



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년09월01일

(11) 등록번호 10-1548876

(24) 등록일자 2015년08월25일

(51) 국제특허분류(Int. Cl.)

H04L 12/26 (2006.01) H04L 12/22 (2006.01)

H04L 9/28 (2006.01)

(21) 출원번호 10-2014-0114008

(22) 출원일자 2014년08월29일

심사청구일자 2014년08월29일

(56) 선행기술조사문헌

KR101184160 B1

(73) 특허권자

이화여자대학교 산학협력단

서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)

(72) 발명자

도인실

인천광역시 연수구 센트럴로 194, 201동 2705호(송도동, 더샵 센트럴파크2)

채기준

서울특별시 강남구 강남대로136길 34

(74) 대리인

남정길

전체 청구항 수 : 총 15 항

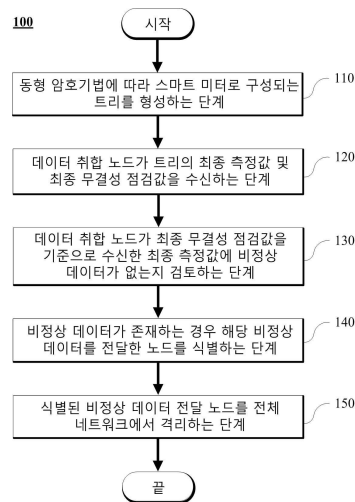
심사관 : 전용혜

(54) 발명의 명칭 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법 및 공격 노드를 식별하는 스마트 그리드 시스템

(57) 요약

스마트 그리드 시스템에서 공격 노드를 식별하는 방법은 루트 노드인 데이터 취합 노드가 소속된 노드들이 동형 암호기법을 사용하여 전달하는 전체 트리의 최종 측정값 및 최종 무결성 점검값을 수신하는 단계, 상기 데이터 취합 노드가 상기 최종 무결성 점검값을 기준으로 수신한 최종 측정값에 비정상 데이터가 있는지 검토하는 단계 및 상기 수신한 최종 측정값에 비정상 데이터가 있는 경우 비정상 데이터를 전달한 노드만 남을때까지 소속된 노드들을 2개의 트리로 분할하고, 분할된 트리의 최종 측정값 및 최종 무결성 점검값을 기준으로 비정상 데이터가 발생한 트리를 선택하는 과정을 반복하는 단계를 포함한다.

대표도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호 2012R1A1A3019459

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)-일반연구자지원사업-여성과학자

연구과제명 사물지능통신(M2M) 응용분야 보안 연구

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2012.05.01 ~ 2015.04.30

특허청구의 범위

청구항 1

루트 노드인 데이터 취합 노드가 소속된 노드들이 동형 암호기법을 사용하여 전달하는 전체 트리의 최종 측정값 및 최종 무결성 점검값을 수신하는 단계;

상기 데이터 취합 노드가 상기 최종 무결성 점검값을 기준으로 수신한 최종 측정값에 비정상 데이터가 없는지 검토하는 단계; 및

상기 수신한 최종 측정값에 비정상 데이터가 있는 경우 상기 비정상 데이터를 전달한 노드만 남을때까지 소속된 노드들을 2개의 서브 트리로 분할하고, 각 서브 트리의 루트 노드가 서브 트리에 소속된 노드들이 동형 암호기법을 사용하여 전달하는 최종 무결성 점검값을 기준으로 상기 소속된 서브 트리의 최종 측정값에 비정상 데이터가 없는지 판단하고, 비정상 데이터가 발생한 서브 트리를 선택하는 과정을 반복하는 단계; 및

상기 트리 분할과정에서 비정상 데이터가 없다고 판단되는 트리를 하나의 트리으로 병합하는 단계를 포함하는 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법.

청구항 2

제1항에 있어서,

상기 소속된 노드는 각각 아래의 수식을 이용하여 무결성 점검값을 연산하여 상위 노드에게 전달하는 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법.

$$Z_i = P_i + (X \times \text{count } i) \pmod{r}$$

(여기서, P_i 는 각 노드에서의 측정값, i 는 각 노드의 ID, $\text{count } i$ 는 연결된 하위 레벨의 총 노드 수, r 은 최대 전력 $\times$ 총 노드 수보다 큰 임의의 자연수, X 는 r 보다 크면서 r 의 배수가 아닌 자연수임)

청구항 3

제2항에 있어서,

상기 데이터 취합 노드는 상기 최종 측정값에서 각 노드의 측정값(P_i)을 복호하여

$\sum P_i + (X \times \sum \text{count } i) \pmod{r}$ 에 대입한 결과값과 상기 최종 무결성 점검값 ($\sum Z_i$)이 동일한지를 비교하여 상기 최종 측정값에 비정상 데이터가 없는지 검토하는 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법.

청구항 4

제1항에 있어서,

상기 트리는 너비 우선 탐색(BFS) 방법으로 구성되는 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법.

청구항 5

제1항에 있어서,

상기 데이터 취합 노드가 상기 비정상 데이터가 발생한 노드를 식별하면 상기 식별한 노드를 제외한 나머지 소속된 노드들로부터 최종 측정값을 수신하는 단계를 더 포함하는 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법.

청구항 6

제1항에 있어서,

상기 소속된 노드들은 복수의 스마트 미터이고 상기 데이터 취합 노드는 상기 복수의 스마트 미터 중 하나이거나, 상기 소속된 노드들은 복수의 스마트 미터이고 상기 데이터 취합 노드는 제어 서버인 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법.

청구항 7

스마트 그리드 시스템에 있어서,

복수의 건물 또는 복수의 구역에 배치된 전력 소비 장치;

상기 건물 또는 상기 구역 별로 상기 전력 소비 장치의 전력 소비량을 측정하는 복수의 스마트 미터 장치; 및

동형 암호기법을 사용하는 상기 복수의 스마트 미터 장치가 너비 우선 탐색(BFS) 트리를 형성하여 전달하는 최종 측정값 및 최종 무결성 점검값을 수신하고, 상기 최종 측정값 및 상기 최종 무결성 점검값을 기준으로 상기 복수의 스마트 미터 장치 중 비정상 데이터를 전달한 스마트 미터를 식별하는 제어 서버를 포함하되,

상기 제어 서버는 상기 수신한 최종 측정값에 비정상 데이터가 있는 경우 비정상 데이터를 전달한 스마트 미터가 남을때까지 상기 복수의 스마트 미터 장치가 형성한 트리를 2개의 트리로 분할하고, 각 트리의 루트 노드가 소속된 노드들이 동형 암호기법을 사용하여 전달하는 분할된 트리의 최종 측정값 및 최종 무결성 점검값을 기준으로 비정상 데이터가 발생하였는지 판단하고, 비정상 데이터가 발생한 트리를 선택하는 과정을 반복하는 공격 노드를 식별하는 스마트 그리드 시스템.

청구항 8

삭제

청구항 9

제7항에 있어서,

상기 스마트 미터는 각각 아래의 수식을 이용하여 무결성 점검값을 연산하여 상기 트리에서 상위 스마트 미터에게 전달하는 공격 노드를 식별하는 스마트 그리드 시스템.

$$Z_i = P_i + (X \times \text{count } i) \pmod{r}$$

(여기서, P_i 는 각 노드에서의 측정값, i 는 각 노드의 ID, $\text{count } i$ 는 연결된 하위 레벨의 총 노드 수, r 은 최대 전력 $\times$ 총 노드 수보다 큰 임의의 자연수, X 는 r 보다 크면서 r 의 배수가 아닌 자연수임)

청구항 10

제9항에 있어서,

상기 제어 서버는

상기 최종 측정값에서 각 스마트 미터의 측정값(P_i)을 복호하여

$\sum P_i + (X \times \sum \text{count } i) \pmod{r}$ 에 대입한 결과값과 상기 최종 무결성 점검값($\sum Z_i$)이 동일한지 않으면 상기 최종 측정값에 비정상 데이터가 있다고 판단하는 공격 노드를 식별하는 스마트 그리드 시스템.

청구항 11

제7항에 있어서,

상기 제어 서버는

상기 비정상 데이터를 전달한 스마트 미터를 식별하면, 상기 식별한 스마트 미터를 제외한 나머지 스마트 미터로부터 최종 측정값을 수신하는 공격 노드를 식별하는 스마트 그리드 시스템.

청구항 12

제7항에 있어서,

상기 제어 서버는

상기 최종 측정값과 상기 최종 무결성 점검값을 이용하여 상기 최종 측정값에 비정상 데이터가 포함되었다고 판단하면 실패 카운트를 증가시키고, 상기 실패 카운트가 기준값을 초과하는 경우에 상기 비정상 데이터가 발생한 트리를 선택하는 과정을 반복하는 공격 노드를 식별하는 스마트 그리드 시스템.

청구항 13

제7항에 있어서,

상기 제어 서버는 상기 복수의 스마트 미터 장치를 복수의 그룹에 분할 배치하고, 상기 그룹마다 상기 그룹에 배치된 스마트 미터 장치 중 각 그룹의 정보를 취합하여 전달하는 그룹 스마트 미터를 선정하여 상기 그룹별로 최종 측정값 및 최종 무결성 점검값을 전달받는 공격 노드를 식별하는 스마트 그리드 시스템.

청구항 14

제13항에 있어서,

상기 제어 서버는

상기 그룹 스마트 미터로 트리를 형성하고, 상기 그룹 스마트 미터로부터 수신한 최종 측정값에 비정상 데이터가 있는 경우 비정상 데이터를 전달한 그룹 스마트 미터가 남을때까지 상기 트리를 2개의 트리로 분할하고, 분할된 트리의 최종 측정값 및 최종 무결성 점검값을 기준으로 비정상 데이터가 발생한 트리를 선택하는 과정을 반복하고, 최종적으로 상기 비정상 데이터를 전달한 그룹 스마트 미터를 제외한 나머지 그룹 스마트 미터로부터 최종 측정값을 수신하는 공격 노드를 식별하는 스마트 그리드 시스템.

청구항 15

제14항에 있어서,

상기 제어 서버는

상기 그룹 스마트 미터로부터 수신하는 상기 최종 측정값과 상기 최종 무결성 점검값을 이용하여 상기 최종 측정값에 비정상 데이터가 포함되었다고 판단하면 실패 카운트를 증가시키고, 상기 실패 카운트가 기준값을 초과하는 경우에 상기 비정상 데이터가 발생한 트리를 선택하는 과정을 반복하여 최종적으로 상기 비정상 데이터를 전달한 그룹 스마트 미터를 식별하는 공격 노드를 식별하는 스마트 그리드 시스템.

청구항 16

제14항에 있어서,

상기 제어 서버는

상기 그룹 스마트 미터로부터 수신하는 상기 최종 측정값과 상기 최종 무결성 점검값을 이용하여 상기 최종 측정값에 비정상 데이터가 있다고 판단하면 실패 카운트를 증가시키고, 상기 최종 측정값에 비정상 데이터가 없다고 판단하면 성공 카운트 증가시키되,

상기 실패 카운트가 기준값을 초과하면서 상기 실패 카운트와 상기 성공 카운트의 비율이 기준 비율값을 초과하는 경우 상기 그룹 스마트 미터로 구성되는 트리 또는 상기 그룹을 구성하는 스마트 미터로 구성되는 트리 중 적어도 하나의 토폴로지를 변경하는 공격 노드를 식별하는 스마트 그리드 시스템.

명세서

기술 분야

이하 설명하는 기술은 스마트 그리드 시스템에서 비정상 데이터를 전달하는 노드를 식별하는 방법 및 스마트 그리드 시스템에 관한 것이다.

[0001]

배경 기술

- [0002] 스마트 그리드(smart grid)는 기존의 전력 망에 정보통신 기술을 접목하여 전력 공급자와 소비자가 양 방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 지능형 전력 망이다.
- [0003] 스마트그리드에서 수집된 정보는 소비자의 개인 정보를 크게 해칠 우려가 있기 때문에 각 가정의 스마트 미터기(smart meter)로부터 최종 게이트웨이까지의 안전한 전송이 보장되어야 한다.
- [0004] 이를 위해 사용되는 기법 중 동형 암호기법(homomorphic encryption)은 평문(plaintext)에 대한 특정 연산이 암호문(ciphertext)에 대한 연산에 의해 수행 되는 특징을 가지고 있다. 이에 따라 중간 과정에서 평문이 직접적으로 드러나지 않게 되므로 기밀성을 보장하기 위한 안전한 암호화 방식이라고 볼 수 있다. 널리 알려진 동형 암호기법으로는 RSA, EL Gamal, Paillier, Naccache-Stern, Boneh-Goh-Nissim (BGN), 등이 존재한다.
- [0005] 한편 스마트 미터가 전달하는 데이터 자체가 제3자의 공격에 의해 위조 또는 변조된 것인지 여부를 판단하기 위한 방법으로 각 노드로부터 별도의 정보를 전달하여 위변조를 판단하는 무결성 검증 방법이 제안되었다.

선행기술문헌

비특허문헌

- [0006] (비특허문헌 0001) 박지혜, 최경, 도인실, 채기준, "무결성 검증을 통한 Homomorphic 방식의 안전한 데이터 aggregation", 제34회 한국정보처리학회 추계학술발표대회 논문집 제17권 제2호(2010.11)

발명의 내용

해결하려는 과제

- [0007] 전술한 무결성 검증 방법은 스마트 미터로부터 비정상 데이터가 전달되는지 여부만을 판단하는 것이다. 특히 네트워크 공격이 지속적으로 위조 또는 변조된 데이터를 전달하는 경우 스마트 그리드 시스템은 상당히 많은 자원을 위조 또는 변조되었는지 여부를 판단하는데 사용하게 되고, 최악의 경우에는 시스템이 정상적인 작동을 하지 못하는 문제가 발생할 수 있다. 이러한 공격을 소위 DoS(Denial of Service)라고 한다.
- [0008] 이하 설명하는 기술은 상기 무결성 검증 기법을 사용하는 스마트 그리드 시스템에서 비정상 데이터를 전달하는 노드를 식별하여 공격당한 노드를 네트워크에서 격리시키고자 하는 것이다.
- [0009] 이하 설명하는 기술은 스마트 그리드 시스템이 공격당한 정도에 따라 공격당한 노드를 격리하거나, 스마트 미터로 구성되는 네트워크 토폴로지를 변경하는 방법에 관한 것이다.
- [0010] 이하 설명하는 기술의 해결과제는 이상에서 언급된 것들에 한정되지 않으며, 언급되지 아니한 다른 해결과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0011] 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법은 루트 노드인 데이터 취합 노드가 소속된 노드들이 동형 암호기법을 사용하여 전달하는 전체 트리의 최종 측정값 및 최종 무결성 점검값을 수신하는 단계, 데이터 취합 노드가 최종 무결성 점검값을 기준으로 수신한 최종 측정값에 비정상 데이터가 있는지 검토하는 단계 및 수신한 최종 측정값에 비정상 데이터가 있는 경우 비정상 데이터를 전달한 노드만 남을 때까지 소속된 노드들을 2개의 트리로 분할하고, 분할된 트리의 최종 측정값 및 최종 무결성 점검값을 기준으로 비정상 데이터가 발생한 트리를 선택하는 과정을 반복하는 단계를 포함한다.
- [0012] 스마트 그리드 시스템은 복수의 건물 또는 복수의 구역에 배치된 전력 소비 장치, 건물 또는 구역 별로 전력 소비 장치의 전력 소비량을 측정하는 복수의 스마트 미터 장치 및 동형 암호기법을 사용하는 복수의 스마트 미터 장치가 너비 우선 탐색(BFS) 트리를 형성하여 전달하는 최종 측정값 및 최종 무결성 점검값을 수신하고, 최종 측정값 및 최종 무결성 점검값을 기준으로 복수의 스마트 미터 장치 중 비정상 데이터를 전달한 스마트 미터를 식별하는 제어 서버를 포함한다.
- [0013] 제어 서버는 수신한 최종 측정값에 비정상 데이터가 있는 경우 비정상 데이터를 전달한 스마트 미터가 남을때까

지 복수의 스마트 미터 장치가 형성한 트리를 2개의 트리로 분할하고, 분할된 트리의 최종 측정값 및 최종 무결성 점검값을 기준으로 비정상 데이터가 발생한 트리를 선택하는 과정을 반복할 수 있다.

[0014] 제어 서버는 비정상 데이터를 전달한 스마트 미터를 식별하면, 식별한 스마트 미터를 제외한 나머지 스마트 미터로부터 최종 측정값을 계속 수신할 수 있다.

[0015] 제어 서버는 최종 측정값과 최종 무결성 점검값을 이용하여 최종 측정값에 비정상 데이터가 포함되었다고 판단하면 실패 카운트를 증가시키고, 실패 카운트가 기준값을 초과하는 경우에 비정상 데이터가 발생한 트리를 선택하는 과정을 반복할 수 있다.

[0016] 제어 서버는 복수의 스마트 미터 장치를 복수의 그룹에 분할 배치하고, 그룹마다 그룹에 배치된 스마트 미터 장치 중 각 그룹을 정보를 취합하여 전달하는 그룹 스마트 미터를 선정하여 그룹별로 최종 측정값 및 최종 무결성 점검값을 전달받을 수 있다.

[0017] 제어 서버는 그룹 스마트 미터로 트리를 형성하고, 그룹 스마트 미터로부터 수신한 최종 측정값에 비정상 데이터가 있는 경우 비정상 데이터를 전달한 그룹 스마트 미터가 남을때까지 트리를 2개의 트리로 분할하고, 분할된 트리의 최종 측정값 및 최종 무결성 점검값을 기준으로 비정상 데이터가 발생한 트리를 선택하는 과정을 반복하고, 최종적으로 비정상 데이터를 전달한 그룹 스마트 미터를 제외한 나머지 그룹 스마트 미터로부터 최종 측정값을 수신할 수 있다.

[0018] 제어 서버는 그룹 스마트 미터로부터 수신하는 최종 측정값과 최종 무결성 점검값을 이용하여 최종 측정값에 비정상 데이터가 포함되었다고 판단하면 실패 카운트를 증가시키고, 실패 카운트가 기준값을 초과하는 경우에 비정상 데이터가 발생한 트리를 선택하는 과정을 반복하여 최종적으로 비정상 데이터를 전달한 그룹 스마트 미터를 식별할 수 있다.

[0019] 제어 서버는 그룹 스마트 미터로부터 수신하는 최종 측정값과 최종 무결성 점검값을 이용하여 최종 측정값에 비정상 데이터가 있다고 판단하면 실패 카운트를 증가시키고, 최종 측정값에 비정상 데이터가 없다고 판단하면 성공 카운트 증가시키되, 실패 카운트가 기준값을 초과하면서 실패 카운트와 성공 카운트의 비율이 기준 비율값을 초과하는 경우 그룹 스마트 미터로 구성되는 트리 또는 그룹을 구성하는 스마트 미터로 구성되는 트리 중 적어도 하나의 토폴로지를 변경할 수 있다.

발명의 효과

[0020] 이하 설명하는 기술은 스마트 그리드 시스템에서 공격 당한 노드를 손쉽게 식별하고 격리하여 DoS 공격에 강인한 시스템을 제공한다.

[0021] 이하 설명하는 기술의 효과는 이상에서 언급된 것들에 한정되지 않으며, 언급되지 아니한 다른 효과들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0022] 도 1은 동형 암호기법을 사용하는 스마트 그리드 시스템에서 데이터 무결성을 판단하기 위한 정보의 흐름을 도시한 트리이다.

도 2는 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법에 대한 순서도의 예이다.

도 3은 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법에서 트리를 분할하여 공격 노드를 식별하는 과정을 예시한 도면이다.

도 4는 스마트 그리드 시스템의 구조를 도시한 블록도의 예이다.

도 5는 스마트 그리드 시스템의 계층적인 구조를 도시한 블록도의 다른 예이다.

발명을 실시하기 위한 구체적인 내용

[0023] 이하 설명하는 기술은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 이하 설명하는 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 이하 설명하는 기술의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하

는 것으로 이해되어야 한다.

- [0024] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어들에 의해 한정되지는 않으며, 단지 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 이하 설명하는 기술의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.
- [0025] 본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함한다" 등의 용어는 실시된 특징, 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 의미하는 것이지, 하나 또는 그 이상의 다른 특징들이나 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하지 않는 것으로 이해되어야 한다.
- [0026] 도면에 대한 상세한 설명을 하기에 앞서, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다. 따라서, 본 명세서를 통해 설명되는 각 구성부들의 존재 여부는 기능적으로 해석되어야 할 것이며, 이러한 이유로 이하 설명하는 기술의 스마트 그리드 시스템(100)에 따른 구성부들의 구성은 이하 설명하는 기술의 목적을 달성할 수 있는 한도 내에서 대응하는 도면과는 상이해질 수 있음을 명확히 밝혀둔다.
- [0027] 또, 방법 또는 동작 방법을 수행함에 있어서, 상기 방법을 이루는 각 과정들은 문맥상 명백하게 특정 순서를 기재하지 않은 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 과정들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.
- [0028] 먼저 동형 암호기법(Homomorphic encryption)을 사용하는 스마트 그리드 시스템에서 데이터 무결성을 판단하는 방법에 대해 살펴보려고 한다. 자세한 내용은 박지혜, 최경, 도인실, 채기준, "무결성 검증을 통한 Homomorphic 방식의 안전한 데이터 aggregation", 제34회 한국정보처리학회 추계학술발표대회 논문집 제17권 제2호(2010.11)』에 설명되어 있다.
- [0029] 동형 암호기법의 원리에 의해, 중간 노드에서 평문의 노출이 발생하지 않으므로 기밀성이 보장 될 수 있다. 하지만 악의적인 공격을 통해 실제 값과 다른 평문으로 복호화 되도록 변조된 암호문을 생성하는 것이 가능하다. 그 결과, 최종적으로 데이터 수집자에게 정확하지 않은 데이터 수집(aggregation) 결과가 전송된다. 이에 변조 여부를 확인하는 기법이 필요한 것이다.
- [0030] 무결성 검증 기법은 트리를 구성하는 각 노드가 측정값 외에 무결성 검증을 위한 추가적인 정보를 전달하는 것을 전제로 한다. 여기서 트리를 구성하는 노드는 전기 장치의 전력 소비량을 측정하는 스마트 미터에 해당할 것이다.
- [0031] 도 1은 동형 암호기법을 사용하는 스마트 그리드 시스템에서 데이터 무결성을 판단하기 위한 정보의 흐름을 도시한 트리이다.
- [0032] 스마트 그리드 시스템에서 동형 암호기법은 일반적으로 스마트 미터를 너비 우선 트리(BFS)로 구성하여 각 스마트 미터가 측정한 데이터를 상위 노드로 전달하는 방식을 갖는다. 도 1에서 C 값이 각 스마트 미터가 측정한 측정값에 해당한다. 도 1을 살펴보면 자식 노드에서 부모 노드로 자신이 측정한 C값을 전달하고, 자식 노드의 측정값을 받은 부모 노드는 C값을 곱한 값에 자신의 C값을 곱하여 전달하는 것을 알 수 있다. 예컨대, 도 1에서 루트 노드에 해당하는 데이터 취합 노드(A)가 획득하는 최종 측정값은 $C_1 * C_2 * C_3 * C_4 * C_5 * C_6 * C_7 * C_8 * C_9$ 에 해당한다.
- [0033] 최종 측정값에 대한 무결성 검토를 위해 각 노드는 무결성 점검값을 측정값과 동시에 상위 노드로 전달한다. 무결성 점검값은 아래의 수학적 식 1을 이용하여 각 노드가 연산하여, 상위 노드는 전달받은 무결성 점검값을 합산하여 전달하게 된다. 결국 데이터 취합 노드(A)가 획득하는 최종 무결성 점검값은 $Z_1 + Z_2 + Z_3 + Z_4 + Z_5 + Z_6 + Z_7$

+ $Z_8 + Z_9$ 에 해당한다. 최종 무결성 점검값은 $\sum Z_i$ 이다.

수학식 1

$$Z_i = P_i + (X \times \text{count } i) \pmod{r}$$

여기서, P_i 는 각 노드에서의 측정값, i 는 각 노드의 ID, $\text{count } i$ 는 연결된 하위 레벨의 총 노드 수, r 은 최대전력 $\times$ 총 노드 수보다 큰 임의의 자연수, X 는 r 보다 크면서 r 의 배수가 아닌 자연수에 해당한다.

r 값은 트리 구성 시 마다 측정값을 취합하는 데이터 취합 노드 또는 별도의 제어 장치가 설정할 수 있다. count 값은 트리 구성 시 모두 0으로 초기화 되어있다. 부모 노드에게 1 증가 시킨 값을 전송하며, 부모노드는 자식 노드들로부터 받은 count 값들을 합하여 자신의 count 값을 갱신한 후, 자신의 부모노드로 전송한다.

한편 $\sum Z_i$ 를 Z_n 이라고 하면, 최종 무결성 점검값은 아래의 수학식 2와 같이 풀이될 수 있다.

수학식 2

$$\begin{aligned} Z_n &= P_1 + X * \text{count } 1 \pmod{r} \\ &\quad + P_2 + X * \text{count } 2 \pmod{r} \\ &\quad + P_3 + X * \text{count } 3 \pmod{r} \\ &\quad \dots \\ &\quad + P_n + X * \text{count } n \pmod{r} \\ &= (P_1 + P_2 + P_3 + P_4 \dots + P_n) + (X * \sum \text{count } i) \pmod{r} \end{aligned}$$

한편 각 노드로부터 최종 측정값을 취합하는 데이터 취합 노드는 자신이 수신한 최종 측정값을 복호하여 각 노드가 측정한 측정값(P_i)을 복호할 수 있다.

데이터 취합 노드는 최종 측정값에서 각 노드의 측정값(P_i)을 복호하여 아래의 수학식 3에 대입한 결과값을 최종 무결성 점검값($\sum Z_i$)과 비교하여 최종 측정값에 비정상 데이터가 없는지 여부를 판단할 수 있다.

수학식 3

$$\sum P_i + (X \times \sum \text{count } i) \pmod{r}$$

이하에서는 도면을 참조하면서 상기 무결성 검증 기법을 응용하여 스마트 그리드 시스템에서 공격 노드를 식별

하는 방법(100) 및 스마트 그리드 시스템(200,300)에 관하여 구체적으로 설명하겠다.

- [0043] 도 2는 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법(100)에 대한 순서도의 예이다.
- [0044] 데이터 취합 노드 또는 제어 장치는 먼저 복수의 스마트 미터로 구성되는 트리를 형성한다(110).
- [0045] 이후 루트 노드인 데이터 취합 노드가 소속된 노드들이 동형 암호기법을 사용하여 전달하는 전체 트리의 최종 측정값 및 최종 무결성 점검값을 수신한다(120). 데이터 취합 노드가 최종 무결성 점검값을 기준으로 수신한 최종 측정값에 비정상 데이터가 없는지 검토한다(130).
- [0046] 수신한 최종 측정값에 비정상 데이터가 있는 경우 해당 비정상 데이터를 전달(생성)한 노드를 식별하게 된다(140). 이후 비정상 데이터를 전달한 노드를 전체 네트워크에서 격리하여 더 이상 잘못된 데이터가 전달되지 않도록 할 수 있다(150).
- [0047] 상기 120 단계 및 130 단계는 도 1과 관련하여 전술한 무결성 검증 단계에 해당한다.
- [0048] 데이터 취합 노드가 무결성 검증을 수행한 결과 수신한 최종 측정값에 오류가 있다고 판단하는 경우 비정상 데이터를 전달한 노드를 식별하는 과정(140)을 수행하게 된다.
- [0049] 비정상 데이터를 식별하는 과정은 비정상 데이터를 전달한 노드만 남을때까지 트리를 2개로 분할하고, 분할된 트리 각각의 최종 측정값 및 최종 무결성 점검값을 기준으로 비정상 데이터가 발생한 트리를 선택하는 과정을 반복하는 과정을 거치게 된다. 이하 도 3을 기준으로 구체적으로 설명한다.
- [0050] 도 3은 동형 암호기법을 사용하는 스마트 그리드 시스템에서 공격 노드를 식별하는 방법에서 트리를 분할하여 공격 노드를 식별하는 과정을 예시한 도면이다. 도 3에서는 트리 구조를 도시하지 않았으나 각 그룹에 속한 노드들은 기본적으로 트리 구조를 갖는다.
- [0051] 도 3(a)는 데이터 취합 노드(A)가 최종 측정값에 비정상 데이터가 포함되었다고 판단하여 전체 트리를 2개의 트리로 분할한 단계이다. 이때 각 그룹에 포함된 노드는 트리 구조를 갖고 각 트리에 대한 최종 측정값 및 최종 무결성 점검값을 재차 연산한다. 이때 측정값 및 무결성 점검값을 노드로부터 다시 받을 필요는 없을 것이고, 데이터 취합 노드가 수신한 전체 트리에 대한 최종 측정값 및 최종 무결성 점검값을 복호하여 분할된 트리에 대한 최종 측정값 및 최종 무결성 점검값을 산출할 수 있을 것이다.
- [0052] 도 3(a)의 우측 트리(그룹)의 최종 무결성 점검값에는 이상이 없었으나, 도 3(a)의 좌측 트리의 최종 무결성 점검값에는 오류가 있는 것으로 판단되었다. 이에 데이터 취합 노드는 좌측 트리를 다시 2개의 트리로 분할하였다(도 3(b)). 이후 도 3(b)의 좌측 2개의 분할된 그룹을 트리로 구성하고, 각 그룹에 포함된 트리에 대한 최종 측정값 및 최종 무결성 점검값을 산출한다.
- [0053] 분할된 그룹에서 다시 무결성 점검값에 오류가 나타난 그룹은 재차 분할하여 도 5(d)와 같은 상태가 되었고, 최종적으로 도 5(e)에서는 하나의 노드가 검출된 상태이다.
- [0054] 상기 과정에서 이상이 없는 정상 노드가 속한 그룹은 이후 통신을 위해 다시 하나의 트리로 병합하는 과정이 필요할 수 있다. 병합 과정은 최종적인 오류 노드가 검출된 후에 할 수 도 있고, 도 3과 같이 각 단계에서 수행할 수도 있을 것이다. 병합 과정도 BFS 트리를 구성하는 과정에 해당할 것이다.
- [0055] 이제 데이터 취합 노드는 오류 데이터(위조 또는 변조 데이터)를 전달하는 노드를 격리한 상태에서 다른 노드로부터 측정값을 전달받아 정상적인 동작이 가능하게 되었다.
- [0056] 이제 전술한 오류 데이터를 전달 내지 생성하는 노드를 식별하는 스마트 그리드 시스템(200, 300)에 대해 설명하기로 한다.
- [0057]
- [0058] 도 4는 스마트 그리드 시스템(200)의 구조를 도시한 블록도의 예이다.
- [0059] 스마트 그리드 시스템(200)은 복수의 건물 또는 복수의 구역에 배치된 전력 소비 장치(50), 건물 또는 구역 별로 전력 소비 장치의 전력 소비량을 측정하는 복수의 스마트 미터 장치(210) 및 동형 암호기법을 사용하는 복수

의 스마트 미터 장치가 너비 우선 탐색(BFS) 트리를 형성하여 전달하는 최종 측정값 및 최종 무결성 점검값을 수신하고, 최종 측정값 및 최종 무결성 점검값을 기준으로 복수의 스마트 미터 장치 중 비정상 데이터를 전달한 스마트 미터를 식별하는 제어 서버(240)를 포함한다.

- [0060] 도 4의 좌측에는 전력 소비 장치(50)가 배치된 건물들을 도시하였다. 이중 중앙에 위치한 건물에 전력 소비 장치(50) 및 스마트 미터 장치(210)를 모두 도시하였고, 나머지 건물에서는 전력 소비 장치(50)를 제외하고 스마트 미터 장치(210)만을 도시하였다. 그러나 각 건물에는 적어도 하나 이상의 전력 소비 장치(50)가 배치된 상태이다. 전력 소비 장치(50)는 가정인 경우 TV, 에어컨, 냉장고 등과 같은 가전 제품을 포함하고, 공장인 경우 각종 기계 장치를 포함하고, 사무실인 경우 컴퓨터, 조명 장치, 냉난방 장치 등을 포함한다. 한편 전력 소비 장치(50)는 특정 건물의 특정 구역별로 하나의 스마트 미터가 사용될 수도 있고, 특정 건물이 아닌 특정 구역(지역)에 배치된 전력 소비 장치(50)가 사용한 전력량을 측정하기 위한 스마트 미터가 사용될 수도 있다.
- [0061] 스마트 미터(210)가 측정한 측정값은 데이터 취합 장치를 거쳐 제어 서버(240)에 전달된다. 한편 별도의 데이터 취합 장치를 사용하지 않고 측정값들이 제어 서버(240)에 전달될 수도 있을 것이다. 도 4에서는 데이터 취합 장치를 별도로 도시하지 않았고, 각 스마트 미터(210)가 측정한 측정값이 공유하는 게이트웨이(220)를 도시하였다. 물론 게이트웨이(220)가 모든 스마트 미터(210)가 측정한 측정값을 취합하는 장치일 수도 있을 것이다.
- [0062] 유틸리티 시스템(230)은 스마트 미터(210)와 함께 전력 소비 장치(50)의 전력 사용을 제어하는 기능을 수행하는 장치이다. 유틸리티 시스템(230)은 스마트 미터(210)에서 측정하는 통계치를 관리할 수도 있고, 각 건물의 전력 비용을 정산하는 역할을 수행할 수도 있다.
- [0063] 제어 서버(240)는 본 발명에서 핵심적인 제어의 역할을 수행하는 구성이다. 제어 서버는 각 스마트 미터(210)가 측정한 측정값에 오류가 있는지 여부를 판단하고, 오류가 있는 스마트 미터(210)를 네트워크에서 격리하거나 네트워크 토폴로지를 변경하는 기능을 수행한다. 한편 제어 서버(240)는 유틸리티 시스템(230)에 오류가 발생한 스마트 미터를 통보하거나 일정한 명령을 전달할 수도 있을 것이다.
- [0064] 도 4에서는 예시적으로 3개의 스마트 미터(210)만을 도시하였으나 실제 이보다 훨씬 많은 스마트 미터가 사용된다. 도 2 및 도 3에서 설명한 바와 같이, 스마트 미터(210)는 데이터를 생성하는 하나의 노드에 해당하고, 데이터를 취합하는 장치 또는 제어 서버(240)는 자신이 관할하는 모든 스마트 미터를 BFS 트리로 구성하고, 최종 측정값 및 최종 무결성 점검값을 수신하게 된다.
- [0065] 제어 서버(240)는 수신한 최종 측정값에 비정상 데이터가 있는 경우 비정상 데이터를 전달한 스마트 미터가 남을때까지 복수의 스마트 미터 장치가 형성한 트리를 2개의 트리로 분할하고, 분할된 트리의 최종 측정값 및 최종 무결성 점검값을 기준으로 비정상 데이터가 발생한 트리를 선택하는 과정을 반복수행한다.
- [0066] 제어 서버(240)가 비정상 데이터를 전달한 스마트 미터를 식별하는 과정 및 해당 스마트 미터를 네트워크에서 격리하는 과정은 도 2 및 도 3에서 설명한 과정과 같다.
- [0067] 한편 제어 서버(240)는 어떤 스마트 미터가 비정상 데이터를 전달했다고 해서 곧바로 해당 스마트 미터를 격리시키기 보다는 일정한 시간 해당 스마트 미터를 모니터링하는 것이 바람직할 수 있다. 네트워크 공격자의 공격이 아닌 기기 오류로 인한 비정상 데이터가 전달될 수도 있고, 전체 스마트 그리드 시스템의 동작을 방해할 정도의 부하가 아니라면 해당 스마트 미터를 지속적으로 모니터링하는 것이 보다 바람직할 것이다.
- [0068] 따라서 제어 서버(240)는 최종 측정값과 최종 무결성 점검값을 이용하여 최종 측정값에 비정상 데이터가 포함되었다고 판단하면 실패 카운트를 증가시키고, 실패 카운트가 기준값을 초과하는 경우에 비정상 데이터가 발생한 스마트 미터를 식별하는 과정을 수행할 수 있다.
- [0069] 도 5는 스마트 그리드 시스템(300)의 계층적인 구조를 도시한 블록도의 다른 예이다. 도 5는 도 4와 달리 스마트 미터(310)가 계층적으로 구성되어 있고, 보다 큰 지역에 걸쳐 일정한 그룹에 스마트 미터(310)가 배치되어 있다. 하위 계층 스마트 미터로 표시한 박스에는 4개의 스마트 미터 그룹을 도시하였다. 각 그룹에서 예시적으로 몇 개의 스마트 미터(310)에 대해서만 도면 부호를 부여하였다. 도 5에서 도시하지 않았지만 각 스마트 미터(310)는 전력 소비 장치와 연결되어 전력 소비량을 측정하게 된다. 도 5에서 도시한 그룹은 하나의 대형 건물일 수도 있고, 큰 지역을 일정한 구역에 따라 구분한 것일 수도 있다.

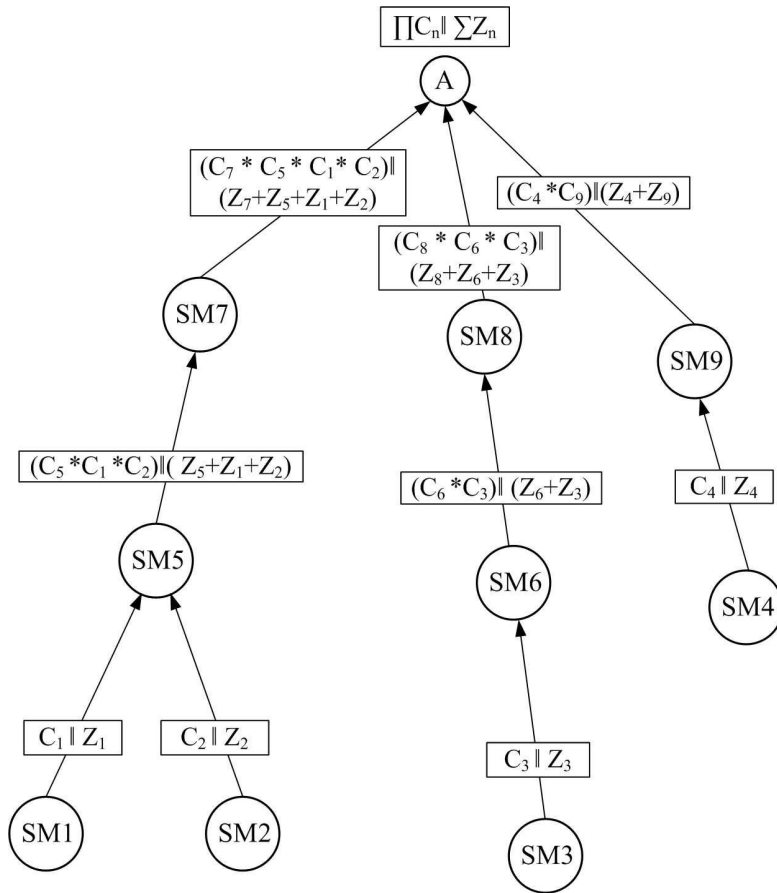
- [0070] 도 5에서 유틸리티 시스템(320)은 도 4와 동일한 기능을 수행하는 구성이다.
- [0071] 상위 계층 스마트 미터로 표시한 블록은 하위 계층 스마트 미터에 존재하는 각 그룹을 대표하는 스마트 미터(310A, 310B, 310C, 310D, 310E)로 구성된다. 각 그룹을 대표하는 스마트 미터를 그룹 스마트 미터라고 명명한다. 그룹 스마트 미터는 해당 그룹 내의 측정값 및 무결성 점검값을 전달하는 역할을 수행한다. 물론 그룹 스마트 미터 대신에 각 그룹과 연결된 개별 게이트웨이를 사용할 수도 있을 것이다. 각 그룹 내부는 동형 암호기법을 사용하는 복수의 스마트 미터가 트리 형태로 구성될 수 있다.
- [0072] 따라서 각 그룹에서 전달되는 최종 측정값 및 최종 무결성 점검값을 이용하여 해당 그룹의 측정값에 비정상 데이터가 없는지 판단할 수 있다. 판단 과정은 제어 서버(330)가 수행할 수도 있고, 경우에 따라서는 각 그룹을 제어하는 별도의 장치 또는 각 그룹 스마트 미터(310A, 310B, 310C, 310D, 310E)가 수행할 수도 있을 것이다.
- [0073] 나아가 제어 서버(330)는 하나의 그룹에서 비정상 데이터를 전달하는 하나의 노드(스마트 미터)를 식별하여 해당 노드를 격리할 수도 있지만, 지역적으로 접근성이 있는 그룹인 경우 공격 노드가 다수 등장할 수 있기 때문에 특정 그룹 자체를 격리하는 조치를 취할 수도 있을 것이다. 이 경우 각 스마트 미터에 대해 데이터 무결성을 점검하지 않고, 그룹 스마트 미터로 구성된 트리에 대해 무결성 점검을 수행할 수 있다. 이후 특정 그룹 스마트 미터가 비정상 데이터를 전달하는 것으로 판단되면, 해당 그룹 전체를 네트워크에서 격리할 수도 있을 것이다.
- [0074] 한편 도 5의 경우에도 하나의 스마트 미터 또는 그룹을 곧바로 격리하기에 앞서 실패 카운트가 기준값을 넘는지 여부를 판단하여 스마트 미터 또는 그룹을 격리하는 조치를 취할 수 있다.
- [0075] 나아가 제어 서버(330)는 그룹 스마트 미터로부터 수신하는 최종 측정값과 최종 무결성 점검값을 이용하여 최종 측정값에 비정상 데이터가 있다고 판단하면 실패 카운트를 증가시키고, 최종 측정값에 비정상 데이터가 없다고 판단하면 성공 카운트 증가시킬 수 있다.
- [0076] 이 경우 제어 서버(330)는 실패 카운트가 기준값을 초과하면서 실패 카운트와 성공 카운트의 비율이 기준 비율 값을 초과하는 경우 그룹 스마트 미터로 구성되는 트리 또는 그룹을 구성하는 스마트 미터로 구성되는 트리 중 적어도 하나의 토폴로지를 변경할 수 있다. 제어 서버(330)가 네트워크의 토폴로지를 변경하는 것은 사전에 마련된 정책에 따를 것이다.
- [0077] 본 실시예 및 본 명세서에 첨부된 도면은 전술한 기술에 포함되는 기술적 사상의 일부를 명확하게 나타내고 있는 것에 불과하며, 전술한 기술의 명세서 및 도면에 포함된 기술적 사상의 범위 내에서 당업자가 용이하게 유추할 수 있는 변형 예와 구체적인 실시예는 모두 전술한 기술의 권리범위에 포함되는 것이 자명하다고 할 것이다.

부호의 설명

- [0078]
- | | |
|-------------------|-------------------|
| 50 : 전력 소비 장치 | 200 : 스마트 그리드 시스템 |
| 210 : 스마트 미터 | 220 : 게이트웨이 |
| 230 : 유틸리티 시스템 | 240 : 제어 서버 |
| 300 : 스마트 그리드 시스템 | 310 : 스마트 미터 |
| 320 : 유틸리티 시스템 | 330 : 제어 서버 |

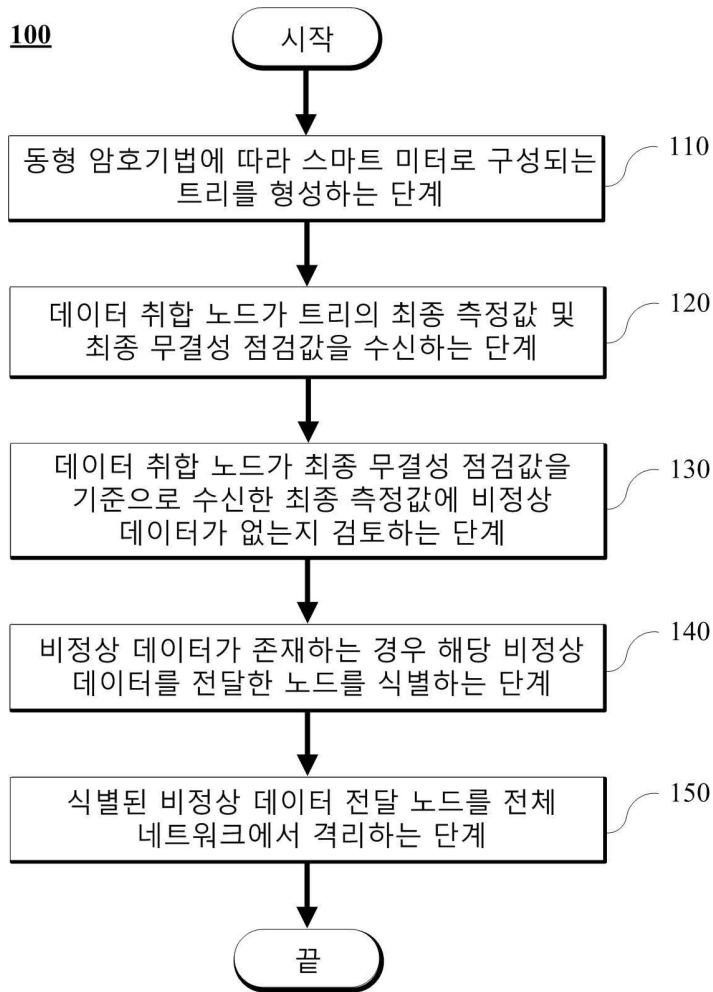
도면

도면1

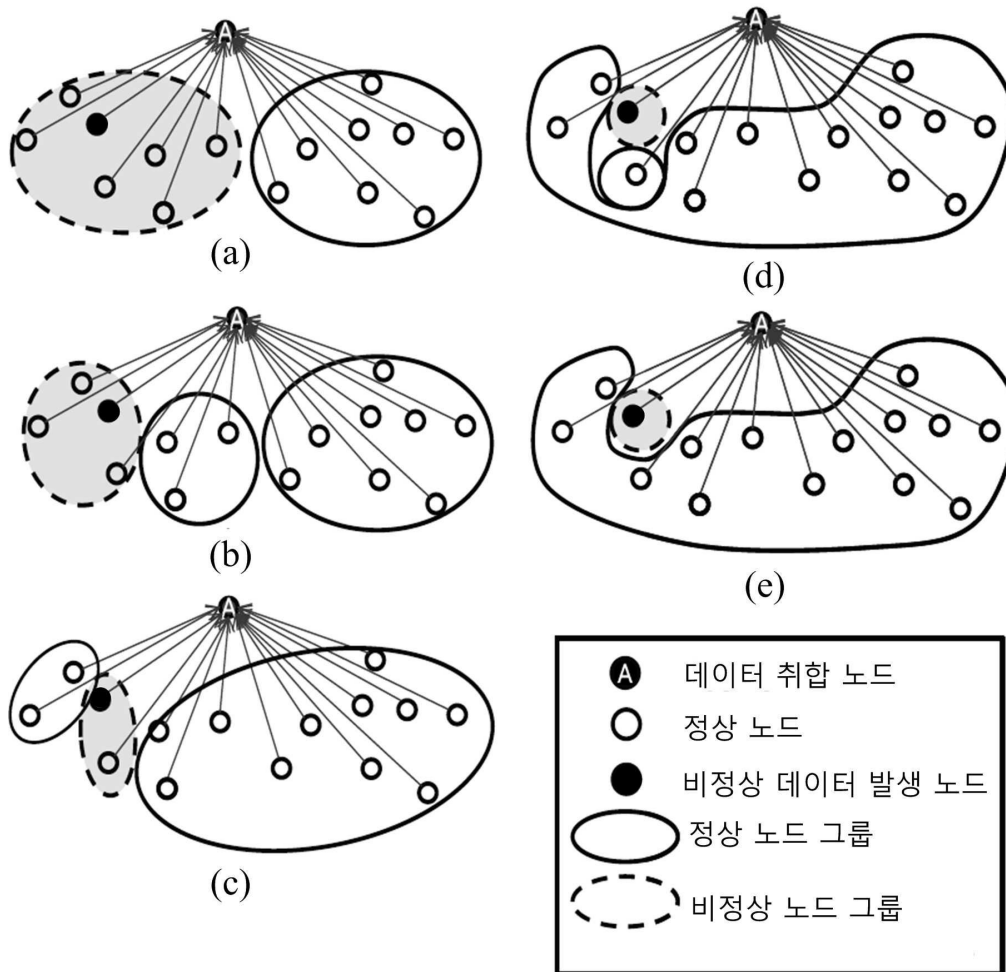


도면2

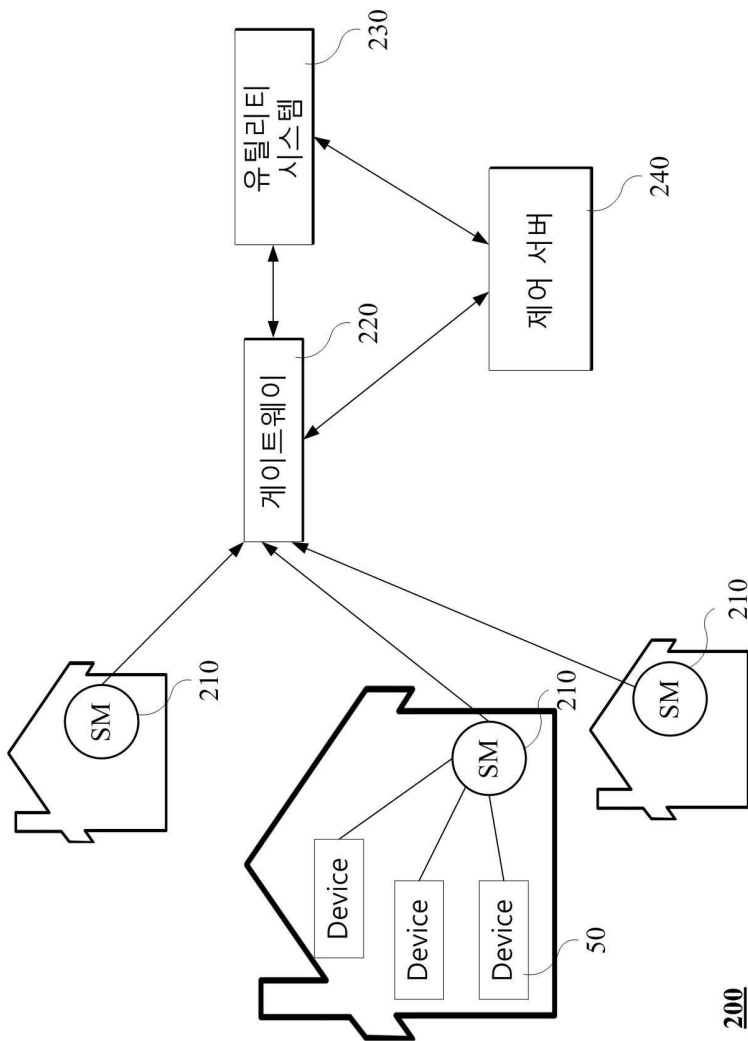
100



도면3



도면4



도면5

