

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)(11) 공개번호 10-2022-0078344
(43) 공개일자 2022년06월10일

(51) 국제특허분류(Int. Cl.)
G06N 20/20 (2019.01) H04B 17/309 (2014.01)
H04W 24/10 (2009.01)
(52) CPC특허분류
G06N 20/20 (2021.08)
H04B 17/309 (2015.01)
(21) 출원번호 10-2020-0167810
(22) 출원일자 2020년12월03일
심사청구일자 2020년12월03일

(71) 출원인
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
한명훈
대전광역시 유성구 북유성대로488번길 160
함재현
대전광역시 유성구 북유성대로488번길 160
(뒷면에 계속)
(74) 대리인
특허법인 광장리앤코

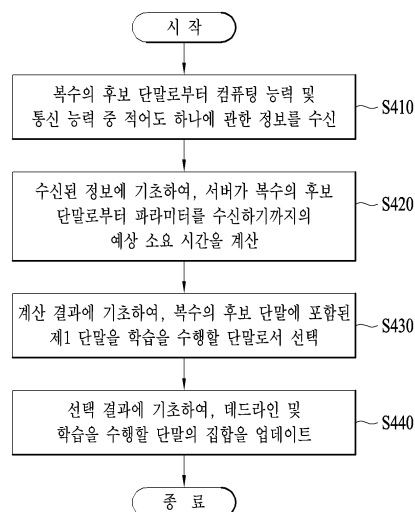
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 연합 학습 수행 방법 및 이를 위한 장치

(57) 요약

복수의 후보 단말로부터 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보를 수신하는 단계, 상기 수신된 정보에 기초하여, 서버가 상기 복수의 후보 단말로부터 파라미터를 수신하기까지의 예상 소요 시간을 계산하는 단계, 상기 계산 결과에 기초하여, 상기 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택하는 단계 및 상기 선택 결과에 기초하여, 데드라인 및 학습을 수행할 단말의 집합을 업데이트하는 단계를 포함하는, 연합 학습 수행 방법을 제공한다.

대표도 - 도4



(52) CPC특허분류

H04W 24/10 (2013.01)

(72) 발명자

백상현

서울특별시 성북구 안암로 145

고한열

서울특별시 성북구 안암로 145

이재욱

서울특별시 성북구 안암로 145

명세서

청구범위

청구항 1

복수의 후보 단말로부터 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보를 수신하는 단계;

상기 수신된 정보에 기초하여, 서버가 상기 복수의 후보 단말로부터 파라미터를 수신하기까지의 예상 소요 시간을 계산하는 단계;

상기 계산의 결과에 기초하여, 상기 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택하는 단계; 및

상기 선택의 결과에 기초하여, 데드라인 및 학습을 수행할 단말의 집합을 업데이트하는 단계를 포함하는, 연합 학습 수행 방법.

청구항 2

제1항에 있어서,

상기 제1 단말은 상기 복수의 후보 단말 중 상기 예상 소요 시간이 가장 짧은 단말인, 연합 학습 수행 방법.

청구항 3

제1항에 있어서,

상기 제1 단말을 학습을 수행할 단말로서 선택하는 단계는,

상기 제1 단말의 예상 소요 시간과 상기 학습을 수행할 단말에 의해 결정된 데드라인에 기초하여, 상기 제1 단말을 학습을 수행할 단말로서 선택하는 단계인, 연합 학습 수행 방법.

청구항 4

제3항에 있어서,

상기 제1 단말의 예상 소요 시간과 상기 학습을 수행할 단말에 의해 결정된 데드라인의 차이가 제1 임계값 이상이 될 때까지 상기 방법은 반복되는 것인, 연합 학습 수행 방법.

청구항 5

제3항에 있어서,

상기 제1 단말의 예상 소요 시간과 상기 학습을 수행할 단말에 의해 결정된 데드라인의 차이가 제1 임계값보다 작으면, 상기 제1 단말을 학습을 수행할 단말로서 선택하는 단계인, 연합 학습 수행 방법.

청구항 6

제1항에 있어서,

상기 데드라인은

상기 학습을 수행할 단말의 집합에 포함된 단말의 예상 소요 시간 중, 가장 긴 예상 소요 시간 및 제1 시간 마진에 기초하여 결정되는 것인, 연합 학습 수행 방법.

청구항 7

제1항에 있어서,

상기 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보는,

FLOPS(floating point operations per second) 정보 및 채널 품질 인덱스(channel quality index, CQI) 정보

중 적어도 하나를 포함하는 것인, 연합 학습 수행 방법.

청구항 8

제1항에 있어서,

상기 방법은 상기 학습을 수행할 단말의 집합에 포함된 단말들의 학습 수행 결과가 모델의 정확도가 제2 임계값 이상이 될 때까지 반복되는 것인, 연합 학습 수행 방법.

청구항 9

적어도 하나의 명령어(instruction)를 저장하는 메모리(memory); 및

상기 적어도 하나의 명령어를 실행하여,

복수의 후보 단말로부터 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보를 수신하고,

상기 수신된 정보에 기초하여, 서버가 상기 복수의 후보 단말로부터 파라미터를 수신하기까지의 예상 소요 시간을 계산하고,

상기 계산의 결과에 기초하여, 상기 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택하고,

상기 선택의 결과에 기초하여, 데드라인 및 학습을 수행할 단말의 집합을 업데이트하는 프로세서(processor)를 포함하는, 연합 학습을 수행하는 장치.

청구항 10

연합 학습 수행 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 비일시적 기록매체로서,

상기 연합 학습 수행 방법은,

복수의 후보 단말로부터 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보를 수신하는 단계;

상기 수신된 정보에 기초하여, 서버가 상기 복수의 후보 단말로부터 파라미터를 수신하기까지의 예상 소요 시간을 계산하는 단계;

상기 계산의 결과에 기초하여, 상기 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택하는 단계; 및

상기 선택의 결과에 기초하여, 데드라인 및 학습을 수행할 단말의 집합을 업데이트하는 단계를 포함하는, 비일시적 기록매체.

발명의 설명

기술 분야

[0001] 본 개시는 연합 학습을 수행하는 방법에 관한 것으로, 더 상세하게는 연합 학습을 수행하는 단말 및 데드라인을 결정하는 방법에 관한 것이다.

배경 기술

[0002] 서버에서 심층 모델(deep model)을 학습하기 위해서는 방대한 데이터를 수집해야 하는데, 이는 네트워크 트래픽의 증가를 야기할 수 있다. 또한, 데이터가 네트워크 상에 노출되기 때문에 데이터 제공자의 개인정보 보호에 어려움이 발생할 수 있다.

[0003] 이러한 문제점을 해결하기 위해 선행발명 PCT/US2018/045992에서는 연합 학습(Federated Learning, FL)이 제안된 바 있다. 연합 학습에서는 단말이 데이터를 서버로 전송하지 않고, 자신들이 가지고 있는 데이터들을 통해 심층 모델을 학습시킨 후, 학습된 심층 모델을 서버로 전송한다. 서버는 일부 데이터들로 학습된 심층 모델들을 하나의 심층 모델로 통합한다. 해당 통합 과정은 심층 모델이 전체 데이터로 학습된 효과를 보일 수 있게 된다. 그 후, 서버는 통합된 심층 모델을 단말들에게 전송하게 되며, 학습시키는 심층 모델의 정확도가 목표치까지 도달할 때까지 상술된 과정을 반복적으로 수행된다.

[0004] 즉, 연합 학습에서는 각 단말이 서버에게 데이터가 아닌 학습된 모델을 전송하고, 서버는 방대한 데이터를 수집할 필요없이 일정한 양의 모델을 수신하기 때문에 연합 학습을 통해 데이터 제공자의 개인정보 보호 문제와 네트워크 부하 증가 문제를 방지할 수 있는 효과가 있다. 이에 따라, 연합 학습에 관한 여러 연구가 진행 중에 있다.

발명의 내용

해결하려는 과제

[0005] 본 실시 예가 해결하고자 하는 과제는, 연합 학습을 수행하는 단말 및 데드라인을 결정하는 방법 및 이를 위한 장치를 제공하는데 있다.

[0006] 본 실시 예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제들로 한정되지 않으며, 이하의 실시 예들로부터 또 다른 기술적 과제들이 유추될 수 있다.

과제의 해결 수단

[0007] 제1 실시 예에 따라, 연합 학습 수행 방법은 복수의 후보 단말로부터 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보를 수신하는 단계, 상기 수신된 정보에 기초하여, 서버가 상기 복수의 후보 단말로부터 파라미터를 수신하기까지의 예상 소요 시간을 계산하는 단계, 상기 계산 결과에 기초하여, 상기 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택하는 단계 및 상기 선택 결과에 기초하여, 데드라인 및 학습을 수행할 단말의 집합을 업데이트하는 단계를 포함할 수 있다.

[0008] 제2 실시 예에 따라, 연합 학습을 수행하는 장치는 적어도 하나의 명령어(instruction)를 저장하는 메모리(memory) 및 상기 적어도 하나의 명령어를 실행하여, 복수의 후보 단말로부터 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보를 수신하고, 상기 수신된 정보에 기초하여, 서버가 상기 복수의 후보 단말로부터 파라미터를 수신하기까지의 예상 소요 시간을 계산하고, 상기 계산의 결과에 기초하여, 상기 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택하고, 상기 선택의 결과에 기초하여, 데드라인 및 학습을 수행할 단말의 집합을 업데이트하는 프로세서(processor)를 포함할 수 있다.

[0009] 제3 실시 예에 따라, 컴퓨터로 읽을 수 있는 기록매체는 연합 학습 수행 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 비일시적 기록매체로서, 상기 연합 학습 수행 방법은 복수의 후보 단말로부터 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보를 수신하는 단계, 상기 수신된 정보에 기초하여, 서버가 상기 복수의 후보 단말로부터 파라미터를 수신하기까지의 예상 소요 시간을 계산하는 단계, 상기 계산의 결과에 기초하여, 상기 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택하는 단계 및 상기 선택의 결과에 기초하여, 데드라인 및 학습을 수행할 단말의 집합을 업데이트하는 단계를 포함할 수 있다.

[0010] 기타 실시 예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

발명의 효과

[0011] 본 개시에 따른 방법 및 장치는 매 라운드마다 단말의 컴퓨팅 능력 및/또는 통신 능력에 기초하여 학습을 수행할 단말 및 데드라인을 결정함으로써, 각 단말 및 서버의 자원의 낭비를 줄이고, 요구되는 모델 정확도에 도달하는 시간을 줄일 수 있는 효과가 있다.

[0012] 발명의 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 청구범위의 기재로부터 당해 기술 분야의 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0013] 도 1은 종래 연합 학습을 수행하는 과정을 위한 도면이다.

도 2는 일 실시예에 따른 연합 학습을 수행하는 과정을 설명하기 위한 도면이다.

도 3은 일 실시예에 따른 연합 학습 시스템을 설명하기 위한 도면이다.

도 4는 일 실시예에 따른 연합 학습을 수행하는 장치를 설명하기 위한 흐름도이다.

도 5는 일 실시예에 따른 연합 학습을 수행하는 방법을 설명하기 위한 도면이다.

도 6 및 도 7은 일 실시예에 따른 연합 학습을 수행하는 방법의 성능을 설명하기 위한 도면이다.

도 8은 일 실시예에 따른 연합 학습을 수행하는 장치를 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

- [0014] 실시 예들에서 사용되는 용어는 본 개시에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 관례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 개시에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 개시의 전반에 걸친 내용을 토대로 정의되어야 한다.
- [0015] 명세서 전체에서 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다.
- [0016] 명세서 전체에서 기재된 "a, b, 및 c 중 적어도 하나"의 표현은, 'a 단독', 'b 단독', 'c 단독', 'a 및 b', 'a 및 c', 'b 및 c', 또는 'a, b, 및 c 모두'를 포괄할 수 있다.
- [0017] 아래에서는 첨부한 도면을 참고하여 본 개시의 실시 예에 대하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다.
- [0018] 이하에서는 도면을 참조하여 본 개시의 실시 예들을 상세히 설명한다.
- [0019] 도 1은 종래 연합 학습을 수행하는 과정을 위한 도면이다.
- [0020] 종래의 연합 학습 기법 중, 학습에 참여할 단말을 선택하여, 선택된 단말들만 연합 학습을 수행하는 방법이 제안된 바 있다. 이때, 단말들이 선택되는 기준은 단말이 가지고 있는 데이터 분포, 이전에 학습에 참여한 횟수 등을 포함할 수 있다.
- [0021] 하지만, 연합 학습에서 서버는 단말들로부터 모델을 수신할 수 밖에 없으므로 낙오자(straggler) 문제가 발생할 가능성이 있었다. 여기서 낙오자 문제는 특정 단말의 컴퓨팅 능력 및/또는 통신 능력이 매우 낮거나 혹은 단말의 이동성, 전원 꺼짐 등의 문제로 학습된 심층 모델을 매우 늦게 전송하여 서버에서의 지연 시간이 길어지는 문제를 의미한다.
- [0022] 이러한 문제를 해결하기 위해서 종래의 연합 학습 수행 방법은 데드라인(deadline)을 결정할 수 있다. 데드라인은 단말로부터 수신되는 파라미터를 기다리는 임계 시간을 의미한다. 서버는 단말의 모델을 수신하기 위해 데드라인까지 기다리고, 데드라인보다 늦게 수신되는 모델은 무시함으로써, 낙오자 문제를 해결할 수 있었다.
- [0023] 또한, 고정된 데드라인 내에 파라미터를 서버에 전송할 수 있는 단말들을 선택하여, 선택된 단말들만 연합 학습에 참여시킴으로써, 필요 없는 컴퓨팅 자원 소비와 기다림을 최소화하였다. 한편, 전역 모델의 파라미터 배포 시점부터 데드라인까지의 구간은 하나의 라운드로 정의할 수 있다. 다시 말해, 서버가 단말에게 심층 모델을 전송하고, 학습된 모델들을 통합하는 과정까지를 라운드로 정의할 수 있다.
- [0024] 도 1을 참고하면, 서버는 매 라운드의 데드라인을 20초로 결정한 후, 제1 단말 내지 제4 단말 중에서 연합 학습을 수행할 단말로서, 데드라인 내 업데이트된 파라미터를 서버에 전송할 수 있는 제1 단말, 제2 단말 및 제4 단말을 선택하고, 전역 모델의 파라미터를 배포할 수 있다. 이때, 서버는 데드라인과 함께, 제1 시간 마진을 더 고려하여 연합 학습을 수행할 단말을 선택할 수 있다. 서버는 데드라인에서 제1 시간 마진 이전에 서버에 업데이트된 파라미터를 전송하는 단말을 선택할 수 있다. 예를 들어, 데드라인은 20초, 제1 시간 마진은 1 초일 수 있으나, 데드라인 및 제1 시간 마진은 이에 제한되지 않으며 시스템 설계 요구사항에 따라 변경될 수 있다.
- [0025] 한편, 도 1의 제1 단말의 활성화 구간(110)은 제1 단말이 학습을 수행하는 시간을 의미하고, 제1 단말의 유후 구간(120)은 제1 단말이 서버에 업데이트된 파라미터를 전송한 후, 데드라인까지 대기하는 시간을 의미한다. 연합 학습에 참여한 각 단말은 서버에 업데이트된 파라미터를 전송한 이후, 해당 라운드의 데드라인이 도래할 때까지 유후 상태(또는 휴지 상태)가 될 수 있다. 예를 들어, 도 1의 제1 라운드에서, 제1 단말의 활성화 구간(110)은 17초이고, 제1 단말의 유후 구간(120)은 3초일 수 있다.
- [0026] 한편, 종래의 데드라인의 경우, 모든 라운드에서 고정되어 있으므로, 단말들의 컴퓨팅 능력 및/또는 통신 능력이 빈번히 변경되는 환경에서는 효율성이 저하될 수 있다.

- [0027] 도 1에서 제2 라운드의 데드라인을 제1 라운드와 같이 20초이라고 가정하면, 단말의 유후 구간이 제1 라운드와 비교하여 길어지기 때문에, 단말들의 자원이 낭비되는 결과를 초래할 수 있다.
- [0028] 구체적으로, 제2 라운드에서 제1 단말과 제3 단말은 5초 안에 학습된 심층 모델(즉, 업데이트된 파라미터)을 전송하지만, 제4 단말은 19초에 심층 모델을 전송할 수 있다.
- [0029] 이러한 상황에서, 제1 단말의 유후 구간과 제3 단말의 유후 구간은 각각 15초와 17초일 수 있다. 즉, 제1 단말과 제3 단말은 각각 15초와 17초동안 자원을 사용하지 않는 유후 상태에 있어야 한다. 또한, 서버는 제4 단말의 심층 모델을 수신하기 위해 제1 단말의 활성화 구간(130)의 종료로부터 14초를 추가로 기다려야 하는 문제가 발생한다.
- [0030] 따라서, 도 1의 제2 라운드를 참고하면, 데드라인이 20초로 고정된 경우에는 19초 안에 한 라운드에서 제1 단말, 제3 단말 및 제4 단말의 학습이 각각 1번씩 수행되어, 총 3번의 학습이 이루어질 수 있다.
- [0031] 도 2는 일 실시예에 따른 연합 학습을 수행하는 과정을 설명하기 위한 도면이다.
- [0032] 본 개시는 단말들의 컴퓨팅 능력 및/또는 통신 능력을 수집하고, 매 라운드에서 데드라인 및 학습을 수행할 단말들을 적응적으로 선택함으로써 자원 사용률을 증가시킬 수 있는 방법을 개시한다.
- [0033] 도 2를 참고하면, 도 1의 제2 라운드와 같은 환경에서 데드라인이 7초로 설정되는 경우, 서버는 학습을 수행할 단말로서, 제1 단말과 제3 단말만 선택할 것이고, 그 이후의 제3 라운드에서도 동일한 환경이라면, 제1 단말과 제3 단말이 7초 안에 심층 모델을 전송할 것이다. 다시 말해, 데드라인이 짧아지게 되면, 제1 단말과 제3 단말이 각각 학습을 2번씩 수행하여 총 4번의 학습이 14초 안에 이루어지게 된다. 이는 본 개시의 방법을 이용하면, 도 1의 제2 라운드에서 총 3번의 학습이 수행되는 것보다 더 많은 학습이 수행될 수 있음을 의미한다.
- [0034] 상술된 바에 의하면, 본 개시는 각 단말들이 유후 상태로 존재하는 시간을 줄여, 단말 및 서버의 자원 낭비를 줄일 수 있다. 또한, 동일한 시간 내 수행되는 라운드의 수가 증가하여 전체 모델을 학습하는 단말의 수가 증가할 수 있다. 이로 인해 요구되는 모델의 정확도에 도달하는 시간을 줄일 수 있는 효과가 있다.
- [0035] 도 3은 일 실시예에 따른 연합 학습 시스템을 설명하기 위한 도면이다.
- [0036] 일 실시예에 따른 연합 학습 시스템(300)은 서버(310) 및 복수의 단말(320 내지 340)을 포함할 수 있다. 복수의 단말(320 내지 340)의 일 예는 모바일 디바이스일 수 있으나, 단말의 종류는 이에 한정되지 않으며, 매 시점마다 서로 다른 컴퓨팅 능력 및/또는 통신 능력을 가질 수 있는 전자 디바이스이면 가능하다.
- [0037] 한편, 연합 학습은 동일한 절차들이 반복적으로 수행되는데, 여기서 라운드는 반복적으로 수행되는 과정의 단위를 의미한다. 매 라운드가 시작될 때 서버(310)는 복수의 단말(320 내지 340)에게 컴퓨팅 능력 및/또는 통신 능력에 대한 정보를 요청하고, 관련 정보를 수집한다. 이후, 서버(310)는 수집된 정보에 기초하여, 해당 라운드의 데드라인을 결정하고, 결정된 데드라인 내 학습된 심층 모델을 전송할 수 있는 단말(320, 340)을 선택할 수 있다.
- [0038] 그리고 나서 서버(310)는 선택된 단말(320, 340)에게 학습할 모델을 전송하고, 모델을 받은 단말부터 저장된 데이터를 이용하여 모델을 학습한다. 학습이 완료된 단말은 서버(310)에 모델 파라미터를 전송하고, 서버(310)는 데드라인이 도래할 때까지 모델 파라미터를 수신한다. 서버(310)는 모든 선택된 단말(320, 340)의 학습된 모델을 다 수신하거나 데드라인이 도래한 경우, 수신된 모델을 하나로 통합시킨다. 서버(310)는 상술된 과정을 모델의 정확성이 기준치 이상일 때까지 반복적으로 수행할 수 있다.
- [0039] 도 4는 일 실시예에 따른 연합 학습을 수행하는 장치를 설명하기 위한 흐름도이다.
- [0040] 단계 S410에서, 본 방법은 복수의 후보 단말로부터 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보를 수신할 수 있다.
- [0041] 여기서, 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보는 FLOPS(floating point operations per second) 정보 및 채널 품질 인덱스(channel quality index, CQI) 정보 중 적어도 하나를 포함할 수 있다.
- [0042] 단계 S420에서, 본 방법은 수신된 정보에 기초하여, 서버가 복수의 후보 단말로부터 파라미터를 수신하기까지의 예상 소요 시간을 계산할 수 있다.
- [0043] 단계 S430에서, 본 방법은 계산의 결과에 기초하여, 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택할 수 있다. 여기서, 제1 단말은 상기 복수의 후보 단말 중 상기 예상 소요 시간이 가장 짧은 단말일

수 있다.

- [0044] 한편, 단계 S430은 제1 단말의 예상 소요 시간과 학습을 수행할 단말에 의해 결정된 데드라인에 기초하여, 제1 단말을 학습을 수행할 단말로서 선택하는 단계일 수 있다.
- [0045] 구체적으로, 본 방법은 제1 단말의 예상 소요 시간과 학습을 수행할 단말에 의해 결정된 데드라인의 차이가 제1 임계값보다 작으면, 제1 단말을 학습을 수행할 단말로서 선택할 수 있다.
- [0046] 또한, 제1 단말의 예상 소요 시간과 학습을 수행할 단말에 의해 결정된 데드라인의 차이가 제1 임계값 이상이 될 때까지 본 방법은 반복될 수 있다.
- [0047] 단계 S440에서, 본 방법은 선택의 결과에 기초하여, 데드라인 및 학습을 수행할 단말의 집합을 업데이트할 수 있다.
- [0048] 한편, 데드라인은 학습을 수행할 단말의 집합에 포함된 단말의 예상 소요 시간 중, 가장 긴 예상 소요 시간 및 제1 시간 마진에 기초하여 결정되는 것일 수 있다.
- [0049] 또한, 본 방법은 학습을 수행할 단말의 집합에 포함된 단말들의 학습 수행 결과가 모델의 정확도가 제2 임계값 이상이 될 때까지 반복되는 것일 수 있다.
- [0050] 도 5는 일 실시예에 따른 연합 학습을 수행하는 방법을 설명하기 위한 도면이다.
- [0051] 본 개시의 방법은 매 라운드마다 각 단말의 컴퓨팅 능력 및/또는 통신 능력에 관한 정보를 수집하고, 수집된 정보에 따라 데드라인과 학습을 수행할 단말들을 결정할 수 있다.
- [0052] 도 5를 참고하면, 전체 단말의 수는 M 이고, 이 중에서 학습을 수행하는 것으로 선택된 단말들의 집합은 M_S 로 정의될 수 있다. 따라서, M 에서 M_S 에 포함되지 않은 단말은 아직 학습을 수행할 단말로 선택되지 않은 후보 단말로 정의될 수 있다.
- [0053] 한편, T_{i*} 는 다음 M_S 에 의한 데드라인을 나타내고, T_B 은 현재 M_S 에 의한 데드라인을 나타낸다. 데드라인은 M_S 에 포함된 단말 중에서 가장 늦게 업데이트된 모델 파라미터를 전송하는 단말의 전송 시간으로 설정될 수 있다.
- [0054] 또한, $T_{D,i}$ 는 i 번째 단말이 전역 모델의 파라미터를 다운로드하는 시간을 의미하고, $T_{T,i}$ 는 모델을 업데이트하는 시간, 즉 학습하는 시간을 나타낸다. 그리고, $T_{U,i}$ 는 i 번째 단말이 서버에 업데이트된 파라미터를 업로드하는 시간을 나타낸다.
- [0055] 도 5를 참고하면, 본 개시는 510에서 파라미터(T_{i*} , T_B , M , M_S)의 초기화를 수행할 수 있다. 이때, $T_{D,i}$, $T_{T,i}$ 및 $T_{U,i}$ 는 알고리즘이 수행되기 전에 단말들로부터 수집한 값으로 설정될 수 있다.
- [0056] 이후, 방법은 520에서 아직 선택되지 않는 단말 중에 가장 빨리 업데이트된 파라미터를 전송할 수 있는 단말(i^*)과 해당 단말(i^*)이 업데이트된 파라미터를 전송하는 데까지 필요한 시간(T_{i*})을 산출할 수 있다.
- [0057] 이때, 산출된 시간(T_{i*})과 이전까지 선택된 단말들에 의해 결정된 데드라인 (T_B)의 차이가 미리 정해진 기준시간 (Θ_T)보다 작은 경우에는 T_B 를 T_{i*} 로 업데이트하고, 해당 단말(i^*)을 선택된 단말의 집합(M_S)에 포함한다. 그렇지 않으면 알고리즘을 종료하고, 해당 라운드의 데드라인은 T_B 이며, 선택된 단말 집합은 M_S 인 것으로 결정할 수 있다.
- [0058] 이후 서버는 결정된 데드라인 및 선택된 단말 집합에 기초하여, 전역 모델의 파라미터를 배포하고, 단말로부터 심층 모델을 수신하여 모델을 학습시킬 수 있다.
- [0059] 도 6 및 도 7은 일 실시예에 따른 연합 학습을 수행하는 방법의 성능을 설명하기 위한 도면이다.
- [0060] 일 실시예에 따른 연합 학습을 수행하는 방법의 성능을 검증하기 위해, 10,000번의 실험을 수행하였으며, 학습한 데이터는 Cifar 데이터 50,000개를 20개의 단말에 임의로 분포시켰으며, 10,000개의 데이터로 성능 평가를 진행하였다. 학습에 참여한 심층 모델은 3계층의 컨볼루션 계층과 3계층의 완전 연결 계층으로 이루어진 CNN 네트워크 구조를 사용하였다. 한편, 각 단말의 컴퓨팅 능력 및/또는 통신 능력은 정규 분포를 따르며, 해당 정규 분포의 평균과 분산은 임의값으로 설정하였다.

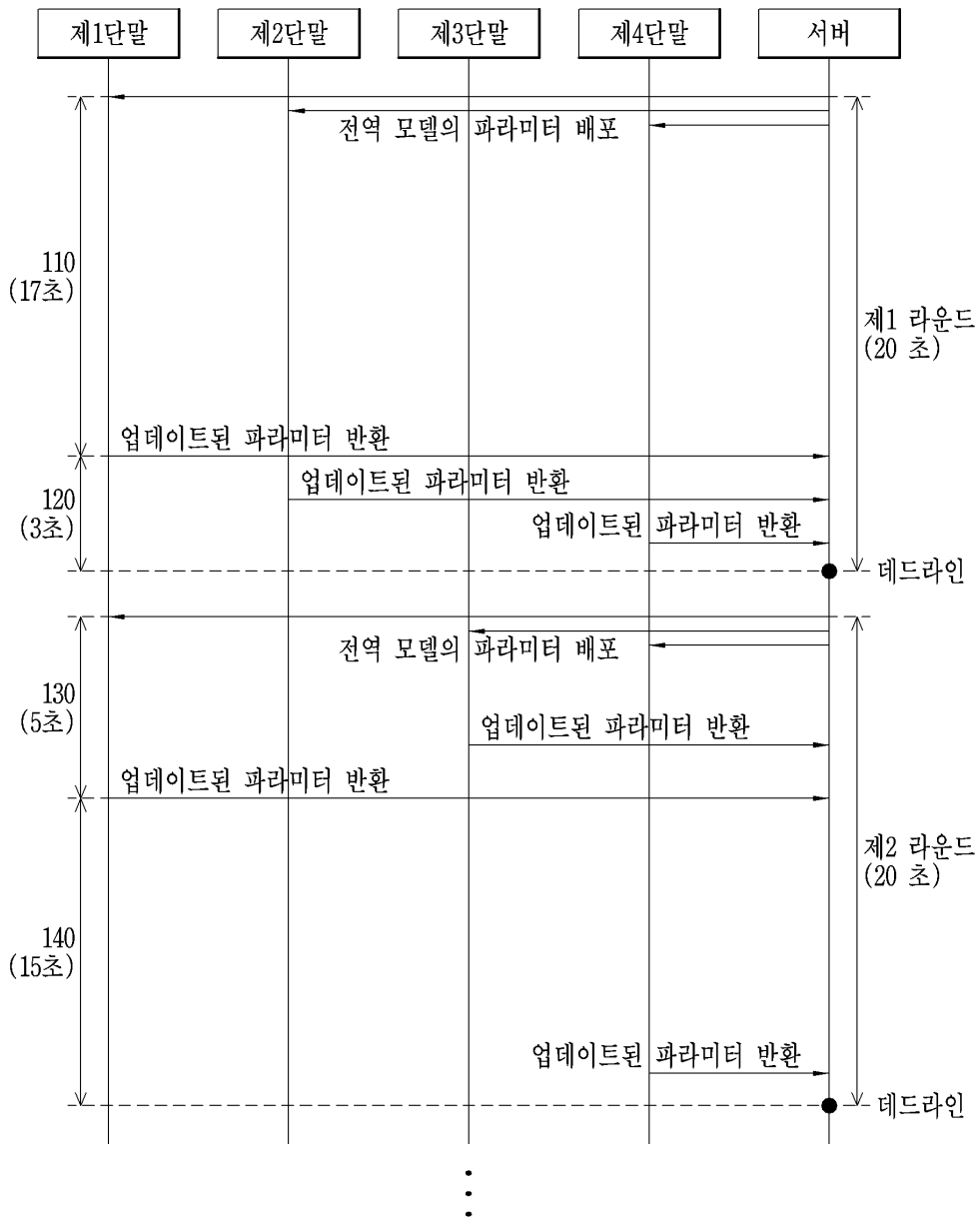
- [0061] 또한 성능의 비교를 위해, 동일한 환경에서 제1 알고리즘 내지 제3 알고리즘에 관한 실험을 수행하였다. 제1 알고리즘은 임의의 단말 n 개를 선택하여 학습을 수행하는 연합 학습 기법이고, 제2 알고리즘은 컴퓨팅 능력 및 통신 능력이 좋은 n 개의 단말을 선택하여 학습을 수행하는 연합 학습 기법이다. 또한, 제3 알고리즘은 고정된 데드라인에 기초하여 단말을 선택하고 학습을 수행하는 연합 학습 기법이다.
- [0062] 도 6을 참고하면, 본 개시의 방법이 다른 알고리즘에 비해 학습 정확도가 높은 것을 확인할 수 있다. 또한, 학습 정확도 0.7에 가장 빠르게 수렴하는 것을 확인할 수 있다.
- [0063] 이는 본 개시가 각 라운드마다 통신 자원 및 컴퓨팅 자원의 활용율을 증가시킬 수 있도록 데드라인을 설정하기 때문에, 서버가 단말들로부터 학습된 모델을 수신하기 위해 기다리는 시간이 짧기 때문이다.
- [0064] 이와 반면에 제1 알고리즘은 각 단말의 컴퓨팅 능력 및 통신 능력에 상관없이 단말을 임의로 선택하기 때문에, 선택된 단말들로부터 모델을 수신하기 위해 기다리는 지연 시간이 증가할 확률이 높아지게 된다. 이에 따라, 제1 알고리즘이 가장 늦게 일정 학습 정확도에 수렴하는 것을 확인할 수 있다.
- [0065] 또한 도 7은 단말의 컴퓨팅 능력 및 통신 능력에 대한 정규 분포의 분산(V)에 따른 단말 평균 자원 사용량을 도시한 도면이다. 즉, V 가 증가할 수록 단말들의 컴퓨팅 능력 및 통신 능력의 편차가 큰 환경인 것을 의미하기 때문에, V 는 환경의 유동성의 척도를 나타낸다.
- [0066] 도 7을 참조하면, 본 개시의 방법이 제1 알고리즘 내지 제3 알고리즘과 비교하여, 자원 사용량이 가장 높을 것을 확인할 수 있다. 이는 본 개시의 방법의 경우, 매 라운드마다 단말의 통신 능력 및/또는 컴퓨팅 능력에 따라 데드라인을 결정하기 때문에, 학습을 수행하는 단말들의 유후 시간 및 서버의 대기 시간이 감소한 결과일 수 있다.
- [0067] 도 8은 일 실시예에 따른 연합 학습을 수행하는 장치를 설명하기 위한 블록도이다.
- [0068] 연합 학습을 수행하는 장치(800)는 일 실시 예에 따라, 메모리(memory)(810) 및 프로세서(processor)(820)를 포함할 수 있다. 도 8에 도시된 연합 학습을 수행하는 장치(800)는 본 실시 예와 관련된 구성요소들만이 도시되어 있다. 따라서, 도 8에 도시된 구성요소들 외에 다른 범용적인 구성요소들이 더 포함될 수 있음을 본 실시 예와 관련된 기술분야에서 통상의 지식을 가진 자라면 이해할 수 있다.
- [0069] 한편, 연합 학습을 수행하는 장치(800)는 상술된 서버에 포함된 구성 요소일 수 있고, 서버 이외 별도의 장치로서, 서버 및 단말을 제어하는 장치에 포함된 구성 요소일 수 있다.
- [0070] 메모리(810)는 연합 학습을 수행하는 장치(800) 내에서 처리되는 각종 데이터들을 저장하는 하드웨어로서, 예를 들어, 메모리(810)는 본 개시의 장치(800)에서 처리된 데이터들 및 처리될 데이터들을 저장할 수 있다. 메모리(810)는 프로세서(820)의 동작을 위한 적어도 하나의 명령어(instruction)를 저장할 수 있다. 또한, 메모리(810)는 본 개시의 장치(800)에 의해 구동될 프로그램 또는 애플리케이션 등을 저장할 수 있다. 메모리(810)는 DRAM(dynamic random access memory), SRAM(static random access memory) 등과 같은 RAM(random access memory), ROM(read-only memory), EEPROM(electrically erasable programmable read-only memory), CD-ROM, 블루레이 또는 다른 광학 디스크 스토리지, HDD(hard disk drive), SSD(solid state drive), 또는 플래시 메모리를 포함할 수 있다.
- [0071] 프로세서(820)는 본 개시의 장치(800)의 전반의 동작을 제어하고 데이터 및 신호를 처리할 수 있다. 프로세서(820)는 메모리(810)에 저장된 적어도 하나의 명령어 또는 적어도 하나의 프로그램을 실행함으로써, 본 개시의 장치(800)를 전반적으로 제어할 수 있다. 프로세서(820)는 CPU(central processing unit), GPU(graphics processing unit), AP(application processor) 등으로 구현될 수 있으나, 이에 제한되지 않는다.
- [0072] 프로세서(820)는 복수의 후보 단말로부터 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보를 수신하고, 수신된 정보에 기초하여 서버가 복수의 후보 단말로부터 파라미터를 수신하기까지의 예상 소요 시간을 계산하고, 계산의 결과에 기초하여 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택하고, 선택의 결과에 기초하여 데드라인 및 학습을 수행할 단말의 집합을 업데이트할 수 있다.
- [0073] 여기서, 컴퓨팅 능력 및 통신 능력 중 적어도 하나에 관한 정보는 FLOPS(floating point operations per second) 정보 및 채널 품질 인덱스(channel quality index, CQI) 정보 중 적어도 하나를 포함할 수 있다.
- [0074] 한편, 프로세서(820)는 계산의 결과에 기초하여, 복수의 후보 단말에 포함된 제1 단말을 학습을 수행할 단말로서 선택할 수 있다. 여기서, 제1 단말은 상기 복수의 후보 단말 중 상기 예상 소요 시간이 가장 짧은 단말일 수

있다.

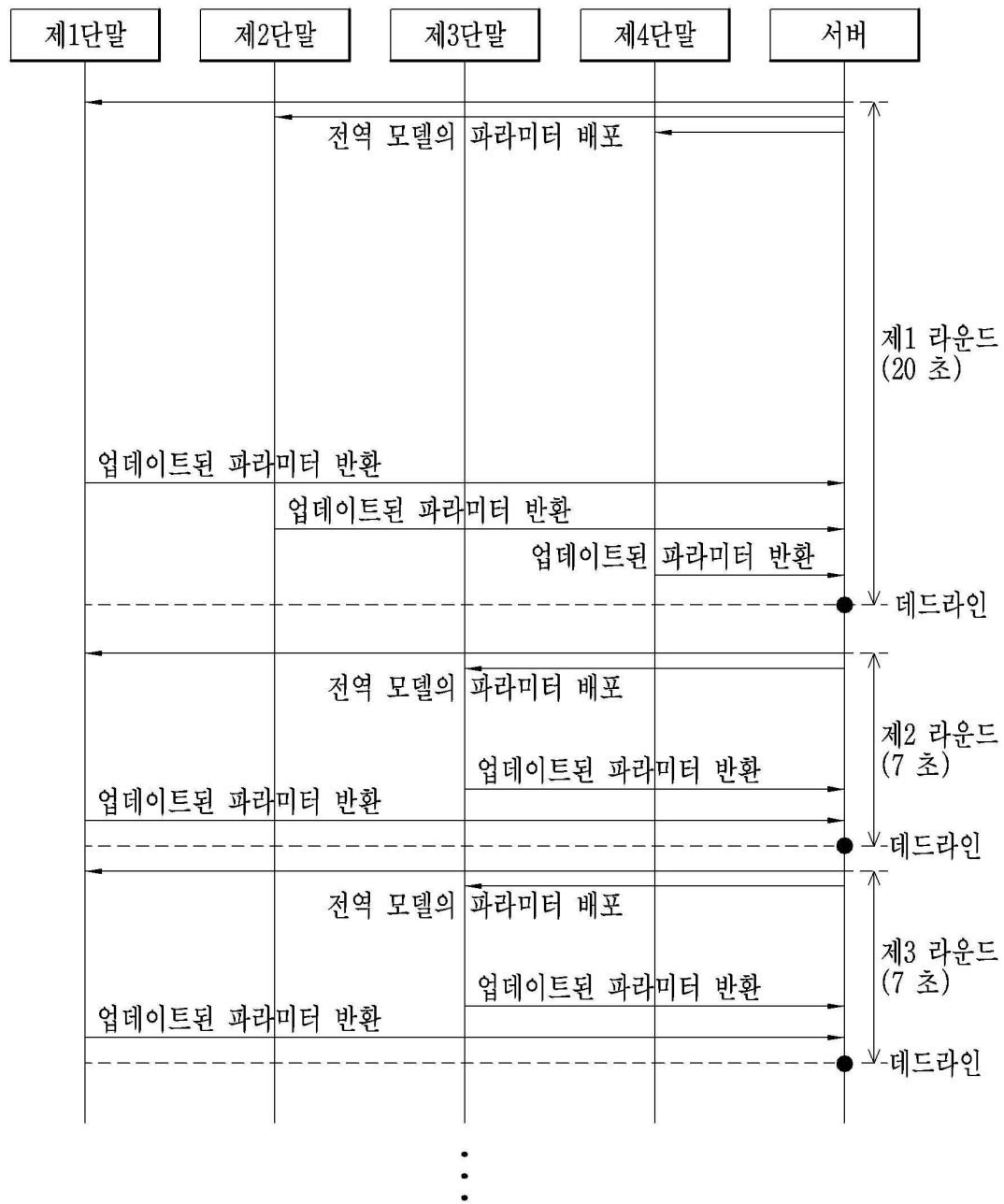
- [0075] 또한, 프로세서(820)는 제1 단말의 예상 소요 시간과 학습을 수행할 단말에 의해 결정된 데드라인에 기초하여, 제1 단말을 학습을 수행할 단말로서 선택할 수 있다.
- [0076] 구체적으로, 프로세서(820)는 제1 단말의 예상 소요 시간과 학습을 수행할 단말에 의해 결정된 데드라인의 차이가 제1 임계값보다 작으면, 제1 단말을 학습을 수행할 단말로서 선택할 수 있다.
- [0077] 또한, 프로세서(820)는 제1 단말의 예상 소요 시간과 학습을 수행할 단말에 의해 결정된 데드라인의 차이가 제1 임계값 이상이 될 때까지 상술된 동작을 반복할 수 있다.
- [0078] 한편, 데드라인은 학습을 수행할 단말의 집합에 포함된 단말의 예상 소요 시간 중, 가장 긴 예상 소요 시간 및 제1 시간 마진에 기초하여 결정되는 것일 수 있다.
- [0079] 또한, 프로세서(820)는 학습을 수행할 단말의 집합에 포함된 단말들의 학습 수행 결과가 모델의 정확도가 제2 임계값 이상이 될 때까지 상술된 동작을 반복할 수 있다.
- [0080] 전술한 실시 예들에 따른 프로세서는 프로세서, 프로그램 데이터를 저장하고 실행하는 메모리, 디스크 드라이브와 같은 영구 저장부(permanent storage), 외부 장치와 통신하는 통신 포트, 터치 패널, 키(key), 버튼 등과 같은 사용자 인터페이스 장치 등을 포함할 수 있다. 소프트웨어 모듈 또는 알고리즘으로 구현되는 방법들은 상기 프로세서상에서 실행 가능한 컴퓨터가 읽을 수 있는 코드들 또는 프로그램 명령들로서 컴퓨터가 읽을 수 있는 기록 매체 상에 저장될 수 있다. 여기서 컴퓨터가 읽을 수 있는 기록 매체로 마그네틱 저장 매체(예컨대, ROM(read-only memory), RAM(random-access memory), 플로피 디스크, 하드 디스크 등) 및 광학적 판독 매체(예컨대, 시디롬(CD-ROM), 디브이디(DVD: Digital Versatile Disc)) 등이 있다. 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템들에 분산되어, 분산 방식으로 컴퓨터가 판독 가능한 코드가 저장되고 실행될 수 있다. 매체는 컴퓨터에 의해 판독 가능하며, 메모리에 저장되고, 프로세서에서 실행될 수 있다.
- [0081] 본 실시 예는 기능적인 블록 구성들 및 다양한 처리 단계들로 나타내어질 수 있다. 이러한 기능 블록들은 특정 기능들을 실행하는 다양한 개수의 하드웨어 또는/및 소프트웨어 구성들로 구현될 수 있다. 예를 들어, 실시 예는 하나 이상의 마이크로프로세서들의 제어 또는 다른 제어 장치들에 의해서 다양한 기능들을 실행할 수 있는, 메모리, 프로세싱, 로직(logic), 룩 업 테이블(look-up table) 등과 같은 직접 회로 구성들을 채용할 수 있다. 구성 요소들이 소프트웨어 프로그래밍 또는 소프트웨어 요소들로 실행될 수 있는 것과 유사하게, 본 실시 예는 데이터 구조, 프로세스들, 루틴들 또는 다른 프로그래밍 구성들의 조합으로 구현되는 다양한 알고리즘을 포함하여, C, C++, 자바(Java), 어셈블러(assembler), 파이썬(Python) 등과 같은 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능적인 측면들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다. 또한, 본 실시 예는 전자적인 환경 설정, 신호 처리, 및/또는 데이터 처리 등을 위하여 종래 기술을 채용할 수 있다. “매커니즘”, “요소”, “수단”, “구성”과 같은 용어는 넓게 사용될 수 있으며, 기계적이고 물리적인 구성들로서 한정되는 것은 아니다. 상기 용어는 프로세서 등과 연계하여 소프트웨어의 일련의 처리들(routines)의 의미를 포함할 수 있다.
- [0082] 전술한 실시 예들은 일 예시일 뿐 후술하는 청구항들의 범위 내에서 다른 실시 예들이 구현될 수 있다.

도면

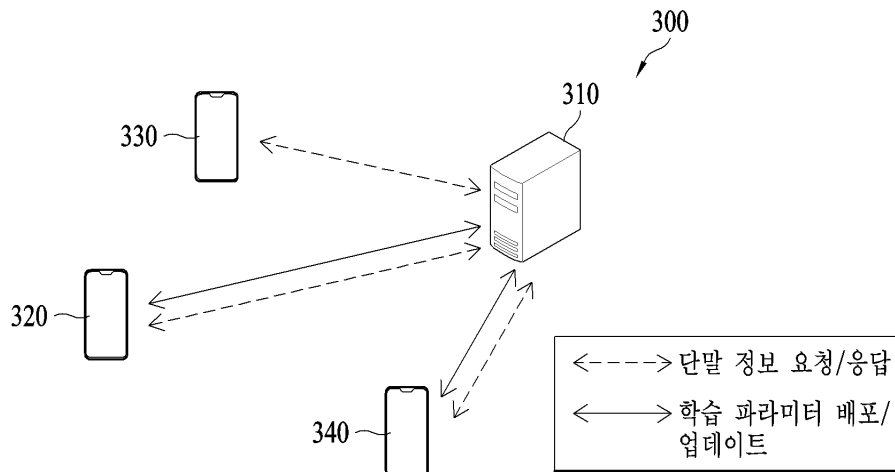
도면1



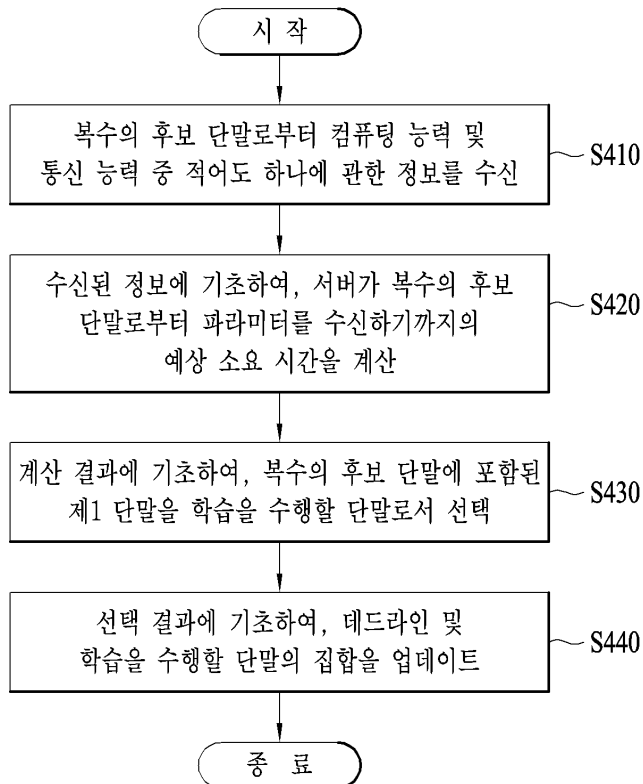
도면2



도면3



도면4

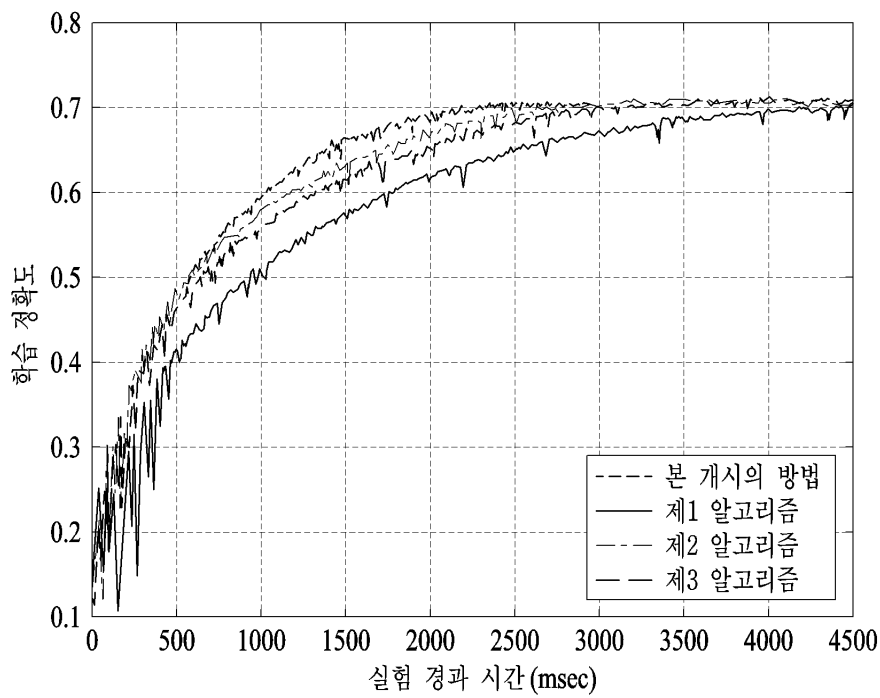


도면5

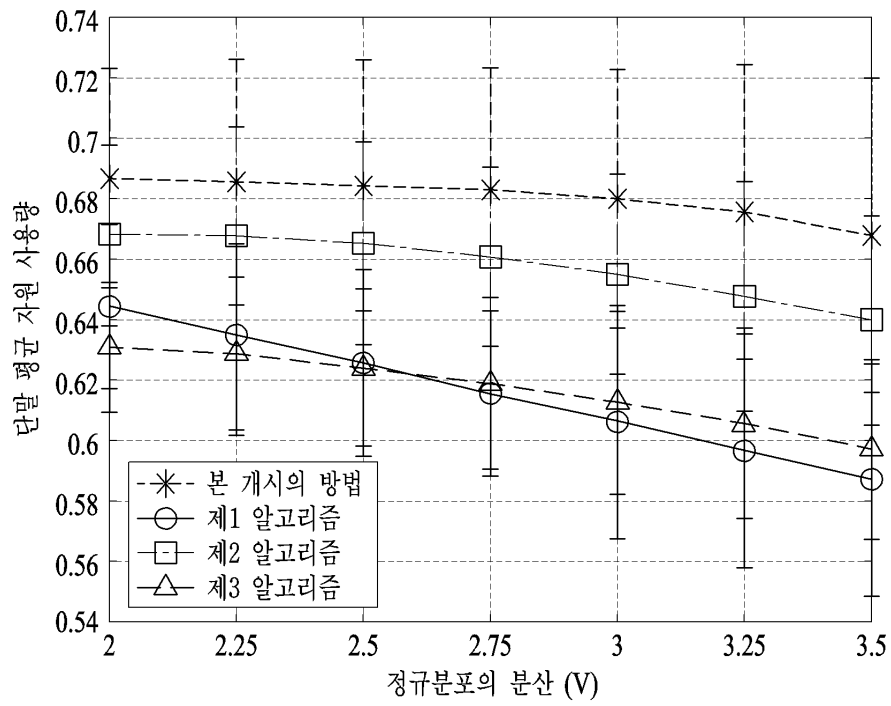
```

510 Input :  $T_i^* \leftarrow 0, T_B \leftarrow 0, M = \{i | \forall i\}, M_S = \emptyset$ 
      repeat
           $T_B \leftarrow T_i^*$ 
520 {  $T_i^* \leftarrow \min_{i \in M} (T_{D,i} + T_{T,i} + T_{U,i})$ 
       $i^* \leftarrow \arg \min_{i \in M} (T_{D,i} + T_{T,i} + T_{U,i})$ 
      단말  $i^*$ 을  $M$ 에서 제외
      단말  $i^*$ 을  $M_S$ 에 포함
      until  $T_i^* - T_B \geq \theta_T$ 
       $D \leftarrow T_B$ 
       $M_S$ 에 포함되어 있는 단말에게 파라미터를 분배
  
```

도면6



도면7



도면8

