

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014년 3월 27일 (27.03.2014)



(10) 국제공개번호
WO 2014/046442 A1

- (51) 국제특허분류:
H04L 1/16 (2006.01)
- (21) 국제출원번호: PCT/KR2013/008375
- (22) 국제출원일: 2013년 9월 16일 (16.09.2013)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2012-0104827 2012년 9월 20일 (20.09.2012) KR
- (71) 출원인: 한국전력공사 (KOREA ELECTRIC POWER CORPORATION) [KR/KR]; 135-791 서울시 강남구 영동대로 512, Seoul (KR).
- (72) 발명자: 백종목 (BAEK, Jong Mock); 305-760 대전시 유성구 문지동 한국전력연구원 스마트에너지연구소, Daejeon (KR). 최문석 (CHOI, Moon Suk); 305-760 대전시 유성구 문지동 한국전력연구원 스마트에너지연구소, Daejeon (KR). 김충호 (KIM, Chung Hyo); 305-760 대전시 유성구 문지동 한국전력연구원 스마트에너지연구소, Daejeon (KR). 장엽 (CHANG, Yeop); 305-315 대전시 유성구 원신동 어울림아파트 1207동 1204호, Daejeon (KR). 민병길 (MIN, Byung Gil); 361-710 충

청북도 청주시 흥덕구 분평동 분평 1단지 프란체아파트 102동 1403호, Chungcheongbuk-do (KR). 김우년 (KIM, Woo Nyon); 305-729 대전시 유성구 전민동 청구나래아파트 108동 705호, Daejeon (KR). 장문수 (JANG, Moon Su); 305-729 대전시 유성구 전민동 청구나래아파트 105동 301호, Daejeon (KR). 윤정한 (YUN, Jeong Han); 302-739 대전시 서구 만년동 상아아파트 108동 1303호, Daejeon (KR).

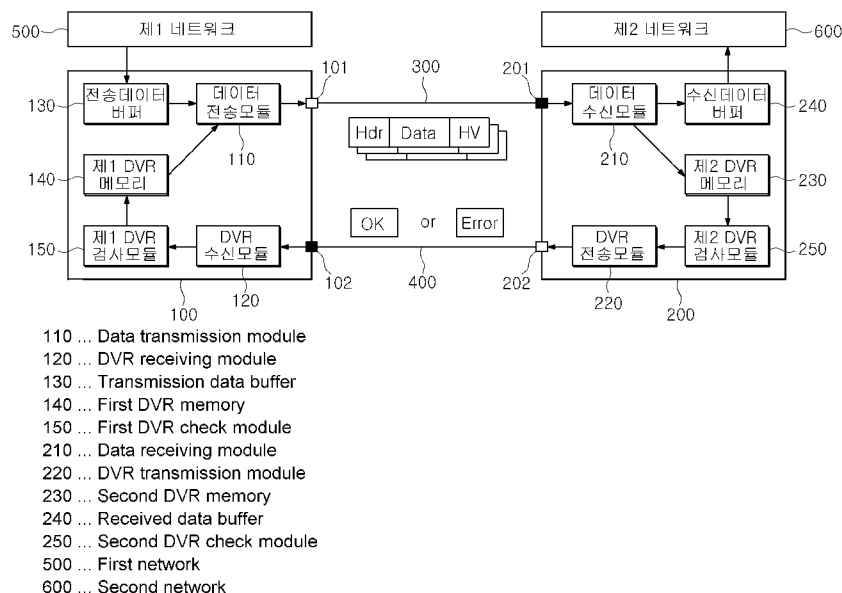
(74) 대리인: 특허법인 아주양현 (AJU KIM CHANG & LEE); 137-860 서울시 서초구 사임당로 174, 세인트하이얀 빌딩 12-13층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[다음 쪽 계속]

(54) Title: SYSTEM AND METHOD FOR UNIDIRECTIONAL DATA TRANSMISSION

(54) 발명의 명칭: 일방향 데이터 전송 시스템 및 그 방법



(57) Abstract: The present invention relates to a system and a method for unidirectional data transmission, in which data is unidirectionally transmitted from a network having a higher security level to a network having a lower security level, and a result of data validation is received through a separate line. Thus, access from a network having a lower security level to a network having a higher security level is physically blocked to ensure security and handle a packet loss or bit error that might occur during the delivery of a material, thus improving transmission reliability.

(57) 요약서:

[다음 쪽 계속]

WO 2014/046442 A1



(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

본 발명은 일방향 데이터 전송 시스템 및 그 방법에 관한 것으로서, 보안레벨이 높은 네트워크에서 보안레벨이 낮은 네트워크로 데이터를 일방향으로 전송하고 데이터 검증결과는 별도의 라인을 통해 수신함으로써 보안레벨이 낮은 네트워크에서 보안레벨이 높은 네트워크로의 접근을 물리적으로 차단하여 보안성을 보장하면서도 자료전달시 발생하는 패킷손실이나 비트에러에 대해 대처할 수 있어 전송 신뢰성을 높일 수 있다.

명세서

발명의 명칭: 일방향 데이터 전송 시스템 및 그 방법

기술분야

- [1] 본 발명은 일방향 데이터 전송 시스템 및 그 방법에 관한 것으로서, 보다 상세하게는 보안레벨이 높은 네트워크에서 보안레벨이 낮은 네트워크로 데이터를 일방향으로 전송하고 데이터 검증결과는 별도의 라인을 통해 수신함으로써 보안레벨이 낮은 네트워크에서 보안레벨이 높은 네트워크로의 접근을 물리적으로 차단하면서도 자료전달의 신뢰성을 높일 수 있도록 한 일방향 데이터 전송 시스템 및 그 방법에 관한 것이다.

[2]

배경기술

- [3] 국방, 제어, 금융과 같이 높은 보안성을 요구하는 시스템에 일방향 자료전달 기술을 활용할 경우 필요한 정보만 외부에 제공하면서 내부 시스템을 외부의 침입으로부터 안전하게 보호할 수 있다.
- [4] 하지만 완벽한 물리적 일방향 시스템을 적용한 경우 패킷 손실이 발생하거나, 비트 에러(bit error)가 발생한 경우 이에 대한 완전한 복구가 어려워 전송된 데이터에 대한 신뢰성 보장이 어렵다.
- [5] 하지만 신뢰성 보장을 위해 보안 레벨이 높은 제 1 네트워크 측에서 보안 레벨이 낮은 제 2 네트워크 측으로 데이터를 전송할 경우, 제 2 네트워크에서 제 1 네트워크로 데이터 수신에 대한 응답을 전송할 때 데이터 통신에 양방향성을 가지게 되므로 제 1 네트워크로의 침투 가능성이 발생하게 되기 때문에 역방향으로의 공격을 차단하면서 데이터 신뢰성을 보장할 수 있는 안전한 방법이 필요할 실정이다.
- [6] 따라서, 신뢰성을 향상시키기 위한 방법으로 자가 오류복구 알고리즘을 사용하는 방식이 존재하나 패킷 손실이나 복구가 불가능한 수준의 에러가 발생할 경우 데이터를 손실하게 되며, 제 2 네트워크에서 수신여부를 제 1 네트워크로 보내기 위해 제한된 정보로 구성된 수신신호를 별도의 신호 채널을 사용하여 보내는 방식이 존재하나 수신 신호에 포함된 정보가 부족하여, 제 2 네트워크에서 제 1 네트워크로 전달된 신호가 제 1 네트워크에서 전달된 데이터에 의한 응답 인지 확인할 수 없어 데이터 전송의 신뢰성을 보장하기 어려운 문제점이 있다.
- [7] 또한, 높은 보안이 필요한 제 1 네트워크에서 낮은 보안이 필요한 제 2 네트워크로 데이터를 전송하는 과정에 있어 의미를 갖는 데이터의 흐름이 일방향성만을 갖는 경우, 제 2 네트워크에서 제 1 네트워크로 물리적 데이터 일방향 자료전달 장치인 일방향 데이터 다이오드를 활용하여 제 2 네트워크와의 연계 접점을 통해서 들어오는 모든 위협으로부터 제 1 네트워크를 보호할 수

있다. 하지만 이러한 데이터 다이오드를 사용하여 일방향으로 데이터 전송시에 통신 매체의 특성상 낮은 확률이지만 데이터 전송 시 에러가 발생가능한 문제점이 있다.

- [8] 이러한 에러를 탐지하고 복구하기 위해 전진 에러 수정 기법(Forward Error Correction)을 이용하는 관련 선행기술로는 대한민국 공개특허 10-2000-0028706호(2000.05.25.) "단방향 데이터 경로 상에서 보안 접속을 확립하는 방법 및 장치"가 있다.

[9]

발명의 상세한 설명

기술적 과제

- [10] 그러나, 이러한 복구 방법에도 전진 에러 수정은 복구 능력 이상의 에러가 발생하거나 데이터 자체에 누락이 생긴 경우 복구가 어려운 문제점이 있으며, 별도의 수신 신호 채널을 통해 제한된 정보를 전송할 경우 제한된 정보(예: 수신 성공시 1 신호 전송, 수신 실패시 0 신호 전송)만을 전송하므로 제 2 네트워크에서 전달된 신호가, 정상적으로 제 1 네트워크에서 보낸 데이터에 대한 수신 신호인지, 이상으로 발생한 값인지에 대한 여부를 정확히 확인할 수 없어 데이터 전송 신뢰성에 한계를 갖는 문제점이 있다.
- [11] 본 발명은 상기와 같은 문제점을 개선하기 위해 창작된 것으로서, 보안레벨이 높은 네트워크에서 보안레벨이 낮은 네트워크로 데이터를 일방향으로 전송하고 데이터 검증결과는 별도의 라인을 통해 수신함으로써 보안레벨이 낮은 네트워크에서 보안레벨이 높은 네트워크로의 접근을 물리적으로 차단하면서도 자료전달의 신뢰성을 높일 수 있도록 한 일방향 데이터 전송 시스템 및 그 방법을 제공하는데 그 목적이 있다.

[12]

과제 해결 수단

- [13] 본 발명의 일 측면에 따른 일방향 데이터 전송 시스템은 보안레벨이 높은 제 1 네트워크에 연결되어 제 1 네트워크로부터 전송된 데이터를 보안레벨인 낮은 제 2 네트워크로 데이터 전송라인을 통해 전송하고 데이터에 대한 데이터 검증결과를 DVR(Data Verification Result) 전송라인을 통해 수신받는 송신장치; 및 보안레벨이 낮은 제 2 네트워크에 연결되어 데이터 전송라인을 통해 송신장치로부터 전송된 데이터를 제 2 네트워크로 전달하고 DVR 전송라인을 통해 데이터에 대한 데이터 검증결과를 전송하는 수신장치;를 포함하는 것을 특징으로 한다.
- [14] 본 발명에서 송신장치는 제 1 네트워크로부터 전송된 데이터를 저장하는 전송데이터 버퍼; 전송데이터 버퍼에 저장된 데이터를 데이터 전송포트를 통해 데이터 전송라인으로 전송하는 데이터 전송모듈; DVR 수신포트를 통해 DVR 전송라인으로 전송된 데이터 검증결과를 수신하는 DVR 수신모듈; DVR

수신모듈을 통해 수신한 데이터 검증결과의 규격을 검사하는 제 1 DVR
검사모듈; 및 제 1 DVR 검사모듈에서 검사결과에 따라 수신된 데이터
검증결과를 저장하는 제 1 DVR 메모리;를 포함하는 것을 특징으로 한다.

[15] 본 발명에서 데이터 전송모듈은 제 1 DVR 메모리에 저장된 데이터 검증결과의
상태에 따라 이전 데이터의 재전송 여부를 결정하여 이전 데이터를
재전송하거나 다음 데이터를 전송하는 것을 특징으로 한다.

[16] 본 발명에서 제 1 DVR 메모리는 제 1 DVR 검사모듈에 대해 쓰기 권한만
부여되고, 데이터 전송모듈에 대해 읽기 권한만 부여되는 것을 특징으로 한다.

[17] 본 발명에서 제 1 네트워크와 송신장치는 제 1 네트워크에서 송신장치로만
데이터를 전송할 수 있도록 연결되는 것을 특징으로 한다.

[18] 본 발명에서 수신장치는 데이터 수신포트를 통해 데이터 전송라인으로 전송된
데이터를 수신하는 데이터 수신모듈; 데이터 수신모듈을 통해 수신된 데이터를
저장하여 제 2 네트워크로 전송하는 수신데이터 버퍼; 데이터 수신모듈에서
수신된 데이터에 대한 데이터 검증결과를 저장하는 제 2 DVR 메모리; 제 2 DVR
메모리에 저장된 데이터 검증결과의 규격을 검사하는 제 2 DVR 검사모듈; 및 제
2 DVR 검사모듈의 결과에 따라 DVR 전송포트를 통해 DVR 전송라인으로
데이터 검증결과를 전송하는 DVR 전송모듈;을 포함하는 것을 특징으로 한다.

[19] 본 발명에서 제 2 DVR 메모리는 데이터 수신모듈에 대해 쓰기 권한만
부여되고, 제 2 DVR 검사모듈에 대해 읽기 권한만 부여되는 것을 특징으로 한다.

[20] 본 발명에서 제 2네트워크와 수신장치는 수신장치에서 제 2 네트워크로만
데이터를 전송할 수 있도록 연결되는 것을 특징으로 한다.

[21] 본 발명에서 데이터 전송라인을 통해 전송되는 데이터의 패킷은 데이터 패킷
그룹의 고유값을 나타내는 Group ID영역, 데이터 패킷 그룹에서 전송할 패킷을
나타내는 Packet Count영역, 데이터 패킷 그룹내의 전송 패킷의 순서를 나타내는
Seq영역, 데이터 패킷의 전송시 패킷을 구별하기 위한 UV(Unique Value)값을
나타내는 Unique Value영역, 데이터 패킷을 나타내는 Data영역 및 데이터 패킷의
해시값을 나타내는 HV영역을 포함하는 것을 특징으로 한다.

[22] 본 발명에서 DVR 전송라인을 통해 전송되는 데이터 검증결과의 패킷은
전송한 데이터 패킷 그룹의 고유값을 나타내는 Group ID영역, 데이터 패킷의
전송시 패킷을 구별하기 위한 UV값을 나타내는 Unique Value영역 및 데이터
패킷의 분석 결과를 나타내는 Signal영역을 포함하는 것을 특징으로 한다.

[23]

[24] 본 발명의 다른 측면에 다른 일방향 데이터 전송 방법은 송신장치에서
데이터의 전송요건이 만족 되는가 판단하는 단계; 데이터의 전송요건에 만족할
경우 데이터를 데이터 전송라인을 통해 전송하는 단계; 데이터를 전송한 후
일정시간 내에 DVR 전송라인을 통한 데이터 검증결과의 수신여부를 판단하는
단계; 데이터 검증결과의 상태에 따라 데이터의 재전송 여부를 판단하는 단계;
및 판단결과에 따라 패킷을 구별하기 위한 UV값을 변경하여 재전송하거나

데이터 검증결과를 저장하는 단계;를 포함하는 것을 특징으로 한다.

[25] 본 발명에서 데이터의 전송요건은 데이터 검증결과의 상태와 전송데이터 버퍼에 전송할 데이터가 존재할 경우인 것을 특징으로 한다.

[26] 본 발명에서 데이터의 재전송 여부를 판단하는 단계는 일정시간 내에 데이터 검증결과가 수신되는가를 판단하는 단계; 수신된 데이터 검증결과가 정의된 구조와 값을 갖는가 판단하는 단계; 수신된 데이터 검증결과가 성공인가 판단하는 단계; 및 전송된 데이터 패킷의 고유값과 UV값이 동일한가 판단하는 단계를 포함하는 것을 특징으로 한다.

[27]

[28] 본 발명의 또 다른 측면에 따른 일방향 데이터 전송 방법은 수신장치에서 데이터 전송라인을 통해 데이터를 수신하는 단계; 수신된 데이터 패킷의 정상 수신여부를 판단하는 단계; 정상 수신여부를 판단하여 데이터 검증결과를 저장하는 단계; 및 저장된 데이터 검증결과를 검사한 후 DVR 전송라인을 통해 전송하는 단계;를 포함하는 것을 특징으로 한다.

[29] 본 발명에서 데이터 패킷의 정상 수신여부를 판단하는 단계는 데이터 패킷이 지정시간 동안 모든 패킷이 수신되는가 판단하는 단계; 및 데이터 패킷의 해쉬값이 계산값과 동일한가 판단하는 단계;를 포함하는 것을 특징으로 한다.

[30]

발명의 효과

[31] 본 발명은 보안레벨이 높은 네트워크에서 보안레벨이 낮은 네트워크로 데이터를 일방향으로 전송하고 데이터 검증결과는 별도의 라인을 통해 수신함으로써 보안레벨이 낮은 네트워크에서 보안레벨이 높은 네트워크로의 접근을 물리적으로 차단하여 보안성을 보장하면서도 자료전달시 발생하는 패킷손실이나 비트에러에 대해 대처할 수 있어 전송 신뢰성을 높일 수 있다.

[32]

도면의 간단한 설명

[33] 도 1은 본 발명의 일 실시예에 따른 일방향 데이터 전송 시스템을 개념도이다.

[34] 도 2는 본 발명의 일 실시예에 따른 일방향 데이터 전송 시스템을 구체적으로 도시한 블록구성도이다.

[35] 도 3은 본 발명의 일 실시예에 따른 일방향 데이터 전송 시스템에서의 데이터 패킷의 구조를 나타낸 도면이다.

[36] 도 4는 본 발명의 일 실시예에 따른 일방향 데이터 전송 시스템에서의 데이터 검증결과의 구조를 나타낸 도면이다.

[37] 도 5는 본 발명의 일 실시예에 따른 일방향 데이터 전송방법에 의한 데이터 전송과정을 설명하기 위한 흐름도이다.

[38] 도 6은 본 발명의 일 실시예에 따른 일방향 데이터 전송방법에 의한 데이터 수신과정을 설명하기 위한 흐름도이다.

[39]

발명의 실시를 위한 형태

[40] 이하, 첨부된 도면을 참조하여 본 발명에 따른 일방향 데이터 전송 시스템 및 그 방법의 일 실시예를 설명한다. 이 과정에서 도면에 도시된 선들의 두께나 구성요소의 크기 등은 설명의 명료성과 편의상 과장되게 도시되어 있을 수 있다. 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례에 따라 달라질 수 있다. 그러므로, 이러한 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[41] 도 1은 본 발명의 일 실시예에 따른 일방향 데이터 전송 시스템을 개념도이다.

[42] 도 1에 도시된 바와 같이 송신장치(100)와 수신장치(200)는 두 개의 분리된 통신 연결을 갖고 있으며 각 통신 연결은 데이터 전송을 위한 데이터 전송라인(300)과 데이터 검증결과(DVR; Data Verification Result, 이하 'DVR'이라 한다)를 전송하기 위한 DVR 전송라인(400)으로 구성된다.

[43] 송신장치(100)는 데이터 전송포트(101)와 DVR 수신포트(102)를 갖고 있으며, 데이터 전송포트(101)를 통해서는 데이터의 전송만이 가능하며, DVR 수신포트(102)를 통해서는 DVR의 수신만이 가능하다.

[44] 수신장치(200)는 데이터 수신포트(201)와 DVR 전송포트(202)를 가지며 데이터 수신포트(201)를 통해서는 데이터의 수신만이 가능하며, DVR 전송포트(202)를 통해서는 DVR의 전송만이 가능하다.

[45] 이러한 전송포트, 수신포트는 광통신의 경우 전송포트에 광출력단자, 수신포트에 광전자셀을 이용하여 구현할 수 있으며, 시리얼 혹은 UTP의 수신선을 제거하는 방식 등으로 구현할 수 있다.

[46] 일방향 데이터 전송에서 신뢰성을 향상시키기 위해 송신장치(100)가 패킷들을 데이터 전송라인(300)을 통해 전송할 때마다 수신장치(200)는 전송된 데이터 패킷의 정상수신 여부에 따른 DVR을 DVR 전송라인(400)을 통해 송신장치(100)에 전달한다. 따라서 송신장치(100)와 수신장치(200) 간에 패킷 에러나 비트 에러가 발생한 경우 이를 확인하고 재전송이 가능하게 되어 일방향 자료전달의 신뢰성이 향상될 수 있다.

[47]

[48] 도 2는 본 발명의 일 실시예에 따른 일방향 데이터 전송 시스템을 구체적으로 도시한 블록구성도이다.

[49] 도 2에 도시된 바와 같이 송신장치(100)는 보안레벨이 높은 제 1 네트워크(500)에 연결되어 제 1 네트워크(500)로부터 전송된 데이터를 보안레벨인 낮은 제 2 네트워크(600)로 데이터 전송라인(300)을 통해 전송하고 데이터에 대한 검증결과인 DVR(Data Verification Result ; 데이터 검증결과)을 DVR 전송라인(400)을 통해 수신 받는다.

- [50] 이때 송신장치(100)는 전송데이터 버퍼(130), 데이터 전송모듈(110), DVR 수신모듈(120), 제 1 DVR 검사모듈(150) 및 제 1 DVR 메모리(140)를 포함한다.
- [51] 전송데이터 버퍼(130)는 제 1 네트워크(500)로부터 전송된 데이터를 저장한다.
- [52] 이때 전송데이터 버퍼(130)는 제 1 네트워크(500)로부터 전송된 데이터만 저장할 수 있을 뿐 전송데이터 버퍼(130)의 정보를 제 1 네트워크(500)에서는 읽을 수 없도록 인터페이스 된다.
- [53] 이와 같이 제 1 네트워크(500)에서 송신장치(100)로만 데이터를 전송할 수 있도록 하여 보안레벨이 높은 제 1 네트워크(500)로의 접속을 차단한다.
- [54] 데이터 전송모듈(110)은 전송데이터 버퍼(130)에 저장된 데이터가 쌓일 때마다 데이터 전송포트(101)를 통해 데이터 전송라인(300)으로 데이터 패킷을 전송한다.
- [55] 그리고, 데이터 전송모듈(110)은 제 1 DVR 메모리(140)에 저장된 DRV의 상태에 따라 이전 데이터의 전송결과가 OK값을 갖을 경우에는 다음 데이터를 전송하고, 에러값을 갖을 경우에는 이전 데이터를 재전송한다.
- [56] DVR 수신모듈(120)은 DVR 수신포트(102)를 통해 DVR 전송라인(400)으로 전송된 DVR을 수신한다.
- [57] 제 1 DVR 검사모듈(150)은 DVR 수신모듈(120)을 통해 수신한 DVR이 정해진 규격에 맞는지 검사한다.
- [58] 제 1 DVR 메모리(140)는 제 1 DVR 검사모듈(150)에서 DVR의 검사결과에 따라 수신된 DVR을 저장한다.
- [59] 이때 제 1 DVR 메모리(140)는 제 1 DVR 검사모듈(150)에 대해 쓰기 권한만 부여되고, 데이터 전송모듈(110)에 대해 읽기 권한만 부여된다.
- [60] 이와 같이 데이터 전송모듈(110)과 DVR 수신모듈(120)은 지정된 제 1 DVR 메모리(140) 만을 통해 데이터를 교환하며 제 1 DVR 메모리(140)에 대해 제 1 DVR 검사모듈(150)은 쓰기만 가능하고, 데이터 전송모듈(110)은 읽기만 가능하도록 함으로써 각 모듈의 독립적인 기능을 보장하도록 한다.
- [61] 또한, 제 1 DVR 메모리(140)는 고정된 작은 크기의 DVR 정보만을 저장하도록 하여 제 1 DVR 메모리(140)를 통한 사이버공격 가능성을 제거한다.
- [62] 이와 같이 송신장치(100)는 데이터 전송모듈(110)이 전송데이터 버퍼(130)에 데이터가 쌓일 때마다 데이터를 전송한 후, 일정시간 동안 제 1 DVR 메모리(140)에 전송한 데이터에 대한 DVR이 저장되기를 대기하고, DVR이 DVR 수신포트(102)를 통해 도착하면 DVR 수신모듈(120)은 DVR이 정해진 데이터 규격에 맞게 들어왔는지 여부를 DVR 검사모듈(150)을 통해 검증한 후 이를 제 1 DVR 메모리(140)에 저장한다.
- [63] 그런다음 데이터 전송모듈(110)은 제 1 DVR 메모리(140)에 쓰여진 값을 통해 성공여부를 확인하고 다음 데이터를 전송할 것인지, 이전 데이터를 재전송할 것인지를 결정하면서 데이터를 전송한다.
- [64]

- [65] 수신장치(200)는 보안레벨이 낮은 제 2 네트워크(600)에 연결되어 데이터 전송라인(300)을 통해 송신장치(100)로부터 전송된 데이터를 제 2 네트워크(600)로 전달하고 DVR 전송라인(400)을 통해 데이터에 대한 데이터 검증결과인 DVR을 전송한다.
- [66] 이때 수신장치(200)는 데이터 수신모듈(210), 수신데이터 버퍼(240), 제 2 DVR 메모리(230), 제 2 DVR 검사모듈(250) 및 DVR 전송모듈(220)을 포함한다.
- [67] 데이터 수신모듈(210)은 데이터 수신포트(201)를 통해 데이터 전송라인(300)으로 전송된 데이터를 수신한다.
- [68] 이때 데이터 수신모듈(210)은 전송된 데이터 패킷들을 분석하여 누락된 패킷이 존재 하는지, 비트 에러 발생 여부를 확인하여 에러가 발생시에 수신된 데이터를 버리고, 분석 결과를 제 2 DVR 메모리(230)에 저장한다.
- [69] 수신데이터 버퍼(240)는 데이터 수신모듈(210)을 통해 수신된 데이터를 저장하여 제 2 네트워크(600)로 전송한다.
- [70] 이때 수신데이터 버퍼(240)는 제 2 네트워크(600)로 데이터를 전송할 수 있을 뿐 제 2 네트워크(600)에서 수신데이터 버퍼(240)로 데이터를 쓸 수는 없도록 인터페이스 된다.
- [71] 제 2 DVR 메모리(230)는 데이터 수신모듈(210)에서 수신된 데이터에 대한 데이터 검증결과인 DVR을 저장한다.
- [72] 제 2 DVR 검사모듈(250)은 제 2 DVR 메모리(230)에 저장된 DVR이 정해진 규격을 검사하여 안전한 DVR이 전송될 수 있도록 한다.
- [73] 이때 제 2 DVR 메모리(230)는 데이터 수신모듈(210)에 대해 쓰기 권한만 부여되고, 제 2 DVR 검사모듈(250)에 대해 읽기 권한만 부여된다.
- [74] 이와 같이 데이터 수신모듈(210)과 제 2 DVR 검사모듈(250)은 지정된 제 2 DVR 메모리(230) 만을 통해 데이터를 교환하며 제 2 DVR 메모리(230)에 대해 제 2 DVR 검사모듈(250)은 읽기만 가능하고, 데이터 수신모듈(210)은 쓰기만 가능하도록 함으로써 각 모듈의 독립적인 기능을 보장하도록 한다.
- [75] 또한, 제 2 DVR 메모리(230)는 고정된 작은 크기의 DVR 정보만을 저장하도록 하여 제 2 DVR 메모리(230)를 통한 사이버공격 가능성을 제거한다.
- [76] DVR 전송모듈(220)은 제 2 DVR 검사모듈(250)의 결과에 따라 DVR 전송포트(202)를 통해 DVR 전송라인(400)으로 데이터 검증결과를 전송한다.
- [77] 이와 같이 수신장치(200)는 데이터 수신모듈(210)에서 전송된 데이터 패킷들을 분석하여 누락된 패킷이 존재 하는지, 비트 에러 발생 여부를 확인하여 에러가 발생시에 수신된 데이터를 버리고, 분석 결과인 DVR을 제 2 DVR 메모리(230)에 저장하면, 제 2 DVR 검사모듈(250)에서 DVR의 규격을 검사하여 사이버공격 가능성을 검사한 후 DVR 전송모듈(220)에서 DVR 전송라인(400)을 통해 송신장치(100)로 전송한다.
- [78] 이와 같이 일방향 데이터 전송에서 신뢰성을 향상시키기 위해 송신장치(100)가 패킷들을 데이터 전송라인(300)을 통해 전송할 때마다 수신장치(200)는 전송된

데이터 패킷의 정상수신 여부에 따른 데이터 검증결과인 DVR을 DVR 전송라인(400)을 통해 송신장치(100)에 전달함으로써 송신장치(100)와 수신장치(200) 간에 패킷 에러나 비트 에러가 발생한 경우 이를 확인하고 재전송이 가능하게 되어 일방향 자료전달의 신뢰성이 향상될 수 있다.

[79] 한편, 운영체제가 송신장치(100)와 수신장치(200)의 제 1 DVR 메모리(140), 제 2 DVR 메모리(230), DVR 수신모듈(120), DVR 전송모듈(220)에 접근할 수 없도록 구현하여 수신장치(200)를 통해 제 1 네트워크(500) 측으로 어떠한 데이터도 전송될 수 없도록 함으로써 수신장치(200)에서 송신장치(100)로 DVR이외의 정보가 전달되지 않도록 하여 안전한 데이터 전달이 이루어질 수 있도록 한다.

[80]

[81] 도 3은 본 발명의 일 실시예에 따른 일방향 데이터 전송 시스템에서의 데이터 패킷의 구조를 나타낸 도면이다.

[82] 도 3에 도시된 바와 같이 데이터의 패킷의 구조는 데이터 전송의 효율성을 향상시키기 위해 하나의 패킷을 전송하고 수신 여부를 확인하는 것만이 아닌 패킷 그룹으로 전송하는 경우로써 Group ID영역(301), Packet Count영역(302), Seq영역(303), Unique Value영역(304), Data영역(305) 및 HV영역(306)을 포함한다.

[83] Group ID영역(301)은 전송할 데이터 패킷 그룹마다 고유한 값을 나타낸다.

[84] Packet Count영역(302)은 해당 패킷 그룹에서 전송할 패킷을 나타낸다.

[85] Seq영역(303)은 패킷 그룹 내 전송 패킷의 순서를 나타낸다.

[86] Unique Value영역(304)은 패킷 재전송 등에서 발생할 수 있는 문제를 해결하기 위한 값으로 모든 패킷 전송시에 구별되는 값을 나타낸다. 순차적인 인덱스, 타임스탬프 값 등이 UV(Unique Value)값으로 활용될 수 있다.

[87] Data영역(305)은 실제 전송되어야 할 데이터를 나타낸다.

[88] HV영역(306)은 해시값을 나타내며, 전송할 패킷이 효율성을 고려해 CRC 등이 활용될 수 있다.

[89] 만약 패킷을 하나씩 전송할 경우 Packet Count영역과 Seq영역은 생략될 수도 있다.

[90]

[91] 도 4는 본 발명의 일 실시예에 따른 일방향 데이터 전송 시스템에서의 데이터 검증결과 구조를 나타낸 도면이다.

[92] 도 4에 도시된 바와 같이 데이터 검증결과인 DVR의 구성은 Group ID영역(401), Unique Value영역(402) 및 Signal영역(403)을 포함한다.

[93] Group ID영역(401)과 Unique Value영역(402)는 송신장치(100)에서 전송된 패킷 그룹의 값을 그대로 사용하는 것으로 Group ID영역(401)은 전송할 데이터 패킷 그룹마다 고유한 값을 나타내고, Unique Value영역(402)은 패킷 재전송 등에서 발생할 수 있는 문제를 해결하기 위한 값으로 모든 패킷 전송시에 구별되는 값을

나타낸다.

- [94] Signal영역(403)은 수신된 데이터 패킷의 분석결과에 따라 OK 혹은 Error 값을 갖는다. 수신장치(200)로 전송하는 DVR의 패킷 크기를 최소화하기 위해서 수신한 패킷 그룹 전체를 대상으로 패킷 수신 결과를 전송할 수 있다.
- [95]
- [96] 도 5는 본 발명의 일 실시예에 따른 일방향 데이터 전송방법에 의한 데이터 전송과정을 설명하기 위한 흐름도이다.
- [97] 도 5에 도시된 바와 같이 본 발명의 일 실시예에 따른 일방향 데이터 전송방법에 의한 데이터 전송과정은 송신장치(100)의 데이터 전송모듈(110)에서 데이터의 전송요건이 만족 되는가 판단한다(S110).
- [98] 데이터의 전송요건은 제 1 DVR 메모리(140)에 저장된 이전 데이터의 데이터 검증결과인 DVR의 상태와 전송데이터 버퍼(130)에 전송할 데이터가 존재하는가 판단한다.
- [99] 이와 같이 데이터 전송요건이 만족될 경우 데이터 전송라인(300)을 통해 데이터 패킷 그룹을 전송한다(S120).
- [100] 데이터 전송모듈(110)은 데이터를 전송한 후 일정시간 내에 DVR 전송라인(400)을 통한 데이터 검증결과인 DVR의 수신여부를 판단한다(S130).
- [101] 그리고, 수신된 DVR이 정의된 구조와 값을 갖는가 판단하고(S140), 수신된 DVR이 OK인가 판단하며(S150), 데이터 전송모듈(110)에서 전송된 데이터 패킷 그룹과 동일한 Group ID와 UV값을 갖는가 판단한다(S160).
- [102] 이와 같이 DVR의 상태를 판단하여 판단결과에 따라 DVR이 OK값을 가지며 데이터 전송모듈(110)에서 마지막으로 보낸 패킷 그룹과 동일한 Group ID와 UV값을 갖는 다면 성공여부를 확인하여 DVR을 제 1 DVR 메모리(140)에 저장하여 다음 데이터를 전송할 수 있도록 한다(S190).
- [103] 만약, 만약 DVR이 Error 값을 갖는다면 이전 패킷 그룹을 재전송하기 위해 이전에 보낸 패킷 그룹과 구별하기 위해 UV값을 변화시킨다(S170).
- [104] 이때 UV값은 이전에 보낸 패킷 그룹에 대한 응답이 늦게 온 경우 마지막으로 보낸 패킷 그룹에 대한 응답 여부인지를 확인하기 위해서 사용된다. 따라서, 재전송을 위해서는 UV값을 변경한 후 이전에 보낸 데이터를 재전송한다(S180).
- [105]
- [106] 도 6은 본 발명의 일 실시예에 따른 일방향 데이터 전송방법에 의한 데이터 수신과정을 설명하기 위한 흐름도이다.
- [107] 도 6에 도시된 바와 같이 본 발명의 일 실시예에 따른 일방향 데이터 전송방법에 의한 데이터 수신과정은 수신장치(200)의 데이터 수신모듈(210)에서 데이터 전송라인(300)을 통해 데이터를 수신한다(210).
- [108] 이후 데이터 수신모듈(210)은 수신한 패킷들의 Packet Count영역과 Seq영역을 비교하여 모든 패킷이 수신되었는지를 판단한다(S220).
- [109] 또한, 모든 패킷들이 정상적으로 수신된 경우 데이터 수신모듈(210)은 데이터

패킷의 HV영역의 해쉬값이 계산값과 동일한가 판단하여 데이터 에러가 발생하였는가 판단한다(S230).

[110] 이때 에러가 발생하지 않았다면 수신장치(200)는 OK의 데이터 검증결과에 따른 DVR을 생성하여 제 2 DVR 메모리(230)에 저장하고(S240), DVR 전송라인(400)을 통해 송신장치(200)로 전송한다(S270).

[111] 그러나, 모든 패킷이 수신되지 않았거나 해쉬값이 계산값과 동일하지 않아 에러가 발생한 경우에는 Error의 데이터 검증결과에 따른 DVR을 생성하여 제 2 DVR 메모리(230)에 저장하고(S250), DVR 전송라인(400)을 통해 송신장치(200)로 전송한다(S270).

[112] 위에서 제 2 DVR 메모리(230)에 저장된 DVR은 DVR 전송모듈(220)에서 DVR이 정의된 구조를 갖는가 검증하여 정상일 경우 전송하고 정상이지 않을 경우 전송하지 않는다(S260)(S280).

[113]

[114] 본 발명은 도면에 도시된 실시예를 참고로 하여 설명되었으나, 이는 예시적인 것에 불과하며, 당해 기술이 속하는 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 기술적 보호범위는 아래의 특허청구범위에 의해서 정하여져야 할 것이다.

[115]

청구범위

- [청구항 1] 보안레벨이 높은 제 1 네트워크에 연결되어 상기 제 1 네트워크로부터 전송된 데이터를 보안레벨인 낮은 제 2 네트워크로 데이터 전송라인을 통해 전송하고 상기 데이터에 대한 상기 데이터 검증결과를 DVR(Data Verification Result) 전송라인을 통해 수신 받는 송신장치; 및
보안레벨이 낮은 상기 제 2 네트워크에 연결되어 상기 데이터 전송라인을 통해 상기 송신장치로부터 전송된 상기 데이터를 상기 제 2 네트워크로 전달하고 상기 DVR 전송라인을 통해 상기 데이터에 대한 상기 데이터 검증결과를 전송하는 수신장치;를 포함하는 것을 특징으로 하는 일방향 데이터 전송 시스템.
- [청구항 2] 제 1항에 있어서, 상기 송신장치는
상기 제 1 네트워크로부터 전송된 상기 데이터를 저장하는 전송데이터 버퍼;
상기 전송데이터 버퍼에 저장된 상기 데이터를 데이터 전송포트를 통해 상기 데이터 전송라인으로 전송하는 데이터 전송모듈;
DVR 수신포트를 통해 상기 DVR 전송라인으로 전송된 상기 데이터 검증결과를 수신하는 DVR 수신모듈;
상기 DVR 수신모듈을 통해 수신한 상기 데이터 검증결과를 규격을 검사하는 제 1 DVR 검사모듈; 및
상기 제 1 DVR 검사모듈에서 검사결과에 따라 수신된 상기 데이터 검증결과를 저장하는 제 1 DVR 메모리;를 포함하는 것을 특징으로 하는 일방향 데이터 전송 시스템.
- [청구항 3] 제 2항에 있어서, 상기 데이터 전송모듈은 상기 제 1 DVR 메모리에 저장된 상기 데이터 검증결과에 따라 이전 데이터의 재전송 여부를 결정하여 상기 이전 데이터를 재전송하거나 다음 데이터를 전송하는 것을 특징으로 하는 일방향 데이터 전송 시스템.
- [청구항 4] 제 2항에 있어서, 상기 제 1 DVR 메모리는 상기 제 1 DVR 검사모듈에 대해 쓰기 권한만 부여되고, 상기 데이터 전송모듈에 대해 읽기 권한만 부여되는 것을 특징으로 하는 일방향 데이터 전송 시스템.
- [청구항 5] 제 1항에 있어서, 상기 제 1 네트워크와 상기 송신장치는 상기 제 1 네트워크에서 상기 송신장치로만 상기 데이터를 전송할 수 있도록 연결되는 것을 특징으로 하는 일방향 데이터 전송 시스템.
- [청구항 6] 제 1항에 있어서, 상기 수신장치는
데이터 수신포트를 통해 상기 데이터 전송라인으로 전송된 상기

데이터를 수신하는 데이터 수신모듈;
 상기 데이터 수신모듈을 통해 수신된 상기 데이터를 저장하여
 상기 제 2 네트워크로 전송하는 수신데이터 버퍼;
 상기 데이터 수신모듈에서 수신된 상기 데이터에 대한 상기
 데이터 검증결과를 저장하는 제 2 DVR 메모리;
 상기 제 2 DVR 메모리에 저장된 상기 데이터 검증결과의 규격을
 검사하는 제 2 DVR 검사모듈; 및
 상기 제 2 DVR 검사모듈의 결과에 따라 DVR 전송포트를 통해
 상기 DVR 전송라인으로 상기 데이터 검증결과를 전송하는 DVR
 전송모듈;을 포함하는 것을 특징으로 하는 일방향 데이터 전송
 시스템.

- [청구항 7] 제 6항에 있어서, 상기 제 2 DVR 메모리는 상기 데이터 수신모듈에 대해 쓰기 권한만 부여되고, 상기 제 2 DVR 검사모듈에 대해 읽기 권한만 부여되는 것을 특징으로 하는 일방향 데이터 전송 시스템.
- [청구항 8] 제 1항에 있어서, 상기 제 2네트워크와 상기 수신장치는 상기 수신장치에서 상기 제 2 네트워크로만 데이터를 전송할 수 있도록 연결되는 것을 특징으로 하는 일방향 데이터 전송 시스템.
- [청구항 9] 제 1항에 있어서, 상기 데이터 전송라인을 통해 전송되는 데이터의 패킷은
 데이터 패킷 그룹의 고유값을 나타내는 Group ID영역,
 상기 데이터 패킷 그룹에서 전송할 패킷을 나타내는 Packet Count영역,
 상기 데이터 패킷 그룹내의 전송 패킷의 순서를 나타내는 Seq영역,
 상기 데이터 패킷의 전송시 패킷을 구별하기 위한 UV(Unique Value)값을 나타내는 Unique Value영역, 데이터 패킷을 나타내는 Data영역 및
 상기 데이터 패킷의 해시값을 나타내는 HV영역을 포함하는 것을 특징으로 하는 일방향 데이터 전송 시스템.
- [청구항 10] 제 1항에 있어서, 상기 DVR 전송라인을 통해 전송되는 상기 데이터 검증결과의 패킷은
 전송한 상기 데이터 패킷 그룹의 고유값을 나타내는 Group ID영역,
 상기 데이터 패킷의 전송시 패킷을 구별하기 위한 UV값을 나타내는 Unique Value영역 및
 상기 데이터 패킷의 분석 결과를 나타내는 Signal영역을 포함하는 것을 특징으로 하는 일방향 데이터 전송 시스템.
- [청구항 11] 송신장치에서 데이터의 전송요건이 만족 되는가 판단하는 단계;

상기 데이터의 전송요건에 만족할 경우 데이터를 데이터 전송라인을 통해 전송하는 단계;
 상기 데이터를 전송한 후 일정시간 내에 DVR 전송라인을 통한 데이터 검증결과에 수신여부를 판단하는 단계;
 상기 데이터 검증결과에 상태에 따라 상기 데이터의 재전송 여부를 판단하는 단계; 및
 상기 판단결과에 따라 패킷을 구별하기 위한 UV값을 변경하여 재전송하거나 상기 데이터 검증결과를 저장하는 단계;를 포함하는 것을 특징으로 하는 일방향 데이터 전송 방법.

[청구항 12]

제 11항에 있어서, 상기 데이터의 전송요건은 상기 데이터 검증결과에 상태와 전송데이터 버퍼에 전송할 상기 데이터가 존재할 경우인 것을 특징으로 하는 일방향 데이터 전송 방법.

[청구항 13]

제 11항에 있어서, 상기 데이터의 재전송 여부를 판단하는 단계는 일정시간 내에 상기 데이터 검증결과가 수신되는가를 판단하는 단계;

수신된 상기 데이터 검증결과가 정의된 구조와 값을 갖는가 판단하는 단계;

수신된 상기 데이터 검증결과가 성공인가 판단하는 단계; 및
 전송된 상기 데이터 패킷의 고유값과 UV값이 동일한가 판단하는 단계를 포함하는 것을 특징으로 하는 일방향 데이터 전송 방법.

[청구항 14]

수신장치에서 데이터 전송라인을 통해 데이터를 수신하는 단계;

수신된 데이터 패킷의 정상 수신여부를 판단하는 단계;

상기 정상 수신여부를 판단하여 데이터 검증결과를 저장하는 단계; 및

저장된 상기 데이터 검증결과를 검사한 후 DVR 전송라인을 통해 전송하는 단계;를 포함하는 것을 특징으로 하는 일방향 데이터 전송 방법.

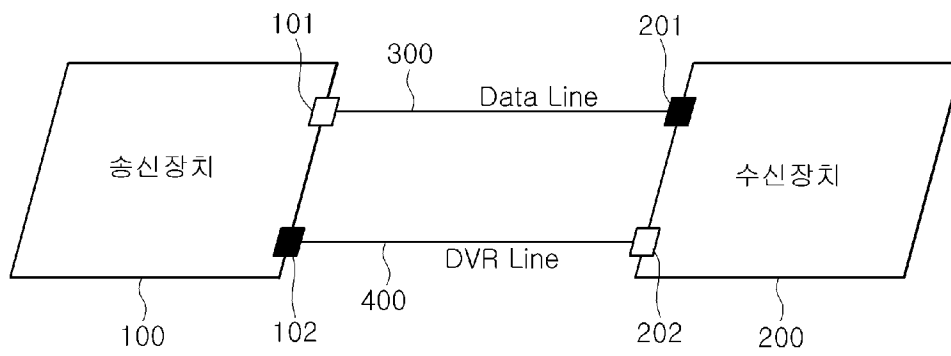
[청구항 15]

제 14항에 있어서, 상기 데이터 패킷의 정상 수신여부를 판단하는 단계는

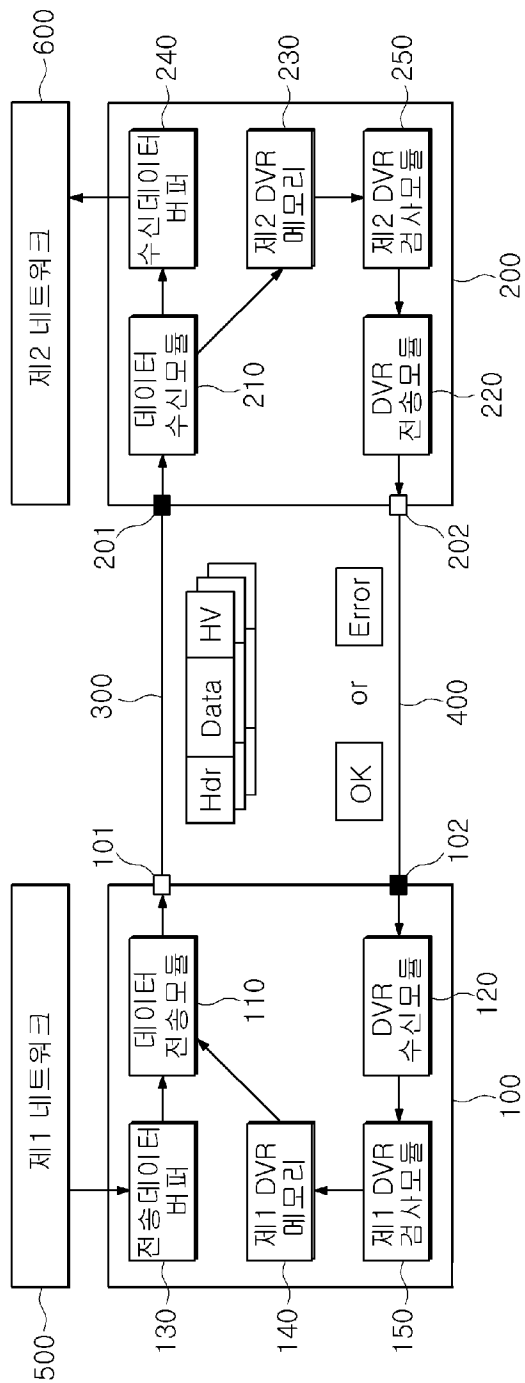
상기 데이터 패킷이 지정시간 동안 모든 패킷이 수신되는가 판단하는 단계; 및

상기 데이터 패킷의 해쉬값이 계산값과 동일한가 판단하는 단계;를 포함하는 것을 특징으로 하는 일방향 데이터 전송 방법.

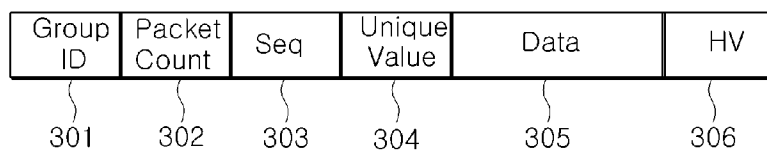
[Fig. 1]



[Fig. 2]



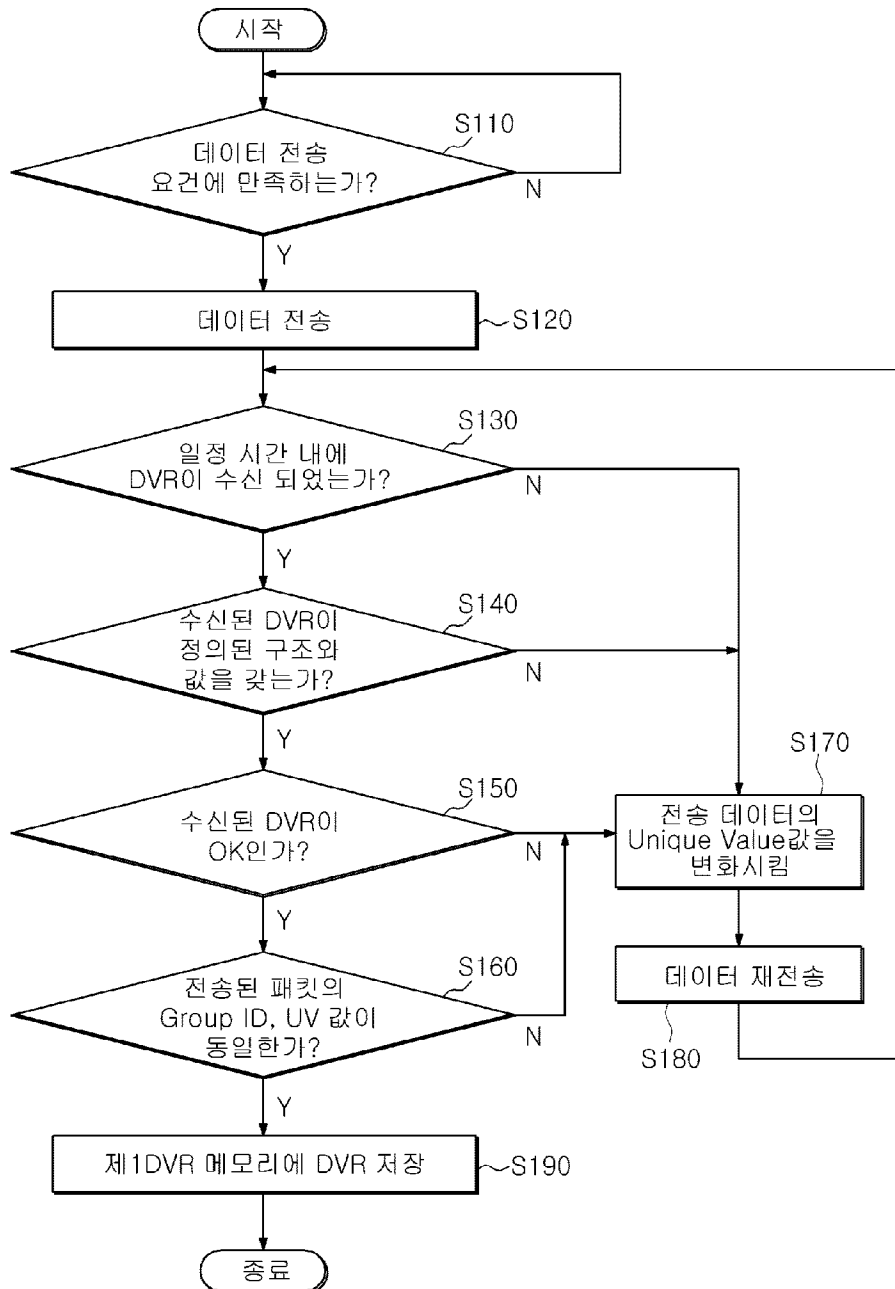
[Fig. 3]



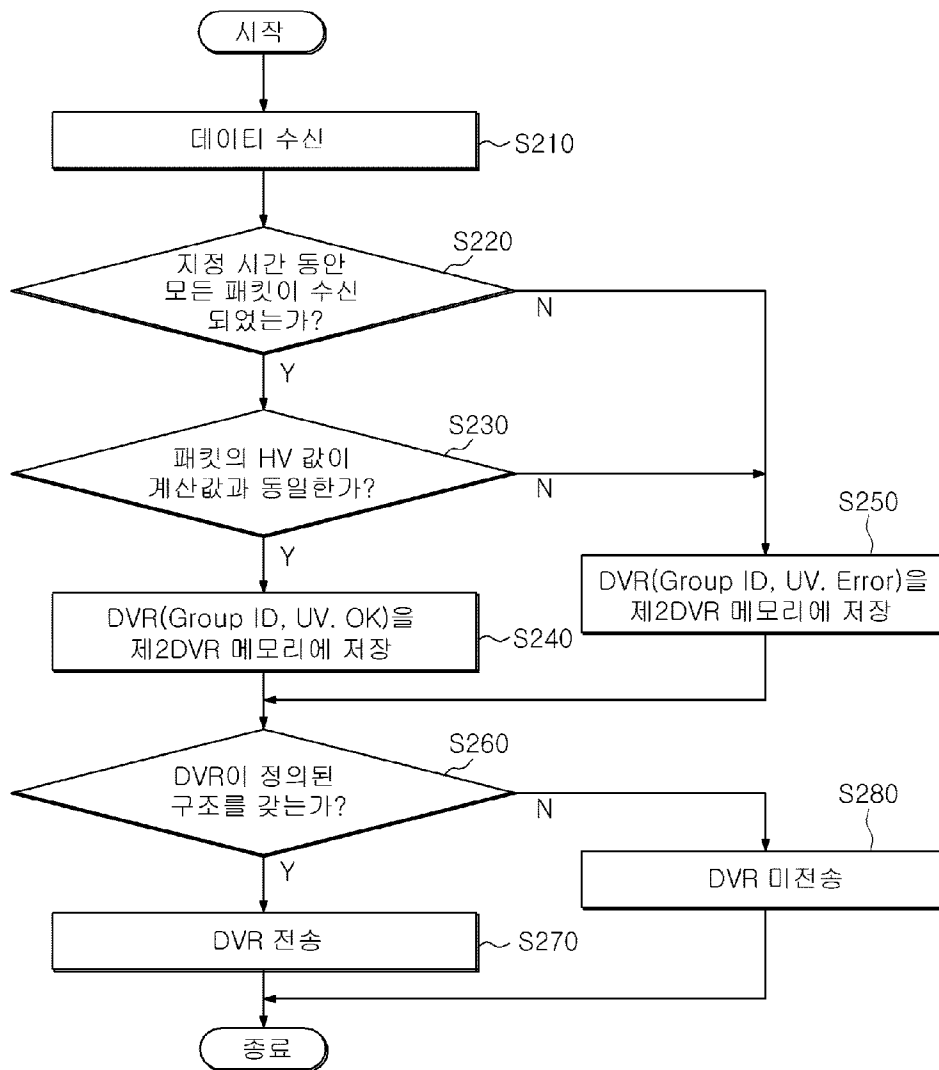
[Fig. 4]

Group ID	Unique Value	Signal (Ok or Error)
401	402	403

[Fig. 5]



[Fig. 6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2013/008375**A. CLASSIFICATION OF SUBJECT MATTER****H04L 1/16(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 1/16; G06F 21/24; G06F 3/06; H04L 29/08; H04L 12/26; H04L 12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: security, verification, forwarding

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 3900058 B2 (HITACHI LTD.) 04 April 2007 See paragraphs [0012, 0021, 0018, 0019 and 0023]	1-15
Y	KR 10-2011-0004248 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 13 January 2011 See abstract, claim 1	1-15
A	JP 4742498 B2 (SONY CORP.) 10 August 2011 See paragraphs [0019, 0025 and 0069]	1-15
A	JP 4074304 B2 (NIPPON TELEGR & TELEPH CORP.) 09 April 2008 See paragraphs [0006-0009, 0017 and 0182]	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

23 OCTOBER 2013 (23.10.2013)

Date of mailing of the international search report

24 OCTOBER 2013 (24.10.2013)

Name and mailing address of the ISA/KR



Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2013/008375

Patent document cited in search report	Publication date	Patent family member	Publication date
JP 3900058 B2	04/04/2007	CN 1295632 C0	17/01/2007
		CN 1497466 A	19/05/2004
		CN 1497466 C0	17/01/2007
		JP 2004-120667 A	15/04/2004
		KR 10-2004-0028571 A	03/04/2004
		TW 232046 A	01/05/2005
		TW 232046 B	01/05/2005
		TW 1232046 B	01/05/2005
		US 2004-0111524 A1	10/06/2004
		US 2006-0026292 A1	02/02/2006
KR 10-2011-0004248 A	13/01/2011	NONE	
JP 4742498 B2	10/08/2011	CN 1300704 C0	14/02/2007
		CN 1637720 A	13/07/2005
		HK 1078662 A1	22/06/2007
		JP 2005-196700 A	21/07/2005
		SG 11353 7A1	29/08/2005
		US 2005-0198514 A1	08/09/2005
		US 2009-0235336 A1	17/09/2009
		US 7555653 B2	30/06/2009
		US 7941670 B2	10/05/2011
JP 4074304 B2	09/04/2008	AU 2005-260881 A1	19/01/2006
		AU 2005-260881 B2	06/03/2008
		AU 2005-260881 C1	11/09/2008
		AU 2005-260881 C1	06/03/2008
		CN 100531126 C	19/08/2009
		CN 1879369 A	13/12/2006
		CN 1879369 C0	13/12/2006
		EP 1768328 A1	28/03/2007
		EP 1768328 B1	26/12/2012
		EP 2424179 A1	29/02/2012
		EP 2424180 A1	29/02/2012
		EP 2485442 A1	08/08/2012
		JP 04-074268B2	09/04/2008
		JP 2005-102157A	14/04/2005
		JP 2006-174406A	29/06/2006
		JP 2007-209040A	16/08/2007
		KR 10-0839881 B1	20/06/2008
		TW 1304298A	11/12/2008
		TW 1304298B	11/12/2008
		US 2008-0279181 A1	13/11/2008
		US 2011-0038373 A1	17/02/2011
		US 7869428 B2	11/01/2011
		WO 2006-006632 A1	19/01/2006

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 1/16(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 1/16; G06F 21/24; G06F 3/06; H04L 29/08; H04L 12/26; H04L 12/56

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 보안, 검증, 포워딩

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	JP 3900058 B2 (HITACHI LTD.) 2007.04.04 본문 [0012, 0021, 0018, 0019, 0023] 참조	1-15
Y	KR 10-2011-0004248 A (한국전자통신연구원) 2011.01.13 요약, 청구항 1 참조	1-15
A	JP 4742498 B2 (SONY CORP.) 2011.08.10 본문 [0019, 0025, 0069] 참조	1-15
A	JP 4074304 B2 (NIPPON TELEGR & TELEPH CORP.) 2008.04.09 본문 [0006-0009, 0017, 0182] 참조	1-15

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2013년 10월 23일 (23.10.2013)

국제조사보고서 발송일

2013년 10월 24일 (24.10.2013)

ISA/KR의 명칭 및 우편주소

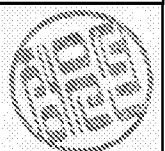
 대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-472-7140

심사관

정은선

전화번호 +82-42-481-5708



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
JP 3900058 B2	2007/04/04	CN 1295632 C0 CN 1497466 A CN 1497466 C0 JP 2004-120667 A KR 10-2004-0028571 A TW 232046 A TW 232046 B TW I232046 B US 2004-0111524 A1 US 2006-0026292 A1	2007/01/17 2004/05/19 2007/01/17 2004/04/15 2004/04/03 2005/05/01 2005/05/01 2005/05/01 2004/06/10 2006/02/02
KR 10-2011-0004248 A	2011/01/13	없음	
JP 4742498 B2	2011/08/10	CN 1300704 C0 CN 1637720 A HK 1078662 A1 JP 2005-196700 A SG 11353 7A1 US 2005-0198514 A1 US 2009-0235336 A1 US 7555653 B2 US 7941670 B2	2007/02/14 2005/07/13 2007/06/22 2005/07/21 2005/08/29 2005/09/08 2009/09/17 2009/06/30 2011/05/10
JP 4074304 B2	2008/04/09	AU 2005-260881 A1 AU 2005-260881 B2 AU 2005-260881 C1 AU 2005-260881 C1 CN 100531126 C CN 1879369 A CN 1879369 C0 EP 1768328 A1 EP 1768328 B1 EP 2424179 A1 EP 2424180 A1 EP 2485442 A1 JP 04-074268B2 JP 2005-102157A JP 2006-174406A JP 2007-209040A KR 10-0839881 B1 TW I304298A TW I304298B US 2008-0279181 A1 US 2011-0038373 A1 US 7869428 B2 WO 2006-006632 A1	2006/01/19 2008/03/06 2008/09/11 2008/03/06 2009/08/19 2006/12/13 2006/12/13 2007/03/28 2012/12/26 2012/02/29 2012/02/29 2012/08/08 2008/04/09 2005/04/14 2006/06/29 2007/08/16 2008/06/20 2008/12/11 2008/12/11 2008/11/13 2011/02/17 2011/01/11 2006/01/19