



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2016년02월22일

(11) 등록번호 10-1594846

(24) 등록일자 2016년02월11일

(51) 국제특허분류(Int. Cl.)

H04L 9/12 (2006.01)

(21) 출원번호 10-2014-0172073

(22) 출원일자 2014년12월03일

심사청구일자 2014년12월03일

(56) 선행기술조사문헌

JP2000134193 A

KR1020010100326 A

(73) 특허권자

조선대학교산학협력단

광주광역시 동구 필문대로 309 (서석동)

동국대학교 산학협력단

서울특별시 중구 필동로1길 30 (필동3가, 동국대학교)

서울대학교산학협력단

서울특별시 관악구 관악로 1 (신림동)

(72) 발명자

임대운

서울특별시 은평구 진관2로 57-37, 243동 1001호

노종선

서울특별시 강남구 광평로10길 15 상록수아파트 109동 406호

김영식

광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호

(74) 대리인

김효성

전체 청구항 수 : 총 14 항

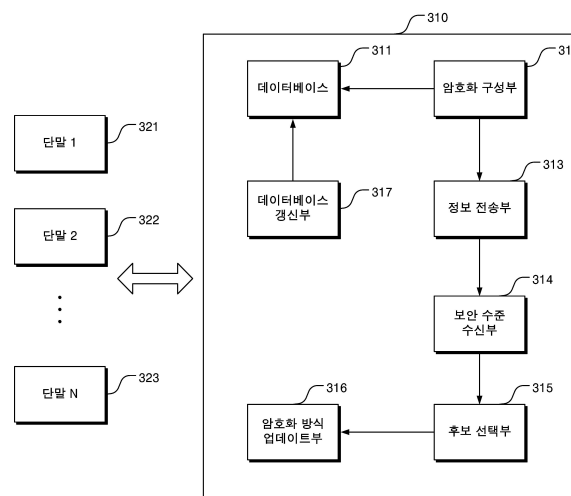
심사관 : 전용해

(54) 발명의 명칭 가변 암호화 기반의 네트워크 보안 장치 및 그 동작 방법

(57) 요약

가변 암호화 기반의 네트워크 보안 장치 및 그 동작 방법이 개시된다. 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치 및 그 동작 방법은 특정 주기 간격으로, 소정의 암호화 방식 정보를 구성하고, 해당 암호화 방식 정보들 간의 보안 수준에 따라서, 가장 높은 보안 수준을 갖는 암호화 방식 정보를 네트워크로 연결되어 있는 복수의 단말들의 데이터 송수신에 사용될 암호화 방식 후보로 선택해 둔 후 상기 복수의 단말들 사이에서 데이터 송수신시에 데이터 암호화 실패와 같은 보안상 문제가 발생하는 경우, 상기 복수의 단말들이 현재 사용하고 있는 암호화 방식을 상기 암호화 방식 후보로 선택된 암호화 방식으로 변경해줌으로써, 네트워크의 보안을 강화시킬 수 있다.

대표도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호 1711014090
 부처명 미래창조과학부
 연구관리전문기관 정보통신산업진흥원
 연구사업명 정보통신기술인력양성
 연구과제명 산업기밀 정보유출 방지를 위한 융합보안 SW 연구 및 전문인력양성
 기 여 율 1/2
 주관기관 중앙대학교 산학협력단
 연구기간 2014.06.01 ~ 2014.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호 1711013664
 부처명 미래창조과학부
 연구관리전문기관 한국연구재단
 연구사업명 중견연구자지원
 연구과제명 포스트 양자 암호의 설계 및 효율적 구현에 관한 연구
 기 여 율 1/2
 주관기관 조선대학교
 연구기간 2014.05.01 ~ 2015.04.30

이 발명을 지원한 국가연구개발사업

과제고유번호 1711014090
 부처명 미래창조과학부
 연구관리전문기관 정보통신산업진흥원
 연구사업명 정보통신기술인력양성
 연구과제명 산업기밀 정보유출 방지를 위한 융합보안 SW 연구 및 전문인력양성
 기 여 율 1/1
 주관기관 중앙대학교 산학협력단
 연구기간 2014.06.01 ~ 2014.12.31

명세서

청구범위

청구항 1

데이터의 암호화와 연관된 복수의 스크램블링(scrambling) 방식들이 저장되어 있는 데이터베이스;

선정된(predetermined) 제1 주기 간격으로, 상기 복수의 스크램블링 방식들 중에서 적어도 하나의 스크램블링 방식을 랜덤하게 선택하고, 데이터에 대해 상기 적어도 하나의 스크램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성하는 암호화 구성부;

상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 구성됨으로써, 상기 암호화 방식 정보가 선정된 개수만큼 생성되면, 상기 선정된 개수의 암호화 방식 정보들을 네트워크로 서로 연결되어 있는 복수의 단말들 중 랜덤하게 선택된 제1 단말로 전송하는 정보 전송부;

상기 제1 단말로부터 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 보안 수준 정보를 수신하는 보안 수준 수신부;

상기 보안 수준 정보를 참조하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제1 암호화 방식 정보를 상기 복수의 단말들 간의 데이터 송수신을 위한 암호화 방식 후보로 선택한 후 상기 암호화 방식 후보로 선택된 상기 제1 암호화 방식 정보를 메모리에 저장하는 후보 선택부; 및

상기 복수의 단말들 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 보안 이벤트가 선정된 기간 이내에 선정된 횟수 이상 발생하는 경우, 상기 복수의 단말들에 대해, 상기 제1 암호화 방식 정보를 전송함으로써, 상기 복수의 단말들이 상기 제1 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어하는 암호화 방식 업데이트부

를 포함하는 가변 암호화 기반의 네트워크 보안 장치.

청구항 2

제1항에 있어서,

상기 정보 전송부는

상기 제1 암호화 방식 정보가 상기 암호화 방식 후보로 선택된 이후 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 신규로 구성됨으로써, 상기 신규로 구성된 암호화 방식 정보가 상기 제1 암호화 방식 정보를 포함하여 상기 선정된 개수만큼 생성되면, 상기 제1 암호화 방식 정보를 포함하는 상기 선정된 개수의 신규 암호화 방식 정보들을 상기 복수의 단말들 중 랜덤하게 재선택된 제2 단말로 전송하고,

상기 보안 수준 수신부는

상기 제2 단말로부터 상기 선정된 개수의 신규 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 신규 보안 수준 정보를 수신하며,

상기 후보 선택부는

상기 신규 보안 수준 정보를 참조하여 상기 선정된 개수의 신규 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제2 암호화 방식 정보를 상기 복수의 단말들 간의 데이터 송수신을 위한 암호화 방식 후보로 재선택한 후 상기 암호화 방식 후보로 재선택된 상기 제2 암호화 방식 정보를 메모리에 저장하며,

상기 암호화 방식 업데이트부는

상기 복수의 단말들 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 상기 보안 이벤트가 상기 선정된 기간 이내에 상기 선정된 횟수 이상 발생하는 경우, 상기 복수의 단말들에 대해, 상기 제2 암호화 방식 정보를 전송함으로써, 상기 복수의 단말들이 상기 제2 암호화 방식 정보를 기초로 데이터를 암호화

화하여 송수신하도록 제어하는 가변 암호화 기반의 네트워크 보안 장치.

청구항 3

제1항에 있어서,

선정된 제2 주기 간격으로, 상기 데이터베이스에 저장되어 있는 상기 복수의 스크램블링 방식들 중에서 랜덤하게 선택된 적어도 하나의 제1 스크램블링 방식을 삭제하고, 적어도 하나의 신규 스크램블링 방식을 생성하여 상기 데이터베이스에 저장하는 데이터베이스 갱신부

를 더 포함하는 가변 암호화 기반의 네트워크 보안 장치.

청구항 4

제1항에 있어서,

상기 제1 단말은

상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 차분 공격 분석(Differential Cryptanalysis)을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율(Propagation Ratio)을 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율이 낮을수록 높은 보안 수준이 할당되도록 상기 보안 수준 정보를 구성하는 가변 암호화 기반의 네트워크 보안 장치.

청구항 5

제1항에 있어서,

상기 제1 단말은

상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 선형 공격 분석(Linear Cryptanalysis)을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스(bias)를 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스가 낮을수록 높은 보안 수준이 할당되도록 상기 보안 수준 정보를 구성하는 가변 암호화 기반의 네트워크 보안 장치.

청구항 6

제1항에 있어서,

상기 복수의 단말들은

어느 하나의 단말로부터 암호화된 데이터가 수신되면, 상기 암호화된 데이터를 복호화한 후 복호화된 데이터를 파싱하여 상기 복호화된 데이터에 포함되어 있는 데이터 헤더(header) 구조를 파악하고, 상기 데이터 헤더 구조와 메모리 상에 기 저장되어 있는 상기 복호화된 데이터의 데이터 교환을 위한 통신 프로토콜 표준 따른 헤더 구조 정보를 비교하여 상기 데이터 헤더 구조가 상기 헤더 구조 정보에 매칭되지 않는 것으로 판단되면, 상기 보안 이벤트를 발생시키는 가변 암호화 기반의 네트워크 보안 장치.

청구항 7

데이터의 암호화와 연관된 복수의 스크램블링(scrambling) 방식들이 저장되어 있는 데이터베이스를 유지하는 단계;

선정된(predetermined) 제1 주기 간격으로, 상기 복수의 스크램블링 방식들 중에서 적어도 하나의 스크램블링 방식을 랜덤하게 선택하고, 데이터에 대해 상기 적어도 하나의 스크램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성하는 단계;

상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 구성됨으로써, 상기 암호화 방식 정보가 선정된 개수만큼 생성되면, 상기 선정된 개수의 암호화 방식 정보들을 네트워크로 서로 연결되어 있는 복수의 단말들 중 랜덤하게 선택된 제1 단말로 전송하는 단계;

상기 제1 단말로부터 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 보안 수준 정보를 수신하는 단계;

상기 보안 수준 정보를 참조하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제1 암호화 방식 정보를 상기 복수의 단말들 간의 데이터 송수신을 위한 암호화 방식 후보로 선택한 후 상기 암호화 방식 후보로 선택된 상기 제1 암호화 방식 정보를 메모리에 저장하는 단계; 및

상기 복수의 단말들 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 보안 이벤트가 선정된 기간 이내에서 선정된 횟수 이상 발생하는 경우, 상기 복수의 단말들에 대해, 상기 제1 암호화 방식 정보를 전송함으로써, 상기 복수의 단말들이 상기 제1 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어하는 단계

를 포함하는 가변 암호화 기반의 네트워크 보안 장치의 동작 방법.

청구항 8

제7항에 있어서,

상기 제1 암호화 방식 정보가 상기 암호화 방식 후보로 선택된 이후 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 신규로 구성됨으로써, 상기 신규로 구성된 암호화 방식 정보가 상기 제1 암호화 방식 정보를 포함하여 상기 선정된 개수만큼 생성되면, 상기 제1 암호화 방식 정보를 포함하는 상기 선정된 개수의 신규 암호화 방식 정보들을 상기 복수의 단말들 중 랜덤하게 재선택된 제2 단말로 전송하는 단계;

상기 제2 단말로부터 상기 선정된 개수의 신규 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 신규 보안 수준 정보를 수신하는 단계;

상기 신규 보안 수준 정보를 참조하여 상기 선정된 개수의 신규 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제2 암호화 방식 정보를 상기 복수의 단말들 간의 데이터 송수신을 위한 암호화 방식 후보로 재선택한 후 상기 암호화 방식 후보로 재선택된 상기 제2 암호화 방식 정보를 메모리에 저장하는 단계; 및

상기 복수의 단말들 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 상기 보안 이벤트가 상기 선정된 기간 이내에서 상기 선정된 횟수 이상 발생하는 경우, 상기 복수의 단말들에 대해, 상기 제2 암호화 방식 정보를 전송함으로써, 상기 복수의 단말들이 상기 제2 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어하는 단계

를 더 포함하는 가변 암호화 기반의 네트워크 보안 장치의 동작 방법.

청구항 9

제7항에 있어서,

선정된 제2 주기 간격으로, 상기 데이터베이스에 저장되어 있는 상기 복수의 스크램블링 방식들 중에서 랜덤하게 선택된 적어도 하나의 제1 스크램블링 방식을 삭제하고, 적어도 하나의 신규 스크램블링 방식을 생성하여 상기 데이터베이스에 저장하는 단계

를 더 포함하는 가변 암호화 기반의 네트워크 보안 장치의 동작 방법.

청구항 10

제7항에 있어서,

상기 제1 단말은

상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 차분 공격 분석(Differential Cryptanalysis)을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율(Propagation Ratio)을 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율이 낮을수록 높은 보안 수준이 할당되도록 상기 보안 수준 정보를 구성하는 가변 암호화 기반의 네트워크 보안 장치의 동작 방법.

청구항 11

제7항에 있어서,

상기 제1 단말은

상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 선형 공격 분석(Linear Cryptanalysis)을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스(bias)를 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스가 낮을수록 높은 보안 수준이 할당되도록 상기 보안 수준 정보를 구성하는 가변 암호화 기반의 네트워크 보안 장치의 동작 방법.

청구항 12

제7항에 있어서,

상기 복수의 단말들은

어느 하나의 단말로부터 암호화된 데이터가 수신되면, 상기 암호화된 데이터를 복호화한 후 복호화된 데이터를 파싱하여 상기 복호화된 데이터에 포함되어 있는 데이터 헤더(header) 구조를 파악하고, 상기 데이터 헤더 구조와 메모리 상에 기 저장되어 있는 상기 복호화된 데이터의 데이터 교환을 위한 통신 프로토콜 표준 따른 헤더 구조 정보를 비교하여 상기 데이터 헤더 구조가 상기 헤더 구조 정보에 매칭되지 않는 것으로 판단되면, 상기 보안 이벤트를 발생시키는 가변 암호화 기반의 네트워크 보안 장치의 동작 방법.

청구항 13

제7항 내지 제12항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 14

제7항 내지 제12항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명의 실시예들은 사물인터넷 시스템(Internet of Thing)과 같이, 다양한 단말들이 서로 네트워크로 연결되어 있는 환경에서 보안을 강화시키기 위한 보안 기술들과 관련된다.

배경 기술

[0002] 최근, 무선 인터넷 또는 이동통신 등과 같은 다양한 네트워크 환경이 구축됨에 따라, 사용자가 네트워크 통신이 가능한 단말을 이용하여 어디에서든지 인터넷에 접속할 수 있게 되었다.

[0003] 이러한 네트워크 환경 구축에 힘입어 최근에는 일상에 존재하는 다양한 사물들이 서로 네트워크로 연결되어, 정보를 공유할 수 있도록 하는 사물인터넷(Internet of Thing) 시스템이 도입되고 있다.

[0004] 이러한 사물인터넷 시스템에서는 네트워크를 통해서 단말 간에 다양한 정보를 주고받는다는 점에서, 정보 보안의 필요성이 아주 중요하다.

[0005] 보통, 정보 보안을 위한 방식으로는 전송측이 수신측으로 데이터를 전달할 때, 해당 데이터에 대해 미리 공유하고 있는 데이터 암호화 방식에 따라 암호화를 수행한 후 수신측으로 전달하면, 수신측이 암호화된 데이터를 복호화하는 방식이 일반적이다.

[0006] 관련하여, 사물인터넷 시스템과 같이, 다양한 단말들이 서로 네트워크로 연결되어 있는 환경에서도 미리 공유된 데이터 암호화 방식에 따라 데이터를 암호화하여 송수신하는 보안 환경을 구축함으로써, 보안성을 강화시킬 수 있다.

[0007] 하지만, 미리 공유된 암호화 방식에 따라 데이터를 암호화하여 송수신하는 환경에서는 해당 암호화 방식이 타인에게 노출될 경우, 보안에 문제가 발생할 수 있다는 점에서, 사물인터넷 시스템과 같이, 다양한 단말들이 서로 네트워크로 연결되어 있는 환경에서 단순히 하나의 암호화 방식에 따라 데이터 암호화를 수행하는 것은 보안상 여러가지 취약점을 가질 수 있다.

[0008] 따라서, 사물인터넷 시스템과 같이, 다양한 단말들이 서로 네트워크로 연결되어 있는 환경에서 단순히 하나의

암호화 방식에 따라 각 단말들 간에 데이터 교환이 수행되도록 하는 것이 아니라, 해당 네트워크에서 발생하는 보안 환경의 변화에 기초하여 각 단말들이 데이터 교환시에 사용하는 암호화 방식을 적응적으로 가변할 수 있도록 하는 보안 기술을 도입함으로써, 보안성을 강화시킬 수 있는 기법에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0009]

본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치 및 그 동작 방법은 특정 주기 간격으로, 소정의 암호화 방식 정보를 구성하고, 해당 암호화 방식 정보들 간의 보안 수준에 따라서, 가장 높은 보안 수준을 갖는 암호화 방식 정보를 네트워크로 연결되어 있는 복수의 단말들의 데이터 송수신에 사용될 암호화 방식 후보로 선택해 둔 후 상기 복수의 단말들 사이에서 데이터 송수신시에 데이터 암호화 실패와 같은 보안상 문제가 발생하는 경우, 상기 복수의 단말들이 현재 사용하고 있는 암호화 방식을 상기 암호화 방식 후보로 선택된 암호화 방식으로 변경해줌으로써, 네트워크의 보안을 강화시킬 수 있도록 한다.

과제의 해결 수단

[0010]

본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치는 데이터의 암호화와 연관된 복수의 스크램블링 방식들이 저장되어 있는 데이터베이스, 선정된 제1 주기 간격으로, 상기 복수의 스크램블링 방식들 중에서 적어도 하나의 스크램블링 방식을 랜덤하게 선택하고, 데이터에 대해 상기 적어도 하나의 스크램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성하는 암호화 구성부, 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 구성됨으로써, 상기 암호화 방식 정보가 선정된 개수만큼 생성되면, 상기 선정된 개수의 암호화 방식 정보들을 네트워크로 서로 연결되어 있는 복수의 단말들 중 랜덤하게 선택된 제1 단말로 전송하는 정보 전송부, 상기 제1 단말로부터 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 보안 수준 정보를 수신하는 보안 수준 수신부, 상기 보안 수준 정보를 참조하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제1 암호화 방식 정보를 상기 복수의 단말들 간의 데이터 송수신을 위한 암호화 방식 후보로 선택한 후 상기 암호화 방식 후보로 선택된 상기 제1 암호화 방식 정보를 메모리에 저장하는 후보 선택부 및 상기 복수의 단말들 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 보안 이벤트가 선정된 기간 이내에서 선정된 횟수 이상 발생하는 경우, 상기 복수의 단말들에 대해, 상기 제1 암호화 방식 정보를 전송함으로써, 상기 복수의 단말들이 상기 제1 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어하는 암호화 방식 업데이트부를 포함한다.

[0011]

또한, 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치의 동작 방법은 데이터의 암호화와 연관된 복수의 스크램블링 방식들이 저장되어 있는 데이터베이스를 유지하는 단계, 선정된 제1 주기 간격으로, 상기 복수의 스크램블링 방식들 중에서 적어도 하나의 스크램블링 방식을 랜덤하게 선택하고, 데이터에 대해 상기 적어도 하나의 스크램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성하는 단계, 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 구성됨으로써, 상기 암호화 방식 정보가 선정된 개수만큼 생성되면, 상기 선정된 개수의 암호화 방식 정보들을 네트워크로 서로 연결되어 있는 복수의 단말들 중 랜덤하게 선택된 제1 단말로 전송하는 단계, 상기 제1 단말로부터 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 보안 수준 정보를 수신하는 단계, 상기 보안 수준 정보를 참조하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제1 암호화 방식 정보를 상기 복수의 단말들 간의 데이터 송수신을 위한 암호화 방식 후보로 선택한 후 상기 암호화 방식 후보로 선택된 상기 제1 암호화 방식 정보를 메모리에 저장하는 단계 및 상기 복수의 단말들 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 보안 이벤트가 선정된 기간 이내에서 선정된 횟수 이상 발생하는 경우, 상기 복수의 단말들에 대해, 상기 제1 암호화 방식 정보를 전송함으로써, 상기 복수의 단말들이 상기 제1 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어하는 단계를 포함한다.

발명의 효과

[0012]

본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치 및 그 동작 방법은 특정 주기 간격으로, 소정의 암호화 방식 정보를 구성하고, 해당 암호화 방식 정보들 간의 보안 수준에 따라서, 가장 높은 보안 수준을 갖는 암호화 방식 정보를 네트워크로 연결되어 있는 복수의 단말들의 데이터 송수신에 사용될 암호화 방식 후보로 선택해 둔 후 상기 복수의 단말들 사이에서 데이터 송수신시에 데이터 암호화 실패와 같은 보안상 문제가

발생하는 경우, 상기 복수의 단말들이 현재 사용하고 있는 암호화 방식을 상기 암호화 방식 후보로 선택된 암호화 방식으로 변경해줌으로써, 네트워크의 보안을 강화시킬 수 있다.

도면의 간단한 설명

- [0013] 도 1은 본 발명의 일실시예에 따른 네트워크 시스템을 개략적으로 도시한 시스템 개념도이다.
- 도 2는 네트워크로 연결되어 있는 복수의 단말들이 데이터의 헤더(header) 구조를 기초로 보안 이벤트를 발생시키는 과정을 설명하기 위한 데이터 헤더 구조의 일례를 도시한 도면이다.
- 도 3은 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치의 구조를 도시한 도면이다.
- 도 4는 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0014] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.
- [0015] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.
- [0016] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0017] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0018] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.
- [0019] 도 1은 본 발명의 일실시예에 따른 네트워크 시스템을 개략적으로 도시한 시스템 개념도이다.
- [0020] 도 1을 참조하면, 상기 네트워크 시스템은 가변 암호화 기반의 네트워크 보안 장치(110) 및 복수의 단말들(121, 122, 123, 124, 125)로 구성될 수 있다.
- [0021] 이때, 복수의 단말들(121, 122, 123, 124, 125)은 네트워크로 서로 연결되어 데이터를 주고받을 수 있고, 가변 암호화 기반의 네트워크 보안 장치(110)는 복수의 단말들(121, 122, 123, 124, 125) 각각과 네트워크로 연결되어 복수의 단말들(121, 122, 123, 124, 125) 각각과 데이터를 주고받을 수 있다.
- [0022] 먼저, 가변 암호화 기반의 네트워크 보안 장치(110)에는 데이터의 암호화와 연관된 복수의 스�크램블링(scrambling) 방식들이 저장되어 있는 데이터베이스가 포함되어 있을 수 있다.
- [0023] 여기서, 스�크램블링 방식이란 평문 데이터의 암호화를 위해서 사용되는 데이터 변경 방식을 의미하는 것으로, 보통 치환(transposition), 대치(substitution), 산술(algebraic) 등의 방식이 존재한다.
- [0024] 예컨대, 평문 데이터 '1010'에 대해서 두 번째 비트와 세 번째 비트를 치환하는 방식으로 데이터 스�크램블링을 수행한다고 하면, 해당 평문 데이터는 '1101'이라는 암호화 데이터로 변경될 수 있다.
- [0025] 이와 관련하여, 상기 데이터베이스에는 하기의 표 1과 같은 형태로 상기 복수의 스�크램블링 방식들이 저장되어 있을 수 있다.

표 1

순번	스크램블링 방식
1	치환
2	대치
3	산술
...	...

이러한 상황 하에서, 가변 암호화 기반의 네트워크 보안 장치(110)는 선정된(predetermined) 제1 주기 간격으로, 상기 복수의 스크램블링 방식들 중에서 적어도 하나의 스크램블링 방식을 랜덤하게 선택하고, 데이터에 대해 상기 적어도 하나의 스크램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성할 수 있다.

예컨대, 상기 선정된 제1 주기를 '24시간'이라고 가정하면, 가변 암호화 기반의 네트워크 보안 장치(110)는 '24시간' 간격으로, 상기 표 1과 같은 데이터베이스 상에 저장되어 있는 복수의 스크램블링 방식들 중에서 적어도 하나의 스크램블링 방식을 랜덤하게 선택하고, 소정의 데이터에 대해 상기 적어도 하나의 스크램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성할 수 있다.

관련하여, 가변 암호화 기반의 네트워크 보안 장치(110)는 첫 번째 주기에서 '치환', '대치'를 선택한 후 소정의 데이터에 대해 '치환', '대치'가 순차적으로 적용되도록 하는 암호화와 연관된 '암호화 방식 정보 1'을 구성할 수 있고, 두 번째 주기에서 '대치', '산술', '치환'을 선택한 후 소정의 데이터에 대해 '대치', '산술', '치환'이 순차적으로 적용되도록 하는 암호화와 연관된 '암호화 방식 정보 2'를 구성할 수 있으며, 이러한 방식으로, '24시간'마다, 상기 복수의 스크램블링 방식들 중에서 적어도 하나의 스크램블링 방식을 랜덤하게 선택하고, 소정의 데이터에 대해 상기 적어도 하나의 스크램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성할 수 있다.

이렇게, 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 구성됨으로써, 상기 암호화 방식 정보가 선정된 개수만큼 생성되면, 가변 암호화 기반의 네트워크 보안 장치(110)는 상기 선정된 개수의 암호화 방식 정보들을 네트워크로 서로 연결되어 있는 복수의 단말들(121, 122, 123, 124, 125) 중 랜덤하게 선택된 제1 단말로 전송할 수 있다.

예컨대, 상기 선정된 개수가 '2개'라고 가정하고, 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 구성됨으로써, 소정의 데이터에 대해 '치환', '대치'가 순차적으로 적용되도록 하는 암호화와 연관된 '암호화 방식 정보 1'과 소정의 데이터에 대해 '대치', '산술', '치환'이 순차적으로 적용되도록 하는 암호화와 연관된 '암호화 방식 정보 2'가 생성되면, 2개의 암호화 방식 정보가 구성되었기 때문에 가변 암호화 기반의 네트워크 보안 장치(110)는 복수의 단말들(121, 122, 123, 124, 125) 중 랜덤하게 선택된 제1 단말로 상기 '암호화 방식 정보 1'과 상기 '암호화 방식 정보 2'를 전송할 수 있다.

이하에서는 상기 제1 단말을 복수의 단말들 중(121, 122, 123, 124, 125)에서 도면부호 122에 해당되는 단말임을 가정하여 설명하기로 한다.

가변 암호화 기반의 네트워크 보안 장치(110)로부터 제1 단말(122)로 상기 선정된 개수의 암호화 방식 정보들이 전송되면, 제1 단말(122)은 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 차분 공격 분석(Differential Cryptanalysis)을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율(Propagation Ratio)을 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율이 낮을수록 높은 보안 수준이 할당되도록 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 정보를 구성할 수 있다.

여기서, 차분 공격 분석은 암호의 안전성을 평가하는 분석 방법으로, 연속된 라운드의 최대 차분 특성 확률(Differential Characteristic Probability)을 고려하고, 마지막 라운드의 키를 추측하여 키의 전수 조사량 보다 적은 계산량으로 키를 복구하는 분석 방법이다. 차분 공격 분석에서는 특정 암호화 방식에 대한 안정성을 표현하기 위한 결과 값으로 전파 비율을 연산할 수 있고, 해당 전파 비율이 낮을수록 안정된 암호화 방식으로 판단할 수 있다.

- [0035] 따라서, 제1 단말(122)은 가변 암호화 기반의 네트워크 보안 장치(110)로부터 상기 선정된 개수의 암호화 방식 정보들이 수신되면, 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 차분 공격 분석을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율을 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율이 낮을수록 높은 보안 수준이 할당되도록 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 정보를 구성할 수 있다.
- [0036] 예컨대, 제1 단말(122)로 '암호화 방식 정보 1'과 '암호화 방식 정보 2'가 수신되었다면, 제1 단말(122)은 '암호화 방식 정보 1'과 '암호화 방식 정보 2'에 따라 데이터를 암호화했을 경우에 대한 차분 공격 분석을 수행한 후 '암호화 방식 정보 1'에 대한 '전파 비율 1'을 연산하고, '암호화 방식 정보 2'에 대한 '전파 비율 2'를 연산할 수 있다.
- [0037] 이때, '전파 비율 1'과 '전파 비율 2' 중에서 '전파 비율 2'가 '전파 비율 1'보다 작은 값을 갖는다면, 제1 단말(122)은 '암호화 방식 정보 2'의 보안 수준을 높은 보안 수준으로 할당하고, '암호화 방식 정보 1'의 보안 수준을 낮은 보안 수준으로 할당하는 형태로 '암호화 방식 정보 1'과 '암호화 방식 정보 2'에 대한 보안 수준 정보를 구성할 수 있다.
- [0038] 이때, 본 발명의 다른 실시예에 따르면, 제1 단말(122)은 가변 암호화 기반의 네트워크 보안 장치(110)로부터 상기 선정된 개수의 암호화 방식 정보들이 수신되면, 상기 차분 공격 분석을 수행하는 것이 아니라, 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 선형 공격 분석(Linear Cryptanalysis)을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스(bias)를 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스가 낮을수록 높은 보안 수준이 할당되도록 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 정보를 구성할 수도 있다.
- [0039] 여기서, 선형 공격 분석은 암호의 안전성을 평가하는 분석 방법으로, 연속된 라운드의 최대 선형 특성 확률(Linear Characteristic Probability)을 고려하여 키의 정보를 복구하는 분석 방법이다. 선형 공격 분석에서는 특정 암호화 방식에 대한 안정성을 표현하기 위한 결과 값으로 바이어스를 연산할 수 있고, 해당 바이어스가 낮을수록 안정된 암호화 방식으로 판단할 수 있다.
- [0040] 따라서, 제1 단말(122)은 가변 암호화 기반의 네트워크 보안 장치(110)로부터 상기 선정된 개수의 암호화 방식 정보들이 수신되면, 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 선형 공격 분석을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스를 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스가 낮을수록 높은 보안 수준이 할당되도록 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 정보를 구성할 수 있다.
- [0041] 이렇게, 제1 단말(122)이 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 정보를 구성을 완료하면, 가변 암호화 기반의 네트워크 보안 장치(110)는 제1 단말(122)로부터 상기 보안 수준 정보를 수신할 수 있다.
- [0042] 그리고 나서, 가변 암호화 기반의 네트워크 보안 장치(110)는 상기 보안 수준 정보를 참조하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제1 암호화 방식 정보를 복수의 단말들(121, 122, 123, 124, 125) 간의 데이터 송수신을 위한 암호화 방식 후보로 선택한 후 상기 암호화 방식 후보로 선택된 상기 제1 암호화 방식 정보를 메모리에 저장할 수 있다.
- [0043] 그 이후, 가변 암호화 기반의 네트워크 보안 장치(110)는 복수의 단말들(121, 122, 123, 124, 125) 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 보안 이벤트가 선정된 기간 이내에서 선정된 횟수 이상 발생하는지 여부를 판단할 수 있다.
- [0044] 관련하여, 복수의 단말들(121, 122, 123, 124)은 어느 하나의 단말로부터 암호화된 데이터가 수신되면, 상기 암호화된 데이터를 복호화한 후 복호화된 데이터를 파싱하여 상기 복호화된 데이터에 포함되어 있는 데이터 헤더(header) 구조를 파악하고, 상기 데이터 헤더 구조와 메모리 상에 기 저장되어 있는 상기 복호화된 데이터의 데이터 교환을 위한 통신 프로토콜 표준 따른 헤더 구조 정보를 비교하여 상기 데이터 헤더 구조가 상기 헤더 구조 정보에 매칭되지 않는 것으로 판단되면, 상기 보안 이벤트를 발생시킬 수 있다.
- [0045] 예컨대, 복수의 단말들(121, 122, 123, 124, 125) 중 단말 1(121)이 단말 2(122)에 대해 IP 기반 데이터를 암호화해서 전송한 경우, 단말 2(122)는 상기 암호화된 데이터를 복호화한 후 복호화된 데이터를 파싱해서 상기 복호화된 데이터에 포함되어 있는 데이터 헤더 구조를 파악할 수 있다.

- [0046] 이때, 데이터는 스램블링되어 암호화되더라도, 해당 데이터의 헤더 구조에 포함되어 있는 각 데이터의 타입이나 비트 수 등은 변경되지 않기 때문에, 단말 2(122)는 상기 복호화된 데이터에 포함되어 있는 데이터 헤더 구조와 도 2에 도시되어 있는 예와 같은 IP 기반 데이터에 대한 통신 프로토콜 표준에 따른 헤더 구조 정보를 비교하여 상기 데이터 헤더 구조가 상기 헤더 구조 정보에 매칭되지 않는 것으로 판단되면, 상기 보안 이벤트를 발생시킬 수 있다.
- [0047] 즉, 상기 복호화된 데이터에 포함되어 있는 데이터 헤더 구조에서는 도 2에 도시되어 있는 예와 같이, IP 버전 4의 경우, 처음 4비트는 이진수로 '0100' 그 다음 4비트는 헤더길이에 따라 5에서 15까지의 값을 갖는 등 위치별로 표준에 규정된 값을 가질 뿐만 아니라, 헤더에 포함된 정보의 체크섬을 계산했을 때 'Header Checksum'에 저장된 값과 일치해야 하지만, 이러한 구조 정보가 도 2에 도시되어 있는 통신 프로토콜 표준에 따른 헤더 구조 정보에 매칭되지 않는다면, 단말 1(121)이 전송한 데이터는 정상적으로 암호화되지 않은 데이터라고 볼 수 있으므로, 단말 2(122)는 데이터 암호화 실패와 연관된 상기 보안 이벤트를 발생시킬 수 있다.
- [0048] 이러한 방식으로, 복수의 단말들(121, 122, 123, 124, 125)은 서로 데이터 교환시에 수신된 데이터의 헤더 구조를 기초로 데이터 암호화가 정상적으로 수행되었는지 여부를 판단한 후 데이터 암호화가 정상적으로 수행되지 않은 것으로 판단되면, 상기 보안 이벤트를 발생시킬 수 있다.
- [0049] 이렇게, 복수의 단말들(121, 122, 123, 124, 125)이 상기 보안 이벤트를 발생시키면, 가변 암호화 기반의 네트워크 보안 장치(110)는 복수의 단말들(121, 122, 123, 124, 125) 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 보안 이벤트가 선정된 기간 이내에 선정된 횟수 이상 발생하는지 여부를 판단할 수 있다.
- [0050] 만약, 복수의 단말들(121, 122, 123, 124, 125) 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 보안 이벤트가 선정된 기간 이내에 선정된 횟수 이상 발생하는 것으로 판단되면, 가변 암호화 기반의 네트워크 보안 장치(110)는 복수의 단말들(121, 122, 123, 124, 125)들에 대해, 상기 제1 암호화 방식 정보를 전송함으로써, 복수의 단말들(121, 122, 123, 124, 125)이 상기 제1 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어할 수 있다.
- [0051] 예컨대, 가변 암호화 기반의 네트워크 보안 장치(110)에서 소정의 데이터에 대해 '대치', '산술', '치환'이 순차적으로 적용되도록 하는 암호화와 연관된 '암호화 방식 정보 2'가 상기 제1 암호화 방식 정보로 결정되어 메모리에 저장되어 있는 상태에서 복수의 단말들(121, 122, 123, 124, 125)이 '치환', '산술'이라는 스램블링 방식이 순차적으로 적용되는 암호화 방식에 따라 데이터를 송수신하는 도중 상기 선정된 기간 이내에 데이터 암호화 실패와 연관된 보안 이벤트를 상기 선정된 횟수 이상 발생시키는 경우, 가변 암호화 기반의 네트워크 보안 장치(110)는 상기 '암호화 방식 정보 2'를 복수의 단말들(121, 122, 123, 124, 125)로 전송함으로써, 복수의 단말들(121, 122, 123, 124, 125)이 '치환', '산술'이라는 스램블링 방식이 순차적으로 적용되는 암호화 방식이 아닌, 상기 '암호화 방식 정보 2'에 따른 '대치', '산술', '치환'이 순차적으로 적용되는 암호화 방식을 기초로 데이터를 암호화하여 송수신하도록 제어할 수 있다.
- [0052] 이를 통해, 복수의 단말들(121, 122, 123, 124, 125)은 기존의 '치환', '산술'이라는 스램블링 방식이 순차적으로 적용되는 암호화 방식을 통해서 데이터를 송수신하는 것이 아니라, '대치', '산술', '치환'이 순차적으로 적용되는 암호화 방식을 통해서 데이터를 송수신할 수 있다.
- [0053] 이때, 본 발명의 일실시예에 따르면, 가변 암호화 기반의 네트워크 보안 장치(110)는 상기 제1 암호화 방식 정보가 상기 암호화 방식 후보로 선택된 이후에도 상기 선정된 제1 주기 간격으로, 상기 복수의 스램블링 방식들 중에서 적어도 하나의 스램블링 방식을 랜덤하게 선택하고, 소정의 데이터에 대해 상기 적어도 하나의 스램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성하는 과정을 계속 수행할 수 있다.
- [0054] 이를 통해, 가변 암호화 기반의 네트워크 보안 장치(110)는 상기 제1 암호화 방식 정보가 상기 암호화 방식 후보로 선택된 이후 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 신규로 구성됨으로써, 상기 신규로 구성된 암호화 방식 정보가 상기 제1 암호화 방식 정보를 포함하여 상기 선정된 개수만큼 생성되면, 상기 제1 암호화 방식 정보를 포함하는 상기 선정된 개수의 신규 암호화 방식 정보들을 복수의 단말들(121, 122, 123, 124, 125) 중 랜덤하게 재선택된 제2 단말로 전송할 수 있다.
- [0055] 그리고, 가변 암호화 기반의 네트워크 보안 장치(110)는 상기 제2 단말로부터 상기 선정된 개수의 신규 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 신규 보안 수준 정보를 수신할 수 있고, 상기

신규 보안 수준 정보를 참조하여 상기 선정된 개수의 신규 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제2 암호화 방식 정보를 복수의 단말들(121, 122, 123, 124, 125) 간의 데이터 송수신을 위한 암호화 방식 후보로 재선택한 후 상기 암호화 방식 후보로 재선택된 상기 제2 암호화 방식 정보를 메모리에 저장할 수 있다.

[0056] 이때, 복수의 단말들(121, 122, 123, 124, 125) 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 상기 보안 이벤트가 상기 선정된 기간 이내에 상기 선정된 횟수 이상 발생하는 경우, 가변 암호화 기반의 네트워크 보안 장치(110)는 복수의 단말들(121, 122, 123, 124, 125)에 대해, 상기 제2 암호화 방식 정보를 전송함으로써, 복수의 단말들(121, 122, 123, 124, 125)이 상기 제2 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어할 수 있다.

[0057] 즉, 가변 암호화 기반의 네트워크 보안 장치(110)는 상기 선정된 제1 주기 간격으로, 암호화 방식 정보를 계속 구성되되, 상기 암호화 방식 정보가 상기 선정된 개수만큼 생성되면, 상기 선정된 개수의 암호화 방식 정보들에 대한 보안 수준 정보를 비교하여 특정 암호화 방식 정보를 복수의 단말들(121, 122, 123, 124, 125) 간의 데이터 송수신을 위한 암호화 방식 후보로 선택하는 과정을 수행하고, 상기 암호화 방식 정보가 상기 선정된 제1 주기 간격으로 계속 구성됨으로써, 새로운 암호화 방식 정보가 생성되면, 기존의 암호화 방식 후보로 선택된 암호화 방식 정보와 새로운 암호화 방식 정보의 총 합계가 상기 선정된 개수에 해당되면, 다시 해당 암호화 방식 정보들에 대한 보안 수준 정보를 비교하여 특정 암호화 방식 정보를 복수의 단말들(121, 122, 123, 124, 125) 간의 데이터 송수신을 위한 암호화 방식 후보로 재선택하는 과정을 반복 수행할 수 있다.

[0058] 이를 통해서, 가변 암호화 기반의 네트워크 보안 장치(110)는 복수의 단말들(121, 122, 123, 124, 125) 간의 데이터 송수신을 위한 암호화 방식 후보를 특정 주기 간격으로 계속 갱신할 수 있다.

[0059] 이렇게, 가변 암호화 기반의 네트워크 보안 장치(110)는 복수의 단말들(121, 122, 123, 124, 125) 간의 데이터 송수신을 위한 암호화 방식 후보를 특정 주기 간격으로 계속 갱신해 놓으면서, 복수의 단말들(121, 122, 123, 124, 125) 사이에서 데이터 암호화 실패와 연관된 보안 이벤트가 특정 시간 이내에 특정 횟수 이상 발생한 것으로 판단되면, 복수의 단말들(121, 122, 123, 124, 125)이 현재 데이터 송수신에 사용하고 있는 암호화 방식에 문제가 있는 것으로 판단하고, 특정 주기 간격으로 갱신해서 메모리 상에 저장하고 있는 암호화 방식 후보를 복수의 단말들(121, 122, 123, 124, 125)로 전달함으로써, 복수의 단말들(121, 122, 123, 124, 125)이 새로운 암호화 방식에 따라 데이터를 송수신하도록 제어하여 보안을 강화시킬 수 있다.

[0060] 이때, 본 발명의 일실시예에 따르면, 가변 암호화 기반의 네트워크 보안 장치(110)는 선정된 제2 주기 간격으로, 상기 데이터베이스에 저장되어 있는 상기 복수의 스�크램블링 방식들 중에서 랜덤하게 선택된 적어도 하나의 제1 스�크램블링 방식을 삭제하고, 적어도 하나의 신규 스�크램블링 방식을 생성하여 상기 데이터베이스에 저장할 수 있다.

[0061] 이를 통해, 가변 암호화 기반의 네트워크 보안 장치(110)는 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보를 구성하는 것과는 별도로, 상기 선정된 제2 주기 간격으로 상기 데이터베이스 자체를 갱신함으로써, 상기 선정된 제1 주기 간격으로 생성되는 상기 암호화 방식 정보의 생성 시나리오를 다양화할 수 있어, 더욱 보안성을 강화시킬 수 있다.

[0062] 도 3은 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치의 구조를 도시한 도면이다.

[0063] 데이터베이스(311)에는 데이터의 암호화와 연관된 복수의 스�크램블링 방식들이 저장되어 있다.

[0064] 암호화 구성부(312)는 선정된 제1 주기 간격으로, 상기 복수의 스�크램블링 방식들 중에서 적어도 하나의 스�크램블링 방식을 랜덤하게 선택하고, 데이터에 대해 상기 적어도 하나의 스�크램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성한다.

[0065] 정보 전송부(313)는 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 구성됨으로써, 상기 암호화 방식 정보가 선정된 개수만큼 생성되면, 상기 선정된 개수의 암호화 방식 정보들을 네트워크로 서로 연결되어 있는 복수의 단말들(321, 322, 323) 중 랜덤하게 선택된 제1 단말로 전송한다.

[0066] 보안 수준 수신부(314)는 상기 제1 단말로부터 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 보안 수준 정보를 수신한다.

[0067] 이때, 본 발명의 일실시예에 따르면, 상기 제1 단말은 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 차분 공격 분석을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에

대한 전과 비율을 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전과 비율이 낮을수록 높은 보안 수준이 할당되도록 상기 보안 수준 정보를 구성할 수 있다.

[0068] 또한, 본 발명의 다른 일실시예에 따르면, 상기 제1 단말은 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 선형 공격 분석을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스를 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스가 낮을수록 높은 보안 수준이 할당되도록 상기 보안 수준 정보를 구성할 수 있다.

[0069] 후보 선택부(315)는 상기 보안 수준 정보를 참조하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제1 암호화 방식 정보를 복수의 단말들(321, 322, 323) 간의 데이터 송수신을 위한 암호화 방식 후보로 선택한 후 상기 암호화 방식 후보로 선택된 상기 제1 암호화 방식 정보를 메모리에 저장한다.

[0070] 암호화 방식 업데이트부(316)는 복수의 단말들(321, 322, 323) 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 보안 이벤트가 선정된 기간 이내에서 선정된 횟수 이상 발생하는 경우, 복수의 단말들(321, 322, 323)에 대해, 상기 제1 암호화 방식 정보를 전송함으로써, 복수의 단말들(321, 322, 323)이 상기 제1 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어한다.

[0071] 이때, 본 발명의 일실시예에 따르면, 복수의 단말들(321, 322, 323)은 어느 하나의 단말로부터 암호화된 데이터가 수신되면, 상기 암호화된 데이터를 복호화한 후 복호화된 데이터를 파싱하여 상기 복호화된 데이터에 포함되어 있는 데이터 헤더 구조를 파악하고, 상기 데이터 헤더 구조와 메모리 상에 기 저장되어 있는 상기 복호화된 데이터의 데이터 교환을 위한 통신 프로토콜 표준 따른 헤더 구조 정보를 비교하여 상기 데이터 헤더 구조가 상기 헤더 구조 정보에 매칭되지 않는 것으로 판단되면, 상기 보안 이벤트를 발생시킬 수 있다.

[0072] 본 발명의 일실시예에 따르면, 정보 전송부(313)는 상기 제1 암호화 방식 정보가 상기 암호화 방식 후보로 선택된 이후 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 신규로 구성됨으로써, 상기 신규로 구성된 암호화 방식 정보가 상기 제1 암호화 방식 정보를 포함하여 상기 선정된 개수만큼 생성되면, 상기 제1 암호화 방식 정보를 포함하는 상기 선정된 개수의 신규 암호화 방식 정보들을 복수의 단말들(321, 322, 323) 중 랜덤하게 재선택된 제2 단말로 전송할 수 있다.

[0073] 이때, 보안 수준 수신부(314)는 상기 제2 단말로부터 상기 선정된 개수의 신규 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 신규 보안 수준 정보를 수신할 수 있고, 후보 선택부(315)는 상기 신규 보안 수준 정보를 참조하여 상기 선정된 개수의 신규 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제2 암호화 방식 정보를 복수의 단말들(321, 322, 323) 간의 데이터 송수신을 위한 암호화 방식 후보로 재선택한 후 상기 암호화 방식 후보로 재선택된 상기 제2 암호화 방식 정보를 메모리에 저장할 수 있다.

[0074] 그리고, 암호화 방식 업데이트부(316)는 복수의 단말들(321, 322, 323) 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 상기 보안 이벤트가 상기 선정된 기간 이내에서 상기 선정된 횟수 이상 발생하는 경우, 복수의 단말들(321, 322, 323)에 대해, 상기 제2 암호화 방식 정보를 전송함으로써, 복수의 단말들(321, 322, 323)이 상기 제2 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어할 수 있다.

[0075] 본 발명의 일실시예에 따르면, 가변 암호화 기반의 네트워크 보안 장치(310)는 선정된 제2 주기 간격으로, 데이터베이스(311)에 저장되어 있는 상기 복수의 스크램블링 방식들 중에서 랜덤하게 선택된 적어도 하나의 제1 스크램블링 방식을 삭제하고, 적어도 하나의 신규 스크램블링 방식을 생성하여 데이터베이스(311)에 저장하는 데이터베이스 갱신부(317)를 더 포함할 수 있다.

[0076] 이상, 도 3을 참조하여 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치(310)의 구조에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치(310)는 도 1과 도 2를 이용하여 설명한 가변 암호화 기반의 네트워크 보안 장치(110)와 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0077] 도 4는 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치의 동작 방법을 도시한 순서도이다.

[0078] 단계(S410)에서는 데이터의 암호화와 연관된 복수의 스크램블링 방식들이 저장되어 있는 데이터베이스를 유지한다.

- [0079] 단계(S420)에서는 선정된 제1 주기 간격으로, 상기 복수의 스크램블링 방식들 중에서 적어도 하나의 스크램블링 방식을 랜덤하게 선택하고, 데이터에 대해 상기 적어도 하나의 스크램블링 방식이 순차적으로 적용되도록 하는 암호화와 연관된 암호화 방식 정보를 구성한다.
- [0080] 단계(S430)에서는 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 구성됨으로써, 상기 암호화 방식 정보가 선정된 개수만큼 생성되면, 상기 선정된 개수의 암호화 방식 정보들을 네트워크로 서로 연결되어 있는 복수의 단말들 중 랜덤하게 선택된 제1 단말로 전송한다.
- [0081] 단계(S440)에서는 상기 제1 단말로부터 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 보안 수준 정보를 수신한다.
- [0082] 이때, 본 발명의 일실시예에 따르면, 상기 제1 단말은 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 차분 공격 분석을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율을 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 전파 비율이 낮을수록 높은 보안 수준이 할당되도록 상기 보안 수준 정보를 구성할 수 있다.
- [0083] 또한, 본 발명의 다른 일실시예에 따르면, 상기 제1 단말은 상기 선정된 개수의 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 선형 공격 분석을 수행하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스를 연산한 후 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 바이어스가 낮을수록 높은 보안 수준이 할당되도록 상기 보안 수준 정보를 구성할 수 있다.
- [0084] 단계(S450)에서는 상기 보안 수준 정보를 참조하여 상기 선정된 개수의 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제1 암호화 방식 정보를 상기 복수의 단말들 간의 데이터 송수신을 위한 암호화 방식 후보로 선택한 후 상기 암호화 방식 후보로 선택된 상기 제1 암호화 방식 정보를 메모리에 저장한다.
- [0085] 단계(S460)에서는 상기 복수의 단말들 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 보안 이벤트가 선정된 기간 이내에서 선정된 횟수 이상 발생하는 경우, 상기 복수의 단말들에 대해, 상기 제1 암호화 방식 정보를 전송함으로써, 상기 복수의 단말들이 상기 제1 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어한다.
- [0086] 이때, 본 발명의 일실시예에 따르면, 상기 복수의 단말들은 어느 하나의 단말로부터 암호화된 데이터가 수신되면, 상기 암호화된 데이터를 복호화한 후 복호화된 데이터를 파싱하여 상기 복호화된 데이터에 포함되어 있는 데이터 헤더 구조를 파악하고, 상기 데이터 헤더 구조와 메모리 상에 기 저장되어 있는 상기 복호화된 데이터의 데이터 교환을 위한 통신 프로토콜 표준 따른 헤더 구조 정보를 비교하여 상기 데이터 헤더 구조가 상기 헤더 구조 정보에 매칭되지 않는 것으로 판단되면, 상기 보안 이벤트를 발생시킬 수 있다.
- [0087] 본 발명의 일실시예에 따르면, 상기 가변 암호화 기반의 네트워크 보안 장치의 동작 방법은 상기 제1 암호화 방식 정보가 상기 암호화 방식 후보로 선택된 이후 상기 선정된 제1 주기 간격으로 상기 암호화 방식 정보가 신규로 구성됨으로써, 상기 신규로 구성된 암호화 방식 정보가 상기 제1 암호화 방식 정보를 포함하여 상기 선정된 개수만큼 생성되면, 상기 제1 암호화 방식 정보를 포함하는 상기 선정된 개수의 신규 암호화 방식 정보들을 상기 복수의 단말들 중 랜덤하게 재선택된 제2 단말로 전송하는 단계, 상기 제2 단말로부터 상기 선정된 개수의 신규 암호화 방식 정보들 각각을 기초로 데이터를 암호화하였을 경우에 대한 신규 보안 수준 정보를 수신하는 단계, 상기 신규 보안 수준 정보를 참조하여 상기 선정된 개수의 신규 암호화 방식 정보들 각각에 대한 보안 수준 중에서 가장 높은 보안 수준을 갖는 제2 암호화 방식 정보를 상기 복수의 단말들 간의 데이터 송수신을 위한 암호화 방식 후보로 재선택한 후 상기 암호화 방식 후보로 재선택된 상기 제2 암호화 방식 정보를 메모리에 저장하는 단계 및 상기 복수의 단말들 사이에서 데이터 송수신이 수행되는 도중, 데이터 암호화 실패와 연관된 상기 보안 이벤트가 상기 선정된 기간 이내에서 상기 선정된 횟수 이상 발생하는 경우, 상기 복수의 단말들에 대해, 상기 제2 암호화 방식 정보를 전송함으로써, 상기 복수의 단말들이 상기 제2 암호화 방식 정보를 기초로 데이터를 암호화하여 송수신하도록 제어하는 단계를 더 포함할 수 있다.
- [0088] 또한, 본 발명의 일실시예에 따르면, 상기 가변 암호화 기반의 네트워크 보안 장치의 동작 방법은 선정된 제2 주기 간격으로, 상기 데이터베이스에 저장되어 있는 상기 복수의 스크램블링 방식들 중에서 랜덤하게 선택된 적어도 하나의 제1 스크램블링 방식을 삭제하고, 적어도 하나의 신규 스크램블링 방식을 생성하여 상기 데이터베이스에 저장하는 단계를 더 포함할 수 있다.

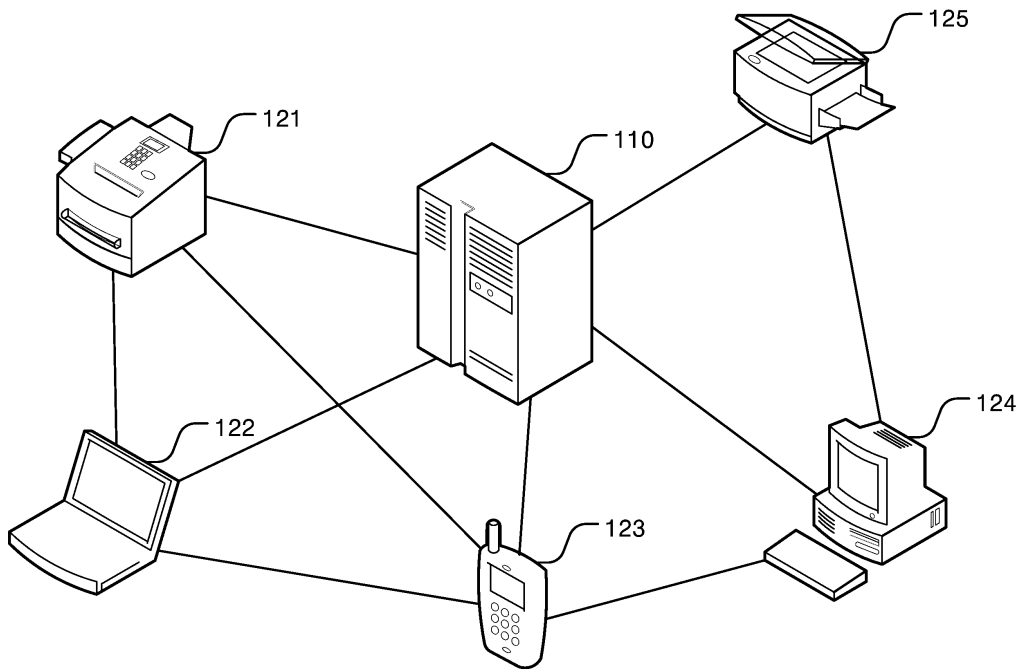
- [0089] 이상, 도 4를 참조하여 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치의 동작 방법은 도 1 내지 도 3을 이용하여 설명한 가변 암호화 기반의 네트워크 보안 장치(110, 310)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.
- [0090] 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.
- [0091] 또한, 본 발명의 일실시예에 따른 가변 암호화 기반의 네트워크 보안 장치의 동작 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0092] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.
- [0093] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

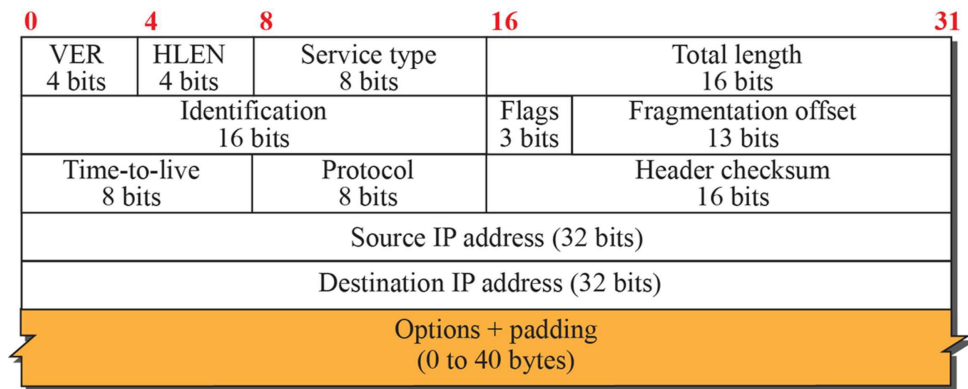
- [0094] 110: 가변 암호화 기반의 네트워크 보안 장치
- 121, 122, 123, 124, 125: 복수의 단말들
- 310: 가변 암호화 기반의 네트워크 보안 장치
- | | |
|-----------------|-------------------|
| 311: 데이터베이스 | 312: 암호화 구성부 |
| 313: 정보 전송부 | 314: 보안 수준 수신부 |
| 315: 후보 선택부 | 316: 암호화 방식 업데이트부 |
| 317: 데이터베이스 갱신부 | |
- 321, 322, 323: 복수의 단말들

도면

도면1

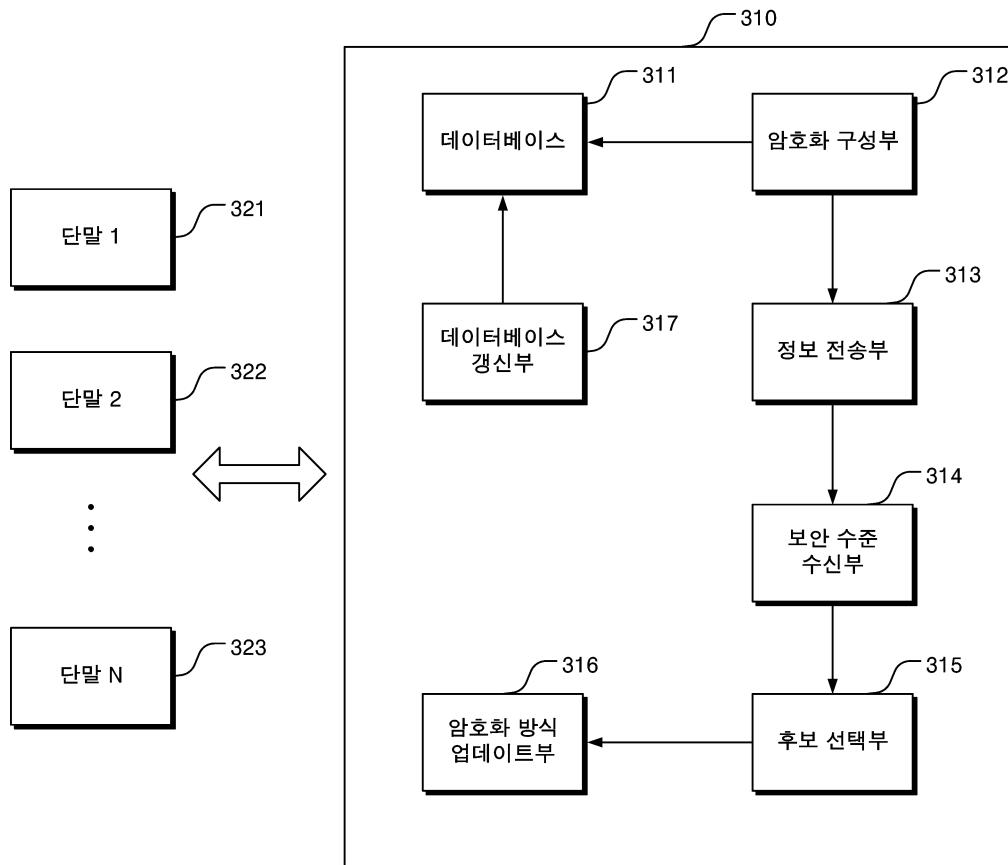


도면2



b. Header format

도면3



도면4

