(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년03월21일
(11) 등록번호 10-1125033
(24) 등록일자 2012년03월02일

(51) 국제특허분류(Int. Cl.)
H04L 9/28 (2006.01) *H04L 9/14* (2006.01)
(21) 출원번호 10-2010-0038880
(22) 출원일자 2010년04월27일
심사청구일자 2010년04월27일
(65) 공개번호 10-2011-0119269
(43) 공개일자 2011년11월02일
(56) 선행기술조사문헌
박기웅, 박규호, "DEVS-Based Evaluation for a Proper Selection of Compression and Encryption in Ubiquitous Computing Environment," 한국차세대컴퓨팅학회 논문지, Vol.4 No.2, 2008년 6월, pp. 16-22.
KR100949420 B1
KR100607020 B1
KR1020040044182 A
전체 청구항 수 : 총 12 항

(73) 특허권자
한국과학기술원
대전 유성구 구성동 373-1
(72) 발명자
박규호
대전광역시 유성구 대학로 291, 한국과학기술원 6-3208호 (구성동)
박기웅
서울특별시 노원구 광운로15길 48 (월계동)
(74) 대리인
김성호

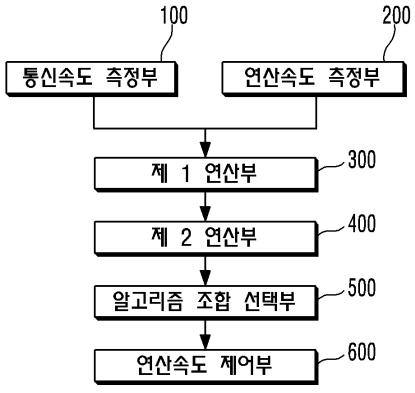
심사관 : 이형일

(54) 발명의 명칭 **최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템, 선택방법과 그 방법을 컴퓨터에서 수행하도록 각각의 단계를 실행시키기 위한 명령어를 기록한 컴퓨터 판독가능 기록매체**

(57) 요 약

본 발명의 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템은, 송신수단과 수신수단의 사이에 연결된 네트워크의 통신속도를 측정하는 통신속도 측정부; 상기 송신수단의 제1 연산속도 및 상기 수신수단의 제2 연산속도를 측정하는 연산속도 측정부; 다수의 설정된 압축알고리즘과 암호알고리즘의 조합에 따라 상기 제1 연산속도 및 상기 제2 연산속도가 변할 때, 상기 다수의 설정된 압축알고리즘과 암호알고리즘의 각각의 조합에 대하여, 상기 통신속도와 상기 제1 연산속도의 제1 차이값과, 상기 통신속도와 상기 제2 연산속도의 제2 차이값을 구하는 제1 연산부; 상기 제1 차이값과 제2 차이값을 변수로 하여 설정된 각각의 인덱스값을 구하는 제2 연산부; 및 상기 송신수단 및 수신수단에서 상기 인덱스값 중에서 최소값을 갖는 상기 압축알고리즘 및 암호알고리즘의 조합을 선택하게 하는 알고리즘 조합 선택부;를 포함한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

송신수단과 수신수단의 사이에 연결된 네트워크의 통신속도를 측정하는 통신속도 측정부;

상기 송신수단의 제1 연산속도 및 상기 수신수단의 제2 연산속도를 측정하는 연산속도 측정부;

다수의 설정된 압축알고리즘과 암호알고리즘의 조합에 따라 상기 제1 연산속도 및 상기 제2 연산속도가 변할 때, 상기 다수의 설정된 압축알고리즘과 암호알고리즘의 각각의 조합에 대하여, 상기 통신속도와 상기 제1 연산속도의 제1 차이값과, 상기 통신속도와 상기 제2 연산속도의 제2 차이값을 구하는 제1 연산부;

상기 제1 차이값과 제2 차이값을 변수로 하여 설정된 각각의 인덱스값을 구하는 제2 연산부; 및

상기 송신수단 및 수신수단에서 상기 인덱스값 중에서 최소값을 갖는 상기 압축알고리즘 및 암호알고리즘의 조합을 선택하게 하는 알고리즘 조합 선택부;

를 포함하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템.

청구항 2

제1항에 있어서,

선택된 압축알고리즘 및 암호알고리즘의 조합을 생성하는 제1 연산속도와 제2 연산속도가 통신속도와 같도록 제어하는 연산속도 제어부를 더 포함하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템.

청구항 3

제1항에 있어서,

상기 알고리즘 조합 선택부는 상기 송신수단 또는 수신수단의 연산속도를 나타내는 각각의 플로팅 스케일의 위치를 정하도록 하여 상기 압축알고리즘 및 암호알고리즘의 조합을 선택하게 하는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템.

청구항 4

제1항에 있어서,

상기 압축알고리즘 및 암호알고리즘의 조합은 무압축 알고리즘과 AES 알고리즘의 조합, RLE 알고리즘과 AES 알고리즘의 조합, LZO 알고리즘과 AES 알고리즘의 조합, GZIP 알고리즘과 AES 알고리즘의 조합, 또는 BZIP 알고리즘과 AES 알고리즘의 조합 중에서 어느 하나인 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템.

청구항 5

송신수단과 수신수단의 사이에 연결된 네트워크의 통신속도를 측정하는 단계;

상기 송신수단의 제1 연산속도 및 상기 수신수단의 제2 연산속도를 측정하는 단계;

다수의 설정된 압축알고리즘과 암호알고리즘의 조합에 따라 상기 제1 연산속도 및 상기 제2 연산속도가 변할 때, 상기 다수의 설정된 압축알고리즘과 암호알고리즘의 각각의 조합에 대하여, 상기 통신속도와 상기 제1 연산속도의 제1 차이값과, 상기 통신속도와 상기 제2 연산속도의 제2 차이값을 구하는 단계;

상기 제1 차이값과 제2 차이값을 변수로 하여 설정된 각각의 인덱스값을 구하는 단계; 및

상기 인덱스값 중에서 최소값을 갖는 상기 압축알고리즘 및 암호알고리즘의 조합을 선택하는 단계;

를 포함하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법.

청구항 6

제5항에 있어서,

상기 제1 연산속도 및 제2 연산속도는 상기 설정된 압축알고리즘의 압축속도와 압축률, 및 암호알고리즘의 암호화속도에 의해 결정되는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법.

청구항 7

제6항에 있어서,

상기 제1 연산속도 및 제2 연산속도는 $\frac{CS+ES}{CRCS+ES}+CS(1-CR)$ 이되, CS, ES, CR은 각각 압축속도, 암호화속도, 압축률인 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법.

청구항 8

제5항에 있어서,

상기 인덱스값은 $\sqrt{d_s^{\,2}+d_r^{\,2}}$ 이되, d_s는 제1 차이값이고, d_r는 제2 차이값인 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법.

청구항 9

제5항에 있어서,

시간의 경과에 따라 실시간으로 상기 압축알고리즘 및 암호알고리즘의 조합을 선택하는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법.

청구항 10

제5항에 있어서,

선택된 압축알고리즘 및 암호알고리즘의 조합을 생성하는 제1 연산속도와 제2 연산속도가 통신속도와 같도록 제어하는 단계를 더 포함하는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법.

청구항 11

제10항에 있어서,

상기 제1 연산속도 또는 제2 연산속도 중에서 통신속도보다 빠른 연산속도의 경우에는 연산속도를 낮추어 상기 통신속도와 같도록 제어하고, 상기 제1 연산속도 또는 제2 연산속도 중에서 통신속도보다 느린 연산속도의 경우에는 연산속도를 높여 상기 통신속도와 같도록 제어하는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법.

청구항 12

제5항 내지 제11항 중의 어느 하나의 항의 방법을 컴퓨터에서 수행하도록 상기 각각의 단계를 실행시키기 위한 명령어를 기록한 컴퓨터 판독가능 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템, 선택방법과 그 방법을 컴퓨터에서 수행하도록 각각의 단계를 실행시키기 위한 명령어를 기록한 컴퓨터 판독가능 기록매체에 관한 것으로, 특히 연산속도와 네트워크 상황이 유동적인 환경에서 최적의 압축알고리즘 및 암호알고리즘을 선택하는 시스템 및 방법과 그 방법을 컴퓨터에서 수행하도록 각각의 단계를 실행시키기 위한 명령어를 기록한 컴퓨터 판독가능 기

록매체에 관한 것이다.

배 경 기 술

[0002] 보안성의 중요성이 증가됨에 따라, 보안에 민감한 컴퓨터 통신에서는 암호화 알고리즘을 이용한다. 즉, 송신측에서는 데이터를 압축하고 압축된 데이터를 암호화하여 수신측에 전송하면, 수신측에서는 수신한 데이터를 해독하고 해독된 데이터의 압축을 해제한다. 압축알고리즘은 암호화할 데이터 및 전송해야 할 데이터의 양을 줄일 수 있기 때문에 통신의 효율성을 높일 수 있다.

[0003] 한편, 송신측에서는 암호화할 데이터가 줄어들게 되어 암호화 연산의 오버헤드를 줄일 수 있고, 전송할 데이터가 줄어들게 되어 통신 오버헤드를 줄일 수 있다. 또한, 수신측에서는 해독할 데이터가 줄어들게 되어 암호화 연산의 오버헤드를 줄일 수 있고, 수신할 데이터가 줄어들게 되어 통신 오버헤드를 줄일 수 있다.

[0004] 반면에, 송신측에서는 압축알고리즘을 수행해야 하므로 압축연산의 오버헤드가 발생하고, 수신측에서는 압축해제를 수행해야 하므로 비압축연산의 오버헤드가 발생한다.

[0005] 또한, 압축알고리즘은 gzip, bzip, LZO 등과 같은 수많은 알고리즘이 존재하는데, 각 알고리즘의 복잡도와 압축률은 모두 다르며, 전송할 데이터에 따라 유동적으로 압축률이 변하게 되므로, 현재의 상황에 가장 적합한 알고리즘을 선택하는 것이 어렵다.

[0006] 예를 들면, 성능이 매우 좋은 서버 단과 성능이 비교적 좋지않은 모바일 단과의 통신환경에서 압축율이 매우 좋은 압축알고리즘을 적용할 경우에, 서버 단에서는 빠른 시간 내에 압축하여 전송하더라도, 모바일 단에서는 수신하여 비 압축연산을 수행하고 해독하기 위해 많은 시간이 소요가 되므로, 이와 같은 경우에 압축알고리즘은 성능을 오히려 저하시킬 수 있다.

[0007] 또한, 두 모바일 장치 간의 통신에서 대역폭이 크게 변경되는 경우, 예를 들어 3G망(256Kbps)이 WiFi 무선통신(10Mbps)으로 변경될 경우 통신속도가 현저히 변하게 된다. 이와 같은 상황에서는 3G를 통하여 통신을 할 경우 특정 압축알고리즘을 사용하여 통신 효율성이 높아지더라도, WiFi망으로 변함에 따라 압축알고리즘이 바틀넥(bottle neck)이 되어 성능이 저하될 수 있다.

[0008] 이와 같이 현재의 상황에서 최적의 압축알고리즘 적용은 통신상황(대역폭), 송신단 및 수신단의 연산속도, 각 압축알고리즘의 압축률 등이 모두 고려되어 선택되어야 통신의 효율성을 높일 수 있으며, 그렇지 않을 경우에 압축알고리즘을 적용하게 되면 더 많은 문제를 발생시킬 수 있다.

[0009] 종래에도 다음과 같은 2가지 압축기술이 있었는데, 구체적으로 살펴보기로 한다.

[0010] 먼저, JSCC(joint source and channel coding)와 같은 비디오 전송기술인데, 비디오 전원와 네트워크 채널을 고려한 적응적인 비디오 압축기술을 제시한다. JSCC에서는 전원과 채널을 모두 수학적으로 모델링하여 최적의 전송속도 및 화질을 갖는 파라미터를 추출하여 최적화를 시도한다.

[0011] 이와 같은 방법은 각 송신측 및 수신측의 상황에 따라 모델링해야 하므로, 실질적인 적용을 위해서는 적용 전의 모든 경우에 대하여 모델링 및 튜닝을 해야 하므로 상당한 어려움이 있다.

[0012] 그리고, 논문 Adaptive On-the-Fly Compression(IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 17, NO. 1, JANUARY 2006)에서는 통신환경에 따라 압축을 적응적으로 적용하는 방법을 제시하는데, 이 논문 역시 수학적인 모델링을 기반으로 최적의 솔루션을 찾는 방법을 제시하고 있으며, 송신측 및 수신측의 연산속도를 고려하지 않은 상태에서 현재의 통신속도만을 고려하므로 송신측 및 수신측의 컴퓨팅파워 차이가 많거나 변하는 환경에 있어서는 최적의 솔루션을 선택하기 어렵다.

[0013] 상기한 바와 같이 종래에는 적응적인 압축알고리즘 적용을 위해 수학적인 모델링을 기반으로 하여 실질 환경에 적용하면, 모델링 오버헤드로 인하여 유용성이 낮다는 문제점이 있었다.

발명의 내용

해결하려는 과제

[0014] 본 발명은 송신측 및 수신측의 연산속도와 네트워크 상황이 실시간으로 변하는 유동적인 환경에서 최적의 압축알고리즘 및 암호알고리즘을 선택하여 통신의 효율성을 증가시키는 시스템 및 방법과 그 방법을 컴퓨터에서 수행하도록 각각의 단계를 실행시키기 위한 명령어를 기록한 컴퓨터 판독가능 기록매체를 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0015] 본 발명의 일 측면은, 송신수단과 수신수단의 사이에 연결된 네트워크의 통신속도를 측정하는 통신속도 측정부; 상기 송신수단의 제1 연산속도 및 상기 수신수단의 제2 연산속도를 측정하는 연산속도 측정부; 다수의 설정된 압축알고리즘과 암호알고리즘의 조합에 따라 상기 제1 연산속도 및 상기 제2 연산속도가 변할 때, 상기 다수의 설정된 압축알고리즘과 암호알고리즘의 각각의 조합에 대하여, 상기 통신속도와 상기 제1 연산속도의 제1 차이값과, 상기 통신속도와 상기 제2 연산속도의 제2 차이값을 구하는 제1 연산부; 상기 제1 차이값과 제2 차이값을 변수로 하여 설정된 각각의 인덱스값을 구하는 제2 연산부; 및 상기 송신수단 및 수신수단에서 상기 인덱스값 중에서 최소값을 갖는 상기 압축알고리즘 및 암호알고리즘의 조합을 선택하게 하는 알고리즘 조합 선택부;를 포함하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템을 제공한다.

[0016] 본 발명의 일 실시예에 따르면, 선택된 압축알고리즘 및 암호알고리즘의 조합을 생성하는 제1 연산속도와 제2 연산속도가 통신속도와 같도록 제어하는 연산속도 제어부를 더 포함하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템을 제공한다.

[0017] 본 발명의 다른 실시예에 따르면, 상기 알고리즘 조합 선택부는 상기 송신수단 또는 수신수단의 연산속도를 나타내는 각각의 플로팅 스케일의 위치를 정하도록 하여 상기 압축알고리즘 및 암호알고리즘의 조합을 선택하게 하는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템을 제공한다.

[0018] 본 발명의 또 다른 실시예에 따르면, 상기 압축알고리즘 및 암호알고리즘의 조합은 무압축 알고리즘과 AES 알고리즘의 조합, RLE 알고리즘과 AES 알고리즘의 조합, LZO 알고리즘과 AES 알고리즘의 조합, GZIP 알고리즘과 AES 알고리즘의 조합, 또는 BZIP 알고리즘과 AES 알고리즘의 조합 중에서 어느 하나인 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템을 제공한다.

[0019] 본 발명의 다른 측면은, 송신수단과 수신수단의 사이에 연결된 네트워크의 통신속도를 측정하는 단계; 상기 송신수단의 제1 연산속도 및 상기 수신수단의 제2 연산속도를 측정하는 단계; 다수의 설정된 압축알고리즘과 암호알고리즘의 조합에 따라 상기 제1 연산속도 및 상기 제2 연산속도가 변할 때, 상기 다수의 설정된 압축알고리즘과 암호알고리즘의 각각의 조합에 대하여, 상기 통신속도와 상기 제1 연산속도의 제1 차이값과, 상기 통신속도와 상기 제2 연산속도의 제2 차이값을 구하는 단계; 상기 제1 차이값과 제2 차이값을 변수로 하여 설정된 각각의 인덱스값을 구하는 단계; 및 상기 인덱스값 중에서 최소값을 갖는 상기 압축알고리즘 및 암호알고리즘의 조합을 선택하는 단계;를 포함하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법을 제공한다.

[0020] 본 발명의 일 실시예에 따르면, 상기 제1 연산속도 및 제2 연산속도는 상기 설정된 압축알고리즘의 압축속도와 압축률, 및 암호알고리즘의 암호화속도에 의해 결정되는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법을 제공한다.

[0021] 본 발명의 다른 실시예에 따르면, 상기 제1 연산속도 및 제2 연산속도는 $\frac{CS+ES}{CRCS+ES}+CS(1-CR)$ 이되, CS, ES, CR은 각각 압축속도, 암호화속도, 압축률인 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법을 제공한다.

[0022] 본 발명의 또 다른 실시예에 따르면, 상기 인덱스값은 $\sqrt{{d_s}^2+{d_r}^2}$ 이되, d_s는 제1 차이값이고, d_r는 제2

차이값인 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법을 제공한다.

[0023] 본 발명의 또 다른 실시예에 따르면, 시간의 경과에 따라 실시간으로 상기 압축알고리즘 및 암호알고리즘의 조합을 선택하는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법을 제공한다.

[0024] 본 발명의 또 다른 실시예에 따르면, 선택된 압축알고리즘 및 암호알고리즘의 조합을 생성하는 제1 연산속도와 제2 연산속도가 통신속도와 같도록 제어하는 단계를 더 포함하는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법을 제공한다.

[0025] 본 발명의 또 다른 실시예에 따르면, 상기 제1 연산속도 또는 제2 연산속도 중에서 통신속도보다 빠른 연산속도의 경우에는 연산속도를 낮추어 상기 통신속도와 같도록 제어하고, 상기 제1 연산속도 또는 제2 연산속도 중에서 통신속도보다 느린 연산속도의 경우에는 연산속도를 높여 상기 통신속도와 같도록 제어하는 것을 특징으로 하는 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택방법을 제공한다.

[0026] 본 발명의 또 다른 측면은, 상기한 방법을 컴퓨터에서 수행하도록 상기 각각의 단계를 실행시키기 위한 명령어를 기록한 컴퓨터 판독가능 기록매체를 제공한다.

발명의 효과

[0027] 본 발명에 따르면, 송신측 및 수신측의 연산속도와 네트워크의 통신속도에 대한 복잡한 수학적 모델링이 없이도, 매우 손쉽고 직관적으로 최적의 압축알고리즘 및 암호알고리즘을 선택할 수 있으므로, 효율적인 통신을 가능하게 한다.

도면의 간단한 설명

[0028] 도 1은 본 발명의 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택과 연산속도 제어를 위한 시스템의 구성도이다.

도 2는 본 발명에 따른 플로팅 스케일의 이동원리를 도시한 개략도이다.

도 3은 본 발명에 따른 통신속도와 제1 연산속도의 차이값 및 통신속도와 제2 연산속도의 차이값에 따라 인덱스 값을 구하는 원리를 도시한 도면이다.

도 4는 본 발명에 따른 송신수단에서 버퍼를 통하여 데이터를 전송하는 경우에 언더플로우가 발생한 경우를 도식화한 개략도이다.

도 5는 본 발명에 따른 송신수단에서 버퍼를 통하여 데이터를 전송하는 경우에 오버플로우가 발생한 경우를 도식화한 개략도이다.

도 6은 본 발명에 따른 수신수단에서 버퍼를 통하여 데이터를 수신하는 경우에 언더플로우가 발생한 경우를 도식화한 개략도이다.

도 7은 본 발명에 따른 수신수단에서 버퍼를 통하여 데이터를 수신하는 경우에 오버플로우가 발생한 경우를 도식화한 개략도이다.

도 8은 본 발명에 따른 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택과 연산속도 제어를 위한 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 이하, 첨부된 도면을 참조하여 본 발명의 실시형태를 설명한다. 그러나, 본 발명의 실시형태는 여러 가지의 다른 형태로 변형될 수 있으며, 본 발명의 범위가 이하 설명하는 실시형태로만 한정되는 것은 아니다. 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있으며, 도면상의 동일한 부호로 표시되는 요소는 동일한 요소이다.

[0030] 도 1은 본 발명의 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택과 연산속도 제어를 위한 시스템의 구성도이다. 도 1을 참조하면, 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택시스템은, 통신속도 측정부 (100), 연산속도 측정부(200), 제1 연산부(300), 제2 연산부(400), 알고리즘 조합 선택부(500)를 포함한다.

[0031] 통신속도 측정부(100)는 송신수단과 수신수단의 사이에 연결된 네트워크의 통신속도를 실시간으로 측정하고, 연산속도 측정부(200)는 송신수단의 제1 연산속도 및 수신수단의 제2 연산속도를 실시간으로 측정한다.

[0032] 제1 연산부(300)는 다수의 설정된 압축알고리즘과 암호알고리즘의 조합에 따라 제1 연산속도 및 제2 연산속도가 변할 때, 다수의 설정된 압축알고리즘과 암호알고리즘의 각각의 조합에 대하여, 통신속도와 제1 연산속도의 제1 차이값과, 통신속도와 제2 연산속도의 제2 차이값을 구하고, 제2 연산부(400)는 제1 차이값과 제2 차이값을 변수로 하여 설정된 각각의 인덱스값을 구한다.

[0033] 알고리즘 조합 선택부(500)는 송신수단 및 수신수단에서 플로팅스케일(floating scale)을 일측과 타측(예를 들어, 상부와 하부)으로 이동시켜 실시간으로 인덱스값 중에서 최소값을 갖는 압축알고리즘 및 암호알고리즘의 조합을 선택하게 한다. 즉, 알고리즘 조합 선택부(500)는 송신수단 또는 수신수단의 연산속도를 나타내는 각각의 플로팅 스케일의 위치를 정하도록 하여 압축알고리즘 및 암호알고리즘의 조합을 선택하게 한다.

[0034] 압축알고리즘 및 암호알고리즘의 조합은 무 압축 알고리즘과 AES(Advanced Encryption Standard) 알고리즘의 조합, RLE(Run -Length Encoding) 알고리즘과 AES 알고리즘의 조합, LZO(Lempel-Ziv-Oberhumer) 알고리즘과 AES 알고리즘의 조합, GZIP(Gnu ZIP) 알고리즘과 AES 알고리즘의 조합, 또는 BZIP(Bnu ZIP) 알고리즘과 AES 알고리즘의 조합 중에서 어느 하나일 수 있으며, 이들 조합에만 한정되지 않고 기타 다른 조합도 가능하다. 예를 들어, 상기 예에서는 암호알고리즘에 있어서 AES만을 사용하였지만, 기타 다른 암호알고리즘을 적용하는 것도 가능하다.

[0035] 연산속도 제어부(600)는 선택된 압축알고리즘 및 암호알고리즘의 조합을 생성하는 제1 연산속도와 제2 연산속도가 통신속도와 같도록 제어한다. 알고리즘 조합 선택부(500)가 최소값을 갖는 압축알고리즘 및 암호알고리즘의 조합을 선택한 후에도 제1 연산속도 및 제2 연산속도가 통신속도와 같지는 않으므로, 제1 연산속도 및 제2 연산속도를 통신속도와 같도록 하여 언더플로우 또는 오버플로우가 발생하지 않도록 하기 위함이다.

[0036] 도 2는 본 발명에 따른 플로팅 스케일의 이동원리를 도시한 개략도이다. 도 2를 참조하면, 플로팅 스케일은 압축알고리즘과 암호알고리즘의 조합에 따라 이동할 수 있음을 알 수 있는데, 무압축 알고리즘과 AES(Advanced Encryption Standard) 알고리즘의 조합을 a로 나타내고, RLE(Run -Length Encoding) 알고리즘과 AES 알고리즘의 조합을 b로 나타내며, LZO(Lempel-Ziv-Oberhumer) 알고리즘과 AES 알고리즘의 조합을 c로 나타내며, GZIP(Gnu ZIP) 알고리즘과 AES 알고리즘의 조합을 d로 나타내며, 또는 BZIP(Bnu ZIP) 알고리즘과 AES 알고리즘의 조합을 e로 나타낼 수 있다. 여기서, AES, LZO, GZIP, BZIP은 압축알고리즘이고, AES는 암호알고리즘이다.

[0037] 이때, 각 눈금은 실 처리속도를 나타내는데, 일 예로 실 처리속도가 빠를수록 상부에 위치하도록 하고 실 처리속도가 느릴수록 하부에 위치하도록 하여 설계할 수 있다. 예를 들어, 가장 상부에 위치하는 a(무압축 알고리즘과 AES 알고리즘의 조합)가 실 처리속도가 가장 빠르며, 가장 하부에 위치하는 e(BZIP 알고리즘과 AES 알고리즘의 조합)가 실 처리속도가 가장 느리다. 여기서, 실 처리속도는 연산속도와 압축알고리즘의 압축률이 반영되어 계산된다. 즉, 압축을 통한 이득과 발생 예상이 가능한 오버헤드가 모두 고려되어 실 처리속도를 구하게 되는 것이며, 송신수단 및 수신수단의 플로팅 스케일은 연산속도 및 통신속도에 따라 상하로 이동한다.

[0038] 한편, 압축알고리즘마다 압축속도와 압축률이 다르고, 암호알고리즘마다 암호화속도가 다르기 때문에, 플로팅 스케일은 압축속도, 압축률, 암호화속도에 의해 영향을 받아 최적의 압축알고리즘 및 암호알고리즘을 선택하도록 이동하게 된다. 즉, 압출률은 매우 좋으나 압축속도가 매우 느릴 경우에는 압축을 하게 되어 암호화를 해야할 양이 줄어들게 되는 장점이 있지만 압축시간이 많이 소요된다는 단점이 있고, 압축률은 좋지 않으나 압축속도가 매우 빠를 경우에는 압축속도가 매우 빠르나 압축률이 낮아 암호화를 해야할 양이 상대적으로 많아진다는 단점이 있다. 이와 같이, 각각의 압축알고리즘의 압축률과 압축속도 및 암호알고리즘의 암호화속도에 따라 장점과 단점이 있는데, 이들을 모두 반영하기 위한 연산속도 V_1을 수학식 1과 같이 적용한다.

수학식 1

[0039] $$V_1 = \frac{CS+ES}{CRCS+ES} + CS(1-CR)$$

[0040] 여기서, CS : 압축속도

[0041] ES : 암호화속도

[0042] CR : 압축률

[0043] 수학식 1의 우변은 제1항인 $\frac{CS+ES}{CRCS+ES}$ 과 제2항인 $CS(1-CR)$ 으로 구분된다. 제1항은 압축알고리즘과 암호알고리즘의 전체 속도를 구하는 항이고, 제2항은 압축알고리즘의 적용으로 전체 크기가 줄어드는 속도를 구하는 항인데, 제1항 및 제2항의 유도 원리를 살펴보면 다음과 같다.

[0044] 제1항은 압축속도와 암호속도의 합을 나타내는 것으로서, 압축과 암호화를 수행하였을 때의 속도를 구하는 항이다. 압축을 수행할 경우, 압축률에 따라 크기가 줄어들어 암호화를 해야할 양이 줄어들기 때문에 압축속도 및 암호속도에 영향을 미치기 때문이다.

[0045] 전체 암축 및 암호화해야할 알고리즘의 크기를 S라 하면, 압축속도와 암호속도의 합 V_2는 전체 암축 및 암호화해야할 알고리즘의 크기를 압축 및 암호화하는 시간으로 나누어 수학식 2와 같이 구할 수 있다.

수학식 2

[0046] $$V_2 = \frac{S}{\frac{S}{CS} + \frac{SCR}{ES}} = \frac{CS+ES}{CRCS+ES}$$

[0047] 제2항은 전체 압축알고리즘의 크기가 줄어드는 속도를 나타내는 것으로서, 전체 압축알고리즘의 크기가 줄어드는 속도 V_3는 전체 압축알고리즘이 줄어든 크기를 압축시간으로 나누어 수학식 3과 같이 구할 수 있다.

수학식 3

[0048] $$V_3 = \frac{S-CRS}{S/CS} = CS(1-CR)$$

[0049] 도 3은 본 발명에 따른 통신속도와 제1 연산속도의 차이값 및 통신속도와 제2 연산속도의 차이값에 따라 인덱스 값을 구하는 원리를 도시한 도면이다. 도 3을 도 2와 함께 참조하면, 송신수단의 플로팅 스케일과 수신수단의 플로팅 스케일의 위치를 보이고 있는데, 플로팅 스케일의 위치가 연산속도를 나타낸다. 즉, 송신수단의 프로팅 스케일이 나타내는 위치가 제1 연산속도를 나타내고, 수신수단의 플로팅 스케일이 나타내는 위치가 제2 연산속도를 나타낸다.

[0050] 이때, 통신속도와 제1 연산속도의 차이값을 ds로 나타내고, 통신속도와 제2 연산속도의 차이값을 dr로 나타낼 때, 설정된 인덱스값 Index는 수학식 4와 같이 구한다.

수학식 4

[0051] $$Index=\sqrt{d_s{}^2+d_r{}^2}$$

[0052] 수학식 4에서 ds와 dr을 각각 평면좌표에서 횡축 및 종축의 좌표라 할 때, Index는 이들 좌표 사이의 거리와 동일하다.

[0053] 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘을 선택할 때, 제1 연산속도가 a, b, c, d, e이고 제2 연산속도가 a', b', c', d', e' 인 경우, Index가 최소값일 경우의 압축알고리즘 및 암호알고리즘의 조합이 선택된다. 즉, Index가 최소값을 갖는 제1 연산속도(송신수단의 연산속도) 및 제2 연산속도(수신수단의 연산속도)가 각각 b, b' 라면, 송신수단과 수신수단은 모두 RLE 알고리즘 및 AES 알고리즘의 조합을 선택하게 된다.

[0054] 도 4는 본 발명에 따른 송신수단에서 버퍼를 통하여 데이터를 전송하는 경우에 언더플로우가 발생한 경우를 도식화한 개략도이다. 도 4를 참조하면, 송신수단에서 압축 및 암호화 후 버퍼를 통하여 데이터를 전송할 때, 제1 연산속도가 통신속도보다 느리게 되어 언더플로우(underflow)가 발생함을 알 수 있다.

[0055] 언더플로우가 발생했을 때, 송신수단의 플로팅 스케일을 하부로 이동시켜 제1 연산속도를 빠르게 하는 압축알고리즘 및 암호알고리즘이 선택된다.

[0056] 도 5는 본 발명에 따른 송신수단에서 버퍼를 통하여 데이터를 전송하는 경우에 오버플로우가 발생한 경우를 도식화한 개략도이다. 도 5를 참조하면, 송신수단에서 압축 및 암호화 후 버퍼를 통하여 데이터를 전송할 때, 제1 연산속도가 통신속도보다 빠르게 되어 오버플로우(overflow)가 발생함을 알 수 있다.

[0057] 오버플로우가 발생했을 때, 송신수단의 플로팅 스케일을 상부로 이동시켜 제1 연산속도를 느리게 하는 압축알고리즘 및 암호알고리즘이 선택된다.

[0058] 도 6은 본 발명에 따른 수신수단에서 버퍼를 통하여 데이터를 수신하는 경우에 언더플로우가 발생한 경우를 도식화한 개략도이다. 도 6을 참조하면, 수신수단에서 버퍼를 통하여 데이터를 수신한 후 비 압축 및 해독할 때, 제2 연산속도가 통신속도보다 느리게 되어 언더플로우가 발생함을 알 수 있다.

[0059] 언더플로우가 발생했을 때, 수신수단의 플로팅 스케일을 하부로 이동시켜 제2 연산속도를 빠르게 하는 압축알고리즘 및 암호알고리즘이 선택된다.

[0060] 도 7은 본 발명에 따른 수신수단에서 버퍼를 통하여 데이터를 수신하는 경우에 오버플로우가 발생한 경우를 도식화한 개략도이다. 도 7을 참조하면, 수신수단에서 버퍼를 통하여 데이터를 수신한 후 비 압축 및 해독할 때, 제2 연산속도가 통신속도보다 빠르게 되어 오버플로우가 발생함을 알 수 있다.

[0061] 오버플로우가 발생했을 때, 수신수단의 플로팅 스케일을 상부로 이동시켜 제2 연산속도를 느리게 하는 압축알고리즘 및 암호알고리즘이 선택된다.

[0062] 도 8은 본 발명에 따른 최적화된 통신환경을 위한 압축알고리즘 및 암호알고리즘 선택과 연산속도 제어를 위한 방법의 흐름도이다. 도 8을 도 1과 함께 살펴보기로 한다.

[0063] 먼저, 통신속도 측정부(100)는 송신수단과 수신수단의 사이에 연결된 네트워크의 통신속도를 측정하고, 연산속

도 측정부(200)는 송신수단의 제1 연산속도 및 수신수단의 제2 연산속도를 측정한다(S100).

[0064] S100 단계 이후, 제1 연산부(300)가 다수의 설정된 압축알고리즘과 암호알고리즘의 조합에 따라 제1 연산속도 및 제2 연산속도가 변할 때, 다수의 설정된 압축알고리즘과 암호알고리즘의 각각의 조합에 대하여, 통신속도와 제1 연산속도의 제1 차이값과, 통신속도와 제2 연산속도의 제2 차이값을 구한다(S200).

[0065] S200 단계 이후, 제2 연산부(400)가 제1 차이값과 제2 차이값을 변수로 하여 설정된 각각의 인덱스값을 구한다(S300). 예를 들어, 인덱스값(Index)은 $Index=\sqrt{d_s^{\,2}+d_r^{\,2}}$ 과 같이 설정하여 제1 차이값 ds와 제2 차이값 dr을 구하여 구할 수 있다.

[0066] S300 단계 이후, 알고리즘 조합 선택부(500)가 인덱스값 중에서 최소값을 갖는 압축알고리즘 및 암호알고리즘의 조합을 선택한다(S400). 즉, 알고리즘 조합 선택부(500)는 송신수단 및 수신수단의 플로팅 스케일을 이동시켜 인덱스값이 최소로 되는 압축알고리즘 및 암호알고리즘의 조합을 선택하도록 한다.

[0067] S400 단계 이후, 연산속도 제어부(600)가 제1 연산속도(또는 제2 연산속도)가 통신속도보다 빠른지를 판단한다(S500). 제1 연산속도(또는 제2 연산속도)가 통신속도보다 빠른 경우에는 오버플로우가 발생한 것이고, 제1 연산속도(또는 제2 연산속도)가 통신속도보다 느린 경우에는 언더플로우가 발생한 것인데, 이와 같이 오버플로우 또는 언더플로우의 여부를 판단하기 위함이다.

[0068] S500 단계 이후, 제1 연산속도(또는 제2 연산속도)가 통신속도보다 빠른 경우에는 연산속도 제어부(600)가 제1 연산속도(또는 제2 연산속도)를 낮추어 통신속도와 같도록 제어하고(S610), 제1 연산속도(또는 제2 연산속도)가 통신속도보다 느린 경우에는 연산속도 제어부(600)가 제1 연산속도(또는 제2 연산속도)를 높여 통신속도와 같도록 제어한다(S620). 이와 같이, 제1 연산속도(또는 제2 연산속도)를 통신속도와 같도록 제어함으로써, 오버플로우 또는 언더플로우가 발생하지 않도록 한다.

[0069] 상기한 바와 같은 최적화된 통신환경을 위한 압축알고리즘 선택방법은, 이와 같은 방법을 컴퓨터에서 수행하도록 각각의 단계를 실행시키기 위한 명령어를 기록한 컴퓨터 판독가능 기록매체에도 기록되어 사용자에 의해 컴퓨터에서 판독될 수 있다.

[0070] 본 발명은 상술한 실시형태 및 첨부된 도면에 의해 한정되지 아니한다. 첨부된 청구범위에 의해 권리범위를 한정하고자 하며, 청구범위에 기재된 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 다양한 형태의 치환, 변형 및 변경이 가능하다는 것은 당 기술분야의 통상의 지식을 가진 자에게 자명할 것이다.

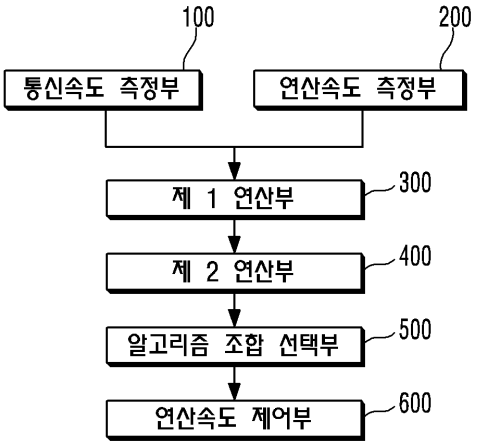
부호의 설명

[0071]

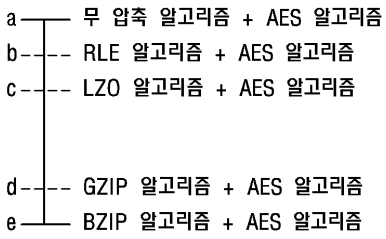
100 : 통신속도 측정부	200 : 연산속도 측정부
300 : 제1 연산부	400 : 제2 연산부
500 : 알고리즘 조합 선택부	600 : 연산속도 제어부

도면

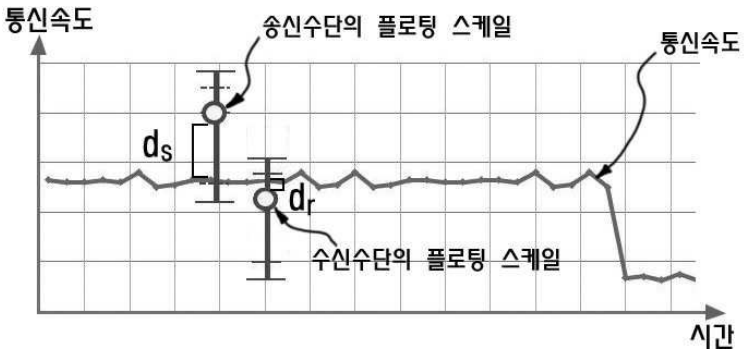
도면1



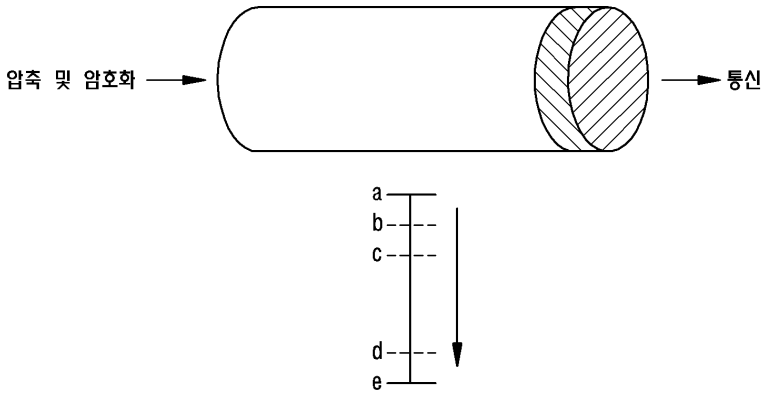
도면2



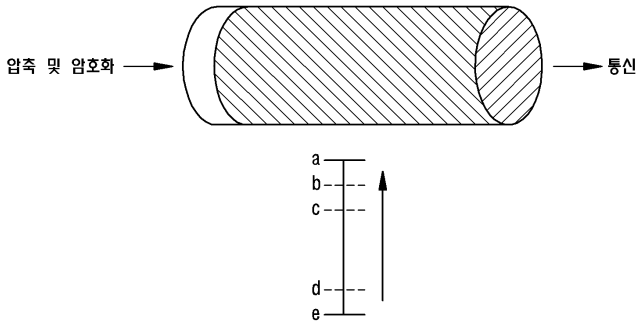
도면3



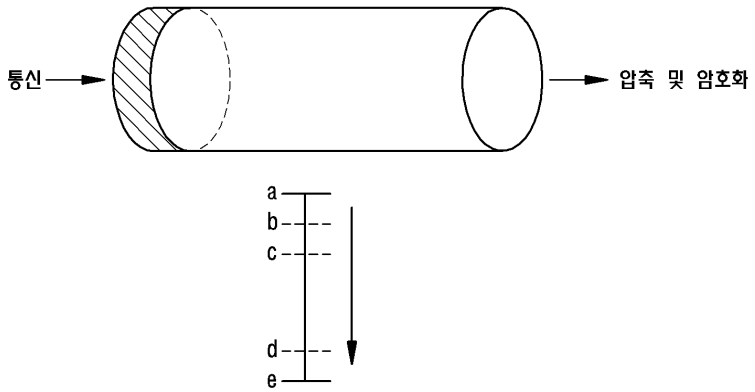
도면4



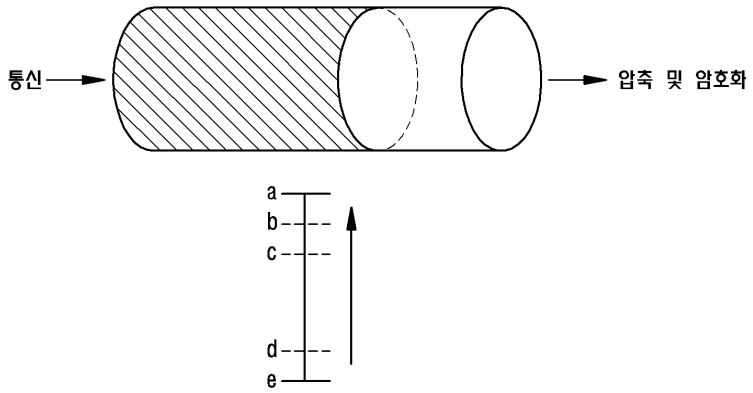
도면5



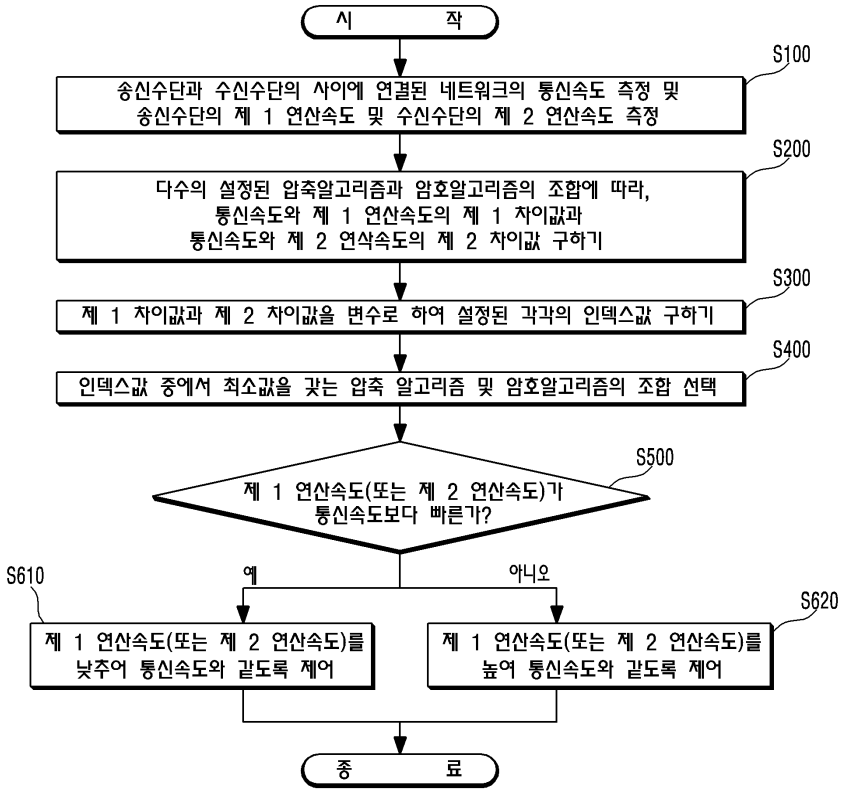
도면6



도면7


통신
압축 및 암호화
a
b
c
d
e

도면8


시 작
S100
송신수단과 수신수단의 사이에 연결된 네트워크의 통신속도 측정 및
송신수단의 제 1 연산속도 및 수신수단의 제 2 연산속도 측정
S200
다수의 설정된 압축알고리즘과 암호알고리즘의 조합에 따라,
통신속도와 제 1 연산속도의 제 1 차이값과
통신속도와 제 2 연삭속도의 제 2 차이값 구하기
S300
제 1 차이값과 제 2 차이값을 변수로 하여 설정된 각각의 인덱스값 구하기
S400
인덱스값 중에서 최소값을 갖는 압축 알고리즘 및 암호알고리즘의 조합 선택
S500
제 1 연산속도(또는 제 2 연산속도)가
통신속도보다 빠른가?
예
아니오
S610
제 1 연산속도(또는 제 2 연산속도)를
낮추어 통신속도와 같도록 제어
S620
제 1 연산속도(또는 제 2 연산속도)를
높여 통신속도와 같도록 제어
종 료