(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년03월24일
(11) 등록번호 10-1719698
(24) 등록일자 2017년03월20일

(51) 국제특허분류(Int. Cl.)
G06F 21/70 (2013.01) *G06F 21/57* (2013.01)
H04L 12/24 (2006.01) *H04L 12/26* (2006.01)
H04L 29/06 (2006.01)
(52) CPC특허분류
G06F 21/70 (2013.01)
G06F 21/57 (2013.01)
(21) 출원번호 10-2016-0008040
(22) 출원일자 2016년01월22일
심사청구일자 2016년01월22일
(65) 공개번호 10-2017-0019302
(43) 공개일자 2017년02월21일
(30) 우선권주장
1020150113028 2015년08월11일 대한민국(KR)
(56) 선행기술조사문헌
KR1020150072725 A*
KR101533961 B1*
*는 심사관에 의하여 인용된 문헌
기술이전 희망 : **기술양도**

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
강성구
대전광역시 유성구 온천북로33번길 22-25, 701호
김신규
대전광역시 유성구 엑스포로 448, 307동 1003호
(74) 대리인
한양특허법인

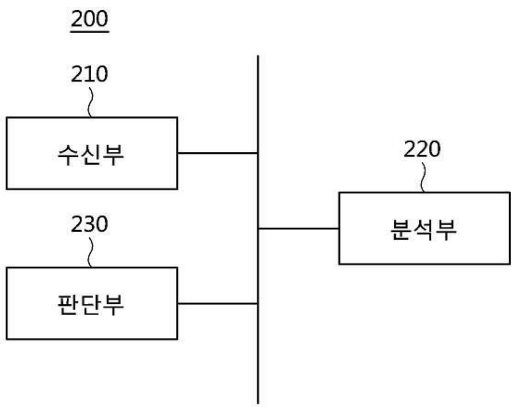
전체 청구항 수 : 총 18 항 심사관 : 구대성

(54) 발명의 명칭 **스마트그리드 기기의 침해사고 탐지 장치 및 방법**

(57) 요 약

스마트그리드 기기의 침해사고 탐지 장치 및 방법이 개시된다. 본 발명에 따른 스마트그리드 기기의 침해사고 탐지 장치는, 복수의 스마트그리드 기기들로부터 각각 비휘발성 메모리 덤프이미지와 시스템 및 어플리케이션 로그 데이터를 포함하는 시스템 변화 정보들을 수신하는 수신부, 수신된 복수의 상기 시스템 변화 정보들을 분석하여, 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 포함하는 추이 정보를 상기 스마트그리드 기기 별로 생성하는 분석부, 그리고 제1 스마트그리드 기기에 상응하는 제1 추이 정보를 상기 제1 스마트그리드 기기를 제외한 나머지 스마트그리드 기기들에 상응하는 제2 추이 정보와 비교하여, 상기 제1 스마트그리드 기기의 보안 침해 사고 발생 여부를 판단하는 판단부를 포함한다.

대 표 도



(52) CPC특허분류
H04L 41/064 (2013.01)
H04L 43/16 (2013.01)
H04L 63/1433 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2012101050004A
부처명 산업통상자원부
연구관리전문기관 한국에너지기술평가원
연구사업명 전력산업융합원천기술개발
연구과제명 스마트그리드 보안 기반기술 연구개발(2단계)
기 여 율 1/1
주관기관 국가보안기술연구소
연구기간 2012.07.01 ~ 2015.06.30

명 세 서

청구범위

청구항 1

복수의 스마트그리드 기기들로부터 각각 비휘발성 메모리 덤프이미지와 시스템 및 어플리케이션 로그데이터를 포함하는 시스템 변화 정보들을 수신하는 수신부,

수신된 복수의 상기 시스템 변화 정보들을 분석하여, 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 포함하는 추이 정보를 상기 스마트그리드 기기 별로 생성하는 분석부, 그리고

제1 스마트그리드 기기에 상응하는 제1 추이 정보를 상기 제1 스마트그리드 기기를 제외한 나머지 스마트그리드 기기들에 상응하는 제2 추이 정보와 비교하여, 상기 제1 스마트그리드 기기의 보안 침해 사고 발생 여부를 판단하는 판단부

를 포함하며,

상기 복수의 스마트그리드 기기들은,

식별 정보, 제조사 정보, 모델명 중에서 적어도 하나가 서로 동일한 것을 특징으로 하는 스마트그리드 기기의 침해 사고 탐지 장치.

청구항 2

제1항에 있어서,

상기 판단부는,

상기 나머지 스마트그리드 기기들로부터 수신된 각각의 상기 파일 시스템 변화 추이 정보 및 상기 로그데이터 변화 추이 정보를 하나의 이벤트로 간주하여, 시간 단위 별 상기 제2 추이 정보를 생성하는 스마트그리드 기기의 침해 사고 탐지 장치.

청구항 3

제2항에 있어서,

상기 판단부는,

시 단위, 일 단위, 주 단위 및 월 단위 중에서 설정된 상기 시간 단위로 상기 제1 추이 정보와 상기 제2 추이 정보를 비교하는 스마트그리드 기기의 침해 사고 탐지 장치.

청구항 4

제3항에 있어서,

상기 판단부는,

설정된 상호 비교의 종류에 상응하도록 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 이용하여 상기 제1 추이 정보와 상기 제2 추이 정보를 비교하는 스마트그리드 기기의 침해 사고 탐지 장치.

청구항 5

제4항에 있어서,

상기 판단부는,

상기 복수의 스마트그리드 기기들로부터 입력된 상기 추이 정보들을 분류 알고리즘을 이용하여 분류하고, 임계치 미만의 수로 분류된 상기 추이 정보에 상응하는 상기 스마트그리드 기기를 상기 보안 침해 사고가 발생한 것으로 판단하는 스마트그리드 기기의 침해 사고 탐지 장치.

청구항 6

제5항에 있어서,

상기 판단부는,

상기 보안 침해 사고가 발생한 것으로 판단된 상기 스마트그리드 기기에 상응하는 상기 추이 정보와 기 저장된 보안 침해 사고에 상응하는 침해 사고 추이 정보를 비교하여, 유사도를 산출하는 스마트그리드 기기의 침해 사고 탐지 장치.

청구항 7

제1항에 있어서,

상기 분석부는,

상기 비휘발성 메모리 덤프이미지를 분석하여 파악된 파일들의 생성 시간, 수정 시간 및 접근 시간 중에서 적어도 하나를 포함하는 시간 정보를 이용하여, 상기 파일 시스템 변화 추이 정보를 생성하는 스마트그리드 기기의 침해 사고 탐지 장치.

청구항 8

제1항에 있어서,

상기 분석부는,

상기 시스템 및 어플리케이션 로그데이터를 분석하여 파악된 시간 정보를 이용하여, 상기 로그데이터 변화 추이 정보를 생성하는 스마트그리드 기기의 침해 사고 탐지 장치.

청구항 9

제1항에 있어서,

상기 분석부는,

상기 비휘발성 메모리 덤프이미지를 분석하여, 파일들의 생성, 수정, 접근 및 삭제 중에서 적어도 하나의 이벤트가 발생한 시간 및 상기 이벤트의 내용을 분석하거나, 상기 시스템 및 어플리케이션 로그데이터를 분석하여, 상기 이벤트가 발생한 시간 및 상기 이벤트의 내용을 분석하는 스마트그리드 기기의 침해 사고 탐지 장치.

청구항 10

삭제

청구항 11

스마트그리드 기기의 침해 사고 탐지 장치에 의해 수행되는 스마트그리드 기기의 침해 사고 탐지 방법에 있어서,

복수의 스마트그리드 기기들로부터 각각 비휘발성 메모리 덤프이미지와 시스템 및 어플리케이션 로그데이터를 포함하는 시스템 변화 정보들을 수신하는 단계,

수신된 복수의 상기 시스템 변화 정보들을 분석하여, 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 포함하는 추이 정보를 상기 스마트그리드 기기 별로 생성하는 단계, 그리고

제1 스마트그리드 기기에 상응하는 제1 추이 정보를 상기 제1 스마트그리드 기기를 제외한 나머지 스마트그리드 기기들에 상응하는 제2 추이 정보와 비교하여, 상기 제1 스마트그리드 기기의 보안 침해 사고 발생 여부를 판단하는 단계

를 포함하며,

상기 복수의 스마트그리드 기기들은,

식별 정보, 제조사 정보, 모델명 중에서 적어도 하나가 서로 동일한 것을 특징으로 하는 스마트그리드 기기의

침해 사고 탐지 방법.

청구항 12

제11항에 있어서,

상기 제1 스마트그리드 기기의 보안 침해 사고 발생 여부를 판단하는 단계는,

상기 나머지 스마트그리드 기기들로부터 수신된 각각의 상기 파일 시스템 변화 추이 정보 및 상기 로그데이터 변화 추이 정보를 하나의 이벤트로 간주하여, 시간 단위 별 상기 제2 추이 정보를 생성하는 단계를 포함하는 스마트그리드 기기의 침해 사고 탐지 방법.

청구항 13

제12항에 있어서,

시 단위, 일 단위, 주 단위 및 월 단위 중에서 설정된 상기 시간 단위로 상기 제1 추이 정보와 상기 제2 추이 정보를 비교하는 단계를 더 포함하는 스마트그리드 기기의 침해 사고 탐지 방법.

청구항 14

제13항에 있어서,

설정된 상호 비교의 종류에 상응하도록 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 이용하여 상기 제1 추이 정보와 상기 제2 추이 정보를 비교하는 단계를 더 포함하는 스마트그리드 기기의 침해 사고 탐지 방법.

청구항 15

제14항에 있어서,

상기 복수의 스마트그리드 기기들로부터 입력된 상기 추이 정보들을 분류 알고리즘을 이용하여 분류하고, 임계치 미만의 수로 분류된 상기 추이 정보에 상응하는 상기 스마트그리드 기기를 상기 보안 침해 사고가 발생한 것으로 판단하는 단계를 더 포함하는 스마트그리드 기기의 침해 사고 탐지 방법.

청구항 16

제15항에 있어서,

상기 보안 침해 사고가 발생한 것으로 판단된 상기 스마트그리드 기기에 상응하는 상기 추이 정보와 기 저장된 보안 침해 사고에 상응하는 침해 사고 추이 정보를 비교하여, 유사도를 산출하는 단계를 더 포함하는 스마트그리드 기기의 침해 사고 탐지 방법.

청구항 17

제11항에 있어서,

상기 추이 정보를 상기 스마트그리드 기기 별로 생성하는 단계는,

상기 비휘발성 메모리 덤프이미지를 분석하여 파악된 파일들의 생성 시간, 수정 시간 및 접근 시간 중에서 적어도 하나를 포함하는 시간 정보를 이용하여, 상기 파일 시스템 변화 추이 정보를 생성하는 스마트그리드 기기의 침해 사고 탐지 방법.

청구항 18

제11항에 있어서,

상기 추이 정보를 상기 스마트그리드 기기 별로 생성하는 단계는,

상기 시스템 및 어플리케이션 로그데이터를 분석하여 파악된 시간 정보를 이용하여, 상기 로그데이터 변화 추이 정보를 생성하는 스마트그리드 기기의 침해 사고 탐지 방법.

청구항 19

제11항에 있어서,

상기 추이 정보를 상기 스마트그리드 기기 별로 생성하는 단계는,

상기 비휘발성 메모리 덤프이미지를 분석하여, 파일들의 생성, 수정, 접근 및 삭제 중에서 적어도 하나의 이벤트가 발생한 시간 및 상기 이벤트의 내용을 분석하거나, 상기 시스템 및 어플리케이션 로그데이터를 분석하여, 상기 이벤트가 발생한 시간 및 상기 이벤트의 내용을 분석하는 스마트그리드 기기의 침해 사고 탐지 방법.

청구항 20

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 스마트그리드 기기의 침해사고 탐지 장치 및 방법에 관한 것으로, 특히 스마트그리드 기기의 시스템 변화 추이를 이용하여, 보안 침해 사고의 발생 여부를 판단하거나, 발생된 보안 침해 사고가 기존에 발생한 보안 침해 사고인지 여부를 판단하는 기술에 관한 것이다.

배 경 기 술

[0002] 스마트그리드(Smart Grid)란 발전, 송배전, 판매 단계로 이어지는 기존의 전력망에 정보기술을 접목한 차세대 지능형 전력망을 의미한다. 스마트그리드는 전력 공급자와 소비자가 양방향으로 정보를 교환하여, 실시간으로 전력 사용현황을 파악하고, 이에 맞게 전력 사용 시간과 양을 통제함으로써, 에너지 효율을 최적화한다.

[0003] 스마트그리드는 개방형 및 양방향 통신환경을 기반으로 다양한 보안 사고가 발생할 수 있으며, 주요기반시설에 대한 사이버 공격은 심각한 피해를 유발할 수 있다. 예를 들어, 지난 2010년 발생한 스턱스넷(Stuxnet)은 전력량, 수압, 온도 및 밸브개폐 등 SCADA 시스템의 파괴를 유발하였다. 또한, 전기배선 조작으로 타인의 전기료를 올리거나, 전기사용을 원격 조정할 수 있는 스마트그리드 보안 위협도 발표되었으며, 스마트그리드를 대상으로 하는 사이버 공격에 대한 해커들의 관심이 증가하고 있다.

[0004] 스마트그리드는 전력망뿐만 아니라 정보통신망을 기반으로 사용자 및 사용자의 정보를 교환함으로써 서비스를 제공한다. 따라서 기존의 IT환경에서의 보안위협과 함께 스마트그리드 특징에 따른 새로운 보안 위협이 추가로 발생할 수 있다. 그리고 스마트그리드는 소비자의 개인정보 및 전력사용정보가 양방향으로 전송됨에 따라 개인정보 및 전력사용정보 유출로 소비자의 프라이버시가 침해될 수 있다. 또한, 전력사용정보에 대한 위변조로 과금 전가 및 우회 등이 발생할 수 있다.

[0005] 소비자가 집 외의 장소에서도 스마트폰이나 인터넷을 통하여 스마트그리드 시스템에 접속할 수 있게 되면서 보안 위협 가능성이 높아졌으며, 다양한 스마트기기의 등장으로 보안위협의 발생 가능성이 증가하였다.

[0006] 스마트그리드 보안 공격은 통제권을 갈취하여 전력공급을 중단하거나, 악의적으로 이용할 수 있으며, 전 국민의 일상생활과 밀접한 관계를 갖는 만큼 스마트그리드 환경에서의 보안 문제가 발생할 경우, 다양한 사회 인프라에 대한 공격으로 확대될 수 있으며, 그 피해 또한 막대할 것으로 예상된다.

[0007] 따라서, 스마트그리드 기기의 보안 침해 사고를 탐지하고, 탐지된 보안 침해 사고에 대응할 수 있는 기술의 개발이 필요하다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국 등록 특허 제10-1547998호, 2015년 08월 27일 공개(명칭: 취약성 분석 정보 제공 장치 및 그 방법)

발명의 내용

해결하려는 과제

[0009] 본 발명의 목적은 스마트그리드 기기의 보안 침해 사고 의심 여부를 판단하여, 각종 보안 위협으로부터 안전한 스마트그리드 환경을 구축할 수 있도록 하는 것이다.

[0010] 또한, 본 발명의 목적은 발생한 보안 침해 사고가 기존에 발생된 보안 침해 사고인지 여부를 판단하여, 발생한 보안 침해 사고에 신속하고 정확하게 대응할 수 있도록 하는 것이다.

과제의 해결 수단

[0011] 상기한 목적을 달성하기 위한 본 발명에 따른 스마트그리드 기기의 침해 사고 탐지 장치는, 복수의 스마트그리드 기기들로부터 각각 비휘발성 메모리 덤프이미지와 시스템 및 어플리케이션 로그데이터를 포함하는 시스템 변화 정보들을 수신하는 수신부, 수신된 복수의 상기 시스템 변화 정보들을 분석하여, 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 포함하는 추이 정보를 상기 스마트그리드 기기 별로 생성하는 분석부, 그리고 제1 스마트그리드 기기에 상응하는 제1 추이 정보를 상기 제1 스마트그리드 기기를 제외한 나머지 스마트그리드 기기들에 상응하는 제2 추이 정보와 비교하여, 상기 제1 스마트그리드 기기의 보안 침해 사고 발생 여부를 판단하는 판단부를 포함한다.

[0012] 이때, 상기 판단부는, 상기 나머지 스마트그리드 기기들로부터 수신된 각각의 상기 파일 시스템 변화 추이 정보 및 상기 로그데이터 변화 추이 정보를 하나의 이벤트로 간주하여, 시간 단위 별 상기 제2 추이 정보를 생성 할 수 있다.

[0013] 이때, 상기 판단부는, 시 단위, 일 단위, 주 단위 및 월 단위 중에서 설정된 상기 시간 단위로 상기 제1 추이 정보와 상기 제2 추이 정보를 비교 할 수 있다.

[0014] 이때, 상기 판단부는, 설정된 상호 비교의 종류에 상응하도록 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 이용하여 상기 제1 추이 정보와 상기 제2 추이 정보를 비교 할 수 있다.

[0015] 이때, 상기 판단부는, 상기 복수의 스마트그리드 기기들로부터 입력된 상기 추이 정보들을 분류 알고리즘을 이용하여 분류하고, 임계치 미만의 수로 분류된 상기 추이 정보에 상응하는 상기 스마트그리드 기기를 상기 보안 침해 사고가 발생한 것으로 판단할 수 있다.

[0016] 이때, 상기 판단부는, 상기 보안 침해 사고가 발생한 것으로 판단된 상기 스마트그리드 기기에 상응하는 상기 추이 정보와 기 저장된 보안 침해 사고에 상응하는 침해 사고 추이 정보를 비교하여, 유사도를 산출할 수 있다.

[0017] 이때, 상기 분석부는, 상기 비휘발성 메모리 덤프이미지를 분석하여 파악된 파일들의 생성 시간, 수정 시간 및 접근 시간 중에서 적어도 하나를 포함하는 시간 정보를 이용하여, 상기 파일 시스템 변화 추이 정보를 생성할 수 있다.

[0018] 이때, 상기 분석부는, 상기 시스템 및 어플리케이션 로그데이터를 분석하여 파악된 시간 정보를 이용하여, 상기 로그데이터 변화 추이 정보를 생성할 수 있다.

[0019] 이때, 상기 분석부는, 상기 비휘발성 메모리 덤프이미지를 분석하여, 파일들의 생성, 수정, 접근 및 삭제 중에서 적어도 하나의 이벤트가 발생한 시간 및 상기 이벤트의 내용을 분석하거나, 상기 시스템 및 어플리케이션 로그데이터를 분석하여, 상기 이벤트가 발생한 시간 및 상기 이벤트의 내용을 분석할 수 있다.

[0020] 이때, 상기 복수의 스마트그리드 기기들은, 식별 정보, 제조사 정보, 모델명 중에서 적어도 하나가 서로 동일한 것일 수 있다.

[0021] 또한, 스마트그리드 기기의 침해 사고 탐지 장치에 의해 수행되는 스마트그리드 기기의 침해 사고 탐지 방법은 복수의 스마트그리드 기기들로부터 각각 비휘발성 메모리 덤프이미지와 시스템 및 어플리케이션 로그데이터를 포함하는 시스템 변화 정보들을 수신하는 단계, 수신된 복수의 상기 시스템 변화 정보들을 분석하여, 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 포함하는 추이 정보를 상기 스마트그리드 기기 별로 생성하는 단계, 그리고 제1 스마트그리드 기기에 상응하는 제1 추이 정보를 상기 제1 스마트그리드 기기를 제외한 나머지 스마트그리드 기기들에 상응하는 제2 추이 정보와 비교하여, 상기 제1 스마트그리드 기기의 보안 침해 사고 발생 여부를 판단하는 단계를 포함한다.

발명의 효과

[0022] 본 발명에 따르면, 스마트그리드 기기의 보안 침해 사고 의심 여부를 판단하여, 각종 보안 위협으로부터 안전한 스마트그리드 환경을 구축할 수 있다.

[0023] 또한, 발생한 보안 침해 사고가 기존에 발생된 보안 침해 사고인지 여부를 판단하여, 발생한 보안 침해 사고에 신속하고 정확하게 대응할 수 있다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 장치가 적용되는 환경을 개략적으로 나타낸 도면이다.

도 2는 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 장치의 구성을 나타낸 블록도이다.

도 3은 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 방법을 나타낸 동작흐름도이다.

도 4는 도 3의 S330 단계에서 보안 침해 사고가 발생하였는지 여부를 판단하는 과정을 설명하기 위한 순서도이다.

도 5는 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 장치가 비휘발성 메모리 덤프이미지를 분석한 결과를 나타낸 예시도이다.

도 6은 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 장치가 시스템 및 어플리케이션 로그데이터를 분석한 결과를 나타낸 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 발명을 첨부된 도면을 참조하여 상세히 설명하면 다음과 같다. 여기서, 반복되는 설명, 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능, 및 구성에 대한 상세한 설명은 생략한다. 본 발명의 실시형태는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되는 것이다. 따라서, 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[0026] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0028] 도 1은 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 장치가 적용되는 환경을 개략적으로 나타낸 도면이다.

[0029] 도 1에 도시된 바와 같이, 스마트그리드 기기의 침해 사고 탐지 장치(200)가 적용되는 환경에는 스마트그리드 기기1(100_1), 스마트그리드 기기2(100_2), ... 스마트그리드 기기 N(100_N)(이하 "복수개의 스마트그리드 기기들"라고도 함.)이 위치한다. 그리고 복수개의 스마트그리드 기기(100)들은 스마트그리드 기기의 침해 사고 탐지 장치(200)와 유선 또는 무선으로 연결된다.

[0030] 복수개의 스마트그리드 기기(100)들은 비휘발성 메모리 덤프이미지, 시스템 및 어플리케이션에 의해 생성되는 로그데이터를 포함하는 시스템 변화 정보를 각각 스마트그리드 기기의 침해 사고 탐지 장치(200)로 전송한다. 여기서 비휘발성 메모리 덤프이미지와 시스템 및 어플리케이션에 의해 생성되는 로그데이터는 스마트그리드 기기(100)의 시스템 변화를 판단함에 있어 기초가 되는 자료이다.

[0031] 또한, 복수개의 스마트그리드 기기(100)들은 스마트그리드 기기(100)의 식별 정보, 제조사 정보, 모델명 정보 중에서 적어도 하나를 포함하는 스마트그리드 기기 정보를 시스템 변화 정보와 함께 스마트그리드 기기의 침해 사고 탐지 장치(200)로 전송할 수 있다. 이 때, 복수개의 스마트그리드 기기(100)들은 식별 정보, 제조사 정보, 모델명 중에서 적어도 하나가 서로 동일한 것일 수 있다.

[0032] 그리고 복수개의 스마트그리드 기기(100)들로부터 시스템 변화 정보를 수신한 스마트그리드 기기의 침해 사고 탐지 장치(200)는 시스템 변화 정보를 분석하고, 비교하여 스마트그리드 기기의 보안 침해 사고 발생 여부를 판단한다.

[0033] 일반적으로 스마트그리드 기기는 일반 PC 또는 서버 시스템과 달리, 특정 기능만을 반복적으로 수행하는 임베디드 기기로, 시스템의 변화가 상대적으로 적다. 또한, 스마트그리드 사업자는 이러한 스마트그리드 기기들을 동일한 제품으로 유사한 환경에 다량으로 설치 및 구축하며, 동일한 운영 정책을 바탕으로 서비스를 제공한다. 따라서, 스마트그리드 사업자에 의해 설치된 스마트그리드 기기들 간 시스템 변화는 거의 유사한 형태를 갖는다.

[0034] 따라서, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 이러한 스마트그리드 기기들의 특성을 활용하여, 시간에 따른 스마트그리드 기기의 시스템 변화 추이를 파악한다. 그리고 탐지의 대상이 되는 스마트그리드 기기에 상응하는 추이 정보와 모델명 또는 제조사 정보 등의 스마트그리드 기기 정보가 동일한 복수개의 스마트그리드 기기들에 상응하는 추이 정보를 상호 비교하여 유사도를 파악한다. 유사도 파악 결과, 유사도가 임계치 미만인 경우, 해당 스마트그리드 기기를 비정상적으로 동작되고 있는 것으로 판단한다.

[0035] 또한, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 특정 보안 침해 사고에 의해 발생된 것으로 파악된 추이 정보와 탐지의 대상이 되는 스마트그리드 기기의 추이 정보를 상호 비교한다.

[0036] 상호 비교 결과, 유사한 정도가 기 설정된 값 이상인 경우, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 해당 보안 침해 사고가 발생한 것으로 판단하거나, 해당 보안 침해 사고가 발생한 것으로 의심할 수 있다.

[0038] 도 2는 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 장치의 구성을 나타낸 블록도이다.

[0039] 도 2와 같이, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 수신부(210), 분석부(220) 및 판단부(230)를 포함한다.

[0040] 먼저, 수신부(210)는 복수의 스마트그리드 기기(100)들로부터 각각 비휘발성 메모리 덤프이미지와 시스템 및 어플리케이션 로그데이터를 포함하는 시스템 변화 정보들을 수신한다.

[0041] 그리고 분석부(220)는 수신된 복수의 시스템 변화 정보들을 분석하여, 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 포함하는 추이 정보를 스마트그리드 기기 별로 생성한다.

[0042] 또한, 분석부(220)는 비휘발성 메모리 덤프이미지를 분석하여 파악된 파일들의 생성 시간, 수정 시간 및 접근 시간 중에서 적어도 하나를 포함하는 시간 정보를 이용하여, 파일 시스템 변화 추이 정보를 생성한다.

[0043] 그리고 분석부(220)는 시스템 및 어플리케이션 로그데이터를 분석하여 파악된 시간 정보를 이용하여, 로그데이터 변화 추이 정보를 생성한다.

[0044] 분석부(220)는 비휘발성 메모리 덤프이미지를 분석하여, 파일들의 생성, 수정, 접근 및 삭제 중에서 적어도 하나의 이벤트가 발생한 시간 및 이벤트의 내용을 분석하거나, 시스템 및 어플리케이션 로그데이터를 분석하여 이벤트가 발생한 시간 및 이벤트의 내용을 분석한다.

[0045] 마지막으로, 판단부(230)는 스마트그리드 기기1(100_1)에 상응하는 제1 추이 정보를 스마트그리드 기기1(100_1)를 제외한 나머지 스마트그리드 기기들에 상응하는 제2 추이 정보와 비교하여, 스마트그리드 기기1(100_1)의 보안 침해 사고 발생 여부를 판단한다.

[0046] 이때, 판단부(230)는 나머지 스마트그리드 기기들로부터 수신된 각각의 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보를 하나의 이벤트로 간주하여, 시간 단위 별 제2 추이 정보를 생성한다.

[0047] 그리고 판단부(230)는 시 단위, 일 단위, 주 단위 및 월 단위 중에서 설정된 시간 단위로 제1 추이 정보와 제2 추이 정보를 비교한다.

[0048] 또한, 판단부(230)는 설정된 상호 비교의 종류에 상응하도록 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 이용하여 제1 추이 정보와 제2 추이 정보를 비교한다.

[0049] 설명의 편의상, 스마트그리드 기기의 침해 사고 탐지 장치(200)가 탐지 대상이 되는 스마트그리드 기기1(100_1)에 상응하는 제1 추이 정보와 나머지 복수의 스마트그리드 기기들에 상응하는 제2 추이 정보를 비교하여, 스마트그리드 기기1(100_1)의 보안 침해 사고 발생 여부를 탐지하는 것으로 설명하였다. 그러나 이에 한정하지 않고, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 복수개의 스마트그리드 기기들에 상응하는 추이 정보들을 이용하여 보안 침해 사고가 발생한 것으로 의심되는 스마트그리드 기기를 검출할 수도 있다.

[0050] 이때, 판단부(230)는 복수의 스마트그리드 기기들로부터 입력된 추이 정보들을 분류 알고리즘을 이용하여 분류하고, 임계치 미만의 수로 분류된 추이 정보에 상응하는 스마트그리드 기기를 보안 침해 사고가 발생한 것으로 판단한다.

[0051] 또한, 판단부(230)는 보안 침해 사고가 발생한 것으로 판단된 스마트그리드 기기에 상응하는 추이 정보와 기 저장된 보안 침해 사고에 상응하는 침해 사고 추이 정보를 비교하여, 유사한 정도를 산출한다. 그리고 유사한 정도가 기 설정된 값 이상인 경우, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 기 저장된 해당 보안 침해 사고가 발생한 것으로 판단하거나, 해당 보안 침해 사고가 발생한 것으로 의심할 수 있다.

[0053] 이하에서는 도 3 및 도 4를 통하여 본 발명의 실시예에 따른 스마트그리드 기기의 침해 사고 탐지 방법에 대하여 더욱 상세하게 설명한다.

[0054] 도 3은 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 방법을 나타낸 동작흐름도이다.

[0055] 먼저, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 복수의 스마트그리드 기기들(100)로부터 시스템 변화 정보를 수신한다(S310).

[0056] 스마트그리드 기기의 침해 사고 탐지 장치(200)는 복수의 스마트그리드 기기들(100)로부터 비휘발성 메모리 덤프이미지, 시스템 및 어플리케이션 로그데이터를 포함하는 시스템 변화 정보를 수신한다.

[0057] 이때, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 시스템 변화 정보를 전송하는 해당 스마트그리드 기기의 식별 정보, 제조사 정보, 모델명 정보 중에서 적어도 하나를 포함하는 스마트그리드 기기 정보를 시스템 변화 정보와 함께 스마트그리드 기기로부터 수신할 수 있다. 또한, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 스마트그리드 기기의 식별 정보, 제조사 정보 및 모델명 정보 등을 기준으로 시스템 변화 정보를 관리하기 위한 데이터베이스 정보를 생성하여 저장할 수 있다.

[0058] 그리고 스마트그리드 기기의 침해 사고 탐지 장치(200)는 수신된 시스템 변화 정보를 분석하여, 추이 정보를 생성한다(S320).

[0059] 스마트그리드 기기의 침해 사고 탐지 장치(200)는 비휘발성 메모리 덤프이미지를 분석하여, 시간별 파일의 생성, 수정, 접근 및 삭제에 상응하는 이벤트를 확인하고, 파일시스템 변화 추이 정보를 생성한다. 이때, 파일시스템 변화 추이 정보는 테이블 형식일 수 있다. 또한, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 비휘발성 메모리 덤프이미지 분석을 통하여, 삭제된 파일을 포함하는 파일들의 생성 시간, 수정 시간 및 접근 시간 정보를 파악하여 파일시스템 변화 추이 정보를 생성할 수 있다.

[0060] 그리고 스마트그리드 기기의 침해 사고 탐지 장치(200)는 시스템 및 어플리케이션 로그데이터를 분석하여, 시간별 시스템 및 어플리케이션 이벤트를 확인하고, 로그데이터 변화 추이 정보를 생성한다. 이때, 로그데이터 변화 추이 정보는 테이블 형식일 수 있다.

[0061] 또한, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 스마트그리드 기기 정보를 기반으로 생성된 추이 정보를 관리할 수 있는 데이터베이스 정보를 생성할 수 있다.

[0062] 마지막으로, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 보안 침해 사고 발생 여부를 판단한다(S330).

[0063] 스마트그리드 기기의 침해 사고 탐지 장치(200)는 스마트그리드 기기1(100_1)에 상응하는 제1 추이 정보를 스마트그리드 기기1(100_1)를 제외한 나머지 스마트그리드 기기들에 상응하는 제2 추이 정보와 비교하여, 스마트그리드 기기1(100_1)의 보안 침해 사고 발생 여부를 판단한다. 이때, 나머지 스마트그리드 기기들은 스마트그리드 기기1(100_1)와 식별 정보, 제조사 정보, 모델명 정보 중에서 적어도 하나가 동일한 것일 수 있다.

[0064] 도 4는 도 3의 S330 단계에서 보안 침해 사고가 발생하였는지 여부를 판단하는 과정을 설명하기 위한 순서도이다.

[0065] 도 4와 같이, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 시간 단위 별 제2 추이 정보를 생성한다(S410).

[0066] 스마트그리드 기기의 침해 사고 탐지 장치(200)는 스마트그리드 기기1(100_1)를 제외한 나머지 스마트그리드 기기들로부터 수신된 각각의 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보를 추이 정보의 내용 구분 없이 하나의 이벤트로 간주하여, 시간 단위 별 제2 추이 정보를 생성한다. 이때, 시간 단위는 분 단위, 시 단위 및 일 단위일 수 있다.

[0067] 그리고 스마트그리드 기기의 침해 사고 탐지 장치(200)는 설정된 시간 단위로 추이 정보를 비교한다(S420).

[0068] 스마트그리드 기기의 침해 사고 탐지 장치(200)는 시 단위, 일 단위, 주 단위, 및 월 단위 중에서 설정된 시간 단위로 제1 추이 정보와 제2 추이 정보를 비교한다.

[0069] 예를 들어, 시 단위 상호 비교로 설정된 경우, 분 단위 별 추이 정보를 활용하고, 일 단위 상호 비교로 설정된 경우, 시 단위 별 추이 정보를 활용하며, 주 단위 또는 월 단위 상호 비교로 설정된 경우 일 단위 별 추이 정보를 활용하여 추이 정보의 상호 비교를 수행할 수 있다.

[0070] 다음으로 스마트그리드 기기의 침해 사고 탐지 장치(200)는 설정된 상호 비교의 종류에 따라 추이 정보를 비교

한다(S430).

[0071] 스마트그리드 기기의 침해 사고 탐지 장치(200)는 설정된 상호 비교의 종류에 상응하도록 파일 시스템 변화 추이 정보 및 로그데이터 변화 추이 정보 중에서 적어도 하나를 이용하여 제1 추이 정보와 제2 추이 정보를 비교한다.

[0072] 상호 비교의 종류는 사용자로부터 설정 받을 수 있으며, 파일 시스템 변화 추이 정보간 비교, 로그데이터 변화 추이 정보간 비교 및 파일 시스템 변화 추이 정보와 로그데이터 변화 추이 정보가 결합된 정보간 비교 중에서 설정된 상호 비교의 종류에 상응하도록 상호 비교를 수행할 수 있다.

[0073] 마지막으로, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 추이 정보를 분류하고, 보안 침해 사고 발생 여부를 판단한다(S440).

[0074] 스마트그리드 기기의 침해 사고 탐지 장치(200)는 복수의 스마트그리드 기기들로부터 입력된 추이 정보들을 분류 알고리즘을 이용하여 분류한다. 그리고 스마트그리드 기기의 침해 사고 탐지 장치(200)는 임계치 미만의 수로 분류된 추이 정보에 상응하는 스마트그리드 기기를 보안 침해 사고가 발생한 것으로 판단한다.

[0075] 또한, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 보안 침해 사고가 발생한 것으로 판단된 스마트그리드 기기에 상응하는 추이 정보와 기 저장된 보안 침해 사고에 상응하는 침해 사고 추이 정보를 비교하여, 유사도를 산출한다.

[0076] 어떠한 스마트그리드 기기에 보안 침해 사고가 발생하였는지 또는 어떠한 스마트그리드 기기가 비정상적으로 동작하고 있는지 여부를 확인하고자 하는 경우, 확인의 대상이 되는 스마트그리드 기기와 스마트그리드 기기 정보가 동일한 복수개의 스마트그리드 기기들로부터 수신된 추이 정보를 입력한다. 그리고 입력된 추이 정보들을 분류 알고리즘을 이용하여 분류한다.

[0077] 이때, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 임계치 미만의 적은 수로 분류된 추이 정보에 상응하는 스마트그리드 기기에 침해 사고 또는 기기 이상이 있는 것으로 판단할 수 있다.

[0078] 또한, 보안 침해 사고가 발생한 것으로 판단된 경우, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 발생한 보안 침해 사고가 기존에 발생한 보안 침해 사고와 동일한 보안 침해 사고인지 여부를 판단한다. 이때, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 특정 보안 침해 사고에 의해 발생된 것으로 파악된 추이 정보와 탐지의 대상이 되는 스마트그리드 기기의 추이 정보를 상호 비교한다.

[0079] 상호 비교 결과, 유사한 정도가 기 설정된 값 이상인 경우, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 탐지의 대상이 되는 스마트그리드 기기에 해당 보안 침해 사고가 발생한 것으로 판단하거나, 해당 보안 침해 사고가 발생한 것으로 의심할 수 있다.

[0081] 이하에서는 도 5 및 도 6을 통하여 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 장치가 생성한 추이 정보에 대하여 더욱 상세하게 설명한다.

[0082] 도 5는 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 장치가 비휘발성 메모리 덤프이미지를 분석한 결과를 나타낸 예시도이다.

[0083] 도 5에 도시한 바와 같이, 스마트그리드 기기의 침해 사고 탐지 장치(200)는 비휘발성 메모리 덤프이미지를 분석하여, 파일들의 생성, 수정, 접근 및 삭제된 이벤트 시간과 해당 이벤트의 내용을 테이블 형식의 데이터베이스 정보로 생성하여 저장할 수 있다.

[0085] 도 6은 본 발명의 일실시예에 따른 스마트그리드 기기의 침해 사고 탐지 장치가 시스템 및 어플리케이션 로그데이터를 분석한 결과를 나타낸 예시도이다.

[0086] 도 6과 같이, 스마그리드 기기의 침해 사고 탐지 장치(200)는 시스템 및 어플리케이션 로그데이터를 분석하여, 이벤트 시간 및 내용을 테이블 형식의 데이터베이스 정보로 생성하여 저장할 수 있다.

[0088] 이상에서와 같이 본 발명에 따른 스마트그리드 기기의 침해사고 탐지 장치 및 방법은 상기한 바와 같이 설명된 실시예들의 구성과 방법이 한정되게 적용될 수 있는 것이 아니라, 상기 실시예들은 다양한 변형이 이루어질 수 있도록 각 실시예들의 전부 또는 일부가 선택적으로 조합되어 구성될 수도 있다.

부호의 설명

[0089] 100: 스마트그리드 기기

200: 스마트그리드 기기의 침해 사고 탐지 장치

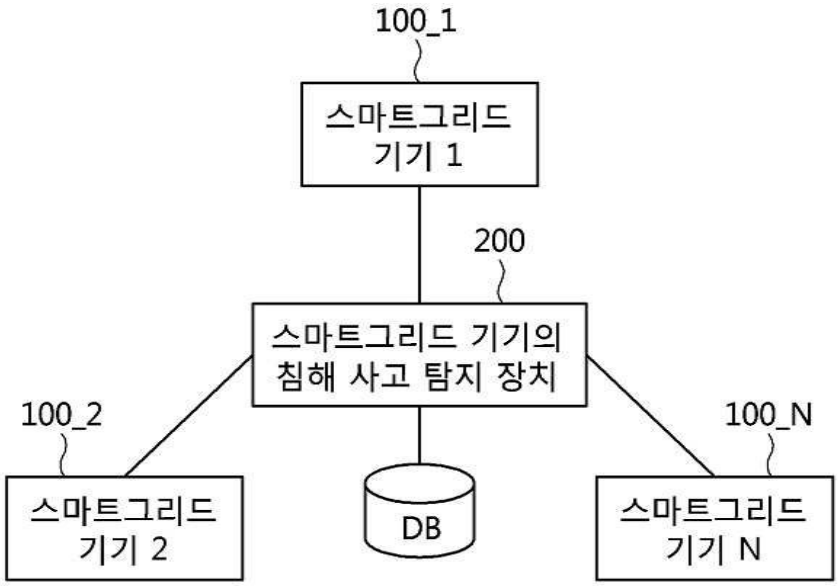
210: 수신부

220: 분석부

230: 판단부

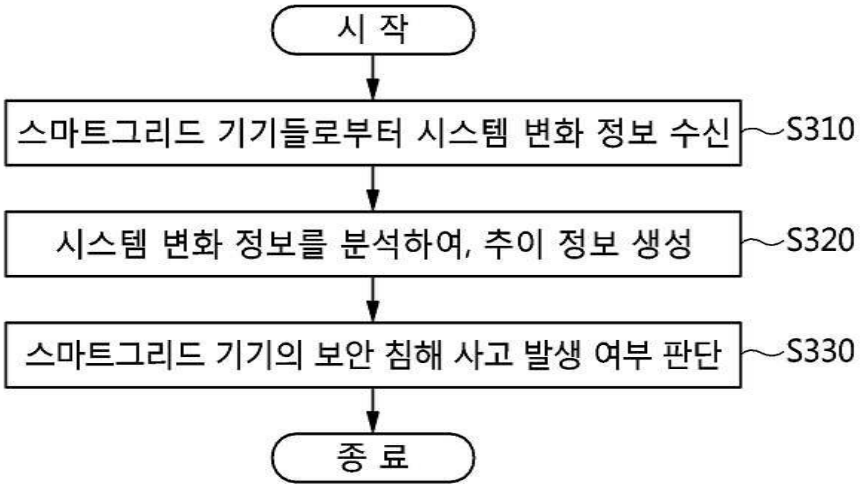
도면

도면1

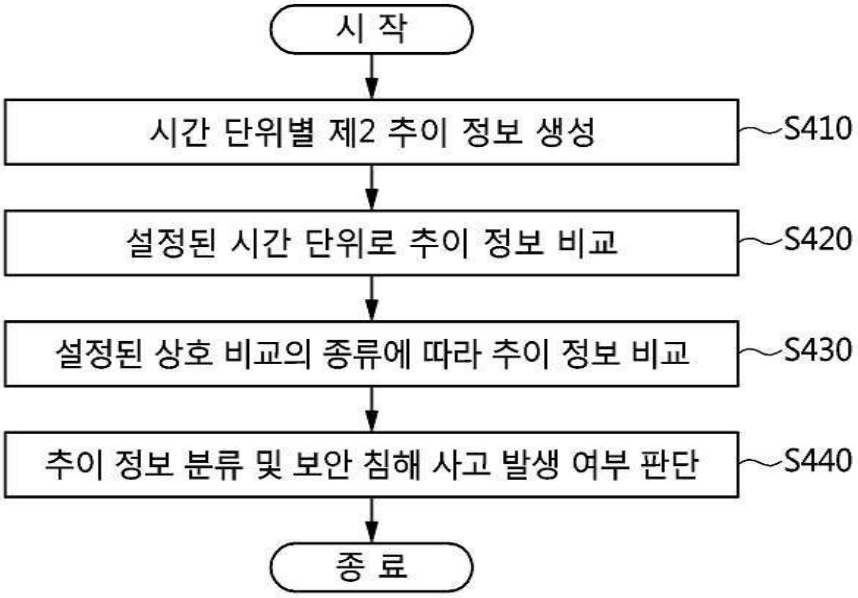


도면2

도면3


시 작
스마트그리드 기기들로부터 시스템 변화 정보 수신
S310
시스템 변화 정보를 분석하여, 추이 정보 생성
S320
스마트그리드 기기의 보안 침해 사고 발생 여부 판단
S330
종 료

도면4


시 작
시간 단위별 제2 추이 정보 생성
S410
설정된 시간 단위로 추이 정보 비교
S420
설정된 상호 비교의 종류에 따라 추이 정보 비교
S430
추이 정보 분류 및 보안 침해 사고 발생 여부 판단
S440
종 료

도면5

시간	이벤트 정보
2015-07-14 00:00:02	create file /bin/ls
2015-07-14 00:01:05	modify file /bin/ls
2015-07-14 01:06:18	access file /tmp/test
2015-07-14 02:09:19	access file /usr/lib/test.lib
2015-07-14 14:45:28	modify file /usr/include/header.h
2015-07-14 21:29:04	access file /lib/lib.so
.	.
.	.
.	.

도면6

시간	이벤트 정보
2015-07-14 00:10:51	sshd connection 192.168.0.1
2015-07-14 02:47:19	dlms packet receiver
2015-07-14 05:07:18	fep packet receiver
2015-07-14 15:46:43	timer dlms packet send
2015-07-14 16:27:18	firmware update request
2015-07-14 20:41:27	ftp connect to server
.	.
.	.
.	.