(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0115338
(43) 공개일자 2015년10월14일

(51) 국제특허분류(Int. Cl.)
H04W 12/12 (2009.01) *H04W 4/12* (2009.01)
(21) 출원번호 10-2014-0040192
(22) 출원일자 2014년04월03일
심사청구일자 없음

(71) 출원인
에스케이텔레콤 주식회사
서울특별시 중구 을지로 65 (을지로2가)
(72) 발명자
윤종철
경기도 구리시 건원대로76번길 134, 416동 1006호 (인창동,주공4단지아파트)
(74) 대리인
이철희

전체 청구항 수 : 총 9 항

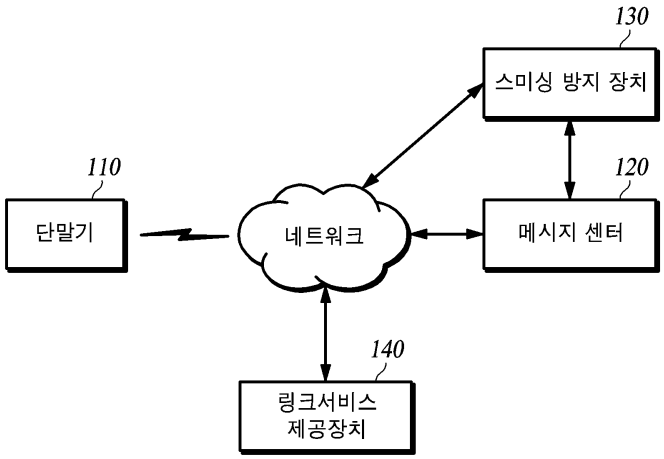
(54) 발명의 명칭 **스미싱 방지장치 및 방법**

(57) 요 약

스미싱 방지하기 위한 장치 및 방법을 개시한다.

단말기로 전송되는 문자 메시지에 포함된 링크정보를 보안 링크정보로 변환하고, 단말기로부터 보안 링크정보에 대한 입력신호가 존재하는 경우, 링크 에뮬레이터 상에서 링크정보로 접속하여 획득한 접속정보를 단말기로 전송되도록 하여 스미싱을 방지하기 위한 장치 및 방법에 관한 것이다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

스미싱 방지장치가 스미싱을 방지하는 방법에 있어서,

단말기로 전송되는 문자 메시지를 수신하는 메시지 수신과정;

상기 문자 메시지에 링크정보가 포함되어 있는 경우, 상기 링크정보를 보안 링크정보로 변환하는 변환과정;

상기 보안 링크정보를 포함하는 문자 메시지를 상기 단말기로 전송하는 과정;

상기 단말기로부터 상기 보안 링크정보에 대한 연결 요청이 있는 경우, 링크서비스 제공장치로 접속하는 접속과정; 및

상기 링크서비스 제공장치의 접속정보를 링크접속 이미지로 생성하여 상기 단말기로 전송하는 이미지 처리과정

을 포함하는 것을 특징으로 하는 스미싱 방지방법.

청구항 2

제 1 항에 있어서,

상기 변환과정은,

상기 문자 메시지에 대응하는 링크 에뮬레이터를 할당하고, 상기 링크정보를 상기 링크 에뮬레이터에 대한 가상 식별정보를 포함하는 상기 보안 링크정보로 변환하는 것을 특징으로 하는 스미싱 방지방법.

청구항 3

제 2 항에 있어서,

상기 링크 접속과정은,

상기 가상 식별정보에 해당하는 상기 링크 에뮬레이터를 실행하고, 상기 링크 에뮬레이터를 기반으로 상기 링크정보를 이용하여 상기 링크서비스 제공장치로 접속하고, 상기 링크서비스 제공장치로부터 상기 접속정보를 획득하는 것을 특징으로 하는 스미싱 방지방법.

청구항 4

제 3 항에 있어서,

상기 이미지 처리과정은,

상기 접속정보를 캡쳐, 스캔 및 이미지 변환 중 적어도 하나의 방식을 이용하여 상기 링크접속 이미지를 생성하는 것을 특징으로 하는 스미싱 방지방법.

청구항 5

제 1 항에 있어서,

상기 단말기로부터 상기 링크접속 이미지 중 일측의 터치입력에 대한 터치 위치정보가 수신되는 경우, 상기 링크 에뮬레이터 상에서 상기 터치 위치정보에 대응하는 기 설정된 추가 링크정보로 접속하는 과정;

상기 링크서비스 제공장치로부터 상기 기 설정된 추가 링크정보에 대응하는 추가 접속정보를 획득하는 과정; 및

상기 추가 접속정보에 대한 링크접속 이미지를 생성하고, 상기 링크접속 이미지를 상기 단말기로 전송하는 과정

을 더 포함하는 것을 특징으로 하는 스미싱 방지 방법.

청구항 6

제 1 항에 있어서,

상기 단말기로부터 상기 링크접속 이미지에 대응하는 원문링크 연결요청 신호가 수신되는 경우, 상기 링크서비스 제공장치의 접속을 종료하고, 상기 단말기가 링크정보로 접속할 수 있도록 제어하는 과정

을 더 포함하는 것을 특징으로 하는 스미싱 방지 방법.

청구항 7

스미싱을 방지하기 위한 장치에 있어서,

문자 메시지를 수신하는 메시지 처리부;

상기 문자 메시지에 링크정보가 포함되어 있는 경우, 상기 링크정보를 보안 링크정보로 변환하는 변환부; 및

상기 보안 링크정보를 포함하는 문자 메시지를 단말기로 전송하고, 상기 단말기로부터 상기 링크정보에 대한 연결 요청신호를 수신하는 단말 통신부;

상기 연결 요청신호에 포함된 가상 식별정보를 확인하고, 상기 가상 식별정보에 대응하는 상기 링크정보를 이용하여 링크서비스 제공장치로 접속하여 접속정보를 획득하는 에뮬레이터 실행부; 및

상기 접속정보에 대응하는 링크접속 이미지를 생성하여 상기 단말기로 전송하는 이미지 처리부

를 포함하는 것을 특징으로 하는 스미싱 방지장치.

청구항 8

제 7 항에 있어서,

상기 변환부는,

상기 문자 메시지에 대응하는 링크 에뮬레이터를 할당하고, 상기 링크 에뮬레이터에 해당하는 상기 가상 식별정보를 포함하는 상기 보안 링크정보로 변환하는 것을 특징으로 하는 스미싱 방지장치.

청구항 9

제 8 항에 있어서,

상기 에뮬레이터 실행부는,

상기 가상 식별정보에 근거하여 실행된 상기 링크 에뮬레이터를 기반으로 상기 링크서비스 제공장치로 접속하는 것을 특징으로 하는 스미싱 방지장치.

발명의 설명

기 술 분 야

[0001] 본 실시예는 문자 메시지에 포함된 링크정보의 스미싱을 방지하기 위한 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 이 부분에 기술된 내용은 단순히 본 실시예에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.

[0003] 스마트폰의 보급이 증가하고, 스마트폰의 기술이 발전함에 따라 스마트폰을 이용한 링크연결이 경우가 자주 발생한다. 이에 따라, 스마트폰의 링크연결을 이용한 범죄도 증가하고 있다.

[0004] 문자 메시지(SMS: Short Message Service)를 이용한 피싱(Phishing)을 결합한 스미싱(Smishing)은 스마트폰 사용자에게 특정 웹사이트로 이동하는 특정 링크가 포함된 문자 메시지를 보내 이용자의 스마트폰에 바이러스성 애플리케이션이나 악성코드를 다운로드 또는 설치시켜 개인정보를 수집하거나 모바일 결제를 유도하는 범죄수법을 말한다.

[0005] 이러한, 스미싱 문자에 담긴 링크들은 사용자가 의도하지 않고, 실수로 터치하더라도 터치된 순간 스마트폰에

악성 애플리케이션이 깔릴 수 있고, 이에 따른 은행 계좌번호나 비밀번호 등의 각종 금융정보, 휴대폰 소액결제 정보 또는 개인정보 등이 유출되어 사용자의 피해가 발생한다.

[0006] 일반적으로 스팸성 문자 또는 전화번호를 필터링하여 차단하는 방식으로 스미싱을 방지하고는 있으나, 스미싱 문자는 모바일 청첩장, 택배조회, 경찰서 등기, 카드사 사칭 등의 내용으로 가장한 링크정보를 포함하여 사용자가 스미싱 문자의 진위 여부를 판단하기 어렵다.

발명의 내용

해결하려는 과제

[0007] 본 실시예는, 단말기로 전송되는 문자 메시지에 포함된 링크정보를 보안 링크정보로 변환하고, 단말기로부터 보안 링크정보에 대한 입력신호가 존재하는 경우, 링크 에뮬레이터 상에서 링크정보로 접속하여 획득한 접속정보를 단말기로 전송되도록 하여 스미싱을 방지하기 위한 장치 및 방법을 제공하는 데 주된 목적이 있다.

과제의 해결 수단

[0008] 본 실시예의 일 측면에 의하면, 스미싱 방지장치가 스미싱을 방지하는 방법에 있어서, 단말기로 전송되는 문자 메시지를 수신하는 메시지 수신과정; 상기 문자 메시지에 링크정보가 포함되어 있는 경우, 상기 링크정보를 보안 링크정보로 변환하는 변환과정; 상기 보안 링크정보를 포함하는 문자 메시지를 상기 단말기로 전송하는 과정; 상기 단말기로부터 상기 보안 링크정보에 대한 연결 요청이 있는 경우, 링크서비스 제공장치로 접속하는 접속과정; 및 상기 링크서비스 제공장치의 접속정보를 링크접속 이미지로 생성하여 상기 단말기로 전송하는 이미지 처리과정을 포함하는 것을 특징으로 하는 스미싱 방지방법을 제공한다.

[0009] 또한, 본 실시예의 다른 측면에 의하면, 스미싱을 방지하기 위한 장치에 있어서, 문자 메시지를 수신하는 메시지 처리부; 상기 문자 메시지에 링크정보가 포함되어 있는 경우, 상기 링크정보를 보안 링크정보로 변환하는 변환부; 및 상기 보안 링크정보를 포함하는 문자 메시지를 단말기로 전송하고, 상기 단말기로부터 상기 링크정보에 대한 연결 요청신호를 수신하는 단말 통신부; 상기 연결 요청신호에 포함된 가상 식별정보를 확인하고, 상기 가상 식별정보에 대응하는 상기 링크정보를 이용하여 링크서비스 제공장치로 접속하여 접속정보를 획득하는 에뮬레이터 실행부; 및 상기 접속정보에 대응하는 링크접속 이미지를 생성하여 상기 단말기로 전송하는 이미지 처리부를 포함하는 것을 특징으로 하는 스미싱 방지장치를 제공한다.

발명의 효과

[0010] 이상에서 설명한 바와 같이 본 실시예에 의하면, 문자 메시지에 포함된 링크정보를 보안 링크정보로 변환하여 단말기로 전송함으로써, 사용자가 실수도 링크정보를 입력하더라도 스미싱 피해가 발생하지 않도록 하는 효과가 있다.

[0011] 또한, 단말기는 스미싱 방지장치로부터 링크접속 페이지를 캡쳐 또는 스캔하여 이미지를 전송하는 미러링 방식을 이용하여 링크정보를 확인함으로써, 단말기에 바이러스성 애플리케이션이나 악성코드가 다운로드 또는 설치되는 것을 방지할 수 있는 효과가 있다.

도면의 간단한 설명

[0012] 도 1은 본 실시예에 따른 스미싱 방지 시스템을 개략적으로 나타낸 블록 구성도이다.

도 2는 본 실시예에 따른 스미싱 방지장치를 개략적으로 나타낸 블록 구성도이다.

도 3은 본 실시예에 따른 스미싱을 방지하기 위해 보안 링크정보가 포함된 문자 메시지를 제공하는 동작을 설명하기 위한 순서도이다.

도 4는 본 실시예에 따른 스미싱을 방지하기 위해 링크 에뮬레이터를 이용하여 링크정보로 접속하는 동작을 설명하기 위한 순서도이다.

도 5는 본 실시예에 따른 보안 링크정보를 포함하는 모바일 청접장을 나타낸 예시도이다.

도 6은 본 실시예에 따른 보안 링크정보를 포함하는 복수의 문자 메시지를 나타낸 예시도이다.

도 7a은 본 실시예에 따른 스미싱을 방지하기 위한 이미지 및 원문링크 연결버튼을 나타낸 예시도이다.

도 7b는 본 실시예에 따른 스미싱을 방지하기 위한 이미지 및 터치입력에 따른 동작을 설명하기 위한 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 이하, 본 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0014] 도 1은 본 실시예에 따른 스미싱 방지 시스템을 개략적으로 나타낸 블록 구성도이다.

[0015] 본 실시예에 따른 스미싱 방지 시스템은 단말기(110), 메시지 센터(120), 스미싱 방지장치(130) 및 링크서비스 제공장치(140)를 포함한다.

[0016] 단말기(110)는 사용자의 입력 또는 조작에 따라 네트워크를 경유하여 음성, 메시지, 신호, 데이터 등을 송수신할 수 있는 단말기를 말하는 것이며, 태블릿 PC(Tablet PC), 랩톱(Laptop), 개인용 컴퓨터(PC: Personal Computer), 스마트폰(Smart Phone), 개인휴대용 정보단말기(PDA: Personal Digital Assistant) 및 이동단말기(Mobile Communication Terminal) 등 중 어느 하나일 수 있다.

[0017] 단말기(110)는 네트워크를 경유하여 통신하기 위한 프로그램 또는 프로토콜을 저장하기 위한 메모리, 해당 프로그램을 실행하여 연산 및 제어하기 위한 마이크로프로세서 등을 구비하고 있는 장치를 의미한다. 단말기(110)는 통신 네트워크와 서버-클라이언트 통신이 가능하다면 그 어떠한 단말기도 가능하다.

[0018] 단말기(110)는 메시지 센터(120)로부터 문자 메시지를 수신한다. 여기서, 문자 메시지는 보안 링크정보를 포함하는 문자 메시지일 수 있고, 일반 텍스트 정보만을 포함하는 메시지일 수도 있다. 여기서, 보안 링크정보는 스미싱 방지장치(130)로 연결되어 가상으로 링크정보를 접속하는 링크 에뮬레이터를 실행하는 시키기 위한 가상 식별정보를 포함하는 정보를 의미한다.

[0019] 본 실시예에 따른 단말기(110)는 메시지 센터(120)로부터 보안 링크정보를 포함하는 문자 메시지가 수신된 경우, 사용자의 조작에 따른 입력에 근거하여 보안 링크정보에 대한 연결요청을 수행한다. 예컨대, 단말기(110)는 문자 메시지에 포함된 보안 링크정보에 대한 터치 입력이 존재하는 경우, 보안 링크정보에 대응하는 연결요청신호를 스미싱 방지장치(130)로 전송한다.

[0020] 단말기(110)는 스미싱 방지장치(130)로부터 연결 요청신호에 대응하는 링크접속 이미지를 수신한다. 여기서, 링크접속 이미지는 스미싱 방지장치(130) 내에서 실행된 링크 에뮬레이터를 기반으로 접속된 링크서비스 제공장치(140)의 접속정보 즉, 링크정보에 대응하는 링크 접속 페이지를 캡쳐, 스캔, 이미지 변환 등의 방식을 이용하여 생성된 이미지를 의미한다.

[0021] 단말기(110)는 보안 링크정보에 대응하는 입력신호가 존재하는 경우, 기 설치된 웹브라우저를 구동하여 보안 링크정보에 대응하는 링크접속 이미지를 출력한다. 단말기(110)는 링크접속 이미지에 구비된 특정영역(예컨대, 링크연결 버튼)에 대한 입력신호가 존재하는 경우, 링크정보에 대응하는 접속정보를 출력할 수도 있다.

[0022] 한편, 단말기(110)는 웹브라우저만을 이용하여 링크접속 이미지를 출력하는 것으로 기재하고 있으나 반드시 이에 한정되는 것은 아니며, 보안 링크정보에 대응하는 입력신호가 존재하는 경우, 특정 애플리케이션(예: 스미싱 방지 애플리케이션)을 구동하고, 특정 애플리케이션을 기반으로 링크접속 이미지를 출력할 수 있다.

[0023] 단말기(110)는 특정 애플리케이션을 이용하여 링크접속 이미지를 출력하는 경우, 사용자는 링크접속 이미지의 소정의 위치에 대한 터치입력을 수행할 수 있다. 더 자세히 설명하자면, 단말기(110)는 특정 애플리케이션을 통해 출력된 링크접속 이미지에 대한 터치입력이 존재하는 경우, 터치 입력에 대한 터치 위치정보(예: x, y 좌표값)를 스미싱 방지장치(130)로 전송한다. 단말기(110)는 스미싱 방지장치(130)로부터 터치 위치정보를 기초로 링크 에뮬레이터 상에서 획득한 접속정보에 대한 링크접속 이미지를 수신하여 출력할 수 있다. 예컨대, 단말기(110)는 특정 애플리케이션을 이용하여 출력된 링크접속 이미지에 대한 터치입력이 존재하는 경우, (3, 5)와 같이 터치 위치정보를 산출하여 스미싱 방지장치(130)로 전송할 수 있다. 단말기(110)는 스미싱 방지장치(130)로부터 터치 위치정보를 기초로 기 설정된 추가 링크정보(예: 카테고리 세부연결 주소)를 이용하여 생성된 링크접속 이미지를 수신하여 출력할 수 있다.

[0024] 메시지 센터(120)는 네트워크를 경유하여 단말기(110)로부터 발신된 메시지를 수신한 후 기 설정한 발신번호에 해당하는 단말기로 전달하거나, 외부 장치 또는 외부 단말기로부터 발신된 메시지를 수신하고, 수신된 메시지에 기 설정한 발신번호에 해당하는 단말기(110)로 전달하는 기능을 수행한다.

[0025] 메시지 센터(120)는 수신된 발신 메시지가 기 설정한 발신번호에 해당하는 단말기(110)로 전달되지 못한 경우, 단말기(110)가 수신 가능한 상태에 이를 때까지 발신 메시지를 저장한다. 메시지 센터(120)에서 단말기(110)의 발신 메시지 수신이 확인되면, 저장된 발신 메시지에 대한 데이터가 삭제된다. 또한, 메시지 센터(120)는 발신 메시지를 전송한 지 일정한 시간이 경과 되거나, 메시지 센터(120)가 지정한 유효 시간까지 전달되지 못한 발신 메시지에 대한 데이터는 삭제된다.

[0026] 본 실시예에 따른 메시지 센터(120)는 단말기(110)에 대한 발신번호가 기 설정된 문자 메시지를 스미싱 방지장치(130)로 전송하고, 스미싱 방지장치(130)로부터 링크정보 포함 여부가 확인된 문자 메시지를 단말기(110)로 전송한다. 여기서, 링크정보 포함 여부가 확인된 문자 메시지는 보안 링크정보를 포함하는 문자 메시지일 수 있으나 반드시 이에 한정되는 것은 아니며, 텍스트만을 포함하는 SMS(Short Message Service), MMS(Multimedia Messaging System) 형태의 문자 메시지일 수 있다.

[0027] 스미싱 방지장치(130)는 링크 에뮬레이터를 기반으로 문자 메시지에 포함된 링크정보에 대응하는 링크서비스 제공장치(140)로 접속하여 획득한 접속정보에 대한 링크접속 이미지를 생성하여 단말기(110)로 전송하는 동작을 수행한다. 여기서, 링크 에뮬레이터는 링크정보를 가상으로 연결하는 프로그램을 의미하며, 가상 폰, 가상 PC와 같은 형태로 스미싱 방지장치(130) 내에 기 설치 또는 기 저장된 형태의 가상 링크연결 프로그램일 수 있다.

[0028] 스미싱 방지장치(130)는 메시지 센터(120)로부터 문자 메시지를 수신하고, 수신된 문자 메시지에 링크정보의 포함 여부를 확인한다. 여기서, 문자 메시지는 URL 주소, Short URL 주소, IP 주소 등의 링크정보를 포함하는 메시지일 수 있으며, 일반 텍스트 정보만을 포함하는 메시지일 수도 있다. 스미싱 방지장치(130)는 문자 메시지에 링크정보가 포함되어 있지 않으면, 동일한 문자 메시지를 메시지 센터(120)로 전송하여 단말기(110)에 전송되도록 한다.

[0029] 스미싱 방지장치(130)는 문자 메시지에 링크정보가 포함되어 있는 경우, 문자 메시지에 대응하는 링크 에뮬레이터를 할당하고, 링크정보를 링크 에뮬레이터에 대응하는 보안 링크정보로 변환한 문자 메시지를 메시지 센터(120)로 전송하여 단말기(110)에 전송되도록 한다. 더 자세히 설명하자면, 스미싱 방지장치(130)는 링크 에뮬레이터에 기 설정된 가상 식별정보를 포함하는 보안 링크정보를 생성하고, 문자 메시지에 포함된 링크정보를 보안 링크정보로 변환하여 단말기(110)에 제공되도록 문자 메시지를 메시지 센터(120)로 전송한다.

[0030] 스미싱 방지장치(130)는 단말기(110)로부터 보안 링크정보에 대한 연결 요청이 있는 경우, 연결 요청에 근거하여 링크 에뮬레이터를 실행하여 링크서비스 제공장치(140)로 접속하고, 접속결과에 대한 링크접속 이미지를 단말기(110)로 전송한다.

[0031] 스미싱 방지장치(130)는 단말기(110)로부터 보안 링크정보에 대한 연결 요청신호가 수신되는 경우, 연결 요청신호에 포함된 가상 식별정보에 해당하는 링크 에뮬레이터를 실행한다. 스미싱 방지장치(130)는 실행된 링크 에뮬레이터를 기반으로 가상 식별정보에 대응하는 링크정보를 이용하여 링크서비스 제공장치(140)로 접속하고, 접속결과에 대한 접속정보를 획득한다. 여기서, 접속정보는 접속된 링크서비스 제공장치(140)로부터 제공하는 링크접속 페이지에 대한 화면정보일 수 있다.

[0032] 스미싱 방지장치(130)는 링크서비스 제공장치(140)로부터 획득한 접속정보에 대응하는 링크접속 이미지를 생성하여 단말기(110)로 전송한다. 여기서, 링크접속 이미지는 접속정보 즉, 링크정보에 대응하는 링크 접속 페이지를 캡쳐, 스캔, 이미지 변환 등의 방식을 이용하여 생성된 이미지를 의미한다.

[0033] 스미싱 방지장치(130)는 단말기(110)로부터 링크접속 이미지의 일측에 대한 터치 위치정보가 수신되는 경우, 터치 위치정보에 대응하는 링크접속 이미지에 대한 영역을 확인하고, 링크 에뮬레이터를 기반으로 해당 영역에 기 설정된 추가 링크정보(예: 카테고리 세부연결 주소)로 접속하여 획득한 접속정보에 대한 링크접속 이미지를 생성하여 단말기(110)로 전송할 수 있다.

[0034] 한편, 스미싱 방지장치(130)는 단말기(110)로부터 링크접속 이미지의 타측에 구비된 원문 링크연결에 대한 입력신호가 수신되는 경우, 실행된 링크 에뮬레이터를 종료하고, 단말기(110)가 링크정보를 이용하여 링크서비스 제공장치(140)에 접속할 수 있도록 제어한다.

[0035] 링크서비스 제공장치(140)는 문자 메시지에 포함된 링크정보를 이용하여 접속할 수 있는 서버를 의미한다. 본 실시예에 따른 링크서비스 제공장치(140)는 스미싱 방지장치(130)에서 실행된 링크 에뮬레이터와 연동하여 접속정보를 전송할 수 있고, 단말기(110)와 직접 연결되어 접속정보를 제공할 수도 있다. 예컨대, 문자 메시지에 포함된 링크정보가 "박람회 안내: http://fair.com"인 경우, 링크서비스 제공장치(140)는 "http://fair.com"인

URL 주소에 대한 웹페이지 정보 또는 데이터를 제공하는 박람회 웹서버일 수 있다.

[0036] 도 2는 본 실시예에 따른 스미싱 방지장치를 개략적으로 나타낸 블록 구성도이다.

[0037] 본 실시예에 따른 스미싱 방지장치(130)는 통신부(210), 변환부(220), 에뮬레이터 실행부(230) 및 이미지 처리부(240)를 포함한다. 스미싱 방지장치(130)의 구성요소들은 버스(Bus)를 통해 서로 연결된다. 도 2에 도시된 스미싱 방지장치(130)는 일 실시예에 따른 것이고, 도 2에 도시된 모든 블록이 필수 구성요소는 아니며, 다른 실시예에서 일부 블록이 추가, 변경 또는 삭제될 수 있다.

[0038] 통신부(210)는 단말기(110) 및 메시지 센터(120)와 연결되어 각종 데이터 또는 신호를 송수신하는 동작을 수행한다.

[0039] 통신부(210)는 메시지 센터(120)로부터 문자 메시지를 수신한다. 여기서, 문자 메시지는 URL 주소, Short URL 주소, IP 주소 등의 링크정보를 포함하는 메시지일 수 있으며, 일반 텍스트 정보만을 포함하는 메시지일 수도 있다. 예컨대, 통신부(210)는 메시지 센터(120)로부터 "박람회 안내: http://fair.com"와 같은 링크정보를 포함하는 문자 메시지를 수신할 수 있다.

[0040] 통신부(210)는 링크정보가 보안 링크정보로 변환된 문자 메시지를 메시지 센터(120)로 전송하여 단말기(110)에 제공되도록 한다. 여기서, 보안 링크정보는 변환부(220)에서 변환된 링크정보로서, 가상으로 링크정보를 접속하는 링크 에뮬레이터를 실행하는 시키기 위한 가상 식별정보를 포함하는 정보를 의미한다.

[0041] 통신부(210)는 단말기(110)로부터 보안 링크정보에 대한 연결 요청신호를 수신하고, 수신된 연결 요청신호를 에뮬레이터 실행부(230)로 전송하여 링크 에뮬레이터가 실행되도록 한다. 또한, 통신부(210)는 실행된 링크 에뮬레이터를 기반으로 생성된 링크접속 이미지를 단말기(110)로 전송하여 출력되도록 한다.

[0042] 통신부(210)는 단말기(110)로부터 링크접속 이미지의 일측에 대한 터치 위치정보를 수신하고, 터치 위치정보에 대응하는 링크접속 이미지를 단말기(110)로 전송한다. 한편, 통신부(210)는 단말기(110)로부터 원문링크 연결요청 신호를 수신할 수도 있다. 여기서, 원문링크 연결요청 신호는 단말기(110)로부터 링크접속 이미지의 타측에 구비된 원문 링크연결 버튼에 대한 입력신호를 의미한다.

[0043] 변환부(220)는 문자 메시지의 링크정보 포함 여부를 확인하고, 링크정보가 포함되어 있는 경우, 문자 메시지에 대응하는 링크 에뮬레이터를 할당하여 링크정보를 링크 에뮬레이터에 대응하는 보안 링크정보로 변환하여 단말기(110)로 전송되도록 하는 동작을 수행한다.

[0044] 변환부(220)는 통신부(210)로부터 수신된 문자 메시지 내에 URL 주소와 같이 외부로 연결 가능한 링크정보의 포함 여부를 확인하고, 문자 메시지 내에 링크정보가 포함된 경우, 스미싱을 방지하기 위한 링크 에뮬레이터를 할당한다. 여기서, 링크 에뮬레이터는 링크정보를 가상으로 연결하는 프로그램을 의미하며, 가상 폰, 가상 PC와 같은 형태로 스미싱 방지장치(130) 내에 기 설치 또는 기 저장된 형태의 가상 링크연결 프로그램일 수 있다.

[0045] 변환부(220)는 할당된 링크 에뮬레이터를 실행시키기 위한 식별정보를 포함하는 보안 링크정보를 생성하고, 문자 메시지에 포함된 링크정보를 보안 링크정보로 변환하여 단말기(110)에 제공되도록 메시지 센터(120)로 전송한다. 예컨대, 변환부(220)는 모바일 청첩장에 대한 "모바일 청첩장: http://m.wedding.com/201403"과 같은 링크정보를 포함하는 문자 메시지를 수신하는 경우, 문자 메시지에 대응하는 링크 에뮬레이터를 할당하고, 링크정보를 링크 에뮬레이터를 실행시키기 위한 "모바일 청첩장: http://smirroring.com/LE00a00a"과 같은 보안 링크정보로 변환한 문자 메시지를 단말기(110)로 전송되도록 한다.

[0046] 에뮬레이터 실행부(230)는 단말기(110)로부터 보안 링크정보에 대한 연결 요청이 있는 경우, 연결 요청에 근거하여 링크 에뮬레이터를 실행하여 링크서비스 제공장치(140)로 접속하는 동작을 수행한다.

[0047] 에뮬레이터 실행부(230)는 단말기(110)로부터 보안 링크정보에 대한 연결 요청신호가 수신되는 경우, 연결 요청신호에 포함된 가상 식별정보에 해당하는 링크 에뮬레이터를 실행한다. 에뮬레이터 실행부(230)는 실행된 링크 에뮬레이터를 기반으로 가상 식별정보에 대응하는 링크정보를 이용하여 링크서비스 제공장치(140)로 접속하고, 접속결과에 대한 접속정보를 획득한다. 여기서, 접속정보는 접속된 링크서비스 제공장치(140)로부터 제공하는 링크 접속 페이지에 대한 화면정보일 수 있다. 에뮬레이터 실행부(230)는 획득한 접속정보를 이미지 처리부(240)로 전송하여 링크접속 이미지가 생성되도록 한다.

[0048] 한편, 에뮬레이터 실행부(230)는 단말기(110)로부터 링크접속 이미지의 일측에 대한 터치 위치정보가 수신되는 경우, 터치 위치정보에 대응하는 링크접속 이미지에 대한 영역을 확인하고, 링크 에뮬레이터를 기반으로 해당

영역에 기 설정된 추가 링크정보를 이용하여 접속정보를 획득할 수 있다. 예컨대, 에뮬레이터 실행부(230)는 단말기(110)로부터 (3, 5)와 같은 터치 위치정보가 수신되면, 링크접속 이미지 중 (3, 5)가 위치하는 영역에 기 설정된 추가 링크정보(예: 카테고리 세부연결 주소)를 확인하고, 추가 링크정보를 이용하여 접속된 링크 접속 페이지(접속 정보)를 획득할 수 있다.

[0049] 또한, 에뮬레이터 실행부(230)는 단말기(110)로부터 링크접속 이미지의 타측에 구비된 원문 링크연결에 대한 입력신호가 수신되는 경우, 링크 에뮬레이터를 종료하고, 단말기(110)가 링크정보를 이용하여 링크서비스 제공장치(140)로 접속되도록 한다.

[0050] 에뮬레이터 실행부(230)는 링크 에뮬레이터를 실행한 후 기 설정된 유효 시간이 경과하거나, 기 설정된 일정시간 동안 단말기(110)로부터 입력신호가 존재하지 않는 경우 링크 에뮬레이터를 종료한다. 또한, 에뮬레이터 실행부(230)는 단말기(110)로부터 문자 메시지가 스팸 메시지인 것으로 판단된 입력신호가 수신되는 경우, 해당 링크정보를 스팸 리스트에 등록하고, 링크 에뮬레이터를 종료할 수도 있다.

[0051] 이미지 처리부(240)는 링크서비스 제공장치(140)로부터 획득한 접속정보에 대응하는 링크접속 이미지를 생성하여 단말기(110)로 전송되도록 한다. 본 실시예에 따른 이미지 처리부(240)는 접속정보 즉, 링크정보에 대응하는 링크 접속 페이지를 캡쳐, 스캔, 이미지 변환 등의 방식을 이용하여 링크접속 이미지를 생성하고, 생성된 링크접속 이미지가 단말기(110)에서 디스플레이되도록 한다.

[0052] 한편, 본 실시예에 따른 이미지 처리부(240)는 접속정보를 캡쳐, 스캔, 이미지 변환 등의 방식을 이용하여 생성된 링크접속 이미지를 단말기(110)로 전송하여 출력되도록 하는 것으로만 기재하고 있으나 반드시 이에 한정되는 것은 아니다. 예컨대, 이미지 처리부(240)는 접속정보에 대한 영상 소스정보를 단말기(110)로 전송하고, 단말기(110)에 구동되는 특정 애플리케이션을 이용하여 디코딩되어 출력되도록 할 수도 있다.

[0053] 도 3은 본 실시예에 따른 스미싱을 방지하기 위해 보안 링크정보가 포함된 문자 메시지를 제공하는 동작을 설명하기 위한 순서도이다.

[0054] 스미싱 방지장치(130)는 메시지 센터(120)로부터 단말기(110)로 전송되는 문자 메시지를 수신한다(S310). 여기서, 문자 메시지는 URL 주소, Short URL 주소, IP 주소 등의 링크정보를 포함하는 메시지일 수 있으며, 일반 텍스트 정보만을 포함하는 메시지일 수도 있다.

[0055] 스미싱 방지장치(130)는 문자 메시지의 링크정보 포함 여부를 확인하고(S320), 문자 메시지에 링크정보가 포함되어 있지 않은 경우 동일한 문자 메시지가 단말기(110)로 전송되도록 한다.

[0056] 단계 S320의 확인결과, 스미싱 방지장치(130)는 문자 메시지에 링크정보가 포함되어 있는 경우, 링크 에뮬레이터를 할당하고(S330), 링크정보를 링크 에뮬레이터에 대한 가상 식별정보를 포함하는 보안 링크정보로 변환한다(S340). 더 자세히 설명하자면, 스미싱 방지장치(130)는 문자 메시지에 링크정보가 포함되면, 문자 메시지에 대응하는 링크 에뮬레이터를 할당하고, 할당된 링크 에뮬레이터에 대응하는 가상 식별정보를 포함한 보안 링크정보로 문자 메시지에 포함된 링크정보를 변환한다. 스미싱 방지장치(130)는 메시지 센터(120)를 경유하여 링크정보가 보안 링크정보로 변환된 문자 메시지가 단말기(110)로 전송되도록 한다(S350)

[0057] 도 4는 본 실시예에 따른 스미싱을 방지하기 위해 링크 에뮬레이터를 이용하여 링크정보로 접속하는 동작을 설명하기 위한 순서도이다.

[0058] 단말기(110)는 수신된 보안 링크정보가 포함된 문자 메시지를 확인하고(S410), 사용자의 조작 또는 입력에 근거하여 연결요청이 있는 경우, 스미싱 방지장치(130)로 연결요청 신호를 전송한다(S420).

[0059] 스미싱 방지장치(130)는 단말기(110)로부터 수신된 연결요청 신호에 포함된 가상 식별정보를 확인하고(S430), 가상 식별정보에 대응하는 링크 에뮬레이터를 실행한다(S440).

[0060] 스미싱 방지장치(130)는 실행된 링크 에뮬레이터를 기반으로 가상 식별정보에 대응하는 링크정보를 이용하여 링크서비스 제공장치(140)에 접속하고(S450), 링크서비스 제공장치(140)의 접속정보를 획득한다(S452). 여기서, 접속정보는 접속된 링크서비스 제공장치(140)로부터 제공하는 링크 접속 페이지에 대한 화면정보일 수 있다.

[0061] 스미싱 방지장치(130)는 접속정보에 대한 링크접속 이미지를 생성하고(S460), 생성된 링크접속 이미지를 단말기(110)로 전송한다(S470). 여기서, 링크접속 이미지는 접속정보 즉, 링크정보에 대응하는 링크 접속 페이지를 캡쳐, 스캔, 이미지 변환 등의 방식을 이용하여 생성된 이미지를 의미한다.

[0062] 스미싱 방지장치(130)는 단말기(110)로부터 링크접속 이미지의 일측에 대한 터치 위치정보가 수신되는 경우

(S480), 터치 위치정보에 대응하는 링크접속 이미지에 대한 영역을 확인하고, 링크 에뮬레이터를 기반으로 해당 영역에 기 설정된 추가 링크정보(예: 카테고리 세부연결 주소)를 이용하여 링크서비스 제공장치(130)로 접속하고(S482), 링크서비스 제공장치(130)로부터 획득한 접속정보에 대한 링크접속 이미지를 생성하여 단말기(110)로 전송한다(S486).

[0063] 한편, 스미싱 방지장치(130)는 단말기(110)로부터 링크접속 이미지의 타측에 구비된 원문 링크연결에 대한 입력신호가 수신되는 경우, 실행된 링크 에뮬레이터를 종료하고, 단말기(110)가 링크정보를 이용하여 링크서비스 제공장치(140)에 접속할 수 있도록 제어한다.

[0064] 스미싱 방지장치(130)는 링크 에뮬레이터를 실행한 후 기 설정된 유효 시간이 경과하거나, 기 설정된 일정시간 동안 단말기(110)로부터 입력신호가 존재하지 않는 경우 링크 에뮬레이터를 종료한다(S490).

[0065] 도 5는 본 실시예에 따른 보안 링크정보를 포함하는 모바일 청접장을 나타낸 예시도이다.

[0066] 도 5의 (a)는 일반적으로 링크정보를 포함하는 메시지(510)를 디스플레이한 화면을 나타낸 도면이고, 도 5의 (b)는 본 실시예에 따른 보안 링크정보를 포함하는 메시지(520)를 디스플레이한 화면을 나타낸 도면이다.

[0067] 도 5의 (b)에 도시된 바와 같이, 스미싱 방지장치(130)는 "http://moa.so/4t"와 같은 모바일 청첩장에 대한 링크정보를 "http://smirroring.com/LE000a00a"와 같은 링크 에뮬레이터를 실행시키기 위한 보안 링크정보로 변환한 메시지(520)를 메시지 센터(120)로 전송하여 단말기(110)에 디스플레이되도록 한다.

[0068] 도 6은 본 실시예에 따른 보안 링크정보를 포함하는 복수의 문자 메시지를 나타낸 예시도이다.

[0069] 도 6의 (a)는 일반적으로 단말기가 수신하는 다양한 내용의 링크정보를 포함하는 메시지(610)를 나타낸 예시이고, 도 6의 (b)는 본 실시예에 따른 보안 링크정보를 포함하는 메시지(620)를 나타낸 예시이다.

[0070] 도 6의 (b)는 스미싱 방지장치(130)에서 링크정보를 포함하는 복수의 메시지(610)를 각각 수신하는 경우, 스미싱 방지장치(130)는 수신된 각각의 메시지에 포함된 링크정보를 할당된 각각의 링크 에뮬레이터에 대한 가상 식별정보를 포함하는 보안 식별정보로 변환한 메시지(620)를 메시지 센터(120)로 전송하여 단말기(110)에 디스플레이되도록 한다.

[0071] 도 7a은 본 실시예에 따른 스미싱을 방지하기 위한 이미지 및 원문링크 연결버튼을 나타낸 예시도이다.

[0072] 스미싱 방지장치(130)는 단말기(110)로부터 보안 링크정보에 대한 연결 요청신호가 수신되면, 연결 요청신호에 포함된 가상 식별정보에 해당하는 링크 에뮬레이터를 실행하고, 링크 에뮬레이터를 기반으로 접속된 링크서비스 제공장치(140)로부터 획득한 접속정보에 대응하는 링크접속 이미지를 단말기(110)로 전송한다.

[0073] 도 7a는 스미싱 방지장치(130)로부터 모바일 청첩장에 대한 링크접속 이미지(710)를 수신하여 출력된 단말기(110) 화면을 나타낸다. 여기서, 모바일 청첩장에 대한 링크접속 이미지(710)의 하단에는 사용자의 터치 입력에 근거하여 링크정보를 연결하기 위한 링크연결 영역(720)이 구비될 수 있다.

[0074] 사용자는 단말기(110)에 출력된 모바일 청첩장에 대한 링크접속 이미지(710)을 확인하여 링크정보가 안전한 것으로 판단되면, 링크연결 영역(720)에 대한 터치입력을 수행하여 원문 링크연결에 대한 입력신호가 스미싱 방지장치(130)로 전송되도록 한다. 여기서, 단말기(110)는 특정 애플리케이션(예: 스미싱 방지 애플리케이션)이 구동되어 링크연결 영역(720)에 대한 입력신호를 스미싱 방지장치(130)로 전송되도록 할 수 있고, 단말기(110)의 웹브라우저 상에서 링크연결 영역(720)에 대한 입력신호를 스미싱 방지장치(130)로 전송되도록 할 수도 있다.

[0075] 스미싱 방지장치(130)는 단말기(110)로부터 원문 링크연결에 대한 입력신호가 수신되는 경우, 실행된 링크 에뮬레이터를 종료하고, 단말기(110)가 링크정보를 이용하여 링크서비스 제공장치(140)에 접속할 수 있도록 제어한다.

[0076] 도 7b는 본 실시예에 따른 스미싱을 방지하기 위한 이미지 및 터치입력에 따른 동작을 설명하기 위한 예시도이다.

[0077] 스미싱 방지장치(130)는 단말기(110)로부터 보안 링크정보에 대한 연결 요청신호가 수신되면, 연결 요청신호에 포함된 가상 식별정보에 해당하는 링크 에뮬레이터를 실행하고, 링크 에뮬레이터를 기반으로 접속된 링크서비스 제공장치(140)로부터 획득한 접속정보에 대응하는 링크접속 이미지를 단말기(110)로 전송한다.

[0078] 도 7b는 스미싱 방지장치(130)로부터 모바일 청첩장에 대한 링크접속 이미지(710)를 수신하여 출력된 단말기(110) 화면을 나타낸다. 단말기(110)는 사용자로부터 모바일 청첩장에 대한 링크접속 이미지(710) 중 '오시는

길'에 대한 영역(730)의 터치 입력이 존재하면, 단말기(110)는 터치 입력에 대한 터치 위치정보를 스미싱 방지 장치(130)로 전송한다. 여기서, 단말기(110)는 특정 애플리케이션(예: 스미싱 방지 애플리케이션)이 구동되어 모바일 청첩장에 대한 링크접속 이미지(710) 중 터치 입력에 대한 터치 위치정보를 산출하여 스미싱 방지장치(130)로 전송할 수 있다.

[0079] 스미싱 방지장치(130)는 수신된 터치 위치정보에 대응하는 링크접속 이미지에 대한 영역을 확인하고, 링크 에뮬레이터를 기반으로 해당 영역에 기 설정된 지도연결 주소(추가 링크정보)로 접속하여 획득한 접속정보에 대한 길안내 이미지(740)를 생성하여 단말기(110)로 전송할 수 있다.

[0080] 이상의 설명은 본 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 실시예들은 본 실시예의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

산업상 이용가능성

[0081] 이상에서 설명한 바와 같이 본 실시예는 단말기를 이용하여 링크를 연결하는 분야에 적용되어, 사용자가 실수도 링크정보를 입력하더라도 스미싱 피해가 발생하지 않도록 하고, 단말기에 바이러스성 애플리케이션이나 악성코드가 다운로드 또는 설치되는 것을 방지할 수 있는 효과를 발생하는 유용한 발명이다.

부호의 설명

[0082] 110: 단말기 120: 메시지 센터

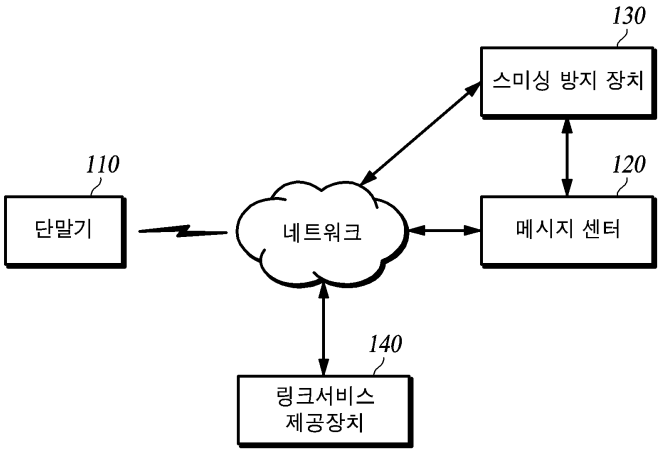
130: 스미싱 방지장치 140: 링크서비스 제공장치

210: 통신부 220: 변환부

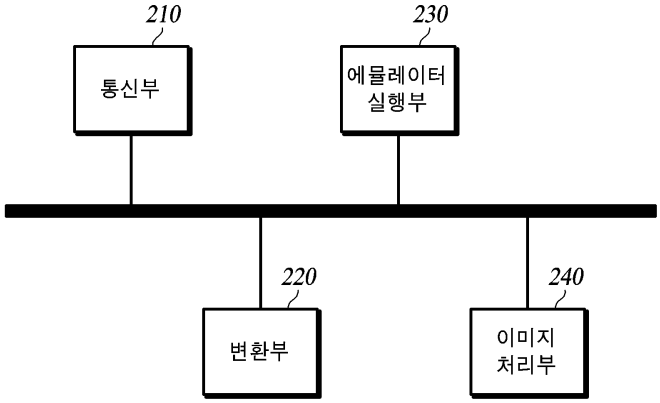
230: 에뮬레이터 실행부 240: 이미지 처리부

도면

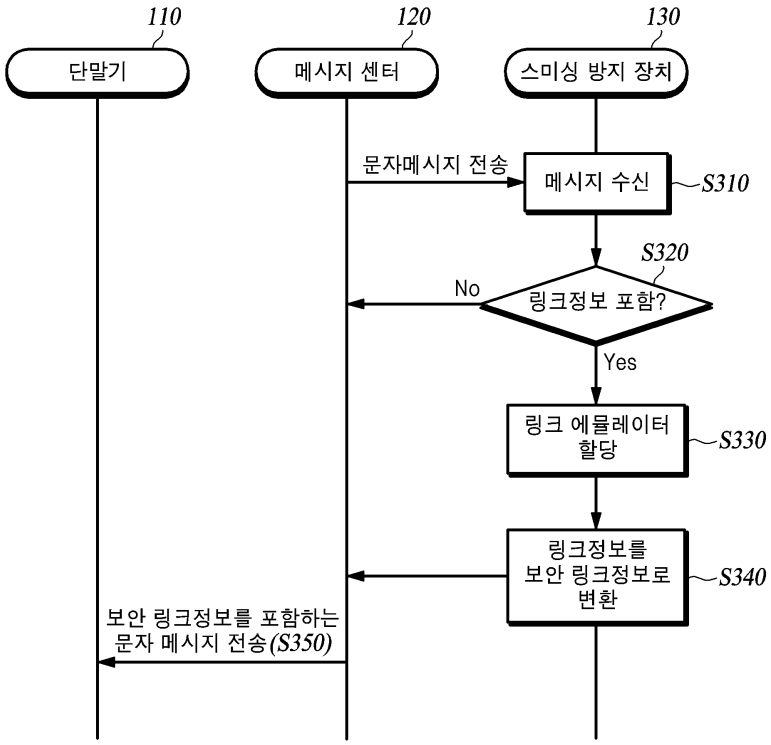
도면1



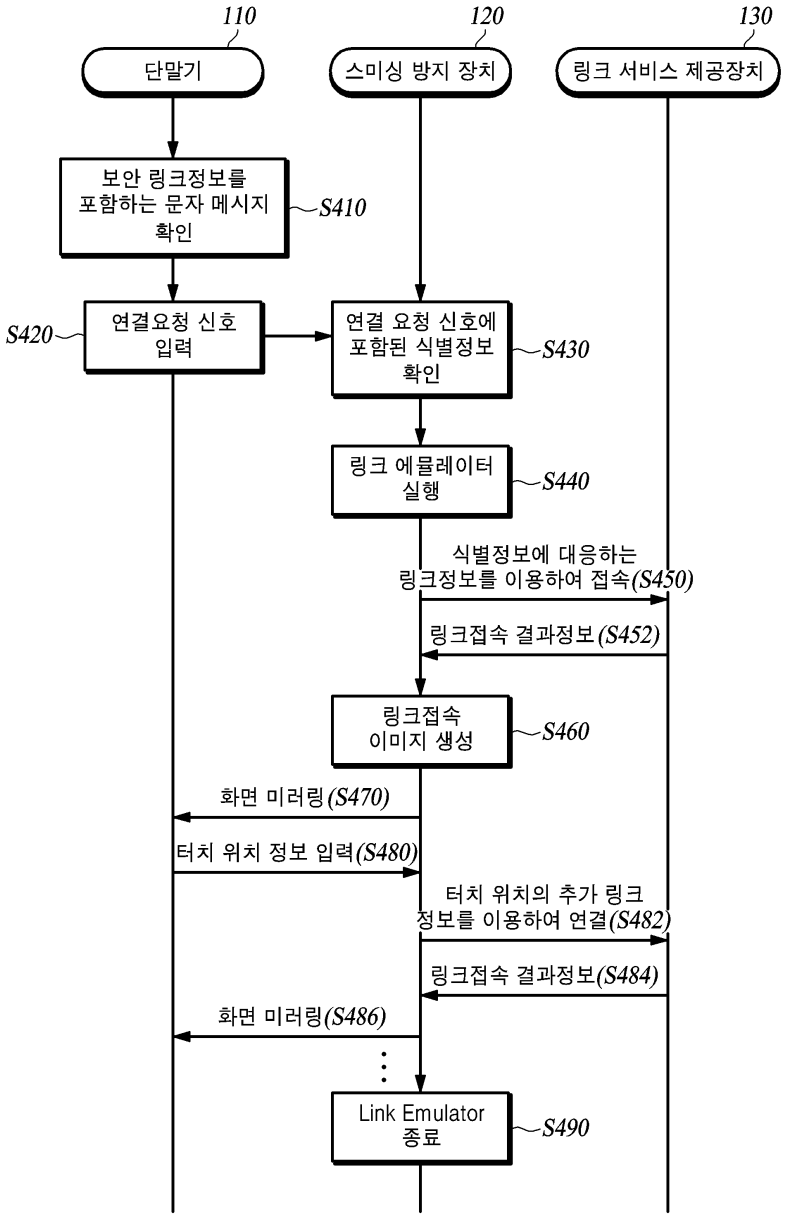
도면2


210
통신부
230
에뮬레이터
실행부
220
변환부
240
이미지
처리부

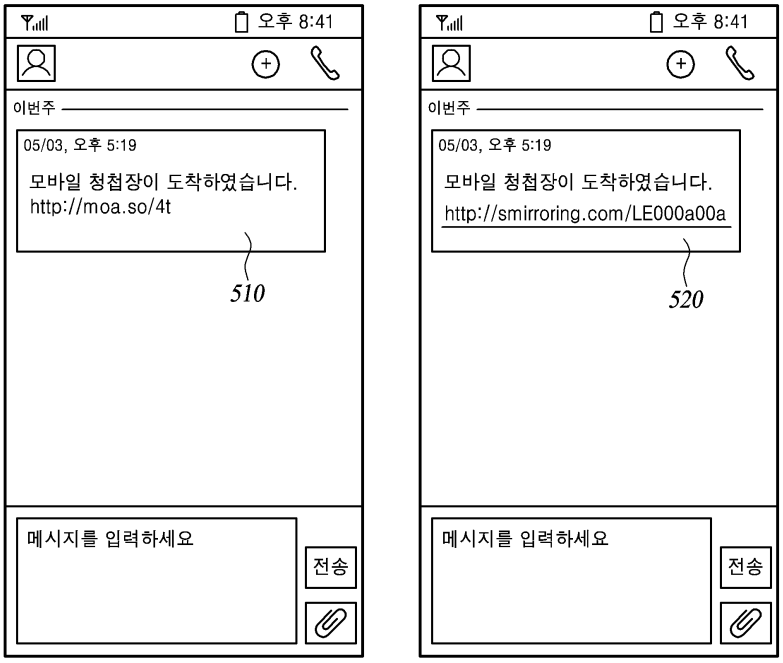
도면3


110
단말기
120
메시지 센터
130
스미싱 방지 장치
문자메시지 전송
메시지 수신
S310
S320
No
링크정보 포함?
Yes
링크 에뮬레이터
할당
S330
링크정보를
보안 링크정보로
변환
S340
보안 링크정보를 포함하는
문자 메시지 전송(S350)

도면4


110
120
130
단말기
스미싱 방지 장치
링크 서비스 제공장치
보안 링크정보를 포함하는 문자 메시지 확인
S410
S420
연결요청 신호 입력
연결 요청 신호에 포함된 식별정보 확인
S430
링크 에뮬레이터 실행
S440
식별정보에 대응하는 링크정보를 이용하여 접속(S450)
링크접속 결과정보(S452)
링크접속 이미지 생성
S460
화면 미러링(S470)
터치 위치 정보 입력(S480)
터치 위치의 추가 링크 정보를 이용하여 연결(S482)
링크접속 결과정보(S484)
화면 미러링(S486)
Link Emulator 종료
S490

도면5



(a) (b)

도면6

이** 나야 전화가 안되서 이걸로 나랑 대화해 많이 급하다 www.kid*******ct.com/kids.apk
하** 나야 전화가 안돼 이걸로 하자 급해 www.adu*******ct.com/adult.apk
김** 나야 전화가 안되서 이걸로 하자 급해 www.mar*******19.com/mars.apk
박**님 데이터사용초과 익월요금합산청구 확인 www.mar*******ct.com/a.apk
하**님 모바일 청첩장이 도착했습니다 www.mar*******1.net/a.apk

610

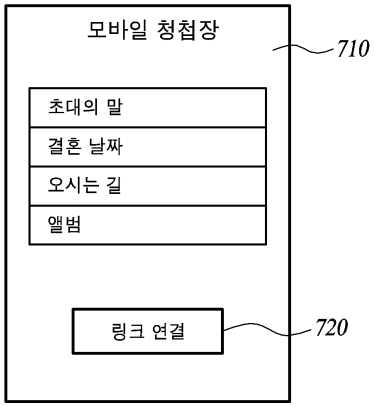
(a)

이** 나야 전화가 안되서 이걸로 나랑 대화해 많이 급하다 http://smirroring.com/VI000b00a
하** 나야 전화가 안돼 이걸로 하자 급해 http://smirroring.com/GE000b00c
김** 나야 전화가 안되서 이걸로 하자 급해 http://smirroring.com/HT000g00d
박**님 데이터사용초과 익월요금합산청구 확인 http://smirroring.com/JT000f00f
하**님 모바일 청첩장이 도착했습니다 http://smirroring.com/LT000g00a

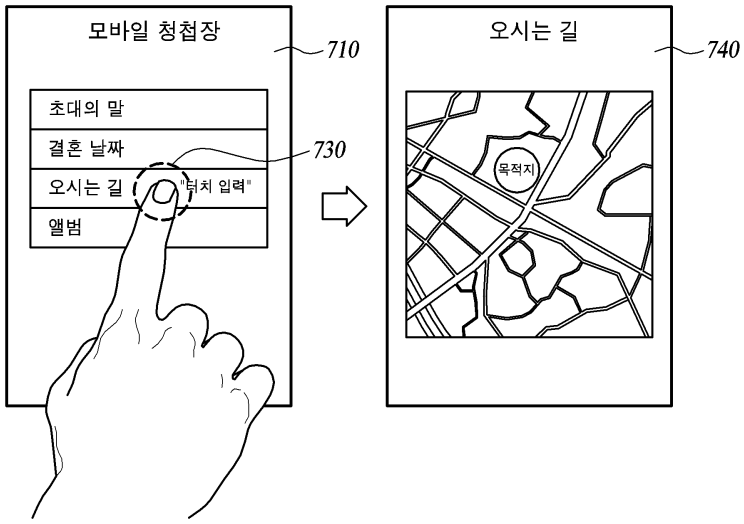
620

(b)

도면7a


모바일 청첩장
710
초대의 말
결혼 날짜
오시는 길
앨범
링크 연결
720

도면7b


모바일 청첩장
710
초대의 말
결혼 날짜
730
오시는 길
"터치 입력"
앨범
오시는 길
740
목적지