情報保護學會論文誌
第18卷 第6(A)號, 2008. 12

무선 네트워크 환경에서의 효과적인 Quality of Protection(QoP) 평가

김 현 승[1†], 임 선 희[1‡], 윤 승 환[1], 이 옥 연[2], 임 종 인[1]
[1]고려대학교 정보경영공학전문대학원, [2]국민대학교 자연과학대학 수학과

Effective Evaluation of Quality of Protection(QoP) in Wireless Network Environments*

Hyeon-Seung Kim[1†], Sun-Hee Lim[1], Seunghwan Yun[1], Okyeon Yi[2‡], Jongin Lim[1]
[1]Graduate School of Information Management and Security, Korea University,
[2]Department of Mathematics, Kookmin University

요 약

Quality of Protection(QoP)은 보안을 제공해야 하는 네트워크들을 평가할 수 있는 기준을 제공하고, 해당 네트워크의 보안 정책에 대한 보안의 강도를 정량화하여 해당 네트워크 시스템의 안정성을 판단할 수 있도록 해준다. 현실적으로, 네트워크에서 적용되는 보안 메커니즘의 안전성과 시스템에서 지원되어야 하는 성능이 반드시 비례하는 것은 아니다. 그렇기 때문에 보안은 적절한 수준에서 적용되는 환경에 맞게 정의되어야 하며, 네트워크의 사용 목적에 맞는 보안 정책을 택하여 사용해야 한다. 무선 네트워크들이 발전함에 따라 안전한 무선네트워크 서비스를 제공하기 위해 다양한 보안 서비스들이 정의되고 있다. 본 논문에서는 무선 네트워크 환경에서의 적절한 보안 정책을 선택할 수 있도록 기존에 연구된 QoP모델의 효용함수 구성에 흐름 기반의 비정상 트래픽 탐지 알고리즘을 통해 객관적으로 구성한 HVM을 도입하고, 총 이익함수의 구성에 상대적 가중치를 도입함으로써 기존에 연구된 QoP모델의 취약점을 보완한다.

ABSTRACT

Quality of Protection(QoP) provides a standard that can evaluate networks offering protection. Also, QoP estimates stability of the system by quantifying intensity of the security. Security should be established based on the circumstance which applied to appropriate level, and this should chose a security policy which fit to propose of network because it is not always proportioned that between stability of security mechanism which is used at network and performance which has to be supported by system. With evolving wireless networks, a variety of security services are defined for providing secure wireless network services.

In this paper, we propose a new QoP model which makes up for weak points of existing QoP model to choose an appropriate security policy for wireless network. Proposed new QoP model use objectively organized HVM by Flow-based Abnormal Traffic Detection Algorithm for constructing Utility function and relative weight for constructing Total reward function.

Keywords : Quality of Protection(QoP), HVM, Flow-based Abnormal Traffic Detection Algorithm

Ⅰ. 서 론

무선랜(WLAN), 휴대 인터넷(WiBro), WCDMA (3GPP)를 비롯한 다양한 무선 이동통신의 발전을 통해 언제, 어디서나 인터넷에 연결하여 필요한 데이터에 접근이 가능해지고 있다. 무선 이동통신 영역이 더욱 발전함에 따라 무선랜이 사용되는 영역도 간단한 서비스에서부터 민감하거나 중요한 데이터를 주고받는 영역에까지 확장되었다[7]. 하지만, 무선 네트워크에서는 무선의 물리적 특성에 따른 보안측면의 취약성 때문에 유선 네트워크와 달리 보다 강화된 보안 요구사항이 정의 및 만족되어야 한다. IEEE 802.11i[2] 표준에서는 무선랜에서의 데이터 계층의 보안성을 지원하기 위하여 TKIP, CCMP를 적용한 데이터 캡슐화(encapsulation)와, IEEE 802.1x PACP(포트접근제어)[1]를 정의한다. 또한 데이터 계층 외에서도 IPSec등의 상위 계층에서의 보안 메커니즘 적용을 요구하고 있다[9]. 이러한 다양한 계층에서의 보안 요구사항을 만족하기 위해 무선 네트워크에서의 보안은 여러 보안 프로토콜들이 결합(Hybrid security policies)되어 사용되도록 만들었다. 하지만, 보안 프로토콜의 사용은 보안 측면과 QoS(Quality of Service) 서비스 지원 간에 trade-off를 발생시킨다. 그렇기 때문에 보안 프로토콜은 QoS에 영향을 미치지 않는 범위에서 사용되어야 한다. 또한 특정한 보안 프로토콜을 사용함에 따른 시스템의 안전성을 미리 예측해 볼 수 있다면, 필수적으로 보안 요구사항이 만족되어야 하는 무선 네트워크에서 각 시스템에서의 최적의 보안 프로토콜을 적용할 수 있게 될 것이다.

본 논문에서는 무선랜(WLAN)이 사용되는 무선 네트워크 환경을 중심으로 분석이 이루어졌으며, 이를 토대로 하여 각 무선 네트워크 시스템에 적합한 최적의 보안 프로토콜을 적용하는 방법으로서 QoP(Quality of Protection)모델을 제시한다. 그리고 시스템의 안전성을 미리 예측할 수 있는 객관적 기준의 제시를 위해, 흐름 기반의 비정상 트래픽 탐지 알고리즘(Flow-based Abnormal Traffic Detection Algorithm)을 이용하여 구성한 Historical Vulnerability Measure(HVM)를 제시하고 QoP모델을 구성하는 효용함수의 구성요소로써 이용된다. HVM은 각각의 보안 프로토콜들이 과거에 어떠한 취약점이 발생했는지를 반영하는 요소로써, 흐름 기반의 비정상 트래픽 탐지 알고리즘을 통해 해당 네트워크에 비정상적인 트래픽의 유입 및 공격 발생 등에 대한 분석을 하여 구성하게 된다.

QoP모델은 보안 프로토콜이 갖추어야 할 기준들과 사용 시의 예상되는 이익 효과에 대해 가중치를 기반으로 한 정량화 방법을 통해서 각 보안 프로토콜을 미시적인 관점에서 평가해 볼 수 있는 효용함수(Utility function)와 효용함수의 수치들을 종합하여 각 보안 프로토콜을 거시적 관점에서 평가해 볼 수 있는 총이익함수(Total reward function)로 평가 기준을 정의한다.

본 논문에서는 보안 프로토콜 측면의 QoP모델 제시를 위해, 2장에서는 Quality of Protection(QoP)을 구성하는 효용함수를 소개하고, 효용함수의 구성 요소 중 [3]에서 소개된 기존의 효용함수를 보완하는 요소인 Historical Vulnerability Measure(HVM)와 이를 구성하는데 사용되는 흐름 기반의 비정상 트래픽 탐지 알고리즘(Flow-based Abnormal Traffic Detection Algorithm)에 대해 살펴 본 후, 효용함수의 구성 방법에 대해 정의하고, 효용함수를 통해 만들어지는 총이익함수를 분석한다. 그리고 3장에서는 본 논문에서 제안한 QoP모델에 대한 평가를 살펴 본 후, 마지막으로 4장에서 본 논문의 결론 및 향후 연구방향에 대해 언급하였다.

Ⅱ. Quality of Protection model

QoP모델을 구성하는 효용함수(Utility function)와 총이익함수(Total reward function)를 도입하기 위해서는 효용함수에 사용되는 평가기준의 적용 방법이 중요하다. 본 논문에서는 이전의 많은 연구자들이 했던 것과 같이 상대평가를 기반으로 효용함수에 적용하였다[3,10]. 물론 상대적으로 점수를 주는 방법이 완전한 방법은 아니지만, 이 문제는 총이익함수에 상대적 가중치(relative weight) 개념을 도입함으로써 해결하였다. 상대적 가중치는 보안 네트워크 설계자가 보안 구성 요소들이 해당 보안 네트워크상에서 중요하게 인식되는 정도를 백분율로 나타낸 것이다.

접수일: 2008년 7월 17일; 수정일: 2008년 10월 3일;
채택일: 2008년 10월 9일
* 이 연구에 참여한 연구자의 일부는 '2단계BK21사업'의 지원비를 받았음
† 주저자, seung34@korea.ac.kr
‡ 교신저자, capsunny@korea.ac.kr

2.1 효용함수(Utility function)

네트워크 성능에 대한 효용을 정량화시키는 효용함수를 만드는 방법은 과거에도 연구가 많이 되었으며, 본 논문에서의 효용함수는 [3]에서 소개된 내용을 개선하기 위해 제시되었다.

기존의 효용함수는 보안 프로토콜의 결합으로 만들어지는 각각의 보안 정책들에 대해 보안 프로토콜이 제공해야 할 기준을 두어 각 항목이 제공하는 보안의 강도를 정량화하여 나타내는 방법으로 이루어진다[3]. 하지만, 이는 각 보안 프로토콜의 특성에 따라 제공하는 보안 특성을 정량화 시켰을 뿐, 실제로 해당 보안 프로토콜이 네트워크 시스템에 적용되었을 경우 어느 정도의 보안에 대한 취약성이 발생하는지에 대한 요소는 반영되지 않았다. 그래서 본 논문에서는 보안 프로토콜이 기본적으로 제공되어야 할 5가지 인증, 상호인증, 기밀성, 무결성, 부인방지 이외에 비정상적인 네트워크 트래픽을 탐지하는 알고리즘을 이용한 Historical Vulnerability Measure(HVM)에 기반을 둔 안전성을 도입하여 총 6가지의 요소로 효용함수를 구성하게 되었다.

2.1.1 흐름 기반의 비정상 트래픽 탐지 알고리즘(Flow-based Abnormal Network Traffic Detection Algorithm)[6]

비정상적인 네트워크 트래픽(Abnormal Network Traffic)은 서비스 거부 공격(DoS), 분산 서비스 거부 공격(DDoS), 인터넷 웜(Worm), 스캐닝(Scanning)과 같이 악의적인 결과를 유발하는 트래픽으로 정의한다[6].

비정상적인 네트워크 트래픽의 탐지는 보안 네트워크 시스템을 모니터링 함으로써 이루어지게 되는데, [6]에서 제안된 흐름 기반의 비정상 트래픽 탐지 알고리즘(Flow-based Abnormal Traffic Detection Algorithm)에 기반을 두어 흐름 헤더 탐지(flow header detection)와 트래픽 패턴 탐지(traffic pattern detection)로 구성을 한다.

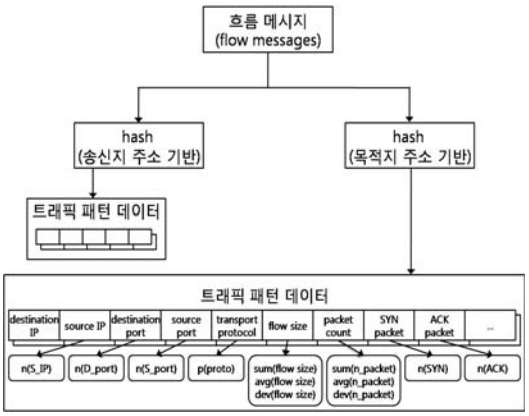
흐름 헤더 탐지는 흐름 헤더의 필드 값이 유효한지를 체크하여, 만일 흐름 헤더의 필드 값이 유효하지 않은 경우에는 [표 1]과 같이 공격을 분류하게 된다.

다음의 [표 1]은 흐름 헤더(flow header)의 필드 값에 따라 공격을 분류한 것을 보여주고 있으며, 표에서 L은 해당 전송 프로토콜이 처리할 수 있는 정상적인 데이터의 범위를 초과하는 경우를 의미한다.

[표 1] 흐름 헤더 검사를 통한 공격 분류

전송 프로토콜	특 징	공격 분류
ICMP	echo request, destination IP address = broadcast	smurf
	flow size/packet count is too high	ping-of-death
	packet count = L, flow size = L	ICMP flooding
TCP	source IP address = destination IP address source port = destination port	land
	packet count = L, flow size = L	TCP flooding
UDP	destination port = reflecting port, source port = reflecting port	ping-pong
	destination port = reflecting port, destination IP address = broadcast	fraggle
	packet count = L, flow size = L	UDP flooding

트래픽 패턴 탐지는 보안 네트워크 공격이 발생하는 경우 특정한 패턴(pattern)을 갖는 트래픽이 생성된다는 사실에 기반을 두어 공격 유형을 탐지하는 방법이다. 이는 흐름 헤더를 통해 공격 여부를 판단하기 어려운 경우에 효과적으로 작용을 하게 되는데, 이를 위해 트래픽 패턴 데이터들을 생성하여 저장을 한다. 트래픽 패턴 데이터를 생성하는 과정은 [그림 1]과 같다. [그림 1]에서는 같은 송신지 주소(source IP), 목적지 주소(destination IP)를 갖는 트래픽들에 대해서 각각 관련된 트래픽들에 해쉬(hash)값을 취해서 나온 정보들을 보관을 하게 된다. 즉, 이 단계에서는 송신지 기반의 트래픽 패턴 데이터(source based traffic pattern data)와 목적지 기반의 트래



[그림 1] 트래픽 패턴 데이터의 생성

[표 2] 트래픽 패턴 데이터에 사용되는 용어

용어	설명
n(flow)	같은 destination IP 주소를 갖는 flow의 수
n(S_IP)	같은 destination IP 주소를 갖지만, 서로 다른 source IP 주소를 갖는 flow의 수
n(D_port)	같은 destination IP 주소를 갖는 destination port의 수
n(S_port)	같은 destination IP 주소를 갖는 source port의 수
p(proto)	같은 destination IP 주소를 갖으면서 가장 빈번하게 나타나는 전송 프로토콜
sum(flow size) avg(flow size) dev(flow size)	같은 destination IP 주소를 갖는 flow size의 총 합, 평균, 편차
sum(n_packet) avg(n_packet) dev(n_packet)	같은 destination IP 주소를 갖는 packet count의 총 합, 평균, 편차
n(SYN) n(ACK)	같은 destination IP 주소를 갖는 SYN, ACK의 총 packet의 수

픽 패턴 데이터(destination based traffic pattern data)가 생성이 되게 된다. 트래픽 패턴 데이터가 생성된 이후에 비정상적인 트래픽이 발견되는 경우에 일차적으로 흐름 헤더의 필드 값 비교를 통해 공격 여부를 판단하고, 흐름 헤더의 필드 값 비교를 통해 공격 여부를 판단하기 힘든 경우, 이차적으로 앞에서 생성된 트래픽 패턴 데이터와의 비교를 통해 공격 여부 및 발생한 공격의 종류를 판단하게 된다.

앞의 [표 2]는 트래픽 패턴 데이터 탐지와 관련하여 사용되는 용어이며, 이는 [그림 1]과 [표 3]에서 사용된다.

다음의 [표 3]은 [그림 1]의 방법을 통해 생성된 트래픽 패턴 데이터와의 비교를 통해서 공격을 분류하는 기준을 나타낸 것으로 목적지 주소를 기반(destination based)으로 하여 공격 여부를 판단하는 경우에는, 전송 프로토콜의 종류에 상관없이 같은 목적지 주소(destination IP address)를 갖는 packet count의 합이 L이고, 같은 목적지 주소를 갖는 flow size의 총 합이 L인 경우, 너무 많은 패킷이 지정된 목적지 주소를 갖는 네트워크로 전송되어 해당 네트워크 시스템이 정상적인 서비스를 제공할 수 없게 되므로 flooding 공격이 일어난 것으로 간주하게 된다. [표 3]에서 L은 해당 전송 프로토콜이 처리할 수 있는 정상적인 데이터의 범위를 초과하는 경우를 의미하며, S는 해당 전송 프로토콜이 처리할 수 있는 정상적인 데이터의 범위에 미달하는 경우를 나타낸다.

[표 3] 트래픽 패턴 데이터 비교를 통한 공격 판단

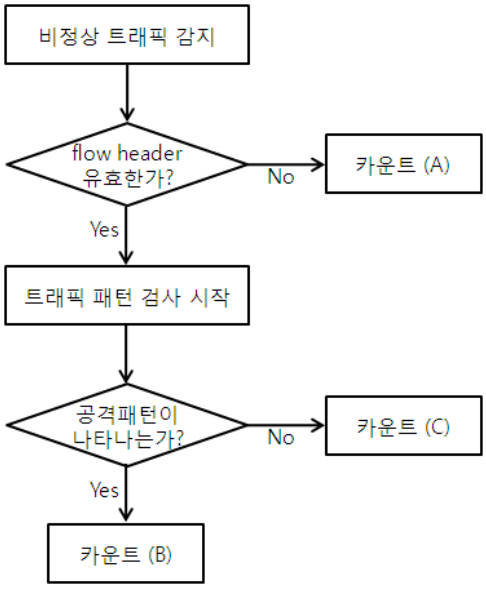
분류 기준	특징		공격 분류
목적지 주소 기반 (destination based)	n(flow)=L avg(flow size)=S avg(n_packet)=S	n(D_port)=L n(S_IP)=S	host scanning
		n(D_port)=S n(ACK)/n(SYN)=S	TCP SYN flood
	sum(n_packet)=L sum(flow size)=L		(ICMP, UDP, TCP) flooding
송신지 주소 기반 (source based)	n(flow)=L avg(flow size)=S avg(n_packet)=S	n(D_IP)=L n(D_port)=S	network scanning
	sum(n_packet)=L sum(flow size)=L		(ICMP,UDP, TCP) flooding

2.1.2 Historical Vulnerability Measure(HVM)

Historical Vulnerability Measure(HVM)는 해당 보안 프로토콜을 적용했을 때 실제적으로 어느 정도의 취약성이 발생했는지를 과거의 경향을 통해 정량화시키는 요소이다[4].

$HV(S)$를 S라는 보안 프로토콜에 대한 취약성이라고 한다. 그러면 $HV(S)$는 취약성의 정도에 따라 High, Medium, Low의 세단계로 구분 지을 수 있는데, 이를 각각 $HV_H(S)$, $HV_M(S)$, $HV_L(S)$로 표기하기로 한다.

본 논문에서는 $HV_H(S), HV_M(S), HV_L(S)$의 구분은 앞에서 소개한 흐름 기반의 비정상 트래픽 탐지 알고리즘(Flow-based Abnormal Traffic Detection Algorithm)을 통해 취약점이 발생하는 빈도를 체크하여 이루어지는데, 자세한 방법은 [그림 2]의 과정을 거치게 된다. 이는 특정 보안 프로토콜을 적용했을 경우, 비정상 트래픽이 감지가 되면, 먼저 흐름 헤더의 필드 값의 유효성을 확인 하게 되는데, 만일 이때 필드 값이 유효하지 않으면, 그에 해당되는 트래픽(A)의 수를 카운트하게 된다. 반면, 필드 값이 유효한 경우에는 흐름 헤더(flow header)의 필드 값으로 알아낼 수 없는 공격이 행해지고 있는지의 여부를 알아내기 위해 트래픽 패턴 검사를 수행하게 되는데, 이때 공격 패턴을 갖는 트래픽(B)이 감지되면, 그런 특성을 갖는 트래픽의 수를 카운트하고, 공격 패턴이 나타나지 않는 경우에도 그에 해당되는 트래픽(C)의 수를 카운트하게 된다. 이때, 공격 패턴이 나타나지 않는 트래픽(C)을 카운트하는 이유는 비정상적인 트래픽이 감지된 상황에서 트래픽을 분석하여 알 수 있는



[그림 2] 비정상 트래픽이 감지된 경우

공격이 탐지되지 않고 있다는 사실로부터 현재까지 알려지지 않은 새로운 공격이 행해지고 있을 수 있는 가능성이 있기 때문이다. [표 4]는 취약성 등급을 구분하는 기준을 보여주고 있는데, 표에서 N은 전체 트래픽의 수, D는 비정상적인 트래픽의 비율을 나타내고, $n(A), n(B), n(C)$는 각각에 해당되는 트래픽의 수를 나타낸다.

[표 4]에서 $0 \le D < n(C)/N$이면서, 공격이 탐지되지 않은 경우에는 취약성 등급을 $HV_L(S)$ 등급에 배정을 하게 되는데, 이는 네트워크에 접속되어 있는 사용자의 실수로 인해 트래픽이 잘 못 흘러들어온 경우를 반영한 것이고, $n(C)/N \le D \le \{n(A)+n(B)+n(C)\}/N$ 이면서, 공격이 탐지되지 않은 경우에 취약성 등급을 $HV_M(S)$ 등급에 배정을 한 것은 여전히 공격이 탐지 되고 있지는 않지만, 비정상 적인 트래픽의 유입이 늘어났다는 사실로부터 어떠한 공격자가 공격을 시도하고 있다고 판단할 수 있기 때문이다. 그리고 $n(C)/N \le D \le \{n(A)+n(B)+n(C)\}/N$이면서, 공격이 탐지된 경우에는 이미 네트워크의 보안 프로토콜이 제 기능을 하지 못하는 경우에 해당되므로 취약성 등급이 가장 높은 $HV_H(S)$등급에 배정을 하게 된다.

[표 4] 취약성 등급의 구분

취약성 등급	기준
$HV_H(S)$	$n(C)/N \le D \le \{n(A)+n(B)+n(C)\}/N$ 이면서, 공격이 탐지된 경우
$HV_M(S)$	$n(C)/N \le D \le \{n(A)+n(B)+n(C)\}/N$ 이면서, 공격이 탐지되지 않은 경우
$HV_L(S)$	$0 \le D < n(C)/N$ 이면서, 공격이 탐지되지 않은 경우

그리고 $HV(S)$는 과거의 경향을 반영하는데, 오래전의 결과일수록 가중치를 적게 두어 평가한다. 이는 오래된 결과일수록 분석이 많이 되고, 취약성을 보완할 수 있는 패치를 만들어 문제를 해결했을 가능성이 높기 때문이다. 그리고 $SS(v_i)$를 취약성 점수(Severity Score of a vulnerability v)라고 정의한다면, $HVM(S)$는 다음과 같이 계산되어 질 수 있다.

$$HVM(S) = \ln \sum_{X \in \{H,M,L\}} w_X \sum_{v_i \in HV_X(S)} SS(v_i)\, \varepsilon^{-\beta Age(v_i)}$$

위의 식에서 β는 시간을 나타내는 변수로서 $SS(v_i)$라는 변수가 얼마나 오래되었는가를 나타낸다. 또한, w_X는 $HV_H(S), HV_M(S), HV_L(S)$에 대한 가중치로서 취약성이 가장 높은 $HV_H(S)$가 가장 높은 가중치를 갖게 되고, 상대적으로 낮은 취약성을 갖는 $HV_M(S)$, $HV_L(S)$는 점진적으로 낮은 가중치를 갖게 된다. 또한, 취약성은 제공되는 보안 특성들의 평균이 아닌 가장 취약한 부분에 의해서 결정된다는 특성을 반영하기위해 $HVM(S)$를 계산하는 과정에서 지수평균을 사용한다.

$HVM(S)$를 계산해봄으로써 얻을 수 있는 효과는, 이 수치가 과거에 S라는 보안 프로토콜을 적용하였을 때 나타난 취약성정도를 나타내는 것이므로, 이를 통하여 앞으로의 해당 보안 프로토콜에 대한 취약성의 발생에 대하여 예측해 볼 수 있게 된다.

2.1.3 효용함수의 구성

효용함수는 앞에서 설명한 $HVM(S)$의 계산 결과에 기반을 둔 안전성을 포함하여, 인증, 상호인증, 기밀성, 무결성, 부인방지의 6가지 요소로 구성이 된다. 기본적인 함수의 구성방법은 [3]에서 제안된 방법과 같지만, 평가항목에 $HVM(S)$에 기반을 둔 안전성을 포함시켜 과거의 경향을 반영한다는 측면에서 더욱 개량된 방법이라 할 수 있다[5].

[표 5] 효용함수의 가중치 점수 배정

평가항목	인증	상호 인증	기밀성	무결성	부인 방지	안전성
WEP-128	0	0	1	1	0	1
TKIP	0	0	2	2	0	2
CCMP	1	0	3	5	0	5
802.1x-EAP -MD5	2	0	0	0	0	4
IPSec	3	1	4 (3DES)	4 (SHA)	1 (ESP)	6
IPSec/802.1 x-EAP	0	0	0	3 (MD5)	0	3
802.1x-EAP -TLS	4	2	0	0	2	7

효용함수는 기준이 되는 6가지 항목에 대하여 특정 프로토콜이 제공하는 보안의 강도에 따라 상대적으로 가중치 점수를 배정하게 된다. 이때, 보안을 전혀 제공하지 않는 항목에 대해서는 0점을 배정하고, 제공되는 보안의 강도에 따라 순차적으로 점수를 배정한다. 안전성의 경우에도 예외 없이 계산된 결과의 값에 따라 상대적으로 가중치 점수를 배정하기로 한다. 단, $HVM(S)$의 경우 계산 결과 수치가 높을수록 과거에 취약성이 많이 발생하였다는 의미가 되기 때문에 $HVM(S)$의 계산 결과 수치가 높을수록 안전성에 상대적으로 낮은 점수를 배정하고, $HVM(S)$의 계산 결과 수치가 낮을수록 안전성에 상대적으로 높은 점수를 배정하기로 한다.

위의 [표 5]는 무선 네트워크에서의 각 보안 프로토콜에 따라 가중치 점수를 배정한 것을 보여주고 있으며, 각 보안 요소의 점수와 함께 쓰여 있는 내용은 해당 항목을 평가하는데 사용된 암호화 알고리즘을 나타낸다. 즉, IPSec의 경우 기밀성을 검증하기 위한 수단으로서 3DES 알고리즘이 사용되었고, 무결성을 검증하기 위해서는 SHA 알고리즘, 그리고 부인방지를 위해 ESP 알고리즘이 사용되었다는 것을 나타낸다.

2.2 총이익함수 (Total reward function)

기존에 [3]에서 도입된 Additive reward function에서는 서로 다른 성질을 갖는 각각의 보안 요소들에 대해 동등한 가중치를 두어 총합을 구하는 방식으로 정량화가 이루어졌다. 하지만, 이러한 방법은 보안 네트워크 설계자가 각기 다른 목적으로 사용되는 보안 네트워크 시스템을 구축해야 하는 상황에서 적절한 보안 정책을 선택하기에 적절하지 않다는 단점이 있었다. 그러한 문제점을 해결하고자 본 논문에서는 상대적 가중치(relative weight)의 개념을 도입하고, w_i로 표기하기로 한다.($단, \sum_i w_i = 1$) 그리고 앞의 효용함수에서 평가되는 항목은 $HVM(S)$에서 사용된 것과 같이 v_i^k로 나타내기로 한다. w_i와 v_i^k에서 k는 k번째 보안 프로토콜의 시행을 나타내고, i는 1일 때 인증, 2일 때 상호인증, 3일 때 기밀성, 4일 때 무결성, 5일 때 부인방지, 6일 때 안전성을 각각 나타낸다.

만일 평가하고자 하는 보안 정책 P가 n개의 보안 프로토콜이 결합되어 있는 형태라고 한다면, 이때 총이익함수(Total reward function) $\Phi(P)$는 다음과 같이 정의된다.

$$\Phi(P) = \sum_{k=1}^{n} \left\{ \sum_{i=1}^{6} v_i^k w_i \right\}$$

예를 들어 보안 정책 P를 구성하는 보안 프로토콜이 802.1x-EAP-TLS-WEP-128이라하면, [표 1]에 근거하였을 때 이 보안 정책은 802.1x-EAP-TLS와 WEP-128이 결합된 형태이므로, $n=2$가 된다. 또한 802.1x-EAP-TLS가 인증서를 사용한 상호 인증 기능을 제공하고, WEP-128은 캡슐화를 통한 기밀성과 인증을 제공한다는 측면에서 볼 때, 제시된 보안 정책 P는 인증에 초점이 맞추어져 있는 무선 네트워크에 적용된 사례라고 볼 수 있다. 이 경우 보안 평가 항목에 대한 상대적 가중치(relative weight)는 인증 및 상호인증에 중점을 두어 $w_1 = 0.2, w_2 = 0.3, w_3 = 0.1, w_4 = 0.1, w_5 = 0.1, w_6 = 0.2$로 줄 수 있고, 이때 총이익함수 $\Phi(P)$는 다음과 같이 계산된다.

$$\Phi(P) = \{4\times0.2 + 2\times0.3 + 2\times0.1 + 7\times0.2\} + \{1\times0.1 + 1\times0.1 + 1\times0.2\} = 3.4$$

기존의 QoP평가 방법에서는 각기 다른 특성을 갖는 보안 기준들에 대해 보안을 제공하는 요소에 대해서는 1, 아닌 경우는 0의 가중치만을 주어서 서로 다른 특성을 갖는 보안 정책들이 같은 결과를 얻게 되어 동일한 수준의 보안을 제공하는 것으로 평가되는 문제점이 있었다[3]. 예를 들면, [표 1]에서 제시된 TKIP과 IPSec/

802.1x-EAP를 개별 보안 정책으로 보고, [3]에서 제시된 방법으로 총이익 함수를 계산해보면 다음과 같은 결과가 나온다.

$$\Phi(TKIP) = 6$$
$$\Phi(IPSec/802.1x - EAP) = 6$$

하지만, 위에서 예로 든 보안 정책을 본 논문에서 제시된 방법으로 총이익 함수를 계산해보면 결과는 다음과 같다. 이때, 각 보안 요소에 대한 가중치는 앞에서 예로 든 것을 사용하기로 한다.

$$\Phi(TKIP) = 0.8$$
$$\Phi(IPSec/802.1x - EAP) = 0.9$$

위의 결과를 보면, 기존의 [3]에서 제시된 방법으로 총이익함수를 계산한 경우 서로 다른 특성을 갖는 보안 정책이 같은 수준의 보안을 제공하는 것으로 평가된다는 것을 확인할 수 있다. 이러한 문제점을 해결하기 위해 [3]에서는 인위적으로 효용함수의 가중치 점수를 조작해야하는 번거로움이 있었다. 하지만, 본 논문에서 제시된 방법으로 계산된 결과를 보면, 서로 다른 특성을 갖는 보안 기준들에 대해 보안 네트워크 설계자가 중점을 두어야 할 사항에 좀 더 높은 상대적 가중치(relative weight)를 할당함으로써 [3]에서 생기는 문제점을 해결할 수 있다.

Ⅲ. 제안한 Quality of Protection model에 대한 평가

기존에 [3]에서 연구되었던 QoP모델의 경우, 각각의 보안 프로토콜들의 특성을 분석하여 인증, 상호인증, 기밀성, 무결성, 부인방지의 5가지 기준에 대해서 해당 알고리즘이 제공하는 보안의 강도에 따라 상대적으로 점수를 배정하는 방법을 통해 효용함수를 구성하였다. 이 경우 각각의 보안 프로토콜들이 제공하는 보안의 강도를 이론적인 분석을 통해 작성된 효용함수 표를 통해 비교해 볼 수 있다는 장점을 가지고 있지만, 해당 보안 프로토콜이 실제적으로 보안 네트워크에 적용이 되었을 때 어느 정도의 안전성이 보장되는지는 알 수 없다는 단점을 가지고 있었다. 그리고 [3]에서 제시된 방법으로 총이익 함수를 계산하는 경우, 서로 다른 특성을 갖는 보안 정책들이 같은 수준의 보안을 제공하는 것으로 평가되는 오류가 있었으며, 이러한 오류를 해결하기 위해 인위적으로 효용함수의 점수를 조작하여 총이익함수를 다시 계산하여야 하는 번거로움이 있었다.

기존에 연구된 [3]에서 생기는 문제점들을 해결하기 위해 [5]에서는 효용함수에 $HVM(S)$에 기반을 둔 안전성을 도입하여 각각의 보안 프로토콜이 실제 보안네트워크에 적용되었을 때 어느 정도의 안전성이 제공되는지 알 수 있도록 하였으며, 총이익함수에는 상대적 가중치를 도입함으로써 [3]에서 생기는 서로 다른 보안정책들이 동일한 보안 수준을 제공하는 것으로 평가되던 문제점들을 해결하였다. 하지만, [5]에서 제안된 QoP 모델의 경우 안전성과 상대적 가중치를 도입함으로써 기존의 [3]에서 생기는 문제점들을 해결하였지만, 안전성을 객관적으로 평가할 수 있는 기준이 없었다.

본 논문에서는 흐름 기반의 비정상 트래픽 탐지 알고리즘(Flow-based Abnormal Traffic Detection Algorithm)을 도입하여 비정상적인 트래픽들에 대해서 보안 네트워크의 안전을 위협하는 공격들을 탐지하는 기준을 제시하고, 안전성의 평가 기준으로 활용되는 $HVM(S)$를 좀 더 명확한 기준을 가지고 계산할 수 있도록 하기위

[표 6] 기존의 연구와 제안한 QoP모델의 비교

	기존 연구	논문 [5]	본 논문
특징	• 효용함수 및 총이익함수 개념 도입 • 보안프로토콜 알고리즘 특성에 따라 효용함수에 상대점수 배정 • 과거의 경향 반영하지 않음 • 총이익함수 계산에 0또는 1의 가중치만을 주어 서로 다른 보안 특성을 갖는 보안 정책이 같은 수준의 보안을 제공하는 것으로 평가되는 문제점 발생	• $HVM(S)$에 기반을 둔 안전성을 도입함으로써 과거의 경향 반영 • 상대적 가중치를 도입함으로써 기존 총이익함수의 취약점 보완 • $HV_H(S)$, $HV_M(S)$, $HV_L(S)$을 구분하는 객관적 기준 결여	• $HVM(S)$에 기반을 둔 안전성을 통해 과거의 경향 반영 • 상대적 가중치를 통해 기존 총이익함수의 취약점 보완 • 흐름 기반의 비정상 트래픽 탐지 알고리즘을 도입하여 공격탐지의 객관적 기준 제시 • $HV_H(S)$, $HV_M(S)$, $HV_L(S)$을 구분하는 객관적 기준 제시

해 취약성 등급 $HV_H(S), HV_M(S), HV_L(S)$을 구분하는 객관적인 기준을 제시하였다. 이를 통해 [5]에서 제시된 QoP모델이 좀 더 객관적인 기준을 가지고 각각의 보안 네트워크에 적용되는 보안 정책들을 평가하는데 사용될 수 있다.

Ⅳ. 결 론

본 논문에서는 기존에 연구되었던 QoP모델들이 가지고 있는 취약점을 분석하여 좀 더 효과적으로 QoP 지수를 산출하는 방법을 제안하였다. 이를 위해 기존[6]에 제안되었던 효용함수에 [5]에서는 $HVM(S)$에 기반을 둔 안전성을 추가하여 각각의 보안 프로토콜들에 대하여 제공되는 기능 및 과거의 경향을 종합하여 판단할 수 있는 기준을 제공하였다. 그리고 $HVM(S)$을 효율적으로 적용시키기 위해 본 논문에서는 흐름 기반의 비정상 트래픽 탐지 알고리즘을 통해 보안 네트워크의 안전을 위협하는 공격을 탐지하는 객관적인 기준을 정하였으며, 이 기준들을 통해 취약성 등급을 나누고 $HVM(S)$의 계산에 적용함으로써 $HVM(S)$가 객관적인 기준을 통해 계산이 가능하게 되었다. 결국 이를 통해 안전성이 객관적인 기준을 바탕으로 하여 평가되도록 하였다. 그리고 총이익함수에는 각각의 보안 평가 항목들에 대해 상대적 가중치(relative weight)를 적용함으로써 각 보안 네트워크의 사용 목적에 따른 보안정책이 이전의 연구보다 적절히 평가할 수 있도록 하였다.

하지만, 본 논문에서 제시된 방법이 효과적으로 적용되기 위해서는 각각의 보안 프로토콜들이 사용되는 보안 네트워크에 대하여 지속적으로 취약성을 분석하는 작업이 필요하다. $HVM(S)$에 기반을 둔 안전성이 과거의 경향을 반영한다는 성질에 의해, 현재의 상황은 바로 가까운 미래에 대한 평가 기준이 될 수 있기 때문이다. 그렇지만, 지속적인 보안 네트워크의 감시는 시스템의 성능에 영향을 미칠 수 있기 때문에, 시스템의 성능에 최소한의 영향을 미치면서 취약성 분석에 대해서는 극대의 효과를 얻을 수 있는 방법에 대한 추가적인 연구가 필요하다. 또한, 본 논문에서 흐름 기반의 비정상 트래픽 탐지 알고리즘을 도입함으로써 보안 네트워크의 공격 탐지에 객관적인 기준을 부여하였지만, 각종 공격 기법들이 나날이 발전하고 있기 때문에 지속적으로 각종 공격기법들을 분석하고, 이를 비정상 트래픽 탐지 알고리즘의 공격 분류 기준에 추가하여 보안 네트워크의 안전성이 좀 더 효율적으로 분석될 수 있도록 하는 작업도 요구된다.

또한, 본 논문에서는 총이익함수의 계산에 상대적 가중치(relative weight)의 개념을 도입하였는데, 여기에 대해서도 각각의 네트워크 특성에 맞는 가중치를 적절히 주는 방법에 대해서도 충분히 연구가 되어야 할 것이다.

그리고 본 논문에서는 QoP모델을 무선랜 부분에 중점을 두어 분석을 하였는데, 본 논문에서 제시된 QoP모델이 더욱 효과적으로 이용되기 위해서는 무선랜(WLAN) 뿐만 아니라, 휴대 인터넷(WiBro), WCDMA(3GPP)등에도 적용을 하여 분석을 하는 작업이 요구된다.

참고문헌

[1] IEEE 802.1x, “IEEE Standard for Local and Metropolitan area networks-Port-Based Network Access Control,” 2001

[2] IEEE Standard 802.11i, “Wireless LAN Medium Access Control and Physical Layer specification: Medium Access Control (MAC) Security Enhancements,” July. 2004.

[3] Avesh K. Agarwal and Wenye Wang, “On the Impact of Quality of Protection in Wireless Local Area Networks with IP Mobility,” Springer Mobile Network Application, Vol. 12, pp. 93-110, November 2006.

[4] Muhammad Abedin and Syeda Nessa and Ehab Al-Shaer and Latifur Khan, “Vulnerability Analysis For Evaluating Quality of Protection of Security Policies,” In: QoP'06, Alexandria, Virginia, USA, 30 October 2006.

[5] 김현승, 임선희, 윤승환, 이옥연, 임종인, “무선 네트워크 환경에서의 효과적인 Quality of Protection (QoP) 평가,” In: CISC W'07 PROCEEDINGS, Seoul, KOREA, pp 651-654, 1 December, 2007.

[6] Myung-Sup Kim, Hun-Jeong Kang, Seong-Cheol Hong, Seung-Hwa Chung, and James W. Hong, “A Flow-based Method for Abnormal Network Traffic Detection”

[7] Hannikainen M and Damalainen TD and Niemi M and Saarinen J, “Trend in personal wireless

data communications," Comput Commun 25(1): 84-99, 2002

[8] Karygiannis T and Owens L, "Wireless network security 802.11, bluetooth and handheld devices," National Institute of Technology, Special Publication, pp 800- 848, November 2002.

[9] Borisov N and Goldberg I and Wagner D, "Intercepting mobile communications: the insecurity of 802.11," In: Proc of the ACM MobiCom'01, ACM, New York, pp 180-189, July 2001.

[10] Ong CS and Nahrstedt K and Yuan W, "Quality of protection for mobile multimedia applications," In: Proceedings of the international conference on multimedia and expo (ICME)'03, vol 2, pp. 137-40. Baltimore, Maryland, 6-9 July 2003.

<著者紹介>

김 현 승 (Hyeon-Seung Kim) 정회원
2006년 8월: 서울대학교 수리과학부 졸업
2007년 3월~현재: 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 정보보호, 무선통신, 보안 정량화

임 선 희 (Sun-Hee Lim) 정회원
1999년 2월: 고려대학교 컴퓨터학과 졸업
2005년 2월: 고려대학교 정보보호대학원 석사
2005년 3월~현재: 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 무선통신, 정보보호

윤 승 환 (Seunghwan Yun) 학생회원
2005년 2월: 국민대학교 수학과 졸업
2007년 2월: 국민대학교 수학과 석사
2007년 3월~현재: 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 무선통신, 정보보호

이 옥 연 (Okyeon Yi) 종신회원
1988년 2월: 고려대학교 수학과 졸업
1990년 2월: 고려대학교 이학석사
1996년 8월: Univ. of Kentucky Ph.D
1999년~2001년: ETRI 선임연구원
2001년~현재: 국민대학교 수학과 부교수
<관심분야> 이동통신 정보보호, 컴퓨터 보안

임 종 인 (Jongin Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 8월: 고려대학교 수학과 박사
1986~1999년: 고려대학교 수학과 교수
2000년~현재: 고려대학교 정보경영공학전문대학원 원장
<관심분야> 정보보호, 암호이론, 프로토콜, 정보이론