Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.613

일방향 전송 네트워크에서의 오류 제어 프로토콜 및 데이터 암호화 메커니즘*

하 재 철,[1†] 김 기 현[2‡]
[1]호서대학교, [2](주)앤앤에스피

Error Control Protocol and Data Encryption Mechanism in the One-Way Network*

Jaecheol Ha,[1†] Kihyun Kim[2‡]
[1]Hoseo University, [2]NNSP Co., Ltd

요 약

데이터가 일방향으로 전송되는 네트워크 환경에서 데이터에 대한 오류 제어는 매우 민감하고 중요한 문제이다. 이 문제를 해결하기 위해서 전방향 오류 정정 부호 기법이나 수신 결과를 회신하여 데이터를 재전송하는 기법이 사용되고 있다. 본 논문에서는 데이터를 일방향으로 전송하는 채널과 수신 결과만 회신할 수 있는 별도의 채널이 있는 네트워크 환경에서 오류 제어 기법 및 연속 데이터 전송을 할 수 있는 프로토콜을 제안한다. 또한, 일방향 네트워크에서 사전 공유키 분배 기법에 기반한 데이터 암호 및 키 업데이트 메커니즘을 제안하고 이를 구현하기 위한 응용 서비스 데이터 단위(ASDU) 구조를 제시한다.

ABSTRACT

Since the error control problem is a critical and sensitive issue in the one-way network, we can adopt a forward error correction code method or data retransmission method based on the response of reception result. In this paper, we propose error control method and continuous data transmission protocol in the one-way network which has unidirectional data transmission channel and special channel to receive only the response of reception result. Furthermore we present data encryption and key update mechanism which is based on the pre-shared key distribution scheme and suggest some ASDU(Application Service Data Unit) formats to implement it in the one-way network.

Keywords: One-Way Network, Error Control Method, Data Encryption, Session Key Updating

I. 서 론

과거에는 전력 공급 시설이나 산업 플랜트의 제어 시스템을 구동하기 위해 독립적인 네트워크를 구성한 뒤 이를 폐쇄망 형태로 운영하였다. 그러나 고속의 정보 통신망을 이용한 원격 관리나 스마트 서비스 제공을 위해 인터넷과 같은 개방형 공중망과의 연결이 필요하게 되었다. 그런데 폐쇄적으로 운영하던 제어망을 공중망과 연결함에 따라 인터넷 망 등을 통한 해킹 시도나 바이러스 침투가 현실화 되면서 이에 대한 보안 대책이 당면 과제로 대두되었다. 따라서 이러한 특성을 고려하여 제어망과 같은 내부망에서 인터넷과 같은 외부망으로 한 방향으로만 데이터를 전달할 수 있는 일방향 전송 장비가 필요하게 되었다[1].

일방향 네트워크(one-way network)장비는 데

Received(04. 04. 2016), Accepted(05.12, 2016)
* 본 논문은 2015년도 동계학술대회에 발표한 우수 논문을 개선 및 확장한 것임
† 주저자, jcha@hoseo.edu
‡ 교신저자, hkim@nnsp.co.kr(Corresponding author)

이터를 한쪽 방향으로만 전송할 수 있도록 하는 네트워크 어플라이언스 또는 디바이스를 말하며,단방향 보안 게이트웨이(unidirectional security gateway) 또는 데이터 다이오드(data diode)라고 불리고 있다[1-3].

일반적인 네트워크에서는 두 통신자간의 신뢰성 있는 통신을 위해 오류 제어(error control)나 흐름 제어(flow control) 기법들을 사용하고 있다. 전방향 오류 정정(FEC, Forward Error Correction) 기법이나 역방향 재전송 요구 기법(ARQ, Automatic Repeat reQuest) 등이 일반적으로 사용되는 신뢰 통신 기법들이다. 특히, 수신측에서는 오류 검출 기법(error detection method)을 이용하여 데이터가 정상적으로 수신되었는지 확인하고 응답하는 기법을 통해 오류가 있는 데이터를 재전송하는 기법을 많이 사용하고 있다.

그러나 이러한 기법들은 오류 정정을 위한 많은 연산량과 부가적인 통신량을 필요로 하고 양방향으로 신호를 주고 받을 수 있는 통신 환경에 적합한 기법들이다. 따라서 제한적인 컴퓨팅 능력을 가진 일방향 통신 환경에 적합하면서 신뢰성 통신을 위한 효율적인 오류 제어 기법과 수신자의 버퍼 능력을 고려하여 데이터를 연속적으로 보낼 수 있는 통신 프로토콜 개발이 필요하다.

또한, 제어망과 같은 내부망에서 생성된 정보는 센싱 정보나 제어 정보와 같은 중요한 데이터를 전송해야 하므로 일방향 네트워크에서 주고 받는 데이터에 대한 기밀성 및 무결성 제공 기술이 필요하다. 특히, 기밀성 유지를 위한 암호화 과정에서 사용되는 세션 키나 주기적으로 업데이트가 필요한 키는 두 통신자 만의 안전한 방법을 통해 갱신되어야 한다.

본 논문에서는 보안 등급이 높은 내부망에서 보안 등급이 낮은 외부망으로만 데이터를 전송하는 일방향 네트워크를 가정하고 신뢰성 있는 통신을 위한 오류 제어 기법과 연속 데이터 전송 프로토콜을 제안한다. 여기에서는 일방향으로 데이터를 전송하는 채널 이외에 수신자 측에서 두 가지 형태의 신호(OK 및 Error)를 회신하는 물리적 환경[4]과 한 가지 형태의 신호(절체 혹은 OFF)를 회신하는 경우를 모두 고려한다[5]. 또한, 데이터에 대한 기밀성 유지를 위해 사용하는 암호용 키의 관리 및 주기적인 업데이트 메커니즘을 제안하고 이를 구현하기 위한 응용 서비스 데이터 단위(ASDU, Application Service Data Unit) 구조를 제시한다.

II. 일방향 데이터 전송 기법 및 장비

물리적인 일방향 통신에 대한 정의는 정부 지침이나 가이드에서 소개하고 있으며 "정보 전달이 필요한 두 시스템 사이에 단방향으로만 정보가 전달되도록 송·수신 회선의 한쪽을 물리적으로 차단한 연결선을 사용하는 방식"으로 정의하고 있다. 또한 일방향 전송 장비는 "데이터 송신용 장비와 수신용 장비를 한 쌍으로 하여 일방향으로만 정보전달이 가능하도록 개발된 전용장비"로 정의하고 있다.

일방향 네트워크를 이용한 통신 개념은 1960년대부터 있었으며, 초기에는 일방향 네트워크를 구성하기 위해 송신측 RX 라인과 수신측의 TX 라인을 물리적으로 자른 RS-232가 데이터 다이오드로 사용되었다. RS-232 케이블링 방식은 역방향으로 데이터를 전송할 수 있는 비밀 채널(covert channel)이 필요한 문제를 가지고 있었는데 이를 개선하기 위해 1990년대 호주의 DSTO(Defence Science and Technology Organization)에서 광 데이터 다이오드가 개발되기도 하였다[1-3].

데이터 다이오드는 케이블링 방식에서 네트워크 어플라이언스 형태로 발전해 왔으며 현재에는 일방향 전송 장비들로 상용화되어 기반 시설 보호를 목적으로 사용되고 있다. 대부분 상용 일방향 전송 장비들은 기반 시설 보호를 위해 보안 등급이 높은 네트워크(제어망)에서 보안 등급이 낮은 네트워크(업무망)로 데이터를 전달하기 위해 사용되고 있다. Fig. 1은 제어망과 내부망에 존재하는 두 시스템간의 일방향 네트워크의 연결 상태를 나타낸 그림이다.

외국의 일방향 전송 장비로는 Waterfall 사의 USG(Unidirectional Security Gateway)[6], Fox-IT사의 FFHDD(Fort Fox Hardware Data Diode)[7], Owl Computing Technologies사의 Dual Diode[8] 등이 있으며 이미 국제 CC(Common Criteria) 인증을 받았다. 국내의 경우, 2010년부터 한국전력공사와 국가보안기술연구소의 "전력제어시스템 보안기술 개발" 과제로 연구되어[9-10] 2013년 한전 KDN으로 "물리적 일방향 자료전달" 기술이 이전되었다. 이후 한전 KDN은 자체 개발을 통하여 한전 전력망 프로토콜인 DNP에 기반한 일방향 장비인 NIMA-1000을 발표하였다. 또한, 2013년에는 (주)NNSP에서 플랜트 제어망 프로토콜인 OPC 및 Modbus에 기반을 둔 일방향 장비인 nNetDiode 제품을 발표하기

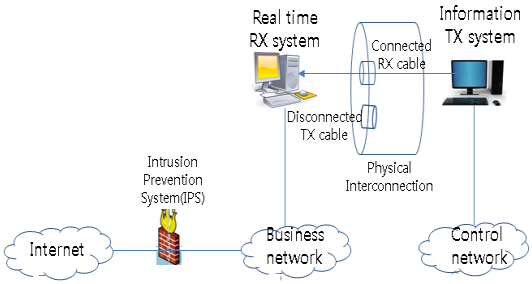

Fig. 1. One-way data transmission between two systems

도 하였다[11].

일반적으로 네트워크에서 오류 문제를 해결하기 위한 방법은 오류 검출 및 정정을 위한 부가 정보(redundancy)를 추가적으로 보내거나 오류 발생 시 데이터를 재전송하는 방법을 많이 사용한다. 특히, 전송 데이터의 오류 여부를 검출하기 위해 데이터 순서 번호(sequence number), 길이(length), 체크섬(checksum) 등과 같은 부가 정보를 보내기도 하며, SHA[12]나 MD5[13]와 같은 해시 함수를 이용하여 무결성 검사 값을 전송하기도 한다.

일방향 네트워크에서의 가장 큰 문제점은 양방향 통신이 어려워 기존 프로토콜의 원활한 적용이 어렵고, 데이터의 전송 오류에 대한 대처 능력이 떨어진다는 것이다. 즉, 중간에 데이터가 변조되거나 분실되었을 때 재전송 기법을 적용하기가 쉽지 않다는 것이다.

일방향 네트워크에서 신뢰성 있는 통신 기능을 을 제공하기 위한 예로서 Owl Computing Technologies사의 Dual Diode에서는 Fig. 2와 같이 ATM AAL5 프로토콜에서 체크섬(checksum) 검사가 이루어지고 응용 레벨에서 MD5를 이용한 무결성 검사를 수행한다[8]. 또한, Waterfall사의 USG나 Fox-IT사의 FFHDD는 전송 데이터 오류를 제어하기 위해 전방향 오류 정정 기법을 사용하고 있다[6-7].

한국전자통신연구원의 문헌[14] "일방향 데이터 전송 시스템 및 방법"에서는 높은 보안이 필요한 네트워크에서 낮은 보안이 필요한 네트워크로 데이터를 일방향 전송할 때 자가 오류 복구에 필요한 정보를 추가하여 인코딩하고 수신된 데이터의 오류 검출 및 자가 복구를 수행하는 방법을 제안하고 있다.

한국전력공사의 문헌[4] "일방향 데이터 전송 시

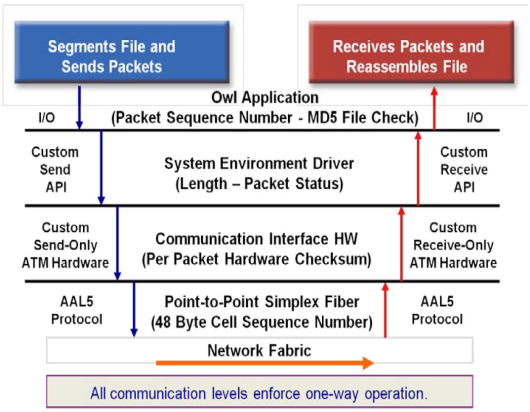

Fig. 2. Dual Diode protocol stack

스템"에서는 Fig. 3과 같이 데이터를 일방향 전송하고 데이터 검증 결과는 별도의 라인을 통해 수신하고 있다. 송신측에서는 오류 검출을 위해 해쉬 값을 전송하며 수신측에서는 이 값을 검사하여 오류 여부를 확인한 후 OK 혹은 Error 신호를 보낸다. 만약, 송신측에서는 Error 신호를 수신하면 기존 데이터를 재전송하게 된다. 그러나 이 방법은 데이터 손실이나 회신 신호 분실에 따른 오류를 확인할 수 없으며 연속적으로 데이터를 보낼 수 없다는 단점을 가지고 있다.

NNSP사와 한국지역난방공사의 문헌[5] "복수의 통신 선로를 통해 데이터 재전송을 수행하는 일방향 송신/수신 장치 및 그것을 이용하는 데이터 전송 방법"에서는 복수의 회선을 사용하고 있지만 신호의 전달 방향은 모두 일방향 성질을 이용한다. 즉, Fig. 4에서 보는 바와 같이 수신측에서 수신된 데이터에 오류가 발생하면 하나의 회선을 절체하는 방식으로 OFF 신호를 보내게 된다. 송신측에서는 두 번째 채널이 절체된 사실을 확인하고 데이터를 재전송하게 된다. 이 방식에서 주목할 점은 수신측에서 두 번째 채널을 통해 OK 혹은 Error와 같이 두 가지 이상의 신호를 전송하는 것이 아니라, 채널 절체를 통해

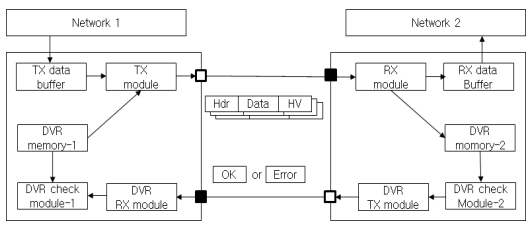

Fig. 3. Retransmission using OK or Error signal

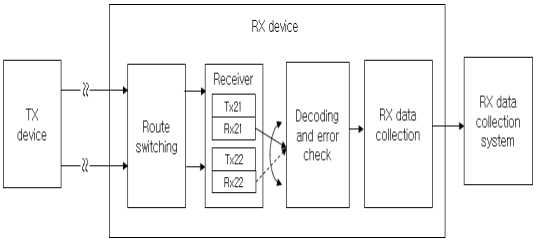

Fig. 4. Retransmission using only OFF signal

OFF 신호 한 종류만 사용하므로 두 채널의 신호는 모두 일방향으로 흐르도록 하고 있다는 것이다.

지금까지 제안된 대부분의 일방향 전송시스템에서는 전방향 오류 정정 부호를 이용하거나 전송 결과에 대한 회신을 이용한 재전송 기법을 이용한 오류 제어 기능만 고려하고 있으며 전송 데이터에 대한 기밀성 유지 기능은 제공하지 않고 있다.

따라서 본 논문에서는 일방향 네트워크에서 첫 번째 채널을 이용하여 데이터를 전송하며, 두 번째 채널을 이용하여 전송 결과를 회신하여 재전송 기법을 적용할 수 있는 물리적 환경하에서 통신의 신뢰성과 기밀성을 유지할 수 있는 기법을 제안하고자 한다. 또한, 제안 기법에서는 전송 효율을 높이기 위해 연속적인 데이터 전송을 수행함을 가정한다.

III. 연속적인 일방향 데이터 전송 기법

3.1 응답 기반의 일방향 데이터 전송

일방향 전송 데이터 보호를 위해 송신측과 수신측에 사전에 비밀 공유 키(pre-shard key)가 분배되어 있고 데이터는 이 키로부터 파생된 세션 키로 암호화하여 전송한다고 가정한다. 먼저, 송신측에서는 응용 서비스 데이터 단위(ASDU, Application Service Data Unit)를 만든 후 무결성 값을 생성하고 이를 암호화한 One-Way ASDU를 전송한다. 수신측에서는 데이터를 복호화하고 무결성을 검사한 후 수신 결과를 OK 또는 Error로 회신한다.

Fig. 5는 수신 데이터에 오류가 없을 경우 ASDU를 수신 버퍼에 저장하는 정규 일방향 모드(normal one-way mode)를 나타낸 것이다. 이 모드는 일반 네트워크 전송 모델 중 정지 후 대기(stop-and-wait)방식과 유사하게 하나의 전송 메시지를 보내고 하나의 응답을 받는 형태이다. 여기서 회신 신호는 오류가 없을 경우 OK 신호를 이용하거

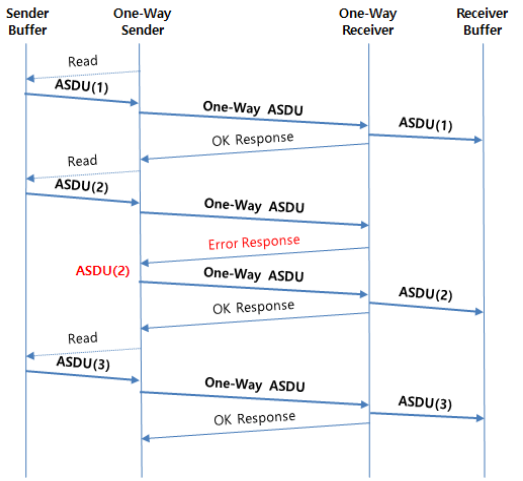

Fig. 5. Normal one-way mode with OK/Error response

나 일정 시간 동안 회신을 보내지 않는 방법도 있다. 또한, 오류가 발생했을 경우에는 Error 신호나 회신을 절체한 OFF 신호를 사용할 수도 있다. 송신측에서는 Error 신호나 OFF 신호가 오면 데이터를 재전송하게 된다.

일방향 통신 시 오류가 발생할 수 있는 상황은 아래와 같이 3가지로 요약할 수 있다.

① 송신측 데이터가 변조되었을 경우
② 송신측 데이터가 분실된 경우
③ 수신측 응답이 분실된 경우

송신측에서 OK 응답을 수신하면 다음 송신 버퍼의 데이터를 읽어 One-Way ASDU를 전송하지만 송신 데이터가 변조되어 Error 응답을 수신하면 이전에 전송한 One-Way ASDU를 재전송하게 된다.

일방향 전송 과정에서 또 다른 오류는 송신측의 One-Way ASDU가 분실되거나 수신측의 응답이 분실되었을 경우이다. 이 두 가지 경우에는 모두 송신측에 응답 신호가 도착하지 않으므로 타이머를 두고 응답 대기 시간(time out)을 체크해야 한다. 송신측에서 데이터를 전송 후 일정한 시간이 지나도록 응답이 오지 않을 경우 이전 One-Way ASDU를 재전송하게 된다.

Fig. 6은 전송 중인 데이터가 분실되거나 응답이 분실되었을 때 데이터를 재전송하는 상황을 나타낸 것이다. 여기서 중요한 점은 수신측에서 데이터가 정상적으로 수신되어 OK 응답을 보냈는데 이 신호가 분실된 경우이다. 이때 송신측은 이전의 ASDU를

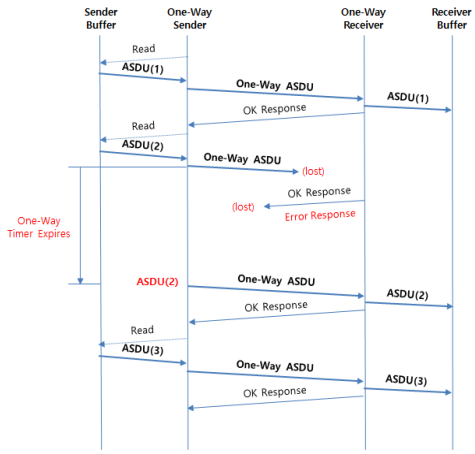

Fig. 6. Normal one-way mode with loss of data or response

보내지만 수신측에서는 이전의 ASDU인지 다음의 ASDU인지 구별하기 어렵다. 따라서 ASDU에는 데이터의 순서 번호를 같이 보내도록 하여 데이터의 중복 수신을 방지할 수 있도록 해야 한다.

3.2 연속적인 일방향 전송 데이터

일방향 시스템에서는 송신 장치와 수신 장치가 멀리 떨어져 있지 않고 같은 공간에 위치할 수도 있으며 전송 효율을 높이기 위해서는 Error 응답이나 OFF 신호만을 이용할 수도 있다. Aggressive one-way mode는 Fig. 7과 같이 One-Way ASDU가 정상이면 응답을 보내지 않고 데이터 변조 오류가 발생할 경우에만 Error (혹은 OFF) 응답을 보내도록 하는 프로토콜이다. 이때 중요한 점은 송신측에서는 Error 응답을 받았을 때 N개 이전의 ASDU부터 재전송해야 한다는 것이다.

여기서 Error 응답은 데이터 오류가 발생한 신호일 뿐 오류가 발생한 ASDU의 순서 번호 등의 정보를 포함하지 않으므로 송신측에서 충분한 수의 이전 데이터로 돌아가 N개 이전 ASDU를 재전송해야 한다. 수신측에서는 데이터의 순서 번호를 통해 이전 데이터를 재전송 받게 되고 변조된 데이터 이후의 데이터를 연속적으로 복구하게 된다. 만약, Fig. 8과 같이 전송 데이터가 중간에 분실되는 경우가 발생해도 순서 번호를 통해 데이터의 분실 유무를 체크할 수 있으므로 수신측에서는 Error 응답을 보내고, 송신측에서 충분한 수의 N개 이전으로 돌아가 ASDU

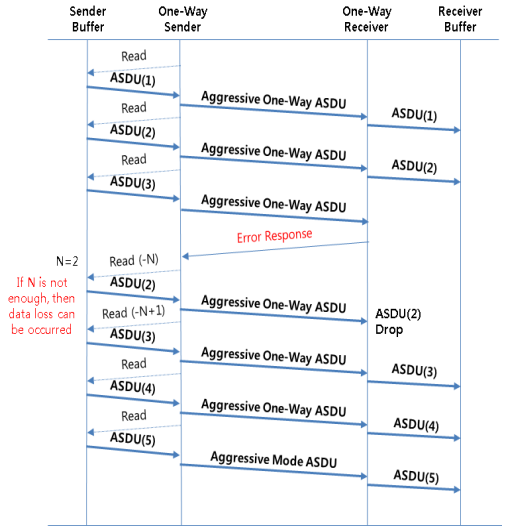

Fig. 7. Aggressive one-way mode with Error response

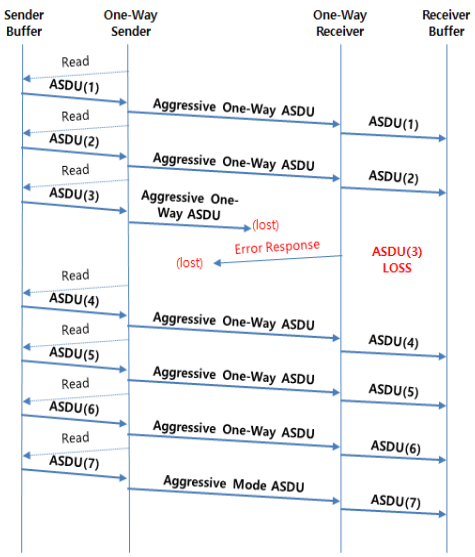

Fig. 8. Aggressive one-way mode with loss of data or response

를 재전송하면 문제를 해결할 수 있다.

문제는 Aggressive one-way mode에서 Error 응답의 유실이다. 이 경우 송신측에서는 연속해서 정상 데이터를 보내게 되므로 수신측에서는 오류 응답에 대한 재전송이 이루어지지 않음을 인지하여 다시 Error 응답을 보내게 된다. 이때에는 두 번째 Error 응답을 보낸 경우가 되므로 충분히 이전의 데이터가 재전송될 수 있도록 N의 크기를 설정해야

한다.

만약, 송신측에서 수신측까지의 전송 지연 시간이 t하고 회신 응답을 인지하는 시간을 f라고 하면 첫 번째 Error 응답이 접수되고 나면 최소한 $(t+f)$보다 이전에 보낸 ASDU를 재전송하여야 한다. 그런데 첫 번째 Error 응답이 분실된 경우를 가정하면 최소한 $2(t+f)$보다 이전에 보낸 ASDU를 보내야 한다. 따라서 Aggressive one-way mode 재전송 시에 보내야 하는 데이터는 Error 응답을 수신하고 나서 수신자가 충분히 중복된 데이터를 받을 수 있을 정도의 N개 이전의 ASDU를 송신해야 한다.

IV. 일방향 네트워크에서의 키 분배

4.1 세션 키 및 업데이트 키 갱신

암호화된 데이터의 일방향 통신을 위해서 처음부터 두 통신자는 공유 키를 분배하고 있음을 가정한다. 그 이후에는 통신이 있을 시마다 세션 키를 사용하거나 주기적으로 키를 갱신하는 절차가 필요하다. 즉, 송신측에서 세션 키(Session Key)나 업데이트 키(Update Key)를 생성하고 이 키를 이용하여 One-Way ASDU를 암호화 한 후 전송하게 된다. 일방향 네트워크에서 세션 키나 업데이트 키를 갱신하는 과정을 나타낸 것이 Fig. 9이다.

먼저, 새로운 키 분배를 위해서는 송신측에서 키 상태(Key Status) 정보를 수신측에 전달하여 One-Way SA(Security Association) 협상 과정을 수행한다. One-Way SA 협상 과정에서 주고받는 키 상태 정보는 Key Wrap 알고리즘, 암호화 알고리즘, 무결성 검증 알고리즘, 키 길이, 암호 모드 등을 포함한다. 일방향성을 가진 네트워크이므로 키 분배는 송신측에서 수신측으로 이루어진다. 또한, 수신측에서는 OK 또는 Error로 처리 결과를 응답할 수도 있으며 신호 절체를 통한 OFF 신호를 사용할 수도 있다. 전송 방식은 위에서 설명한 정규 일방향 모드를 사용하여 오류 제어 문제를 해결한다.

수신측에서는 송신측에서 보낸 키 상태 정보를 검사하여 암호 알고리즘 및 기존 키를 사용할 수 있으면 OK 응답을 보내고, 송신측에서 제시한 SA를 적용할 수 없으면 Error 응답을 전송한다. 송신측에서 Error 응답을 수신하면 키 상태 정보를 변경하여 Fig. 10과 같이 수신측에 다시 제시하며 OK 응답을 수신할 때까지 반복한다.

Key Status를 이용한 One-Way SA 협상이 완료되면 키 갱신 과정인 Key Change를 수행한다. Key Change는 송신측에서 다음 키로 사용할 난수(random number)를 발생시키고 무결성 값을 붙인 후 Key Wrap 알고리즘을 이용하여 암호화하여 전송한다. 여기에 사용되는 최초 키는 사전 공유 키이며 현재의 키를 가지고 다음에 사용될 키를 암호화하여 전송한다. Key Change 과정에서 데이터 오류가 발생하면 수신측에서는 Error 응답을 전송하고, 송신측에서는 새로운 난수를 발생시키고 동일한 방법으로 Key Change 패킷을 재전송한다.

Fig. 11은 송신측에서 전송한 Key Status 또는 Key Change 패킷이 분실되거나 수신측에서 전송한 OK/Error 응답이 분실되었을 때 처리 메커니즘

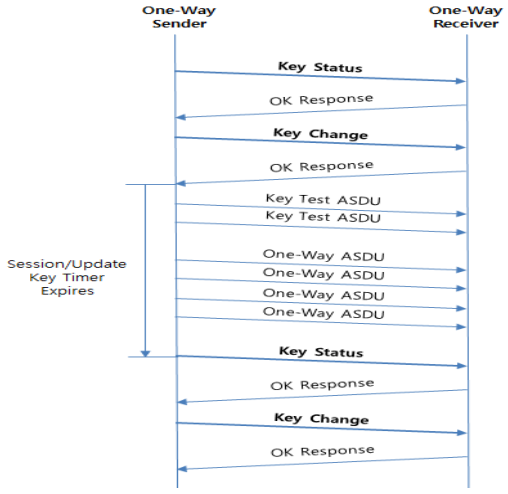

Fig. 9. One-way key distribution

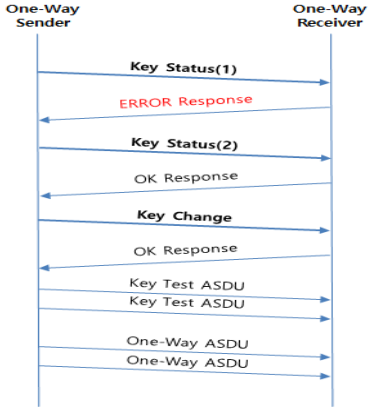

Fig. 10. Retransmission of Key Status

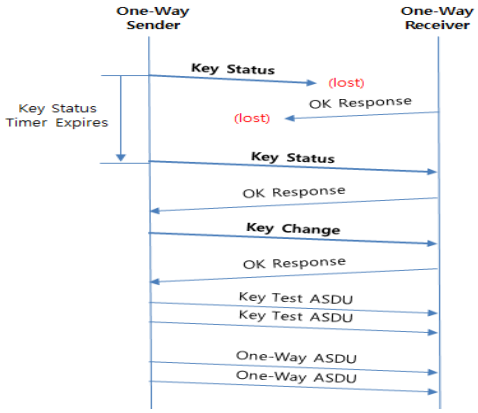

Fig. 11. Normal one-way mode with loss of Key Status or Response

을 나타낸 것이다. 두 경우 모두 송신측에서 타이머를 작동시켜 응답 대기 시간이 초과하면 새로운 Key Status 또는 Key Change를 재전송하는 방법을 사용한다.

지금까지 기술한 안전한 일방향 데이터 전송 과정을 정리한 것이 Fig. 12이다. 그림에서 보는 바와 같이 송신측에서는 Key Status 정보가 완전히 전송된 것을 확인하고 Key Change 정보를 송신하게 된다. Key Status의 전달 정보를 통해 SA 협상을 완료하고 실제 사용하는 키는 Key Change 정보를 통해 전송하게 된다. 그리고 Key Test용 ASDU를 통해 키가 정확히 공유된 것을 확인하면 새롭게 갱신된 키를 이용하여 실제 데이터를 암호화하여 전송한다.

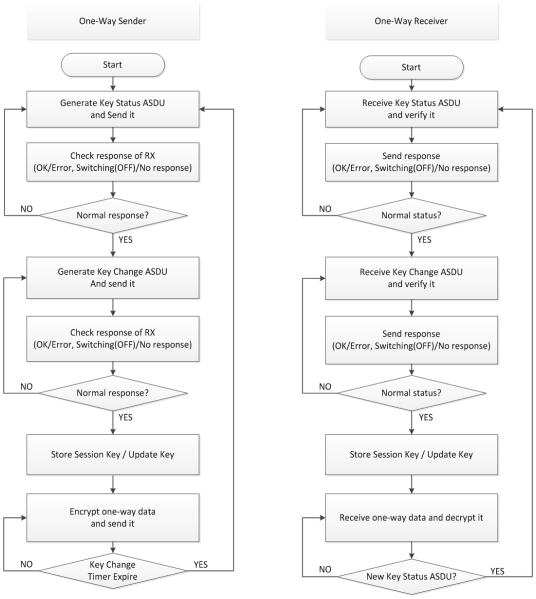

Fig. 12. Flow chart of secure one-way data transmission

상기한 바와 같이 두 통신자는 OK 응답이나 Error 응답과 같이 두 종류의 신호 회신을 통해 오류 제어를 수행할 수 있다. 그러나 회선 절체를 통해 OFF 신호만 전송할 수 있는 환경에서는 Key Status나 Key Change 정보에 대한 응답이 정상적이면 OFF 신호를 보내고 비정상적이면 타이머를 구동하여 일정시간이 지나고 OFF 신호가 없으면 재전송하는 기법을 사용할 수 있다. 이 경우 OFF 신호는 OK 신호와 동일하게 긍정 응답 신호(ACK, Acknowledgement)로 작용한다. 그러나 암호화된 실제 메시지를 보내는 과정에서는 오류가 발생했을 때만 OFF 신호를 보내는 방법을 사용할 수 있다.

따라서 실제 메시지를 보내는 과정에서는 OFF 신호를 부정 응답(NAK, Negative Acknowledgement) 신호로 사용할 수 있다. 즉, 응답 신호로 OFF 신호 하나만 사용할 경우에는 Key Status 정보 및 Key Change 정보에 대한 긍정 응답으로 사용할 수 있지만 데이터 전송 시에는 오류 발생을 회신하는 부정 응답 신호로도 해석될 수 있음을 주의하여야 한다.

4.2 일방향 통신용 서비스 데이터 단위

논문에서는 일방향 네트워크에서의 안전한 통신을 위하여 사용할 수 있는 ASDU 패킷 구조를 구성하였다. Fig. 13은 Key Status 정보 및 Key Change 패킷의 서비스 데이터 단위를 나타낸 것이다. Key Status 정보는 ASDU 식별자, ASDU 순서번호, 단방향 시스템 식별자, 보호 연관 데이터, 랜덤 데이터 길이, 의사 랜덤 데이터(Pseudo-random Data) 그리고 무결성 검사 값으로 구성된다. 이 중에서 보호 연관 데이터는 무결성 알고리즘, 암호 알고리즘, 키랩(Key Wrap) 알고리즘 및 관련 알고리즘 속성을 포함한다. 또한, 의사 랜덤 데이터는 난수 발생기를 통해 생성되는데 수신 장치에서 Key Change ASDU에 포함된 암호화된 의사 랜덤 데이터를 복호화하여 같은지 비교함으로써 암호 알고리즘과 암호 키 변경이 정상적으로 수행되었는지 검증하게 된다. 그리고 마지막 필드인 무결성 검사 값은 Key Status ASDU의 무결성을 검사하기 위해 사용된다.

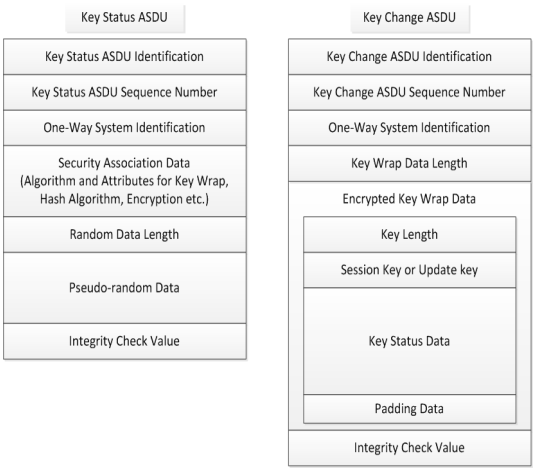

Fig. 13. Packet format of Key Status and Key Change ASDUs

Key Change 정보는 ASDU 식별자, ASDU 순서번호, 단방향 시스템 식별자, 키랩 데이터 길이(Key Wrap Data Length), 암호화된 키랩 데이터(Encrypted Key Wrap Data) 그리고 무결성 검사 값으로 구성한다. 이 중에서 키랩 데이터 길이는 암호화된 키랩 데이터의 길이를 의미하며, 암호화된 키랩 데이터는 키 길이, 세션 키 또는 업데이트 키, 키 상태 데이터를 키랩 알고리즘을 이용하여 암호화한 것을 나타낸다. 여기서 세션 키 또는 업데이트 키는 새로이 생성된 암호 키를 나타내며, 키 상태 데이터는 이전 Key Status ASDU 중에서 무결성 검사 값을 제외한 데이터이다.

암호화된 Key Status 데이터는 단방향 수신 장치에서 복호화되고 이전에 수신한 키 상태 데이터의 의사 랜덤 데이터와 비교하여 데이터가 정상적으로 수신되었는지 확인하는데 사용된다. 이와 같이 Key Change 패킷의 복호화 데이터가 정상적이고 무결성 검사 값이 이상이 없을 경우에는 새로운 키로 업데이트하여 사용하게 된다.

V. 결 론

최근 제어망과 같은 높은 보안성을 요구하는 네트워크에서 낮은 보안성을 가진 일반 네트워크쪽으로 데이터를 일방향으로 전송하는 기술이 주목을 받고 있다. 그러나 수신측에서 송신측으로 데이터 수신 결과를 OK 응답이나 Error 응답만으로 보내는 환경이나 회선 절체(OFF)와 같은 단일 신호만 보내는 경우에서는 신뢰성 있는 데이터 전달을 위한 많은 제약 사항이 존재하게 된다. 특히, 한쪽 방향으로만 데이터를 전송한다는 물리적 조건으로 인해 오류 제어 문제가 새롭게 이슈화 되고 있다.

본 논문에서는 데이터 수신 응답을 OK/Error와 같이 두 종류의 신호만 사용하거나 신호 절체 와 같은 단일 신호만 보내는 일방향 네트워크에서데이터를 연속적으로 보내는 방안을 제안하였다. 또한, 데이터 기밀성 및 무결성 제공을 위한 메커니즘을 제안하고 여기에 사용되는 세션 키나 업데이트 키의 갱신 방안을 제시하였다. 논문에서 제시한 일방향 데이터 전송 프로토콜은 고도의 보안성이 요구되는 공공망이나 민간 기반 시설을 연결한 네트워크에서 일반 업무망으로 데이터를 전송하는 일방향 네트워크 환경에서 매우 유용하게 활용할 수 있을 것으로 전망된다.

References

[1] M. Stevens and M. Pope, “Data diodes,” Electronics and Surveillance Research Laboratory (DSTO), Technical Report-DSTO-TR-0209, July 1995.

[2] M. Anderson, C. North, J. Griffin, R. Milner, J. Yesberg, and K. Yiu, “Starlight: interactive link,” Computer Security Applications Conference, IEEE computer society, Dec. 1996.

[3] M. Stevens, “An implication of an optical data diode,” Electronics and Surveillance Research Laboratory (DSTO), Technical Report- DSTO-TR-0785, May 1999.

[4] Korea Electric Power Corporation, “System for transferring data only in one direction,” KR Patent number : 10-1334240, Sep. 2012.

[5] NNSP Co. and Korea District Heating Co., “Unidirectional data transmitting/receiving device capable of re-transmitting data through plurality of communication lines, and method of transmitting data using the same,” KR Patent number : 10-1562309, March 2015.

[6] Waterfall Security Solutions, “Introduction to Waterfall unidirectional

security gateways: True Unidirectionality, True Security," Proprietary Information, Aug. 2012.
〔7〕 Fox-IT, "Fox DataDiode: A preferred solution for high-security real-time electronic unidirectional data transfer between networks," White Paper, Jan. 2008.
〔8〕 J. Menoher, "All data diode are not equal," Owl Computing Technologies White Paper, Sep. 2013.
〔9〕 K. Kim, Y. Jang, H. Kim, J. Yun, and W. Kim, "Physical one-way data transfer system design for control system network," Journal of KISS : Information Networking, vol. 40, no. 2, pp. 126-130, April 2013.
〔10〕 K. Kim, Y. Jang, H. Kim, J. Yun, and W. Kim, "Reply-type based agent generation of legacy service on one-way data transfer system," Journal of The Korea Institute of Information Security & Cryptology(JKIISC), vol. 23, no. 2, pp. 299-305, April 2013.
〔11〕 J. Park, E, Park, K. Kim, and J. Ha, "Data encryption and key distribution in the one-way network," Proceedings of Conference on Information Security and Cryptology-Winter(CISC-W'15), Vol. 15, No. 2, Dec. 2015.
〔12〕 National Institute of Standards and Technology, "FIPS PUB 180-4 (Secure Hash Standard)," March 2012.
〔13〕 R. Rivest, "The MD5 message digest algorithm," RFC 1321, April 1992.
〔14〕 Electronics and Telecommunications Research Institute(ETRI), "System and apparatus for transferring data only in one direction," KR Patent number : 10-1063152, Oct. 2009.

〈저자소개〉

하 재 철 (Jaecheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 졸업
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2007년 3월~현재: 호서대학교 컴퓨터정보공학부 정보보호전공 교수
2013년 1월~현재: 한국정보보호학회 부회장
2009년 1월~현재: 한국산학기술학회 이사
〈관심분야〉 암호 알고리듬, 네트워크 보안, 부채널 공격

김 기 현 (Kihyun Kim) 종신회원
1993년 2월: 경북대학교 전자공학과 졸업
1995년 2월: 경북대학교 전자공학과 석사
2011년 8월: 충북대학교 컴퓨터공학과 박사
2014년 5월~현재: (주)앤앤에스피 연구소장
2013년 3월~현재: 호서대학교 정보보호학과 겸임교수
〈관심분야〉 시스템 및 네트워크 보안, 보안 관제, 제어망 보안