해석 알고리즘

본 절에서는 상기의 추정 내지 예측 알고리즘을 기반으로 AMI 기반 네트워크에 대한 데이터를 검증할 수 있는 알고리즘의 기본적 구조에 대해 소개한다. AMI가 보급되면, 최종 말단의 스마트 가전기기부터, 스마트 홈, 커뮤니티의 형태로 계층적인 구조를 형성하게 될 것이다[그림 9]. 하위 계층의 에너지 사용합은 상위 계층의 에너지 사용량과 일치하여야 한다. 예를 들면, 특정 스마트 홈에서의 가전기기들이 사용하는 에너지 사용합은 홈 전체의 에너지 사용량과 동일하여야 하고, 그렇지 않은 경우는 에너지가 다른 곳으로 새고 있거나, 데이터에 이상이 생긴 것으로 간주할 수 있다. 또한 개별 기기와 홈, 커뮤니티는 상기 절에서의 자기 상관관계에 기반하여 데이터를 검증할 수 있으며, 또한 타 기기 및 타 가구와의 비교를 통해 데이터의 무결성 여부를 중복 검증할 수 있다. 즉, AMI 네트워크로 인해 증가하는 연결성을 통해 상호 중복적으로 검증함으로써 데이터의 무결성을 개선한다는 개념이다. [그림 10]은 이러한 개념을 도식화 한 것이다. 데이터 검증의 방법은 크게 3가지로 자기 상관관계(autocorrelat-ion), 기기 및 홈 간 상관관계(correlation), 개별 측정치와 에너지 합산량을 비교하는 방식이 있다.

관계성에 기반하여 데이터 무결성을 검증한다면, 연결성이 증가함으로써, 잠재적 위협의 유입구도 많아지지만 그만큼 상호비교의 기회가 증가하므로 보안성도 동시에 증가될 수 있다.

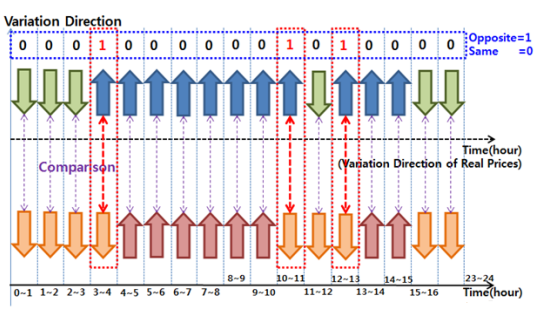


〔그림 9〕 AMI 기반 연결성 및 사회적 네트워크에 근거한 데이터 검증 방안



〔그림 10〕 네트워크 관계성에 기반한 데이터 검증 절차

최종 소비자 단에서의 스마트그리드 서비스는 소셜 네트워크 서비스와 접목되고 있으며, 이러한 접근방법은 소셜 네트워크의 고유의 네트워크 분석 방법론과 결합될 수 있다. IoT 개념과의 접목을 통해 상호 관계성의 증가와, 개별 기기의 자율성 증가는 사회적 네트워크 속성을 증가시키고 있으며, 이러한 환경에서는 기존의 트래픽 패턴을 단순 감시하는 방법만으로는 분명한 한계가 존재한다. 특히, 사이버 공격의 패턴도 점차 APT(Advanced Persistent Threats) 기반으로 옮겨가고 있기 때문에, 개별 기기나 접속점이 아닌 전체의 맥락(context)을 분석할 수 있는 접근법이 필요하다. 맥락을 전산적으로 처리하기 위해서는 이를 정량화할 필요가 있으며, 전체의 관계성을 정방형 형태의 매트릭스 형태로 표현할 수 있다. 다음 그림은 이러한 관계성을 정량화하는 사례를 보인 것으로, 예를 들어 2개의 기기나 변수 간에 행동 패턴을 비교할 때, 자유도가 2라면 이동 방향에 따라, 0과 1의 2가지 숫자로 표현할 수 있고, 그 관계를 Boolean 대수 형태로 표현하고 연산할 수 있다. 예를 들면, 방향성이 같을 경우 0, 방향성이 다를 경우 1을 부여하는 방식이다. 물론 그 반대도 가능하다.



〔그림 11〕 관계성 분석 사례

Ⅵ. 결 론

본 논문에서는 네트워크의 관계성에 기반하여 데이터의 무결성을 검증하는 개념적 방법론을 소개하였다. 해당 개념은 '상태추정'이라는 용어로 대규모 계통에서 유사한 방법론이 활용 중인데, 이를 AMI 기반의 개방형 네트워크에 적용하기 위한 기본적 구성에 대한 것이다. 특히, 스마트그리드가 스마트 홈 중심으로 재편되고, 그러한 과정에 IoT 개념과 만나게 되면서, 소셜 네트워크 서비스와도 융합되는 현상을 보이고 있다. 이는 개방성과 더불어 스마트 가전기기들의 다양한 연결성이 확대될 것이라는 전조로 볼 수 있다. 이러한 흐름은 거스를 수 없는 것이기 때문에, 기존의 보안 솔루션이 주로 취하던 연결성 제한과 고립화 방법보다는 오히려 그러한 연결성을 보안 솔루션에 적극적으로 활용할 필요가 있다. 특히, 최근에 증가하고 있는 APT 기반의 공격 방법은 어느 특정 접속점이나 기기에 대한 분석을 통해서는 감지가 쉽지 않기 때문에, 시스템 전체의 맥락을 분석할 수 있는 기술이 필요하고 이를 위해서는 사회적 네트워크의 관계성에 대한 분석과 이를 정량화하는 방법론이 필요해질 것이다. 본 연구는 그러한 접근방법의 기본적 개념을 설계하는 단계의 연구로 인식할 수 있으며, 향후 소셜 네트워크 및 빅데이터 분석법들과 결합하여 보다 정제된 방법론으로 개발해갈 계획이다.

참 고 문 헌

[1] 강동주, 김휘강, "스마트그리드에서의 CPS (cyber-physical system) 시뮬레이션 구현을 위한 제반 연구이슈 및 방법론 검토", *한국정보보호학회지*, 22(5), pp. 62-72, 2012.

[2] D.J. Kang, J.J. Lee, S.J. Kim, and J.H. Park, "Analysis on cyber threats to SCADA systems", *Transmission & Distribution Conference & Exposition: Asia and Pacific*, 2009.

[3] S. Massoud Amin, "Cyber and Critical Infrastructure Security: Toward Smarter and More Secure Power and Energy Infrastructures", *Canada-U.S. Workshop on Smart Grid Technologies*, 2010.

[4] Matias Negrete-Pincetic, Felipe Yoshida and George Gross, "Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment", Power -Tech, *2009 IEEE Bucharest,* 2009.

[5] David Kuipers and Mark Fabro, *Control Systems Cyber Security: Defense in Depth Strategies*, Idaho National Lab, 2006.

[6] Deepa Kundar, Xianyong Feng, Shan Liu, Takis Zourntos, Karen L. Butler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid", *1st IEEE International Conference on Smart Grid Communications*, 2010.

[7] D.J. Kang, D.K. Kang, and B.H. Kim, "Visualization Issues of Mass Data for Efficient HMI Design on Control System in Electric Power Industry - Visualization in Computerized Operation and Simulation Tools", *International Association of Societies of Design Research Conference Seoul*, 2009.

[8] D.J. Kang, *Development of Price Forecast -ing Program based on Modular Design,* Hongik University, 2012.

[9] Jianli Pan, *A Survey of Network Simulation Tools: Current Status and Future Developments*, http://www.cse.wustl.edu/~jain/cse567-08/ftp/simtools.pdf.

〈저 자 소 개〉

강 동 주 (Dong Joo Kang)
비회원

1999년 2월 : 홍익대학교 전자전기제어공학과 학사
2001년 8월 : 홍익대학교 전기정보제어공학과 석사
2012년 2월 : 홍익대학교 전기정보제어공학과 박사
2001년 9월~현재 : 한국전기연구원 선임연구원
2012년 9월~현재 : 고려대학교 정보보호대학원 박사과정
관심분야 : 스마트그리드 정보보호, 전력시장 시뮬레이션, 소셜 네트워크

김 발 호 (Balho H. Kim)
비회원

1984년 2월 : 서울대학교 전기공학과 학사
1992년 8월 : University of Texas at Austin 전기공학과 석사 (공업경제 전공)
1996년 : University of Texas at Austin 전기공학과 박사 (전력경제 전공)
1984~1990년 : 한국전력공사 기술연구본부 전력경제연구실 근무
1999년~현재 : 홍익대학교 전자전기공학부 교수
관심분야 : OPF, 최적화, 송전계통계획, 전력경제, 전원계획, 전력시장, 전력계통 신뢰도

김 휘 강 (Huy Kang Kim)
종신회원

1998년 2월 : KAIST 산업경영학과 학사
2000년 2월 : KAIST 산업공학과 석사
2009년 2월 : KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월 : 엔시소프트 정보보안실장, Technical Director
2010년 3월~현재 : 고려대학교 정보보호대학원 조교수
관심분야 : 온라인게임 보안, 네트워크 보안, 네트워크 포렌식