IPv6 환경에서의 일방향 통신 알고리즘에 대한 연구★

고 근 호*, 안 성 진**

요 약

1990년대 초반에 IETF(Internet Engineering TaskForce)는 IPv4의 주소 고갈 문제에 대한 임시해결책인 CIDR(Classless Inter-Domain Routing), NAT, 사설 IP 주소 등의 도입과 함께 기존 IPv4 주소 체계에서의 많은 단점들을 수정 및 보완할 수 있는 새로운 주소체계 도입에 관한 논의를 시작하였다. 그 결과 새로운 주소 체계와 관련된 다양한 표준안들이 제안되었는데, 이들 중 가장 발전 가능성이 높은 방안으로 SIPP(Simple Internet Protocol Plus)가 채택되어 지금의 IPv6로 발전하였다. 기존의 IPv4에서 실시간 데이터의 처리 능력과 QoS 관련 성능, 보안, 라우팅의 효율성 등의 많은 분야와 관련하여 부족했던 부분들이 수정 및 보완됨과 동시에 새로운 개념들이 도입되었다. 하지만 IPv6 환경에서도 보안을 위협할 만한 다양한 요소들이 존재하며, 이에 따라 안정적인 데이터 통신 환경의 필요성이 꾸준히 제기되어 왔다. 본 논문에서는 일방향으로 데이터를 전송하면 불확실하고 잠재적인 위협 요소로부터 시스템을 보호할 가능성이 높아진다는 점에 착안하여, IPv6 환경에서의 일방향 통신 알고리즘을 개발하였다. 먼저 기반 환경인 IPv6 및 ICMPv6에 대해 조사 및 분석하고 그에 따른 해결방안인 일방향 통신 알고리즘을 제시한다.

A Study on the Algorithms for One-way Transmission in IPv6 Environment

Keun Ho Koh*, Seong Jin Ahn**

ABSTRACT

In the early 1990s, IETF(Internet Engineering TaskForce) had started the discussion on new address protocol that can modify and supplement various drawbacks of existing IPv4 address protocol with the introduction of CIDR(Classless Inter-Domain Routing) which is a temporary solution for IPv4 address depletion, NAT, private IP address. While various standards related to new address protocol has been proposed, the SIPP(Simple Internet Protocol Plus) was adopted among them because it is regarded as the most promising solution. And this protocol has been developed into current IPv6. The new concepts are introduced with modifying a lot of deficiencies in the exisitng IPv4 such as real-time data processing, performance on QoS, security and the efficiency of routing. Since many security threats in IPv6 environment still exist, the necessity of stable data communication environment has been brought up continuously. This paper deveopled one-way communication algorithm in IPv6 based on the high possibility of protecting the system from uncertain and potential risk factors if the data is transmitted in one way. After the analysis of existing IPv6 and ICMPv6, this paper suggests one-way communication algorithm as a solution for existing IPv6 and ICMPv6 environment.

Key words : IPv6, ICMPv6, One-Way Transmission

접수일(2017년 11월 13일), 수정일(1차: 2017년 12월 22일), 게재확정일(2017년 12월 31일)

★ 본 연구는 과학기술정보통신부 및 정보통신진흥센터 의 SW컴퓨팅산업원천기술개발 사업의 일환으로 수행하 였음. [R0126-15-1095, 사이버·물리시스템에서의 물리적 단방향 보안 게이트웨이 개발]

* 성균관대학교 컴퓨터교육과

** 성균관대학교 컴퓨터교육과

1. 서 론

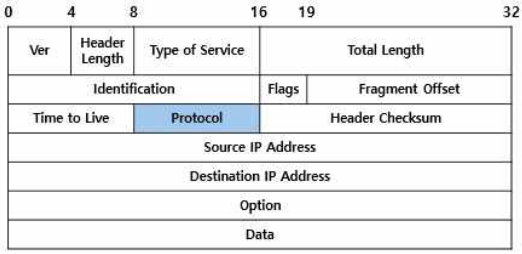
1990년대 초반에 IETF(Internet Engineering TaskForce)는 IPv4의 주소 고갈 문제에 대한 임시해결책인 CIDR(Classless Inter-Domain Routing), NAT, 사설 IP 주소 등의 도입과 함께 기존 IPv4 주소 체계에서의 많은 단점들을 수정 및 보완할 수 있는 새로운 주소체계 도입에 관한 논의를 시작하였다. 그 결과 새로운 주소 체계와 관련된 다양한 표준안들이 제안되었는데, 이들 중 가장 발전 가능성이 높은 방안으로 SIPP(Simple Internet Protocol Plus)가 채택되어 지금의 IPv6로 발전하였다. 기존의 IPv4에서 실시간 데이터의 처리 능력과 QoS 관련 성능, 보안, 라우팅의 효율성 등의 많은 분야와 관련하여 부족했던 부분들이 수정 및 보완됨과 동시에 새로운 개념들이 도입되었다. 하지만 IPv6 환경에서도 보안을 위협할 만한 다양한 요소들이 존재하며, 이에 따라 안정적인 데이터 통신 환경의 필요성이 꾸준히 제기되어 왔다.

본 논문에서는 일방향으로 데이터를 전송하면 불확실하고 잠재적인 위협 요소로부터 시스템을 보호할 가능성이 높아진다는 점에 착안하여, IPv6 환경에서의 일방향 통신 알고리즘을 개발하였다. 먼저 기반 환경인 IPv6 및 ICMPv6에 대해 조사 및 분석하고 그에 따른 해결방안인 일방향 통신 알고리즘을 제시한다.

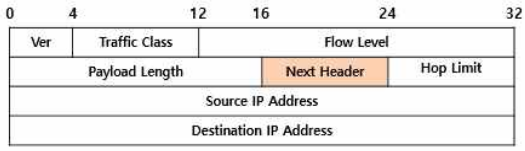
2. IPv6/ICMPv6 분석

2.1 IPv6

IPv6는 Internet Protocol Version 6의 줄임말이며, 현재 사용되고 있는 IP 주소체계인 IPv4의 여러 단점을 개선하기 위해 새롭게 개발된 IP 주소체계를 뜻한다. IPv6는 IPv4에 비해 많은 특성들이 수정 및 보완되었는데, 주요 변경사항 중 하나로 IPv6 헤더는 <그림 2>와 같이 기존 IPv4 헤더보다 구조가 단순해짐으로써 성능이 향상되었다.



<그림 1> IPv4 헤더의 구조



<그림 2> IPv6 헤더의 구조

또한 IPv6에서는 패킷을 전송할 때 일반적으로 기본 헤더로만 구성된 패킷을 사용하다가 필요시 'Next Header'의 값에 따른 확장 헤더를 기본헤더 뒤에 추가시킨다. <표 1>는 'Next Header'의 값에 따른 확장헤더의 종류를 나타낸다.

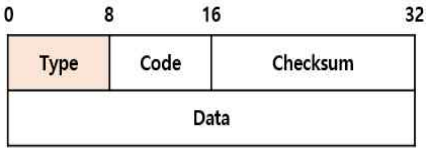
<표 1> 'Next Header'의 값에 따른 확장헤더의 종류

value	Header
0	Hop-by-Hop Options Header
6	TCP
17	UDP
41	Encapsulated IPv6 Header
43	Routing Header
44	Fragment Header
50	Encapsulating Security Payload
51	Authentication Header
58	ICMPv6
59	No Next Header
60	Destination Options Header

2.2 ICMPv6

또한 본 연구에서는 'Next Header'의 값이 58인 ICMPv6에 주목하였다. IPv6의 특성상 송신 노드가 수신 노드로 데이터를 전송해도, 송신 노드는 수신

노드로부터 데이터가 잘 도착했는지에 대한 응답을 받지 못한다. ICMPv6는 이를 보완하기 위해 IPv6를 통한 데이터 패킷이 제대로 전송되었는지, 도중에 손상 및 분실되었는지 등에 대한 피드백을 준다. ICMPv6의 패킷 구조는 <그림 3>과 같다.



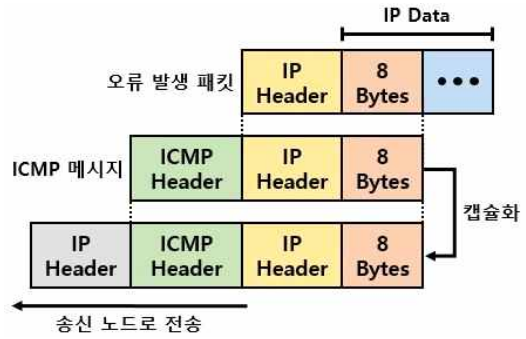
<그림 3> ICMPv6 패킷의 구조

ICMPv6 메시지의 종류는 'Type'의 값에 따라 여러 가지로 구분되는데 0부터 127번까지는 에러(Error) 메시지로 정의되고, 128번부터 255까지는 정보(Information) 메시지로 정의된다. <표 2>는 IPv6 통신에서 주요한 역할을 수행하는 ICMPv6 메시지의 종류를 나타낸 것이다.

<표 2> ICMPv6 메시지의 종류

종류	Type	내용	유형
일반	1	Destination Unreachable	에러
	2	Packet Too big	
	3	Time Exceeded	
	4	Parameter Problem	
	128	Echo Request	정보
	129	Echo Reply	
MLD	130	Multicast Listener Query	
	131	Multicast Listener Report	
	132	Multicast Listener Done	
NDP	133	Router Solicitation	
	134	Router Advertisement	
	135	Neighbor Solicitation	
	136	Neighbor Advertisement	
	137	Redirect	

ICMPv6 메시지는 <그림 4>와 같이 ICMP 헤더, 오류가 발생한 패킷의 IP 헤더 그리고 데이터 앞부분의 8 Bytes로 구성된다. 이렇게 구성된 ICMPv6 메시지는 다시 IP 헤더로 캡슐화되어 송신 노드로 전송된다.

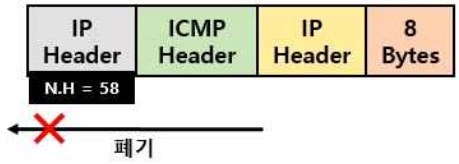


<그림 4> ICMPv6 메시지의 구성 및 전송

3. 일방향 통신 알고리즘

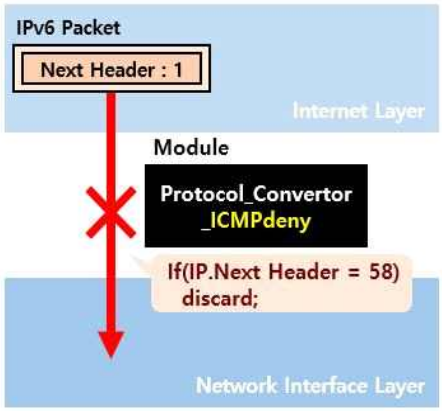
3.1 ICMP_DENY

본 방안에서는 ICMPv6 메시지를 통해 전송 오류에 대한 세부적인 정보를 파악할 수 있지만 이 과정이 생략되어도 실질적으로 데이터 전송에 문제 되지 않는다는 점에 착안하여, 모든 ICMPv6 메시지가 통과되지 않도록 하였다. 즉, <그림 5>와 같이 가장 앞단에 있는 IP 헤더의 'Next Header' 값이 58이면 해당 패킷을 폐기한다.



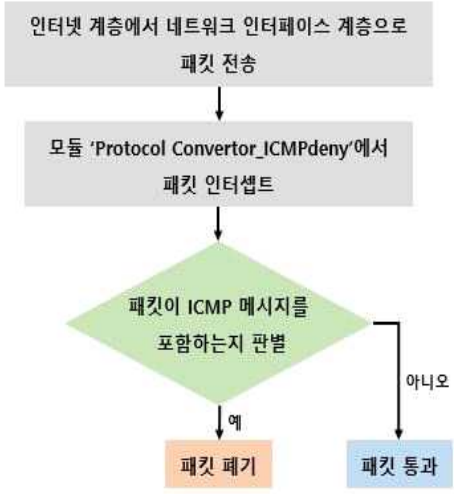
<그림 5> 알고리즘 'ICMP_DENY'의 작동 방식

이를 위해 IP 헤더의 'Next Header' 값을 통해 ICMPv6 메시지를 포함하는지 판별하고, 포함할 경우 해당 패킷을 폐기하는 기능을 수행하는 모듈 'Protocol_Convertor_ICMPdeny'를 송수신노드 양쪽에 구축하였다. <그림 6>은 송신 노드에서의 모듈 'Protocol_Convertor_ICMPdeny'에 대한 설계도를 나타낸 것이다. 수신 노드에서도 이와 동일하게 설계하도록 한다.



<그림 6> 'Protocol Convertor_ICMPdeny'의 설계

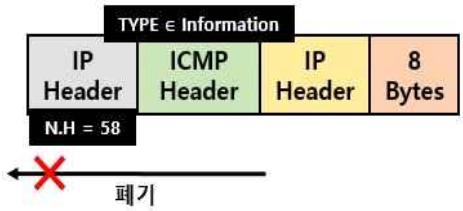
알고리즘 'ICMP_DENY'의 전체적인 흐름은 <그림 7>과 같다.



<그림 7> 알고리즘 'ICMP_DENY'의 흐름

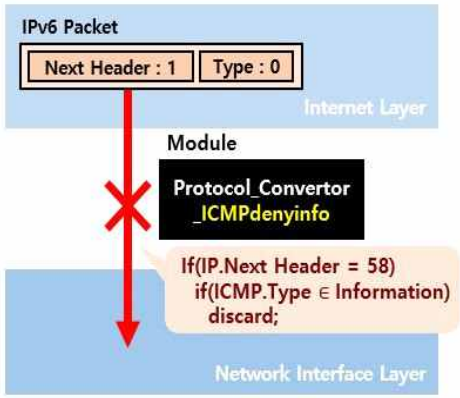
3.2 ICMP_DENYInfo

본 방안에서는 ICMPv6 메시지 중 정보(Information) 메시지는 정보를 요청하고 이에 대한 응답을 받기 위한 성격이 짙다는 점에 착안하여, 에러 메시지만 허용하고 정보 메시지는 통과되지 못하도록 하였다. 먼저 인터넷 계층으로부터 내려온 패킷이 ICMPv6 메시지를 포함하는지 판별한다. ICMPv6 메시지를 포함한 경우 이 메시지의 타입이 정보 메시지인지 판별하고 정보 메시지라면 해당 패킷을 폐기한다. 즉, <그림 8>과 같이 가장 앞단에 있는 IP 헤더의 'Next Header' 값이 58이고, ICMP 헤더의 'Type' 값이 정보 메시지에 포함되면 해당 패킷을 폐기한다.



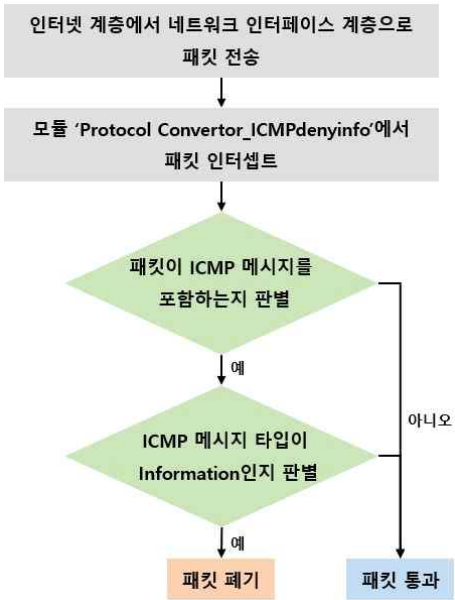
<그림 8> 알고리즘 'ICMP_DENYInfo'의 작동 방식

이를 위해 IP 헤더의 'Next Header' 값을 통해 ICMPv6 메시지를 포함하는지 판별하고, 포함할 경우 ICMP 헤더의 'Type' 값을 통해 이 메시지가 정보 메시지인지 판별하고, 정보 메시지일 경우 해당 패킷을 폐기하는 기능을 수행하는 모듈 'Protocol_Convertor_ICMPdenyinfo'를 송수신노드 양쪽에 구축하였다. <그림 9>는 송신 노드에서의 모듈 'Protocol_Convertor_ICMPdenyinfo'에 대한 설계도를 나타낸 것이다. 수신 노드에서도 이와 동일하게 설계하도록 한다.



<그림 9> 'Protocol_Convertor_ICMPdenyinfo'의 설계

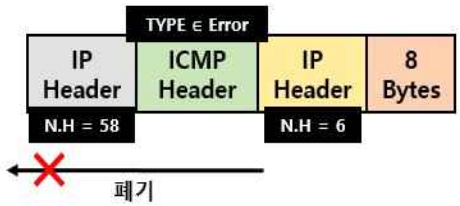
알고리즘 'ICMP_DENYInfo'의 전체적인 흐름은 <그림 10>과 같다.



<그림 10> 알고리즘 'ICMP_DENYInfo'의 흐름

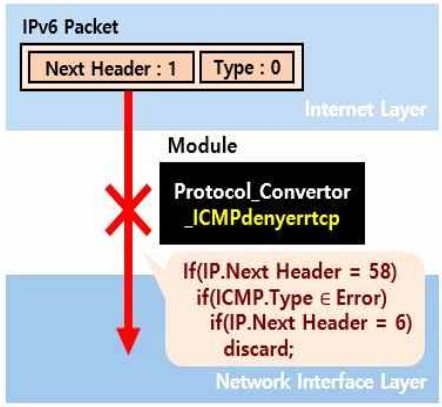
3.3 ICMP_DENYErrTCP

본 방안은 앞서 언급한 알고리즘 'ICMP_DENY Info'에 다른 조건 하나를 추가한 것이다. ICMPv6 메시지는 오류가 발생한 IP 패킷의 헤더를 포함하고 있는데, 이 IP 헤더의 'Next Header' 값을 통해 해당 패킷이 상위 계층에서 어떤 프로토콜 서비스와 관련되었는지 파악할 수 있다. 'Next Header'의 값이 17이면 UDP 서비스를 이용한 경우인데, 이는 비연결 지향적이면서 전송되는 패킷에 대해 확인/응답 절차를 거치지 않아 신뢰성 있는 데이터 전송 환경을 제공하지 않는다. 따라서 에러 메시지를 통해서 피드백을 주어야 할 필요가 있다. 반면 'Next Header'의 값이 6인 TCP 서비스를 이용한 경우에는 자체적으로 전송 계층에서 오류 및 혼잡 제어 기능이 존재하므로, 이 경우에는 해당 패킷이 통과되지 못하도록 하였다. 즉, <그림 11>과 같이 가장 앞단에 있는 IP 헤더의 'Next Header' 값이 58이고, ICMP 헤더의 'Type' 값이 에러 메시지에 포함되고, 그 다음에 따라오는 IP 헤더의 'Next Header' 값이 6이면 해당 패킷을 폐기한다.



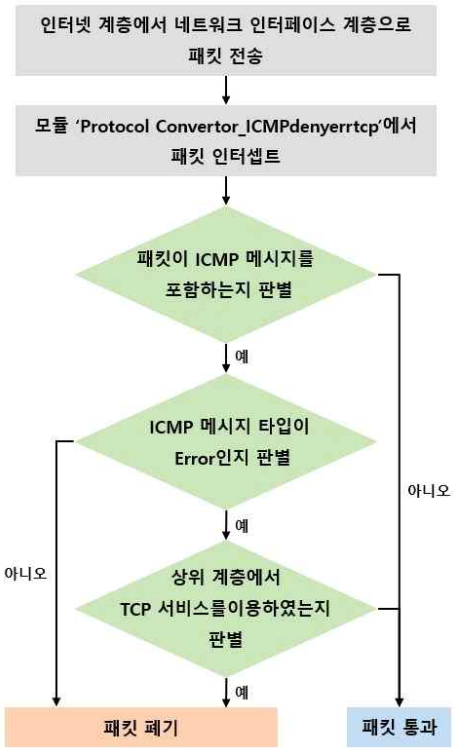
<그림 11> 알고리즘 'ICMP_DENYErrTCP'의 작동 방식

이를 위해 IP 헤더의 'Next Header' 값을 통해 ICMP 메시지를 포함하는지 판별하고, 포함할 경우 ICMP 헤더의 'Type' 값을 통해 이 메시지가 에러 메시지인지 판별하고, 에러 메시지일 경우 IP 헤더의 'Next Header' 값을 통해 상위 계층에서 TCP 서비스와 관련되었는지 판별하고, 관련되었을 경우 해당 패킷을 폐기하는 기능을 수행하는 모듈 'Protocol_Convertor_ICMPdenyerrtcp'를 송수신노드 양쪽에 구축하였다. <그림 12>는 송신 노드에서의 모듈 'Protocol_Convertor_ICMPdenyerrtcp'에 대한 설계도를 나타낸 것이다. 수신 노드에서도 이와 동일하게 설계하도록 한다.



<그림 12> 'Protocol_Convertor_ICMPdenyerrtcp'의 설계

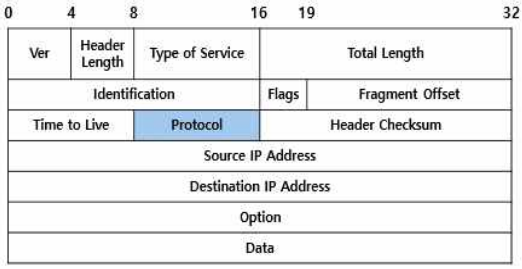
알고리즘 'ICMP_DENYErrTCP'의 전체적인 흐름은 <그림 13>과 같다.



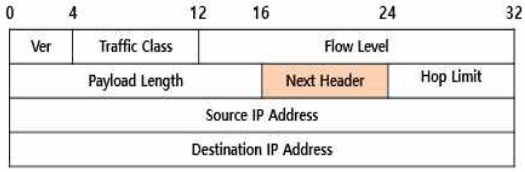
<그림 13> 알고리즘 'ICMP_DENYErrTCP'의 흐름

4. 비교 및 분석

본 논문의 3절에서는 Ipv6 환경에서의 일방향 통신 알고리즘 3개를 소개하였다. 본 절에서는 기존의 IPv4 환경에서 IPv6 환경으로 바뀌면서 알고리즘 작동 방식에서 어떤 점이 변화하였는지 알아본다. 알고리즘 3개 모두 IP 헤더 구조의 변화로 인해 IPv4 환경에서의 작동 방식과 IPv6 환경에서의 작동 방식 사이에 차이점이 발생한다. IPv4 환경에서는 IP 헤더에 'Protocol'이라는 필드가 존재한다. 이 필드는 IP 패킷을 통해 어떤 서비스와 관련된 패킷을 전달하는지를 나타낸다. 본 논문에서 소개한 알고리즘들은 이 필드를 이용하여 일방향 통신을 수행한다. 하지만 IPv6 환경에서는 'Protocol' 필드가 사라진 대신에 이와 유사한 기능을 하는 'Next Header' 필드를 이용하여 일방향 통신을 수행한다.



<그림 14> IPv4 헤더의 구조



<그림 15> IPv6 헤더의 구조

<표 3> IPv4/IPv6 환경에서의 알고리즘 작동 방식 차이

알고리즘	IPv4	IPv6
3.1 ICMP DENY	IP 헤더의 'Protocol' 값이 1이면 해당 패킷 폐기	IP 헤더의 'Next Header' 값이 58이면 해당 패킷 폐기
3.2 ICMP DENYinfo	IP 헤더의 'Protocol' 값이 1이고, ICMP 헤더의 'Type' 값이 정보 메시지에 포함될 경우 해당 패킷 폐기	IP 헤더의 'Next Header' 값이 58이고, ICMP 헤더의 'Type' 값이 정보 메시지에 포함될 경우 해당 패킷 폐기
3.3 ICMP DENYErrTCP	IP 헤더의 'Protocol' 값이 1이고, ICMP 헤더의 'Type' 값이 에러 메시지에 포함되고, 다음에 따라오는 IP 헤더의 'Protocol' 값이 6이면 해당 패킷 폐기	IP 헤더의 'Next Header' 값이 58이고, ICMP 헤더의 'Type' 값이 에러 메시지에 포함되고, 다음에 따라오는 IP 헤더의 'Next Header' 값이 6이면 해당 패킷 폐기

5. 결 론

본 논문에서는 일방향으로 데이터를 전송하면 불확실하고 언제 있을지 모르는 잠재적인 위협 요소로부터 시스템을 보호할 가능성이 높아진다는 점에 착안하여. IPv6 환경에서의 다양한 위협요소들부터 대응할 수 있는 일방향 통신 알고리즘에 대해 다루었다. 본 논문에서 개발한 일방향 통신 알고리즘은 총 3가지로 분류되며, 각 알고리즘마다 동작 방식에서 차이를 보인다. 첫 번째 알고리즘은 'ICMP_DENY'로 모든 ICMP 메시지를 폐기하는 방안이다. 두 번째 알고리즘은 'ICMP_DENYInfo'로 ICMP 메시지 중 정보 메시지만 폐기하는 것이다. 세 번째 알고리즘은 'ICMP_DENYErrTCP'로 ICMP 에러 메시지 중 상위 계층에서 UDP 서비스를 이용한 메시지들만 통과되도록 하는 방안이다. 이와 같이 본 논문에서 개발한 알고리즘들은 일방향 통신 네트워크 구축 시 자율적 환경 설정 가능, 일방향 통신 환경에 대한 정책 수립 등 다양하게 활용될 것으로 보인다.

참 고 문 헌

[1] 김진홍, 나중찬, 이성현, "상용 NIC 기반 단방향 통신 방법에 관한 연구", 정보보호학회논문지, 2016.

[2] 김평수, "IPv6 기본 개념 및 관련 기술의 이해", 한국통신학회논문지, 2015.

[3] 송중석, 이행곤, 박학수, "IPv6 보안기술 국제표준화 동향", 정보보호학회논문지, 2012.

[4] 신명기, 김형준, "IPv6 전환 환경에서의 보안 기술 분석", 전자통신동향분석, 2006.

[5] 윤종호, "TCP/IP와 라우팅 프로토콜", 교학사, 2003.

[6] 진강훈, "후니의 쉽게 쓴 시스코 네트워킹", 성안당, 2010.

[7] 양대일, "정보 보안 개론과 실습 - 네트워크 해킹과 보안", 한빛미디어, 2010.

[8] Iman Akour, "Between Transition from IP v4 and IPv6 Adaption: The Case of Jordanian Government", International Journal of Advanced Computer Sciences and Applications, 2016

[9] Forourzan, Behrouz A., "Data Communications and Networking", McGraw-Hill, 2007.

[10] Loshin, Peter, "IPv6: theory, protocol, and practice", Morgan Kaufmann, 2004.

〔저자소개〕

고 근 호 (Keun Ho Koh)
성균관대학교 컴퓨터교육과 소속
email : keuno0923@gmail.com

안 성 진 (Seong Jin Ahn)
1988년 2월 학사
1990년 2월 석사
성균관대학교 대학원
정보공학과 공학석사
1998년 8월 박사
성균관대학교 대학원
정보공학과 공학박사
email : sjahn@skku..edu