

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2014-0062866 (43) 공개일자 2014년05월26일
(51) 국제특허분류(Int. Cl.) H04W 40/18 (2009.01) H04W 84/18 (2009.01)	(71) 출원인 경희대학교 산학협력단 경기도 용인시 기흥구 덕영대로 1732, 국제캠퍼스 내 (서천동, 경희대학교)	
(21) 출원번호 10-2012-0129743		
(22) 출원일자 2012년11월15일	(72) 발명자	
심사청구일자 2012년11월15일	홍충선 경기 용인시 수지구 상현로 30-10, 233동 101호 (상현동, 정원3차상떼빌아파트)	
	김가린 경남 통영시 원문로 11, 101동 1307호 (북신동, 진우마리나타운)	
	조웅준 경기 수원시 영통구 청명로59번길 54, 103호 (영통동)	
	(74) 대리인 서재승	

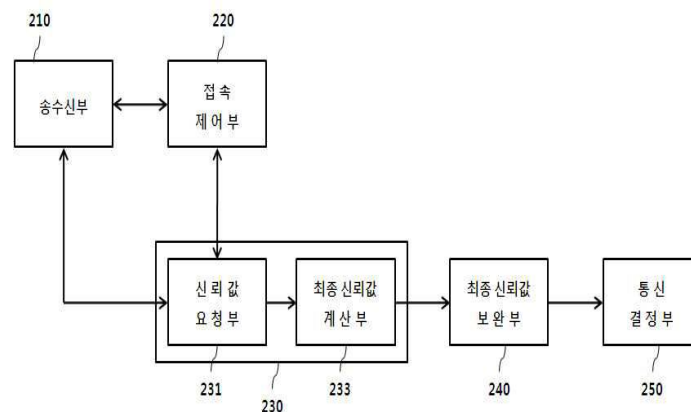
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 애드-혹 통신 네트워크에서 신뢰값에 기초한 데이터 교환 방법

(57) 요약

본 발명은 애드-혹 통신 네트워크에서 데이터 교환 방법에 관한 것으로, 보다 구체적으로 상대방의 신뢰값에 기초하여 상대방과의 데이터 교환 여부를 결정함으로써 임의의 통신 노드들이 자유롭게 가입하거나 탈퇴 가능한 애드-혹 통신 네트워크에서 개인 정보 누출, 스팸 정보 배포 등을 수행하는 악의 사용자로부터 사용자를 보호할 수 있는 데이터 교환 방법에 관한 것이다.

대표도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호	0891105002-120010100
부처명	방송통신위원회
연구사업명	방송통신기술개발사업
연구과제명	미래 인터넷을 위한 센서 네트워크 관리 프레임워크 개발 (초정밀 측정 및 분석 기술 연구)
기 여 율	1/1
주관기관	경희대학교 산학협력단
연구기간	2012.03.01 ~ 2013.02.28

특허청구의 범위

청구항 1

다수의 노드를 구비하는 통신 네트워크에서 노드 신뢰도에 기초하여 데이터를 교환하는 방법에 있어서,

제1 노드에서 제2 노드로부터 접속 요청 메시지를 수신하는 단계;

상기 접속 요청 메시지에 응답하여 상기 제1 노드에서 상기 제2 노드로 접속 응답 메시지를 송신하는 단계;

상기 제1 노드에서 상기 제1 노드의 주변 노드로 상기 주변 노드가 가진 상기 제2 노드의 상대 신뢰값을 요청하는 단계; 및

상기 주변 노드로부터 수신한 상기 상대 신뢰값으로부터 상기 제2 노드의 최종 신뢰값을 계산하는 단계를 포함하는 것을 특징으로 하는 데이터 교환 방법.

청구항 2

제 1 항에 있어서, 상기 통신 네트워크는

에드-hoc 네트워크(ad-hoc)인 것을 특징으로 하는 데이터 교환 방법.

청구항 3

제 2 항에 있어서, 상기 데이터 교환 방법은

상기 접속 응답 메시지에 응답하여 상기 제1 노드에서 상기 제2 노드로부터 상기 제2 노드의 자신 신뢰값을 수신하는 단계를 더 포함하며,

상기 최종 신뢰값은 상기 자신 신뢰값과 상기 상대 신뢰값으로부터 계산되는 것을 특징으로 하는 데이터 교환 방법.

청구항 4

제 3 항에 있어서, 상기 데이터 교환 방법은

상기 제1 노드에서 상기 최종 신뢰값이 임계값을 초과하는지 판단하여 상기 제1 노드와 제2 노드 사이의 데이터 교환 여부를 결정하는 단계를 더 포함하는 것을 특징으로 하는 데이터 교환 방법.

청구항 5

제 4 항에 있어서, 상기 자신 신뢰값은

상기 제2 노드로부터 상기 주변 노드로 송신되는 교환 데이터의 악의성에 기초하여 상기 제2 노드에서 증감되어 계산되는 것을 특징으로 데이터 교환 방법.

청구항 6

제 4 항에 있어서, 상기 상대 신뢰값은

상기 제2 노드와 데이터를 교환한 상기 주변 노드에서 상기 제2 노드로부터 수신한 교환 데이터의 악의성에 기초하여 증감되어 계산되는 것을 특징으로 하는 데이터 교환 방법.

청구항 7

제 3 항에 있어서, 상기 최종 신뢰값(FT)은 아래의 수학적식(1)에 의해 계산되며,

[수학식 1]

$$FT = \frac{\alpha \times T_i + \beta \times \sum_{j=1}^N T_{ij}}{1+N}$$

여기서 T_i 는 상기 제2 노드(i)의 자신 신뢰값이고 상기 T_{ij} 는 상기 제2 노드(i)에 대한 상기 주변 노드(j)의 상대 신뢰값이며, α 와 β 는 각각 상기 자신 신뢰값과 상대 신뢰값에 대한 가중치인 것을 특징으로 하는 데이터 교환 방법.

청구항 8

제 3 항에 있어서, 상기 데이터 교환 방법은

상기 상대 신뢰값의 평균값과 상기 자신 신뢰값의 차이값을 계산하고, 상기 차이값이 임계 차이값보다 큰지 판단하는 단계; 및

상기 상대 신뢰값의 평균값과 상기 자신 신뢰값의 차이값이 임계 차이값보다 큰 경우 상기 최종 신뢰값을 감소하여 상기 최종 신뢰값을 보완하는 단계를 더 포함하는 것을 특징으로 하는 데이터 교환 방법.

청구항 9

통신 네트워크에 존재하는 제1 노드로부터 접속 요청 메시지를 수신하는 경우, 주변 노드로 상기 제1 노드의 상대 신뢰값을 요청하는 신뢰값 요청부;

상기 주변 노드로부터 상기 상대 신뢰값을 수신하는 경우, 상기 상대 신뢰값에 기초하여 상기 제1 노드의 최종 신뢰값을 계산하는 신뢰값 계산부; 및

상기 최종 신뢰값이 임계값을 초과하는지 판단하여 상기 제1 노드와 데이터 교환 여부를 결정하는 통신 결정부를 포함하는 것을 특징으로 하는 통신 노드.

청구항 10

제 9 항에 있어서, 상기 통신 네트워크는

에드혹 네트워크인 것을 특징으로 하는 통신 노드.

청구항 11

제 10 항에 있어서,

상기 신뢰값 요청부는 상기 제1 노드로 상기 제1 노드의 자신 신뢰값을 요청하며,

상기 신뢰값 계산부는 상기 상대 신뢰값과 상기 자신 신뢰값에 기초하여 아래의 수학식(2)에 따라 계산하며,

[수학식 2]

$$FT = \frac{\alpha \times T_i + \beta \times \sum_{j=1}^N T_{ij}}{1+N}$$

여기서 T_i 는 상기 제1 노드(i)의 자신 신뢰값이고 상기 T_{ij} 는 상기 제1 노드(i)에 대한 상기 주변 노드(j)의 상대 신뢰값이며, α 와 β 는 각각 상기 자신 신뢰값과 상대 신뢰값에 대한 가중치인 것을 특징으로 하는 통신 노드.

청구항 12

제 11 항에 있어서, 상기 통신 노드는

상기 상대 신뢰값의 평균값과 상기 자신 신뢰값의 차이값에 기초하여 상기 최종 신뢰값을 보완하는 보완부를 더 포함하는 것을 특징으로 하는 통신 노드.

명세서

기술 분야

[0001] 본 발명은 애드-혹 통신 네트워크에서 데이터 교환 방법에 관한 것으로, 보다 구체적으로 상대방의 신뢰값에 기초하여 상대방과의 데이터 교환 여부를 결정함으로써 임의의 통신 노드들이 자유롭게 가입하거나 탈퇴 가능한 애드-혹 통신 네트워크에서 개인 정보 누출, 스캠 정보 배포 등을 수행하는 악의 사용자로부터 사용자를 보호할 수 있는 데이터 교환 방법에 관한 것이다.

배경 기술

[0002] 소셜 네트워크(social network)는 개인이나 집단을 통신 네트워크의 1 노드로 파악하여 실제 현실 사회에서 사람들 사이의 인맥을 형성하는 것과 같이, 통신 네트워크를 통해 서로 데이터를 교환하는 네트워크를 의미한다. 초기 소셜 네트워크 서비스는 인터넷망을 사용하여 그룹을 형성하는 멤버들과 데이터를 교환하는 방식으로 이루어졌지만, 최근에는 애드-혹 네트워크를 통해 시간과 장소에 상관없이 주변에 위치하는 주변 사용자와 서로 데이터를 교환하는 방식으로 이루어지고 있다.

[0003] 애드-혹 네트워크(AD-hoc network)는 노드(node)들에 의해 자율적으로 구성되는 기반 구조가 없는 네트워크로, 네트워크의 구성 및 유지를 위해 기지국이나 액세스 포인트와 같은 기반 네트워크 장치를 필요로 하지 않는다. 애드-혹(Ad-hoc) 노드들은 무선 인터페이스를 사용하여 서로 통신하고, 멀티 홉 라우팅 기능에 의해 무선 인터페이스가 가지는 통신 거리상의 제약을 극복하며, 노드들의 이동이 자유롭기 때문에 네트워크 토폴로지가 동적으로 변화되는 특징이 있다. 애드-혹 네트워크는 완전 독립형이 될 수도 있고, 인터넷 게이트웨이를 거쳐 인터넷과 같은 기반 네트워크와 연동될 수도 있다.

[0004] 이러한 애드-혹 네트워크에서는 임의의 사용자가 어떠한 제한없이 자유롭게 네트워크에 참여하거나 탈퇴 가능하기 때문에, 사용자 중에는 다른 사용자에게 스캠 정보를 제공하거나 다른 사용자들에게 불쾌감을 주는 정보를 제공하는 악의적 사용자가 존재할 수 있다. 또한 애드-혹 네트워크에서는 네트워크의 참여를 제어하는 마스터가 존재하지 않는 이유로, 악의적 사용자가 존재하는 경우에도 악의적 사용자를 네트워크에 제외시킬 수 없다는 문제점을 가진다.

발명의 내용

해결하려는 과제

[0005] 이러한 애드-혹 네트워크에서 악의적 노드에 의해 개인의 정보가 도청될 가능성이 높아지며, 악의적 노드가 의도적으로 통신 네트워크에 접근한 후 특정한 개인의 여러 정보를 얻어 개인의 정보를 유추할 수 있기 때문에 개인의 프라이버시 침해 문제를 일으킬 수 있다. 또한 근접 노드들 간의 통신으로 통신을 제어할 수 있는 중앙 장치가 존재하지 않아 노드 스스로 악의적 노드의 악의적 행동, 예를 들어 스캠 살포, 개인 정보 도출, 유언비어의 배포 등으로부터 사용자를 보호할 기술이 필요하다. 따라서 애드-혹 네트워크 방식의 소셜 네트워크에서는 악의적 사용자를 판단하고 악의적 사용자와의 데이터 교환 여부를 거부할 수 있는 기술이 요구된다.

[0006] 본 발명은 위에서 언급한 종래 소셜 네트워크의 데이터 교환 방법이 가지는 문제점들을 해결하기 위한 것으로, 본 발명이 이루고자 하는 목적은 통신하고자 하는 상대방 사용자의 신뢰도를 판단하고 판단한 신뢰도에 기초하여 상대방 사용자와의 데이터 교환 여부를 결정할 수 있는 데이터 교환 방법을 제공하는 것이다.

[0007] 본 발명이 이루고자 하는 다른 목적은 통신하고자 하는 상대방 사용자의 신뢰도를 상대방 사용자로부터 수신한 상대방 사용자의 자신 신뢰도뿐만 아니라 주변 사용자가 상대방 사용자에게 대해 가지는 상대 신뢰도에 기초하여 상대방 사용자의 신뢰도를 정확하게 판단하여 데이터 교환을 결정할 수 있는 데이터 교환 방법을 제공하는 것이다.

[0008] 본 발명이 이루고자 하는 또 다른 목적은 상대방 사용자가 갖는 자신 신뢰도와 주변 사용자가 상대방 사용자에게 대해 갖는 상대 신뢰도의 차이에 기초하여 상대방 사용자의 최종 신뢰도를 보완할 수 있는 데이터 교환 방법을

제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 목적을 달성하기 위하여, 본 발명에 따른 데이터 교환 방법은 제1 노드에서 제2 노드로부터 접속 요청 메시지를 수신하는 단계와, 접속 요청 메시지에 응답하여 제1 노드에서 제2 노드로 접속 응답 메시지를 송신하는 단계와, 제1 노드에서 제1 노드의 주변 노드로 주변 노드가 가진 제2 노드의 상대 신뢰값을 요청하는 단계와, 주변 노드로부터 수신한 상대 신뢰값으로부터 제2 노드의 최종 신뢰값을 계산하는 단계를 포함한다.

[0010] 여기서 통신 네트워크는 애드-혹 네트워크(ad-hoc) 네트워크인 것을 특징으로 한다.

[0011] 바람직하게, 본 발명에 따른 데이터 교환 방법은 접속 응답 메시지에 응답하여 제1 노드에서 제2 노드로부터 제2 노드의 자신 신뢰값을 수신하는 단계를 더 포함하며, 최종 신뢰값은 자신 신뢰값과 상대 신뢰값으로부터 계산된다.

[0012] 더욱 바람직하게, 본 발명에 따른 데이터 교환 방법은 제1 노드에서 최종 신뢰값이 임계값을 초과하는지 판단하여 제1 노드와 제2 노드 사이의 데이터 교환 여부를 결정하는 단계를 더 포함한다.

[0013] 여기서 자신 신뢰값은 제2 노드로부터 주변 노드로 송신되는 교환 데이터의 악의성에 기초하여 제2 노드에서 증감되어 계산되는 것을 특징으로 한다.

[0014] 여기서 상대 신뢰값은 제2 노드와 데이터를 교환한 주변 노드에서 제2 노드로부터 수신한 교환 데이터의 악의성에 기초하여 증감되어 계산되는 것을 특징으로 한다.

[0015] 바람직하게, 최종 신뢰값(FT)은 아래의 수학식에 의해 계산되며,

[0016] [수학식]

$$FT = \frac{\alpha \times T_i + \beta \times \sum_{j=1}^N T_{ij}}{1 + N}$$

[0017]

[0018] 여기서 T_i 는 제2 노드(i)의 자신 신뢰값이고 T_{ij} 는 제2 노드(i)에 대한 주변 노드(j)의 상대 신뢰값이며, α 와 β 는 각각 자신 신뢰값과 상대 신뢰값에 대한 가중치인 것을 특징으로 한다.

[0019] 바람직하게, 본 발명에 따른 데이터 교환 방법은 상대 신뢰값의 평균값과 자신 신뢰값의 차이값을 계산하고 차이값이 임계 차이값보다 큰지 판단하는 단계와, 상대 신뢰값의 평균값과 자신 신뢰값의 차이값이 임계 차이값보다 큰 경우 최종 신뢰값을 감소하여 최종 신뢰값을 보완하는 단계를 더 포함한다.

[0020] 본 발명에 따른 통신 노드는 통신 네트워크에 존재하는 제1 노드로부터 접속 요청 메시지를 수신하는 경우 주변 노드로 제1 노드의 상대 신뢰값을 요청하는 신뢰값 요청부와, 주변 노드로부터 상대 신뢰값을 수신하는 경우 상대 신뢰값에 기초하여 제1 노드의 최종 신뢰값을 계산하는 신뢰값 계산부와, 최종 신뢰값이 임계값을 초과하는지 판단하여 제1 노드와 데이터 교환 여부를 결정하는 통신 결정부를 포함한다.

[0021] 여기서 신뢰값 요청부는 제1 노드로 상기 제1 노드의 자신 신뢰값을 요청하며,

[0022] 신뢰값 계산부는 상대 신뢰값과 자신 신뢰값에 기초하여 아래의 수학식에 따라 계산하며,

[0023] [수학식]

$$FT = \frac{\alpha \times T_i + \beta \times \sum_{j=1}^N T_{ij}}{1 + N}$$

[0024]

[0025] T_i 는 상기 제1 노드(i)의 자신 신뢰값이고 T_{ij} 는 제1 노드(i)에 대한 주변 노드(j)의 상대 신뢰값이며, α 와 β 는 각각 자신 신뢰값과 상대 신뢰값에 대한 가중치이다.

[0026] 바람직하게, 본 발명에 따른 통신 노드는 상대 신뢰값의 평균값과 자신 신뢰값의 차이값에 기초하여 최종 신뢰값을 보완하는 보완부를 더 포함한다.

발명의 효과

[0027] 본 발명에 따른, 소셜 네트워크에서 노드 사이의 데이터 교환 방법은 종래 데이터 교환 방법과 비교하여 다음과 같은 다양한 효과들을 가진다.

[0028] 첫째, 본 발명에 따른 데이터 교환 방법은 통신하고자 하는 상대방 사용자의 신뢰도를 판단하고 판단한 신뢰도에 기초하여 상대방 사용자와의 데이터 교환을 결정함으로써, 통신 네트워크에서 악의적 사용자를 판단하여 신뢰있는 데이터 교환이 가능하다.

[0029] 둘째, 본 발명에 따른 데이터 교환 방법은 통신하고자 하는 상대방 사용자의 신뢰도를 상대방 사용자 자신이 갖는 자신 신뢰도뿐만 아니라 주변 사용자가 상대방 사용자에 대해 갖는 상대 신뢰도에 기초하여 상대방 사용자의 신뢰도를 계산함으로써, 상대방 사용자와 이전 데이터 교환을 통해 상대방 사용자에 대한 다수 주변 사용자의 신뢰도에 기초하여 상대방 사용자의 신뢰도를 정확하게 판단할 수 있다.

[0030] 셋째, 본 발명에 따른 데이터 교환 방법은 상대방 사용자가 갖는 자신 신뢰도와 주변 사용자가 상대방 사용자에 대해 갖는 상대 신뢰도의 차이에 기초하여 상대방 사용자의 최종 신뢰도를 보완함으로써, 상대방 사용자가 자신 신뢰도를 임의로 조작하는지를 판단하여 임의 조작된 자신 신뢰도에 기초하여 계산한 최종 신뢰도를 보완할 수 있다.

도면의 간단한 설명

[0031] 도 1은 애드-혹 네트워크에서 본 발명에 따른 데이터 교환 방법을 설명하기 위한 도면이다.

도 2는 자신 신뢰값 또는 상대 신뢰값을 계산하는 본 발명에 따른 통신 노드를 설명하기 위한 기능 블록도이다.

도 3은 최종 신뢰값을 계산하는 본 발명에 따른 통신 노드를 설명하기 위한 기능 블록도이다.

도 4는 통신 네트워크에서 송수신되는 메시지를 설명하기 위한 도면이다.

도 5는 본 발명에 따른 데이터 교환 방법을 설명하기 위한 흐름도이다.

도 6은 본 발명에 따른 자신 신뢰값을 계산하는 방법을 설명하는 흐름도이다.

도 7은 본 발명에 따른 상대 신뢰값을 계산하는 방법을 설명하는 흐름도이다.

도 8은 주변 노드에 저장되어 있는 상대방 노드의 상대 신뢰값의 일 예를 도시하고 있다.

발명을 실시하기 위한 구체적인 내용

[0032] 이하 첨부한 도면을 참고로 본 발명에 따른 소셜 네트워크에서 노드 사이의 데이터 교환 방법에 대해 보다 구체적으로 살펴본다. 이하에서 설명하는 사용자 노드, 상대방 노드, 주변 노드는 데이터를 송수신하거나 자신 신뢰도 또는 상대 신뢰도를 계산하는 주체에 따라 동일한 통신 노드가 사용자 노드로 동작하거나 상대방 노드 또는 주변 노드로 변경되어 동작한다.

[0033] 도 1은 애드-혹 네트워크에서 본 발명에 따른 데이터 교환 방법을 설명하기 위한 도면이다.

[0034] 도 1을 참고로 보다 구체적으로 살펴보면, 애드-혹 네트워크에는 다수의 통신 노드들이 배포되어 있다. 통신 노드들은 1홉 이내에 위치하는 주변 통신 노드와 데이터 송수신을 통해 데이터를 교환하며, 1홉을 초과하여 위치하는 주변 통신 노드와는 멀티 홉 방식으로 데이터를 교환한다.

[0035] 먼저 사용자 노드(N)는 데이터를 교환하고자 하는 상대방 노드(CN)로부터 접속 요청 메시지를 수신하는 경우, 접속 요청 메시지에 응답하여 상대방 노드(CN)로 접속 응답 메시지를 송신한다. 사용자 노드(N)는 상대방 노드(CN)로부터 접속 요청 메시지를 수신하는 경우 사용자 노드(N)의 주변 노드(NN)로 상대방 노드(CN)의 상대 신뢰값을 요청하며, 사용자 노드(N)로부터 상대 신뢰값 요청을 받은 주변 노드(NN)들 중 상대방 노드(CN)에 대한 상대 신뢰값을 가지는 주변 노드(NN)는 사용자 노드(N)로 상대방 노드(CN)의 상대 신뢰값을 송신한다.

[0036] 사용자 노드(N)는 주변 노드(NN)로부터 수신한 상대방 노드(CN)의 상대 신뢰값 또는 상대방 노드(CN)로부터 수

신한 자신 신뢰값에 기초하여 상대방 노드(CN)의 최종 신뢰값을 계산하며, 계산한 최종 신뢰값에 기초하여 상대방 노드(CN)와 데이터 교환 여부를 결정한다.

[0037] 여기서 상대방 노드(CN)의 초기 자신 신뢰값은 일정 값으로 초기화되어 있는데, 상대방 노드(CN)는 주변 노드(NN)와 데이터 교환을 수행하는 동안 상대방 노드(CN)가 주변 노드(NN)로 송신하는 데이터가 악의적인지 판단하고, 악의적 데이터를 송신할 때마다 자신 신뢰값을 감소시키며, 악의적 데이터가 송신되지 않는 경우 자신 신뢰값을 증가시킨다. 한편, 상대방 노드(CN)와 데이터를 교환한 주변 노드(NN)는 상대방 노드(CN)로부터 수신되는 데이터가 악의적인지 판단하고, 악의적 데이터를 수신할 때마다 상대방 노드(CN)의 상대 신뢰값을 감소시키며 악의적 데이터가 송신되지 않는 경우 상대방 노드(CN)의 상대 신뢰값을 증가시킨다. 자신 신뢰값은 상대방 노드(CN)에 저장되며, 상대 신뢰값은 상대방 노드와 통신을 수행한 각 주변 노드에 저장되어 있다.

[0038] 도 2는 자신 신뢰값 또는 상대 신뢰값을 계산하는 본 발명에 따른 통신 노드를 설명하기 위한 기능 블록도이다.

[0039] 도 2를 참고로 통신 노드가 상대방 단말기로 데이터를 송신하는 사용자 노드로 동작하는 경우 사용자 노드의 자신 신뢰값을 계산하는 통신 노드를 구체적으로 살펴보면, 송수신부(110)는 상대방 노드로부터 데이터 요청 메시지를 수신하는 경우 데이터 요청 메시지에 응답하여 상대방 노드가 요청하는 데이터를 구비하는 데이터 응답 메시지를 상대방 노드로 송신한다. 악의 검색부(120)는 데이터 응답 메시지에 구비되어 있는 데이터에 악의성 데이터가 존재하는지 검색한다. 여기서 악의성 데이터는 데이터 응답 메시지에 구비되어 있는 데이터의 색인어 또는 메타 정보로부터 검색하는데, 본 발명이 적용되는 분야에 따라 악의성 데이터는 상이하게 설정될 수 있다. 예를 들어 채팅을 수행하는 과정에서 송수신되는 채팅 데이터인 경우 송수신되는 채팅 데이터의 색인어와 악의 단어 사전을 비교하여 채팅 데이터가 악의 단어 사전에 포함되어 있는 단어인 경우 악의성 데이터로 검색하거나 데이터 응답 메시지에 구비되어 있는 콘텐츠의 메타 정보에 기초하여 메타 정보가 악의 단어 사전에 포함되어 있는 단어인 경우 악의성 데이터로 검색한다.

[0040] 신뢰값 계산부(130)는 악의 판단부(120)에서 악의 데이터가 검색되는지 여부에 따라, 설정 주기 시간 동안 상대방 노드로 송신되는 데이터에서 악의 데이터가 검색될 때마다 초기 설정되어 있는 사용자 노드의 자신 신뢰값을 감소시킨다. 한편, 신뢰값 계산부(130)는 설정 주기 시간 동안 상대방 노드로 송신되는 데이터에서 악의 데이터가 검색되지 않는 경우 사용자 노드의 자신 신뢰값을 증가시킨다. 신뢰값 계산부(130)에서 계산된 자신 신뢰값은 신뢰값 데이터베이스(140)에 저장되며, 신뢰값 제어부(150)는 사용자 노드가 다른 상대방 노드와 데이터 교환하고자 하는 경우 신뢰값 데이터베이스(140)에서 자신 신뢰값을 추출하여 다른 상대방 노드로 송신 제어한다.

[0041] 한편, 통신 노드가 상대방 단말기로부터 데이터를 수신하는 사용자 노드로 동작하는 경우 상대방 노드의 상대 신뢰값을 계산하는 통신 노드를 구체적으로 살펴보면, 송수신부(110)는 상대방 노드로부터 사용자 노드가 요청하는 데이터를 구비하는 데이터 응답 메시지를 수신한다. 악의 검색부(120)는 수신한 데이터 응답 메시지에 구비되어 있는 데이터에 악의성 데이터가 존재하는지 검색한다.

[0042] 신뢰값 계산부(130)는 악의 판단부(120)에서 악의 데이터가 검색되는지 여부에 따라, 설정 주기 시간 동안 상대방 노드로부터 수신되는 데이터에서 악의 데이터가 검색될 때마다 상대방 노드로부터 수신한 상대방 노드의 상대 신뢰값을 감소시켜 사용자 노드가 보유하는 상대방 노드의 상대 신뢰값을 계산한다. 한편, 신뢰값 계산부(130)는 설정 주기 시간 동안 상대방 노드로 수신되는 데이터에서 악의 데이터가 검색되지 않는 경우 상대방 노드의 상대 신뢰값을 증가시켜 사용자 노드가 보유하는 상대방 노드의 상대 신뢰값을 계산한다. 신뢰값 계산부(130)에서 계산된 상대 신뢰값은 신뢰값 데이터베이스(140)에 상대방 노드의 식별자에 매핑되어 저장되며, 신뢰값 제어부(150)는 주변 노드로부터 상대방 노드의 상대 신뢰값의 요청이 있는 경우 신뢰값 데이터베이스(140)에서 상대방 노드의 상대 신뢰값을 추출하여 주변 노드로 송신 제어한다.

[0043] 바람직하게, 본 발명에서 상대방 노드의 상대 신뢰값은 악의 검색부(120)와 신뢰값 계산부(130)에서 계산되더라도 사용자 노드의 사용자는 상대방 노드로부터 수신한 데이터를 모니터링하여 상대방 노드의 상대 신뢰값을 직접 사용자 인터페이스(160)를 통해 입력할 수 있다. 이러한 경우, 신뢰값 데이터베이스(140)에는 악의 검색부(120)와 신뢰값 계산부(130)에서 계산된 상대방 노드의 상대 신뢰값과 사용자 인터페이스(160)를 통해 입력된 수정 상대 신뢰값이 함께 저장되거나 상대 신뢰값을 수정 상대 신뢰값으로 갱신한다. 신뢰값 제어부(150)는 상대 신뢰값 또는 수정 상대 신뢰값 중 어느 하나 또는 모두를 추출하여 주변 노드로 송신 제어한다.

- [0044] 도 3은 최종 신뢰값을 계산하는 본 발명에 따른 통신 노드를 설명하기 위한 기능 블록도이다.
- [0045] 도 3을 참고로 통신 노드가 사용자 노드로 동작하여 상대방 단말기의 최종 신뢰도를 계산하는 통신 노드를 살펴 보면, 송수신부(210)는 상대방 노드로부터 접속 요청 메시지를 수신하며, 접속 제어부(220)는 접속 요청 메시지에 응답하여 접속 응답 메시지를 생성하여 송수신부(210)를 통해 상대방 노드로 송신 제어한다. 여기서 접속 요청 메시지에는 상대방 노드의 관심 키워드와 상대방 노드의 자신 신뢰값이 포함되어 있으며, 사용자 노드의 접속 제어부(220)는 상대방 노드의 관심 키워드 또는 자신 신뢰값에 기초하여 접속 여부를 1차 결정한다. 접속 제어부(220)는 사용자 노드에 저장되어 있는 관심 키워드와 상대방 노드의 관심 키워드가 일치하는지 여부 또는 자신 신뢰값이 임계 자신 신뢰값을 초과하는지 여부에 따라 접속 여부를 1차 결정한다. 관심 키워드가 일치하거나 상대방 노드의 자신 신뢰값이 임계 자신 신뢰값을 초과하는 경우 접속을 1차 허용하여 접속 응답 메시지를 송신하며, 관심 키워드가 일치하지 않거나 자신 신뢰값이 임계 자신 신뢰값보다 작은 경우 접속을 허용하지 않는 접속 응답 메시지를 송신한다.
- [0046] 접속을 허용하는 접속 응답 메시지를 상대방 노드로 송신하는 경우, 신뢰값 요청부(231)는 송수신부(210)를 통해 사용자 노드에 인접하여 위치하는 주변 노드에 상대방 노드의 상대 신뢰값을 요청한다. 주변 노드 중 이전에 상대방 노드와 데이터를 교환하여 상대방 노드에 대한 상대 신뢰값을 저장하고 있는 주변 노드로부터 송수신부(210)를 통해 상대방 노드의 상대 신뢰값을 수신하는 경우, 최종 신뢰값 계산부(233)는 수신한 상대방 노드의 상대 신뢰값에 기초하여 상대방 노드의 최종 신뢰값을 계산한다.
- [0047] 바람직하게, 신뢰값 계산부(233)는 상대 신뢰값과 자신 신뢰값을 이용하여 상대방 노드의 최종 신뢰값을 계산한다.
- [0048] 최종 신뢰값 보완부(240)는 상대방 노드로부터 수신한 자신 신뢰값과 평균 상대 신뢰값의 차이를 계산하고, 자신 신뢰값과 평균 상대 신뢰값의 차이에 비례하는 보완값을 계산하여 최종 신뢰값을 보완한다. 통신 결정부(250)는 최종 신뢰값에 기초하여 또는 보완한 최종 신뢰값에 기초하여 상대방 노드와 데이터를 교환할지를 결정한다.
- [0049] 도 4는 통신 네트워크에서 송수신되는 메시지를 설명하기 위한 도면이다.
- [0050] 도 4를 참고로 보다 구체적으로 살펴보면, 사용자 노드는 사용자 노드와 데이터를 교환하고자 하는 상대방 노드로부터 접속 요청 메시지를 수신하는 경우(S10), 접속 요청 메시지에 구비되어 있는 상대방 노드 식별자, 상대방 노드의 관심 키워드와 자신 신뢰값에 기초하여 접속 허용 여부를 1차적으로 결정하고 접속 허용 여부를 나타내는 접속 식별자를 구비하는 접속 응답 메시지를 생성하여 상대방 노드로 송신한다(S20).
- [0051] 상대방 노드와의 접속을 허용하는 경우 사용자 노드는 사용자 노드에 인접하여 위치하는 주변 노드들로 신뢰도 요청 메시지(S30)를 송신한다. 신뢰도 요청 메시지에는 상대방 노드의 식별자가 구비되어 있다. 신뢰도 요청 메시지를 수신한 주변 노드들은 상대방 노드의 식별자에 해당하는 상대방 노드의 상대 신뢰값이 주변 노드에 저장되어 있는지 판단하고, 상대방 노드의 상대 신뢰값이 저장되어 있는 경우 신뢰값 응답 메시지에 주변 노드가 저장하고 있는 상대방 노드의 상대 신뢰값을 구비하여 사용자 노드로 송신한다(S40). 예를 들어, 신뢰값 요청 메시지를 수신한 주변 노드 1, 2, 3, 4 중 상대방 노드와 이전에 데이터를 송수신하여 상대방 노드의 상대 신뢰값을 계산하여 저장하고 있는 주변 노드 1, 3, 4로부터 상대방 노드의 상대 신뢰값을 구비하는 신뢰값 응답 메시지를 수신한다.
- [0052] 사용자 노드는 상대방 노드의 자신 신뢰값과 상대방 노드의 상대 신뢰값에 기초하여 상대방 노드와의 데이터 교환 여부를 결정하여 데이터 교환 여부를 나타내는 식별자를 구비하는 통신 결정 메시지를 상대방 노드로 송신하며(S50), 통신 결정 메시지를 수신한 상대방 노드는 통신 결정 메시지에 응답하여 사용자 노드로 통신 응답 메시지를 송신한다(S60). 통신 응답 메시지를 수신한 사용자 노드는 상대방 노드를 신뢰하며 상대방 노드와 데이터를 교환한다.
- [0053] 도 5는 본 발명에 따른 데이터 교환 방법을 설명하기 위한 흐름도이다.
- [0054] 도 5를 참고로 살펴보면, 사용자 노드는 사용자 노드의 주변 노드로부터 상대방 노드의 상대 신뢰값을 수신하고

(S110), 수신한 상대방 노드의 상대 신뢰값 또는 자신 신뢰값으로부터 상대방 노드의 최종 신뢰값을 계산한다 (S120). 상대방 노드의 최종 신뢰값(FT)은 아래의 수학적식(1)에 의해 계산된다.

[수학적식 1]

$$FT = \frac{\alpha \times T_i + \beta \times \sum_{j=1}^N T_{ij}}{1 + N}$$

여기서 T_i 는 상대방 노드(i)의 자신 신뢰값이고 T_{ij} 는 상대방 노드(i)에 대한 주변 노드(j)가 갖는 상대 신뢰값이며, α 와 β 는 각각 자신 신뢰값과 상대 신뢰값에 대한 가중치인 것을 특징으로 한다.

바람직하게, 자신 신뢰값에 대한 가중치를 0으로 하는 경우 상대방 노드의 최종 신뢰값은 상대 신뢰값에 의해서만 계산되며, 자신 신뢰값에 대한 가중치를 0으로 하지 않는 경우 상대방 노드의 최종 신뢰값은 상대 신뢰값과 자신 신뢰값으로부터 계산된다.

더욱 바람직하게, 자신 신뢰값과 상대 신뢰값의 가중치를 동일하거나 서로 상이하게 설정함으로써, 자신 신뢰값 또는 상대 신뢰값의 비중을 달리하여 최종 신뢰값을 계산할 수 있다.

상대 신뢰값의 평균값과 자신 신뢰값이 차이에 기초하여 최종 신뢰값을 보완하여 보완 최종 신뢰값을 계산한다 (S130). 상대 신뢰값의 평균값과 자신 신뢰값의 차이값을 계산하여 차이값이 임계 차이값보다 큰지 판단하며, 상대 신뢰값의 평균값과 자신 신뢰값의 차이값이 임계 차이값보다 큰 경우 차이값에 비례하여 최종 신뢰값을 감소시켜 최종 신뢰값을 보완한다. 자신 신뢰값은 상대방 노드에 의해 조작되어 변경될 수 있으나 상대 신뢰값은 상대방 노드에 의해 계산되는 값이므로 조작 변경이 불가능하다. 만약 자신 신뢰값이 변경되어 평균 상대 신뢰값과 자신 신뢰값의 차이가 임계 차이값보다 큰 경우 상대방 노드가 자신 신뢰값을 임의 조작 변경한 것으로 판단하여 최종 신뢰값을 보완함으로써, 상대방 노드의 신뢰값을 더욱 정확하게 판단할 수 있다.

최종 신뢰값 또는 보완한 최종 신뢰값이 임계값을 초과하는지 판단하여 최종 신뢰값 또는 보완한 최종 신뢰값이 임계값을 초과하는 경우 사용자 노드는 상대방 노드와의 데이터 교환 여부를 결정한다(S140).

도 6은 본 발명에 따른 자신 신뢰값을 계산하는 방법을 설명하는 흐름도이다.

자신 신뢰값은 사용자 노드가 상대방 노드로 송신하는 데이터에 기초하여 사용자 노드에서 계산하는데, 도 6을 참고로 보다 구체적으로 살펴보면, 사용자 노드가 상대방 노드로 데이터를 송신하는 경우(S210), 송신하는 데이터에 악의 데이터가 존재하는지 검색한다(S220). 검색 결과 상대방 노드로 송신되는 데이터에서 악의 데이터가 검색되는 않는 경우 자신 신뢰값을 증가시키고(S230), 악의 데이터가 검색되는 경우 자신 신뢰값을 감소시킨다(S240).

바람직하게, 악의 데이터의 검색은 설정 주기 시간별로 이루어지는데 단위 설정 주기에 검색된 악의 데이터의 수 또는 데이터 송신 시간에 해당하는 전체 설정 주기 중에서 악의 데이터가 검색된 설정 주기의 수에 따라 비례하여 자신 신뢰값을 증가시키거나 감소시킨다.

계산한 자신 신뢰값을 신뢰값 데이터베이스에 저장 관리한다(S250).

도 7은 본 발명에 따른 상대 신뢰값을 계산하는 방법을 설명하는 흐름도이다.

상대 신뢰값은 사용자 노드가 상대방 노드로부터 수신하는 데이터에 기초하여 사용자 노드에서 계산하는데, 도 7을 참고로 보다 구체적으로 살펴보면 사용자 노드가 상대방 노드로부터 데이터를 수신하는 경우(S310), 수신하는 데이터에 악의 데이터가 존재하는지 검색한다(S320). 검색 결과 상대방 노드로부터 수신되는 데이터에서 악의 데이터가 검색되는 않는 경우 상대 신뢰값을 증가시키고(S330), 악의 데이터가 검색되는 경우 상대 신뢰값을 감소시킨다(S340).

바람직하게, 악의 데이터의 검색은 단위 설정 주기별로 이루어지는데 단위 설정 주기에 검색된 악의 데이터의 수 또는 데이터 수신 시간에 해당하는 전체 설정 주기 중에서 악의 데이터가 검색된 단위 설정 주기의 수에 따

라 비례하여 상대 신뢰값을 증가시키거나 감소시킨다.

[0069] 사용자 인터페이스를 통해 수정 상대 신뢰값이 입력되는지 판단하여(S350), 수정 상대 신뢰값이 입력되는 경우 계산한 상대 신뢰값을 수정 상대 신뢰값으로 갱신한다(S360). 도 8은 사용자 노드에 저장되어 있는 상대방 노드의 상대 신뢰값의 일 예로, 상대방 노드와 이전 데이터를 교환한 사용자 노드는 실제 상대방 노드와의 데이터 교환을 통해 상대방 노드의 상대 신뢰값을 판단할 수 있으며 계산한 상대방 노드의 상대 신뢰값 대신 주변 노드가 직접 판단한 수정 상대 신뢰값으로 상대 신뢰값을 갱신할 수 있다.

[0070] 계산한 상대 신뢰값 또는 수정 상대 신뢰값을 신뢰값 데이터베이스에 저장 관리한다(S370).

[0071]

[0072] 한편, 상술한 본 발명의 실시 예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0073] 상기 컴퓨터로 읽을 수 있는 기록 매체는 마그네틱 저장 매체(예를 들어, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.

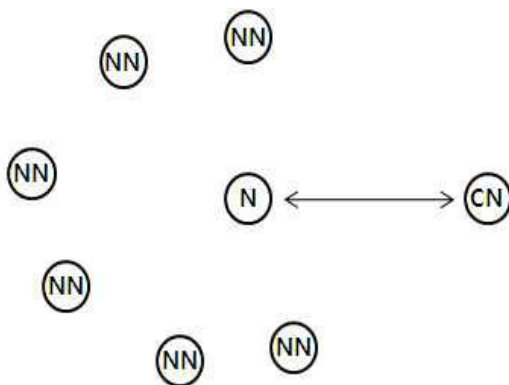
[0074] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

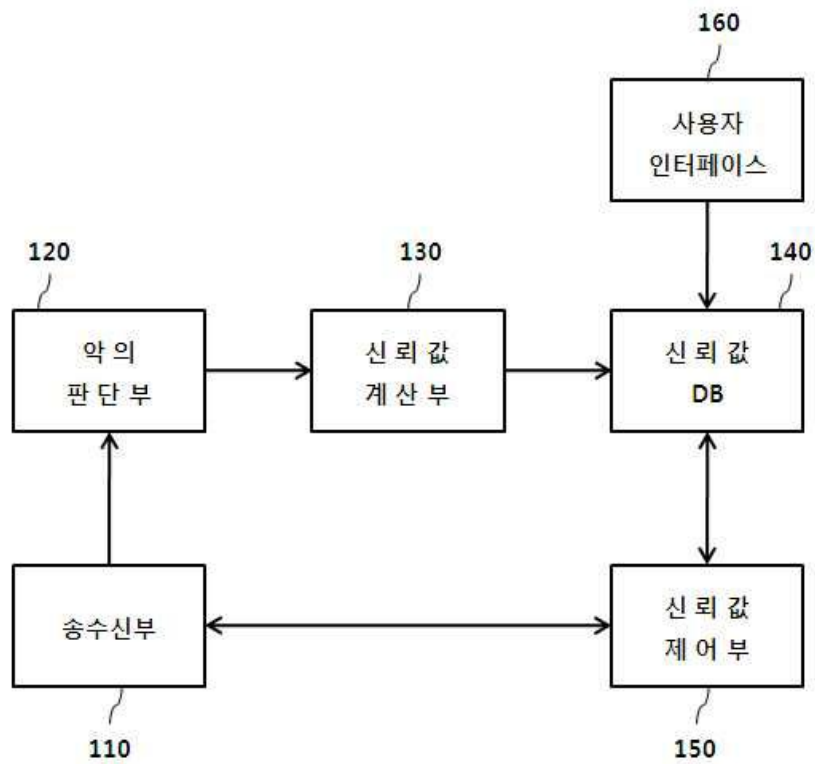
[0075]	110, 210: 송수신부	120: 악의 검색부
	130: 신뢰값 계산부	140: 신뢰값 DB
	150: 신뢰값 제어부	160: 사용자 인터페이스
	220: 접속 제어부	230: 신뢰값 계산부
	231: 신뢰값 요청부	233: 최종 신뢰값 계산부
	240: 최종 신뢰값 보완부	250: 통신 결정부

도면

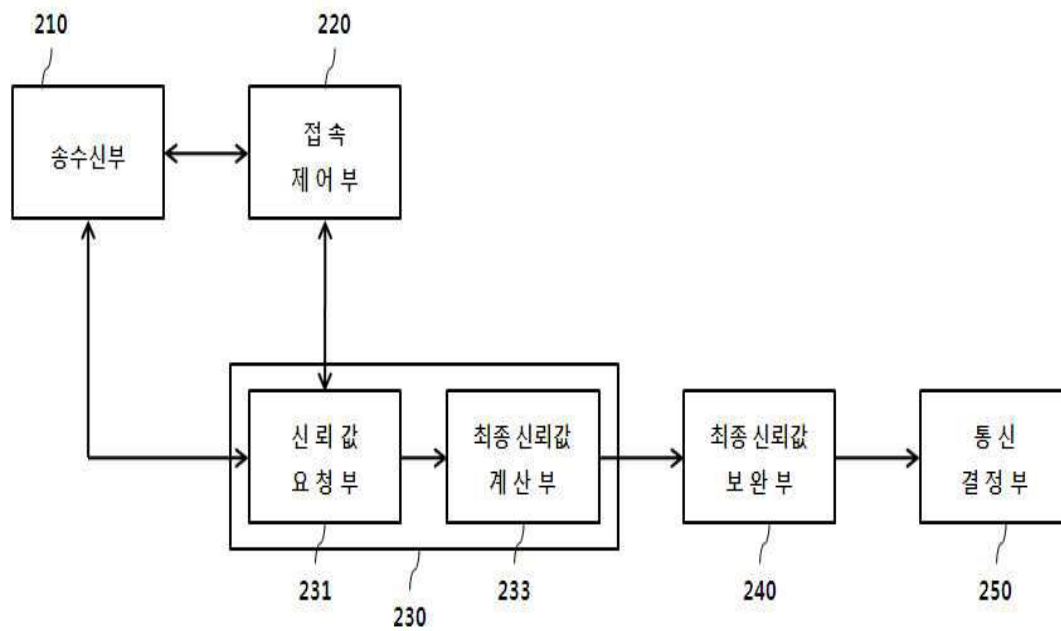
도면1



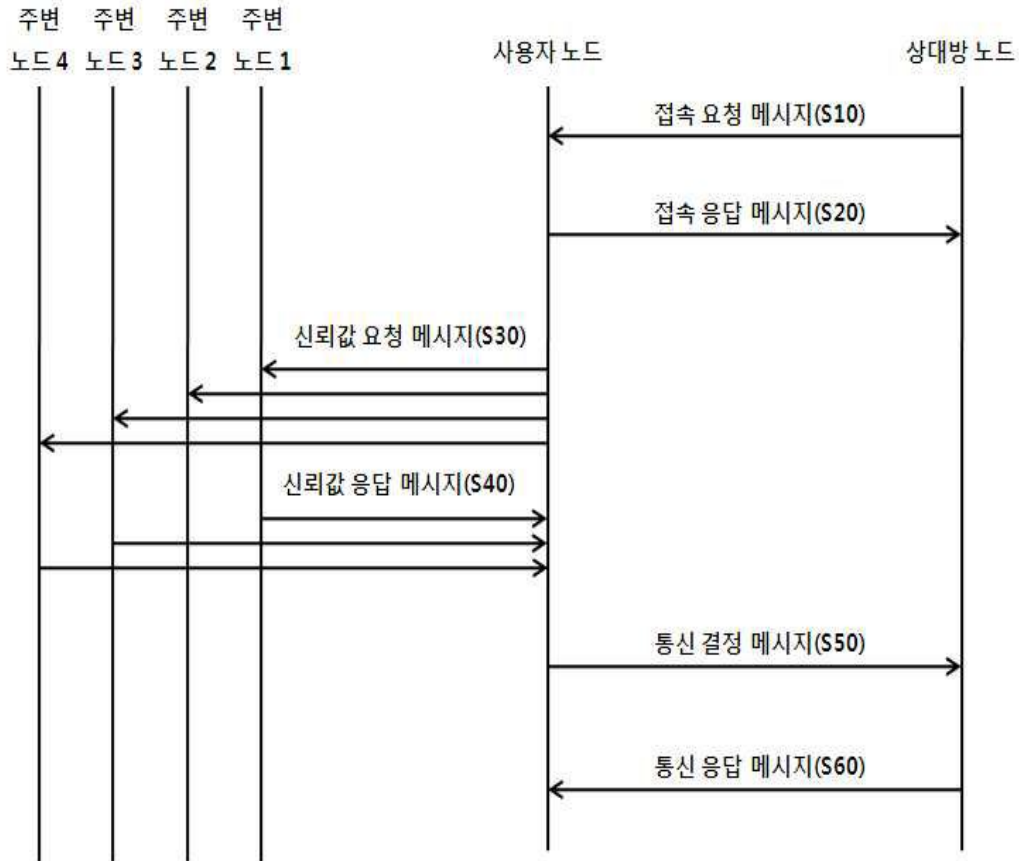
도면2



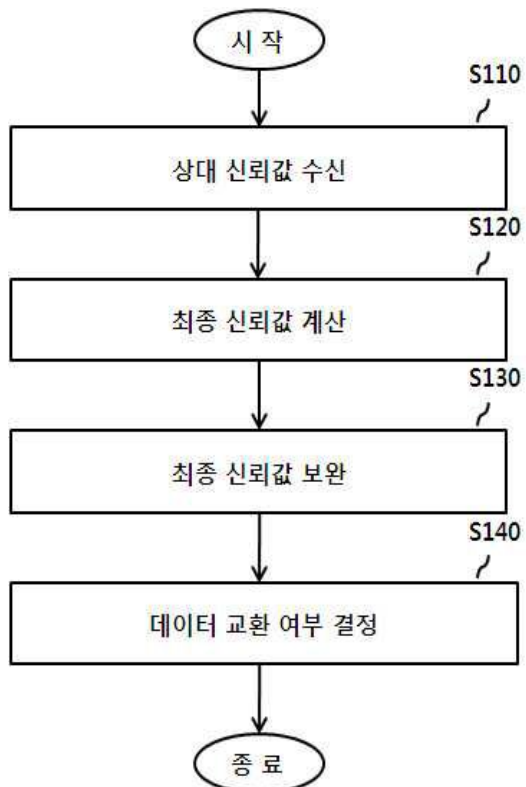
도면3



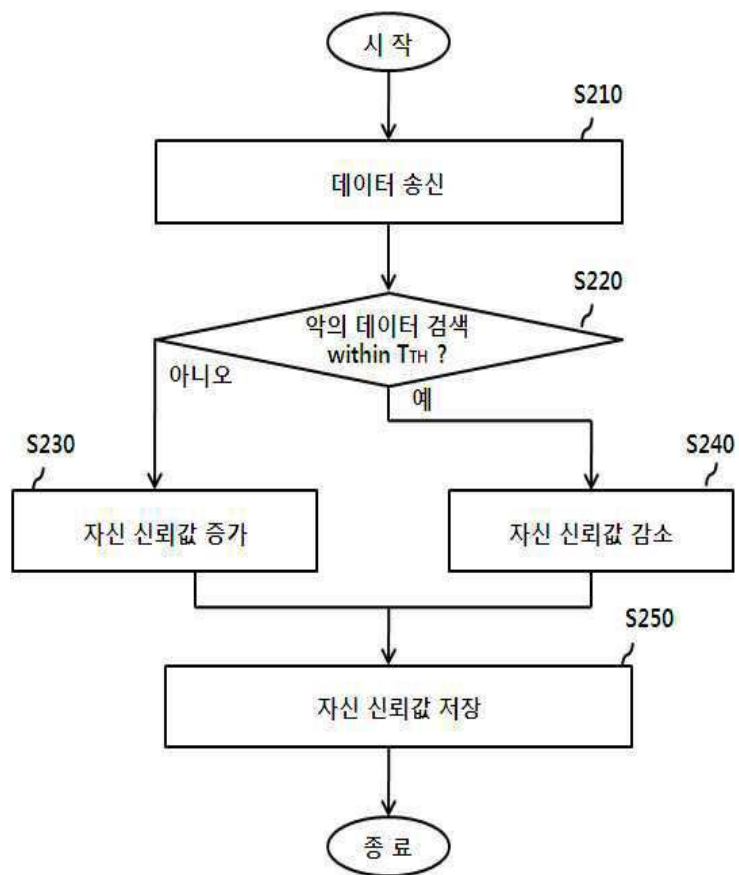
도면4



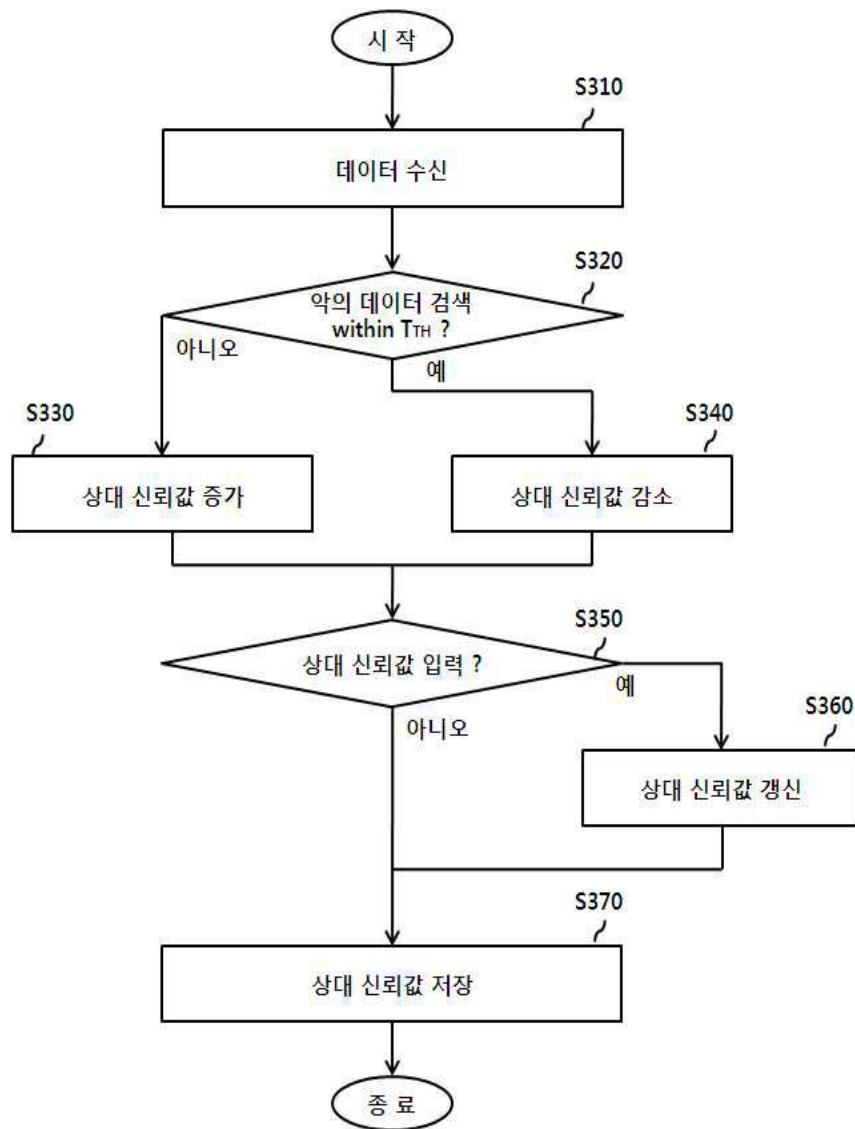
도면5



도면6



도면7



도면8

상대노드 식별자	상대 신뢰값	수정 상대 신뢰값
A	0.6	
B	0.7	0.2
C	0.5	
D	0.6	
E	0.8	
F	0.3	
G	0.4	0.7