Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.5, Oct. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.5.1129

제한적 양방향 통신 시스템 설계

김 동 욱,† 민 병 길‡
ETRI 부설연구소

Design of a Limited Two-Way Communications System

Dongwook Kim,† Byunggil Min‡
The Attached Institute of ETRI

요 약

물리적 단방향 송신만을 허용하는 단방향 전송 시스템은 백워드 링크를 물리적으로 제거하여 외부에서 네트워크를 통한 침입을 원천 차단한다. 이러한 단방향 전송 시스템은 역방향 송신 또는 양방향 통신이 필요한 환경에서는 적용하기 어렵다. 본 논문에서는 outbound TCP 양방향 통신을 허용하는 제한적 양방향 통신 시스템(LimTway, Limited Two-way communications system)을 제안한다. LimTway는 포워드 및 백워드 단방향 링크를 사용하며, 포워드 단방향 링크는 outbound UDP 트래픽의 단방향 송신을 위해 항상 활성화 상태로 유지되는 반면, 백워드 단방향 링크는 허용된 outbound TCP 세션이 설립된 동안만 활성화된다. 백워드 단방향 링크가 활성화 상태인 기간 동안 발생할 수 있는 외부로부터의 침입을 차단하기 위해, outbound TCP 트래픽 및 outbound UDP 단방향 트래픽만을 허용하도록 소프트웨어를 설계하였다.

ABSTRACT

Unidirectional data transmission system, which allows physical one way transmission, removes the backward link physically to prevent the intrusion from the outside through the network. However, the system is difficult to apply to the environment requiring either backward transmissions or bi-directional communications. In this paper, we proposed Limited Two-way communications system, called as LimTway, which only allows outbound TCP two-way communications. LimTway uses two one-way links(forward, backward). While the forward one-way link is staying to be activated so that an allowed outbound UDP traffic could be transmitted one-way always, the backward one-way link is activated while allowed outbound TCP sessions are established. In order to prevent the intrusion from the outside during the period, the software of LimTway is designed to allow only the transmissions of both outbound TCP two-way communication traffics and outbound UDP traffics.

Keywords: Unidirectional Data Transmission System, Limited Two-way communication system, forward one-way link, backward one-way link

I. 서 론

단방향 전송 기술 또는 시스템([1-7])은 한 네트워크(예, 내부망)에서 다른 네트워크(예, 외부망)로 물리적으로 단방향 전송만을 허용하는 기술이다. 단방향 기술은 산업 제어시스템 네트워크 등의 보안이 중요하며, 보안수준 구분이 필요한 시스템 사이에 적용되어 보안 수준이 높은 시스템의 보안 강화를 위해서 사용될 수 있다. 상용 단방향 전송 기술로는 Waterfall 사의 USG(Unidirectional Security Gateway)[1]와 Fox-IT사의 FFHDD(Fort Fox

Received(08. 14. 2017), Accepted(10. 12. 2017)
† 주저자, dwkim1980@nsr.re.kr
‡ 교신저자, bgmin@nsr.re.kr (Corresponding author)

Hardware Data Diode)[2] 및 Owl사의 Dual-Diode[4]가 있다.

단방향 전송 기술은 외부망에서 내부망으로의 물리적인 백워드 링크(backward link)를 제거하였기 때문에 종단간 TCP(Transport Control Protocol)의 적용이 불가능하다. 이를 해결하기 위해 단방향 전송 기술은 프록시 방식을 사용한다. Waterfall사의 경우 USG에 적용가능한 다양한 산업용 응용프로그램과 데이터베이스, 산업용 프로토콜들에 대한 프록시 솔루션들을 지원하고 있으며, Owl사 및 Fox-IT사도 이와 유사한 솔루션들을 지원하고 있다.

하지만, 기업이 내부망에서 외부망으로 단방향 기술을 적용함에 있어, 프록시 구현의 어려움으로 인해 기존에 사용하던 프로그램(비공개 전용 프로그램 등)을 변경없이 사용하는 것이 어렵거나 불가능할 수 있다. 또한, 내부망 장치들의 시스템 업데이트나 백신 업데이트 등을 위해 파일 수신이 필요할 수 있는데, 단방향 전송 기술은 이를 지원할 수 없다.

본 논문에서는 단방향 전송 기술을 적용하기 용이하지 않은 환경(예, 비정기적 파일수신, 비공개 전용 outbound TCP 프로그램 사용 등)을 지원하기 위해 제한적 양방향 통신 시스템(LimTway, Limited Two-way communications system)을 설계하였다. 제안하는 시스템은 outbound TCP 통신 및 outbound 단방향 통신을 허용한다. 이를 위해 내부망에서 외부망으로의 단방향 링크(포워드 단방향 링크)와 외부망에서 내부망으로의 단방향 링크(백워드 단방향 링크)를 각각 사용한다. 포워드 단방향 링크는 항상 활성화되어 있으나, 백워드 단방향 링크의 경우 outbound TCP 세션이 설립된 동안에만 활성화된다. 백워드 단방향 링크가 활성화 상태인 기간 동안 발생할 수 있는 외부로부터의 침입을 차단하기 위해, outbound TCP 트래픽 및 outbound UDP 단방향 트래픽만을 허용하도록 소프트웨어를 설계하였다. 또한 백워드 단방향 링크 활성화에 소요되는 시간동안 발생하는 패킷 손실을 제거하기 위해 버퍼링을 적용하였다.

본 논문의 나머지 구성은 다음과 같다. 2장에서는 배경, 해결해야 할 이슈, 단방향 전송 기술 개요 및 관련 연구에 대해서 살펴본다. 3장에서는 제안하는 제한적 양방향 통신 시스템 설계 내용, 제한적 양방향 통신 시스템 사용 시 트래픽 전송 과정 및 제한적 양방향 통신 시스템의 장점에 대해서 기술한다. 4장에서는 제안하는 시스템의 구현과 관련한 내용을 기술하며, 5장에서는 결론을 맺는다.

II. 배경, 이슈 및 관련 연구

2.1 배경 및 이슈

망분리는 두 개의 망(내부망, 외부망)을 물리적으로 분리하는 것으로 2012년 8월 개정된 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"에서 망분리 조치 의무화에 의해 본격적으로 시행되었다. 물리적 망분리는 외부망을 통한 내부망으로의 사이버공격 위협을 및 내부망의 자료 유출을 원천 차단할 수 있다 하지만, 업무 등에 의해 분리된 망의 내부망에서 외부망으로 혹은 그 반대방향으로의 데이터 전송에 대한 소요가 발생하여, USB 등의 휴대용 저장 매체 또는 망간자료전송 시스템 등을 사용하기 시작했다.

망간자료전송 시스템은 분리된 망을 연계하기 위해 내부망과 외부망의 양단 끝에 각각 설치되는 내부망용 전송통제서버 및 외부망용 전송통제서버와 두 개의 전송통제서버들을 연계하는 중간매체로 구성된다. 망간자료전송 시스템은 구성 방식에 따라 중계시스템 기반, 시리얼 연계방식, 공유스토리지 연계 방식으로 구분되나[10], 자료전송이나 스트림 연계(분리된 망간 존재하는 서버간 서비스 연계) 기능을 지원하는 점에서 유사하다. 하지만, 이러한 망간자료전송 시스템은 전송통제서버간은 물리적인 양방향으로 연결되어 있다. 즉, 일반적인 망간자료전송 시스템은 논리적인 단방향을 지원한다.

단방향 전송 기술은 망간자료전송 기술 중의 하나로 물리적인 단방향을 지원한다. 단방향 전송 기술은 물리적으로 백워드 링크를 사용하지 않아, 적용된 방향에 따라 내부망에서 외부망 혹은 그 반대방향으로의 자료전달만 가능하다. Fig.1.은 송신시스템(Transmission System)과 수신시스템(Reception System)으로 구성된 단방향 데이터

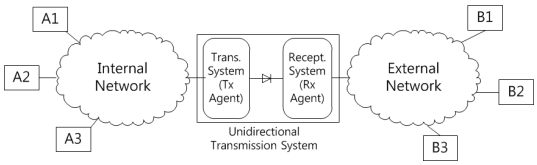


Fig. 1. An example of networks applying unidirectional data transmission system

전송 시스템을 적용한 예를 나타낸다. Fig.1.에서 내부망의 A1~A3에서 외부망의 B1~B3로 데이터 전송은 가능하나 B1~B3에서 A1~A3로 데이터 전송은 물리적으로 불가능함을 확인할 수 있다. 즉, 외부망으로부터의 침투를 허용하지 않으면서 내부망의 자료를 외부로 편리하게 전달할 수 있다. 하지만, 단방향 전송 기술은 백워드 링크가 없는 구조적인 한계점으로 인해 패킷 손실이 발생할 수 있으며[8], 또한 양방향 통신이 필요한 환경[11]에서는 단방향 기술만을 적용하기가 어렵다.

Waterfall사에서는 양방향 통신이 필요한 환경을 지원하기 위해 엄격한 통제를 기반으로 물리적으로 역방향 채널을 허용하는 다양한 기술(Secure Bypass, Inbound/Outbound gateway, FLIP)들을 제시하고 있다. 본 논문에서는 이러한 기술들과 유사하게 양방향 통신이 필요한 환경을 제한적으로 지원하는 시스템 설계를 목적으로 한다.

2.2 단방향 전송 기술 개요

본 절에서는 단방향 전송 기술의 동작과정에 대해서 살펴보자. 단방향 전송 기술에서 내부망에서 외부망으로의 TCP 기반 데이터 전송을 위해서는 프록시 및 복제 기술이 필요하다. Fig.2.는 TCP 기반의 데이터 전송을 위한 TCP 프록시 및 복제 기술에 대한 설명을 위한 그림을 나타낸다. 단방향 전송 시스템에서 TCP 프록시는 TCP destination 프록시(Tx Agent)와 TCP sender 프록시(Rx Agent)로 구성되어 있으며, 각각의 프록시는 TCP sender와 TCP destination과 세션을 맺는다. TCP sender가 전송하는 모든 데이터는 TCP destination 프록시(Tx Agent)로 전달된다. 데이터의 전송이 완료되거나, 전송 중에 Tx Agent는 Rx Agent로 데이터를 복제(replication)하며, 이 때 UDP 등의 단방향 통신을 사용한다. 마지막으로, TCP sender

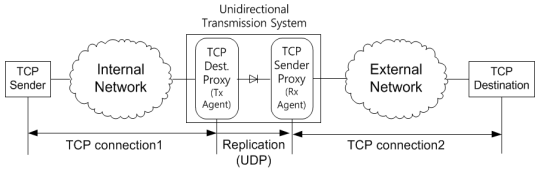


Fig. 2. An example using a TCP proxy and replication in an unidirectional transmission system

프록시는 TCP destination과 TCP session을 맺고 수신한 트래픽을 전송한다.

2.3 관련 연구

단방향 기술은 물리적인 백워드 링크를 제거하였기 때문에 end-to-end TCP를 적용하는 것이 불가능하므로, 패킷 손실[8]이 발생할 수 있다. 이러한 패킷 손실 문제를 완화하기 위해 다수의 기술[1,4,5,7,9]들이 제안되었다. [9]은 Tx Agent는 Rx Agent로부터 손실 패킷 정보를 수신(GPIO(General Purpose Input Output)기반 백워드 채널 사용)하여 재전송함으로써, 패킷 손실 문제를 해결하였다. 미리 정의된 목적으로 백워드 링크를 사용하는 방법과는 달리, 물리적 단방향을 그대로 유지하는 접근법으로 에러 정정 코드[1,4,5] 또는 중복 전송[7] 등을 활용하여 손실이 발생한 패킷을 정정할 수 있도록 한 방법들도 제안되었다.

양방향 통신이 필요한 환경에서는 단방향 기술만을 적용하는 것이 불가능하다. [11]은 많은 공장시스템들이 외부 시스템과의 인터페이스를 필요로 하며, 소프트웨어 업데이트 및 외부에서 안전한 원격 접속 등을 위해서도 외부망에서 내부망으로의 접근이 필요하다고 기술하고 있다. Waterfall사[1]는 양방향 통신이 필요한 정도 및 상황에 따라 활용가능한 다양한 기술(Secure Bypass, Inbound/Outbound gateway, FLIP)들을 개발하였다. Fig.3.은 Secure Bypass, Inbound/Outbound gateway, FLIP을 각각 나타낸 그림이다.

Secure Bypass(Fig.3.(a))는 단방향 장치와 함께 사용되는 장치로 긴급 시 양방향 통신을 사용할 수 있도록 bypass 기능을 지원하는 장치이다. 필요 시 내부망과 외부망간 양방향 네트워크 연결을 물리적으로 지원한다. 해당 장치는 하드웨어 기반 혹은 스케줄링 기반으로 동작할 수 있으며, 설정된 시간 혹은 기간 동안 사용 후에 자동으로 물리적으로 끊어진다. 사용자는 외부에서의 원격 접속 또는 소프트웨어 업데이트 등의 외부 연결이 필요한 경우 해당 장치를 활성화하여 사용할 수 있다. Secure Bypass는 양방향 통신이 비활성화되어 있는 동안은 단방향 장치와 동일한 보안 수준을 제공하며, 활성화되어 있는 동안은 방화벽만큼의 보안 수준을 제공할 수 있다.

Inbound/Outbound gateway(Fig.3.(b))는

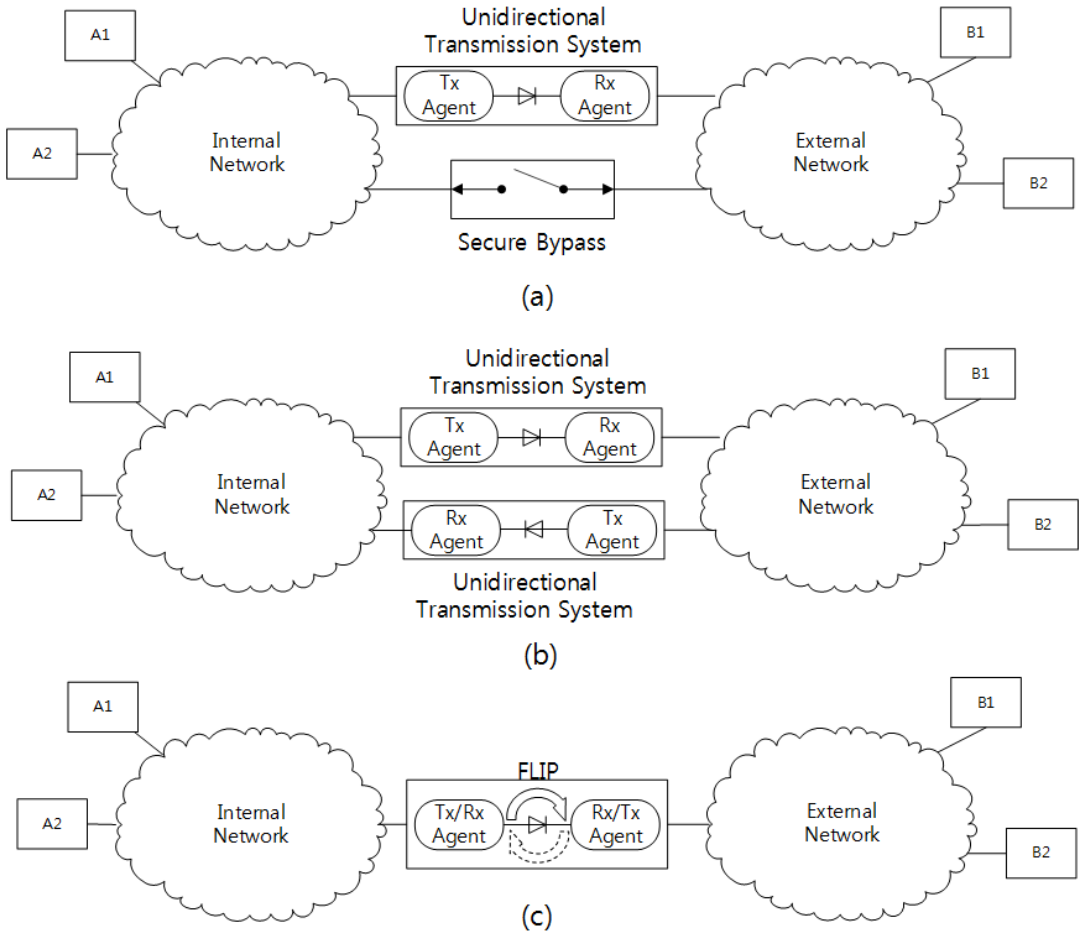


Fig. 3. Waterfall's various products for supporting the environment where bi-directional communications are required: (a) secure bypass, (b) Inbound/Outbound, (c) FLIP

2대의 단방향 장치를 물리적으로 분리된 위치에 설치하여 내부망에서 외부망으로 외부망에서 내부망으로 데이터를 각각 단방향으로 전달할 수 있도록 하는 장치이다. 이 장치를 사용하면, 단방향 기반 소프트웨어 업데이트파일을 외부망으로부터 수신할 수 있으나 원격접속 등의 대화형(interactive) 양방향 통신은 어렵다. 이론적으로 대화형 양방향 통신이 가능하지만, 내부자의 도움이 필요하다. 즉, 해당 장치를 사용한 환경에서는 원격 제어 공격(remote control attack)이 이론적으로는 가능하나, 현실적으로는 내부자의 지원이 필요하다.

마지막으로 FLIP(Fig.3.(c))은 스케줄에 따라 역방향으로 방향 전환("FLIP OVER")을 지원하는 방향 전환이 가능한 단방향 장치이다. FLIP은 컨트롤러에 의해 물리적으로 양방향 연결이 불가능하도록 구현되어 있다. 컨트롤러는 버튼 등의 물리적인 장치 혹은 스케줄링 등의 소프트웨어 기반으로 트리거링할 수 있다. FLIP을 사용한 환경에서는 원격 제어 공격이 원천적으로 불가능하다. 이는 방화벽 및 이동식 미디어보다 보안성이 강하며, waterfall의 Secure Bypass에 비해서도 보안성이 강하다.

본 논문에서는 outbound TCP 통신 및 outbound 단방향 통신을 필요로 하는 환경을 지원하는 제한적 양방향 통신 시스템(LimTway, (Limited Two way communications system)을 제안한다. 제안하는 시스템은 outbound TCP 양방향 통신이 필요한 프로그램들 중에 프록시 프로그램 구현이 어렵거나 불가능(SSL/TLS (Secure

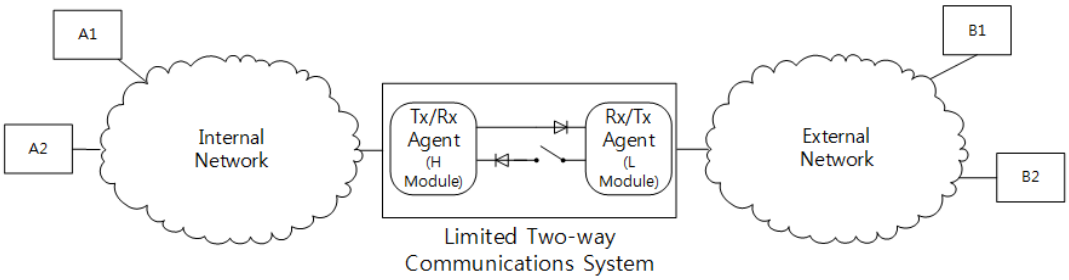


Fig. 4. LimTway overview

Socket Layer/Transport Layer Security)를 사용한 서버/클라이언트 프로그램 등)하거나 파일의 수신이 필요한 프로그램(백신 업데이트 등)에 적용되어 사용할 수 있다. 또한 Secure Bypass와 함께 사용하면 보안성을 더 강화할 수 있을 것으로 기대한다.

III. 제한적 양방향 통신 시스템 설계

본 장에서는 제안하는 제한적 양방향 통신 시스템(LimTway)에 대해서 상세히 설명한다.

Fig.4.는 LimTway를 적용한 네트워크의 예시를 나타낸다. LimTway는 기존의 FLIP 시스템과 유사하게 Tx/Rx Agent(H module) 및 Rx/Tx Agent(L module)로 구성되어 있다. Agent는 각각 3개의 NIC(Network Interface Card)을 가지고 있으며, 이 중 두 개의 NIC은 포워드 단방향 링크와 백워드 단방향 링크에 활용된다. 포워드 단방향 링크는 H module에서 L module로의 단방향 링크를 의미하며, 백워드 단방향 링크는 L module에서 H module로의 단방향 링크를 의미한다. 포워드 단방향 링크는 항상 활성화되어 있으며, 백워드 단방향 링크는 허용된 outbound TCP 세션이 설립된 동안만 활성화된다. 백워드 단방향 링크가 활성화 상태인 기간 동안 발생할 수 있는 외부로부터의 침입을 차단하기 위해, outbound TCP 트래픽 및 outbound UDP 단방향 트래픽만을 허용하도록 소프트웨어를 설계하였다.

세부 절에서는 LimTway의 H module(3.1)과 L module(3.2)에 대해 상세히 살펴본다. 3.3에서는 트래픽 전송 동안의 LimTway 동작과정에 대해서 설명하고, 마지막으로 3.4에서는 LimTway 장점에 대해 설명한다.

3.1 Tx/Rx Agent (H module)

Fig.5.는 LimTway의 전체 세부 구조를 나타낸다. 그림에서 볼 수 있듯이 H module은 Packet Processing, Proxy ARP, Packet Filtering(whitelist based/TCP session management table based), TCP Session Manager, NIC3 On/Off Manager 및 NIC2 Packet Buffering로 구성되어 있다. H module은 3개의 NIC을 탑재(NIC1, NIC2, NIC3)하고 있는데, NIC1의 경우 내부망과 연결되어 있으며, NIC2(NIC3)는 L module의 NIC2(NIC3)와 각각 단방향으로 연결되어 있다.

Packet Processing은 NIC1(내부망)으로부터 받는 패킷들과 NIC3(L module)로부터 받는 패킷들을 처리하는 기능을 수행한다.

NIC1으로부터 받는 패킷들을 처리하는 과정은 Table 1.과 같다. NIC1으로부터 수신한 패킷의

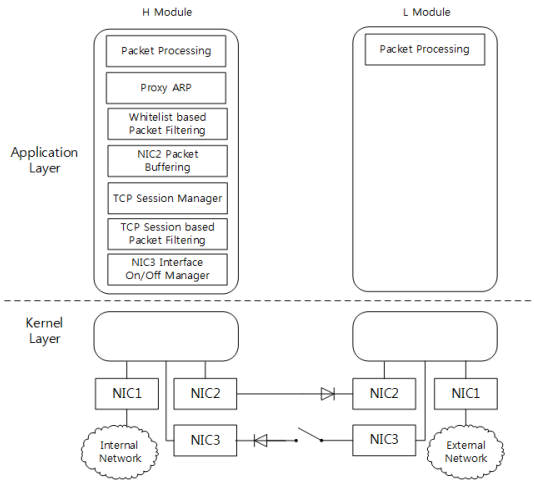


Fig. 5. Detailed LimTway Architecture

Table 1. NIC1 Packet Processing Procedure

```
Function. NIC1 Packet Processing Procedure
1: Definition:
2:   ST: TCP Session Management Table
3:   WL: Whitelist
4:   4T: 4 Tuple (Src/Dst IP, Src/Dst port)
5:   5T: 4T+ Protocol(TCP/UDP) type
6:   NS: NIC3 On/Off Status
7:   Buf: Buffer
8: Input
9:   P: a new packet captured in NIC1
10:Start
11:  if type(P)==ARP request
12:    Proxy ARP function
13:  end if
14:  if type(P)==IP
15:    if proto(P)==TCP && ∃a∈ST:4T in P==a
16:      TCP Session Manager function
17:      forwards P to NIC2
18:    else if ∃b∈WL:5T in P==b
19:      TCP Session Manager function
20:      if type(P)==TCP and NS is off
21:        NIC3 On Request
22:        Inserting P to Buf (buffering)
23:        Goto post-processing
24:      else forwards P to NIC2
25:      end if
26:   else delete P
27:  end if
28:  post-processing:
29:    waiting until NS is On
30:    forwards ∀packet in Buf to NIC2
31: End
```

type이 ARP request 패킷인 경우(Table 1.의 line 11) Proxy ARP 기능을 수행한다. IP 패킷(Table 1.의 line 14)이며 TCP 프로토콜인 경우, TCP 세션 관리 테이블(TCP session management table)에 항목이 존재하는지를 판단(Table 1.의 line 15)한다. 존재하는 경우, 해당 항목을 갱신(TCP Session Manager function)(Table 1.의 line 16)하고, 수신 패킷을 NIC2로 포워딩한다. 수신 패킷이 TCP 세션 관리 테이블에서는 관리되고 있지는 않으나 whitelist에는 존재하는 경우(Table 1.의 line 18), TCP 세션 관리 항목을 생성하여 테이블에 삽입(TCP Session Manager function)한다. NIC3 On/Off Status가 비활성화(Off)인 경우 NIC3를 활성화(On)할 것을 요청(NIC3 On/Off Manager)한 뒤, 패킷을 버퍼에 저장한다(Table 1.의 line 22-23). NIC3가 활성화되면, 버퍼링된 패킷들은 일시에 NIC2로 포워딩된다(*post-processing*). Whitelist에 존재하지 않는 패킷들은 모두 삭제된다(Table 1.의 line 26).

Table 2. NIC3 Packet Processing Procedure

```
Function. NIC3 Packet Processing Procedure
1: Definition:
2:   ST: TCP Session Management Table
3:   WL: Whitelist
4:   4T: 4 Tuple (Src/Dst IP, Src/Dst port)
8: Input
9:   P: a new packet captured in NIC3
10:Start
11:  if type(P)==IP and proto(P)==TCP
12:    if ∃a∈ST:4T in P==a
13:      TCP Session Manager function
14:      forwards P to NIC1
15:    else delete P
16:    end if
17:  else delete P
18:  end if
19: End
```

NIC3에서 수신한 패킷을 처리하는 과정은 Table 2.와 같다. NIC3로부터 수신한 패킷의 type이 IP 이외의 패킷은 모두 삭제하며(Table 2.의 line 17), IP 패킷인 경우, 현재 TCP 세션 관리 테이블에 항목이 존재하는 경우에만 해당 항목을 갱신(TCP Session Manager function)하고, NIC1으로 해당 패킷을 포워딩한다. 즉, TCP 세션 관리 테이블에 항목이 존재하지 않는 경우 NIC3로부터의 패킷은 드롭된다.

이제 Proxy ARP 기능을 살펴보자. Proxy ARP는 내부망의 장치가 외부망의 장치로 ARP request 패킷을 보낼 때 이를 대신하여 응답하는 기능이다. H module은 Fig.4.의 LimTway 적용 예시를 기반으로 Table 3.과 같은 Proxy ARP list를 설정할 수 있다. 예를 들어, Fig.4.의 A1이 Target IP address가 B1인 ARP request 패킷을 브로드캐스팅한다고 가정해보자. H module은 ARP request 패킷을 수신한 뒤 Proxy ARP

Table 3. An Example of an Proxy ARP list in H module

Sender IP Address	Sender MAC address	Target IP Address
A1's IP	A1's MAC	B1's IP
A1's IP	A1's MAC	B2's IP
A2's IP	A2's MAC	B1's IP

List에 있음을 판단하고, B1을 대신하여 A1으로 ARP reply 패킷을 전송한다. 이 때, ARP reply 패킷은 H module의 NIC1의 MAC address를 포함하고 있다. A1의 ARP request 패킷은 외부망으로 전달되지 않는다. ARP reply 패킷을 수신한 A1은 B1으로 패킷 전송 시, Destination MAC address에 H module의 MAC address를 설정하여 전송한다.

Whitelist 기반 패킷 필터링(Whitelist based Packet Filtering)은 NIC1으로부터 whitelist 정책에 위배되는 패킷을 수신하였을 때 필터링하는 기능을 수행한다. Whitelist는 기본적으로 많이 사용하는 5 tuple(Source IP, Source Port, Destination IP, Destination Port, Protocol)과 세션 허용시간(second)으로 구성된다. Fig.4.의 LimTway 적용 예시를 기반으로 〈A1's IP, 1000, B1's IP, 2000, TCP, 100〉과 같은 항목을 생성할 수 있다. 이는 A1의 1000번 포트에서 B1의 2000번 포트로 TCP 연결을 100초 동안 허용한다는 의미이다. 예를 들어 설명해보자. A1의 1000번 포트에서 B1의 2000번 포트로 TCP 연결을 수행하는 프로그램이 A1과 B1에 각각 동작하고 있다고 가정하자. 앞서 설명한 Proxy ARP 기능을 통해 H module은 A1이 B1으로 전송하는 패킷들을 수신할 수 있다. H module이 A1으로부터 패킷을 수신하면, 패킷에서 5tuple을 추출하여 whitelist에 상응하는 항목이 존재하는 경우에 한해 수신한 패킷을 NIC2를 통해 L module로 포워딩한다. Whitelist 내에 존재하지 않는 경우, 즉 whitelist 정책에 위배되는 경우 해당 패킷은 드롭한다.

TCP 세션 관리 테이블 기반 패킷 필터링(TCP 세션 관리 테이블 기반 패킷 필터링)은 NIC3로부터 TCP Session Manager에서 관리하는 TCP 세션 관리 테이블에 존재하지 않는 패킷을 수신하였을 때 필터링하는 기능을 수행한다.

TCP Session Manager는 TCP의 세션이 설립되고 종료될 때까지의 전주기를 관리하는 기능을 수행한다. TCP Session Manager는 whitelist의 5 tuple에 해당하는 TCP SYN를 NIC1으로부터 받으면 TCP 세션 관리 테이블에 하나의 항목을 생성한다. 이 때 whitelist의 세션 허용 시간을 참조하여 해당 항목의 잔여시간을 할당한다. 하지만, NIC3(외부망)로부터 TCP SYN를 받은 경우는 해당 패킷을 삭제한다. TCP Session Manager는 NIC1 또는 NIC3로부터 TCP FIN을 받으면, TCP 세션 관리 테이블의 항목들과 비교를 하여 해당 세션을 삭제한다. TCP의 세션은 TCP FIN/TCP FIN-ACK/TCP ACK으로 구성된 모든 메시지들이 차례로 교환되어야 종료되지만, 모든 메시지를 확인하는 것은 제한적 양방향 시스템에 부하를 줄 수 있으므로 TCP FIN을 수신하고 일정 시간 뒤(예, 1초)에 항목을 삭제하도록 설계한다. 즉, TCP Session Manager는 관리하고 있는 특정 항목에 대해, TCP FIN을 수신하거나 허용시간이 만료되면 삭제한다. 이 때, 관리하는 TCP 세션이 더 이상 없는 경우, NIC3 On/Off Manager에게 NIC3 상태를 Off로 전환할 것을 요청한다.

NIC3 On/Off Manager는 Packet Processing의 활성화(On) 요청 또는 TCP Session Manager의 비활성화(Off)요청에 따라 NIC3를 활성화(On) 또는 비활성화(Off)를 실행하는 기능과 NIC3의 상태를 관리하는 수행한다. NIC3의 'On'은 백워드 단방향 링크(H module ← L module)를 활성화한다는 의미이다. NIC3의 'Off'는 백워드 단방향 링크(H module ← L module)를 비활성화한다는 의미이다. H module은 whitelist의 정책에 허용된 TCP 세션이 설립되는 시점에 NIC3를 'On'하여 백워드 단방향 링크를 활성화한다. 그리고, 관리되는 세션이 하나밖에 없는 경우, TCP 세션이 종료되는 시점 혹은 세션 허용시간이 만료되는 시점에 NIC3를 'Off'하여 백워드 단방향 링크를 비활성화한다. TCP 세션이 설립되는 시점은 내부망의 장치로부터 TCP SYN를 받는 시점이다. TCP 세션이 종료되는 시점은 내부망의 장치 혹은 외부망의 장치로부터 TCP FIN을 받는 시점이다.

NIC2 Packet Buffering은 NIC3가 활성화되기 전까지 TCP 패킷을 버퍼링하는 기능을 의미한다. NIC3가 Off의 비활성화 상태에서 에서 On의 활성화 상태로 전환되기까지는 일정시간이 소요되는데 이 기간 동안 외부망의 장치가 전송하는 패킷(예, TCP SYN-ACK)이 손실될 수가 있다. 따라서 이러한 패킷 손실을 제거하기 위해서 NIC3가 On의 활성화 상태로 변경이 완료되기 전까지 NIC2로 포워딩 되는 패킷을 버퍼링하고 있다가, 활성화 상태로 변경되면, 버퍼링하고 있던 패킷을 NIC2로 전송한다. 이 때, TCP 세션 설립은 NIC3 활성화에 요구되는 시간동안 늦춰진다.

3.2 Rx/Tx Agent(L module)

이제 L module에 대해서 살펴보자. L module은 H module과 마찬가지로 3개의 NIC을 탑재(NIC1, NIC2, NIC3)하고 있는데, NIC1의 경우 외부망과 연결되어 있으며, NIC2는 H module의 NIC2와 NIC3의 경우 H module의 NIC3와 각각 단방향으로 연결되어 있다. 하지만, H module이 지원하는 다양한 기능과는 달리, L module은 Packet Processing 기능만 수행한다.

L module의 Packet Processing 기능은 NIC1(외부망)으로부터 받는 패킷들과 NIC2(H module)로부터 받는 패킷들을 포워딩하는 기능을 수행한다. NIC1으로부터 수신한 패킷들을 파싱하여 TCP 패킷인 경우 NIC3로 포워딩한다. NIC2로부터 수신한 패킷들은 파싱없이 NIC1으로 포워딩한다.

허용된 outbound TCP 세션 기반 NIC3의 On/Off를 제어하는 H module과는 달리, L module은 NIC3는 항상 On 상태이며, 제어되지 않는다. L module의 NIC3는 항상 H module로의 연결되어 있다고 판단한다. 즉, H module이 off의 상태이더라도 L module은 이를 식별하지 못한다. 따라서, H module의 On/Off 상태의 노출을 L module을 포함한 외부망으로부터 차단할 수 있다.

3.3 트래픽 전송 동안의 LimTway 동작 과정

3.3.1 Outbound TCP 세션 생성 및 종료 과정동안의 LimTway 동작 과정

Fig.4.와 같이 내부망과 외부망로 구성된 환경에서 A1의 2000번 포트에서 B1의 2000번 포트로 TCP 연결을 수행하는 프로그램이 있다고 가정하자. H module의 Proxy ARP list의 3 tuple(Sender IP Address, Sender MAC Address, Target IP Address)이 〈A1's IP, A1's MAC address, B1's IP)로 설정되어 있다. 또한 H module의 whitelist의 5 tuple이 〈A1's IP, 2000, B1's IP, 2000, TCP〉이며, 허용시간은 10초로 할당되어 있다고 가정한다. L module에는 어떠한 설정도 되어 있지 않다.

Fig.6.은 TCP 세션 생성과정동안의 LimTway

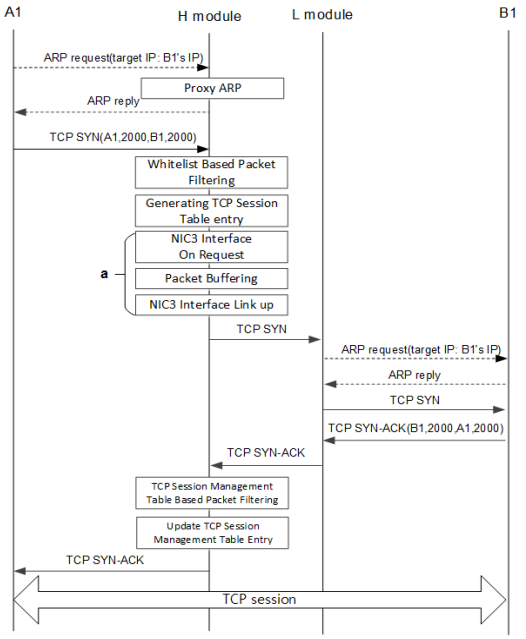


Fig. 6. The operation of LimTway during the outbound TCP session establishment

의 동작과정을 나타낸다. A1은 B1과 TCP 세션을 맺기 위해 TCP SYN를 생성하여 전송할 것이다. A1은 자신의 ARP table에 B1에 대한 MAC 주소를 가지고 있지 않을 경우, Target IP address를 B1의 IP로 설정한 ARP request 패킷을 내부망에 브로드캐스팅한다. H module은 ARP request 패킷을 수신한 뒤, B1을 대신하여 ARP reply 패킷을 전송한다. 이 때 ARP reply 패킷의 Sender MAC 주소는 H module의 NIC1의 MAC 주소로 설정되어 있다. ARP reply 패킷을 수신한 A1은 이제 TCP SYN를 H module로 전송할 수 있다.

TCP SYN를 수신한 H module은 5 tuple기반 whitelist 정책에 허용된 패킷인지를 식별한다. H module의 TCP Session Manager는 수신한 TCP SYN 기반으로 TCP 세션 관리 테이블에 항목을 생성하며, 허용 시간은 whitelist 정책의 허용 시간 필드를 참조한다.

이와 동시에, NIC3 On/Off Manager에게 NIC3 On을 요청하며, NIC3 On/Off Manager는 NIC3를 활성화한다. H module은 수신한 TCP SYN를 NIC2로 포워딩하여 L module로 전송한다. H module은 NIC3의 활성화가 완료되기 전까지는 L module로부터 데이터를 수신할 수 없다

(Fig.6.에서 'a' 시간). 즉, TCP SYN에 대한 응답 메시지인 TCP SYN+ACK의 손실이 발생할 수도 있는데, 이를 위해서 H module의 NIC3의 활성화가 완료되기 전까지 H module에서 TCP SYN를 버퍼링한다. H module NIC3의 활성화가 완료되면, H module은 버퍼링하고 있던 TCP SYN를 L module로 전송한다.

이제, L module은 H module로부터 TCP SYN를 수신하고, 이를 외부망으로 전송한다. 이 때 L module은 TCP SYN의 destination IP인 B1에 대한 MAC 주소를 가지고 있지 않으므로, ARP 과정을 통해 B1의 MAC 주소를 획득한 뒤 TCP SYN를 목적지인 B1으로 전송한다. B1이 TCP-SYN에 대한 응답으로 TCP SYN-ACK을 A1으로 전송하며, destination MAC 주소는 L module의 NIC1 MAC주소로 설정한다. L module은 TCP SYN-ACK을 수신하며, NIC3로 포워딩한다. H module의 NIC3가 활성화 상태이므로, TCP SYN-ACK을 수신할 수 있으며, 또한 TCP 세션 관리 테이블에 관리되고 있으므로, A1으로 정상 전송될 수 있다. H module은 해당 TCP 패킷에 대해 TCP 세션 관리 테이블을 갱신한 뒤 A1으로 전송한다.

Fig.7.은 Fig.6.에서 설립된 TCP 세션의 종료

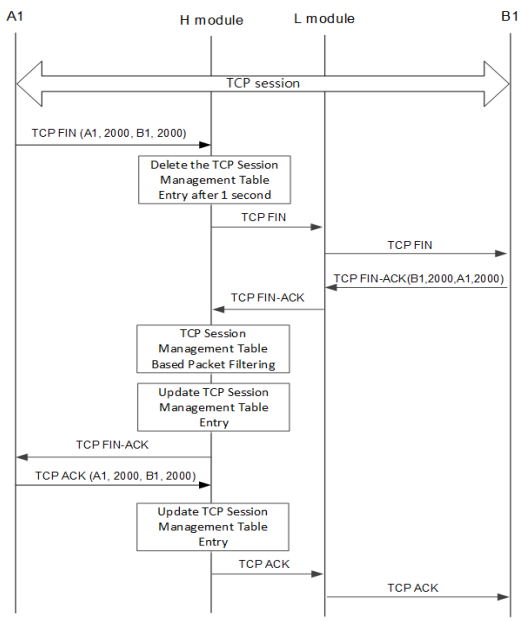


Fig. 7. The operation of LimTway during the outbound TCP session termination

과정동안의 동작과정을 나타낸다. A1은 B1과 TCP 세션을 종료하기 위해 TCP FIN을 생성하여 전송할 것이다. A1은 ARP table에 B1 MAC 주소(H module의 MAC 주소)를 알고 있으므로, ARP 과정 없이 TCP FIN을 H module로 전송할 수 있다. H module은 해당 TCP 세션에 대한 관리 항목을 1초 뒤에 TCP 세션 관리 테이블에서 삭제하며, TCP FIN을 L module을 통해 B1으로 전송한다. B1은 TCP FIN에 대한 응답으로 TCP FIN-ACK을 전송하며, H module은 이를 수신하고, TCP 세션 관리 테이블 based packet filtering을 수행한다. TCP FIN-ACK의 세션이 TCP 세션 관리 테이블에 관리되고 있으므로, 해당 table을 갱신한 뒤 A1으로 전송한다. 마찬가지로 A1이 전송하는 TCP ACK도 table을 갱신한 뒤 B1으로 전송된다.

3.3.2 Outbound UDP 패킷 전송과정 동안의 LimTway 동작 과정

Fig.4.와 같이 내부망과 외부망으로 구성된 환경에서 A2의 1000번 포트에서 B2의 1000번 포트로 UDP 패킷을 전송하는 프로그램이 있다고 가정하자. H module의 Proxy ARP list의 3 tuple(Sender IP Address, Sender MAC Address, Target IP Address)이 〈A2's IP, A2's MAC address, B2's IP)로 설정되어 있다. 또한 H module의 whitelist의 5 tuple이 〈A2's IP, 1000, B2's IP, 1000, UDP〉이며, 허용시간은 없다고 가정한다. L module은 어떠한 설정도 되어 있지 않다.

A2은 B2에게 UDP 패킷은 전송하기에 앞서 B2에 대한 MAC주소가 없을 경우 Fig.6.의 ARP 동작과정을 수행할 것이다. 이후 H module은 A2가 전송하는 UDP 패킷을 수신하며, whitelist 기반 패킷 필터링을 수행한다. 해당 UDP 패킷은 허용된 패킷이므로 L module로 전송하며, L module은 B2와의 ARP동작과정 후에 B2로 UDP 패킷을 전송한다.

3.4 LimTway 장점

본 절에서는 LimTway 사용 시의 이점에 대해서 설명한다. LimTway는 Fig.5.와 같은 하드웨어 구

조 및 Table 1. 및 Table 2.와 같은 소프트웨어 설계를 기반으로 다음의 장점을 가진다.

첫째, LimTway는 outbound TCP 및 UDP에 대해서만 허용한다. 즉, outbound TCP 세션이 없는 동안(NIC3 Off)은 inbound 트래픽 수신이 하드웨어적으로 불가능하며, outbound TCP 세션이 설립된 기간 동안(NIC3 On)은 소프트웨어적으로 불가능(수신된 inbound 트래픽 중 TCP SYN 및 UDP는 Table 2.의 line 11과 12의 동작과정에서 삭제)하다.

둘째, 외부망(L module 포함)의 장치에서 H module의 NIC3 활성화(On)/비활성화(Off) 상태의 명시적인 판단은 불가능하다. 공격자는 트래픽 분석을 통해 활성화 상태의 추측은 할 수 있으나, 이는 H module에서 가짜 트래픽(fake traffic)을 생성하여 전송함으로써 추측 성공 가능성을 낮출수 있다.

또한, 외부망에서 H module의 관리 페이지, ftp, telnet, ssh에 대한 접속이 어렵다. 외부망의 장치에서 H module의 관리 페이지 접속을 위해서는 H module의 routing table 및 ARP table의 변경이 필요하다. 즉, 관리자의 별도 설정없이도 외부망의 공격자가 H module로의 네트워크를 통한 접속을 차단할 수 있다.

마지막으로, 내부망의 장치 및 H module이 공격에 노출될 시간을 outbound TCP가 존재하는 동안으로 줄일 수 있다. 즉, 방화벽 대비 시간 측면에서의 attack surface를 줄이는 효과가 있다. 예를 들어, 1일에 100Mbytes의 파일 수신이 필요한 경우, 약 8초(100Mbps link기준)의 시간동안만 백워드 단방향 링크가 활성화되며, 이는 1일의 0.009%에 해당하는 시간이다.

IV. 제한적 양방향 데이터 통신 시스템 구현

본 장에서는 제한적 양방향 데이터 통신 시스템을 구현한 내용에 대해서 설명한다. H module과 L module의 구현은 각각 라즈베리파이2를 사용하였다. 라즈베리파이2는 하나의 이더넷 포트를 제공하므로, 구현에 필요한 나머지 2개의 이더넷 포트는 AX88179 chipset 기반 USB-to-Ethernet을 활용하였다. 각 이더넷은 10/100base-T급의 이더넷이다. 그리고 고속의 패킷 캡쳐를 위해 PF_RING[12]을 사용하였다.

먼저, H module의 NIC2(또는 L module의 NIC3)에서 L module의 NIC2(또는 H module의 NIC3)로의 물리적 단방향 링크 구현에 대해서 살펴보자. 10/100base-T의 경우 TX/RX 가 물리적으로 구분되어 있어 케이블의 RX를 제거하는 것만으로 단방향 구현이 가능하다. 하지만, 이더넷이 정상 통신하기 위해서는 H module의 NIC2(또는 L module의 NIC3) 및 L module의 NIC2(또는 H module의 NIC3)는 상호 연결되어 있다고 판단해야 한다. 그러나, H module의 NIC2에서 RX를 제거하면, 상호 연결 되어 있음을 판단하는 것이 불가능하다. 이를 해결하기 위해 keystone jack을 사용하였다. Keystone jack은 2개의 connector (RJ-45, punch down)로 구성되어 있다. keystone jack을 이용하여 "H module NIC2 ↔ KeyStone Jack(KJ1) ↔ KeyStone Jack(KJ2) ↔ L module NIC2" 및 "L module NIC3 ↔ KeyStone Jack(KJ1) ↔ KeyStone Jack(KJ2) ↔ H module NIC3"으로 단방향 이더넷 링크를 구성하였다. KJ1의 TX+ 및 TX-를 KJ1과 KJ2의 RX+ 및 RX-로 연결하여, loop back과 물리적 단방향을 구현하였다.

일반적으로 이더넷은 초기화 과정에서 auto negotiation을 수행한다. 이는 연결되어 있는 상대방의 전송 속도(10Mbps/100Mbps/1Gbps) 및 통신 방식(Full Duplex/Half Duplex)등에 대한 정보가 없는 상황에서 자동으로 가장 적합한 전송 속도 및 통신 방식으로 설정하는 기술을 의미한다. Auto negotiation을 위해서는 장비간 양방향 통신이 이루어져야 하므로, 단방향 링크 구간에서는 활용이 불가능하다. 이를 해결하기 위해, ethtool을 사용하여 H module과 L module의 모든 NIC은 auto-negotiation 기능을 off하고, 모든 NIC의 전송속도 및 통신 방식을 100Mbps/Full duplex로 고정 설정하였다.

PF_RING[12]은 ring 버퍼를 사용하여 기존의 libpcap의 성능을 개선한 NAPI(New API)이며, 현재는 100Gbps까지 지원하는 PF_RING ZC(Zero Copy)[13]가 개발되었다. ntop 웹페이지는 관련 source code 및 사용법 등을 공개하고 있다.

제한적 양방향 통신 시스템의 H module과 L module의 소프트웨어는 라즈비안 운영체제에서 C 언어를 사용하여 구현하였다. H module에서 패킷 버퍼링 기능을 사용한 결과 버퍼링 기능을 사용하지

않았을 때와 비교하였을 때, TCP 세션이 빠르게 설립되는 것을 확인할 수 있었다. 버퍼링을 하지 않을 경우 NIC3의 link up에 소요되는 시간보다 H module에서 TCP SYN의 목적지까지의 RTT(round trip time)가 작은 경우에 첫 번째 TCP SYN에 대한 응답인 TCP SYN-ACK은 H module에서 수신할 수 없다. Fig.4.와 같은 테스트 환경을 구축하여 테스트한 결과 link up 시간은 500ms 이상이 소요되었으며, RTT는 link up 시간 대비 매우 적은 시간이 소요되어, 첫 번째 TCP SYN-ACK의 손실이 발생하였다. 이로 인해 송신측에서는 TCP SYN를 재전송하게 되며, 결국 TCP 세션이 설립되는 시간이 TCP SYN를 재전송까지 소요되는 시간동안 늦춰지게 된다. 패킷 버퍼링 기능을 사용할 경우 TCP SYN-ACK의 손실을 제거할 수 있음을 확인하였다.

V. 결 론

본 논문에서는 outbound TCP 양방향 통신이 필요한 환경을 지원하기 위해 제한적 양방향 통신 시스템(LimTway)을 제안하였다. LimTway는 백워드 단방향 링크(H module ← L module) 의 활성화/비활성화 제어를 통해 outbound TCP 세션을 지원하며 외부의 침입을 효과적으로 차단한다. 또한, H module에서 버퍼링을 사용하여 TCP SYN-ACK 패킷의 손실을 제거하였다. 라즈베리파이 기반 구현 및 실험을 통해 제안하는 시스템의 효과를 테스트하였다. 향후 단방향 링크 활성화에 소요되는 시간을 최소화하는 방안에 대해서 연구할 예정이다.

References

[1] Waterfall One-Way. [Online]. Available: http://www.waterfallsecur-ity.com

[2] Fox-IT, "Fox DataDiode: A Pereferred Solution for high-security real-time electronic unidirectional data transfer between networks," White paper, Jan. 2008.

[3] J. Menoher, "All Data Diodes Are Not Equal", White Paper, 2013.

[4] Dual diode. [Online]. Available: http://www.owlcti.com

[5] Y. Heo, B. Kim, D. Kang, S. Shon, and J. Na, "A Design of Unidirectional Security Gateway for Enforcement Security and Reliability for Transfer Data", The Korean Institute of Communications and Information Sciences, pp.827-828, Jan. 2016.

[6] K. Kim, Y. Chang, H. Kim, J. Yun, and W. Kim, "Physical One-way Data Transfer System Design for Control System Network", Journal of KISS: Information Networking, 40(2), pp.126-130. Apr. 2014.

[7] D. Kim and B. Min, "Design of a Reliable Data Diode System", Journal of the Korea Institute of Information Security & Cryptology, 26(6), pp. 1571-1582, Dec. 2016.

[8] Lin Honggang, "Research on Packet Loss Issues in Unidirectional Transmission", Journal of Computers, vol. 8, no. 10, pp. 2664-2671, Oct. 2013.

[9] K. Kim, J. Yun, H. Kim, M. Jung, W. Kim, E. Park, and S. Park, "Physical One Direction Communication Device and Method Thereof", Korea Patent No. 10-1593168, Feb. 02, 2016.

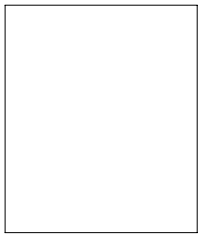
[10] H. Lee, D. Cho, and K. Kou, "A Study of Unidirectional Data Transmission System Security Model for Secure Data transmission in Separated Network", Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol.5, no.6, pp.539-547, Dec. 2015.

[11] Sid Snitkin, "Unidirectional Security Gateways Reduce Risk of Industrial Cyber Attacks", ARC View, Jul. 2015.

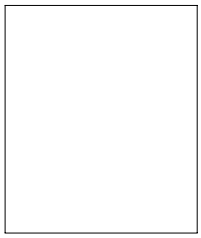
[12] PF_RING, www.ntop.org/products/packet-capture/pf_ring/

[13] PF_RING ZC, www.ntop.org/products/packet-capture/pf_ring/pf_ring-zc-zero-copy

〈저 자 소 개〉



김 동 욱 (Dongwook Kim) 정회원
2005년 2월: 경북대학교 컴퓨터공학과 학사
2012년 2월: 포항공과대학교 컴퓨터공학과 박사
2012년 4월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 통신공학, 제어시스템 보안, 정보보호



민 병 길 (Byunggil Min) 정회원
2002년 2월: 충북대학교 컴퓨터공학과 학사
2004년 2월: 포항공과대학교 컴퓨터공학과 석사
2004년 3월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 제어시스템 보안, 침입탐지 시스템, 취약성 분석