(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년02월04일
(11) 등록번호 10-1591306
(24) 등록일자 2016년01월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
H04L 29/12 (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
H04L 9/0841 (2013.01)
H04L 61/20 (2013.01)
(21) 출원번호 10-2015-0057902
(22) 출원일자 2015년04월24일
심사청구일자 2015년04월24일
(56) 선행기술조사문헌
KR101410380 B1
KR101506564 B1

(73) 특허권자
한밭대학교 산학협력단
XXXXXXXXXXXXXXXXXXXXXXXX
(72) 발명자
김은기
XXXXXXXXXXXXXXXXX
안재원
XXXXXXXXXXXXXXXXX
(뒷면에 계속)
(74) 대리인
특허법인충정

전체 청구항 수 : 총 8 항 심사관 : 문형섭

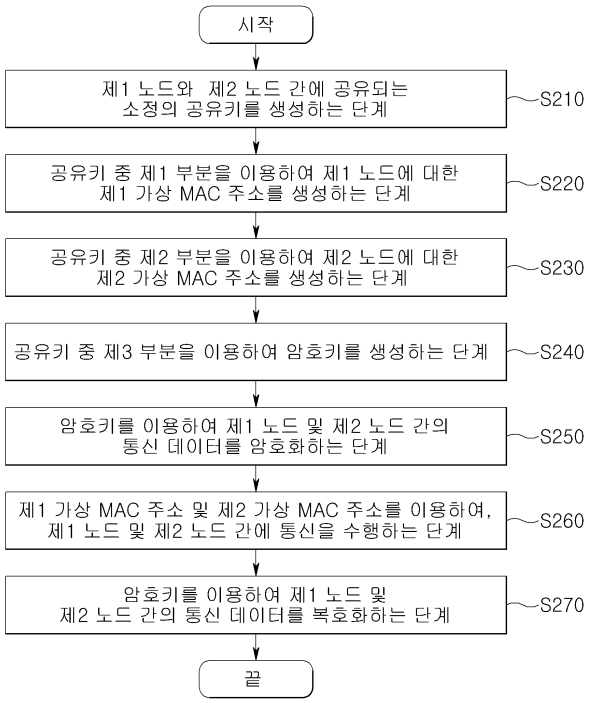
(54) 발명의 명칭 **가상의 MAC 주소를 이용한 통신 방법 및 장치**

(57) 요 약

본 발명은 가상의 MAC 주소를 이용한 통신 방법 및 장치에 관한 것으로서, 보다 구체적으로는 통신 네트워크의 양 노드에서 상호간의 공개 코드 교환을 통하여 소정의 공유키를 생성한 후, 상기 공유키 중 일부를 상기 양 노드에 대한 가상의 MAC 주소로 할당하여 통신을 수행하는 가상의 MAC 주소를 이용한 통신 방법 및 장치에 관한 것

(뒷면에 계속)

대 표 도 - 도2



이다.

본 발명은 통신 네트워크에서 제1 노드와 제2 노드 간의 통신 방법에 있어서, 상기 제1 노드와 상기 제2 노드 간에 공유되는 소정의 공유키를 생성하는 단계; 상기 공유키 중 제1 부분을 이용하여 상기 제1 노드에 대한 제1 가상 MAC 주소를 생성하는 단계; 상기 공유키 중 제2 부분을 이용하여 상기 제2 노드에 대한 제2 가상 MAC 주소를 생성하는 단계; 및 상기 제1 가상 MAC 주소 및 상기 제2 가상 MAC 주소를 이용하여, 상기 제1 노드 및 제2 노드 간에 통신을 수행하는 단계를 포함하는 것을 특징으로 하는 통신 방법을 개시하는 효과를 갖는다.

(52) CPC특허분류
H04L 63/06 (2013.01)
H04L 9/3013 (2013.01)

최범진
XXXXXXXXXXXXXXXXXXXXXXXXX

(72) 발명자
이재원
XXXXXXXXXXXXXXXXXXX

이 발명을 지원한 국가연구개발사업
과제고유번호 1345222771
부처명 교육부
연구관리전문기관 한국연구재단
연구사업명 지역혁신창의인력양성사업
연구과제명 IEEE p1609.2 Version 2 규격의 WAVE 보안 시스템 구현
기 여 율 1/1
주관기관 한밭대학교
연구기간 2014.05.01 ~ 2016.04.30

명 세 서

청구범위

청구항 1

통신 네트워크에서 제1 노드와 제2 노드 간의 통신 방법에 있어서,

상기 제1 노드와 상기 제2 노드 간에 공유되는 소정의 공유키를 생성하는 단계;

상기 공유키 중 제1 부분을 이용하여 상기 제1 노드에 대한 제1 가상 MAC 주소를 생성하는 단계;

상기 공유키 중 제2 부분을 이용하여 상기 제2 노드에 대한 제2 가상 MAC 주소를 생성하는 단계; 및

상기 제1 가상 MAC 주소 및 상기 제2 가상 MAC 주소를 이용하여, 상기 제1 노드 및 제2 노드 간에 통신을 수행하는 단계를 포함하며,

상기 공유키를 생성하는 단계는,

상기 제1 노드의 제1 공개 코드 및 상기 제2 노드의 제2 공개 코드를 상호간에 교환하는 단계; 및

상기 제1 노드 및 상기 제2 노드에서 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성하는 단계를 포함하는 것을 특징으로 하는 통신 방법.

청구항 2

제1항에 있어서,

상기 공유키 중 제3 부분을 이용하여 암호키를 생성하는 단계; 및

상기 암호키를 이용하여 상기 제1 노드 및 상기 제2 노드 간의 통신 데이터를 암호화하는 단계를 더 포함하는 것을 특징으로 하는 통신 방법.

청구항 3

제2항에 있어서,

상기 암호키를 이용하여 상기 제1 노드 및 상기 제2 노드 간의 통신 데이터를 복호화하는 단계를 더 포함하는 것을 특징으로 하는 통신 방법.

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 제1 노드 및 상기 제2 노드에서 디피-헬만 키 교환(Diffie-Hellman key exchange) 방식을 이용하여 상호간에 상기 제1 공개 코드 및 상기 제2 공개 코드를 교환하고,

상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성하는 것을 특징으로 하는 통신 방법.

청구항 6

통신 네트워크에서 제2 노드와 통신을 수행하는 통신 장치에 있어서,

상기 제2 노드와 공유되는 공유키를 생성하는 공유키 생성부;

상기 공유키 중 제1 부분을 이용하여 상기 통신 장치에 대한 제1 가상 MAC 주소를 생성하고, 상기 공유키 중 제2 부분을 이용하여 상기 제2 노드에 대한 제2 가상 MAC 주소를 생성하는 가상 MAC 주소 생성부; 및

상기 제1 가상 MAC 주소 및 상기 제2 가상 MAC 주소를 이용하여, 상기 제2 노드과 통신을 수행하는 통신부를 포

함하여 구성되며,

상기 공유키 생성부에서는,

상기 통신 장치의 제1 공개 코드 및 상기 제2 노드의 제2 공개 코드를 상호간에 교환한 후, 상기 통신 장치 및 상기 제2 노드에서 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성하는 것을 특징으로 하는 통신 장치.

청구항 7

제6항에 있어서,

상기 공유키 중 제3 부분을 이용하여 암호키를 생성하는 암호키 생성부; 및

상기 암호키를 이용하여 상기 제2 노드로 송신할 통신 데이터를 암호화하는 데이터 암호화부를 더 포함하는 것을 특징으로 하는 통신 장치.

청구항 8

제7항에 있어서,

상기 암호키를 이용하여 상기 제2 노드로부터 수신한 통신 데이터를 복호화하는 데이터 복호화부를 더 포함하는 것을 특징으로 하는 통신 장치.

청구항 9

삭제

청구항 10

제6항에 있어서,

상기 공유키 생성부에서는,

디피-헬만 키 교환(Diffie-Hellman key exchange) 방식을 이용하여 상기 제2 노드와 상기 제1 공개 코드 및 상기 제2 공개 코드를 교환하고,

상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성하는 것을 특징으로 하는 통신 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 가상의 MAC 주소를 이용한 통신 방법 및 장치에 관한 것으로서, 보다 구체적으로는 통신 네트워크의 양 노드에서 상호간의 공개 코드 교환을 통하여 소정의 공유키를 생성한 후, 상기 공유키 중 일부를 상기 양 노드에 대한 가상의 MAC 주소로 할당하여 통신을 수행하는 가상의 MAC 주소를 이용한 통신 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 근래 통신 서비스의 일반화와 함께, 해킹에 의한 개인 정보의 유출, 네트워크 장애, 금융 사고 등 다양한 유형의 문제가 발생하고 있으며, 이에 따라 네트워크 보안에 대한 관심이 크게 높아지고 있는 상황이다.

[0003] 상기 해킹의 수법에는 매우 다양한 종류가 있겠으나, 네트워크에 대한 주요 해킹 기법으로는 ARP(Address Resolution Protocol) 스푸핑(Spoofing), DoS(Denial on Service), DDoS(Distributed Denial on Service) 등을 들 수 있다. 예를 들어, ARP 스푸핑은 공격을 하고자 하는 대상의 MAC 주소를 위조하여 스위치나 기타 네트워크 장비의 ARP 캐시(cache) 테이블 상의 정보를 조작함으로써, 공격 대상이 되는 컴퓨터 등 제1 노드와 서버 등 제2 노드 사이의 트래픽을 공격자의 컴퓨터 등 제3 노드로 우회시켜 상기 우회된 트래픽으로부터 소정의 정보를 취득하는 방법을 말한다. 이와 같이 ARP 스푸핑 기법 등을 사용하여 공격자는 공격 대상에 대한 패스워드 정보 등 소정의 정보를 취득하거나, 상기 공격 대상이 되는 컴퓨터 등의 오동작을 유발하거나, 상기 공격 대상을 무력화시킬 수도 있게 된다.

[0004] 이에 대하여, 상기 ARP 스푸핑 공격 등을 방지하기 위한 종래의 기술로서, 동일한 로컬(local) 네트워크 장비의 ARP 테이블을 스캔하여 동일한 MAC 주소를 가진 여러 개의 IP가 지속적으로 발견되면 일단 ARP 스푸핑 공격이 행하여 진 것으로 의심하고, 문제가 되는 장비에 대하여 악성 코드를 포함하는 실행 파일이 실행 중인지 검사를 거쳐 ARP 스푸핑 공격을 차단하는 방법 등이 사용되었다. 그러나, 악성 코드 등은 지속적으로 변경하거나 진화하게 되는 바, 상기와 같은 대응 방안은 일시적인 방편이 될 수 있을 뿐, 근본적인 해결책이 될 수는 없었다.

[0005] 나아가, 상기 ARP 스푸핑 공격 외에도 공격 대상의 MAC 주소를 이용하는 다양한 해킹 기법이 존재하고 있는 바, 상기 MAC 주소를 이용한 해킹에 대비할 수 있는 보다 근본적인 방안이 요구되고 있으나, 이에 대한 적절한 해법이 아직 제시되지 못하고 있다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 특허공개공보 제10-2011-0060271호(2011년 06월 08일 공개)

발명의 내용

해결하려는 과제

[0007] 본 발명은 상기와 같은 종래 기술의 문제점을 해결하기 위해 창안된 것으로, 공격자가 공격 대상의 MAC 주소를 이용하여 공격 대상의 통신을 해킹하는 것을 방지할 수 있는 통신 방법 및 장치를 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0008] 상기한 과제를 해결하기 위한 본 발명의 한 측면에 따른 통신 방법은,

[0009] 통신 네트워크에서 제1 노드와 제2 노드 간의 통신 방법으로서, 상기 제1 노드와 상기 제2 노드 간에 공유되는 소정의 공유키를 생성하는 단계; 상기 공유키 중 제1 부분을 이용하여 상기 제1 노드에 대한 제1 가상 MAC 주소를 생성하는 단계; 상기 공유키 중 제2 부분을 이용하여 상기 제2 노드에 대한 제2 가상 MAC 주소를 생성하는 단계; 및 상기 제1 가상 MAC 주소 및 상기 제2 가상 MAC 주소를 이용하여, 상기 제1 노드 및 제2 노드 간에 통신을 수행하는 단계를 포함하는 것을 특징으로 한다.

[0010] 여기서, 상기 공유키 중 제3 부분을 이용하여 암호키를 생성하는 단계; 및 상기 암호키를 이용하여 상기 제1 노드 및 상기 제2 노드 간의 통신 데이터를 암호화하는 단계를 더 포함할 수 있다.

[0011] 또한, 상기 암호키를 이용하여 상기 제1 노드 및 상기 제2 노드 간의 통신 데이터를 복호화하는 단계를 더 포함할 수 있다.

[0012] 한편, 상기 공유키를 생성하는 단계는, 상기 제1 노드의 제1 공개 코드 및 상기 제2 노드의 제2 공개 코드를 상호간에 교환하는 단계; 및 상기 제1 노드 및 상기 제2 노드에서 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성하는 단계를 포함할 수 있다.

[0013] 이때, 상기 제1 노드 및 상기 제2 노드에서 디피-헬만 키 교환(Diffie-Hellman key exchange) 방식을 이용하여 상호간에 상기 제1 공개 코드 및 상기 제2 공개 코드를 교환하고, 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성할 수 있다.

[0014] 본 발명의 다른 측면에 따른 통신 장치는,

[0015] 통신 네트워크에서 제2 노드와 통신을 수행하는 통신 장치로서, 상기 제2 노드와 공유되는 공유키를 생성하는 공유키 생성부; 상기 공유키 중 제1 부분을 이용하여 상기 통신 장치에 대한 제1 가상 MAC 주소를 생성하고, 상기 공유키 중 제2 부분을 이용하여 상기 제2 노드에 대한 제2 가상 MAC 주소를 생성하는 가상 MAC 주소 생성부; 및 상기 제1 가상 MAC 주소 및 상기 제2 가상 MAC 주소를 이용하여, 상기 제2 노드과 통신을 수행하는 통신부를 포함하여 구성되는 것을 특징으로 한다.

[0016] 이때, 상기 공유키 중 제3 부분을 이용하여 암호키를 생성하는 암호키 생성부; 및 상기 암호키를 이용하여 상기

제2 노드로 송신할 통신 데이터를 암호화하는 데이터 암호화부를 더 포함할 수 있다.

[0017] 또한, 상기 암호키를 이용하여 상기 제2 노드로부터 수신한 통신 데이터를 복호화하는 데이터 복호화부를 더 포함할 수 있다.

[0018] 한편, 상기 공유키 생성부에서는, 상기 통신 장치의 제1 공개 코드 및 상기 제2 노드의 제2 공개 코드를 상호간에 교환한 후, 상기 통신 장치 및 상기 제2 노드에서 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성할 수 있다.

[0019] 또한, 상기 공유키 생성부에서는, 디피-헬만 키 교환(Diffie-Hellman key exchange) 방식을 이용하여 상기 제2 노드와 상기 제1 공개 코드 및 상기 제2 공개 코드를 교환하고, 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성할 수 있다.

발명의 효과

[0020] 본 발명의 실시예에 따르면, 통신 네트워크의 양 노드에서 상호간의 공개 코드 교환을 통하여 소정의 공유키를 생성한 후, 상기 공유키 중 일부를 상기 양 노드에 대한 가상의 MAC 주소로 할당하여 통신을 수행함으로써, 공격자가 공격 대상의 MAC 주소를 이용하여 공격 대상의 통신을 해킹하는 것을 방지할 수 있는 가상의 MAC 주소를 이용한 통신 방법 및 장치를 제공할 수 있게 된다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시 예에 따른 통신 시스템의 구성도이다.

도 2는 본 발명의 일 실시 예에 따른 통신 방법의 순서도이다.

도 3은 발명의 일 실시 예에 따른 공유키 생성 과정을 설명하기 위한 설명도이다.

도 4는 본 발명의 일 실시 예에 따른 MAC 프레임의 구성도이다.

도 5는 본 발명의 다른 실시 예에 따른 MAC 프레임의 구성도이다.

도 6은 본 발명의 일 실시 예에 따른 통신 장치의 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 이하에서는 특정 실시예들을 첨부된 도면을 기초로 상세히 설명하고자 한다.

[0023] 이하의 실시예는 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0024] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시 예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0025] 또한, 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되는 것은 아니며, 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0026] 이하에서는, 본 발명에 따른 가상의 MAC 주소를 이용한 통신 방법 및 장치의 예시적인 실시 형태들을 첨부된 도면을 참조하여 상세히 설명한다.

[0027] 먼저, 도 1에서는 본 발명의 일 실시예에 따른 가상의 MAC 주소를 이용한 통신 시스템(100)의 구성도를 예시하

고 있다.

[0028] 도 1에서 볼 수 있는 바와 같이 본 발명의 일 실시예에 따른 가상의 MAC 주소를 이용한 통신 시스템(100)은 가상의 MAC 주소를 이용하여 통신을 수행하는 제1 노드(110) 및 제2 노드(120), 상기 제1 노드(110)와 제2 노드(120) 간의 통신을 위한 통신 네트워크(140)를 포함하여 구성될 수 있다.

[0029] 또한, 상기 제1 노드(110)의 통신을 해킹하는 제3 노드(130)가 상기 통신 네트워크(140)에 연결될 수 있다.

[0030] 여기서, 상기 제1 노드(110), 제2 노드(120) 및 제3 노드(130)는 통신 네트워크(140)를 구성하는 단위 구성 요소인 교환기, 라우터 등 통신 장비이거나 상기 통신 네트워크(140)에 연결되어 통신을 수행할 수 있는 퍼스널 컴퓨터(PC), 노트북 PC 등일 수도 있으며, 또는 스마트폰, 태블릿 PC, PDA, 휴대전화 등의 휴대 단말기 등 다양한 종류의 단말기일 수도 있다.

[0031] 또한, 상기 통신 네트워크(140)는 유선 네트워크와 무선 네트워크를 포함할 수 있으며, 구체적으로, 근거리 네트워크(LAN: Local Area Network), 도시권 네트워크(MAN: Metropolitan Area Network), 광역 네트워크(WAN: Wide Area Network) 등의 다양한 네트워크를 포함할 수 있다. 나아가, 상기 통신 네트워크(140)는 상기 열거된 네트워크에 국한되지 않고, 공지의 무선 데이터 네트워크나 공지의 유무선 네트워크를 적어도 일부로 포함할 수도 있다.

[0032] 상기 도1 에서 상기 제1 노드(110)와 제2 노드(120)는 상호간의 공개 코드 교환을 통하여 소정의 공유키를 생성한 후, 상기 공유키 중 일부를 상기 제1 노드(110)와 제2 노드(120)에 대한 가상의 MAC 주소로 할당하여 통신을 수행함으로써, 공격자가 상기 제3 노드(130)를 사용하여 상기 제1 노드(110)의 MAC 주소를 이용하여 상기 제1 노드(110)의 통신을 해킹하는 것을 방지할 수 있게 된다.

[0033] 또한, 도 2에서는 본 발명의 일 실시예에 따른 가상의 MAC 주소를 이용한 통신 방법의 순서도를 도시하고 있다.

[0034] 도 2에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 가상의 MAC 주소를 이용한 통신 방법은, 제1 노드와 제2 노드 간에 공유되는 소정의 공유키를 생성하는 단계(S210), 공유키 중 제1 부분을 이용하여 제1 노드에 대한 제1 가상 MAC 주소를 생성하는 단계(S220), 공유키 중 제2 부분을 이용하여 제2 노드에 대한 제2 가상 MAC 주소를 생성하는 단계(S230), 공유키 중 제3 부분을 이용하여 암호키를 생성하는 단계(S240), 암호키를 이용하여 제1 노드 및 제2 노드 간의 통신 데이터를 암호화하는 단계(S250), 제1 가상 MAC 주소 및 제2 가상 MAC 주소를 이용하여, 제1 노드 및 제2 노드 간에 통신을 수행하는 단계(S260), 암호키를 이용하여 제1 노드 및 제2 노드 간의 통신 데이터를 복호화하는 단계(S270)를 포함할 수 있다.

[0035] 아래에서는 도 1 및 도 2를 참조하여, 본 발명의 일 실시예에 따른 가상의 MAC 주소를 이용한 통신 시스템(100) 및 방법을 보다 자세하게 살핀다.

[0036] 먼저, S210 단계에서는 제1 노드(110)와 제2 노드(120) 간에 공유되는 소정의 공유키를 생성하게 된다. 이때, 상기 공유키를 생성하는 방법에는 여러가지 방법이 이용될 수 있겠으나, 예를 들어, 상기 제1 노드(110) 및 상기 제2 노드(120)에서 디피-헬만 키 교환(Diffie-Hellman key exchange) 방식을 이용하여 상호간에 상기 제1 공개 코드 및 상기 제2 공개 코드를 교환한 후, 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성하는 방법을 사용할 수도 있다.

[0037] 도 3에서는 상기 디피-헬만 키 교환(Diffie-Hellman key exchange) 방식을 이용하여 상기 제1 노드(110) 및 상기 제2 노드(120)가 상기 제1 공개 코드 및 상기 제2 공개 코드를 교환한 후, 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성하는 과정을 보다 자세하게 예시하고 있다.

[0038] 도 3에서 볼 수 있는 바와 같이, 먼저 제1 노드(110)에서는 제1 비밀 코드(a)를 생성하고, 제2 노드(120)에서는 제2 비밀 코드(b)를 생성(도 3의 ①)한다.

[0039] 이어서, 상기 제1 노드(110)는 상기 제1 비밀 코드(a)로부터 제1 공개 코드(g^a (mod p))를 생성하여 상기 제2 노드(120)로 전달하고, 상기 제2 노드(120)는 상기 제2 비밀 코드(b)로부터 제2 공개 코드(g^b (mod p))를 생성하여 상기 제1 노드(110)로 전달(도 3의 ②)한다. 여기서, 상기 g와 p는 미리 생성되어 공유된 값으로서 공개된 값을 사용할 수도 있다.

[0040] 다음으로, 제1 노드(110)는 전달받은 제2 공개 코드(g^b (mod p))로부터 공유키(shared key) g^{ab} (mod p) 를 산출하게 되고, 마찬가지로 제2 노드(120)도 전달받은 제1 공개 코드(g^a (mod p))로부터 공유키(shared key) g^{ab}

(mod p) 를 산출(도 3의 ③)할 수 있게 되므로, 결국 제1 노드(110) 및 제2 노드(120)는 공통된 공유키(g^{ab} (mod p))를 생성하여 공유(도 3의 ④)할 수 있게 된다.

[0041] 이에 따라, 상기 제1 노드(110) 및 제2 노드(120) 외에는 상기 제1 비밀 코드(a), 제2 비밀 코드(b) 및 공유키(g^{ab} (mod p)) 값을 알 수 없게 된다.

[0042] 또한, 앞서 디피-헬만 키 교환(Diffie-Hellman key exchange) 방식을 이용하여 제1 노드(110) 및 제2 노드(120) 간에 공유되는 비밀 공유키를 생성하는 방법에 대하여 설명하였으나, 본 발명이 반드시 이에 한정되는 것은 아니며 이외에도 상기 제1 노드(110) 및 제2 노드(120) 간에 공유되는 비밀 공유키를 적절하게 생성할 수 있는 방법이라면 특별한 제한이 없이 적용될 수 있다.

[0043] 다음으로, S220 단계에서는 상기 S210 단계에서 생성된 공유키 중 제1 부분을 이용하여 제1 노드(110)에 대한 제1 가상 MAC 주소를 생성하게 된다.

[0044] 이때, MAC 주소라 함은 이더넷 등의 네트워크 통신에서 노드-대-노드(node-to-node) 전달에 사용되는 물리적인 주소로서, 네트워크 인터페이스 카드(Network Interface Card, NIC)의 고유 식별자(identifier)가 된다. 이와 관련하여, 도 4(a)의 통상적인 MAC 프레임의 구조를 예시하고 있으며, 도 4(a)에서 볼 수 있는 바와 같이, MAC 주소는 MAC 프레임에 포함되어 네트워크 통신에 사용되게 된다. 이때, 상기 MAC 프레임에는 수신(destination) MAC 주소(11), 송신(sender) MAC 주소(12)가 포함될 수 있으며, 나아가 데이터(14)에 담겨있는 상위 프로토콜 타입(13) 정보를 포함할 수도 있다. 통상적으로 상기 수신(destination) MAC 주소(11)와 송신(sender) MAC 주소(12)로는 48비트(bit) 값이 사용될 수 있다.

[0045] 그런데, 상기 도 4(a)의 종래 기술에 따른 MAC 프레임 구조에서 볼 수 있는 바와 같이, 공격자가 제3 노드(130) 등을 이용하여 상기 MAC 프레임을 스푸핑(spoofing) 하는 등의 방법으로 상기 MAC 프레임을 수신할 수 있다면, 상기 MAC 프레임에 포함된 상기 수신(destination) MAC 주소(11)와 송신(sender) MAC 주소(12) 값을 참조하여, 상기 MAC 프레임의 발송자와 수신자를 쉽게 파악할 수 있으며, 또한 상기 발송자와 수신자 간에 전달되는 데이터(14)의 내용도 손쉽게 수집할 수 있게 된다.

[0046] 이에 대하여, 본 발명의 일 실시예에 따른 가상의 MAC 주소를 이용한 통신 방법에서는, 상기 S210 단계에서 생성된 공유키 중 일부인 제1 부분으로부터 상기 제1 노드(110)에 대한 제1 가상 MAC 주소를 생성할 수 있게 된다. 예를 들어, 상기 S210 단계에서 생성된 공유키 중 최상위 48비트(bit)를 상기 제1 가상 MAC 주소로 사용할 수 있다. 물론 경우에 따라서는 상기 생성된 공유키 중 일부인 제1 부분으로부터 소정의 처리 과정을 거쳐 상기 제1 노드(110)에 대한 제1 가상 MAC 주소를 산출하는 방식도 가능하다.

[0047] 이러한 경우, 공격자로서는 상기 S210 단계에서 생성된 공유키를 알 수 없기 때문에, 공격하고자 하는 제1 노드(110)의 제1 가상 MAC 주소를 알 수 없게 되어, IP 주소와 MAC 주소를 위조하는 패킷을 생성하기 어려워지므로, ARP 스푸핑 등의 공격 기법을 이용하여 상기 제1 노드(110)를 공격하기 힘들어지게 된다.

[0048] 또한, S230 단계에서도 마찬가지로 상기 S210 단계에서 생성된 공유키 중 제2 부분을 이용하여 제2 노드(120)에 대한 제2 가상 MAC 주소를 생성하게 된다.

[0049] 이때, 앞서 살핀 S220 단계에서와 유사하게 상기 S210 단계에서 생성된 공유키 중 일부인 제2 부분으로부터 상기 제2 노드(120)에 대한 제2 가상 MAC 주소를 생성할 수 있게 된다. 예를 들어, 상기 S210 단계에서 생성된 공유키 중 상위 49비트 내지 96비트를 상기 제2 가상 MAC 주소로 사용할 수 있다. 물론 경우에 따라서는 상기 생성된 공유키 중 일부인 제2 부분으로부터 소정의 처리 과정을 거쳐 상기 제2 노드(120)에 대한 제2 가상 MAC 주소를 산출하는 방식도 가능하다.

[0050] 상기 S220 단계 및 S230 단계에서와 같이 생성된 제1 가상 MAC 주소 및 제2 가상 MAC 주소는 도 4(b)에서 볼 수 있는 바와 같이 수신 가상 MAC 주소(21) 또는 송신 가상 MAC 주소(22)로 사용되어 MAC 프레임을 구성할 수 있게 되며, 이에 따라, 공격자가 공격 대상의 MAC 주소를 이용하여 공격 대상의 통신을 해킹하는 것을 방지할 수 있게 된다.

[0051] 나아가, S240 단계에서는 상기 S210 단계에서 생성된 공유키 중 제3 부분을 이용하여 암호키를 생성할 수 있다. 예를 들어, 상기 S210 단계에서 생성된 공유키 중 하위 바이트를 상기 암호키로 사용하는 것도 가능하다. 나아가, 상기 생성된 공유키 중 일부인 제3 부분으로부터 소정의 처리 과정을 거쳐 상기 암호키를 산출하는 것도 가능하다.

[0052] 상기와 같이 암호키가 생성되면, 상기 제1 노드(110)과 제2 노드(120)는 동일한 암호키를 공유하게 되므로, 상기 암호키를 사용하여 전송하고자 하는 데이터를 암호화하여 송신하고, 수신받은 암호화된 데이터를 복호화하여 원상으로 복원함으로써, 공격자가 상기 MAC 프레임을 가로채더라도 상기 데이터를 보호할 수 있게 된다.

[0053] 또한, S250 단계에서는 상기 S240 단계에서 생성된 암호키를 이용하여 상기 제1 노드(110) 및 제2 노드(120) 간의 통신 데이터를 암호화하게 된다. 이에 대한 일 실시예로서 도 5에서는 암호화된 데이터를 포함하는 MAC 프레임의 구조를 예시하고 있다.

[0054] 이어서, S260 단계에서는 상기 제1 가상 MAC 주소 및 제2 가상 MAC 주소를 이용하여 상기 제1 노드(110) 및 제2 노드(120) 간에 통신을 수행하게 되며, 또한 S270 단계에서는 상기 제1 노드(110)가 송신한 암호화된 MAC 프레임을 수신한 제2 노드(120)가 상기 암호키를 이용하여 통신 데이터를 복호화하게 된다.

[0055] 도 6에서는 본 발명의 다른 실시예에 따른 가상의 MAC 주소를 이용한 통신 장치(110)의 구성도를 예시하고 있다.

[0056] 상기 통신 장치(110)는 교환기, 라우터 등 통신 장비일 수도 있으며, 또는 상기 통신 네트워크(140)에 연결되어 통신을 수행할 수 있는 퍼스널 컴퓨터(PC), 노트북 PC 등이거나, 스마트폰, 태블릿 PC, PDA, 휴대전화 등 다양한 단말기일 수도 있다.

[0057] 도 6에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 가상의 MAC 주소를 이용한 통신 장치(110)는 공유키 생성부(111), 가상 MAC 주소 생성부(112), 통신부(113), 암호키 생성부(114), 데이터 암호화부(115) 및 데이터 복호화부(116)를 포함하여 구성될 수 있다.

[0058] 아래에서는 도 6을 참조하여 본 발명의 일 실시예에 따른 가상의 MAC 주소를 이용한 통신 장치(110)를 구성 요소 별로 자세하게 살핀다.

[0059] 먼저, 공유키 생성부(111)에서는 통신 네트워크(140)에 연결된 제2 노드(120)에 대하여, 상기 제2 노드(120)와 공유되는 공유키를 생성하게 된다. 이때, 상기 공유키 생성부(111)에서는 상기 통신 장치(110)에서 생성되는 제1 공개 코드 및 상기 제2 노드에서 생성되는 제2 공개 코드를 상호간에 교환한 후, 상기 통신 장치(110) 및 상기 제2 노드(120)에서 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성할 수 있다.

[0060] 나아가, 상기 상기 공유키 생성부(111)에서는, 디피-헬만 키 교환(Diffie-Hellman key exchange) 방식을 이용하여 상기 제2 노드(120)와 상기 제1 공개 코드 및 상기 제2 공개 코드를 교환한 후, 상기 제1 공개 코드 및 상기 제2 공개 코드를 이용하여 상기 공유키를 생성할 수도 있다.

[0061] 다음으로, 가상 MAC 주소 생성부(112)에서는 상기 공유키 생성부(111)에서 생성된 공유키 중 제1 부분을 이용하여 상기 통신 장치(110)에 대한 제1 가상 MAC 주소를 생성하고, 상기 공유키 중 제2 부분을 이용하여 상기 제2 노드(120)에 대한 제2 가상 MAC 주소를 생성하게 된다.

[0062] 또한, 통신부(113)에서는 상기 제1 가상 MAC 주소 및 상기 제2 가상 MAC 주소를 이용하여, 상기 제2 노드과 통신을 수행하게 된다.

[0063] 나아가, 암호키 생성부(114)에서는 상기 공유키 생성부(111)에서 생성된 공유키 중 제3 부분을 이용하여 암호키를 생성하게 된다.

[0064] 또한, 데이터 암호화부(115)에서는 상기 암호키 생성부(114)에서 생성된 암호키를 이용하여 전송하고자 하는 데이터를 암호화하게 되고, 이어서 데이터 복호화부(116)에서는 상기 제2 노드(120)로부터 수신한 통신 데이터를 복호화하게 된다.

[0065] 상기와 같이 가상의 MAC 주소를 사용하고, 나아가 데이터를 암호화하여 송수신함으로써, 공격자가 공격 대상의 MAC 주소를 이용하여 공격 대상의 통신을 해킹하는 것을 효과적으로 방지할 수 있게 된다.

[0066] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0067] 100 : 통신 시스템

110 : 제1 노드

120 : 제2 노드

130 : 제3 노드

140 : 통신 네트워크

111 : 공유키 생성부

112 : 가상 MAC 주소 생성부

113 : 통신부

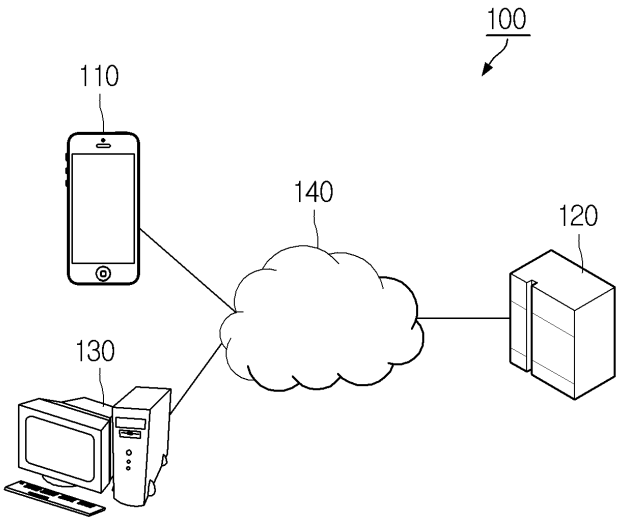
114 : 암호키 생성부

115 : 데이터 암호화부

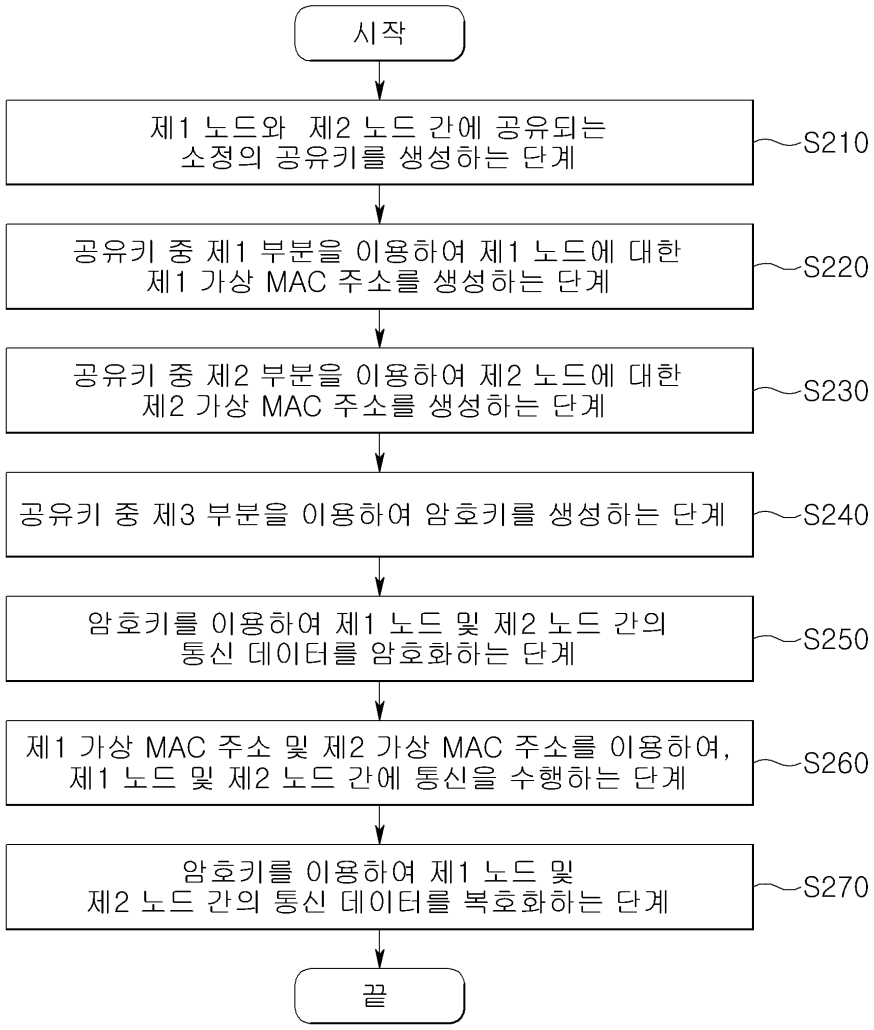
116 : 데이터 복호화부

도면

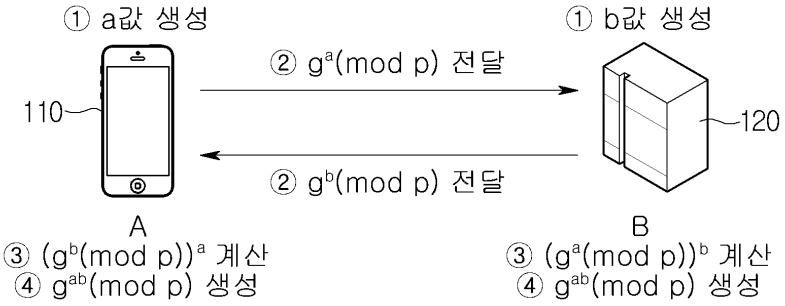
도면1



도면2

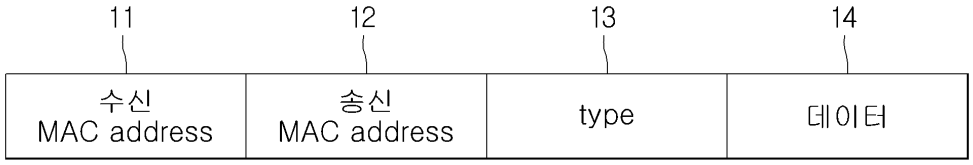

시작
제1 노드와 제2 노드 간에 공유되는 소정의 공유키를 생성하는 단계
S210
공유키 중 제1 부분을 이용하여 제1 노드에 대한 제1 가상 MAC 주소를 생성하는 단계
S220
공유키 중 제2 부분을 이용하여 제2 노드에 대한 제2 가상 MAC 주소를 생성하는 단계
S230
공유키 중 제3 부분을 이용하여 암호키를 생성하는 단계
S240
암호키를 이용하여 제1 노드 및 제2 노드 간의 통신 데이터를 암호화하는 단계
S250
제1 가상 MAC 주소 및 제2 가상 MAC 주소를 이용하여, 제1 노드 및 제2 노드 간에 통신을 수행하는 단계
S260
암호키를 이용하여 제1 노드 및 제2 노드 간의 통신 데이터를 복호화하는 단계
S270
끝

도면3



① A와 B는 각자의 컴퓨터에서 비밀값 a와 b를 생성한다.
② A는 g^a(mod p) 값을 계산하여 B에게 전달 한다.
B는 g^a(mod p) 값을 계산하여 A에게 전달 한다.
③ A는 받은 값을 이용하여 $(g^b(\text{mod } p))^a$ 를 계산한다.
B는 받은 값을 이용하여 $(g^a(\text{mod } p))^b$ 를 계산한다.
④ A와 B는 공통된 Key g^{ab}(mod p) 를 갖는다.

도면4

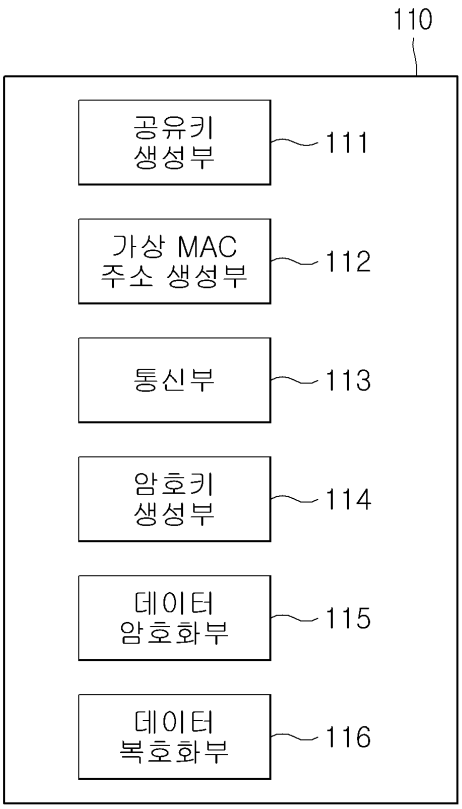


(a)

(b)

도면5

도면6


110
공유키 생성부
111
가상 MAC 주소 생성부
112
통신부
113
암호키 생성부
114
데이터 암호화부
115
데이터 복호화부
116