情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

스마트그리드 환경에서 공증기관을 이용한 디지털 증거 수집 기법*

조 영 준,† 최 재 덕, 김 신 규,‡ 서 정 택
ETRI 부설연구소

Digital Evidence Acquisition Scheme using the Trusted Third Party in Smart Grid Infrastructure*

Youngjun Cho,† Jaeduck Choi, Sinkyu Kim,‡ Jungtaek Seo
The Attached Institute of ETRI

요 약

세계 주요 국가들은 전력수요 증가, 환경오염 등의 문제를 해결하기 위해 자국의 전력망을 스마트그리드로 변경하기 위한 노력을 기울이고 있다. 국내에서도 스마트그리드 도입을 위한 다방면의 연구가 진행되고 있다. 그러나 양방향 통신을 적용한 스마트그리드에는 기존 IT에 존재하는 사이버 위협이 적용되어, 국가적 차원에서 사회적 경제적 혼란을 야기할 수 있는 사이버 테러의 위험도 증가하고 있다. 이러한 사이버 공격에 대응하기 위해 사이버 침해사고 발생 시 이에 대한 조사와 이를 분석하고 재발 방지를 위한 노력이 필수적이다. 침해사고에 대응하기 위한 디지털 증거 수집에 대한 연구는 그간 꾸준히 진행되고 있으나 스마트그리드 환경에 적합한 디지털 증거 수집 방안에 대한 연구는 아직까지 미흡하다. 본 논문에서는 스마트그리드 환경에서 필요한 증거 수집 요구사항과 기존까지 연구된 디지털 증거 수집 방안을 분석하여 스마트그리드 환경에 적합한 디지털 증거 수집 기법에 대해 제안한다.

ABSTRACT

Considerable number of major countries have put great efforts to leverage the efficiency of power consumption using Smart Grid in order to resolve the critical issues with drastical growing demands regarding electricity, the crisis of environmental pollution and so on. There has been increasing number of researches to construct Smart Grid in Korea as well. The threats of cyber terror attacks which might cause national crisises in terms of economy and society have been climbing up because of the fact that Smart Grid employs bi-directional communications embedding the cyber threats from existing/legacy communication networks. Consequently, it is required to build concrete response processes including investigation and analysis on cyber breaches into Smart Grid. However, the digital evidence acquisition techniques do not suffice to be deployed in Smart Grid systems despite of the fact that the techniques, against cyber breaches into well-known networks, have been studied in plenty of time. This work proposes a novel digital evidence acquisition scheme appropriate to Smart Grid systems through intensive investigation of the evidence acquisition requirements in Smart Grid and the historical evidence acquisition methods.

Keywords: Smart Grid, Digital Evidence, Evidence Acquisition

접수일(2013년 2월 20일), 수정일(2013년 4월 8일), 게재확정일(2013년 4월 9일)
* 본 연구는 2012년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다.(No. 2012101050004A)
† 주저자, yjcho@ensec.re.kr
‡ 교신저자, skkim@ensec.re.kr

I. 서 론

스마트그리드 환경은 기존 일방향의 폐쇄적 전력망 운영에서 정보 통신 기술을 적용하여 양방향 통신을 통해 에너지 소비를 보다 효율적으로 관리할 수 있도록 해준다. 그러나 양방향 통신으로 인해 기존 통신 기술에 존재하는 보안 취약점 역시 전력망에 적용되어 전력망을 대상으로 한 사이버 침해사고가 발생할 수 있다. 이는 국가기반시설을 대상으로 하는 공격으로 대규모 정전과 같은 결과를 가져올 수 있어 사이버 테러의 첫 번째 목표로 스마트그리드가 부상하고 있다. 이에 각 국에서는 스마트그리드 보안 연구를 활발히 진행하고 있다. 사이버 침해사고가 발생할 경우, 기본적인 사고 대응 활동 이외에도 사고 발생 원인을 조사하고 취약점을 확인하여 재발 방지를 위한 노력이 필수적이다. 이러한 사고 원인 조사 및 재발방지를 위해서는 법적 신뢰성을 확보할 수 있는 디지털 증거 수집 기술이 필수적이다. 따라서 스마트그리드 보안 연구에서도 디지털 증거 수집을 통한 사고분석에 대한 연구가 진행되고 있다.

SCADA 환경에서 포렌식을 위한 환경 및 구조에 대한 연구가 진행되었으며[1], PCS(Process Control System) 또는 SCADA(Supervisory Control and Data Acquisition) 환경에서 EnCase를 이용한 증거 수집 과정에 대한 연구가 진행되었다[2]. 또한, SCADA 환경에서 포렌식을 위한 요구사항에 대한 연구도 진행되었으며[3][4], 온라인 영역의 디지털 증거의 가용성을 높이기 위한 발명[5], 메시지 변조 코드를 활용하여 효율적인 디지털 증거 수집이 가능한 방안이 연구되었다[6]. 마지막으로 TTP(Trusted Third Party)를 이용하여 디지털 증거의 법적 신뢰성을 향상시키고 가용성을 제공할 수 있는 방안이 연구되었다[7]. 그러나 이러한 연구 중 디지털 증거 수집 기법에 대한 연구는 스마트그리드 환경에서 적용하기 어렵거나 법적 신뢰성 확보에 대해 고려하지 않은 측면이 있다.

이에 본 논문에서는 기존 디지털 증거 수집 기법을 활용하면서 스마트그리드 환경에서 적용가능하며, 법적 증거 능력을 충분히 갖출 수 있는 디지털 증거 수집 기법 및 방법을 제안한다. 더 나아가, 증거 수집 담당자 또는 증거 수집도구의 신뢰성에 의존하지 않는 디지털 증거 수집 방안을 제안함으로써, 향후 수많은 기기들로 구축되는 스마트그리드 환경에서 법적 신뢰성을 확보하는 동시에 자동화된 원격 수집 방안 연구에 기초가 될 것으로 기대된다.

〔표 1〕 법적 증거 능력을 갖추기 위한 필요 요소

	의미
원본 유지성	- 디지털 증거가 최초로 생성된 것이 매체의 변화에도 불구하고 그 내용이 변함이 없어야 함[9]
진정성	- 제출된 증거가 저장, 수집과정에서 오류가 없으며, 특정한 사람의 행위의 결과가 정확히 표현되었고 그로 인해 생성된 자료인 것임을 인정되어야 함[10]
무결성	- 디지털 증거가 다른 증거와 달리 변경, 훼손이 용이하므로, 최초의 저장된 매체에서 법정에 제출되기 까지 변경이나 훼손이 없었다는 점을 입증해야 함[11]
신뢰성	- 수집 및 분석 절차에 적용된 과학적 원리 또는 이론의 신뢰성, 그 원리 또는 이론을 구현한 기술의 신뢰성, 기술 적용의 구체적 타당성이 증명되어야 함[9]
전문 법칙의 적용	- 사실인정의 기초가 되는 경험적 사실을 경험자 자신이 직접 법원에 진술하지 않고 다른 형태에 의하여 간접적으로 보고가 되었음이 확인되어야 함[9]

본 논문의 구성은 2장에서 스마트그리드 관련 환경 분석과 기존 디지털 증거 수집 방안에 대해 분석하고, 3장에서는 스마트그리드 환경에 적합한 디지털 증거 수집 기법을 제안한다. 이어, 4장에서는 제안한 디지털 증거 수집 기법의 타당성을 분석, 평가하고 5장에서 결론을 맺는다.

II. 배경 및 관련 연구

2.1 디지털 증거 수집 요구사항

디지털 증거는 전자적 증거, 전파기록, 전파적 기록, 컴퓨터 관련 증거, 컴퓨터 전자 기록 등 의 용어로 표현되기도 한다[8]. 디지털 증거가 법적 증거 능력의 요건을 갖추기 위해서는 〔표 1〕과 같이 원본 유지성, 진정성, 무결성, 신뢰성, 전문법칙의 적용을 보장해야 한다. 이 중에서 전문법칙의 적용은 사람의 진술에 대해 법원에 진술하지 않더라도 다른 형태로 확인되어야 함을 의미하는 것으로 본 수집 기법에서는 증거수집도구를 통해 직접 증거를 수집하고 있으므로 고려 대상이 아니다.

스마트그리드 환경에서는 전력 서비스 특성상 최우선적으로 요구되는 사항은 지속적인 서비스 제공을 보장하는 가용성이다[3][4]. 또한, 다수의 시스템들이 물리적으로 가정 또는 빌딩 등에 설치되어 외부에 노

〔표 2〕 스마트그리드 환경에서 디지털 증거 수집 요구사항

특성	설명
가용성 보장	침해사고 조사를 위해 임의로 시스템을 종료시키거나 네트워크 연결을 차단시킬 수 없으므로, 원본 유지성, 무결성을 보장하면서 동시에 시스템의 가용성을 만족시키는 증거 수집이 가능해야 한다.
확장성 고려	스마트그리드 기기는 전국 각지에 널리 보급되어 이용될 수 있다. 따라서 충분히 숙련된 전문 증거 수집가가 빠른 시간에 도달할 수 없는 문제가 있다. 이를 위해 증거 수집 권한을 많은 담당자에게 부여한다면 디지털 증거 수집 담당자의 신뢰 문제가 낮아질 수 있다. 따라서 증거 수집 담당자의 신뢰도에 의존하지 않거나 원격 증거 수집 등 확장성을 고려하는 증거 수집이 가능해야 한다.
다양한 플랫폼 고려	스마트그리드 기기는 제조사에 따라 다양한 플랫폼이 존재한다. 또한, 저사양의 기기에서도 사고 조사를 진행해야 하므로, 이 점을 모두 고려하여 증거수집 도구가 다양한 환경을 지원할 수 있도록 해야 한다.

출되고 다양한 장소에 설치되어 운영 되고 있는 특징이 있다〔2〕. 스마트그리드 유틸리티 영역에 존재하는 시스템들의 경우, 고사양의 서버 시스템들이 대부분이며 이에 반해 필드 영역에 존재하는 시스템들의 경우는 저사양의 임베디드 시스템이 대부분이다. 특히, 저사양의 임베디드 시스템의 경우 제조사에 따라 RTOS, Non-RTOS, 펌웨어 형태의 다양한 플랫폼 기반을 이용한다〔3〕〔4〕.

이와 같은 스마트그리드 환경의 특성으로 인해 스마트그리드 환경에서 발생하는 침해사고 조사를 위한 디지털 증거 수집은 다음 〔표 2〕와 같은 특성을 만족해야 한다.

2.2 기존 연구 분석

T.Kilpatrick 등이 제안한 논문에서는 SCADA 환경에서 네트워크 포렌식을 위해 사전에 포렌식 에이전트를 별도 서버로 구성하여 트래픽 정보를 가공하여, DB역할을 하는 데이터 저장소에 수집하고 수집한 데이터에서 디지털 증거를 분석하는 방법을 제안하였다〔1〕. 제안한 방법은 가용성, 확장성, 다양한 플랫폼 기반에서의 증거 수집은 가능하나 원본 유지성, 무결성 보장을 고려하지 않았다. 또한 포렌식 에이전트와 데이터저장소가 오류 또는 의도되지 않은 동작으로 인한 진정성 보장이 어렵다.

Regis Friend Cassidy 등이 제안한 논문에서는 PCS 환경에서 EnCase 포렌식 툴을 이용한 원격 포렌식 방법에 대해 제안하였다〔2〕. 제안한 방법을 이용하여 가용성, 무결성은 보장할 수 있으나, EnCase에서 지원되지 않는 제품의 사용이 불가능하다. 또한, EnCase 제품이 먼저 신뢰되어야 하므로 진정성, 신뢰성이 보장되지 않는다.

한국전자통신연구원에서 2009년 출원한 특허인 “증거 데이터 수집 장치 및 그 방법”에서는 저장매체를 확보하기 어려운 인터넷 상의 웹 데이터, 기업 DB 쿼리를 통해 얻은 온라인 데이터 혹은 정보통신 공간상에서 수집된 온라인 데이터 등의 무결성을 보장하기 위해 타임스탬프 기능과 스크린캡쳐 기능을 이용하여 해당 시점 데이터 증거의 원본성 및 유효성을 확보하는 방법을 제안했다〔5〕. 제안하는 방법을 이용할 경우, 가용성, 확장성을 보장할 수 있다. 그러나 다양한 플랫폼 환경에서는 고려하지 않았다.

디지털 증거 수집 과정에서 개선된 디지털 증거의 무결성 보장 방안으로 공개키 기반구조의 공증 방식과 변조 탐지 코드 사용 방식을 선택적으로 사용하는 방안이 연구되었다〔6〕. 이 방식의 경우, 현행 수집 방법에 비해 공개키 기반의 공증 방식과 변조 탐지 코드 사용 방식을 적절히 사용하여 디지털 증거의 무결성을 보장받음과 동시에 불필요한 절차 이행으로 인한 비용, 시간 부담을 감소시켜 확장성을 만족할 수 있다. 그러나 가용성과 다양한 플랫폼 환경에 대한 개선 사항은 고려되지 않았다.

디지털 증거 수집과 관련하여 또 다른 연구로 디지털 컴퓨팅 환경의 디지털 증거화를 위한 침해 데이터 보증 메커니즘이 있다〔7〕. 이 연구에서는 TTP를 이용하여, 현행 방식에 비해 법적 신뢰성을 높이고 증거 관리를 체계적으로 함으로써, 가용성을 제공한다. 그러나 확장성과 다양한 플랫폼 환경에 대한 개선 사항은 고려되지 않았다.

기존 연구에서는 법적 신뢰성을 갖출 수 있는 모든 요구사항과 스마트그리드 환경에 존재하는 요구사항을 모두 만족하는 경우는 없다. 특히, 신뢰성의 경우 증거 수집도구의 신뢰성에 기반하고 있다는 특징이 있다. 따라서 본 논문에서는 스마트그리드 환경에서의 요구사항과 법적 신뢰성을 모두 보장하며, 증거 수집 과정에서 데이터의 위변조 또는 노출을 최소화 할 수 있도록 암호화 하는 방안을 제안한다.

III. 제안하는 기법

3.1 시스템 구성

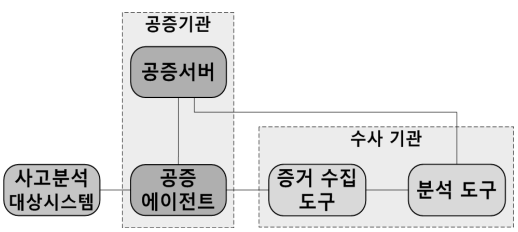
본 논문에서 제안하는 기법의 시스템 구성은 〔그림 1〕과 같다.

사고분석 대상 시스템은 디지털 증거를 수집해야 할 대상을 의미한다. 공증기관은 디지털 증거의 신뢰성을 보증할 수 있도록 신뢰된 기관을 의미하며, 수사기관은 디지털 수집, 분석을 담당하는 기관으로 대검찰청이 해당될 수 있다.

공증기관은 스마트그리드 환경에 새로운 기기가 도입될 경우, 해당 기기로부터 증거 데이터를 수집할 수 있도록 공증에이전트를 업데이트하며, 공증에이전트의 암호모듈과 주요 기능이 문제없이 동작할 수 있도록 관리하는 역할을 수행한다. 정기적인 취약점 점검 상태 점검을 수행해야 한다. 또한, 공증에이전트가 증거 수집 시 생성하는 관련 정보를 공증 서버에 저장하고 공증에이전트가 사용할 랜덤키를 생성해서 전송해 주며, 증거 분석 시에는 랜덤 키를 분석 도구에게 전달하여 복호화 할 수 있도록 해준다. 공증 서버에 저장되는 수집 정보, 랜덤키, 서명값은 무결성 검증에 이용된다.

공증에이전트는 사전에 공증기관으로부터 인증 받은 S/W 또는 H/W가 될 수 있으며, S/W로 구성할 경우 증거 수집 도구에 설치하도록 한다. 공증 에이전트는 전국 수사기관에 배치하고 공증기관에서 안전하게 관리한다. 공증에이전트는 사고분석 대상 시스템으로부터 디지털 원본을 수신하여 이에 대한 무결성 값 생성, 암호화를 담당한다.

증거 수집 도구는 공증에이전트가 전달하는 암호화된 데이터를 수집하여 분석가에게 전달하는 역할을 담당한다. 기존 수집 도구를 그대로 이용하거나, 암호화 데이터를 저장하고 분석 도구까지 전달해 줄 수 있는 별도의 도구를 개발할 수도 있다.



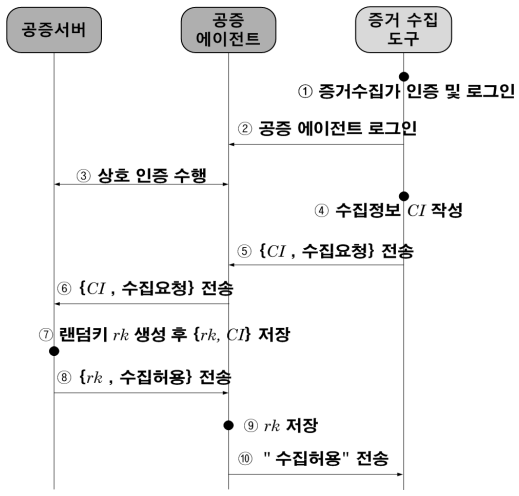
〔그림 1〕 제안하는 증거 수집 기법의 시스템 구성도

3.2 증거 수집 절차

3.2.1 증거 수집 준비 단계

침해사고 조사를 위해 대상 시스템이 결정되면 증거 수집가는 공증에이전트, 증거 수집도구를 수령 받고 현장으로 출동한다. 현장에 도착한 후, 대상 시스템에 공증에이전트를 연결하고 공증에이전트와 증거 수집도구를 연결한다. 이후 수행 과정은 〔그림 2〕와 같다.

① 증거 수집가는 증거 수집도구에 아이디/패스워드 기반의 사용자 인증을 수행
② 증거 수집도구는 공증에이전트에 증거 수집가 사용자 정보를 이용하여 로그인 수행
③ 공증에이전트는 증거 수집도구와 연결이 성공하면 공증서버와 상호인증을 수행함
(PKI 기반의 인증서를 통해 상호 인증을 수행하며 이후에는 SSL, TLS, 또는 이와 유사한 암호화 통신 수행)
④ 증거 수집가는 〔표 3〕과 같은 내용을 포함하는 수집정보 CI를 작성
⑤ 증거 수집도구는 수집정보와 수집요청 메시지를 공증에이전트에 전송
⑥ 공증에이전트는 수집정보와 수집요청 메시지를 공증서버에 전송
⑦ 공증서버는 랜덤키 rk를 생성하여 수집정보와 함께 저장
(랜덤키 생성 시, Hash_DRBG, HMAC_DRBG, CTR_DRBG 또는 이와 유사한



〔그림 2〕 디지털 증거 수집 준비 단계 수행 절차

〔표 3〕 수집정보 내용

CI (수집정보)	수집 사건 식별 번호
	수집 시작 일시
	수집 사건 대상 시스템 명
	수집 시스템 종류(플랫폼, 제조사)
	증거 수집가 명
	수집 도구 ID
	대상 시스템 담당자 또는 관리자 명
	기타 참고 사항

강도의 난수 발생기를 이용)

⑧ 공증서버는 rk와 수집허용 메시지를 공증에이전트에 전달

⑨ 공증에이전트는 전송받은 랜덤키를 안전하게 저장

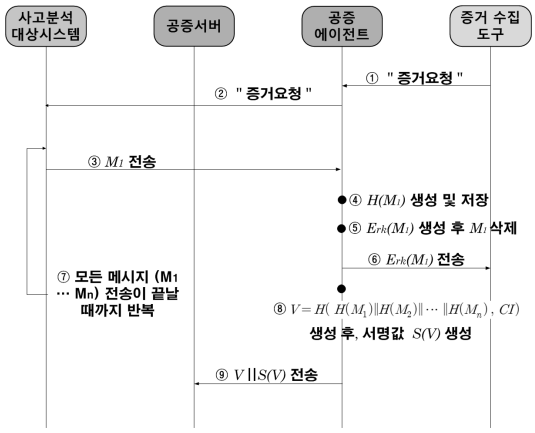
⑩ 공증에이전트는 수집허용메시지를 증거 수집도구에 전송

위와 같은 절차가 완료되면, 증거 수집을 위한 준비단계는 종료된다. 각 단계에서 정상적인 동작이 이루어지지 않은 경우 모든 단계는 중단되고, 에러메시지를 증거 수집가에게 전달한다.

3.2.2 증거 수집 단계

증거 수집 준비가 완료되면 실제로 증거를 수집하는 증거 수집 단계를 수행한다. 증거 수집 단계는 〔그림 3〕과 같은 절차로 수행된다.

① 증거 수집도구는 공증에이전트에게 증거 데이터를 요청



〔그림 3〕 디지털 증거 수집 단계 수행 절차

〔표 4〕 대상시스템으로부터 증거 수집도구까지 증거 데이터 흐름

대상시스템	공증에이전트	증거 수집도구
③ M_1 →	④ $H(M_1)$ 생성, 저장 ⑤,⑥ $E_{rk}(M_1)$ →	$E_{rk}(M_1)$저장
③ M_2 →	④ $H(M_2)$ 생성, 저장 ⑤,⑥ $E_{rk}(M_2)$ →	$E_{rk}(M_2)$저장
…	…	…
③ M_n →	④ $H(M_n)$ 생성, 저장 ⑤,⑥ $E_{rk}(M_n)$ →	$E_{rk}(M_n)$저장

② 공증에이전트는 대상시스템에게 증거 데이터를 요청

③ 대상시스템은 증거 데이터 원본을 블록 단위로 전송($M_1, M_2, \cdots, M_n$)

④ 공증에이전트는 전송받은 블록에 대해 해시값 $H(M_1)$을 생성하고 해시값을 저장

(해시 함수는 SHA-256 또는 이와 유사한 강도의 암호학적 해시 함수를 이용)

⑤ 공증에이전트는 전송받은 블록에 대해 준비단계에서 공증서버로부터 수신한 랜덤키 rk로 암호화를 수행하여 $E_{rk}(M_1)$ 생성 후, M_1 삭제

⑥ 공증에이전트는 생성한 암호화 데이터 $E_{rk}(M_1)$를 증거 수집도구에게 전송

⑦ 모든 원본데이터를 전송할때 까지 〔표 4〕와 같이 ③~⑥ 단계를 반복

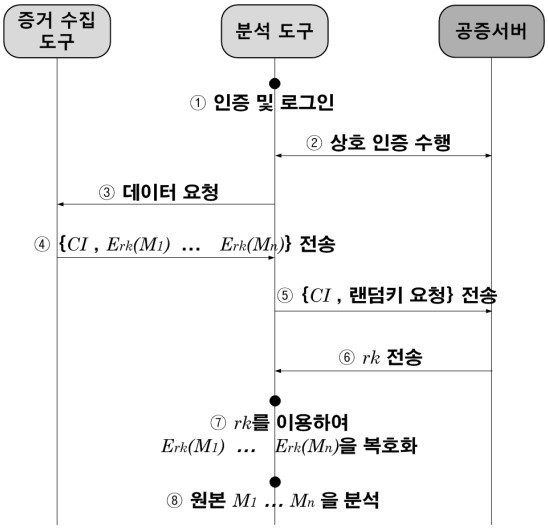
⑧ 공증에이전트는 저장된 해시값들과 사건정보 *CI*를 이용하여 검증값 V를 생성하고 V에 대해 서명

$V = H(\ H(M_1)\|H(M_2)\|\cdots\|H(M_n), CI)$

(전자서명은 ECDSA, EC-KCDSA, 또는 이와 유사한 암호강도를 갖는 전자서명 이용)

⑨ 공증에이전트는 자신의 개인키로 서명된 검증값 ($V\|S(V)$)을 공증서버에 전송

위와 같은 절차대로 증거 데이터를 수집하며, 각 단계에서 정상적인 동작이 이루어지지 않을 경우, 모든 단계는 중단되고 에러메시지를 증거 수집가에게 전달한다. 이 과정이 정상적으로 종료될 경우, 공증에이전트는 랜덤키 rk를 삭제하고 초기 상태로 안전하게 되돌아간다.



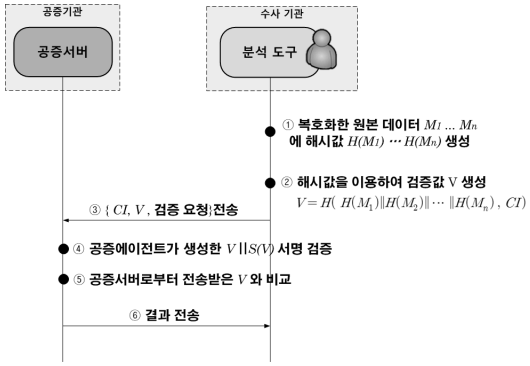
〔그림 4〕 데이터의 증거 분석을 위한 복호화 수행 절차

3.2.3 증거 분석 및 무결성 검증 단계

증거 수집이 종료되고 증거 분석을 위해서 증거 분석가는 증거 수집가로부터 인계받은 증거 수집도구를 분석도구와 연결한다. 이 후, 실제 디지털 증거 분석을 위한 데이터 복호화 과정은 〔그림 4〕와 같다.

① 증거분석가는 분석도구에 아이디/패스워드 기반의 사용자 인증을 통해 로그인
② 분석도구와 공증서버는 서로가 정당한 기기임을 확인하는 상호인증 수행
(PKI 기반의 인증서를 통해 상호 인증을 수행하며 이후에는 SSL, TLS, 또는 이와 유사한 암호화 통신 수행)
③ 분석도구는 증거 수집도구에게 데이터 요청
④ 증거 수집도구는 수집정보, 암호화된 데이터를 분석도구에 전송
⑤ 분석도구는 수신한 수집정보와 랜덤키 요청메시지를 공증서버에 전송
⑥ 공증서버는 수집정보에 해당하는 랜덤키를 분석도구에 전송
⑦ 분석도구는 수신한 암호화된 데이터와 랜덤키를 이용하여 증거 데이터 원본 획득
⑧ 증거분석가는 분석도구를 이용하여 증거 데이터 원본의 분석을 시작

암호화된 디지털 증거를 복호화 하여, 원본 상태에서 분석을 시작할 수 있다. 분석을 시작하기 전 필요



〔그림 5〕 데이터 무결성 검증 수행 절차

에 따라 무결성 검증을 먼저 수행한 후, 분석을 시작할 수 있다. 무결성 검증을 위한 방법은 전송받은 검증값과 복호화 한 원본에 대해 검증값을 생성하여 이 두 값을 비교하여 간단히 수행할 수 있다. 사법기관의 요청에 따라 외부 기관에서 무결성을 검증할 경우 〔그림 5〕와 같은 절차를 통해 무결성 보증이 가능하다.

① 복호화한 원본 데이터로부터 각 블록 별 해시 값을 생성
$M_1, M_2, \cdots, M_n \rightarrow H(M_1), H(M_2), \cdots, H(M_N)$
② 생성한 해시값들을 이용하여 검증값 V 생성
$V = H(\ H(M_1) \| H(M_2) \| \cdots \| H(M_n), CI)$
③ 수집정보 CI와 V, 검증요청 메시지를 공증서버에 전송
④ 공증기관은 공증에이전트가 생성한 $V \| S(V)$에서 서명을 검증
⑤ 공증기관은 공증에이전트가 서명한 V와 수사기관이 전송한 V가 일치하는지 확인
⑥ 일치하면 무결성이 확인되었음을, 일치하지 않으면 무결성이 깨어졌음을 수사기관에 알림

IV. 제안한 증거 수집 기법 분석

4.1 제안한 기법의 분석 방법

제안한 증거 수집 기법은 기존 디지털 증거 수집 기법을 활용하면서 법적 신뢰성을 확보할 수 있도록 앞에서 제시한 원본 유지성, 진정성, 무결성, 신뢰성을 만족할 수 있어야 한다. 이와 같은 요구사항을 만족하지 못할 경우 법적 효력을 가질 수 없으며 증거 수집을 통해 나온 어떠한 결과에 대해서도 신뢰성을 확보할 수 없다. 또한, 앞에서 제시한 스마트그리드 환경

의 요구사항인 가용성 제공, 확장성 만족, 다양한 플랫폼에서 적용 가능한 증거 수집 절차임을 평가해야 한다. 또한, 추가적으로 수집도구 또는 증거 수집 담당자의 신뢰성에 의존하는지 평가해야 한다. 증거 수집도구 또는 증거 수집 담당자의 악의적인 행위로 인해 증거 데이터의 신뢰도가 훼손될 수 있으므로, 증거 수집도구나 증거 수집담당자에게 전적으로 의존하지 않는지 평가한다.

위와 같은 평가 요구사항을 각 항목별로 분석하여 제안한 증거 수집 기법의 타당성을 설명하고 앞에서 제시한 현행 증거 수집 기법과 제안되었던 방식들과 비교 분석하도록 한다.

4.2 제안한 증거 수집 기법 분석

4.2.1 원본 유지성

제안한 기법은 가용성을 보장하는 방식으로 시스템을 종료하고 물리적으로 디지털 데이터의 원본이 되는 저장장치의 획득은 수행하지 않는다. 그러나, 데이터 원본을 공증에이전트에서 수집하는 동시에 해시값을 생성하고 암호화를 수행한다. 공증에이전트는 공증기관에서 검증된 것으로 데이터 원본을 수집하는 과정을 신뢰할 수 있고, 정상적인 암호 알고리즘을 이용하고 있음을 신뢰한다. 따라서 정당한 방식으로 원본 데이터를 암호화하고 서명한 데이터는 복호화 시, 원본과 동일한 데이터가 생성되므로 원본은 유지되었음을 확인할 수 있다.

4.2.2 진정성

제안한 방식에서는 공증기관이 존재함에 따라 공증에이전트가 수행하는 검증값 생성, 암호화 과정은 신뢰할 수 있다고 가정한다. 즉, 공증기관 또는 공증기관에서 생성하는 검증값, 암호화된 데이터는 과학적으로 정당하게 생성되었음을 신뢰할 수 있으며, 복호화한 데이터를 이용한 검증값이 공증에이전트가 생성한 검증값과 동일한 경우, 이를 신뢰할 수 있다. 따라서 제안한 방식에서 증거 수집 과정은 증거 데이터의 진정성 확보가 가능하다.

4.2.3 무결성

제안한 방식에서 무결성이 훼손되었을 경우, 검증값 비교 과정에서 이를 확인할 수 있다. 즉 원본데이터 중 하나인 M_i에 위조 또는 변조 되어 M'이 되었을 경우, $H(M'_i)$가 생성되어 최종 검증값은 $H(H(M_1)\|\cdots\|H(M'_i)\|\cdots\|H(M_n), CT)$로 실제 검증값 V와는 다른 값이 생성된다. 검증된 공증에이전트가 생성한 검증값 V는 신뢰할 수 있으므로 복호화 후, 분석한 데이터의 검증값이 공증에이전트가 생성한 검증값 V와 일치한다면 무결성이 보장되었음을 확인할 수 있다.

4.2.4 신뢰성

공증에이전트는 공증기관에서 검증된 암호 알고리즘, 해시값 생성 알고리즘을 사용하여 과학적으로 정당함을 검증할 수 있다. 공증기관은 공증에이전트에서 동작하는 어플리케이션의 취약점 점검을 수시로 진행하고 새로운 기기 도입으로 인한 업데이트나 취약점으로 인한 보안 패치를 일괄적으로 수행할 수 있도록 체계를 구축하고 정비한다. 이를 통해 제안한 디지털 증거 수집 절차의 신뢰성을 확보할 수 있다. 공증기관의 인증을 받지 못한 시스템이 공증에이전트로 가장할 경우, 공증서버와 인증서 기반의 상호 인증이 실패하게 되어 증거 수집이 불가능하다.

4.2.5 가용성

제안한 절차에 따라 증거 수집 시, 실제 대상 시스템의 전원을 종료하지 않고 해당 시점의 증거 데이터를 수집하여 전달함으로써, 가용성을 보장할 수 있다. 스마트그리드 기기는 동작 중에 공증에이전트에 요청에 따라 저장된 데이터를 보내는 동시에 전력 서비스는 꾸준히 제공할 수 있으며, 공증에이전트는 증거 수집이 전력 서비스를 방해하지 않도록 설계부터 고려하여 개발된다. 또한, 증거 수집으로 인해 가용성을 침해하는 경우가 발생한다면 공증기관은 바로 업데이트하여 모든 공증에이전트가 가용성을 침해할 수 없도록 한다.

4.2.6 확장성

제안한 디지털 증거 수집 기법은 기존 디지털 증거 수집 기법을 최대한 활용하여 상대적으로 쉽게 스마트그리드 환경에 적용 가능하도록 제안하였다. 또한 증거 수집 과정에서 증거 데이터는 공증에이전트에서 수

집 시, 무결성 검증값을 생성한 뒤 바로 암호화 된다. 따라서 증거 데이터에 포함될 수 있는 개인정보는 증거 수집가에게도 노출되지 않으며, 분석 시 분석가에게만 노출된다. 이는 증거 수집가 또는 증거 수집도구의 신뢰도에 의존하지 않고 숙련된 전문가가 아니더라도 각 지방의 수사기관에서 어떠한 인력도 손쉽게 디지털 증거 수집이 가능함을 의미한다. 이를 이용하여 전국 넓은 지역에 설치되는 스마트그리드 기기의 증거 수집이 더욱 용이해질 수 있다. 또한, 공증에이전트와 대상 시스템과 안전한 통신만 확보된다면 원격으로 증거 데이터를 분석가에게 전송하여 넓은 지역에 설치된 스마트그리드 기기의 빠른 분석이 가능해질 수 있다.

4.2.7 다양한 플랫폼 환경

제안된 증거 수집 기법은 기존 디지털 증거 수집 기법을 최대한 활용하여 대상 시스템이나 증거 분석 도구에 별도의 모듈 설치가 필요 없다. 따라서 스마트그리드 기기가 새로 도입 시, 공증기관에서는 새로운 기기에 대해 공증에이전트가 증거 데이터를 수집할 수 있도록 기존 공증에이전트를 일괄 업데이트 하거나, 유틸리티와 협의하여 도입 이전부터 공증에이전트가 증거 데이터 수집이 가능하도록 협의할 수 있다. 즉, 다양한 성능과 플랫폼 환경에서 각 기기에 설치할 별도의 모듈 개발 없이 공증에이전트만 수정함으로써 손쉽게 다양한 환경에 적용 가능하다.

4.2.8 수집도구 또는 담당자의 신뢰성 의존도

기존 디지털 증거 수집 기법에서는 증거 수집도구에 영향을 많이 받고 있으며, 증거 수집담당자의 중간 개입을 차단할 방법이 없다. 그러나 제안한 증거 수집 기법에서는 공증에이전트를 활용하여 증거 수집도구의 취약점을 이용한 증거 데이터 위변조에도 영향을 받지 않으며, 증거 수집담당자의 실수 또는 악의적인 중간 개입을 차단할 수 있다.

4.3 제안한 증거 수집 기법 비교 분석

위에서 요구사항에 대해 디지털 증거 수집 기법을 현행 방식, 기존 연구된 방식을 비교한 결과는 〔표 5〕와 같다.

기존 연구된 디지털 증거 수집 방안과 달리, 제안하는 기법으로 디지털 증거를 수집할 경우, 법적 효력을 가질 수 있도록 모든 요건을 만족함과 동시에, 스마트그리드 환경에서 요구하는 요구사항을 만족함을 확인하였다. 또한, 제안하는 방안은 수집도구 또는 수집 담당자의 신뢰성에 의존하지 않으므로 인해 수집도구의 취약점으로 인한 오류 또는 수집 담당자의 실수로부터 보다 신뢰성 있는 증거 수집이 가능하다.

〔표 5〕 증거 수집 기법 비교

요구사항	〔1〕	〔2〕	〔5〕	〔6〕	〔7〕	제안 방식
법적 신뢰성을 위한 요구사항 만족 여부	-	-	O	△	O	O
가용성	O	O	O	X	O	O
확장성	O	X	O	O	X	O
다양한 플랫폼 지원	O	X	X	X	X	O
수집도구 또는 담당자 신뢰성 의존도	높음	높음	높음	높음	높음	낮음

V. 결 론

본 논문에서는 스마트그리드 환경에서 침해사고 조사를 위한 디지털 증거 수집에 있어서 필요한 요구사항을 분석하고, 분석한 요구사항을 모두 만족할 수 있는 디지털 증거 수집 방안을 제안하였다.

제안한 방법은 기존 디지털 포렌식 기법을 그대로 활용하며 공증 기관을 통해 디지털 증거의 신뢰성을 확보할 수 있는 방법으로, 다양한 환경에서 사용 가능하며, 가용성과 확장성을 보장함으로써 스마트그리드 환경에서 적합한 기법으로 분석하였다. 이러한 디지털 증거 수집 기법은 국가 전력망을 대상으로 한 스마트그리드 사이버 범죄에 대한 수사절차와 디지털 증거에 대한 신뢰성 향상에 기여하여 국가기반시설 보호에 큰 역할을 수행할 수 있다.

그러나 제안한 기법에서는 사고 분석 대상시스템이 자체적으로 데이터를 은폐할 경우, 이에 대한 증거 수집이 어려운 단점이 존재한다.

향후에는 본 논문에서 연구된 결과를 바탕으로 증거 수집을 원격으로 수행하여 전국 수천만대의 스마트그리드 기기가 보급되는 광역 환경에서 효율적인 자동 증거 수집 기법에 대한 연구가 필요하며, 사고분석 대상시스템이 악의적으로 데이터를 은폐할 경우, 이를 해결할 방안에 대한 연구가 필요하다.

참고문헌

〔1〕 Tim Kilpatrick, Jesus Gonzalez, Rodrigo Chandia, Mauricio Papa and Sujeet Shenoi, "An Architecture for SCADA Network Forensics," International Federation for Information Processing, Vol. 222, pp. 273-285, 2006

〔2〕 Regis Friend Cassidy, Adrian Chavez, Jason Trent and Jorge Urrea, "Remote Forensic Analysis of Process Control Systems," International Federation for Information Processing, Vol. 253, pp. 223-235, 2007

〔3〕 Irfan Ahmed, Sebastian Obermeier, Martin Naedele and Golden G. Richart Ⅲ, "SCADA Systems: Challenges for Forensic Investigators," IEEE Computer Society, Vol.45 no.12, pp. 44-51, Dec. 2012

〔4〕 Mark Fabro and Eric Cournelius, "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," INL/EXT-08-14231, INL, Aug. 2008

〔5〕 한국전자통신연구원, "증거 데이터 수집 장치 및 그 방법," 출원번호 2009-0079567, 2009. 8. 27.

〔6〕 조상수, 신용태, "디지털 증거의 무결성 보장 절차에 대한 개선," 정보과학회논문지, 정보통신 39(2), pp. 184-191 2012년 4월

〔7〕 장은겸, "디지털 컴퓨팅 환경의 디지털 증거화를 위한 침해 데이터 보증 메커니즘," 한국인터넷정보학회, 11(4), pp. 129-141, 2010년 8월

〔8〕 조국, "컴퓨터 전자기록에 대한 대물적 강제처분의 해선론적 쟁점," 한국형사정책학회 22(1), pp. 99-123, 2010년 6월

〔9〕 권오걸, "디지털 증거의 개념 · 특성 및 증거능력의 요건," IT와 法연구 제5집, pp. 291-318, 2011년 2월

〔10〕 양근원, "디지털 포렌식과 법적 문제 고찰," 형사정책연구 통권 제66호, pp. 205-246, 2006년 6월

〔11〕 박혁수, "개정 형사소송법 상 디지털 증거의 증거능력," 해외연수검사 연구논문, 부산지방검찰청, 2009년 7월

〈著者紹介〉

사 진

조 영 준 (Youngjun Cho) 정회원
2008년 8월: 성균관대학교 컴퓨터공학과 졸업
2010년 2월: 성균관대학교 전자전기컴퓨터공학과 석사
2010년 2월~2011년 12월 : 한국인터넷진흥원 주임연구원
2011년 12월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 스마트그리드 보안, 보안성 평가·인증, 제어시스템 보안, 침해사고 대응

사 진

최 재 덕 (Jaeduck Choi) 정회원
2002년 2월: 숭실대학교 정보통신전자공학부 졸업
2004년 2월: 숭실대학교 정보통신공학과 석사
2009년 2월: 숭실대학교 전자공학과 박사
2004년 1월~12월: ㈜애드팍테크놀러지 S/W 연구원
2009년 3월~2010년 1월: 숭실대학교 전자공학과 박사후 연구원
2010년 2월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 스마트그리드 보안, 제어시스템 보안, 이동 네트워크 보안, 차량 네트워크 보안, 인증 및 키 관리

사 진

김 신 규 (Sinkyu Kim) 정회원
2000년 2월: 연세대학교 기계전자공학부 졸업
2002년 2월: 연세대학교 컴퓨터과학과 석사
2007년 8월: 연세대학교 컴퓨터과학과 박사수료
2003년 12월~현재: ETRI 부설연구소 선임연구원/스마트그리드보안팀장
〈관심분야〉 스마트그리드 보안, 국가기반시설 보안, 취약점 분석

사 진

서 정 택 (Jungtaek Seo) 종신회원
1999년 2월: 충주대학교 컴퓨터공학과 졸업
2001년 2월: 아주대학교 컴퓨터공학과 석사
2006년 2월: 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년 11월~현재: ETRI 부설연구소 선임연구원/스마트그리드보안연구실장
2011년 11월~현재: 고려대학교 정보보호대학원 겸임교수
〈관심분야〉 스마트그리드 보안, 제어시스템 보안, 원자력 사이버 보안, 취약성 분석평가, DDoS 공격 탐지 및 대응